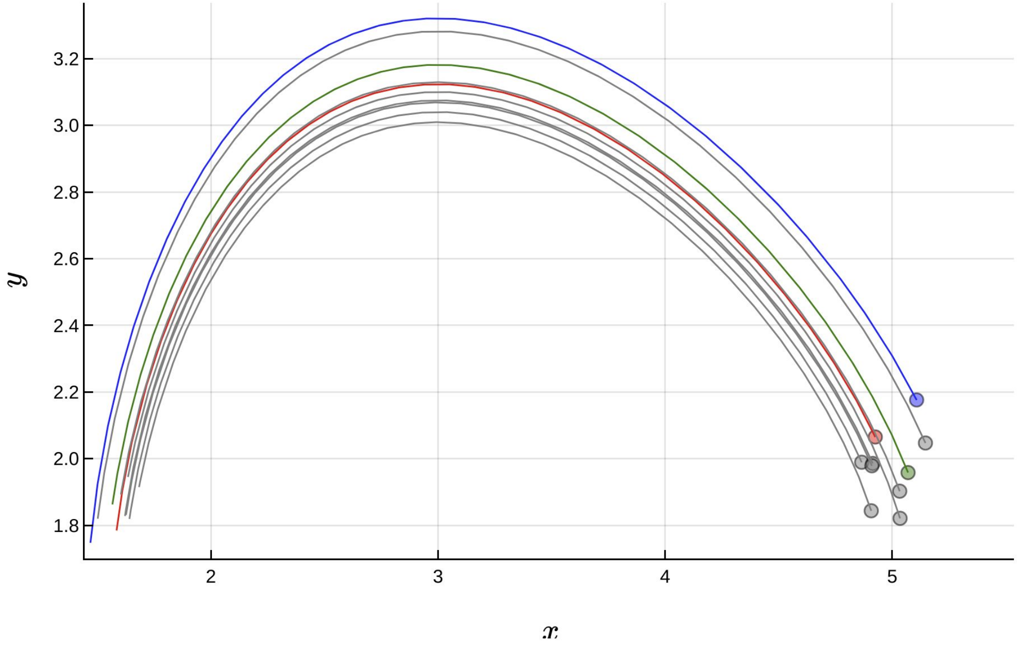
Efficient reachability analysis of parametric linear hybrid systems with time-triggered transitions

Marcelo Forets, CURE, UdelaR, Uruguay
Daniel Freire, IFFC, UdelaR, Uruguay
Christian Schilling, IST Austria and Univ. Konstanz

18th ACM-IEEE International Conference on Formal Methods and Models for System Design
Jaipur, India, December 2-4, 2020

- **Preliminaries**
- Reachability with time-triggered events
- Case study: Electromechanical break
- Conclusions

Verification problem



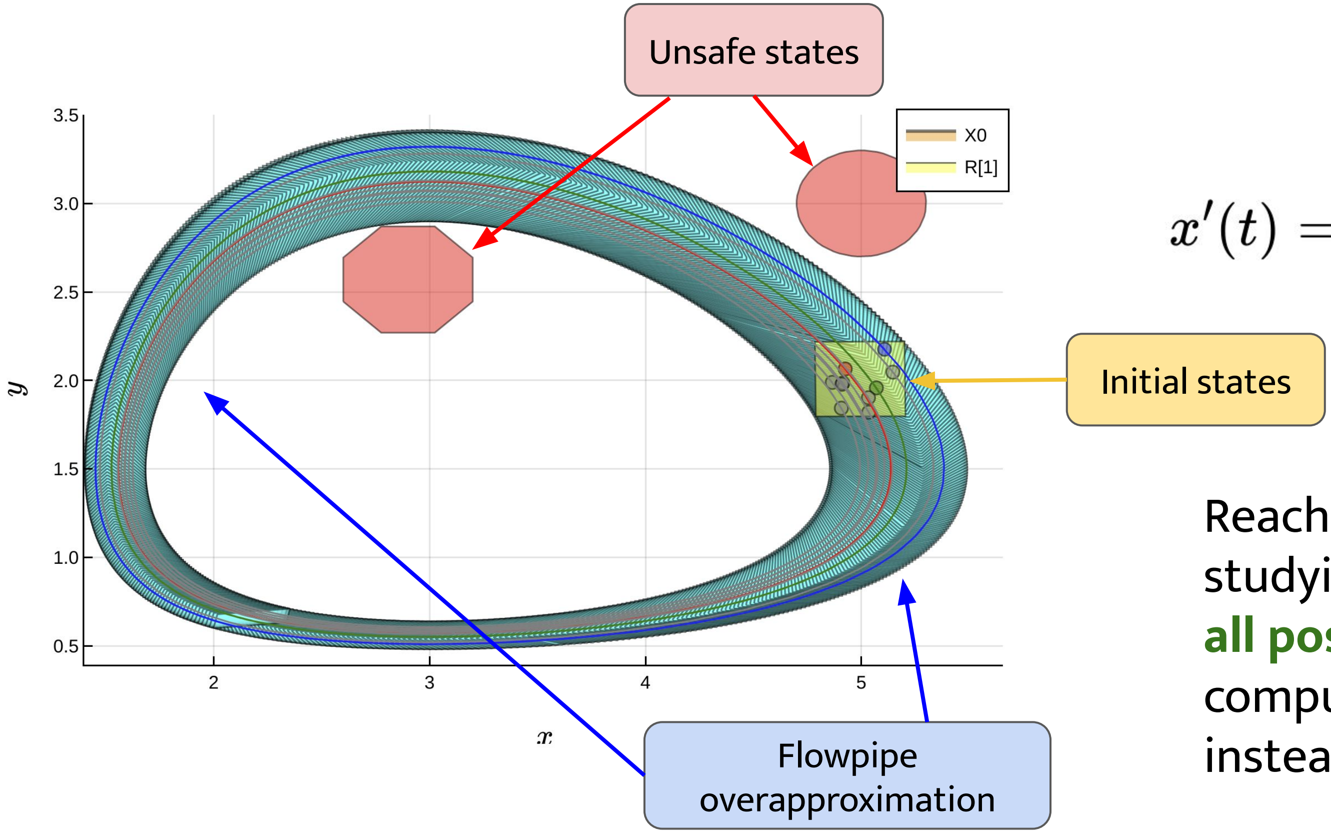
Model

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

- *x(t)* : state
- *u(t)* : controlled or uncontrolled inputs
- *p(t)* : parameters

Uncertainty → Coverage problem

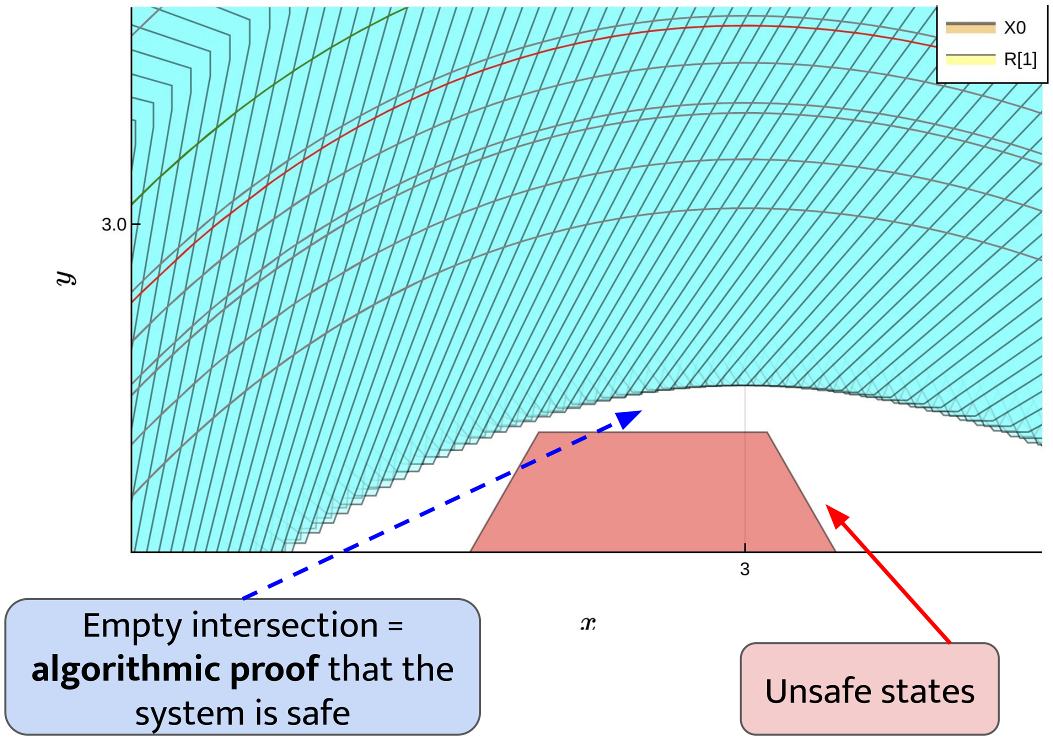
Verification problem



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

Reachability analysis: studying the set of **all possible behaviors**, computing with **sets** instead of scalars

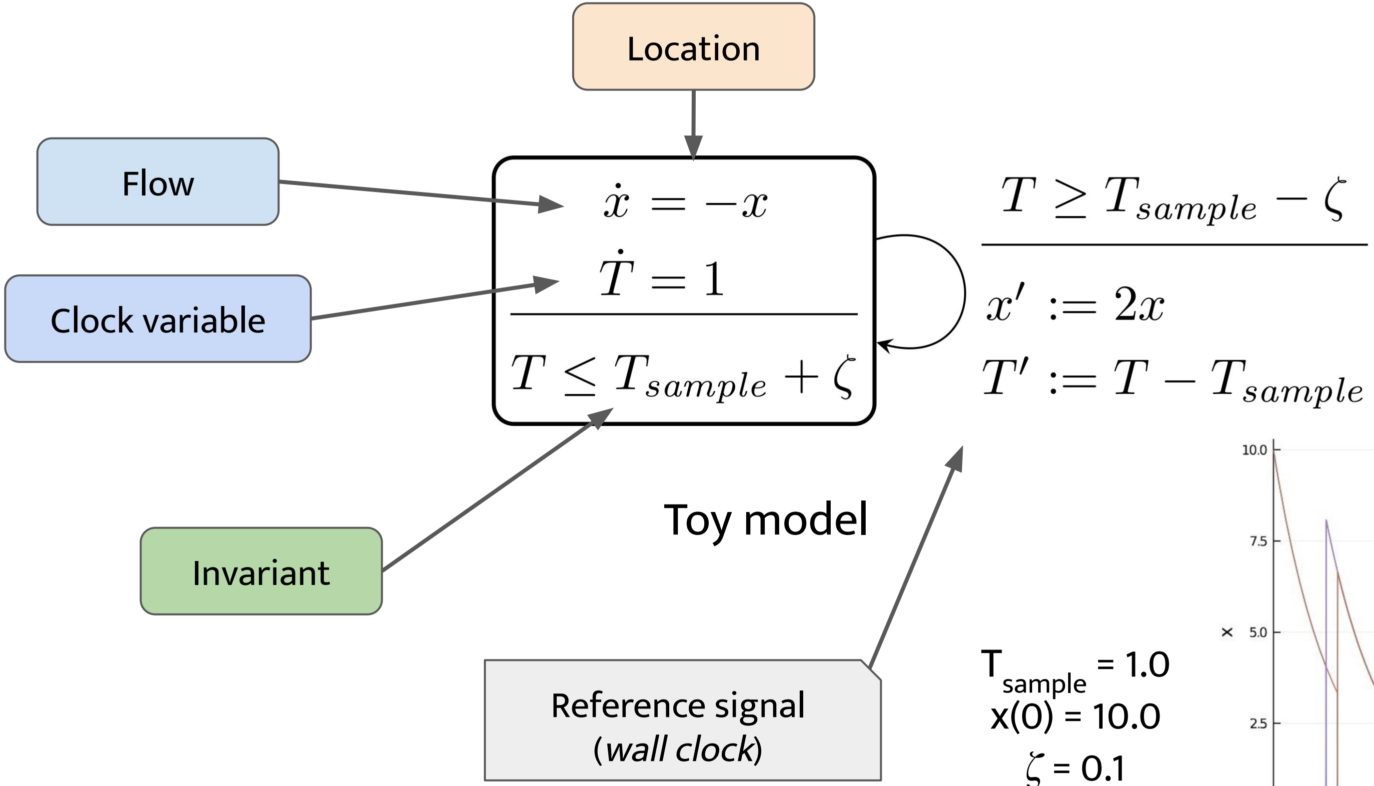
Verification problem

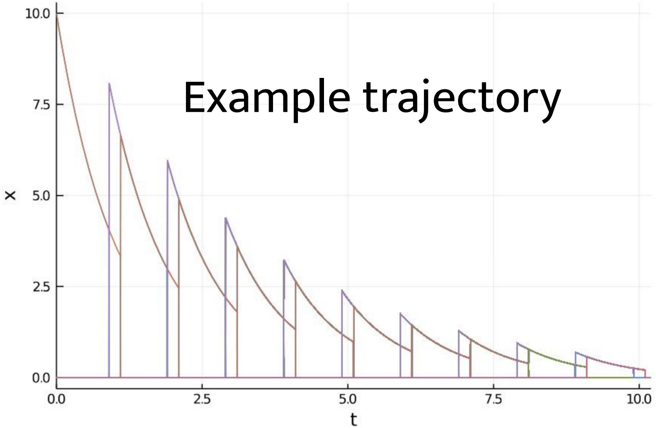


$$x'(t) = f(x(t), u(t), p(t))$$

Is there a trajectory such that the **solution enters the unsafe set** within the given time bound?

Hybrid automaton with time-triggered events





Verification of timed hybrid systems

- Numerical verification of hybrid systems is a challenging task: simulations may **miss jumps**, have an **increased cost** due to root-finding algorithms, may produce **spurious behavior**, and number of feasible runs increases **exponentially** in the presence of nondeterminism [F16].
- Periodically controlled systems with **fast-switching controller dynamics** require small simulation time scales ~10^{-9}s and relatively large time horizons ~10^{-2} s. **Thousands of discrete transitions**.
- Accurate set-based verification is a viable approach but requires to efficiently mitigate the **overapproximation error**.

[F16] Lecture Notes on *Formal Verification of Piecewise Affine Hybrid Systems* by G. Frehse from DigiCosme Spring School, May 12, 2016.

- ➔ Preliminaries
- ➔ **Reachability with time-triggered events**
- ➔ Case study: Electromechanical break
- ➔ Conclusions

Verification process

Model

$$\begin{aligned} \dot{x} &= -x \\ \dot{T} &= 1 \end{aligned}$$
$$T \leq T_{sample} + \zeta$$

$$\frac{T \geq T_{sample} - \zeta}{\begin{aligned} x' &:= 2x \\ T' &:= T - T_{sample} \end{aligned}}$$

Requirements

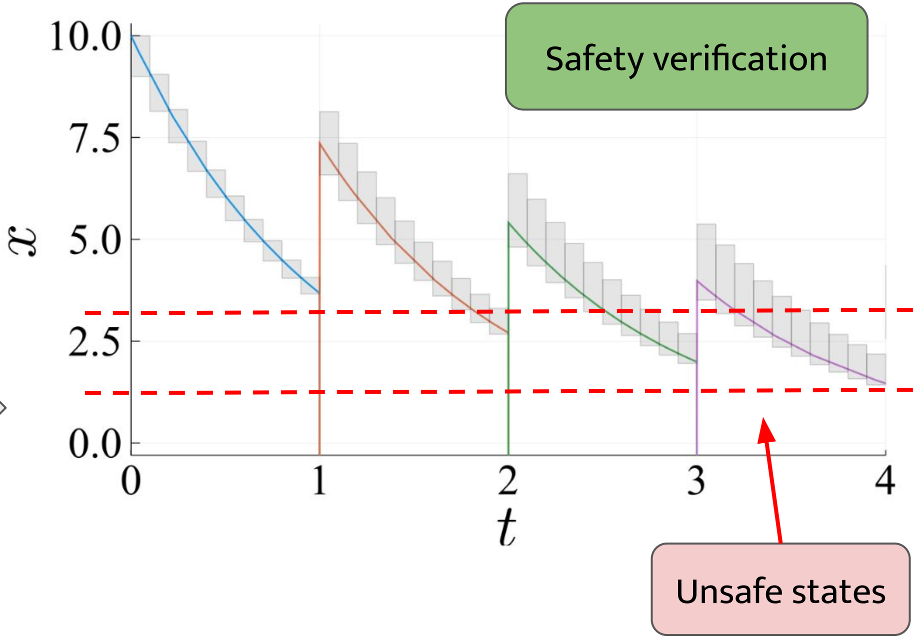
$$|x - x_0| \leq \varepsilon, \forall t \geq t_c$$

Time discretization

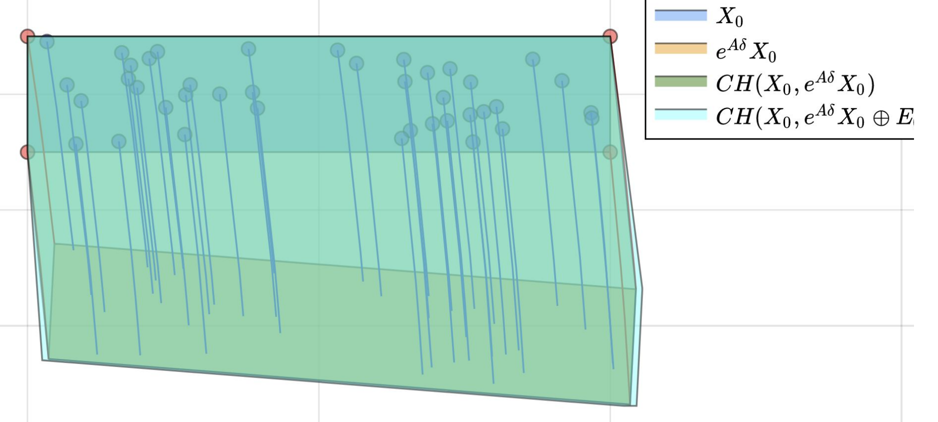
Non-deterministic events

Deterministic events

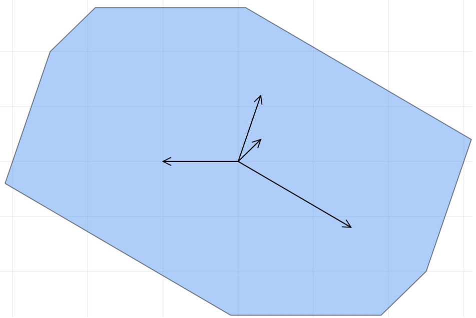
Parametric dynamics



Continuous post-operator



- **Conservative** time discretization [F11].
- $\mathcal{X}(k) = \Phi\mathcal{X}(k-1) \oplus \mathcal{V}, \quad k > 0$
- A is a scalar matrix: **zonotope-based** algorithm [GLGM06].
  - Non-recursive. **Wrapping free.**
  - Fixed order if V = 0.

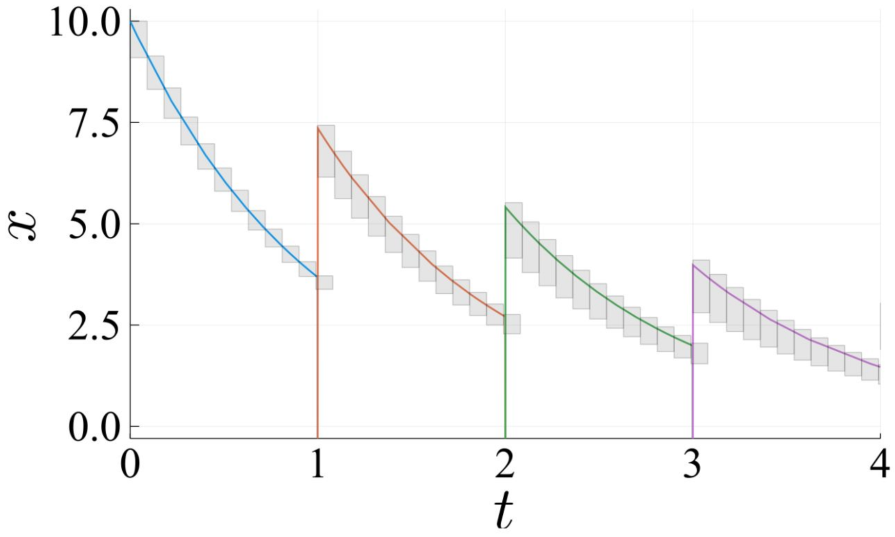


- A is uncertain: **interval matrices** acting on zonotopes [ASB07].
  - Interval matrix powers is hard (**non-associativity**, **dependency problem**).
  - Recursive. Can't avoid **wrapping effect**.
  - Dimension of the system **doesn't increase** with # uncertain parameters.

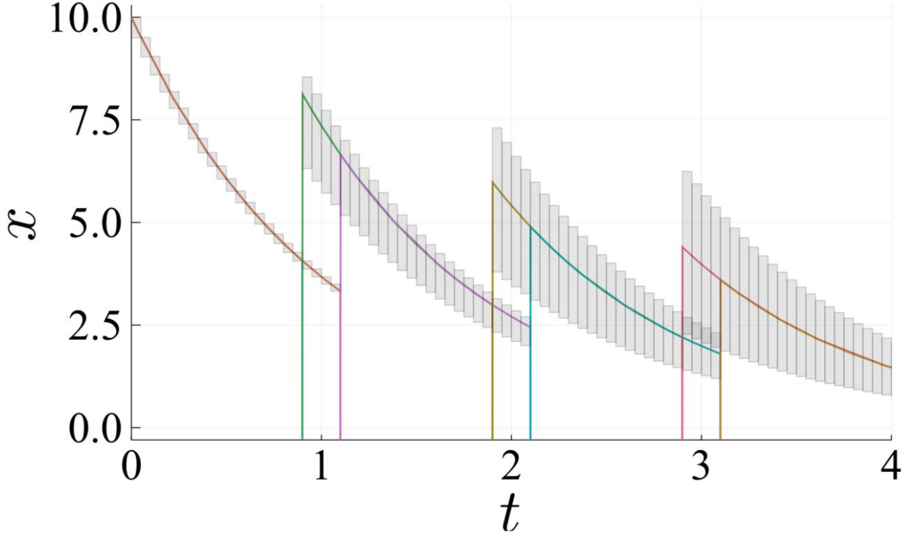
Discrete post-operator

$$\begin{array}{c} \dot{x} = -x \\ \dot{T} = 1 \\ \hline T \leq T_{sample} + \zeta \end{array} \qquad \begin{array}{l} T \geq T_{sample} - \zeta \\ \hline x' := 2x \\ T' := T - T_{sample} \end{array}$$

Deterministic switching

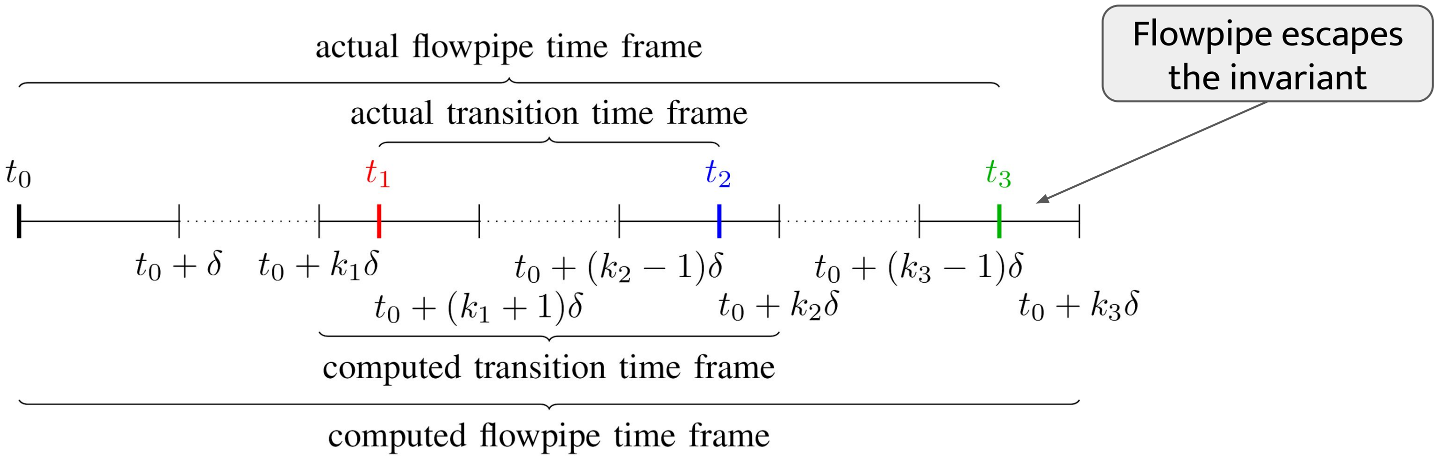


Non-deterministic switching



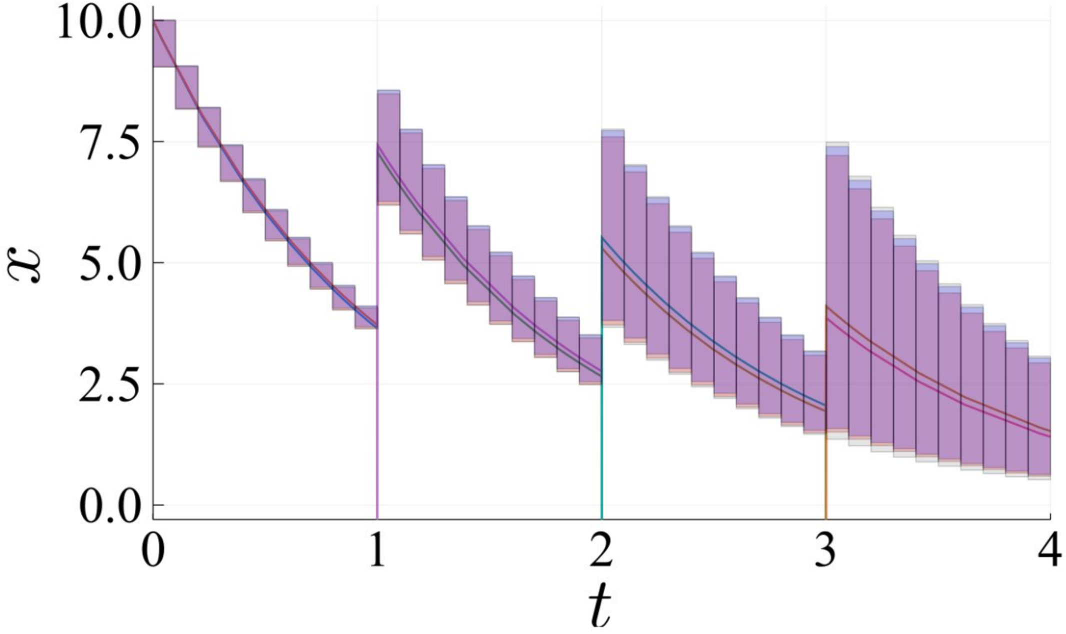
- **Decoupling** the time variable with respect to the spatial variables we **avoid** expensive set-based intersections.

Timeline of relevant events



- Time points when a **guard is enabled** lie in some interval $[t_1, t_2]$.
- We precompute integers k_1, k_2, k_3 such that we need to compute reach-sets **only in the time interval $[t_0, t_0 + k_3\delta]$** and take the transition for the reach-sets only in the time intervals from **$[t_0 + k_1\delta, t_0 + k_2\delta]$**.
- Non-deterministic case requires **clustering** of sets.

Non-deterministic switching and parameter variation



$$\dot{x} = Ax$$
$$\dot{T} = 1$$
$$T \leq T_{sample} + \zeta$$

$$\frac{T \geq T_{sample} - \zeta}{x' := 2x \quad T' := T - T_{sample}}$$

$$\boldsymbol{A} := ([-1.01, -0.99])$$

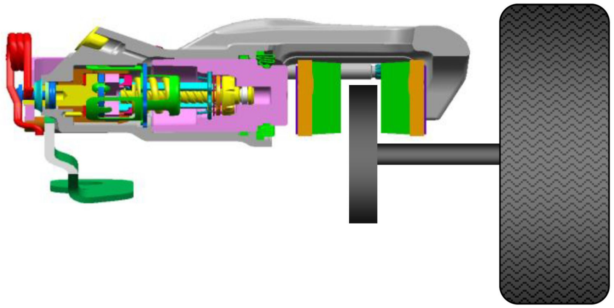
$$\frac{d}{dt}\begin{bmatrix} x \\ T \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x \\ T \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

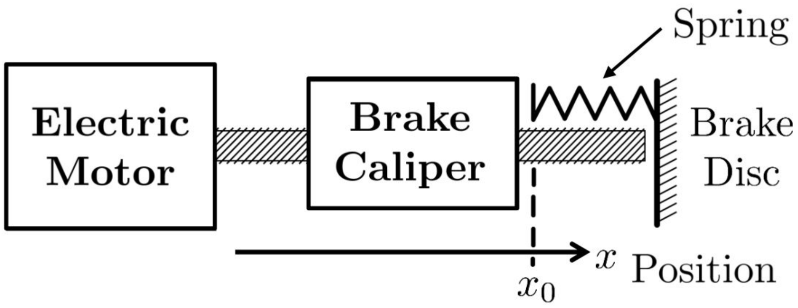
$$\boldsymbol{A}_l := ([-1.1, -1])$$

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

- ➔ Preliminaries
- ➔ Reachability with time-triggered events
- ➔ **Case study: Electromechanical break**
- ➔ Conclusions

Case study: Electromechanical break





- **Closed-loop system**: plant model and a discrete controller [SO15].
- Two source of uncertainty considered:
  - Variation in **model's parameters**.
  - **Sampling jitter** (i.e. nondeterministic switching of discrete PI controller).
- Set-based verification took **~13 hours** using the tool Flow*.

[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).

Hybrid Automaton with time-triggered transitions

Hybrid automaton model

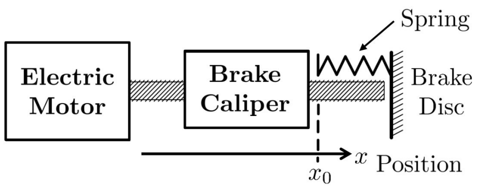
Nonlinear model → Linearized model with discrete controller →

$$
\begin{aligned}
\dot{I} &= \tfrac{1}{L}\cdot(K_P\cdot x_e \\
&\qquad +K_I\cdot x_c) \\
&\qquad -\tfrac{I}{L}\left(R+\tfrac{K^2}{d_{rot}}\right) \\
\dot{x} &= \tfrac{K}{i\cdot d_{rot}}\cdot I \\
\dot{x}_e &= 0 \\
\dot{x}_c &= 0 \\
\dot{T} &= 1
\end{aligned}
$$

$$T \le T_{sample} + \zeta$$

$$T \ge T_{sample} - \zeta$$

$$
\begin{aligned}
x'_e &:= x_0 - x \\
x'_c &:= x_c + T_{sample}\cdot(x_0 - x) \\
T' &:= T - T_{sample}
\end{aligned}
$$



- Several model parameters:
  - **Physical parameters** of the brake hardware.
  - Parameters of the **PI controller**.
- Controller **samples the distance x_0 - x** at multiples of the sampling time T_{sample}.
- **Sampling jitter** with periodic clock: discrete transitions enabled at **$[kT_{sample} + \zeta-, kT_{sample} + \zeta+]$ for k > 0.**

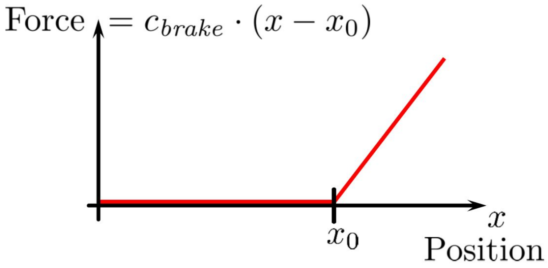
Model requirements

$$
\begin{aligned}
\dot{I} &= \frac{1}{L} \cdot \Big((K_P \cdot x_e + K_I \cdot x_c) - (R + \frac{K^2}{d_{rot}}) \cdot I \Big) \\
\dot{x} &= \frac{K}{i \cdot d_{rot}} \cdot I \\
\dot{x}_e &= 0 \\
\dot{x}_c &= 0 \\
\dot{T} &= 1
\end{aligned}
$$

$$T \leq T_{sample} + \zeta$$

$$T \geq T_{sample} - \zeta$$

$$
\begin{aligned}
x_e' &:= x_0 - x \\
x_c' &:= x_c + T_{sample} \cdot (x_0 - x) \\
T' &:= T - T_{sample}
\end{aligned}
$$



- **Maximum elapsed time** since the braking request until the caliper and the disk get in contact:

$$|x - x_0| \leq \varepsilon, \forall t \geq t_c$$

- The caliper's **velocity stays below** the value **v_r [mm/s]** upon contact ($t>t_c$).

Numerical evaluation

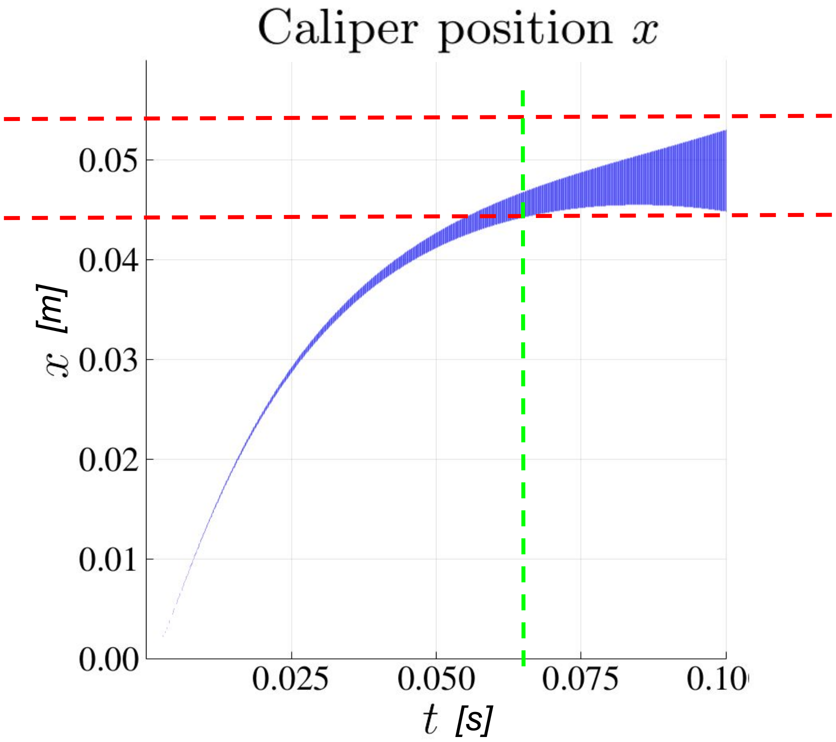
- We consider three settings:

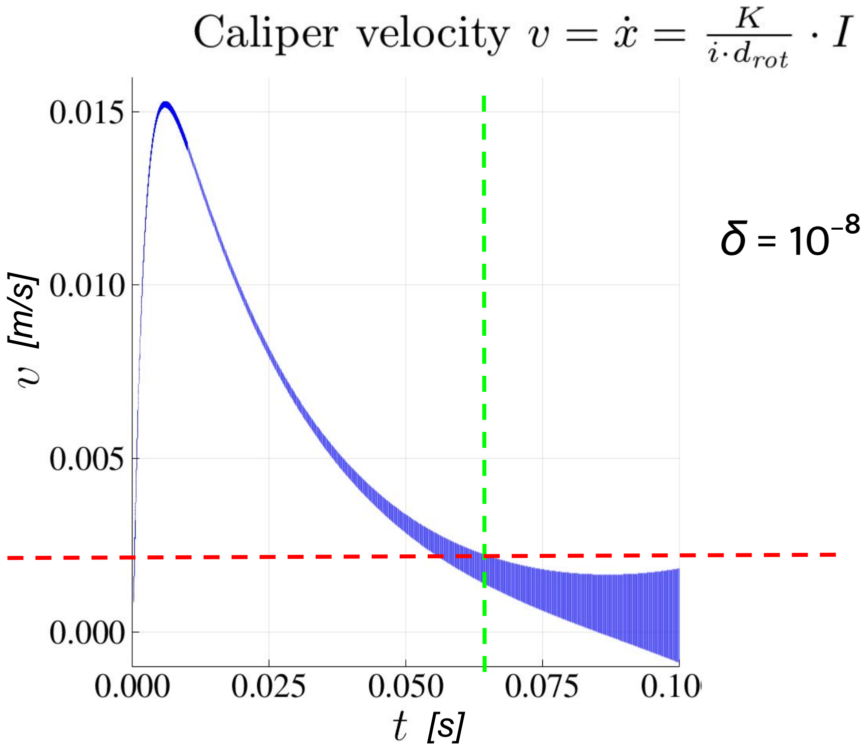
  1) **Fixed** parameters (case *no pv*).
  2) Parameter variation in one coefficient around **5%** of its nominal value (case *pv1*).
  3) Parameter variation in **all of the 7 physical parameters** of the model around 1% of their nominal value (case *pv2*).

- For each of the above cases we consider two scenarios: with and without **nondeterministic switches** (jitter) for comparison.

- If applicable we consider **different algorithm choices**.

Results





$\delta = 10^{-8}$ s

Scenario with **parameter variation** in one coefficient (*pv1*) and jitter $\zeta = [-10^{-8}; 10^{-7}]$ s

Results

ζ (y/n)	δ [s]	final diameter		time [s]	requirements		
		I	x ($\times 10^{-5}$)		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

- **Fixed** parameters
- **Parallelotope** set representation [GLGM06]
- Fixed time step $\delta = 10^{-9}$ s over 0.1s time span: **~100 million reach-sets**
- Scenarios with jitter use switching uncertainty **$\zeta = [-10^{-8}; 10^{-7}]$ s**

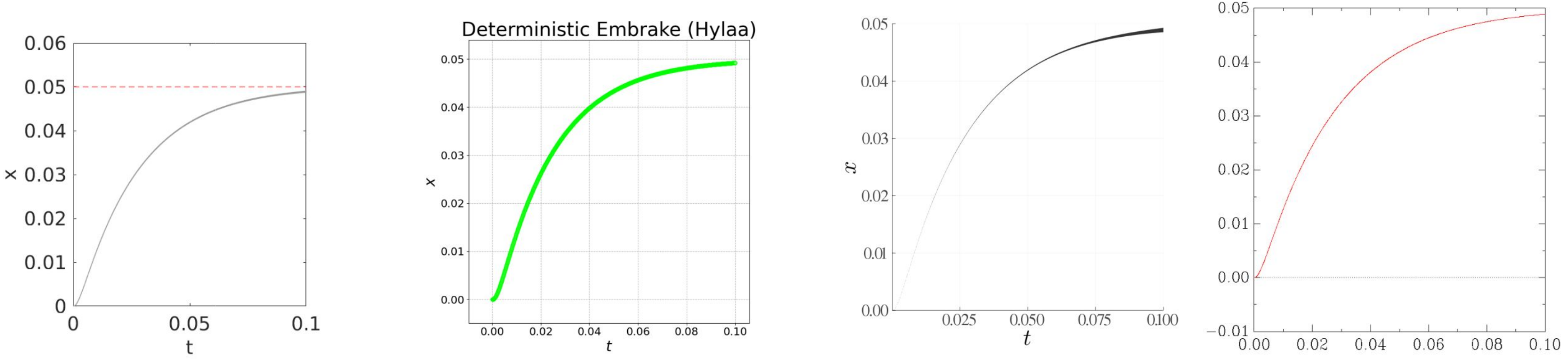
Results

case	ζ (y/n)	order	final diameter		time [s]	requirements		
			I	x $(\times 10^{-3})$		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	–	–	–

Computation time of *pv1* is **5000x faster** than previous attempts [SO15]

- Parameter **variation**
- **Reduced order zonotopes** set representation [ASB07]
- Fixed time step $\delta = 10^{-8}$ s over 0.1s time span: **~10 million reach-sets**
- Scenarios with jitter use switching uncertainty **ζ = [-10^{-8}; 10^{-7}] s**

Comparison with other tools



(a) CORA. (b) Hylaa (BRKDC01). (c) JuliaReach. (d) SpaceEx.

- Large number of **1001 discrete jumps** within the 0.1s time horizon.
- Null initial conditions, and we use x_0 = 0.05m, T_{sample} = 10^{-4}s.
- For the parametric instance, report the largest time horizon T_{max} such that $\mathbf{x < x_0}$ holds.

See Althoff, M., Bak, S., Bao, S., Forets, M., Frehse, G. Freire, D., Kochdumper, N., Li, Y., Mitra, S., Ray, R., Schilling, C., Schupp, S. and Wetzlinger, M. (2020). ARCH-COMP20 Category Report: Continuous and Hybrid Systems with Linear Continuous Dynamics. *EPiC Series in Computing*, *74*, 16-48.

Comparison with other tools

tool	BRKDC01	BRKNC01	BRKP01	language
CORA	4.84	427	496	MATLAB
HyDRA	–	–	–	C++
JuliaReach	0.82	0.99	12.2	Julia
SpaceEx	19.22	–	–	C++
XSpeed	–	–	–	C++
	discrete-time tools			
Hylaa	230	–	–	Python
JuliaReach	0.65	0.97	12.0	Julia

- **BRKDC01**: verify that **$x < x_0$ holds for T = 0.1s**. Fixed parameters, no jitter
- **BRKDC01**: Same as BRKDC01 but with non-deterministic switching **ζ = [-10^{-8}; 10^{-7}] s**
- **BRKNP01**: Same as *pv1* from [SO15]. With jitter and **parameter variation** in one coefficient

See Althoff, M., Bak, S., Bao, S., Forets, M., Frehse, G. Freire, D., Kochdumper, N., Li, Y., Mitra, S., Ray, R., Schilling, C., Schupp, S. and Wetzlinger, M. (2020). ARCH-COMP20 Category Report: Continuous and Hybrid Systems with Linear Continuous Dynamics. *EPiC Series in Computing*, *74*, 16-48.

- ➔ Preliminaries
- ➔ Reachability with time-triggered events
- ➔ Case study: Electromechanical break
- ➔ **Conclusions**

Conclusions

- Our work **unifies** existing conservative flowpipe approximation ideas to give rise to a method that **exceeds the prior state-of-the-art**.
- Decouple system into temporal and spatial variables: **make use of structure**.
- Events happening at **non-deterministic times** handled by **precomputing the transition times** effectively avoids flowpipe-guard intersections.
- Reachability algorithm for **parametric linear hybrid systems** with periodic controls, with uncertain parameters enclosed with **interval matrix maps** has **constant complexity w.r.t number of uncertain parameters**.

Conclusions

- Demonstration of our approach was made on an electro-mechanical brake model representative of real challenges in the **automotive industry** [SO15].
- **Highly efficient implementation** computes **~10 million successors** in less than one minute on a standard laptop for the case **with parameter variation** and **jitter**.
- Reduced runtimes allow engineers to introduce more **expressiveness** in their models with a relatively inexpensive computational cost (e.g. *pv2* scenario).

Perspectives

- Improving the **approximation quality** in the presence of jitter by elaborating the clustering strategy with higher-order zonotopes. Interplay of our framework with **nonlinear models.**

References

- [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).

- [ARCHCOMP2020] Althoff, M., Bak, S., Bao, S., Forets, M., Frehse, G. Freire, D., Kochdumper, N., Li, Y., Mitra, S., Ray, R., Schilling, C., Schupp, S. and Wetzlinger, M. (2020). ARCH-COMP20 Category Report: Continuous and Hybrid Systems with Linear Continuous Dynamics. *EPiC Series in Computing*, *74*, 16-48.

- [F16] Lecture Notes on *Formal Verification of Piecewise Affine Hybrid Systems* by G. Frehse from DigiCosme Spring School, May 12, 2016.

- [F11] Frehse, G., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., ... & Maler, O. (2011, July). *SpaceEx: Scalable verification of hybrid systems*. In International Conference on Computer Aided Verification (pp. 379-395). Springer, Berlin, Heidelberg.

- [GLGM06] Girard, A., Le Guernic, C., & Maler, O. (2006, March). *Efficient computation of reachable sets of linear time-invariant systems with inputs*. In International Workshop on Hybrid Systems: Computation and Control (pp. 257-271). Springer, Berlin, Heidelberg.

- [ASB07] M. Althoff, O. Stursberg, and M. Buss. *Reachability analysis of linear systems with uncertain parameters and inputs.* In Proc. of the 46th IEEE Conference on Decision and Control, pages 726–732, 2007.