Frontier: Collaborative Research: Correct-by-Design Control Software Synthesis for Highly Dynamic Systems

Jessy Grizzle, Aaron Ames, Hartmut Geyer, Huei Peng, and Paulo Tabuada

A Classical to Modern Transition

- Classical control geared toward
  - Asymptotically stabilize a point or set
  - Track a set of trajectories
  - Create and stabilize periodic behavior
- Modern engineered systems
  - require the composition of these classical components to meet higher level objectives
- Design requirements typically written in plain English, specifying desired sequence of intermediate objectives
  - start-up and shut-down
  - different modes of operation (e.g., adaptive cruise controllers)
  - priority requirements among conflicting objectives (e.g., safety critical components always take precedence over comfort)

NSF **CPS**

A Classical to Modern Transition

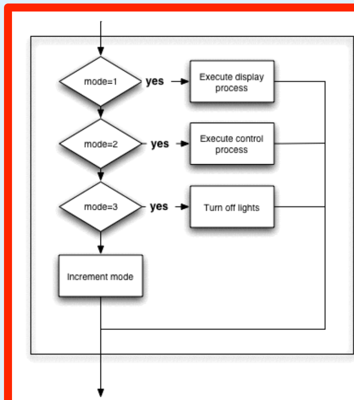
- Outstanding engineers write software attempting to <u>choreograph</u> a suite of classical controllers…

- …to produce complex controllers fulfilling all the design requirements.

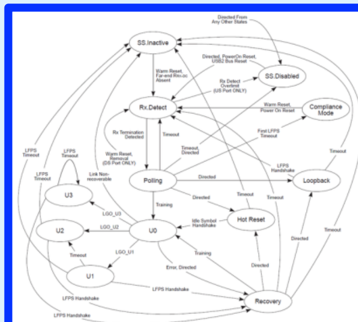
- At least we hope!

- Help! Verification required!

IF-THEN-ELSE



State Machines



Deadlock!

Big Picture: Our Project

CPS

- "Choreography" in English replaced by a **specification in a formal logic (LTL)**

- From specification, **synthesize control software**

  - **that is correct by construction.**
  - for systems of ODEs
  - with time-critical safety requirements…

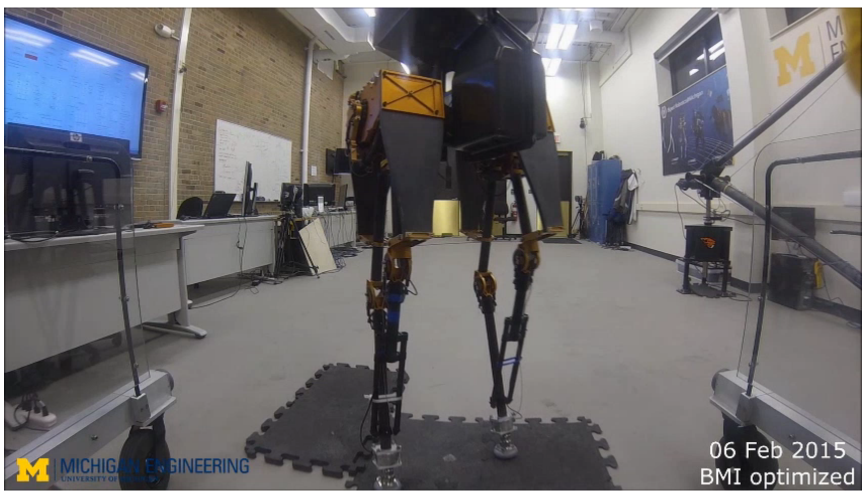
- Evaluate on hardware---robotics and automotive

CPS

Big Picture: Bipedal Locomotion

- Robotics: bipedal locomotion

Understanding how to formally realize guarantees on dynamic locomotion can allow for richer interactions between humans and robots



→

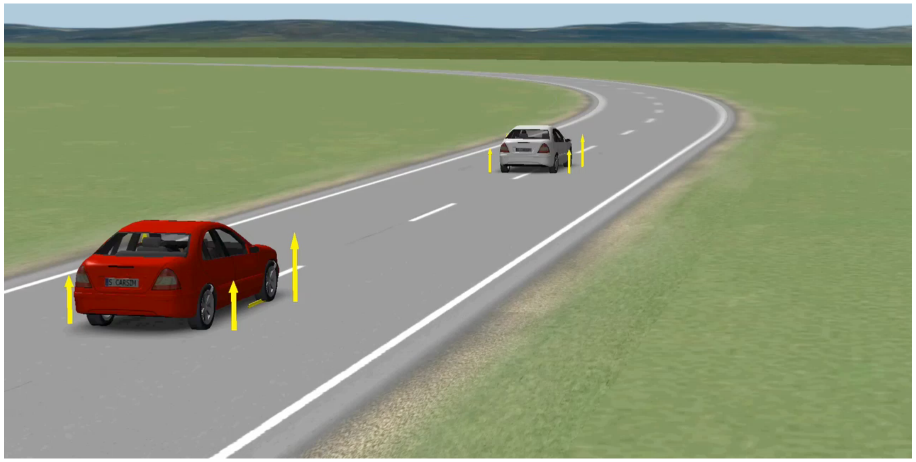
Safety → Dependability → Trust

Big Picture: Automotive

CPS

- Automotive: driver convenience and safety

Understanding how to formally realize guarantees on automotive systems can lead to dependability and trust in smart cities



Safety → Dependability → Trust

Industrial Partners

Ford

TOYOTA

Beginning discussions with Eaton Corp.

Input from Ford and Toyota

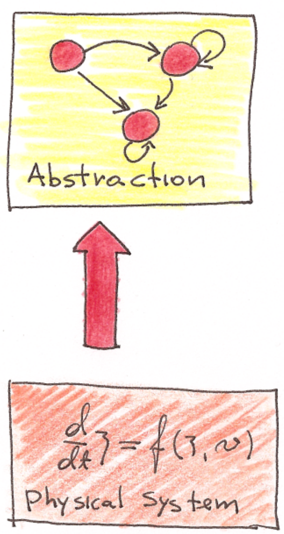
Suggested automotive problems

- Adaptive Cruise Control (ACC)
- Lane Keeping
- Obstacle avoidance
- Composition

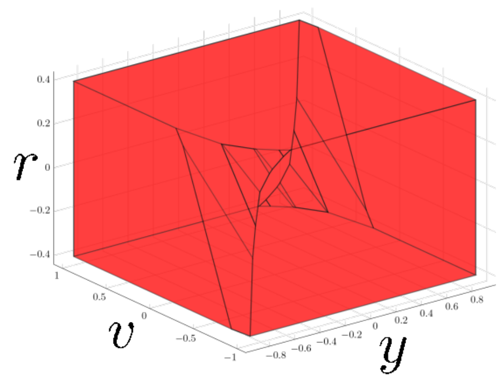
Approaches we are following

- PESSOA ←Abstraction via spatial and temporal discretization
- PCIS ← Linear models and controlled-invariant polyhedra
- Barrier Functions ← Adding formal safety guarantees to classical control

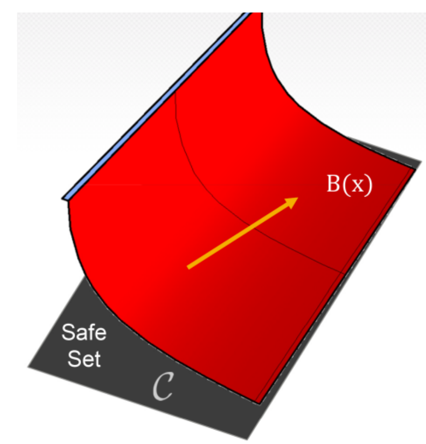
PESSOA



PCIS



Barrier Function



Features One May Care About

	PCIS	Pessoa	Barrier fun.
Complex specifications	TBD	Yes	TBD
Turn-key automation	For LTI	Almost	TBD
Approximation bounds	For LTI	For δ-ISS	Maybe
Parameter tuning	Yes	Some	Yes
Nonlinear	Not now	Yes	Yes
High-dimensional	Not now	Not now	Yes
Termination guarantees	Approximate	Yes	N/A

Supervisor of legacy software	**Yes**	**Yes**	**Yes**

Advances in Control Barrier Functions

Aaron Ames, Xiangru Xu
Jessy Grizzle, Paulo Tabuada

Motivation: Performance & Safety

Goal:

Unify **control objectives** with **safety specifications** in a formal and provably correct manner

Main Idea:

Define **control barrier functions** that allow for the unification in an optimization-based framework

Control Barrier Functions: Last Year

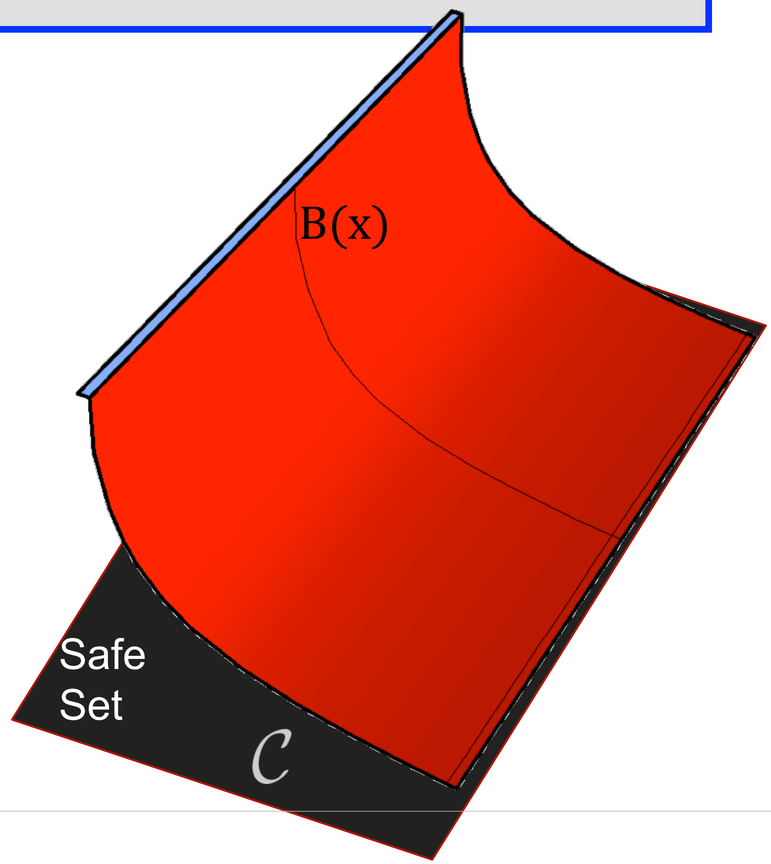
Control Barrier Functions: provably ensure satisfaction of safety specifications

- Define the safe set, $\mathcal{C}$
- Consider a **barrier** function:

$$\inf_{x \in \mathrm{Int}(\mathcal{C})} B(x) \geq 0, \qquad \lim_{x \to \partial \mathcal{C}} B(x) = \infty.$$

- Ensure invariance of the safe set through the requirement:

$$\inf_{u \in \mathcal{U}} \dot{B}(x,u) \leq \frac{\gamma}{B(x)}$$



Control Barrier Functions: Last Year

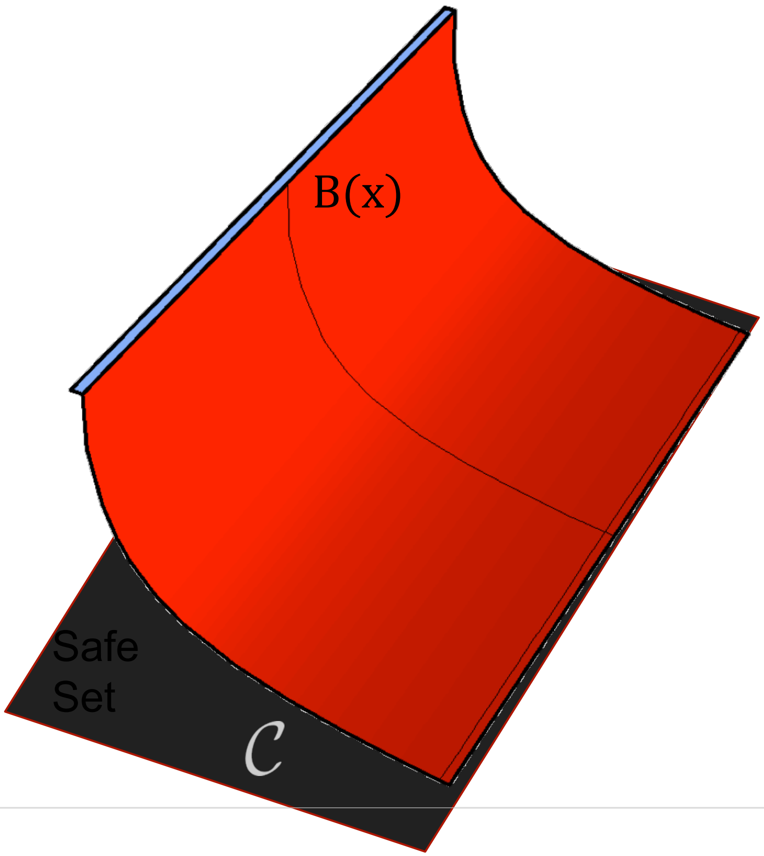
Reciprocal Barrier and Control Barrier Function

$$\inf_{x \in \mathrm{Int}(\mathcal{C})} B(x) \geq 0, \qquad \lim_{x \to \partial \mathcal{C}} B(x) = \infty.$$

and

$$\inf_{u \in \mathcal{U}} \dot{B}(x,u) \leq \frac{\gamma}{B(x)}$$

then the set $\mathcal{C}$ is forward invariant, i.e., the set is provably safe.



Starting Point for a New Barrier Function

- **Generality:** $$\inf_{u \in U} \dot{B}(x,u) \leq \frac{\gamma}{B(x)} \Rightarrow \mathcal{C} \ \text{ safe}$$

The converse? $$\mathcal{C} \ \text{safe} \ \Rightarrow \inf_{u \in U} \dot{B}(x,u) \leq \frac{\gamma}{B(x)} \ ?$$

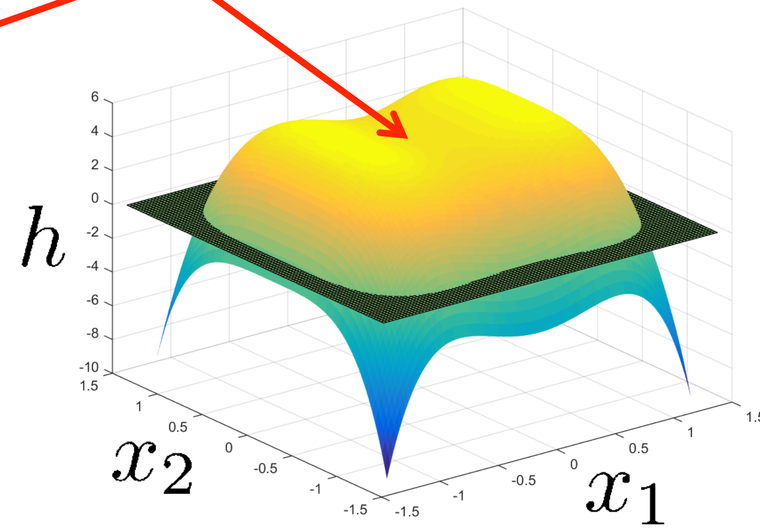
- **Why important?** Less restrictive safety condition implies more freedom for control performance.

- **Robustness:** Model uncertainty [rogue traffic] may force the system out of the safe set. What happens?

Zeroing Barriers

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

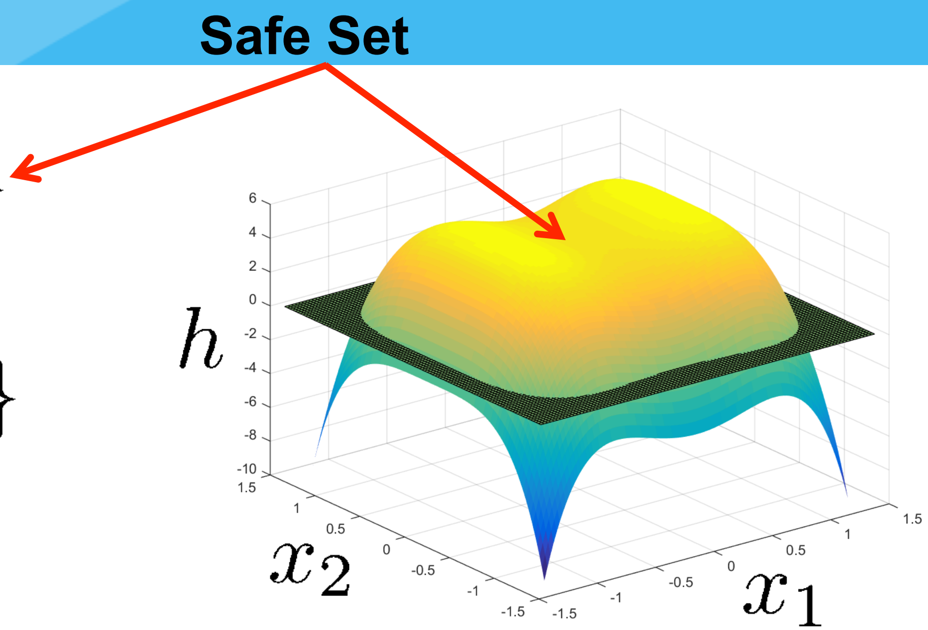
Safe Set



Zeroing Barriers

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

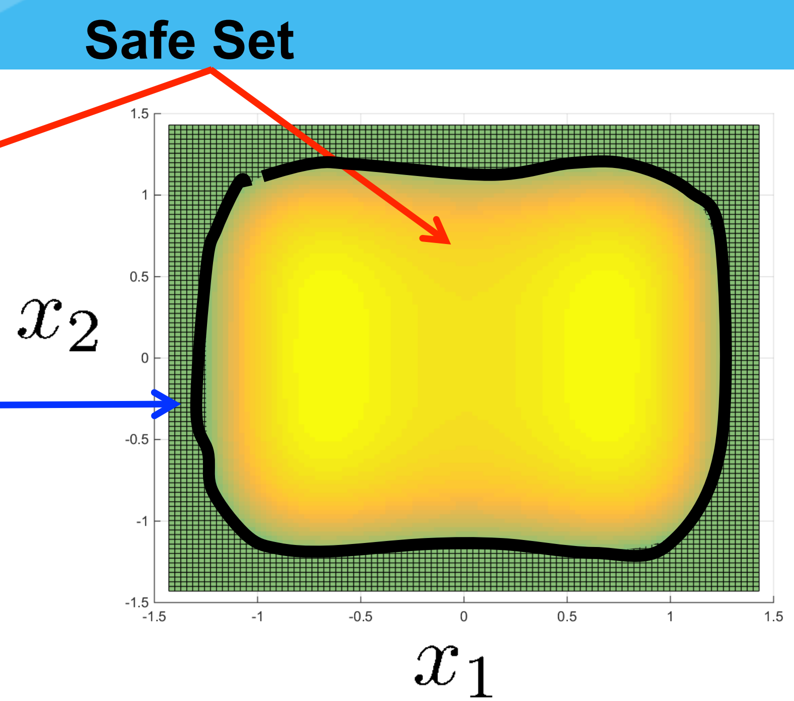
$$\partial\mathcal{C} = \{x \in \mathbb{R}^n : h(x) = 0\}$$



Zeroing Barriers

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

$$\partial\mathcal{C} = \{x \in \mathbb{R}^n : h(x) = 0\}$$

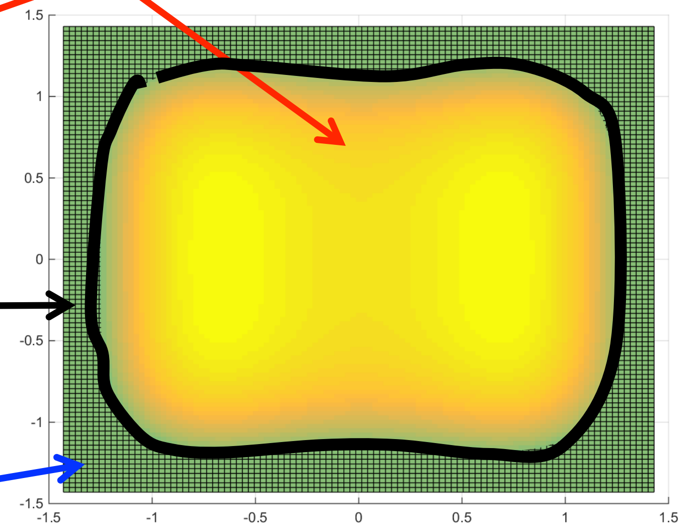


Zeroing Barriers

Safe Set

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

$$\partial\mathcal{C} = \{x \in \mathbb{R}^n : \underline{h(x) = 0}\}$$



x_2

x_1

$$\mathcal{C} \subset \mathcal{D} \subset R^n$$

Def. $h : \mathcal{D} \to \mathbb{R}$ **Zeroing Barrier Function**

$$\dot{h}(x) \geq -\alpha(h(x)) = \begin{cases} > 0 & \text{outside } \mathcal{C} \\ 0 & x \in \partial\mathcal{C} \\ * & x \in \mathrm{Int}(\mathcal{C}) \end{cases}$$

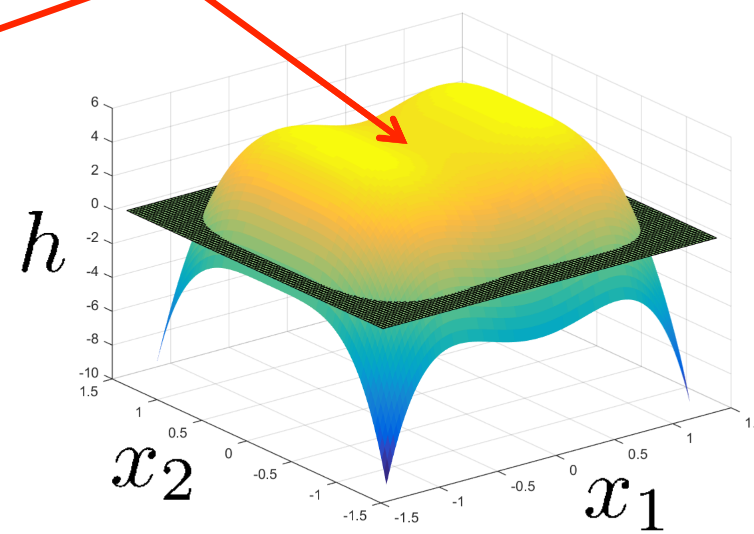
Zeroing Barriers

Safe Set

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

$$\partial\mathcal{C} = \{x \in \mathbb{R}^n : h(x) = 0\}$$

$$\mathcal{C} \subset \mathcal{D} \subset R^n$$



Def. $h : \mathcal{D} \to \mathbb{R}$ **Zeroing Control Barrier Function**

$$\inf_{u \in U} \dot{h}(x,u) \geq -\alpha(h(x)) = \begin{cases} > 0 & \text{outside } \mathcal{C} \\ 0 & x \in \partial\mathcal{C} \\ * & x \in \mathrm{Int}(\mathcal{C}) \end{cases}$$

Zeroing Barriers

Theorem: Selecting control inputs according to

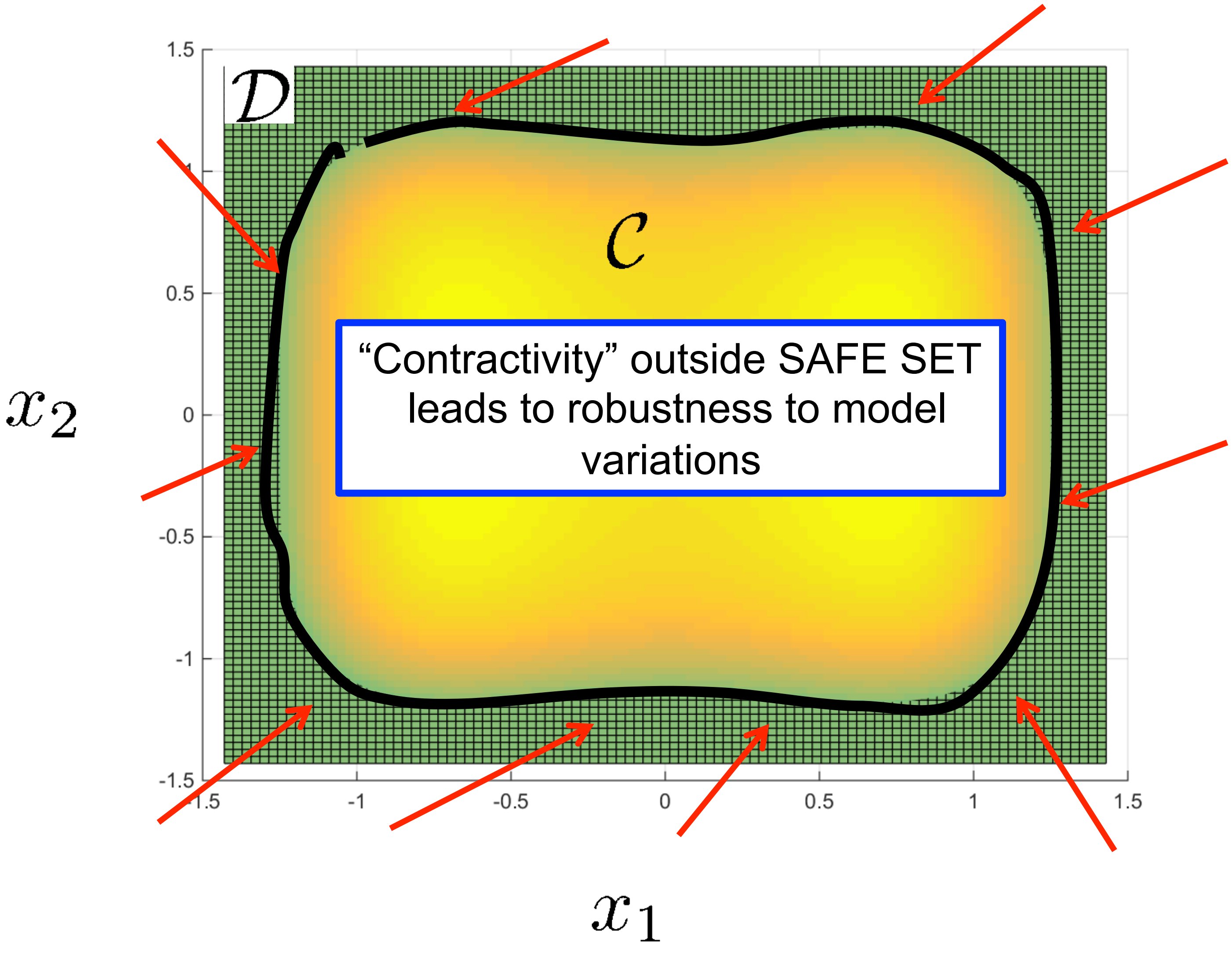
$$\inf_{u \in U} \dot{h}(x,u) \geq -\alpha(h(x))$$

guarantees forward invariance of $\mathcal{C}$ and hence, safety.

Def. $h : \mathcal{D} \to \mathbb{R}$ **Zeroing Control Barrier Function**

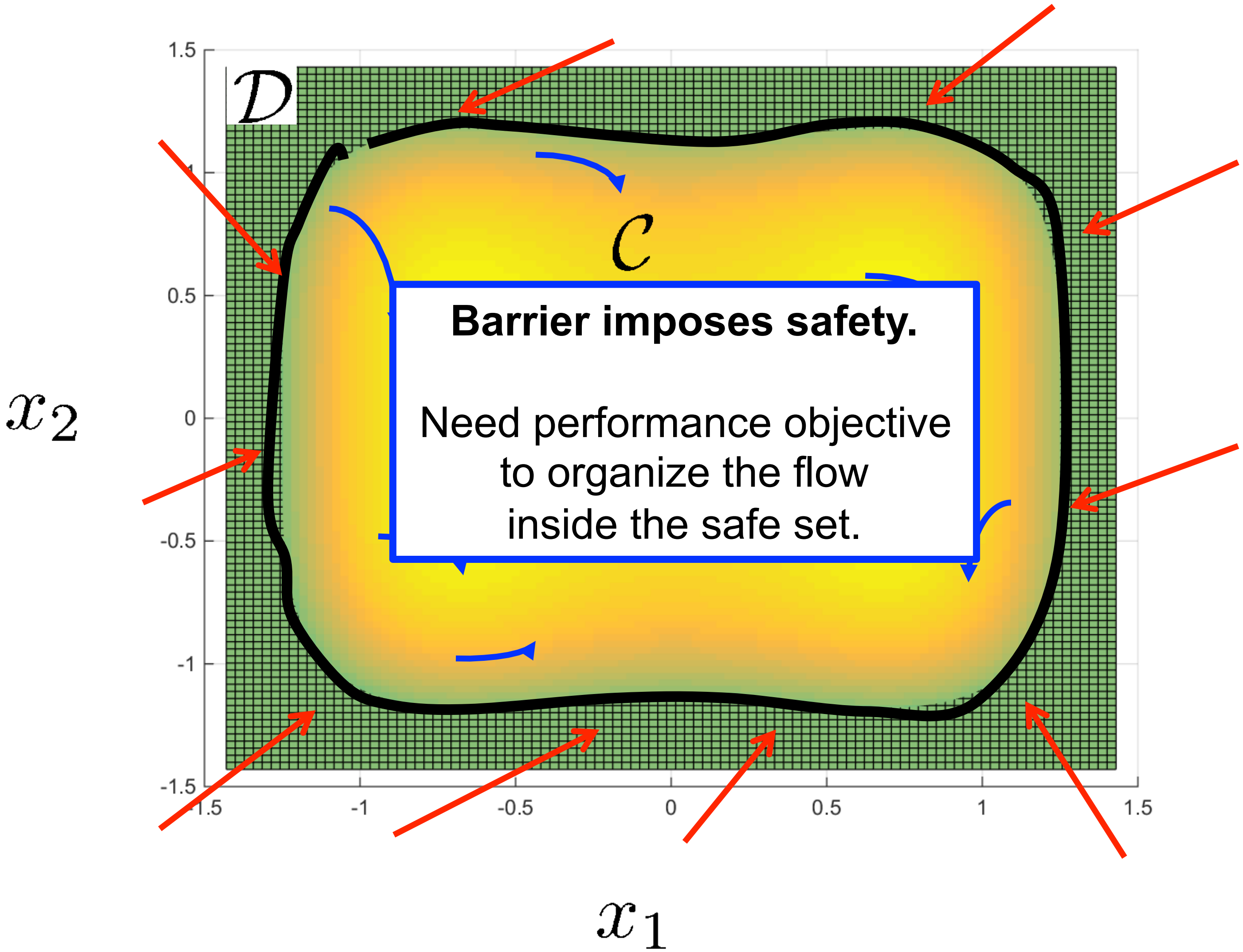
$$\inf_{u \in U} \dot{h}(x,u) \geq -\alpha(h(x)) = \begin{cases} > 0 & \text{outside } \mathcal{C} \\ 0 & x \in \partial \mathcal{C} \\ * & x \in \mathrm{Int}(\mathcal{C}) \end{cases}$$

Zeroing Barriers



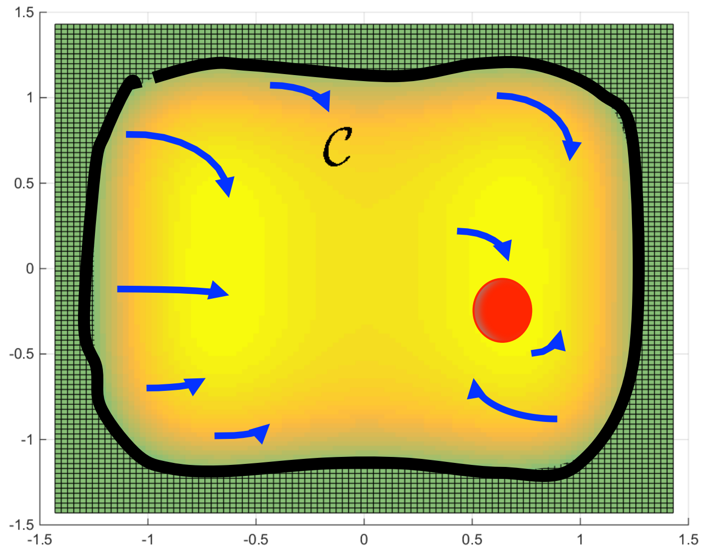
"Contractivity" outside SAFE SET leads to robustness to model variations

Zeroing Barriers

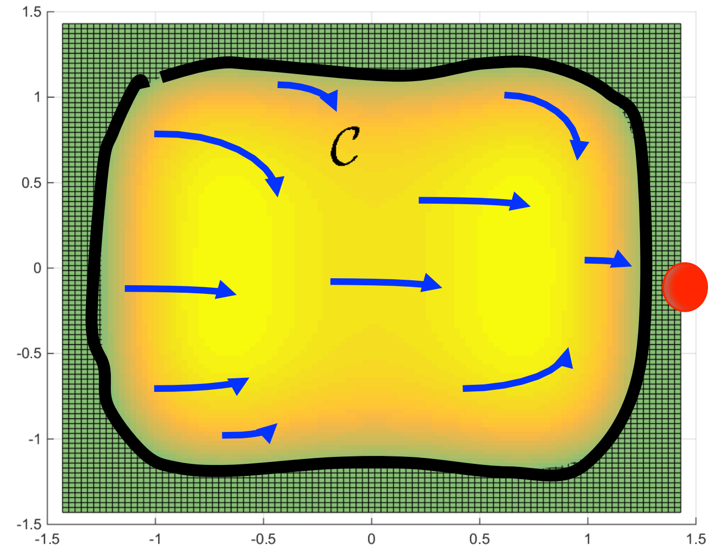


Safety + Performance: 2 Cases

Performance Objective In Safe Set



Performance Objective not in Safe Set



How to combine both cases in a unified framework?

Our answer: Quadratic Program

Multi-Objective QP

Safe Set & Barrier $$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$$

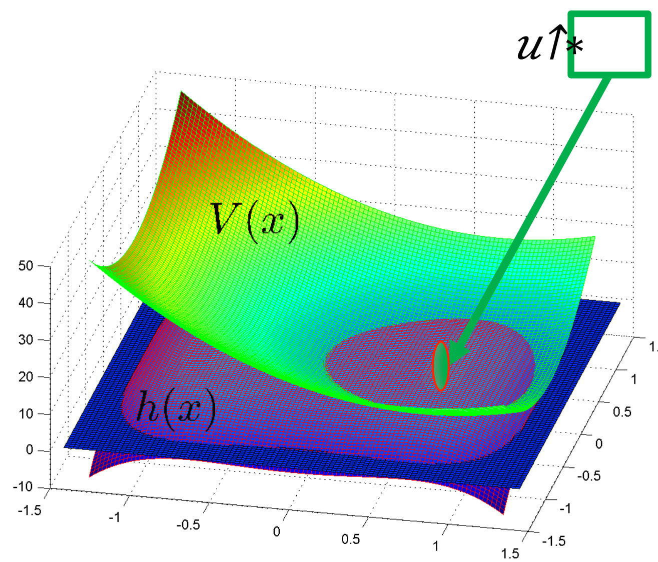
Control System $$\dot{x} = f(x) + g(x)u$$

u*(x) = smallest control input assuring safety

$$\dot{h}(x,u) \geq -\alpha(h(x))$$

…and performance as "close as possible"

$$\dot{V}(x,u) \approx -cV(x)$$

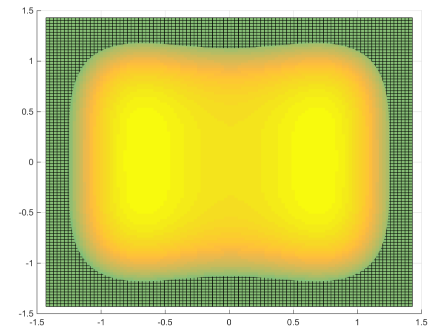


First: QP for Safety Only

CPS

Safe Set & Barrier $\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$

Control System $\dot{x} = f(x) + g(x)u$



Smallest control input assuring safety

$$u^*(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \quad u^\top u$$

$$\text{s.t.} \quad \dot{h}(x,u) \geq -\alpha(h(x))$$

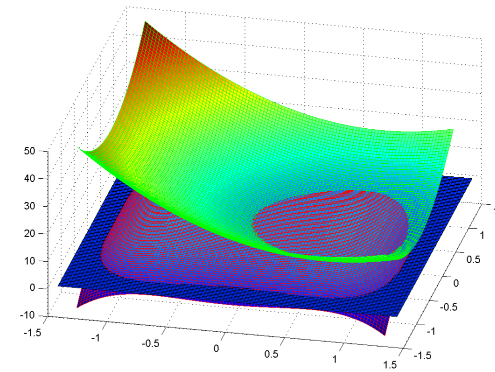
$$\dot{h}(x,u) = L_f h(x) + L_g h(x) u$$

CPS

Now: QP for Safety and Performance

Safe Set & Barrier $\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$

Control System $\dot{x} = f(x) + g(x)u$



Smallest control input assuring safety

$$u^*(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \quad u^\top u$$

$$\text{s.t.} \quad L_f h(x) + L_g h(x) u \geq -\alpha(h(x))$$

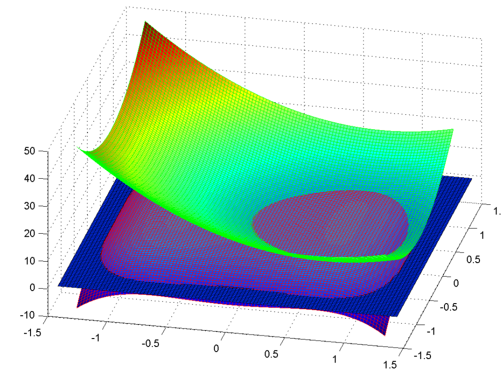
…AND performance as "close as possible"

$$\boxed{\dot{V}(x,u) \approx -cV(x)}$$

Multi-Objective QP

Safe Set & Barrier $\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$

Control System $\dot{x} = f(x) + g(x)u$



Smallest control input assuring safety

+ performance

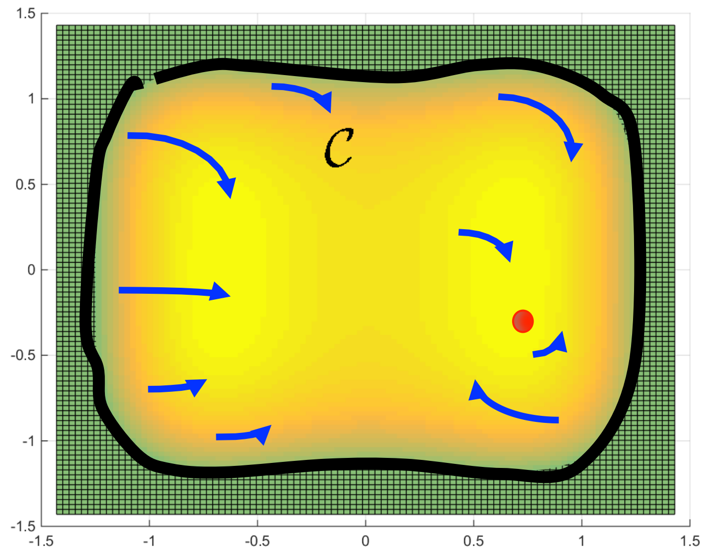
$$u^*(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \quad u^\top u + 10^2 \delta^2$$

$$\text{s.t.} \quad L_f h(x) + L_g h(x) u \geq -\alpha(h(x))$$

$$L_f V(x) + L_g V(x) u \leq -cV(x) + \delta$$

Multi-Objective QP

CPS



Feasible w/o relaxation

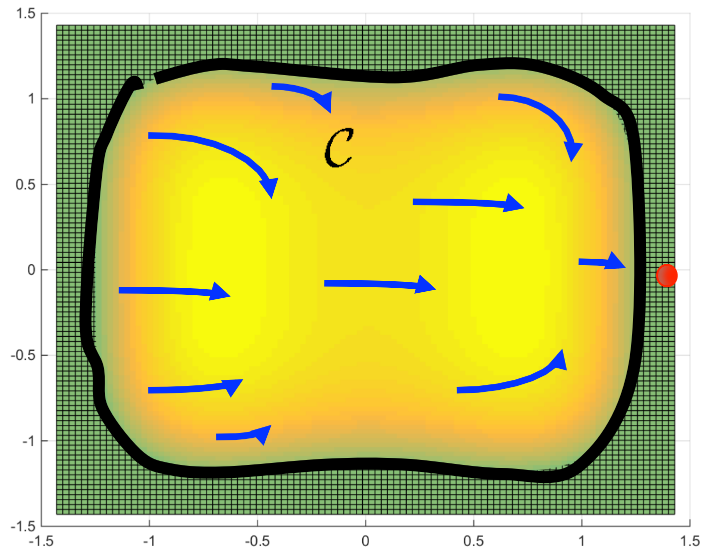
$$u^*(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \quad u^\top u + 10^2 \delta^2$$

$$\text{s.t.} \quad L_f h(x) + L_g h(x) u \geq -\alpha(h(x))$$

$$L_f V(x) + L_g V(x) u \leq -cV(x) + \delta$$

called relaxation parameter

Multi-Objective QP



Infeasible w/o relaxation

$$u^*(x) = \underset{u \in \mathbb{R}^m}{\text{argmin}} \quad u^\top u + 10^2 \delta^2$$

$$\text{s.t.} \qquad L_f h(x) + L_g h(x) u \geq -\alpha(h(x))$$

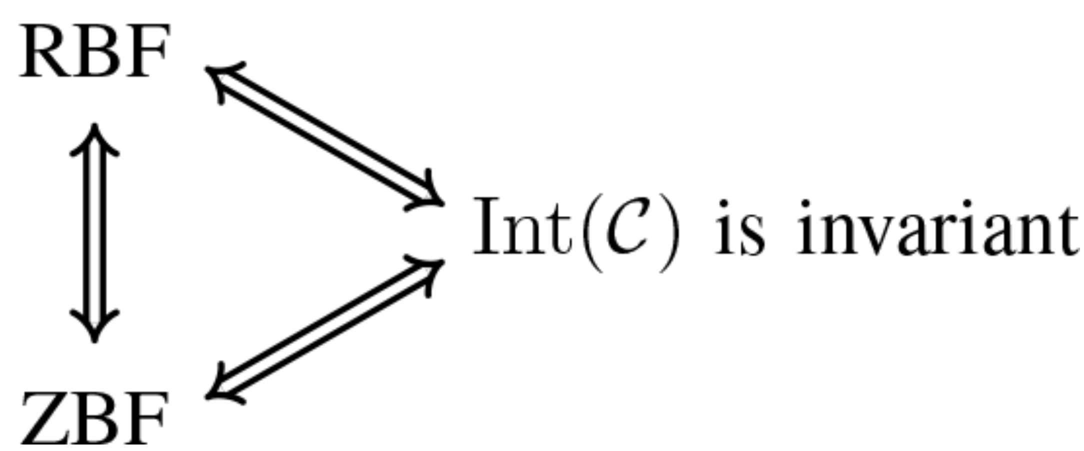
$$L_f V(x) + L_g V(x) u \leq -cV(x) + \delta$$

called relaxation parameter

Characterization

- When QPs produce Lipschitz controllers
- Robustness to disturbances
- Relationships

Theorem 2:
(Assume $\mathcal{C}$ is compact and contractive)

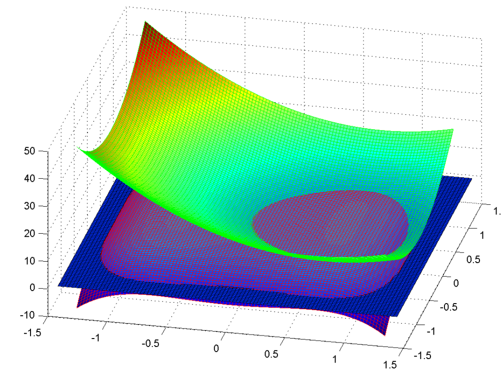


CPS

Lipschitz Continuity of QPs

Safe Set & Barrier $\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}$

Control System $\dot{x} = f(x) + g(x)u$



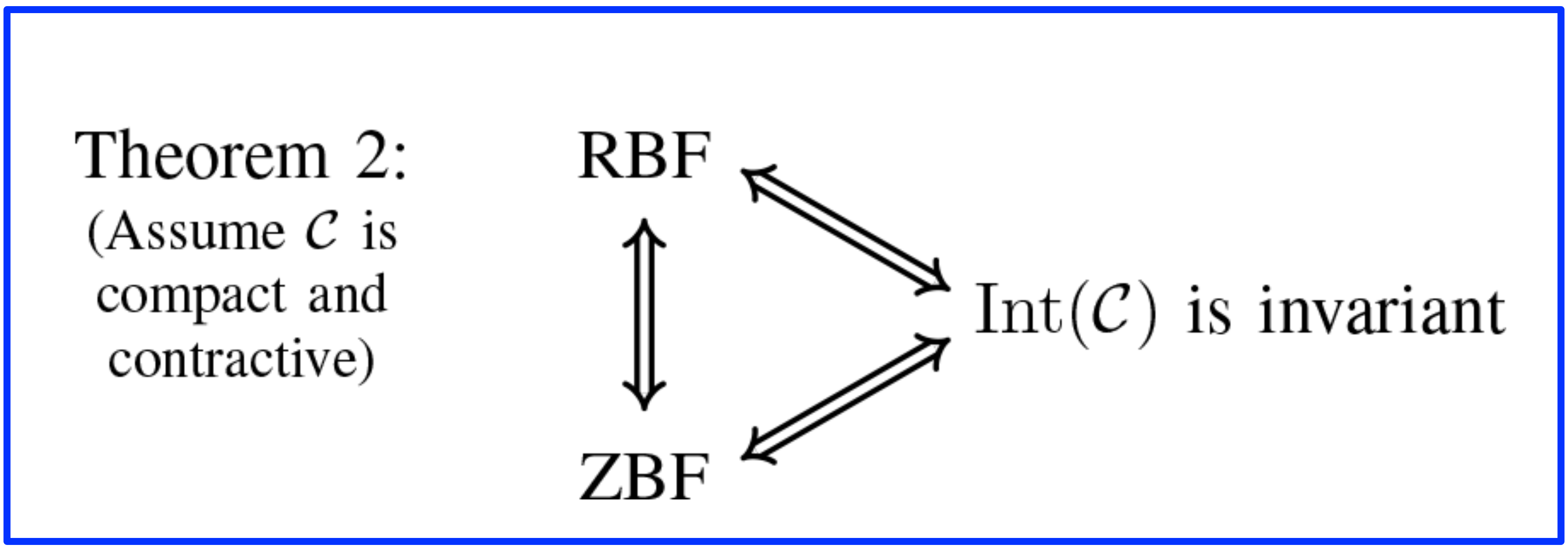
- Theorem: QPs produce Lipschitz continuous controls when

$$L_g h(x) = \frac{\partial h(x)}{\partial x} g(x) \neq 0, \quad x \in \mathcal{C}$$

$$\begin{aligned}
\mathbf{u}^*(x) = \quad & \underset{\mathbf{u}=(u,\delta)\in\mathbb{R}^m\times\mathbb{R}}{\operatorname{argmin}} \quad \frac{1}{2}u^\top u + 10^2\delta^2 \\
\text{s.t.} \quad & L_fV(x) + L_gV(x)u + c_3V(x) - \delta \leq 0, \\
& L_fh(x) + L_gh(x)u + \alpha(h(x)) \geq 0,
\end{aligned}$$

Relations

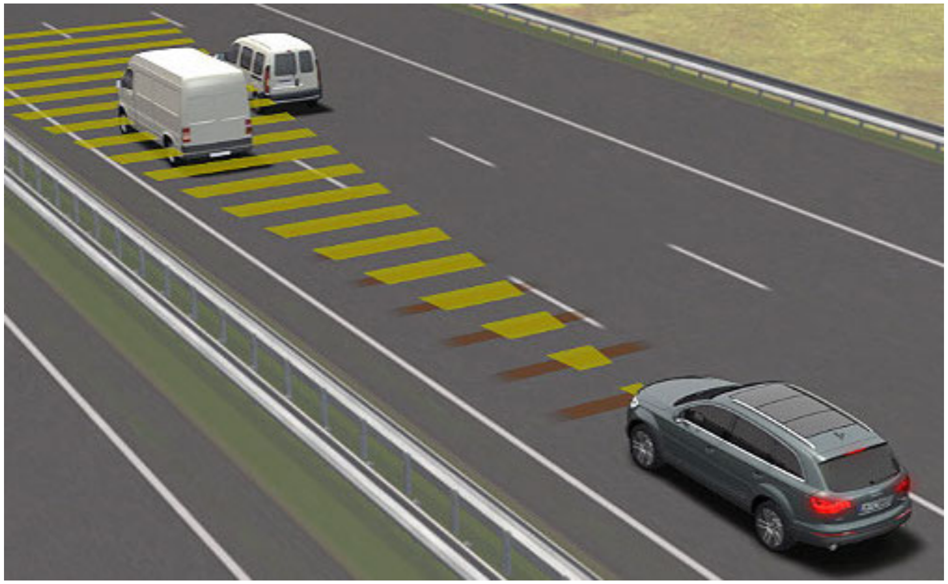
- **Relationship:** Under certain conditions, controlled invariance, RBF and ZBF are equivalent



Applications

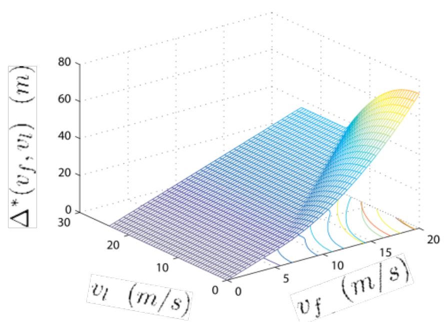
- ACC
- Lane Keeping
- *Working on* composition: LK + ACC
- Others are already using our work

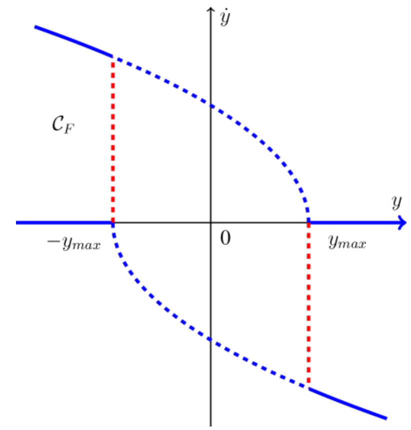
Applications



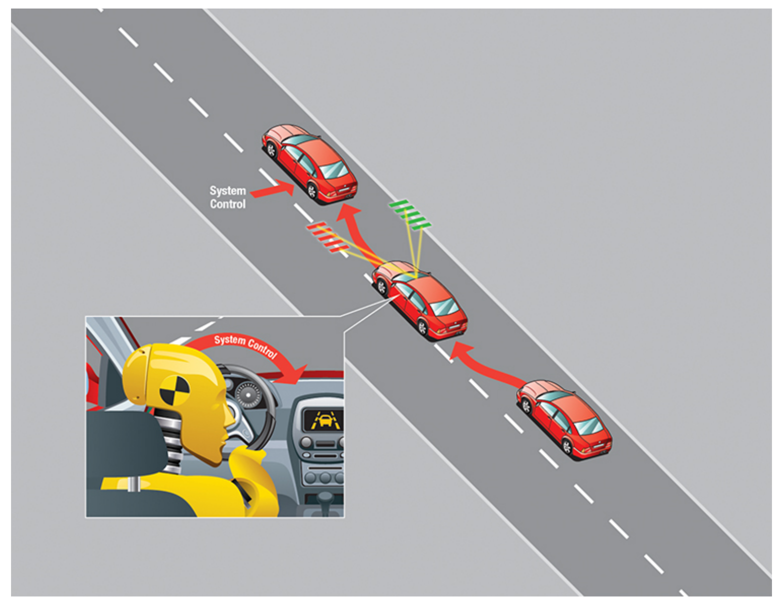
From http://www.proctorcars.com/how-does-adaptive-cruise-control-work/

Adaptive Cruise Control



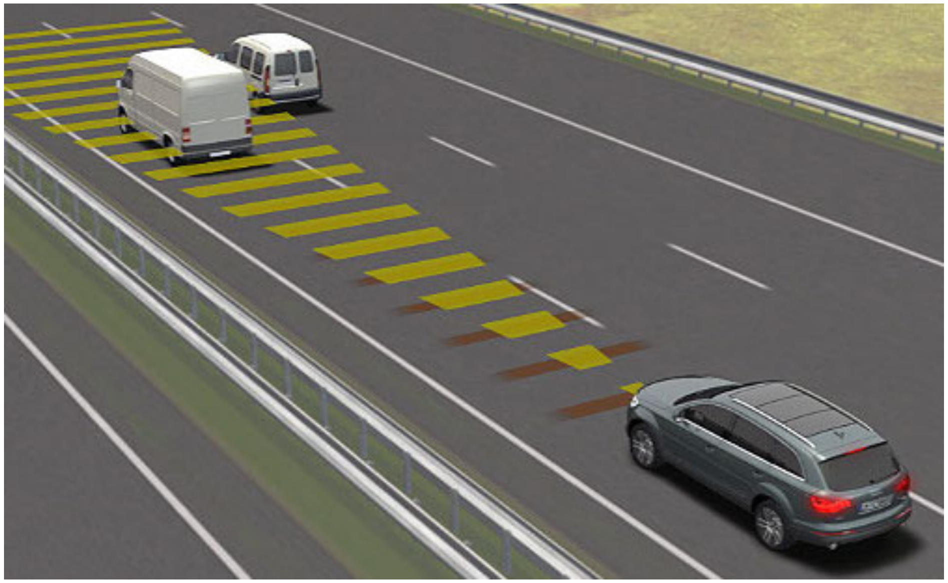


Lane Keeping



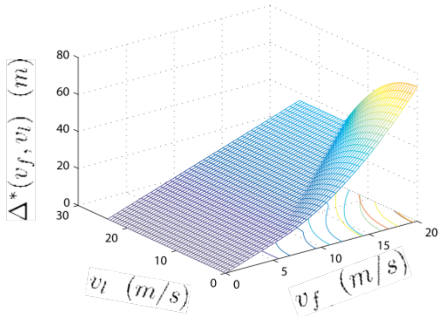
CPS

Applications



From http://www.proctorcars.com/how-does-adaptive-cruise-control-work/

Adaptive Cruise Control



Robustness to Road Grade Uncertainty

Current Challenge Composition

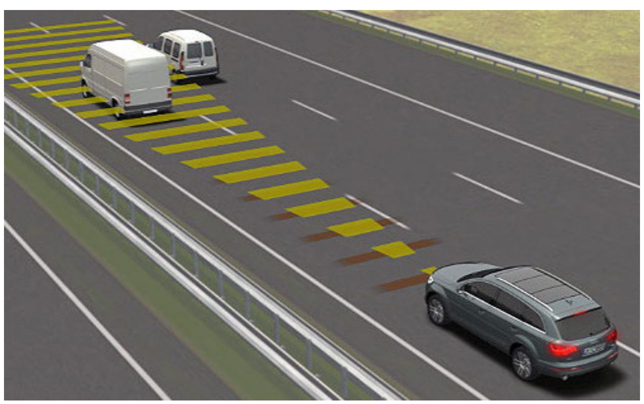
$$\Box S_U \wedge \Box \left(\bigwedge_{i=1}^{2} (\Box(M_i \implies \Diamond\Box T_i)) \right) \bigwedge ?$$

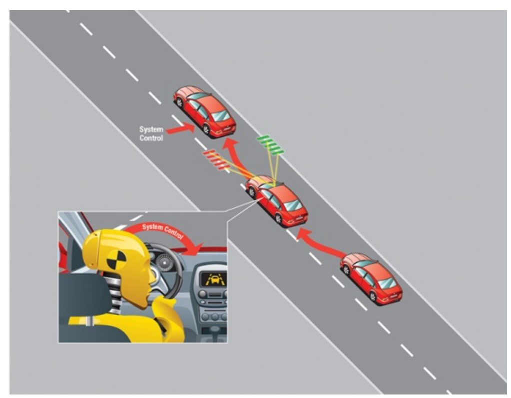
$$\Box(y \in [-0.9, 0.9] \wedge \ddot{y} \in [-0.3g, 0.3g])$$

Current Challenge Composition

$$\frac{d}{dt}\begin{bmatrix} y \\ \nu \\ \psi - \psi_d \\ r \end{bmatrix} = \begin{bmatrix} 0 & 1 & v_f & 0 \\ 0 & -\frac{C_{\alpha f}+C_{\alpha r}}{m\, v_f} & 0 & \frac{bC_{\alpha r}-aC_{\alpha f}}{m\, v_f} - v_f \\ 0 & 0 & 0 & 1 \\ 0 & \frac{bC_{\alpha r}-aC_{\alpha f}}{I_z\, v_f} & 0 & -\frac{a^2C_{\alpha f}+b^2C_{\alpha r}}{I_z\, v_f} \end{bmatrix} \begin{bmatrix} y \\ \nu \\ \psi - \psi_d \\ r \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{C_{\alpha f}}{m} \\ 0 \\ a\frac{C_{\alpha f}}{I_z} \end{bmatrix} \delta_f + \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} r_d$$

$$\frac{d}{dt}\begin{bmatrix} v_f \\ v_l \\ D \end{bmatrix} = \begin{bmatrix} -F_r/m + u \\ a_L \\ v_l - v_f \end{bmatrix}$$

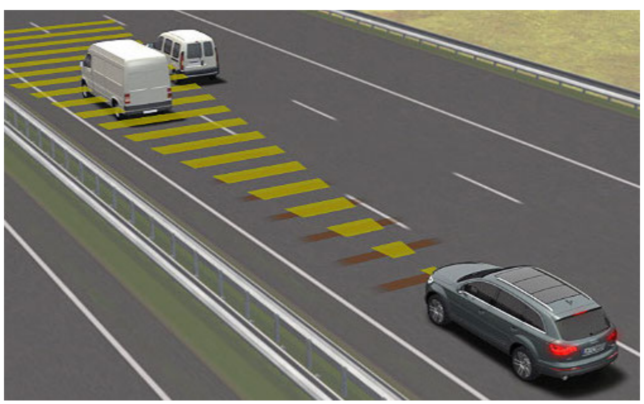


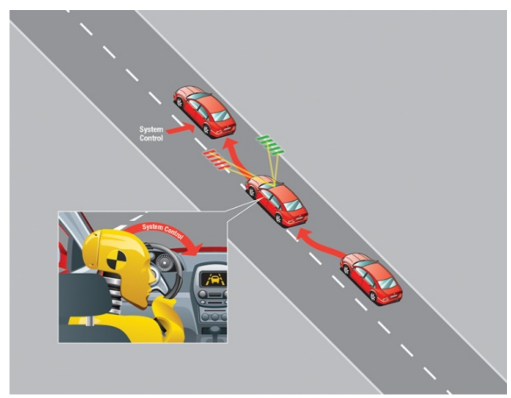


Current Challenge Composition

$$\frac{d}{dt}\begin{bmatrix} y \\ \nu \\ \psi - \psi_d \\ r \end{bmatrix} = \begin{bmatrix} 0 & 1 & v_f & 0 \\ 0 & -\frac{C_{\alpha f}+C_{\alpha r}}{m\ v_f} & 0 & \frac{bC_{\alpha r}-aC_{\alpha f}}{m\ v_f} - v_f \\ 0 & 0 & 0 & 1 \\ 0 & \frac{bC_{\alpha r}-aC_{\alpha f}}{I_z\ v_f} & 0 & -\frac{a^2C_{\alpha f}+b^2C_{\alpha r}}{I_z\ v_f} \end{bmatrix}\begin{bmatrix} y \\ \nu \\ \psi - \psi_d \\ r \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{C_{\alpha f}}{m} \\ 0 \\ a\frac{C_{\alpha f}}{I_z} \end{bmatrix}\delta_f + \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} r_d$$

$$\frac{d}{dt}\begin{bmatrix} v_f \\ v_l \\ D \end{bmatrix} = \begin{bmatrix} -F_r/m + u/m - \nu r \\ a_L \\ v_l - v_f \end{bmatrix}$$

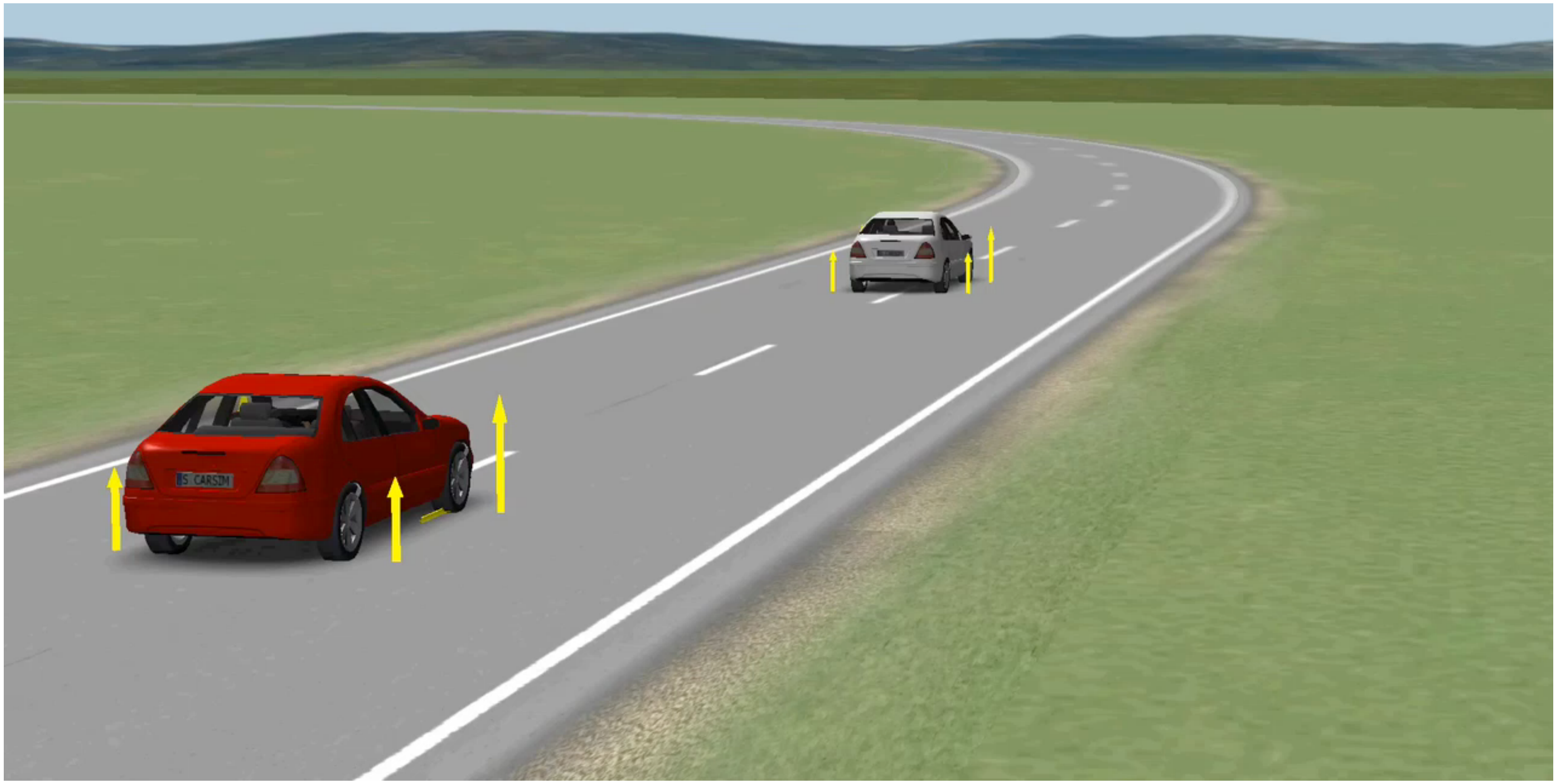




CarSim—16 DOF Model

CPS

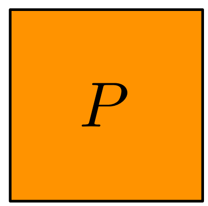
Have a start on it



Composition

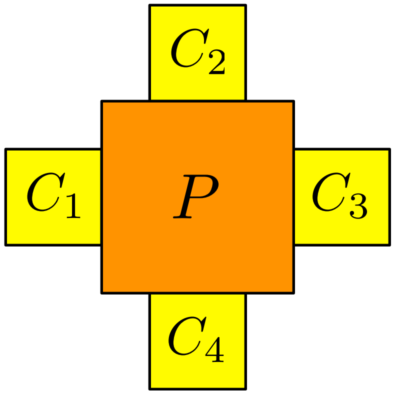
Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:



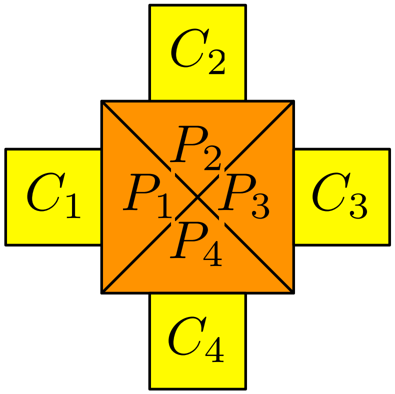
Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:



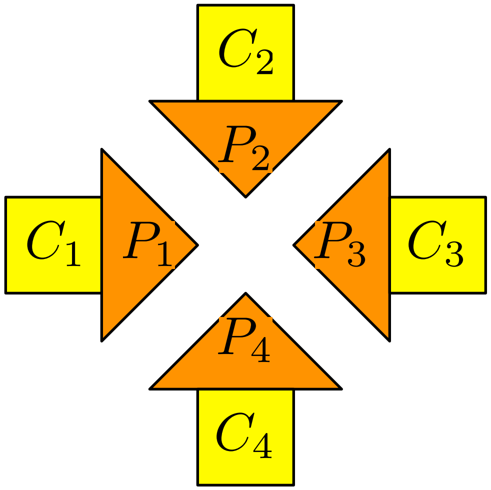
Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:



Composing, decomposing, recomposing, …

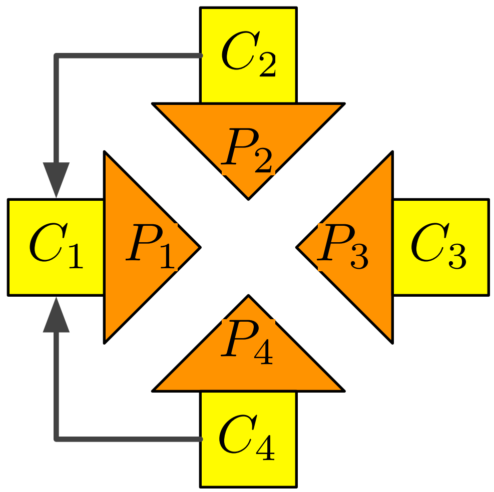
Three approaches to the compositional synthesis problem:



Composing, decomposing, recomposing, …

CPS

Three approaches to the compositional synthesis problem:

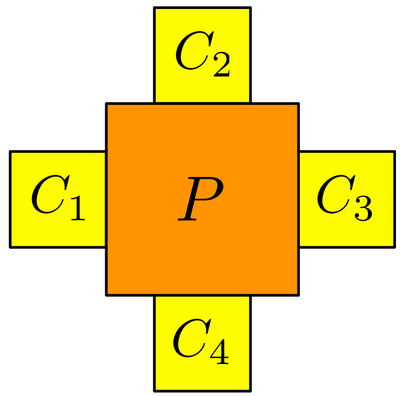


	[DT15]		
View	Internal		
Models	Discrete		
Key ingredient	Ranking functions		

[DT15] On Compositional Symbolic Controller Synthesis Inspired by Small-Gain Theorems. E. Dallal and P. Tabuada. To appear in CDC15, 2015.

Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:



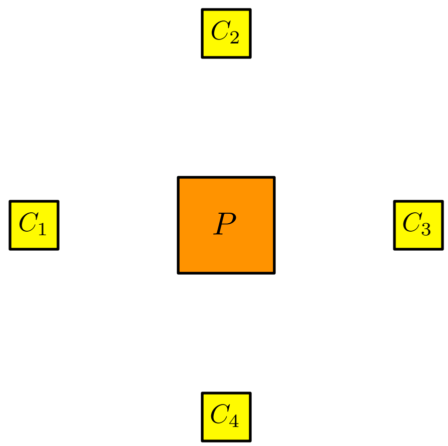
	[DT15]	[XOG15]	
View	Internal	Input-output	
Models	Discrete	Discrete/continuous	
Key ingredient	Ranking functions	Passivity indices	

[XOG15] Passivity Degradation in Discrete Control Implementations: An Approximate Bisimulation Approach, X. Xu, N. Ozay, V. Gupta, To appear in CDC15, 2015

CPS

Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:



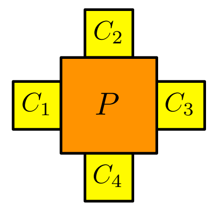
	[DT15]	[XOG15]	
View	Internal	Input-output	
Models	Discrete	Discrete/continuous	
Key ingredient	Ranking functions	Passivity indices	

[XOG15] Passivity Degradation in Discrete Control Implementations: An Approximate Bisimulation Approach. X. Xu, N. Ozay, V. Gupta. To appear in CDC15, 2015

Composing, decomposing, recomposing, …

CPS

Three approaches to the compositional synthesis problem:



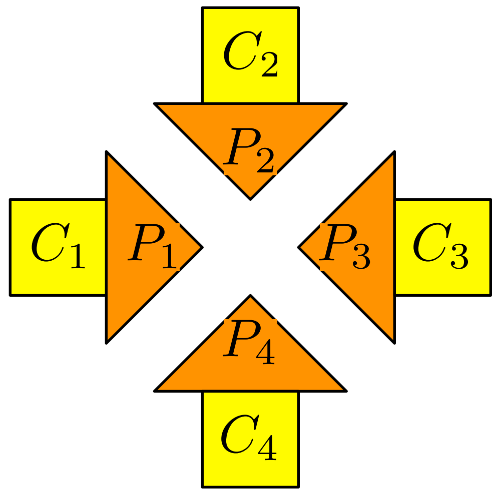
	[DT15]	[XOG15]	
View	Internal	Input-output	
Models	Discrete	Discrete/continuous	
Key ingredient	Ranking functions	Passivity indices	

[XOG15] Passivity Degradation in Discrete Control Implementations: An Approximate Bisimulation Approach. X. Xu, N. Ozay, V. Gupta. To appear in CDC15, 2015

CPS

Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:

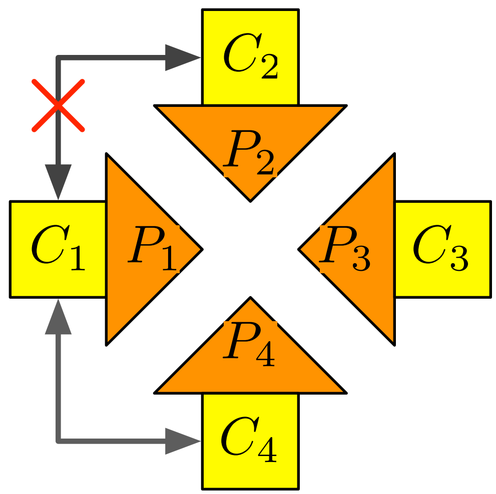


	[DT15]	[XO15]	[NO15]
View	Internal	Input-output	Internal
Models	Discrete	Discrete/continuous	Continuous
Key ingredient	Ranking functions	Passivity indices	Robust invariance

[NO15] Synthesis of separable controlled invariant sets for modular local control design. P. Nilsson and N. Ozay. Submitted to ACC15, 2015

Composing, decomposing, recomposing, …

Three approaches to the compositional synthesis problem:



	[DT15]	[XO15]	[NO15]
View	Internal	Input-output	Internal
Models	Discrete	Discrete/continuous	Continuous
Key ingredient	Ranking functions	Passivity indices	Robust invariance

[NO15] Synthesis of separable controlled invariant sets for modular local control design. P. Nilsson and N. Ozay. Submitted to ACC15, 2015

CPS

Formal Controller Synthesis for Bipedal Robotic Walking

MICHIGAN

UCLA

GT

Motivation

Formal Methods in Robotics

Necessary to create and certify the next generation of robotic walking behaviors:

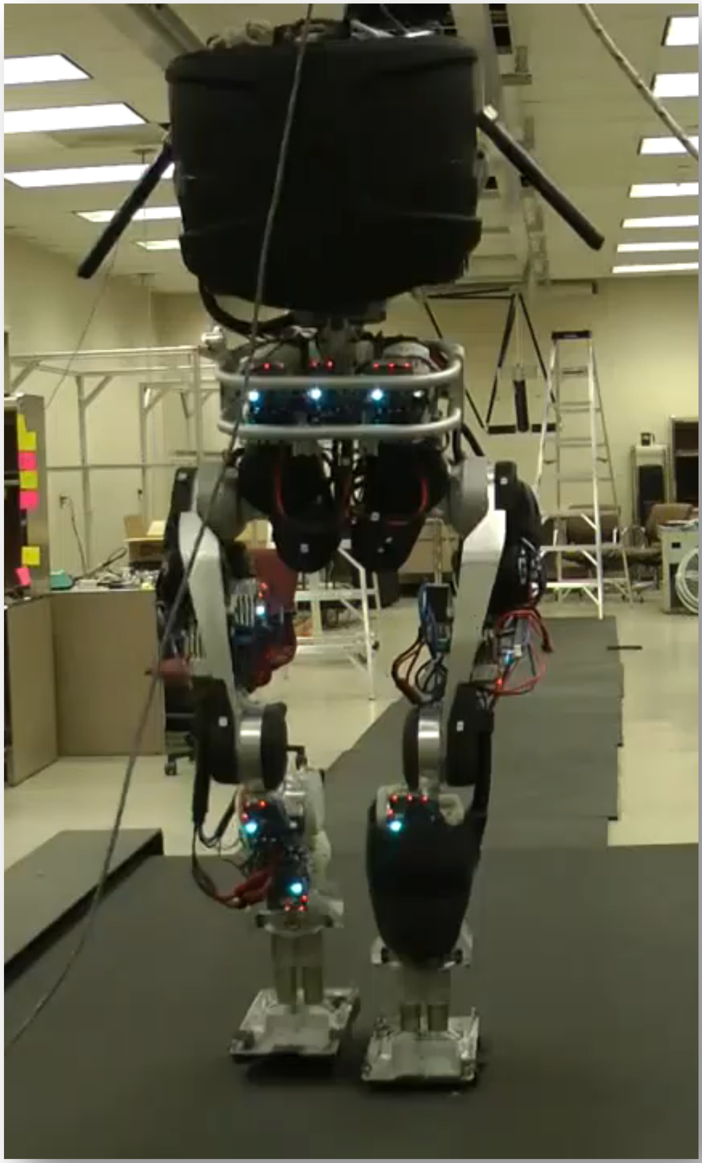
Correct by construction control…
if you design it, it will work!

Challenges:

- *High dimensional:* over 50 dimensions
- *Highly dynamic:* traditional notions of stability are not sufficient
- *Hybrid:* Dynamics involve both discrete and continuous behavior

Approach:

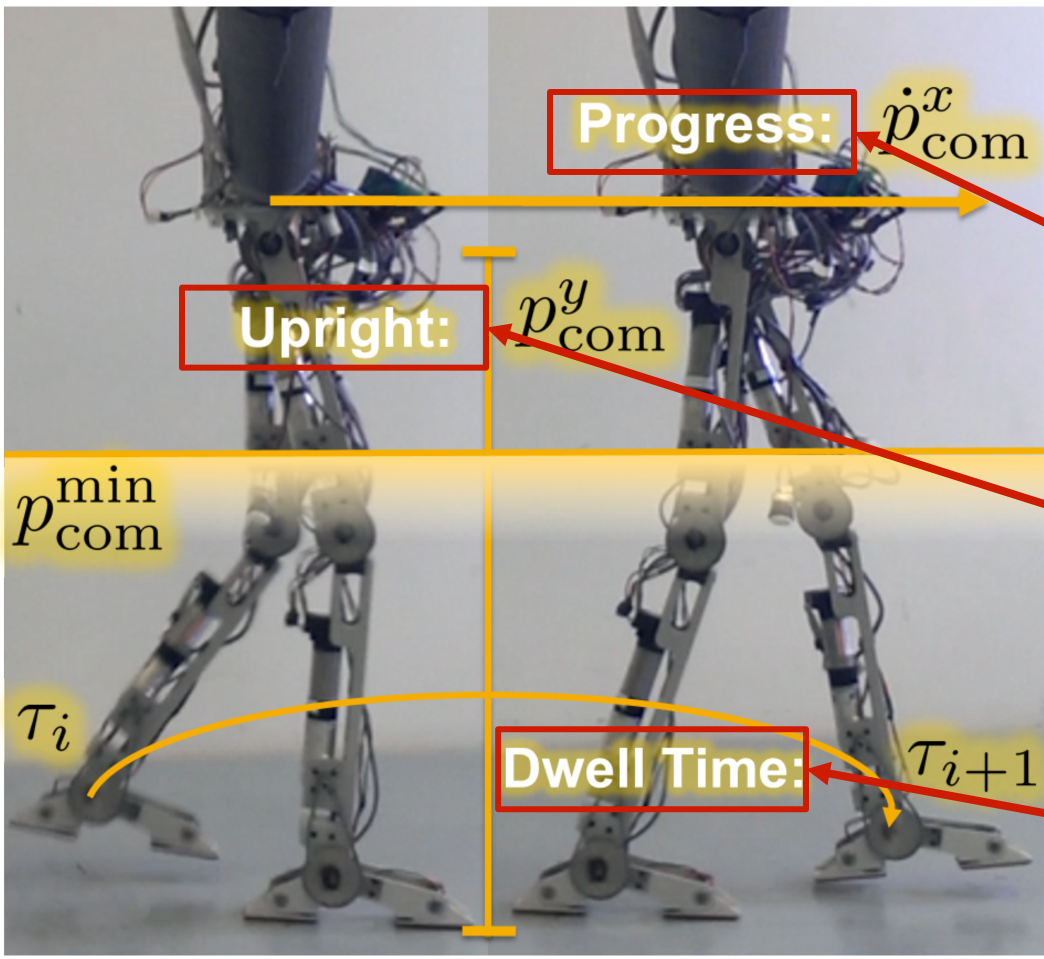
Unify formal methods and feedback control to overcome curse of dimensionality



What is Walking?

CPS

Synthesis Objective: $\Box(P_1 \cap P_2 \cap P_3)$, *i.e., render a subset* $P \subseteq P_1 \cap P_2 \cap P_3$ *invariant.*



- ☑ Forward progression of the center of mass
- ☑ Center of mass stays upright
- ☑ Each step takes nonzero time to complete

Specifications

CPS

Synthesis Objective: $\square(P_1 \cap P_2 \cap P_3)$, *i.e., render a subset* $P \subseteq P_1 \cap P_2 \cap P_3$ *invariant.*

Maximum torque is not exceeded

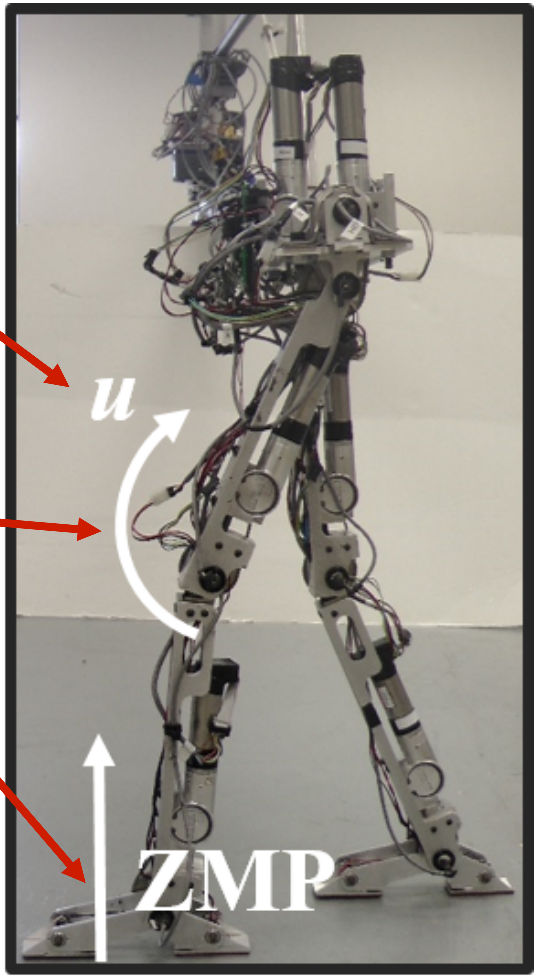
$$P_1 = \{z \in \mathcal{D}_{\mathbf{PZ}} : |u(\vartheta_r(z), \dot{\vartheta}_r(z))| < u_{\max}\}$$

Maximum speed is not exceeded

$$P_2 = \{z \in \mathcal{D}_{\mathbf{PZ}} : |\dot{\vartheta}_r(z)| < \dot{\theta}_{\max}\}$$

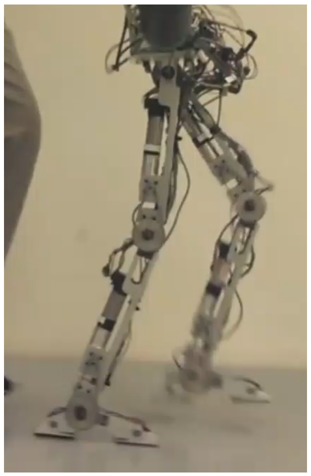
Foot stays flat on the ground (ZMP stays in the foot)

$$P_3 = \{z \in \mathcal{D}_{\mathbf{PZ}} : A_{\mathrm{ZMP}} F_{st}(\vartheta_r(z), \dot{\vartheta}_r(z), u(\vartheta_r(z), \dot{\vartheta}_r(z))) < 0\}$$



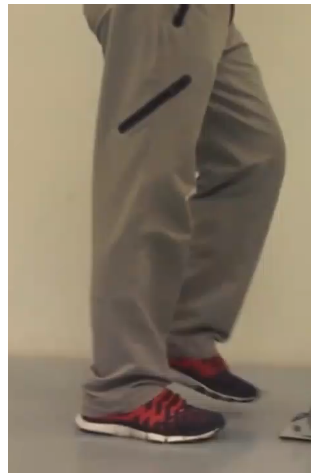
CPS

Controller Synthesis

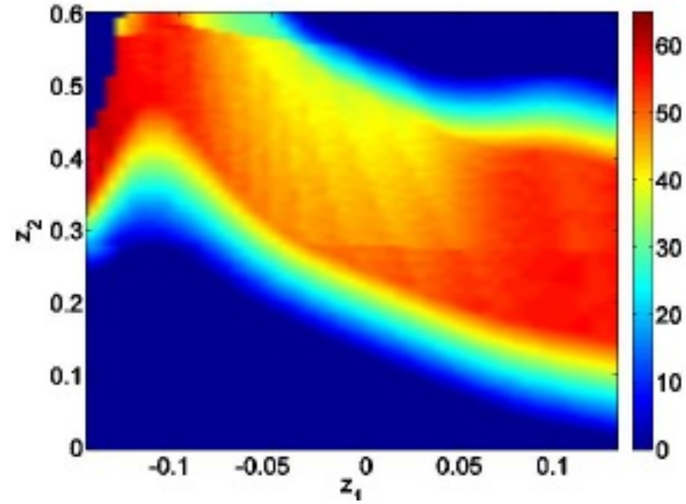


Actual Outputs: y_a

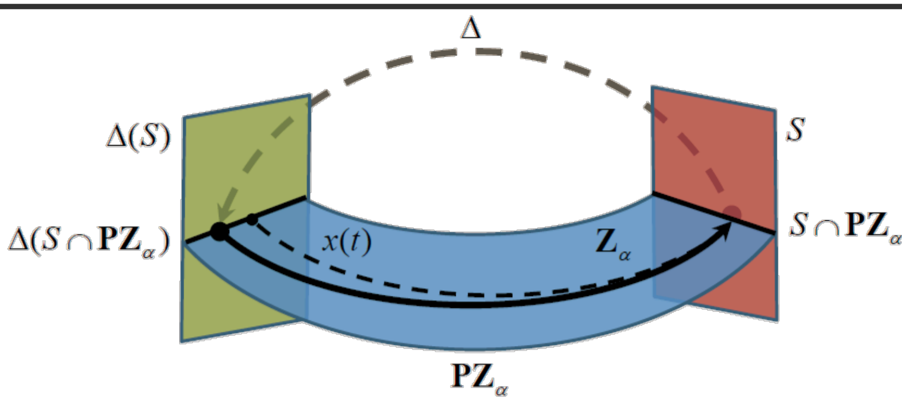
Drive: $y_a \to y_d$



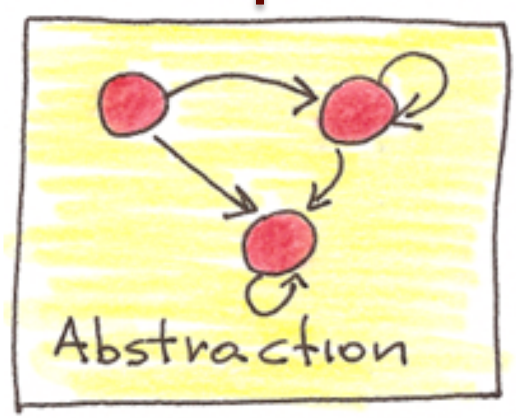
Desired Outputs: y_d



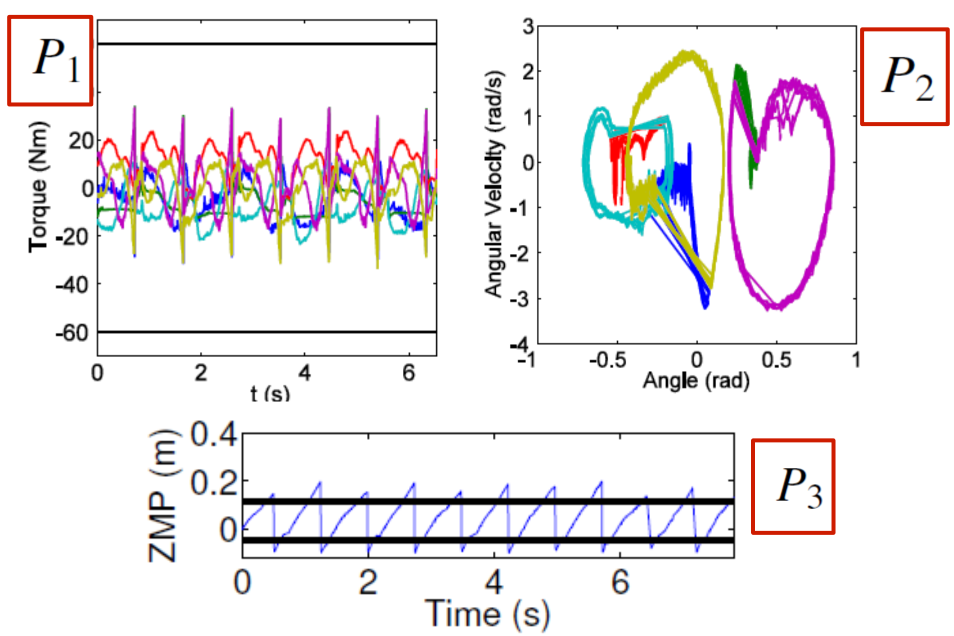
Safe set and number of inputs allowed by the controller in each state.



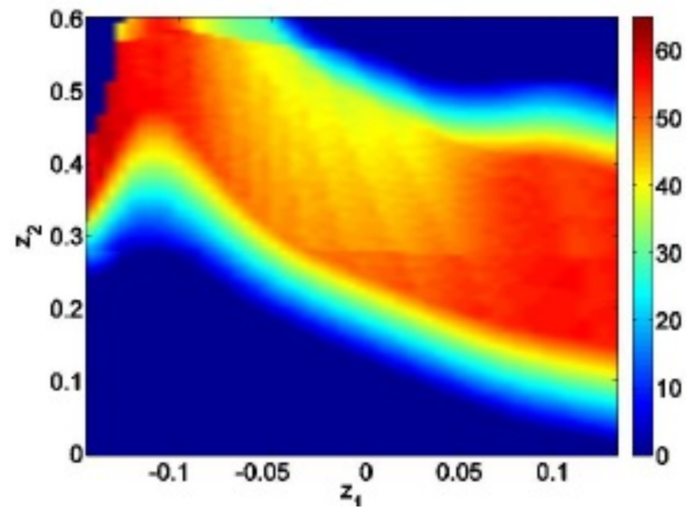
Reduced order representation given by hybrid zero dynamics



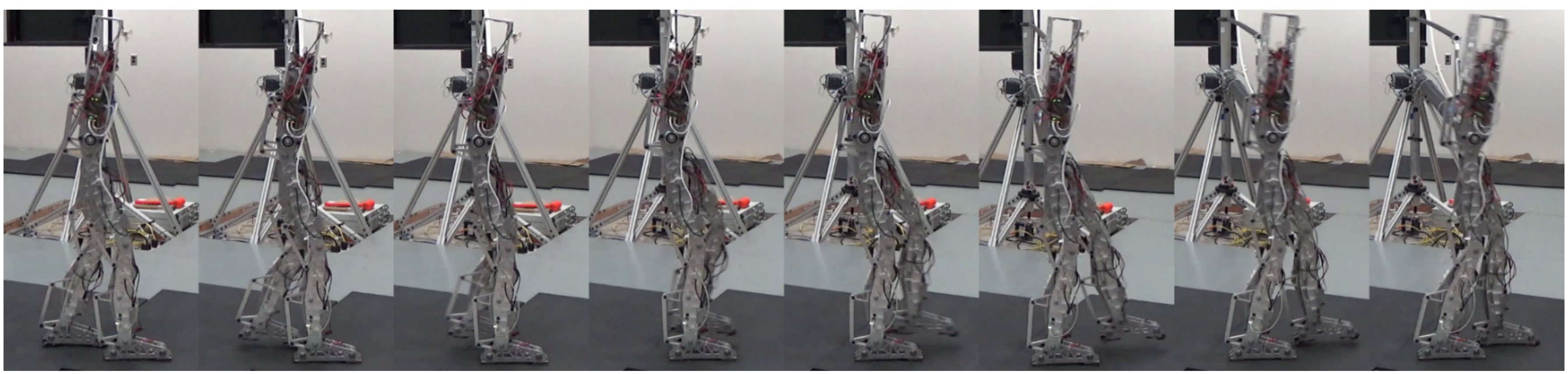
Physical Realization



All specifications are "satisfied": $\square(P_1 \wedge P_2 \wedge P_3)$

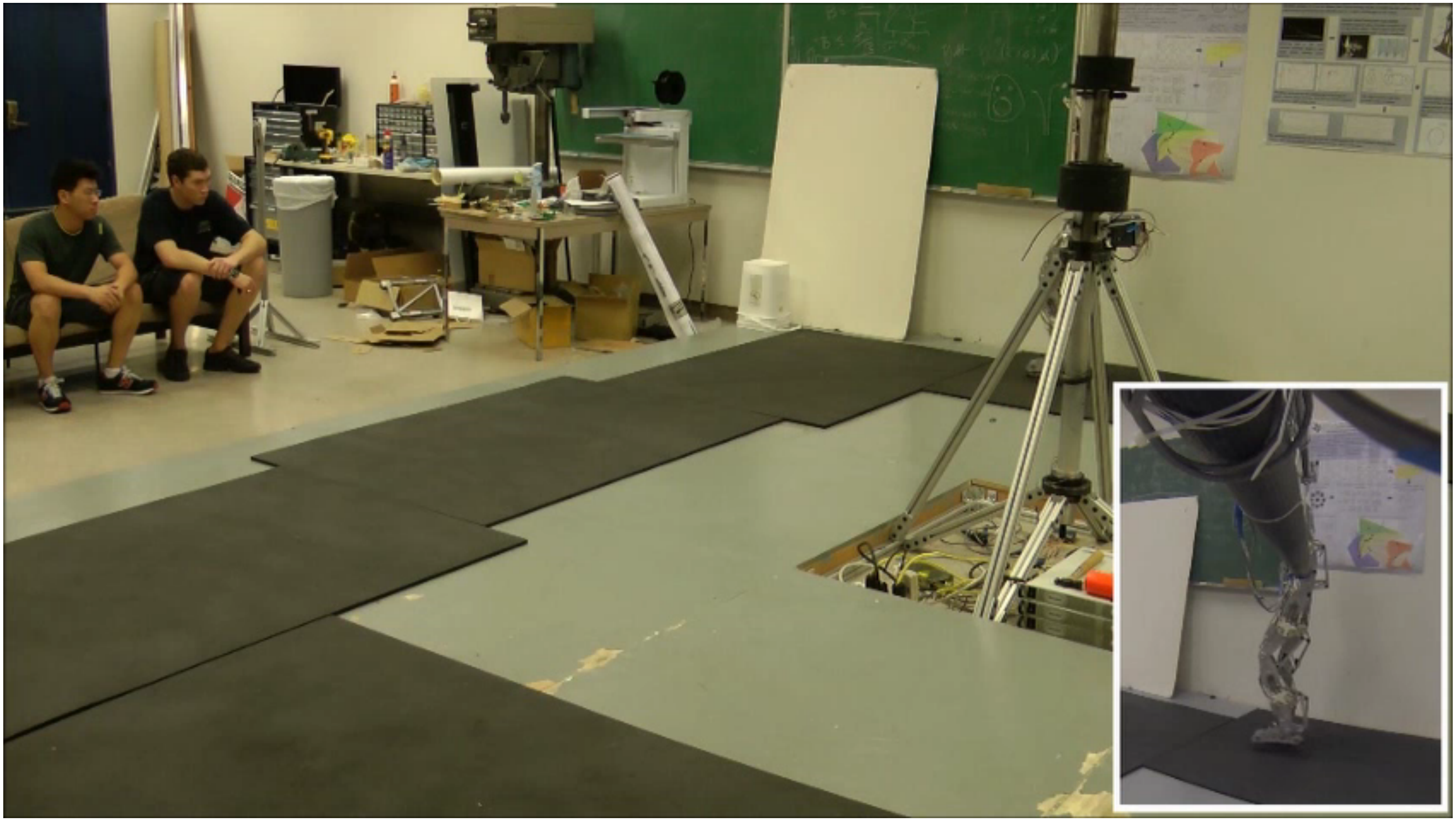


Safe set and number of inputs allowed by the controller in each state.



CPS

Formally Synthesized Walking

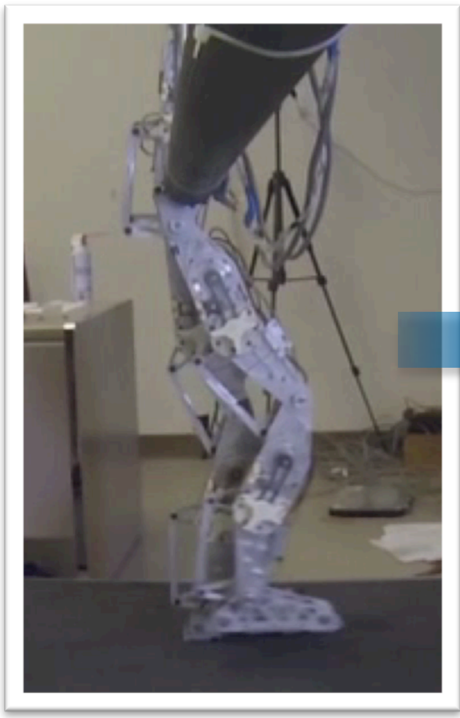


First experimental realization of formal methods on a bipedal walking robot

Future Work

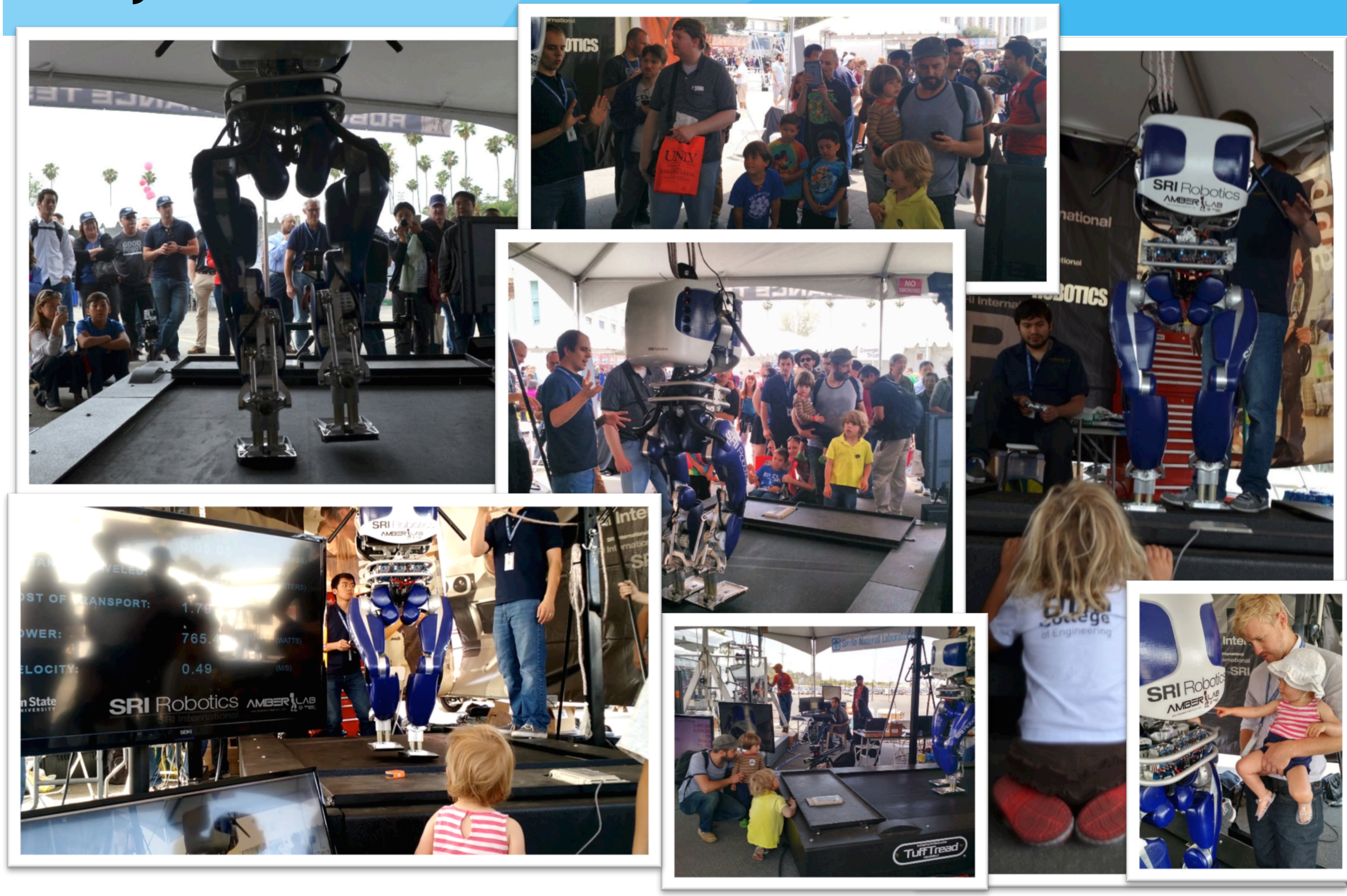
Next Steps

Implement correct-by-construction controllers experimentally on the humanoid robot DURUS



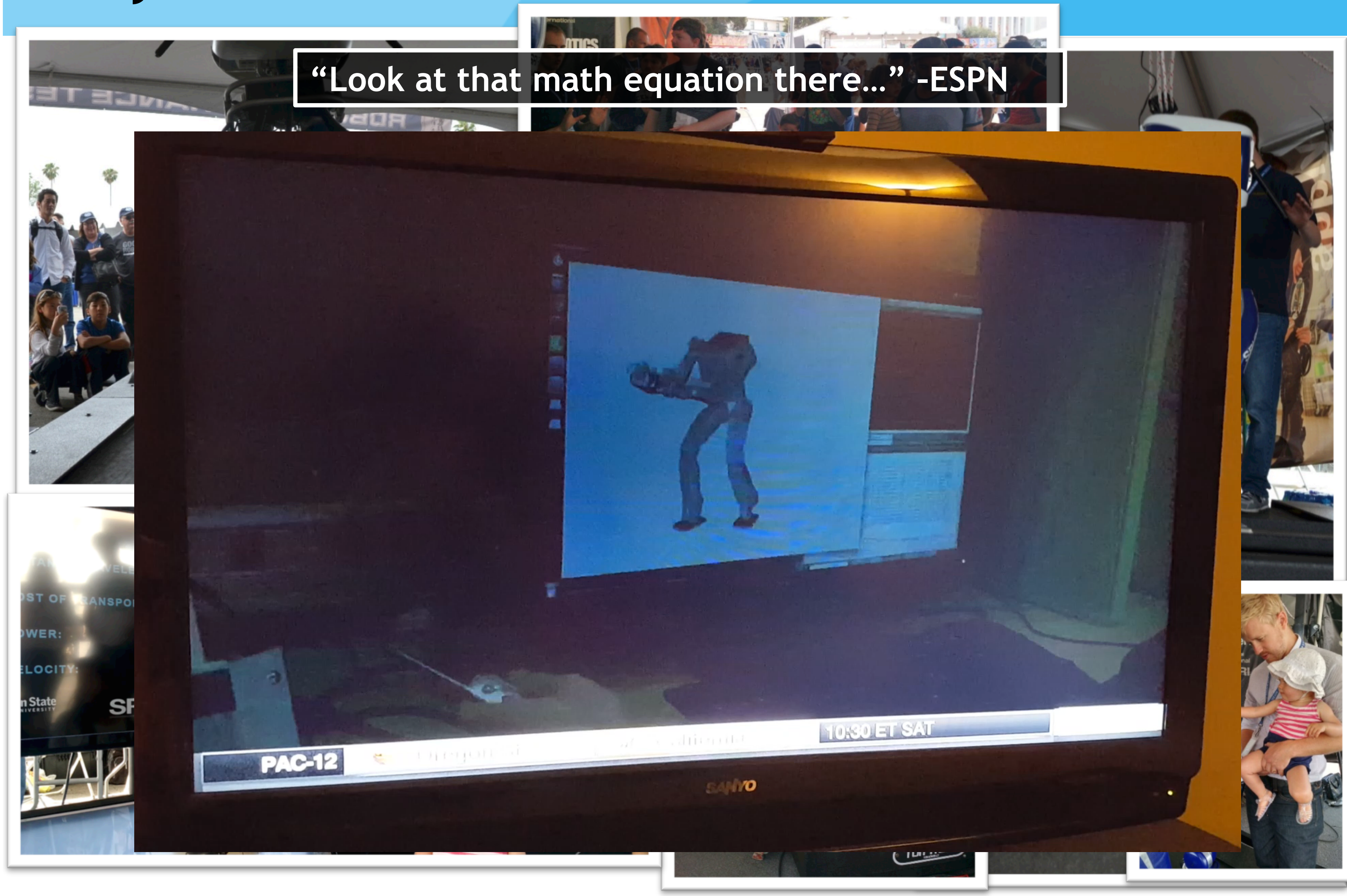
Why? Because robots are Cool…

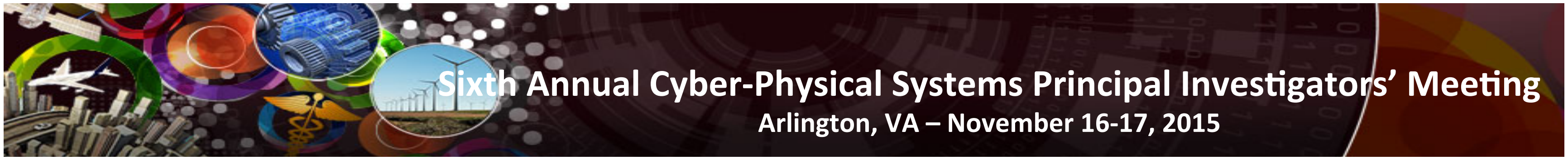
CPS



Why? Because robots are Cool…

CPS





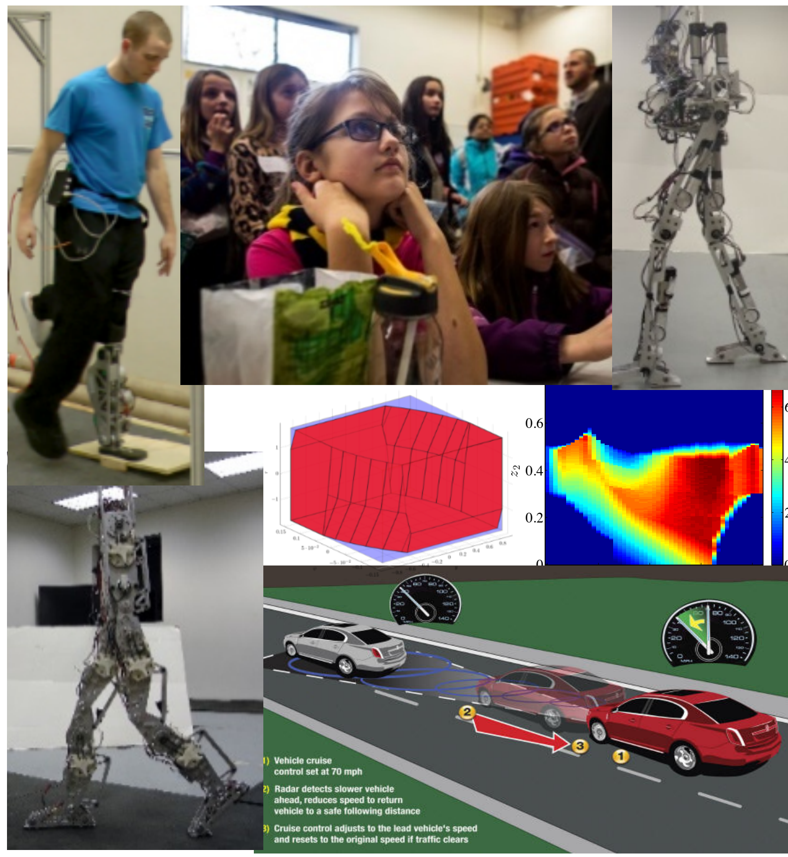
Correct-by-Design Control Software Synthesis for Highly Dynamic Systems

Challenge:

- From a formal specification, synthesize control software for highly dynamic CPS with nonlinear (hybrid) dynamics.
- Implement and evaluate on automotive and robotic hardware.

Solution:

- Two abstraction and fixed-point methods (PESSOA and PCIS).
- Control Barrier Functions.
- Safety and performance guaranteed integration via real-time quadratic programs.



CPS Awards 1239055, 1239037, and 1239085

J.W Grizzle and H. Peng (U. Michigan), A. Ames (GaTech), H. Geyer (CMU), and P. Tabuada (UCLA)

Scientific Impact:

- Use of models vetted by industry.
- Solutions to practical engineering problems with formal safety guarantees.
- Formal methods on a 14 dim. robot model with experiments.

Broader Impact:

- Two automotive safety systems:
  - Adaptive Cruise Control
  - Lane Keeping
- Presented to
  - Ford, Toyota and Eaton Corp.

Use of our Work

CPS

Obtaining precise footstep placements with periodic walking controllers (HZD) was always a problem, **not any more** - thanks to your fantastic creation of CBFs in your CDC 2014 paper. Here's a video

Prof. Koushil Sreenath, CMU

Use of our Work

Obtaining precise footstep placements with periodic walking controllers (HZD) was always a problem, **not any more** - thanks to your fantastic creation of CBFs in your CDC 2014 paper. Here's a video

Prof. Koushil Sreenath, CMU

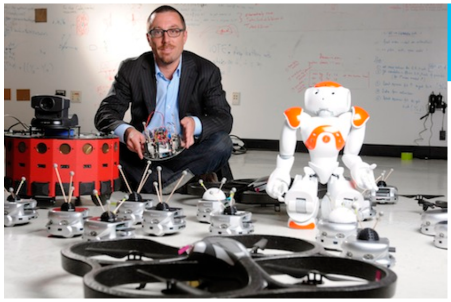
Dim. 10 model

Precise Footstep Placement for Dynamic Bipedal Walking with Control Barrier Functions

Dim. 10 model

CPS

Use of our Work



Controlling robot swarms with CBFs

Prof. Magnus Egerstedt, Georgia Tech