Symbolic Computations in Hybrid Systems Verification

Why symbolic computations are required for hybrid systems analysis

André Platzer   Edmund M. Clarke

Carnegie Mellon University, Computer Science Department, Pittsburgh, PA

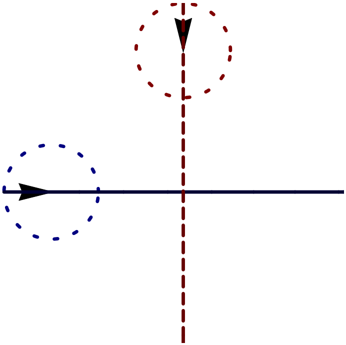
NSF Workshop on
Symbolic Computation for Constraint Satisfaction Problems
Arlington, VA 2008

Outline

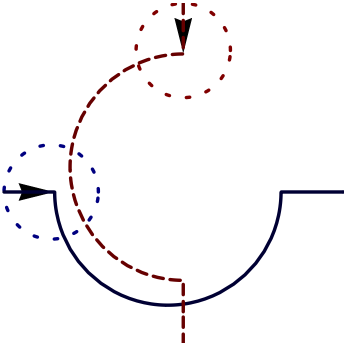
1. Motivation
   - Air Traffic Control
   - The Importance of Verification
   - Image Computation in Hybrid Systems
2. Approximation in Model Checking
   - Approximation Refinement Model Checking
   - Exact Image Computation: Polynomials and Beyond
   - Image Approximation
3. Flow Approximation
   - Bounded Flow Approximation
   - Continuous Image Computation
   - Probabilistic Model Checking
   - Differential Flow Approximation
4. Symbolic Differential Invariants
5. Case Studies
6. Conclusions and Future Work

Outline

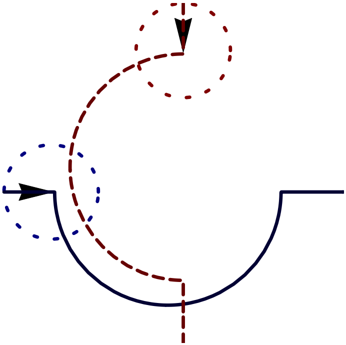
Air Traffic Control



Air Traffic Control



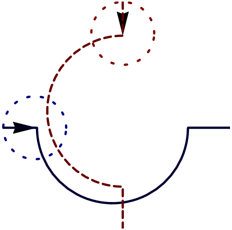
Air Traffic Control



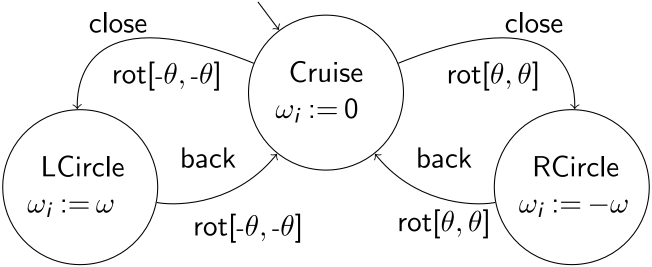
Hybrid Systems

continuous evolution along differential equations + discrete change

ATC: Roundabout Maneuver Automaton

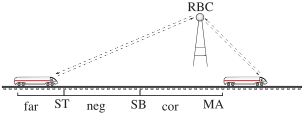


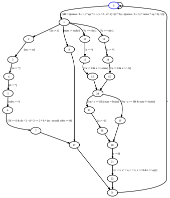
$$\begin{bmatrix} \dot{x} & = -v_1 & +v_2 \cos\phi & +\omega_1 y \\ \dot{y} & = & v_2 \sin\phi & -\omega_1 x \\ \dot{\phi} & = & \omega_2 & -\omega_1 \end{bmatrix}$$

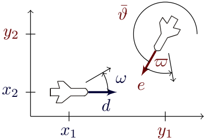


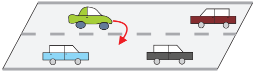
Details

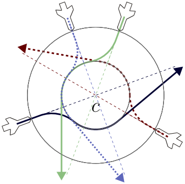
Hybrid Systems Verification is Important for . . .











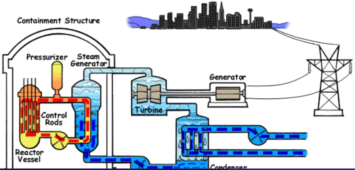
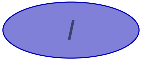
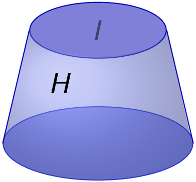


Image Computation in Hybrid Systems



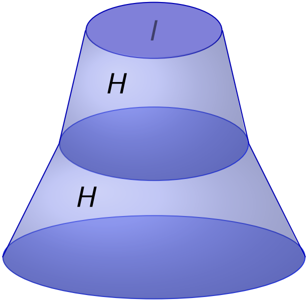
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



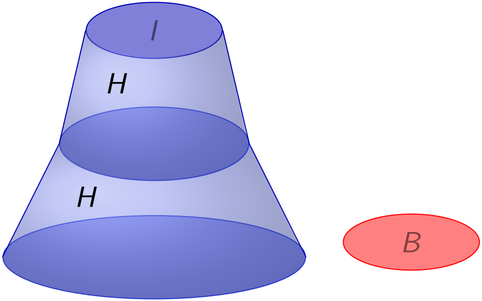
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



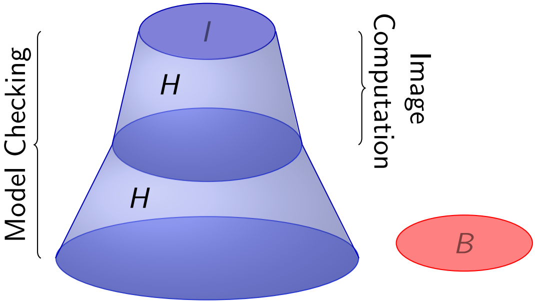
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



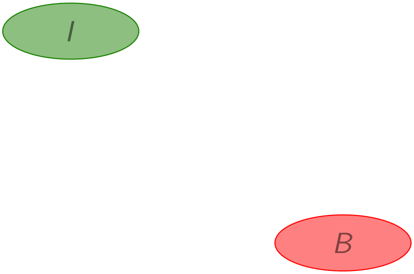
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Outline

AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

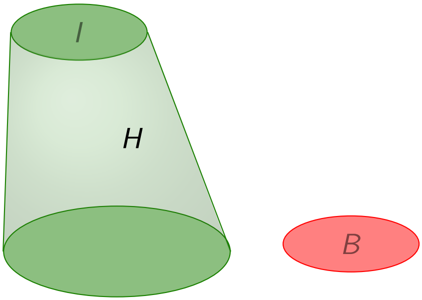
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

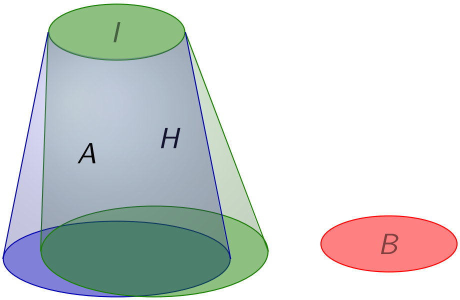
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

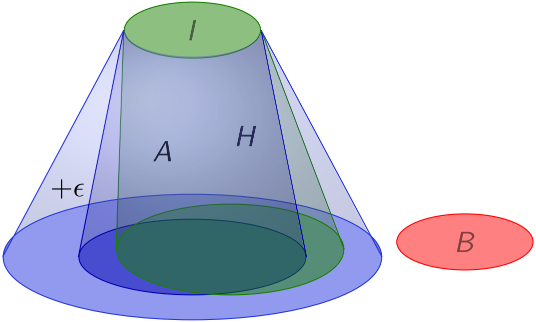
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

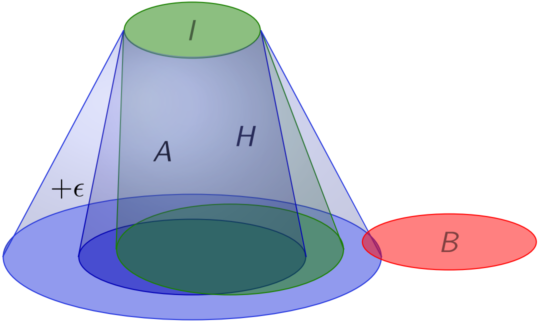
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

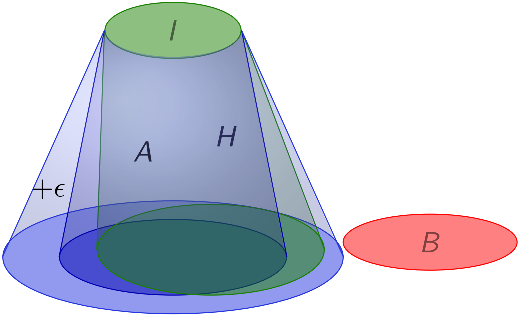
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Exact Image Computation

AMC(B reachable from I in H):

1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe

Proposition

check and blur can be implemented for

- *I and B semialgebraic*
- *A with polynomial flows over* $\mathbf{R}$
- *+Piecewise definitions*
- *+Rational extensions (e.g. multivariate rational splines)*

AMC: Image Approximation

AMC(B reachable from I in H):

1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe

Proposition

approx exists for all uniform errors $\epsilon > 0$ when

- *using polynomials to build A*
- *Flows $\varphi \in C(D, \mathbf{R}^n)$ of H*
- *$D \subset \mathbf{R} \times \mathbf{R}^n$ compact closure of an open set*

Outline

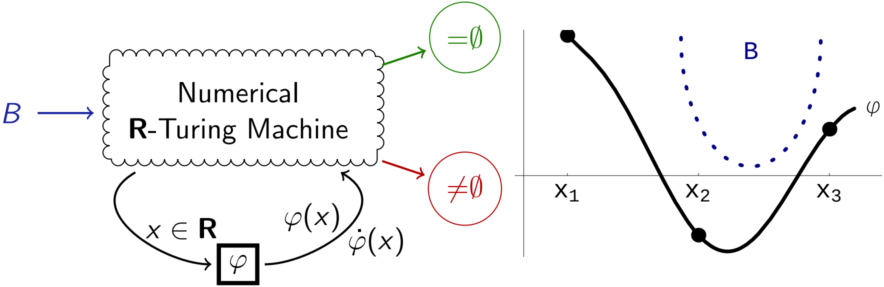
Bounded Flow Approximation

Proposition (Effective Weierstraß approximation)

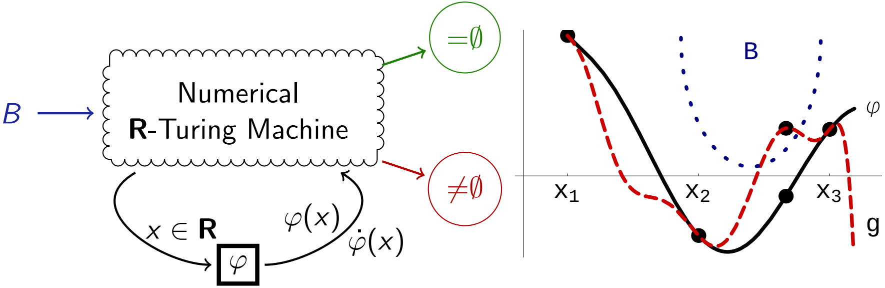
- *Flows* $\varphi \in C^1(D, \mathbf{R}^n)$
- *Bounds* $b := \max_{x \in D} \|\dot{\varphi}(x)\|$

$\Rightarrow$ *approx computable, hence image computation decidable*

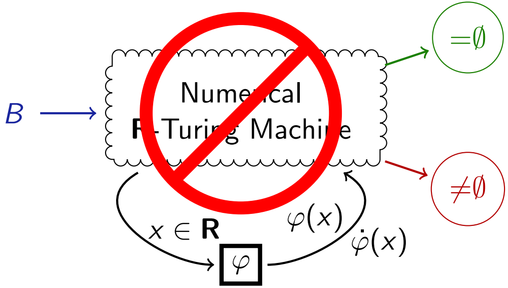
Continuous Image Computation

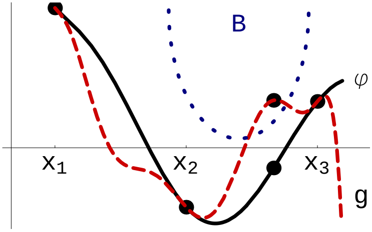


Continuous Image Computation



Continuous Image Computation

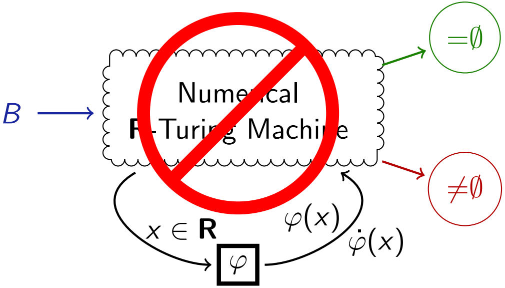


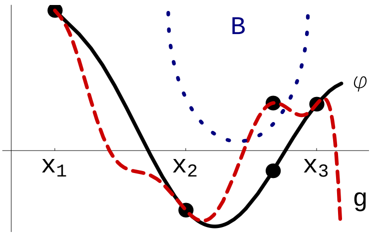


Proposition (Image computation undecidable for. . .)

- *arbitrarily effective flow* $\varphi \in C^k(D \subseteq \mathbf{R}^n, \mathbf{R}^m)$*; D, B effective*
- *tolerate error* $\epsilon > 0$ *in decisions*

Continuous Image Computation

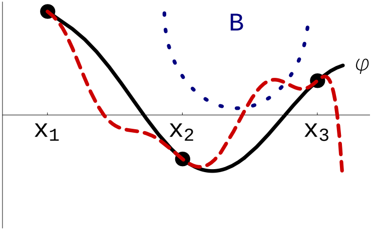




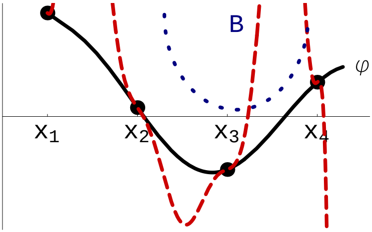
Proposition (Image computation undecidable for. . .)

- *arbitrarily effective flow* $\varphi \in C^k(D \subseteq \mathbf{R}^n, \mathbf{R}^m)$*; D, B effective*
- *tolerate error* $\epsilon > 0$ *in decisions*
- φ *smooth polynomial function with* $\mathbf{Q}$*-coefficients*

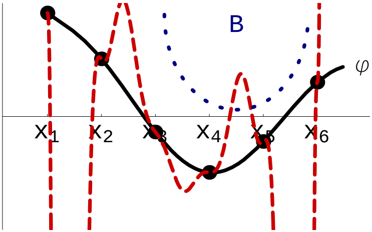
Probabilistic Model Checking



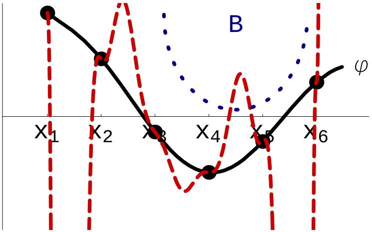
Probabilistic Model Checking



Probabilistic Model Checking



Probabilistic Model Checking

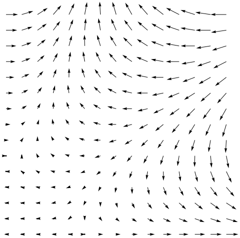


Proposition

- $P(\|\dot{\varphi}\|_\infty > b) \to 0$ *as* $b \to \infty$
- φ *evaluated on finite subset* $X = \{x_i\}$ *of open or compact* D

$\Rightarrow$ $P(\textit{decision correct}) \to 1$ *as* $\|d(\cdot, X)\|_\infty \to 0$

Differential Flow Approximation



φ solves
$\dot{x}(t) = f(t, x)$

Proposition

- *Flow* φ *is solution of* $\dot{x}(t) = f(t, x)$
- $f \in C([a, b] \times \mathbf{R}^n, \mathbf{R}^n)$
- ℓ*-Lipschitz-continuous:* $\|f(t, x_1) - f(t, x_2)\| \leq \ell \|x_1 - x_2\|$

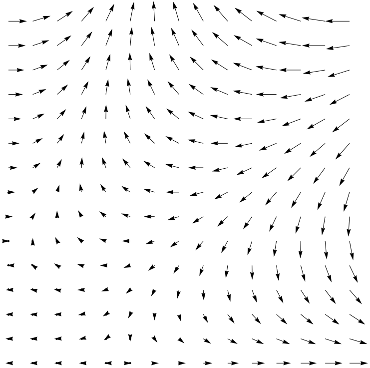
$\Rightarrow$ *Continuous image computation decidable*

Outline

Symbolic: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

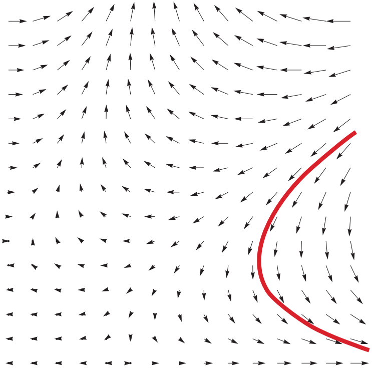
"Property that remains true in the direction of the dynamics"



Symbolic: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

"Property that remains true in the direction of the dynamics"

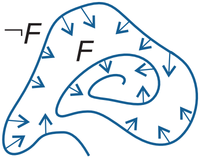


Symbolic: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

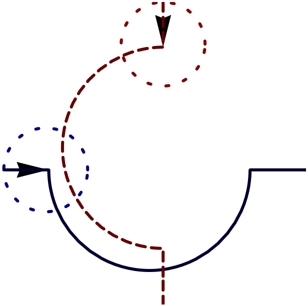
"Property that remains true in the direction of the dynamics"

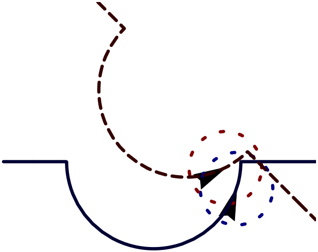
$$\nabla_{\dot{x}_1 = f_1(x), \ldots, \dot{x}_n = f_n(x)} F \quad \text{is} \quad \bigwedge_{(b \geq c) \in F} \left(\sum_{i=1}^{n} \frac{\partial b}{\partial x_i} f_i(x) \geq \sum_{i=1}^{n} \frac{\partial c}{\partial x_i} f_i(x) \right)$$

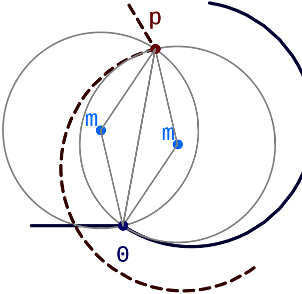


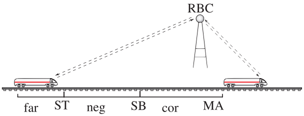
Outline

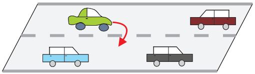
Case Studies

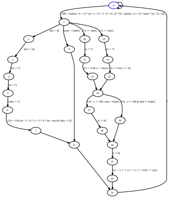












Outline

Conclusions

- Image computation in hybrid systems model checking
  1. approx uniformly
  2. blur by uniform error
  3. check for B

flows	approx / image computation
continuous	uniform approx exists, but...
smooth	undecidable numerically
bounded by b	decidable
bound probabilities	probabilistically decidable
ODE ℓ-Lipschitz	decidable

- Differential invariants:
  1. based on symbolic computations
  2. sound!
  3. scalable

Challenges

- Symbolic computation techniques for hybrid systems are strictly required!
- Scaling symbolic computation to nontrivial dynamics
- Combine numerical algorithms with symbolic analysis
- Joint symbolic stochastic analysis

A. Platzer and E. M. Clarke.
The image computation problem in hybrid systems model checking.
In A. Bemporad, A. Bicchi, and G. Buttazzo, editor, *HSCC*, 2007.

A. Platzer and E. M. Clarke.
Computing differential invariants of hybrid systems as fixedpoints.
In A. Gupta and S.Malik, editor, *CAV*, 2008.