15-819/18-879: Logical Analysis of Hybrid Systems
04: Hybrid Systems Examples

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA
Outline

1. Hybrid Systems Examples
   - Linear Air Traffic Control
   - Bouncing Ball
   - Train Control
   - Water Tank
1 Hybrid Systems Examples
- Linear Air Traffic Control
- Bouncing Ball
- Train Control
- Water Tank
Hybrid Automaton for Collision Avoidance

\[ x' = v \sin \theta, \quad x' = v \cos \theta \]

\[ \|x - y\| \geq \alpha \]

\[ x' = v \sin \theta, \quad x' = v \cos \theta, \quad \tau' = 1 \]

\[ \|x - y\| < 10 \]

\[ \theta := \theta + \pi / 4 \]

\[ \theta := \theta - \pi / 4 \]

\[ \tau \leq 0 \]

\[ \theta := \theta + \pi / 4 \]
Hybrid Automaton for Collision Avoidance

\[ x'_1 = v \sin \vartheta \]
\[ x'_2 = v \cos \vartheta \]
\[ \|x-y\| \geq \alpha \]

- **cruise**
  \[ x'_1 = v \sin \vartheta \]
  \[ x'_2 = v \cos \vartheta \]
  \[ \|x-y\| < 10 \]

- **left**
  \[ x'_1 = v \sin \vartheta \]
  \[ x'_2 = v \cos \vartheta \]
  \[ \tau' = 1 \]
  \[ \vartheta := \vartheta + \frac{\pi}{4} \]

- **right**
  \[ x'_1 = v \sin \vartheta \]
  \[ x'_2 = v \cos \vartheta \]
  \[ \tau' = -1 \]
  \[ \tau \geq 0 \]
  \[ \vartheta := \vartheta - \frac{\pi}{4} \]

- **straight**
  \[ x'_1 = v \sin \vartheta \]
  \[ x'_2 = v \cos \vartheta \]
  \[ \vartheta := \vartheta - \frac{\pi}{4} \]
\[ \varphi_q(t; x, y, \tau) = \begin{pmatrix} x_1 + tv \sin \vartheta \\ x_2 + tv \cos \vartheta \\ y_1 + tu \sin \varsigma \\ y_2 + tu \cos \varsigma \\ \tau + t \end{pmatrix} \]
\[ \text{inv}_{\text{cruise}} \equiv \| x - y \| \geq \alpha \]
\[ \text{inv}_{\text{cruise}} \equiv \| x - y \| \geq \alpha \]

\[ \text{inv}_{\text{right}} \equiv \tau \geq 0 \]
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{\text{cruise}} \equiv \|x - y\| \geq \alpha$
- $inv_{\text{right}} \equiv \tau \geq 0$
- $inv_{\text{left}} \equiv inv_{\text{straight}} \equiv \text{true}$
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{\text{cruise}} \equiv \|x - y\| \geq \alpha$
- $inv_{\text{right}} \equiv \tau \geq 0$
- $inv_{\text{left}} \equiv inv_{\text{straight}} \equiv \text{true}$
- $jump_e(x, x^+) \equiv guard_e(x) \land reset_e(x, x^+)$

André Platzer (CMU)
- $\text{inv}_{\text{cruise}} \equiv \|x - y\| \geq \alpha$
- $\text{inv}_{\text{right}} \equiv \tau \geq 0$
- $\text{inv}_{\text{left}} \equiv \text{inv}_{\text{straight}} \equiv \text{true}$
- $\text{jump}_e(x, x^+) \equiv \text{guard}_e(x) \land \text{reset}_e(x, x^+)$
- $\text{guard}_{\text{cruise, left}} \equiv \|x - y\| < 10$
inv\textsubscript{cruise} \equiv \|x - y\| \geq \alpha

inv\textsubscript{right} \equiv \tau \geq 0

inv\textsubscript{left} \equiv inv\textsubscript{straight} \equiv true

jump\textsubscript{e}(x, x^+) \equiv guard\textsubscript{e}(x) \land reset\textsubscript{e}(x, x^+)

guard\textsubscript{cruise, left} \equiv \|x - y\| < 10

reset\textsubscript{cruise, left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}
- \( \text{inv}_{\text{cruise}} \equiv \| x - y \| \geq \alpha \)
- \( \text{inv}_{\text{right}} \equiv \tau \geq 0 \)
- \( \text{inv}_{\text{left}} \equiv \text{inv}_{\text{straight}} \equiv \text{true} \)
- \( \text{jump}_e (x, x^+) \equiv \text{guard}_e (x) \land \text{reset}_e (x, x^+) \)
- \( \text{guard}_{\text{cruise, left}} \equiv \| x - y \| < 10 \)
- \( \text{reset}_{\text{cruise, left}} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4} \)
- \( \text{reset}_{\text{left, straight}} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4} \)
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv ||x - y|| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \land reset_e(x, x^+)$
- $guard_{cruise, left} \equiv ||x - y|| < 10$
- $reset_{cruise, left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$
- $reset_{left, straight} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $reset_{straight, right} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$

\[\vartheta := \vartheta + \frac{\pi}{4}\]
\[\vartheta := \vartheta - \frac{\pi}{4}\]
\[\tau \leq 0\]
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{\text{cruise}} \equiv \|x - y\| \geq \alpha$
- $inv_{\text{right}} \equiv \tau \geq 0$
- $inv_{\text{left}} \equiv inv_{\text{straight}} \equiv \text{true}$
- $jump_e(x, x^+) \equiv guard_e(x) \land reset_e(x, x^+)$
- $guard_{\text{cruise, left}} \equiv \|x - y\| < 10$
- $reset_{\text{cruise, left}} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$
- $reset_{\text{left, straight}} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $reset_{\text{straight, right}} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $guard_{\text{right, cruise}} \equiv \tau \leq 0$
Hybrid Automaton for Collision Avoidance: Formal

- \( \text{inv}_{\text{cruise}} \equiv \| x - y \| \geq \alpha \)
- \( \text{inv}_{\text{right}} \equiv \tau \geq 0 \)
- \( \text{inv}_{\text{left}} \equiv \text{inv}_{\text{straight}} \equiv \text{true} \)
- \( \text{jump}_e(x, x^+ \equiv \text{guard}_e(x) \land \text{reset}_e(x, x^+) \)
- \( \text{guard}_{\text{cruise, left}} \equiv \| x - y \| < 10 \)
- \( \text{reset}_{\text{cruise, left}} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4} \)
- \( \text{reset}_{\text{left, straight}} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4} \)
- \( \text{reset}_{\text{straight, right}} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4} \)
- \( \text{guard}_{\text{right, cruise}} \equiv \tau \leq 0 \)
- \( \text{reset}_{\text{right, cruise}} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4} \)
Example (Property)
If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

Example (Property)
If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?
Definition (Hybrid Automata → Hybrid System as LTS)

- LTS State space $(Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}$
- Discrete transition $(q, x) \xrightarrow{a} (q^+, x^+)$ iff there is an edge $e$ from $q$ to $q^+$ with input $a$ such that $(x, x^+) \in jump_e$
- Continuous transition $(q, x) \xrightarrow{r} (q, x^+)$ iff $x^+ = \varphi_q(r; x)$ for $r \geq 0$ and $\varphi_q(t; x) \in inv_q$ for all $0 \leq t \leq r$. 

André Platzer (CMU)
Definition (Hybrid Automata → Hybrid System as LTS)

- LTS State space \((Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}\)
- Discrete transition \((q, x) \xrightarrow{a} (q^+, x^+)\) iff there is an edge \(e\) from \(q\) to \(q^+\) with input \(a\) such that \((x, x^+) \in jump_e\)
- Continuous transition \((q, x) \xrightarrow{r} (q, x^+)\) iff \(x^+ = \varphi_q(r; x)\) for \(r \geq 0\) and \(\varphi_q(t; x) \in inv_q\) for all \(0 \leq t \leq r\).
Hybrid Systems

Definition (Hybrid Automata → Hybrid System as LTS)

- LTS State space \((Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}\)
- Discrete transition \((q, x) \xrightarrow{a} (q^+, x^+)\) iff there is an edge \(e\) from \(q\) to \(q^+\) with input \(a\) such that \((x, x^+) \in jump_e\)
- Continuous transition \((q, x) \xrightarrow{r} (q, x^+)\) iff \(x^+ = \varphi_q(r; x)\) for \(r \geq 0\) and \(\varphi_q(t; x) \in inv_q\) for all \(0 \leq t \leq r\).
Hybrid Systems

Definition (Hybrid Automata → Hybrid System as LTS)

- LTS State space \((Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}\)
- Discrete transition \((q, x) \xrightarrow{a} (q^+, x^+)\) iff there is an edge \(e\) from \(q\) to \(q^+\) with input \(a\) such that \((x, x^+) \in \text{jump}_e\)
- Continuous transition \((q, x) \xrightarrow{r} (q, x^+)\) iff \(x^+ = \varphi_q(r; x)\) for \(r \geq 0\) and \(\varphi_q(t; x) \in inv_q\) for all \(0 \leq t \leq r\).
Hybrid Systems

Definition (Hybrid Automata \(\rightarrow\) Hybrid System as LTS)

- LTS State space \((Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}\)
- Discrete transition \((q, x) \xrightarrow{a} (q^+, x^+\)) iff there is an edge \(e\) from \(q\) to \(q^+\) with input \(a\) such that \((x, x^+) \in jump_e\)
- Continuous transition \((q, x) \xrightarrow{r} (q, x^+)\) iff \(x^+ = \varphi_q(r; x)\) for \(r \geq 0\) and \(\varphi_q(t; x) \in inv_q\) for all \(0 \leq t \leq r\).
Hybrid Systems

Definition (Hybrid Automata → Hybrid System as LTS)

- LTS State space \((Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}\)
- Discrete transition \((q, x) \xrightarrow{a} (q^+, x^+)\) iff there is an edge \(e\) from \(q\) to \(q^+\) with input \(a\) such that \((x, x^+) \in jump_e\)
- Continuous transition \((q, x) \xrightarrow{r} (q, x^+)\) iff \(x^+ = \varphi_q(r; x)\) for \(r \geq 0\) and \(\varphi_q(t; x) \in inv_q\) for all \(0 \leq t \leq r\).
Hybrid Systems

Definition (Hybrid Automata $\rightarrow$ Hybrid System as LTS)

- **LTS State space** $(Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}$
- **Discrete transition** $(q, x) \xrightarrow{a} (q^+, x^+)$ iff there is an edge $e$ from $q$ to $q^+$ with input $a$ such that $(x, x^+) \in jump_e$
- **Continuous transition** $(q, x) \xrightarrow{r} (q, x^+)$ iff $x^+ = \varphi_q(r; x)$ for $r \geq 0$ and $\varphi_q(t; x) \in inv_q$ for all $0 \leq t \leq r$. 
Hybrid Systems

Definition (Hybrid Automata $\rightarrow$ Hybrid System as LTS)

- LTS State space $(Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}$
- Discrete transition $(q, x) \xrightarrow{a} (q^+, x^+)$ iff there is an edge $e$ from $q$ to $q^+$ with input $a$ such that $(x, x^+) \in jump_e$
- Continuous transition $(q, x) \xrightarrow{r} (q, x^+)$ iff $x^+ = \varphi_q(r; x)$ for $r \geq 0$ and $\varphi_q(t; x) \in inv_q$ for all $0 \leq t \leq r$. 

Andre Platzer (CMU)

LAHS/04: Hybrid Systems Examples
Definition (Hybrid Automata → Hybrid System as LTS)

- LTS State space $\left( Q \times \mathbb{R}^n \right) \cap \{(q, x) : x \in inv_q\}$

- Discrete transition $(q, x) \xrightarrow{a} (q^+, x^+)$ iff there is an edge $e$ from $q$ to $q^+$ with input $a$ such that $(x, x^+) \in \text{jump}_e$

- Continuous transition $(q, x) \xrightarrow{r} (q, x^+)$ iff $x^+ = \varphi_q(r; x)$ for $r \geq 0$ and $\varphi_q(t; x) \in inv_q$ for all $0 \leq t \leq r$. 

\[ Q_0 \xrightarrow{Post_A(Q_0)} Q_1 = Post_A(Q_0) \]
Hybrid Systems

Definition (Hybrid Automata $\rightarrow$ Hybrid System as LTS)

- LTS State space $(Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}$
- Discrete transition $(q, x) \xrightarrow{a} (q^+, x^+)$ iff there is an edge $e$ from $q$ to $q^+$ with input $a$ such that $(x, x^+) \in jump_e$
- Continuous transition $(q, x) \xrightarrow{r} (q, x^+)$ iff $x^+ = \varphi_q(r; x)$ for $r \geq 0$ and $\varphi_q(t; x) \in inv_q$ for all $0 \leq t \leq r$.

\[ Q_0 \xrightarrow{Post_A(Q_0)} Q_1 = Post_A(Q_0) \]  
\[ Q_2 = Post_A^2(Q_0) \]
Hybrid Systems

Definition (Hybrid Automata $\rightarrow$ Hybrid System as LTS)

- LTS State space $(Q \times \mathbb{R}^n) \cap \{(q, x) : x \in inv_q\}$
- Discrete transition $(q, x) \xrightarrow{a} (q^+, x^+)$ iff there is an edge $e$ from $q$ to $q^+$ with input $a$ such that $(x, x^+) \in jump_e$
- Continuous transition $(q, x) \xrightarrow{r} (q, x^+)$ iff $x^+ = \varphi_q(r; x)$ for $r \geq 0$ and $\varphi_q(t; x) \in inv_q$ for all $0 \leq t \leq r$.

André Platzer (CMU)
**Definition (Hybrid Systems Model Checking Problem for Reachability)**

Given initial states $Q_0 \subseteq Q$ and bad states $B \subseteq Q$ for a hybrid automaton, check whether there is a trace from some $q_0 \in Q_0$ to some $q_b \in B$. 
Definition (Hybrid Systems Model Checking Problem for Reachability)

Given initial states $Q_0 \subseteq Q$ and bad states $B \subseteq Q$ for a hybrid automaton, check whether there is a trace from some $q_0 \in Q_0$ to some $q_b \in B$.

Central question: How to compute?
Definition (Hybrid Systems Model Checking Problem for Reachability)

Given initial states $Q_0 \subseteq Q$ and bad states $B \subseteq Q$ for a hybrid automaton, check whether there is a trace from some $q_0 \in Q_0$ to some $q_b \in B$.

Central question: How to compute? Stay tuned . . .
Bouncing Ball as a Hybrid System

\[ h' = v, \quad v' = -g \quad h \geq 0 \]
\[ v = -cv, \quad h = 0 \]

Example (Property)
If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)? No!

Initial \( v > 0 \) then climbs first. Does bouncing ever stop?
Bouncing Ball as a Hybrid System

\[
\begin{align*}
h' &= v \\
v' &= -g \\
h &\geq 0
\end{align*}
\]

Example (Property)

If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?

No!

Initial \( v > 0 \) then climbs first. Does bouncing ever stop?
Bouncing Ball as a Hybrid System

\[ h' = v \]
\[ v' = -g \]
\[ h \geq 0 \]
\[ v := -cv \]
\[ h = 0 \]

**Example (Property)**

If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?
Bouncing Ball as a Hybrid System

\[
\begin{align*}
  \dot{h} &= v \\
  \dot{v} &= -g \\
  v &:= -cv \\
  h \geq 0
\end{align*}
\]

Example (Property)

If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?

No!

Initial \( v > 0 \) then climbs first. Does bouncing ever stop?

André Platzer (CMU)
LAHS/04: Hybrid Systems Examples
Bouncing Ball as a Hybrid System

\[ h' = v \]
\[ v' = -g \]
\[ h \geq 0 \]
\[ v := -cv \]

Example (Property)
If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?

No!
Example (Property)

If initially $h = H$, then bouncing ball always $0 \leq h \leq H$?  

No!

Initial $v > 0$ then climbs first. Does bouncing ever stop?
There is wind resistance, so the ODE should be

\[ h' = v, \quad v' = -g \]
There is wind resistance, so the ODE should be

\[ h' = v, \quad v' = -g \]
Aerodynamical Bouncing Ball as a Hybrid System

\[ h' = v \]
\[ v' = -g + dv^2 \]
\[ h \geq 0 \]
\[ v \leq 0 \]
\[ v := -cv \]

\[ h' = v \]
\[ v' = -g - dv^2 \]
\[ h \geq 0 \]
\[ v \geq 0 \]
\[ v := -cv \]

Example (Property)

If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?
Aerodynamical Bouncing Ball as a Hybrid System

\[ h' = v \]
\[ v' = -g + dv^2 \]
\[ h \geq 0 \]
\[ v \leq 0 \]
\[ v := -cv \]

\[ h' = v \]
\[ v' = -g - dv^2 \]
\[ h \geq 0 \]
\[ v \geq 0 \]
\[ v := -cv \]

Example (Property)

If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?
Aerodynamical Bouncing Ball as a Hybrid System

\[ h' = v \\
\frac{dv}{dt} = -g + dv^2 \]

\[ h \geq 0 \]
\[ v \leq 0 \]

\[ v := -cv \]

\[ h = 0 \]

\[ v = 0 \]
\[ h = 0 \]

\[ \frac{dv}{dt} = -g - dv^2 \]

\[ h \geq 0 \]
\[ v \geq 0 \]

\[ v := -cv \]

Example (Property)

If initially \( h = H \), then bouncing ball always \( 0 \leq h \leq H \)?

No!
Train Control Challenge

**Challenge**

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control Challenge: Overly Simplistic Example

Example (Overly Simplistic Train Control)

\[ \text{accel} \]
\[ z' = v \]
\[ v' = a \]

\[ \text{brake} \]
\[ z \geq SB \]
\[ a := -b \]
\[ v \leq 1 \]
\[ a := a + 5 \]

\[ v \geq 0 \]
Simple Water Tank

Example (Property)

If initially $1 \leq x \leq 10$, then water tank always $1 \leq x \leq 10$?

No!

Can stay in open too long, even until $x = 0$. 

André Platzer (CMU)
Example (Property)

If initially $1 \leq x \leq 10$, then water tank always $1 \leq x \leq 10$?

No!

Can stay in open too long, even until $x = 0$. 

Andre Platzer (CMU)
Simple Water Tank

Example (Property)
If initially $1 \leq x \leq 10$, then water tank always $1 \leq x \leq 10$?
Example (Property)

If initially $1 \leq x \leq 10$, then water tank always $1 \leq x \leq 10$?
Example (Property)

If initially $1 \leq x \leq 10$, then water tank always $1 \leq x \leq 10$?  

No!
Example (Property)

If initially $1 \leq x \leq 10$, then water tank always $1 \leq x \leq 10$? \textbf{No!}

Can stay in \textit{open} too long, even until $x = 0$
T. Krilavičius.
Bestiarius of hybrid systems.

A. Platzer.
*Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.*