CIS 4930/6930: Principles of Cyber-Physical Systems

Chapter 4: Hybrid Systems - Hybrid Automata

Hao Zheng

Department of Computer Science and Engineering
University of South Florida

Ref.: An Introduction to Hybrid Automata

http://link.springer.com/chapter/10.1007%2F0-8176-4404-0_21

Skip sec. 3.2, 4.2, skim sec. 5.

Hybrid Automata: Syntax

A hybrid automata is defined with (ignoring discrete variables)

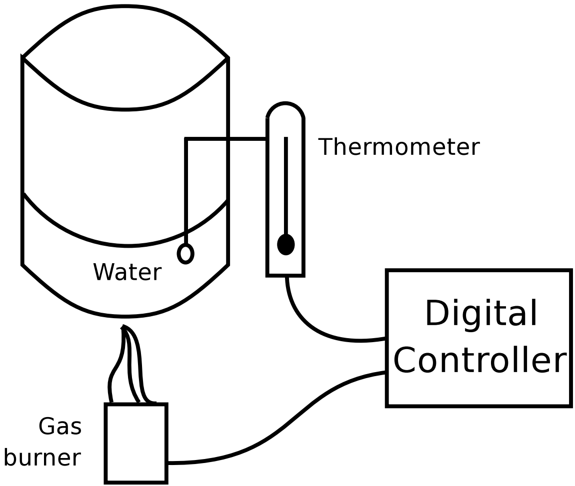
- L: a finite set of locations.
- $l_0 \in L$: the initial location.
- X: a finite set of real-valued variables.
- A: a finite set of actions.
- E: a finite set of edges connecting locations.
- Inv: location invariants.
- $Flow$: definition of continuous evolution on $(X \cup \dot{X})$ in locations.
- $Init$: initial values of $X \cup \dot{X}$.

For each $e \in E$, $e = (l_1, \alpha, Jump, l_2)$ where

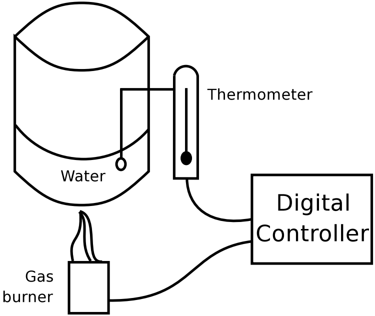
- $\alpha \in A$ is an action,
- $Jump$ defines how $X \cup X'$ are updated when e happens.

X' represents updates to X after e is taken.

A Running Example

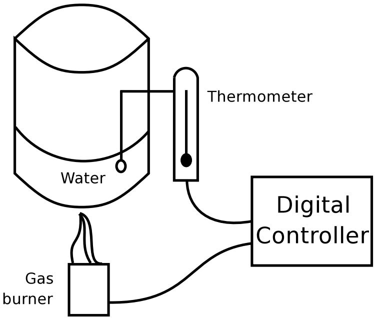


A Running Example



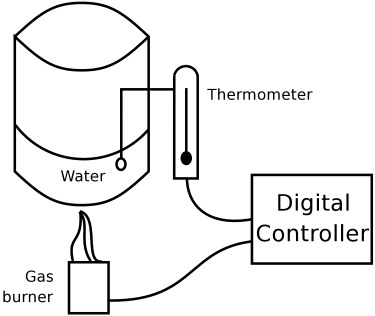
- When the burner is **Off**, water temp. x decreses def'ed by $x(t) = Ie^{-Kt}$ when $x(t) > 20$.
  - I: initial water temp..
  - K: heat transfer constant of tank.

A Running Example



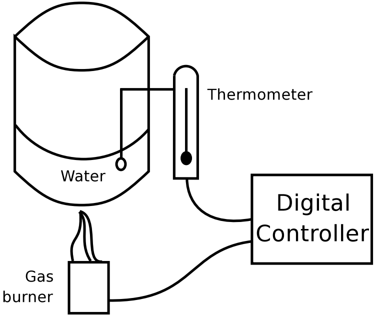
- When the burner is **Off**, water temp. x decreses def'ed by $x(t) = Ie^{-Kt}$ when $x(t) > 20$.
  - I: initial water temp..
  - K: heat transfer constant of tank.
- When $x \leq 20$, x stays constant.

A Running Example



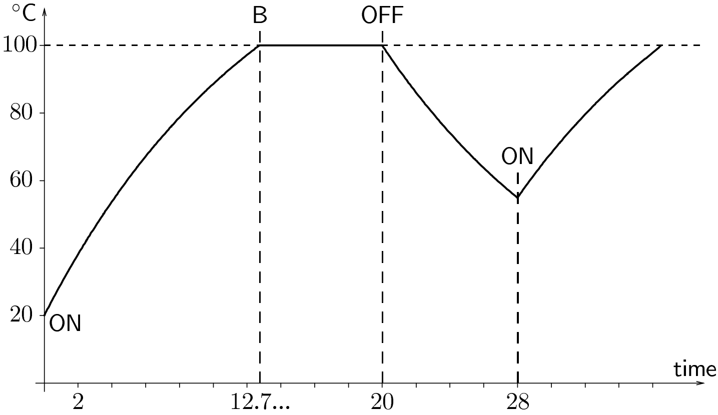
- When the burner is **Off**, water temp. x decreses def'ed by $x(t) = Ie^{-Kt}$ when $x(t) > 20$.
  - I: initial water temp..
  - K: heat transfer constant of tank.
- When $x \leq 20$, x stays constant.
- When the burner is **On**, water temp. x decreses def'ed by $x(t) = Ie^{-Kt} + h(1 - e^{-Kt})$ when $x(t) < 100$.
  - h: constant relative to the power of the burner.

A Running Example

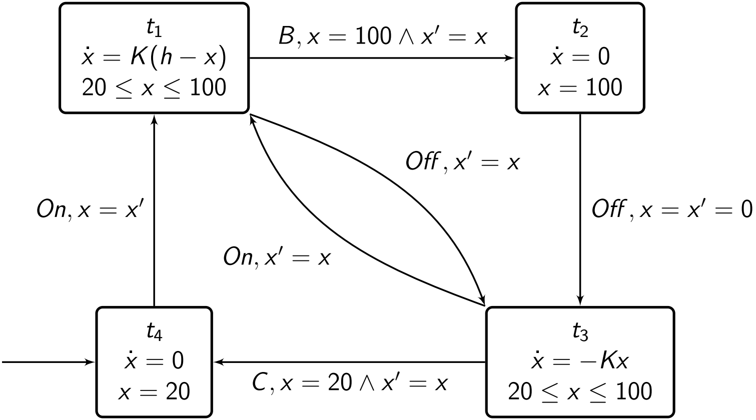


- When the burner is **Off**, water temp. x decreses def'ed by $x(t) = Ie^{-Kt}$ when $x(t) > 20$.
  - I: initial water temp..
  - K: heat transfer constant of tank.
- When $x \leq 20$, x stays constant.
- When the burner is **On**, water temp. x decreses def'ed by $x(t) = Ie^{-Kt} + h(1 - e^{-Kt})$ when $x(t) < 100$.
  - h: constant relative to the power of the burner.
- When $x = 100$, x stays 100.

A Possible Behavior of the Tank



Water Tank: Hybrid Automata



Hybrid Automata: Semantics

Transitions

Let $\eta : X \rightarrow \mathbb{R}$.

- A state of a hybrid automata is (l, η).
- The initial state is (l_0, η_0).

Discrete transition: $(l_1, \eta_1) \xrightarrow{e} (l_2, \eta_2)$

- An edge $e = (l_1, \alpha, Jump, l_2) \in E$ is enabled/executable in a state (l_1, η_1) if
  - $\eta_1 \models Jump(X)$, and
  - there is a matching synchronization action to α.
- A new state (l_2, η_2) after executing e such that

$$\eta_2 \models Jump(X').$$

Transitions (Cont'd)

Continuous transition: $(l, \eta_1) \xrightarrow{\delta} (l, \eta_2),\ \delta \in \mathbb{R}^+$

There is a differentiable function $f : [0, \delta] \rightarrow \mathbb{R}^m$, with the first derivative $\dot{f} : [0, \delta] \rightarrow \mathbb{R}^m$, such that

- $f(0) = \eta_1$,
- $f(\delta) = \eta_2$,
- For all $t \in [0, \delta]$, $f(t) \models Inv(l)$ and $\dot{f}(t) \models Flow(l)$.

Intuitively, a hybrid automata can stay in a location by letting time pass by without violating the location invariant, and the valuation of X during that period of time is constrained by the flow condition labeled in that location.

Execution Traces

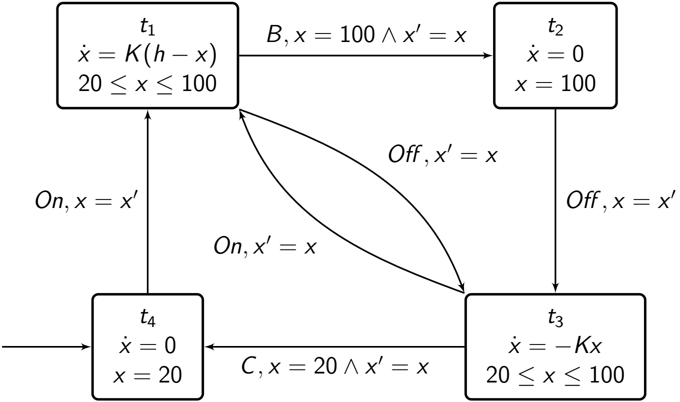
- Execution step: $\rightarrow = \xrightarrow{e} \cup \xrightarrow{\delta}$
- Execution trace:

$$(l_0, u_0) \rightarrow (l_1, \eta_1) \rightarrow (l_2, \eta_2) \ldots$$

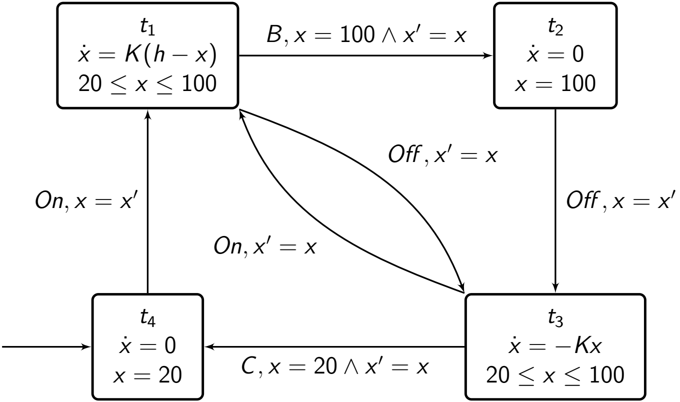
- Reachability: (i, η) is reachable if there exists a trace

$$(l_0, \eta_0) \rightarrow (l_1, \eta_1) \ldots \rightarrow (l_n, \eta_n)$$

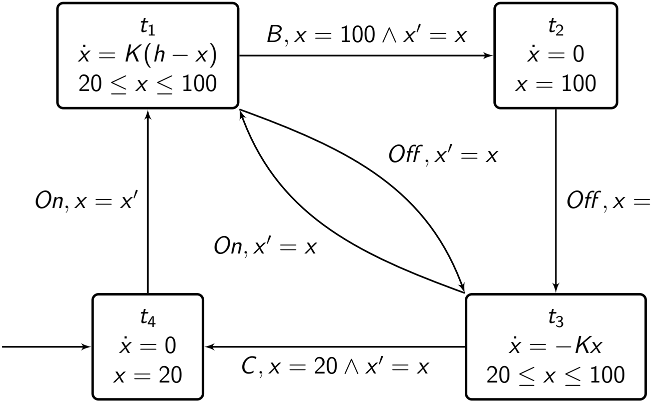
such that $l = l_n$ and $u = \eta_n$.



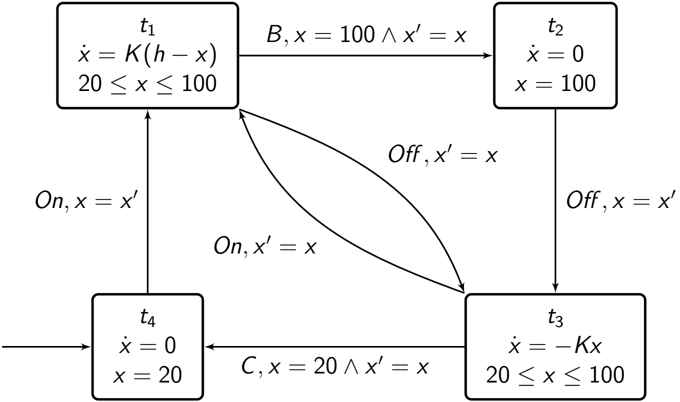
$$(t_4, x = 20) \xrightarrow{On} (t_1, x = 20)$$



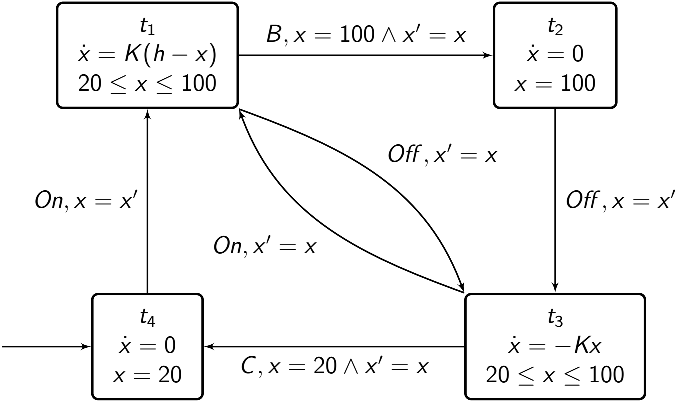
$$(t_4, x = 20) \xrightarrow{On} (t_1, x = 20) \xrightarrow{10} (t_1, x = 88.59)$$



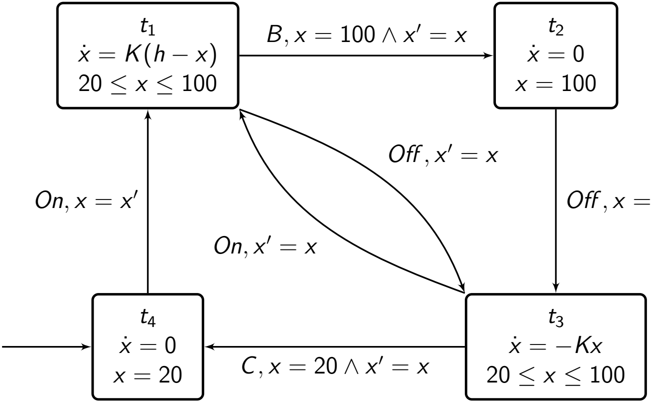
$$(t_4, x = 20) \xrightarrow{On} (t_1, x = 20) \xrightarrow{10} (t_1, x = 88.59) \xrightarrow{2.74} (t_1, x = 100)$$



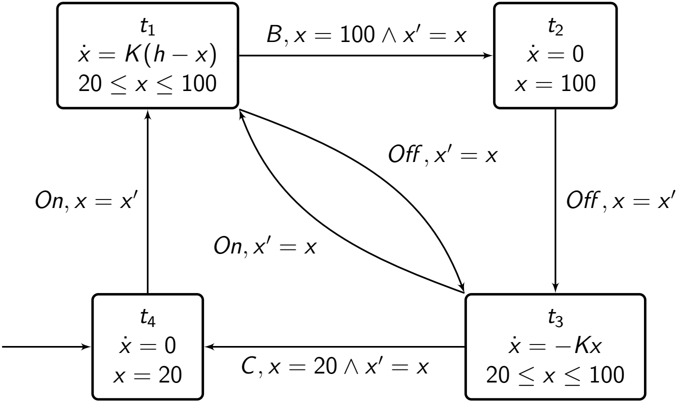
$$(t_4, x = 20) \xrightarrow{On} (t_1, x = 20) \xrightarrow{10} (t_1, x = 88.59) \xrightarrow{2.74} (t_1, x = 100) \xrightarrow{B} (t_2, x = 100)$$



$$(t_4, x = 20) \xrightarrow{On} (t_1, x = 20) \xrightarrow{10} (t_1, x = 88.59) \xrightarrow{2.74} (t_1, x = 100)$$
$$\xrightarrow{B} (t_2, x = 100) \xrightarrow{5} (t_2, x = 100)$$



$$(t_4, x = 20) \xrightarrow{On} (t_1, x = 20) \xrightarrow{10} (t_1, x = 88.59) \xrightarrow{2.74} (t_1, x = 100)$$
$$\xrightarrow{B} (t_2, x = 100) \xrightarrow{5} (t_2, x = 100) \xrightarrow{Off} (t_3, x = 100)$$



$$
\begin{aligned}
&(t_4, x = 20) \xrightarrow{On} (t_1, x = 20) \xrightarrow{10} (t_1, x = 88.59) \xrightarrow{2.74} (t_1, x = 100) \\
&\quad \xrightarrow{B} (t_2, x = 100) \xrightarrow{5} (t_2, x = 100) \xrightarrow{Off} (t_3, x = 100) \\
&\quad \xrightarrow{8} (t_3, x = 54.88), \ldots
\end{aligned}
$$

Composing Hybrid Automata

Parallel Composition of Hyrbid Automata

Two HAs $H_1 = (L_1, l_{10}, X_1, A_1, E_1, Inv_1, Flow_1, Init_1)$ and $H_2 = (L_2, l_{20}, X_2, A_2, E_2, Inv_2, Flow_2, Init_2)$ such that $L_1 \cap L_2 = \emptyset$, their parallel composition, $H_1 \| H_2$ is a HA (L, l_0, C, A, E, Inv) where

- $L = L_1 \times L_2$,
- $l_0 = (l_{10}, l_{20})$;
- $X = X_1 \cup X_2$,
- $A = A_1 \cup A_2$,
- $E = \{\ldots\}$, defined in the next slide,
- $Inv(l_1, l_2) = Inv_1(l_1) \wedge Inv_2(l_2)$ for all $(l_1, l_2) \in L$,
- $Flow(l_1, l_2) = Flow_1(l_1) \wedge Flow_2(l_2)$ for all $(l_1, l_2) \in L$,
- $Init = Init_1 \wedge Init_2$.

Parallel Composition of Timed Automata

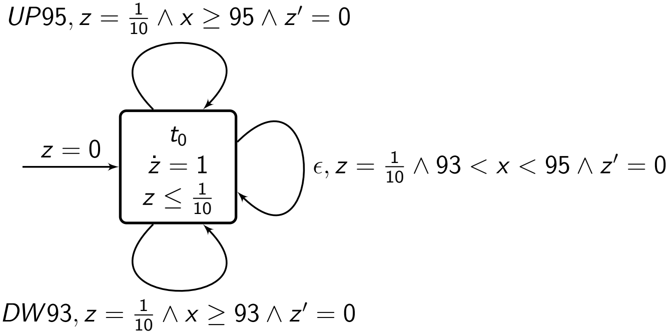
$E = \{(l_1, l_2), \alpha, Jump, (l_1', l_2')\}$ includes edges defined as follows.

$$\frac{(l_1, \alpha, Jump_1, l_1') \in E_1 \quad (l_2, \alpha, Jump_2, l_2') \in E_2}{((l_1, l_2), \alpha, Jump_1 \wedge Jump_2, (l_1', l_2')) \in E} \; Sync$$

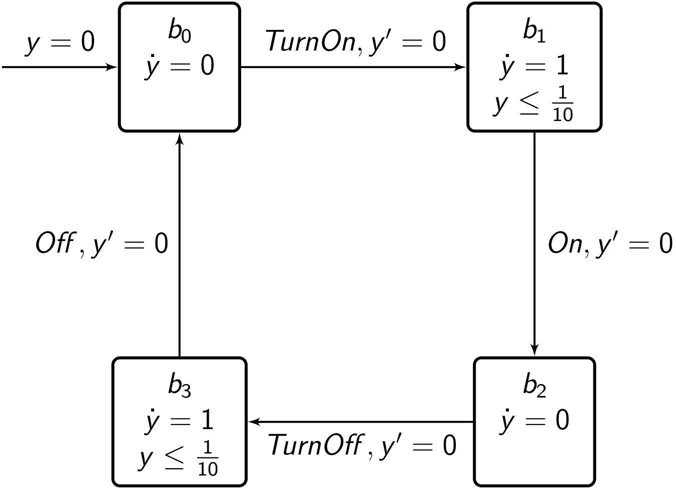
$$\frac{(l_1, \alpha, Jump_1, l_1') \in E_1 \quad \alpha \notin A_2}{((l_1, l_2), \alpha, Jump_1 \wedge \bigwedge_{x \in X_2 - X_1} x' = x, (l_1', l_2)) \in E} \; Async$$

$$\frac{(l_2, \alpha, cc_2, reset_2, l_2') \in E_2 \quad \alpha \notin A_1}{((l_1, l_2), \alpha, Jump_2 \wedge \bigwedge_{x \in X_1 - X_2} x' = x, (l_1, l_2')) \in E} \; Async$$

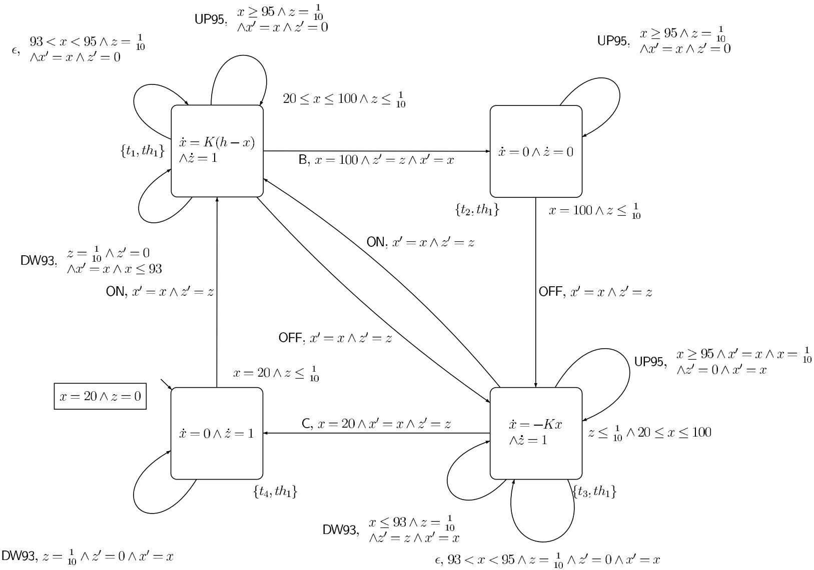
Modeling Thermometer



Modeling Burner



Product of Tank and Thermometer

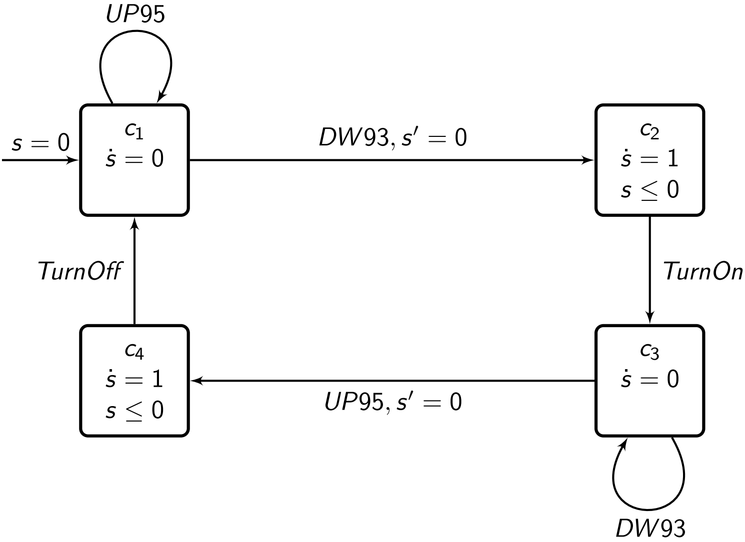


Hybrid Automata: Properties

Safety Property

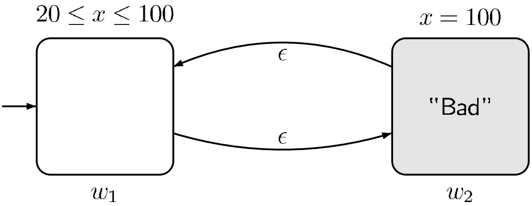
- Nothing bad happens!
- Liveness is difficult to check for an undecidable problem.
- Water thank: design a controller to satisfy
  - **R1** Temp. x of tank is always less than 100°.
  - **R2** After 15 seconds of operation, the temp. x of tank stays between 91° and 97°.
  - **R3** When $91^\circ \leq x \leq 97^\circ$, the burner is never **On** continuously for more than 2 seconds.

A Proposed Controller



Monitor for Safety Property

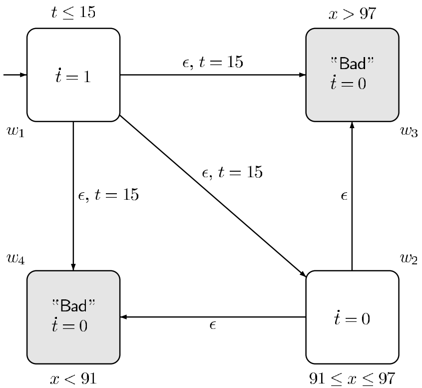
R1: Temp. x of tank is always less than 100°.



(a) Monitor for property $(R1)$

Monitor for Safety Property

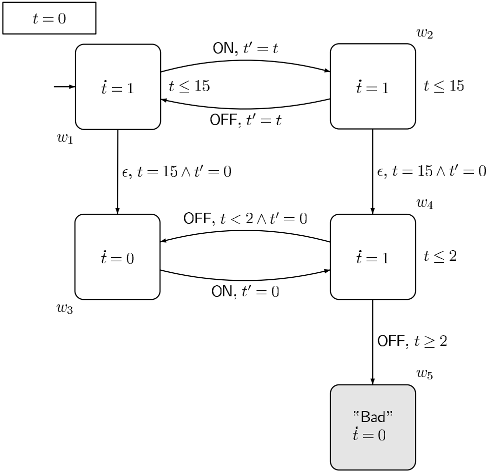
R2: After 15 seconds of operation, the temp. *x* of tank stays between 91° and 97°.



(b) Monitor for property ($R2$)

Monitor for Safety Property

R3: When $91^\circ \leq x \leq 97^\circ$, the burner is never **On** continuously for more than 2 seconds.



(c) Monitor for property ($R3$)

Rectangular Hybrid Automata

Rectangular Automata: Overview

- Analyzing general hybrid automata is very difficult.
    - It is also undecidable!
- Rectangular automata is a subclass of hybrid automata.
    - More expressive than timed automata,
    - Verification is decidable under additional conditions.
- Safety properties are usually the focus for analyzing hybrid automata.

Rectangular Automata: Definition

- $\mathbb{Q}$ is the set of rational numbers.
- Let $I = \{(a, b), [a, b), (a, b], [a, b]\}$ denote an intervals where
  - $a \in \mathbb{Q} \cup \{-\infty\}$, $b \in \mathbb{Q} \cup \{\infty\}$, and $a \leq b$.

Rectangular predicates

Predicates over variables X are rectangular if they are defined by the following rules

$$\phi_1, \phi_2 := \textbf{false} \mid \textbf{true} \mid x \in I \mid \phi_1 \wedge \phi_2$$

Let $Rect(X)$ be the set of all rectangular predicates defined over X.

Note that $x \in (-1, 3]$ is the same as $-1 < x \leq 3$,
Example: $-1 < x \leq 3 \wedge 0 \leq y$.

Rectangular Automata: Definition

Rectangular update predicates

Rectangular update predicates, denoted by $\mathit{updateRect}(X)$, is the set of all rectangular predicates over $X \cup X'$ defined below.

$$\phi_1, \phi_2 := \textbf{false} \mid \textbf{true} \mid x \in I \mid x' \in I \mid x' = x \mid \phi_1 \wedge \phi_2$$

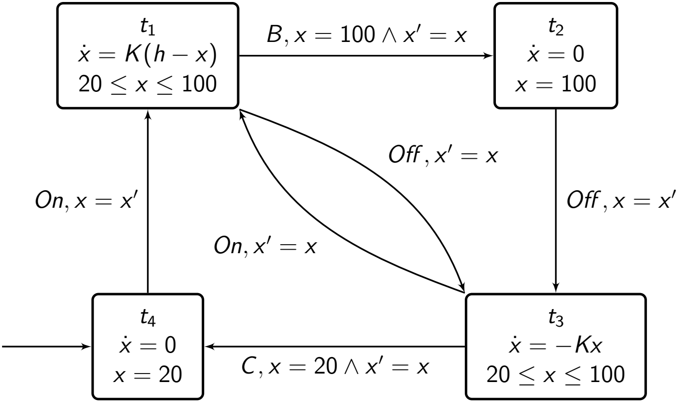
Rectangular Automata

A rectangular is a hybrid automata where

- $\mathit{Init} \in \mathit{Rect}(X)$,
- $\mathit{Inv}(l) \in \mathit{Rect}(X)$ for every $l \in L$,
- $\mathit{Flow}(l) \in \mathit{Rect}(\dot{X})$ for every $l \in L$,
- $\mathit{Jump}(e) \in \mathit{updateRect}(X)$ for every $e \in E$.

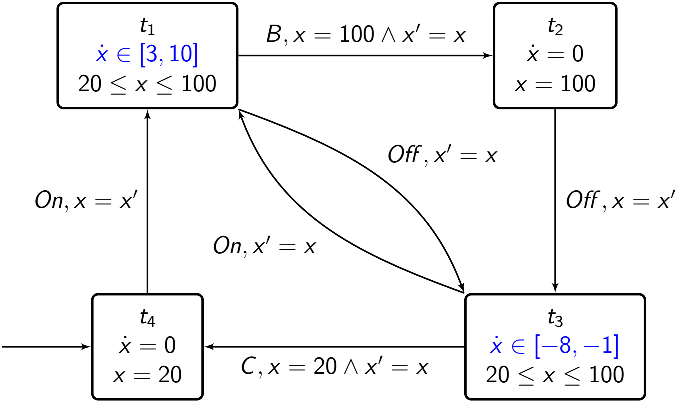
Rectangular Automata for the Water Tank

Original hybrid automata for the water tank.



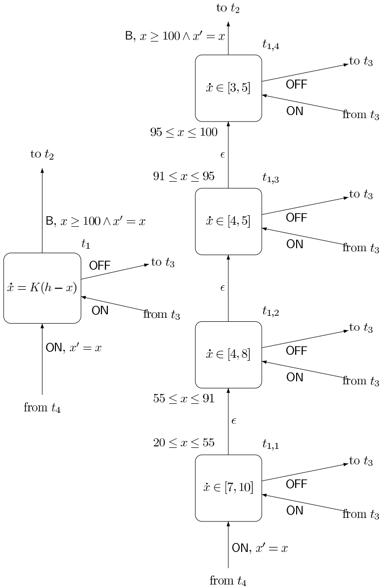
Rectangular Automata for the Water Tank

Converted rectangular automata.



Rectangular automata is over-approximation of the original HA. If a property is verified in the rectangular automata, it is also true in the original HA.

Rectangular Automata: Refinement



Train-Gate Control in Hybrid Automata

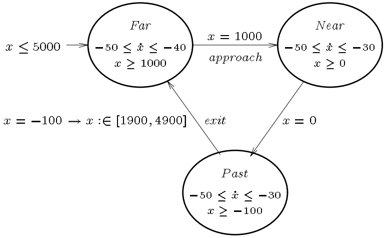


Figure 2: Train automaton

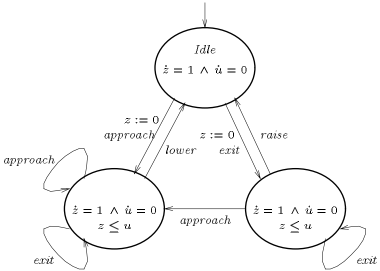


Figure 3: Controller automaton