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

• \( \dot{x} = f(x), \Theta \subseteq \mathbb{R}^n \)
• Denote \( \xi(\theta, t) \) as a trajectory from \( \theta \in \Theta \)
• Simulation-based Verification
  • Finite cover of \( \Theta \)
  • 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

Definition. Functions $V: X \times X \to \mathbb{R}^{\geq 0}$ and $\beta: \mathbb{R}^{\geq 0} \times T \to \mathbb{R}^{\geq 0}$ define a discrepancy of the system if for any two states $\theta_1$ and $\theta_2 \in \Theta$, for any $t$,

$$V(\xi(\theta, t), \xi(\theta', t)) \leq \beta(|\theta - \theta'|, t)$$

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

- 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 \( \beta \in \mathbb{R} \) and the coefficients of \( R(v, w) = \begin{bmatrix} \sum a_{ij} v^i w^j \\ \sum b_{ij} v^i w^j \\ \sum c_{ij} v^i w^j \end{bmatrix} \), s.t. \( 0 \leq i + j \leq 2, R > 0, \) and \( J^T R + RJ + \dot{R} < -\beta M \)

\[ d_R(\xi(\theta, t), \xi(\theta', t)) \leq e^{-\beta t} d_R(\theta, \theta') \]

Scalability of Finding Annotation

\[ |L| = |L_1| \times |L_2| \]

Input-to-State (IS) Discrepancy

Definition. Functions $V: X_1 \times X_1 \rightarrow \mathbb{R}^{\geq 0}$, $\beta: \mathbb{R}^{\geq 0} \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ and $\gamma: \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ define an 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 $\gamma_1(\cdot) \rightarrow 0$ as $u_1 \rightarrow u_1'$

$(\xi_1, \xi_2)$ and $(\xi_1', \xi_2')$ 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:

\[ V(\xi(\theta, u, t), \xi(\theta', u', t)) \leq \beta(|\theta - \theta'|, t) + \int_0^t \gamma(|u(s) - u'(s)|)\,ds \]

• 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 \( \dot{x} = f(x) + Bu \).

IS Discrepancy $\implies$ Reachability

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

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

- **Theorem:** for small enough $\delta$ and precise enough simulation, the over-approximation can be computed arbitrarily precise.
Construction of the Reduced Model

• Reduced model $M(\delta)$

• $\dot{x} = f_M(x)$ with $x = \langle m_1, m_2, \text{clk} \rangle$

\[
\begin{bmatrix}
\dot{m}_1 \\
\dot{m}_2 \\
\dot{\text{clk}}
\end{bmatrix} =
\begin{bmatrix}
\beta_1(\delta, \text{clk}) + \gamma_1(m_2) \\
\beta_2(\delta, \text{clk}) + \gamma_2(m_1) \\
1
\end{bmatrix}
\]

• $m_i(0) = \beta_i(\delta, 0), \text{clk}(0) = 0$

• $M(\delta)$ has a unique trajectory $\mu(t)$.
Reduced Model $\implies$ 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:
\[
\begin{align*}
V_1(\xi_1(t), \xi_1'(t)) &\leq \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds \\
V_2(\xi_2(t), \xi_2'(t)) &\leq \beta_2(|\theta_2 - \theta_2'|, t) + \int_0^t \gamma_2(|\xi_1(s) - \xi_1'(s)|)ds
\end{align*}
\]

• **Lemma:** $|\theta_1 - \theta_1'| \leq \delta$, and $|\theta_2 - \theta_2'| \leq \delta$ $\implies$ $V_1(\xi_1(t), \xi_1'(t)) \leq m_1(t)$, 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

Simulation Engine

Reach set over-approximation

Trajectory

Bloating factor

Refinement

Sat Inv?

Proof

Counter Example

Refinement

IS Discrepancy

Reduced Model

Pace Maker

HSCC 2014, Berlin
Soundness and Relative Complete

• Robustness Assumption:
  • Invariant is closed.
  • If an initial set $\Theta$ satisfies the invariant, $\exists \epsilon > 0$, such that all trajectories are at least $\epsilon$ distance from the boundary of the invariant.

• **Theorem**: the Algorithm is sound and relatively complete

• We verify systems with upto 30 dimensions in minutes.

<table>
<thead>
<tr>
<th>System</th>
<th># Variables</th>
<th># Module</th>
<th># Init. cover</th>
<th>Run Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lin. Sync</td>
<td>24</td>
<td>6</td>
<td>128</td>
<td>135.1</td>
</tr>
<tr>
<td>Nonli. WT</td>
<td>30</td>
<td>6</td>
<td>128</td>
<td>140.0</td>
</tr>
<tr>
<td>Nonli. Robot</td>
<td>6</td>
<td>2</td>
<td>216</td>
<td>166.8</td>
</tr>
</tbody>
</table>
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!