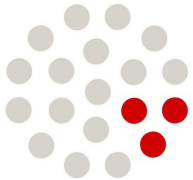
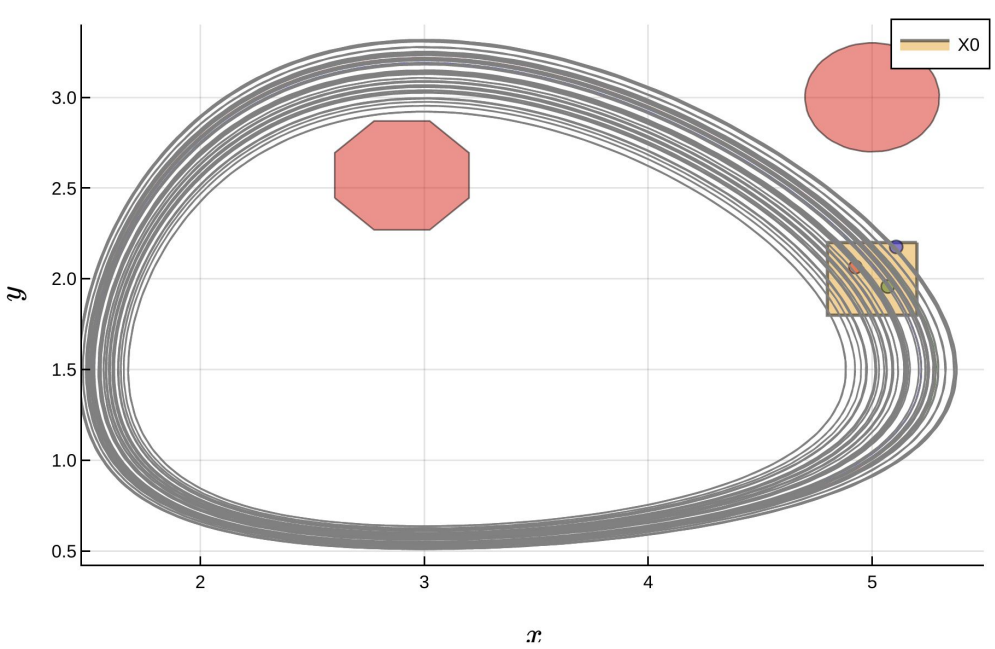


Verificación formal de sistemas controlados por reloj

Marcelo Forets, CURE, UdelaR
Daniel Freire, IFFC, UdelaR
Christian Schilling, IST Austria, Austria

arXiv: https://arxiv.org/abs/2006.12325

Parte 1: El problema de verificación

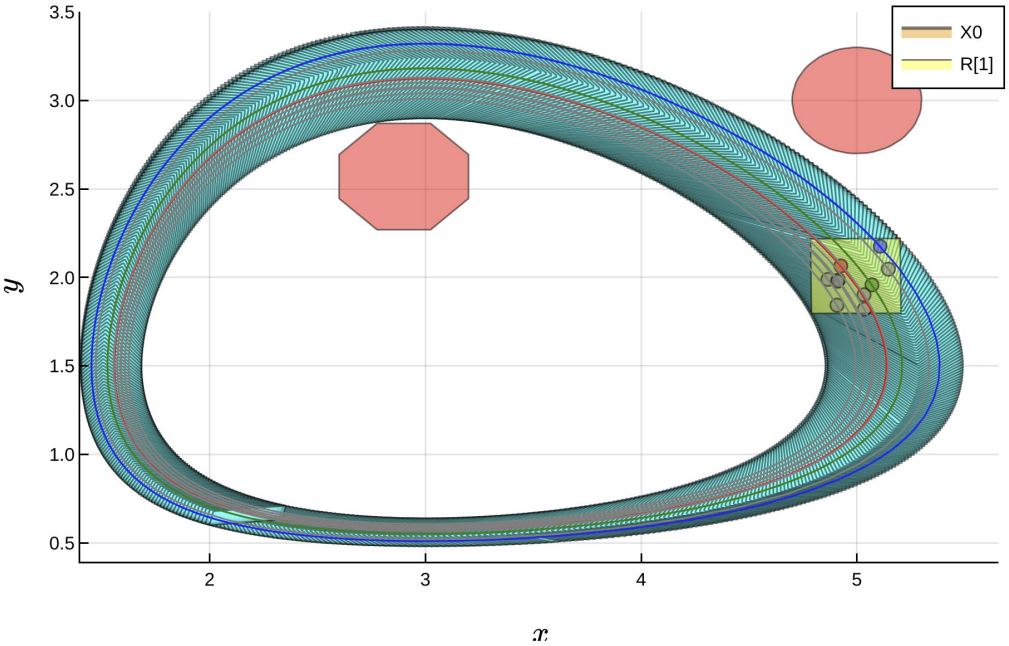


$$x'(t) = f(x(t), u(t), p(t))$$

Seminarios de grupo (http://fisicanolineal.fisica.edu.uy/?page_id=55)

10/09/2020: Verificación formal de sistemas controlados por reloj [Parte 1] (Dr. Daniel Freire, Dr. Marcelo Forets) (presentación)

Parte 1: El problema de verificación



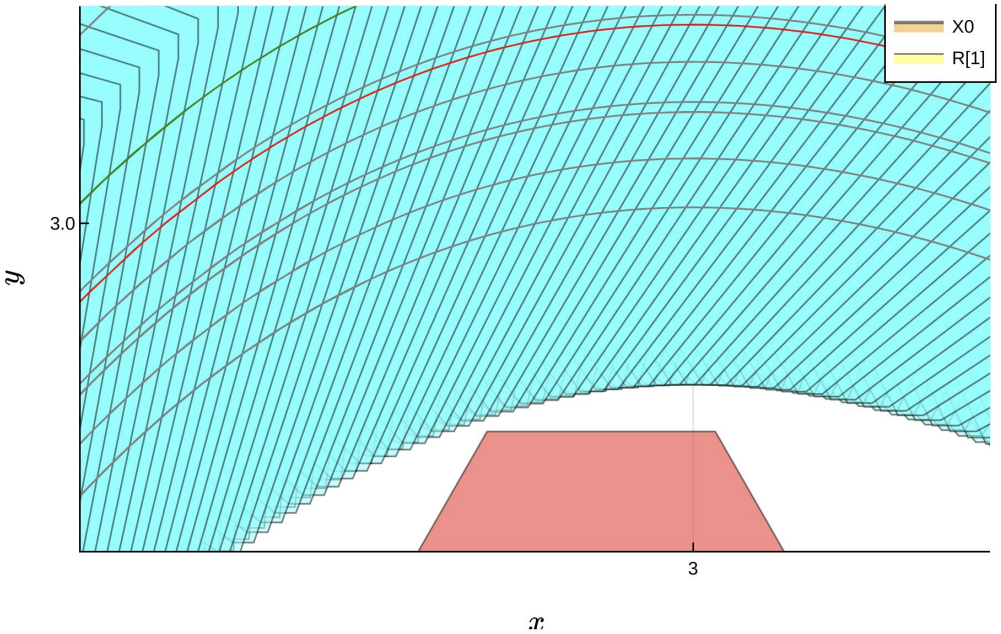
$$x'(t) = f(x(t), u(t), p(t))$$

Si el conjunto de estados alcanzables **no** se intersecta con los estados “malos”, el sistema se dice seguro.

Seminarios de grupo (http://fisicanolineal.fisica.edu.uy/?page_id=55)

10/09/2020: Verificación formal de sistemas controlados por reloj [Parte 1] (Dr. Daniel Freire, Dr. Marcelo Forets) (presentación)

Parte 1: El problema de verificación



$$x'(t) = f(x(t), u(t), p(t))$$

El método de *reachability analysis* es exhaustivo (cubre todos los comportamientos admitidos) y riguroso (en sentido matemático, incluyendo robustez numérica respecto a errores de punto flotante).

Seminarios de grupo (http://fisicanolineal.fisica.edu.uy/?page_id=55)
10/09/2020: Verificación formal de sistemas controlados por reloj [Parte 1] (Dr. Daniel Freire, Dr. Marcelo Forets) (presentación)

Parte 2:

Sistemas híbridos

Cornell University

We gratefully acknowledge support from the Simons Foundation and member institutions.

arXiv.org > eess > arXiv:2006.12325

Search... All fields Search

Help | Advanced Search

Electrical Engineering and Systems Science > Systems and Control

[Submitted on 22 Jun 2020]

Efficient reachability analysis of parametric linear hybrid systems with time-triggered transitions

Marcelo Forets, Daniel Freire, Christian Schilling

Download:

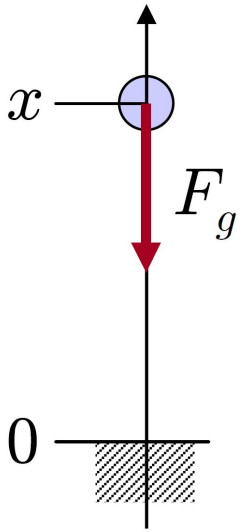
- PDF
- Other formats

(license)

Current browse context:
eess.SY

< prev | next >

Ejemplo: bouncing ball

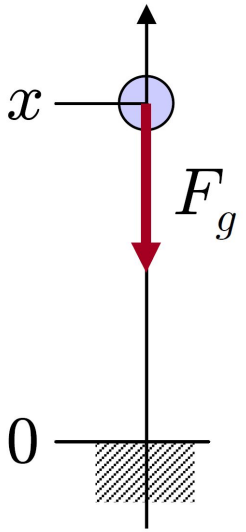


$$
\begin{aligned}
F_g &= -mg \\
m\ddot{x} &= F_g
\end{aligned}
$$

$$
\begin{aligned}
\dot{x} &= v \\
\dot{v} &= -g
\end{aligned}
$$

$$
\frac{d}{dt}\begin{bmatrix} x \\ v \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ v \end{bmatrix} + \begin{bmatrix} 0 \\ -g \end{bmatrix}
$$

Ejemplo: bouncing ball



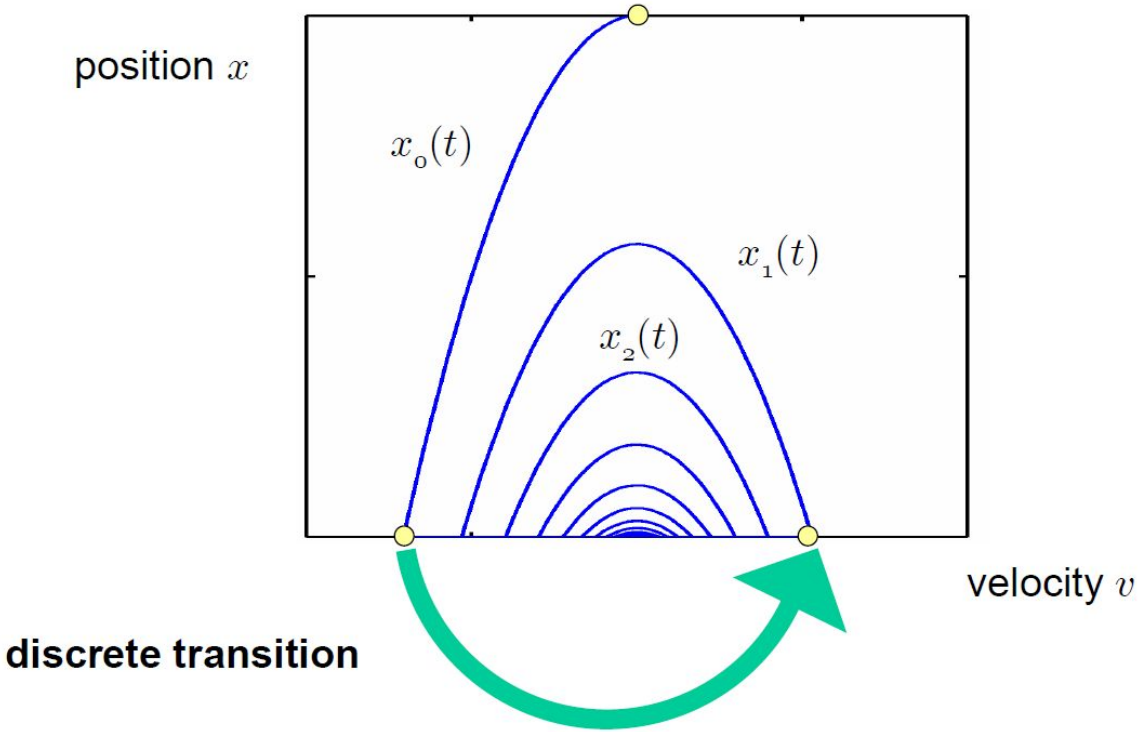
$$\begin{aligned} F_g &= -mg \\ m\ddot{x} &= F_g \end{aligned}$$

$$v := -cv,\ 0 \leq c \leq 1$$

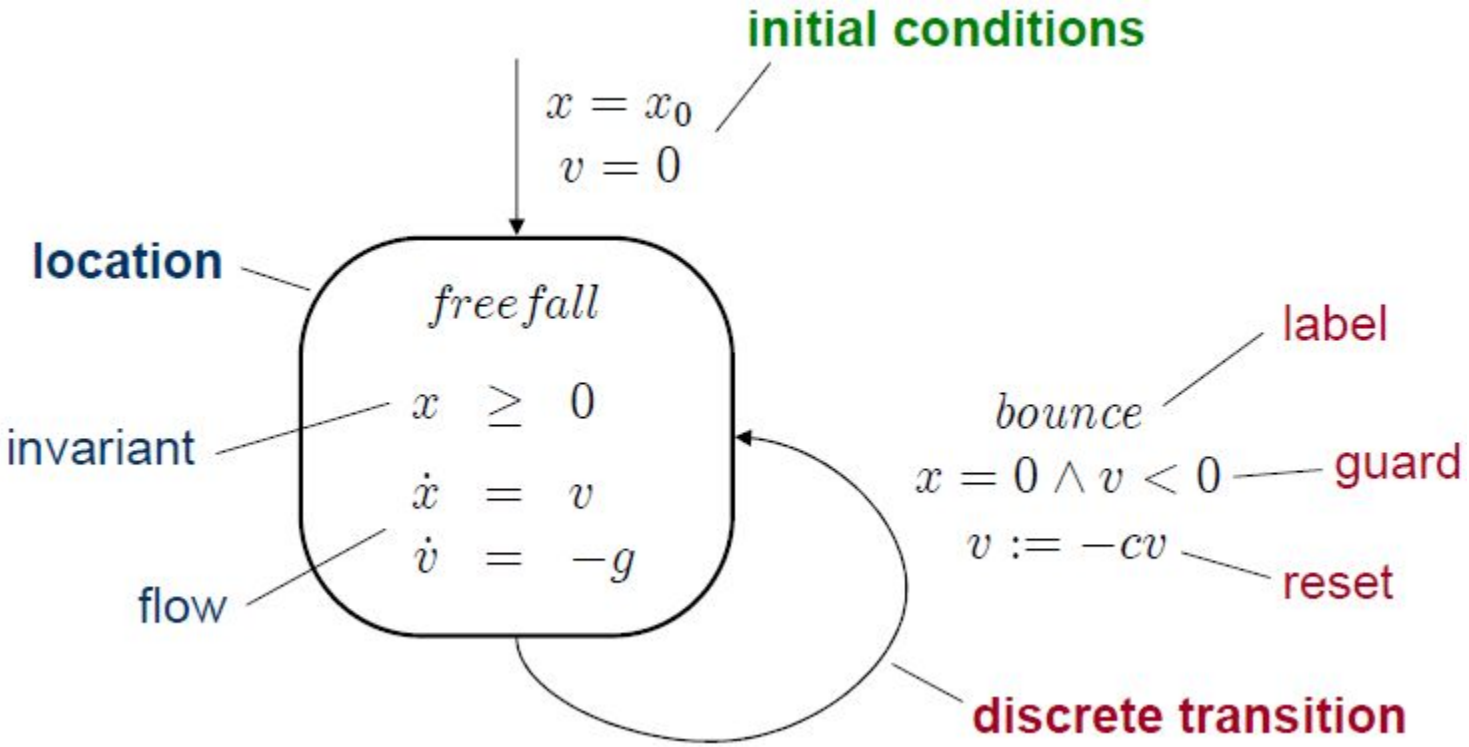
$$\begin{aligned} \dot{x} &= v \\ \dot{v} &= -g \end{aligned}$$

$$\frac{d}{dt}\begin{bmatrix} x \\ v \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ v \end{bmatrix} + \begin{bmatrix} 0 \\ -g \end{bmatrix}$$

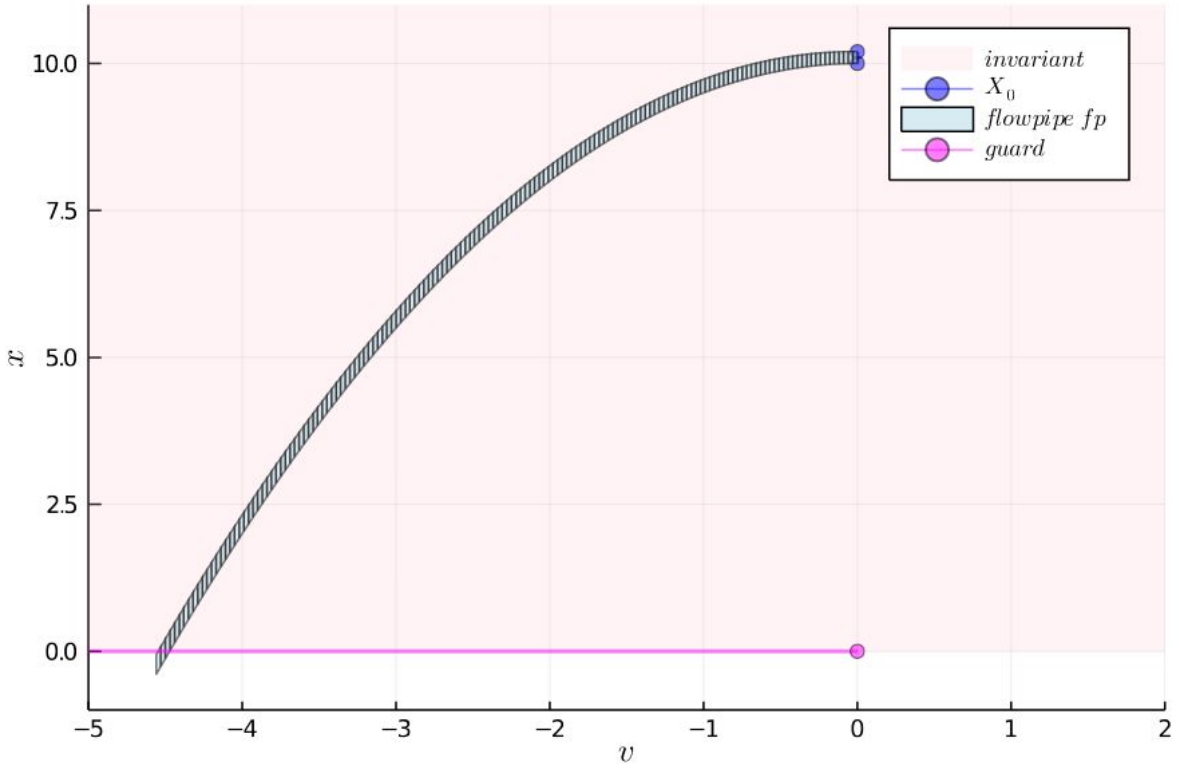
Modelo de autómata híbrido



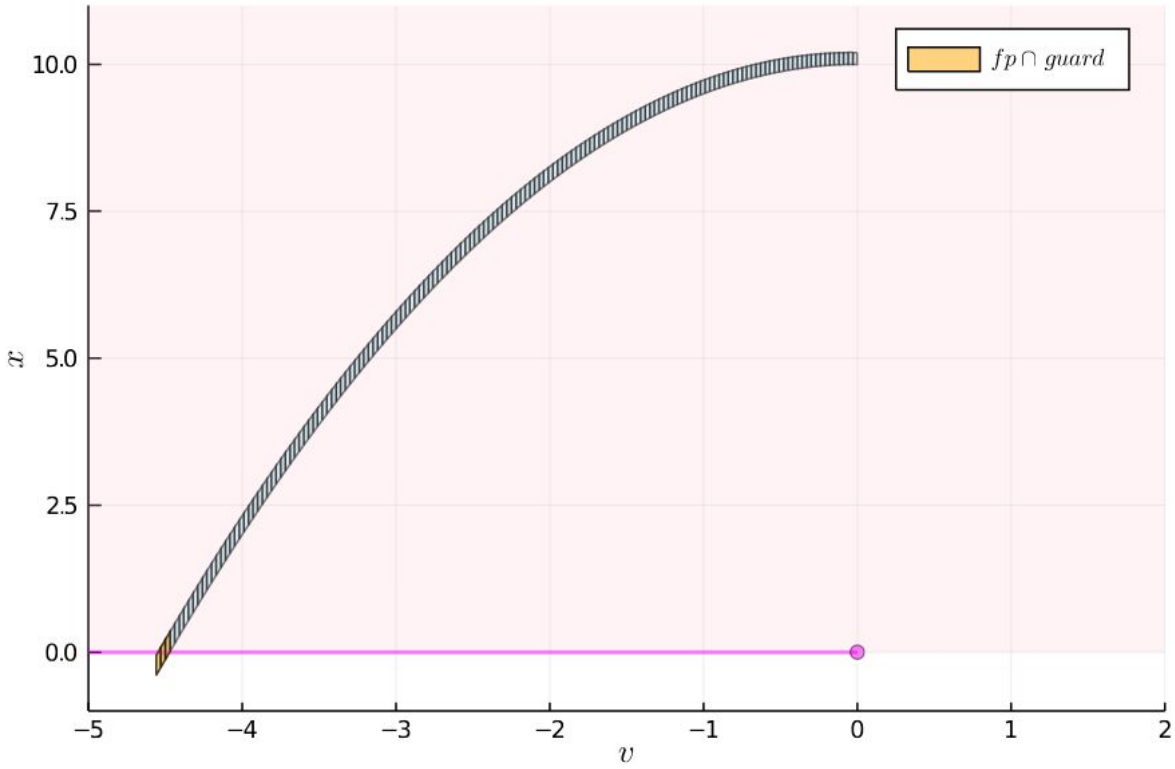
Modelo de autómata híbrido



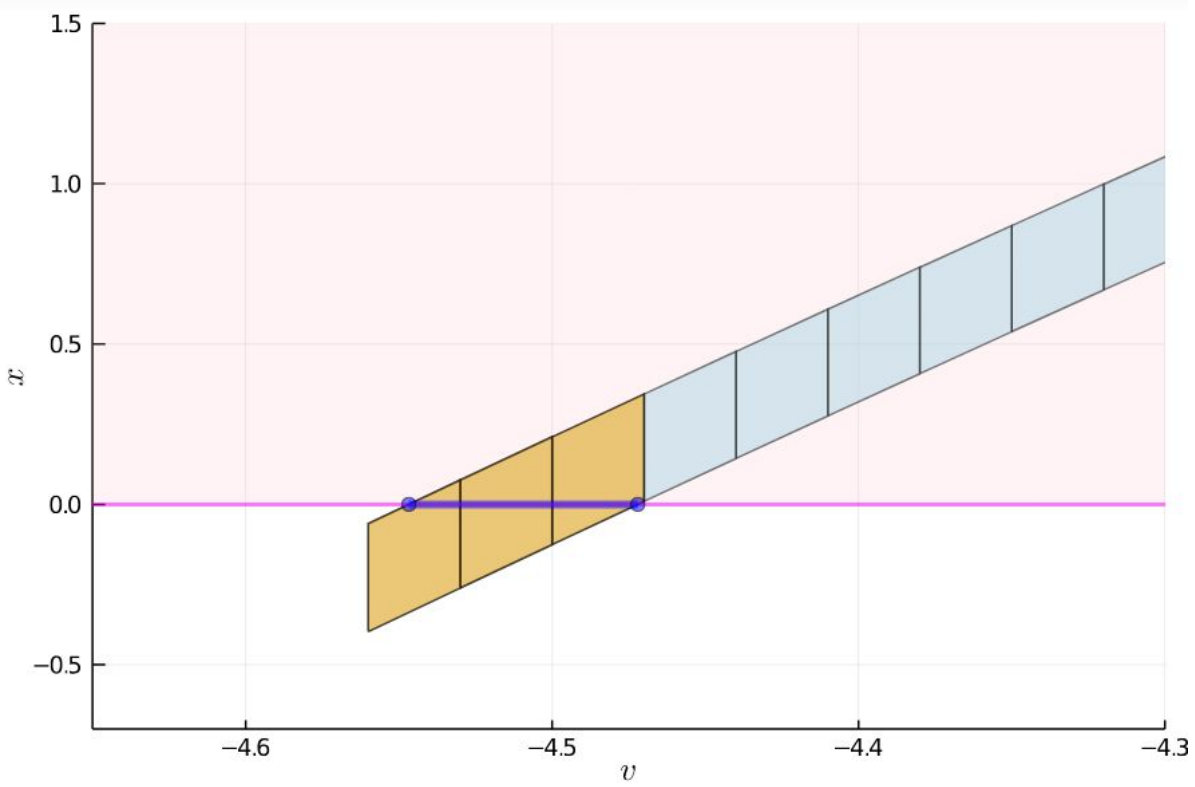
Ejemplo: bouncing ball (*c=0.75, x(0)=10±0.1, v(0)=0*)



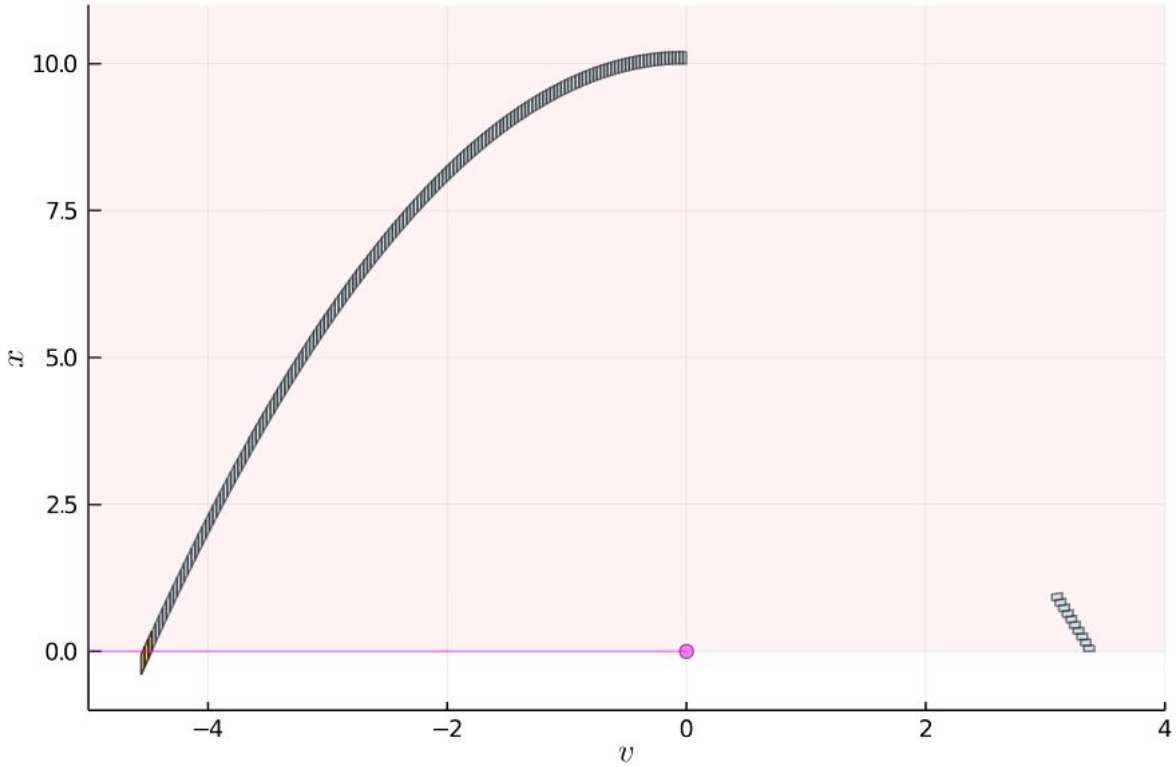
Ejemplo: bouncing ball (*c=0.75, x(0)=10±0.1, v(0)=0*)



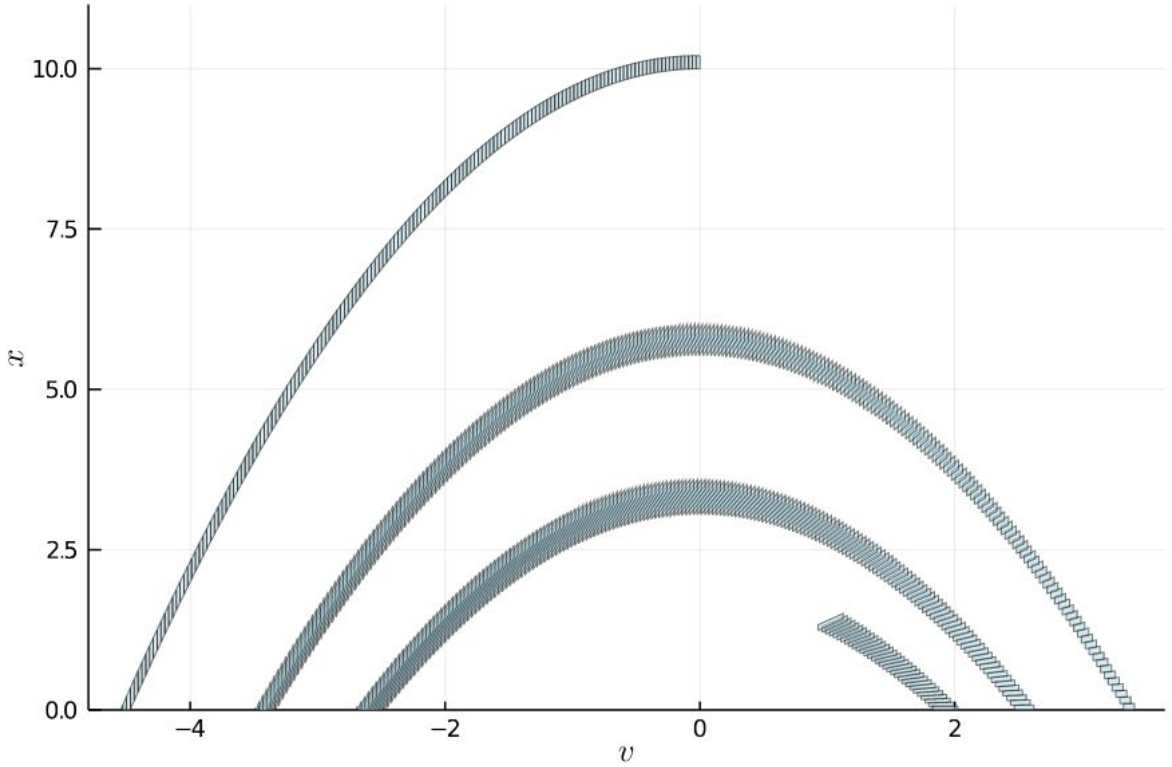
Ejemplo: bouncing ball (*c=0.75, x(0)=10±0.1, v(0)=0*)



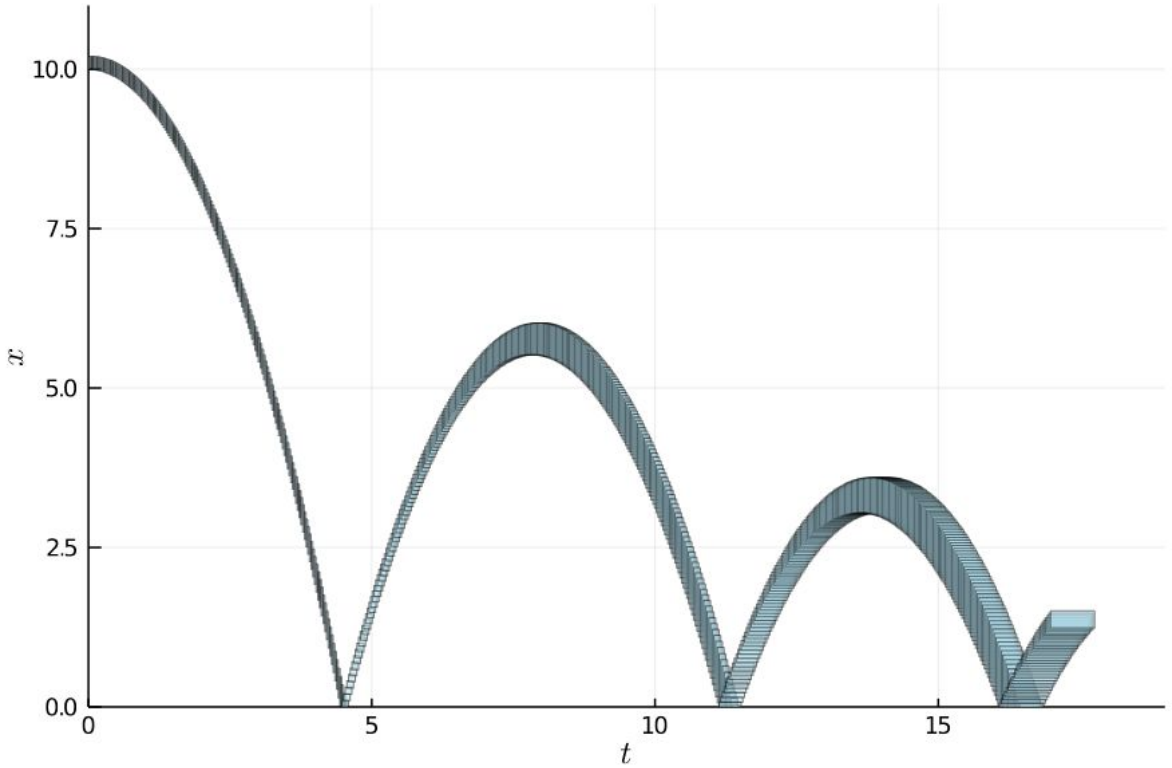
Ejemplo: bouncing ball (*c=0.75, x(0)=10±0.1, v(0)=0*)



Ejemplo: bouncing ball (*c=0.75, x(0)=10±0.1, v(0)=0*)



Ejemplo: bouncing ball (*c=0.75, x(0)=10±0.1, v(0)=0*)

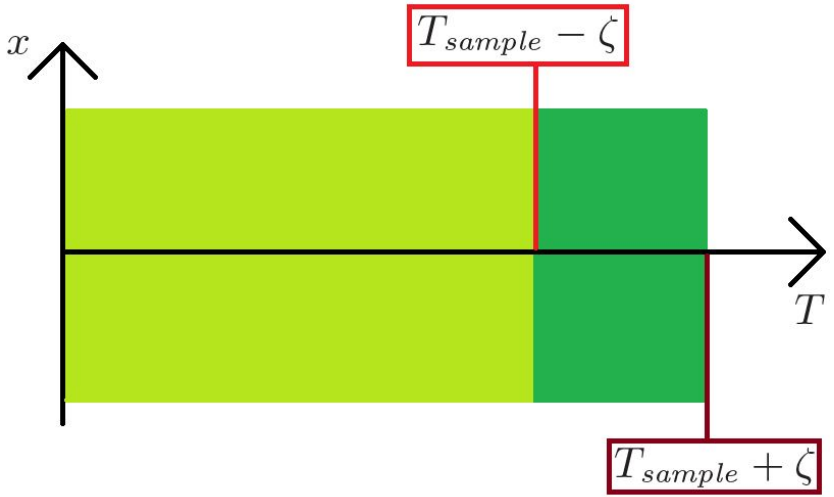


Sistema híbrido con transiciones controladas por reloj

Transiciones controladas por reloj

$$\frac{\dot{x} = -x \quad \dot{T} = 1}{T \leq T_{sample} + \zeta} \qquad \frac{T \geq T_{sample} - \zeta}{x' := 2x \quad T' := T - T_{sample}}$$

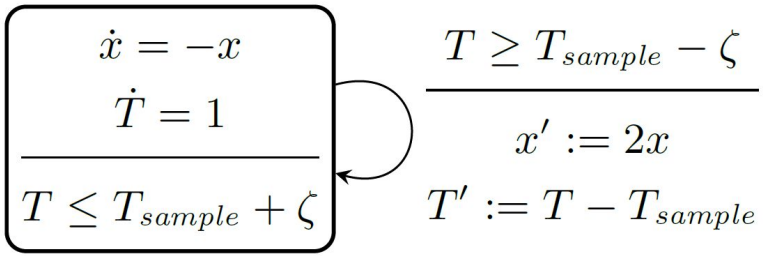
$$\frac{d}{dt}\begin{bmatrix} x \\ T \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ T \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



Transiciones controladas por reloj

Incerteza en el tiempo de *switching*:

- caso determinista: la transición en el instante *Tsample* (ζ=0)
- caso no-determinista: transición en algún instante *T* ϵ [*Tsample*-ζ,*Tsample*+ζ]



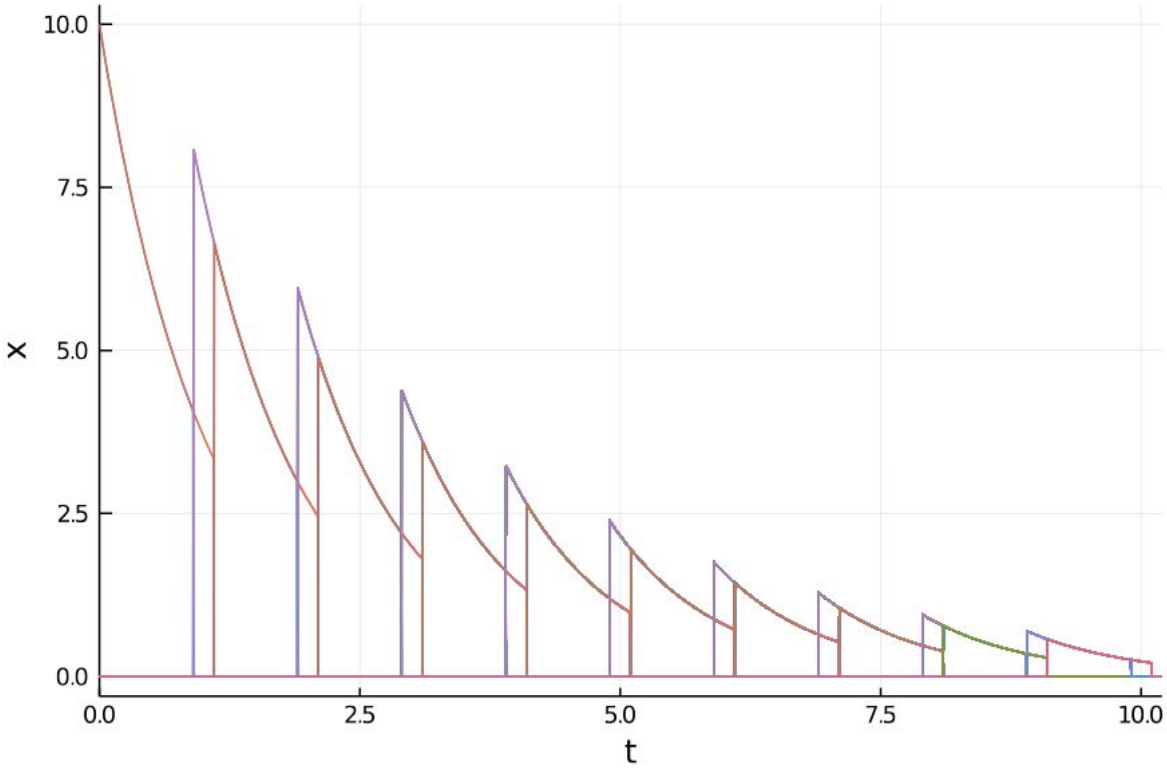
Solución analítica

Tsample = 1.0

ζ = 0.1

x(0) = 10.0

$$\frac{\dot{x} = -x \quad \dot{T} = 1}{T \leq T_{sample} + \zeta} \qquad \frac{T \geq T_{sample} - \zeta}{x' := 2x \quad T' := T - T_{sample}}$$



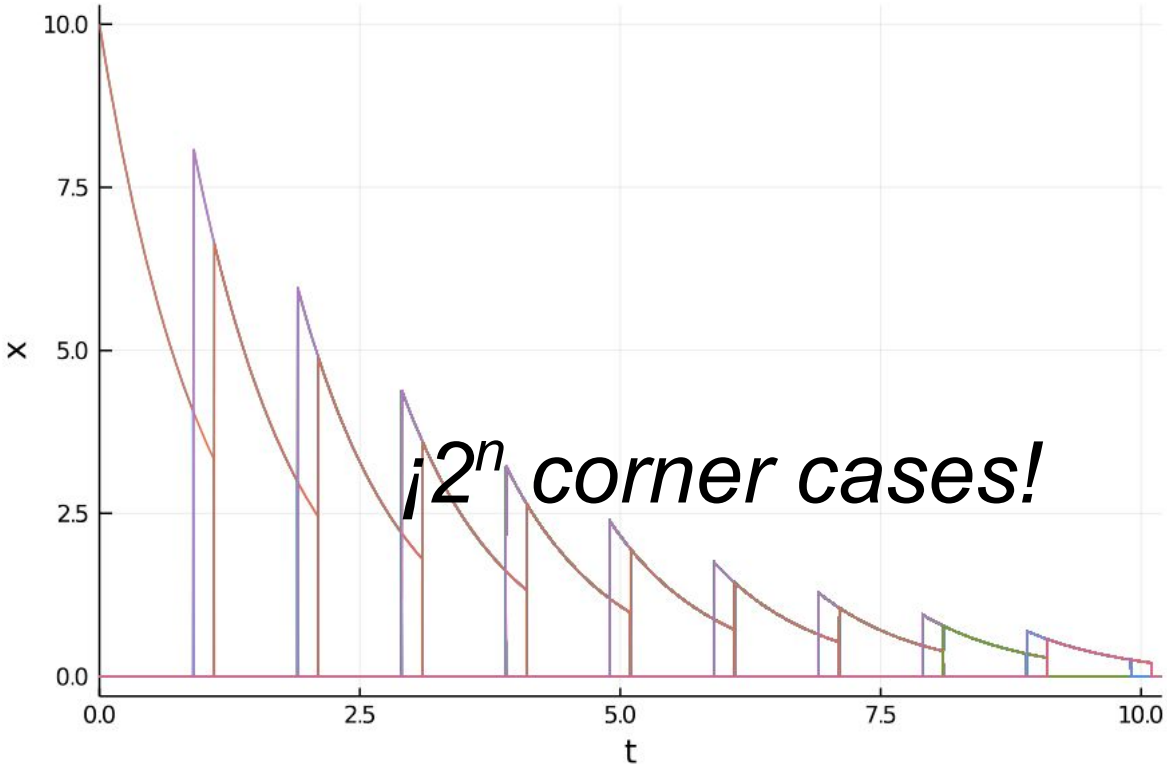
Solución analítica

Tsample = 1.0

ζ = 0.1

x(0) = 10.0

$$\frac{\dot{x} = -x \quad \dot{T} = 1}{T \leq T_{sample} + \zeta} \qquad \frac{T \geq T_{sample} - \zeta}{x' := 2x \quad T' := T - T_{sample}}$$



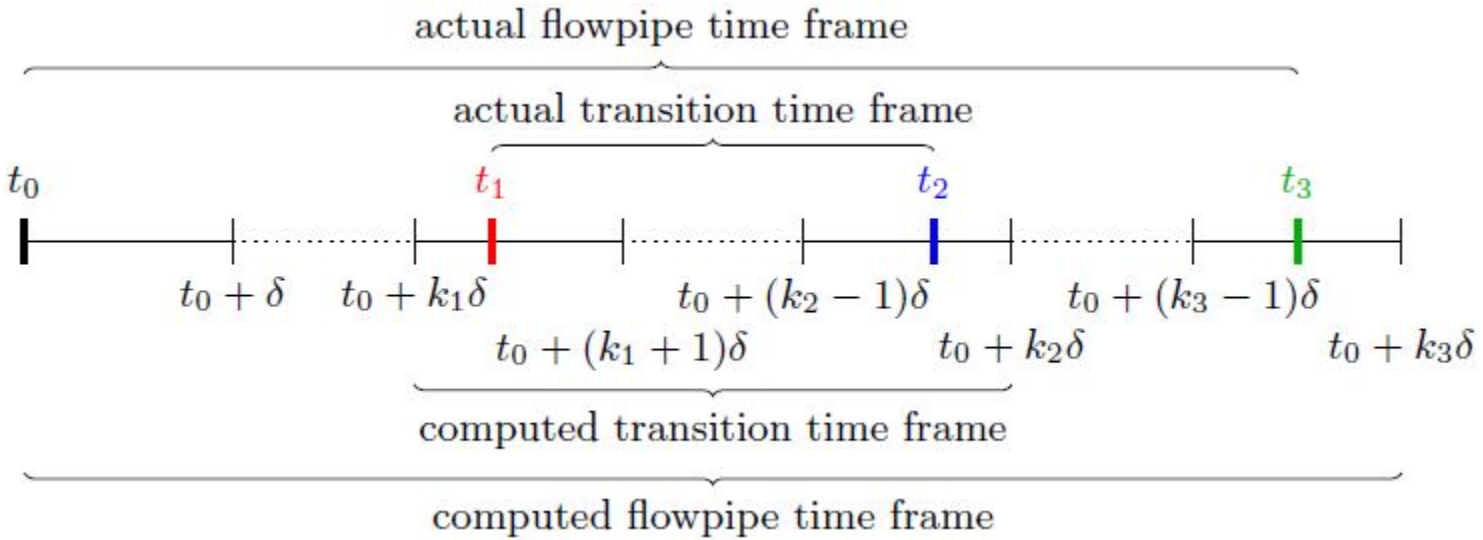
¡2^n corner cases!

Transiciones controladas por reloj

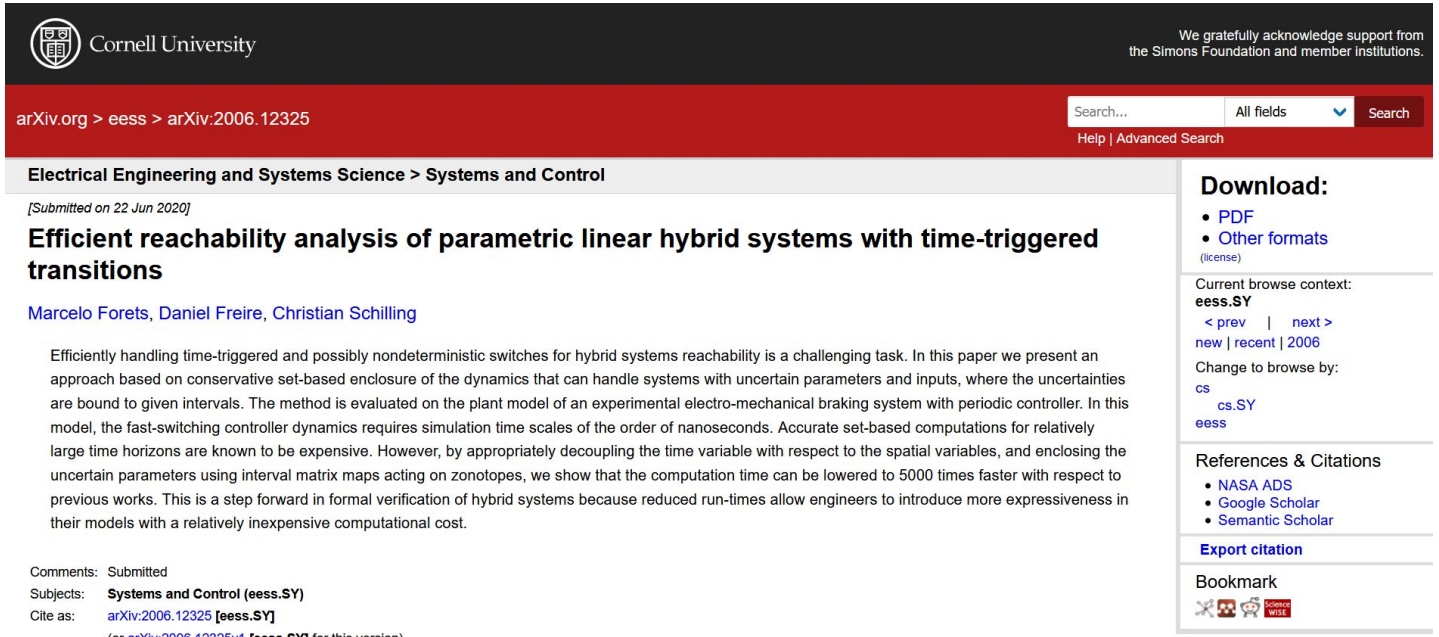
- El momento de la transición es controlado puramente por el tiempo *T* (reloj)
- La dinámica de *T* es independiente de las otras variables de estado (*x*)

Transiciones controladas por reloj

- El momento de la transición es controlado puramente por el tiempo *T* (reloj)
- La dinámica de *T* es independiente de las otras variables de estado (*x*)



Eliminar reloj de las variables de estado



Cornell University

We gratefully acknowledge support from the Simons Foundation and member institutions.

arXiv.org > eess > arXiv:2006.12325

Search... All fields Search

Help | Advanced Search

Electrical Engineering and Systems Science > Systems and Control

[Submitted on 22 Jun 2020]

Efficient reachability analysis of parametric linear hybrid systems with time-triggered transitions

Marcelo Forets, Daniel Freire, Christian Schilling

Efficiently handling time-triggered and possibly nondeterministic switches for hybrid systems reachability is a challenging task. In this paper we present an approach based on conservative set-based enclosure of the dynamics that can handle systems with uncertain parameters and inputs, where the uncertainties are bound to given intervals. The method is evaluated on the plant model of an experimental electro-mechanical braking system with periodic controller. In this model, the fast-switching controller dynamics requires simulation time scales of the order of nanoseconds. Accurate set-based computations for relatively large time horizons are known to be expensive. However, by appropriately decoupling the time variable with respect to the spatial variables, and enclosing the uncertain parameters using interval matrix maps acting on zonotopes, we show that the computation time can be lowered to 5000 times faster with respect to previous works. This is a step forward in formal verification of hybrid systems because reduced run-times allow engineers to introduce more expressiveness in their models with a relatively inexpensive computational cost.

Comments: Submitted
Subjects: **Systems and Control (eess.SY)**
Cite as: arXiv:2006.12325 **[eess.SY]**
(or arXiv:2006.12325v1 **[eess.SY]** for this version)

Download:

- PDF
- Other formats

(license)

Current browse context:
eess.SY

< prev | next >
new | recent | 2006

Change to browse by:
cs
cs.SY
eess

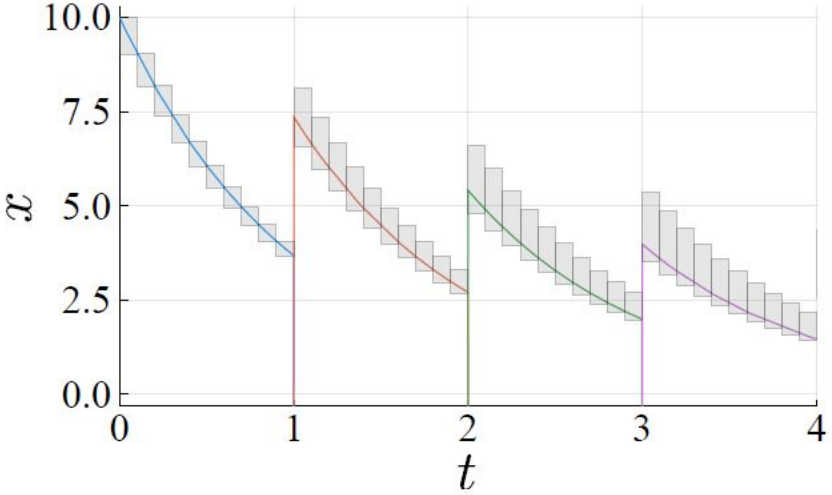
References & Citations

- NASA ADS
- Google Scholar
- Semantic Scholar

Export citation

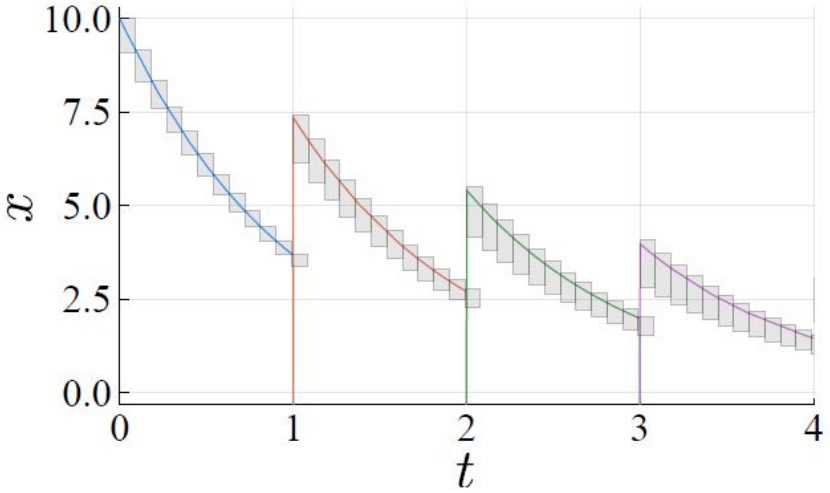
Bookmark

Caso determinista a)



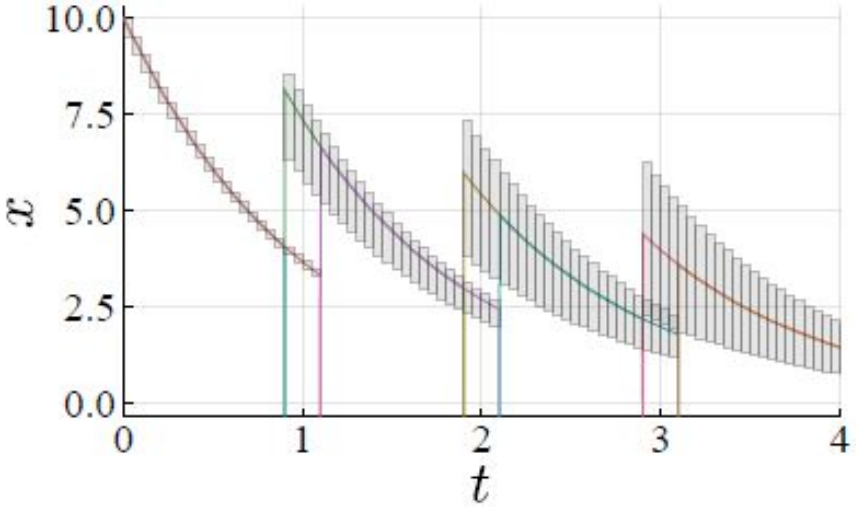
(b) Flowpipes for switches at multiples of the sampling time ($\delta = 0.1$).

Caso determinista b)



(c) Flowpipes for switches not at multiples of the sampling time ($\delta = 0.09$).

Caso no determinista



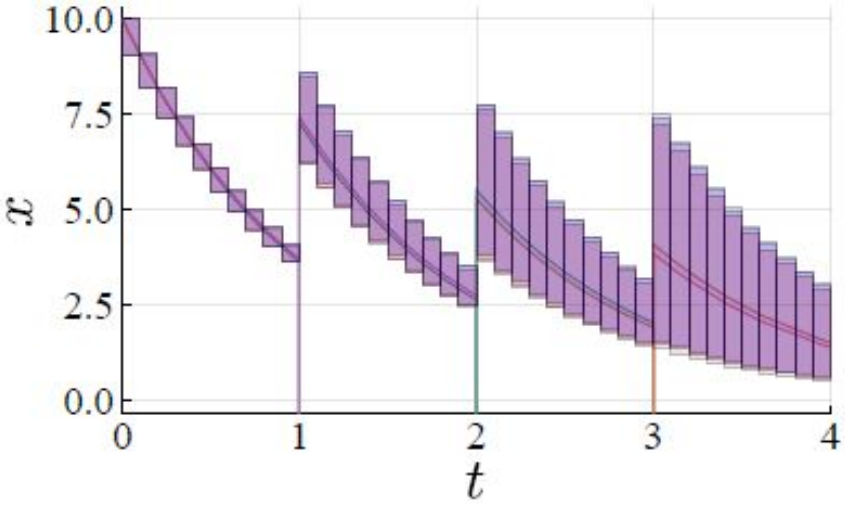
(a) Two trajectories and flowpipes for the nondeterministic instantiation $\zeta = 0.1$ and step size $\delta = 0.05$.

Caso paramétrico

$$\frac{d}{dt}\begin{bmatrix} x \\ T \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ T \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

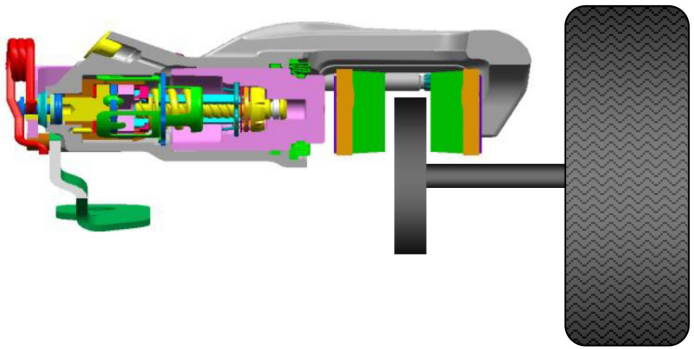
$$\boldsymbol{A}_l := ([-1.1, -1])$$

$$\boldsymbol{A}_h := ([-1, -0.9])$$

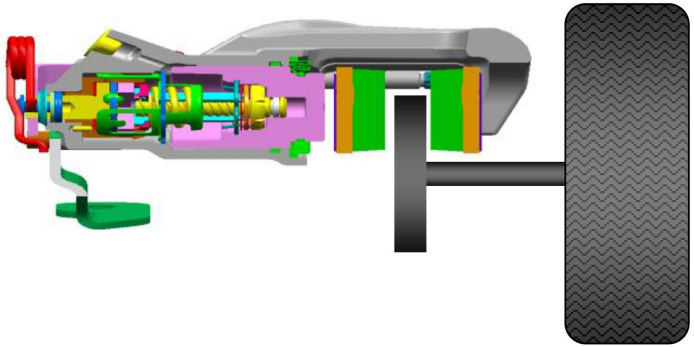


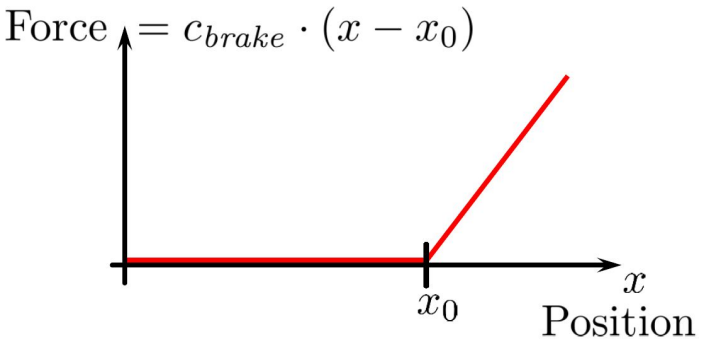
(b) Two trajectories and flowpipes for the parametric setting with interval matrix $\boldsymbol{A}$ (gray) and with interval matrices $\boldsymbol{A}_l$ and $\boldsymbol{A}_h$ (red and blue) and step size $\delta = 0.1$.

Aplicación: Freno electro-mecánico



Aplicación: Freno electro-mecánico



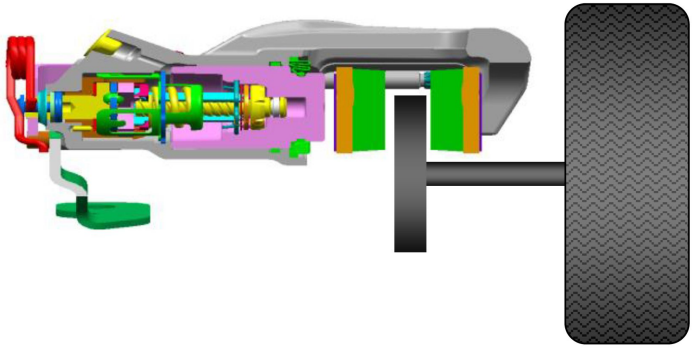


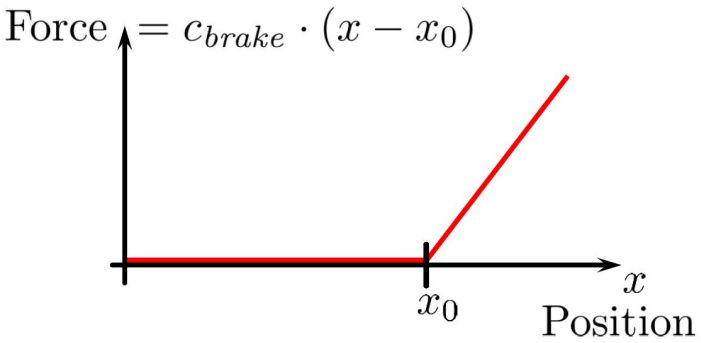
Strathmann and Oehlerking, 2015 [SO15]

Motor eléctrico que empuja el lado interno del calibre (con posición *x*) compuesto por:

- Hardware: las tolerancias de los parámetros físicos asociados a las piezas mecánicas están sujetos a su desgaste
- PI controller (proportional integral): controlador a tiempo discreto que muestrea la distancia (*x-x0*) en tiempos *N*Tsample*.

Aplicación: Freno electro-mecánico

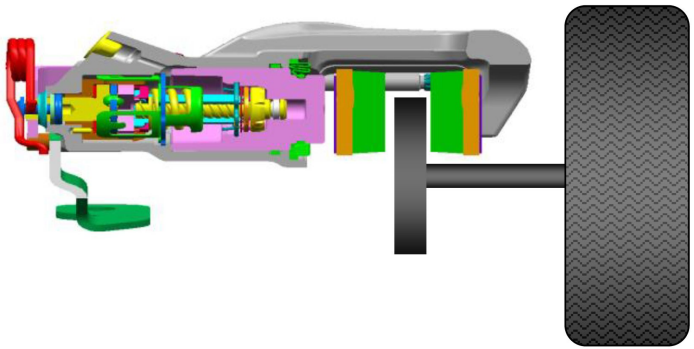




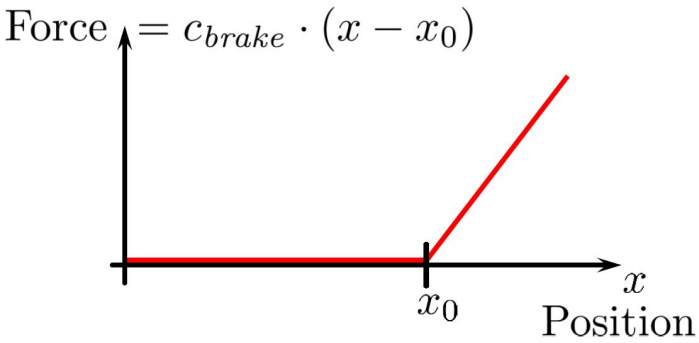
Especificaciones:

- Una vez solicitado el frenado, el calibre debe tomar contacto con el disco (*x=x0*) en un tiempo máximo de 23 ms.
- Cuando comienza el accionar del freno (*x>x0*), la velocidad del calibre debe mantenerse por debajo de 2 mm/s para topear vibraciones.

Aplicación: Freno electro-mecánico



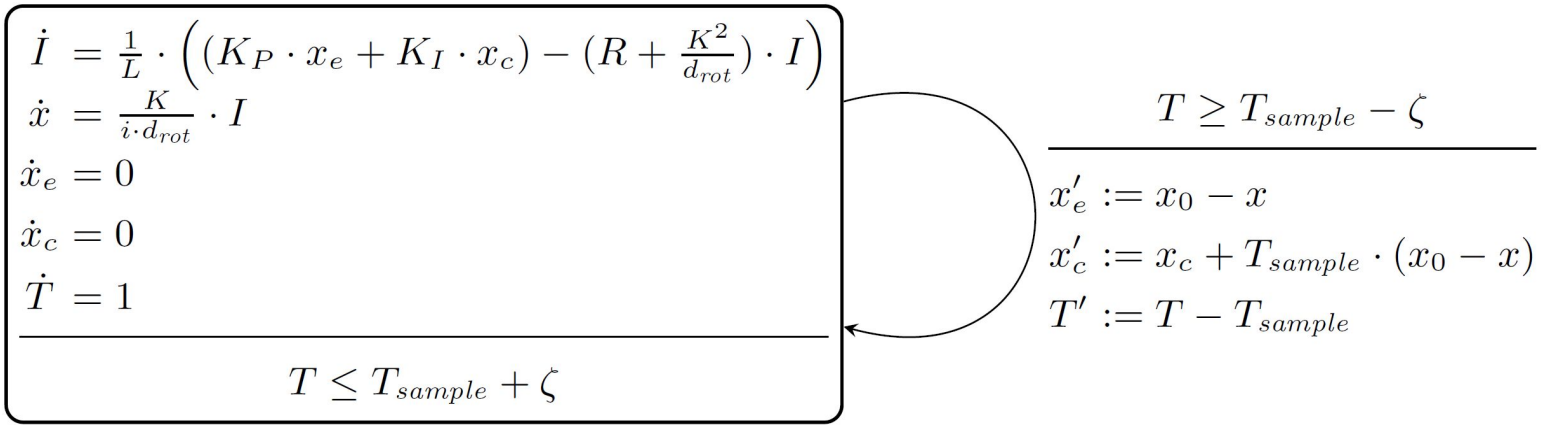
$$
\begin{aligned}
\dot{I} &= \frac{1}{L} \cdot (V - \tanh(100 \cdot I) \cdot V_{brush} - R \cdot I - K \cdot \omega) \\
\dot{\omega} &= \frac{1}{J} \cdot (K \cdot I - c_{gear} \cdot (\varphi - i \cdot x) - d_{rot} \cdot \omega) \\
\dot{\varphi} &= \omega \\
\dot{v} &= \frac{1}{m} \cdot (c_{gear} \cdot (\varphi - i \cdot x) \cdot i - c_{brake} \cdot x_1 - d_{trans} \cdot v) \\
\dot{x} &= v
\end{aligned}
$$



$$
x_1 = \begin{cases} x - x_0 & \text{if } x \geq x_0 \\ 0 & \text{otherwise} \end{cases}
$$

Aplicación: Freno electro-mecánico

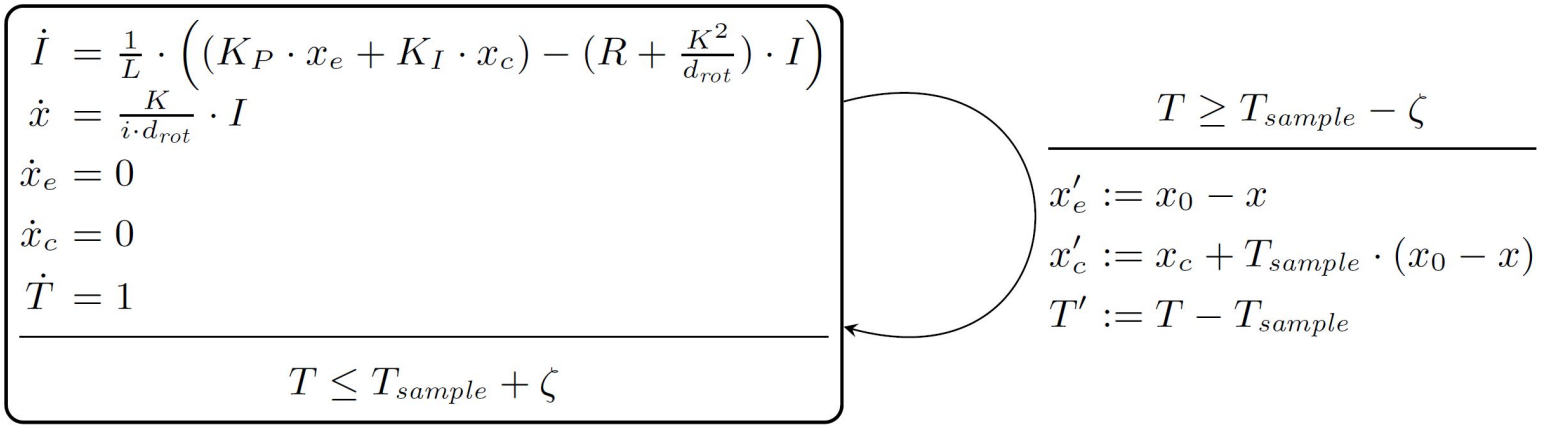
El controlador se modela como un autómata híbrido (*hybrid automaton*) con un único modo (*location*) con una auto-bucle (transición hacia el mismo modo) cada vez que se mide la distancia *x-x0*.



Aplicación: Freno electro-mecánico

Dos casos según el tipo de reloj que se use para el control:

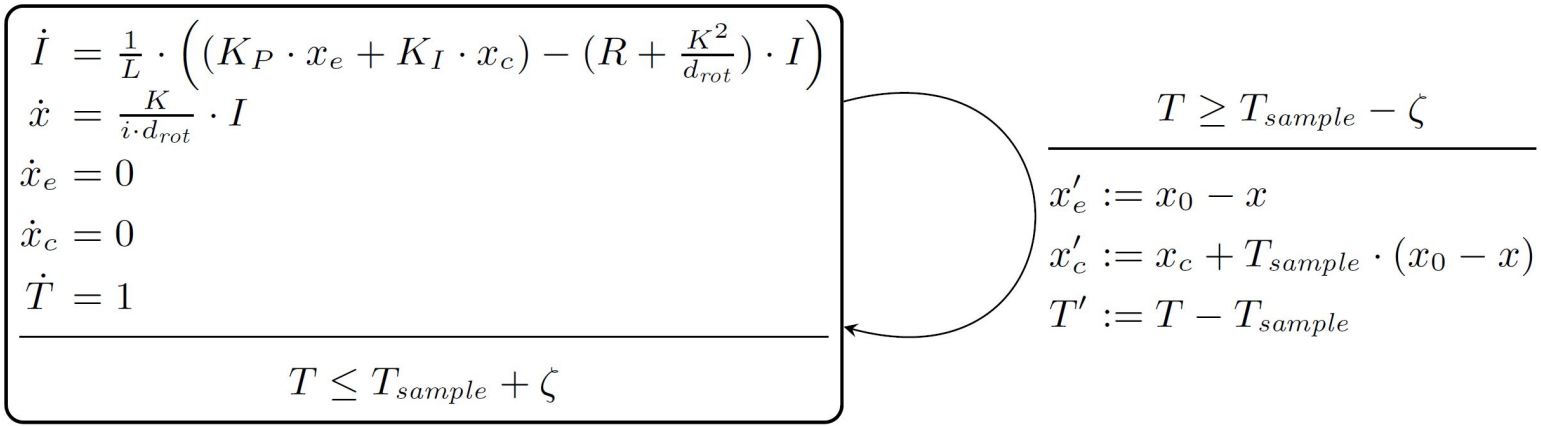
- Determinista: cada vez que se alcanza el tiempo *Tsample*, se mide *x-x0*
- No-determinista: incerteza en el instante de muestreo (***sampling jitter***) ζ, por lo que la medición (y transición) es en $T \in [Tsample - \zeta, Tsample + \zeta]$



Aplicación: Freno electro-mecánico

El controlador es de conmutación rápida (*fast-switching*) y requiere escalas temporales de simulación del orden de nanosegundos.

Para tiempo de integración (*time horizon*) relativamente grandes, el costo computacional es elevado.



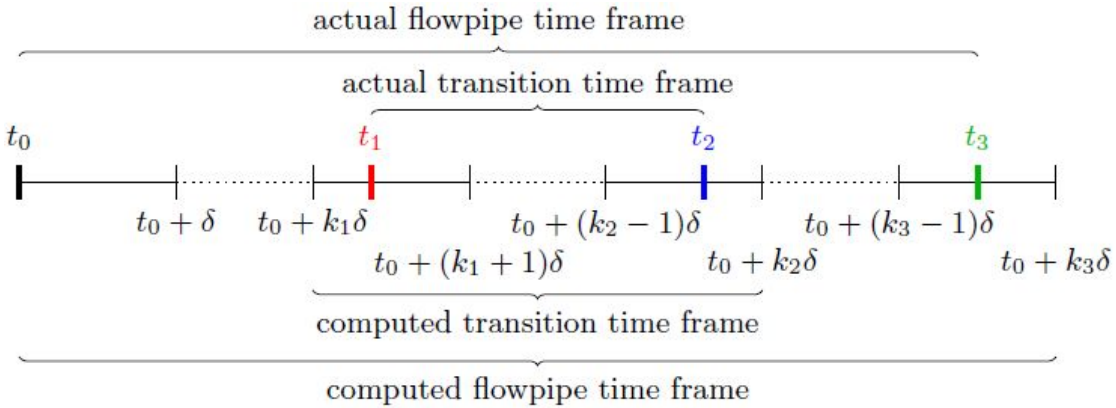
Aplicación: Freno electro-mecánico [SO15]

- Las transiciones son puramente disparadas por reloj (*time-triggered*)
- El reloj evoluciona de manera independiente de las otras variables de estado

Aplicación: Freno electro-mecánico [SO15]

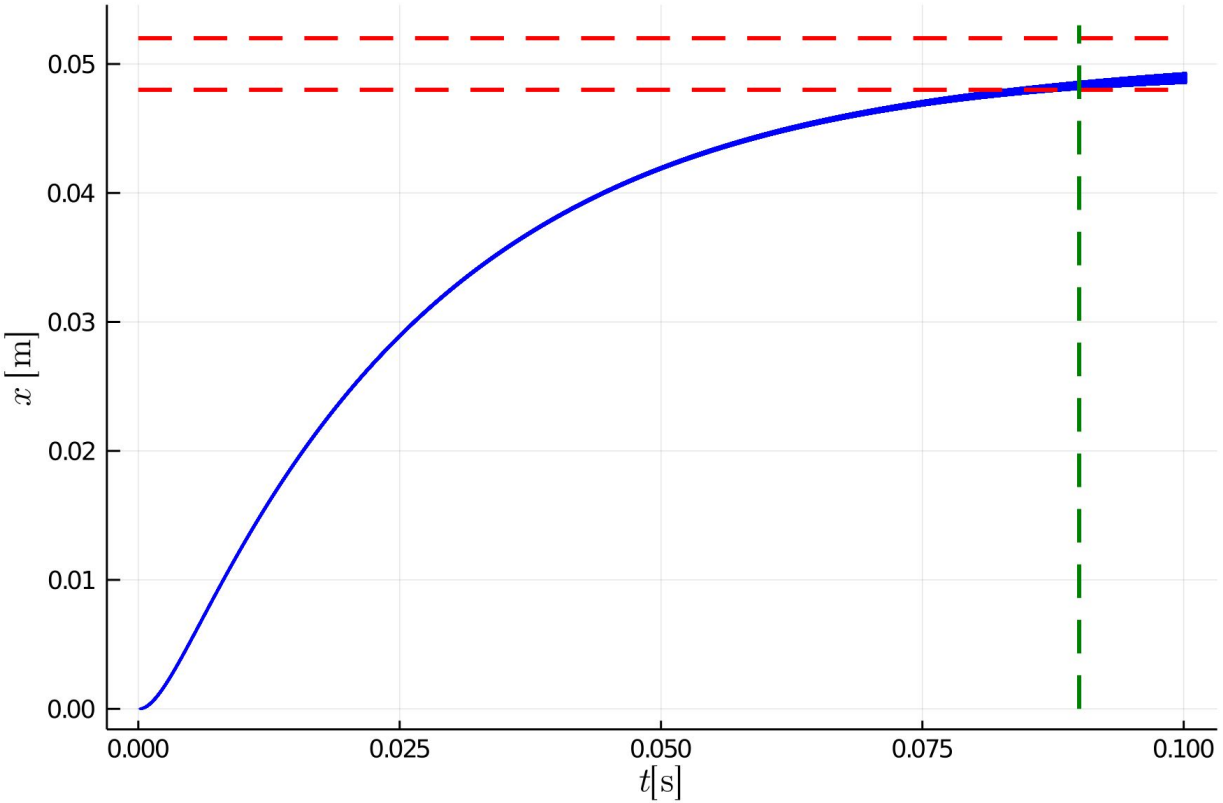
- Las transiciones son puramente disparadas por reloj (*time-triggered*)
- El reloj evoluciona de manera independiente de las otras variables de estado

Entonces, proponemos razonar de manera independiente los intervalos de tiempo en que se habilita la transición, con un reloj externo.



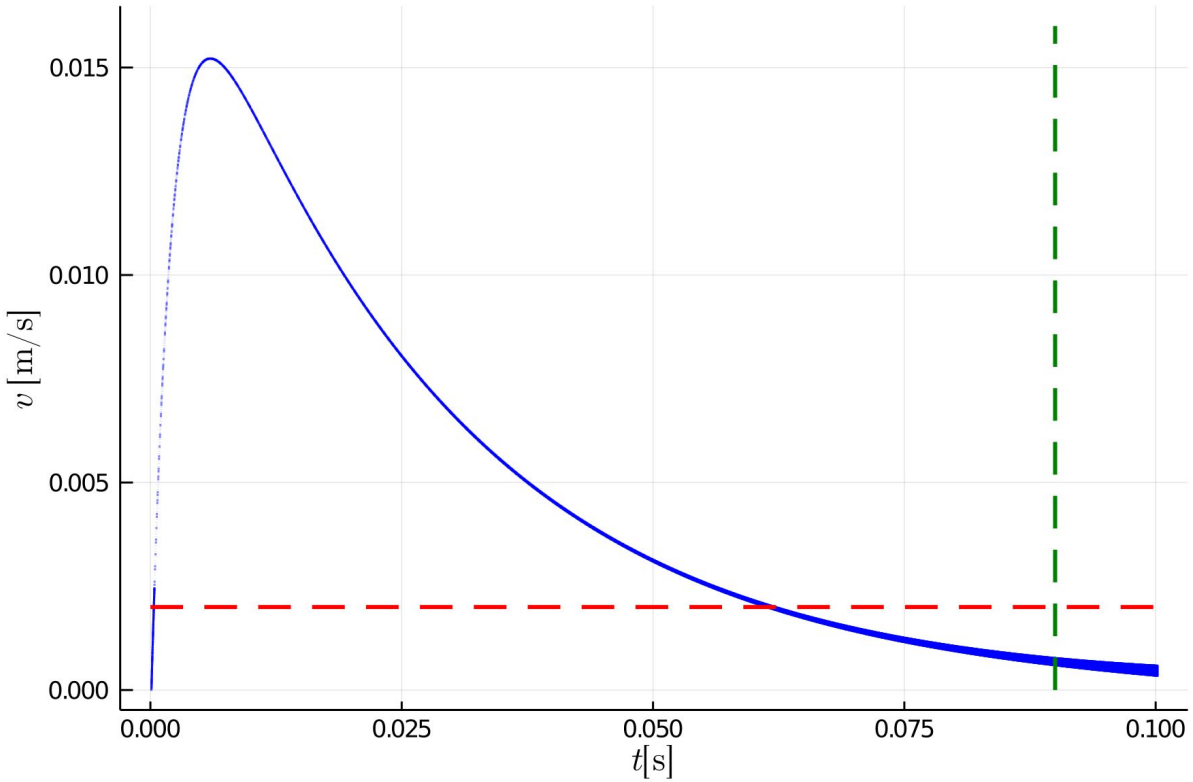
Aplicación: Freno electro-mecánico

T_{sample}=10^{-4} s, número de reachsets 10^6 - 10^7



Aplicación: Freno electro-mecánico

$$v = \dot{x} = \frac{K}{i \cdot d_{rot}} \cdot I$$



Aplicación: Freno electro-mecánico

Requerimientos generalizados para el modelo lineal **simplificado**:

- t_c: $|x - x_o| \leqslant \varepsilon$, $\forall\ t \geqslant t_c$
- $v_r \leqslant v_{rc}$, $\forall\ t \geqslant t_c$

$$
\begin{array}{l}
\dot{I} = \frac{1}{L} \cdot \left((K_P \cdot x_e + K_I \cdot x_c) - (R + \frac{K^2}{d_{rot}}) \cdot I \right) \\
\dot{x} = \frac{K}{i \cdot d_{rot}} \cdot I \\
\dot{x}_e = 0 \\
\dot{x}_c = 0 \\
\dot{T} = 1 \\
\hline
T \leq T_{sample} + \zeta
\end{array}
\qquad
\begin{array}{c}
T \geq T_{sample} - \zeta \\
\hline
x_e' := x_0 - x \\
x_c' := x_c + T_{sample} \cdot (x_0 - x) \\
T' := T - T_{sample}
\end{array}
$$

Aplicación: Freno electro-mecánico

```
R = 0.5
L = 1.e-3
KP = 10000.
KI = 1000.
K = 0.02
drot = 0.1
i = 113.1167

Tsample=1.E-4

# initial conditions
Io  = Singleton([0.0])
xo  = Singleton([0.0])
xeo = Singleton([0.0])
xco = Singleton([0.0])
Xo = Io × xo × xeo × xco
```

$\zeta = [-10^{-8}, 10^{-7}]$ s

		final diameter		computation	requirements		
ζ (y/n)	δ [s]	I	x ($\times 10^{-5}$)	time [s]	ε [m]	t_c [ms]	v_r [mm/s]
no	10^{-7}	13.707	73.519	0.231	0.002	88.8	0.80
	10^{-8}	1.369	7.343	1.08	0.002	85.8	0.81
	10^{-9}	0.137	0.7343	17.0	0.002	85.5	0.81
no (*)	10^{-8}	9.78×10^{-6}	0.0000471	1.15	0.002	85.5	0.81
yes	10^{-7}	54.71	293	0.229	0.005	64.8	1.93
	10^{-8}	17.75	95.183	0.979	0.002	90.1	0.80
	10^{-9}	16.56	88.8	21.1	0.01	44.7	3.84

Aplicación: Freno electro-mecánico

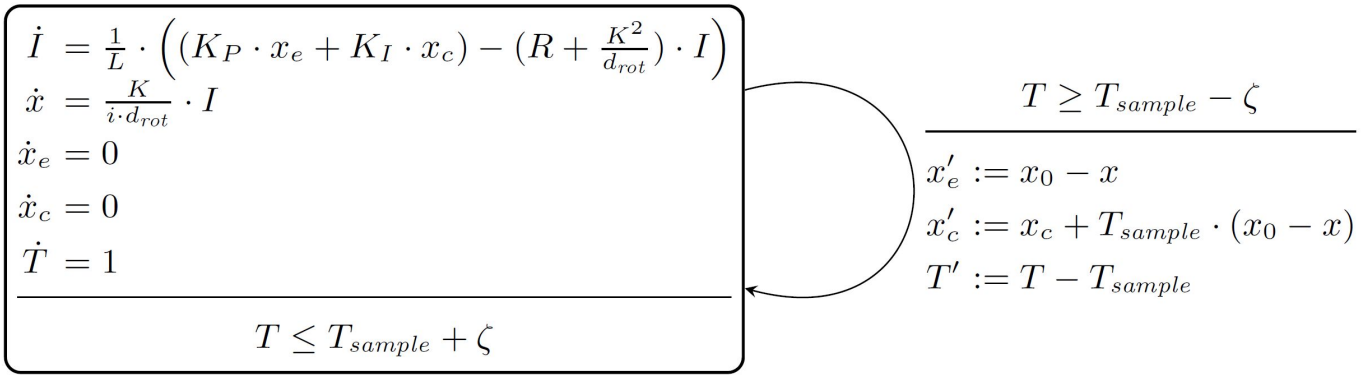
```
R = 0.5
L = 1.e-3
KP = 10000.
KI = 1000.
K = 0.02
drot = 0.1
i = 113.1167

Tsample=1.E-4

# initial conditions
Io  = Singleton([0.0])
xo  = Singleton([0.0])
xeo = Singleton([0.0])
xco = Singleton([0.0])
Xo = Io × xo × xeo × xco
```

$\zeta = [-10^{-8}, 10^{-7}]$ s

ζ (y/n)	δ [s]	final diameter I	final diameter x ($\times 10^{-5}$)	computation time [s]	requirements ε [m]	requirements t_c [ms]	requirements v_r [mm/s]
no	10^{-7}	13.707	73.519	0.231	0.002	88.8	0.80
	10^{-8}	1.369	7.343	1.08	0.002	85.8	0.81
	10^{-9}	0.137	0.7343	17.0	0.002	85.5	0.81
no (*)	10^{-8}	9.78×10^{-6}	0.0000471	1.15	0.002	85.5	0.81
yes	10^{-7}	54.71	293	0.229	0.005	64.8	1.93
	10^{-8}	17.75	95.183	0.979	0.002	90.1	0.80
	10^{-9}	16.56	88.8	21.1	0.01	44.7	3.84

Speedup respecto a herramientas de referencia (*Flow** en [SO15]): **x5000**

Aplicación: Freno electro-mecánico



$$\dot{x} = Ax$$

$$A = \begin{bmatrix} p & 0 & K_P/L & K_I/L \\ K/(i \cdot d_{rot}) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \text{ con } p = -(R + K^2/d_{rot})/L$$

Aplicación: Freno electro-mecánico

Caso *pv1*:

$$A = \begin{bmatrix} p \pm \Delta & 0 & K_P/L & K_I/L \\ K/(i \cdot d_{rot}) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Aplicación: Freno electro-mecánico

Caso *pv2*:

$$R \pm \chi\%$$
$$L \pm \chi\%$$
$$K_P \pm \chi\%$$
$$K_I \pm \chi\%$$
$$K \pm \chi\%$$
$$d_{rot} \pm \chi\%$$
$$i \pm \chi\%$$

Aplicación: Freno electro-mecánico

case	ζ (y/n)	order	final diameter		computation	requirements		
			I	x $(\times 10^{-3})$	time [s]	ε [m]	t_c [ms]	v_r [mm/s]
pv1	no	1	137.25	7.305	8.817	0.005	70.5	1.89
		2	4.25	0.186	36.538	0.002	87.0	0.82
		3	2.94	0.123	39.958	0.002	86.5	0.82
	yes	1	154.21	8.210	8.995	0.005	72.4	1.88
pv2, $\chi = 1\%$	no	1	2080.79	107.708	10.63	–	–	–
		2	58.31	2.620	44.79	0.02	84.6	8.80
		3	39.05	1.687	45.90	0.02	58.0	8.90
	yes	1	2106.50	109.84	10.24	–	–	–

Aplicación: Freno electro-mecánico

case	ζ (y/n)	order	final diameter		computation	requirements		
			I	x $(\times 10^{-3})$	time [s]	ε [m]	t_c [ms]	v_r [mm/s]
pv1	no	1	137.25	7.305	8.817	0.005	70.5	1.89
		2	4.25	0.186	36.538	0.002	87.0	0.82
		3	2.94	0.123	39.958	0.002	86.5	0.82
	yes	1	154.21	8.210	8.995	0.005	72.4	1.88
pv2, $\chi = 1\%$	no	1	2080.79	107.708	10.63	–	–	–
		2	58.31	2.620	44.79	0.02	84.6	8.80
		3	39.05	1.687	45.90	0.02	58.0	8.90
	yes	1	2106.50	109.84	10.24	–	–	–

El caso *pv2* no se planteaba en [SO15] ya que *pv1* ya resultaba complejo

Conclusiones

- Explotando la estructura del sistema híbrido podemos verificar problemas de mayor complejidad.

- Posible extensión: considerar el modelo **no lineal** del freno.

JuliaReach

Reachability Computations for Dynamical Systems in Julia

http://juliareach.com/

Perspectivas

- Trabajos interdisciplinarios en curso: electrónica analógica, mecánica estructural, verificación de redes neuronales, etc.
- Sistemas caóticos: cuencas de estabilidad
- Reachability probabilístico
- Reachability para PDEs
- Código paralelo, GPU cuda_arrays…

Ofrecer un curso de grado / posgrado sobre métodos formales y aplicaciones en Ciencias e Ingeniería

¡Gracias!
¿Preguntas?

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

CURE Centro Universitario Regional del Este

FACULTAD DE CIENCIAS UDELAR fcien.edu.uy

FACULTAD DE INGENIERIA

IST AUSTRIA Institute of Science and Technology

Universidad Nacional Autónoma de México

Massachusetts Institute of Technology

Referencias

[SO15] Strathmann, T., Oehlerking, J.: Verifying properties of an electro-mechanical braking system. In: ARCH@CPSWeek. EPiC Series in Computing, vol. 34, pp. 49-56.EasyChair (2015)

[FFS20] Forets, M., Freire, D., & Schilling, C. (2020). Efficient reachability analysis of parametric linear hybrid systems with time-triggered transitions. arXiv preprint arXiv:2006.12325.