Counter-Example Guided Inductive Synthesis Approach for Stabilization

Hadi Ravanbakhsh
Mohamed Amin Ben Sassi   Sriram Sankaranarayanan
University of Colorado, Boulder

Problem

Dynamical System

$$\boxed{\begin{gathered}\dot{x} = f(x) \\ \dot{x} = f(x, u)\end{gathered}}$$

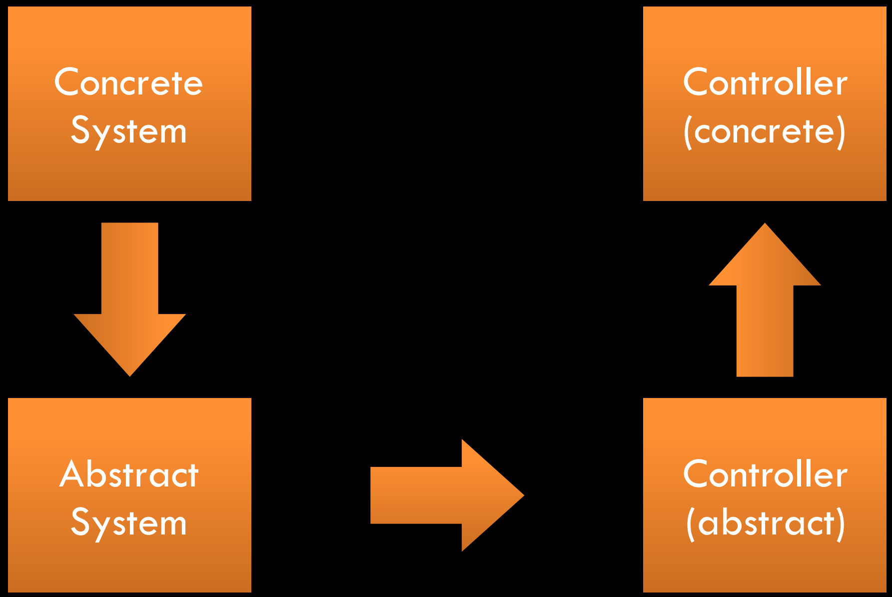
Property

Stability

Abstraction Vs Constraint based Approaches

Abstraction-Based

- PESSOA
- CoSyMA
- TuLiP
- HyNeSs
- …



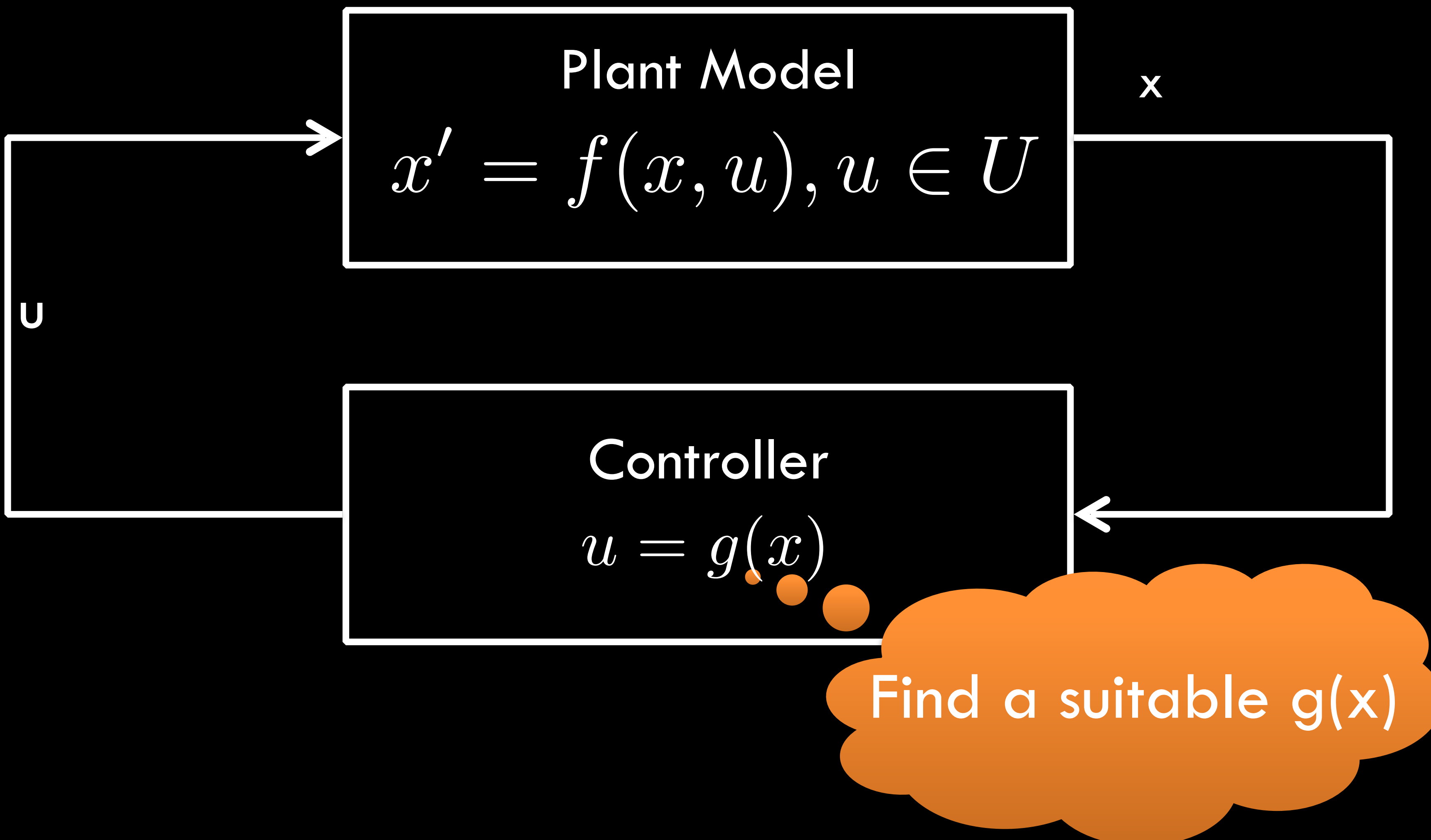
Constraint-Based

Constraint Based Techniques

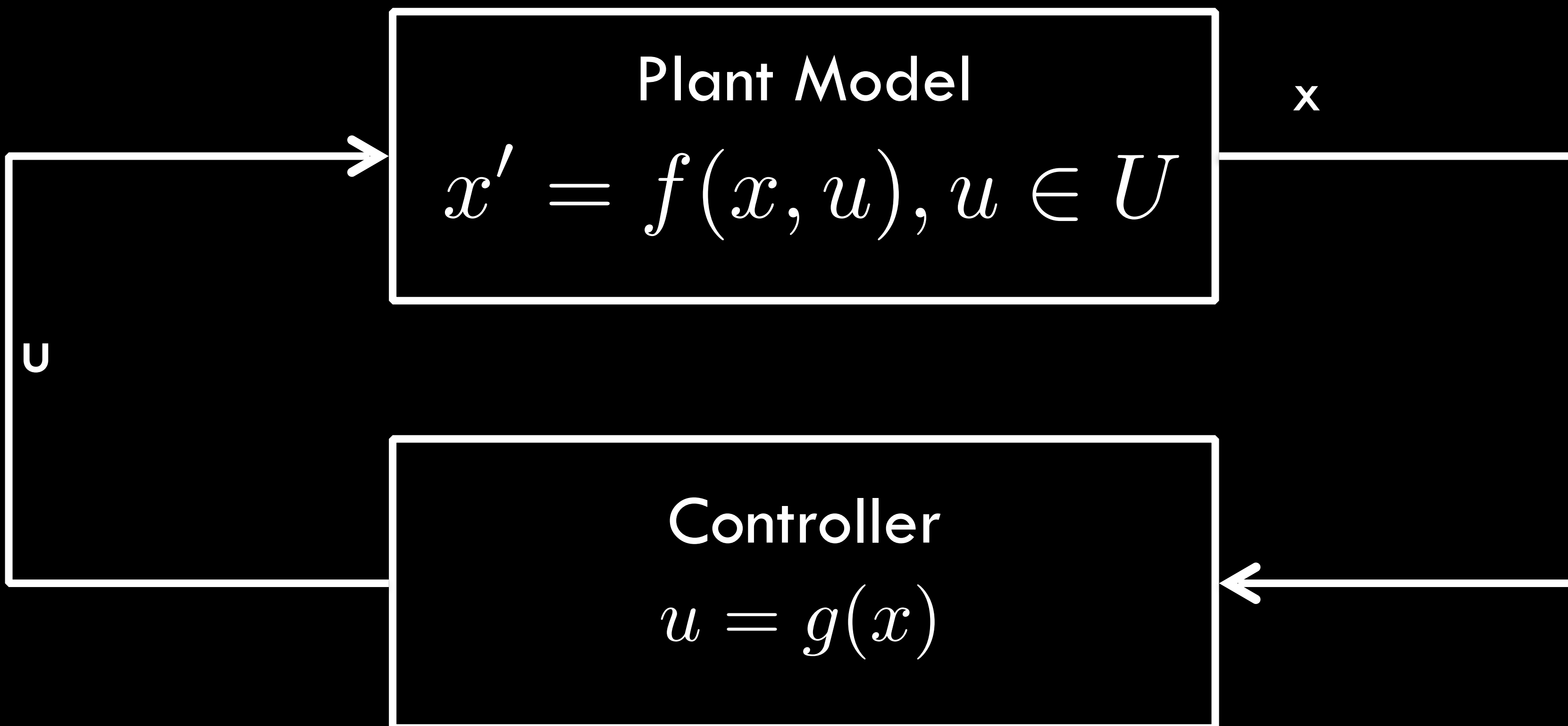
Verification	Synthesis
Certificate V	Certificate V + Control Strategy C
Find V (LMI / LI)	Find V + C (BMI / BI, ∀∃)
Prove Stability	Stabilize

Synthesis for Stabilization

Problem Setup

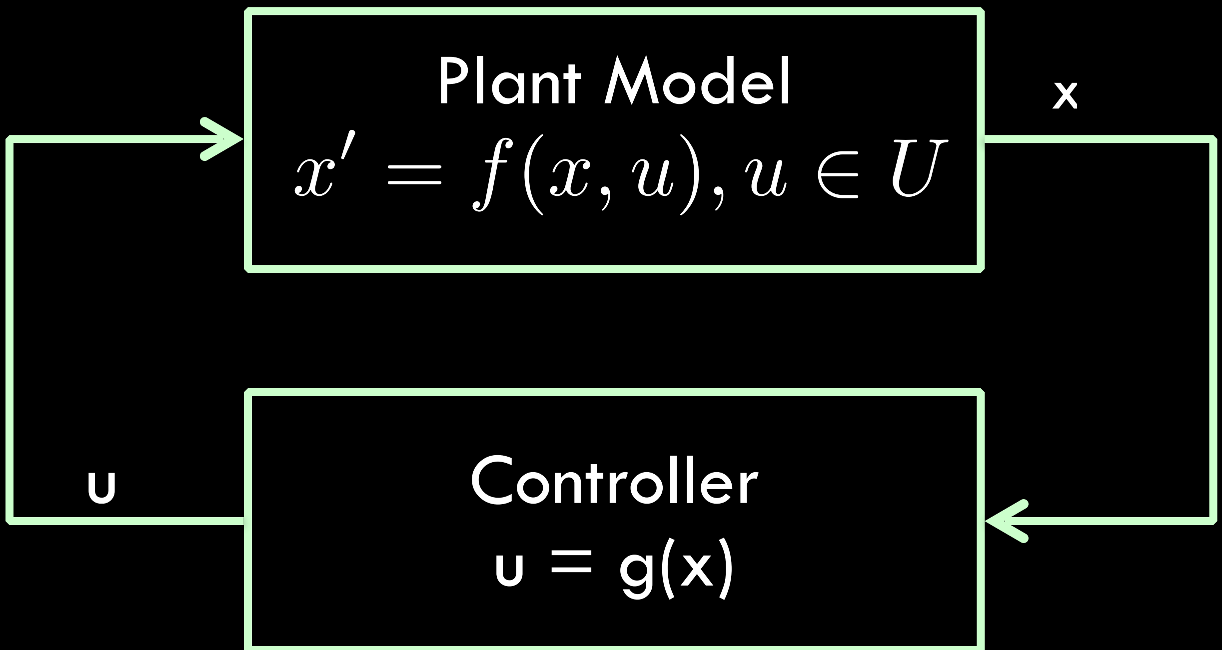


Problem Setup



Find $g(x)$ s.t. closed loop $x' = f(x, g(x))$ is asymp. stable

Static Feedback



$$V(x) = \sum_i c_i x^i$$

$$g(x) = \sum_i \theta_i x^i$$

BMI / BI

[Tan & Packard, El Ghaoui & Balakrishnan, Ben Sassi + S]

V-K iterations

Control Lyapunov Function

[Artstein; Sontag; …]

- Lyapunov function: V(x)

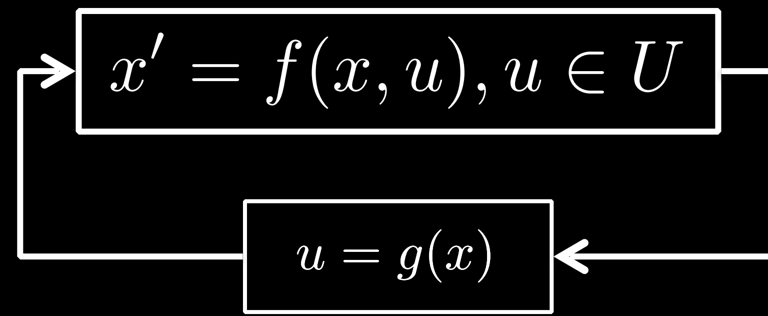
- V(x) is positive definite.

- A control input chosen s.t. derivative is negative definite.

$$\underbrace{(\forall\ x \neq x^*)}_{\forall}\ \underbrace{(\exists u \in U)}_{\exists}\ V'(x) = \nabla_x V(x) \cdot f(x,u) < 0$$

From CLF to controller

Option #1: Extract g from CLF

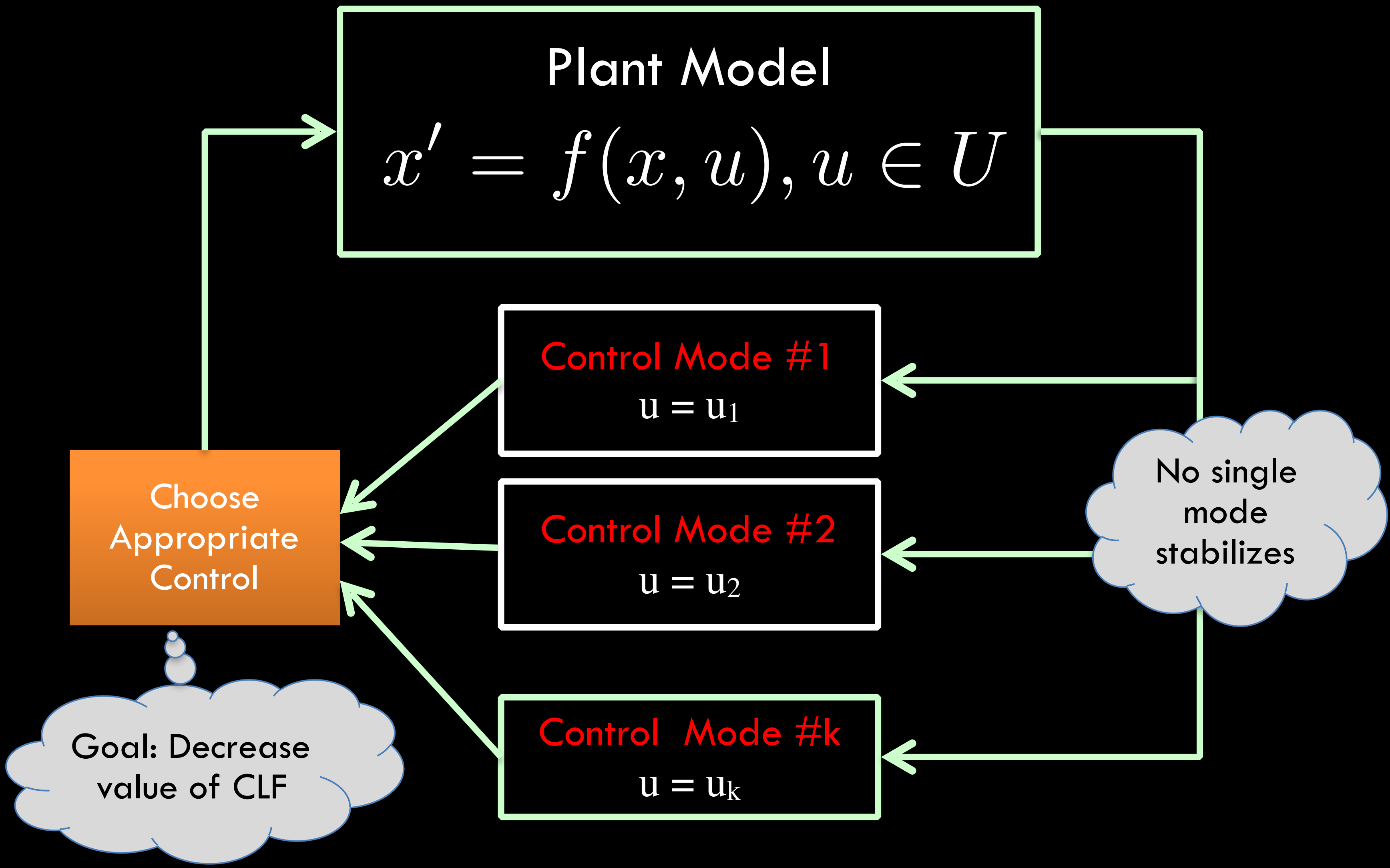


[Sontag 1989]

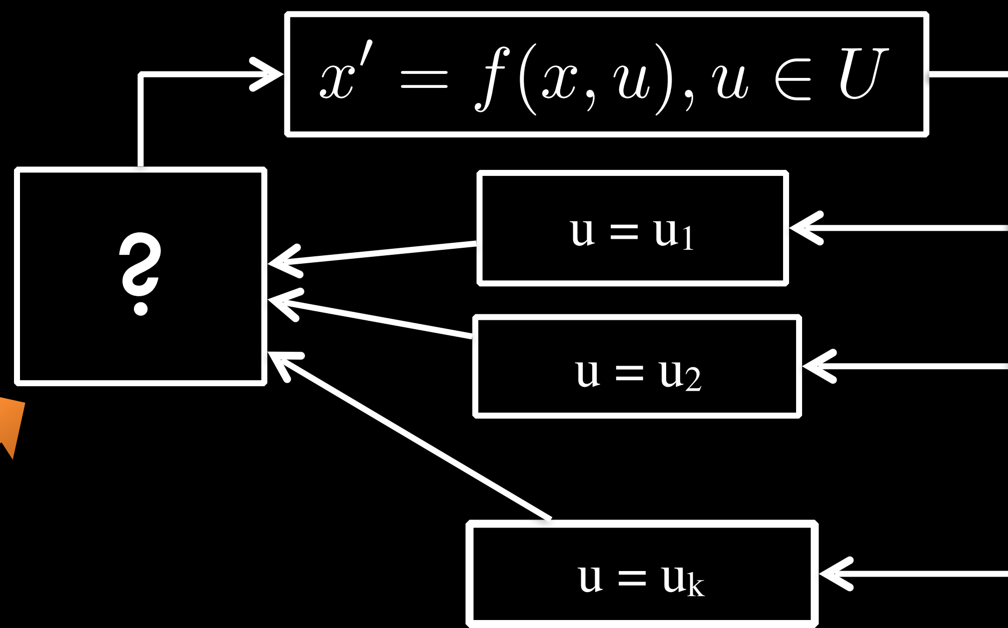
Option #2 : Dynamically choose u

Control affine inside Polytopes: finitely many value for u

Switched Stabilization



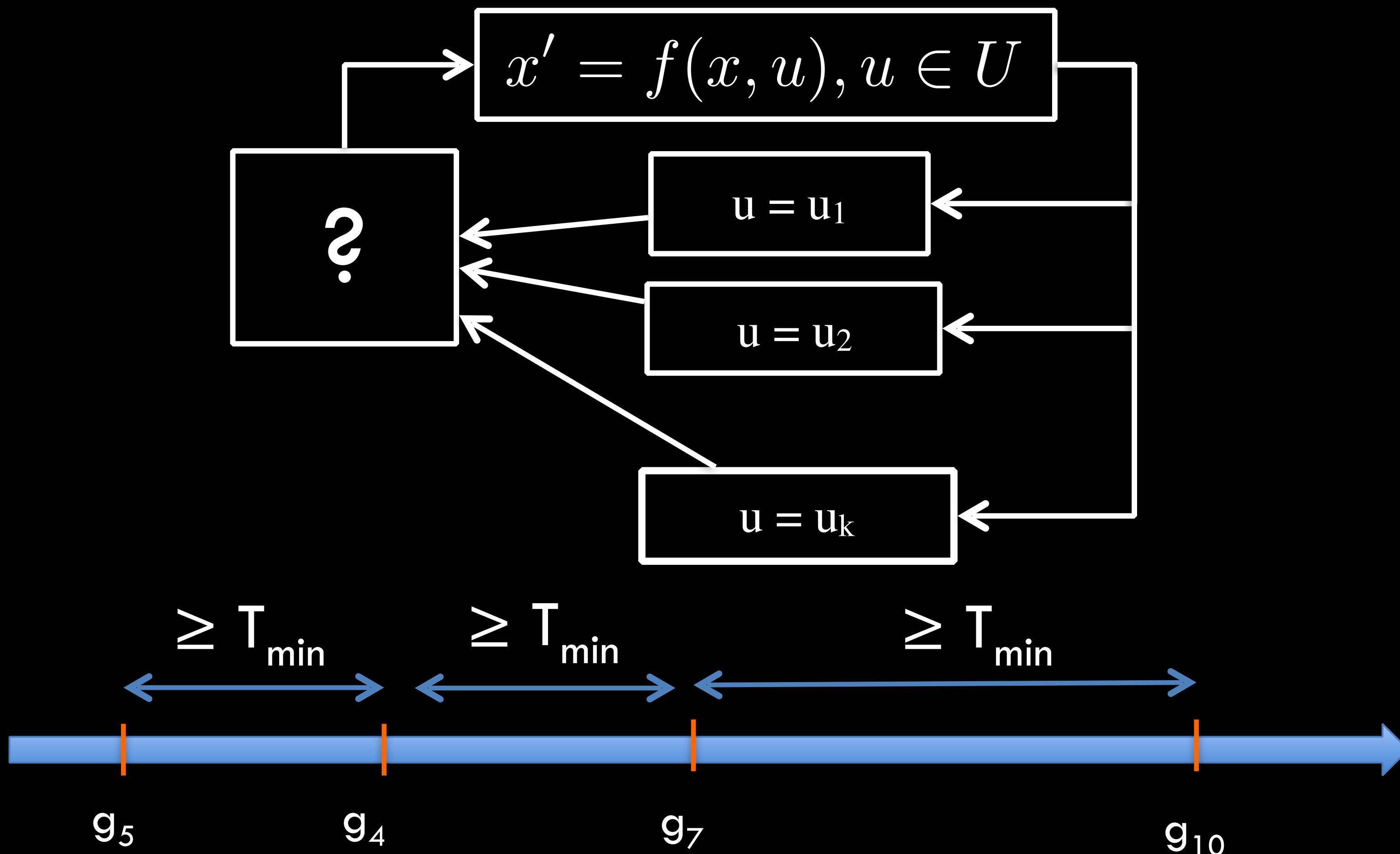
Issue: Zenoness



From $u_{1,\ldots,} u_k$ choose a mode that causes V(x) to decrease

Potentially Switch Infinitely Often in a finite time interval

Minimum Dwell Time Switching



Contribution*

- Define restrictions on CLF V s.t.
  - V(x) allows a switching strategy with a minimal dwell time.
  - Provide a lower bound for the minimal dwell time.

$$V(x) \geq \epsilon ||x||_2^2$$

$$V'(x) \leq -\hat{\epsilon}\varphi(x)$$

$$\text{Some relation between } V'' \text{ and } \varphi$$

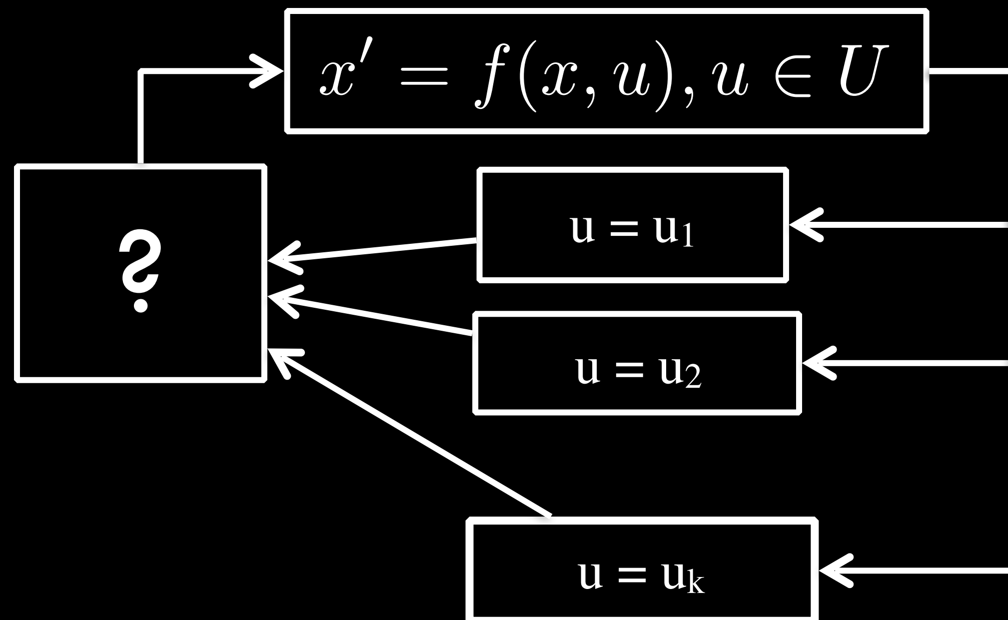
[Ravanbaksh+S'15]

Main Contribution

Discovering CLFs ($\forall\exists$)

Counter-Example Guided Inductive Synthesis.

CLF Conditions for the Switched Case



$$(\forall\ x \neq x^*) V(x) \geq \epsilon ||x||_2^2$$

$$(\forall\ x \neq x^*)(\exists i\ \in \{1,\ldots,k\}) \boxed{(\nabla V)\ f(x,u_k) \leq -\hat{\epsilon}\varphi(x)}$$

V can be made to decrease by some choice of u_i

Synthesizing CLFs

- Fix a template (ansatz) for the CLF with unknown coefficients.

$$V(x_1, x_2) : \ c_0 + c_1 x_1 + c_2 x_2 + c_3 x_1 x_2 + c_4 x_1^2 + c_5 x_2^2$$

- Enforce CLF constraints on the unknown form.

$$(\exists\ \vec{c})\ (\forall\ \vec{x})\ (\exists i \in [1, k]) \cdots$$

SOS relaxations cannot be used.

More Complex Constraints.

CEGIS Approach

Constraints to be solved: [Solar-Lezama, Alur,…]

$$(\exists c)\ (\forall x)\ \psi(c, x)$$

Template Parameters

System States

Iterative Procedure:

- Finite set X_i : $\{x_1, \ldots, x_k\}$
- Instantiate the $\forall$ quantifier

Basic CEGIS Loop

$$\boxed{(\exists c)}\ \boxed{(\forall x)}\ \psi(c, x)$$

1. Check SATisfiability of the formula:

$$(\exists c)\ \psi(c, x_1) \wedge \psi(c, x_2) \wedge \ldots \wedge \psi(c, x_k)$$

SAT, c_k

SAT, x_{k+1}

UNSAT, Failure

2. Check SATisfiability of

$$(\exists x)\ \neg\psi(c_k, x)$$

UNSAT, Success

Applying CEGIS to synthesis CLFs

$$(\exists c)\ (\forall x \neq x^*) \boxed{\begin{bmatrix} V(x) \geq \epsilon ||x||_2^2 \\ \bigvee_{i=1}^{k} (\nabla V) f(x, u_i) \leq -\hat{\epsilon}\varphi(x \end{bmatrix}}$$

1. When x is instantiated:

$$(\exists c)\ \psi(c, x_1) \wedge \psi(c, x_2) \wedge \ldots \wedge \psi(c, x_k)$$

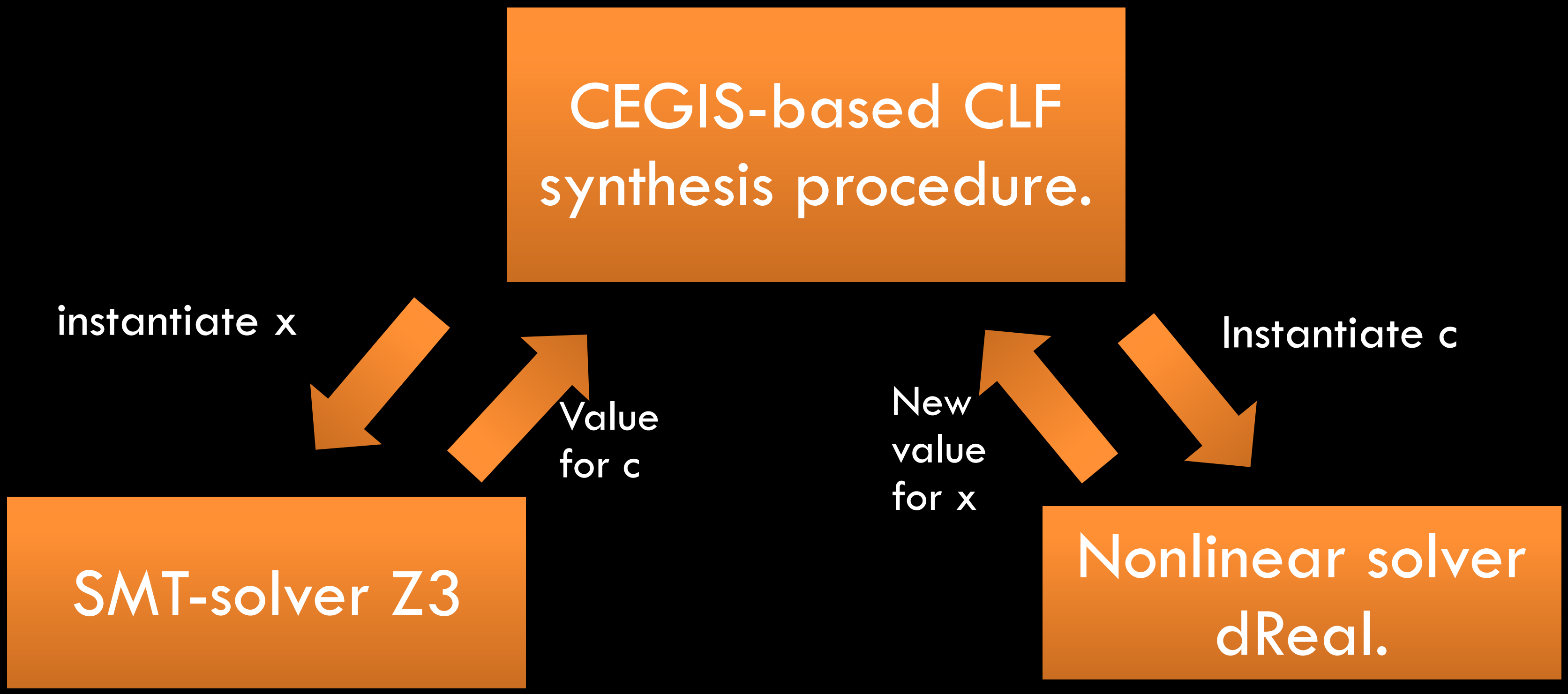
Linear Arithmetic over c.

2. When c is instantiated,

$$(\exists x)\ \neg\psi(c_k, x)$$

non-linear arithmetic over x.

Integrating SMT solvers



[De Moura et al.]

[Gao et al.]

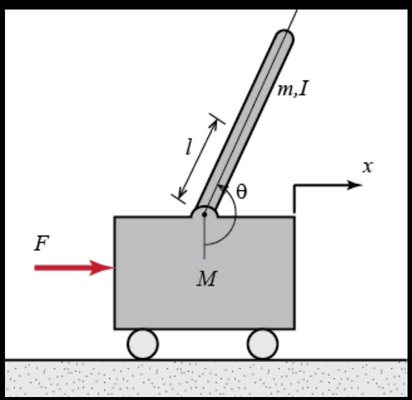
CEGIS: novelties

- CEGIS procedure is off-the-shelf. But
  - Prove *eventual termination* of the CEGIS procedure for our problem.
  - Provide heuristics to speedup termination by choosing the good counter-examples.

RESULTS

Inverted Pendulum: Bang-Bang Control Synthesis

$$\dot{\theta} = \omega, \quad \dot{\omega} = \frac{g}{l} sin(\theta) - \frac{h}{ml^2}\omega + \frac{1}{ml} cos(\theta) u\,,$$



http://ctms.engin.umich.edu/CTMS/

$$\boxed{g = 9.8,\ h = 2,\ l = 2 \text{ and } m = 0.5}$$

Control Mode #1: u = +30

Control Mode #2: u = - 30

$$\boxed{V([\theta\ \omega]^T) = 10\theta^2 + 1.5312\theta\omega + 2.5859\omega^2}$$

Discrete Controller

- min-dwell time δ
- control sampling time $\boldsymbol{\tau}$
- $\delta \geq 0.0002$s

Derive a lower-bound on δ

- $\boldsymbol{\tau} = 0.0002\text{s}$ ($\boldsymbol{\tau} \leq \delta$)

Controller for Inverted Pendulum

$$\dot{\omega} = \frac{g}{l} sin(\theta) - \frac{h}{ml^2}\omega + \frac{1}{ml} cos(\theta) u$$

$$\dot{\theta} = \omega$$

ω

θ

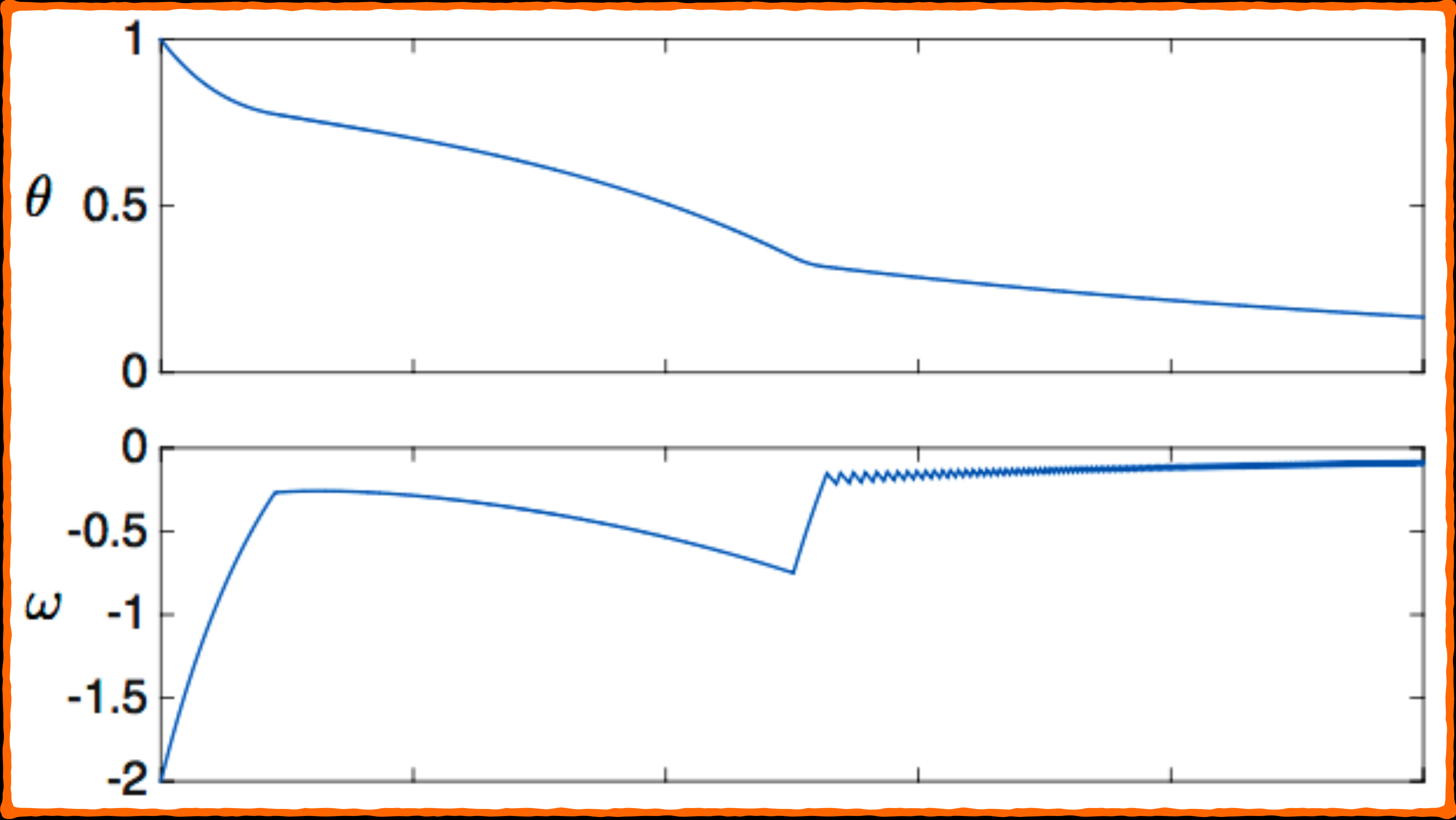
u

```
function [ur] = fcn(t, u, theta, omega)
  if(not (tau | t))
    ur = u;
    return;
  end
  if (dV(theta, omega, u) < -5*(theta^2+omega^2))
    ur = u;
    return;
  end
  ur = min_dV_u(theta, omega);
end
```

Discrete Controller

Not Switch if possible

Simulation



all Results

2-6 System Variables
2-6 control modes

benchmarks from literature switched or control affine systems

17 out of 20 benchmarks up to 3 variables

Problem			Results				
ID	n	|Q|	# itr	z3 T	dReal T	Tot. Time	Status
1	2	2	15	0,4	4,6	5,3	✔
2	2	2	15	0,5	5,6	6,6	✔
3	2	2	7	0,0	2,3	2,5	✔
4	2	5	1	0,0	0,8	0,8	✔
5	2	2	3	0,0	3,4	3,6	✔
6	2	3	13	0,1	49,2	50,0	✔
7	2	2	6	0,1	1,6	2,0	✔
8	2	2	6	0,1	3,6	4,0	✔
9	3	4	1	0,0	2,8	2,8	✔
10	3	4	8	4,4	80,0	86,2	✔
11	3	3	15	25,3	59,6	86,3	✔
12	3	5	8	8,0	41,4	50,4	✔
13	3	2	17	61,7	116,1	179,8	✔
14	3	2	36	48,1	57,3	108,4	✔
15	4	5	1	0,0	27,8	27,8	✔
16	4	2	4	TO			✘
17	4	2	4	TO			✘
18	5	6	1	0,0	649,7	650,0	✔
19	6	4	2	0,5	2994,0	2995,6	✔
20	9	4	1	TO			✘

FUTURE WORK

Future Work

- Moving to Safety + Stability Synthesis.
  – Reach While Avoid Properties.
- Handle more general temporal objectives
- Control of Stochastic Systems.

Thank You

Supported in part by US NSF CAREER Award # 0953941.