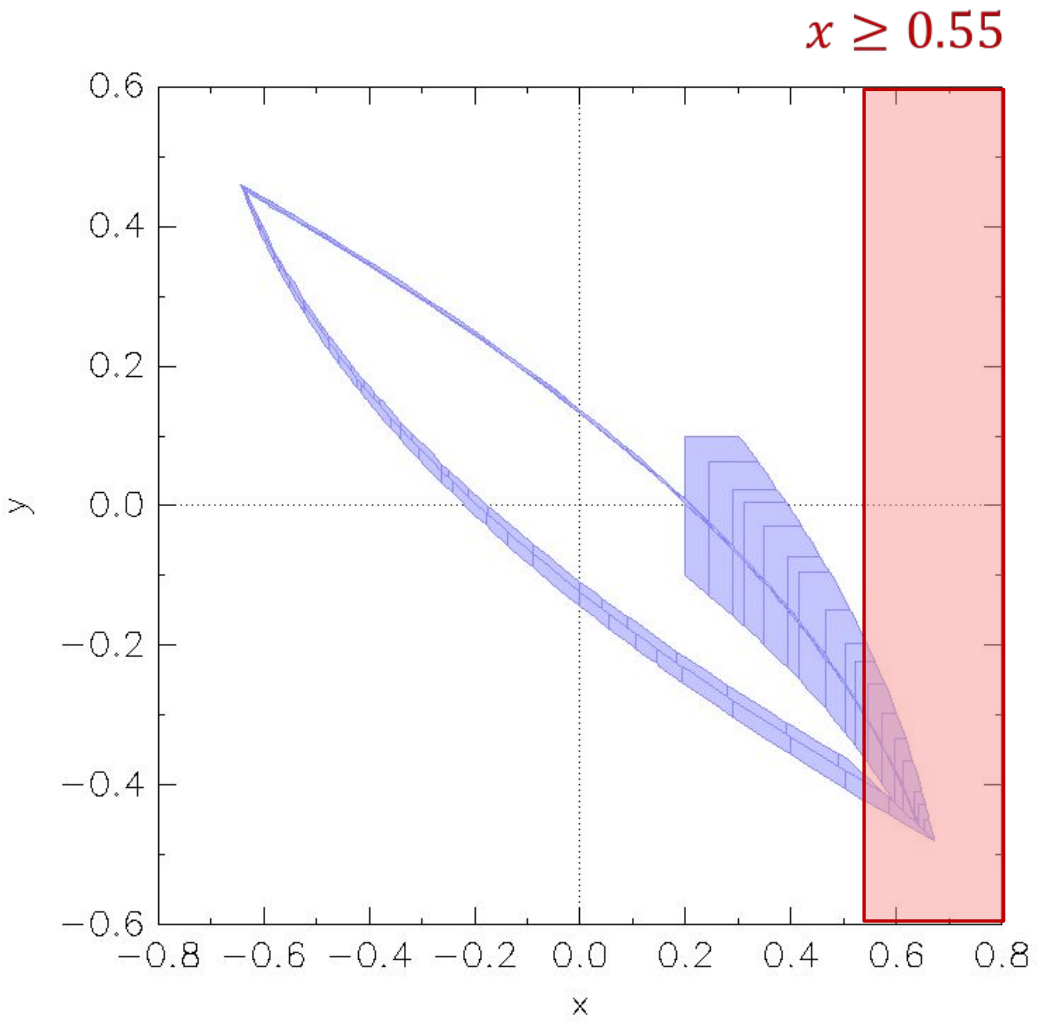
Analysis and Design of Hybrid Systems
Oxford, UK

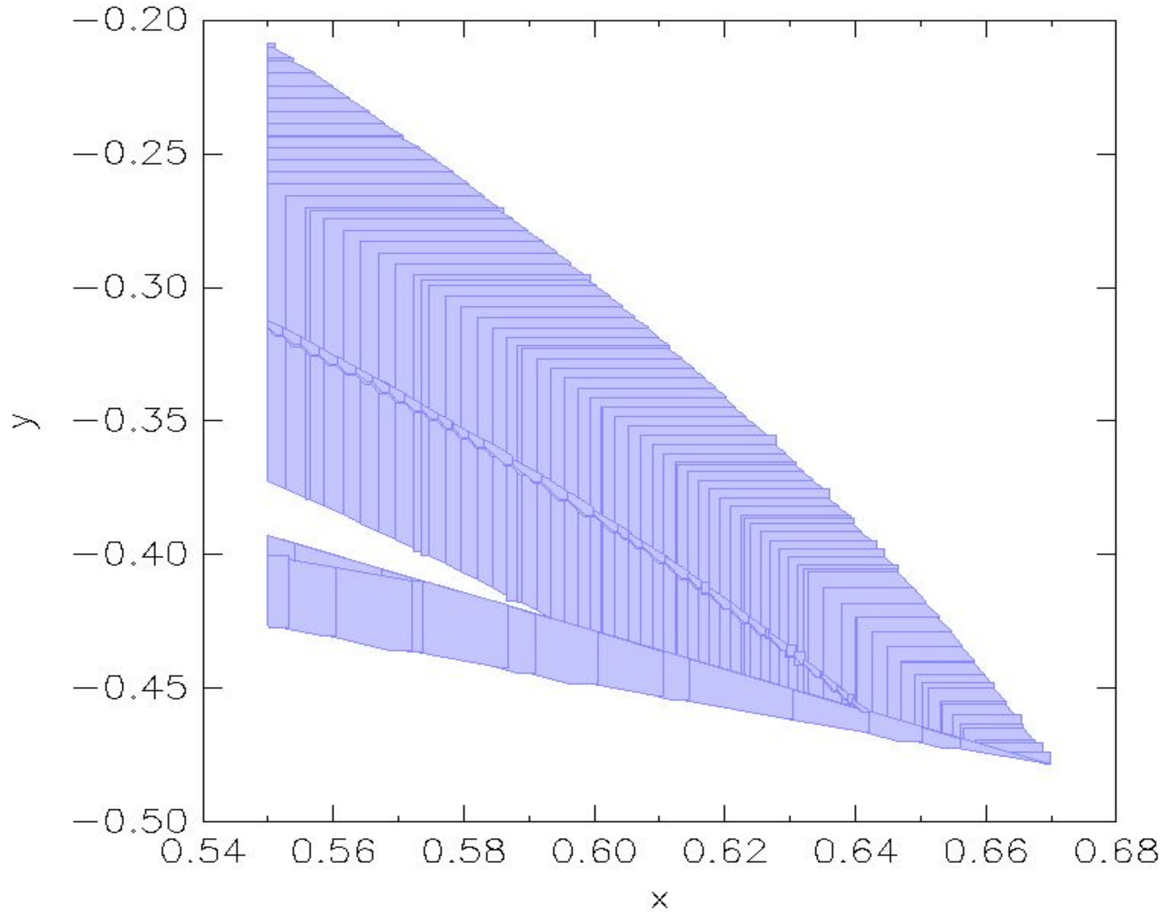
On Generating a Variety of Counterexamples for Linear Dynamical Systems

Manish Goyal
Parasara Sridhar
Duggirala

July 12, 2018

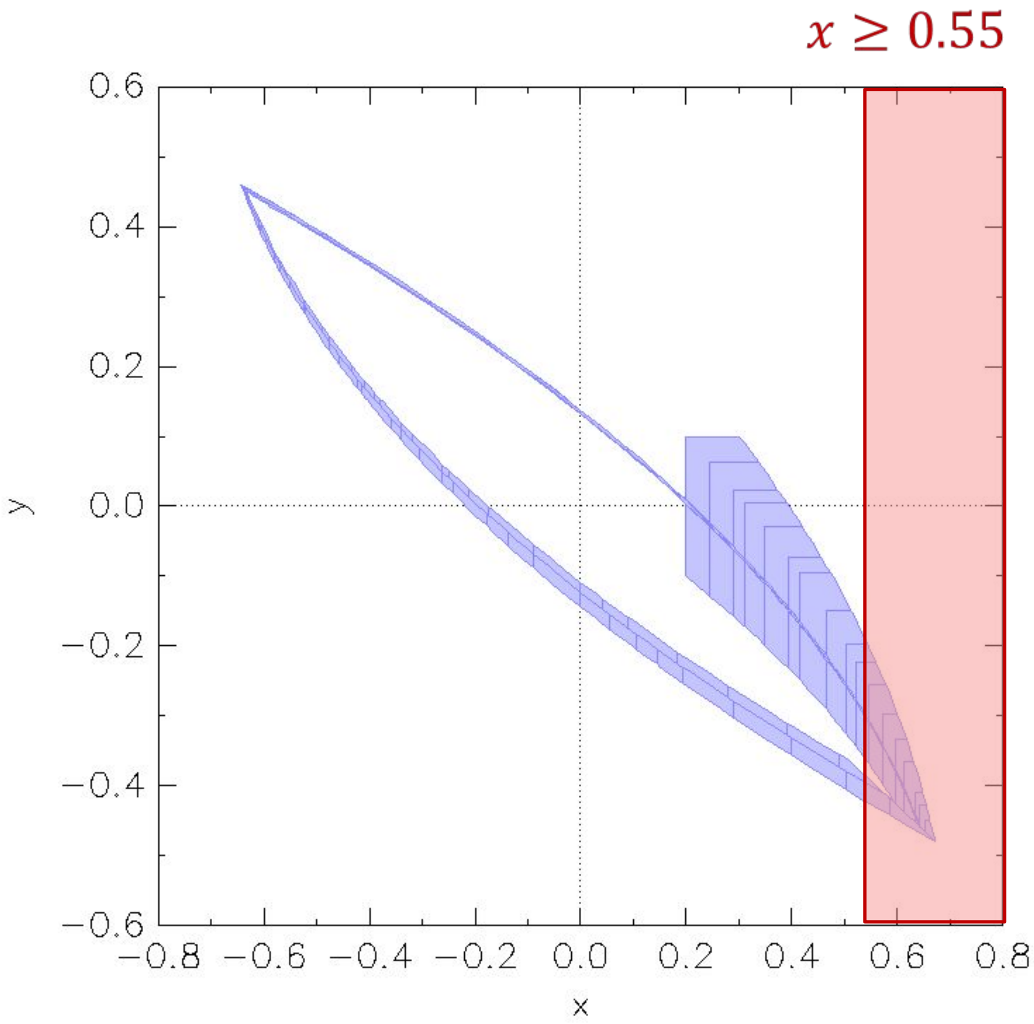
Verification



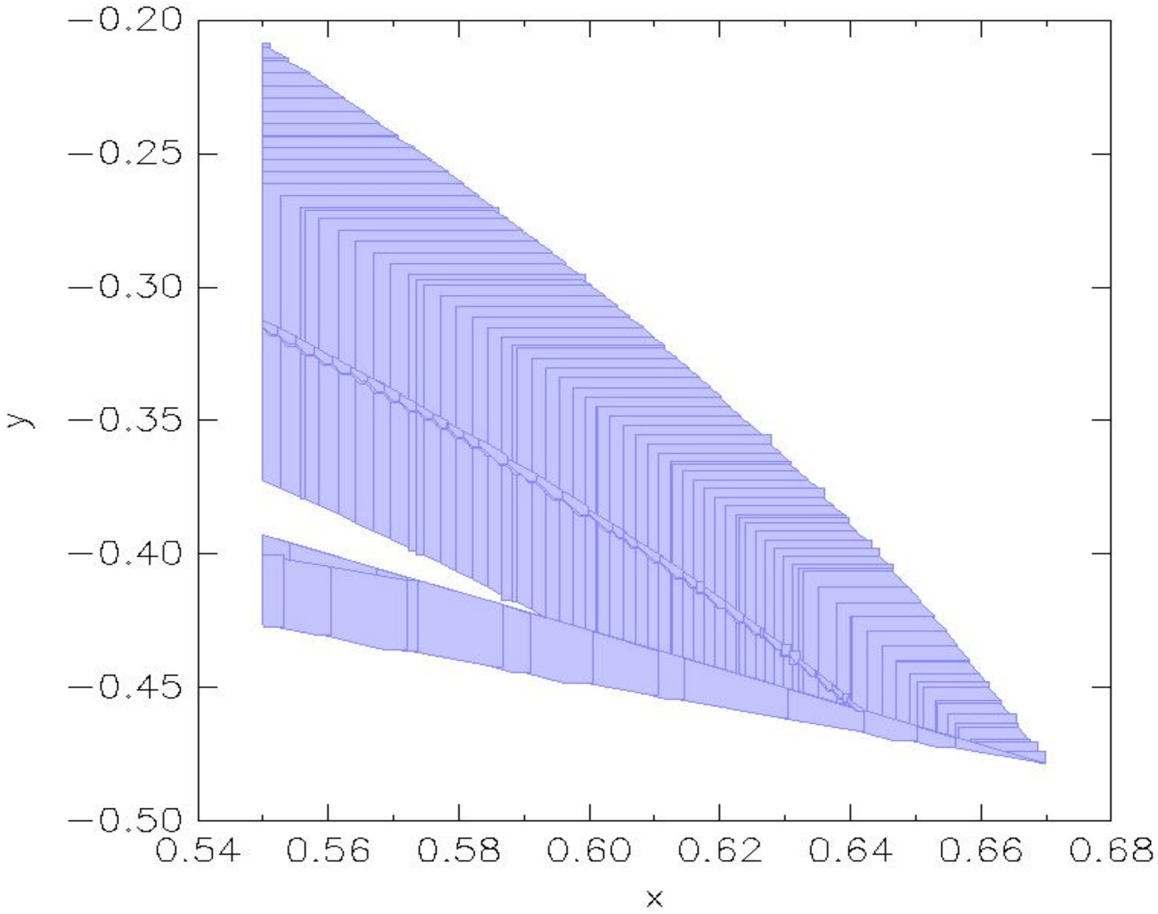


SpaceEx: Filtered Oscillator

Verification

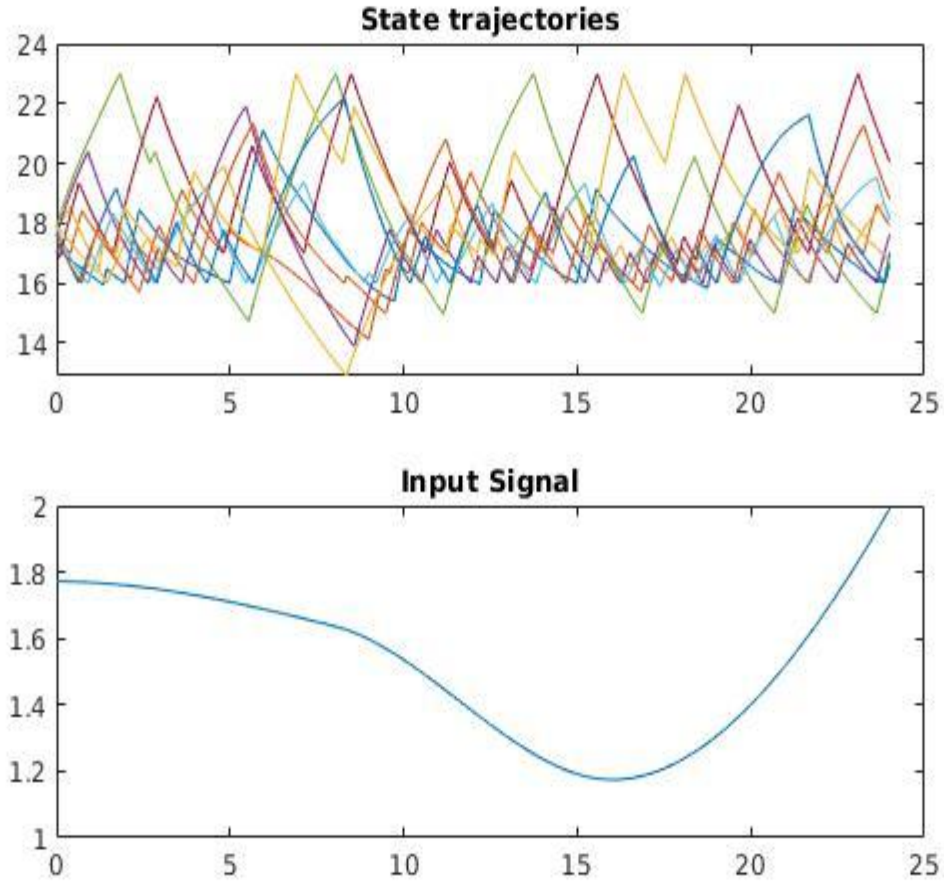


The entire ‘unsafe’ reachable set

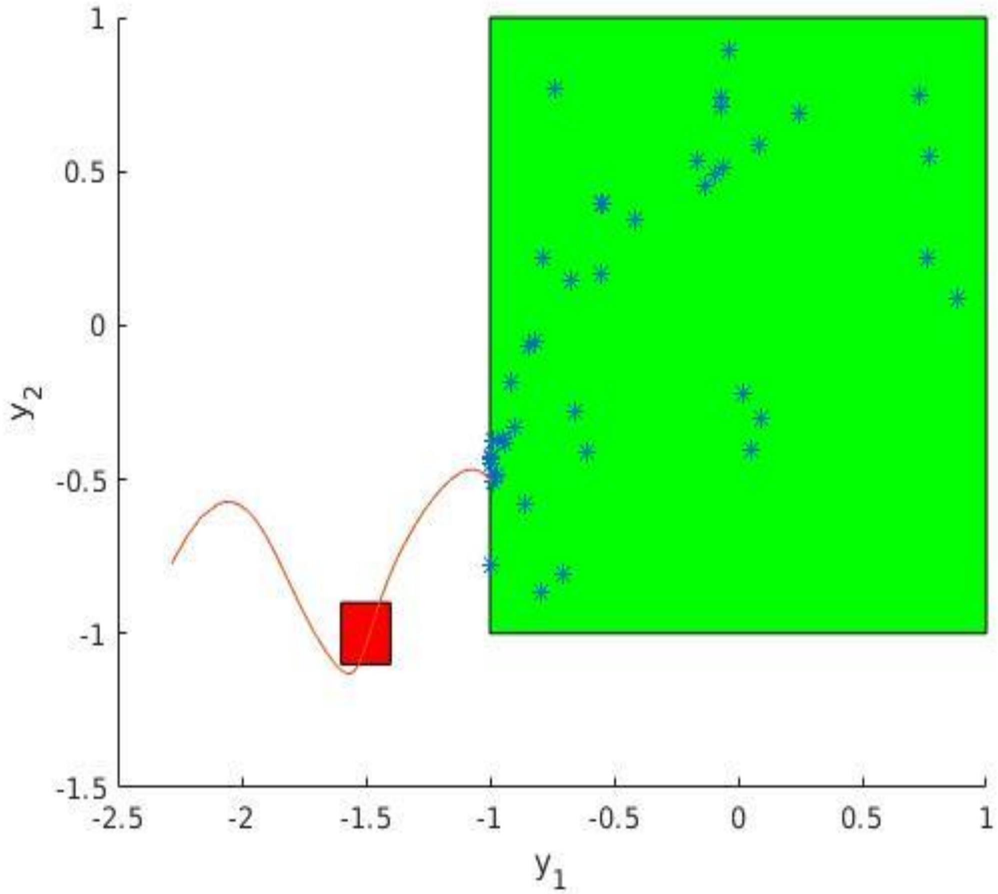


SpaceEx: Filtered Oscillator

Falsification



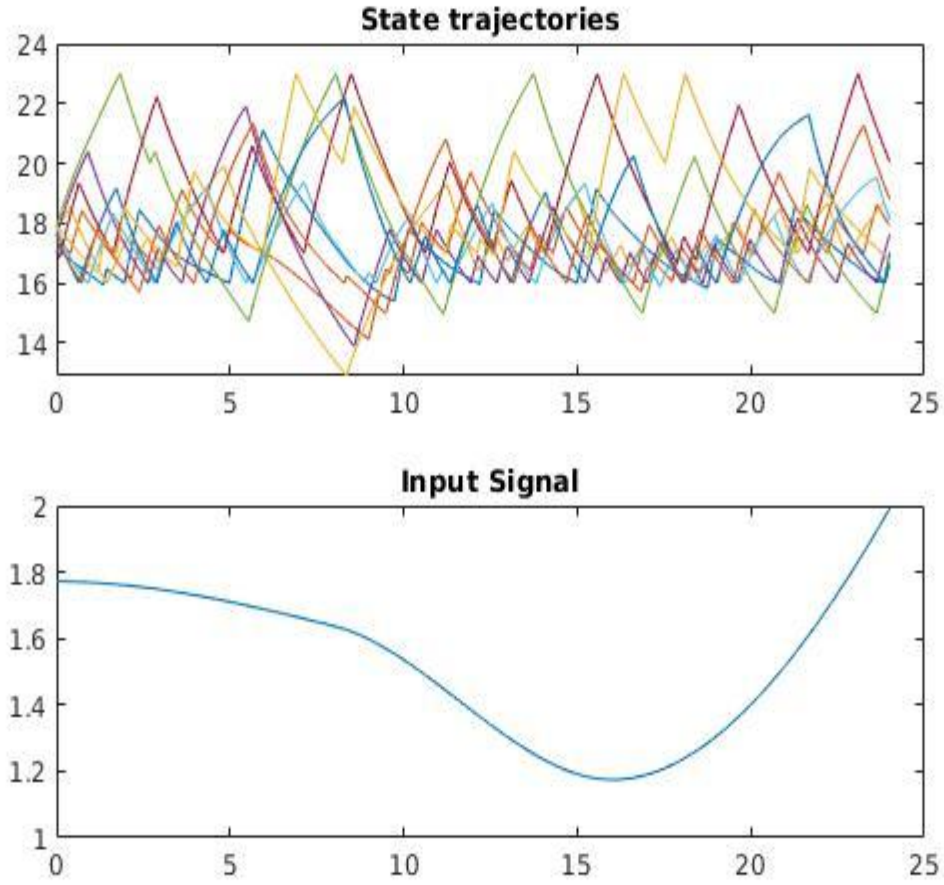
Staliro: Room Heating



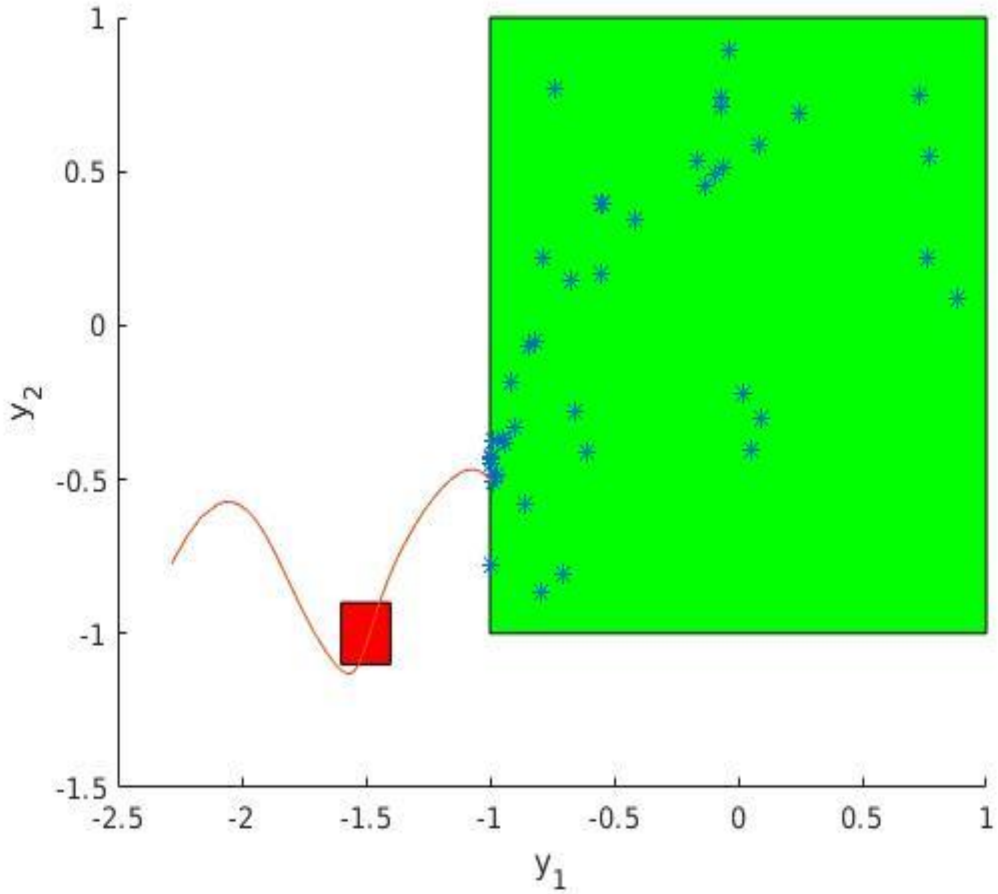
Staliro: Nonlinear System

Falsification

Some randomly generated counterexample



Staliro: Room Heating



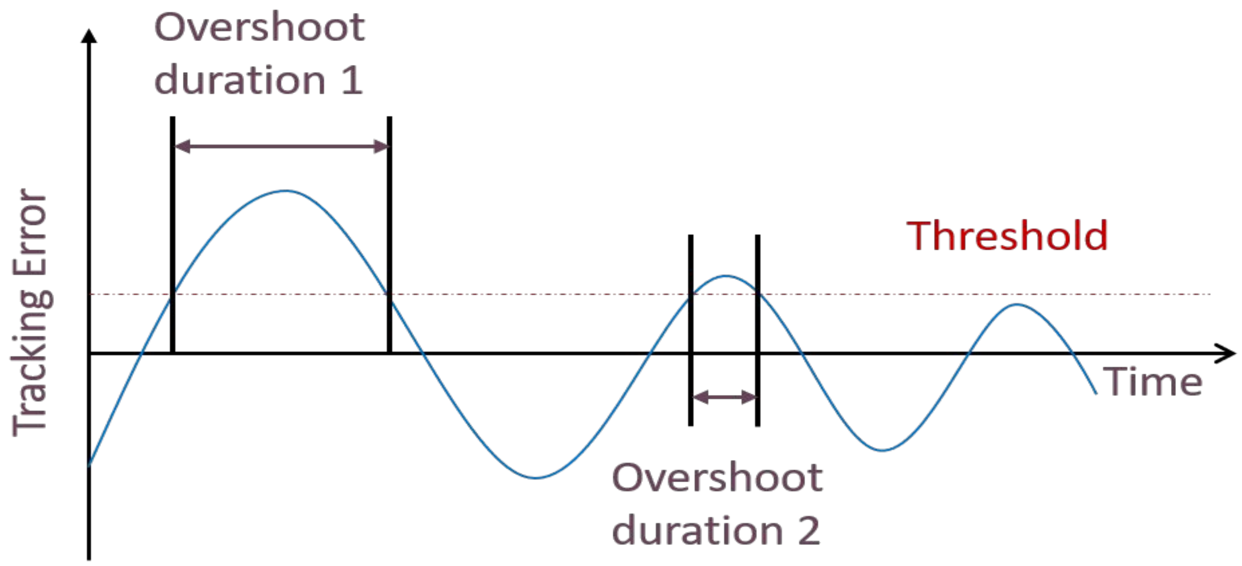
Staliro: Nonlinear System

Verification or Falsification

The entire ‘unsafe’ reachable set

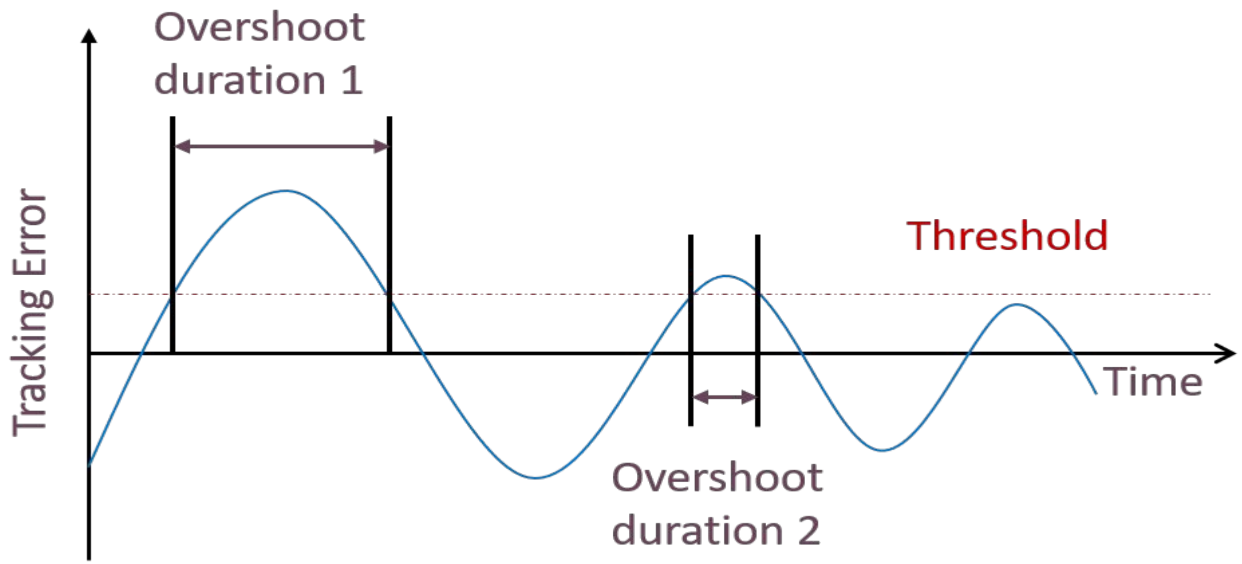
Randomly generated counterexample

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

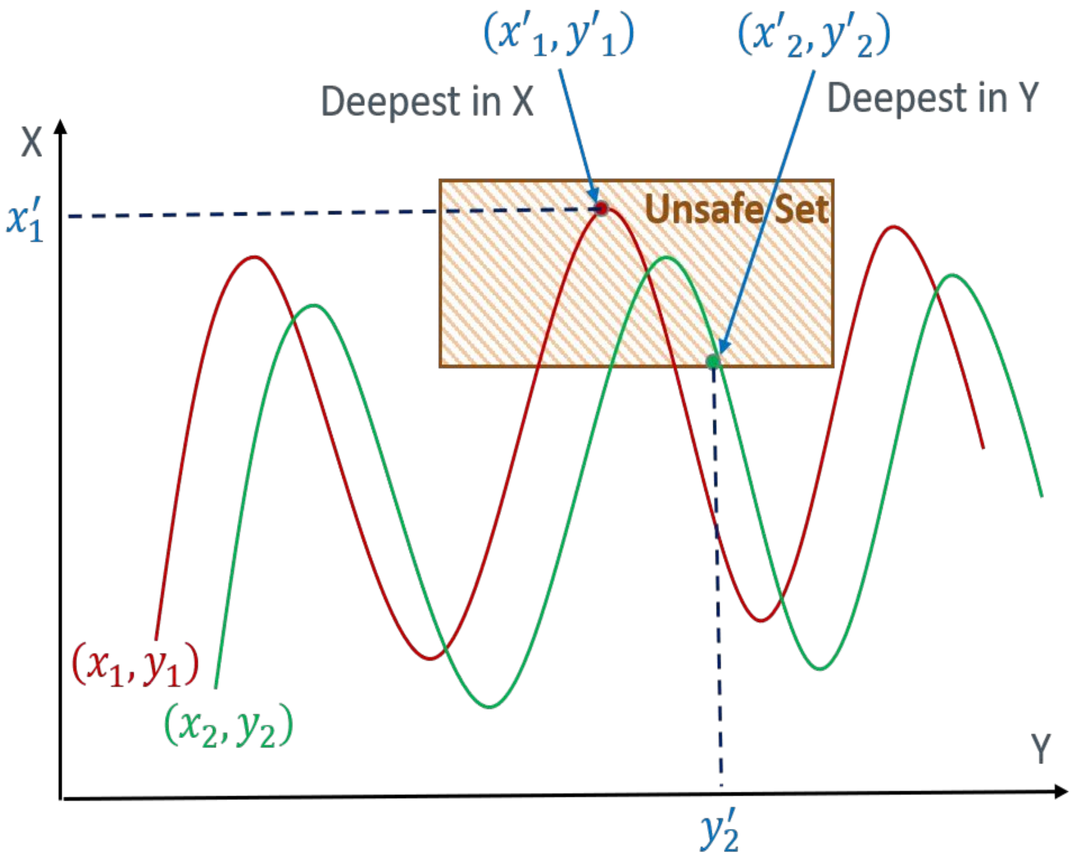
Contribution

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

Outline

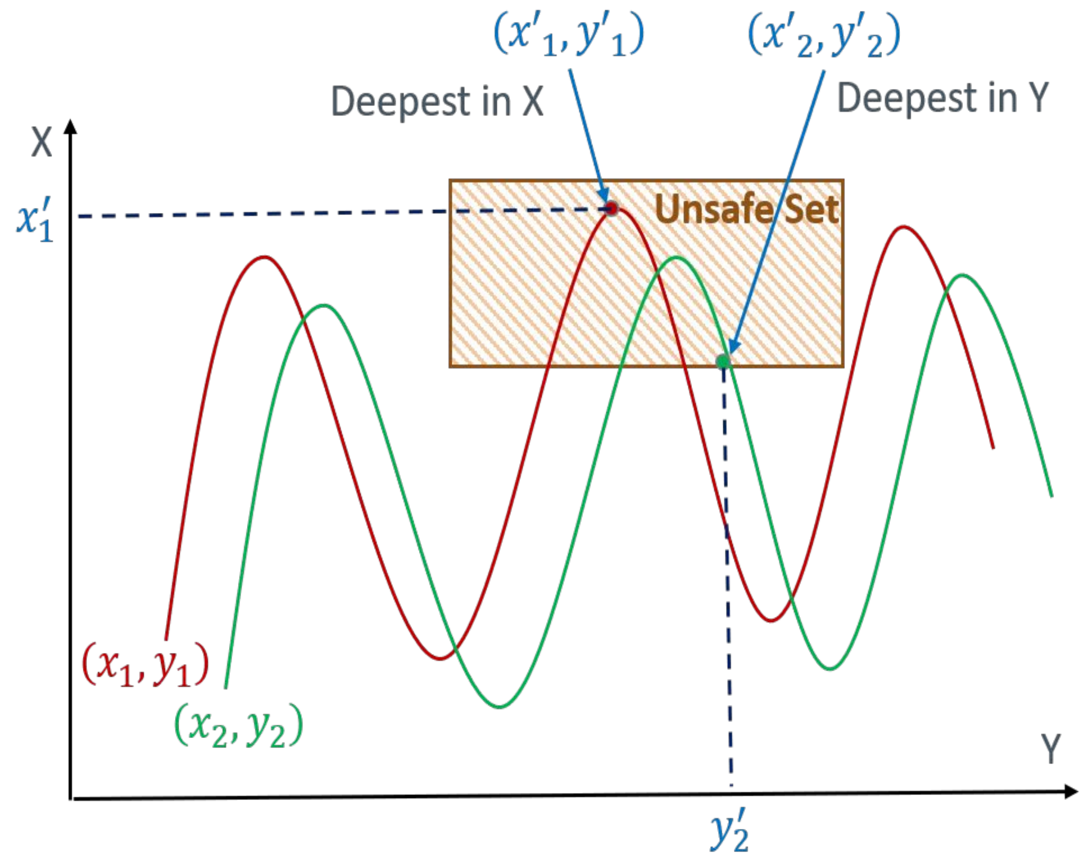
- Introduction
- Preliminaries
- Methodology
- Experimentation
- Discussion

Introduction

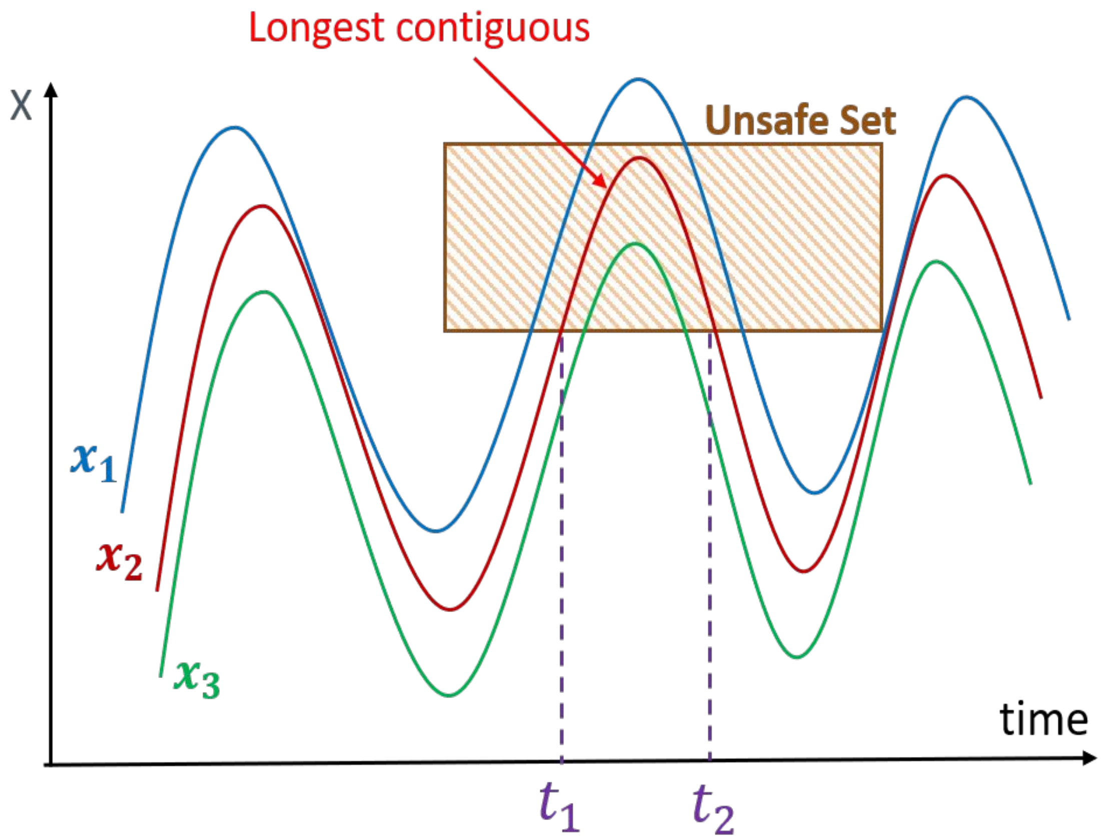


Deepest Counterexample

Introduction



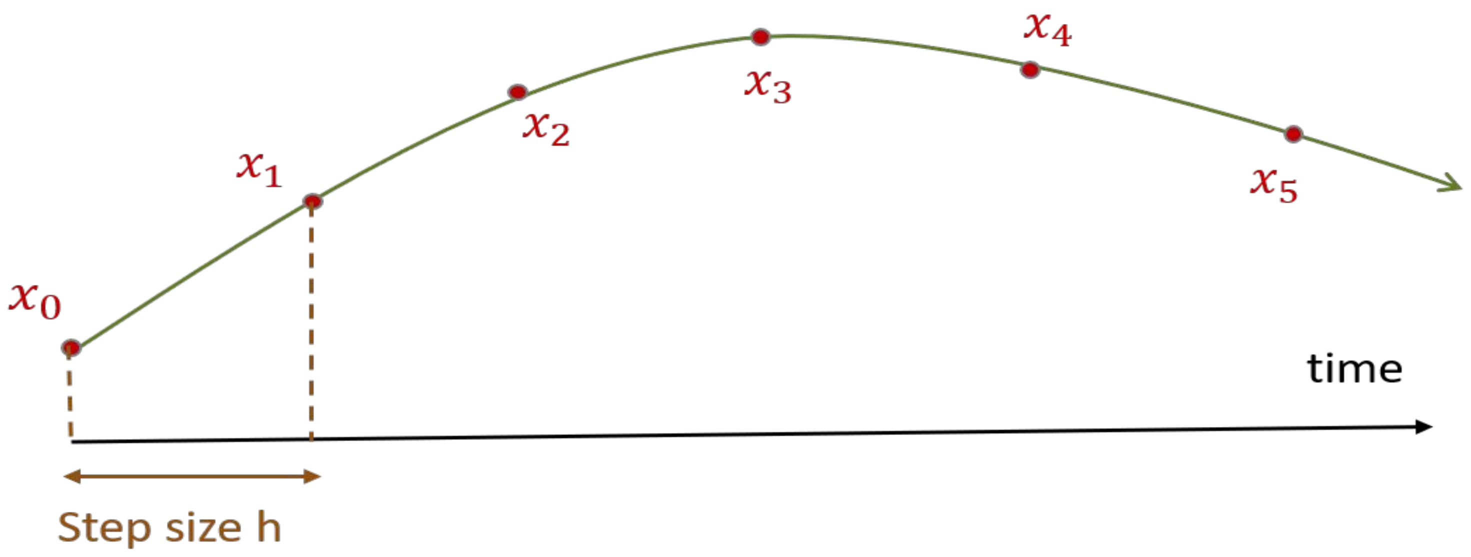
Deepest Counterexample



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 $\tau_H(x_0, h)$ = $x_0, x_1, x_2, \dots$, 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.

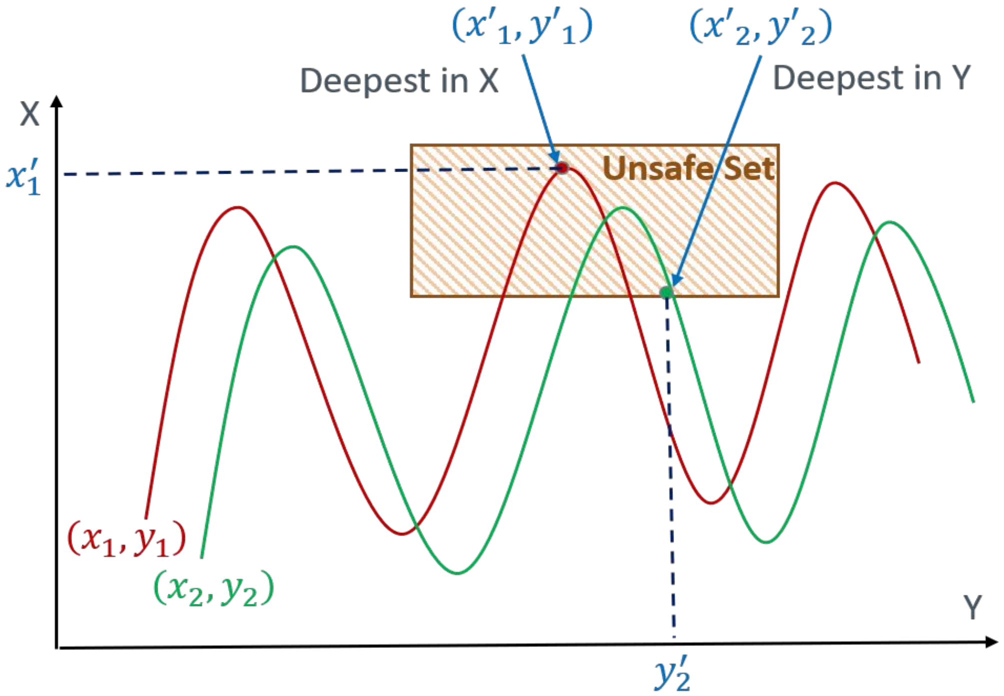
Deepest Counterexample

Given a direction v and the unsafe set U, the depth of a simulation τ is defined as

$$depth(\tau, v) = max\{v \cdot x_i \mid x_i \in \tau \wedge x_i \in U\}$$

For a direction v and a set of unsafe simulations T_U, the deepest counterexample is

$$deepest\_ce(v) = \tau \text{ such that } depth(\tau, v) \geq depth(\tau', v) \text{ for all } \tau, \tau' \in \mathrm{T}_U.$$

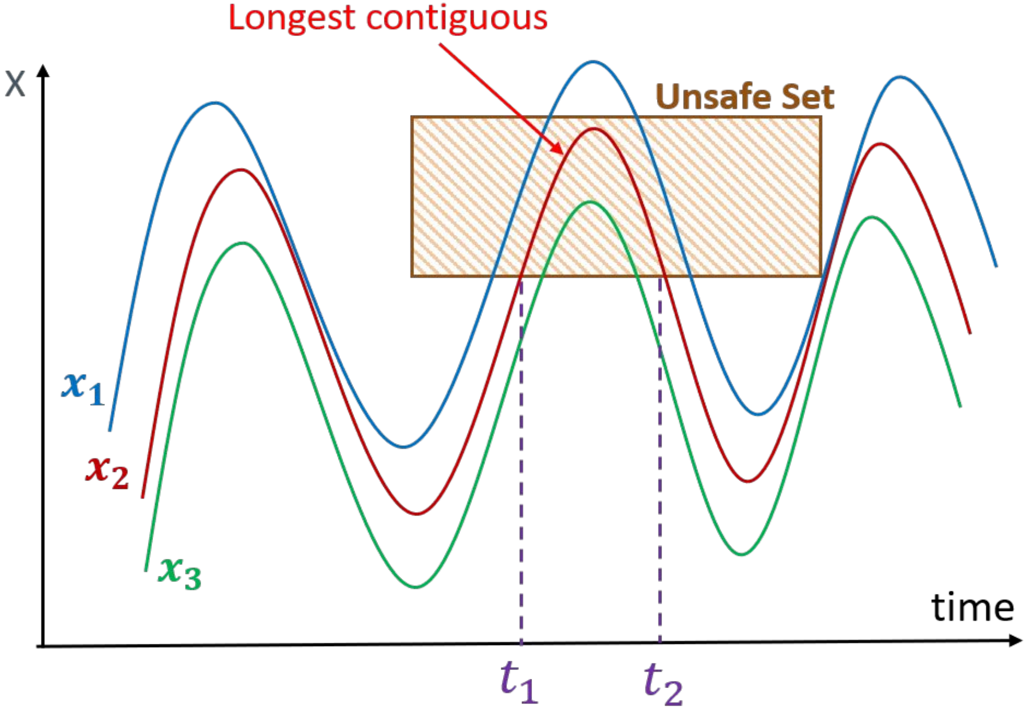


Longest Counterexample

Given the unsafe set U, the length of a simulation τ is defined as

length(τ) = *max*{ *len* | $\exists\ x_i, x_{i+1}, \ldots, x_{i+len-1}$ ∈ τ such that ∀ $i \leq j \leq i$ + *len* -1, $x_j \in U$}

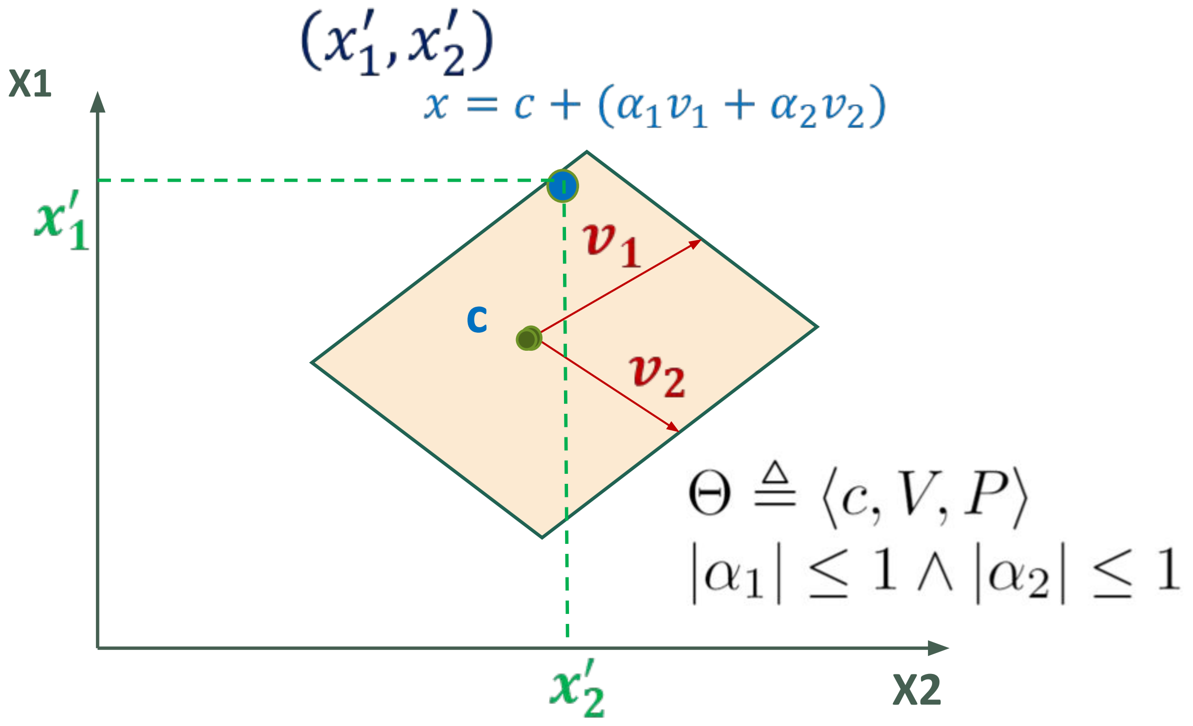
The simulation with maximum length among the set of unsafe simulations is called the longest counterexample.



Star Representation

A *generalized star* Θ 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 $P : \mathbb{R}^n \to \{\top, \bot\}$ is a predicate, defined as

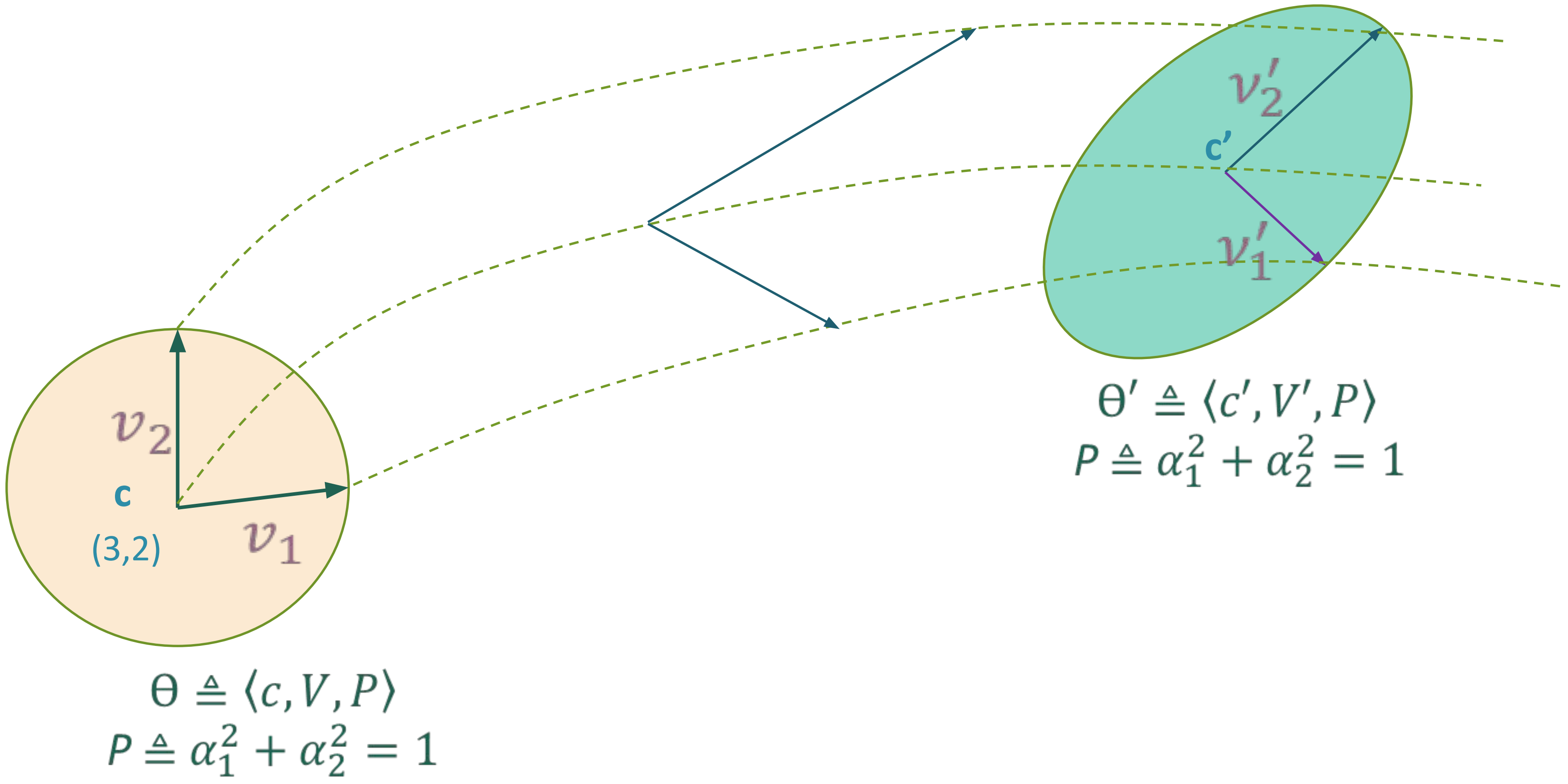
$$[\![\Theta]\!] = \{x \mid \exists\bar{\alpha} = [\alpha_1, \ldots, \alpha_m]^T \text{ such that } x = c + \Sigma_{i=1}^{n}\alpha_i v_i \text{ and } P(\bar{\alpha}) = \top\}$$



Variables

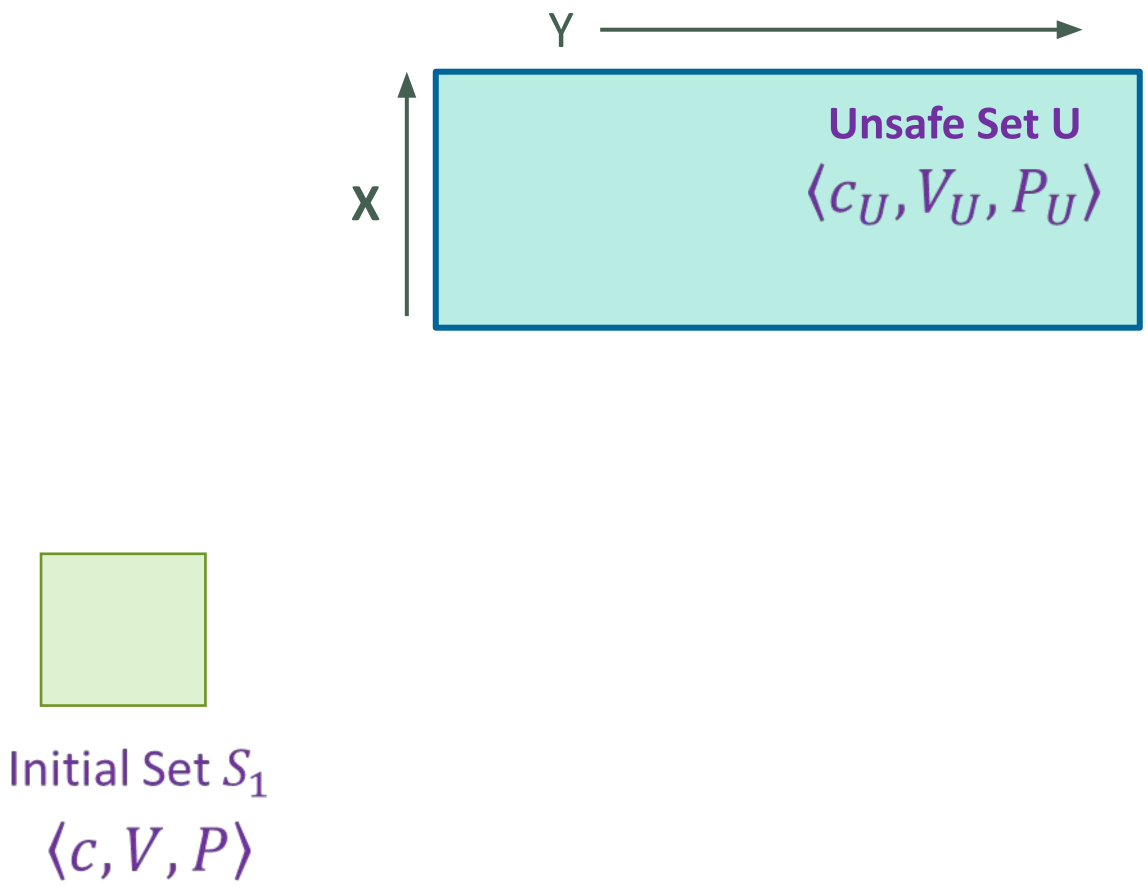
- Orthonormal: x_1' and x_2'
- Basis: α_1 and α_2

Reachable Set Computation

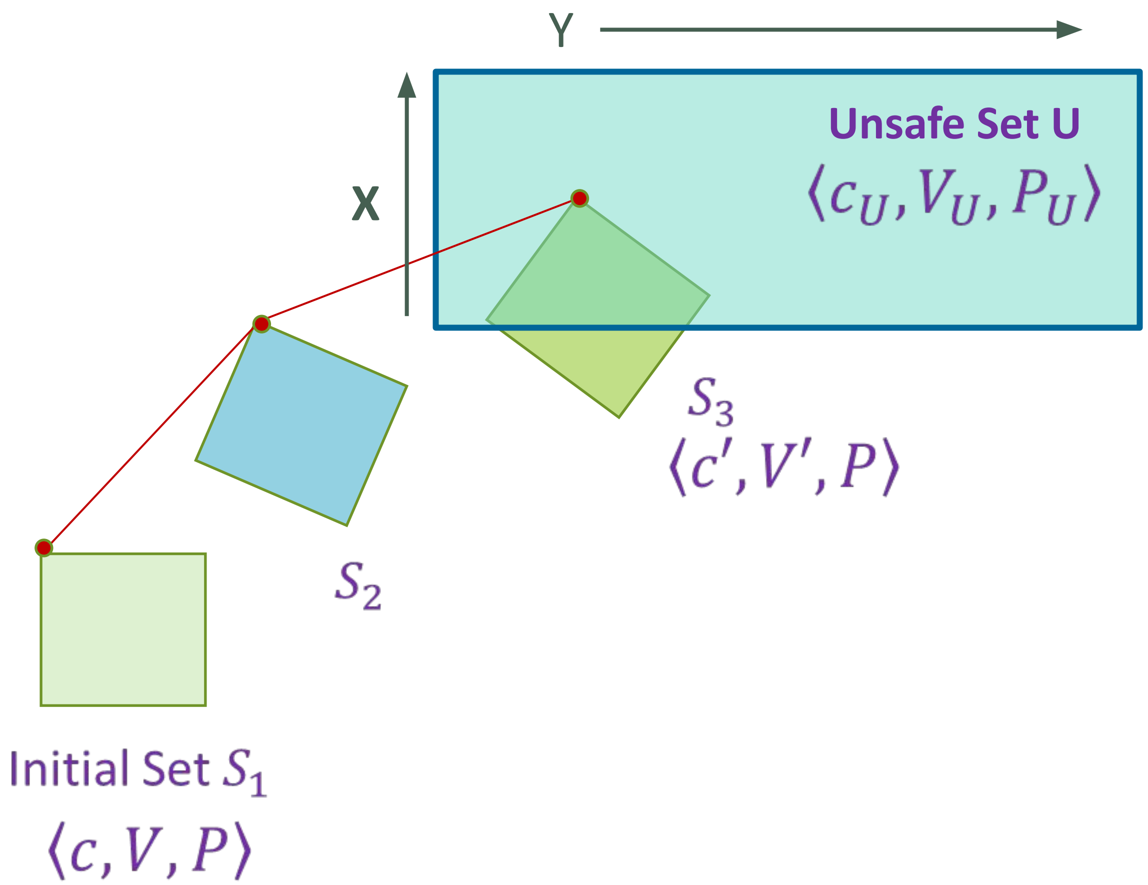


- Represented using simulations and generalized star
- The predicate P that defines reachable set remains the same

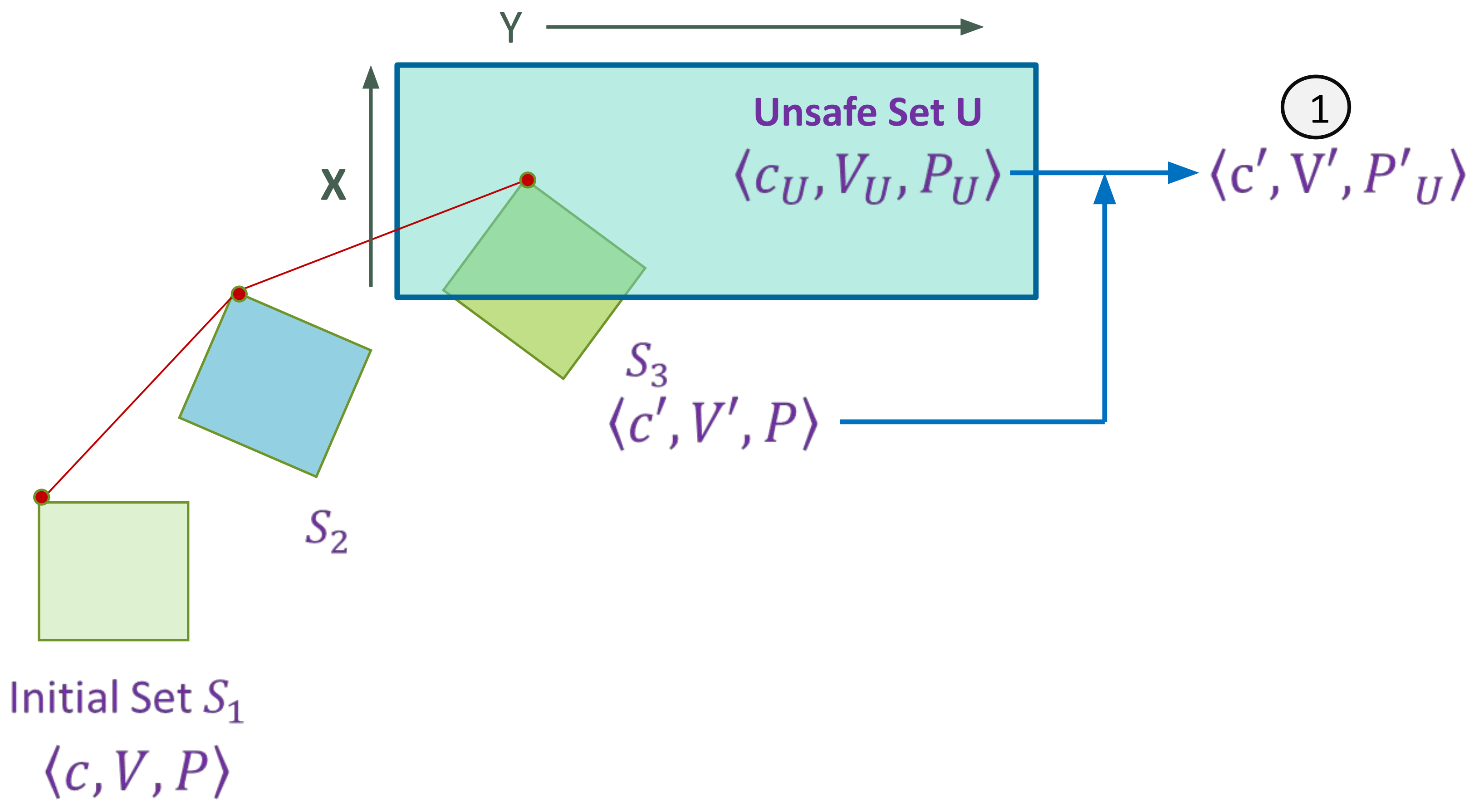
Constraint Propagation



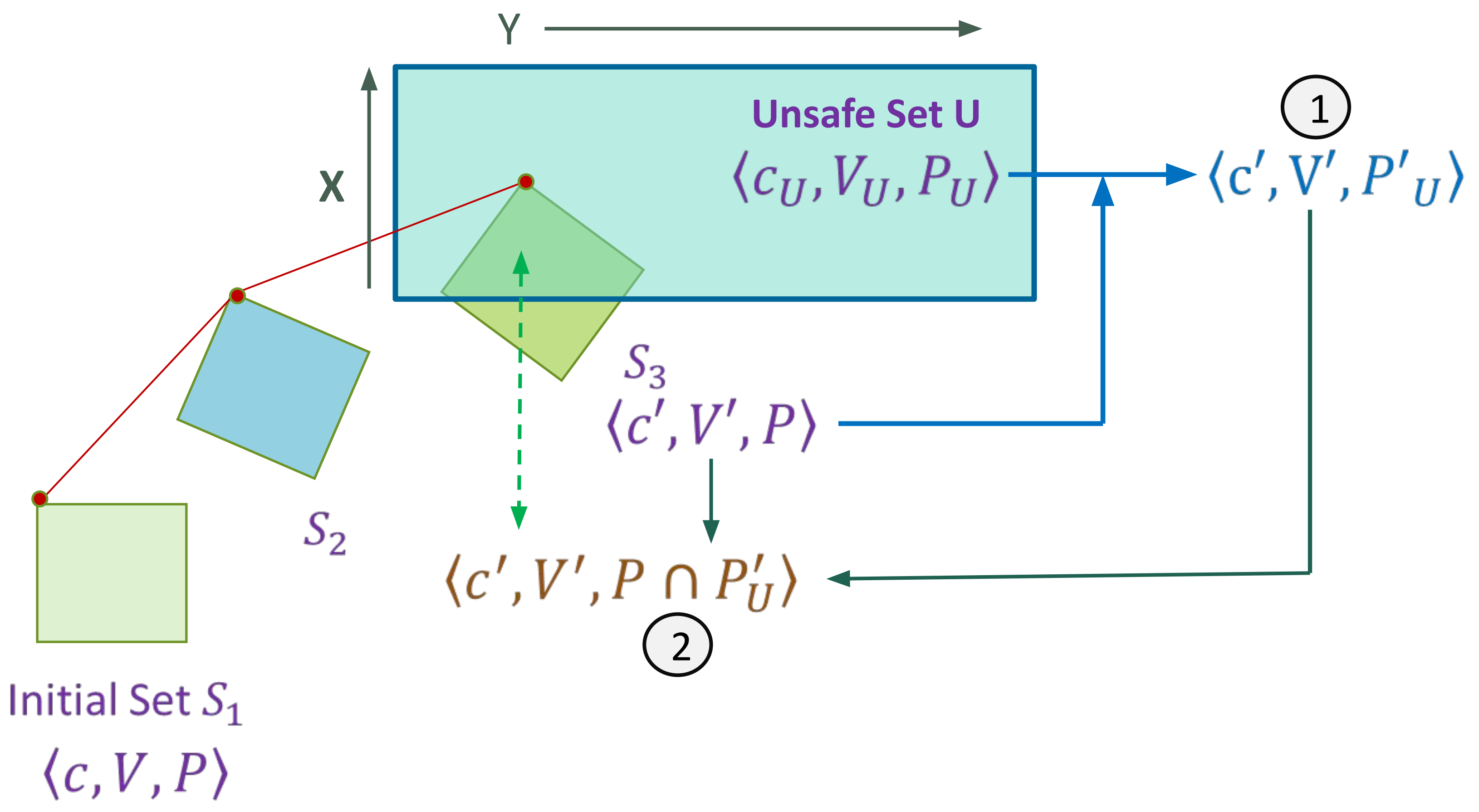
Constraint Propagation



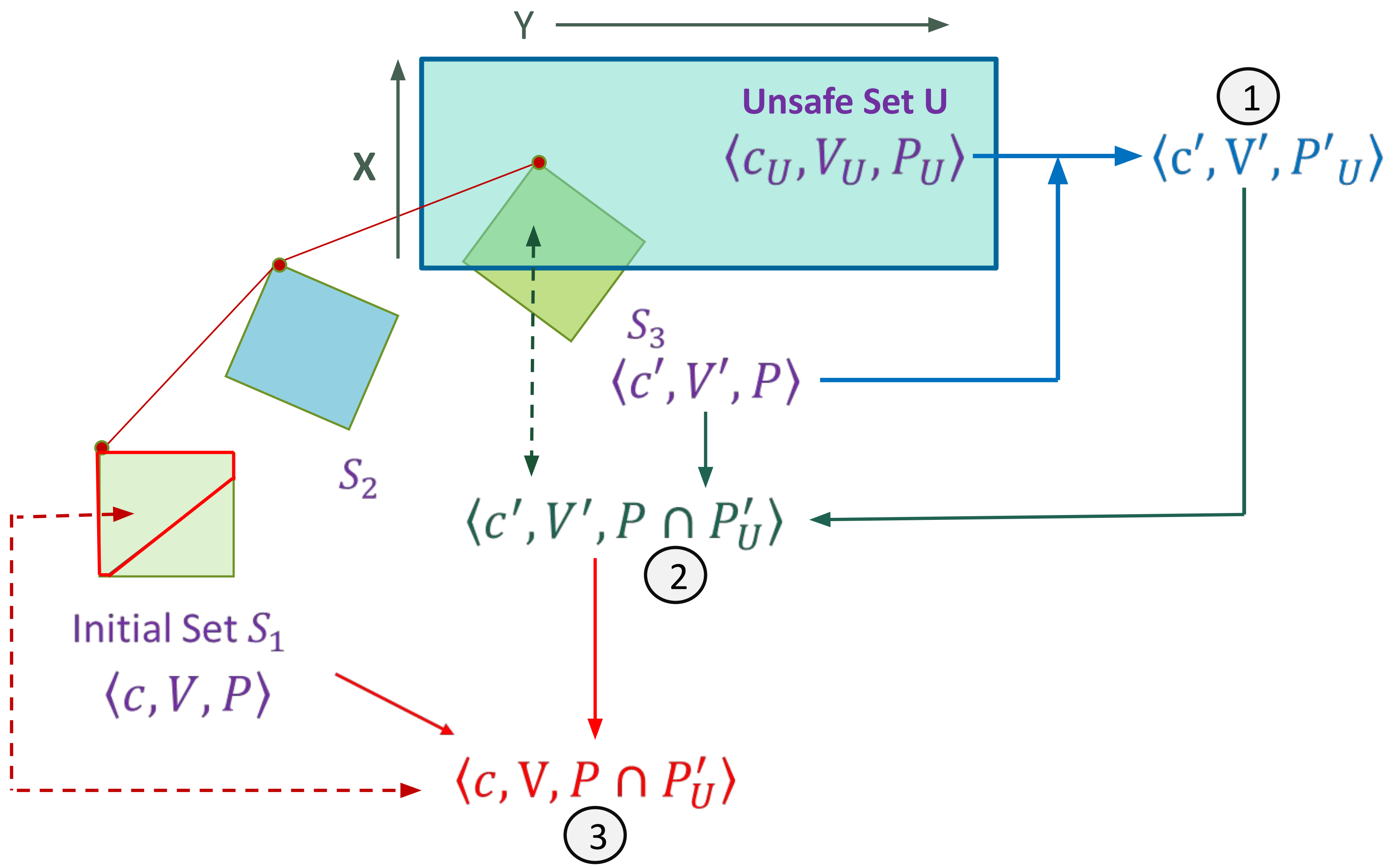
Constraint Propagation



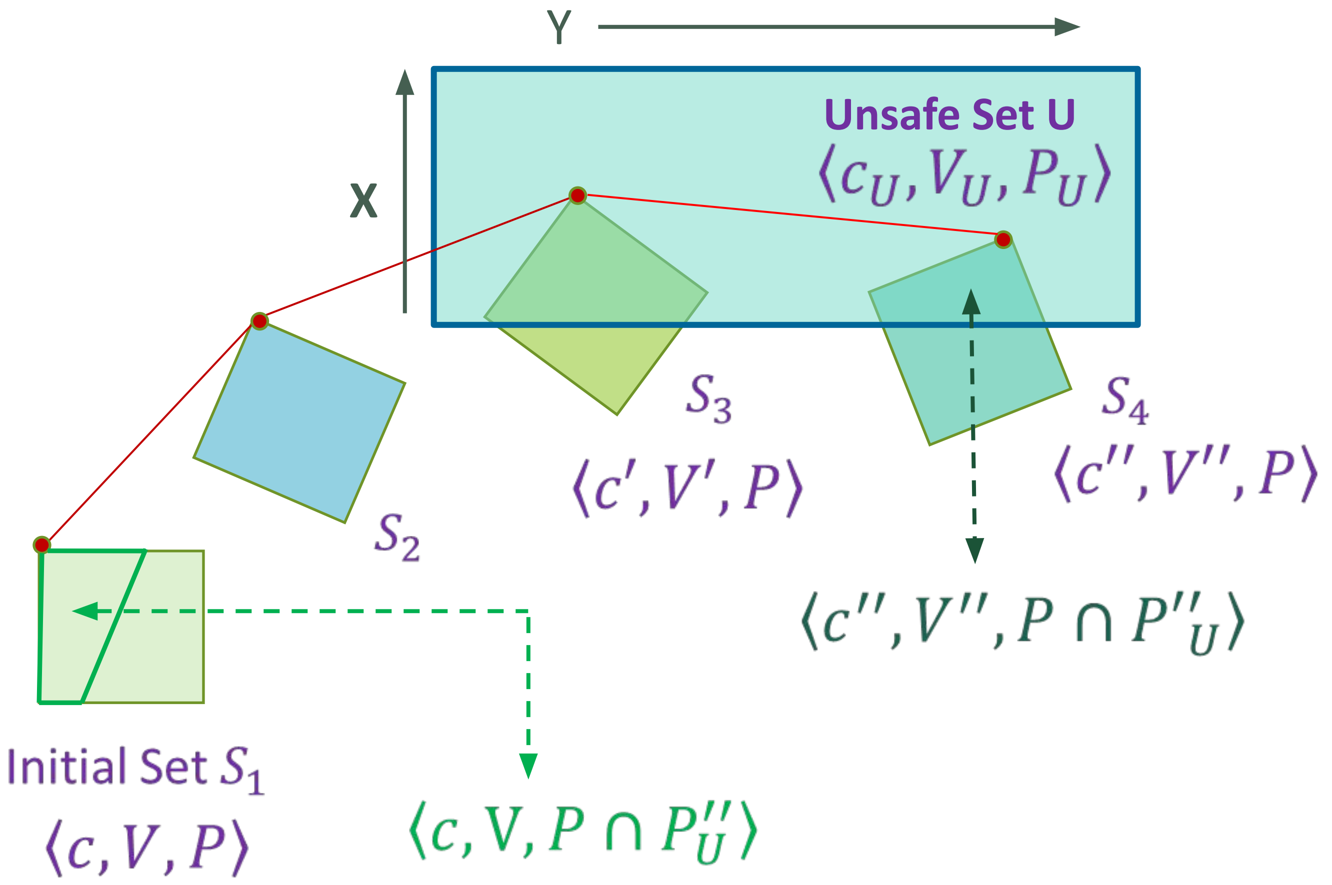
Constraint Propagation



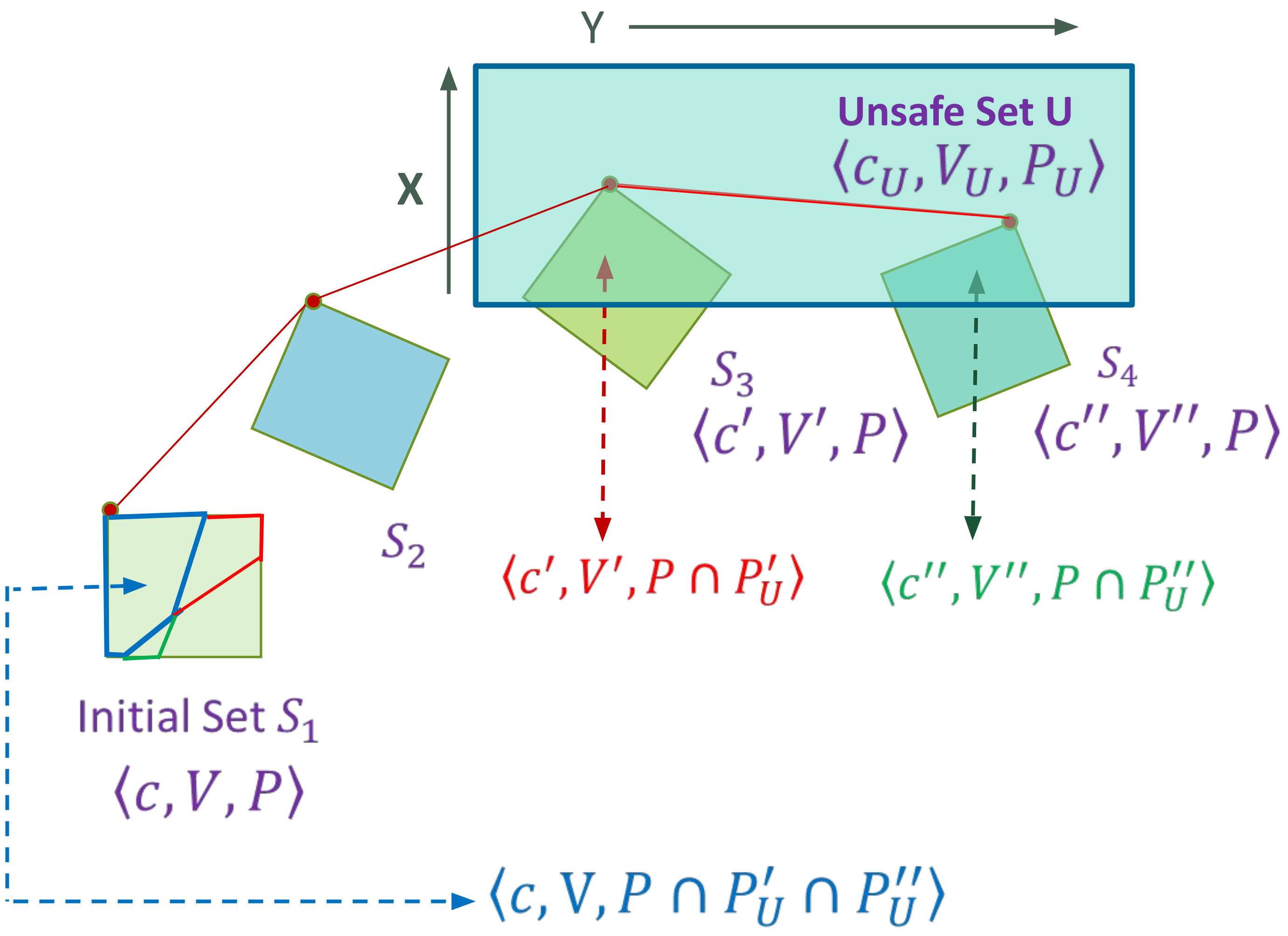
Constraint Propagation



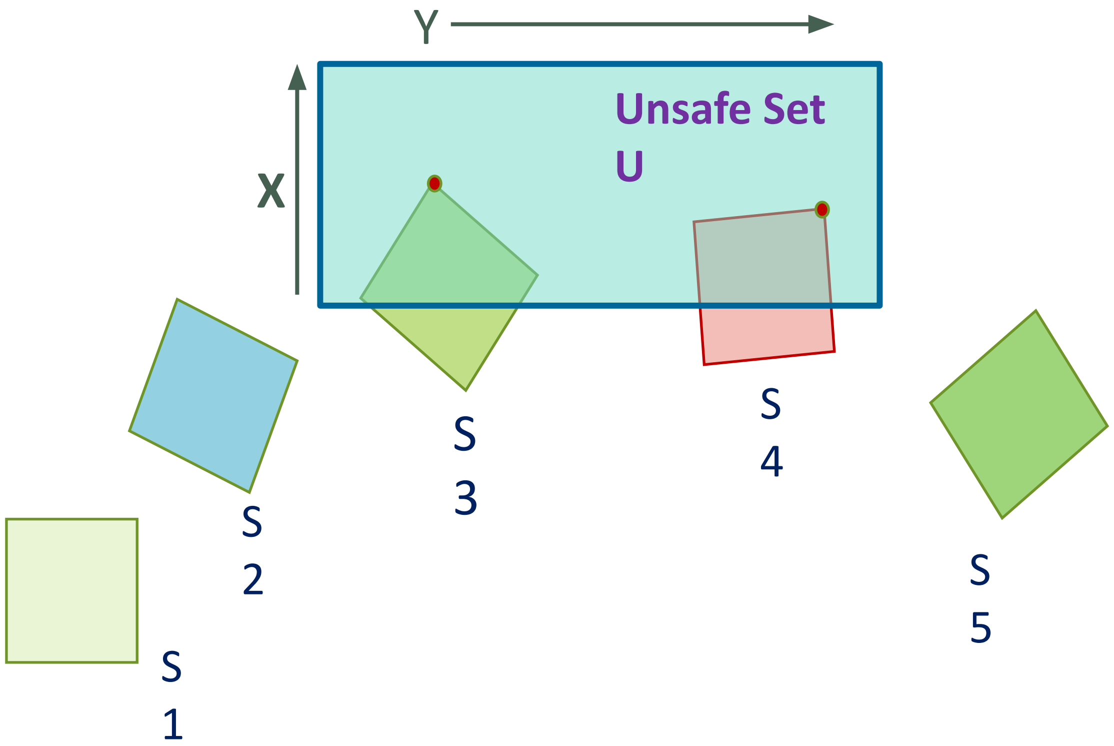
Constraint Propagation



Constraint Propagation

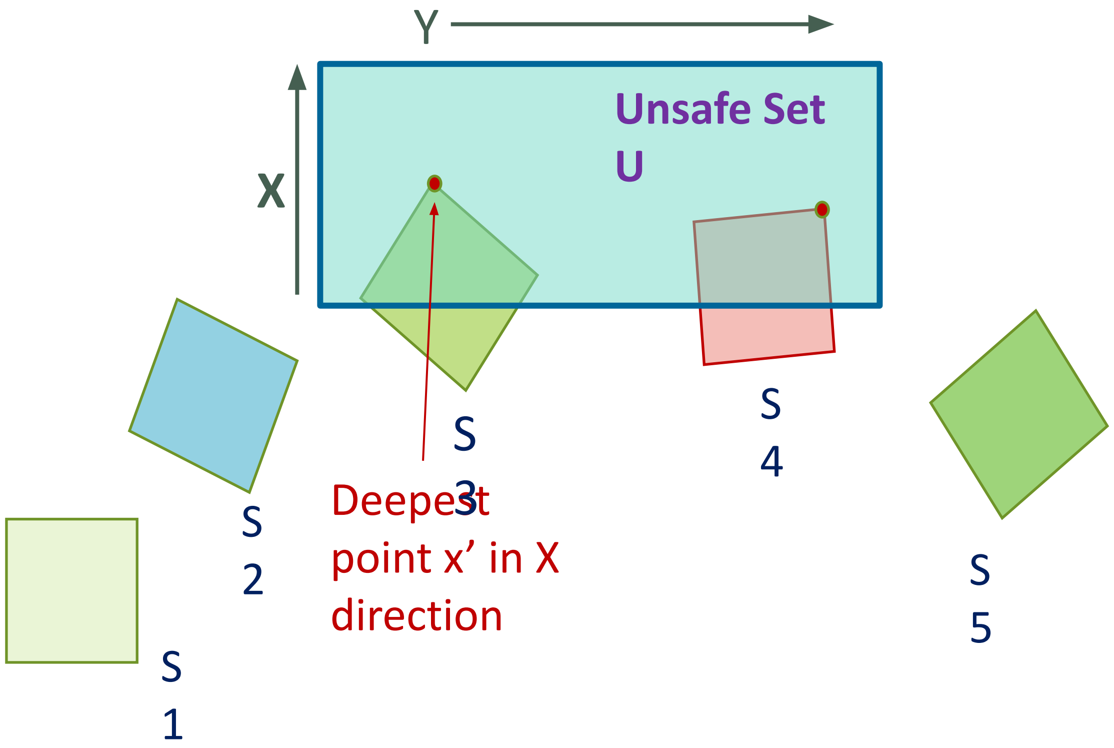


Deepest Counterexample



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

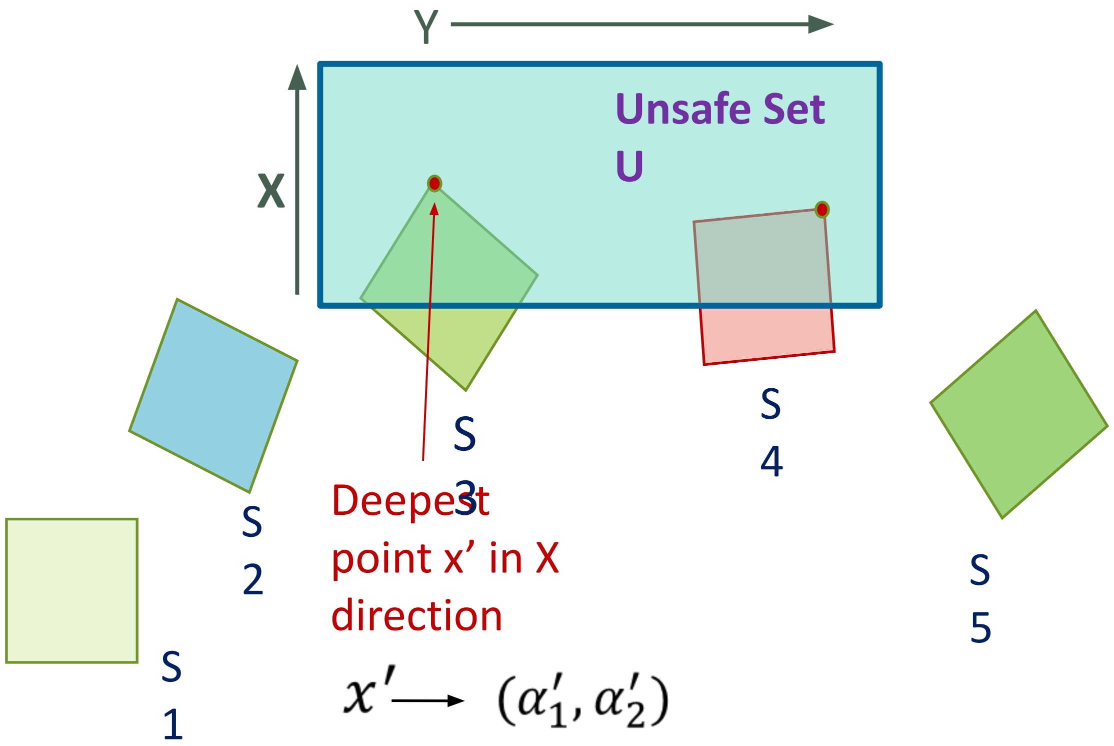
Deepest Counterexample



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

Pick the state x’ with maximum depth

Deepest Counterexample

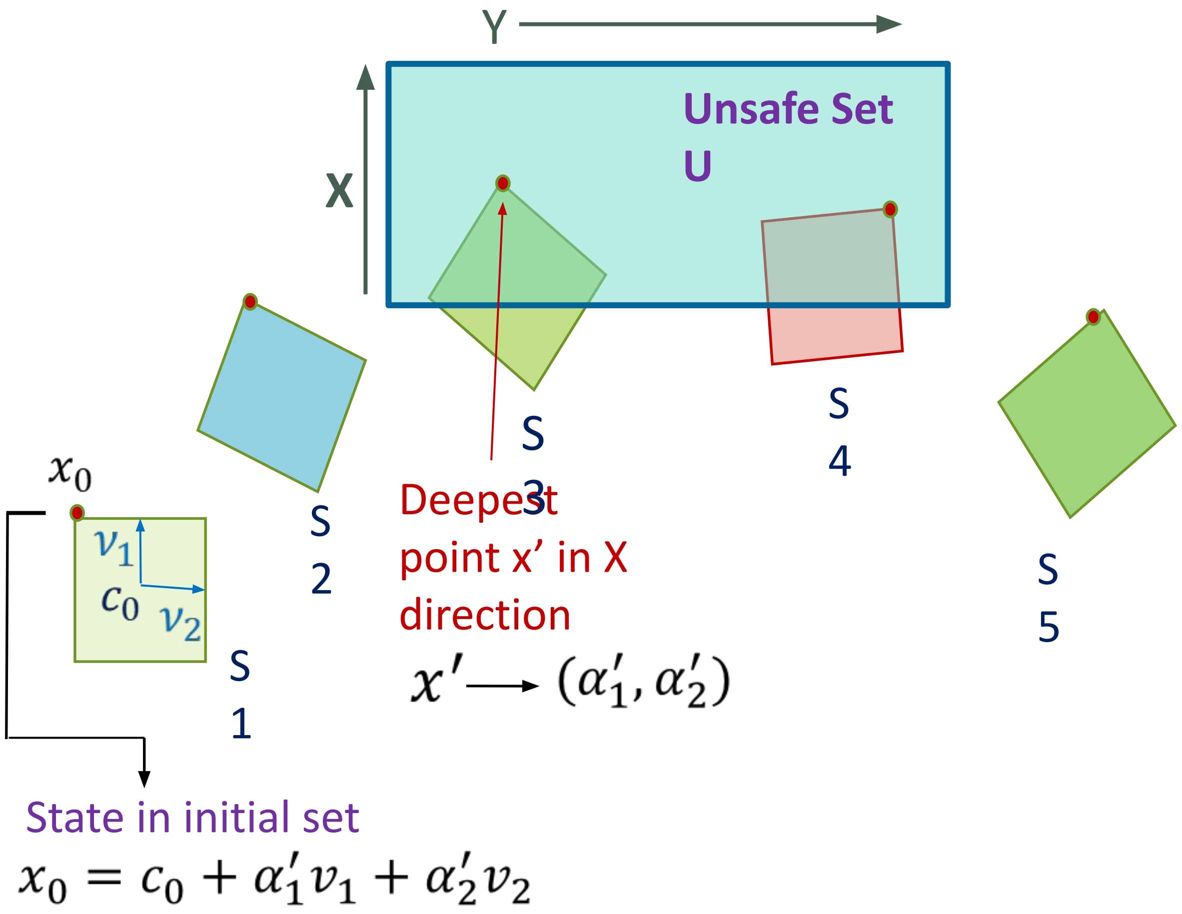


For each star S_i having $S_i \cap U \neq \emptyset$,
find depth: max {v . x_i}

Pick the state x’ with maximum depth

Convert x’ in star basis variables α'_1andα'_2

Deepest Counterexample



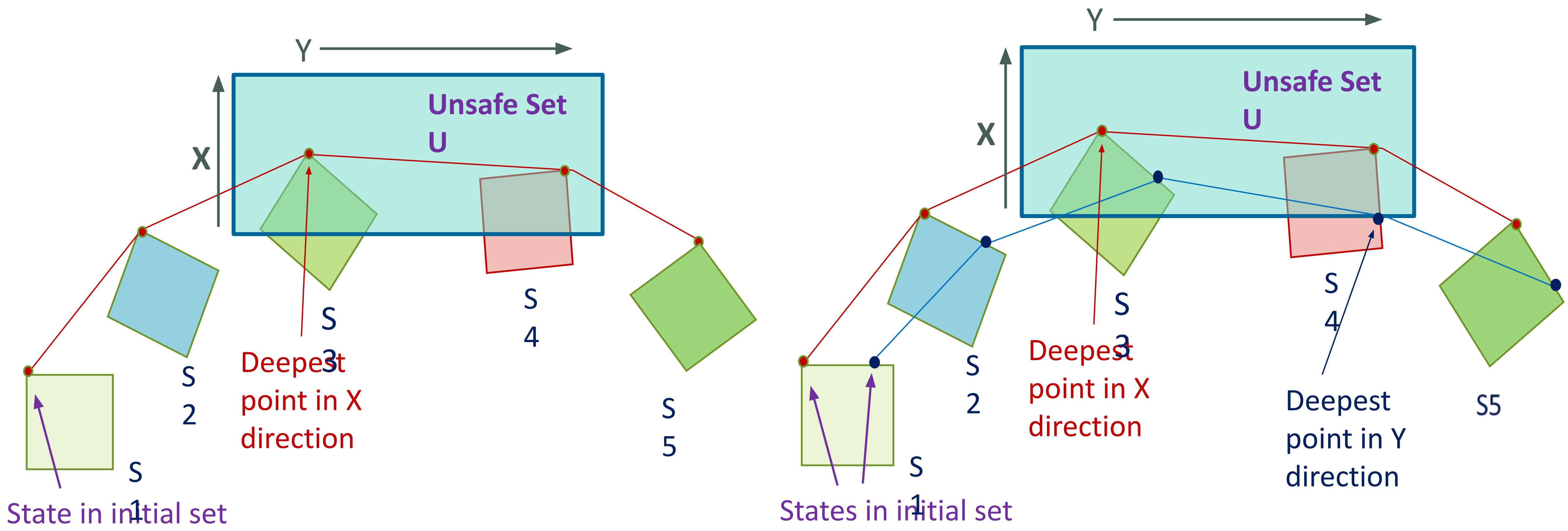
For each star S_i having $S_i \cap U \neq \emptyset$,
find depth: max {v . x_i}

Pick the state x' with maximum depth

Convert x' in star basis variables α_1' and α_2'

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

Deepest Counterexample



Deepest Counterexample: Algorithm

Input : Initial set Θ, the simulation-equivalent reachable sequence, direction v, and Unsafe set U

Output : Counterexample with maximum depth

max_depth $\leftarrow \perp$, *max_star* $\leftarrow \perp$

for each star S in the sequence **do**

  if S intersects with U **then**

    Find its *depth* in the given direction v

    if *depth* > *max_depth* **then**

      Update *max_depth* and *max_star*

      Compute corresponding basis-variables

    end

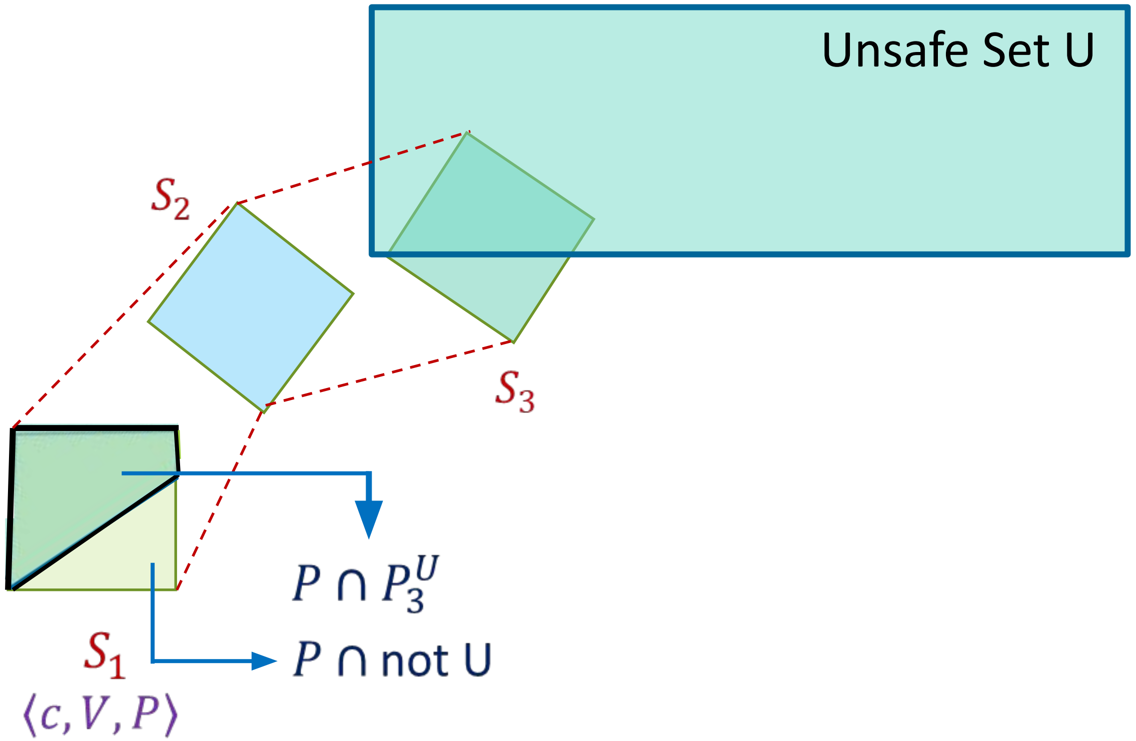
  end

end

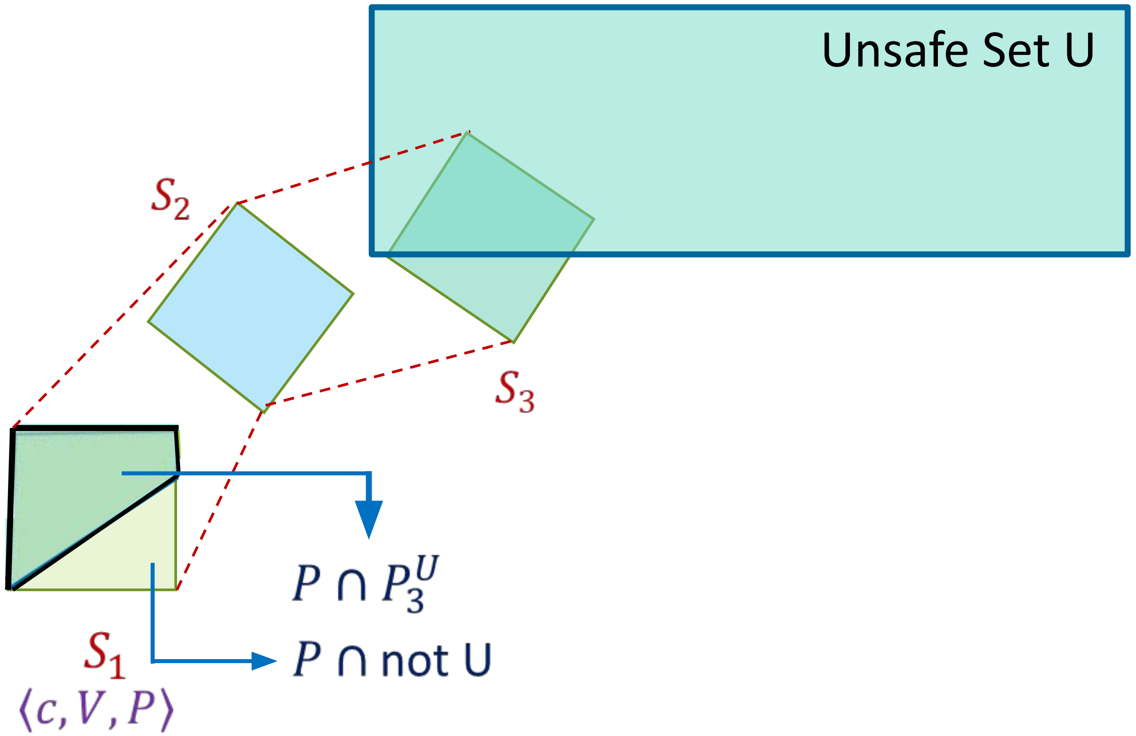
Propagate max_depth basis_variables to the initial set Θ

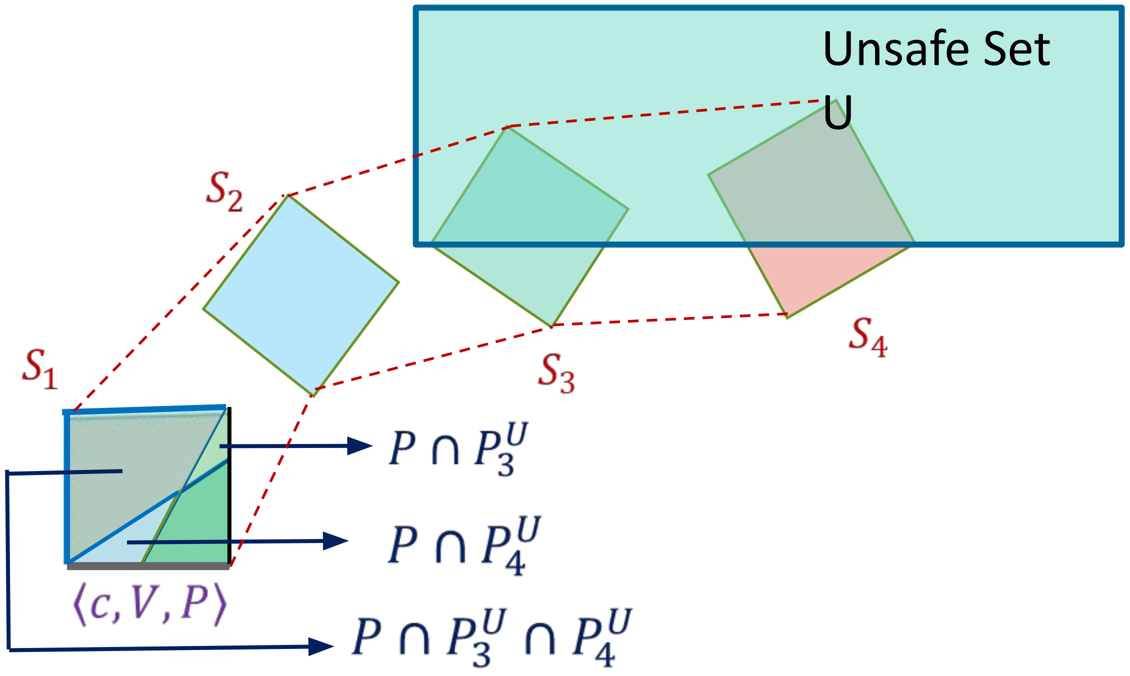
Obtain initial state as the deepest counterexample

Longest Counterexample

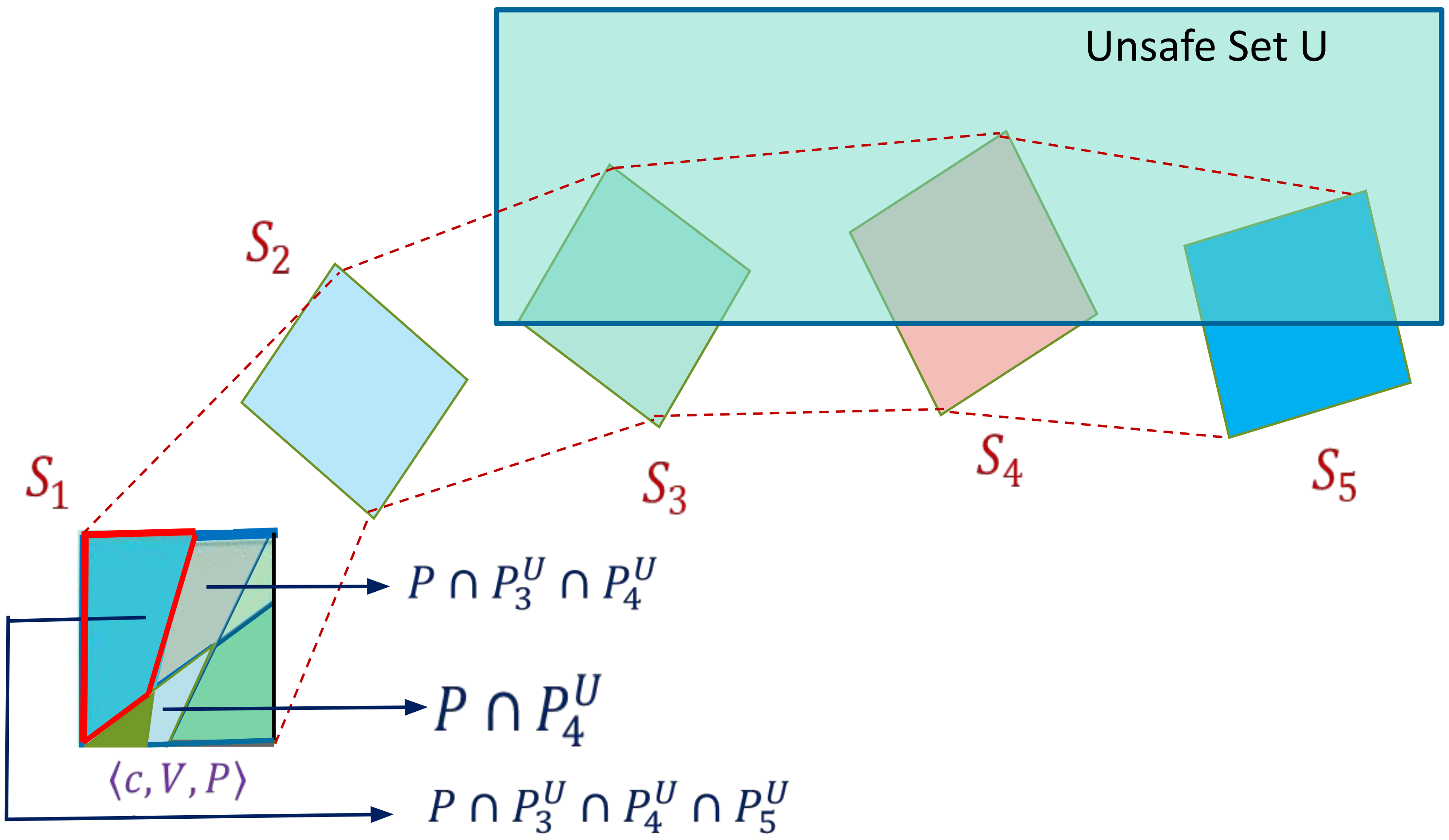


Longest Counterexample





Longest Counterexample



Longest Counterexample: Algorithm

Input : Initial set Θ, the simulation-equivalent reachable sequence, and Unsafe set U

Output : Counterexample with longest contiguous time

max_depth $\leftarrow \perp$

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 > *max_length* **then**

      Update *max_length*

    end

  end

end

Propagate constraints maximum length L subsequence to initial set Θ

Solve to obtain the longest counterexample

Benchmark: Harmonic Oscillator

- Dynamics

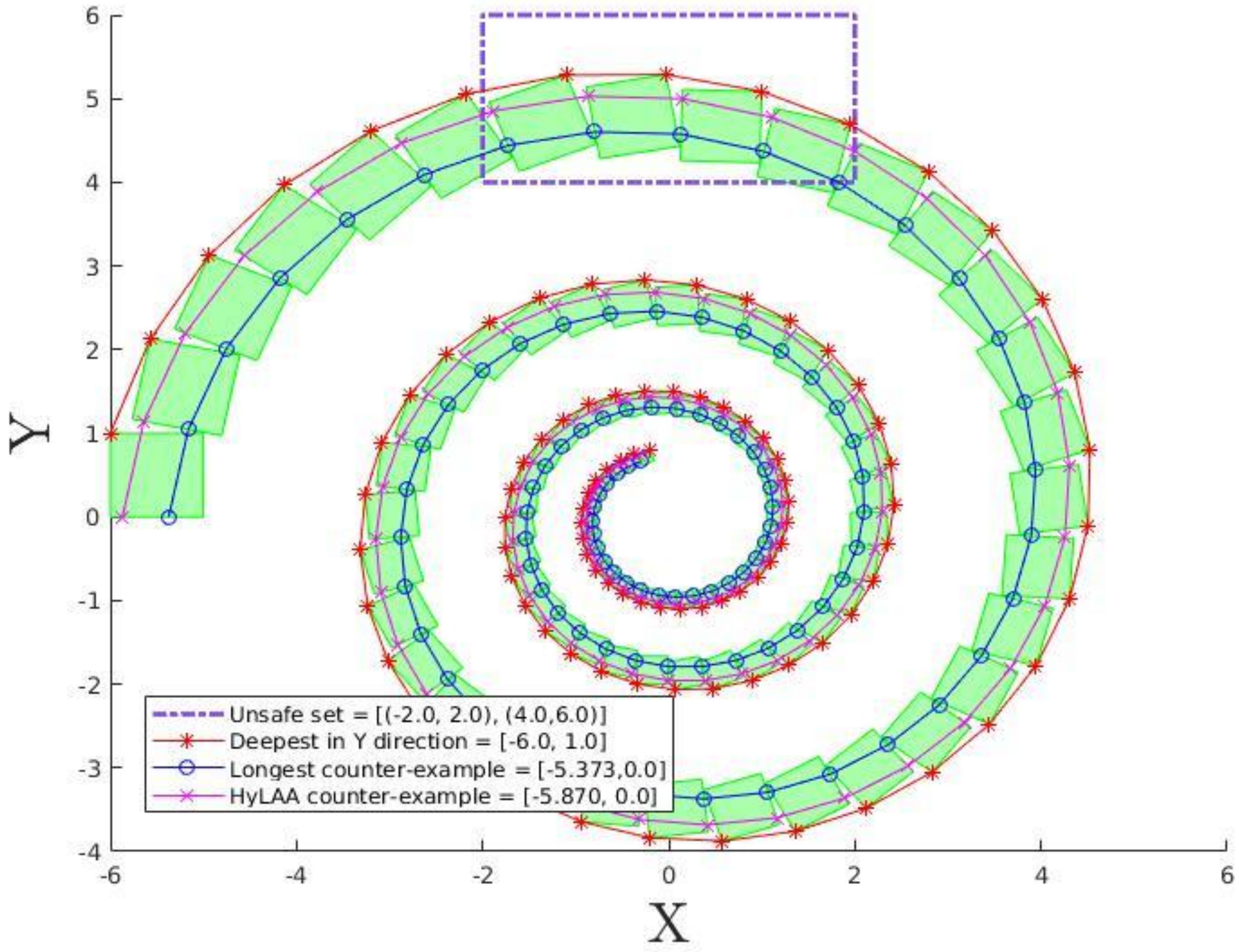
$$\dot{x} = -0.1 * x + y$$
$$\dot{y} = -x - 0.1 * y$$

- 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

$$\dot{s} = (v_l - v_f)$$
$$\dot{v}_f = a_f - k_{\mathrm{aero}} \cdot v_f$$
$$\dot{a}_f = -2 \cdot a_f - 2(v_f - v_l)$$

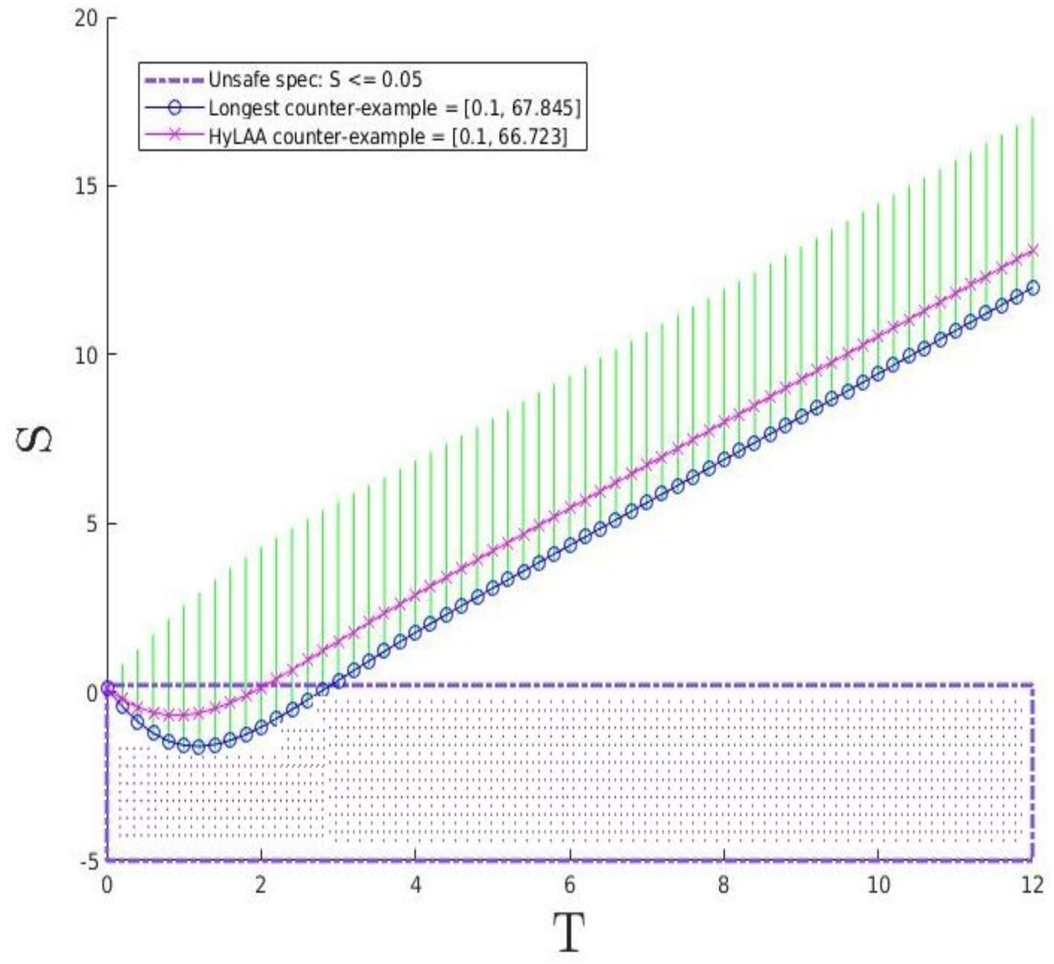
- Initial Set

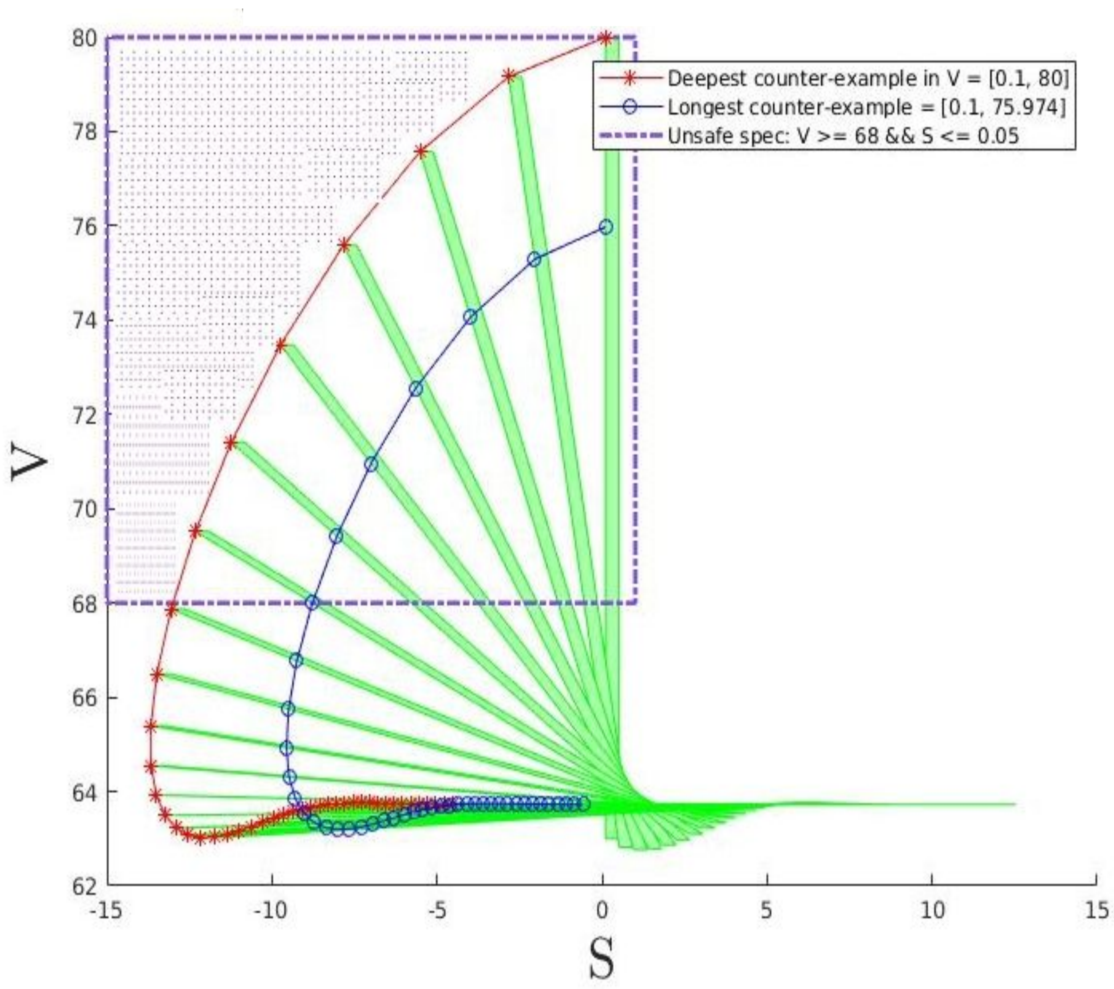
$$s \in [0.1, 0.4]$$
$$v_f \in [63, 68]$$

- Unsafe Set

$$s \leq 0.05 \; \& \; v \geq 68$$

Benchmark: Adaptive Cruise Control





Results: Deepest Counterexample

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

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

Model	Dims	Longest Counter-Example	Actual Inter. Duration	LCE Duration	Verification Time (sec)	LCE Gen Time (sec)
Damped Oscillator	2	[-5.37295 0.0]	[5 10]	[6 10]	0.17	0.01
		[-5.0 0.3968]	[4 10][33 44] [66 74]	[33 44]	0.22	0.03
		[-5 0.296]	[3 10][29 49] [59 100]	[59 100]	0.28	0.17
Vehicle Platoon 1	15	$x_8 = 1.0475$ $x_{2,5} = 1.1$ $x_i = 0.9$	[27 41]	[29 41]	1.82	0.18
		$x_{6,9} = 1.1$ $x_{12} = 1.0761$ $x_i = 0.9$	[27 73]	[27 73]	2.90	1.40
		same as above	[27 100]	[27 100]	3.51	3.78
Vehicle Platoon 2	30	$x_9 = 0.9223$ $x_5 = 1.0204$ $x_i \in 0.9, 1.1$	[42 48]	[44 48]	4.86	0.23
		$x_{19} = 1.0501$ $x_i \in \{0.9, 1.1\}$	[42, 53]	[45 53]	5.20	0.43
		$x_i = 0.9$	[36 100]	[36 100]	10.73	9.81

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

Thank you!

- 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