Deductive Verification Of Hybrid Systems

Lectures on Formal Methods for Cyber-Physical Systems
SOKENDAI, 07/29/19

Jérémy Dubut
National Institute of Informatics
Japanese-French Laboratory of Informatics

Objectives of this lecture

- <u>Deductive system to prove invariants of hybrid systems</u>
- Representability of HS (hybrid programs)
- Platzer's Differential Dynamic Logic
- Sequent calculus for this logic

References

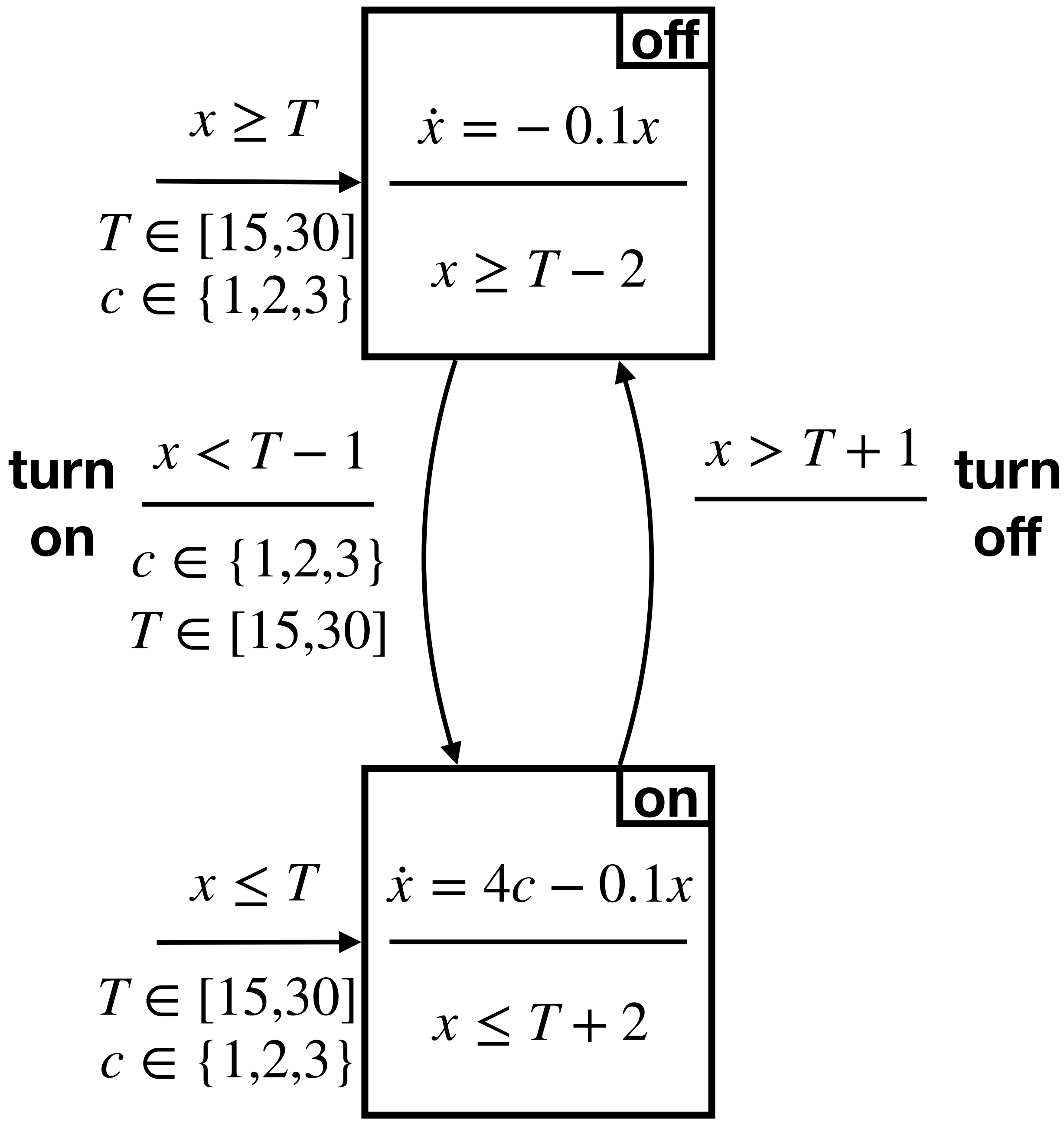
- T. A. Henzinger, The Theory of Hybrid Automata, *Verification of Digital and Hybrid Systems,* volume 170 of the *NATO ASI Series*, pp 265-292. Springer, 2000.

- A. Platzer's group. http://symbolaris.com

- A. Platzer, *Logical Foundations of Cyber-Physical Systems.* Springer, 2018.

- J. Kolčák, I. Hasuo, J. Dubut, S. Katsumata, D. Sprunger, A. Yamada, Relational Differential Dynamic Logic. Preprint arXiv:1903.00153.

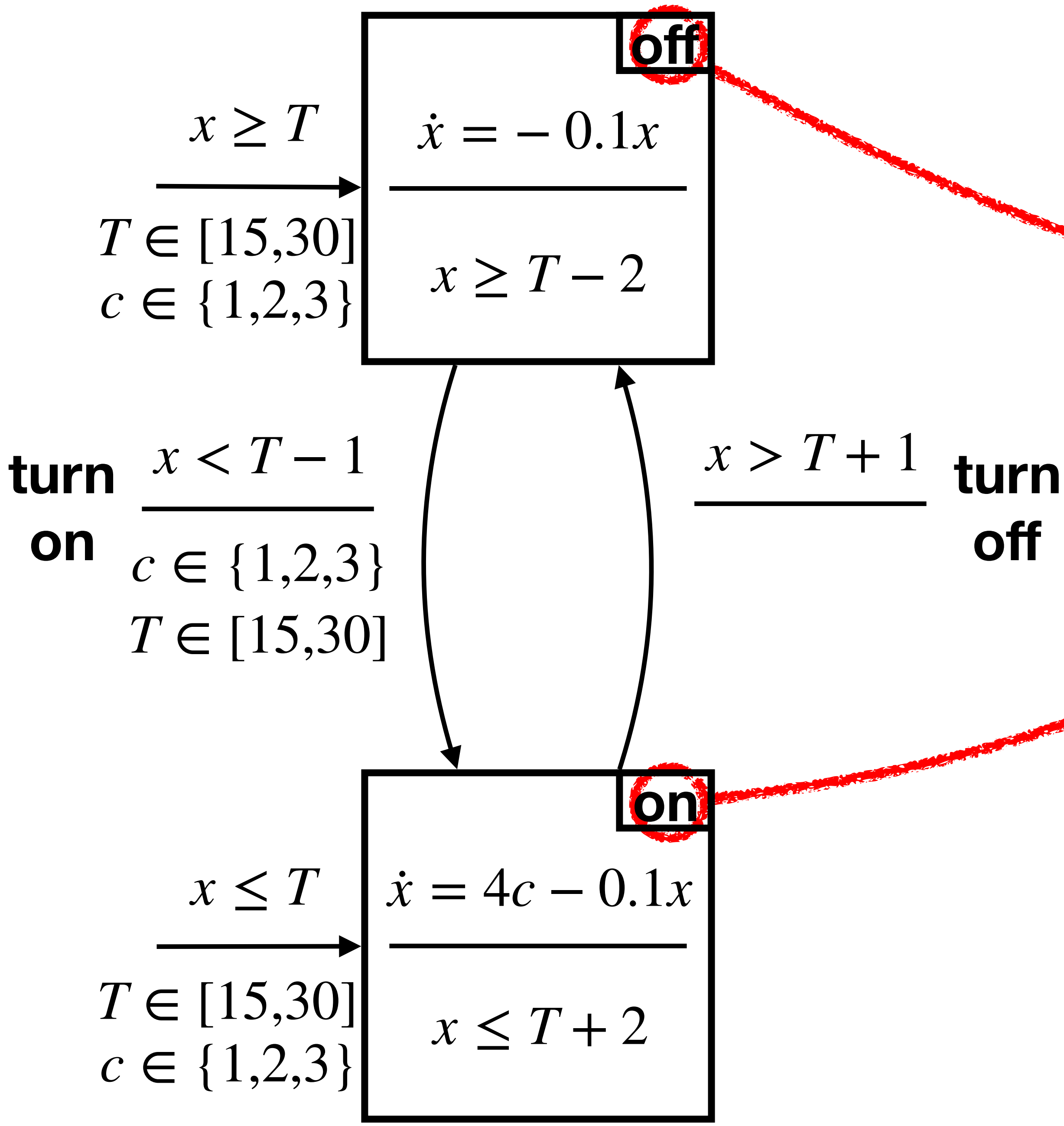
Recap' on hybrid automata



Thermostat system

A **hybrid automaton** is:

Recap' on hybrid automata



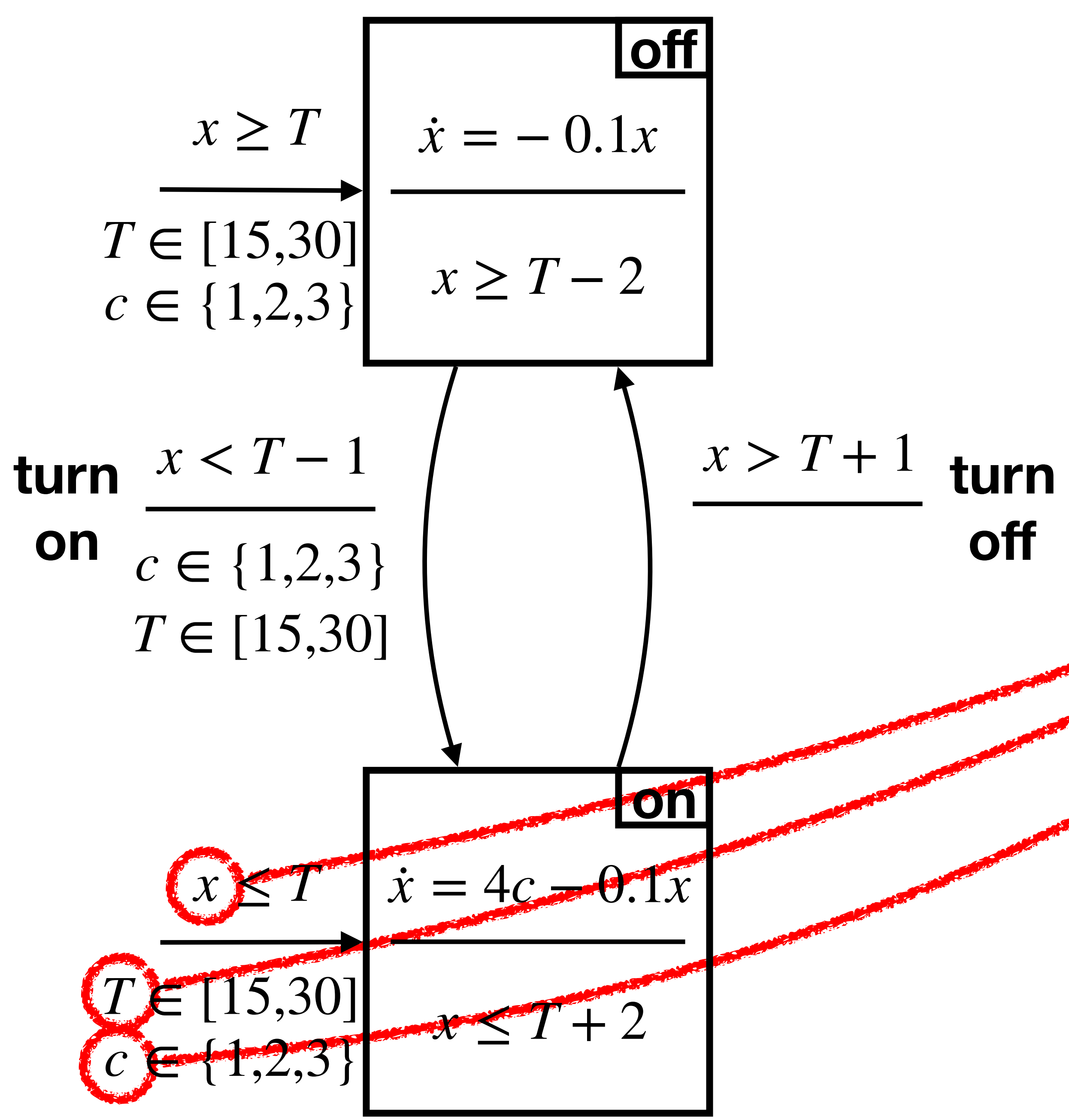
Thermostat system

A **hybrid automaton** is:

- a set M of **modes**

M = {on, off}

Recap' on hybrid automata



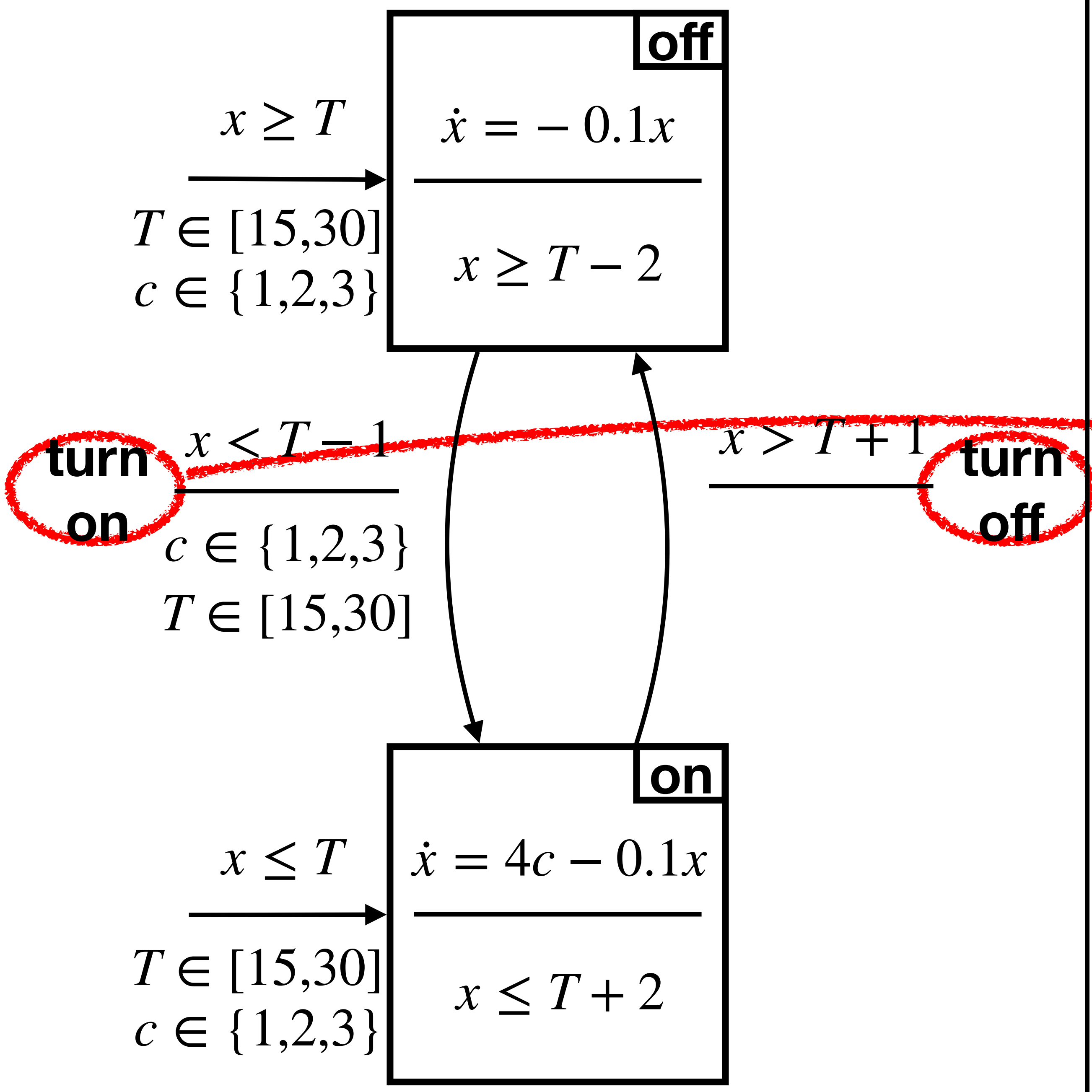
Thermostat system

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**

V = {x, c, T}

Recap' on hybrid automata



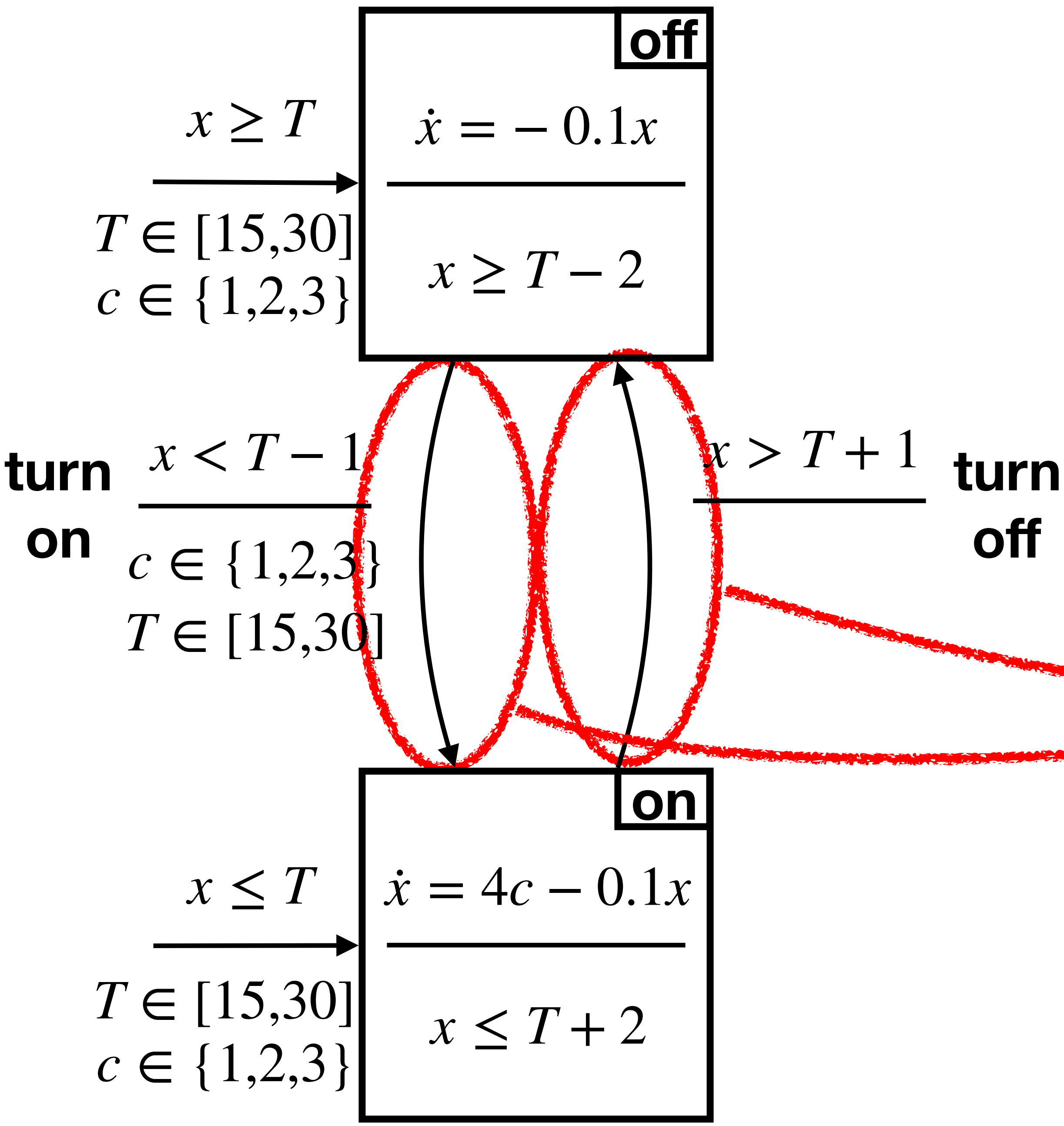
Thermostat system

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**

E = {turn on, turn off}

Recap' on hybrid automata



Thermostat system

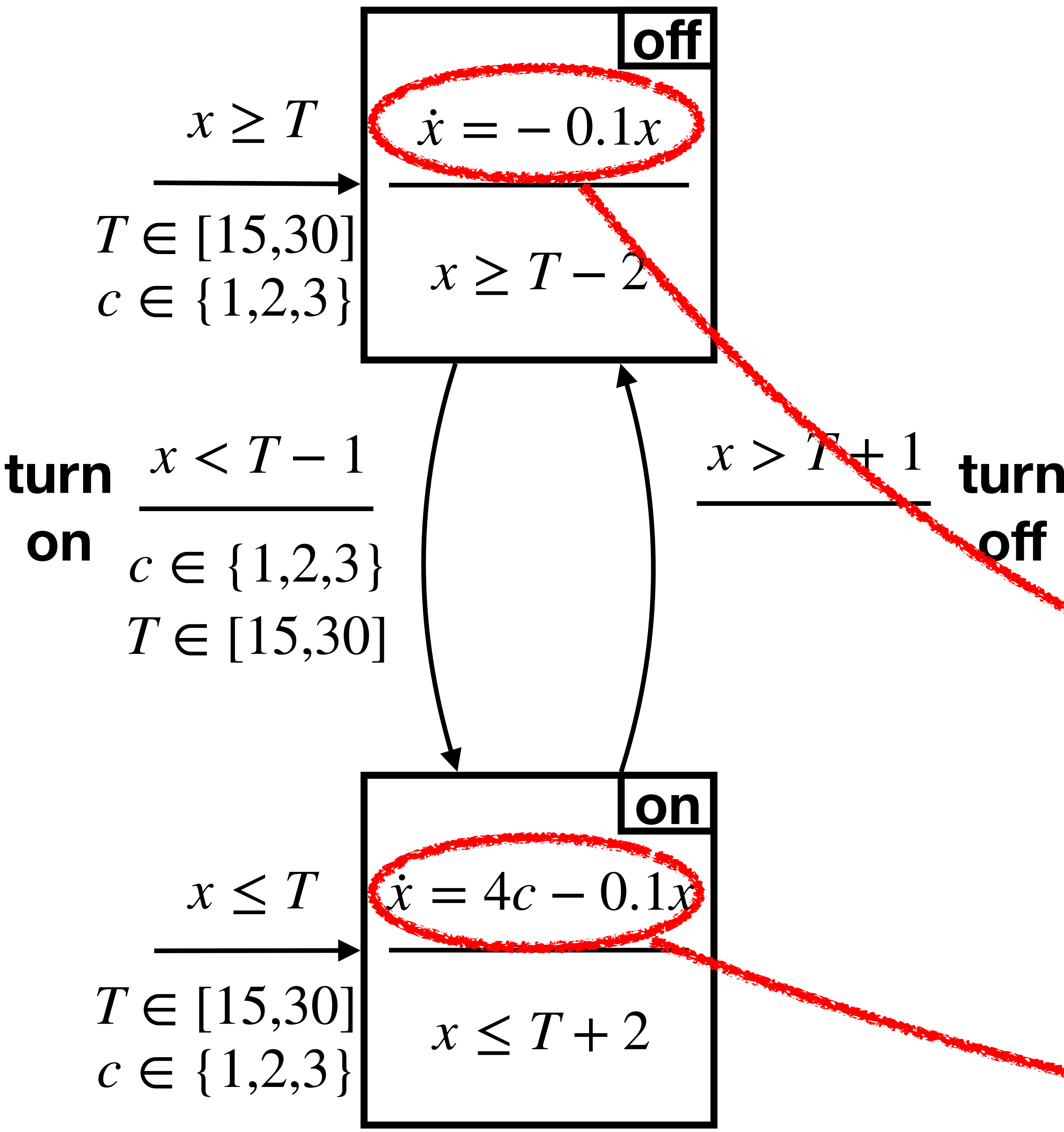
A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

s(turn off) = on
s(turn on) = off
t(turn off) = off
t(turn on) = on

Recap' on hybrid automata



Thermostat system

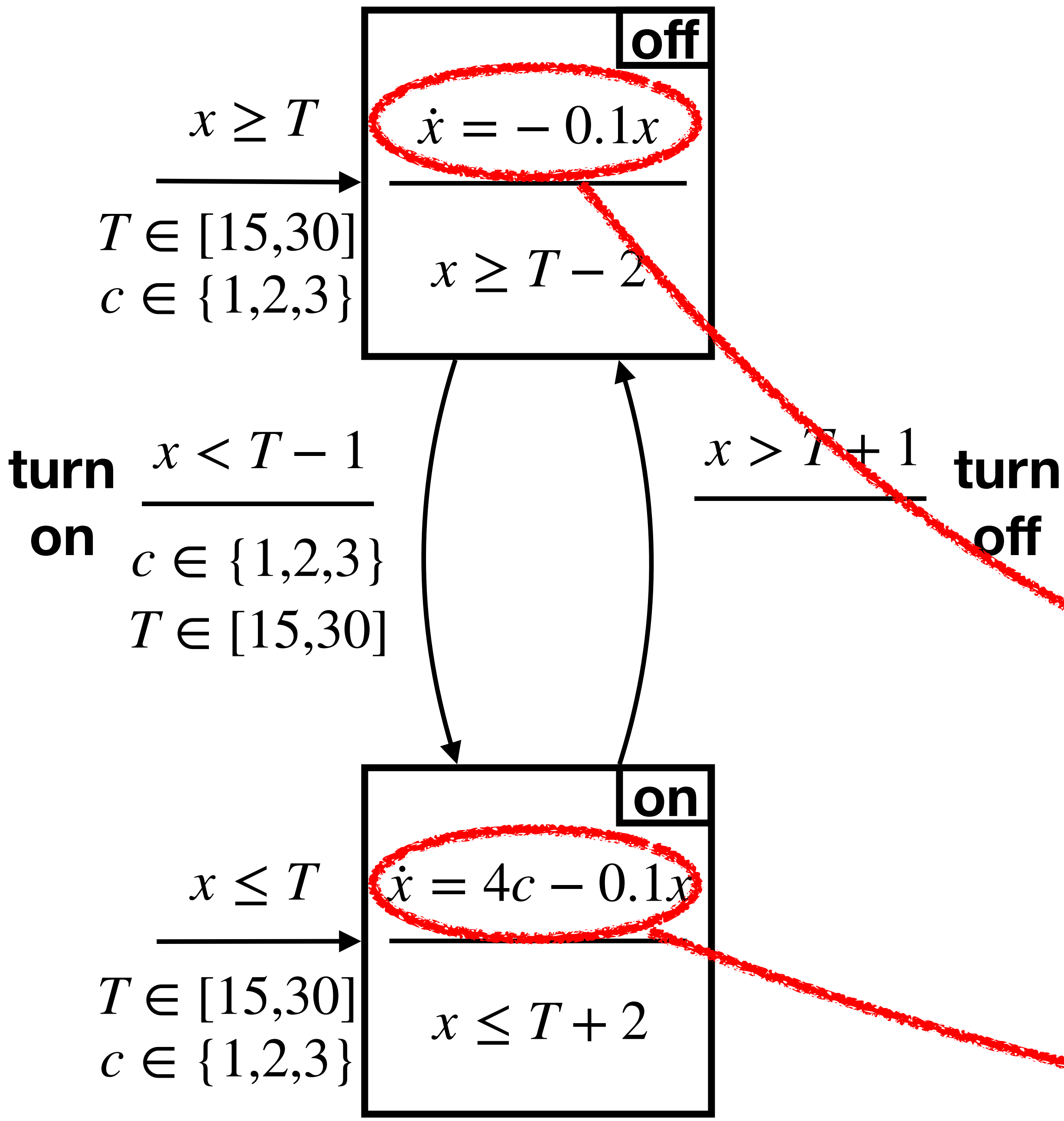
A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$

$$\boxed{F_{off}(x, c, T, t) = (-0.1x, 0, 0)}$$

$$\boxed{F_{on}(x, c, T, t) = (4c - 0.1x, 0, 0)}$$

Recap' on hybrid automata



Thermostat system

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

$$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$

$$\boxed{F_{off}(x, c, T, t) = (-0.1x, 0, 0)}$$

$x(t) =$ **cst** $\exp(-0.1t)$

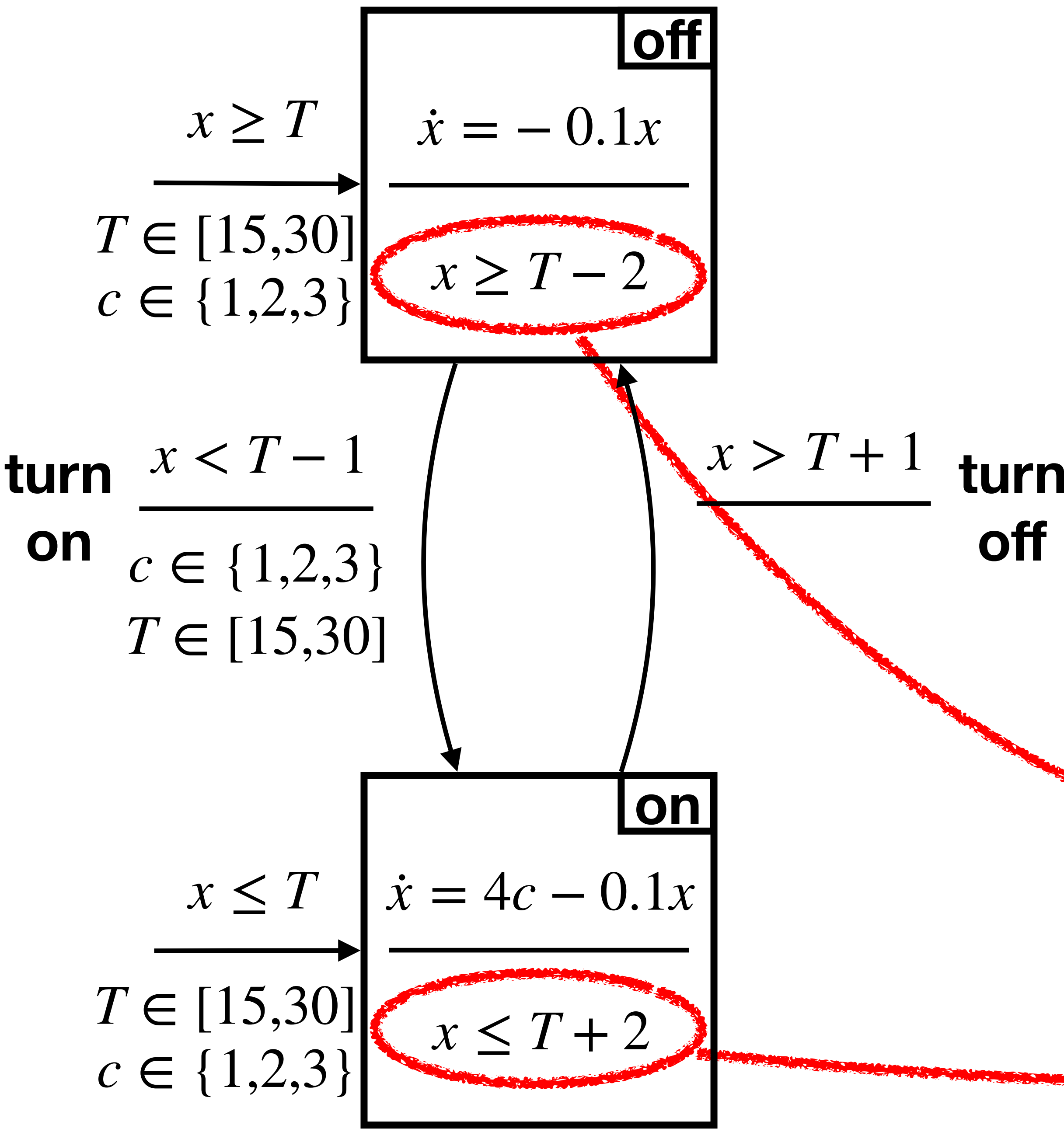
$c =$ **cst**, $T =$ **cst**

$$\boxed{F_{on}(x, c, T, t) = (4c - 0.1x, 0, 0)}$$

$x(t) = 40c +$ **cst** $\exp(-0.1t)$

$c =$ **cst**, $T =$ **cst**

Recap' on hybrid automata



Thermostat system

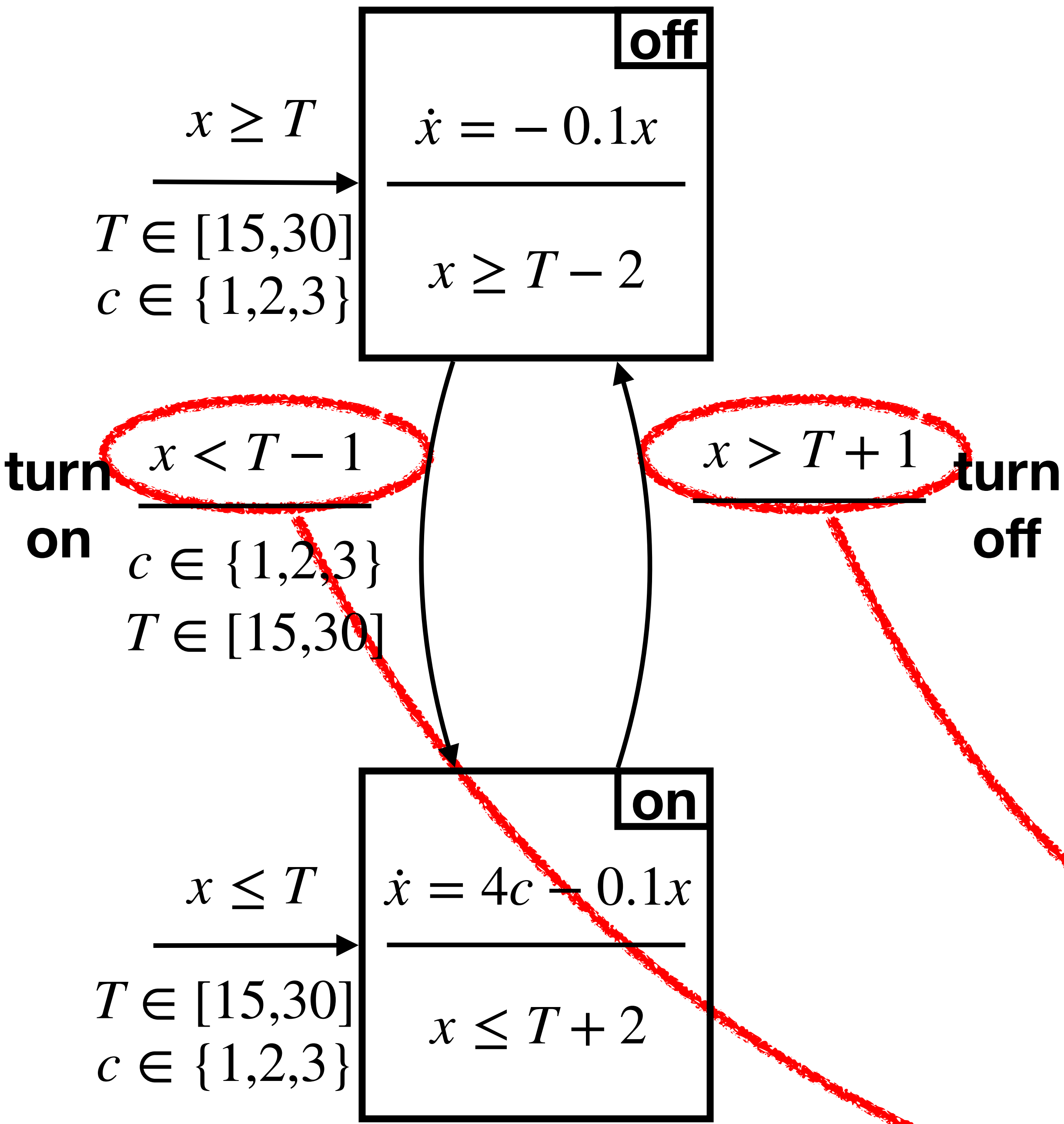
A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate
  $$I_m \subseteq \mathbb{R}^V$$

$$\boxed{I_{off} = \{(x, c, T) \mid x \geq T - 2\}}$$

$$\boxed{I_{on} = \{(x, c, T) \mid x \leq T + 2\}}$$

Recap' on hybrid automata



Thermostat system

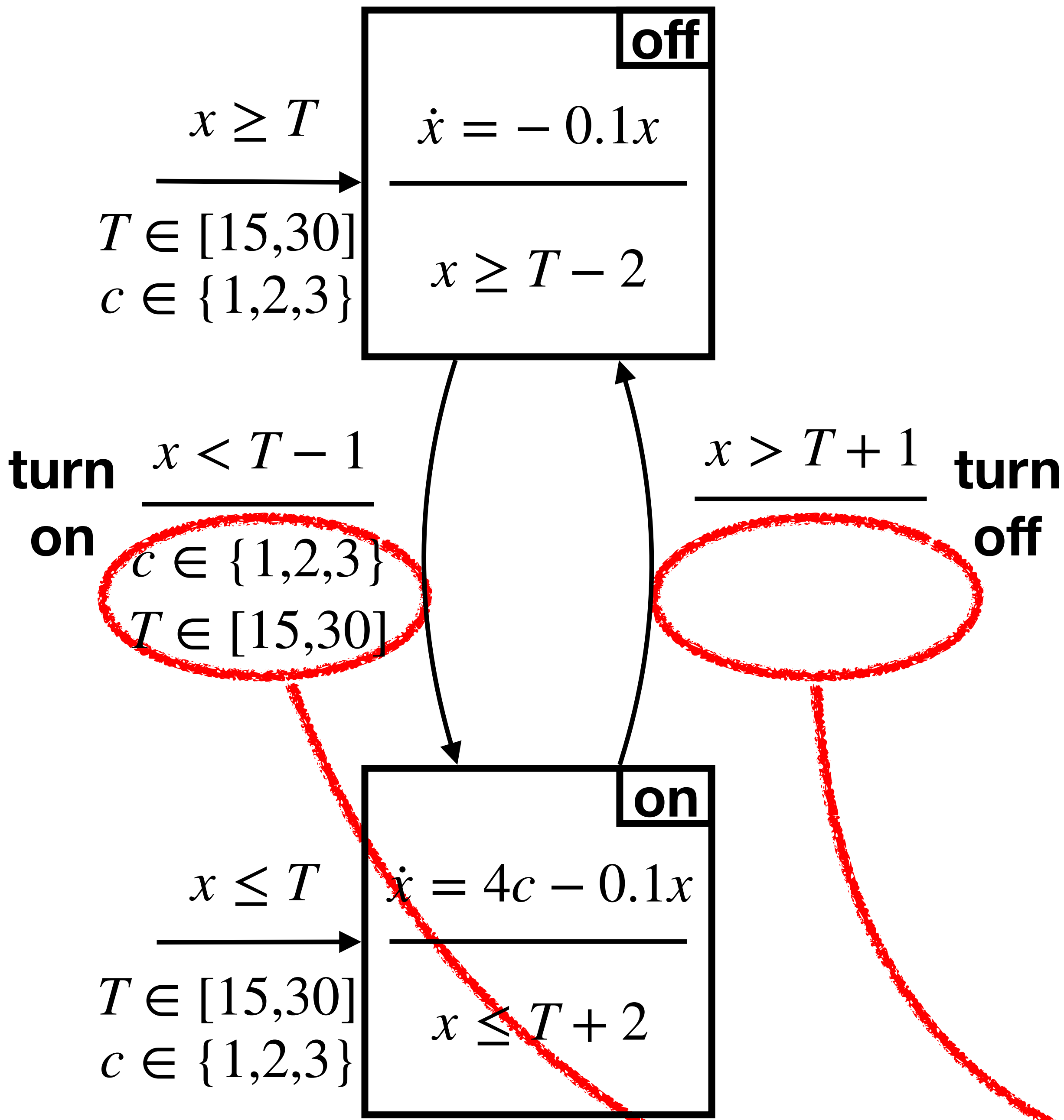
A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate
  $$I_m \subseteq \mathbb{R}^V$$
- for every event e, a **guard** predicate
  $$G_e \subseteq \mathbb{R}^V$$

$$\boxed{G_{turn\ off} = \{(x, c, T) \mid x > T + 1\}}$$

$$\boxed{G_{turn\ on} = \{(x, c, T) \mid x < T - 1\}}$$

Recap' on hybrid automata



Thermostat system

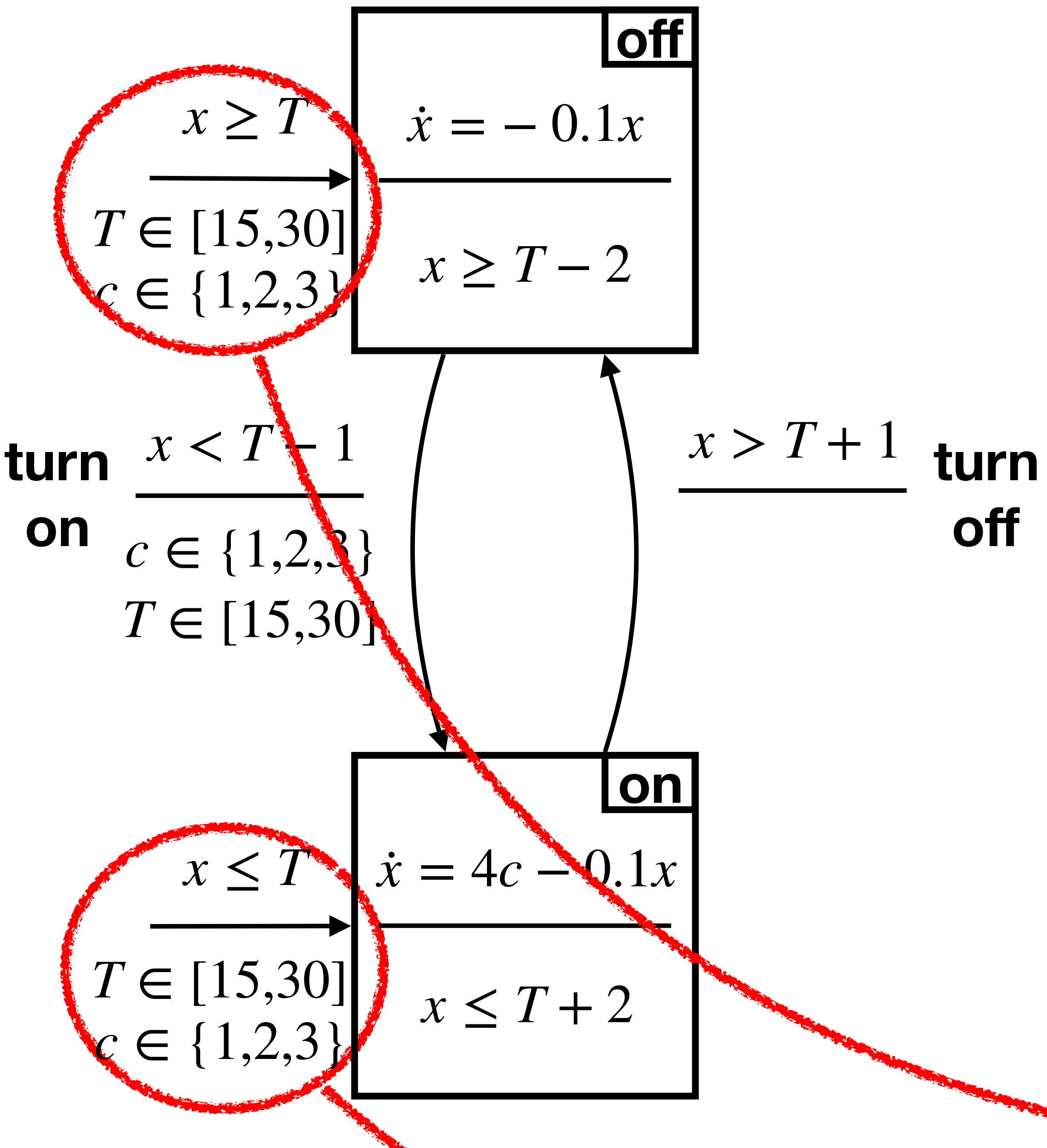
A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate
  $$I_m \subseteq \mathbb{R}^V$$
- for every event e, a **guard** predicate
  $$G_e \subseteq \mathbb{R}^V$$
- for every event e, a **jump** relation
  $$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$

$$\boxed{J_{turn\ off} = \{(x, c, T, x', c', T') \mid x = x' \land c = c' \land T = T'\}}$$

$$\boxed{J_{turn\ on} = \{(x, c, T, x', c', T') \mid x = x' \land c' \in \{1,2,3\} \land T' \in [15,30]\}}$$

Recap' on hybrid automata



Thermostat system

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate
  $$I_m \subseteq \mathbb{R}^V$$
- for every event e, a **guard** predicate
  $$G_e \subseteq \mathbb{R}^V$$
- for every event e, a **jump** relation
  $$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$
- for every mode m, an **initial** predicate
  $$I_{0,m} \subseteq \mathbb{R}^V$$

$$\boxed{I_{0,off} = \{(x, c, T) \mid x \geq T \wedge c \in \{1,2,3\} \wedge T \in [15,30]\}}$$

$$\boxed{I_{0,on} = \{(x, c, T) \mid x \leq T \wedge c \in \{1,2,3\} \wedge T \in [15,30]\}}$$

Goal: prove that the system is not going wrong

This means proving some properties on the set of *reachable configurations*

Configurations of a hybrid automaton

A **configuration** is an element of the form

$$(m, \omega) \in M \times \mathbb{R}^V$$

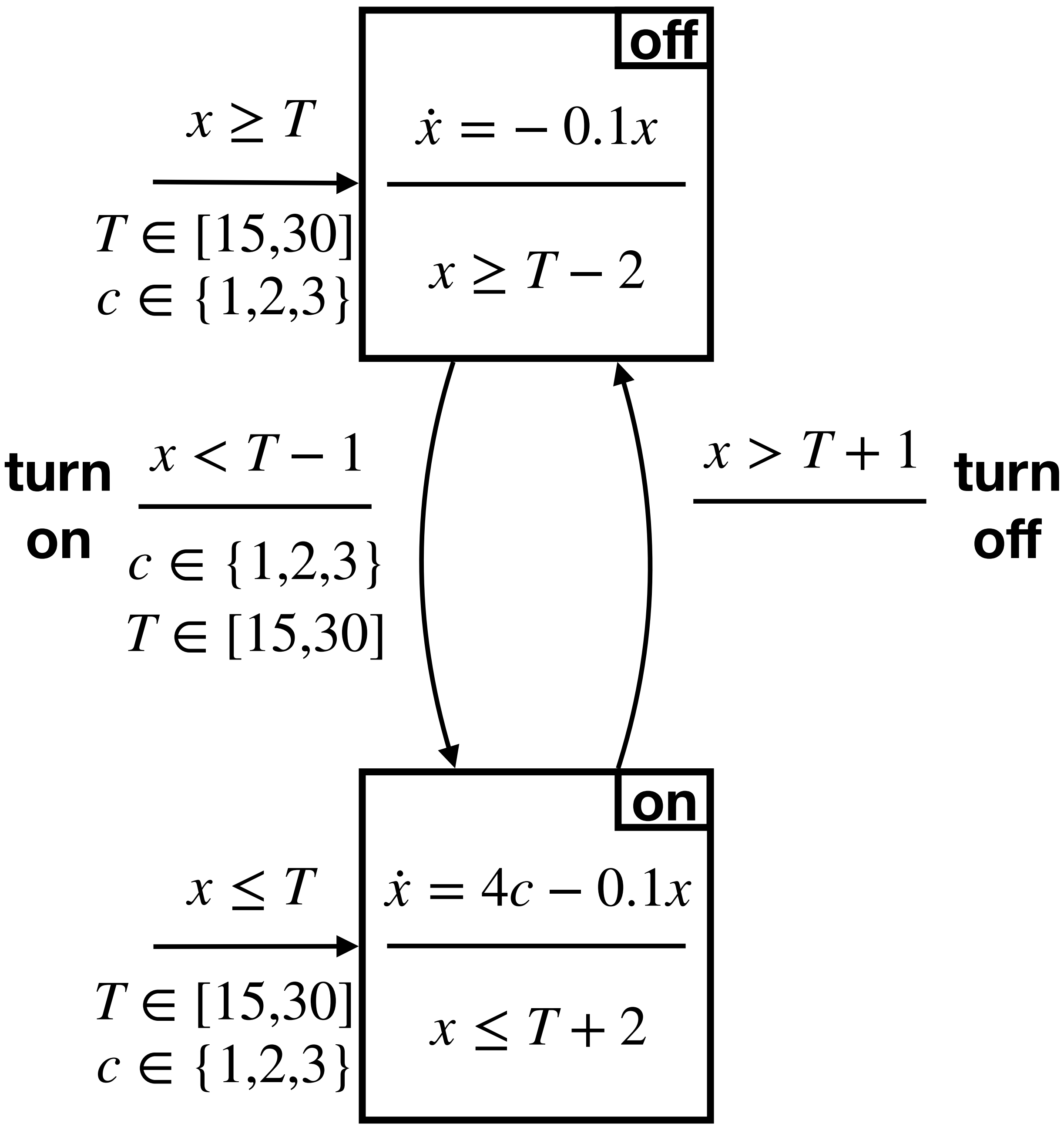
An **initial configuration** is a configuration (m, ω) such that $\omega \in I_{0,m}$.

A **valid configuration** is a configuration (m, ω) such that $\omega \in I_m$.

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate
  $$I_m \subseteq \mathbb{R}^V$$
- for every event e, a **guard** predicate
  $$G_e \subseteq \mathbb{R}^V$$
- for every event e, a **jump** relation
  $$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$
- for every mode m, an **initial** predicate
  $$I_{0,m} \subseteq \mathbb{R}^V$$

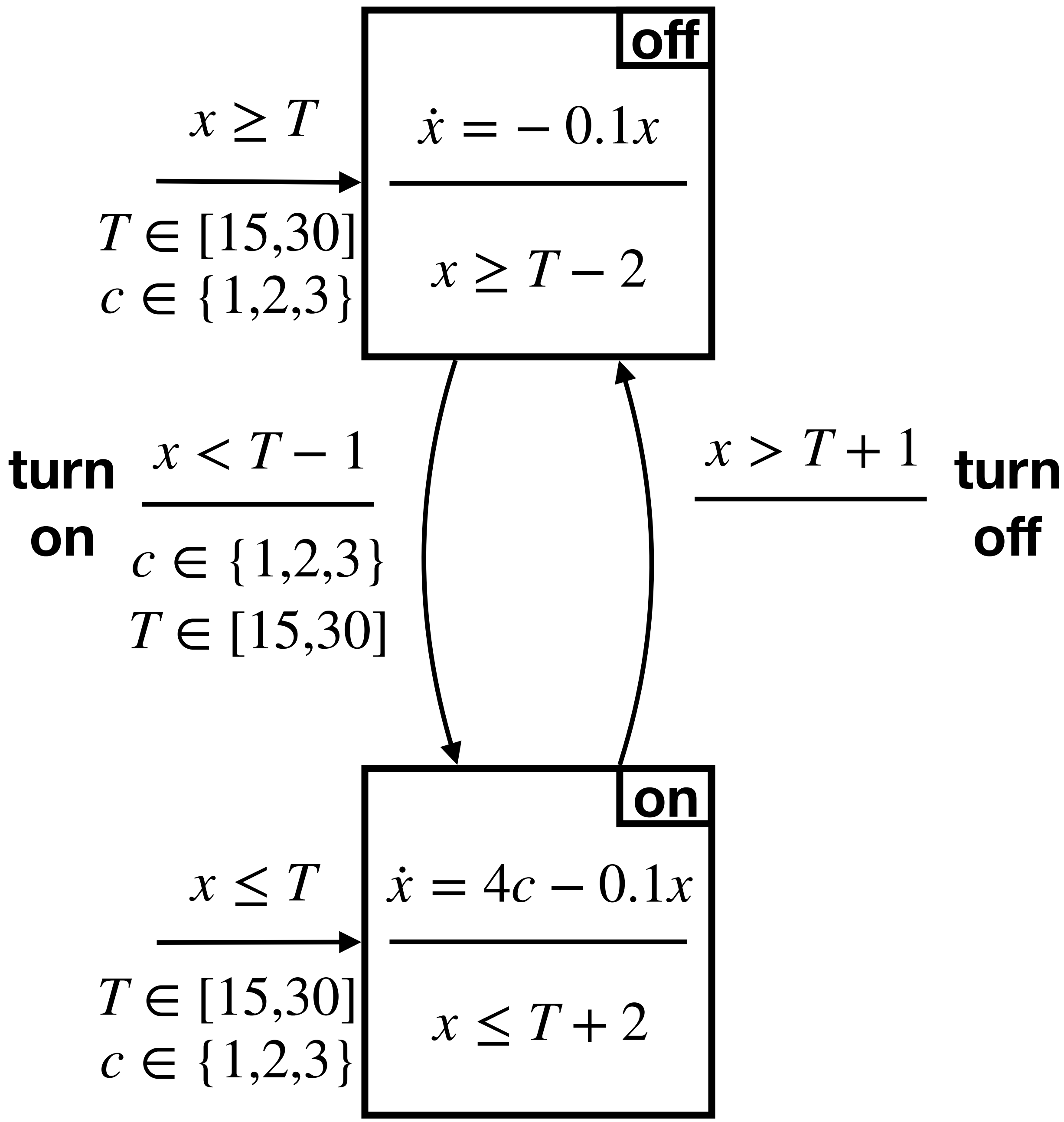
Example



Thermostat system

configuration (m, x, c, T)	initial	valid
(**off**,18,1,20)		
(**off**,17,2,20)		
(**on**,17,2,20)		
(**on**,21,1,20)		

Example



Thermostat system

configuration (m, x, c, T)	initial	valid
(**off**,18,1,20)	No	Yes
(**off**,17,2,20)	No	No
(**on**,17,2,20)	Yes	Yes
(**on**,21,1,20)	No	Yes

Discrete transitions of HA

Given two valid configurations

$$(m_1, \omega_1) \text{ and } (m_2, \omega_2)$$

we have a **discrete transition**

$$(m_1, \omega_1) \longrightarrow_d (m_2, \omega_2)$$

if there is an event $e \in E$ such that:

- $s(e) = m_1$ and $t(e) = m_2$
- $\omega_1 \in G_e$
- $(\omega_1, \omega_2) \in J_e$

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

$$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$

- for every mode m, an **invariant** predicate

$$I_m \subseteq \mathbb{R}^V$$

- for every event e, a **guard** predicate

$$G_e \subseteq \mathbb{R}^V$$

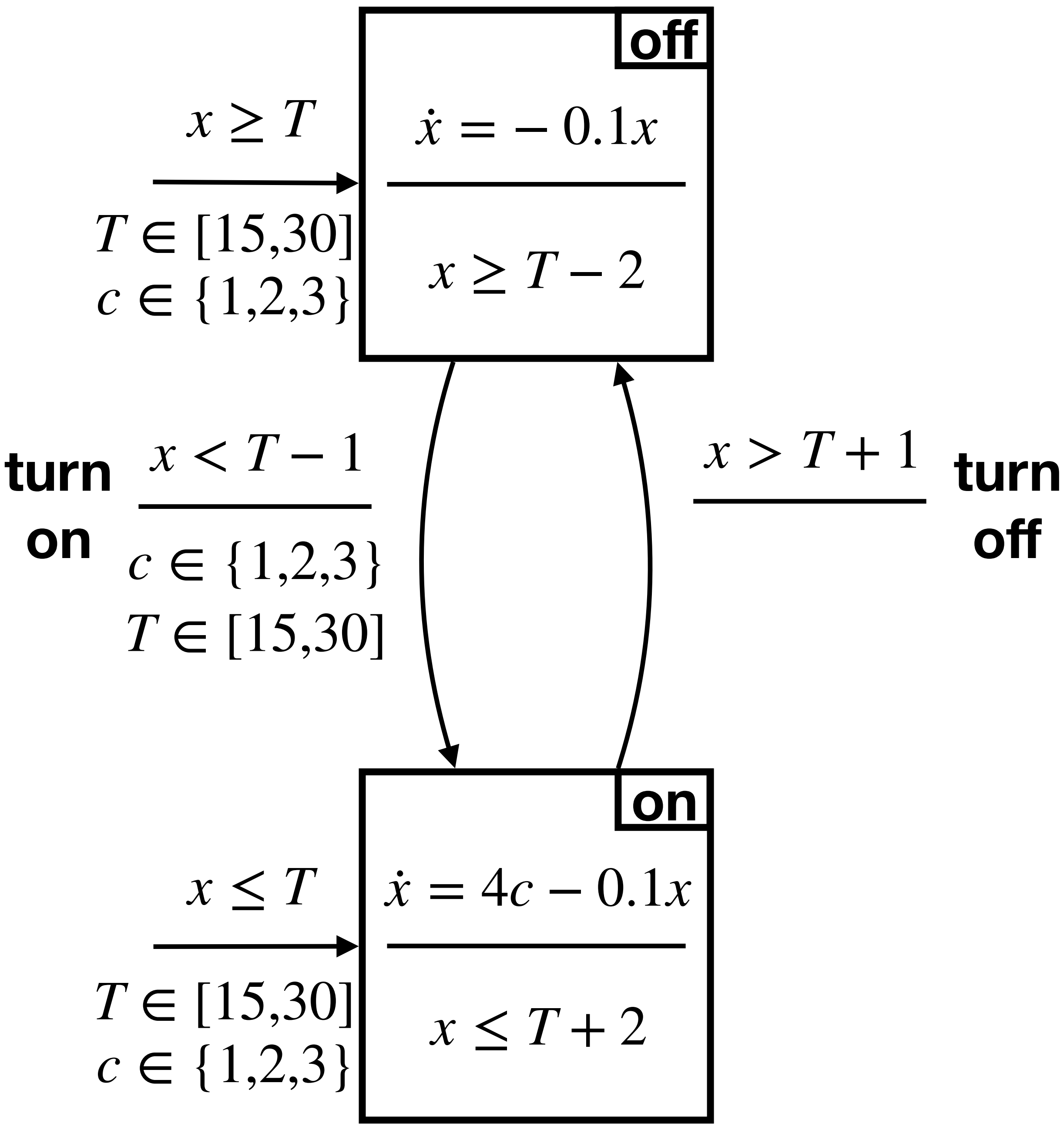
- for every event e, a **jump** relation

$$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$

- for every mode m, an **initial** predicate

$$I_{0,m} \subseteq \mathbb{R}^V$$

Example



Thermostat system

$$(m, x, c, T) \longrightarrow_d (m', x', c', T')$$

$(\textbf{off}, 19, 1, 20.5) \longrightarrow_d (\textbf{on}, 19, 2, 21)$??

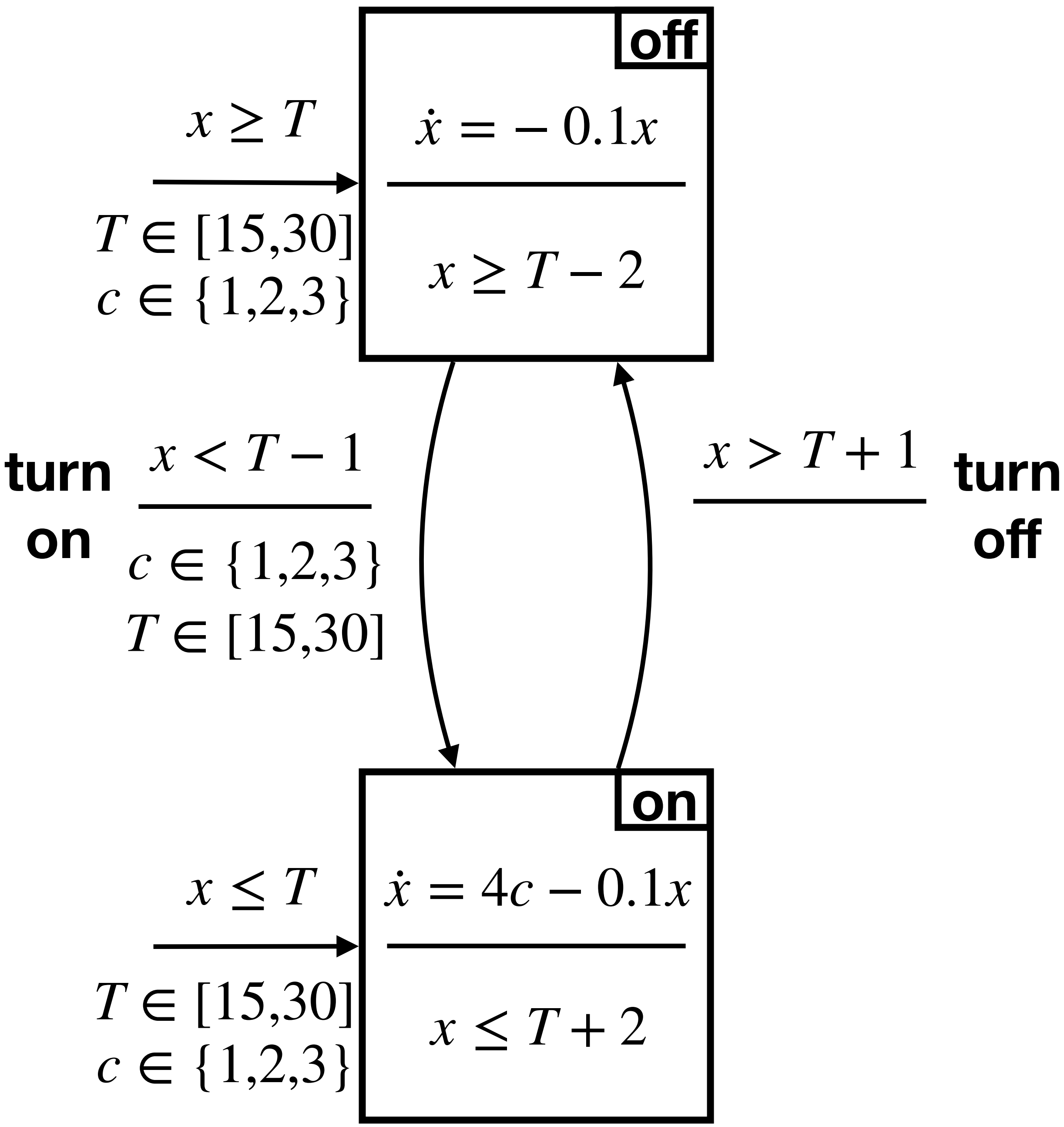
$(\textbf{off}, 19, 1, 20) \longrightarrow_d (\textbf{off}, 19, 2, 21)$??

$(\textbf{off}, 19, 1, 20) \longrightarrow_d (\textbf{on}, 20, 2, 21)$??

$(\textbf{off}, 19, 1, 20) \longrightarrow_d (\textbf{on}, 19, 2, 16)$??

$(\textbf{off}, 20, 1, 20) \longrightarrow_d (\textbf{on}, 20, 2, 21)$??

Example



Thermostat system

$$(m, x, c, T) \longrightarrow_d (m', x', c', T')$$

$(\textbf{off}, 19, 1, 20.5) \longrightarrow_d (\textbf{on}, 19, 2, 21)$	Yes
$(\textbf{off}, 19, 1, 20) \longrightarrow_d (\textbf{off}, 19, 2, 21)$	No
$(\textbf{off}, 19, 1, 20) \longrightarrow_d (\textbf{on}, 20, 2, 21)$	No
$(\textbf{off}, 19, 1, 20) \longrightarrow_d (\textbf{on}, 19, 2, 16)$	No
$(\textbf{off}, 20, 1, 20) \longrightarrow_d (\textbf{on}, 20, 2, 21)$	No

Continuous transitions of HA

Given two valid configurations

$$(m_1, \omega_1) \text{ and } (m_2, \omega_2)$$

we have a **continuous transition**

$$(m_1, \omega_1) \longrightarrow_c (m_2, \omega_2)$$

if the following holds:

- $m_1 = m_2$
- there is a continuous function

  $$\Psi : [0,T] \longrightarrow \mathbb{R}^V \quad (T \geq 0)$$

  derivable on]0,T[such that:
  - ★ $\forall s \in]0,T[\,.\, \dot{\Psi}(s) = F_{m_1}(\Psi(s), s)$
  - ★ $\Psi(0) = \omega_1$ and $\Psi(T) = \omega_2$
  - ★ $\forall s \in [0,T] \,.\, \Psi(s) \in I_{m_1}$

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions

  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function

  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate

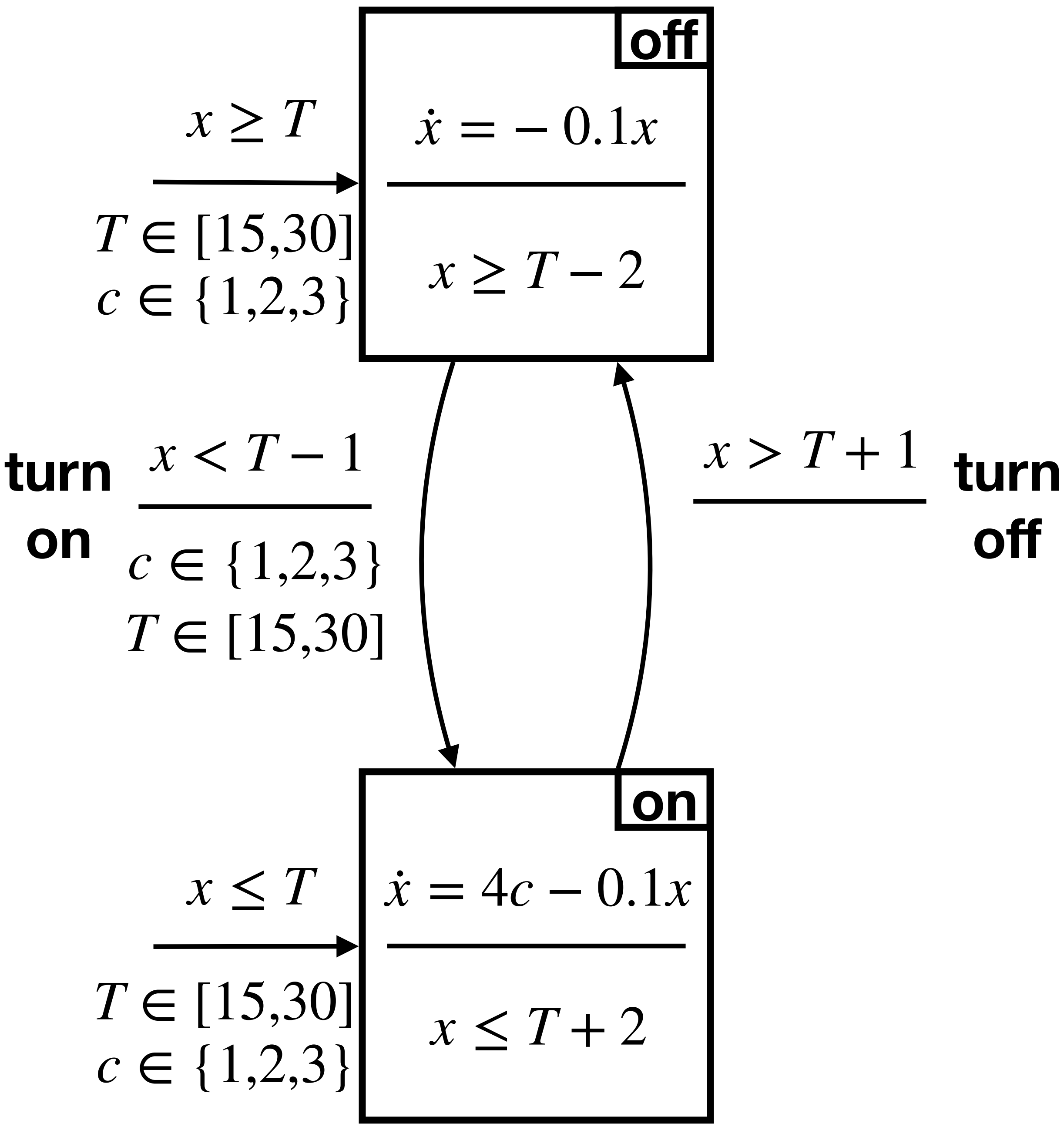
  $$I_m \subseteq \mathbb{R}^V$$
- for every event e, a **guard** predicate

  $$G_e \subseteq \mathbb{R}^V$$
- for every event e, a **jump** relation

  $$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$
- for every mode m, an **initial** predicate

  $$I_{0,m} \subseteq \mathbb{R}^V$$

Example



Thermostat system

$$(m, x, c, T) \longrightarrow_c (m', x', c', T')$$

$(\textbf{off}, 19, 1, 20) \longrightarrow_c (\textbf{off}, 18, 1, 20)$??

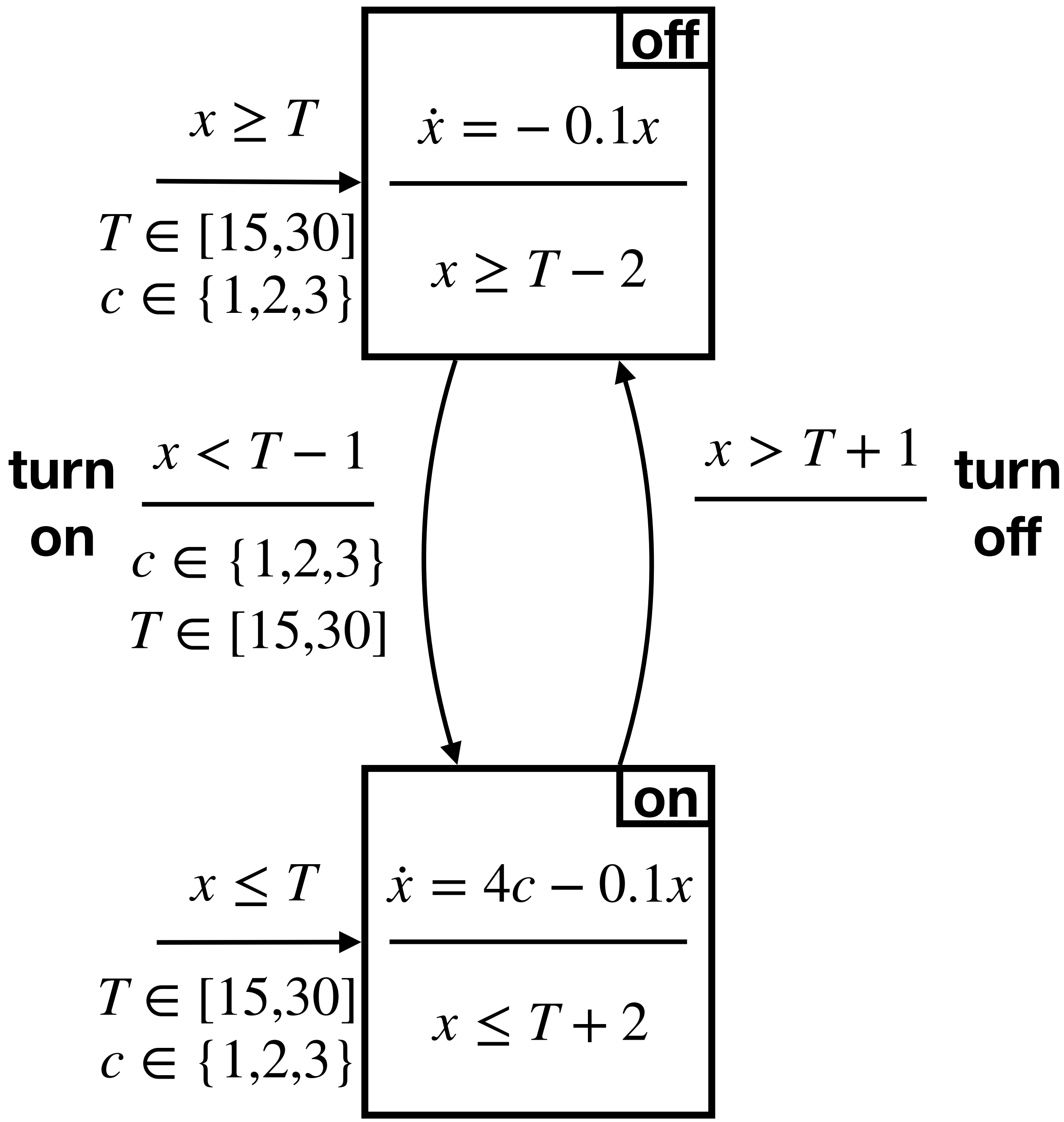
$(\textbf{off}, 19, 1, 20) \longrightarrow_c (\textbf{on}, 18, 1, 20)$??

$(\textbf{off}, 19, 1, 20) \longrightarrow_c (\textbf{off}, 19, 1, 20)$??

$(\textbf{off}, 19, 1, 20) \longrightarrow_c (\textbf{off}, 18, 2, 23)$??

$(\textbf{off}, 19, 1, 20) \longrightarrow_c (\textbf{off}, 20, 1, 20)$??

Example



Thermostat system

$$(m, x, c, T) \longrightarrow_c (m', x', c', T')$$

$(\textbf{off},19,1,20) \longrightarrow_c (\textbf{off},18,1,20)$	Yes
$(\textbf{off},19,1,20) \longrightarrow_c (\textbf{on},18,1,20)$	No
$(\textbf{off},19,1,20) \longrightarrow_c (\textbf{off},19,1,20)$	Yes
$(\textbf{off},19,1,20) \longrightarrow_c (\textbf{off},18,2,23)$	No
$(\textbf{off},19,1,20) \longrightarrow_c (\textbf{off},20,1,20)$	No

Reachability set of HA

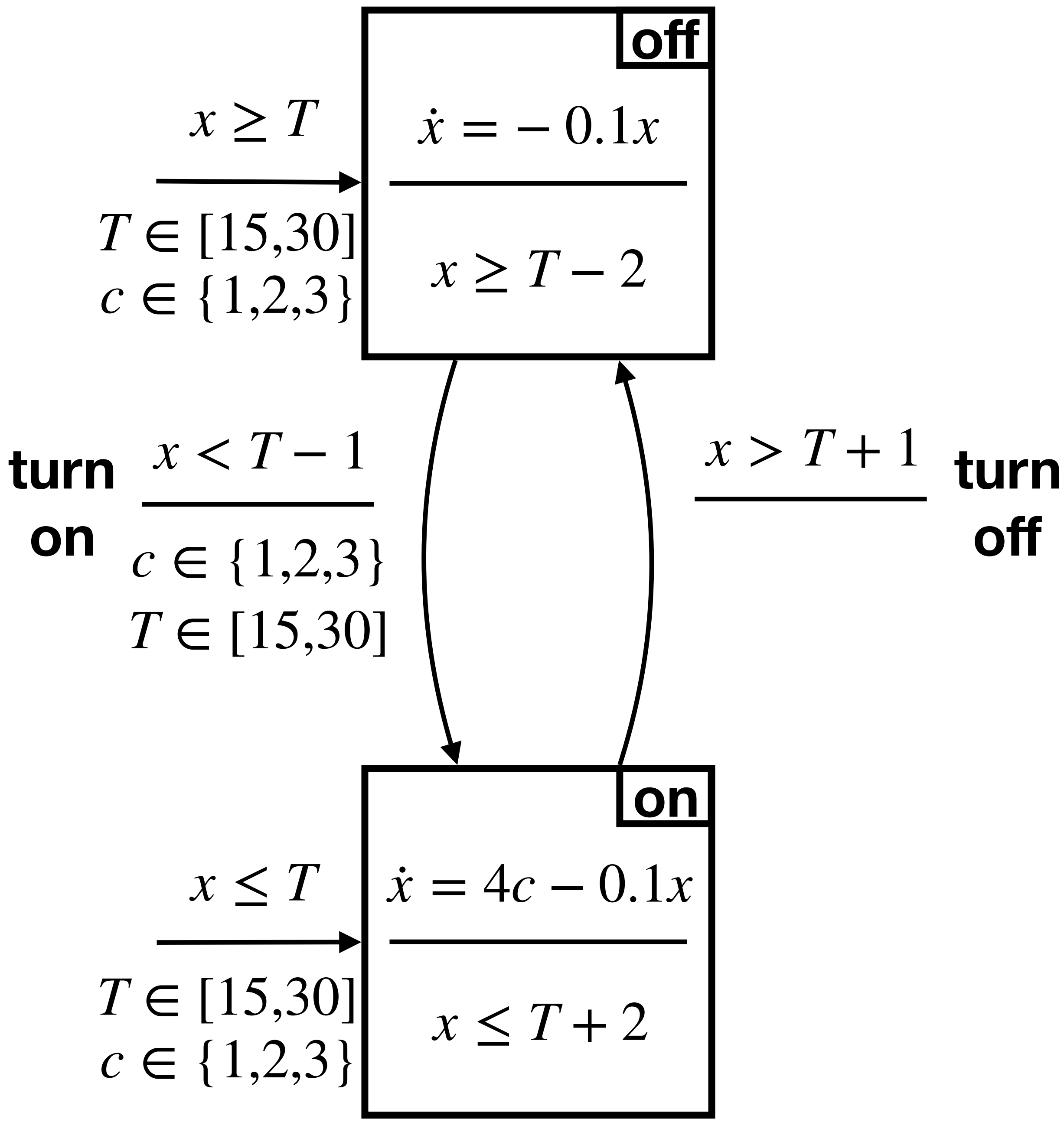
A configuration is **reachable** if there is a finite sequence of continuous and discrete transitions from a valid initial configuration, that is:

$$\textbf{Reach} = \{(m,\omega) \mid \exists m_0 \,.\, \omega_0 \in I_{0,m_0} \cap I_{m_0} \,.\, (m_0,\omega_0)\ (\rightarrow_d \cup \rightarrow_c)^\star\ (m,\omega)\}$$

A **hybrid automaton** is:

- a set M of **modes**
- a set V of **variables**
- a set E of **events**
- **source** and **target** functions
  $$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
  $$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$
- for every mode m, an **invariant** predicate
  $$I_m \subseteq \mathbb{R}^V$$
- for every event e, a **guard** predicate
  $$G_e \subseteq \mathbb{R}^V$$
- for every event e, a **jump** relation
  $$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$
- for every mode m, an **initial** predicate
  $$I_{0,m} \subseteq \mathbb{R}^V$$

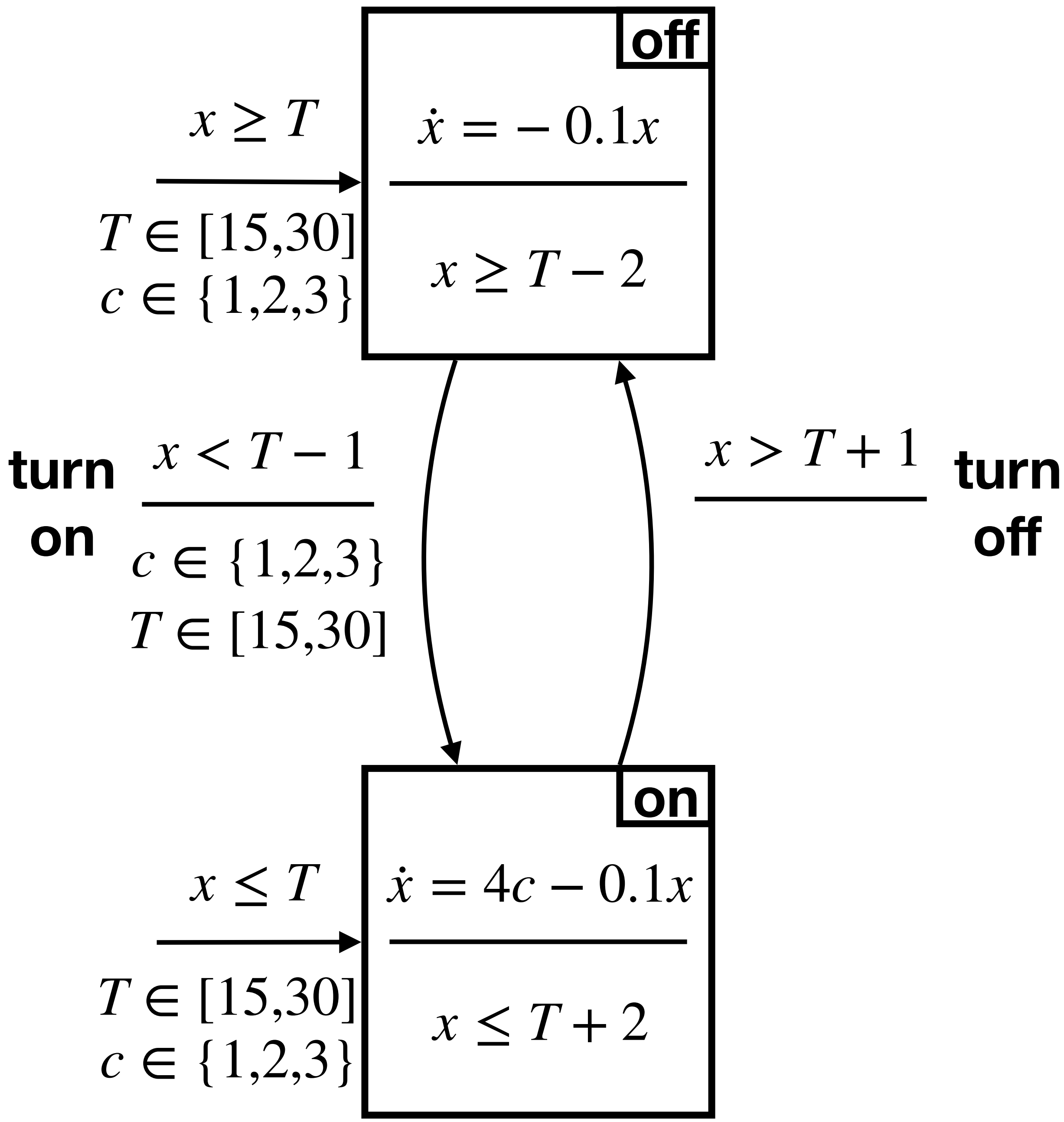
Example



Thermostat system

configuration (m, x, c, T)	**initial**	**valid**	**reachable**
(**off**,$18,1,20$)	No	Yes	
(**off**,$17,2,20$)	No	No	
(**on**,$17,2,20$)	Yes	Yes	
(**on**,$21,1,20$)	No	Yes	

Example



Thermostat system

configuration (m, x, c, T)	initial	valid	reachable
(**off**,18,1,20)	No	Yes	Yes
(**off**,17,2,20)	No	No	No
(**on**,17,2,20)	Yes	Yes	Yes
(**on**,21,1,20)	No	Yes	Yes

Actually, initial $\Rightarrow$ valid = reachable

Representability of functions

In practice, we cannot use any function

$$F_m : \mathbb{R}^V \times \mathbb{R} \longrightarrow \mathbb{R}^V$$

as we need a finite representation of it.

Here, we assume that F_m is given by polynomials on $V \sqcup \{t\}$.

Remark:

This is not much of a restriction, as many dynamics can be modelled by polynomial ones, by adding variables.

Examples:

$$\dot{x} = \frac{f(x,t)}{g(x,t)} \;\Rightarrow\; \text{introduce } \; y = \frac{1}{g(x,t)} \;\Rightarrow\; \dot{x} = f(x,t)\,.\,y, \dot{y} = -\,y^2\,.\left(\frac{\partial g}{\partial x}(x,t)\,.\,f(x,t)\,.\,y + \frac{\partial g}{\partial t}(x,t)\right)$$

$$\dot{x} = cos(x)\,.\,f(x,t) \;\Rightarrow\; \text{introduce} \left|\begin{array}{l} y = cos(x) \\ z = sin(x) \end{array}\right. \;\Rightarrow\; \left|\begin{array}{l} \dot{x} = f(x,t)\,.\,y \\ \dot{y} = -f(x,t)\,.\,y\,.\,z \\ \dot{z} = f(x,t)\,.\,y^2 \end{array}\right.$$

Representability of predicates and relations

In practice, we cannot use any predicate

$$I_m, G_e, I_{0,m} \subseteq \mathbb{R}^V$$

or any relation

$$J_e \subseteq \mathbb{R}^V \times \mathbb{R}^V$$

Here, we assume that there are given by first order formulae of real arithmetic.
Concretely, we assume given a countable set X of variables containing $V \sqcup \widehat{V}$.

$$t, t' ::= X \mid \mathbb{Q} \mid t\,.\,t' \mid t + t' \mid -t \mid t/t'$$
$$\phi, \phi' ::= t \leq t' \mid \top \mid \phi \wedge \phi' \mid \neg\phi \mid \exists x\,.\,\phi$$

<u>Semantics:</u>
Given ϕ whose free variables are **fv**(ϕ)

$$[\![\, \phi \,]\!] \in \mathbb{R}^{\mathbf{fv}(\phi)}$$

<u>Ex:</u> $(r_x, r_y, r_z) \in [\![\, x + y \leq z \,]\!]$ iff $r_x + r_y \leq r_z$

<u>Interest:</u>
Validity and satisfibility of first order real arithmetic are decidable.

For hybrid systems, we assume the existence of such formulae:

$\phi_{I,m}, \phi_{G,e}, \phi_{I,0,m}$ whose free variables are V and

$$[\![\, \phi_{I,m} \,]\!] = I_m, [\![\, \phi_{G,e} \,]\!] = G_e, [\![\, \phi_{I,0,m} \,]\!] = I_{0,m}$$

$\phi_{J,e}$ whose free variables are $V \sqcup \widehat{V}$ and

$$[\![\, \phi_{J,e} \,]\!] = J_e$$

Loop invariants for HA

Remember:

$$\textbf{Reach} = (\to_d \cup \to_c)^\star(\bigcup_{m \in M} I_{0,m} \cap I_m)$$

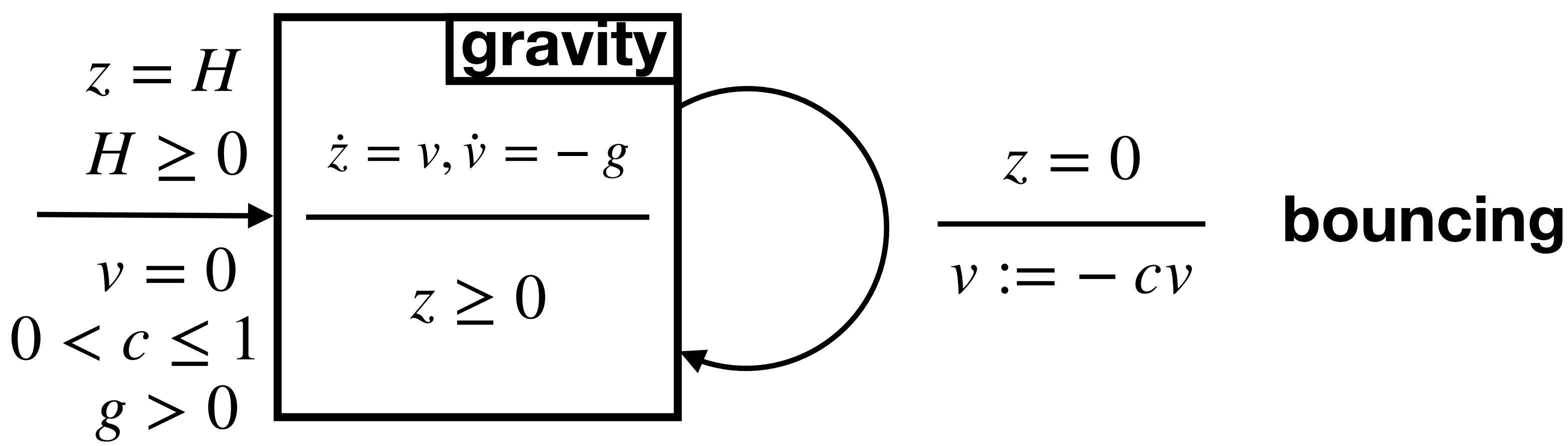
So to prove that every elements of **Reach** satisfies some property, we have to prove some sorts of ***loop invariants***.

To prove **Reach** $\subseteq$ **Prop**, you find **Inv** $\subseteq$ **Prop** such that:

- $\forall m \in M, I_{0,m} \cap I_m \subseteq$ **Inv**
- if $(m, \omega) \in$ **Inv** and $(m, \omega) \to_d (m', \omega')$ then $(m', \omega') \in$ **Inv**
- if $(m, \omega) \in$ **Inv** and $(m, \omega) \to_c (m', \omega')$ then $(m', \omega') \in$ **Inv**

Example: the bouncing ball

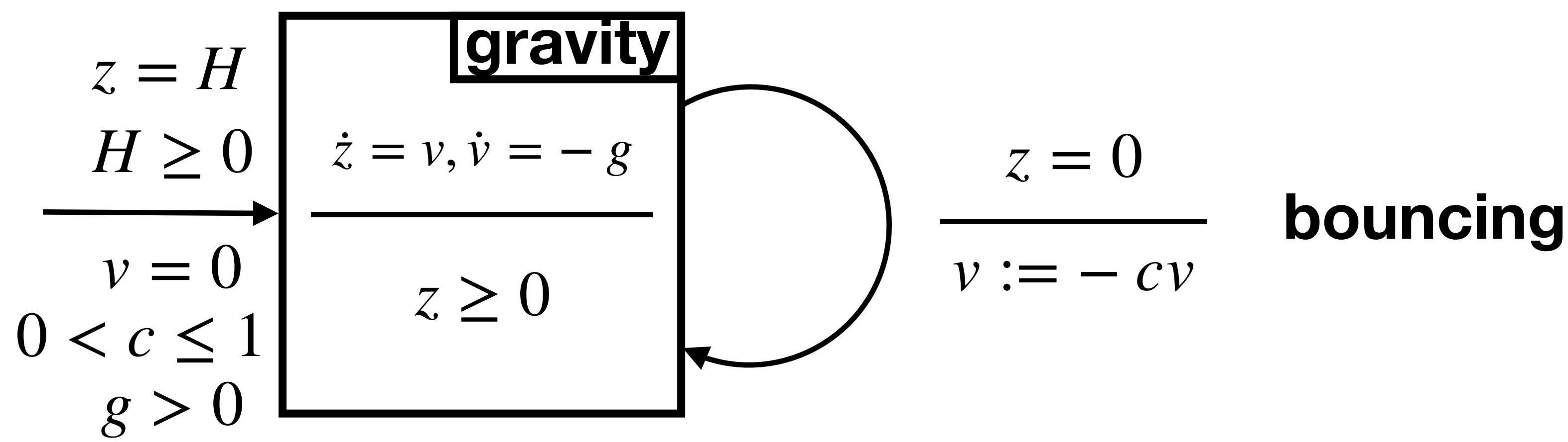
We model a bouncing ball that we drop at height H without initial velocity.



We want to prove that

at every instant, the height of the ball is between 0 and H

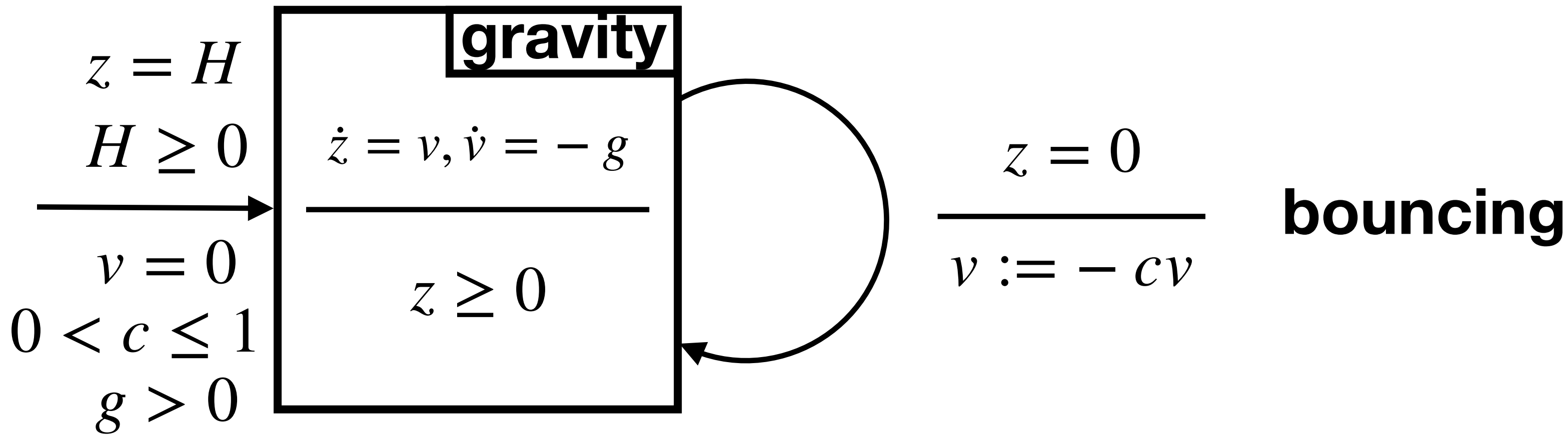
Example: the bouncing ball



We want to prove that
at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.
Can we use **Inv** $=$ **Prop**?

Example: the bouncing ball



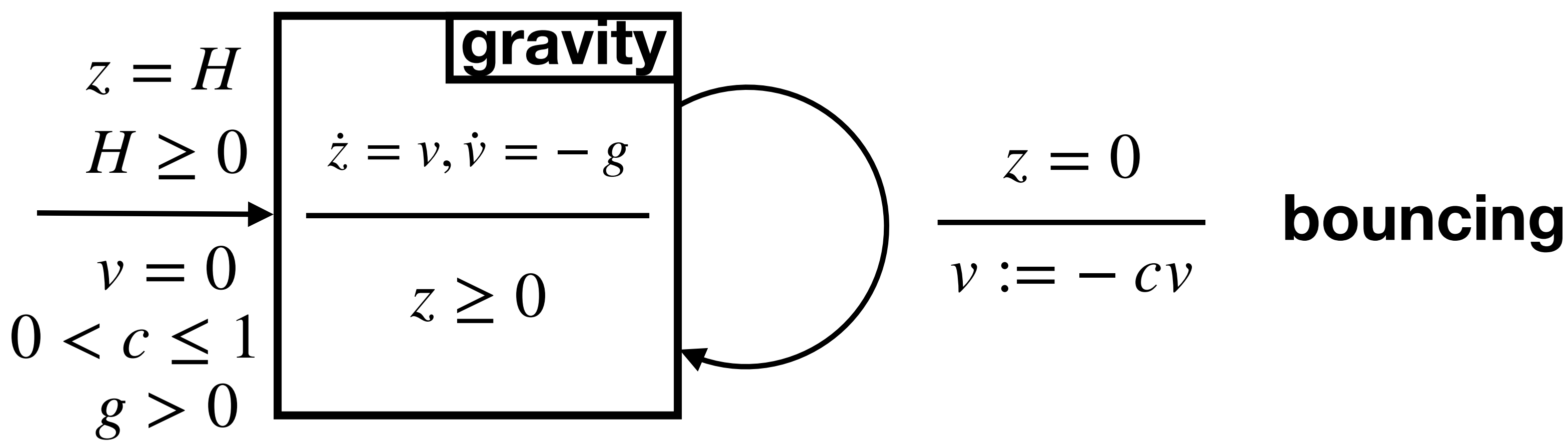
We want to prove that
at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

Can we use **Inv** $=$ **Prop**?

Initially, $z = H$ and $H \geq 0$, so **OK**

Example: the bouncing ball



We want to prove that

at every instant, the height of the ball is between 0 and H

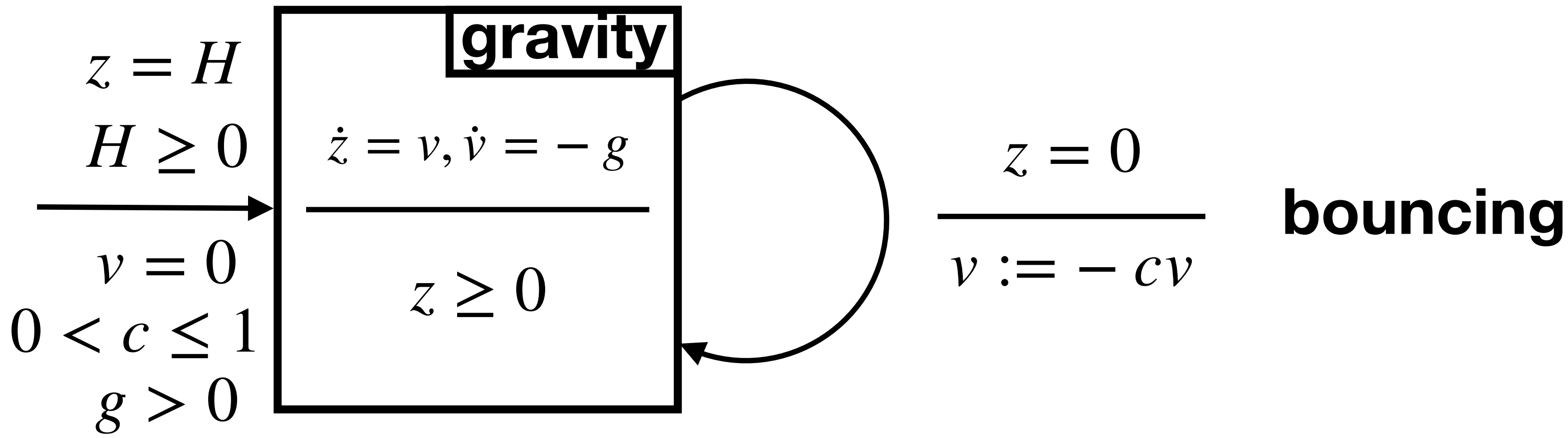
We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

Can we use **Inv** $=$ **Prop**?

Initially, $z = H$ and $H \geq 0$, so **OK**

If (**gravity**, $z, v, H, c, g) \rightarrow_d$ (**gravity**, z', v', H', c', g') then $z = z'$ and $H = H'$, so **OK**

Example: the bouncing ball



We want to prove that

at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

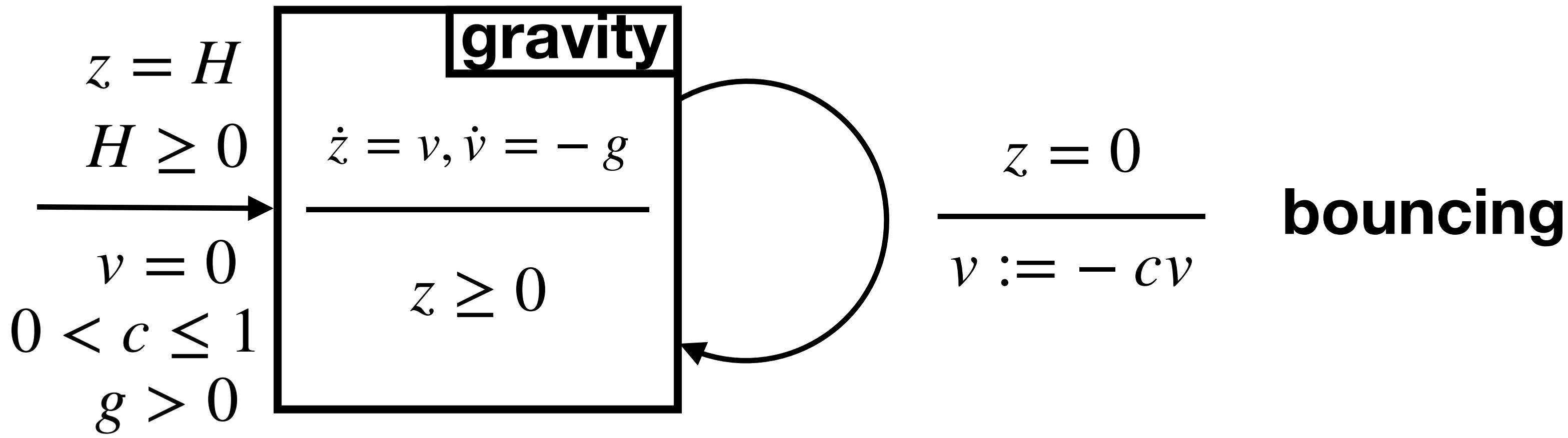
Can we use **Inv** $=$ **Prop**?

Initially, $z = H$ and $H \geq 0$, so **OK**

If (**gravity**, $z, v, H, c, g) \rightarrow_d$ (**gravity**, z', v', H', c', g') then $z = z'$ and $H = H'$, so **OK**

If (**gravity**, $z, v, H, c, g) \rightarrow_c$ (**gravity**, z', v', H', c', g') then, by $I_{\textbf{gravity}}$, $z' \geq 0$.

Example: the bouncing ball



We want to prove that

at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

Can we use **Inv** $=$ **Prop**?

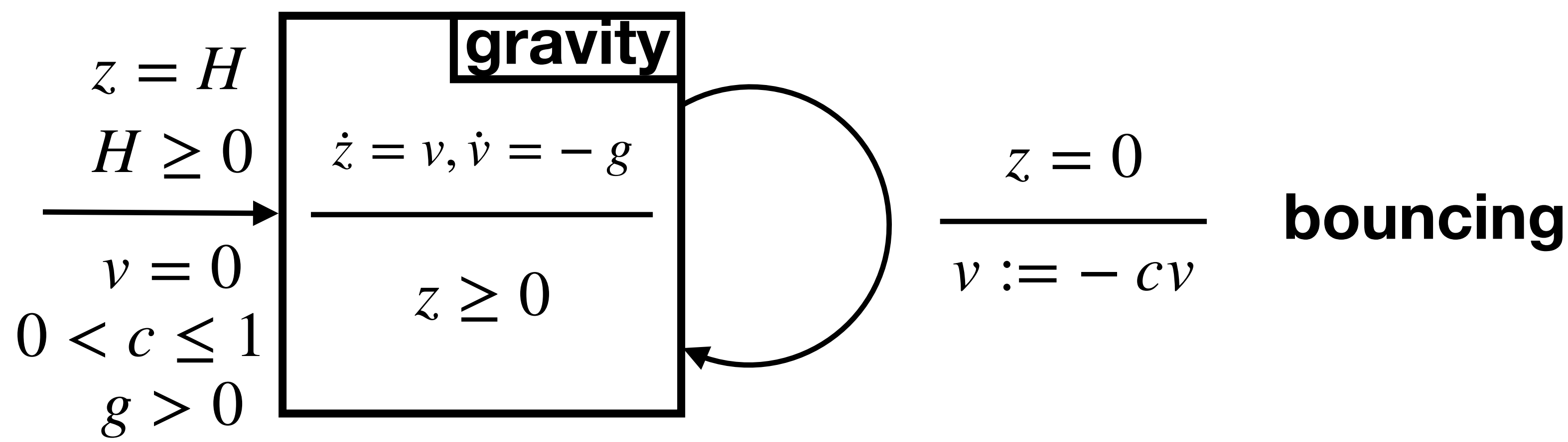
Initially, $z = H$ and $H \geq 0$, so **OK**

If (**gravity**, $z, v, H, c, g) \rightarrow_d$ (**gravity**, $z', v', H', c', g')$ then $z = z'$ and $H = H'$, so **OK**

If (**gravity**, $z, v, H, c, g) \rightarrow_c$ (**gravity**, $z', v', H', c', g')$ then, by $I_{\textbf{gravity}}$, $z' \geq 0$.

Assuming $0 \leq z \leq H$, can we prove $z' \leq H'$?

Example: the bouncing ball



We want to prove that

at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

Can we use **Inv** $=$ **Prop**?

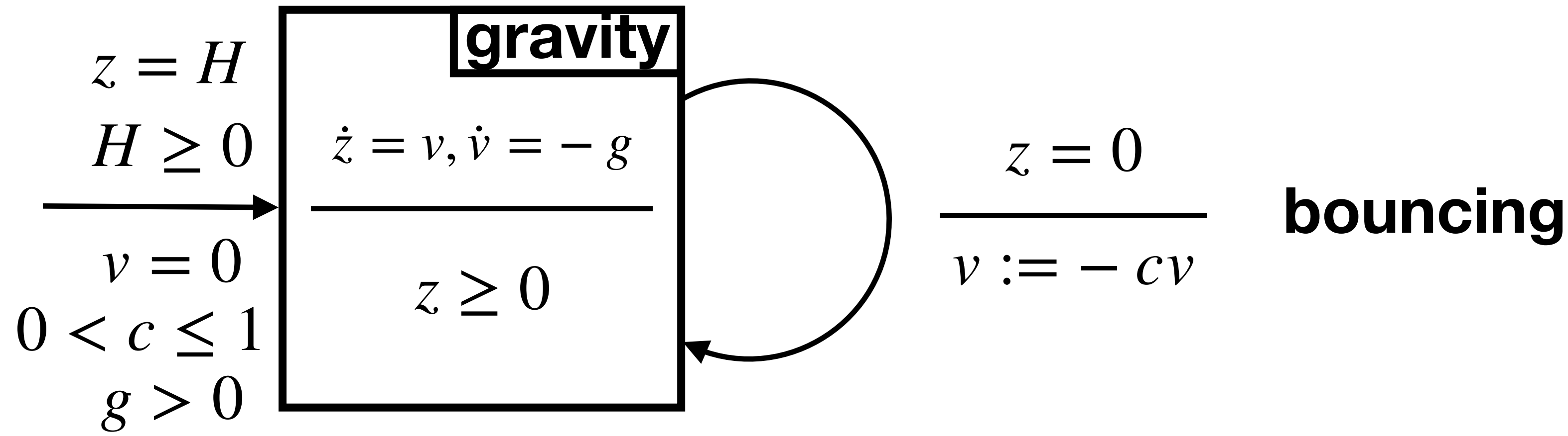
Initially, $z = H$ and $H \geq 0$, so **OK**

If $(\textbf{gravity}, z, v, H, c, g) \rightarrow_d (\textbf{gravity}, z', v', H', c', g')$ then $z = z'$ and $H = H'$, so **OK**

If $(\textbf{gravity}, z, v, H, c, g) \rightarrow_c (\textbf{gravity}, z', v', H', c', g')$ then, by $I_{\textbf{gravity}}$, $z' \geq 0$.

Assuming $0 \leq z \leq H$, can we prove $z' \leq H'$? **No! Take v very large for example.**

Example: the bouncing ball



We want to prove that

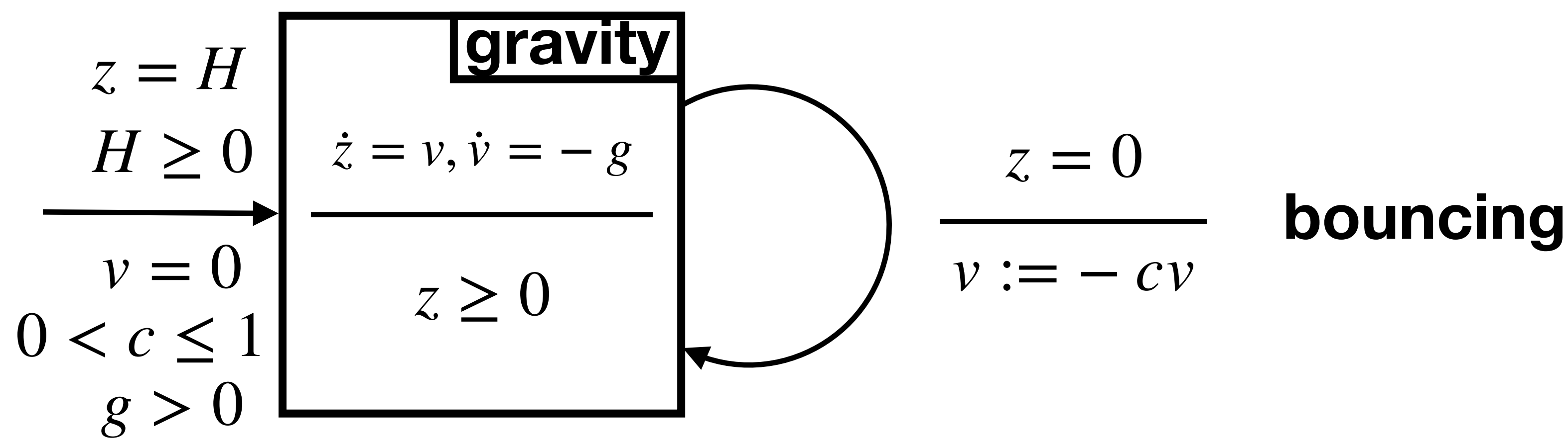
at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

Spoiler: use **Inv** $= \{(z, v, H, c, g) \mid z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2\}$

Initially, $z = H$ and $v = 0$, so **OK**

Example: the bouncing ball



We want to prove that

at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

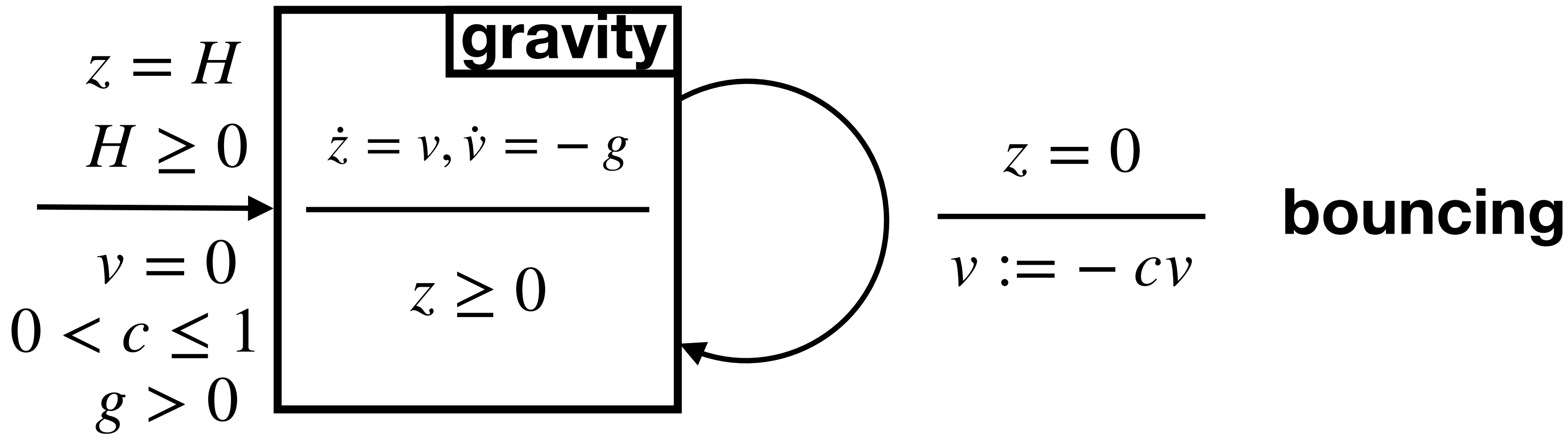
Spoiler: use **Inv** $= \{(z, v, H, c, g) \mid z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2\}$

Initially, $z = H$ and $v = 0$, so **OK**

If (**gravity**, z, v, H, c, g) $\rightarrow_d$ (**gravity**, z', v', H', c', g') and $(z, v, H, c, g) \in$ **Inv** then

$2g'z' = 2gz \leq 2gH - v^2 = 2g'H' - v^2 \leq 2g'H' - c^2v^2 = 2g'H' - v'^2$, so **OK**

Example: the bouncing ball



We want to prove that

at every instant, the height of the ball is between 0 and H

We want **Prop** $= \{(z, v, H, c, g) \mid 0 \leq z \leq H\}$.

Spoiler: use **Inv** $= \{(z, v, H, c, g) \mid z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2\}$

Initially, $z = H$ and $v = 0$, so **OK**

If $($**gravity**$, z, v, H, c, g) \rightarrow_d ($**gravity**$, z', v', H', c', g')$ and $(z, v, H, c, g) \in$ **Inv** then

$2g'z' = 2gz \leq 2gH - v^2 = 2g'H' - v^2 \leq 2g'H' - c^2v^2 = 2g'H' - v'^2$, so **OK**

If $($**gravity**$, z, v, H, c, g) \rightarrow_c ($**gravity**$, z', v', H', c', g')$, then $v' = -gt + v$ and

$z' = -gt^2 + vt + z$ for some t.

After computation: $2g'H' - 2g'z' - v'^2 = 2gH - 2gz - v^2 + g^2t^2$, so **OK**

Objective

- Formalize those kinds of arguments in a Hoare triple/sequent calculus style
- Issues:
  - We need a presentation of HA adapted to this style

    Idea: use Reach $= (\rightarrow_d \cup \rightarrow_c)^\star (\bigcup_{m \in M} I_{0,m} \cap I_m)$

  - $\rightarrow_d$ and $\rightarrow_c$ are semantical objects, so we cannot use them
  - We cannot use closed forms of solutions of differential equations in proofs in general!

Syntax of Hybrid Programs

We assume given a countable set X of variables.

Hybrid Programs are given by the following grammar:

$\alpha, \beta ::= ?\phi$ where ϕ is a first order formula of real arithmetic **(conditional)**

$\mid \mathbf{x} := \mathbf{e}$ where $\mathbf{x}$ (resp. $\mathbf{e}$) is a vector of variables (resp. polynomials) **(assignment)**

$\mid \dot{\mathbf{x}} = \mathbf{e} \ \& \ \phi$ where $\mathbf{x}$ (resp. $\mathbf{e}$) is a vector of variables (resp. polynomials) and ϕ is a first order formula of real arithmetic **(dynamics)**

$\mid \alpha; \beta$ **(sequential composition)**

$\mid \alpha \cup \beta$ **(non-deterministic choice)**

$\mid \alpha^\star$ **(loop)**

Semantics of HP

$[\![\alpha]\!] \subseteq \mathbb{R}^X \times \mathbb{R}^X$ is defined by induction:

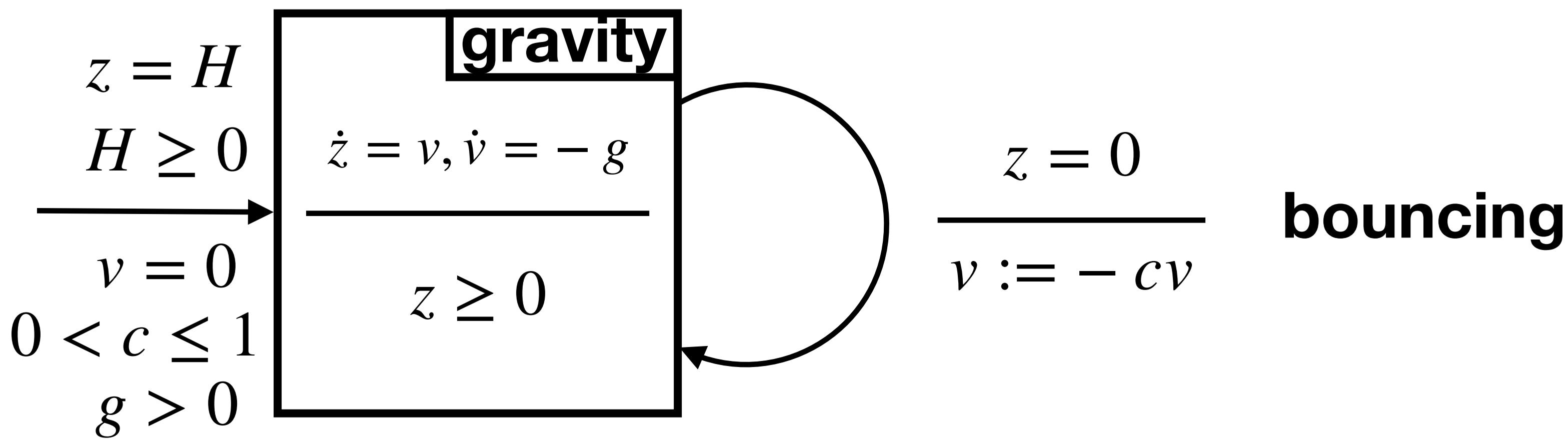
- $[\![?\phi]\!] = \{(\omega,\omega) \mid \omega \in [\![\phi]\!]\}$
- $[\![\mathbf{x} := \mathbf{e}]\!] = \{(\omega,\omega') \mid \forall x \in \mathbf{x}, \omega'_x = e_x(\omega) \wedge \forall x \notin \mathbf{x}, \omega'_x = \omega_x\}$
- $(\omega,\omega') \in [\![\dot{\mathbf{x}} = \mathbf{e} \;\&\; \phi]\!]$ iff there is a continuous function $\psi : [0,T] \to \mathbb{R}^{\mathbf{x}}$ such that:
  - $\omega = \omega(0)$ and $\omega' = \omega(T)$
  - ψ is derivable on $]0,T[$ and for all $t \in]0,T[$, $\dot{\psi}(t) = e(\omega(t))$
  - for all $t \in [0,T], \omega(t) \in [\![\phi]\!]$
- $[\![\alpha;\beta]\!] = \{(\omega,\omega'') \mid \exists\omega', (\omega,\omega') \in [\![\alpha]\!] \wedge (\omega',\omega'') \in [\![\beta]\!]\}$
- $[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- $[\![\alpha^\star]\!] = \{(\omega,\omega') \mid \exists n \in \mathbb{N}, \omega_0, \ldots, \omega_n, \omega = \omega_0 \wedge \omega' = \omega_n \wedge (\omega_i,\omega_{i+1}) \in [\![\alpha]\!]\}$

$\omega(t) \in \mathbb{R}^X$ **denotes:**

- $\forall x \in \mathbf{x}, \omega(t)_x = \psi(t)_x$
- $\forall x \notin \mathbf{x}, \omega(t)_x = \omega_x$

From HA to HP, the example of the bouncing ball

We can describe the bouncing ball as a HP



$$\cong \qquad [\![\alpha]\!] = (\rightarrow_d \cup \rightarrow_c)^\star$$

$$\alpha = (\underbrace{\boxed{(?z = 0; v := -cv)}}_{\rightarrow_d} \cup \underbrace{\boxed{(\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0)}}_{\rightarrow_c})^\star$$

From HA to HP, in general

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

F_m polynomial on $V \sqcup \{t\}$

- for every mode m, an **invariant** predicate

$\phi_{I,m}$ formula on V

- for every event e, a **guard** predicate

$\phi_{G,e}$ formula on V

- for every event e, a **jump** relation

$\phi_{J,e}$ formula on $V \sqcup \widehat{V}$

- for every mode m, an **initial** predicate

$\phi_{I,0,m}$ formula on V

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

F_m polynomial on $V \sqcup \cancel{\{t\}}$

- for every mode m, an **invariant** predicate

$\phi_{I,m}$ formula on V

- for every event e, a **guard** predicate

$\phi_{G,e}$ formula on V

- for every event e, a **jump** relation

$\phi_{J,e}$ formula on $V \sqcup \widehat{V}$

- for every mode m, an **initial** predicate

$\phi_{I,0,m}$ formula on V

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

F_m polynomial on $V \sqcup \cancel{\{t\}}$

- for every mode m, an **invariant** predicate

$\phi_{I,m}$ formula on V

- for every event e, a **guard** predicate

$\phi_{G,e}$ formula on V

- for every event e, a **jump** relation

$\phi_{J,e}$ formula on $V \sqcup \widehat{V}$

of the form $\bigwedge_{x \in V} \widehat{x} = P_x$

where P_x **is a polynomial on** V

- for every mode m, an **initial** predicate

$\phi_{I,0,m}$ formula on V

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

F_m polynomial on $V \sqcup \cancel{\{t\}}$

- for every mode m, an **invariant** predicate

$\phi_{I,m}$ formula on V

- for every event e, a **guard** predicate

$\phi_{G,e}$ formula on V

- for every event e, a **jump** relation

$\phi_{J,e}$ formula on $V \sqcup \widehat{V}$

of the form $\bigwedge_{x \in V} \widehat{x} = P_x$

where P_x is a polynomial on V

- for every mode m, an **initial** predicate

$\phi_{I,0,m}$ formula on V

Assume $V \subseteq X$, and **mode** $\in X \backslash V$

Assume $M \subseteq \mathbb{N}$.

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

$$F_m \text{ polynomial on } V \sqcup \cancel{\{t\}}$$

- for every mode m, an **invariant** predicate

$$\phi_{I,m} \text{ formula on } V$$

- for every event e, a **guard** predicate

$$\phi_{G,e} \text{ formula on V}$$

- for every event e, a **jump** relation

$$\phi_{J,e} \text{ formula on } V \sqcup \widehat{V}$$

of the form $\bigwedge_{x \in V} \widehat{x} = P_x$

where P_x is a polynomial on V

- for every mode m, an **initial** predicate

$$\phi_{I,0,m} \text{ formula on } V$$

Assume $V \subseteq X$, and **mode** $\in X \backslash V$.

Assume $M \subseteq \mathbb{N}$.

$$\Bigg(\bigcup_{m \in M} \Big(?\textbf{mode} = m; \Big(\bigcup_{e \in E | s(e) = m} ?\phi_{G,e} \wedge \phi_{I,m}; \; V := P_V; \; \textbf{mode} := t(e); \; ?\phi_{I,t(e)} \Big) \bigcup \big(\dot{V} = F_m \;\&\; \phi_{I_m}\big) \Big) \Bigg)^\star$$

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

F_m polynomial on $V \sqcup \cancel{\{t\}}$

- for every mode m, an **invariant** predicate

$\phi_{I,m}$ formula on V

- for every event e, a **guard** predicate

$\phi_{G,e}$ formula on V

- for every event e, a **jump** relation

$\phi_{J,e}$ formula on $V \sqcup \widehat{V}$

of the form $\bigwedge_{x \in V} \widehat{x} = P_x$

where P_x **is a polynomial on** V

- for every mode m, an **initial** predicate

$\phi_{I,0,m}$ formula on V

Assume $V \subseteq X$, and **mode** $\in X \backslash V$.

Assume $M \subseteq \mathbb{N}$.

check the mode

$$\Bigg(\bigcup_{m \in M} \Bigg(\boxed{?\textbf{mode} = m;} \Bigg(\bigcup_{e \in E | s(e) = m} ?\phi_{G,e} \wedge \phi_{I,m};\ V := P_V;\ \textbf{mode} := t(e);\ ?\phi_{I,t(e)} \Bigg) \cup \left(\dot{V} = F_m \ \&\ \phi_{I_m} \right) \Bigg) \Bigg)^{\star}$$

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions
$$s, t : E \longrightarrow M$$
- for every mode m, a **flow** function
F_m polynomial on $V \sqcup \cancel{\{t\}}$
- for every mode m, an **invariant** predicate
$\phi_{I,m}$ formula on V
- for every event e, a **guard** predicate
$\phi_{G,e}$ formula on V
- for every event e, a **jump** relation
$\phi_{J,e}$ formula on $V \sqcup \widehat{V}$
of the form $\bigwedge_{x\in V} \widehat{x} = P_x$
where P_x is a polynomial on V
- for every mode m, an **initial** predicate
$\phi_{I,0,m}$ formula on V

Assume $V \subseteq X$, and **mode** $\in X \backslash V$.

Assume $M \subseteq \mathbb{N}$.

either do a discrete transition

$$\Bigg(\bigcup_{m\in M} \Big(?\mathbf{mode} = m; \boxed{\Big(\bigcup_{e\in E|s(e)=m} ?\phi_{G,e} \wedge \phi_{I,m}; \; V := P_V; \; \mathbf{mode} := t(e); \; ?\phi_{I,t(e)} \Big)} \cup \big(\dot{V} = F_m \;\&\; \phi_{I_m} \big) \Big) \Bigg)^\star$$

From HA to HP, in general (simplified version)

A **hybrid automaton** is:

- a finite set M of **modes**
- a finite set V of **variables**
- a finite set E of **events**
- **source** and **target** functions

$$s, t : E \longrightarrow M$$

- for every mode m, a **flow** function

$$F_m \text{ polynomial on } V \sqcup \cancel{\{t\}}$$

- for every mode m, an **invariant** predicate

$$\phi_{I,m} \text{ formula on } V$$

- for every event e, a **guard** predicate

$$\phi_{G,e} \text{ formula on V}$$

- for every event e, a **jump** relation

$$\phi_{J,e} \text{ formula on } V \sqcup \widehat{V}$$

of the form $\bigwedge_{x\in V} \widehat{x} = P_x$

where P_x is a polynomial on V

- for every mode m, an **initial** predicate

$$\phi_{I,0,m} \text{ formula on } V$$

Assume $V \subseteq X$, and **mode** $\in X \backslash V$.

Assume $M \subseteq \mathbb{N}$.

or do a continuous transition

$$\left(\bigcup_{m\in M} \Big(?\textbf{mode} = m; \Big(\bigcup_{e\in E | s(e)=m} ?\phi_{G,e} \wedge \phi_{I,m};\ V := P_V;\ \textbf{mode} := t(e);\ ?\phi_{I,t(e)} \Big) \cup \boxed{\left(\dot{V} = F_m \ \&\ \phi_{I_m}\right)} \Big) \right)^{\star}$$

Sequent/Hoare triple style for HP

$$\left\{ \text{Preconditions} \right\} \quad \text{Execute the system} \quad \left\{ \text{Postconditions} \right\}$$

Sequent/Hoare triple style for HP

$$\left\{ \text{Preconditions} \right\} \quad \text{Execute the system} \quad \left\{ \text{Postconditions} \right\}$$

$$\Gamma$$

A set of first order formulae of real arithmetic

Sequent/Hoare triple style for HP

$\Big\{$ **Preconditions** $\Big\}$ **Execute the system** $\Big\{$ **Postconditions** $\Big\}$

$$\Gamma \qquad\qquad \alpha$$

A set of first order formulae of real arithmetic

A hybrid program

Sequent/Hoare triple style for HP

$$\{\text{Preconditions}\}\quad \text{Execute the system} \quad \{\text{Postconditions}\}$$

$$\Gamma \qquad \alpha \qquad P$$

Γ	α	P
A set of first order formulae of real arithmetic	A hybrid program	A first order formula of real arithmetic

Sequent/Hoare triple style for HP

$$\left\{ \text{Preconditions} \right\} \quad \text{Execute the system} \quad \left\{ \text{Postconditions} \right\}$$

$$\Gamma \vdash [\alpha] \quad P$$

A set of first order formulae of real arithmetic

A hybrid program

A first order formula of real arithmetic

$\boxed{\text{Sequent}}$

A sequent calculus for HP

$$\Gamma \vdash [\alpha]P$$

- Γ a set of first order formulae of real arithmetic
- α a hybrid program
- P a first order formula of real arithmetic

A sequent calculus for HP

$$\Gamma \vdash [\alpha_1]\dots[\alpha_n]P$$

- Γ a set of first order formulae of real arithmetic
- $\alpha_1, \dots, \alpha_n$ hybrid programs
- P a first order formula of real arithmetic

In particular, when $n = 0$ we have a first order sequent of real arithmetic

A sequent $\Gamma \vdash [\alpha_1]\dots[\alpha_n]P$ is said to be **valid** if

$$\{\omega_n \mid \exists \omega_0, \dots \omega_{n-1}, \omega_0 \in \bigcap_{\phi \in \Gamma} [\![\phi]\!] \wedge \forall i, (\omega_{i-1}, \omega_i) \in [\![\alpha_i]\!]\} \subseteq [\![P]\!]$$

<u>Objective of this lecture:</u> prove that $I_{0,\textbf{gravity}} \vdash [\alpha_{ball}]\ 0 \leq z \leq H$ is valid

Deductive system for HP

We will see some **proof rules** to prove validity of sequents:

$$\frac{\Gamma_1 \vdash [\alpha_1^1]\ldots[\alpha_{n_1}^1]\,P_1 \quad \ldots \quad \Gamma_k \vdash [\alpha_1^k]\ldots[\alpha_{n_k}^k]\,P_k}{\Gamma \vdash [\alpha_1]\ldots[\alpha_n]\,P}$$

whose meaning are

To prove that $\Gamma \vdash [\alpha_1]\ldots[\alpha_n]\,P$ ***is valid, it is enough to prove that all*** $\Gamma_i \vdash [\alpha_1^i]\ldots[\alpha_{n_i}^i]\,P_i$ ***are valid.***

Rules that satisfy this property are called **sound**.

Bouncing ball

Notations:

$$I_0 \equiv z = H, H \geq 0, v = 0, 0 < c \leq 1, g > 0$$

$$\textbf{ball} \equiv \Big(\big(?z = 0; v := -cv\big) \cup \big(\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0\big) \Big)^{\star}$$

Sequents to prove:

$$\boxed{I_0 \vdash [\textbf{ball}]\, 0 \leq z \wedge z \leq H}$$

Rule for loop invariants

$$\frac{\Gamma \vdash \textbf{Inv} \quad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \quad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha^\star]\,P}\ \textbf{(LI)}$$

Rule for loop invariants

$$\frac{\Gamma \vdash \textbf{Inv} \quad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \quad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha^\star]\,P} \ \textbf{(LI)}$$

Proof of soundness. Assume that:

1. $\Gamma \vdash$ **Inv** is valid, that is $\cap_{\phi\in\Gamma} [\![\,\phi\,]\!] \subseteq [\![\,\textbf{Inv}\,]\!]$
2. **Inv** $\vdash [\alpha]$ **Inv** is valid, that is $\{\omega' \mid \exists\omega \in [\![\,\textbf{Inv}\,]\!], (\omega,\omega') \in [\![\,\alpha\,]\!]\} \subseteq [\![\,\textbf{Inv}\,]\!]$
3. **Inv** $\vdash P$ is valid, that is, $[\![\,\textbf{Inv}\,]\!] \subseteq [\![\,P\,]\!]$

We want to prove that $\Gamma \vdash [\alpha^\star]\,P$ is valid. Let:

A. $\omega_0 \in \cap_{\phi\in\Gamma} [\![\,\phi\,]\!]$

B. $\omega_1, \ldots, \omega_n$ such that $(\omega_i, \omega_{i+1}) \in [\![\,\alpha\,]\!]$

We want to prove that $\omega_n \in [\![\,P\,]\!]$. By 3., it is enough to prove that $\omega_i \in [\![\,\textbf{Inv}\,]\!]$ by induction on i:

- case $i = 0$: by 1. and A.
- inductive case: assume $\omega_i \in [\![\,\textbf{Inv}\,]\!]$, then by 2. and B., $\omega_{i+1} \in [\![\,\textbf{Inv}\,]\!]$.QED.

Rule for loop invariants

$$\frac{\Gamma \vdash \textbf{Inv} \quad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \quad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha^\star]\,P}\ \textbf{(LI)}$$

To prove the validity of:

$$I_0 \vdash [\textbf{ball}]\ 0 \leq z \leq H$$

it is enough to prove of:

$$I_0 \vdash \textbf{Inv}$$

$$\textbf{Inv} \vdash [\big(?z = 0; v := -cv\big) \cup \big(\dot{z} = v, \dot{v} = -g\ \&\ z \geq 0\big)]\ \textbf{Inv}$$

$$\textbf{Inv} \vdash 0 \leq z \leq H$$

where

$$\textbf{Inv} \equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$$

Bounding ball

Notations:

$I_0 \equiv z = H, H \geq 0, v = 0, 0 < c \leq 1, g > 0$
Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$\boxed{I_0 \vdash \textbf{Inv}}$
Inv $\vdash [\left(?z = 0; v := -cv\right) \cup \left(\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0\right)]$ **Inv**
$\boxed{\textbf{Inv} \vdash 0 \leq z \leq H}$

Rule for real arithmetic

$$\frac{\bigcap_{\phi \in \Gamma} [\![\phi]\!] \subseteq [\![P]\!]}{\Gamma \vdash P} \ \textbf{(RA)}$$

This is implementable since the first order theory of reals is decidable!

To prove the validity of:

$$I_0 \vdash \textbf{Inv}$$

$$\textbf{Inv} \vdash 0 \leq z \leq H$$

it is enough the following inclusions:

$$\{(z, v, H, g, c) \mid z = H \wedge H \geq 0 \wedge v = 0 \wedge 0 < c \leq 1 \wedge g > 0\}$$

$$\subseteq$$

$$\{(z, v, H, g, c) \mid z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2\}$$

$$\{(z, v, H, g, c) \mid z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2\} \subseteq \{(z, v, H, g, c) \mid 0 \leq z \leq H\}$$

Bouncing ball

Notations:

Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$\boxed{\textbf{Inv} \vdash [\big(?z = 0; v := -cv\big) \cup \big(\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0\big)]\ \textbf{Inv}}$

Rule for non-deterministic choices

$$\frac{\Gamma \vdash [\alpha]P \quad \Gamma \vdash [\beta]P}{\Gamma \vdash [\alpha \cup \beta]P} \; (\cup)$$

To prove the validity of:

$$\textbf{Inv} \vdash [\left(?z = 0; v := -cv\right) \cup \left(\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0\right)] \; \textbf{Inv}$$

it is enough to prove the validity of :

$$\textbf{Inv} \vdash [?z = 0; v := -cv] \; \textbf{Inv}$$

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0] \; \textbf{Inv}$$

Bouncing ball

Notations:

$$\textbf{Inv} \equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$$

Sequents to prove:

$$\boxed{\textbf{Inv} \vdash [?z = 0; v := -cv]\ \textbf{Inv}}$$

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g\ \&\ z \geq 0]\ \textbf{Inv}$$

Rule for sequential compositions

$$\frac{\Gamma \vdash [\alpha][\beta]P}{\Gamma \vdash [\alpha;\beta]P} \quad \textbf{(;)}$$

To prove the validity of:

$$\textbf{Inv} \vdash [?z = 0; v := -cv] \ \textbf{Inv}$$

it is enough to prove the validity of :

$$\textbf{Inv} \vdash [?z = 0][v := -cv] \ \textbf{Inv}$$

Bouncing ball

Notations:

Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$\boxed{\textbf{Inv} \vdash [?z = 0][v := -cv]\ \textbf{Inv}}$

Inv $\vdash [\dot{z} = v, \dot{v} = -g\ \&\ z \geq 0]$ **Inv**

Rule for conditionals

$$\frac{\Gamma, Q \vdash P}{\Gamma \vdash [?Q]P} \; \textbf{(?)}$$

To prove the validity of:

$$\textbf{Inv} \vdash [?z = 0][v := -cv] \; \textbf{Inv}$$

it is enough to prove the validity of :

$$\textbf{Inv}, z = 0 \vdash [v := -cv] \; \textbf{Inv}$$

Bouncing ball

Notations:

Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$\boxed{\textbf{Inv}, z = 0 \vdash [v := -cv]\ \textbf{Inv}}$

Inv $\vdash [\dot{z} = v, \dot{v} = -g \ \&\ z \geq 0]$ **Inv**

Rule for conditionals

$$\frac{\Gamma \vdash P(\mathbf{x} \leftarrow \mathbf{e})}{\Gamma \vdash [\mathbf{x} := \mathbf{e}]P} \quad \textbf{(:=)}$$

To prove the validity of:

$$\textbf{Inv}, z = 0 \vdash [v := -cv] \ \textbf{Inv}$$

it is enough to prove the validity of :

$$\textbf{Inv}, z = 0 \vdash z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - (-cv)^2$$

which can be proved using the **(RA)** rule.

Bouncing ball

Notations:

Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$\boxed{\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ \textbf{Inv}}$

Rule for simplifying the postconditions

$$\frac{\Gamma \vdash [\alpha]P \quad \Gamma \vdash [\alpha]Q}{\Gamma \vdash [\alpha]P \wedge Q} \; \textbf{([]}_{\wedge}\textbf{)}$$

To prove the validity of:

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0] \; \textbf{Inv}$$

it is enough to prove the validity of :

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0] \; z \geq 0$$

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0] \; 0 < c \leq 1 \wedge g > 0$$

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \;\&\; z \geq 0] \; 2gz \leq 2gH - v^2$$

Bouncing ball

Notations:

Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$\boxed{\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ z \geq 0}$

Inv $\vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ 0 < c \leq 1 \wedge g > 0$

Inv $\vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ 2gz \leq 2gH - v^2$

Rule for differential weakening

$$\frac{Q \vdash P}{\Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \ \& \ Q]P} \quad \textbf{(dW)}$$

To prove the validity of:

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ z \geq 0$$

it is enough to prove the validity of :

$$z \geq 0 \vdash z \geq 0$$

which is obvious.

Bouncing ball

Notations:

Inv $\equiv z \geq 0 \wedge 0 < c \leq 1 \wedge g > 0 \wedge 2gz \leq 2gH - v^2$

Sequents to prove:

$$\boxed{\begin{array}{l}\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0]\ 0 < c \leq 1 \wedge g > 0 \\ \textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0]\ 2gz \leq 2gH - v^2\end{array}}$$

Rule for constant properties

$$\frac{\Gamma \vdash P \quad \mathbf{fv}(P) \cap \mathbf{x} = \emptyset}{\Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \ \& \ Q]P} \ \textbf{(cst)}$$

To prove the validity of:

$$\mathbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ 0 < c \leq 1 \wedge g > 0$$

it is enough to prove the validity of :

$$\mathbf{Inv} \vdash 0 < c \leq 1 \wedge g > 0$$

which is obvious.

What about $\mathbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ 2gz \leq 2gH - v^2$?

Invariant of a dynamics, and Lie derivative

$$\dot{\mathbf{x}} = \mathbf{e} \;\&\; Q \quad \simeq \quad \big(?Q; \mathbf{x} := \mathbf{x} + dt\,.\,\mathbf{e}\big)^{\star}; ?Q$$

$$\frac{\Gamma, Q \vdash \mathbf{Inv} \qquad \mathbf{Inv}, Q \vdash \mathbf{Inv}(\mathbf{x} \leftarrow \mathbf{x} + dt\,.\,\mathbf{e}) \qquad \mathbf{Inv} \vdash P}{\Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \;\&\; Q]P} \; \textbf{(dtI)}$$

Assume that $P = \mathbf{Inv} \equiv f \geq 0$. We want something to ensure:

$$f(\omega) \geq 0 \Rightarrow f(\omega + dt\,.\,\mathbf{e}(\omega)) \geq 0$$

It is enough to require that f is constant along the dynamics, that is, if ψ is a solution of $\dot{\mathbf{x}} = \mathbf{e}$, then $K : t \mapsto f(\psi(t))$ is constant, that is, its derivative is zero.

$$\dot{K}(t) = \sum_{x \in \mathbf{X}} \frac{\partial f}{\partial x}(\psi(t))\,.\,\dot{\psi}(t) = \sum_{x \in \mathbf{X}} \frac{\partial f}{\partial x}(\psi(t))\,.\,\mathbf{e}_x(\psi(t))$$

So it is enough that the function $\mathscr{L}_{\mathbf{e}} f = \sum_{x \in \mathbf{X}} \frac{\partial f}{\partial x}\,.\,\mathbf{e}_x$ to be zero along the dynamics.

Rule for differential invariants

$$\frac{\Gamma, Q \vdash f \geq 0 \quad \Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \ \& \ Q]\mathscr{L}_{\mathbf{e}} f = 0}{\Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \ \& \ Q] f \geq 0} \ \textbf{(dI)}$$

To prove the validity of:

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ 2gz \leq 2gH - v^2$$

it is enough to prove the validity of :

$$\textbf{Inv}, z \geq 0 \vdash 2gz \leq 2gH - v^2$$

which is obvious and of:

$$\textbf{Inv} \vdash [\dot{z} = v, \dot{v} = -g \ \& \ z \geq 0] \ \mathscr{L}_{\mathbf{e}} f = 0$$

which is true after computation of the Lie derivative.

Bouncing ball

Notations:

Sequents to prove:

No more!

Keymaera X

https://web.keymaerax.org