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
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.
A hybrid automaton is a tuple

\[
H = ((Q, X), (\Sigma_c, U), (M^\text{disc}_c, M^\text{cts}_c), (\Sigma_e, D), (M^\text{disc}_e, M^\text{cts}_e), (\delta, f))
\]

Configuration
- \( Q \) finite set of modes
- \( X \subseteq \mathbb{R}^n \) set of cont. states

Control
- \( \Sigma_c \) finite set of discrete events
- \( \Sigma^\epsilon_c = \Sigma_c \cup \{\epsilon\} \), \( \epsilon \) silent move
- \( M^\text{disc}_c : Q \times X \rightarrow 2^{\Sigma^\epsilon_c} \setminus \{\} \)
- \( \Sigma^\epsilon_e = \Sigma_e \cup \{\epsilon\} \), \( \epsilon \) silent move
- \( M^\text{disc}_e : Q \times X \rightarrow 2^{\Sigma^\epsilon_e} \setminus \{\} \)

Disturbance
- \( D \subseteq \mathbb{R}^P \) set of cont. values
- \( \Sigma^\epsilon_e = \Sigma_e \cup \{\epsilon\} \), \( \epsilon \) silent move
- \( M^\text{disc}_e : Q \times X \rightarrow 2^D \setminus \{\} \)

Transition Funct.
- \( \delta : Q \times X \times \Sigma^\epsilon_c \times \Sigma^\epsilon_e \rightarrow 2^{Q \times X} \setminus \{\} \)
- \( \delta(q, x, \sigma_c, \sigma_e) = W \subseteq Q \times X \)
- \( \delta(q, x, \epsilon, \epsilon) = \{(q, x)\} \)

\( f : Q \times X \times U \times D \rightarrow \mathbb{R}^n \)
- \( \dot{x}(t) = f_q(x(t), u(t), d(t)) \)
- \( x(t_0) = x_0 \)
The set of full-state feedback static controllers for $H$ is the pair $C = (T^{\text{disc}}, T^{\text{cts}})$, $T^{\text{disc}} : Q \times X \rightarrow 2^{\Sigma^e} \setminus \{\}$, $T^{\text{cts}} : Q \times X \rightarrow 2^U \setminus \{\}$ and $\forall (q, x) \in Q \times X$, $T^{\text{disc}}(q, x) \subseteq M^{\text{disc}}_c(q, x)$ and $T^{\text{cts}}(q, x) \subseteq M^{\text{cts}}_c(q, x)$.

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

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

$H_C$ is obtained from $H$ by replacing the discrete controller move function with $T^{\text{disc}}$ and the continuous controller move function with $T^{\text{cts}}$. 
Closed-Loop Hybrid Automaton $H_C$

- $\sigma_e \in \Sigma^e_e$
- $d \in D$
- $\sigma_c \in \Sigma^e_c$
- $u \in U$
- $q \in Q$
- $\in X$

PLANT
- dynamics continuous: $f$
- discrete: $\delta$

ENVIRONMENT

CONTROLLER
Hybrid Thermic Model of the Room

\[ \begin{align*}
Q &= \{q_1, q_2, q_3, q_4\} \\
X &= t_c \times T_{ae} \\
\Sigma_c &= \{\text{stove\_on, stove\_off}\} \\
U &= [0, U_b] \\
M_c^{\text{disc}} &= \epsilon \text{ if } t_c < 0, \ldots \\
M_c^{\text{cts}} &= U \\
\Sigma_e &= \\
D &= [0, D_e] \\
M_e^{\text{disc}} &= \epsilon \text{ if } t_c < 0, \ldots \\
M_e^{\text{cts}} &= D
\end{align*} \]
Maximal Safe Set and Maximal Controller

Given a set $\text{Good} \subset Q \times X$ of configurations that do not violate a safety property, the Maximal Safe Set, $\text{Safe}$, is the maximal robust controlled invariant set contained in $\text{Good}$.

The Maximal Controller is the family of all feedback controllers such that, given any configuration $(q, x)$ in $\text{Safe}$, keep it in $\text{Safe}$.

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

```plaintext
procedure Safe = $P(H, \text{Good})$
$W^0 := \text{Good}$
$i := -1$
repeat {
    $i := i + 1$
    $W^{i+1} := W^i \setminus [Pre^e_H(W^i) \cup Unavoid_Pre^H(Pre^e_H(W^i) \cup \overline{W^i}, Pre^c_H(W^i))]$
} until $(W^{i+1} = W^i)$
Safe := $W^i$
```
\[ Pre_e(W^i) = \{(q, x) \in Q \times X : \forall \sigma_c \in M_{disc}^d(q, x). \exists \sigma_e \in M_{disc}^e(q, x). (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \land \delta(q, x, \sigma_c, \sigma_e) \not\subseteq W^i \} \]

\[ Pre_c(W^i) = \{(q, x) \in Q \times X : \exists \sigma_c \in M_{disc}^d(q, x). \forall \sigma_e \in M_{disc}^e(q, x). (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \land \delta(q, x, \sigma_c, \sigma_e) \subseteq W^i \} \].

\[ Unavoid\_Pre(B, E) = \{(q, \hat{x}) \in Q \times X | \forall u \in M_{cts}^c \exists \bar{t} > 0 \exists d \in M_{cts}^e \text{ such that for the trajectory } x(t) = \psi_q(u, d, \hat{x}, t) \text{ we have } \forall \tau \in [0, \bar{t}) (q, x(\tau)) \in Wait \land \overline{E} \land (q, x(t)) \in B \} \]
When designing a hybrid system, we may have to guarantee that there is always a delay of at least $\Delta$ 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 $-\Delta \leq t_c < 0$. 
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 $\Delta$. 
procedure \([Safe_0, Safe_{-\Delta}] = \mathcal{P}_{tc}^c(H, Good)\)

\(W_0^0 := Good\)

\(W_{-\Delta}^0 := Good\)

\(i := -1\)

repeat 

\(i := i + 1\)

\(W_{0}^{i+1} := W_0^i \setminus [Pre_e^H(W_{-\Delta}^i) \cup Unavoid_{Pre_e^H}(Pre_e^H(W_{-\Delta}^i) \cup \overline{W_0^i}, Pre_c^H(W_{-\Delta}^i))]\)

\(W_{-\Delta}^{i+1} := W_{-\Delta}^{i} \setminus Unavoid_{Pre_e^H}_{(-\Delta,0]}(Good, \overline{W_0^{i+1}})\)

\} until \((W_{0}^{i+1} = W_0^i \text{ and } W_{-\Delta}^{i+1} = W_{-\Delta}^{i})\)

\(Safe_0 := W_0^i\)

\(Safe_{-\Delta} := W_{-\Delta}^i\)
Given a set of configurations $K \subseteq Q \times \tilde{X}$:

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

2. $\pi_{(0)} : Q \times \tilde{X} \rightarrow Q \times X$ 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 $t_c \geq 0$. 
The sets $W^i_0$, $W^i_{-\Delta}$ computed by procedure $\mathcal{P}^{tc}(H, Good)$ are the projections, respectively, for $t_c \geq 0$ and $t_c = -\Delta$, of the sets $W^i$ computed by the procedure $\mathcal{P}(\tilde{H}, \tilde{Good})$, where $\tilde{Good} = Good \times \mathbb{R}$, i.e.,

$$W^i_0 = \pi_0(W^i),$$
$$W^i_{-\Delta} = \pi_{(-\Delta)}(W^i).$$

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

$$Safe_0 = \pi_0(Safe),$$
$$Safe_{-\Delta} = \pi_{(-\Delta)}(Safe).$$
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.
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 $T_{ae} := rT_{ae}$.

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

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

$$H(t_c^*, T_{ae}^*, \lambda_1, \lambda_2, d^*, u^*) = 0$$

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