Parametric Verification and Test Coverage for Hybrid Automata Using the Inverse Method

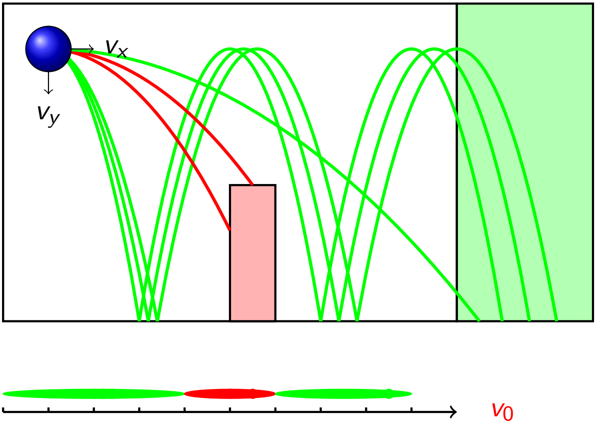
Laurent Fribourg[1] Ulrich Kühne[2]

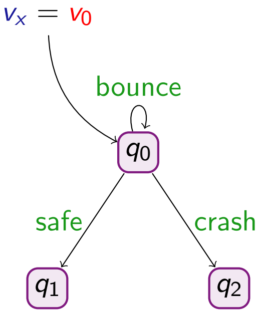
[1]LSV ENS de Cachan, CNRS

[2]University of Bremen

2011/10/28

A hybrid system



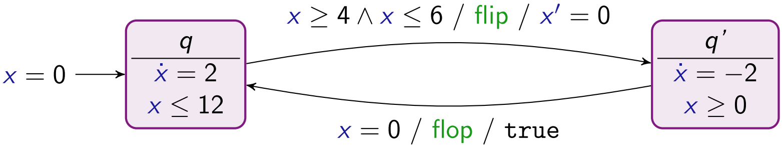


Hybrid Automata

Hybrid Automaton

$\mathcal{A} = (\Sigma, Q, q_0, I, D, \rightarrow)$ over a set of variables X, where

- actions Σ
- locations Q with initial location $q_0 \in Q$
- invariant I_q for each location q
- activity $D_q : \mathbb{R}^n \rightarrow \mathbb{R}^n$ for each location q
- discrete transitions $q \xrightarrow{g,a,\mu} q'$



Restriction: I_q, g, μ (and D_q) are linear convex constraints

Hybrid Automata

Concrete state

In a LHA, a concrete state is a pair (q, w) with a location q and a valuation w of the variables and parameters

Symbolic state

In a LHA, a symbolic state is a pair (q, C) with a location q and a constraint C on the variables and parameters

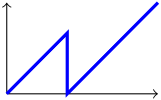
$$q_0 \xRightarrow{a_0} q_1 \xRightarrow{a_1} \cdots \xRightarrow{a_{n-1}} q_n$$

trace

Hybrid Automata

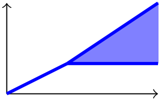
timed (TA)

q: $\dot{x} = 1$ $\xrightarrow{x = 4 \;/\; a \;/\; x' = 0}$ q': $\dot{x} = 1$



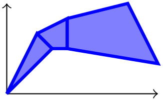
rectangular (RA)

q: $\dot{x} = 2$, $\dot{y} = 3$ $\xrightarrow{x = 4 \;/\; a \;/\; x' \leq 4}$ q': $\dot{x} = 1$, $\dot{y} \in [1, 2]$



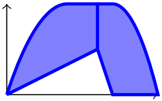
linear (LHA)

q: $\dot{x} = 2$, $\dot{y} \leq 2\dot{x}$ $\xrightarrow{x = 4 \;/\; a \;/\; x' \leq y}$ q': $\dot{x} + \dot{y} = 7$, $\dot{x} \in [1, 2]$



affine (AHA)

q: $\dot{x} = -x$, $\dot{y} = 0.4y$ $\xrightarrow{x = 4 \;/\; a \;/\; x' \leq y}$ q': $\dot{x} = 4y - 5$, $\dot{y} < x - \dot{x}$



Parameterized Hybrid Automata

Parameters

Given a HA $\mathcal{A}$ with variables X, we introduce *parameters* P with $P \cap X = \varnothing$. Given a constraint on the parameters K, in a parameterized HA $\mathcal{A}(K)$, *invariants*, *guards* and *jump predicates* can depend on parameters, but *not* the activities.

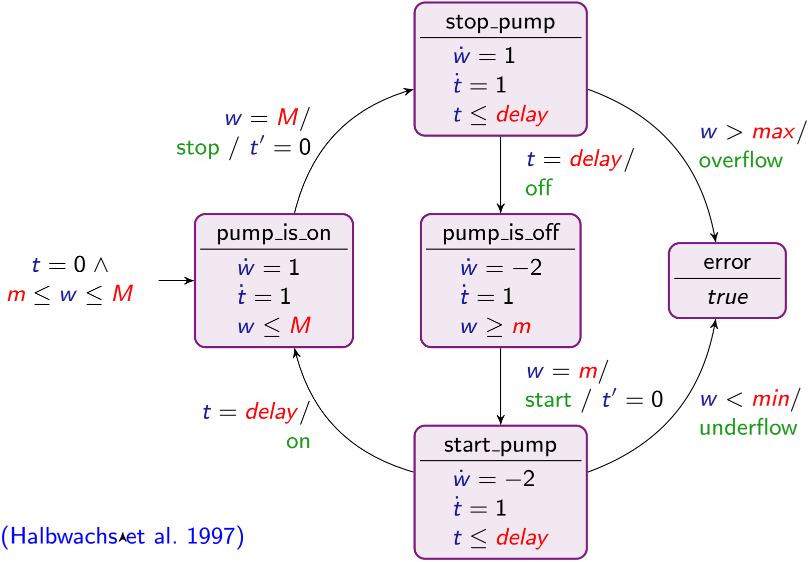
In the modeling and verification of hybrid systems, parameters can be used to model

- Unknown inputs
- Environment constraints
- System parameters to optimize

Valuation / instantiation

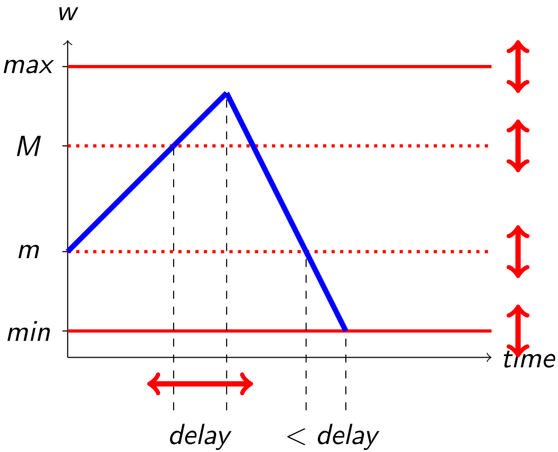
A parameter valuation is a function $\pi : P \to \mathbb{R}$. A complete valuation π turns a parameterized HA $\mathcal{A}(K)$ into a HA $\mathcal{A}[\pi]$.

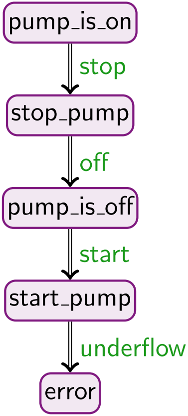
Example – water tank



(Halbwachs et al. 1997)

Example – water tank





- How to choose min, max, m, M and delay, such that always $min < w < max$?

Parametric verification and test coverage

Given HA $\mathcal{A}(K)$ with reachable states $Reach_{\mathcal{A}(K)}$ and a set of bad locations $\mathcal{B}$, consider the simple reachability (safety) property:

$\mathcal{S}_{\mathcal{B}}$: The reachable locations of $\mathcal{A}(K)$ and $\mathcal{B}$ are disjunct

Parameter synthesis

Given $\mathcal{B}$, compute all parameter valuations such that $\mathcal{S}_{\mathcal{B}}$ holds

Inverse problem

Given $\mathcal{B}$ and a valuation π_o such that $\mathcal{S}_{\mathcal{B}}$ holds for $\mathcal{A}[\pi_0]$, compute a constraint K_0 with $\pi_0 \models K_0$, such that for all valuations $\pi \models K_0$, $\mathcal{A}[\pi]$ has the same set of traces

Test coverage

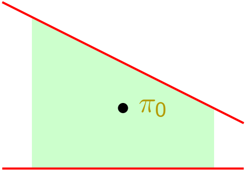
Given $\mathcal{A}(K)$, compute a (minimal) set of valuations V covering all admissible traces of $\mathcal{A}(K)$, such that for all $\pi_1, \pi_2 \in V$, the traces of $\mathcal{A}[\pi_1]$ and $\mathcal{A}[\pi_2]$ are distinct

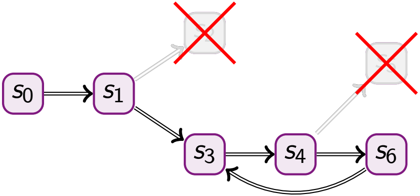
Related Work

- Parameter synthesis
  - Reachability and projection (Henzinger and Wong-Toi 1996)
  - CEGAR-based approach for LHA (Frehse et al. 2008)
- Inverse problem
  - Inverse Method for TA (André et al. 2009)
  - Behavioral Cartography for TA (André and Fribourg 2010)
- Test coverage
  - Robust test generation for hybrid systems (Julius et al. 2007)
  - Backward trace analysis for Simulink models (Alur et al. 2008)

$\Rightarrow$ **Here: adapt Inverse Method for HA**

The Inverse Method





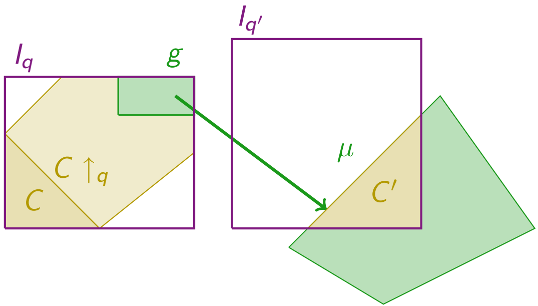
Inverse Method

- A state (q, C) is π_0-*incompatible*, if $\pi_0 \not\models C$
- During reachability, remove consecutively all π_0-incompatible states
- Accumulate negated incompatible terms in a constraint K_0

Behavioral Cartography

- Given a rectangular region V_0 of the parameter space, step sizes δ_i
- Repeat the Inverse method until all grid points are covered

Reachability of LHA



Forward-reachable states of a symbolic state $s = (q, C)$

- Operations on symbolic states $\triangleq$ *convex* polyhedra
- Compute the *time elapse* $s \uparrow_q$ wrt. activity D_q
- Compute the *discrete successor* wrt. transition $q \xrightarrow{g,a,\mu} q'$

The Inverse Method for LHA

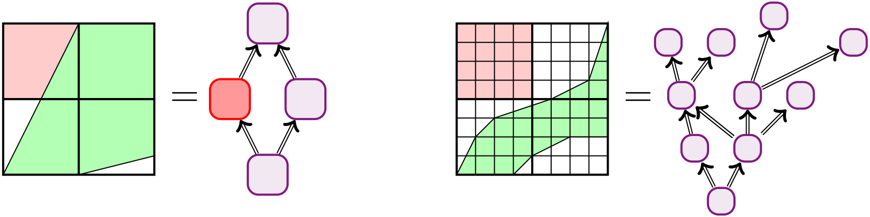
Observation

- Convexity is preserved during reachability
- Monotonicity holds: $(q, C) \overset{*}{\Rightarrow} (q', C') \quad \Rightarrow \quad C' \downarrow_P \subseteq \; C \downarrow_P$
- Inverse Method can be adapted straight forward for LHA

- But poor results for approximated affine systems

The Inverse Method for LHA

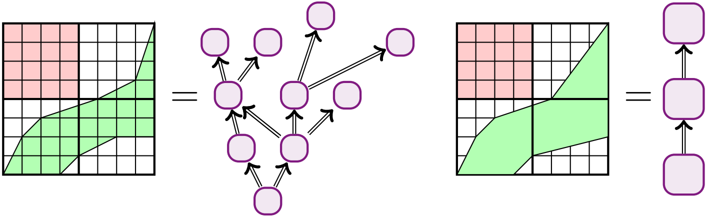
Application to a linearized affine system:



- Partitioning necessary to verify safety
- Fine grained partitioning leads to complex traces
- Small changes in parameters lead to different traces
- Constraints generated by IM are very small

Extended algorithm for affine dynamics

- Idea: Join states from neighboring partitions of the same location



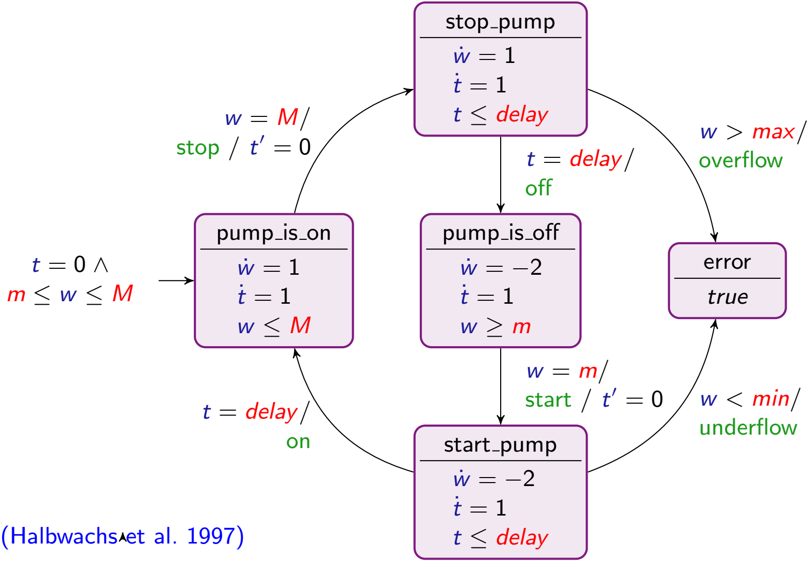
Enhanced reachability algorithm for affine HA

1. Build local partitions P of the invariant I_q
2. Compute a linear over-approximation $\hat{D}_P$ of D_q for each partition P
3. Compute the locally reachable states S wrt. partitions P and dynamics $\hat{D}_P$
4. Compute the convex hull of the states S

Extended algorithm for affine dynamics

- Advantages
  - Leads to less computed states
  - Produces simpler trace sets
  - IM can compute larger constraints
  - Can be as precise as fine grained linearization
- Disadvantages
  - Computational overhead for convex hull operation
  - Loss of precision by convex hull
- Implemented in *IMITATOR 3* (also known as *HyMITATOR*)
- Alpha version available at
  `www.lsv.ens-cachan.fr/Software/imitator`

Example – water tank



(Halbwachs et al. 1997)

Water tank – Inverse Method

Safety for the water tank

$\mathcal{S}$: The bad state $\mathcal{B} = \{error\}$ is not reachable

- Choose sufficient margins $|max - M|$ and $|m - min|$ and a short $delay$
- $\pi_0 = (min \mapsto 0, m \mapsto 10, M \mapsto 20, max \mapsto 30, delay \mapsto 1)$ works fine
- Can we do better?

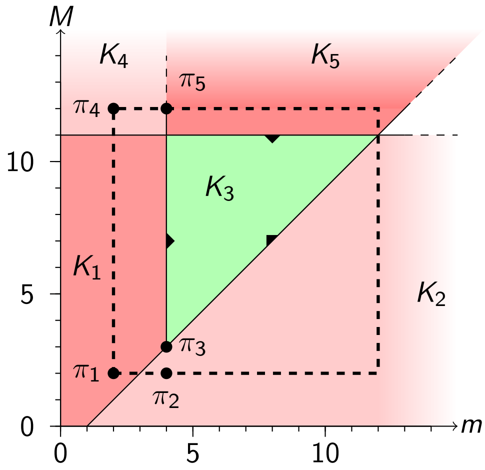
Inverse Method

$IM(\pi_0) : M + delay \geq m \ \wedge \ m \geq min + 2 \cdot delay \ \wedge \ max \geq M + delay$
guarantees the same trace set as π_0

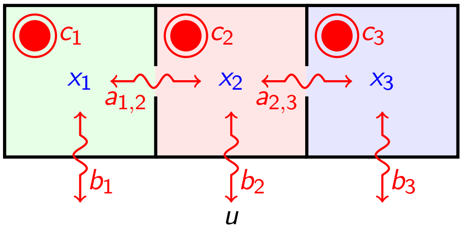
- Are there other good behaviors?

Water tank – Behavioral Cartography

Exploring the m, M-plane with min, max and $delay$ fixed as in π_0

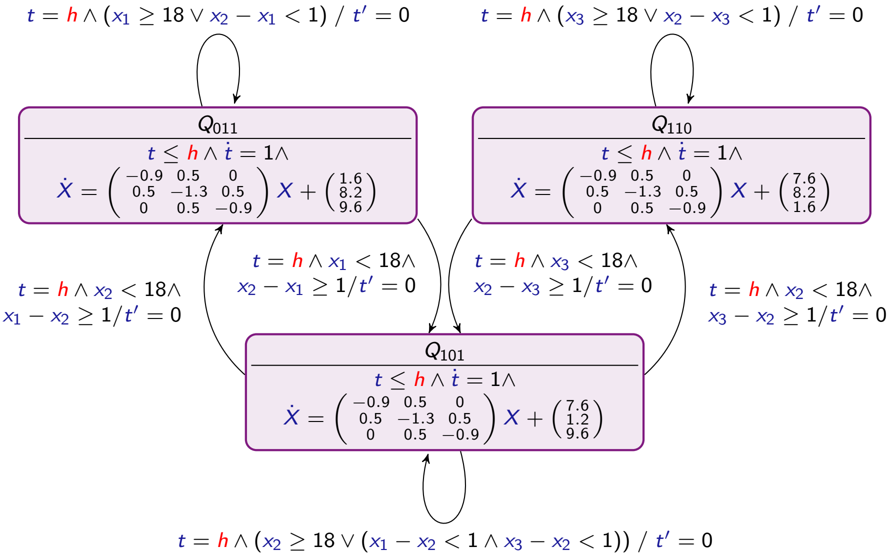


Application – room heating benchmark



- Hybrid system benchmark (Fehnker and Ivancic 2004)
- Two movable heaters in three adjacent rooms
- Temperature flow between rooms ($a_{i,j}$) and to the outside (b_i)
- Move heaters at difference (dif) and threshold (get) temperature
- Keep all rooms within temperature range $[min, max]$

Room heating benchmark – automaton



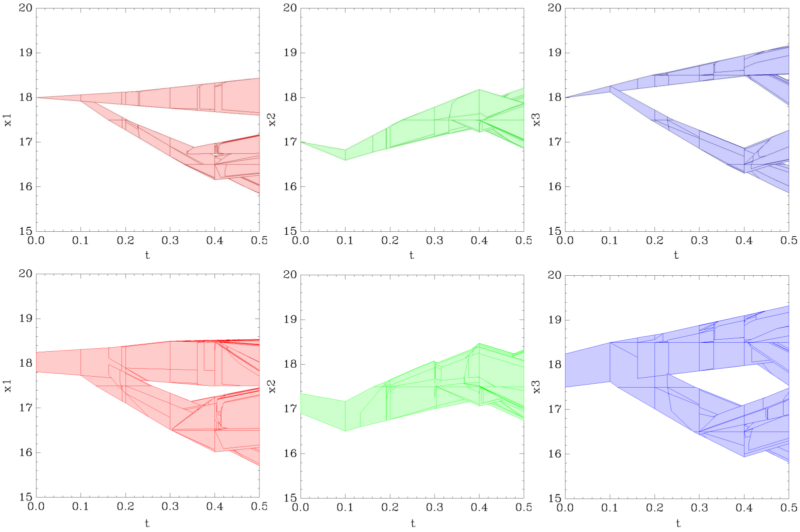
Room heating benchmark – overview

- Complex affine dynamics
- Eliminated some non-determinism using time discretization
- Parameters
  - Sample time h (fixed for experiments)
  - Initial temperatures a_1, a_2, a_3

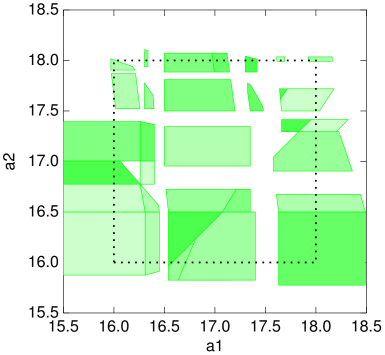
Bounded liveness

At least one of the heaters will be moved within a given time interval $[0, t_{max}]$ with $t_{max} = \frac{1}{2}$ $[hour]$ and a sample time of $h = 6$ $[minutes]$

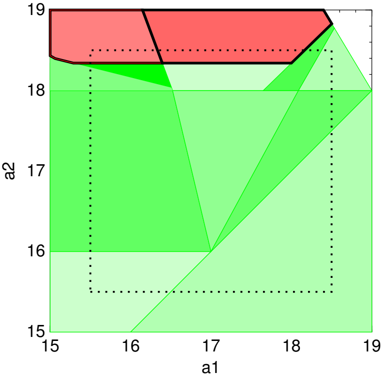
Room heating benchmark – Inverse Method



Room heating benchmark – test coverage



a) Statically linearized LHA, about 55% coverage



b) With enhanced algorithm, coarse linearization

Conclusions

- Adaptation of the Inverse Method for hybrid automata
- Extended algorithm for affine systems
- Application to parameter optimization
- Behavioral Cartography for test coverage
- Good results for LHA
- Mixed results for affine systems
  - High (and volatile) runtimes
  - Reachability for affine automata needs luck and artistry

References I

Alur, R., Kanade, A., Ramesh, S., & Shashidhar, K. (2008).
Symbolic analysis for improving simulation coverage of simulink/stateflow models.
In: *EMSOFT*, pages 89–98.

André, E., Chatain, T., Encrenaz, E., & Fribourg, L. (2009).
An inverse method for parametric timed automata.
IJFCS, 20(5):819–836.

André, E. & Fribourg, L. (2010).
Behavioral cartography of timed automata.
In: *RP*, volume 6227 of *LNCS*, pages 76–90. Springer.

Fehnker, A. & Ivancic, F. (2004).
Benchmarks for hybrid systems verification.
In: *HSCC*, pages 326–341. Springer.

References II

Frehse, G., Jha, S., & Krogh, B. (2008).
A counterexample-guided approach to parameter synthesis for linear hybrid automata.
In: *HSCC*, volume 4981 of *LNCS*.

Halbwachs, N., Proy, Y.-E., & Roumanoff, P. (1997).
Verification of real-time systems using linear relation analysis.
In: *Formal Methods In System Design*, pages 157–185.

Henzinger, T. & Wong-Toi, H. (1996).
Using HyTech to synthesize control parameters for a steam boiler.
In: *Formal Methods for Industrial Applications, Specifying and Programming the Steam Boiler Control*, pages 265–282. Springer.

Julius, A., Fainekos, G., Anand, M., Lee, I., & Pappas, G. (2007).
Robust test generation and coverage for hybrid systems.
In: *HSCC*, volume 4416 of *LNCS*.