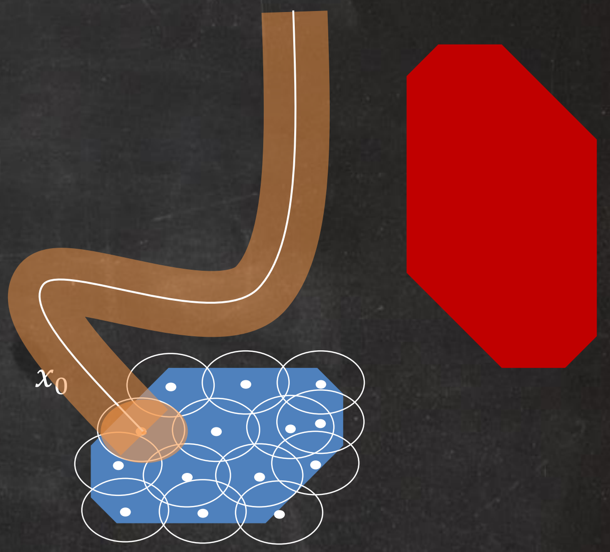
SIMULATION TO PROOFS IN C2E2

Parasara Sridhar Duggirala

A simple (often the only) strategy

- Given start S and target T
- 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/containment with T
- Refine



[Girard et al 2006],
[Donze et al 2008],...
(obviously incomplete)

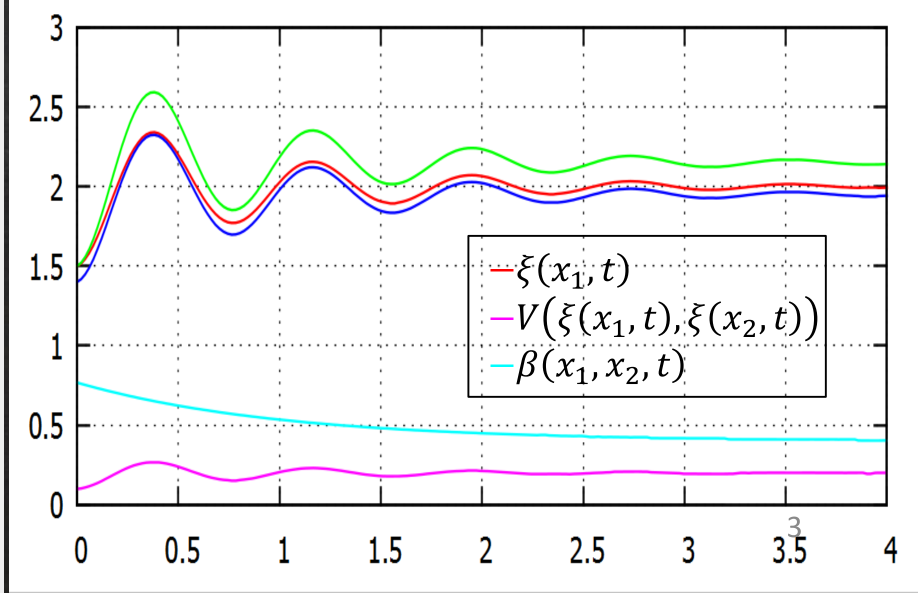
- How much to bloat?
- How to handle mode switches?

Discrepancy (Spirit of Loop Invariants)

Definition. $\beta: \mathbb{R}^{2n} \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ defines a discrepancy of the system if for any two states x_1 and $x_2 \in X$, For any t,

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

$x := 0$
invariant $x \leq 10$
until $x \geq 10$
do
    $x := x + 1$
od



Computing Discrepancy

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

If $\dot{x} = Ax$ Lyapunov function $x^T Mx$ that proves exponenial stability, then $|\xi(x_1, t) - \xi(x_2, t)| \leq Ke^{\gamma t}|x_1 - x_2|$ where $K = Func(M)$

Similar observation by [Deng et al 2013]

What about Nonlinear Systems?

Computing Discrepancy

If *M* is a contraction metric, that is, a positive definite matrix such that $\exists b_M > 0{:}\ J^T M + M J + b_M M \preccurlyeq 0$, *where J is the Jacobian for f*, then $\exists k, \delta > 0$ such that $|\xi(x,t) - \xi(x',t)|^2 \leq k|x - x'|^2 e^{-\delta t}$ [Lohmiller & Slotine '98].

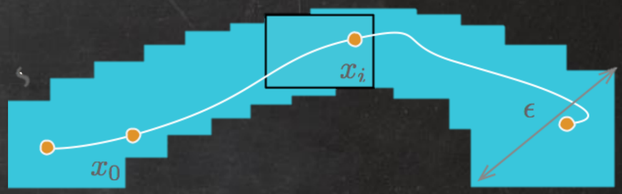
New algorithm: computes local discrepancy by estimating maximum eigenvalue of the Jacobian matrix over a neighborhood [Fan & Mitra 2014].

Inferring Contraction Metric from simulations [Balkan et al 2014]

What next?

Simulations+Annotation → Reachtubes

simulation$(\boldsymbol{x_0}, \boldsymbol{h}, \boldsymbol{\epsilon}, \boldsymbol{T})$ of gives a sequence $S_0, \ldots, S_k$: $dia(S_i) \leq \epsilon$ & at any time $t \in [ih, (i+1)h]$, solution $\xi(x_0, t) \in S_i$.



reachtube$(\boldsymbol{S}, \boldsymbol{\epsilon}, \boldsymbol{T})$ of $\dot{x} = f(x)$ is a sequence $R_0, \ldots, R_k$ such that $dia(R_i) \leq \epsilon$ and from any $x_0 \in S$, for each time $t \in [ih, (i+1)h]$, $\xi(x_0, t) \in R_i$.

$\langle S_0, \ldots, S_k, \epsilon_1 \rangle \leftarrow valSim(x_0, T, f)$

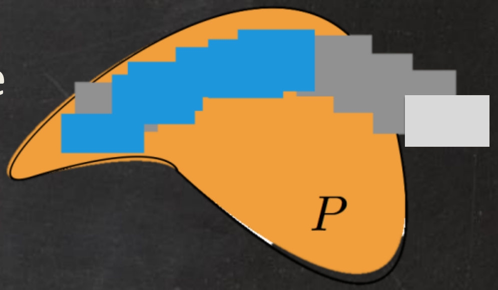
For each $i \in [k]$

$$\epsilon_2 \leftarrow \sup_{t \in T_i, x, x' \in B_\delta(x_0)} \beta(x_1, x_2, t)$$

$$R_i \leftarrow B_{\epsilon_2}(S_i)$$

How to get completeness for hybrid systems?

Track & propagate may and $must$ fragments of reachtube



$$\boldsymbol{tagRegion}(\boldsymbol{R},\boldsymbol{P}) = \begin{cases} must & R \subseteq P \\ may & R \cap P \neq \emptyset \\ not & R \cap P = \emptyset \end{cases}$$

$\boldsymbol{invariantPrefix}(\boldsymbol{\psi},\boldsymbol{S}) =$

$\langle R_0, tag_0, \ldots, R_m, tag_m \rangle$, such that either

$tag_i = must$ if all the $R_j's$ before it are must

$tag_i = may$ if all the $R_j's$ before it are at least may and at least one of them is not must

Hybrid Reachtubes: Guards & Resets

$\boldsymbol{nextRegions(\varphi)}$ returns a set of tagged regions N.
$\langle R', tag' \rangle \in N$ iff $\exists\ a, R_i$ such that $R' = Reset_a(R_i)$ and:

$R_i \subseteq Guard_a, tag_i = tag' = must$

$R_i \cap Guard_a \neq \emptyset, R_i \notin Guard_a, tag_i = must, tag' = may$

$R_i \cap Guard_a \neq \emptyset, tag_i = tag' = may$

Sound & Relatively Complete

Theorem. (Soundness). If Algorithm returns safe or unsafe, then A is safe or unsafe.

Definition Given HA $A\ = \langle V, Loc, A, D, T\ \rangle$, an **$\epsilon$-perturbation** of A is a new HA A' that is identical except, $\Theta' = B_\epsilon(\Theta)$, $\forall\ \ell \in Loc, Inv' = B_\epsilon(Inv)$ (b) a ∈ A, $Guard_a = B_\epsilon(Guard_a)$.

A is **robustly safe** iff $\exists \epsilon > 0$, such that A' is safe for U_ϵ upto time bound T, and transition bound N. Robustly unsafe iff $\exists\ \epsilon < 0$ such that A' is safe for U_ϵ.

Theorem. (Relative Completeness) Algorithm always terminates whenever the A is either robustly safe or robustly unsafe.

C2E2

publish.illinois.edu/c2e2-tool/

Apps | Writers' Representati | Microsoft Exchange | Technology | Art | Music News and Rev | Neurophilosophy | Neurophilosophy | S | News, Culture and V | » | Other Bookmarks

C2E2 Verification Tool

A Verification Tool for Simulink/Stateflow Models

Search

Home About Documents Download

Main

Compare Execute Check Enginer (C2E2) is a tool for verifying bounded-time invariant properties of Stateflow models. It supports models with nonlinear dynamics, discrete transitions, and sets of initial states. The invariant properties have to be specified by conjunctions of linear inequalities. Internally,C2E2 implements the simulation-based verification algorithms described in the sequence of publications Duggirala et al. [2013, 2014], Sukumar and Mitra [2011]. In a nutshell, it parses and transforms the Stateflow model to a mathematical representation, generates faithful numerical simulations of this model using a validated numerical simulator, bloats these simulations using user provided annotations to construct over-approximations of the bounded time reachable set, and finally, iteratively refines these over-approximations to prove the invariant or announce candidate counter examples. C2E2 has a GUI for loading and editing properties associated with Stateflow models, launching the verifier, and plotting 2D sections of the reach sets computed by the verifier. It saves the properties and the models in an internal HyXML format that can be later reloaded. The reach tubes computed for verification are

Part II

TWO APPLICATIONS

Duggirala ∘ Wang ∘ Mitra ∘ Munoz ∘ Viswanathan (FM 2014)

Huang ∘ Fan ∘ Meracre ∘ Mitra ∘ Kiwatkowska (CAV 2014)

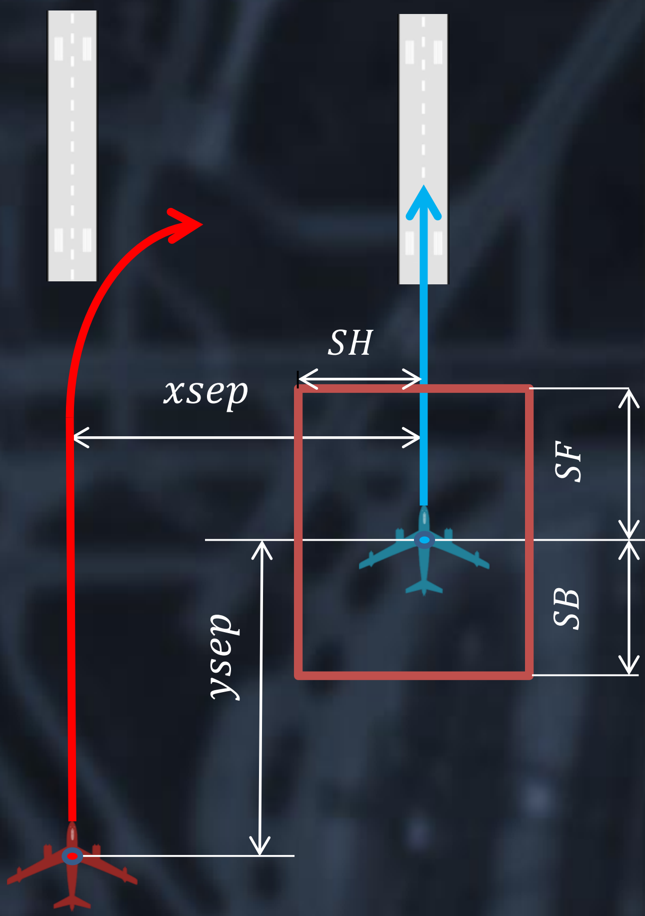
SAPA-ALAS Parallel Landing Protocol

Ownship and *Intruder* approaching parallel runways with small separation

ALAS (at ownship) protocol is supposed to raise an alarm if within T time units the *Intruder* can violate safe separation based on 3 different projections

Verify Alert$\preccurlyeq_b$Unsafe for different runway and aircraft scenarios

Scenario 1. With xsep [.11,.12] Nm ysep [.1,.21] Nm, $\phi = 30^o$ $\phi_{max} = 45^o$ vy_o= 136 Nmph, vy_i = 155 Nmph



SAPA-ALAS Parallel Landing Protocol

$Alert_i = \{\, x \mid \exists\, t \in [0, T], proj_i(x,t) \in Unsafe\}$, where $proj_i$ defined as solution of ODE $\dot{x} = g_i(x,t)$

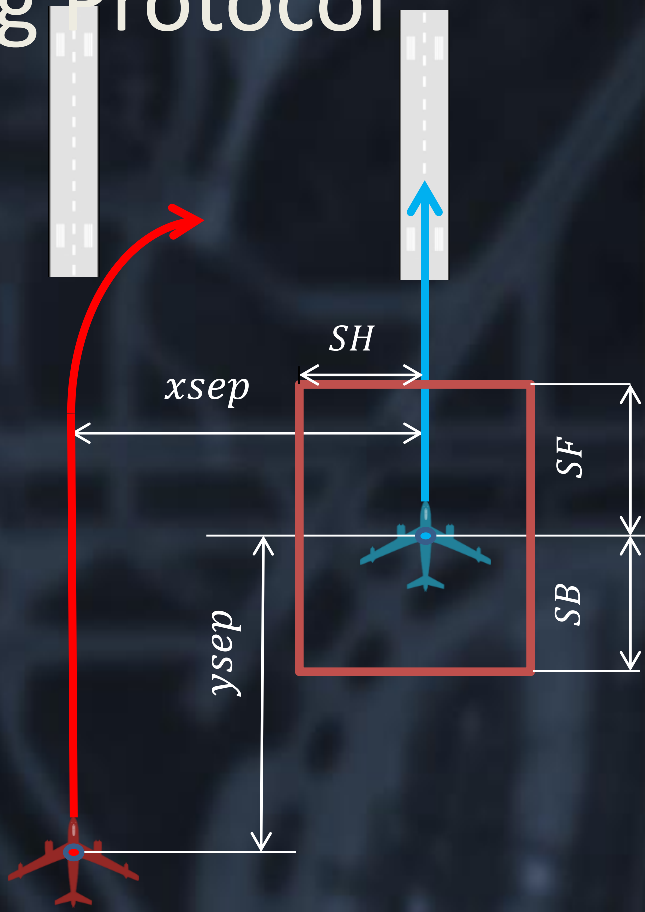
Use simulations and annotations of g_i to compute $must$ intervals when $x \in Alert_i$

$Alert \prec_b P_2$ is **satisfied** by Reachtube ψ

if $\forall\, I_2 \in Must(P_2) \cup May(P_2)$ there exists $I_1 \in Must(Alert)$ such that $I_1 < I_2 - b$

$Alert \prec_b P_2$ is **violated** by Reachtube ψ

if $\exists\, I_2 \in Must(P_2)$ for all $I_1 \in Must(Alert) \cup May(Alert)$ such that $I_1 > I_2 - b$



Duggirala, Wang, Mitra, Munoz, Viswanathan FM 2013

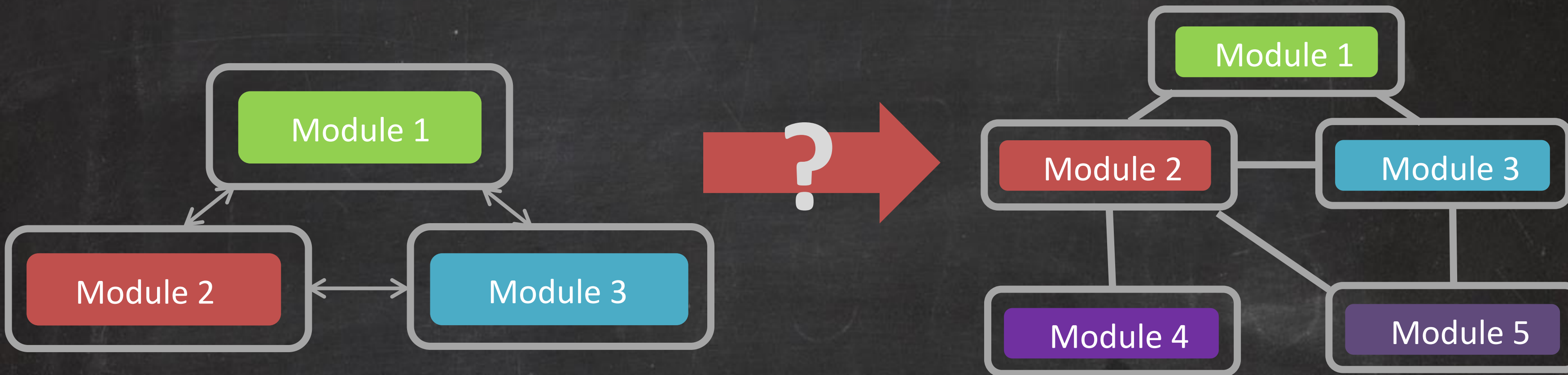
Real-time Alerting Protocol

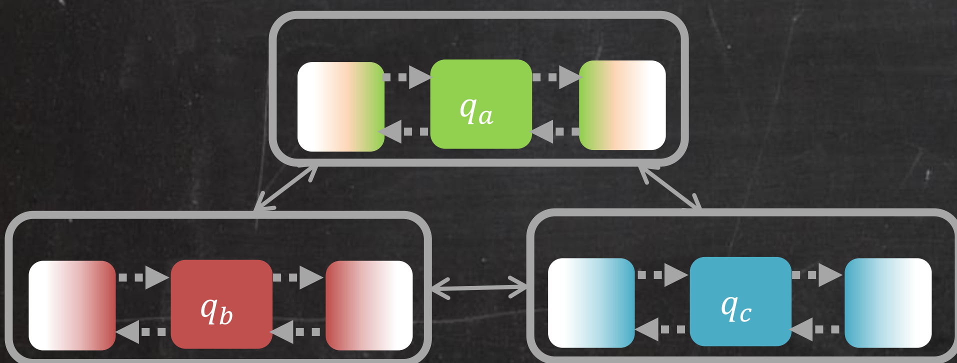
Scenario	Alert $\preccurlyeq_4$ Unsafe	Running time (mins:sec)	Alert $\preccurlyeq_?$ Unsafe
6	False	3:27	2.16
7	True	1:13	–
8	True	2:21	–
6.1	False	7:18	1.54
7.1	True	2:34	–
8.1	True	4:55	–
9	False	2:18	1.8
10	False	3:04	2.4
9.1	False	4:30	1.8
10.1	False	6:11	2.4

Sound & robustly completeness

C2E2 verifies interesting scenarios in reasonable time; shows that false alarms are possible; found scenarios where alarm may be missed

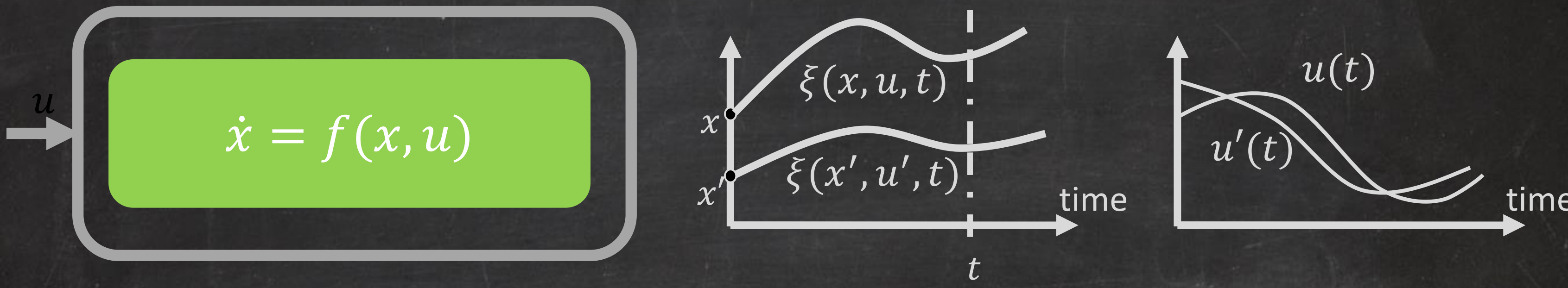
Exploiting Modularity





$$\boxed{\begin{aligned}\dot{x}_1 &= f_a(x_1, x_2, x_3)\\ \dot{x}_2 &= f_b(x_2, x_1, x_3)\\ \dot{x}_3 &= f_c(x_3, x_1, x_2)\end{aligned}} \times L^N$$

Input-to-State (IS) Discrepancy



Definition. **IS discrepancy** is defined by β and γ such that for any initial states x, x' and any inputs u, u',

$$|\xi(x,u,t) - \xi(x',u',t)| \leq \beta(x,x',t) + \int_0^t \gamma(|u(s) - u'(s)|)ds$$

$\beta \rightarrow 0$ as $x \rightarrow x'$, and $\gamma \rightarrow 0$ as $u \rightarrow u'$

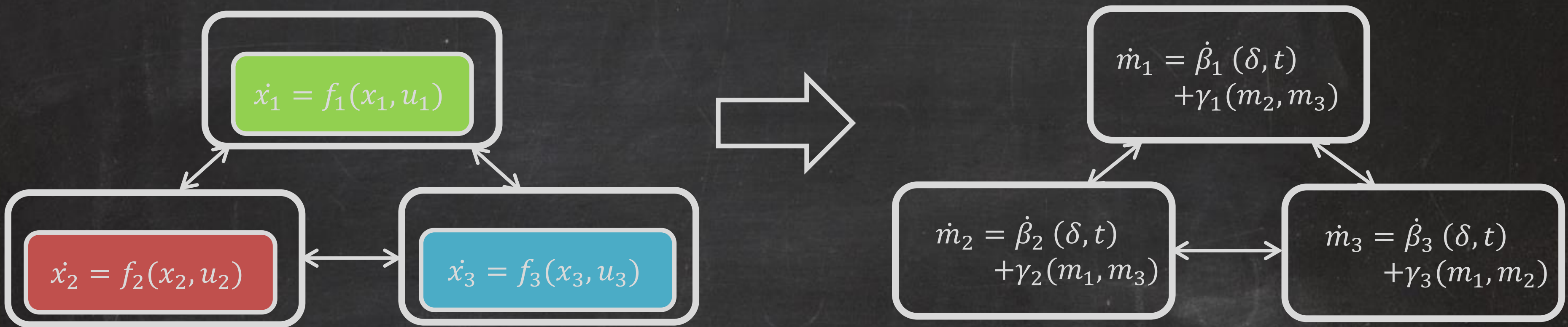
Reduced System $M(\delta_1, \delta_2, V_1, V_2)$

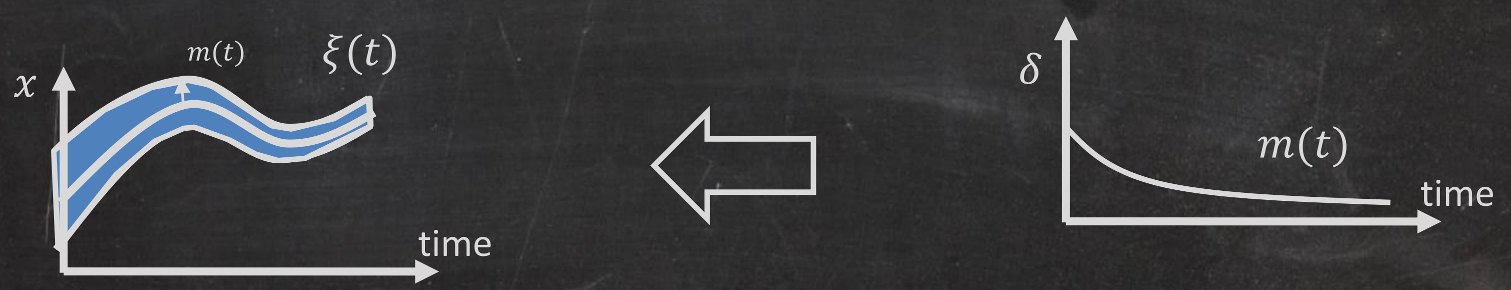
$$\dot{x} = f_M(x)$$

$$x = \langle m_1, m_2, clk \rangle$$

$$\begin{bmatrix} \dot{m}_1 \\ m_2 \\ clk \end{bmatrix} = f_M(x) = \begin{bmatrix} \dot{\beta}_1(\delta_1, clk) + \gamma_1(m_2) \\ \dot{\beta}_2(\delta_2, clk) + \gamma_2(m_1) \\ 1 \end{bmatrix}$$

Bloating with Reduced Model





The bloated tube contains all trajectories start from the δ-ball of x.

The over-approximation can be computed arbitrarily precise.

Reduced M gives effective Discrepancy of A

Theorem. For any $\delta = \langle \delta_1, \delta_2 \rangle, V = \langle V_1, V_2 \rangle$ and T
$Reach_A(B_\delta(x), T) \subseteq \bigcup_{t \le T} B^V_{\mu(t)}(\xi(x,t))$

Theorem. For any $\epsilon > 0$ there exists $\delta = \langle \delta_1, \delta_2 \rangle$ such that
$\bigcup_{t \le T} B^V_{\mu(t)}(\xi(x,t)) \subseteq B_\epsilon(Reach_A(B_\delta(x), T)$

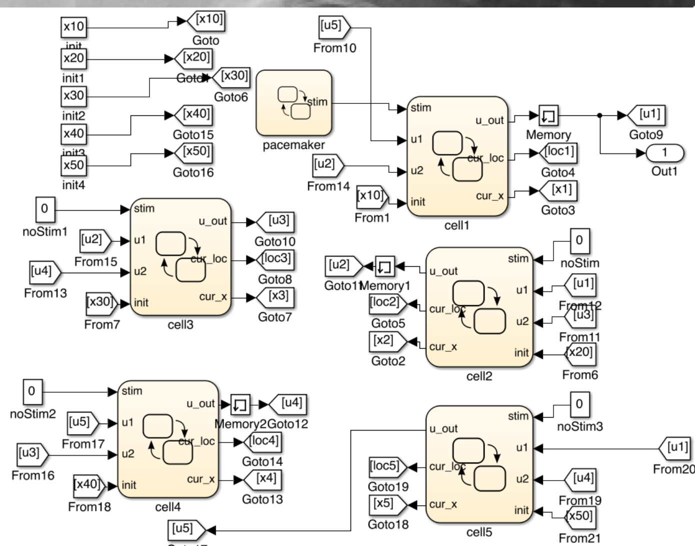
Here $\mu(t)$ is the solution of $M(\delta_1, \delta_2, V_1, V_2)$.

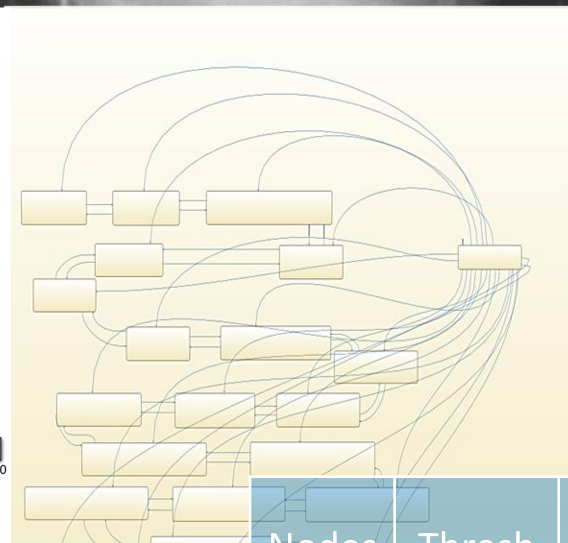
Huang & Mitra, HSCC 2013

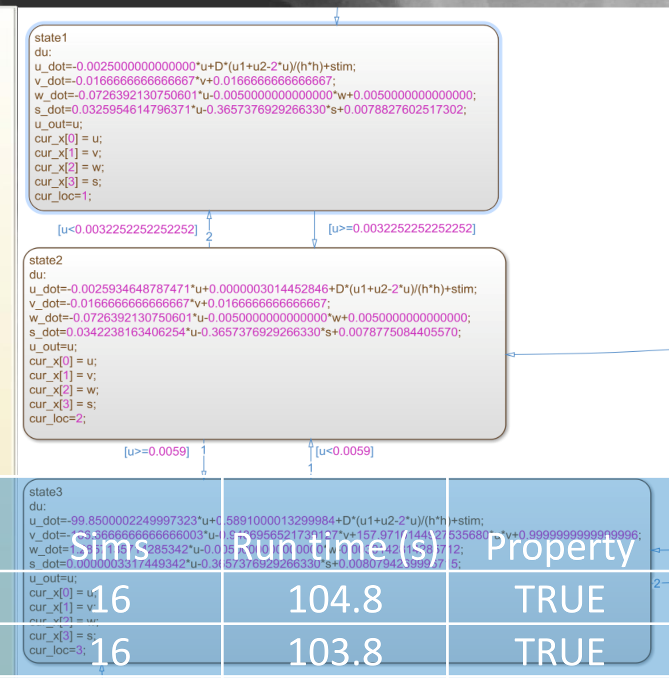
Pacemaker + Cardiac Network

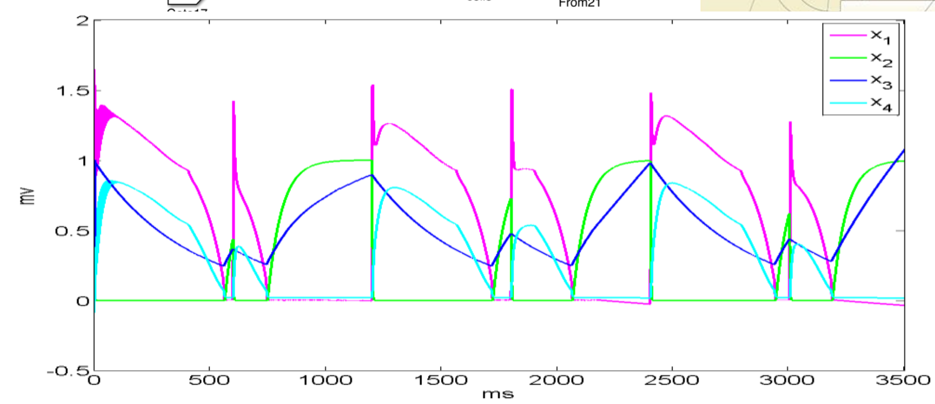
Action potential remains in specific range

No alternation of action potentials









Nodes	Thresh	Sims	Run time (s)	Property
3	2	16	104.8	TRUE
3	1.65	16	103.8	TRUE
5	2	3	208	TRUE
5	1.65	5	281.6	TRUE
5	1.5	NA	63.4	FALSE
8	2	3	240.1	TRUE
8	1.65	73	2376.5	TRUE

Summary and Outlook

- Tractable reachability of nonlinear hybrid models
  - scales reasonably with time horizon and precision
  - exponential dependence on initial set (plenty of room to exploit parallelism)
- Promising for synthesis of switching surfaces

Challenges

- Theory to support nondeterministic models using decomposition into deterministic part and state-dependent uncertainty:
  - Use cases: advanced controller, adversary, failures
- Compositional inference of annotations of large models from <u>known</u> annotations of smaller blocks
  - Use case: direct support of Simulink models directly
- Abstraction refinement-based algorithm for synthesis
- Connect synthesis engine with a specific complex hardware platform, for example, a quadcopter or a bipedal robotic system