On Generating a Variety of Counterexamples for Linear Dynamical Systems

Manish Goyal
Parasara Sridhar
Duggirala

July 12, 2018
Verification

\[ x \geq 0.55 \]

SpaceEx: Filtered Oscillator
**Verification**

$x \geq 0.55$

The entire ‘unsafe’ reachable set

**SpaceEx: Filtered Oscillator**
Falsification

Staliro: Room Heating

Staliro: Nonlinear System
Falsification

Some randomly generated counterexample

Staliro: Room Heating

Staliro: Nonlinear System
Verification or Falsification

The entire ‘unsafe’ reachable set

Randomly generated counterexample

Control Designer
Regulation Control Problem

- Requirement: To make the error between the observation and the desired value to be 0
Regulation Control Problem

- **Requirement**: To make the error between the observation and the desired value to be 0
- The control designer is most concerned about
  - The amount of overshoot that occurred, and
  - The duration for which the value of error was above the threshold
Contribution

- Define Deepest and Longest Counterexamples
- Constraint Propagation
- Experimental Results
Outline

- Introduction
- Preliminaries
- Methodology
- Experimentation
- Discussion
Introduction

Deepest Counterexample
Introduction

Deepest Counterexample

Longest Counterexample
Simulation-equivalent Analysis

For a dynamical system $H$ with affine linear dynamics $\dot{x} = Ax + B$, the simulation starting from a state $x_0$ is computed as a sequence $\tau_H(x_0, h)$ of states at discrete time steps with step size $h$.

In the sequence $\tau_H(x_0, h) = x_0, x_1, x_2, \ldots$, each pair $(x_i, x_{i+1})$ corresponds to a continuous trajectory starting at $x_i$ and reaching $x_{i+1}$ after $h$ time units.
Deepest Counterexample

Given a direction $\nu$ and the unsafe set $U$, the depth of a simulation $\tau$ is defined as

$$\text{depth}(\tau, \nu) = \max\{\nu \cdot x_i \mid x_i \in \tau \land x_i \in U\}$$

For a direction $\nu$ and a set of unsafe simulations $T_U$, the deepest counterexample is $\text{deepest}_\text{ce}(\nu) = \tau$ such that $\text{depth}(\tau, \nu) \geq \text{depth}(\tau', \nu)$ for all $\tau, \tau' \in T_U$. 
Longest Counterexample

Given the unsafe set $U$, the length of a simulation $\tau$ is defined as
\[
\text{length}(\tau) = \max \{ \text{len} \mid \exists x_i, x_{i+1}, \ldots, x_{i+\text{len}-1} \in \tau \text{ such that } \forall i \leq j \leq i + \text{len} - 1, \; x_j \in U \}
\]
The simulation with maximum length among the set of unsafe simulations is called the longest counterexample.
Star Representation

A generalized star $\Theta$ is a tuple $\langle c, V, P \rangle$ where $c \in \mathbb{R}^n$ is called the center, $V = \{v_1, v_2, \ldots, v_m\}$ is a set of $m$ ($\leq n$) vectors in $\mathbb{R}^n$ called the basis vectors, and $P : \mathbb{R}^n \rightarrow \{\top, \bot\}$ is a predicate, defined as

$$[[\Theta]] = \{x \mid \exists \bar{\alpha} = [\alpha_1, \ldots, \alpha_m]^T \text{ such that } x = c + \sum_{i=1}^{n} \alpha_i v_i \text{ and } P(\bar{\alpha}) = \top\}$$

$$(x_1', x_2')$$

$x = c + (\alpha_1 v_1 + \alpha_2 v_2)$

Variables

- Orthonormal: $x_1'$ and $x_2'$
- Basis: $\alpha_1$ and $\alpha_2$
Reachable Set Computation

\[ \Theta \triangleq \langle c, V, P \rangle \]
\[ P \triangleq \alpha_1^2 + \alpha_2^2 = 1 \]

- Represented using simulations and generalized star
- The predicate \( P \) that defines reachable set remains the same
Constraint Propagation

Unsafe Set $U$

$\langle c_U, V_U, P_U \rangle$

Initial Set $S_1$

$\langle c, V, P \rangle$
Constraint Propagation

Unsafe Set $U$

$\langle c_U, V_U, P_U \rangle$

Initial Set $S_1$

$\langle c, V, P \rangle$

$S_2$

$S_3$

$\langle c', V', P \rangle$
Constraint Propagation

Unsafe Set $U$

Initial Set $S_1$

$\langle c, V, P \rangle$

$S_2$

$S_3$

$\langle c', V', P \rangle$

$\langle c, V, P \rangle$

$\langle c', V', P' \rangle$

Constraint Propagation
Constraint Propagation

Unsafe Set $U$

$\langle c_U, V_U, P_U \rangle$

Initial Set $S_1$

$\langle c, V, P \rangle$

$S_2$

$S_3$

$\langle c', V', P \rangle$

$\langle c', V', P \cap P'_U \rangle$

$\langle c', V', P'_U \rangle$

$1$

$2$
Constraint Propagation

Unsafe Set \( U \) \\[ (c_U, V_U, P_U) \]

Initial Set \( S_1 \) \\[ (c, V, P) \]

\( S_2 \)

\( S_3 \) \\[ (c', V', P) \]

\( c, V, P \cap P'_U \)

\( c', V', P'_U \)
Constraint Propagation

Unsafe Set $U$

$\langle c_U, V_U, P_U \rangle$

$\langle c', V', P \rangle$

$\langle c'', V'', P \rangle$

$\langle c''', V''', P \cap P''_U \rangle$

Initial Set $S_1$

$\langle c, V, P \rangle$

$\langle c, V, P \cap P''_U \rangle$
Constraint Propagation

Unsafe Set $U$

$\langle c_U, V_U, P_U \rangle$

$S_2$

$\langle c', V', P \cap P'_U \rangle$

$S_3$

$\langle c', V', P \rangle$

$S_4$

$\langle c'', V'', P \cap P''_U \rangle$

Initial Set $S_1$

$\langle c, V, P \rangle$

$\langle c, V, P \cap P'_U \cap P''_U \rangle$
Deepest Counterexample

For each star $S_i$ having $S_i \cap U \neq \emptyset$, find depth: $\max \{v \cdot x_i\}$
Deepest Counterexample

For each star $S_i$ having $S_i \cap U \neq \emptyset$, find depth: $\max \{v \cdot x_i\}$

Pick the state $x'$ with maximum depth
Deepest Counterexample

For each star $S_i$ having $S_i \cap U \neq \emptyset$, find depth: max \{v \cdot x_i\}

Pick the state $x'$ with maximum depth

Convert $x'$ in star basis variables $\alpha'_1$ and $\alpha'_2$

$x' \rightarrow (\alpha'_1, \alpha'_2)$
Deepest Counterexample

For each star $S_i$ having $S_i \cap U \neq \emptyset$, find depth: $\max \{v \cdot x_i\}$

Pick the state $x'$ with maximum depth

Convert $x'$ in star basis variables $\alpha'_1$ and $\alpha'_2$

Migrate these basis variables to compute The corresponding state in the initial set

State in initial set

$x_0 = c_0 + \alpha'_1 v_1 + \alpha'_2 v_2$
Deepest Counterexample
Deepest Counterexample: Algorithm

**Input**: Initial set $\emptyset$, the simulation-equivalent reachable sequence, direction $v$, and Unsafe set $U$

**Output**: Counterexample with maximum depth

$\text{max\_depth} \leftarrow \bot, \text{max\_star} \leftarrow \bot$

for each star $S$ in the sequence do

if $S$ intersects with $U$ then

Find its $\text{depth}$ in the given direction $v$

if $\text{depth} > \text{max\_depth}$ then

Update $\text{max\_depth}$ and $\text{max\_star}$

Compute corresponding basis-variables

end

end

Propagate $\text{max\_depth}$ basis-variables to the initial set $\emptyset$

Obtain initial state as the deepest counterexample
Longest Counterexample

Unsafe Set U

\[ P \cap P_3^U \]

\[ P \cap \text{not } U \]

\[ \langle c, V, P \rangle \]
Longest Counterexample
Longest Counterexample
Longest Counterexample: Algorithm

**Input**: Initial set $\emptyset$, the simulation-equivalent reachable sequence, and Unsafe set $U$

**Output**: Counterexample with longest contiguous time

$\text{max\_depth} \leftarrow \bot$

for each star $S$ in the sequence do

if $S$ intersects with $U$ then

Transform $U$ using star center and basis vectors

Find the longest subsequence of length $L$ starting at $S$

if $L > \text{max\_length}$ then

Update $\text{max\_length}$

end

end

end

Propagate constraints maximum length $L$ subsequence to initial set $\emptyset$

Solve to obtain the longest counterexample
Benchmark: Harmonic Oscillator

- Dynamics
  \[ \dot{x} = -0.1 \times x + y \]
  \[ \dot{y} = -x - 0.1 \times y \]

- Initial Set
  \[ x \in [-6, -5] \]
  \[ y \in [0,1] \]

- Unsafe Set
  \[ x \in [-2,2] \]
  \[ y \in [4,6] \]
Benchmark: Adaptive Cruise Control

Two cars in the leader-follower system. The trailing car is required to maintain safe separation \( s \) with the leading car. \( v_l \) is the velocity of the leading car, and \( v_f \) is of the follower. \( a_f \) is the follower’s acceleration and \( k_{aero} \) is a constant.

- **Dynamics**
  \[
  \dot{s} = (v_l - v_f) \\
  \dot{v}_f = a_f - k_{aero} \cdot v_f \\
  \dot{a}_f = -2 \cdot a_f - 2(v_f - v_l)
  \]

- **Initial Set**
  \[
  s \in [0.1, 0.4] \\
  v_f \in [63, 68]
  \]

- **Unsafe Set**
  \[
  s \leq 0.05 \& v \geq 68
  \]
Benchmark: Adaptive Cruise Control
### Results: Deepest Counterexample

<table>
<thead>
<tr>
<th>Model</th>
<th>Dims</th>
<th>Deepest Counter-Example</th>
<th>Direction</th>
<th>Depth</th>
<th>Verification Time (sec)</th>
<th>DCE Gen Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damped Osc.</td>
<td>2</td>
<td>[-5.459 0.1881]</td>
<td>$x_1 = 1$</td>
<td>2.0</td>
<td>0.17</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[-6 0.8829]</td>
<td>$x_2 = 1$</td>
<td>5.0</td>
<td>0.22</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[-6 1]</td>
<td>$x_2 = 1$</td>
<td>5.288</td>
<td>0.28</td>
<td>0.01</td>
</tr>
<tr>
<td>Vehicle Platoon 1</td>
<td>15</td>
<td>$x_1 = 1.071$</td>
<td>$x_2 = 1$</td>
<td>-0.182486</td>
<td>1.82</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_2 = 0.993$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_{3,6,9,12,15} = 1.1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i = 0.9$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_{3,6,9,12,15} = 1.1$</td>
<td>$x_2 = 1$</td>
<td>0.0170</td>
<td>2.9</td>
<td>0.39</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i = 0.9$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_{3,6,9,12,15} = 1.1$</td>
<td>$x_2 = 1$</td>
<td>0.0170</td>
<td>3.51</td>
<td>0.40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i = 0.9$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vehicle Platoon 2</td>
<td>30</td>
<td>$x_5 = 0.9005$</td>
<td>$x_5 = 1$</td>
<td>-0.26347</td>
<td>4.86</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_{23} = 1.0473$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i \in {0.9, 1.1}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_5 = 0.91327$</td>
<td>$x_5 = 1$</td>
<td>-0.2217</td>
<td>5.20</td>
<td>0.27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i = 0.9$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_4 = 0.9389$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_5 = 1.1, x_i = 0.9$</td>
<td>$x_5 = 1$</td>
<td>0.01745</td>
<td>10.73</td>
<td>1.87</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i \in {0.9, 1.1}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Direction** is the direction in which the maximum depth is computed. **DCE Time** is the time Hylaa takes to generate the deepest counterexample.
## Results: Longest Counterexample

<table>
<thead>
<tr>
<th>Model</th>
<th>Dims</th>
<th>Longest Counter-Example</th>
<th>Actual Inter. Duration</th>
<th>LCE Duration</th>
<th>Verification Time (sec)</th>
<th>LCE Gen Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damped Oscillator</td>
<td>2</td>
<td>[-5.37295 0.0]</td>
<td>[5 10]</td>
<td>[6 10]</td>
<td>0.17</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[-5.0 0.3968]</td>
<td>[4 10][33 44]</td>
<td>[33 44]</td>
<td>0.22</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[-5 0.296]</td>
<td>[3 10][29 49]</td>
<td>[59 100]</td>
<td>0.28</td>
<td>0.17</td>
</tr>
<tr>
<td>Vehicle Platoon 1</td>
<td>15</td>
<td>$x_8 = 1.0475, x_{2,5} = 1.1, x_i = 0.9, x_{6,9} = 1.1, x_{12} = 1.0761, x_i = 0.9$</td>
<td>[27 41]</td>
<td>[29 41]</td>
<td>1.82</td>
<td>0.18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[27 73]</td>
<td>[27 73]</td>
<td>2.90</td>
<td>1.40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>same as above</td>
<td>[27 100]</td>
<td>[27 100]</td>
<td>3.51</td>
<td>3.78</td>
</tr>
<tr>
<td>Vehicle Platoon 2</td>
<td>30</td>
<td>$x_9 = 0.9223, x_5 = 1.0204, x_i \in (0.9, 1.1), x_{19} = 1.0501, x_i \in {0.9, 1.1}, x_i = 0.9$</td>
<td>[42 48]</td>
<td>[44 48]</td>
<td>4.86</td>
<td>0.23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[42, 53]</td>
<td>[45 53]</td>
<td>5.20</td>
<td>0.43</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[36 100]</td>
<td>[36 100]</td>
<td>10.73</td>
<td>9.81</td>
</tr>
</tbody>
</table>

**LCE Duration** is the interval in discrete time steps for longest counterexample. **Verification Time** is the time Hylaa takes for verification, **LCE Time** is the time taken to generate the longest counterexample.
Discussion

• Search in the space of basis variables that define the initial set
Discussion

- Search in the space of basis variables that define the initial set
- Counterexamples are depicted in discrete time
Discussion

• Search in the space of basis variables that define the initial set
• Counterexamples are depicted in discrete time
• Variations in the size of the unsafe region and depth direction
Discussion

• Search in the space of basis variables that define the initial set
• Counterexamples are depicted in discrete time
• Variations in the size of the unsafe region and depth direction
• Counterexample length and generation time
Discussion

• Search in the space of basis variables that define the initial set

• Counterexamples are depicted in discrete time

• Variations in the size of the unsafe region and depth direction

• Counterexample length and generation time

Thank you!