Proofs from Simulations and Modular Annotations

Zhenqi Huang and Sayan Mitra
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

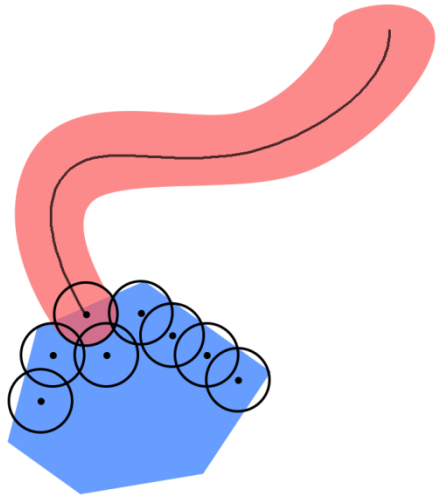
Background

- Invariant verification for dynamical systems.
  - Through computing the set of state the system can reach (reach set)
  - Exact Reach set computation is in general undecidable ⇒ Over-approximation

- Static analysis and symbolic approaches
  - E.g. SpaceEx, PHAVer, CheckMate, d/dt

- Dynamic+Static analysis using numerical simulations
  - E.g. S-TaLiRo, Breach, C2E2

Simulation-based Reachability



- $\dot{x} = f(x), \Theta \subseteq R^n$
- Denote $\xi(\theta, t)$ as a trajectory from $\theta \in \Theta$
- Simulation-based Verification
  - Finite cover of Θ ( ).
  - Simulate from the center of each cover.
  - Bloat the simulation with some factor, such that the bloated tube contains all trajectories starting from the cover.
  - Union of all such tubes gives an over-approximation of reach set
- In [1], we expect the bloating factor to be given by the user as an annotation to the model

[1] Duggirala, Mitra, Viswannathan. EMSOFT2013

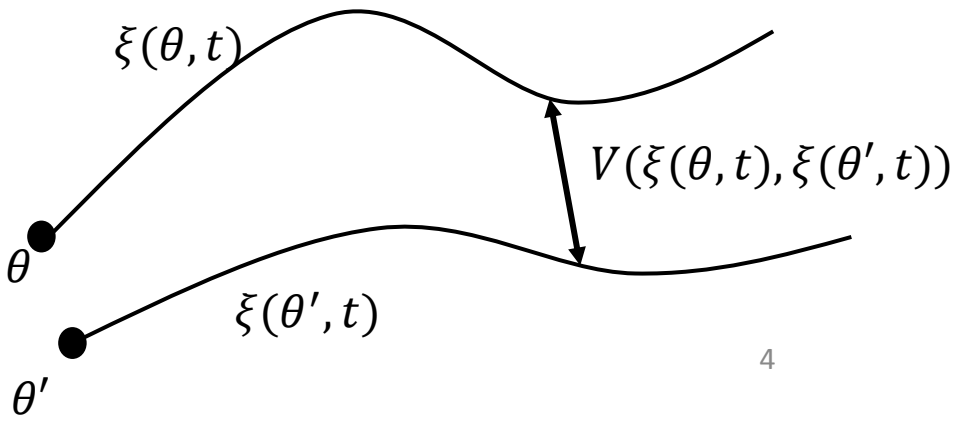
Annotation: Discrepancy Function

Definition. Functions $\mathrm{V}: X \times X \rightarrow \mathbb{R}^{\geq 0}$ and β: $\mathbb{R}^{\geq 0} \times T \rightarrow \mathbb{R}^{\geq 0}$ define a discrepancy of the system if for any two states θ_1 and $\theta_2 \in \Theta$, For any t,

$$\mathrm{V}\big(\xi(\theta, t), \xi(\theta', t)\big) \leq \beta(|\theta - \theta'|, t)$$

where, $\beta \rightarrow 0$ as $\theta \rightarrow \theta'$

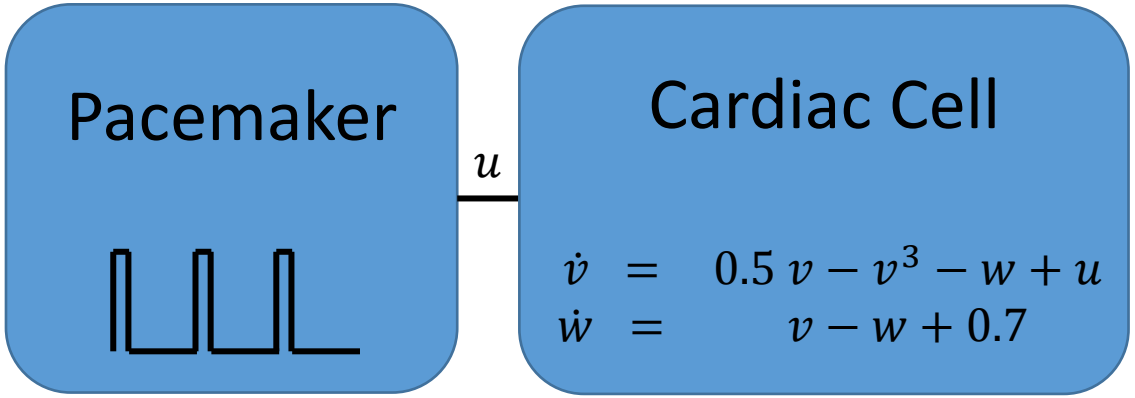
- Stability not required
- Discrepancy can be found automatically for linear systems
- For nonlinear systems, several template-based heuristics were proposed



Key challenge: Finding Discrepancy Functions for Large Models

Models of Cardiac Cell Networks

- FitzHugh–Nagumo (FHN) model [1]
- Invariant property
  - Threshold of voltage
  - Periodicity of behavior



- Find quadratic contraction metric [2]:
- $J(v,w) = \begin{bmatrix} 0.5 - 3v^2 & -1 \\ 1 & -1 \end{bmatrix}$
- Search for $\beta \in \Re$ and the coefficients of

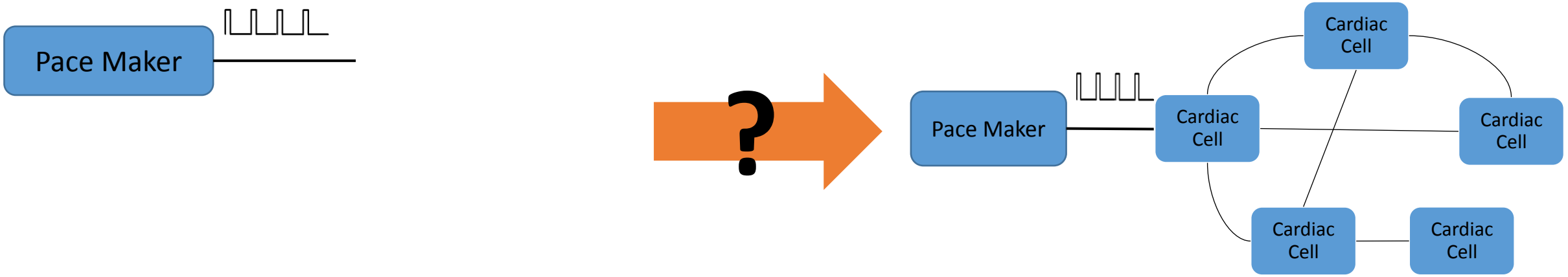
$$R(v,w) = \begin{bmatrix} \sum a_{ij}\, v^i w^j & \sum b_{ij}\, v^i w^j \\ \sum b_{ij}\, v^i w^j & \sum c_{ij}\, v^i w^j \end{bmatrix},$$

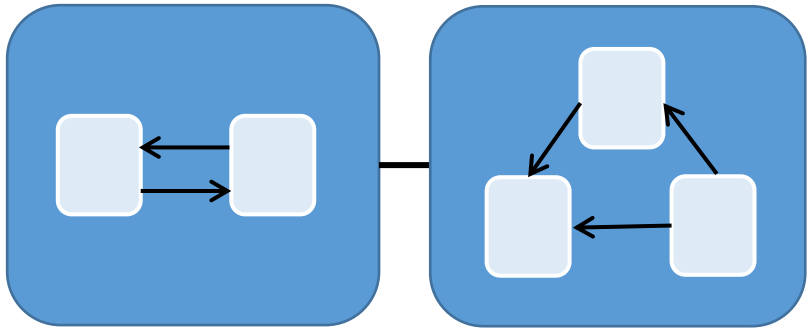
s.t. $0 \le i + j \le 2, R \succ 0$, and $J^T R + RJ + \dot{R} \prec -\beta M$

$$\boxed{\underbrace{d_R(\xi(\theta,t),\xi(\theta',t))}_{V} \le \underbrace{e^{-\beta t} d_R(\theta,\theta')}_{\beta}}$$

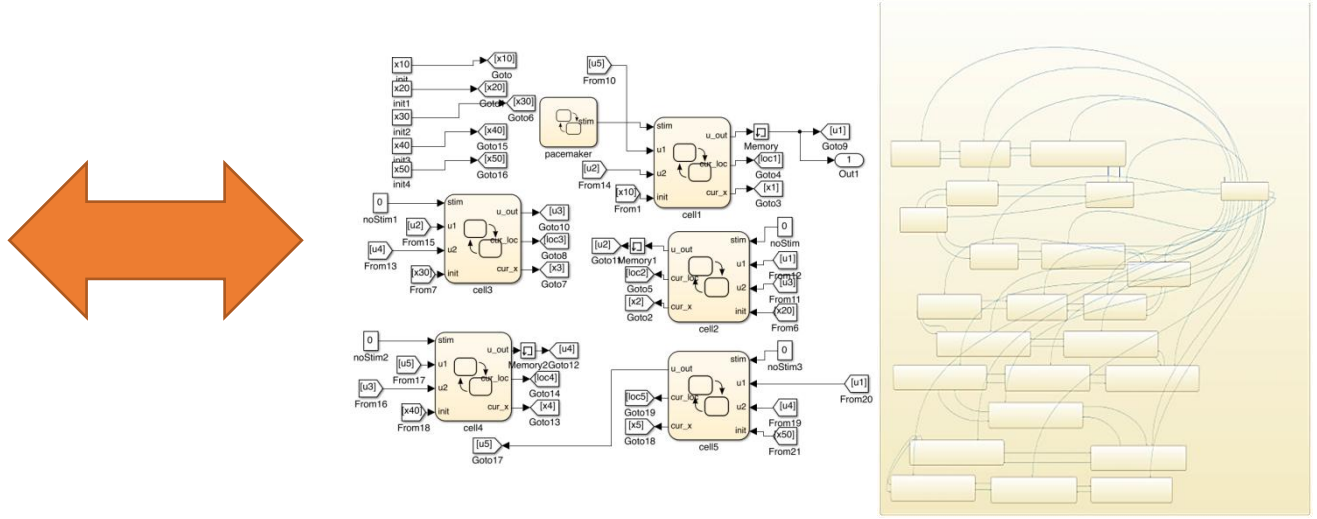
[1] FitzHugh. Biophysical J. 1961
[2] Aylward,Parrilo, Slotine. Automatica. 2008

Scalability of Finding Annotation





$$|L| = |L_1| \times |L_2|$$



[1]

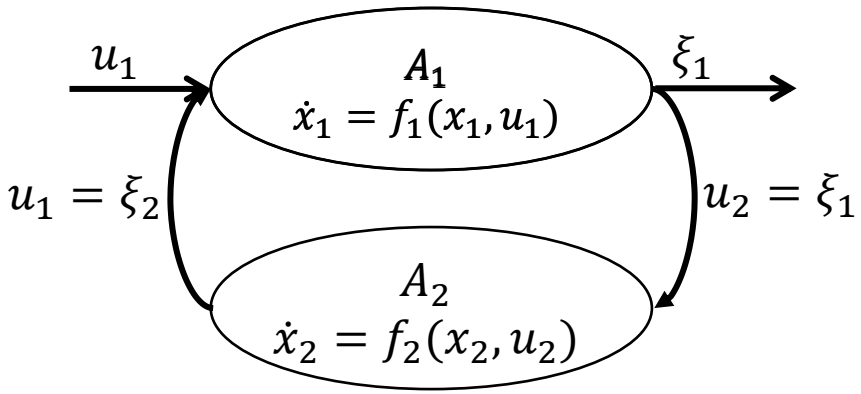
[1] Grosu, et al. CAV2011

Input-to-State (IS) Discrepancy

Definition. Functions $V: X_1 \times X_1 \to \mathbb{R}^{\geq 0}$, $\beta: \mathbb{R}^{\geq 0} \times \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ and $\gamma: \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ define a IS discrepancy of the system:

$$V_1(\xi_1(\theta_1, u_1, t), \xi(\theta_1', u_1', t)) \leq \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^T \gamma_1(|u_1(s) - u_1'(s)|)ds$$

and $\gamma_1(\cdot) \to 0$ as $u_1 \to u_1'$



(ξ_1, ξ_2) and (ξ_1', ξ_2') are a pair of trajectories of the overall ring:

$$\begin{cases} V_1(\xi_1(t), \xi_1'(t)) \leq \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds \\ V_2(\xi_2(t), \xi_2'(t)) \leq \beta_2(|\theta_2 - \theta_2'|, t) + \int_0^t \gamma_2(|\xi_1(s) - \xi_1'(s)|)ds \end{cases}$$

More on IS Discrepancy

- IS Discrepancy:

$$V\big(\xi(\theta,u,t),\xi(\theta',u',t)\big) \le \beta(|\theta-\theta'|,t) + \int_0^t \gamma(|u(s)-u'(s)|)ds$$

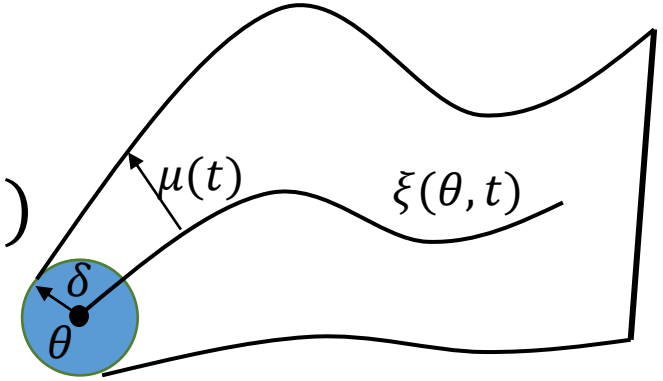
- Incremental integral input-to-state stability [1], except no stability property is required.
- Most methods of finding discrepancy of $\dot{x} = f(x)$ can be modified to find IS discrepancy systems with linear input $\dot{x} = f(x) + Bu$.

[1] Angeli D. TAC. 2009

IS Discrepancy $\Longrightarrow$ Reachability

- We will build a reduced model $M(\delta)$ with a unique trajectory $\mu(t)$ using the IS Discrepancy.

- **Theorem**: $Reach(B_\delta^V(\theta), T) \subseteq \bigcup_{t\in[0,T]} B_{\mu(t)}^V(\xi(\theta,t))$



- **Theorem**: for small enough δ and precise enough simulation, the over-approximation can be computed arbitrarily precise.

Construction of the Reduced Model

ξ_1, u_2

- Reduced model $M(\delta)$
- $\dot{x} = f_M(x)$ with $x = \langle m_1, m_2, clk \rangle$
- $\begin{bmatrix} \dot{m}_1 \\ m_2 \\ \dot{clk} \end{bmatrix} = \begin{bmatrix} \dot{\beta}_1(\delta, clk) + \gamma_1\ (m_2) \\ \dot{\beta}_2(\delta, clk) + \gamma_2\ (m_1) \\ 1 \end{bmatrix}$
- $m_i(0) = \beta_i(\delta, 0), clk(0) = 0$

ξ_2, u_1

- $M(\delta)$ has a unique trajectory $\mu(t)$.

Reduced Model $\Longrightarrow$ Bloating Factor

The ODE of the reduced model $M(\delta)$:

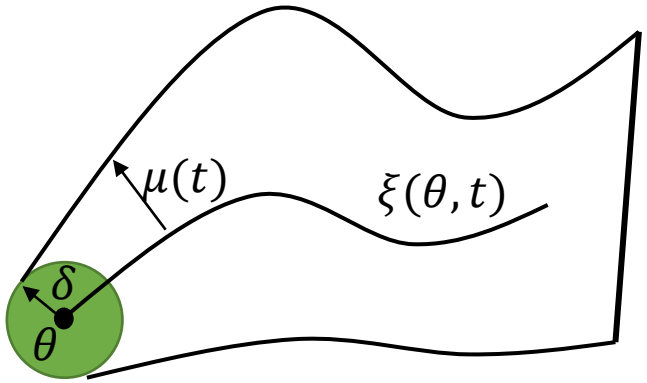
$$\begin{pmatrix} \dot{m}_1 \\ m_2 \\ \dot{clk} \end{pmatrix} = \begin{pmatrix} \dot{\beta}_1(\delta, clk) + \gamma_1\ (m_2) \\ \dot{\beta}_2(\delta, clk) + \gamma_2\ (m_1) \\ 1 \end{pmatrix}$$

The IS Discrepancy functions:

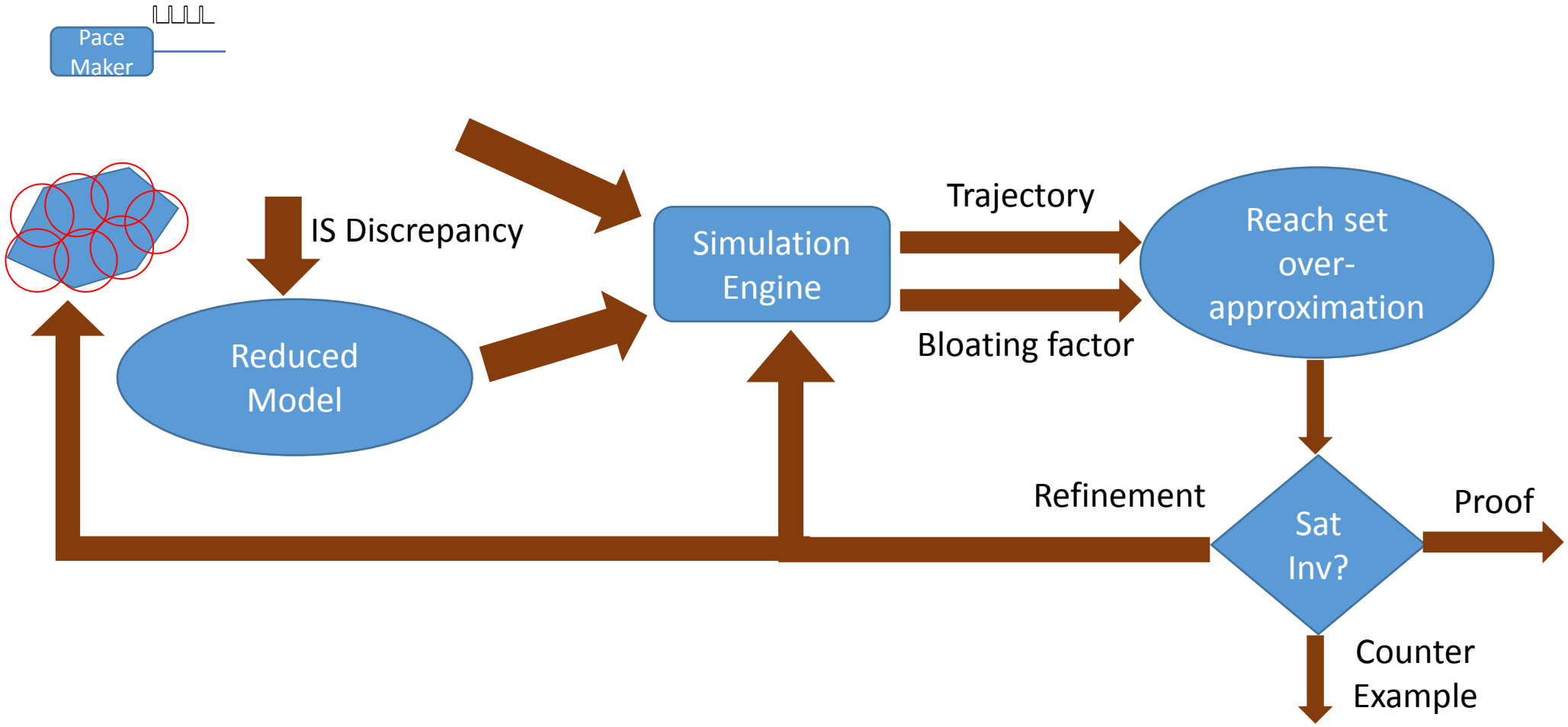
$$\begin{cases} V_1(\xi_1(t), \xi_1{}'(t)) \leq \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds \\ V_2(\xi_2(t), \xi_2{}'(t)) \leq \beta_2(|\theta_2 - \theta_2'|, t) + \int_0^t \gamma_2(|\xi_1(s) - \xi_1'(s)|)ds \end{cases}$$

- **Lemma**: $|\theta_1 - \theta_1'| \leq \delta$, and $|\theta_2 - \theta_2'| \leq \delta \quad \Longrightarrow$
  $V_1(\xi_1(t), \xi_1'(t)) \leq m_1(t)$, and $V_2(\xi_2(t), \xi_2'(t)) \leq m_2(t)$.

- Thus, bloating $\xi(\theta, t)$ by $\mu(t)$ gives an over-approximation of reach set from a ball.



Simulation & Modular Annotation ⟹ Proof



Soundness and Relative Complete

- Robustness Assumption:
  - Invariant is closed.
  - If an initial set Θ satisfies the invariant, $\exists \epsilon > 0$, such that all trajectories are at least ϵ distance from the boundary of the invariant.
- **Theorem**: the Algorithm is sound and relatively complete

- We verify systems with upto 30 dimensions in minutes.

System	# Variables	# Module	# Init. cover	Run Time
Lin. Sync	24	6	128	135.1
Nonli. WT	30	6	128	140.0
Nonli. Robot	6	2	216	166.8

Conclusion

- A scalable technique to verify nonlinear dynamical systems using modular annotations
- Modular annotations are used to construct a reduced model of the overall system whose trajectory gives the discrepancy of trajectories
- Sound and relatively complete

- Ongoing: extension to hybrid, cardiac cell network with 5 cells each has 4 continuous var. and 29 locations

- Thank you for your attention!