MAXIMAL CONTROLLERS FOR HYBRID SYSTEMS WITH MULTIPLE TIME EVENT SEPARATIONS

by

Andrea Balluchi, Luca Benvenuti, Tiziano Villa,
Howard Wong-Toi and Alberto L. Sangiovanni-Vincentelli

Memorandum No. UCB/ERL M03/8

11 April 2003

MAXIMAL CONTROLLERS FOR HYBRID SYSTEMS WITH MULTIPLE TIME EVENT SEPARATIONS

by

Andrea Balluchi, Luca Benvenuti, Tiziano Villa,
Howard Wong-Toi and Alberto L. Sangiovanni-Vincentelli

Memorandum No. UCB/ERL M03/8

11 April 2003

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley

Maximal Controllers for Hybrid Systems with Multiple Time Event Separations

Andrea Balluchi[§] Luca Benvenuti[¶] Tiziano Villa[§,¶¶*] Howard Wong-Toi[†]
Alberto L. Sangiovanni-Vincentelli[§‡]

April 11, 2003

Abstract

A systematic procedure for synthesizing all full-state feedback controllers for a hybrid system subject to a safety (state-invariance) specification has been proposed in the literature. The interaction between the controller and a nondeterministic hybrid plant is viewed as a two-person game. The controller wins if it keeps the state of the closed-loop system within a specified set of good states; its adversarial environment tries to force the system outside the good set. The synthesis procedure iteratively augments the set of states from which the environment wins via either one additional discrete step, or one additional continuous flow. The key difficulty in carrying out the synthesis procedure lies in the computations for continuous flows. One must essentially solve a differential game in which the environment is trying to drive the system into its target set at the same time as avoiding the target set of the controller.

In this paper, we study hybrid systems with lower bounds on the separation between occurrence times of consecutive discrete moves. These systems arise when modeling minimal delay times between events, either in the controller, or in the environment. For such systems, we provide techniques for solving the differential games in reduced state spaces. The main idea is to discretize information about whether discrete moves are enabled or not.

We demonstrate our technique by successfully synthesizing the maximal set of controllers for a hybrid model of a heating system with discrete controls and disturbances, and continuous controls and disturbances.

*Corresponding author.

§ PARADES, Via di S.Pantaleo, 66, 00186 Roma, Italy. Tel: +39 06 6880-7923; Fax: +39 06 6880-7926; Email: {lucab, balluchi, villa, alberto}@parades.rm.cnr.it.

¶ Dipartimento Informatica e Sistemistica, Università di Roma "La Sapienza", Via Eudossiana 18, 00184 Roma, Italy Tel: +39 06 44585-973; Fax: +39 06 44585-367; Email: luca.benvenuti@uniroma1.it.

¶¶ Dipartimento di Ingegneria Elettronica, Gestionale e Meccanica, Università di Udine. Tel: +39 0432 55-8245 Fax: +39 0432 55-8251; Email: villa@uniud.it.

† Cadence Berkeley Labs, 2001 Addison St., Third Floor, Berkeley, CA 94704, USA. Tel: +1 510 647-2829; Fax: +1 510 486-0205; Email: howard@cadence.com.

‡ Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720, USA. Tel: +1 510 642-1792; Fax: +1 510 643-5052; Email: alberto@eecs.berkeley.edu.

1 Introduction

A systematic procedure for synthesizing all full-state feedback controllers for a hybrid system subject to a *safety* specification has been proposed in [TLS98, LTS99]. A safety specification is a state-invariance property, and specifies a set of good states within which the closed-loop system must remain. The interaction between the controller and a nondeterministic hybrid plant is viewed as a two-person zero-sum game. Each player moves by setting both discrete and continuous control inputs. The controller wins if it keeps the state of the system within a specified set of good states; its adversarial environment tries to force the system outside the good set.

The synthesis procedure iteratively augments the set of states from which the environment wins via either one additional discrete step, or one additional continuous flow. At the k-th iteration of the procedure, we have determined the set W_k of *k-winning* states, namely those states from which the environment wins the game within k discrete steps, interspersed with continuous flows. At the $(k+1)$st iteration, one first computes the states W' from which the environment can win within one additional discrete step. This computation can be performed using case analysis. Then one must solve a dynamic differential game to find those states from which the environment can force the system into $W_k \cup W'$ via a continuous flow. Thus the environment steers the system toward $W_k \cup W'$, while the controller attempts to thwart it by using its continuous input values to either keep the system trajectories away from $W_k \cup W'$ indefinitely, or to steer toward a state from which it can initiate a discrete jump into the complement of $W_k \cup W'$ (i.e., to "escape" from the environment's intended trajectory toward $W_k \cup W'$).

The key difficulty in carrying out the synthesis procedure lies in the computation for continuous flows. While the necessary calculations can be performed manually in some cases [TLS98, LTS99], they quickly become complicated in even low-dimensional linear systems [BBV+99]. One approach to this problem is to solve the dynamic game using numerical computation for solving partial differential equations [TLS99].

In this paper, we advocate a different approach. We present techniques to exploit the structure of the closed-loop system while performing the computational step for continuous flows. Our method applies to systems where there is a lower bound on the delay time between each player's discrete moves. Such systems can model communication or computational delays that prevent a player from making distinct discrete actions in quick succession. Indeed the placement of such delay constraints is often used to prevent the synthesis of Zeno controllers which satisfy the safety property only by virtue of enforcing infinitely many events in finite time. The idea we pursue is to avoid solving a single complicated dynamic game, instead breaking it into a number of simpler dynamic games played over lower dimensions.

We present methods for each of two different classes of systems. The first class that we consider—1-bounded systems— are hybrid systems with global lower bounds on event separations. In these systems, the difference between the occurrence times of all consecutive discrete moves in the closed-loop system is bounded below by some fixed constant Δ. Thus if the controller makes a discrete action at time T, then it cannot make another discrete action until at least time $T + \Delta$. However, it is also the case that the environment cannot take any discrete action before time $T + \Delta$ either. Thus the timing constraint couples the discrete moves of the controller and the environment. Class A systems occur most naturally when the controller is hybrid with lower-bounded separations between discrete actions and the plant is purely continuous (in this case, the only discrete actions originate in the controller). For 1-bounded systems, a single timer variable t is used to enforce the lower bound on event separation times. Every time a discrete action takes place, the timer is reset

to $-\Delta$, and the next discrete event cannot occur until the timer value is greater than or equal to 0.

We show how it is not necessary to solve a differential game over a state space that includes the timer variable, but rather that it suffices to solve games in a reduced state space without the timer variable. In the reduced state space, we record only discrete information related to the value of the timer, namely whether it is equal to $-\Delta$ and whether it is greater than or equal to 0. An intuitive justification follows. Once the timer is positive, its value is irrelevant: we need only note the fact that the timing delay between discrete events has been met. We need to know which states with $t_c = -\Delta$ are winning or losing, since this information is required to compute states that are winning via discrete moves. Given the set of states with $t_c \geq 0$ that are winning for the environment, one can find the states that are winning for the environment with $t_c = -\Delta$ via a continuous flow by solving a time-bounded game over the reduced state space.

The second class of systems we consider—2-bounded systems—have lower bounds on the separation times between consecutive discrete *controller* actions, and also lower bounds on the separation times between consecutive discrete *environment* actions. The two lower bounds are independent, with the occurrence times of discrete controller actions not placing any restrictions on the occurrence times of the discrete environment actions, and vice versa. Thus 2-bounded systems naturally model the coupling of a hybrid plant with a hybrid controller. A hybrid automaton model for a 2-bounded system would include two timers, one each for enforcing the lower bound properties for the discrete moves of the controller and of the environment. We show how the differential games that arise in the synthesis procedure can be solved by considering a set of simpler games over states spaces that drop one or both of the timer variables. The technique used is a generalization of that for 1-bounded systems. The extension of the previous technique to systems that require more than 2 timers to enforce event separation—k-bounded systems—is sketched in Sec. 5.

The practicality of our approach is demonstrated on a heating system for a room that is first studied in [BBV+99]. The controller has at its disposal both discrete and continuous inputs for operating a stove and a boiler. Its adversarial environment also has both discrete and continuous inputs, modeling the opening and closing a door and the nondeterministic disturbance of heat generated by electrical appliances in the room. Controller computations cause a delay of at least a time delay Δ between decisions to turn on and off the stove. In the environment, there is a delay of at least a time delay 2 Δ between opening and closing of the door. It is a 2-bounded system. Our initial attempts to synthesize controllers using the procedure as expressed in [TLS98] turned out to be highly impractical due to the complicated differential games to be solved.

Here, we first apply our approach to a simplified form of the heating system, where only a single timer appears. This corresponds to a 1-bounded system. Our method enables a simpler controller derivation for this simplified case than the original synthesis procedure, which, for completeness, appear in the appendix of this paper. Furthermore, we are also able to complete the synthesis procedure for the more complicated 2-bounded system, where the original technique presented in [TLS98] failed, by using our reduction techniques.

2 Background: synthesis of maximal controllers

We briefly review the synthesis procedure outlined by Tomlin, Lygeros, and Sastry [TLS98, LTS99] as it applies to our variant of the hybrid automaton model [BBV+99].

2.1 Hybrid Automata

A diagram depicting the plant with its input/output terminals appears in Figure 1. We model the system as a hybrid automaton. Intuitively, the hybrid automaton models a game board. This modeling formalism merges the game features (explicitly-defined independent moves) of [AMPS98] into the hybrid automata model (input structure and hybrid dynamics) found in [TLS98, LTS98].

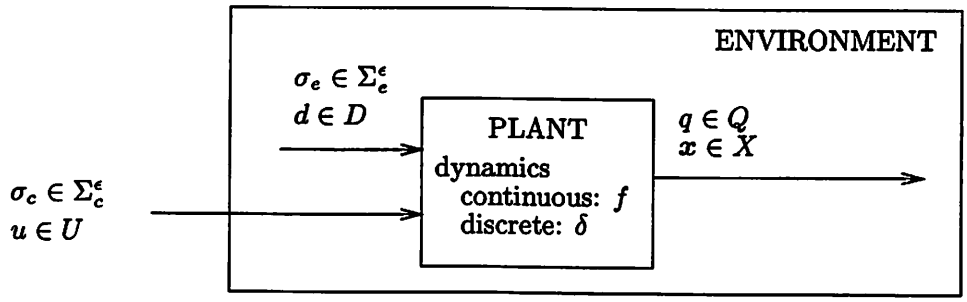


Figure 1: Open-loop hybrid automaton H

2.1.1 Syntax

Definition 2.1 *A* hybrid automaton *is a tuple* $H = ((Q, X), (U, \Sigma_c), (M_c^{cts}, M_c^{disc}), (D, \Sigma_e), (M_e^{cts}, M_e^{disc}), (f, \delta))$, *where*

State space

- Q *is the finite set of* modes *or* locations.
- X *is the set of (continuous)* states.

Control input

- $U \subseteq \mathbb{R}^m$ *is the domain of* continuous control values. $\mathcal{U} = \{u(.) \in PC^0 | u(t) \in U, \forall t \in \mathbb{R}\}$ *is the class of control functions.*
- Σ_c *is the finite domain of* discrete control events. *We define* $\Sigma_c^\epsilon = \Sigma_c \cup \{\epsilon\}$ *to be the set of* discrete control moves, *with the special* ϵ *move being the* silent *move.*
- $M_c^{disc} : Q \times X \rightarrow 2^{\Sigma_c^\epsilon} \setminus \{\}$ *is the* discrete controller feasible move function.
- $M_c^{cts} : Q \times X \rightarrow 2^U \setminus \{\}$ *is the* continuous controller feasible move function.

Disturbance input

- $D \subseteq \mathbb{R}^p$ *is the domain of* continuous disturbance values. $\mathcal{D} = \{d(.) \in PC^0 | d(t) \in D, \forall t \in \mathbb{R}\}$ *is the class of disturbance functions.*
- Σ_e *is the finite set of* discrete disturbance events. *We define* $\Sigma_e^\epsilon = \Sigma_e \cup \{\epsilon\}$ *to be the set of* discrete disturbance moves.

- $M_e^{disc} : Q \times X \to 2^{\Sigma_e^\epsilon} \setminus \{\}$ *is the* discrete disturbance feasible move function.
- $M_e^{cts} : Q \times X \to 2^D \setminus \{\}$ *is the* continuous disturbance feasible move function.

Transitions

- $f : Q \times X \times U \times D \to \mathbb{R}^n$ *models the time-invariant continuous dynamics, which depend on the mode. We assume that function f is such that, for any control function $u \in \mathcal{U}$ and any disturbance function $d \in \mathcal{D}$ and for any $x_0 \in \mathbb{R}^n$, there is a unique solution of the differential equation $\dot{x}(t) = f(q, x(t), u(t), d(t))$ (written also as $f_q(x(t), u(t), d(t))$), with initial value $x(0) = x_0$, denoted by $x(t) = \psi_q(u|_{[0,t)}, d|_{[0,t)}, x_0, t)$, $\forall t \geq 0$. Such a dynamical system is said to be* nicely complete *in [Sus83].*
- $\delta : Q \times X \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times X} \setminus \{\}$ *is the* transition function *modeling the discrete dynamics. It defines the transitions for the joint moves of the controller and the disturbance, subject to the restriction that for all $(q, x) \in Q \times X$, $\delta(q, x, \epsilon, \epsilon) = \{(q, x)\}$.*

Both the controller and the environment make their moves simultaneously. At the configuration (q, x), the controller chooses a pair (σ_c, u) out of $M_c^{disc}(q, x) \times M_c^{cts}(q, x)$. The environment does likewise, choosing a pair $(\sigma_c, d) \in M_e^{disc}(q, x) \times M_e^{cts}(q, x)$. If either of the players chooses a non-silent discrete move, then a non-trivial discrete move takes place, with label (σ_c, σ_e). The discrete transition function δ determines the effect on the system. The resultant configuration is any configuration in $\delta(q, x, \sigma_c, \sigma_e)$. As long as both players choose ϵ as their discrete move, then time may progress. In this case, the discrete mode remains fixed, and the continuous variables evolve according to the continuous control u chosen by the controller, the continuous disturbance d chosen by the environment, and the continuous dynamics specified by the function f. One may think of the interaction between the players as a continuous game with occasional discrete interruptions.

We denote by *Wait* the set of configurations in which both players may choose not to play a discrete move, but instead wait for time to pass. We define *Wait* by introducing first $Wait_c$ ($Wait_e$) the set of configurations in which the controller (the environment) may let time pass:

Definition 2.2 $Wait_c = \{(q, x) \mid \epsilon \in M_c^{disc}(q, x)\}$.

Definition 2.3 $Wait_e = \{(q, x) \mid \epsilon \in M_e^{disc}(q, x)\}$.

Definition 2.4 $Wait = Wait_c \cap Wait_e$.

The requirement that for all $(q, x) \in Q \times X$, $\delta(q, x, \epsilon, \epsilon) = \{(q, x)\}$ means that if both players agree not to make a non-trivial discrete move, there is no discrete change in configuration.

Different discrete move choices of the players can be modeled as follows. If $M_c^{disc}(q, x) = \{\epsilon\}$, then there is no "real" discrete move the controller can take; in this case, it can only let time pass. If $M_c^{disc}(q, x) = \{\sigma_c, \epsilon\}$, then it is possible either to let time pass, or to take the discrete move σ_c. If $M_c^{disc}(q, x) = \{\sigma_c\}$, then it is possible to make only the discrete move labeled σ_c, but it is not possible to let time pass (i.e., the move is forced to occur). The use of M_e^{disc} is similar.

Remark. We enforce a well-posedness condition on when time can flow. We require that for each mode q, the set $\{x \mid \epsilon \in M_c^{disc}(q, x) \wedge \epsilon \in M_e^{disc}(q, x)\}$ is an open set, so that the contradictory requirement that a flow be integrated for a null interval is never specified. Indeed, by enforcing the previous assumption the current process of integration terminates just before the time of the next

jump. Hence the flows are integrated on intervals closed on the left and open on the right. With this topological hypothesis and the fact that by construction the move functions are never empty follows that the hybrid automaton is never blocked.

2.1.2 Semantics

Hybrid automata evolve using two different kinds of behaviors: discrete and continuous. There is a *discrete step* from configuration (q, x) to configuration (q', x') if there exists a pair $(\sigma_c, \sigma_e) \in \Sigma_c^\epsilon \times \Sigma_e^\epsilon \setminus \{(\epsilon, \epsilon)\}$ such that

- $\sigma_c \in M_c^{disc}(q, x)$, $\sigma_e \in M_e^{disc}(q, x)$,
- $(q', x') \in \delta(q, x, \sigma_c, \sigma_e)$.

We explicitly exclude discrete steps labeled (ϵ, ϵ).

There is a *continuous arc of trajectory* from (q, x) to (q', x') if $q' = q$ and there exist a time $t' > 0$, a control function $u : [0, t') \to U$ and a disturbance function $d : [0, t') \to D$, such that

- $x(t') = \psi_q(t', x, u, d) = x'$,
- $(q, x(\tau)) \in Wait \quad \forall \tau \in [0, t')$

i.e., the trajectory following the dynamics at mode q subject to control u and disturbance d leads from x to x', and throughout the trajectory, both the controller and the environment are willing to let time pass, (meaning that their discrete move functions include ϵ).

A *trajectory* of the hybrid automaton is a (finite or infinite) sequence of discrete steps and continuous arcs of trajectories.

A *safety property* asserts that nothing bad happens along trajectories. It can be characterized by the set *Good* of good configurations that do not violate the property. The hybrid automaton with initial configurations $(Q \times X)_0$ satisfies the safety property *Good* if all its trajectories that start in $(Q \times X)_0$ remain within *Good*.

2.2 Synthesis of hybrid feedback memory-less controllers

We review the synthesis methodology introduced in [TLS98]. The design of a controller proceeds in two steps. In the first part of the procedure, the maximal safe set W is computed. By construction, from any configuration $q \in W$, the controller has a strategy to keep the system forever in W. In the second part of the synthesis procedure, the control strategy is explicitly extracted from W.

2.2.1 Controllers

A controller watches the entire state of the system at all times, and decides whether to (1) take discrete control actions that may cause an instantaneous change in the configuration, or to (2) let time pass under a continuous input u with the continuous variables evolving according to dynamics at the current mode.

Definition 2.5 *A feedback memory-less controller for a hybrid automaton is a pair* $C = (T^{disc}, T^{cts})$, *where* $T^{disc} : Q \times X \to 2^{\Sigma_c^\epsilon} \setminus \{\}$ *and* $T^{cts} : Q \times X \to 2^U \setminus \{\}$ *model the values allowed by the controller. The controller can only offer values permitted by the move functions, and hence, for all* $(q, x) \in Q \times X$, *it must hold that* $T^{disc}(q, x) \subseteq M_c^{disc}(q, x)$ *and* $T^{cts}(q, x) \subseteq M_c^{cts}(q, x)$.

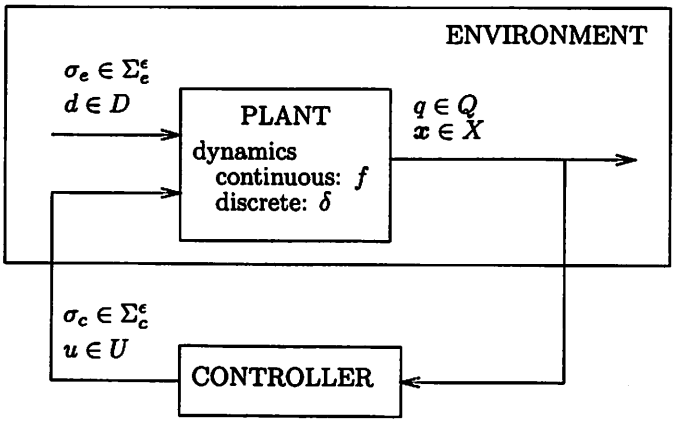


Figure 2: Closed-loop hybrid automaton H_C

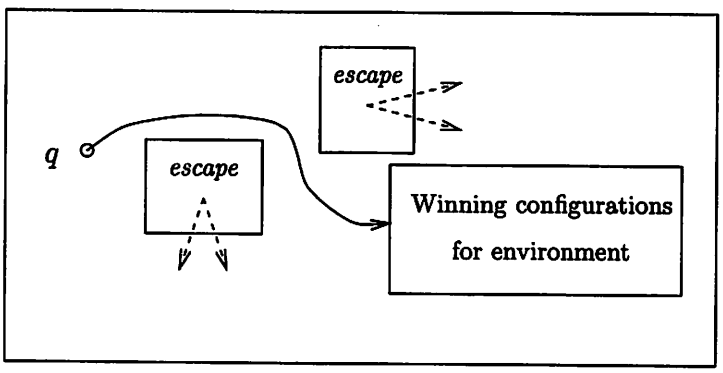


Figure 3: Continuous uncontrollable predecessor q, from which environment can cause flow around the escape regions to a known winning configuration for the environment

Definition 2.6 *The coupling of the hybrid automaton H with the full-state feedback memory-less controller $C = (T^{cts}, T^{disc})$ is the closed-loop hybrid automaton*

$$H_C = ((Q, X), (U, \Sigma_c), (T^{cts}, T^{disc}), (D, \Sigma_e), (M_e^{cts}, M_e^{disc}), (f, \delta)).$$

H_C is obtained from H by replacing the discrete controller move function with T^{disc} and the continuous controller move function with T^{cts}. The controller is *safe* with respect to the specification *Good* if the closed-loop system H_C satisfies the specification *Good*. A diagram depicting the closed-loop system appears in Figure 2.

A configuration (q, x) is *safe* for the automaton H and safety specification *Good* if there exists a controller such that the closed-loop system with initial configuration (q, x) satisfies the specification. A set of configurations is a *controllable safe set* if all its configurations satisfy the specification, and from all its configurations there exists a controller strategy to remain in the set.

2.2.2 Computing maximal safe sets

The procedure to synthesize the maximal controller first computes the maximal controllable safe set [LTS98]. This maximal set is obtained by first overapproximating it with all the safe configu-

rations. Then one calculates all configurations from which the environment can drive the system into an unsafe configuration via either one discrete jump, or one continuous flow. These are the configurations from which the environment can win within one "step", and should be avoided by the controller. One iterates this computation, finding successively the configurations from which the environment can win within i steps. If the procedure terminates, we have determined the maximal controllable safe set.

Consider when the environment can win within one additional discrete step. Suppose that from a configuration q no matter what discrete move the controller may make, the environment has some discrete move such that the system is taken into a known winning configuration for the environment. Then configuration q is a winning configuration for the environment.

Consider when the environment can win within one additional continuous step. Suppose that from configuration q no matter what continuous input function u the controller chooses there is a continuous disturbance function d such that the resulting continuous flow reaches a known winning configuration for the environment, avoiding along the way all configurations where the controller could "escape" by causing a discrete move to a non-winning configuration for the environment. Then q is a winning configuration for the environment. See Figure 3.

We define the necessary predecessor operators required to capture these notions.

2.2.3 Discrete predecessor operators

The *discrete uncontrollable predecessors* operator $Pre_e : 2^{(Q\times X)} \rightarrow 2^{(Q\times X)}$ is defined as follows:

$$Pre_e(K, M_c^{disc}, M_e^{disc}) =$$
$$\{(q,x) \in Q \times X : \forall \sigma_c \in M_c^{disc}(q,x). \exists \sigma_e \in M_e^{disc}(q,x).\ (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \wedge\ \delta(q,x,\sigma_c,\sigma_e) \not\subseteq K\}.$$

Intuitively, for a given K, $Pre_e(K, M_c^{disc}, M_e^{disc})$ is the set of configurations such that, whatever is the controller's discrete move, there is a discrete environment move that forces the configuration into $\overline{K}$ in one non-trivial discrete step. The uncontrollable action may be empty and may depend on the controllable action.

The escaping configurations [Won97, LTS98] are characterized by the *discrete controllable predecessors* operator $Pre_c : 2^{(Q\times X)} \rightarrow 2^{(Q\times X)}$, defined as follows:

$$Pre_c(K, M_c^{disc}, M_e^{disc}) =$$
$$\{(q,x) \in Q \times X : \exists \sigma_c \in M_c^{disc}(q,x). \forall \sigma_e \in M_e^{disc}(q,x).\ (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \wedge \delta(q,x,\sigma_c,\sigma_e) \subseteq K\}.$$

Intuitively, for a given K, $Pre_c(K, M_c^{disc}, M_e^{disc})$ is the set of configurations that can be forced into K in one non-trivial discrete step, regardless of what discrete move the environment chooses to take. The controllable action may be empty, as long as $\epsilon \notin M_e^{disc}(q,x)$.

Notice that we introduced as arguments in Pre_e and Pre_c the sets M_c^{disc} and M_e^{disc}, because we will describe formulas in which the operators Pre_e and Pre_c act contextually on different hybrid automata and so the move functions will have to be annoted explicitly. When obvious from the context, the arguments M_c^{disc} and M_e^{disc} may be dropped.

2.2.4 Continuous uncontrollable predecessors

The configurations that the environment can force into a set in one continuous step are characterized by the continuous uncontrollable predecessor operator $Unavoid\_Pre : 2^{(Q\times X)} \times 2^{(Q\times X)} \rightarrow 2^{(Q\times X)}$,

$W^0 := Good$
$i := -1$
repeat {
$i := i + 1$
$W^{i+1} := W^i \setminus [Pre_e(W^i) \cup Unavoid\_Pre(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i))]$
} until $(W^{i+1} = W^i)$
$Safe := W^i$

Figure 4: Computation of Maximal Safe Set [TLS98].

defined below. The operator takes two arguments. The first is the set of configurations the environment is trying to reach, and the second is a set it must avoid.

$$\begin{aligned} Unavoid\_Pre(B, E) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists \bar{t} > 0\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & \quad (q, x(\bar{t})) \in B\} \\ & \quad \forall \tau \in [0, \bar{t})\ [u(\tau) \in M_c^{cts}(q, x(\tau)) \wedge d(\tau) \in M_e^{cts}(q, x(\tau)) \wedge (q, x(\tau)) \in Wait \cap \overline{E}] \end{aligned} \tag{1}$$

where *Wait* is the set of configurations in which both players may choose not to play a discrete move, but instead wait for time to pass, see definition 2.4.

2.2.5 Main synthesis procedure

Figure 4 shows the fixed-point computation to obtain the maximal safe set. The procedure successively prunes away configurations that are found to be losing upon one additional discrete step ($Pre_e(W^i)$), or a continuous step to a losing configuration ($Unavoid\_Pre(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i))$). It is not guaranteed to stop within a finite number of steps.

2.3 Controller extraction

Extracting the maximal control strategy from the maximal safe set W amounts to determining for every configuration in W, which control choices will keep the system in W. The available control choices either (1) force a discrete control action, or (2) allow time to pass. In case (1), the value of u is irrelevant, since a discrete jump will occur. In case (2), we must ensure that the choice for the input control vector u is such that, in the event that the environment also lets time pass, the ensuing continuous flow will keep the configuration in W.

The control strategy (T^{disc}, T^{cts}) derived from W is defined by the following three rules:

1. For all $s = (q, x) \in Q \times X$, we set $T^{disc}(s) = M_c^{disc}(s)$ if $s \notin W$, and otherwise:
   - For all $\sigma_0 \in \Sigma_0$, we have $\sigma_0 \in T^{disc}(s)$ iff $\sigma_0 \in M_c^{disc}(s)$ and for all $\sigma_1 \in M_e^{disc}(s)$, $\delta(q, x, \sigma_0, \sigma_1) \subseteq W$.

- We have $\epsilon \in T^{disc}(s)$ iff there exists a $u \in M_c^{cts}(s)$ such that for all $d \in M_e^{cts}(s)$, the vector $f(q,x,u,d)$ is tangential to or points into W at (q,x). More formally, for a set $A \subseteq Q \times X$, let $A_q \subseteq \mathbb{R}^n$ be the set $\{y \mid (q,y) \in A\}$. Let $h_q : \mathbb{R}^n \to \mathbb{R}$ be a function that is 0 precisely on the surface of A_q and has normal pointing out of A_q. Let the *inward tangent space* of A at (q,x) be the set $\{y \in \mathbb{R}^n \mid y.\frac{\partial h_q}{\partial y}(x) \leq 0\}$. Then we require that for all disturbances $d \in M_e^{cts}(s)$, the vector $f(q,x,u,d)$ lies in the inward tangent space of W.

2. For all $s = (q,x) \in Q \times X$, we set $T^{cts}(s) = M_c^{cts}(s)$ if $s \notin W$ or $\epsilon \notin T^{disc}(s)$, and otherwise for all $u \in U$, we have $u \in T^{cts}(s)$ iff the following two conditions hold:
   (a) $u \in M_c^{cts}(s)$.
   (b) For all disturbances $d \in M_e^{cts}(s)$, the vector $f(q,x,u,d)$ is in the inward tangent space of W at (q,x).

The allowable control values u are often easily obtained from the calculations used in computing the *Unavoid_Pre* operator. For a configuration (q,x), where the state x is on the interior of W_q, whenever there is some $(\epsilon,u') \in g_W(q)$, then $(\epsilon,u) \in g_W(q)$ for all u.

3 Controller synthesis with a lower bound on event separation enforced by one timer

When designing a hybrid system, we may have to guarantee that there is always a delay of at least Δ time units between pairs of consecutive discrete events (e.g., to ensure nonZenoness). This lower bound can be enforced by introducing a timer t_c (a timer is a continuous variable with rate of increment $\dot{t_c} = 1$). Events are enabled when $t_c \geq 0$ and jumps reset the timer to $t_c = -\Delta$, so that no discrete event is allowed in the interval $-\Delta < t_c < 0$. We could apply the synthesis procedure of Fig. 4 to the hybrid system augmented with variable t_c. However, our previous experience with a heating system shows that the addition of a variable can complicate reasoning about the dynamics of the system substantially [BBV+99]. It would be convenient to apply the synthesis procedure to the hybrid system without variable t_c. In this section we develop a revised synthesis procedure where only the variables in the original state space need to be stored, instead of working in the extended space $\tilde{X} = (X, t_c)$.

The intuitive idea is that since there is only *one* timer t_c, information about its value can be discretized into the two parts: $t_c = -\Delta$ and $t_c \geq 0$, and the continuous computations over the extended $(n+1)$-dimensional state space $\tilde{X}$ can be replaced with time-bounded computations over the reduced n-dimensional space X. In other words, it does not matter what the specific timer value is, because (1) if $t_c \geq 0$, then it suffices to know that a discrete jump is enabled, whereas the specific value of t_c does not matter; (2) if $-\Delta < t_c < 0$, we should memorize the value of t_c, but since t_c after a jump is always reset to $-\Delta$, the value of t_c can be determined by knowing the integration time. Thus we can move between the two separated parts for $t_c = -\Delta$ and $t_c \geq 0$ by integrating between them for a fixed time Δ.

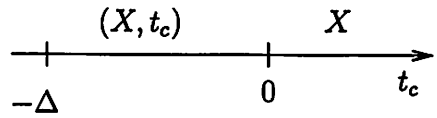


Figure 5: Structure of dependencies for 1-bounded systems

3.1 Extension of hybrid automaton with one timer

Let $\tilde{H} = ((Q, \tilde{X}), (U, \Sigma_c), (\tilde{M}_c^{cts}, \tilde{M}_c^{disc}), (D, \Sigma_e), (\tilde{M}_e^{cts}, \tilde{M}_e^{disc}), (\tilde{f}, \tilde{\delta}))$, be the hybrid automaton obtained extending the hybrid automaton H with one timer t_c.

State space

- $\tilde{X} = X \times \mathbb{R}$

Control input

- $\tilde{M}_c^{disc} : Q \times \tilde{X} \to 2^{\Sigma_c^\epsilon} \setminus \{\}$ is defined as $\tilde{M}_c^{disc}(q, (x, t_c)) = \begin{cases} \{\epsilon\} & -\Delta \le t_c < 0 \\ M_c^{disc}(q, x) & t_c \ge 0 \end{cases}$
- $\tilde{M}_c^{cts} : Q \times \tilde{X} \to 2^U \setminus \{\}$ is defined as $\tilde{M}_c^{cts}(q, (x, t_c)) = M_c^{cts}(q, x) \quad \forall t_c$

Disturbance input

- $\tilde{M}_e^{disc} : Q \times \tilde{X} \to 2^{\Sigma_e^\epsilon} \setminus \{\}$ is defined as $\tilde{M}_e^{disc}(q, (x, t_c)) = \begin{cases} \{\epsilon\} & -\Delta \le t_c < 0 \\ M_e^{disc}(q, x) & t_c \ge 0 \end{cases}$
- $\tilde{M}_e^{cts} : Q \times \tilde{X} \to 2^D \setminus \{\}$ is defined as $\tilde{M}_e^{cts}(q, (x, t_c)) = M_e^{cts}(q, x) \quad \forall t_c$

Transitions

- $\tilde{f} : Q \times \tilde{X} \times U \times D \to \mathbb{R}^{n+1}$ are such that at each mode the same flows as in f apply, together with the flow $\dot{t}_c = 1$.
- $\tilde{\delta} : Q \times \tilde{X} \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times \tilde{X}} \setminus \{\}$ is defined as

$$\tilde{\delta}(q, (x, t_c), \sigma_c, \sigma_e) = \begin{cases} (q, x, t_c) & -\Delta \le t_c < 0 \\ (q, x, t_c) & t_c \ge 0 \ \wedge \ (\sigma_c, \sigma_e) = (\epsilon, \epsilon) \\ \delta(q, x, \sigma_c, \sigma_e) \times \{-\Delta\} & t_c \ge 0 \ \wedge \ (\sigma_c, \sigma_e) \ne (\epsilon, \epsilon) \end{cases}$$

- $\widetilde{Wait} = Q \times X \times [-\Delta, 0) \cup Wait \times [0, \infty)$

3.2 Timer-reduced sets

The basis of our simplified view of the calculations for continuous flows is that the value of the timer is irrelevant once it has exceeded 0, i.e., the lower bound on the timing delay between discrete events has been satisfied already, and the value of the timer is no longer needed.

Figure 5 depicts a cross-section of the continuous state space projected onto the timer state space. The figure indicates the variables that intuitively are relevant at each section of the projection. For instance, in the right region where $t_c \ge 0$, it suffices to know the value of X in order to

determine the future evolution of the system: the timer value is not relevant, since the lower bound on event separations has passed. This diagram motivates the following definition.

A set $G \subseteq \Pi_{j=1..k} Y_j$ for domains Y_j is *independent* of the variable y_i having domain Y_i if for all $j \neq i$, $y_j \in Y_j$ implies that for all $y', y'' \in Y_i$, we have $(y_1, \ldots, y_{i-1}, y', y_{i+1}, \ldots, y_k) \in G$ iff $(y_1, \ldots, y_{i-1}, y'', y_{i+1}, \ldots, y_k) \in G$. In other words, membership of a point in G can be determined independently of the value of y_i.

Definition 3.1 *A set $G \subseteq \tilde{X}$ is* timer-reduced *if the set G restricted to the domain where $t_c \geq 0$ is independent of t_c.*

The set $W \subseteq Q \times \tilde{X}$ of configurations is *timer-reduced* if for every mode $q \in Q$, the set $\{\tilde{x} \in \tilde{X} \mid (q, \tilde{x}) \in W\}$ is timer-reduced.

We use the values of the timers to partition the state space $\tilde{X}$ into subsets as follows: $\tilde{X} = \tilde{X}_- \cup \tilde{X}_+$. The subscript refers to the value of t_c, with "$-$" indicating the range $[-\Delta, 0)$ and "$+$" indicating the range $[0, \infty)$ and the sets are defined explicitly below:

1. $\tilde{X}_- = \{\tilde{x} \in \tilde{X} \mid t_c \in [-\Delta, 0)\}$.
2. $\tilde{X}_+ = \{\tilde{x} \in \tilde{X} \mid t_c \in [0, \infty)\}$.

The set $Pre_c(W)$ is disjoint from the region $t_c < 0$.

Lemma 3.1 *The set $Pre_c(W)$ is timer-reduced.*

Lemma 3.2 *The set $Pre_e(W)$ is timer-reduced.*

Lemma 3.3 *Given timer-reduced sets B and E of configurations, the set Unavoid_Pre(B, E) is timer-reduced.*

Lemma 3.4 *If the specification Good is timer-reduced, then the set Safe and also every set W^i computed in the synthesis procedure of Figure 4 is timer-reduced.*

The proofs of Lemmas 3.1, 3.2, 3.3, and 3.4 are reported in Appendix.

3.3 Projections of maximal safe set computations

In Sec. 3.2, we proved that the sets Pre_c, Pre_e, *Unavoid_Pre* preserve "strips", i.e., the independence from t_c, when $t_c \geq 0$. For easier algebra, it is convenient to introduce the following projections operators, where $W \subseteq Q \times \tilde{X}$ is a set of configurations:

1. $R_{(-\Delta)} : Q \times \tilde{X} \to Q \times X$ is such that $R_{(-\Delta)}(W) = \{(q, x) \in Q \times X | (q, x, -\Delta) \in W\}$, and
2. $R_{(0)} : Q \times \tilde{X} \to Q \times X$ is such that $R_{(0)}(W) = \{(q, x) \in Q \times X | (q, x, 0) \in W\}$.

Notice that if W is timer-reduced, then

$$R_{(0)}(W) \times [0, \infty) = W \cap [Q \times X \times [0, \infty)].$$

Let us find out how the operators to compute the uncontrollable predecessors evaluate under projection at $t_c = -\Delta$ and $t_c \geq 0$. In fact, it will be shown that the computation of the safe set can be carried out using only the projections of the sets W for $t_c = -\Delta$ and $t_c \geq 0$.

We study first the operators Pre_c and Pre_e.

Lemma 3.5

$$
\begin{aligned}
R_{(0)}(Pre_c(W, \tilde{M}_c^{disc}, \tilde{M}_e^{disc})) &= Pre_c(R_{(-\Delta)}(W), M_c^{disc}, M_e^{disc}), \\
R_{(0)}(Pre_e(W, \tilde{M}_c^{disc}, \tilde{M}_e^{disc})) &= Pre_e(R_{(-\Delta)}(W), M_c^{disc}, M_e^{disc}), \\
Pre_c(W, \tilde{M}_c^{disc}, \tilde{M}_e^{disc}) \cap [X \times (-\infty, 0)] &= \emptyset, \\
Pre_e(W, \tilde{M}_c^{disc}, \tilde{M}_e^{disc}) \cap [X \times (-\infty, 0)] &= \emptyset,
\end{aligned}
$$

From the two latter identities follow the special cases:

$$
\begin{aligned}
R_{(-\Delta)}(Pre_c(W, \tilde{M}_c^{disc}, \tilde{M}_e^{disc})) &= \emptyset, \\
R_{(-\Delta)}(Pre_e(W, \tilde{M}_c^{disc}, \tilde{M}_e^{disc})) &= \emptyset.
\end{aligned}
$$

The proof is reported in Appendix. The projections of the set $Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))$ for $t_c = -\Delta$ and $t_c \geq 0$ are obtained considering that the effect of *Unavoid_Pre* for $W \subseteq Q \times \tilde{X}$ is accounted for by the contributions of the following cases:

1. the configurations that starting from $t_c \geq 0$ unavoidably lose at $t_c \geq 0$,
2. the configurations that starting from $t_c = -\Delta$
   (a) unavoidably lose at $-\Delta < t_c < 0$,
   (b) unavoidably lose at $t_c = 0$ (after a fixed integration time Δ),
   (c) unavoidably lose at $t_c > 0$.

The configurations defined by case 1. are handled by the following

Lemma 3.6

$$
\begin{aligned}
&R_{(0)}(Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))) = \\
&\qquad Unavoid\_Pre(Pre_e(R_{(-\Delta)}(W)) \cup R_{(0)}(\overline{W}), Pre_c(R_{(-\Delta)}(W))) \ .
\end{aligned}
$$

Proof. The proof is reported in Appendix. □

While, the configurations defined by case 2. are handled by the following

Lemma 3.7 *If W is timer-reduced, then*

$$
\begin{aligned}
&R_{(-\Delta)}(Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))) = \qquad (3) \\
&\{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U} \ \exists \ \bar{t} \in (0, \Delta] \ \exists d \in \mathcal{D} \text{ such that} \\
&\quad \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \text{ we have} \\
&\qquad (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W} \ \wedge \ \bar{t} < \Delta \ \vee \\
&\qquad (q, x(\Delta)) \in R_{(0)}(\overline{W \setminus (Pre_e(W) \cup Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W)))}) \ \wedge \ \bar{t} = \Delta\}.
\end{aligned}
$$

Proof. The proof is reported in Appendix. □

Condition $(q, x(\bar{t}), -\Delta + t) \in \overline{W}$ on the right hand side of Eq. 3 collects the configurations defined by case 2.a, while condition $(q, x(\Delta)) \in R_{(0)}((Pre_e(W) \cup \overline{W}) \cup Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W)))$ collects those defined by case 2.b and case 2.c. In particular the term $Pre_e(W) \cup \overline{W}$ in $R_{(0)}(\cdot)$ is

related to case 2.b, and the term $Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))$ to case 2.c. Then, according to Eq. 3, we introduce the following operator

$$\begin{aligned} Unavoid\_Pre_{(-\Delta,0]}(B_G, B) \;=\; \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\, \bar{t} \in (0,\Delta]\ \exists d \in \mathcal{D} \text{ such that} \\ \text{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \text{ we have} \\ (q, x(\bar{t})) \in B_G \wedge \bar{t} < \Delta \vee \\ (q, x(\bar{t})) \in B \wedge \bar{t} = \Delta\}\,. \end{aligned} \tag{4}$$

It will be shown that, except for the first step of the procedure, the above operator can be simplified to the following one which considers only trajectories $\psi_q(u,d,\hat{x},t)$ on the time interval $[0,\Delta]$:

$$\begin{aligned} Unavoid\_Pre_{-\Delta}(B) \;=\; \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D} \text{ such that} \\ \text{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \text{ we have} \\ (q, x(\Delta)) \in B\}\,. \end{aligned} \tag{5}$$

Based on the operators previously defined, we are now able to devise a procedure for the computation of the maximal safe set when a lower bound on event separation is introduced.

Such procedure computes the projections $Safe_{-\Delta} \subset Q \times X$, for $t_c = -\Delta$, and $Safe_0 \subset Q \times X$, for $t_c = 0$, of the maximal safe set $Safe \subset Q \times (X \times R)$ for the hybrid automaton $\tilde{H}$. The proposed procedure makes use of the definitions of the original hybrid automaton H and proceeds computing intermediate sets $W_0^i \subset Q \times X$, $W_{-\Delta}^i \subset Q \times X$ related respectively to $t_c = -\Delta$ and $t_c = 0$.

Figure 6 shows the fixed-point computation with timer projection to obtain the maximal safe set.

The correctness of the proposed procedure is proved by the fact that the sets $Safe_{-\Delta}$ and $Safe_0$ computed according to the procedure reported in Figure 6 are equal to the projection of the maximal safe set $Safe$ for the hybrid automaton $\tilde{H}$ computed by the procedure reported in Figure 4.

Theorem 3.1 *The sets W_0^i, $W_{-\Delta}^i$ computed by the procedure in Fig. 6 are the projections, respectively, for $t_c \geq 0$ and $t_c = -\Delta$ of the sets W^i computed by the procedure in Fig. 4 initialized with set of good configurations $W^0 = Good \times \mathbb{R}$, i.e.,*

$$\begin{aligned} W_0^i &= R_{(0)}(W^i), \\ W_{-\Delta}^i &= R_{(-\Delta)}(W^i). \end{aligned}$$

In particular, the repeat cycle of the procedure in Fig. 6 converges if and only if the one of the procedure in Fig. 4 does, and if so

$$\begin{aligned} Safe_0 &= R_{(0)}(Safe), \\ Safe_{-\Delta} &= R_{(-\Delta)}(Safe). \end{aligned}$$

Proof. The two procedures are correctly initialized, namely:

$$R_{(0)}(W^0) = R_{(0)}(Good \times \mathbb{R}) = Good = W_0^0, \tag{6}$$

$$R_{(-\Delta)}(W^0) = R_{(-\Delta)}(Good \times \mathbb{R}) = Good = W_{-\Delta}^0, \tag{7}$$

since $W^0 = Good \times \mathbb{R}$.

Good assumed to be independent from t_c
$W_0^0 := Good$
$W_{-\Delta}^0 := Good$
$W_0^1 := W_0^0 \setminus [Pre_e(W_{-\Delta}^0) \cup Unavoid\_Pre(Pre_e(W_{-\Delta}^0) \cup \overline{W_0^0}, Pre_c(W_{-\Delta}^0))]$
$W_{-\Delta}^1 := W_{-\Delta}^0 \setminus Unavoid\_Pre_{(-\Delta,0]}(\overline{Good}, \overline{W_0^1})$
$i := 0$
repeat {
  $i := i + 1$
  $W_0^{i+1} := W_0^i \setminus [Pre_e(W_{-\Delta}^i) \cup Unavoid\_Pre(Pre_e(W_{-\Delta}^i) \cup \overline{W_0^i}, Pre_c(W_{-\Delta}^i))]$
  $W_{-\Delta}^{i+1} := W_{-\Delta}^i \setminus Unavoid\_Pre_{-\Delta}(\overline{W_0^{i+1}})$
} until ($W_0^{i+1} = W_0^i$ and $W_{-\Delta}^{i+1} = W_{-\Delta}^i$)
$Safe_0 := W_0^i$
$Safe_{-\Delta} := W_{-\Delta}^i$

Figure 6: Computation of Maximal Safe Set with Projection of 1 Timer.

The proof proceeds by induction on the index of iteration i for $i \geq 2$. First, we show that $R_{(0)}(W^1) = W_0^1$ and $R_{(-\Delta)}(W^1) = W_{-\Delta}^1$.

According to the procedure in Fig. 4, it is

$$W^1 = W^0 \setminus [Pre_e(W^0) \cup Unavoid\_Pre(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0))]. \tag{8}$$

Let us show that

$$R_{(0)}(W^1) = W_0^1 \ . \tag{9}$$

By distributivity of the projection $R_{(0)}$ over the set operations $\setminus$ and $\cup$, from Eq. 8, we have

$$R_{(0)}(W^1) = R_{(0)}(W^0) \ \setminus \ [R_{(0)}(Pre_e(W^0)) \cup R_{(0)}(Unavoid\_Pre(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0)))],$$

and, by Lemmas 3.5 and 3.6,

$$R_{(0)}(W^1) = R_{(0)}(W^0) \ \setminus$$
$$[Pre_e(R_{(-\Delta)}(W^0)) \cup Unavoid\_Pre(Pre_e(R_{(-\Delta)}(W^0)) \cup R_{(0)}(\overline{W^0}), Pre_c(R_{(-\Delta)}(W^0)))].$$

Using the property $\overline{R_{(0)}(W^0)} = R_{(0)}(\overline{W^0})$, by Eq. 6 and Eq. 7, we have

$$R_{(0)}(W^1) = W_0^0 \ \setminus \ [Pre_e(W_{-\Delta}^0) \cup Unavoid\_Pre(Pre_e(W_{-\Delta}^0) \cup \overline{W_0^0}, Pre_c(W_{-\Delta}^0))] = W_0^1 \tag{10}$$

according to the procedure in Fig. 6.

We now show that

$$R_{(-\Delta)}(W^1) = W_{-\Delta}^1. \tag{11}$$

By distributivity of the projection $R_{(-\Delta)}$ over the set operation $\setminus$, from Eq. 8 we have

$$\begin{aligned} R_{(-\Delta)}(W^1) &= R_{(-\Delta)}(W^0) \ \setminus \ R_{(-\Delta)}(Pre_e(W^0) \cup Unavoid\_Pre(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0))) \\ &= R_{(-\Delta)}(W^0) \ \setminus \ R_{(-\Delta)}(Unavoid\_Pre(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0))), \end{aligned}$$

being, by Lemma 3.5, $R_{(-\Delta)}(Pre_e(W^0)) = \emptyset$. By Lemma 3.7

$$
\begin{aligned}
&R_{(-\Delta)}(W^1) = R_{(-\Delta)}(W^0) \ \setminus \\
&\quad \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U} \ \exists \ \bar{t} \in (0,\Delta] \ \exists d \in \mathcal{D} \textit{ such that} \\
&\quad \textit{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \textit{ we have} \\
&\qquad (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^0} \ \wedge \ \bar{t} < \Delta \ \vee \\
&\qquad (q, x(\Delta)) \in R_{(0)}(\overline{W \setminus (Pre_e(W^0) \cup \mathit{Unavoid\_Pre}(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0)))}) \ \wedge \ \bar{t} = \Delta\}.
\end{aligned}
\tag{12}
$$

By the property $\overline{R_{(0)}(W)} = R_{(0)}(\overline{W})$, distributivity of $R_{(0)}$ over $\setminus$ and $\cup$, Lemmas 3.5 and 3.6 and Eqs. 6 and 7, we have

$$
\begin{aligned}
&\overline{R_{(0)}(W^0 \setminus (Pre_e(W^0) \cup \mathit{Unavoid\_Pre}(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0))))} = \\
&\overline{R_{(0)}(W^0) \setminus (R_{(0)}(Pre_e(W^0)) \cup R_{(0)}(\mathit{Unavoid\_Pre}(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0))))} = \\
&\overline{R_{(0)}(W^0) \setminus Pre_e(R_{(-\Delta)}(W^0)) \cup \mathit{Unavoid\_Pre}(Pre_e(R_{(-\Delta)}(W^0)) \cup R_{(0)}(\overline{W^0}), Pre_c(R_{(-\Delta)}(W^0)))} = \\
&\overline{W_0^0 \setminus (Pre_e(W_{-\Delta}^0) \cup \mathit{Unavoid\_Pre}(Pre_e(W_{-\Delta}^0) \cup \overline{W_0^0}, Pre_c(W_{-\Delta}^0)))}
\end{aligned}
\tag{13}
$$

which, according to Eq. 10, is equal to $\overline{W_0^1}$.

Furthermore, from $W^0 = \mathit{Good} \times \mathbb{R}$, we have $(q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^0} = \overline{\mathit{Good} \times \mathbb{R}} = \overline{\mathit{Good}} \times \mathbb{R}$ if and only if $(q, x(\bar{t})) \in \overline{\mathit{Good}}$. Hence, Eq. 12 can be rewritten as follows

$$
\begin{aligned}
&R_{(-\Delta)}(W^1) = R_{(-\Delta)}(W^0) \ \setminus \\
&\quad \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U} \ \exists \ \bar{t} \in (0,\Delta] \ \exists d \in \mathcal{D} \textit{ such that} \\
&\quad \textit{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \textit{ we have} \\
&\qquad (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{\mathit{Good}} \ \wedge \ \bar{t} < \Delta \ \vee \\
&\qquad (q, x(\Delta)) \in \overline{W_0^1} \ \wedge \ \bar{t} = \Delta\}.
\end{aligned}
$$

Then, by the definition given in Eq. 4, we have

$$
R_{(-\Delta)}(W^1) = W_{-\Delta}^0 \ \setminus \ \mathit{Unavoid\_Pre}_{(-\Delta,0]}(\overline{\mathit{Good}}, \overline{W_0^1})
$$

which, according to the procedure in Fig. 6, is equal to $W_{-\Delta}^1$.

Suppose by induction hypothesis that $R_{(0)}(W^i) = W_0^i$ and $R_{(-\Delta)}(W^i) = W_{-\Delta}^i$. We want to show that $R_{(0)}(W^{i+1}) = W_0^{i+1}$ and $R_{(-\Delta)}(W^{i+1}) = W_{-\Delta}^{i+1}$ for $i \geq 1$.

According to the procedure in Fig. 4 it is

$$
W^{i+1} = W^i \setminus [Pre_e(W^i) \cup \mathit{Unavoid\_Pre}(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i))]. \tag{14}
$$

Let us show that

$$
R_{(0)}(W^{i+1}) = W_0^{i+1} \ .
$$

By distributivity of the projection $R_{(0)}$ and by Lemmas 3.5 and 3.6, from Eq. 14 we obtain

$$
\begin{aligned}
&R_{(0)}(W^{i+1}) = R_{(0)}(W^i) \ \setminus \\
&\qquad [Pre_e(R_{(-\Delta)}(W^i)) \cup \mathit{Unavoid\_Pre}(Pre_e(R_{(-\Delta)}(W^i)) \cup R_{(0)}(\overline{W^i}), Pre_c(R_{(-\Delta)}(W^i)))].
\end{aligned}
$$

Hence, using the property $\overline{R_{(0)}(W^i)} = R_{(0)}(\overline{W^i})$, by the induction hypothesis we have

$$R_{(0)}(W^{i+1}) = W_0^i \setminus [Pre_e(W^i_{-\Delta}) \cup Unavoid\_Pre(Pre_e(W^i_{-\Delta}) \cup \overline{W_0^i}, Pre_c(W^i_{-\Delta}))] = W_0^{i+1} \quad (15)$$

according to the procedure in Fig. 6.

Let us show that

$$R_{(-\Delta)}(W^{i+1}) = W^{i+1}_{-\Delta}.$$

By distributivity of the projection $R_{(-\Delta)}$ over $\setminus$, the induction hypothesis, Lemmas 3.5 and 3.7, and Eq. 13 (which applies also to W^i and justifies the last clause $(q, x(\Delta)) \in \overline{W_0^{i+1}}$), from Eq. 14 we obtain

$$\begin{aligned} R_{(-\Delta)}(W^{i+1}) = {} & W^i_{-\Delta} \setminus \\ & \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \text{ we have} \\ & \quad (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^i} \text{ for some } \bar{t} \in (0,\Delta) \ \vee \\ & \quad (q, x(\Delta)) \in \overline{W_0^{i+1}}\} \end{aligned} \quad (16)$$

with W_0^{i+1} as in the procedure in Fig. 6.

Since, for any mode $q \in Q$, the continuous time dynamics $\dot{x}(t) = f_q(x(t), u(t), d(t))$ is causal, that is, for any $\tau > 0$, $x(\tau) = \psi_q(u, d, \hat{x}, \tau)$ does not depend on $u(t)$ and $d(t)$ for $t > \tau$, then the classes $\mathcal{U}$ and $\mathcal{D}$ on the right hand side of Eq. 16 can be replaced by the classes $\mathcal{U}^0 \subset \mathcal{U}$ and $\mathcal{D}^0 \subset \mathcal{D}$, respectively, defined as follows:

$$\mathcal{U}^0 = \{u(t) \in \mathcal{U}, \text{defined on the interval } [0,\Delta]\}, \quad \mathcal{D}^0 = \{d(t) \in \mathcal{D}, \text{defined on the interval } [0,\Delta]\}\ .$$

Namely, the set in Eq. 16 contains configurations $(q,\hat{x}) \in Q \times X$, such that

$$\forall u \in \mathcal{U}^0.\ \exists d \in \mathcal{D}^0.\ (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^i} \text{ for some } \bar{t} \in (0,\Delta) \ \vee\ (q, x(\Delta)) \in \overline{W_0^{i+1}}\ . \quad (17)$$

Let us show that, given a configuration $(q,\hat{x}) \in Q \times X$, the trajectory $x(t) = \psi_q(u,d,\hat{x},t)$ satisfies Eq. 17 if and only if

$$\forall u \in \mathcal{U}^0.\ \exists d \in \mathcal{D}^0.\ (q, x(\Delta)) \in \overline{W_0^{i+1}}\ . \quad (18)$$

Condition Eq. 17 is trivially implied by 18. To show that also Eq. 17 implies Eq. 18, consider the set W^i. According to the procedure in Fig. 4 and Eq. 1, we have

$$\begin{aligned} \overline{W^i} &= \overline{W^{i-1} \setminus [Pre_e(W^{i-1}) \cup Unavoid\_Pre(Pre_e(W^{i-1}) \cup \overline{W^{i-1}}, Pre_c(W^{i-1}))]} \\ &= \overline{W^{i-1}} \cup Pre_e(W^{i-1}) \cup Unavoid\_Pre(Pre_e(W^{i-1}) \cup \overline{W^{i-1}}, Pre_c(W^{i-1})) \\ &= B \cup Unavoid\_Pre(B, E) \\ &= B \cup \{(q,\hat{x},t_c) \in Q \times X \times \mathbb{R} \mid \forall u \in \mathcal{U}^0\ \exists \bar{t} > 0\ \exists d \in \mathcal{D}^0 \text{ such that} \\ &\qquad \forall \tau \in [0,\bar{t})\ (q, x(\tau), t_c + \tau) \in \widetilde{\mathrm{W}}ait \cap \overline{E} \wedge \\ &\qquad (q, x(\bar{t}), t_c + \bar{t}) \in B\} \end{aligned}$$

where $B = \overline{W^{i-1}} \cup Pre_e(W^{i-1})$ and $E = Pre_c(W^{i-1})$. As already observed, set $\overline{W^i}$ is the playable set for the continuous dynamic game between the disturbance and the controller with target set B and state constraint $\overline{\widetilde{W}ait} \cap \overline{E}$.

In particular, let us consider the set $\overline{W^i}$ in the region $t_c \in [-\Delta, 0]$. Being $\dot{t}_c = 1$, any configuration (q, x', t_c), with $t_c \in [-\Delta, 0)$, which belongs to the boundary $\partial\overline{W^i}$ of $\overline{W^i}$, is steered in time $-t_c$, by the inputs $u^*(t)$, $d^*(t)$ solutions of the dynamic game, to a point on the surfaces $\partial\overline{W^i} \cap Q \times X \times \{0\}$. The set $\partial\overline{W^i} \cap Q \times X \times \{0\}$ corresponds to $R_{(0)}(\partial\overline{W^i})$ in the $Q \times X$ reduced configuration space, which, by the induction hypothesis, is equal to $\partial\overline{W_0^i}$.

Hence, consider a configuration $(q, \hat{x}, -\Delta) \in Q \times X \times \mathbb{R}$, which, under the action of some control $u(t)$ and disturbance $d(t)$, reaches the boundary $\partial\overline{W^i}$ at some time $\bar{t} < \Delta$, i.e. $(q, x(\bar{t}), -\Delta + \bar{t}) \in \partial\overline{W^i}$. The signals

$$u'(t) = \begin{cases} u(t) & \text{for } t \in [0, \bar{t}) \\ u^*(t + \bar{t}) & \text{for } t \in [\bar{t}, \Delta - \bar{t}] \end{cases} \qquad d'(t) = \begin{cases} d(t) & \text{for } t \in [0, \bar{t}) \\ d^*(t + t_c) & \text{for } t \in [\bar{t}, \Delta - \bar{t}] \end{cases} \tag{19}$$

steer, in time Δ, the configuration $(q, \hat{x}, -\Delta) \in Q \times X \times \mathbb{R}$ to $\partial\overline{W^i} \cap Q \times X \times \{0\}$; that is, $u'(t)$ and $d'(t)$ steer, in time Δ, $(q, \hat{x}) \in Q \times X$ to $(q, x(\Delta)) \in \partial\overline{W_0^i}$. If $\partial\overline{W_0^i} \subset \overline{W_0^i}$, then $(q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^i}$ and $(q, x(\Delta)) \in \overline{W_0^i}$. Otherwise, changing in the definition of $u'(t)$, Eq. 19, the switching point between $u(t)$ and $u^*(t)$ from $\bar{t}$ to $\bar{t} + \epsilon$, with $\epsilon > 0$ small enough, we obtain $(q, x(\bar{t} + \epsilon), -\Delta + \bar{t} + \epsilon) \in \overline{W^i}$ and $(q, x(\Delta)) \in \overline{W_0^i}$. In both cases, being, by Eq. 15, $\overline{W_0^i} \subseteq \overline{W_0^{i+1}}$, we have $(q, x(\Delta)) \in \overline{W_0^{i+1}}$.

Then, we conclude that, given a configuration $(q, \hat{x}) \in Q \times X$,

$$\begin{aligned} \forall u \in \mathcal{U}^0.\ \forall d \in \mathcal{D}^0.\ [(q, \psi_q(u, d, \hat{x}, \bar{t}), -\Delta + \bar{t}) \in \overline{W^i} \textit{ for some } \bar{t} \in (0, \Delta) \quad \Longrightarrow \\ \exists u' \in \mathcal{U}^0.\ \exists d' \in \mathcal{D}^0.\ (q, \psi_q(u', d', \hat{x}, \Delta)) \in \overline{W_0^{i+1}}]\ . \end{aligned} \tag{20}$$

Further, given a configuration $(q, \hat{x}) \in Q \times X$, consider the classes $\mathcal{U}' \subset \mathcal{U}^0$ and $\mathcal{D}' \subset \mathcal{D}^0$ of signals $u(t)$ and $d(t)$ such that: if $x(\bar{t}) \in \partial\overline{W^i}$ for some $\bar{t} \in [0, \Delta)$, then $u(t) = u'(t)$ and $d(t) = d'(t)$, with $u'(t)$ and $d'(t)$ as in Eq. 19. Eq. 20 is written as follows

$$\begin{aligned} \forall u \in \mathcal{U}'.\ \forall d \in \mathcal{D}'.\ [(q, \psi_q(u, d, \hat{x}, \bar{t}), -\Delta + \bar{t}) \in \overline{W^i} \textit{ for some } \bar{t} \in (0, \Delta) \quad \Longrightarrow \\ (q, \psi_q(u, d, \hat{x}, \Delta)) \in \overline{W_0^{i+1}}]\ . \end{aligned} \tag{21}$$

In fact, since, given a configuration $(q, \hat{x}) \in Q \times X$, Eq. 17 is verified if and only if

$$\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^i} \textit{ for some } \bar{t} \in (0, \Delta)\ \vee\ (q, x(\Delta)) \in \overline{W_0^{i+1}}\ , \tag{22}$$

one can restrict the class of trajectories $\psi_q(u, d, \hat{x}, t)$ to be analized only to those generated by input signals in the classes $\mathcal{U}'$ and $\mathcal{D}'$. The equivalence of Eq. 22 and Eq. 17 is given by the fact that the restriction on the input signals given by classes $\mathcal{U}'$ and $\mathcal{D}'$

- due to causality, has no effect on the clause "$(q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^i}$ *for some* $\bar{t} \in (0, \Delta)$",
- does not apply on signals which make true the clause "$(q, x(\Delta)) \in \overline{W_0^{i+1}}$".

Introducing

$$\begin{aligned} A(u, d) &= (q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W^i} \textit{ for some } \bar{t} \in (0, \Delta), \\ B(u, d) &= (q, x(\Delta)) \in \overline{W_0^{i+1}}, \end{aligned}$$

Eq. 21 is rewritten as $\forall u \in \mathcal{U}'.\ \forall d \in \mathcal{D}'.\ [A(u,d) \Longrightarrow B(u,d)]$. Hence, assuming Eq. 17 to hold, we have

$$
\begin{aligned}
&\{\forall u \in \mathcal{U}^0.\ \exists d \in \mathcal{D}^0.\ [A(u,d) \vee B(u,d)]\} \wedge \{\forall u \in \mathcal{U}'.\ \forall d \in \mathcal{D}'.\ [A(u,d) \Rightarrow B(u,d)]\} \iff \\
&\{\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ [A(u,d) \vee B(u,d)]\} \wedge \{\forall u \in \mathcal{U}'.\ \forall d \in \mathcal{D}'.\ [A(u,d) \Rightarrow B(u,d)]\} \iff \\
&\forall u \in \mathcal{U}'.\ \{(\exists d \in \mathcal{D}'.\ [A(u,d) \vee B(u,d)]) \wedge (\forall d \in \mathcal{D}'.\ [A(u,d) \Rightarrow B(u,d)])\} \Longrightarrow \\
&\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ \{[A(u,d) \vee B(u,d)] \wedge [A(u,d) \Rightarrow B(u,d)]\} \iff \\
&\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ \{[A(u,d) \vee B(u,d)] \wedge [\overline{A(u,d)} \vee B(u,d)]\} \iff \\
&\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ \{[A(u,d) \wedge \overline{A(u,d)}] \vee [A(u,d) \wedge B(u,d)] \\
&\qquad \vee [B(u,d) \wedge \overline{A(u,d)}] \vee [B(u,d) \wedge B(u,d)]\} \iff \\
&\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ \{[B(u,d) \wedge (A(u,d) \vee \overline{A(u,d)})] \vee B(u,d)\} \iff \\
&\forall u \in \mathcal{U}'.\ \exists d \in \mathcal{D}'.\ B(u,d) \iff \\
&\forall u \in \mathcal{U}^0.\ \exists d \in \mathcal{D}^0.\ B(u,d)
\end{aligned}
$$

that is Eq. (18).

In conclusion, since Eq. 17 is equivalent to Eq. 18, the clause "$(q, x(\bar{t}), -\Delta+\bar{t}) \in \overline{W^i}$ *for some* $\bar{t} \in (0, \Delta)$" can be removed from Eq. 16. Then, by the definition given in Eq. 5, Eq. 16 can be rewritten as

$$R_{(-\Delta)}(W^{i+1}) = W^i_{-\Delta} \setminus \mathit{Unavoid\_Pre}_{-\Delta}(\overline{W_0^{i+1}}) = W^{i+1}_{-\Delta}$$

according to the procedure in Fig. 6. □

To reconstruct the set *Safe*, the knowledge of the segments $Safe_0$ and $Safe_{-\Delta}$ is not sufficient; instead one has to obtain also the boundary curves that join them, by means of backward integration from the extremes of the segments.

4 Controller synthesis with lower bounds on event separation enforced by two timers

In this section, we consider 2-bounded systems, which have lower bounds on the separation times between consecutive discrete *controller* actions, and also lower bounds on the separation times between consecutive discrete *environment* actions. The two lower bounds are independent, with the occurrence times of discrete controller actions not placing any restrictions on the occurrence times of the discrete environment actions, and vice versa. Thus 2-bounded systems naturally model the coupling of a plant having discrete actions at its disposal with a hybrid controller that also has discrete actions at its disposal. A hybrid automaton model for a 2-bounded system includes two timers, one each for enforcing the lower bound properties for the discrete moves of the controller and of the environment. Whenever the controller makes a non-trivial discrete move, the timer for the controller is reset to $-\Delta_c$, where the lower bound on event separation for the controller is Δ_c. The lower bounding restriction is enforced by disallowing non-trivial discrete moves in the controller until the timer has reached at least 0. The timer for the environment acts similarly.

4.1 Extension of hybrid automaton with two timers

We formalize the definition of 2-bounded systems described intuitively above. Given a hybrid automaton H, the 2-bounded $\tilde{H}$ derived from H with constants Δ_c and Δ_e is the automaton

$\tilde{H} = (Q, \tilde{X}), (U, \Sigma_c), (\tilde{M}_c^{cts}, \tilde{M}_c^{disc}), (D, \Sigma_e), (\tilde{M}_e^{cts}, \tilde{M}_e^{disc}), (\tilde{f}, \tilde{\delta}))$, where the entities not yet defined are:

State space

- $\tilde{X} = X \times \mathbb{R}^2$, where the $n+1$-th coordinate represents the value of the timer t_c and the $n+2$-th coordinate represents the value of the timer t_e.

Control input

- $\tilde{M}_c^{disc} : Q \times \tilde{X} \to 2^{\Sigma_c^\epsilon} \setminus \{\}$ is defined as $\tilde{M}_c^{disc}(q, (x, t_c, t_e)) = \begin{cases} \{\epsilon\} & -\Delta_c \leq t_c < 0 \\ M_c^{disc}(q, x) & t_c \geq 0 \end{cases}$
- $\tilde{M}_c^{cts} : Q \times \tilde{X} \to 2^U \setminus \{\}$ is defined as $\tilde{M}_c^{cts}(q, (x, t_c, t_e)) = M_c^{cts}(q, x) \quad \forall t_c, t_e$

Disturbance input

- $\tilde{M}_e^{disc} : Q \times \tilde{X} \to 2^{\Sigma_e^\epsilon} \setminus \{\}$ is defined as $\tilde{M}_e^{disc}(q, (x, t_c, t_e)) = \begin{cases} \{\epsilon\} & -\Delta_e \leq t_e < 0 \\ M_e^{disc}(q, x) & t_e \geq 0 \end{cases}$
- $\tilde{M}_e^{cts} : Q \times \tilde{X} \to 2^D \setminus \{\}$ is defined as $\tilde{M}_e^{cts}(q, (x, t_c, t_e)) = M_e^{cts}(q, x) \quad \forall t_c, t_e$

Transitions

- $\tilde{f} : Q \times \tilde{X} \times U \times D \to \mathbb{R}^{n+2}$ are such that at each mode the same flows as in f apply, together with the flows $\dot{t}_c = 1$ and $\dot{t}_e = 1$.
- $\tilde{\delta} : Q \times \tilde{X} \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times \tilde{X}} \setminus \{\}$ is defined as

$$\tilde{\delta}(q, (x, t_c, t_e), \sigma_c, \sigma_e) = \begin{cases} \delta(q, x, \sigma_c, \sigma_e) \times \{(t_c, t_e)\} & (\sigma_c, \sigma_e) = (\epsilon, \epsilon) \\ \delta(q, x, \sigma_c, \sigma_e) \times \{(-\Delta_c, t_e)\} & \sigma_c \neq \epsilon \wedge \sigma_e = \epsilon \\ \delta(q, x, \sigma_c, \sigma_e) \times \{(t_c, -\Delta_e)\} & \sigma_c = \epsilon \wedge \sigma_e \neq \epsilon \\ \delta(q, x, \sigma_c, \sigma_e) \times \{(-\Delta_c, -\Delta_e)\} & \sigma_c \neq \epsilon \wedge \sigma_e \neq \epsilon \end{cases}$$

- $\widetilde{Wait} = Q \times X \times [-\Delta_c, 0) \times [-\Delta_e, 0) \cup Wait \times [0, \infty) \times [0, \infty)$
  $\cup\ Wait_c \times [-\Delta_c, 0) \times [0, \infty) \ \cup\ Wait_e \times [0, \infty) \times [-\Delta_e, 0)$

4.2 Timer-reduced sets

The basis of our simplified view of the calculations for continuous flows is that the value of each timer is irrelevant once it has exceeded 0, i.e., the lower bound on the timing delay between discrete events has been satisfied already, and the value of the timer is no longer needed.

Figure 7 depicts a cross-section of the continuous state space projected onto the timer state space for the variables t_c and t_e. The figure indicates the variables that intuitively are relevant at each section of the projection. For instance, in the upper right region where $t_c \geq 0 \wedge t_e \geq 0$, it suffices to know the value of X in order to determine the future evolution of the system: neither of the timer values are relevant, since both the lower bounds on event separations have passed. In the region $-\Delta < t_e \leq 0 \wedge t_c \geq 0$, it suffices to know the values for X and t_e, since t_c is irrelevant because the lower bound on event separations in the controller has passed. This diagram motivates the following definition.

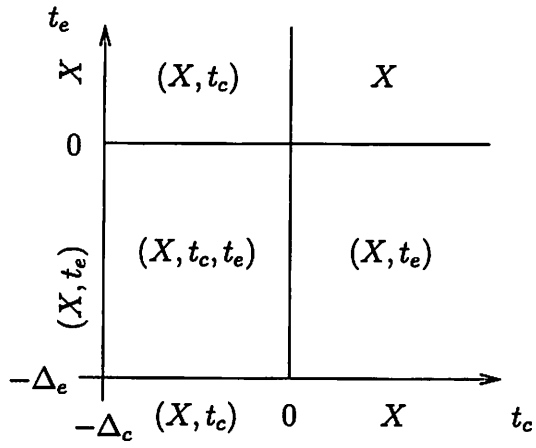


Figure 7: Structure of dependencies for 2-bounded systems.

A set $G \subseteq \Pi_{j=1..k} Y_j$ for domains Y_j is *independent* of the variable y_i having domain Y_i if for all $j \neq i$, $y_j \in Y_j$ implies that for all $y', y'' \in Y_i$, we have $(y_1, \ldots, y_{i-1}, y', y_{i+1}, \ldots, y_k) \in G$ iff $(y_1, \ldots, y_{i-1}, y'', y_{i+1}, \ldots, y_k) \in G$. In other words, membership of a point in G can be determined independently of the value of y_i.

Definition 4.1 *A set $G \subseteq \tilde{X}$ is* timer-reduced *if*

- *the set G restricted to the domain where $t_c \geq 0$ is independent of t_c, and*
- *the set G restricted to the domain where $t_e \geq 0$ is independent of t_e.*

Clearly, for any set G, the set G restricted to the domain $x = k$, for a variable x and constant k is independent of the variable x. Further facts about variable independence can be inferred for timer-reduced sets when one of its variables is fixed: for instance, for a timer-reduced set G, the set G restricted to the domain $t_e = 0$ is independent of t_e.

The set $W \subseteq Q \times \tilde{X}$ of configurations is *timer-reduced* if for every mode $q \in Q$, the set $\{\tilde{x} \in \tilde{X} \mid (q, \tilde{x}) \in W\}$ is timer-reduced.

We use the values of the timers to partition the state space $\tilde{X}$ into subsets as follows: $\tilde{X} = \tilde{X}_{-\Delta_c,-} \cup \tilde{X}_{-\Delta_c,+} \cup \tilde{X}_{-,-\Delta_e} \cup \tilde{X}_{-,-} \cup \tilde{X}_{-,+} \cup \tilde{X}_{+,-\Delta_e} \cup \tilde{X}_{+,-} \cup \tilde{X}_{+,+}$. The first subscript refers to the value of t_c, with "$-$" indicating the range $[-\Delta_c, 0)$ and "$+$" indicating the range $[0, \infty)$. The second subscript refers to the range of t_e in a similar way. The sets appear in Figure 8 and are defined explicitly below:

1. $\tilde{X}_{-\Delta_c,-} = \{\tilde{x} \in \tilde{X} \mid t_c = -\Delta_c \wedge t_e \in (-\Delta_e, 0)\}$.
2. $\tilde{X}_{-\Delta_c,+} = \{\tilde{x} \in \tilde{X} \mid t_c = -\Delta_c \wedge t_e \in [0, \infty)\}$.
3. $\tilde{X}_{-,-\Delta_e} = \{\tilde{x} \in \tilde{X} \mid t_c \in [-\Delta_c, 0) \wedge t_e = -\Delta_e\}$.
4. $\tilde{X}_{-,-} = \{\tilde{x} \in \tilde{X} \mid t_c \in (-\Delta_c, 0) \wedge t_e \in (-\Delta_e, 0)\}$.
5. $\tilde{X}_{-,+} = \{\tilde{x} \in \tilde{X} \mid t_c \in (-\Delta_c, 0) \wedge t_e \in [0, \infty)\}$.

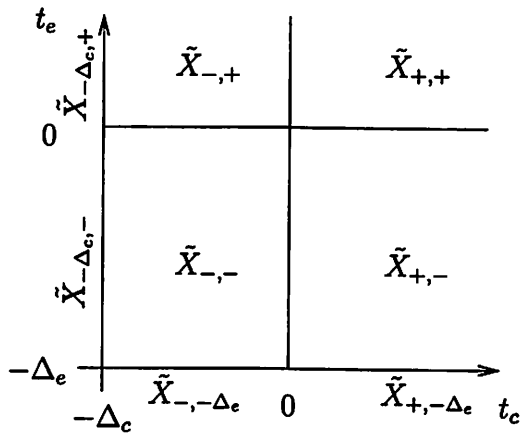


Figure 8: Partition of continuous state space.

6. $\tilde{X}_{+,-\Delta_e} = \{\tilde{x} \in \tilde{X} \mid t_c \in [0,\infty) \wedge t_e = -\Delta_e\}$.
7. $\tilde{X}_{+,-} = \{\tilde{x} \in \tilde{X} \mid t_c \in [0,\infty) \wedge t_e \in (-\Delta_e, 0)\}$.
8. $\tilde{X}_{+,+} = \{\tilde{x} \in \tilde{X} \mid t_c \in [0,\infty) \wedge t_e \in [0,\infty)\}$.

The sets $Pre_c(W)$ and $Pre_e(W)$ are disjoint from the region $t_c < 0 \wedge t_e < 0$. Figure 9 captures intuitively the dependencies of the sets Pre_c and Pre_e over various regions of the projected state space.

Lemma 4.1 *Given a timer-reduced set W of configurations, the set $Pre_c(W)$ is timer-reduced.*

Lemma 4.2 *Given a timer-reduced set W of configurations, the set $Pre_e(W)$ is timer-reduced.*

Lemma 4.3 *Given timer-reduced sets B and E of configurations, the set $Unavoid\_Pre(B, E)$ is timer-reduced.*

Lemma 4.4 *If the specification Good is timer-reduced, then the set Safe and also every set W^i computed in the synthesis procedure of Figure 4 is timer-reduced.*

The proofs of lemmas 4.1, 4.2, 4.3, and 4.4 are reported in Appendix.

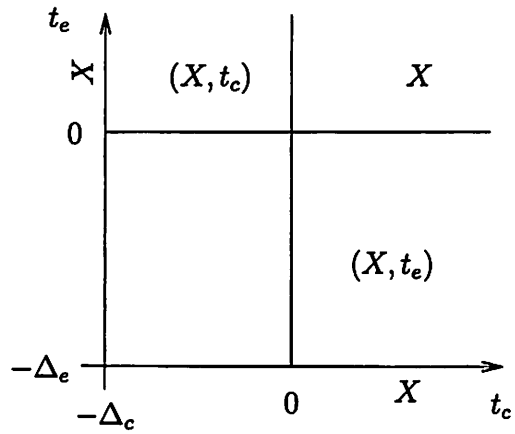


Figure 9: Structure of sets resulting from applying Pre_c and Pre_e to a timer-reduced set.

4.3 Projections of maximal safe set computations

We now present a revised formulation of the synthesis procedure, taking into account the fact that the winning sets at each iteration are timer-reduced. The basic idea is to use the reduced dependencies to reexpress the differential game as a number of differential games over a reduced state space. For example, for computing *Unavoid_Pre* in the upper right region where $t_c \geq 0 \wedge t_e \geq 0$, we need only solve a game over the reduced state space X instead of $\tilde{X}$.

In Sec. 4.2, we proved that the sets Pre_c, Pre_e, *Unavoid_Pre* preserve independence from t_c, when $t_c \geq 0$, and from t_e, when $t_e \geq 0$. For easier algebra, it is convenient to introduce the following operators, where $W \subseteq Q \times \tilde{X}$ is a set of configurations:

1. $R_{(0,0)} : Q \times \tilde{X} \rightarrow Q \times X$ is such that
   $R_{(0,0)}(W) = \{(q,x) \in Q \times X | (q,x,0,0) \in W\}$

2. $R_{(0,-)} : Q \times \tilde{X} \rightarrow Q \times X \times [-\Delta_e, 0)$ is such that
   $R_{(0,-)}(W) = \{(q,x,t_e) \in Q \times X \times [-\Delta_e, 0) | (q,x,0,t_e) \in W \wedge t_e \in [-\Delta_e, 0)\}$

3. $R_{(-,0)} : Q \times \tilde{X} \rightarrow Q \times X \times [-\Delta_c, 0)$ is such that
   $R_{(-,0)}(W) = \{(q,x,t_c) \in Q \times X \times [-\Delta_c, 0) | (q,x,t_c,0) \in W \wedge t_c \in [-\Delta_c, 0)\}$

4. $R_{(-\Delta_c,-)} : Q \times \tilde{X} \rightarrow Q \times X \times [-\Delta_e, 0)$ is such that
   $R_{(-\Delta_c,-)}(W) = \{(q,x,t_e) \in Q \times X \times [-\Delta_e, 0) |\ (q,x,-\Delta_c,t_e) \in W \wedge t_e \in [-\Delta_e, 0)\}$

5. $R_{(-,-\Delta_e)} : Q \times \tilde{X} \rightarrow Q \times X \times [-\Delta_c, 0)$ is such that
   $R_{(-,-\Delta_e)}(W) = \{(q,x,t_c) \in Q \times X \times [-\Delta_c, 0) |\ (q,x,t_c,-\Delta_e) \in W \wedge t_c \in [-\Delta_c, 0)\}$.

Furthermore, we denote by $W(\alpha)$ the following projection operator:

$$(q,x) \in W(\alpha) \subseteq Q \times X \ \ \textit{iff} \ \ (q,x,\alpha) \in W \subseteq Q \times X \times R,$$

and we introduce the short notations: $R_{(0,-)}(W)(\alpha) \equiv R_{(0,\alpha)}(W)$, $R_{(-,0)}(W)(\alpha) \equiv R_{(\alpha,0)}(W)$, $R_{(-\Delta_c,-)}(W)(\alpha) \equiv R_{(-\Delta_c,\alpha)}(W)$ and $R_{(-,-\Delta_e)}(W)(\alpha) \equiv R_{(\alpha,-\Delta_e)}(W)$. Notice that if W is timer-reduced, then

$$R_{(0,0)}(W) \times [0,\infty) \times [0,\infty) = W \cap [Q \times X \times [0,\infty) \times [0,\infty)].$$

Let us find out how the operators to compute the uncontrollable predecessors evaluate under projection.

Lemma 4.5 *Given* $W \subseteq Q \times \tilde{X}$,

$$\begin{aligned}
R_{(0,0)}(Pre_c(W)) &= Pre_c(R_{(0,-\Delta_e)}(W)) \\
&\quad \cup [Pre_c(R_{(-\Delta_c,0)}(W)) \cap Pre_c(R_{(-\Delta_c,-\Delta_e)}(W))] \\
R_{(0,0)}(Pre_e(W)) &= Pre_e(R_{(0,-\Delta_e)}(W)) \\
&\quad \cap [Pre_e(R_{(-\Delta_c,0)}(W)) \cup Pre_e(R_{(-\Delta_c,-\Delta_e)}(W))] \\
R_{(0,\alpha_e)}(Pre_c(W)) &= Pre_c(R_{(-\Delta_c,\alpha_e)}(W)) \\
R_{(0,\alpha_e)}(Pre_e(W)) &= Pre_e(R_{(-\Delta_c,\alpha_e)}(W)) \\
R_{(\alpha_c,0)}(Pre_c(W)) &= Pre_c(R_{(\alpha_c,-\Delta_e)}(W)) \\
R_{(\alpha_c,0)}(Pre_e(W)) &= Pre_e(R_{(\alpha_c,-\Delta_e)}(W)) \\
R_{(-\Delta_c,\alpha_e)}(Pre_c(W)) &= \emptyset \\
R_{(-\Delta_c,\alpha_e)}(Pre_e(W)) &= \emptyset \\
R_{(\alpha_c,-\Delta_e)}(Pre_c(W)) &= \emptyset \\
R_{(\alpha_c,-\Delta_e)}(Pre_c(W)) &= \emptyset
\end{aligned}$$

The proof is reported in Appendix.

Every timer-reduced set can be represented as a collection of subsets of reduced state spaces. The reduced dependencies have been shown in Fig. 7. To solve the synthesis game, instead of applying directly the procedure in Fig. 6 on the extended state space, one can play a collection of games in the regions $X_{+,+}$, $X_{+,-}$, $X_{-,+}$, $X_{-,-}$. In the latter region, which is the only one to depend on all variables (X, t_c, t_e), it is convenient to distinguish the following subregions and define a synthesis game for each of them:

$$\begin{aligned}
\tilde{X}_{-,-} \cap T_1 &= \tilde{X}_{-,-} \cap \{\tilde{x} \in \tilde{X} \mid t_e > t_c\} \\
\tilde{X}_{-,-} \cap T_2 &= \tilde{X}_{-,-} \cap \{\tilde{x} \in \tilde{X} \mid t_c + \Delta_c \geq t_e + \Delta_e\} \\
\tilde{X}_{-,-} \cap T_3 &= \tilde{X}_{-,-} \cap \{\tilde{x} \in \tilde{X} \mid t_c = t_e\} \\
\tilde{X}_{-,-} \cap T_4 &= \tilde{X}_{-,-} \cap \{\tilde{x} \in \tilde{X} \mid t_e < t_c < t_e + \Delta_e - \Delta_c\}.
\end{aligned}$$

In the sequel, we assume also $\Delta_e \geq \Delta_c$.

More precisely, one can repeat until convergence (if achievable) the following cycle of synthesis games, applied initially to the set *Good*, to remove incrementally the unsafe configurations (see Fig. 11 for a pictorial display of the sets mentioned in the maximal safe set computation, where $W(\alpha)$ stands for a parametrization of the set W with respect to a parameter α):

1.

$$\begin{aligned}
&W^i_{(0,0)} \setminus [Pre_e(W^i_{(0,-)}(-\Delta_e)) \cap [Pre_e(W^i_{(-,0)}(-\Delta_c)) \cup Pre_e(W^i_{(-,-\Delta_e)}(-\Delta_c))] \\
&\cup \mathit{Unavoid_Pre}(Pre_e(W^i_{(0,-)}(-\Delta_e)) \cap [Pre_e(W^i_{(-,0)}(-\Delta_c)) \cup Pre_e(W^i_{(-,-\Delta_e)}(-\Delta_c)) \\
&\cup \overline{W^i_{(0,0)}}, Pre_c(R_{(0,-)}(W)(-\Delta_e)) \cup [Pre_c(R_{(-,0)}(W)(-\Delta_c)) \cap Pre_c(R_{(-,-\Delta_e)}(W)(-\Delta_c))]]
\end{aligned}$$

$Good \subseteq Q \times X$ independent from t_c, t_e, $\Delta_e \geq \Delta_c$

$\alpha_e \in [-\Delta_e, 0)$, $\alpha_c \in [-\Delta_c, 0)$ are parameters indexing the sets W

$W^0_{(0,0)} = W^0_{(0,-)}(\alpha_e) = W^0_{(-,0)}(\alpha_c) = W^0_{(-\Delta_c,-)}(\alpha_e) = W^0_{(-,-\Delta_e)}(\alpha_c) := Good$

$Pre^1_{e,(0,0)} := Pre_e(W^0_{(0,-)}(-\Delta_e) \cup W^0_{(-,0)}(-\Delta_c) \cup W^0_{(-,-\Delta_e)}(-\Delta_c))$

$Pre^1_{c,(0,0)} := Pre_c(W^0_{(0,-)}(-\Delta_e) \cup W^0_{(-,0)}(-\Delta_c) \cup W^0_{(-,-\Delta_e)}(-\Delta_c))$

$W^1_{(0,0)} := W^0_{(0,0)} \setminus [Pre^0_{e,(0,0)} \cup Unavoid\_Pre(Pre^0_{e,(0,0)} \cup \overline{W^0_{(0,0)}}, Pre^0_{c,(0,0)})]$

$W^0_{(-\Delta_c,-)}(.) := \{W^0_{(-\Delta_c,-)}(\beta_e)\}_{\beta_e \in [-\Delta_e,0)}$; $W^0_{(-,-\Delta_e)}(.) := \{W^0_{(-,-\Delta_e)}(\beta_c)\}_{\beta_c \in [-\Delta_c,0)}$

$W^1_{(0,-)}(\alpha_e) := W^0_{(0,-)}(\alpha_e) \setminus [Pre_e(W^0_{(-\Delta_c,-)}(\alpha_e)) \cup$
$Unavoid\_Pre_{(+,-)}(Pre_e(W^0_{(-\Delta_c,-)}(.)) \cup \overline{W^1_{(0,0)}}, Pre_c(W^0_{(-\Delta_c,-)}(.)), \alpha_e)]$

$W^1_{(-,0)}(\alpha_c) := W^0_{(-,0)}(\alpha_c) \setminus [Pre_e(W^0_{(-,-\Delta_e)}(\alpha_c)) \cup$
$Unavoid\_Pre_{(-,+)}(Pre_e(W^0_{(-,-\Delta_e)}(.)) \cup \overline{W^1_{(0,0)}}, Pre_c(W^0_{(-,-\Delta_e)}(.)), \alpha_c)]$

$W^1_{(-,-\Delta_e)}(\alpha_c) := W^0_{(-,-\Delta_e)}(\alpha_c) \setminus Unavoid\_Pre^0_{T_1}(\overline{Good}, \overline{W^1_{(0,-)}}(-\Delta_e - \alpha_c), \alpha_c)$

$W^1_{(-\Delta_c,-)}(\alpha_e) := W^0_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre^0_{T_2}(\overline{Good}, \overline{W^1_{(-,0)}}(-\Delta_c - \alpha_e), \alpha_e)$, $\alpha_e \in (-\Delta_c, 0)$

$W^1_{(-\Delta_c,-)}(\alpha_e) := W^0_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre^0_{T_3}(\overline{Good}, \overline{W^1_{(0,0)}})$, if $\alpha_e = -\Delta_c$

$W^1_{(-\Delta_c,-)}(\alpha_e) := W^0_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre^0_{T_4}(\overline{Good}, \overline{W^1_{(0,-)}}(\alpha_e + \Delta_c), \alpha_e)$ if $\alpha_e \in [-\Delta_e, -\Delta_c)$

$i := 0$

repeat {

$i := i + 1$

$Pre^i_{e,(0,0)} := Pre_e(W^i_{(0,-)}(-\Delta_e)) \cap [Pre_e(W^i_{(-,0)}(-\Delta_c)) \cup Pre_e(W^i_{(-,-\Delta_e)}(-\Delta_c))]$

$Pre^i_{c,(0,0)} := Pre_c(W^i_{(0,-)}(-\Delta_e)) \cup [Pre_c(W^i_{(-,0)}(-\Delta_c)) \cap Pre_e(W^i_{(-,-\Delta_e)}(-\Delta_c))]$

$W^{i+1}_{(0,0)} := W^i_{(0,0)} \setminus [Pre^i_{e,(0,0)} \cup Unavoid\_Pre(Pre^i_{e,(0,0)} \cup \overline{W^i_{(0,0)}}, Pre^i_{c,(0,0)})]$

$W^i_{(-\Delta_c,-)}(.) := \{W^i_{(-\Delta_c,-)}(\beta_e)\}_{\beta_e \in [-\Delta_e,0)}$; $W^i_{(-,-\Delta_e)}(.) := \{W^i_{(-,-\Delta_e)}(\beta_c)\}_{\beta_c \in [-\Delta_c,0)}$

$W^{i+1}_{(0,-)}(\alpha_e) := W^i_{(0,-)}(\alpha_e) \setminus [Pre_e(W^i_{(-\Delta_c,-)}(\alpha_e)) \cup$
$Unavoid\_Pre_{(+,-)}(Pre_e(W^i_{(-\Delta_c,-)}(.)) \cup \overline{W^{i+1}_{(0,0)}}, Pre_c(W^i_{(-\Delta_c,-)}(.)), \alpha_e)]$

$W^{i+1}_{(-,0)}(\alpha_c) := W^i_{(-,0)}(\alpha_c) \setminus [Pre_e(W^i_{(-,-\Delta_e)}(\alpha_c)) \cup$
$Unavoid\_Pre_{(-,+)}(Pre_e(W^i_{(-,-\Delta_e)}(.)) \cup \overline{W^{i+1}_{(0,0)}}, Pre_c(W^i_{(-,-\Delta_e)}(.)), \alpha_c)]$

$W^{i+1}_{(-,-\Delta_e)}(\alpha_c) := W^i_{(-,-\Delta_e)}(\alpha_c) \setminus Unavoid\_Pre_{T_1}(\overline{W^{i+1}_{(0,-)}}(-\Delta_e - \alpha_c), \alpha_c)$

$W^{i+1}_{(-\Delta_c,-)}(\alpha_e) := W^i_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre_{T_2}(\overline{W^{i+1}_{(-,0)}}(-\Delta_c - \alpha_e), \alpha_e)$, if $\alpha_e \in (-\Delta_c, 0)$

$W^{i+1}_{(-\Delta_c,-)}(\alpha_e) := W^i_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre_{T_3}(\overline{W^{i+1}_{(0,0)}})$, if $\alpha_e = -\Delta_c$

$W^{i+1}_{(-\Delta_c,-)}(\alpha_e) := W^i_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre_{T_4}(\overline{W^{i+1}_{(0,-)}}(\alpha_e + \Delta_c), \alpha_e)$, if $\alpha_e \in [-\Delta_e, -\Delta_c)$

} until ($W^i_{(0,0)}$, $W^i_{(0,-)}(\alpha_e)$, $W^i_{(-,0)}(\alpha_c)$, $W^i_{(-\Delta_c,-)}(\alpha_e)$, $W^i_{(-,-\Delta_e)}(\alpha_c)$ do not change)

$Safe_{(0,0)} := W^i_{(0,0)}$

$Safe_{(0,-)}(\alpha_e) := W^i_{(0,-)}(\alpha_e)$

$Safe_{(-,0)}(\alpha_c) := W^i_{(-,0)}(\alpha_c)$

$Safe_{(-\Delta_c,-)}(\alpha_e) := W^i_{(-\Delta_c,-)}(\alpha_e)$

$Safe_{(-,-\Delta_e)}(\alpha_c) := W^i_{(-,-\Delta_e)}(\alpha_c)$

Figure 10: Computation of Maximal Safe Set with Projection of 2 Timers.

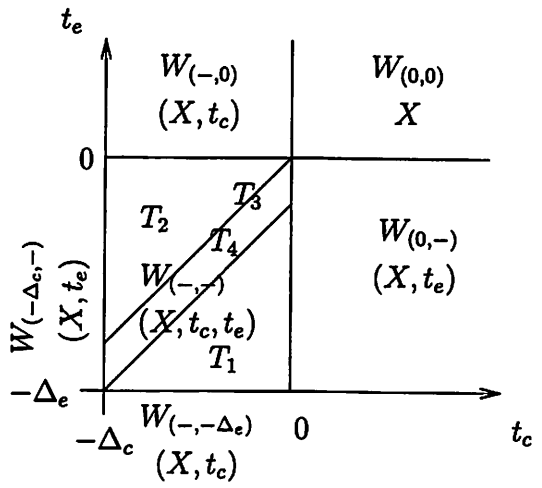


Figure 11: Sets involved in the maximal set computations.

removes from the set $W^i_{(0,0)}$ the configurations that unavoidably loose either with a discrete step $(Pre_e(W^i_{(0,-)}(-\Delta_e)) \cap [Pre_e(W^i_{(-,0)}(-\Delta_c)) \cup Pre_e(W^i_{(-,-\Delta_e)}(-\Delta_c))])$ or with a continuous flow according to the standard operator *Unavoid_Pre* defined by Eq. 1. Lemma 4.5 accounts for the algebraic form of the sets Pre_e and Pre_c.

2.

$$W^i_{(0,-)}(\alpha_e) \setminus [Pre_e(W^i_{(-\Delta_c,-)}(\alpha_e)) \cup$$
$$Unavoid\_Pre_{(+,-)}(Pre_e(W^i_{(-\Delta_c,-)}(\beta_e)) \cup \overline{W^{i+1}_{(0,0)}}, Pre_c(W^i_{(-\Delta_c,-)}(\beta_e)), \alpha_e)]$$

removes from the set $W^i_{(0,-)}(\alpha_e)$ (whose support is parametrized by $\alpha_e \in [-\Delta_e, 0)$) the configurations that unavoidably loose either with a discrete step $Pre_e(W^i_{(-\Delta_c,-)}(\alpha_e))$ [1] or with a continuous flow according to the operator $Unavoid\_Pre_{(+,-)}$ defined by Eq. 23:

$$\begin{aligned} Unavoid\_Pre_{(+,-)}(B(.), E(.), \alpha) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\ 0 < \bar{t} \leq -\alpha\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & \quad \forall \tau \in [0, \bar{t}]\ (q, x(\tau)) \in Wait_c \cap \overline{E}(\alpha + \tau) \wedge \\ & \quad (q, x(\bar{t})) \in B(\alpha + \bar{t})\ \} \end{aligned} \tag{23}$$

Notice that $Unavoid\_Pre_{(+,-)}$ is invoked with the "bad" set $\overline{W^{i+1}_{(0,0)}}$.

[1] It can only be $\sigma_c \neq \epsilon, \sigma_e = \epsilon$ so that t_c is reset to $-\Delta_c$ and $W^i_{(0,-)}(\alpha_e)$ is mapped to $W^i_{(-\Delta_c,-)}(\alpha_e)$.

3.

$$W^i_{(-,0)}(\alpha_c) \setminus [Pre_e(W^i_{(-,-\Delta_e)}(\alpha_c)) \cup$$
$$Unavoid\_Pre_{(-,+)}(Pre_e(W^i_{(-,-\Delta_e)}(\beta_c)) \cup \overline{W^{i+1}_{(0,0)}}([-\Delta_c, 0)), Pre_c(W^i_{(-,-\Delta_e)}(\beta_c)), \alpha_c)]$$

removes from the set $W^i_{(-,0)}(\alpha_c)$ (whose support is parametrized by $\alpha_c \in [-\Delta_c, 0)$) the configurations that unavoidably loose either with a discrete step $Pre_e(W^i_{(-,-\Delta_e)}(\alpha_c))$ [2] or with a continuous flow according to the operator $Unavoid\_Pre_{(-,+)}$ defined by Eq. 24:

$$\begin{aligned} Unavoid\_Pre_{(-,+)}(B(.), E(.), \alpha) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\ 0 < \bar{t} \leq -\alpha\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & \quad \forall \tau \in [0, \bar{t}]\ (q, x(\tau)) \in Wait_e\ \cap \overline{E}(\alpha + \tau) \wedge \\ & \quad (q, x(\bar{t})) \in B(\alpha + \bar{t})\ \} \end{aligned} \tag{24}$$

Notice that $Unavoid\_Pre_{(-,+)}$ is invoked with the "bad" set $\overline{W^{i+1}_{(0,0)}}$.

4.

$$W^i_{(-,-\Delta_e)}(\alpha_c) \setminus Unavoid\_Pre_{T_1}(\overline{W^{i+1}_{(0,-)}}(-\Delta_e - \alpha_c), \alpha_c)$$

removes from the set $W^i_{(-,-\Delta_e)}(\alpha_c)$ (whose support is parametrized by $\alpha_c \in [-\Delta_c, 0)$) the configurations that unavoidably loose with a continuous flow according to the operator $Unavoid\_Pre_{T_1}$ defined by Eqs. 25 and 26 (the former is invoked the first time, then the latter is applied):

$$\begin{aligned} Unavoid\_Pre^0_{T_1}(B_G, B(-\Delta_e - \alpha), \alpha) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\ 0 < \bar{t} \leq -\alpha\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & \quad (q, x(\bar{t})) \in B_G\ \vee\ (q, x(-\alpha)) \in B(-\Delta_e - \alpha)\ \} \end{aligned} \tag{25}$$

$$\begin{aligned} Unavoid\_Pre_{T_1}(B(-\Delta_e - \alpha), \alpha) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & \quad (q, x(-\alpha)) \in B(-\Delta_e - \alpha)\ \} \end{aligned} \tag{26}$$

Notice that in this region the sets Pre_e and Pre_c are empty and that $Unavoid\_Pre_{T_1}$ is invoked with the "bad" set $\overline{W^{i+1}_{(0,-)}}(-\Delta_e - \alpha_c)$.

5.

$$W^i_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre_{T_2}(\overline{W^{i+1}_{(-,0)}}(-\Delta_c - \alpha_e), \alpha_e)$$

[2] It can only be $\sigma_c = \epsilon, \sigma_e \neq \epsilon$ so that t_e is reset to $-\Delta_e$ and $W^i_{(-,0)}(\alpha_c)$ is mapped to $W^i_{(-,-\Delta_e)}(\alpha_c)$.

removes from the set $W^i_{(-\Delta_c,-)}(\alpha_e)$ (whose support is parametrized by $\alpha_e \in (-\Delta_c, 0)$) the configurations that unavoidably loose with a continuous flow according to the operator $Unavoid\_Pre_{T_2}$ defined by Eqs. 27 and 28 (the former is invoked the first time, then the latter is applied):

$$\begin{aligned} Unavoid\_Pre^0_{T_2}(B_G, B(-\Delta_c - \alpha), \alpha) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\ 0 < \bar{t} \leq -\alpha\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & (q, x(\bar{t})) \in B_G\ \vee\ (q, x(-\alpha)) \in B(-\Delta_c - \alpha)\ \} \end{aligned} \tag{27}$$

$$\begin{aligned} Unavoid\_Pre_{T_2}(B(-\Delta_c - \alpha), \alpha) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & (q, x(-\alpha)) \in B(-\Delta_c - \alpha)\ \} \end{aligned} \tag{28}$$

Notice that in this region the sets Pre_e and Pre_c are empty and that $Unavoid\_Pre_{T_2}$ is invoked with the "bad" set $\overline{W^{i+1}_{(-,0)}}(-\Delta_c - \alpha_e)$.

6.

$$W^i_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre_{T_3}(\overline{W^{i+1}_{(0,0)}})$$

removes from the set $W^i_{(-\Delta_c,-)}(\alpha_e)$ (whose support is parametrized by $\alpha_e = -\Delta_c$) the configurations that unavoidably loose with a continuous flow according to the operator $Unavoid\_Pre_{T_3}$ defined by Eqs. 29 and 30 (the former is invoked the first time, then the latter is applied):

$$\begin{aligned} Unavoid\_Pre^0_{T_3}(B_G, B) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\ 0 < \bar{t} \leq \Delta_c\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & (q, x(\bar{t})) \in B_G\ \vee\ (q, x(\Delta_c)) \in B\ \} \end{aligned} \tag{29}$$

$$\begin{aligned} Unavoid\_Pre_{T_3}(B) \quad = \quad & \{(q, \hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D} \text{ such that} \\ & \text{for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \\ & \text{we have} \\ & (q, x(\Delta_c)) \in B\} \end{aligned} \tag{30}$$

Notice that in this region the sets Pre_e and Pre_c are empty and that $Unavoid\_Pre_{T_3}$ is invoked with the "bad" set $\overline{W^{i+1}_{(0,0)}}$.

7.

$$W^i_{(-\Delta_c,-)}(\alpha_e) \setminus Unavoid\_Pre_{T_4}(\overline{W^{i+1}_{(0,-)}}(\alpha_e + \Delta_c), \alpha_e)$$

removes from the set $W^i_{(-\Delta_c,-)}(\alpha_e)$ (whose support is parametrized by $\alpha_e \in [-\Delta_e, -\Delta_c)$) the configurations that unavoidably loose with a continuous flow according to the operator

Unavoid_Pre$_{T_4}$ defined by Eqs. 31 and 32 (the former is invoked the first time, then the latter is applied):

$$\begin{aligned} \textit{Unavoid\_Pre}^0_{T_4}(B_G, B(\alpha+\Delta_c), \alpha) \;=\; \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\ 0 < \bar{t} \leq \Delta_c\ \exists d \in \mathcal{D} \textit{ such that} \\ \textit{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \\ \textit{we have} \\ (q, x(\bar{t})) \in B_G \ \vee\ (q, x(\Delta_c)) \in B(\alpha+\Delta_c)\ \} \end{aligned} \tag{31}$$

$$\begin{aligned} \textit{Unavoid\_Pre}_{T_4}(B(\alpha+\Delta_c), \alpha) \;=\; \{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D} \textit{ such that} \\ \textit{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \\ \textit{we have} \\ (q, x(\Delta_c)) \in B(\alpha+\Delta_c)\ \} \end{aligned} \tag{32}$$

Notice that in this region the sets Pre_e and Pre_c are empty and that *Unavoid_Pre*$_{T_4}$ is invoked with the "bad" set $\overline{W^{i+1}_{(0,-)}}(\alpha_e + \Delta_c)$.

The previous sequence of games can be computed by the procedure given in Fig. 10 Then one can prove that the following is true:

Theorem 4.1 *The sets* $W^i_{(0,0)}$, $W^i_{(0,-)}(\alpha_e)$, $W^i_{(-,0)}(\alpha_c)$, $W^i_{(-\Delta_c,-)}(\alpha_e)$ *and* $W^i_{(-,-\Delta_e)}(\alpha_c)$ *computed by the procedure in Fig. 10 are the projections, respectively, under* $R_{(0,0)}$, $R_{(0,\alpha_e)}(W^i)$, $R_{(\alpha_c,0)}(W^i)$, $R_{(-\Delta_c,\alpha_e)}(W^i)$ *and* $R_{(\alpha_c,-\Delta_e)}$, *of the sets* W^i *computed by the procedure in Fig. 4, i.e.,*

$$\begin{aligned} R_{(0,0)}(W^i) &= W^i_{(0,0)} \\ R_{(0,\alpha_e)}(W^i) &= W^i_{(0,-)}(\alpha_e) \\ R_{(\alpha_c,0)}(W^i) &= W^i_{(-,0)}(\alpha_c) \\ R_{(-\Delta_c,\alpha_e)}(W^i) &= W^i_{(-\Delta_c,-)}(\alpha_e) \\ R_{(\alpha_c,-\Delta_e)}(W^i) &= W^i_{(-,-\Delta_e)}(\alpha_c). \end{aligned}$$

5 Controller synthesis with lower bounds on event separation enforced by k timers

It is conceivable to extend the notion of 1-bounded and 2-bounded systems to k-bounded systems, $k > 2$, i.e., systems with independent lower bounds on event separation enforced by k timers, $k > 2$. The case $k > 2$ is needed when, for a given system, different disturbance events in Σ_e and/or different control events in Σ_c may be associated to different time separations, e.g., it may be the case that a delay of $\Delta_{\sigma'}$ separates the occurrence of event $\sigma' \in \Sigma = \Sigma_e \cup \Sigma_c$ and that of any successive event, whereas between the occurrence of $\sigma'' \in \Sigma = \Sigma_e \cup \Sigma_c$ and that of any successive event there is a separation of $\Delta_{\sigma''} \neq \Delta_{\sigma'}$. So one might partition the events in $\Sigma = \Sigma_e \cup \Sigma_c$ into k classes such that the same delay separation is associated to the events in the same class and then introduce k related timers to keep track of these separations. Notice that the case $k = 3$ is especially useful when there are transitions forced by the fact that guards are hit as an effect of the

continuous dynamics. In our formulation forced transitions can be modelled adding some special events to Σ_e. Since the timer associated to these special events would model some internal inertia of the plant, it should be different from the timers associated to external disturbance events and to control events. So a third timer should be added besides the two introduced for a 2-bounded system.

The theory developed in Sec. 4 can be generalized to the case of k timers, with $k > 2$. Even though the concrete details become more complicated, the proposed steps and theorems carry through the general case. In particular one extends first the definition of the hybrid automaton H to $\tilde{H}$ over $\tilde{X} = X \times \mathbb{R}^{n+k}$, adding k timers $t_i, i = 1, \ldots, k$. and modifying accordingly the move and transition functions: once timer t_i is reset to $-\Delta_i$ then no transition guarded by t_i is allowed before the timer reaches 0. Then one generalizes the theory of timer-reduced sets, that are sets independent of $t_i, i = 1, \ldots, k$ when restricted to the domain where $t_i \geq 0$. Again one can show that the operators Pre_c, Pre_e and *Unavoid_Pre* preserve timer-reduced sets. This results allow to find the projections of the maximal safe set computations.

Given k timers $t_i, i = 1, \ldots, k$ in the extended space, one can define 2^k regions with respect to the subsets of timers that are enabled. In particular, in one such region no timer is enabled (call it the *timer cube*, $-\Delta_i \leq t_i < 0, i = 1, \ldots, k$), in another such region all timers are enabled, and in the remaining $2^k - 2$ regions some timers are disabled and some are enabled. For each of the $2^k - 1$ regions where at least one timer is enabled, specialized versions of Pre_c, Pre_e and *Unavoid_Pre* are defined in order to compute the currently safe points on the k inner faces of the closed timer cube (a cube of dimension k has 2 k subcubes - faces - of dimension $k-1$; at an inner face exactly one timer has value 0). Finally one has to specialize the *Unavoid_Pre* computation within the timer cube to compute the current safe sets on the k outer faces of the timer cube (at an outer face exactly one timer, say t_i, has value $-\Delta_i$), partitioning some of the outer faces into subfaces along parallels to the diagonal flows $\dot{t}_i = 1, i = 1, \ldots, k$.

These specialized operators allow to set up the procedure to compute the maximal safe set with projection of k timers, similarly as in Fig. 10 for 2-bounded systems. Notice that the computations in each of the $2^k - 1$ regions (timer cube excepted) exhibit reduced dependency on timers, more precisely they do not depend on the value of timers enabled in a given region. Finally a generalization of Th. 4.1 can be stated for k-bounded systems.

6 Case Study of a Heating System

6.1 A thermic model of a room

Our heating system has discrete and continuous components in its state, its control input, and its disturbance. The control objective is to maintain the temperature T_a of the air in a room within the range $[T_a^{min}, T_a^{max}]$, whatever the disturbances happen to be. The controller has at its disposal a boiler and a stove. It operates under full state feedback. The boiler can be viewed as a heating element that admits continuous settings: it receives a continuous input control variable $u_b \in [0, U_b]$ and outputs this power value instantaneously. The stove has only discrete settings. It is switched on or off by a two-valued input control variable $u_s \in \{0, 1\}$. When switched on, the stove delivers heat $w_s = w_s^{max}$; when switched off, it delivers heat $w_s = 0$.

The room is subject to non-deterministic disturbances that affect the temperature. First, the room contains electrical appliances whose operation generates heat as a side effect—modeled by a

continuous input disturbance variable $d_e \in [0, D_e]$. Second, the room has a door that may be either closed or open. Its state is set by a two-valued input disturbance variable $d_d \in \{0, 1\}$. When the door is opened the air temperature of the room suddenly decreases. Its difference from the external temperature T_e is multiplied by a ratio $r < 1$, i.e., T_a is updated to $T_e + r(T_a - T_e)$. For physical reasons, we rule out the possibility of the door opening and closing infinitely often in zero time by assuming that at least Δ time passes between changes in the status of the door.

The continuous dynamics of the system are captured by two first-order differential equations whose unknowns are the room air temperature $T_a(t)$, and the door timer $t_d(t)$, with $\dot{t}_d(t) = 1$. For convenience, we translate the temperature variable to $T_{ae} = T_a - T_e$. We derive the following equation for T_{ae}:

$$\begin{aligned} \dot{T}_{ae}(t) = &-\frac{1}{c_a}(\mu_{ae} + \mu_d(d_d))T_{ae}(t) + \\ &\frac{1}{c_a}(u_b(t) + d_e(t) + w_s(u_s)) \end{aligned} \tag{33}$$

where $\mu_d(d_d) = \mu_{do}$ if $d_d = 1$ and $\mu_d(d_d) = \mu_{dc}$ if $d_d = 0$, and $w_s(u_s) = w_s^{max}$ if $u_s = 1$ and $w_s(u_s) = 0$ if $u_s = 0$, for the thermic conductance parameters μ_{ae}, (resp. μ_{dc}, μ_{do}) for the walls between the room and the environment (resp. the closed door, the open door), and c_a the air thermic capacitance.

6.2 Hybrid automaton model of the heating system

Say that we are going to model the room first as a 1-bounded system, then as a 2-bounded system. For a 1-bounded system (one timer) we synthesize the maximal controller both with the standard procedure on the extended space and with the modified procedure on the original space. For a 2-bounded system (two timers) we synthesize the maximal controller with the modified procedure.

6.2.1 The heating system with event separation enforced by one timer

The system described in Section 6.1 can be modeled by a hybrid automaton. It is depicted in Figure 12, and characterized as follows:

State space

- The set Q of modes consists of $q_1 = (off, closed)$, $q_2 = (on, closed)$, $q_3 = (on, open)$, and $q_4 = (off, open)$. The first component of each tuple refers to the status of the stove, and the second to the door.
- $X = \{(t_c, T_{ae}) \mid (t_c, T_{ae}) \in \mathbb{R}^2 \}$.

Controller input

- The domain of continuous input values is $U = \{u_b \mid u_b \in [0, U_b]\}$.
- The set of control events is $\Sigma_c = \{stove\_on, stove\_off\}$, (modeling the input discrete control variable of values u_s of Sec 6.1).
- We have $\epsilon \in M_c^{disc}(q, x)$ for all (q, x), i.e., the controller is never forced to make a discrete action. The event *stove_off* appears in the discrete controller move function whenever the mode is $(on, open)$ or $(on, closed)$, and $t_d \geq 0$. In addition, *stove_on* is allowed whenever the mode is $(off, open)$ or $(off, closed)$, and $t_d \geq 0$.

- For all (q,x), $M_c^{cts}(q,x) = U$, i.e., there are no restrictions on the continuous controller input values.

Environment input

- The domain of continuous disturbance values is $D = \{d_e \mid d_e \in [0, D_e]\}$.
- The set of disturbance events is $\Sigma_e = \{door\_close, door\_open\}$, (modeling the input discrete disturbance variable of values d_d of Sec 6.1).
- We have $\epsilon \in M_e^{disc}(q,x)$ for all (q,x), i.e., the environment is never forced to make a discrete action. The event *door_open* appears in the discrete environment move function whenever the mode is $(off, closed)$ or $(on, closed)$, and $t_d \geq 0$. In addition, *door_close* is allowed whenever the mode is $(off, open)$ or $(on, open)$, and $t_d \geq 0$.
- For all (q,x), $M_e^{cts}(q,x) = D$.

Transitions

- We specify the continuous dynamics f by defining functions $f_q : X \times U \times D \rightarrow X$ for each $q \in Q$. The functions f_q specify the following dynamics for T_{ae}:

$$\begin{array}{rcl} f_{q_1} : \dot{T}_{ae}(t) & = & -\frac{1}{c_a}(\mu_{ae} + \mu_{dc})T_{ae}(t) + \frac{1}{c_a}(u_b(t) + d_e(t)) \\ f_{q_2} : \dot{T}_{ae}(t) & = & -\frac{1}{c_a}(\mu_{ae} + \mu_{dc})T_{ae}(t) + \frac{1}{c_a}(u_b(t) + d_e(t) + w_s^{max}) \\ f_{q_3} : \dot{T}_{ae}(t) & = & -\frac{1}{c_a}(\mu_{ae} + \mu_{do})T_{ae}(t) + \frac{1}{c_a}(u_b(t) + d_e(t) + w_s^{max}) \\ f_{q_4} : \dot{T}_{ae}(t) & = & -\frac{1}{c_a}(\mu_{ae} + \mu_{do})T_{ae}(t) + \frac{1}{c_a}(u_b(t) + d_e(t)). \end{array} \tag{34}$$

  In all modes, the dynamics of the door timer are specified as $\dot{t}_d(t) = 1$.
- The δ discrete transition function is depicted in Figure 12.

Moreover, to avoid nonZeno controllers (which appear to enforce safety properties but only by virtue of causing time to stop), we model the delay between controller actions by introducing a new timer variable t_c with $\dot{t}_c(t) = 1$. The presence of two timers (t_d and t_c) complicates enormously the subsequent task of computing the maximal safe set if our procedure presented in the previous section is not used.

6.3 Parameter settings

The ensuing explanations of the computations required to synthesize a controller are largely independent of the specific parameters chosen. However, for illustrative purposes, we explicitly perform the computations over particular parametrizations in order to demonstrate the procedure in practice.

The parameters are specified for the hybrid automaton model that appears in Figure 12. The safety requirement for the system is to maintain the temperature between a lower threshold value of $T_{ae}^{min} = 18$ and an upper threshold value of $T_{ae}^{max} = 20$. The only parameter affecting the discrete dynamics is the reset ratio, which is set to $r = 0.95$.

The continuous dynamics is expressed via a normalized value of $c_a = 1$. The domain of continuous controller input values is $U = [0, U_b = 0.5]$. The domain of continuous disturbance input values is $D = [0, D_e = 0.01]$. The maximum power of the stove is $w_s^{max} = 0.2$. The conductances

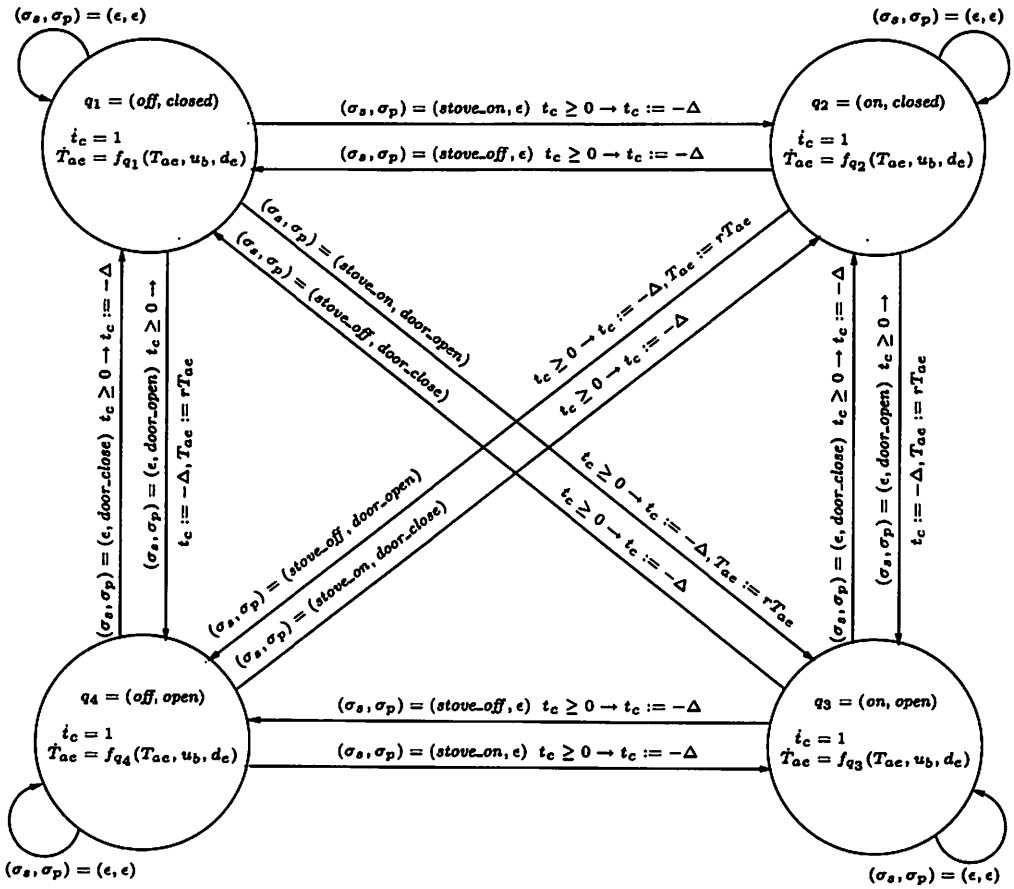


Figure 12: Hybrid model of the room.

are such that $\mu_{ae} + \mu_{dc} = 0.001$ and $\mu_{ae} + \mu_{do} = 0.002$. Thus the dynamics at mode q in (34) can be reexpressed as

$$\dot{T}_{ae}(t) = -\mu(q)T_{ae}(t) + w(q) + u(t) + d(t) \tag{35}$$

where

$$\mu(q) = \begin{cases} 0.002 & \text{if } q \in \{(on, open), (off, open)\} \\ 0.001 & \text{if } q \in \{(on, closed), (off, closed)\} \end{cases}$$

and

$$w(q) = \begin{cases} 0.2 & \text{if } q \in \{(on, open), (on, closed)\} \\ 0 & \text{if } q \in \{(off, open), (off, closed)\} \end{cases}$$

7 Controller Synthesis of Heater + 1 Timer with Standard Procedure

7.1 Computation of discrete controllable predecessors

We show how to compute $Pre_c(W)$ mode by mode. Consider q_1. The controller has two choices of actions (*stove_on* and ϵ) to force a discrete move to the set W. Consider first the *stove_on* action. It is only enabled when $t_c \geq 0$. In the hybrid automaton, there may be a discrete jump to either q_2 or q_3, depending on the discrete move of the environment. Suppose the environment chooses $\sigma_e = \epsilon$, thereby causing a jump to q_2. Then since the timer is reset to $t_c = -\Delta$ and the temperature unchanged, the states (t_c, T_{ae}) land in $W|_{q_2}$ iff $(-\Delta, T_{ae}) \in W|_{q_2}$ and $t_c \geq 0$ iff $(t_c, T_{ae}) \in W|_{q_2}^{-\Delta} \cap \mathcal{T}_{\geq 0}$. Suppose the environment chooses $\sigma_e =$ *door_open*, thereby causing a jump to q_3. Then since the timer is reset to $t_c = -\Delta$ and the temperature T_{ae} is reset to rT_{ae}, the states (t_c, T_{ae}) land in $W|_{q_3}$ iff $(-\Delta, r\ T_{ae}) \in W|_{q_3}$ and $t_c \geq 0$ iff $(t_c, T_{ae}) \in W|_{q_3}^{-\Delta r} \cap \mathcal{T}_{\geq 0}$. Thus the discrete action *stove_on* witnesses the inclusion of (q_1, x) in $Pre_c(W)$ iff $x = (t_c, T_{ae})$ meets both the conditions above for the choice of environment action iff $(t_c, T_{ae}) \in W|_{q_2}^{-\Delta} \cap W|_{q_3}^{-\Delta r} \cap \mathcal{T}_{\geq 0}$.

Consider next the case of the ϵ action. The action is always enabled in the controller. Furthermore, the ϵ move is always enabled in the environment, i.e., for all $(q, x) \in \mathcal{C}$, $\epsilon \in M_e^{disc}(q, x)$. Thus the condition $(\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \wedge \delta((q, x), (\sigma_c, \sigma_e)) \subseteq W$ inside the quantifications in the definition of Pre_c is FALSE because of the first conjunct. Therefore $\sigma_c = \epsilon$ cannot be an existential witness for any (q, x).

Analogous reasoning for the other modes yields the set $Pre_c(W)$ given by:

$$\begin{aligned} Pre_c(W)|_{q_1} &= W|_{q_2}^{-\Delta} \cap W|_{q_3}^{-\Delta r} \cap \mathcal{T}_{\geq 0} \\ Pre_c(W)|_{q_2} &= W|_{q_1}^{-\Delta} \cap W|_{q_4}^{-\Delta r} \cap \mathcal{T}_{\geq 0} \\ Pre_c(W)|_{q_3} &= W|_{q_1}^{-\Delta} \cap W|_{q_4}^{-\Delta} \cap \mathcal{T}_{\geq 0} \\ Pre_c(W)|_{q_4} &= W|_{q_2}^{-\Delta} \cap W|_{q_3}^{-\Delta} \cap \mathcal{T}_{\geq 0} \end{aligned} \tag{36}$$

7.2 Computation of discrete uncontrollable predecessors

The set $Pre_e(W)$ of discrete uncontrollable predecessors can also be computed mode by mode. Consider, for example, q_1. The enabled controller events for this mode are *stove_on* and ϵ. We need to evaluate for each choice the sets of configurations satisfying the inner existential quantification appearing in Definition 2.2.3, and take their intersection. Consider the *stove_on* action. It is in the M_c^{disc} set iff $t_c \geq 0$. If it is enabled, then there exists a witnessing σ_e iff the jump to either q_2 or q_3 lands outside W. The jump to q_2 resets the timer to $t_c = -\Delta$, and so the states (t_c, T_{ae}) land outside of $W|_{q_2}$ iff $(-\Delta, T_{ae}) \notin W|_{q_2}$ and $t_c \geq 0$ iff $(t_c, T_{ae}) \notin W|_{q_2}^{-\Delta} \cap \mathcal{T}_{\geq 0}$. The jump to q_3 resets the timer to $t_c = -\Delta$ and changes the temperature T_{ae} to rT_{ae}, so the states (t_c, T_{ae}) land outside of $W|_{q_3}$ iff $(-\Delta, r\ T_{ae}) \notin W|_{q_3}$ and $t_c \geq 0$ iff $(t_c, T_{ae}) \notin W|_{q_3}^{-\Delta r} \cap \mathcal{T}_{\geq 0}$. So if the controller chooses *stove_on*, then the environment can force the system out of W iff $(t_c, T_{ae}) \in (\overline{W|_{q_2}^{-\Delta}} \cup \overline{W|_{q_3}^{-\Delta r}}) \cap \mathcal{T}_{\geq 0}$.

For the ϵ controller action, the existential formula is satisfied iff $(q, x) \in \overline{W|_{q_4}^{-\Delta r}} \cap \mathcal{T}_{\geq 0}$, corresponding to the *door_open* environmental discrete action. Finally, observe that for $t_c < 0$, no non-trivial pairs of discrete actions are enabled. Thus putting it all together, we get that the configurations at q_1 in the Pre_e set have $(t_c, T_{ae}) \in (\overline{W|_{q_2}^{-\Delta}} \cup \overline{W|_{q_3}^{-\Delta r}}) \cap \overline{W|_{q_4}^{-\Delta r}} \cap \mathcal{T}_{\geq 0}$

The set $Pre_e(W)$ is computed mode by mode as:

$$\begin{aligned}
Pre_e(W)|_{q_1} &= (\overline{W|_{q_3}^{-\Delta r}} \cup \overline{W|_{q_2}^{-\Delta}}) \cap (\overline{W|_{q_4}^{-\Delta r}} \cap \mathcal{T}_{\geq 0}) \\
Pre_e(W)|_{q_2} &= (\overline{W|_{q_4}^{-\Delta r}} \cup \overline{W|_{q_1}^{-\Delta}}) \cap (\overline{W|_{q_3}^{-\Delta r}} \cap \mathcal{T}_{\geq 0}) \\
Pre_e(W)|_{q_3} &= (\overline{W|_{q_4}^{-\Delta}} \cup \overline{W|_{q_1}^{-\Delta}}) \cap (\overline{W|_{q_2}^{-\Delta}} \cap \mathcal{T}_{\geq 0}) \\
Pre_e(W)|_{q_4} &= (\overline{W|_{q_3}^{-\Delta}} \cup \overline{W|_{q_2}^{-\Delta}}) \cap (\overline{W|_{q_1}^{-\Delta}} \cap \mathcal{T}_{\geq 0})
\end{aligned} \tag{37}$$

7.3 Computation of continuous uncontrollable predecessors

In a continuous–time step of the procedure reported in Figure 4, the set $Unavoid\_Pre(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i)) \subset Q \times X$ is computed as the union of the sets

$$(q, Unavoid\_Pre(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i)) \qquad \text{for } q \in \{q_1, q_2, q_3, q_4\} ,$$

where, introducing $B = Pre_e(W^i) \cup \overline{W^i}$ and $E = Pre_c(W^i)$ and according to (1),

$$\begin{aligned}
Unavoid_Pre(B,E)|_q = \{\hat{x} \in X \mid \forall u_b \in \mathcal{U}_b \; \exists \bar{t} \in \mathbb{R}_{>0} \exists d_e \in \mathcal{D}_e \textit{ such that for the trajectory} \\
x : \mathbb{R}_{\geq 0} \to X \textit{ defined by } x(t) = \psi_q(u_b, d_e, \hat{x}, t) \textit{ for all } t \geq 0, \textit{ we have:} \\
\forall \tau \in [0, \bar{t}) \; x(\tau) \in Wait|_q \cap \overline{E}|_q \; \wedge \; x(\bar{t}) \in B|_q\}.
\end{aligned} \tag{38}$$

We restrict the analysis to $X = [-\Delta, \infty) \times \mathbb{R}$, since t_c is always reset to $-\Delta$ and $\dot{t}_c = 1 > 0$.

In the computation of $Unavoid\_Pre(B,E)|_q$ both the state q and the sets $B|_q$, $E|_q$ are fixed. Hence, we rewrite the continuous–time dynamics as

$$\dot{t}_c = 1 \tag{39}$$

$$\dot{T}_{ae} = aT_{ae} + b(u_b + d_e) + b_0 \tag{40}$$

with a, b and b_0 chosen according to (34).

Since in (38) the objective is to find the states that can be steered to $B|_q$ without passing through $E|_q$, and then to remove them from $W^i|_q$, the region to be investigated can be limited to the set

$$R|_q = W^i|_q \setminus (E|_q \cup B|_q) . \tag{41}$$

The boundary $\partial R|_q$ of $R|_q$ is made by arcs of $\partial E|_q$ and arcs of $\partial B|_q$, boundaries of $E|_q$ and $B|_q$ respectively, and segments that lie on $t_c = -\Delta$. Since $\dot{t}_c = 1$, trajectories starting inside $R|_q$ cannot exit $R|_q$ through the boundary of $R|_q$ that lies on $t_c = -\Delta$. That is, for any $\hat{x} \in R|_q$, under any $u_b \in \mathcal{U}_b$ and $d_e \in \mathcal{D}_e$, either $\psi_q(u_b, d_e, \hat{x}, t)$ remains in $R|_q$ for all $t > 0$ or intersects, at some time $t = \bar{t}$, either $\partial E|_q \cap \partial R|_q$ or $\partial B|_q \cap \partial R|_q$.

By definition (38), the set $Unavoid\_Pre(B,E)|_q$ corresponds to the playable set for the disturbance d_e in a two–player differential game defined as follows (see [Isa67]).

Problem 7.1 *Given an initial state $x_0 \in R|_q$, the disturbance d_e wants to steer x_0 to $\partial B|_q \cap \partial R|_q$, while the control u_b opposes it (u_b wants to steer x_0 to $\partial E|_q \cap \partial R|_q$).*

Definition 7.1 *The playable set for d_e in the two–player differential game 7.1 is given by the points of $R|_q$ from which the player d_e can guarantee to drive the initial state to the target set $\partial B|_q \cap \partial R|_q$, no matter what control actions are taken by u_b to the contrary.*

7.3.1 Candidate boundary curves from the solution of a Min–Max Problem.

In the sequel it is shown how a family of curves sufficient for the description of the boundary of the playable set for d_e can be derived from the solution of a min–max problem (see [VG97]).

Introduce the adjoint variables λ_1, λ_2 and the Hamiltonian associated to the dynamics (39),(40)

$$H(t_c, T_{ae}, \lambda_1, \lambda_2, d_e, u_b) = \lambda_1 \dot{t}_c + \lambda_2 \dot{T}_{ae} = \lambda_1 + \lambda_2 (a T_{ae} + b(u_b + d_e) + b_0) \ . \tag{42}$$

If $d_e^\star(t), u_b^\star(t)$ generate a trajectory $[t_c^\star(t), T_{ae}^\star(t)]^T$ on the boundary of the playable set, then there exists a nonzero continuous trajectory $[\lambda_1(t), \lambda_2(t)]^T$, satisfying

$$\dot{\lambda}_1 = -\frac{\partial H}{\partial t_c} = 0 \ \text{ and } \ \dot{\lambda}_2 = -\frac{\partial H}{\partial T_{ae}} = -a\lambda_2 \ , \tag{43}$$

such that $[\lambda_1(t), \lambda_2(t)]^T$ is an outward normal to the boundary of the playable set and

$$\min_{d_e \in \mathcal{D}_e} \max_{u_b \in \mathcal{U}_b} H(t_c^\star, T_{ae}^\star, \lambda_1, \lambda_2, d_e, u_b) = H(t_c^\star, T_{ae}^\star, \lambda_1, \lambda_2, d_e^\star, u_b^\star) = 0 \ . \tag{44}$$

By (42), the signals $d_e^\star(t)$, $u_b^\star(t)$ that satisfy the min–max condition (44) are such that $d_e^\star(t) = \arg\min_{d_e \in \mathcal{D}_e} \{\lambda_2(t) b \ d_e\}$ and $u_b^\star(t) = \arg\max_{u_b \in \mathcal{U}_b} \{\lambda_2(t) b \ u_b\}$, that is

$$d_e^\star(t) = \begin{cases} 0, & \text{if } b\lambda_2(t) > 0 \\ D_e, & \text{if } b\lambda_2(t) < 0 \end{cases} \ \text{ and } \ u_b^\star(t) = \begin{cases} U_b, & \text{if } b\lambda_2(t) > 0 \\ 0, & \text{if } b\lambda_2(t) < 0 \end{cases} \ . \tag{45}$$

Since by (43) $\lambda_2(t) = e^{-at}\lambda_{20}$, where $\lambda_{20} = \lambda_2(0)$, then if $\lambda_{20} \neq 0$, d_e and u_b are constant along the boundary of the playable set, because $b\lambda_2(t)$ never changes in sign. Moreover, by (43), λ_1 is also constant, say $\lambda_1(t) = \lambda_{10}$.

If $\lambda_{20} = 0$ then $\lambda_2(t) = 0$ for all t and a singular control may occur. However, singular controls cannot take place; in fact, by (44),(42) $\lambda_1(t)$ has to be zero if $\lambda_2(t) = 0$, which is against the request of $[\lambda_1(t), \lambda_2(t)]^T$ being nonzero.

Then, a trajectory

$$\begin{bmatrix} t_c(t) \\ T_{ae}(t) \end{bmatrix} = \begin{bmatrix} t_c(0) + t \\ e^{at} T_{ae}(0) + \left(1 - e^{at}\right) \left[-a^{-1} b \left(u_b + d_e\right) - a^{-1} b_0\right] \end{bmatrix} \ . \tag{46}$$

solution to (39),(40) with constant inputs $u_b = u_b^\star$ and $d_e = d_e^\star$ chosen according to (45) satisfies the min–max necessary condition to belong to the boundary of the playable set.

One can easily check that along a trajectory of type (46), T_{ae} is monotonic with respect to t_c. Hence, if an arc of trajectory (46) lies on the boundary of the playable set then the playable set is either below or above it, and an outward normal $[\lambda_1(t), \lambda_2(t)]^T$ of the playable set has either $\lambda_2 > 0$ in the former case (the arc is an upper boundary) or $\lambda_2 < 0$ in the latter case (the arc is a lower boundary). According to (45), if such trajectory defines an upper boundary, then (since $\lambda_2 > 0$) necessarily $d_e = 0$ and $u_b = U_b$; else if it defines a lower boundary, then (since $\lambda_2 < 0$) $d_e = D_e$ and $u_b = 0$.

In conclusion, a family of curves whose arcs can be part of the boundary of the playable set for the disturbance d_e in the two–player differential game 7.1 is given by

$$\varphi^{upper}_{(\hat{t}_c, \hat{T}_{ae})} = \left\{ \begin{bmatrix} t_c \\ T_{ae} \end{bmatrix} \Big| \begin{bmatrix} t_c \\ T_{ae} \end{bmatrix} = \begin{bmatrix} \hat{t}_c + \beta \\ e^{a\beta} \hat{T}_{ae} + \left(1 - e^{a\beta}\right) \left[-a^{-1} b U_b - a^{-1} b_0\right] \end{bmatrix} \text{ with } \beta \geq -\hat{t}_c - \Delta \right\} \tag{47}$$

for an upper boundary of the playable set and

$$\varphi^{lower}_{(\hat{t}_c,\hat{T}_{ae})} = \left\{ \begin{bmatrix} t_c \\ T_{ae} \end{bmatrix} \mid \begin{bmatrix} t_c \\ T_{ae} \end{bmatrix} = \begin{bmatrix} \hat{t}_c + \beta \\ e^{a\beta}\hat{T}_{ae} + (1 - e^{a\beta})\left[-a^{-1}b\, D_e - a^{-1}b_0\right] \end{bmatrix} \text{ with } \beta \geq -\hat{t}_c - \Delta \right\} \tag{48}$$

for a lower boundary of the playable set. Curves $\varphi^{upper}_{(\hat{t}_c,\hat{T}_{ae})}$, $\varphi^{lower}_{(\hat{t}_c,\hat{T}_{ae})}$ in (47),(48) are parametrized by the point $(\hat{t}_c, \hat{T}_{ae})$ through which they pass.

7.3.2 Geometric properties of $B|_q$ and $E|_q$.

By induction, it will be shown that at any step of the procedure the sets $B|_q = (Pre_e(W^i) \cup \overline{W^i})|_q$ and $E|_q = Pre_c(W^i)|_q$ satisfy the following properties:

P1 *There exist* T^{0d}_{ae}, T^{0u}_{ae} *such that*

$$E|_q \;=\; \{(t_c, T_{ae}) | t_c \geq 0,\; T^{0d}_{ae} < T_{ae} < T^{0u}_{ae}\} \tag{49}$$

P2 *For any* $\bar{t}_c \geq -\Delta$ *the set of points* (t_c, T_{ae}) *that lie on the line* $t_c = \bar{t}_c$ *and do not belong to* $B|_q$ *is connected, i.e., either it is the empty set or it is a segment.*

Introduce $B^u|_q$, $B^d|_q$ such that $B|_q = B^u|_q \cup B^d|_q$ and, for any $t_c \geq -\Delta$, $B^u|_q$ contains the upper part of $B|_q$ while $B^d|_q$ contains the lower part of $B|_q$.

P3 *There exist* T^{1u}_{ae}, T^{1d}_{ae} *such that*

$$B^u|_q \cap \{(t_c, T_{ae}) | t_c \geq 0\} \;=\; \{(t_c, T_{ae}) | t_c \geq 0,\; T_{ae} \geq T^{1u}_{ae}\} \tag{50}$$

$$B^d|_q \cap \{(t_c, T_{ae}) | t_c \geq 0\} \;=\; \{(t_c, T_{ae}) | t_c \geq 0,\; T_{ae} \leq T^{1d}_{ae}\} \tag{51}$$

P4 $\partial E|_q \cap (\partial B^u|_q \cup \partial B^d|_q) \neq \emptyset$.

Lemma 7.1 *By property* **P4**, *in (49), (50) and (51), either* $T^{1u}_{ae} = T^{0u}_{ae}$ *(if* $\partial E|_q \cap \partial B^u|_q \neq \emptyset$ *) or* $T^{1d}_{ae} = T^{0d}_{ae}$, *(if* $\partial E|_q \cap \partial B^d|_q \neq \emptyset$ *), or both.*

It is easy to verify that properties **P1-4** hold at the initial step where $W^0 = Good$. According to (36) and (37), $E|_q$, $B|_q$ evaluate to (see Figure 13)

$$\begin{array}{lcll} B^u|_q &=& \{(t_c, T_{ae}) | t_c \geq -\Delta, T_{ae} \geq T^{max}_{ae}\} & \text{for } q = q_1, q_2, q_3, q_4 \\ B^d|_q &=& \{(t_c, T_{ae}) | t_c \geq -\Delta, T_{ae} \leq T^{min}_{ae} \text{ if } t_c < 0, T_{ae} \leq (1/r)T^{min}_{ae} \text{ if } t_c \geq 0\} & \text{for } q = q_1, q_2 \\ B^d|_q &=& \{(t_c, T_{ae}) | t_c \geq -\Delta, T_{ae} \leq T^{min}_{ae}\} & \text{for } q = q_3, q_4 \\ E|_q &=& \{(t_c, T_{ae}) | t_c \geq 0, (1/r)T^{min}_{ae} < T_{ae} < T^{max}_{ae}\} & \text{for } q = q_1, q_2 \\ E|_q &=& \{(t_c, T_{ae}) | t_c \geq 0, T^{min}_{ae} < T_{ae} < T^{max}_{ae}\} & \text{for } q = q_3, q_4 \end{array} \tag{52}$$

Hence, choosing in (50),(51),(49)

$$T^{1u}_{ae} = T^{0u}_{ae} = T^{max}_{ae}, \qquad T^{1d}_{ae} = T^{0d}_{ae} = \begin{cases} (1/r)T^{min}_{ae} & \text{for } q = q_1, q_2 \\ T^{min}_{ae} & \text{for } q = q_3, q_4 \end{cases} \tag{53}$$

properties **P1-4** are verified.

The induction proof will be completed by showing that, assuming **P1-4** to hold at step i for $(Pre_e(W^i) \cup \overline{W^i})|_q$ and $Pre_c(W^i)|_q$, the continuous step produces a set $W^{(i+1)}$ such that **P1-4** will be also verified by $(Pre_e(W^{i+1}) \cup \overline{W^{i+1}})|_q$ and $Pre_c(W^{i+1})|_q$, computed as in Sections 7.2 and 7.1 respectively.

7.3.3 Boundary curves of $Unavoid\_Pre^i|_q = Unavoid\_Pre(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i))|_q$.

As a consequence of **P2**, namely that $B|_q$ consists of two disconnected sets $B^u|_q$ and $B^d|_q$, if follows that the playable set for d_e, i.e., the set $Unavoid\_Pre^i|_q$, is also the union of two sets. Let the curves Π^i_{down} and Π^i_{up} denote, respectively, the lower boundary of the upper part and the upper boundary of the lower part of $Unavoid\_Pre^i|_q$.

Boundary curves of $Unavoid\_Pre^0|_q$. Let us consider the step 0 of the procedure and let us evaluate the boundaries Π^0_{up} and Π^0_{down} of $Unavoid\_Pre(Pre_e(W^0) \cup \overline{W^0}, Pre_c(W^0))|_q$ with $W^0 = Good$. $B|_q = (Pre_e(W^0) \cup \overline{W^0})|_q$ and $E|_q = Pre_c(W^0))|_q$ as in (52) are reported in Figure 13. From (41), the sets $R|_q$ of interest in the continuous part of the procedure are

$$R|_q = \{(t_c, T_{ae}) | -\Delta \le t_c < 0, T_{ae}^{min} < T_{ae} < T_{ae}^{max}\} \qquad \text{for } q = q_1, q_2, q_3, q_4.$$

Note that in this case all the sets $R|_q$ are defined for $t_c \le 0$.

In Section 7.3.1 it has been shown that arcs on the curves $\varphi^{upper}_{(\hat{t}_c, \hat{T}_{ae})}$, $\varphi^{lower}_{(\hat{t}_c, \hat{T}_{ae})}$ of type (47),(48) are candidates to be pieces of the boundary Π^0_{up} and Π^0_{down}, respectively, under a proper choice of $(\hat{t}_c, \hat{T}_{ae})$.

Consider first the computation of the upper boundary Π^0_{up} of the lower part of $Unavoid\_Pre^0|_q$ and refer to Step 0 in Figure 13. By (45), the min–max control is $d_e(t) = d_e^* = D_e$ and $u_b(t) = u_b^* = 0$, whose corresponding equilibrium temperature evaluates to $-\frac{b}{a} D_e - \frac{b_0}{a}$.

- If T_{ae}^{max} is lower than $-\frac{b}{a} D_e - \frac{b_0}{a}$ then, along any arc $\varphi^{lower}_{(\hat{t}_c, \hat{T}_{ae})} \cap R|_q$, T_{ae} versus t_c is increasing. Then, for any choice of the control $u_b(t) \in \mathcal{U}_b$, the disturbance $d_e(t) = d_e^* = D_e$ can force a state $\hat{x} \in R|_q$ in a neighborhood of $T_{ae} = T_{ae}^{max}$ to enter $B^u|_q$. Further, the boundary of the set of points $\hat{x} \in R|_q$ that can be steered by d_e to $B^u|_q$ without intersecting first $E|_q$ is given by $\varphi^{lower}_{(0, T_{ae}^{max})} \cap R|_q$. Note that the end point (t_c^l, T_{ae}^l) of $\varphi^{lower}_{(0, T_{ae}^{max})} \cap R|_q$ different from $(0, T_{ae}^{max})$ has either $t_c^l = -\Delta$ and $T_{ae}^l \in [T_{ae}^{min}, T_{ae}^{max})$, or $t_c^l > -\Delta$ and $T_{ae}^l = T_{ae}^{min}$.

  Hence, according to (38), Π^0_{up} is made by: the arc $\varphi^{lower}_{(0, T_{ae}^{max})} \cap R|_q$, the half line $[0, \infty) \times T_{ae}^{max}$ obtained choosing in (38) $\bar{t} = 0$, and, if $t_c^l > -\Delta$, the segment $[-\Delta, t_c^l] \times T_{ae}^{min}$.

- Otherwise, if $T_{ae}^{max} \ge -\frac{b}{a} D_e - \frac{b_0}{a}$, then there exists some control $u_b \in \mathcal{U}_b$ such that for any disturbance d_e, T_{ae} decreases. Hence, d_e cannot force a state $\hat{x} \in R|_q$ in a neighborhood of $T_{ae} = T_{ae}^{max}$ to enter $B^u|_q$. In this case, the boundary Π^0_{up} is obtained choosing $\bar{t} = 0$ in (38) and coincides with the boundary $[-\Delta, \infty) \times T_{ae}^{max}$ of $B^u|_q$.

Summarizing

$$\Pi^0_{up} = \begin{cases} \varphi^{lower}_{(0, T_{ae}^{max})} \cap R|_q \cup [0, \infty) \times T_{ae}^{max} & \text{if } t_c^l = -\Delta \\ & \text{if } T_{ae}^{max} < -\frac{b}{a} D_e - \frac{b_0}{a} \\ \varphi^{lower}_{(0, T_{ae}^{max})} \cap R|_q \cup [0, \infty) \times T_{ae}^{max} \cup [-\Delta, t_c^l] \times T_{ae}^{min} & \text{if } t_c^l > -\Delta \\ [-\Delta, \infty) \times T_{ae}^{max} & \text{if } T_{ae}^{max} \ge -\frac{b}{a} D_e - \frac{b_0}{a} \end{cases} \tag{54}$$

Consider now the computation of the lower boundary Π^0_{down} of the upper part of $Unavoid\_Pre^0|_q$ and refer again to Step 0 in Figure 13. The evaluation of Π^0_{down} for the modes q_3 and q_4, where

$T_{ae}^{1d} = T_{ae}^{0d} = T_{ae}^{min}$, is completely analogous to the development above and is reported first. A little more involved is the evaluation of Π_{down}^0 for q_1 and q_2, where $T_{ae}^{1d} = T_{ae}^{0d} = (1/r)T_{ae}^{min} > T_{ae}^{min}$.

Consider first q_3 and q_4.

- If T_{ae}^{min} is greater than $-\frac{b}{a}U_b - \frac{b_0}{a}$, i.e., the equilibrium temperature under the min–max control $d_e(t) = d_e^* = 0$ and $u_b(t) = u_b^* = U_b$ (see (45)), then along any arc $\varphi^{upper}_{(\hat{t}_c,\hat{T}_{ae})} \cap R|_q$, given by (47), T_{ae} versus t_c is decreasing. Hence, for any choice of $u_b(t) \in \mathcal{U}_b$, $d_e(t) = d_e^* = 0$ can force a state $\hat{x} \in R|_q$ in a neighborhood of $T_{ae} = T_{ae}^{min}$ to enter $B^d|_q$. Further, the boundary of the set of points in $R|_q$ that can be steered by d_e to $B^d|_q$ without intersecting first $E|_q$ is given by $\varphi^{upper}_{(0,T_{ae}^{min})} \cap R|_q$. Note that the end point (t_c^u, T_{ae}^u) of $\varphi^{upper}_{(0,T_{ae}^{min})} \cap R|_q$ different from $(0, T_{ae}^{min})$ has either $t_c^u = -\Delta$ and $T_{ae}^u \in (T_{ae}^{min}, T_{ae}^{max}]$, or $t_c^u > -\Delta$ and $T_{ae}^u = T_{ae}^{max}$. According to (38), Π_{down}^0 is made by: the arc $\varphi^{upper}_{(0,T_{ae}^{min})} \cap R|_q$, the half line $[0,\infty) \times T_{ae}^{min}$ obtained choosing in (38) $\bar{t} = 0$, and, if $t_c^u > -\Delta$, the segment $[-\Delta, t_c^u) \times T_{ae}^{max}$.
- Otherwise, if $T_{ae}^{min} \leq -\frac{b}{a}U_b - \frac{b_0}{a}$, the disturbance d_e cannot force a state in a neighborhood of $T_{ae} = T_{ae}^{min}$ to enter $B^d|_q$, and the boundary Π_{down}^0 coincides with the boundary $[-\Delta, \infty) \times T_{ae}^{min}$ of $B^d|_q$.

Hence,

$$\Pi_{down}^0 = \begin{cases} \varphi^{upper}_{(0,T_{ae}^{min})} \cap R|_q \cup [0,\infty) \times T_{ae}^{min} & \text{if } t_c^u = -\Delta \\ & \text{if } T_{ae}^{min} > -\frac{b}{a}U_b - \frac{b_0}{a} \\ \varphi^{upper}_{(0,T_{ae}^{min})} \cap R|_q \cup [0,\infty) \times T_{ae}^{min} \cup [-\Delta, t_c^u] \times T_{ae}^{max} & \text{if } t_c^u > -\Delta \\ [-\Delta,\infty) \times T_{ae}^{min} & \text{if } T_{ae}^{min} \leq -\frac{b}{a}U_b - \frac{b_0}{a} \end{cases} \tag{55}$$

Let us now evaluate the boundary Π_{down}^0 for the modes q_1 and q_2, where $T_{ae}^{1d} = T_{ae}^{0d} = (1/r)T_{ae}^{min} > T_{ae}^{min}$.

- Since by (39) t_c always increases, no matter whether or not the temperature T_{ae} increases, states in a neighborhood of the boundary of $B^d|_q$ along the line $t_c = 0$ reach $B^d|_q$ under any d_e and u_b. Again, the boundary of the set of points $\hat{x} \in R|_q$ that can be steered by d_e to $B^u|_q$, without intersecting first $E|_q$, is given by an arc on a curve of type (47) passing through the point $(0, T_{ae}^{1d}) = (0, T_{ae}^{0d})$, i.e., the arc belonging to Π_{down}^0 is $\varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q$.

  The end point (t_c^u, T_{ae}^u) of $\varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q$ has any of $t_c^u = -\Delta$ and $T_{ae}^u \in [T_{ae}^{min}, T_{ae}^{max}]$, $t_c^u > -\Delta$ and $T_{ae}^u = T_{ae}^{max}$, or $t_c^u > -\Delta$ and $T_{ae}^u = T_{ae}^{min}$. Hence, according to (38), Π_{down}^0 is made by: the arc $\varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q$, the half line $[0,\infty) \times T_{ae}^{1d}$ obtained choosing in (38) $\bar{t} = 0$, and if $T_{ae}^u = T_{ae}^{max}$ the segment $[-\Delta, t_c^u] \times T_{ae}^{max}$ else if $T_{ae}^u = T_{ae}^{min}$ the segment $[-\Delta, t_c^u] \times T_{ae}^{min}$.

That is:

$$\Pi_{down}^0 = \begin{cases} \varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{1d} & \text{if } t_c^u = -\Delta \\ \varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{1d} \cup [-\Delta, t_c^u] \times T_{ae}^{min} & \text{if } T_{ae}^u = T_{ae}^{min} \\ \varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{1d} \cup [-\Delta, t_c^u] \times T_{ae}^{max} & \text{if } T_{ae}^u = T_{ae}^{max} \end{cases} \tag{56}$$

Finally, note that the boundaries Π^0_{up} and Π^0_{down} of the two sets that define $Unavoid\_Pre^0|_q$ may actually intersect, in which case the set is connected.

Boundary curves of $Unavoid\_Pre^i|_q$ for $i > 0$. The computation of Π^i_{up} and Π^i_{down} for $i > 0$ makes use of arguments similar to those presented in the computation of Π^0_{down} for $q = q_1, q_2$ reported above, but with the further complication that the sets $R|_q$ are defined also for $t_c > 0$.

The main point here is to establish which points in $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ can be driven by the disturbance to $B|_q = (Pre_e(W^i) \cup \overline{W^i})|_q$ without intersecting first $E|_q = Pre_c(W^i)|_q$.

By properties **P1**, **P3** and Lemma 7.1,

$$R|_q \cap \{(t_c, T_{ae}) | t_c > 0\} = \begin{cases} \{(t_c, T_{ae}) | t_c > 0, T^{0u}_{ae} < T_{ae} < T^{1u}_{ae}\} & \text{if } T^{1d}_{ae} = T^{0d}_{ae} \\ \{(t_c, T_{ae}) | t_c > 0, T^{1d}_{ae} < T_{ae} < T^{0d}_{ae}\} & \text{if } T^{1u}_{ae} = T^{0u}_{ae} \end{cases}$$

for $q = q_1, q_2, q_3, q_4$. Namely, for decreasing values of T_{ae}, sets $R|_q$,$B|_q$ and $E|_q$ for $t_c > 0$ can be in the two following sequences: either (1) $BREB = B^u|_q - R|_q - E|_q - B^d|_q$, if $T^{1d}_{ae} = T^{0d}_{ae}$; or (2) $BERB = B^u|_q - E|_q - R|_q - B^d|_q$, if $T^{1u}_{ae} = T^{0u}_{ae}$.

1. In the case $BREB$ the critical boundary of $R|_q$ is the upper one. In fact, if the disturbance can force T_{ae} to increase, then the trajectories will reach $B^u|_q$ with no escape path through $E|_q$ and $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ will be unsafe.

2. In the case $BERB$ the critical boundary of $R|_q$ is the lower one. In fact, if the disturbance can force T_{ae} to decrease, then the trajectories will reach $B^d|_q$ with no escape path through $E|_q$ and $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ will be unsafe.

In the sequel we illustrate under what conditions the disturbance can force the state to reach $B|_q$.

For the upper boundary Π^i_{up}:

- If $T^{1u}_{ae} < -\frac{b}{a} D_e - \frac{b_0}{a}$, the controller, even setting $u_b = 0$, cannot prevent the temperature from increasing and reaching $B^u|_q$. In the case $BREB$ (i.e., $T^{1d}_{ae} = T^{0d}_{ae}$), $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ is unsafe. Hence $\varphi^{lower}_{(0, T^{0u}_{ae})} \cap R|_q \subset \Pi^i_{up}$;

- If $T^{1u}_{ae} \geq -\frac{b}{a} D_e - \frac{b_0}{a}$, then the disturbance cannot force T_{ae} to increase and in the case $BREB$ (i.e., $T^{1d}_{ae} = T^{0d}_{ae}$), $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ is safe. We have: $\varphi^{lower}_{(0, T^{1u}_{ae})} \cap R|_q \subset \Pi^i_{up}$.

Summarizing, the upper boundary Π^i_{up} of $Unavoid\_Pre^i|_q$ for $i > 0$ is obtained as follows:

$$\Pi^i_{up} = \begin{cases} \begin{cases} \varphi^{lower}_{(0, T^{0u}_{ae})} \cap R|_q \cup [0, \infty) \times T^{0u}_{ae} \cup [-\Delta, t^l_c] \times T^{min}_{ae} & \text{if } t^l_c > -\Delta \\ \varphi^{lower}_{(0, T^{0u}_{ae})} \cap R|_q \cup [0, \infty) \times T^{0u}_{ae} & \text{if } t^l_c = -\Delta \end{cases} & \text{if } T^{1u}_{ae} < -\frac{b}{a} D_e - \frac{b_0}{a} \\ \begin{cases} \varphi^{lower}_{(0, T^{1u}_{ae})} \cap R|_q \cup [0, \infty) \times T^{1u}_{ae} \cup [-\Delta, t^l_c] \times T^{min}_{ae} & \text{if } t^l_c > -\Delta \\ \varphi^{lower}_{(0, T^{1u}_{ae})} \cap R|_q \cup [0, \infty) \times T^{1u}_{ae} & \text{if } t^l_c = -\Delta \end{cases} & \text{if } T^{1u}_{ae} \geq -\frac{b}{a} D_e - \frac{b_0}{a} \end{cases} \tag{57}$$

For the lower boundary Π^i_{down}:

- If $T_{ae}^{1d} > -\frac{b}{a}U_b - \frac{b_0}{a}$, the controller, even setting $u_b = U_b$, cannot prevent the temperature from decreasing and reaching $B^d|_q$. In the case $BERB$ (i.e., $T_{ae}^{1u} = T_{ae}^{0u}$), $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ is unsafe. Hence $\varphi^{upper}_{(0,T_{ae}^{0d})} \cap R|_q \subset \Pi^i_{down}$;

- If $T_{ae}^{1d} \leq -\frac{b}{a}U_b - \frac{b_0}{a}$, then the disturbance cannot force T_{ae} to decrease and in the case $BERB$ (i.e., $T_{ae}^{1u} = T_{ae}^{0u}$), $R|_q \cap \{(t_c, T_{ae}) | t_c > 0\}$ is safe. We have: $\varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q \subset \Pi^i_{down}$.

Hence, the lower boundary Π^i_{down} of $Unavoid\_Pre^i|_q$ for $i > 0$ is:

$$\Pi^i_{down} = \begin{cases} \varphi^{upper}_{(0,T_{ae}^{0d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{0d} \cup [-\Delta, t_c^u] \times T_{ae}^{max} & \text{if } t_c^u > -\Delta \\ & \text{if } T_{ae}^{1d} > -\frac{b}{a}U_b - \frac{b_0}{a} \\ \varphi^{upper}_{(0,T_{ae}^{0d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{0d} & \text{if } t_c^u = -\Delta \\ \varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{1d} \cup [-\Delta, t_c^u] \times T_{ae}^{max} & \text{if } t_c^u > -\Delta \\ & \text{if } T_{ae}^{1d} \leq -\frac{b}{a}U_b - \frac{b_0}{a} \\ \varphi^{upper}_{(0,T_{ae}^{1d})} \cap R|_q \cup [0,\infty) \times T_{ae}^{1d} & \text{if } t_c^u = -\Delta \end{cases} \tag{58}$$

Notice that, also for $i > 0$, it can occur that the boundaries Π^i_{up} and Π^i_{down} of the two sets that define $Unavoid\_Pre^i|_q$ intersect each other, in which case the set becomes connected.

Further, since by (53) $T_{ae}^{1u} = T_{ae}^{0u} = T_{ae}^{max}$ and $T_{ae}^{1d} = T_{ae}^{0d}$, expressions (57),(58) actually apply also for $i = 0$.

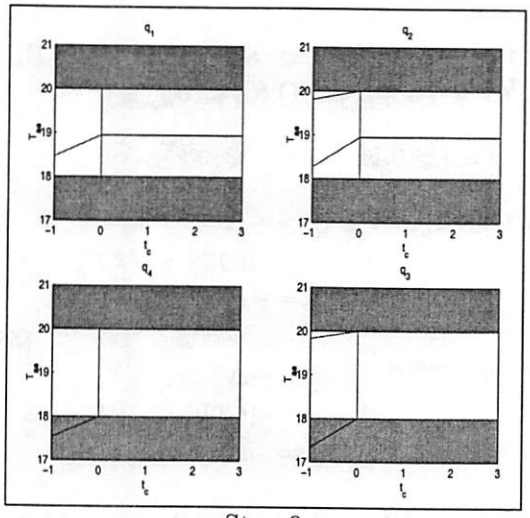
Proof of geometric properties of $B|_q$ and $E|_q$. It is easy to prove by induction that, as assumed in **P1-4**, at any step of the procedure, for $t_c \geq 0$, $B^u|_q$, $B^d|_q$ and $E|_q$ are strips parallel to the t_c axis of the form (50),(51),(49), respectively. In fact, in (53) this is shown to hold for $i = 0$ and the induction step is as follows. Suppose (50),(51),(49) hold for the i-th step of the procedure, then by (57),(58) the boundary Π^i_{up},Π^i_{down} of $Unavoid\_Pre^i|_q$ is made by half lines parallel to the t_c axis for $t_c \geq 0$ and, according to Figure 4, so is the boundary of $W^{i+1}|_q = W^i|_q \setminus (Pre_e(W^i) \cup Unavoid\_Pre^i|_q)$. Hence, from (36) and (37), $(Pree(W^{i+1}) \cup \overline{W^{i+1}})|_q$ and $Pre_c(W^{i+1})|_q$ are strips parallel to the t_c axis for $t_c \geq 0$.

The iterations of the synthesis procedure for the parameters given in Sec. 6.3 appear in Figure 13. We also consider the system with parameter settings as above, except that the controller input is restricted to the range $[0, 0.2]$ instead of $[0, 0.5]$. In this case, there is no valid controller. The initial iterations of the synthesis procedure for this latter system appear in Figure 14.

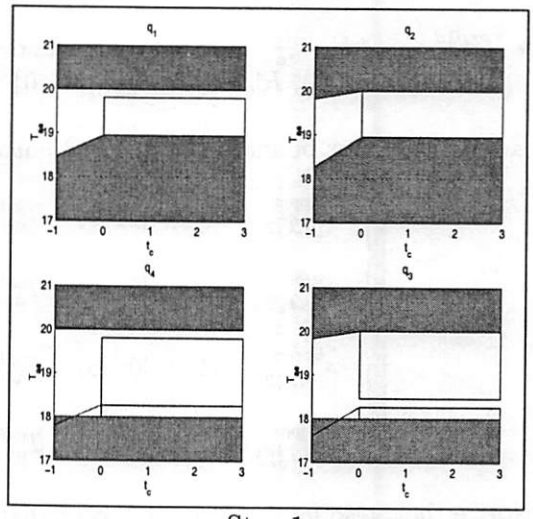
7.4 Controller extraction

The controller derived from the maximal safe set computed in Figure 13 is depicted in Figure 15. The *stove_on* and *stove_off* actions are permitted only in the indicated regions. The watching strategy of playing (ϵ, u) for all u is permitted everywhere, except where otherwise indicated. For instance, no (ϵ, u) event is permitted in modes $(on, open)$ and $(on, open)$ along $T_{ae} = 20$ where $t_c \geq 0$. In particular, this implies that the *stove_off* action must be played by the controller at these configurations.

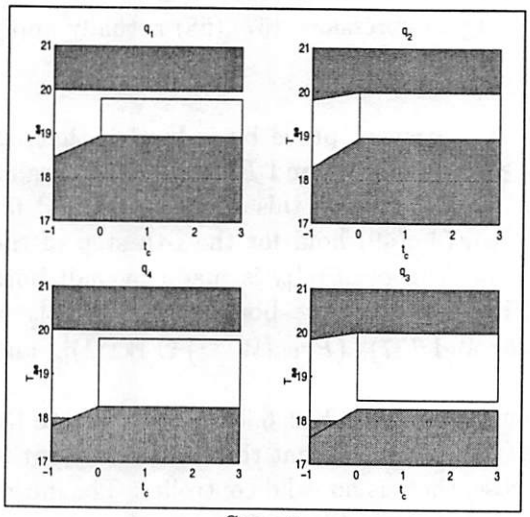
The values of T^{disc} and T^{cts} may be set arbitrarily over $\overline{W}$, since the controller does not operate in that region. Over the set W, the function T^{disc} is defined according to the following rules:



Step 0



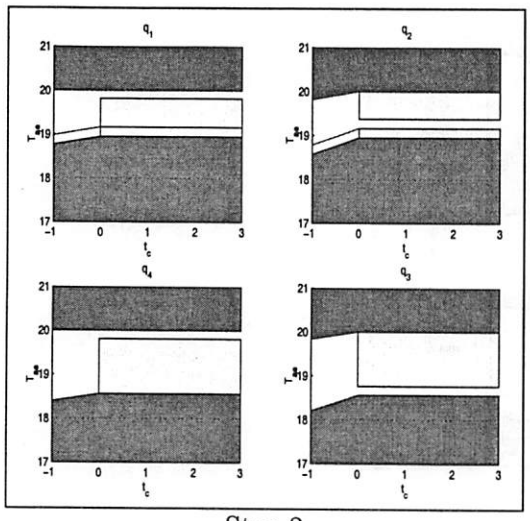
Step 1



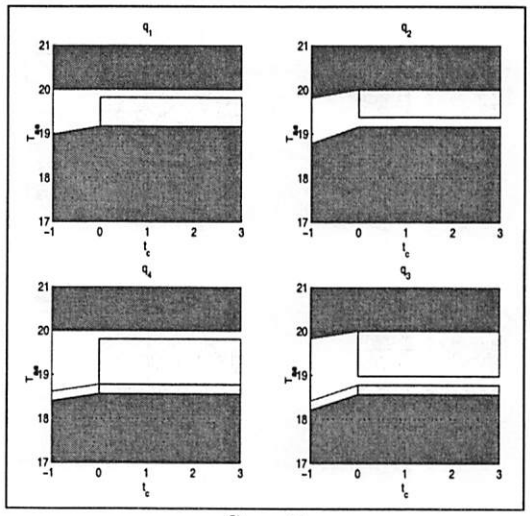
Step 2

Legend. At each step of the procedure the interesting sets are depicted by means of their projection in the continuous space X for all modes q_1, q_2, q_3, q_4. The sets $\overline{W^i}$, $(Pre_0(W^i) \cap W^i)|_q$ and $(Pre_1(W^i) \cap W^i)|_q$ are represented respectively in dark gray, light green and light violet. The set $(Pre_1(W^i) \cup \overline{W^i})|_q$ used in the procedure is given by the union of the light violet and dark gray regions. Arcs of trajectories $\varphi_{(\cdot)}$ candidate to be pieces of the boundary of $Unavoid\_Pre(B^i, E^i)|_q$ are reported for $t_c \in [-\Delta, 0]$.

Figure 13: The procedure converges in three steps and returns the safe set: the set of initial configurations $Safe \subset Q \times X$ from which there is a control strategy $u_b(t)$, σ_s guaranteed to maintain the state trajectory inside $Good$, no matter what actions are taken by the disturbances $d_e(t)$, σ_d. The control actions of the heater $u_b(t)$ (continuous-time) and of the stove σ_s (discrete event) are powerful enough to counteract the disturbances produced by the appliance $d_e(t)$ (continuous-time) and the door σ_d (discrete event).



Step 2



Step 3

Figure 14: The procedure converges but the safe set is empty. From the third step the procedure evolves in a periodic fashion, repeating alternatively patterns similar to those of Step 2 and Step 3, until W^i becomes empty.

Turning on the stove: $stove\_on \in T^{disc}(q, x)$ iff either of the following two conditions hold:

1. $q = (off, closed)$ and $\eta_{closed} \leq T_{ae} \leq \alpha_{closed}$ and $t \geq 0$, or
2. $q = (off, open)$ and $\beta_{on} \leq T_{ae} \leq \alpha_{open}$ and $t \geq 0$.

Turning off the stove: $stove\_off \in T^{disc}(q, x)$ iff either of the following two conditions hold:

1. $q = (on, closed)$ and $\eta_{closed} \leq T_{ae} \leq 20$ and $t \geq 0$, or
2. $q = (on, open)$ and $\beta_{off} \leq T_{ae} \leq 20$ and $t \geq 0$.

Letting time pass: Time may pass in the interior of the safe set, and also at the boundaries, unless there is insufficient control required to counteract the disturbance from making the temperature rise beyond 20 while the stove is on.

- For all $(q, x) \in W$, we have $\epsilon \in T^{disc}(q, x)$ unless $q \in \{(on, closed), (on, open)\}$ and x satisfies $T_{ae} = 20 \wedge t \geq 0$. The excluded configurations are those for which the *stove_off* event must be taken by the controller to remain within the safe set W. In this configurations, setting the continuous control u to its minimal value of 0 will result in the temperature rising above 20, regardless of the continuous disturbance d.

The function T^{cts} is defined over W as follows:

Time passing on the interior of W: For all $(q, x) \in int(W)$, we have $T^{cts}(s) = M_c^{cts}(s) = U$.

Dummy values when time is not allowed to pass: For all configurations $s = (q, x)$ for which $q \in \{(on, closed), (on, open)\}$ and x satisfies $T_{ae} = 20 \wedge t \geq 0$, we set $T^{cts}(s) = M_c^{cts}(s) = U$.

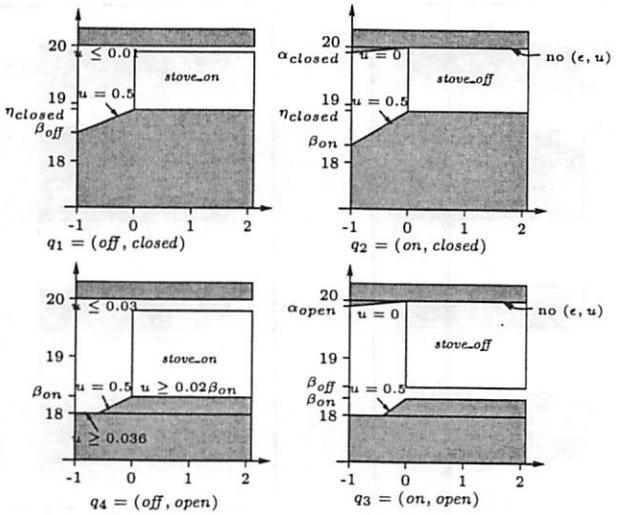


Figure 15: Controller

Time passing on the boundary of W: On the rest of the boundary of W, time is allowed to pass, and we now specify the u values allowed by T^{cts}.

1. For s on the exponential curves that provide lower bounds on W, we set $T^{cts}(s) = \{U_{max}\} = \{0.5\}$, i.e., along the curves passing through $(\gamma_{on}, 18)$ to $(0, \beta_{on})$ in mode $(on, open)$, passing through $(\gamma_{off}, 18)$ to $(0, \beta_{on})$ in mode $(off, open)$, passing through $(-1, \beta_{on})$ to $(0, \eta_{closed})$ in mode $(on, closed)$, and passing through $(-1, \beta_{off})$ to $(0, \eta_{closed})$ in mode $(off, closed)$.
2. For s on the exponential curves that provide upper bounds on W, we set $T^{cts}(s) = \{U_{min}\} = \{0\}$, i.e., along the curves passing through $(-1, \alpha_{open})$ to $(0, 20)$ in mode $(on, open)$ and passing through $(-1, \alpha_{closed})$ to $(0, 20)$ in mode $(on, closed)$.
3. For s along the $T_{ae} = 20$ line in mode $(off, closed)$, we have set $T^{cts}(s) = [0, 0.01]$. The u values are precisely those for which the controller can guarantee the flow remains in W, and are derived from $\dot{T}_{ae} = -0.001T_{ae} + u + d \leq 0$ for all $d \in [0, 0.01]$ iff $\dot{T}_{ae} = -0.001T_{ae} + u + 0.01 \leq 0$ iff $u \leq 0.01$.
4. For s along the $T_{ae} = 20$ line in mode $(off, open)$, we set $T^{cts}(s) = [0, 0.03]$, since $\dot{T}_{ae} = -0.002T_{ae} + u + 0.01 \leq 0$ whenever $u \leq 0.03$.
5. For s along the $T_{ae} = \eta_{closed} \wedge t \geq 0$ segment in mode $(off, closed)$, we set $T^{cts}(s) = [\hat{u}, 0.5]$, where $\hat{u} = 0.0189$, since $\dot{T}_{ae} = -0.001T_{ae} + u \geq 0$ whenever $u \geq 0.001\eta_{closed} = 0.0189$.
6. For s along the $T_{ae} = \eta_{closed} \wedge t \geq 0$ segment in mode $(on, closed)$, we set $T^{cts}(s) = [0, 0.5]$, since $\dot{T}_{ae} = -0.001T_{ae} + 0.2 + u \geq 0$ for all $u \geq 0$.
7. For s along the $T_{ae} = 18$ and $T_{ae} = \beta_{on}$ segments in mode $(on, open)$, we set $T^{cts}(s) = [0, 0.5]$, since $\dot{T}_{ae} = -0.002T_{ae} + 0.2 + u \geq 0$ for all $u \geq 0$.
8. For s along the $T_{ae} = 18$ segment in mode $(off, open)$, we set $T^{cts}(s) = [0.036, 0.5]$, since $\dot{T}_{ae} = -0.002T_{ae} + u \geq 0$ for all $u \geq 0.036$.

9. For s along the $T_{ae} = \beta_{on}$ segment in mode $(off, open)$, we set $T^{cts}(s) = [0.002\beta_{on}, 0.5]$, since $\dot{T}_{ae} = -0.002T_{ae} + u \geq 0$ for all $u \geq 0.002\beta_{on} = 0.036522$.

7.5 Sample trajectories of the controlled system

We provide sample trajectories of the controlled system in order to further highlight the operation of the controller. From any configuration in the maximal safe set W, the controller can act in such a way as to maintain the system configuration in W indefinitely, no matter what the adversarial environment does in its attempts to drive the configuration out of W. Once the configuration is outside W, the specification is not necessarily violated. However, the environment does have a strategy to drive the system into a configuration that violates the specification.

7.5.1 Following a winning controller strategy

We demonstrate the controller's strategy at the lower end of the good interval $[18, 20]$. Let the environment try its best to drive the temperature below 18. The environment can be using either discrete actions (opening and closing the door), or continuous means (varying the disturbance term d) to lower the temperature. Intuitively, as far as discrete actions, the environment's best strategy is to open the door as often as possible, since each instance of opening the door results in a large instantaneous temperature drop. As for its strategy over continuous variables, it should set d to be the minimal value of 0 in order to keep the temperature low.

Suppose the configuration is in mode $(on, open)$ with continuous state $(t, T_{ae}) = (-1, 18)$. Now, suppose the controller sets $u = 0.25$, and the environment sets $d = 0$. See Figure 16. After 1 second, the continuous state is at $\lambda_1 = (-225 + 18)e^{-0.002} + 225 = 18.414$. The configuration is still in W since $\lambda_1 > \beta_{on}$. If the environment closes the door now while the controller stands by watching, then the mode changes to $(on, closed)$, and the continuous state to $(-1, \lambda_1)$. The controller can maintain the u value of 0.25 until the configuration hits the boundary of W, along the flow from $(-1, \beta_{on})$ to $(0, \eta_{closed})$. When the boundary is hit, the controller must set u to its maximal value of 0.5 to stay in the safe set. If the environment causes the door to open as soon as it can, i.e., at continuous state $(0, \eta_{closed})$, then the configuration moves to mode $(on, open)$ with continuous state $(-1, 18)$, and the trajectory segment can repeat.

Consider the slightly different scenario where the environment does not cause the door to open as aggressively. See Figure 16. From mode $(on, open)$ and continuous state $(-1, 18)$, suppose the environment performs no discrete action for 2 seconds. Then the continuous state evolves to $\lambda_2 = (-225 + 18)e^{-0.004} + 225 = 18.826$. The configuration is now in the Pre_0 region of W. It is safe for the controller to close the stove. Suppose that the environment shuts the door at the same time. Then the resultant configuration has mode $(off, closed)$ and continuous state $(-1, \lambda_2)$. With $u = 0.5$, after 1 second, the system arrives at $(0, \lambda_3)$, where $\lambda_3 = (-500 + \lambda_2)e^{-0.001} + 500 = 19.307$. The controller now turns on the stove, with the environment potentially also opening the door. These joint actions lead the configuration to the mode $(on, open)$ with continuous state $(-1, \lambda_4)$, where $\lambda_4 = 0.95\lambda_3 = 18.342$. The trajectory can safely continue with similar controller decisions to those above.

7.5.2 Deviating from a winning controller strategy

We demonstrate example trajectories where a fictitious controller fails to maintain the configuration within W. These trajectories are not allowed by the controller we synthesize. They are merely

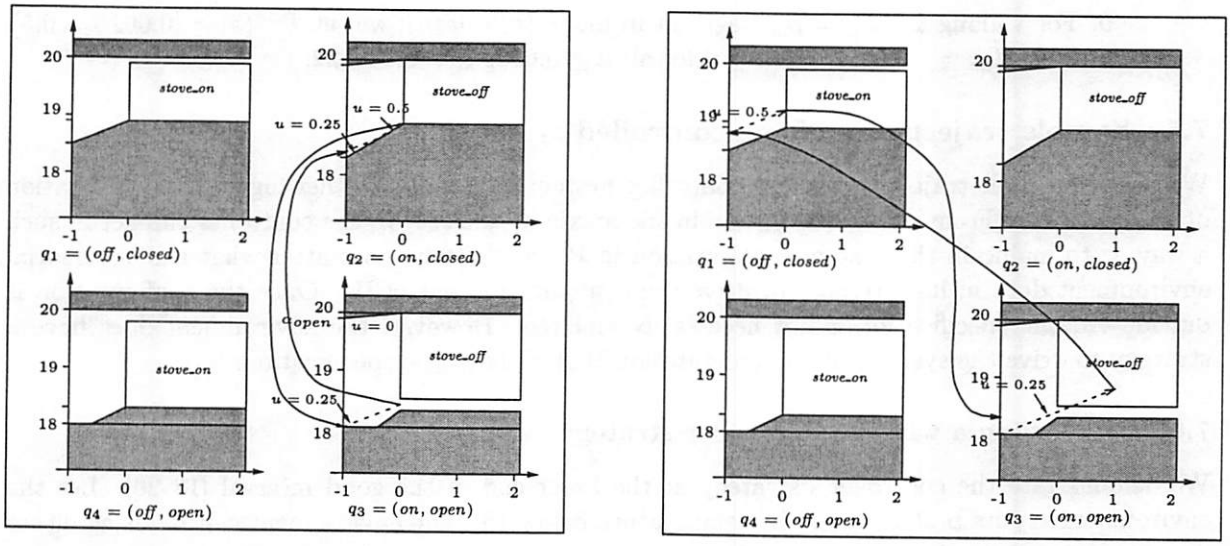


Figure 16: Admissible trajectories: continuous flows are depicted with a dashed line, discrete jumps with dotted line

included to demonstrate what can go wrong if the control strategy drifts from the synthesized one.

If the controller does not maintain sufficiently high u values, the system is in danger of exiting W. We again start at mode $(on, open)$ and continuous state $(-1, 18)$. See Figure 17. For example, with $u = 0.1$, after some time less than 1 second, the system reaches the boundary of W. The controller should then increase u to its maximum value of 0.5. Suppose it fails to do so. Then when $t_c = 0$, the continuous state is at $(0, \lambda_5) \notin W$ where $\lambda_5 = (-150 + 18)e^{-0.002} + 150 = 18.264 < \beta_{on}$. Although the configuration still satisfies the specification, the fact that it is outside W implies that the controller can no longer guarantee that the configuration remains safe indefinitely. An environment action to close the door changes the continuous state to $(-1, \lambda_5)$. The optimal strategy for the controller is to keep the stove on, leading to the mode $(on, closed)$. With maximal control $u = 0.5$, after 1 second the temperature will reach no higher than $\lambda_6 = (-350 + \lambda_5)e^{-0.002} + 350 = 18.927 < \eta_{closed}$. Thus if the door opens then, the temperature will drop to $0.95\lambda_6 = 17.98$, and the safety property is violated.

Finally, we provide a trajectory where a fictitious controller makes a discrete action it should not make. See Figure 17. We start from the same initial configuration as above. This time, the controller sets $u = 0.25$. After 1 second, the temperature hits $\lambda_7 = (-225 + 18)e^{-0.002} + 225 = 18.414$. This temperature lies between β_{on} and β_{off}, and thus the configuration is not in $Pre_0(W)$. If the controller unwisely decides to turn off the stove, disaster can occur, although not immediately. Suppose the door closes at the same time. Then the new configuration is in mode $(off, closed)$ with continuous state $(-1, \lambda_7)$, which is outside W. Now consider the controller's best strategy to keep the temperature from falling below 18. The controller can try to raise the temperature as much as possible by setting $u = 0.5$. After 1 second the temperature is at least, but possibly no more than, $\lambda_8 = (-500 + \lambda_7)e^{-0.001} + 500 = 18.895$. If the door opens now, the new temperature will be $0.95\lambda_8 = 17.950$, thereby violating the specification, regardless of whether the controller turns on the stove to help increase the temperature or not.

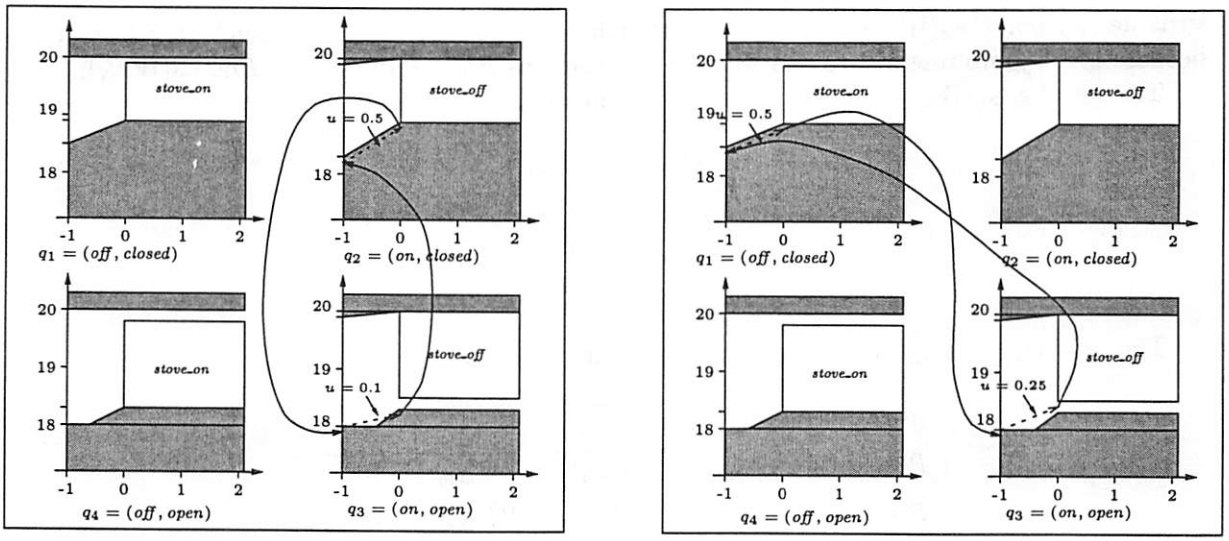


Figure 17: Unadmissible trajectories: controller fails to maintain high enough u value (on the left), controller chooses unwise control action (on the right).

8 Controller Synthesis of Heater + 1 Timer with Timer Projection

We demonstrate the synthesis procedure for hybrid controllers on our heating system. We show how to compute the Pre_c, Pre_e, and *Unavoid_Pre* operators at each iteration for the hybrid automaton shown in Fig. 12. The next subsection describes the parameters in the particular systems we consider. The following subsection examines the discrete controllable and uncontrollable predecessor operators, and the final one the continuous uncontrollable predecessor operator.

8.1 Computation of discrete controllable and uncontrollable predecessors

We first define three useful auxiliary operators. Let $W \subseteq \mathcal{C}$ be a set of configurations, and $q \in Q$ be a mode.

1. Let $W|_q = \{x \in X \mid (q, x) \in W\}$ denote the projection of elements of W onto the continuous state only. The operator $|_q$ distributes with respect to $\cap$ and $\cup$.
2. Let $W|_q^{-\Delta} = \{(t_c, T_{ae}) \mid (-\Delta, T_{ae}) \in W|_q\}$ denote the set of points for which resetting t_c to $-\Delta$ results in a point in $W|_q$.
3. Let $W|_q^{-\Delta r} = \{(t_c, T_{ae}) \mid (-\Delta, r\ T_{ae}) \in W|_q\}$ denote the set of points for which resetting t_c to $-\Delta$ and multiplying T_{ae} by r results in a point in $W|_q$.

In addition, we also define the sets $\mathcal{T}_{\geq 0} = \{(t_c, T_{ae}) \mid t_c \in [0, \infty)\}$ and $\mathcal{T}_{[-\Delta,0)} = \{(t_c, T_{ae}) \mid t_c \in [-\Delta, 0)\}$.

Restricting W to be $W_{-\Delta}$ and $W_{\geq 0}$, the computations of $Pre_c(W)$ and $Pre_e(W)$ can be reformulated as $Pre_{c,\geq 0}(W_{-\Delta}, W_{\geq 0})$ and $Pre_{e,\geq 0}(W_{-\Delta}, W_{\geq 0})$ [3], that are equivalent to projecting away

[3] The sets $Pre_{c,-\Delta}(W_{-\Delta}, W_{\geq 0})$ and $Pre_{e,-\Delta}(W_{-\Delta}, W_{\geq 0})$ do not make sense because no jump is enabled when $t_c = -\Delta$.

variable t_c from $Pre_c(W)$ and $Pre_e(W)$. Actually $Pre_{c,\geq 0}$ and $Pre_{e,\geq 0}$ depend only from $W_{-\Delta}$ because every jump resets t_c to $-\Delta$, so we write them as $Pre_{c,\geq 0}(W_{-\Delta})$ and $Pre_{e,\geq 0}(W_{-\Delta})$.

The set $Pre_{c,\geq 0}(W_{-\Delta})$ is computed mode by mode as:

$$\begin{aligned} Pre_{c,\geq 0}(W_{-\Delta})|_{q_1} &= W_{-\Delta}|_{q_2} \cap W_{-\Delta}|^r_{q_3} \\ Pre_{c,\geq 0}(W_{-\Delta})|_{q_2} &= W_{-\Delta}|_{q_1} \cap W_{-\Delta}|^r_{q_4} \\ Pre_{c,\geq 0}(W_{-\Delta})|_{q_3} &= W_{-\Delta}|_{q_1} \cap W_{-\Delta}|_{q_4} \\ Pre_{c,\geq 0}(W_{-\Delta})|_{q_4} &= W_{-\Delta}|_{q_2} \cap W_{-\Delta}|_{q_3} \end{aligned}$$

The set $Pre_{e,\geq 0}(W_{-\Delta})$ is computed mode by mode as:

$$\begin{aligned} Pre_{e,\geq 0}(W_{-\Delta})|_{q_1} &= (\overline{W_{-\Delta}|^r_{q_3}} \cup \overline{W_{-\Delta}|_{q_2}}) \cap \overline{W_{-\Delta}|^r_{q_4}} \\ Pre_{e,\geq 0}(W_{-\Delta})|_{q_2} &= (\overline{W_{-\Delta}|^r_{q_4}} \cup \overline{W_{-\Delta}|_{q_1}}) \cap \overline{W_{-\Delta}|^r_{q_3}} \\ Pre_{e,\geq 0}(W_{-\Delta})|_{q_3} &= (\overline{W_{-\Delta}|_{q_4}} \cup \overline{W_{-\Delta}|_{q_1}}) \cap \overline{W_{-\Delta}|_{q_2}} \\ Pre_{e,\geq 0}(W_{-\Delta})|_{q_4} &= (\overline{W_{-\Delta}|_{q_3}} \cup \overline{W_{-\Delta}|_{q_2}}) \cap \overline{W_{-\Delta}|_{q_1}} \end{aligned}$$

8.2 Computation of continuous uncontrollable predecessors

In Fig. 18 the set computations for the heater example reported in Fig. 13 are shown again after elimination of the timer t_c. Instead of bi-dimensional sets in (t_c, T_{ae}), here we obtain vertical segments in T_{ae}. Notice that in this example it holds:

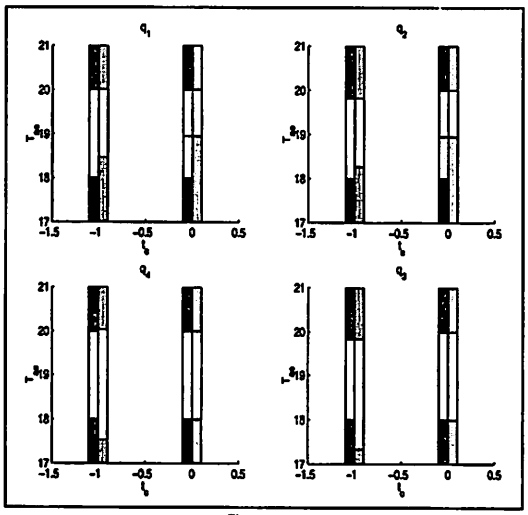
$$Unavoid\_Pre_{\geq 0}(Pre_{e,\geq 0}(W^i_{-\Delta}) \cup \overline{W^i_{\geq 0}}, Pre_{c,\geq 0}(W^i_{-\Delta})) = Pre_{e,\geq 0}(W^i_{-\Delta}) \cup \overline{W^i_{\geq 0}}.$$

9 Controller Synthesis of Heater + 2 Timers with Timers Projection

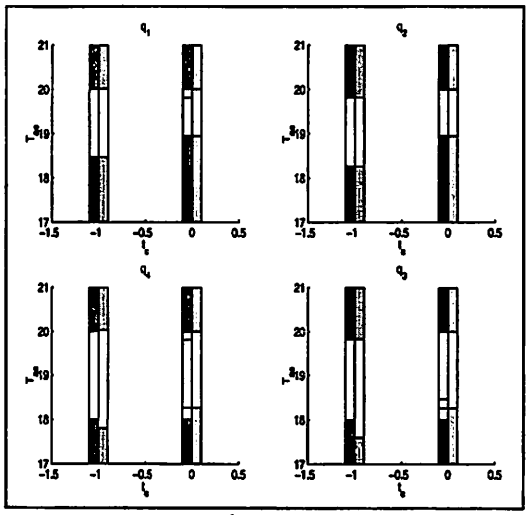
In Fig. 19 the set computations for the heater example reported in Fig. 13 are shown again after elimination of timers t_c and t_e. Instead of three-dimensional sets in (t_c, t_e, T_{ae}), here we obtain vertical segments in T_{ae}.

10 Conclusions

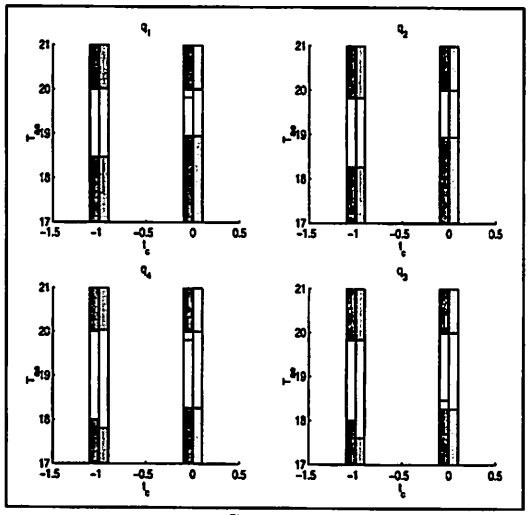
We considered hybrid systems with lower bounds on the separation between occurrence times of consecutive discrete moves. These systems arise when modeling minimal delay times between events, either in the controller, or in the environment. Indeed the placement of such delay constraints is often used to prevent the synthesis of Zeno controllers which satisfy the safety property only by virtue of enforcing infinitely many events in finite time. Our initial attempts to synthesize controllers using the procedure as expressed in [TLS98] for a heating system with lower bounds between occurrence times of consecutive discrete moves, first studied in [BBV+99], failed due to the complexity of the differential games. Motivated by our experience trying to solve this problem, we provided techniques for solving the differential games in reduced state spaces. The main idea is to discretize information about whether discrete moves are enabled or not.



Step 0



Step 1



Step 2

Legend. At each step of the procedure the interesting sets are projected in the continuous space T_{ae} for all modes q_1, q_2, q_3, q_4. We portray the segments over T_{ae} as vertical thick bars; the t_c grid only shows where the segments lie in the original space $X = (t_c, T_{ae})$. For each state there are 2 bars on the left ($t_c = -\Delta$) and 2 bars on the right ($t_c \geq 0$). The first left bar represents the set $\overline{W^i_{-\Delta}}|_q$ (dark gray) and the second left bar represents $\mathit{Unavoid\_Pre}_{-\Delta}(\overline{\mathit{Good}}, \overline{W^{i+1}_{\geq 0}})|_q$ (red). The first right bar represents the sets $\overline{W^i_{\geq 0}}|_q$ (dark grey), $(\mathit{Pre}_{c,\geq 0}(W^i_{-\Delta}) \cap W^i_{\geq 0})|_q$ (light green) and $(\mathit{Pre}_{e,\geq 0}(W^i_{-\Delta}) \cap W^i_{\geq 0})|_q$ (light violet). The second right bar represents $\mathit{Unavoid\_Pre}_{\geq 0}(\mathit{Pre}_{e,\geq 0}(W^i_{-\Delta}) \cup \overline{W^i_{\geq 0}}, \mathit{Pre}_{c,\geq 0}(W^i_{-\Delta}))|_q$ (orange).

Figure 18: Set computations for heater example in Fig. 13 revisited after elimination of timer t_c.

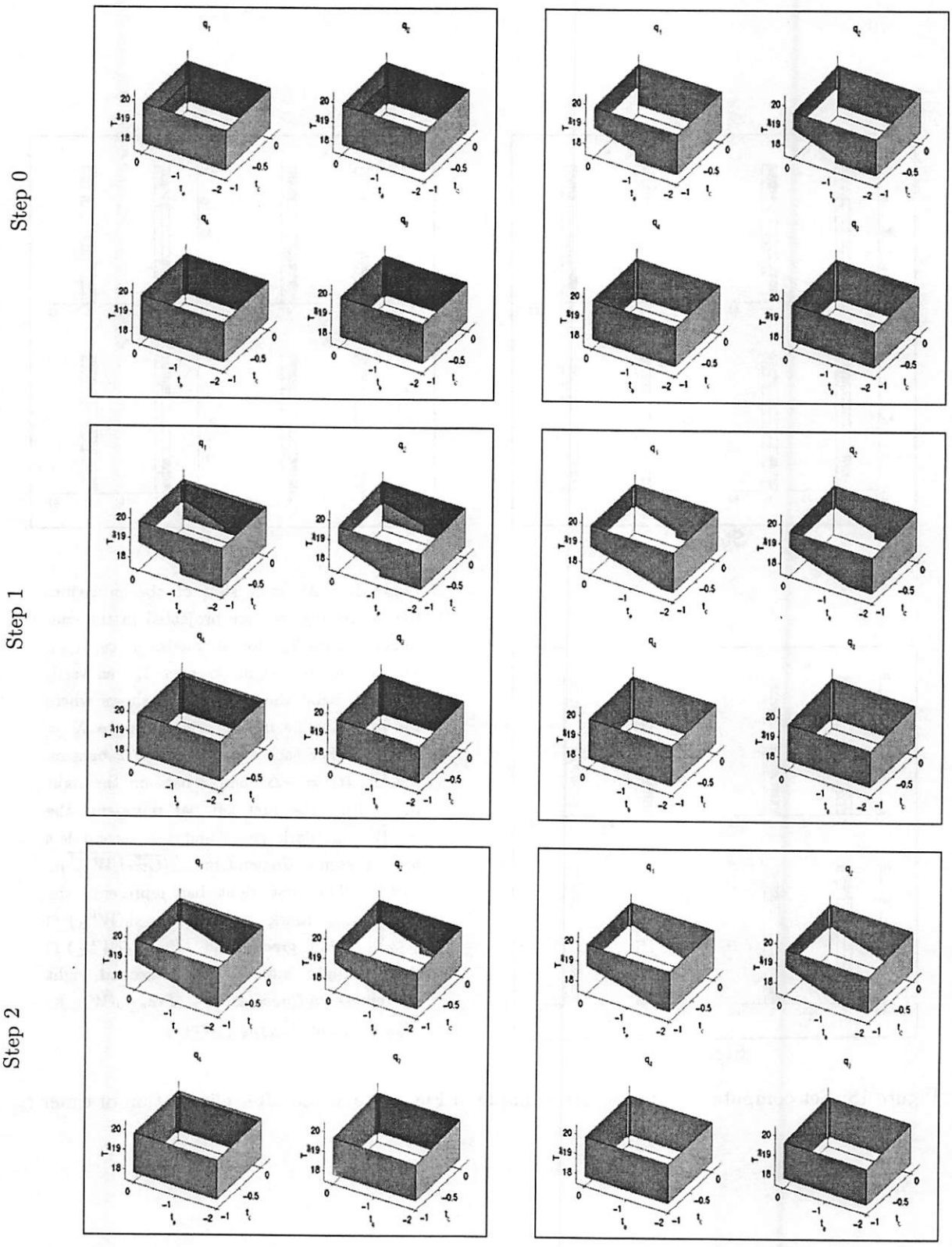


Figure 19: Set computations for heater example in Fig. 13 revisited after elimination of timers t_c, t_e.

The practicality of our approach was demonstrated on the heating system [BBV+99] by successfully synthesizing the maximal set of controllers with discrete controls and disturbances, and continuous controls and disturbances and with lower bounds on the separation between occurrence times of consecutive discrete moves.

Appendix to Section 3

Proof of Lemma 3.1. By definition, a configuration $(q, \tilde{x})$ cannot lie in $Pre_c(W)$ unless there is a non-trivial discrete jump enabled at $(q, \tilde{x})$. Thus we conclude that all configurations in $Pre_c(W)$ satisfy $t_c \geq 0$, and we need not consider the sets $\tilde{X}_-$, which has empty intersection with $Pre_c(W)$.

In the remaining region, $\tilde{X}_+$, we claim that $Pre_c(W)$ satisfies the required independence property for timer-reducibility, and therefore $Pre_c(W)$ is timer-reduced. Suppose that $(q, \tilde{x}) \in Pre_c(W)$ with witness σ_c, i.e., for all $s \in \tilde{M}_e^{disc}(q, \tilde{x})$ (if $\sigma_c \neq \epsilon$ then it may be $s = \epsilon$), we have $\tilde{\delta}(q, \tilde{x}, (\sigma_c, s)) \subseteq W$, and so $\bigcup_{s \in \tilde{M}_e^{disc}(q,\tilde{x})} \tilde{\delta}(q, \tilde{x}, \sigma_c, s) \subseteq W$.

Consider a configuration $(q, \hat{x}) \in \tilde{X}_+$ that differs from $(q, \tilde{x})$ only in the value of the timer. We will show that it is also contained in $Pre_c(W)$ with witness σ_c. We consider $\tilde{\delta}(q, \tilde{x}, \sigma_c, s)$ for each $s \in \tilde{M}_e^{disc}(q, \tilde{x})$ (if $\sigma_c \neq \epsilon$ then it may be $s = \epsilon$). Observe that $\tilde{\delta}(q, \hat{x}, \sigma_c, s)$ is a subset of W since the definition of the automaton $\tilde{H}$ implies that the $\tilde{\delta}$ successor sets for $(q, \tilde{x})$ and $(q, \hat{x})$ match over the variables in X and the value of t_c (being reset to $-\Delta$). Thus $\bigcup_{s \in \tilde{M}_e^{disc}(q,\hat{x})} \tilde{\delta}(q, \hat{x}, \sigma_c, s) \subseteq W$, and so $(q, \hat{x}) \in Pre_c(W)$.

We conclude then that the restriction of $Pre_c(W)$ to the set $\tilde{X}_+$ satisfies the independence property for timer t_c. □

Proof of Lemma 3.2. Analogous to the proof of Lemma 3.1. □

Proof of Lemma 3.3. Clearly, it suffices to consider a fixed mode q. The key idea is that once a configuration is in a region which is independent of a timer variable, then all trajectories will flow in regions independent of that timer variable.

Consider $\tilde{X}_+$. By hypothesis, the sets B and E are both independent of the timer. Suppose that (q, x, t_c) is in $Unavoid\_Pre(B, E) \cap \tilde{X}_+$. We will show that for all t_c' such that $(q, x, t_c') \in \tilde{X}_+$, the configuration (q, x, t_c') is also in $Unavoid\_Pre(B, E)$.

Since (q, x, t_c) is in $Unavoid\_Pre(B, E)$, it follows that for all $u \in \mathcal{U}$, there exists a $d \in \mathcal{D}$ such that the trajectory $\tilde{x}(\cdot) = \psi_q(u, d, (x, t_c), \cdot)$ starting from (x, t_c) at time $t = 0$ enters B at some time $\bar{t}$ and is in $Wait \cap \overline{E}$ for all $0 < t' < \bar{t}$. Now consider (q, x, t_c'). For every control input $u \in \mathcal{U}$, choose the same $d \in \mathcal{D}$ as for (q, x, t_c). The resulting trajectory $\tilde{x}'(\cdot)$ matches $\tilde{x}(\cdot)$ over the domain X by the definition of the continuous dynamics in $\tilde{H}$ and the fact that f is time-invariant. Then since B and E are independent of t_c, $\tilde{x}'(\cdot)$ is a trajectory for (q, x, t_c'), i.e., it passes through $Wait \cap \overline{E}$ on its way to B. □

Proof of Lemma 3.4. The set W^0 is equal to *Good* and therefore timer-reduced. Each successive W^i is calculated using complements and unions (which preserve timer-reduced sets) and the operators Pre_c, Pre_e, and $Unavoid\_Pre$ (which also preserve timer-reduced sets, by Lemmas 3.1, 3.2, and 3.3). □

Proof of Lemma 3.5. Given $W \subseteq Q \times \tilde{X}$, applying the definition of Pre_c from Sec. 2.2.3 it is

$$\begin{aligned} Pre_c(W) &= \{(q,(x,t_c)) \in Q \times \tilde{X} : \exists \sigma_c \in \tilde{M}_c^{disc}(q,(x,t_c)).\forall \sigma_e \in \tilde{M}_e^{disc}(q,(x,t_c)).\ (\sigma_c,\sigma_e) \neq (\epsilon,\epsilon) \\ &\quad \wedge\ \tilde{\delta}(q,(x,t_c),\sigma_c,\sigma_e) \subseteq W\}. \end{aligned}$$

If $t_c \geq 0$, then $\tilde{M}_c^{disc}(q,(x,t_c)) = M_c^{disc}(q,x)$, $\tilde{M}_e^{disc}(q,(x,t_c)) = M_e^{disc}(q,x)$; moreover, since $(\sigma_c,\sigma_e) \neq (\epsilon,\epsilon)$ then $\tilde{\delta}(q,(x,t_c),\sigma_c,\sigma_e) = \delta(q,x,\sigma_c,\sigma_e) \times \{-\Delta\}$, i.e., if $\tilde{\delta}(q,(x,t_c),\sigma_c,\sigma_e) \subseteq W$ then $\delta(q,x,\sigma_c,\sigma_e) \subseteq R_{(-\Delta)}(W)$. Therefore

$$\begin{aligned} R_{(0)}(Pre_c(W)) &= \{(q,x) \in Q \times X : (q,(x,0)) \in Pre_c(W)\} \\ &= \{(q,x) \in Q \times X : \exists \sigma_c \in \tilde{M}_c^{disc}(q,(x,0)).\forall \sigma_e \in \tilde{M}_e^{disc}(q,(x,0)). \\ &\quad (\sigma_c,\sigma_e) \neq (\epsilon,\epsilon)\ \wedge\ \tilde{\delta}(q,(x,0),\sigma_c,\sigma_e) \subseteq W\} \\ &= \{(q,x) \in Q \times X : \exists \sigma_c \in M_c^{disc}(q,x).\forall \sigma_e \in M_e^{disc}(q,x). \\ &\quad (\sigma_c,\sigma_e) \neq (\epsilon,\epsilon)\ \wedge\ \delta(q,x,\sigma_c,\sigma_e) \subseteq R_{(-\Delta)}(W)\} \\ &= Pre_c(R_{(-\Delta)}(W)). \end{aligned}$$

If $t_c < 0$, then $\tilde{M}_c^{disc}(q,(x,t_c)) = \tilde{M}_e^{disc}(q,(x,t_c)) = \{\epsilon\}$, and so

$$R_{(-\Delta)}(Pre_c(W)) = \emptyset.$$

Similar equalities hold for the projections of $Pre_e(W)$. In conclusion,

$$\begin{aligned} R_{(0)}(Pre_c(W,\tilde{M}_c^{disc},\tilde{M}_e^{disc})) &= Pre_c(R_{(-\Delta)}(W,M_c^{disc},M_e^{disc})), \\ R_{(0)}(Pre_e(W,\tilde{M}_c^{disc},\tilde{M}_e^{disc})) &= Pre_e(R_{(-\Delta)}(W,M_c^{disc},M_e^{disc})), \\ R_{(-\Delta)}(Pre_c(W,\tilde{M}_c^{disc},\tilde{M}_e^{disc})) &= \emptyset, \\ R_{(-\Delta)}(Pre_e(W,\tilde{M}_c^{disc},\tilde{M}_e^{disc})) &= \emptyset. \end{aligned}$$

Regarding the two latter equalities, notice that on the left-hand side the argument of $R_{(0)}$ takes values in $Q \times \tilde{X}$, while on the right-hand side the argument of Pre_c (Pre_e) takes values in $Q \times X$. So using the standard Pre operators introduced in Sec. 2.2.3 we have shown how to project Pre_c and Pre_e from the extended $\tilde{X}$ space to the original X space. □

Proof of Lemma 3.6. If $t_c \geq 0$, it is true that

1. the arguments of *Unavoid_Pre* depend only on $t_c \geq 0$ because time flows only ahead,
2. the regions of interest are strips, i.e., rectangles of the type $R_{(0)}(W) \times [0,\infty]$ by the lemmas of Sec. 3.2 on preservation of the timer-reduced property.

So we can write

$$\begin{aligned} &Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W)))\} = \\ &Unavoid\_Pre([R_{(0)}(Pre_e(W)) \times [0,\infty)] \cup [R_{(0)}(\overline{W}) \times [0,\infty)], R_{(0)}(Pre_c(W)) \times [0,\infty)), \end{aligned}$$

since $Pre_e(W) = R_{(0)}(Pre_e(W)) \times [0,\infty)$ by Lemma 3.2, $Pre_c(W) = R_{(0)}(Pre_c(W)) \times [0,\infty)$ by Lemma 3.1 and $\overline{W} = R_{(0)}(\overline{W}) \times [0,\infty)$ by Lemma 3.4. It follows that

$$\begin{aligned}
R_{(0)}(\mathit{Unavoid_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W))) &= \\
\{(q,x) \in Q \times X | (q,(x,0)) \in \mathit{Unavoid_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W)))\} &= \\
\{(q,x) \in Q \times X | (q,(x,0)) \in & \\
\mathit{Unavoid_Pre}([R_{(0)}(Pre_e(W)) \times [0,\infty)] \cup [R_{(0)}(\overline{W}) \times [0,\infty)], R_{(0)}(Pre_c(W)) \times [0,\infty))\} &= \\
\{(q,x) \in Q \times X | (q,x) \in \mathit{Unavoid_Pre}(R_{(0)}(Pre_e(W)) \cup R_{(0)}(\overline{W}), R_{(0)}(Pre_c(W))\} &= \\
\{(q,x) \in Q \times X | (q,x) \in \mathit{Unavoid_Pre}(Pre_e(R_{(-\Delta)}(W)) \cup R_{(0)}(\overline{W}), Pre_c(R_{(-\Delta)}(W))\} &= \\
\mathit{Unavoid_Pre}(Pre_e(R_{(-\Delta)}(W)) \cup R_{(0)}(\overline{W}), Pre_c(R_{(-\Delta)}(W))), &
\end{aligned}$$

where the next-to-last identity is established by Lemma 3.5. Notice that on the left-hand side the argument of $R_{(0)}$ takes values in $Q \times \tilde{X}$, while on the right-hand side the argument of *Unavoid_Pre* takes values in $Q \times X$. So, if $t_c \geq 0$, using the standard *Unavoid_Pre* operator defined in Sec. 2.2.4, we have shown how to project *Unavoid_Pre* from the extended $\tilde{X}$ space to the original X space. □

Proof of Lemma 3.7. Let us consider the set $Pre_e(W) \cup \mathit{Unavoid\_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W))$ which appears in the repeat cycle of the procedure reported in Fig. 4. Since $t_c \in [-\Delta, \infty)$ (because $(q,x,t_c) \notin \widetilde{\mathrm{W}}ait$ when $t_c < -\Delta$), then such set can be partitioned as follows

$$Pre_e(W) \cup \mathit{Unavoid\_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W)) = \mathrm{UP}_{[0,\infty)} \cup \mathrm{UP}_{[-\Delta,0)} \tag{59}$$

with $\mathrm{UP}_{[0,\infty)}$ and $\mathrm{UP}_{[-\Delta,0)}$ defined as follows

$$\mathrm{UP}_{[0,\infty)} = [Pre_e(W) \cup \mathit{Unavoid\_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W))] \cap [Q \times X \times [0,\infty)], \tag{60}$$

$$\mathrm{UP}_{[-\Delta,0)} = [Pre_e(W) \cup \mathit{Unavoid\_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W))] \cap [Q \times X \times [-\Delta,0)]. \tag{61}$$

Since, by Lemma 3.5, $Pre_e(W) \cap [Q \times X \times (-\infty, 0)] = \emptyset$, then $Pre_e(W) \cap [Q \times X \times [0,\infty)] = Pre_e(W)$. Furthermore, since, by Lemma 3.2, the set $Pre_e(W)$ is timer-reduced, under the hypothesis that W is timer-reduced, $Pre_e(W) \cup \overline{W}$ is also timer-reduced. Hence, since by Lemma 3.1 $Pre_c(W)$ is timer-reduced, by Lemma 3.3 $\mathit{Unavoid\_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W))$ is timer-reduced. Then, Eq. 60 gives

$$\mathrm{UP}_{[0,\infty)} = Pre_e(W) \cup [R_{(0)}(\mathit{Unavoid\_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W))) \times [0,\infty)]. \tag{62}$$

By Eq. 1, rewrite Eq. 61 as follows

$$\begin{aligned}
\mathrm{UP}_{[-\Delta,0)} = \{(q,\hat{x},t_c) \in Q \times X \times [-\Delta,0) \mid \forall u \in \mathcal{U}\ \exists \bar{t} > 0\ \exists d \in \mathcal{D} \textit{ such that} \\
\forall \tau \in [0,\bar{t})\ (q, x(\tau), t_c + \tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)}\ \wedge \\
(q, x(\bar{t}), t_c + \bar{t}) \in Pre_e(W) \cup \overline{W}\ \}.
\end{aligned} \tag{63}$$

Introduce

$$\begin{aligned}
\mathrm{UP}^{\star}_{[-\Delta,0)} = \{(q,\hat{x},t_c) \in Q \times X \times [-\Delta,0) \mid \forall u \in \mathcal{U}\ \exists\ \bar{t} \in (0,-t_c]\ \exists d \in \mathcal{D} \textit{ such that} \\
(q, x(\bar{t}), t_c + \bar{t}) \in \overline{W}\ \wedge\ \bar{t} < -t_c\ \vee \\
(q, x(-t_c)) \in R_{(0)}(Pre_e(W) \cup \overline{W} \cup \mathit{Unavoid_Pre}(Pre_e(W) \cup \overline{W}, Pre_c(W)))\ \wedge\ \bar{t} = -t_c\}.
\end{aligned} \tag{64}$$

We now show that

$$\mathrm{UP}_{[-\Delta,0)} \;=\; \mathrm{UP}^{\star}_{[-\Delta,0)}\,. \tag{65}$$

- $\mathrm{UP}_{[-\Delta,0)} \subseteq \mathrm{UP}^{\star}_{[-\Delta,0)}$. Assume $(q,\hat{x},t_c) \in \mathrm{UP}_{[-\Delta,0)}$. By Eq. 63, for all $u' \in \mathcal{U}$, there exists a time $\bar{t} \geq 0$ and a disturbance $d' \in \mathcal{D}$ such that

$$\forall \tau \in [0,\bar{t})\ (q,x'(\tau),t_c+\tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)} \ \wedge\ (q,x'(\bar{t}),t_c+\bar{t}) \in Pre_e(W) \cup \overline{W} \tag{66}$$

where $x'(t)$ denotes the trajectory $\psi_q(u',d',\hat{x},t)$ for $[0,\bar{t}\,)$.

Before detailing a case analysis, we list the following identities that are a direct consequence of Lemma 3.5 and the definition of $\widetilde{\mathrm{W}}ait$:

$$\begin{aligned} Pre_c(W) \cap [Q \times X \times [-\Delta,0)] \;&=\; Pre_e(W) \cap [Q \times X \times [-\Delta,0)] = \emptyset, \\ \widetilde{\mathrm{W}}ait \cap [Q \times \cap X \times [-\Delta,0)] \;&=\; Q \times X \times [-\Delta,0), \end{aligned} \tag{67}$$

and so

$$[Pre_e(W) \cup \overline{W}] \cap [Q \times X \times [-\Delta,0)] = \overline{W} \cap [Q \times X \times [-\Delta,0)], \tag{68}$$

$$\widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)} \cap [Q \times X \times [-\Delta,0)] = Q \times X \times [-\Delta,0), \tag{69}$$

  - Consider the case when, for a given u', $\bar{t} < -t_c$. From $\tau \in [0,\bar{t}) \subset [0,-t_c)$, it is $\tau < \bar{t} < -t_c$ and $\tau + t_c < 0$, and from $t_c \geq -\Delta$ and $\tau \geq 0$, it is $\tau + t_c \geq -\Delta$, i.e., $-\Delta \leq \tau + t_c < 0$. Therefore Eq. 66 is defined only in the interval $[-\Delta,0)$. Applying Eqs. 68 and 69, Eq. 66 reduces to

$$(q,x'(\bar{t}),t_c+\bar{t}) \in \overline{W}. \tag{70}$$

  - Consider the case when, for a given u', $\bar{t} = -t_c$. From $\tau \in [0,\bar{t}) = [0,-t_c)$, it is $\tau < \bar{t} = -t_c$ and finally $-\Delta \leq \tau + t_c < 0$. Then, by Eq. 66, the configuration $(q,\hat{x},t_c)$ is such that under the control signal u' and the disturbance d' as in Eq. 66 at time $\bar{t} = -t_c$ it holds

$$\begin{aligned} &\forall \tau \in [0,-t_c)\ (q,x'(\tau),t_c+\tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)} \ \wedge \\ &(q,x'(-t_c),0) \in Pre_e(W) \cup \overline{W}, \end{aligned}$$

    that is, by Eq. 69,

$$(q,x'(-t_c)) \in R_{(0)}(Pre_e(W) \cup \overline{W}). \tag{71}$$

  - Consider the case when, for a given u', $\bar{t} > -t_c$. From $\tau \in [0,-t_c)$, it is $\tau < -t_c$ and finally $-\Delta \leq \tau + t_c < 0$. The configuration $(q,\hat{x}'',0) = (q,x'(-t_c),0)$ is reached by the hybrid system under inputs u', d' at time $-t_c$. For any control signal $u'' \in \mathcal{U}$ which steers such configuration, there exists a signal u' (as in Eq. 66) such that $u'(t) = u''(t+t_c)$ for $t > -t_c$. Hence, the disturbance $d'' \in \mathcal{D}$ defined by $d''(t) = d'(t-t_c)$ for $t \geq 0$, with d' as in Eq. 66, is such that

$$\begin{aligned} &\forall \tau \in [0,t_c+\bar{t})\ (q,x'(-t_c+\tau),\tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)} \ \wedge \\ &(q,x'(\bar{t}),t_c+\bar{t}) \in Pre_e(W) \cup \overline{W}, \end{aligned}$$

that is

$$\forall \tau \in [0, t_c + \bar{t})\ (q, x''(\tau), \tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)}\ \wedge$$
$$(q, x''(t_c + \bar{t}), t_c + \bar{t}) \in Pre_e(W) \cup \overline{W},$$

where $x''(t) = \psi_q(u'', d'', \hat{x}'', t)$ for $[0, t_c + \bar{t})$. Then, by Eq. 1, $(q, \hat{x}'', 0) = (q, x'(-t_c), 0) \in$ $Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))$ and

$$(q, \hat{x}'') \in R_{(0)}(Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))).$$

Then, by Eq. 66, the configuration $(q, \hat{x}, t_c) \in \mathrm{UP}_{[-\Delta,0)}$ is such that for all $u' \in \mathcal{U}$, with $\bar{t} > -t_c$, under the disturbance d' as in Eq. 66 we have

$$\forall \tau \in [0, -t_c)(q, x'(\tau), t_c + \tau) \in \widetilde{\mathrm{W}}ait\ \cap \overline{Pre_c(W)}\ \wedge$$
$$(q, x'(-t_c)) \in R_{(0)}(Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W)))$$

which, by Eq. 69, is equivalent to

$$(q, x'(-t_c)) \in R_{(0)}(Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W))) \tag{72}$$

In conclusion, by Eq. 70, Eq. 71 and Eq. 72, given $(q, \hat{x}, t_c) \in \mathrm{UP}_{[-\Delta,0)}$, for all $u' \in \mathcal{U}$, the disturbance d' as in Eq. 66 is such that

$$(q, x(\bar{t}), t_c + \bar{t}) \in \overline{W}\ \wedge\ \bar{t} < -t_c\ \vee$$
$$(q, x(-t_c)) \in R_{(0)}(Pre_e(W) \cup \overline{W} \cup Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W)))\ \wedge\ \bar{t} = -t_c$$

and, by Eq. 64 $(q, \hat{x}, t_c) \in \mathrm{UP}^*_{[-\Delta,0)}$.

- $\mathrm{UP}_{[-\Delta,0)} \supseteq \mathrm{UP}^*_{[-\Delta,0)}$. Assume $(q, \hat{x}, t_c) \in \mathrm{UP}^*_{[-\Delta,0)}$. By Eq. 64, for all $u' \in \mathcal{U}$, there exists a time $\bar{t} \geq 0$ and a disturbance $d' \in \mathcal{D}$ such that

$$(q, x'(\bar{t}), t_c + \bar{t}) \in \overline{W}\ \wedge\ \bar{t} < -t_c\ \vee$$
$$(q, x'(-t_c)) \in R_{(0)}(Pre_e(W) \cup \overline{W} \cup Unavoid\_Pre(Pre_e(W) \cup \overline{W}, Pre_c(W)))\ \wedge\ \bar{t} = -t_c \tag{73}$$

where $x'(t)$ denotes the trajectory $\psi_q(u', d', \hat{x}, t)$ for $t \in [0, -t_c)$.

  - Consider the case when, for a given u', $\bar{t} < -t_c$. By Eq. 68 and Eq. 69 condition

$$(q, x'(\bar{t}), t_c + \bar{t}) \in \overline{W} \tag{74}$$

    in Eq. 73 is equivalent to

$$\tau \in [0, \bar{t})\ (q, x''(\tau), t_c + \tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)} \wedge (q, x(\bar{t}), t_c + \bar{t}) \in Pre_e(W) \cup \overline{W}. \tag{75}$$

  - Consider the case when, for a given u', $\bar{t} = -t_c$ and $(q, x'(-t_c)) \in R_{(0)}(Pre_e(W) \cup \overline{W})$. For the configuration $(q, \hat{x}, t_c)$ we have that, for all $u \in \mathcal{U}$, there exists a time $\bar{t} = -t_c$ and a disturbance $d = d' \in \mathcal{D}$ (with d' as in Eq. 73 for $u' = u$), such that $(q, x(\bar{t}), t_c + \bar{t}) \in$ $Pre_e(W) \cup \overline{W}$. Moreover, by Eq. 69,

$$\forall \tau \in [0, \bar{t})\ (q, x''(\tau), t_c + \tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)}. \tag{76}$$

    In summary,

$$\tau \in [0, \bar{t})\ (q, x''(\tau), t_c + \tau) \in \widetilde{\mathrm{W}}ait \cap \overline{Pre_c(W)} \wedge (q, x(\bar{t}), t_c + \bar{t}) \in Pre_e(W) \cup \overline{W}. \tag{77}$$

– Consider the case when, for a given u', $\bar{t} = -t_c$ and $(q, x'(-t_c)) \in R_{(0)}(\mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W)))$. For the configuration $(q, \hat{x}'', 0) = (q, x'(-t_c), 0)$, by Eq. 1, for all $u'' \in \mathcal{U}$, there exists a time $\bar{\bar{t}} > 0$ and a disturbance $d'' \in \mathcal{D}$ such that

$$\forall \tau \in [0, \bar{\bar{t}}) \ (q, x''(\tau), \tau) \in \widetilde{\mathit{Wait}} \cap \overline{\mathit{Pre}_c(W)} \ \wedge \ (q, x''(\bar{\bar{t}}), \bar{\bar{t}}) \in \mathit{Pre}_e(W) \cup \overline{W} \tag{78}$$

where $x''(t)$ denotes the trajectory $\psi_q(u'', d'', \hat{x}'', t)$ for $t \in [0, \bar{\bar{t}})$. Given any $u \in \mathcal{U}$, one can always associate to u a u' and a u'' such that $u'(t) = u(t)$ for $t \in [0, -t_c)$, and $u''(t) = u(t - t_c)$ for $t \in [0, \bar{\bar{t}})$. Hence, the disturbance $d \in \mathcal{D}$ defined by

$$d(t) = \begin{cases} d'(t) & \text{for } t \in [0, -t_c) \\ d''(t + t_c) & \text{for } t \in [-t_c, -t_c + \bar{\bar{t}}) \end{cases}$$

with d' as in Eq. 73 corresponding to u', and d'' as in Eq. 78 corresponding to u'', is such that the trajectory

$$x(t) = \psi_q(u, d, \hat{x}, t) = \begin{cases} x'(t) & \text{for } t \in [0, -t_c) \\ x''(t + t_c) & \text{for } t \in [-t_c, -t_c + \bar{\bar{t}}) \end{cases}$$

satisfies

$$\forall \tau \in [0, -t_c + \bar{\bar{t}}) \ (q, x(\tau), t_c + \tau) \in \widetilde{\mathit{Wait}} \cap \overline{\mathit{Pre}_c(W)} \ \wedge \ (q, x(-t_c + \bar{\bar{t}}), \bar{\bar{t}}) \in \mathit{Pre}_e(W) \cup \overline{W}. \tag{79}$$

Indeed, by Eq. 69 condition $(q, x(\tau), \tau) \in \widetilde{\mathit{Wait}} \cap \overline{\mathit{Pre}_c(W)}$ holds also for all $\tau \in [0, -t_c)$.

Hence, from Eq. 75, Eq. 77 and Eq. 79 $(q, \hat{x}, t_c) \in \mathrm{UP}_{[-\Delta, 0)}$.

Substituting Eq. 62 and Eq. 65 in Eq. 59, we have

$$\begin{aligned} &\mathit{Pre}_e(W) \cup \mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W)) = \\ &\quad \mathit{Pre}_e(W) \cup [R_{(0)}(\mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W))) \times [0, \infty)] \cup \mathrm{UP}^{\star}_{[-\Delta, 0)} \ . \end{aligned} \tag{80}$$

Since, by Lemma 3.5, $R_{(-\Delta)}(\mathit{Pre}_e(W)) = \emptyset$ and

$$R_{(-\Delta)}(R_{(0)}(\mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W))) \times [0, \infty))) = \emptyset,$$

then, by Eq. 80, we have

$$R_{(-\Delta)}(\mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W))) = R_{(-\Delta)}(\mathrm{UP}^{\star}_{[-\Delta, 0)}).$$

Finally, noticing that in Eq. 64

$$\begin{aligned} &\mathit{Pre}_e(W) \cup \overline{W} \cup \mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W)) = \\ &\quad \overline{W} \cup (\mathit{Pre}_e(W) \cup \mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W))) = \\ &\quad \overline{W \setminus (\mathit{Pre}_e(W) \cup \mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W)))} \end{aligned}$$

and replacing in Eq. 64 t_c with $-\Delta$, we obtain

$$R_{(-\Delta)}(\mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W))) =$$
$$\{(q,\hat{x}) \in Q \times X \mid \forall u \in \mathcal{U}\ \exists\, \bar{t} \in (0,\Delta]\ \exists d \in \mathcal{D} \textit{ such that}$$
$$\textit{for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \textit{ we have}$$
$$(q, x(\bar{t}), -\Delta + \bar{t}) \in \overline{W} \wedge \bar{t} < \Delta \vee$$
$$(q, x(\Delta)) \in R_{(0)}(\overline{W \setminus (\mathit{Pre}_e(W) \cup \mathit{Unavoid\_Pre}(\mathit{Pre}_e(W) \cup \overline{W}, \mathit{Pre}_c(W)))}) \wedge \bar{t} = \Delta\}.$$

□

Appendix to Section 4

Proof of Lemma 4.1. By definition, a configuration $(q,\tilde{x})$ cannot lie in $\mathit{Pre}_c(W)$ unless there is a non-trivial discrete jump enabled at $(q,\tilde{x})$. Thus we conclude that all configurations in $\mathit{Pre}_c(W)$ satisfy $t_c \geq 0 \vee t_e \geq 0$, and we need not consider the sets $\tilde{X}_{-,-}$, $\tilde{X}_{-\Delta_c,-}$, and $\tilde{X}_{-,-\Delta_e}$, which all have empty intersection with $\mathit{Pre}_c(W)$.

In each of the five remaining regions, we claim that $\mathit{Pre}_c(W)$ satisfies the required independence properties for timer-reducibility, and therefore $\mathit{Pre}_c(W)$ is timer-reduced. Suppose that $(q,\tilde{x}) \in \mathit{Pre}_c(W)$ with witness σ_c, i.e., for all $\sigma_e \in \tilde{M}_e^{disc}(q,\tilde{x})$, we have $(\sigma_c,\sigma_e) \neq (\epsilon,\epsilon) \wedge \tilde{\delta}(q,\tilde{x},(\sigma_c,\sigma_e)) \subseteq W$.

- Consider $\tilde{X}_{+,+}$. We examine two cases for the witnessing move σ_c.

  1. Case 1: Suppose $\sigma_c \in \Sigma_c$, corresponding to a non-trivial discrete controller move. The resulting successors states $\bigcup_{s \in \tilde{M}_e^{disc}(q,\tilde{x})} \tilde{\delta}(q,\tilde{x},\sigma_c,s)$ must be contained in W.

     Consider the configuration $(q,\hat{x}) \in \tilde{X}_{+,+}$ that differs from $(q,\tilde{x})$ only in the value of the timers. We will show that it is also contained in $\mathit{Pre}_c(W)$ with witness σ_c. We consider $\tilde{\delta}(q,\tilde{x},\sigma_c,s)$ for each $s \in \tilde{M}_e^{disc}(q,\tilde{x})$. First, suppose $s = \epsilon$. Observe that $\tilde{\delta}(q,\hat{x},\sigma_c,\epsilon)$ is a subset of W since the definition of the automaton $\tilde{H}$ implies that the $\tilde{\delta}$ successor sets for $(q,\tilde{x})$ and $(q,\hat{x})$ match over the variables in X and the value of t_c (being $-\Delta_c$), and the $\tilde{\delta}$ successor sets are in the region $\tilde{X}_{-\Delta_c,+}$, which is independent of the value of t_e since W is timer-reduced. Second, suppose $s \in \Sigma_e$. In this case, the successors have both timers reset with $t_c = -\Delta_c$ and $t_e = -\Delta_e$, and $\tilde{\delta}(q,\hat{x},\sigma_c,\sigma_e) = \tilde{\delta}(q,\tilde{x},\sigma_c,\sigma_e)$, by definition of $\tilde{H}$, and this set is contained in W since $(q,\tilde{x}) \in \mathit{Pre}_c(W)$. Thus $\bigcup_{s \in \tilde{M}_e^{disc}(q,\hat{x})} \tilde{\delta}(q,\hat{x},\sigma_c,s) \subseteq W$, and so $(q,\hat{x}) \in \mathit{Pre}_c(W)$.

  2. Case 2: Suppose witnessing discrete move is ϵ, corresponding to a empty discrete controller move. Then by definition of Pre_c, we have $\epsilon \notin \tilde{M}_e^{disc}(q,\tilde{x})$, and $\bigcup_{s \in \tilde{M}_e^{disc}(q,\tilde{x})} \tilde{\delta}(q,\tilde{x},\epsilon,s)$ must be contained in W.

     Consider the configuration $(q,\hat{x}) \in \tilde{X}_{+,+}$ that differs from $(q,\tilde{x})$ only in the value of the timers. We will show that it is also contained in $\mathit{Pre}_c(W)$ with witness ϵ. By definition of $\tilde{H}$, we know that $\epsilon \notin \tilde{M}_e^{disc}(q,\hat{x})$, since it is not in $\tilde{M}_e^{disc}(q,\tilde{x})$. We consider $\tilde{\delta}(q,\hat{x},\epsilon,s)$ for each (non-ϵ) $s \in \tilde{M}_e^{disc}(q,\hat{x})$. In all elements of $\tilde{\delta}(q,\hat{x},\epsilon,s)$, the timer t_c has the same value as in $\hat{x}$, and $t_e = -\Delta_e$, by definition of $\tilde{H}$. Since $\tilde{\delta}(q,\tilde{x},\epsilon,s)$ lies in the timer-reduced set W, in the region $\tilde{X}_{+,-\Delta_e}$ where t_c is not relevant, it follows that

$\tilde{\delta}(q, \hat{x}, \epsilon, s)$, which matches $\tilde{\delta}(q, \tilde{x}, \epsilon, s)$ except for the value of t_c, is contained in W as required.

We conclude then that the restriction of $Pre_c(W)$ to the set $\tilde{X}_{+,+}$ satisfies the independence property for both timers t_c and t_e.

- Consider $\tilde{X}_{+,-}$. As before we examine two cases for the discrete controller move σ_c that witnesses existence in $Pre_c(W)$.

  - Case 1: Suppose $\sigma_c \in \Sigma_c$, i.e., that it corresponds to a non-trivial discrete controller move. Then the resulting successors states $\bigcup_{s \in \tilde{M}_e^{disc}(q,\tilde{x})} \tilde{\delta}(q, \tilde{x}, \sigma_c, s)$ are a subset of W. Consider the configuration $(q, \hat{x}) \in \tilde{X}_{+,-}$ that differs from $(q, \tilde{x})$ only in the value of the timer t_c. We will show that it also lies in $Pre_c(W)$ with witness σ_c, by showing that $\bigcup_{s \in \tilde{M}_e^{disc}(q,\hat{x})} \tilde{\delta}(q, \hat{x}, \sigma_c, s)$ is a subset of W.

    First, observe that $s \in \tilde{M}_e^{disc}(q, \tilde{x})$ implies $s = \epsilon$, by construction of $\tilde{H}$ (it is impossible for the environment to make a non-silent move when $t_e < 0$). Similarly, $s \in \tilde{M}_e^{disc}(q, \hat{x})$ implies $s = \epsilon$. Thus it suffices to establish that $\tilde{\delta}(q, \hat{x}, \sigma_c, \epsilon) \subseteq W$.

    For the silent discrete environment move ϵ, we have that the $\tilde{\delta}$ successors sets for $(q, \tilde{x})$ and $(q, \hat{x})$ match over the variables in $X \times \mathcal{T}_e$ and the value of t_c (being $-\Delta_c$), by definition of $\tilde{H}$, i.e., $\tilde{\delta}(q, \hat{x}, \sigma_c, \epsilon) = \tilde{\delta}(q, \tilde{x}, \sigma_c, \epsilon)$, and so $\tilde{\delta}(q, \hat{x}, \sigma_c, \epsilon) \subseteq W$ since $\tilde{\delta}(q, \tilde{x}, \sigma_c, \epsilon) \subseteq W$.
  - Case 2: Suppose $\sigma_c = \epsilon$. Then, by definition of Pre_c, it must be impossible for the environment to make a silent move at $(q, \tilde{x})$. By definition of $\tilde{H}$, it is also impossible for the environment to make a non-silent move, since $t_e < 0$. However, since a move must always be possible, we obtain a contradiction, and thus σ_c cannot be ϵ.

  We conclude that the restriction of $Pre_c(W)$ to the set $\tilde{X}_{+,-}$ satisfies the independence property for the timer t_c.

- The arguments for the remaining three cases ($\tilde{X}_{+,-\Delta_e}$, $\tilde{X}_{-\Delta_c,+}$, and $\tilde{X}_{-,+}$) are similar.

□

Proofof Lemma 4.2. Analogous to the proof of Lemma 4.1. □

Proof of Lemma 4.3. Clearly, it suffices to consider a fixed mode q. The proof considers the intersection of the set *Unavoid_Pre*(B, E) with each of the partitioning regions $\tilde{X}_{\alpha,\beta}$ in turn. The key idea is that once a configuration is in a region which is independent of a timer variable, then all trajectories will flow in regions independent of that timer variable.

- Consider $\tilde{X}_{+,+}$. By hypothesis, the sets B and E are both independent of each timer. Suppose that (q, x, t_c, t_e) is in *Unavoid_Pre*$(B, E) \cap \tilde{X}_{+,+}$. We will show that for all t_c' and t_e' such that $(q, x, t_c', t_e') \in \tilde{X}_{+,+}$, the configuration (q, x, t_c', t_e') is also in *Unavoid_Pre*(B, E).

  Since (q, x, t_c, t_e) is in *Unavoid_Pre*(B, E), it follows that for all $u \in \mathcal{U}$, there exists a $d \in \mathcal{D}$ such that the trajectory $\tilde{x}(\cdot) = \psi_q(u, d, (x, t_c, t_e), \cdot)$ starting from (x, t_c, t_e) at time $t = 0$ enters B at some time $\bar{t}$ and is in $Wait \cap \overline{E}$ for all $0 < t' < \bar{t}$. Now consider (q, x, t_c', t_e'). For every

control input $u \in \mathcal{U}$, choose the same $d \in \mathcal{D}$ as for (q, x, t_c, t_e). The resulting trajectory $\tilde{x}'(\cdot)$ matches $\tilde{x}(\cdot)$ over the domain X by the definition of the continuous dynamics in $\tilde{H}$. Then since B and E are independent of t_c and t_e, $\tilde{x}'(\cdot)$ is a trajectory for (q, x, t_c', t_e'), i.e., it passes through $Wait \cap \overline{E}$ on its way to B.

- Consider $\tilde{X}_{+,-}$. The sets B and E are independent of t_c in $\tilde{X}_{+,-}$. Suppose (q, x, t_c, t_e) is in $Unavoid\_Pre(B, E) \cap \tilde{X}_{+,-}$. We will show that for all t_c' such that $(q, x, t_c', t_e) \in \tilde{X}_{+,-}$, the configuration (q, x, t_c', t_e) is also in $Unavoid\_Pre(B, E)$.

  Since (q, x, t_c, t_e) is in $Unavoid\_Pre(B, E)$, it follows that for all $u \in \mathcal{U}$, there exists a $d \in \mathcal{D}$ such that the witnessing trajectory $\tilde{x}(\cdot) = \psi_q(u, d, (x, t_c, t_e), \cdot)$ enters B at some time $\bar{t}$ and is in $Wait \cap \overline{E}$ for all $0 < t' < \bar{t}$. We claim that the same witnesses $d \in \mathcal{D}$ as for (q, x, t_c, t_e) suffice for (q, x, t_c', t_e). This is because the resulting trajectories $\tilde{x}'(\cdot) = \psi_q(u, d, (x, t_c', t_e), \cdot)$ remain in $\tilde{X}_{+,-} \cup \tilde{X}_{+,+}$, both of which are independent of t_c, and since $\tilde{x}(\cdot)$ matches $\tilde{x}'(\cdot)$ over variables other than t_c.

- The remaining cases are similar.

□

Proof of Lemma 4.4. The set W^0 is equal to *Good* and therefore timer-reduced. Each successive W^i is calculated using complements and unions (which preserve timer-reduced sets) and the operators Pre_c, Pre_e, and *Unavoid_Pre* (which also preserve timer-reduced sets, by Lemmas 4.1, 4.2, and 4.3). □

Proof of Lemma 4.5. Let us prove the first equality. Given $W \subseteq Q \times \tilde{X}$, applying the definition of Pre_c from Sec. 2.2.3 it is

$$\begin{aligned} Pre_c(W) \;=\; & \{(q, (x, t_c, t_e)) \in (Q \times \tilde{X}) : \exists \sigma_c \in \tilde{M}_c^{disc}(q, (x, t_c, t_e)). \forall \sigma_e \in \tilde{M}_e^{disc}(q, (x, t_c, t_e)). \\ & (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \;\wedge\; \tilde{\delta}(q, (x, t_c, t_e), \sigma_c, \sigma_e) \subseteq W\}. \end{aligned}$$

If $t_c \geq 0$ and $t_e \geq 0$, then $\tilde{M}_c^{disc}(q, (x, t_c, t_e)) = M_c^{disc}(q, x)$, $\tilde{M}_e^{disc}(q, (x, t_c, t_e)) = M_e^{disc}$; moreover, since $(\sigma_c, \sigma_e) \neq (\epsilon, \epsilon)$, then

$$\tilde{\delta}(q, (x, t_c, t_e), \sigma_c, \sigma_e) = \begin{cases} \delta(q, x, \sigma_c, \sigma_e) \times \{(t_c, -\Delta_e)\} & \sigma_c = \epsilon \wedge \sigma_e \neq \epsilon \\ \delta(q, x, \sigma_c, \sigma_e) \times \{(-\Delta_c, t_e)\} & \sigma_c \neq \epsilon \wedge \sigma_e = \epsilon \\ \delta(q, x, \sigma_c, \sigma_e) \times \{(-\Delta_c, -\Delta_e)\} & \sigma_c \neq \epsilon \wedge \sigma_e \neq \epsilon \end{cases}$$

i.e., if $\tilde{\delta}(q, (x, t_c, t_e), \sigma_c, \sigma_e) \subseteq W$ and $(\sigma_c, \sigma_e) \neq (\epsilon, \epsilon)$, then, either $\delta(q, x, \epsilon, \sigma_e) \subseteq R_{(0, -\Delta_e)}(W)$, or $\delta(q, x, \sigma_c, \epsilon) \subseteq R_{(-\Delta_c, 0)}(W)$, or $\delta(q, x, \sigma_c, \sigma_e) \subseteq R_{(-\Delta_c, -\Delta_e)}(W)$. Therefore

$$\begin{aligned} R_{(0,0)}(Pre_c(W)) \;=\; & \{(q, x) \in (Q \times X) : (q, (x, 0, 0)) \in Pre_c(W)\} \\ =\; & \{(q, x) \in (Q \times X) : \exists \sigma_c \in \tilde{M}_c^{disc}(q, (x, 0, 0)). \\ & \forall \sigma_e \in \tilde{M}_e^{disc}(q, (x, 0, 0)). \; (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \;\wedge\; \tilde{\delta}(q, (x, 0, 0), \sigma_c, \sigma_e) \subseteq W\} \\ =\; & \{(q, x) \in (Q \times X) : \forall \sigma_e \in M_e^{disc}(q, x) \setminus \{\epsilon\}. \\ & \delta(q, x, \epsilon, \sigma_e) \subseteq W_{(0,-)}(-\Delta_e) \vee \exists \sigma_c \in M_c^{disc}(q, x) \setminus \{\epsilon\}. \end{aligned}$$

$$
\begin{aligned}
& [\delta(q,x,\sigma_c,\epsilon) \subseteq W_{(-,0)}(-\Delta_c) \wedge \ \forall \sigma_e \in M_e^{disc}(q,x) \setminus \{\epsilon\}. \\
& \delta(q,x,\sigma_c,\sigma_e) \subseteq W_{(-,-\Delta_e)}(-\Delta_c)]\} \\
= \ & \{(q,x) \in (Q \times X) : \forall \sigma_e \in M_e^{disc}(q,x) \setminus \{\epsilon\}. \\
& \delta(q,x,\epsilon,\sigma_e) \subseteq W_{(0,-)}(-\Delta_e) \vee \ [\exists \sigma_c \in M_c^{disc}(q,x) \setminus \{\epsilon\}. \\
& \delta(q,x,\sigma_c,\epsilon) \subseteq W_{(-,0)}(-\Delta_c) \wedge \ \exists \sigma_c \in M_e^{disc}(q,x) \setminus \{\epsilon\}. \\
& \forall \sigma_e \in M_e^{disc}(q,x) \setminus \{\epsilon\}. \ \delta(q,x,\sigma_c,\sigma_e) \subseteq W_{(-,-\Delta_e)}(-\Delta_c)]\} \\
= \ & Pre_c(R_{(0,-)}(W)(-\Delta_e)) \cup [Pre_c(R_{(-,0)}(W)(-\Delta_c)) \cap Pre_c(R_{(-,-\Delta_e)}(W)(-\Delta_c))].
\end{aligned}
$$

Similar considerations prove the other identities. □

References

[AMPS98] E. Asarin, O. Maler, A. Pnueli, and J. Sifakis. Controller synthesis for timed automata. In *Proceedings of System Structure and Control.* IFAC, Elsevier, July 1998.

[BBV+99] A. Balluchi, L. Benvenuti, T. Villa, H. Wong-Toi, and A. L. Sangiovanni-Vincentelli. A case study of hybrid controller synthesis of a heating system. In *Proc. 5th European Control Conference*, Karlsruhe, Germany, September 1999.

[Isa67] R. Isaacs. *Differential Games.* John Wiley, New York, 1967.

[LTS98] J. Lygeros, C. Tomlin, and S. Sastry. On controller synthesis for nonlinear hybrid systems. In *Proc. of the 37th IEEE Conference on Decision and Control*, pages 2101–2106, 1998.

[LTS99] J. Lygeros, C. Tomlin, and S. Sastry. Controllers for reachability specifications for hybrid systems. *Automatica*, 35(3):349–370, March 1999.

[Sus83] H. J. Sussmann. Lie brackets, real analyticity and geometric control. In R. W. Brockett, R. S. Millman, and H. J. Sussmann, editors, *Differential Geometric Control Theory*, volume 27 of *Progress in Mathematics*, pages 1–117. Birkhäuser, Boston Basel Stuttgart, 1983.

[TLS98] C. Tomlin, J. Lygeros, and S. Sastry. Synthesizing controllers for nonlinear hybrid systems. In T. Henzinger and S. Sastry, editors, *First International Workshop, HSCC'98, Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science 1386, pages 360–373, 1998.

[TLS99] C. Tomlin, J. Lygeros, and S. Sastry. Computing controllers for nonlinear hybrid systems. In F. W. Vaandrager and J. H. van Schuppen, editors, *Second International Workshop, HSCC'99, Hybrid Systems: Computation and Control*, volume 1569 of *Lecture Notes in Computer Science*, pages 238–255. Springer-Verlag, 1999.

[VG97] T. L. Vincent and W. J. Grantham. *Nonlinear and Optimal Control Systems.* John Wiley & Sons, Inc., New York, 1997.

[Won97] H. Wong-Toi. The synthesis of controllers for linear hybrid automata. In *Proceedings of the 36th Conference on Decision and Control*, pages 4607–4612. IEEE Press, 1997.