Proving Abstractions of Dynamical Systems

Using Numerical Simulations

Sayan Mitra

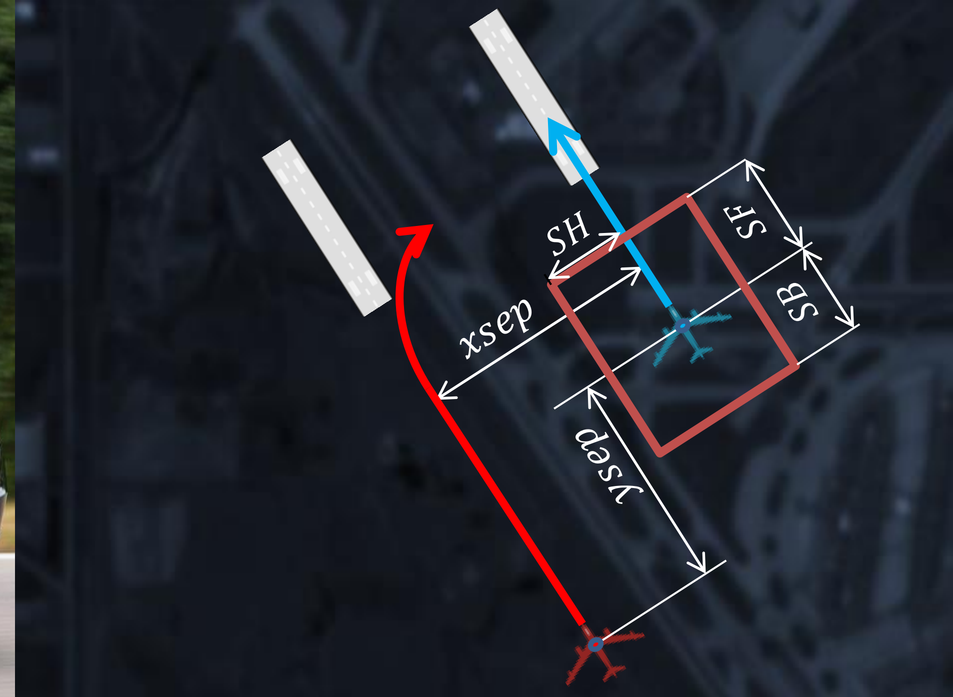
mitras@Illinois.edu

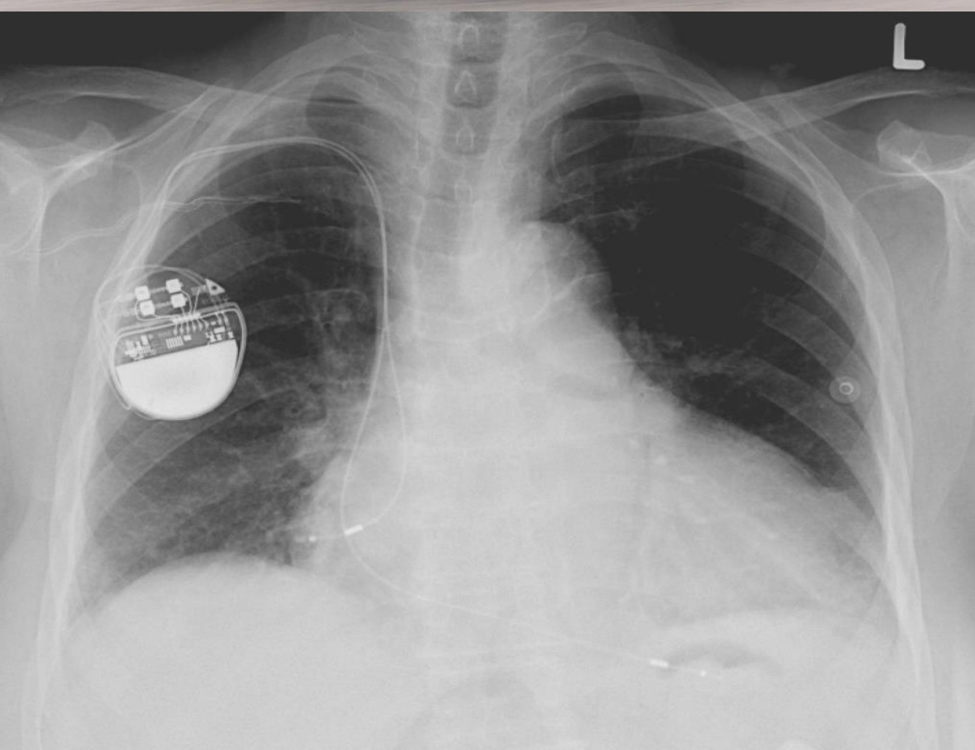
Department of Electrical and Computer Engineering

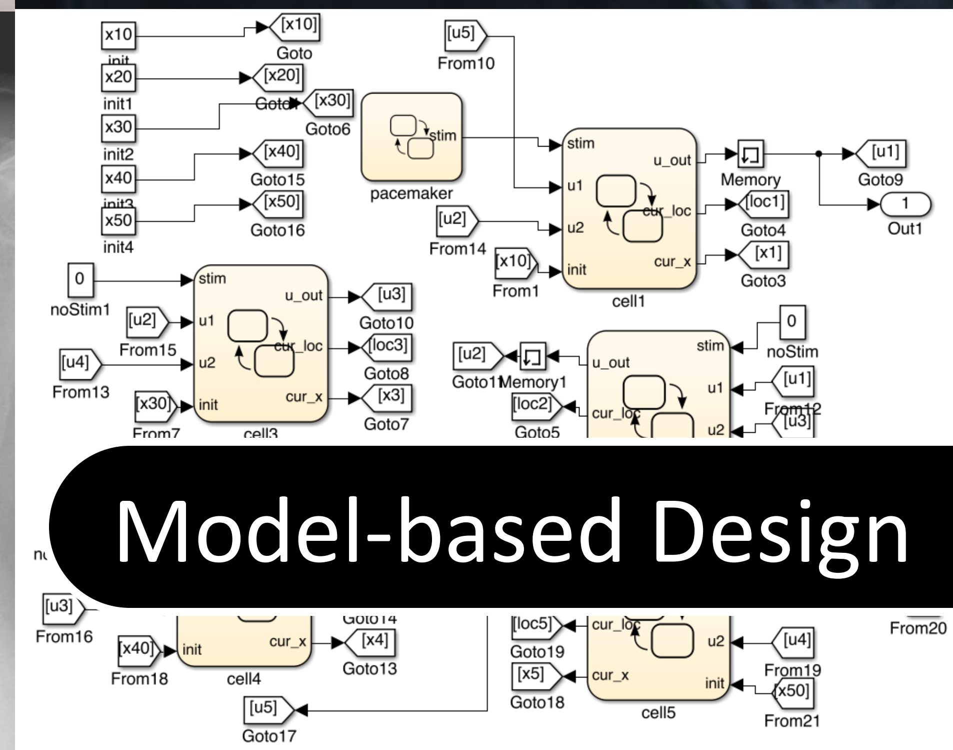
University of Illinois at Urbana Champaign

April 9th 2014

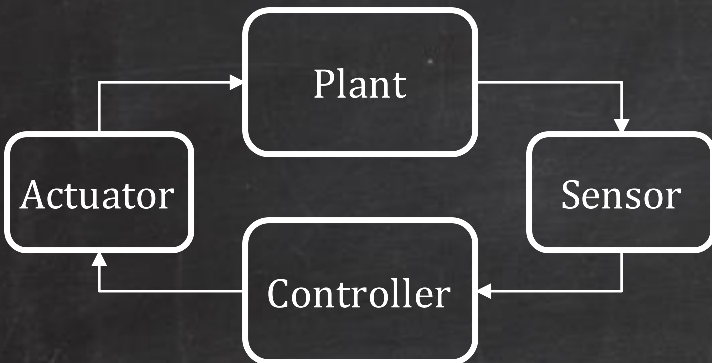

Autonomy
S 500 INTELLIGENT DRIVE
BB BF 2013


SH
SF
SB
xsep
ysep

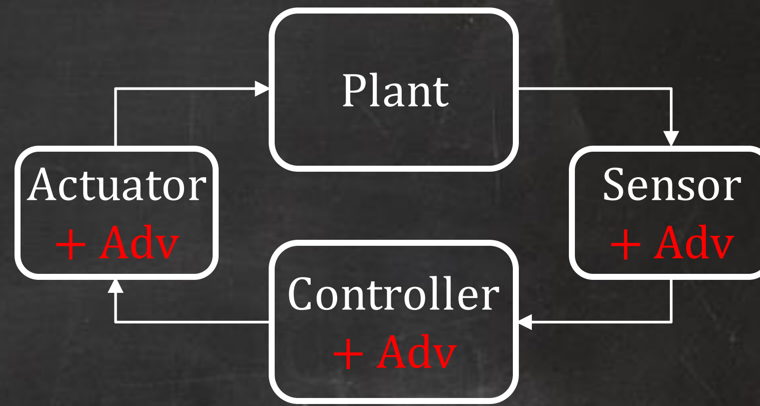

L


Model-based Design
x10
init
[x10]
Goto
x20
init1
[x20]
x30
init2
[x30]
Goto6
x40
[x40]
Goto15
x50
init4
[x50]
Goto16
[u5]
From10
pacemaker
stim
cell1
u_out
u1
u2
cur_loc
init
cur_x
Memory
[u1]
Goto9
1
Out1
[loc1]
Goto4
[x1]
Goto3
[u2]
From14
[x10]
From1
0
noStim1
From15
[u4]
From13
[x30]
cell3
[u3]
Goto10
[loc3]
Goto8
[x3]
Goto7
Goto11
Memory1
[loc2]
Goto5
noStim
From12
From16
[x40]
From18
cell4
[x4]
Goto13
[loc5]
Goto19
[x5]
Goto18
[u5]
Goto17
cell5
From19
[x50]
From21
From20

System Models and Attacks



$\mathrm{A}, \mathrm{Execs}_{\mathrm{A}}$

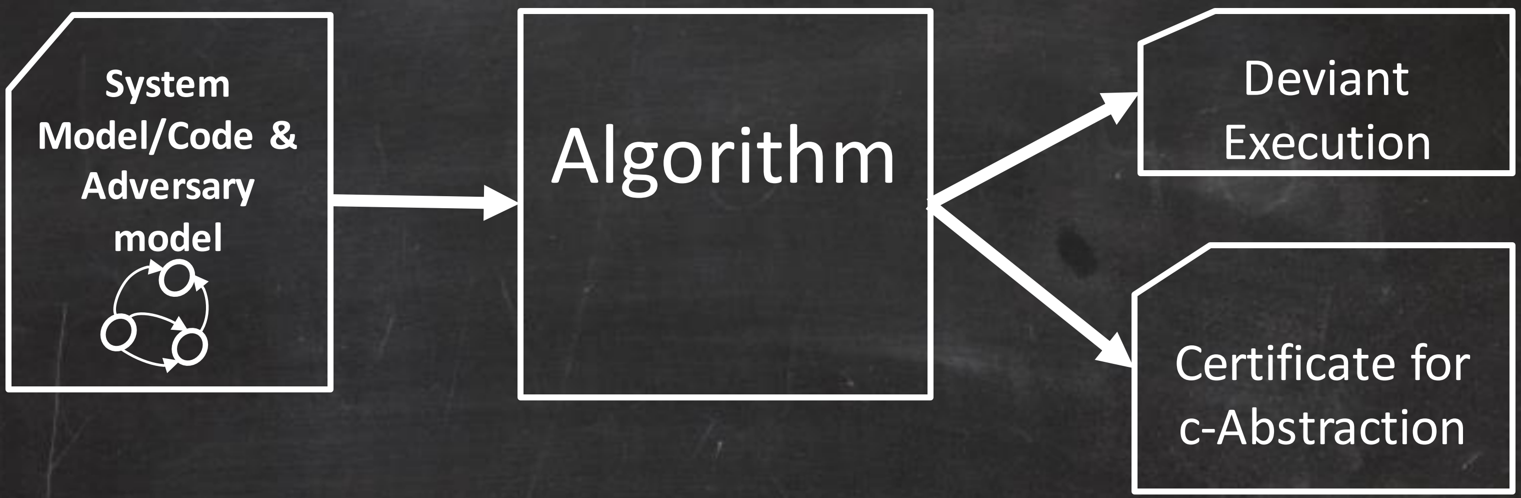


$\mathrm{A(Adv)}, \mathrm{Execs}_{\mathrm{A(Adv)}}$

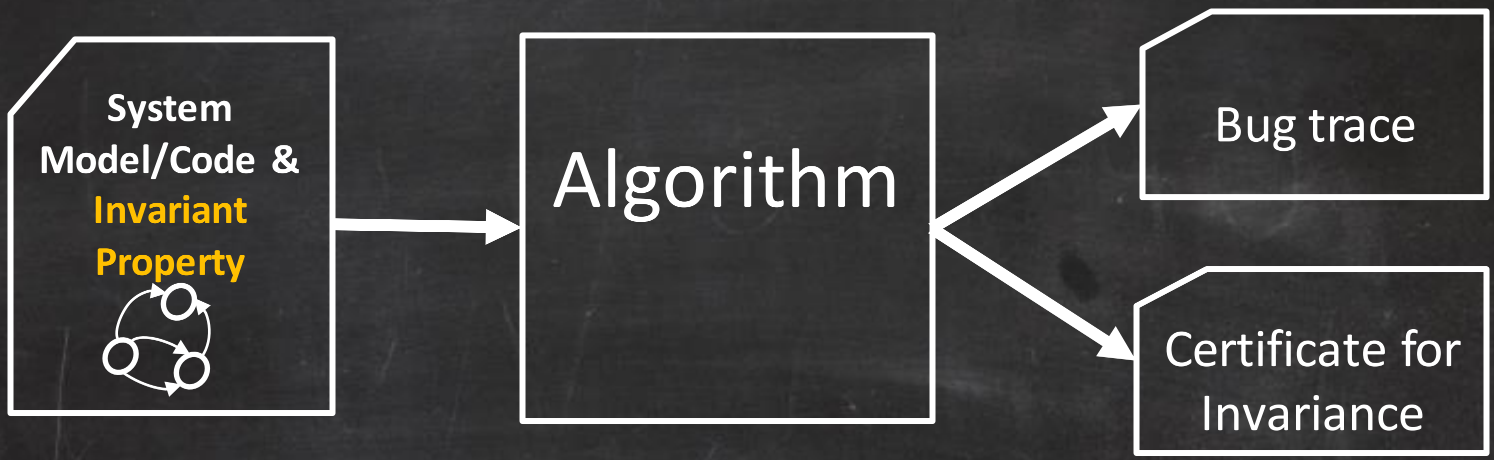
Q1: How much does Adv compromise X of A ?
X = availability, safety, …

d: Metric on executions
Q2: $\mathrm{d}\left(\mathrm{Execs}_{\mathrm{A(Adv)}}, \mathrm{Execs}_{\mathrm{A}}\right) \leq \mathrm{c}$?
Every behavior of $A(Adv)$ is **close** to some behavior of A

Abstraction Verification Decision Problem



Invariant Verification Problem



Duggirala, Huang, Mitra, Viswanathan:
EMSOFT 2013, HSCC 2014, FM 2014

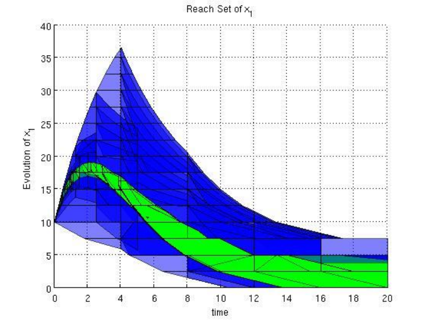
Nonlinear Models

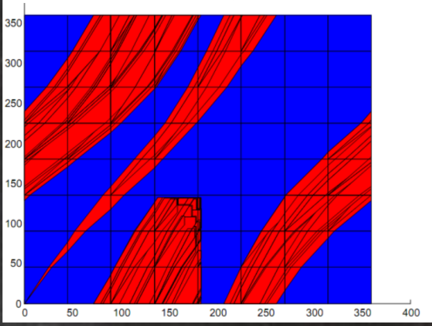
- Dynamics $\dot{x}(t) = f\big(x(t)\big)$
- Initial state $\Theta \subseteq R^n$
- Execution: $\xi: R^n \times R_{\geq 0} \rightarrow R^n, \xi(x(0), t) \in R^n$
- Output map: $g: R^n \rightarrow R^m,\ g(\xi(x(0), t))$

Bounded Safety Property

- Bounded safety (U, T_b): $\forall t \leq T_b, x(0) \in \Theta, \xi(x(0, t) \notin U$

Hybrid Verification





Early 90's: Exactly compute unbounded time reach set

– Decidable for timed automata [Alur Dill 92]
– Undecidable even for rectangular dynamics [Henzinger 95]

Late 90's: Approximate bounded time reach set

– Polytopes [Henzinger 97], ellipsoids [Kurzhanski] zonotopes [Girard 05], support functions [Frehse 08]
– Predicate abstraction [Alur 03], CEGAR [Clarke 03] [Mitra 13]
– Hamilton-Jacobi-Bellman approach [Tomlin et al. 02]

Current research: Scalable approximations

– Simulation-based methods [Julius 02] [Mitra 10-13][Donze 07]

Our Algorithms: Static-Dynamic Analysis

Validated Simulation Data

+

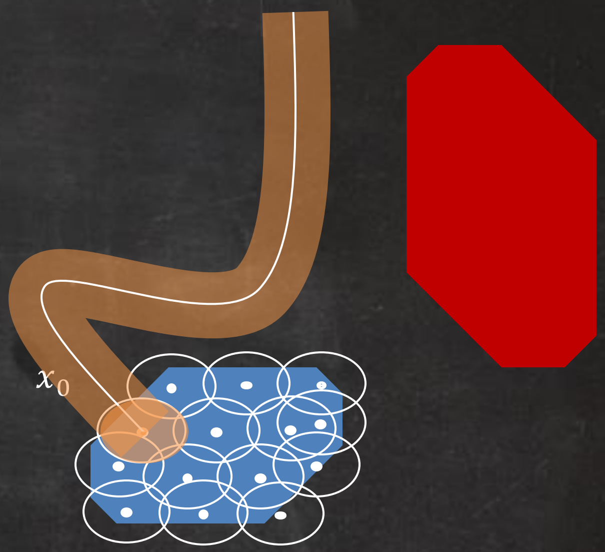
Static Annotations (Discrepancy)

=

Sound, Complete & Scalable
Verification of Robust Properties

Algorithm Sketch for Invariant Verification

- Given initial set  and unsafe set 
- Compute finite cover of initial set
- Simulate from the center x_0 of each cover
- **Bloat** simulation so that bloated tube contains all trajectories from the cover
- Union = over-approximation of reach set
- Check intersection with unsafe set



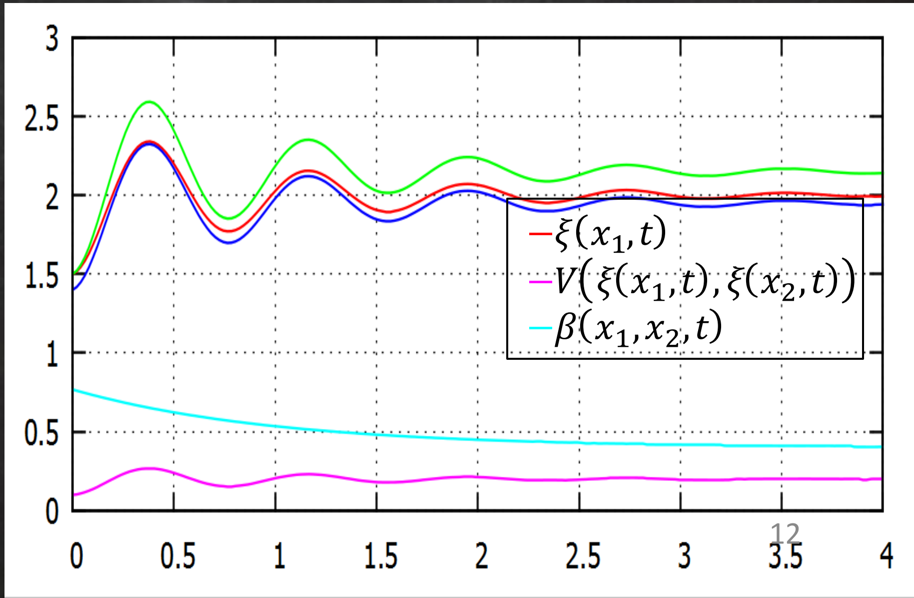
- How much to bloat?
- How to get completeness?

Discrepancy

Definition. Functions $V: X \times X \rightarrow \mathbb{R}^{\geq 0}$ and $\beta: \mathbb{R}^{\geq 0} \times T \rightarrow \mathbb{R}^{\geq 0}$ define a discrepancy of the system if for any two states x_1 and $x_2 \in X$

1. $V(x_1, x_2) = 0 \Leftrightarrow x_1 = x_2$
2. For any t, $V(\xi(x_1, t), \xi(x_2, t)) \leq \beta(|x_1 - x_2|, t)$ and $\beta \rightarrow 0$ as $x_1 \rightarrow x_2$

- Stability not required



Lipschitz Constant

Proposition 1. If L is a Lipschitz constant for *f(x,t)* then $V\big(\xi(x_1, t), \xi(x_2, t)\big) \leq e^{Lt}|x_1 - x_2|$.

Contraction Metrics

Theorem [Lohmiller & Slotine '98]. A positive definite matrix M is a **contraction metric** if there is a constant $b_M > 0$ such that the Jacobian *J* of *f satisfies:*

$$J^T M + M\, J + b_M M \preccurlyeq 0.$$

If *M* is a contraction metric then $\exists k, \delta > 0$ such that $|\xi(x, t) -$

Algorithm Sketch for Invariants

$Init \leftarrow \Theta$

While $Init \neq \emptyset$

$\{x_j\} \leftarrow Cover(\delta, Init)$

$sim[x_j] \leftarrow Simulate(A, x_i, \epsilon, \tau, T)$

$tube[x_j] \leftarrow Bloat\left(sim[x_j], \max_{t \in [0,T]} \beta(\delta, t)\right)$

If $tube[x_j] \cap U = \emptyset$

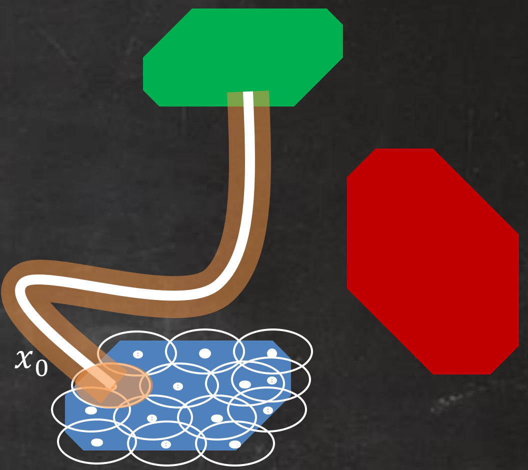
$Init \leftarrow Init \setminus B_\delta(x_j)$

Elsif some segment of $tube[x_j] \subseteq U$

Return COUNTER-EXAMPLE x_j

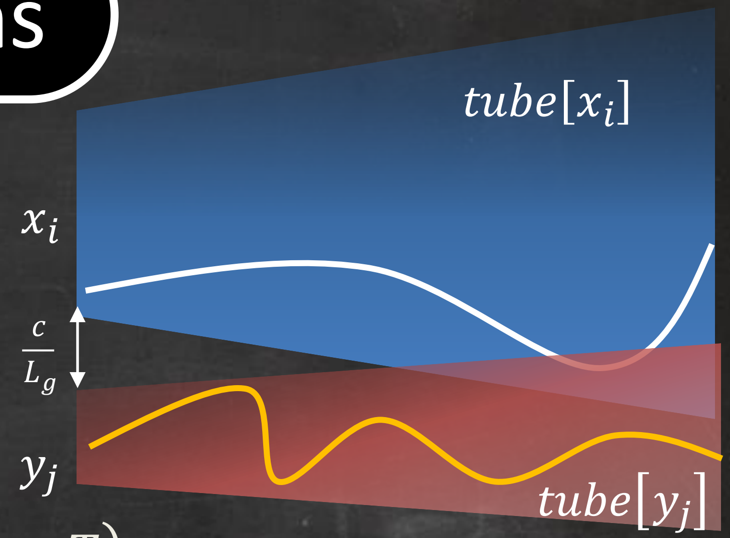
Else $\delta \leftarrow \frac{\delta}{2}; \tau \leftarrow \frac{\tau}{2}; \epsilon \leftarrow \frac{\epsilon}{2}$

Return SAFE



EMSOFT 2013, HSCC 2014, FM 2014

Algorithm for Abstractions



$Init \leftarrow \Theta_A$

While $Init \neq \emptyset$

$\{x_j\} \leftarrow Cover(\delta, Init)$

$\{y_j\} \leftarrow Cover(\delta, \Theta_B)$

For each x_i, y_j

$tube[x_j] \leftarrow SimBloat(sim[x_j], V_A, \delta, \epsilon, \tau, T)$

$tube[y_j] \leftarrow SimBloat(sim[y_j], V_B, \delta, \epsilon, \tau, T)$

For each x_i

If $\exists y_j\ d_H(tube[x_i], tube[y_j]) \leq \frac{c}{L_g} \wedge dia(tube[x_i]) \leq \frac{c}{2L_g} \wedge dia(tube[y_j]) \leq \frac{c}{2Lg}$

$Init \leftarrow Init \setminus B_\delta(x_i)$

Elsif $\forall\ y_j\ \ d_H(tube[x_i], tube[y_j]) \geq \frac{c}{S_g} \wedge dia(tube[x_i]) \leq \frac{c}{2S_g}$

Return COUNTER EXAMPLE x_i

Else $\delta \leftarrow \frac{\delta}{2}; \tau \leftarrow \frac{\tau}{2}; \epsilon \leftarrow \frac{\epsilon}{2}$

Return c-ABSTRACTION

Sound & Complete

Theorem. Whenever algorithm terminates with answer (c-Abstraction/Counter example), the answer is correct.

Theorem. The algorithm terminates either if B is at least a $\frac{c}{2}$-abstraction of A or if there exists a trace of A which is at least $2c$ distance away from all traces of B.

Conclusions and Ongoing Work

- (Simulation) **Data** + (some information about) **Model**

  Sound, Precise and **Scalable Analysis**
  - Scalable invariant verification
  - Checking abstraction relation (Scalable?)
- Applications: Systems with **Software** + **Physics**
  - Alerting protocol, fault-tolerance mechanisms, run-time safety assurance, engine control, aircraft power system
- Ongoing: **Experiments, Adversary Models & Symbolic Simulations**