Locally Optimal Reach Set Over-approximation for Nonlinear Systems

EMSOFT 2016

Chuchu Fan  Sayan Mitra  Jim Kapinski  Xiaoqing Jin
How to check safety of an autonomous maneuver?

Given controller and separation requirement, check safety with respect to ranges of initial relative positions, speeds, road conditions.
Verification challenge

Bug discovery $\rightarrow$ faster development
Certificate $\rightarrow$ evidence for DO178C, ISO26262, etc.

Challenge: models of complex control systems often do not have analytical solutions $\rightarrow$ Simulation $\Rightarrow$ proofs?
Safety verification problem

Consider nonlinear ODE $\dot{x} = f(x), x \in \mathbb{R}^n$

- **Trajectory** $\xi(x_0, t)$: state at time $t$ from initial state $x_0$
- **Reachtube** $\xi(B(x_0, \delta), T)$: all states reachable from initial set $B(x_0, \delta) \subseteq \mathbb{R}^n$ up to time $T$

Safety verification problem: given initial set $B(x_0, \delta)$, unsafe set $U$, time bound $T$, decide $\xi(B(x_0, \delta), T) \cap U = \emptyset$?
Simulation-driven verification strategy

Given start $\Theta$ and unsafe $U$

Compute finite cover of initial set

Simulate from the center $x_0$ of each cover

**Generalize** simulation to reachtube so that reachtube contains all trajectories from the cover

Check intersection/containment with $U$

Refine

Union $= \text{over-approximation of reach set}$

Key step: $\xi(x_0, t) \rightarrow \xi(B(x_0, \delta), T)$
Main problem: How to quantify generalization?

Discrepancy formalizes generalization:

**Discrepancy** is a continuous function $\beta$ that bounds the distance between neighboring trajectories:

$$\|\xi(x_1, t) - \xi(x_2, t)\| \leq \beta(\|x_1 - x_2\|, t),$$

From a single simulation of $\xi(x_1, t)$ and discrepancy $\beta$ we can over-approximate the reachtube.
A simple example of discrepancy function

If $f(x)$ has a Lipschitz constant $L$:

$$\forall x, y \in \mathbb{R}^n, \|f(x) - f(y)\| \leq L\|x - y\|$$

Example: $\dot{x} = -2x$, Lipschitz constant $L = 2$

then a (bad) discrepancy function is

$$\|\xi(x_1, t) - \xi(x_2, t)\| \leq \|x_1 - x_2\|e^{Lt} = \beta(\|x_1 - x_2\|, t)$$
A simple example of discrepancy function

\[ \dot{x} = -2x, \text{ Lipschitz constant } L = 2, \delta = 1 \]
What is a good discrepancy?

General: Applies to general nonlinear $f$

Accurate: Small error in $\beta$

Effective: Computing $\beta$ is fast (in practice)
Matrix measures can give tight discrepancy

**Theorem [Sontag 10]:** For any $\mathcal{D} \subseteq \mathbb{R}^n$, if all trajectories starting from the line between any two initial states $x_1$ and $x_2$ remains in $\mathcal{D}$ then: $\|\xi(x_1, t) - \xi(x_2, t)\| \leq \|x_1 - x_2\|e^{ct}$, where $c = \max_{x \in \mathcal{D}} \mu(J(x))$ and

$$\mu(J(x))$$ is a matrix measure of Jacobian

$J(x) = \left( \frac{\partial f_i(x)}{\partial x_j} \right)$ is the Jacobian matrix of $f$

This $c$ can be $< 0$, usually $<<$ Lipschitz constant

Example: $\begin{bmatrix} \dot{v} \\ \dot{w} \end{bmatrix} = \begin{bmatrix} v^2 + w^2 \\ -v \end{bmatrix}$

Jacobian: $J\left(\begin{bmatrix} v \\ w \end{bmatrix}\right) = \begin{bmatrix} 2v & 2w \\ -1 & 0 \end{bmatrix}$
Matrix measure for $A \in \mathbb{R}^{n\times n}$

Matrix norm

$$\|A\| = \max_{x \neq 0} \frac{\|Ax\|}{\|x\|}$$

$$\|A\|_2 = \sqrt{\lambda_{\text{max}}(A^T A)}$$

Matrix measure [Dahlquist 59]:

$$\mu(A) = \lim_{t \to 0^+} \frac{\|I + tA\| - \|I\|}{t}$$

2-norm: $\mu(A) = \lambda_{\text{max}} \left( \frac{A + A^T}{2} \right)$
**Definition of matrix measure**

For any matrix $A$:

$$c = \max_{x \in \mathcal{D}} \mu(j(x))$$

$$\equiv c = \max_{x \in \mathcal{D}} \lim_{t \to 0^+} \frac{\|I + tf(x)\| - \|I\|}{t}$$

$$\min c$$

s.t. $\forall A \in \mathcal{A}(D, J)$, $MA + A^T M \leq 2cI$

$M > 0$

From original problem to an SDP problem in the next slides
Baseline algorithm with 2-norm [Fan and Mitra ATVA15]

Choosing ordinary matrix 2-norm, \( \mu(J(x)) \) becomes:

\[
\lambda_{\text{max}} \left( \frac{J(x) + J^T(x)}{2} \right)
\]

[ATVA15] uses eigenvalue of center Jacobian matrix and perturbation bound to maximize this quantity over \( \mathcal{D} \)

[CAV15] application to Powertrain verification problem [Jin 16]

[CAV16] tool C2E2 implementing this algorithm
Coordinate transformation makes reachtube tighter

Under 2-norm, approximations are represented by spheres.

Using linear coordinate transformations of state, we can get tighter over-approximations with ellipsoids.

Under coordinate transformation $P$: matrix measure is $\mu_P(A) = \mu(PAP^{-1})$. 

$\beta(\|x_1 - x_2\|, t)$
Coordinate transformation makes reachable tube tighter

\[ c = \max_{x \in \mathcal{D}} \mu(J(x)) \]
\[ \equiv c = \max_{x \in \mathcal{D}} \lim_{t \to 0^+} \frac{\|I + tj(x)\| - \|I\|}{t} \]
\[ \equiv c = \max_{x \in \mathcal{D}} \lambda_{max} \left( \frac{PJ(x)P^{-1} + (P^{-1})^TJ(x)P^T}{2} \right) \]

[Original problem]

Plug in definition

[Using coordinate transformation]
Approximating $J(x)$ with an interval matrix

$\mathcal{D}$ is a compact set

Each $J_{ij}: \mathcal{D} \to \mathbb{R}$ is continuous and has upper ($u_{ij}$) and lower bounds ($l_{ij}$)

Compute interval matrix $\mathcal{A}(\mathcal{D}, J) = \begin{bmatrix} [*,*] & \cdots & [*,*] \\ \vdots & [l_{ij}, u_{ij}] & \vdots \\ [*,*] & \cdots & [*,*] \end{bmatrix}$

For all $x \in \mathcal{D}, J(x) \in \mathcal{A}(\mathcal{D}, J)$
Approximating $J(x)$ with interval matrix:

$c = \max_{x \in D} \mu(J(x))$

[Original problem]

$\equiv c = \max_{x \in D} \lim_{t \to 0^+} \frac{\|I + tJ(x)\| - \|I\|}{t}$

$\equiv c = \max_{x \in D} \lambda_{\text{max}} \left( \frac{PJ(x)P^{-1} + (P^{-1})^T J(x)P^T}{2} \right)$

[Using coordinate transformation]

$\equiv \max_{\mathcal{A} \in \mathcal{A}(D,J)} \lambda_{\text{max}} \left( \frac{PAP^{-1} + (P^{-1})^T AP^T}{2} \right)$

[Bound $J(x)$ with interval matrix]
Make it a semi-definite problem

\[
\max_{A \in \mathcal{A}(\mathcal{D},J)} \lambda_{\text{max}} \left( \frac{PP^{-1} + (P^{-1})^TAP^T}{2} \right)
\]

\[
\equiv \min c
\quad \text{s.t.} \quad \forall A \in \mathcal{A}(\mathcal{D},J) \quad \underbrace{P^T PA}_M + \underbrace{AP^T P}_M \leq 2cl
\]

\[
\equiv \min c
\quad \text{s.t.} \quad \forall A \in \mathcal{A}(\mathcal{D},J), \quad MA + A^T M \leq 2cl
\]
Bound the matrix measure by solving SDP problem

\textbf{OPT1:} \quad \min \quad c \\
\text{s.t.} \quad MA + A^T M \leq 2cM, \quad \forall A \in \mathcal{A}(\mathcal{D}, J) \\
M > 0

\textbf{Theorem.} The solution $c$ of OPT1 gives \textbf{locally optimal} discrepancy $\|x_1 - x_2\|_M e^{ct}$.

Gives smallest $c$ for any choice of $M$ over $\mathcal{D}$

Not an ordinary SDP, infinite number of constraints!
Vertex matrix algorithm

\[ A(\mathcal{D}, J) = \begin{pmatrix} [*,*] & \cdots & [*,*] \\ \vdots & \ddots & \vdots \\ [*,*] & \cdots & [*,*] \end{pmatrix} = \text{interval}([B, C]) \]

where

\[ B = \begin{pmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{pmatrix}, \quad C = \begin{pmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{pmatrix} \]

For any interval matrix \( A(\mathcal{D}, J) = \text{interval}([B, C]) \), its vertex matrices are:

\[ \mathcal{V} = \{ V \in \mathbb{R}^{n \times n} \mid v_{ij} = b_{ij} \lor v_{ij} = c_{ij} \} \]

**Theorem.** \( \text{OPT1} \equiv \text{OPT2} \):

\[ \text{OPT1: } \min_c \quad \text{s.t. } MA + A^T M \preceq 2cM, \quad \forall A \in \mathcal{A}(\mathcal{D}, J) \]

\[ M > 0 \]

\[ \text{OPT2: } \min_c \quad \text{s.t. } \forall V \in \mathcal{V}, \quad MV + V^T M \preceq 2cM \]

\[ M > 0 \]

Potentially \( 2^{n^2} \) of inequalities
Center matrix algorithm

For any interval matrix $\mathcal{A}(\mathcal{D}, J) = \text{interval}([B, C])$, its center matrix is $\text{CT}(\mathcal{A}(\mathcal{D}, J)) = \frac{B+C}{2}$.

\[
\begin{pmatrix}
[*] & \cdots & [*] \\
\vdots & \ddots & \vdots \\
[*] & \cdots & [*]
\end{pmatrix}
\rightarrow
\begin{pmatrix}
\frac{+*}{2} & \cdots & \frac{+*}{2} \\
\vdots & \ddots & \vdots \\
\frac{+*}{2} & \cdots & \frac{+*}{2}
\end{pmatrix}
\]

Solve the optimization problem

**OPT3:** \[
\min c'
\text{ s.t. } MCT(\mathcal{A}(\mathcal{D}, J)) + CT(\mathcal{A}(\mathcal{D}, J))^T M \leq 2c'M \\
M > 0
\]

Compute error bound

\[\delta \geq \|E^T M + ME\|_2, \forall E \in \mathcal{A} - \text{CT}(\mathcal{A})\]

\[c = c' + \frac{\delta}{\lambda_{\text{min}}(M)}\]

Theorem. The above $c$ is an upper bound of the solution of OPT1.
How to compute the error bound

- Compute error bound $\delta \geq \| E^T M + ME \|_2, \forall E \in \mathcal{A} - CT(\mathcal{A})$

  is equivalent to $\delta \geq [\mathcal{E}]_2$, where $\mathcal{E} = (\mathcal{A} - CT(\mathcal{A}))^T M + M(\mathcal{A} - CT(\mathcal{A}))$ is also an interval matrix

- Interval matrix norm: $[\mathcal{A}] = \sup_{A \in \mathcal{A}}\|A\|$

- Theorem: for any interval matrix $\mathcal{A} = \text{interval}([B, C])$, for $p = 1, \infty$

  $$[\mathcal{A}]_p = \left\| \left| \frac{B+C}{2} \right| + \frac{C-B}{2} \right\|_p$$
Putting it all together

Upper-bounding with a single $c$ for entire time horizon can be too conservative.

Compute piece-wise or local upper-bounds.

That is, $M_i$, $c_i$ for each time interval $[t_i, t_{i+1}]$ in $T$.

\[
\begin{align*}
\dot{x}_1 &= -x_2; \\
\dot{x}_2 &= (x_1^2 - 1)x_2 + x_1;
\end{align*}
\]
Putting it all together

upper-bounding matrix measure for all $t$ can be too conservative

Compute piece-wise or local upper-bounds on the matrix measure

Divide $[0, T]$ into $N$ consecutive time intervals, and Compute exponent of discrepancy $M_i, c_i$ for each time interval $[t_i, t_{i+1}]$
Locally optimal algorithms: accuracy

(Arbitrary precision) Approximation error $\to 0$ when size of the initial set $\delta \to 0$

(Asymptotic convergence) Approximation error $\to 0$ as $t \to \infty$ for contractive nonlinear system and stable linear systems
Algorithm using 2-norm (without transformation)

Matrix perturbation theorem [Teschl, 99]: If $A$ and $E$ are $n \times n$ symmetric matrices, then

$$|\lambda_k(A + E) - \lambda_k(A)| \leq \|E\|_2$$

Method [Fan 15]:

- Find the center point $d_0$ of $\mathcal{D}$, compute $J_c = J(d_0)$
- Compute the largest eigenvalue $\lambda$ of $SJ_c = (J_c^T + J_c)/2$
- Compute error bound $e \geq \|SJ(x) - SJ_c\|_2$, $\forall x \in \mathcal{D}$
- $c = \lambda + e$
### Summary: Locally optimal discrepancy

<table>
<thead>
<tr>
<th>Methods</th>
<th>Baseline algorithm</th>
<th>Locally optimal algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Largest eigenvalue of center matrix and perturbation bound</td>
<td>Vertex matrix</td>
</tr>
<tr>
<td># optimization problems</td>
<td>0</td>
<td>1 convex problem with up to $2^{n^2} + 1$ constraints</td>
</tr>
<tr>
<td>Tightness of the discrepancy</td>
<td>No local optimality guarantee</td>
<td>Locally optimal</td>
</tr>
</tbody>
</table>
Running time comparison

<table>
<thead>
<tr>
<th>Flow*</th>
<th>Locally optimal Algorithm</th>
<th>Baseline Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>2628</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>105</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0.003</td>
<td>0.003</td>
<td>0.003</td>
</tr>
<tr>
<td>0.00002</td>
<td>0.00002</td>
<td>0.00002</td>
</tr>
</tbody>
</table>

Dimensions: 2 to 28
Accuracy comparison

Laub-Loomis Biology ModeAS Polynomial Helicopter (L)

Flow*
Locally optimal Algorithm
Baseline Algorithm
Future directions: Applications in automotive systems

sx (blue): relative distance along road direction
sy (green): relative distance orthogonal to sx
Debugging systems with high-fidelity models
Summary and future directions

Simulation + discrepancy analysis ⇒ proofs (reachtube)

Discrepancy analysis influences efficiency and conservativeness of verification

Matrix measures enable automatic locally optimal reachability analysis

Future: methods for systems with partially known models
Links and references

Pictures links:
https://images.google.com/

References:


Thank you

for your precious time and attention