Control and Computation - Review Meeting
26-28 January 2004, Roma, Italy

Controller Synthesis for Hybrid Systems with a Lower Bound on Event Separation

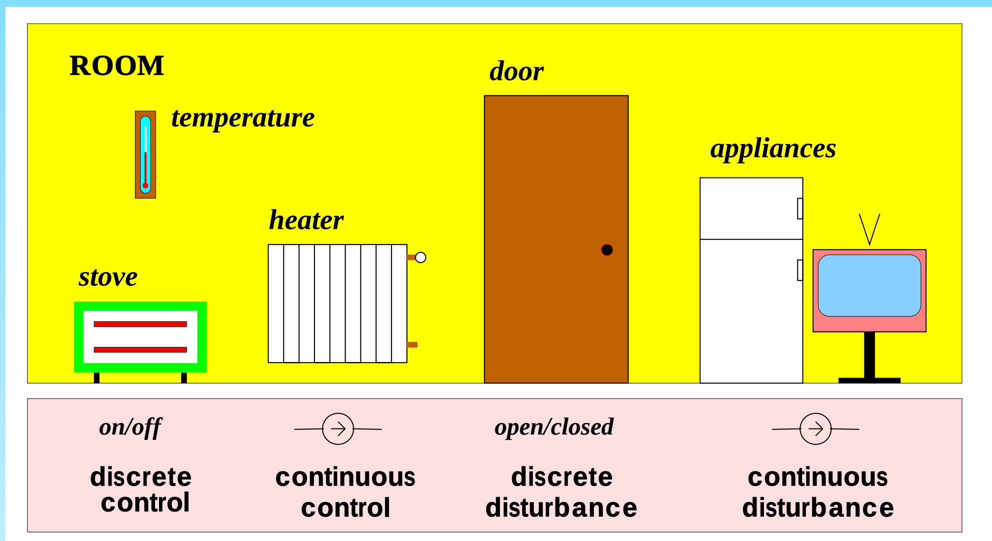
A. Balluchi[§], L. Benvenuti[§], T. Villa[§ †], and A. L. Sangiovanni-Vincentelli[§ ‡]

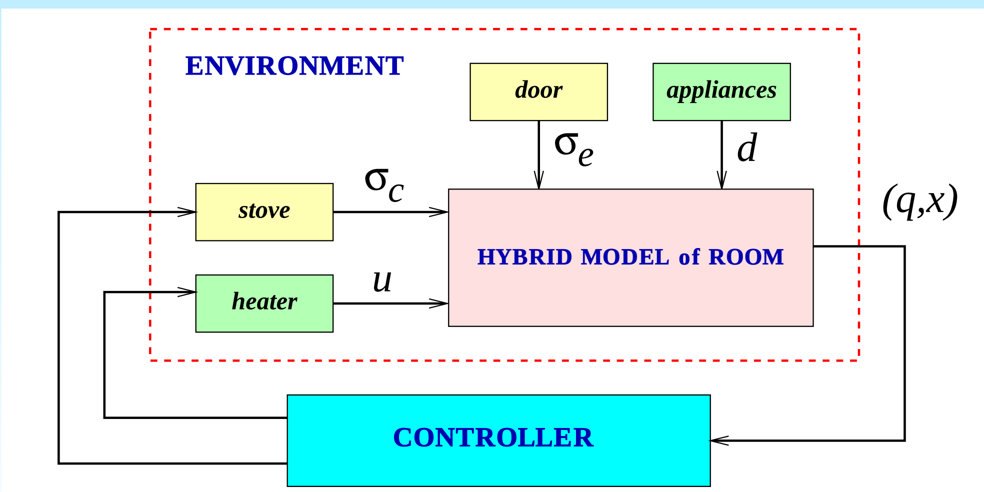
[§]PARADES G.E.I.E., Rome, Italy
[†]DIEGM, Universita' di Udine, Italy
[‡]Dept. of Electrical Engineering and Computer Sciences,
University of California, Berkeley, California, USA

Outline

- description of the control problem
- hybrid automaton formalism
- example of hybrid thermic model of a room
- the maximal safe set and the maximal controller
- event separation by a timer
- maximal safe set with timer projection
- conclusions

Description of the Control Problem





Find a set of states for which there exists a control strategy, for the *stove* and the *heater*, which maintains the room temperature within a specified range, no matter what the *door* and the *appliances* do, assuming that there is a delay between two successive discrete actions of the door and the stove.

Hybrid Automaton Formalism

A ***hybrid automaton*** is a tuple

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

Configuration	Q finite set of *modes*	$X \subseteq \mathbb{R}^n$ set of *cont. states*
domain	Σ_c finite set of *discrete events*	$U \subseteq \mathbb{R}^m$ set of *cont. values*
Control	$\Sigma_c^\epsilon = \Sigma_c \cup \{\epsilon\}$, ϵ *silent move*	$\mathcal{U} = \{u(\cdot) \in PC^0 \mid u(t) \in U, \forall t\}$
feasible funct.	$M_c^{disc} : Q \times X \to 2^{\Sigma_c^\epsilon} \setminus \{\}$	$M_c^{cts} : Q \times X \to 2^U \setminus \{\}$
domain	Σ_e finite set of *discrete events*	$D \subseteq \mathbb{R}^p$ set of *cont. values*
Disturbance	$\Sigma_e^\epsilon = \Sigma_e \cup \{\epsilon\}$, ϵ *silent move*	$\mathcal{D} = \{d(\cdot) \in PC^0 \mid d(t) \in D, \forall t\}$
feasible funct.	$M_e^{disc} : Q \times X \to 2^{\Sigma_e^\epsilon} \setminus \{\}$	$M_e^{cts} : Q \times X \to 2^D \setminus \{\}$
	$\delta : Q \times X \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times X} \setminus \{\}$	$f : Q \times X \times U \times D \to \mathbb{R}^n$
Transition Funct.	$\delta(q, x, \sigma_c, \sigma_e) = W \subseteq Q \times X$	$\dot{x}(t) = f_q(x(t), u(t), d(t))$
	$\delta(q, x, \epsilon, \epsilon) = \{(q, x)\}$	$x(t_0) = x_0$

Full-state Controller

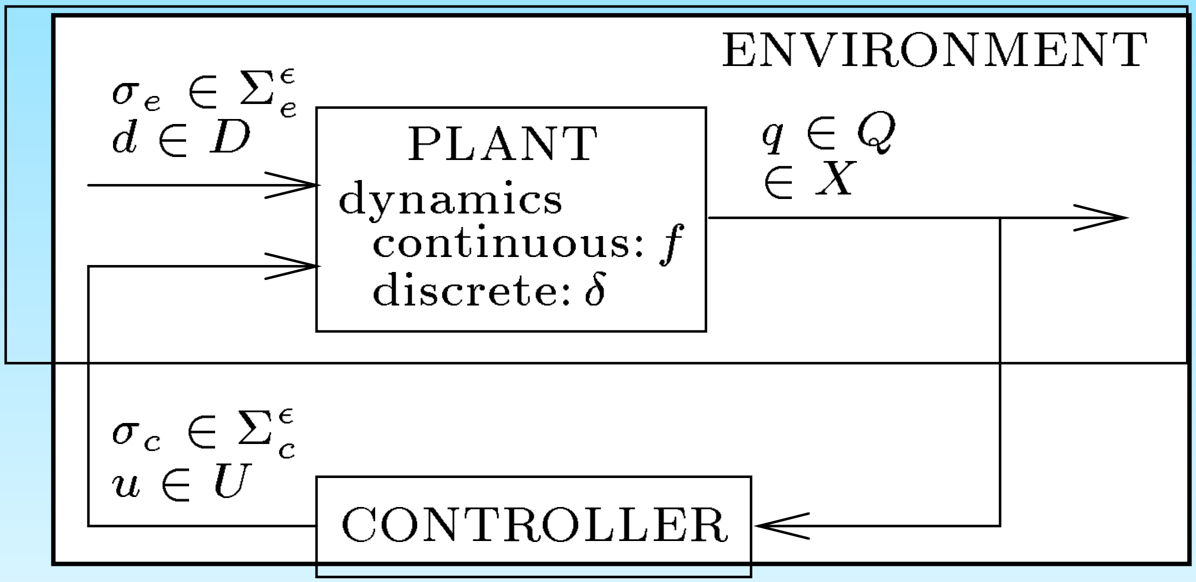
The set of full-state feedback static controllers for H is the pair $C = (T^{disc}, T^{cts})$, $T^{disc} : Q \times X \to 2^{\Sigma_c^\epsilon} \setminus \{\}$, $T^{cts} : Q \times X \to 2^U \setminus \{\}$ and $\forall (q, x) \in Q \times X$, $T^{disc}(q, x) \subseteq M_c^{disc}(q, x)$ and $T^{cts}(q, x) \subseteq M_c^{cts}(q, x)$.

The coupling of the hybrid automaton H with the class $C = (T^{cts}, T^{disc})$ of full-state feedback static controllers is the closed-loop hybrid automaton

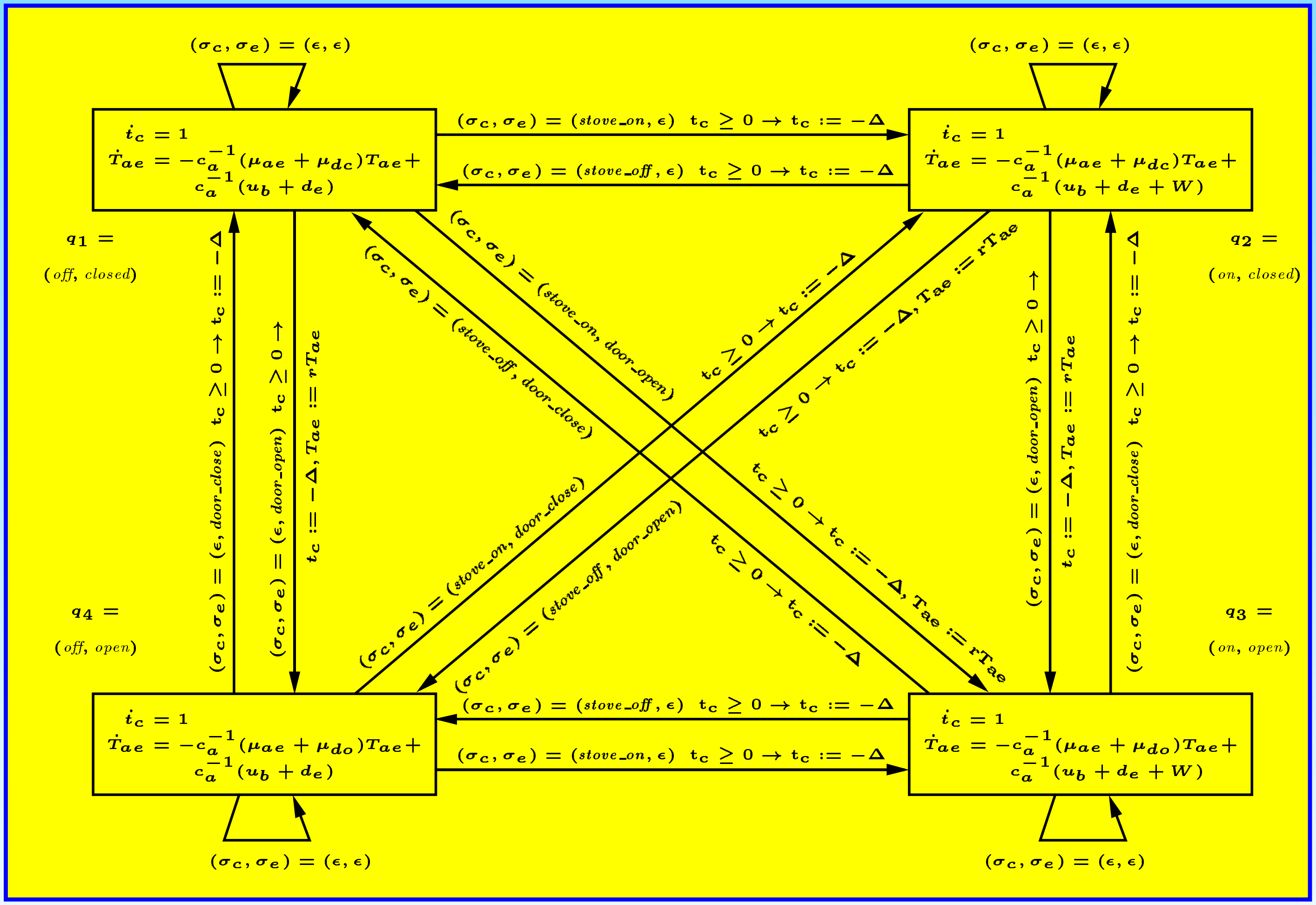
$$H_C = ((Q, X), (U, \Sigma_c), (T^{cts}, T^{disc}), (D, \Sigma_e), (M_e^{cts}, M_e^{disc}), (f, \delta)).$$

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}.

Closed-Loop Hybrid Automaton H_C



Hybrid Thermic Model of the Room



$Q = \{q_1, q_2, q_3, q_4\}$

$X = t_c \times T_{ae}$

$\Sigma_c = \{\text{stove\_on}, \text{stove\_off}\}$

$U = [0, U_b]$

$M_c^{disc} = \epsilon$ if $t_c < 0, \ldots$

$M_c^{cts} = U$

$\Sigma_e = \{\text{door\_close}, \text{door\_open}\}$

$D = [0, D_e]$

$M_e^{disc} = \epsilon$ if $t_c < 0, \ldots$

$M_e^{cts} = D$

Maximal Safe Set and Maximal Controller

Given a set $Good \subset Q \times X$ of configurations that do not violate a *safety property*,

- the *Maximal Safe Set*, *Safe*, is the maximal robust controlled invariant set contained in *Good*,
- the *Maximal Controller* is the family of all feedback controllers such that, given any configuration (q, x) in *Safe*, keep it in *Safe*.

Fixed–Point Procedure [Tomlin, Lygeros, Sastry - HSCC98]

procedure $Safe = \mathcal{P}(H, Good)$

$W^0 := Good$

$i := -1$

repeat {

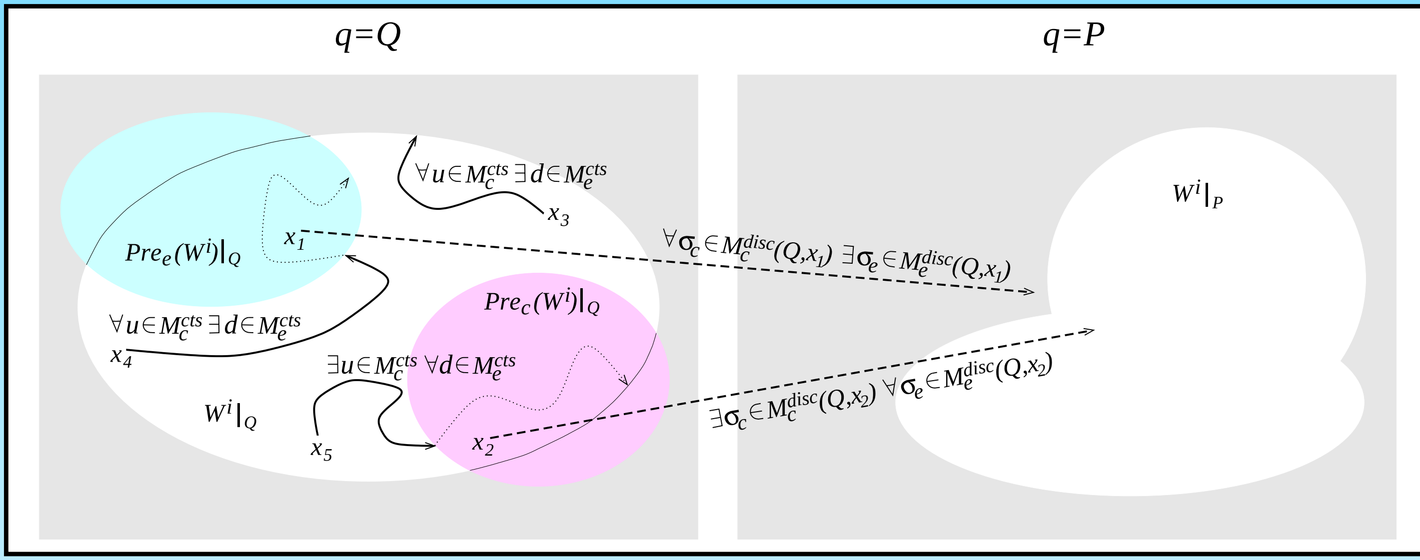
$\quad i := i + 1$

$\quad W^{i+1} := W^i \setminus [Pre_e^H(W^i) \cup Unavoid\_Pre^H(Pre_e^H(W^i) \cup \overline{W^i}, Pre_c^H(W^i))]$

} until $(W^{i+1} = W^i)$

$Safe := W^i$

Discrete and Continuous Operators



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

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

$$Unavoid\_Pre(B,E) = \{(q,\hat{x}) \in Q \times X \mid \forall u \in M_c^{cts}\ \exists \bar{t} > 0\ \exists d \in M_e^{cts} \\ \textit{such that for the trajectory } x(t) = \psi_q(u,d,\hat{x},t) \textit{ we have} \\ \forall \tau \in [0,\bar{t})\ (q,x(\tau)) \in Wait \cap \overline{E} \wedge (q,x(\bar{t})) \in B\}$$

Lower Bound on Event Separation

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 ($\dot{t}_c = 1$): 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 $-\Delta \leq t_c < 0$.

Safe Set on Extended State Space

How to avoid computing the maximal safe set in the extended space $\tilde{X} = (X, t_c)$?

Since there is only *one* timer t_c, information about its value can be discretized into the two parts — $t_c = -\Delta$ and $t_c \geq 0$:

1. if $t_c \geq 0$, then it suffices to know that a discrete jump is enabled, whereas the specific value of t_c irrelevant;
2. if $-\Delta \leq t_c < 0$, 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.

Maximal Safe Set with Timer Projection

procedure $[Safe_0, Safe_{-\Delta}] = \mathcal{P}^{t_c}(H, Good)$

$W_0^0 := Good$

$W_{-\Delta}^0 := Good$

$i := -1$

repeat {

$i := i + 1$

$W_0^{i+1} := W_0^i \setminus [Pre_e^H(W_{-\Delta}^i) \cup$
$Unavoid\_Pre^H(Pre_e^H(W_{-\Delta}^i) \cup \overline{W_0^i}, Pre_c^H(W_{-\Delta}^i))]$

$W_{-\Delta}^{i+1} := W_{-\Delta}^i \setminus Unavoid\_Pre^H_{(-\Delta,0]}(\overline{Good}, \overline{W_0^{i+1}})$

} until $(W_0^{i+1} = W_0^i$ and $W_{-\Delta}^{i+1} = W_{-\Delta}^i)$

$Safe_0 := W_0^i$

$Safe_{-\Delta} := W_{-\Delta}^i$

Projection Operators

Given a set of configurations $K \subseteq Q \times \tilde{X}$:

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

The computation of the safe set can be carried out using only the projections of the sets K for $t_c = -\Delta$ and $t_c \geq 0$.

Projection Theorem

The sets W_0^i, $W_{-\Delta}^i$ computed by procedure $\mathcal{P}^{t_c}(H, Good)$ are the projections, respectively, for $t_c \geq 0$ and $t_c = -\Delta$, of the sets W^i computed by the procedure $\mathcal{P}(\tilde{H}, \widetilde{Good})$, where $\widetilde{Good} = Good \times \mathbb{R}$, i.e.,

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

In particular, the repeat cycle of procedure $\mathcal{P}^{t_c}(H, Good)$ converges if and only if the cycle of procedure $\mathcal{P}(\tilde{H}, \widetilde{Good})$ does, and if so

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

Caveat to the Projection Theorem

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.

Results

Since no transition is enabled for $t_c < 0$,

$$Pre_e(W^i)|_q \cap ([-\Delta, 0) \times \mathbb{R}) = \emptyset$$

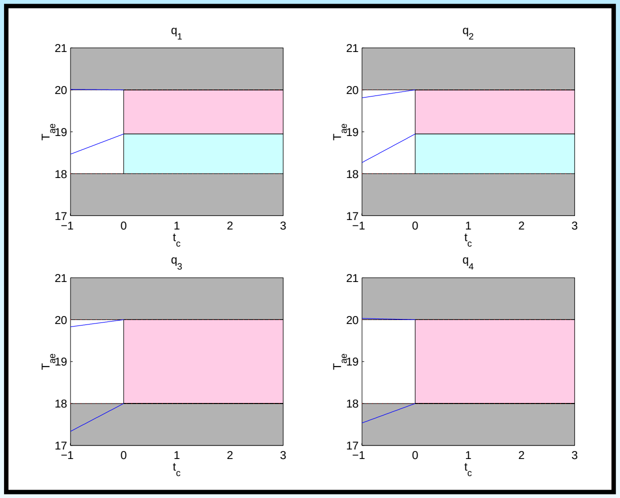
$$Pre_c(W^i)|_q \cap ([-\Delta, 0) \times \mathbb{R}) = \emptyset$$

From modes (*off*, *closed*) and (*on*, *closed*) to modes (*off*, *open*) and (*on*, *open*) the temperature is reset to $T_{ae} := rT_{ae}$.

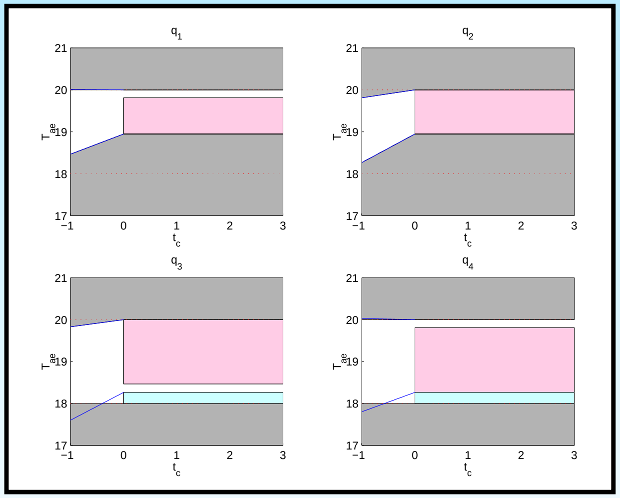
Unavoid_Pre() is the playable set in a 2-player dynamic game between d and u:

$$\min_{d \in \mathcal{D}} \max_{u \in \mathcal{U}} H(t_c^*, T_{ae}^*, \lambda_1, \lambda_2, d, u) = H(t_c^*, T_{ae}^*, \lambda_1, \lambda_2, d^*, u^*) = 0$$

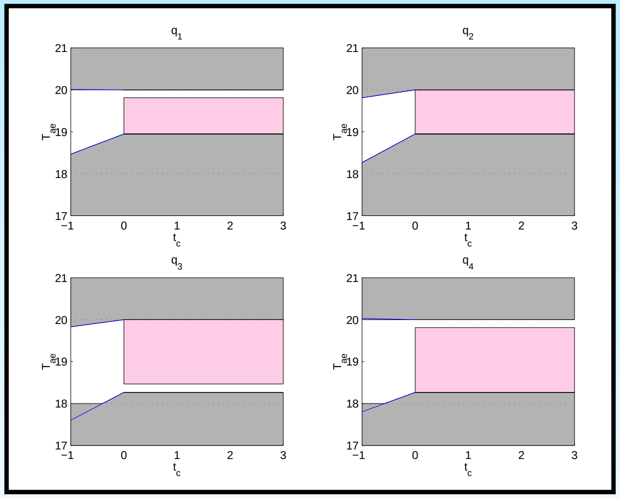
$$(d^*, u^*) = \begin{cases} (0, U_b) & \textit{upper boundary} \\ (D_e, 0) & \textit{lower boundary} \end{cases}$$



Step 1



Step 2



Step 3

Conclusions

- $Pre_e(\cdot)$, $Pre_c(\cdot)$ can be written easily in closed form
- no general solution available for $Unavoid\_Pre(\cdot)$:
  - exploit system structure, e.g. reduce game to lower dimensions
  - approximate conservative solutions
- timer for discrete event separation
- handle event separation in the discrete domain
- selection of a controller inside the maximal safe set
- application to "idle regime" in engine control