Synthesis of separable controlled invariant sets with tunable complexity

Petter Nilsson and Necmiye Ozay

University of Michigan

American Control Conference
Boston, MA
July 8, 2016

UNIVERSITY OF MICHIGAN

Research funded by NSF

Why formal methods?

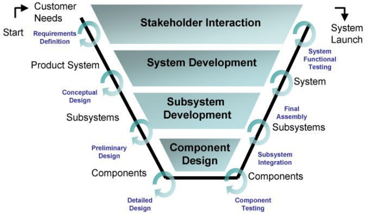


Image credit: http://digitalwrap.com

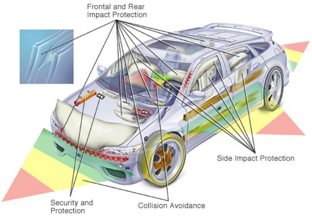


Image credit: MIT SDM

- Vision: “Specify-and-compile” instead of “test-and-tune”

Why formal methods?

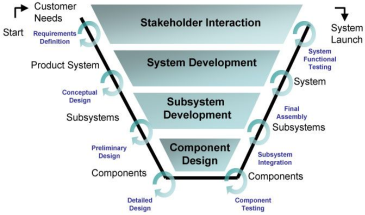


Image credit: http://digitalwrap.com

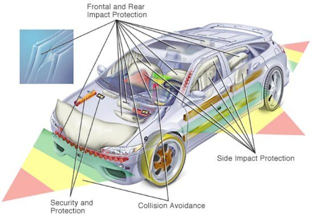


Image credit: MIT SDM

- Vision: "Specify-and-compile" instead of "test-and-tune"
- Performance guarantees: explicit treatment of requirements and assumptions

Why formal methods?

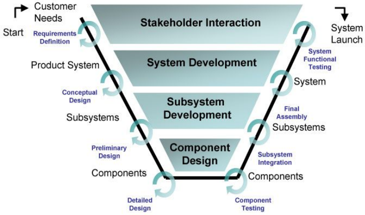


Image credit: http://digitalwrap.com

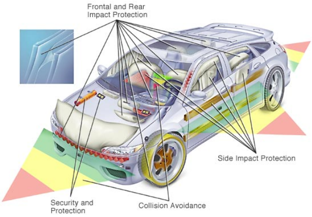
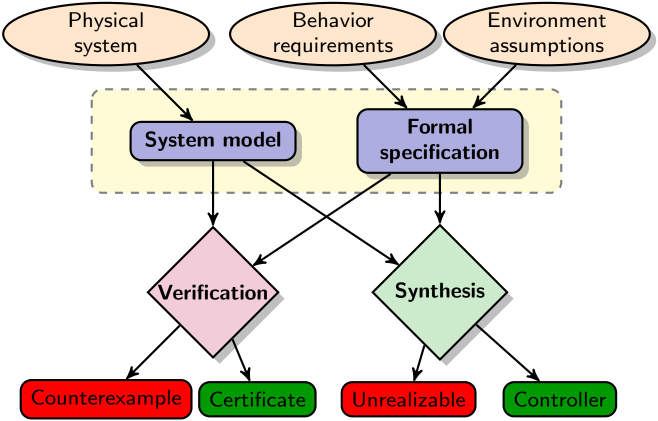


Image credit: MIT SDM

- Vision: "Specify-and-compile" instead of "test-and-tune"
- Performance guarantees: explicit treatment of requirements and assumptions
- Composition: formal contracts enable modular design

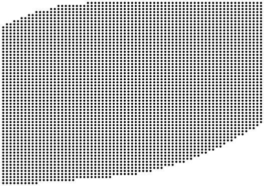
Verification and synthesis

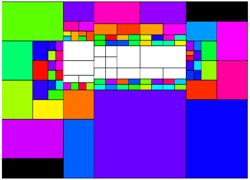


- Formal guarantees are essentially set membership guarantees
- Formal synthesis relies heavily on set computations

Issue: Curse of dimensionality

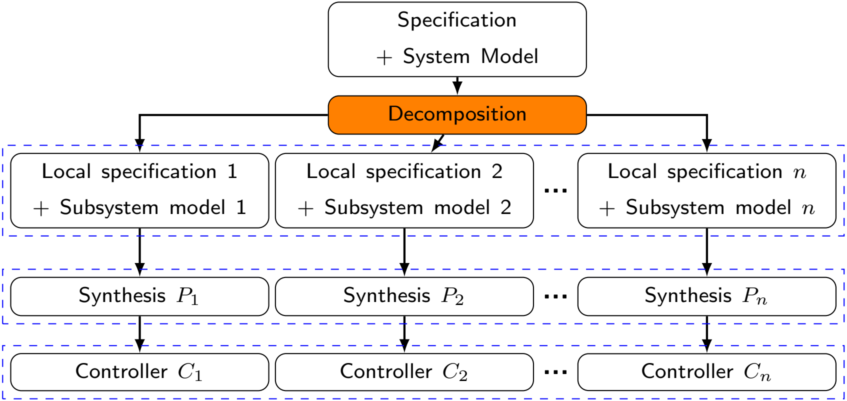
- State of the art in formal synthesis:
  - Bisimulation-based abstractions (e.g., Mazo Jr, Davitian, and Tabuada, 2010)
  - Partition-based abstractions (e.g., Liu et al., 2013)
  - Hamilton-Jacobi-Bellman methods + numerical PDE solving (e.g., Mitchell, Bayen, and Tomlin, 2005)
  - Occupation measures + SoS (e.g., Shia et al., 2014)
- With increasing dimensionality:
  - Abstraction size and partition complexity grow exponentially
  - Precise numerical PDE solving becomes intractable
  - SoS give large SDP's





Approach: Decomposition

- Solve smaller subproblems such that composition is correct



With compositional correctness guarantees

- Inspiration: ACC + Lane keeping + active steering + ...

Decomposition of dynamically coupled systems

$$\boxed{\begin{bmatrix} x_1^+ \\ x_2^+ \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}}$$

- Natural decomposition if A_{12} and A_{21} are “small”

Decomposition of dynamically coupled systems

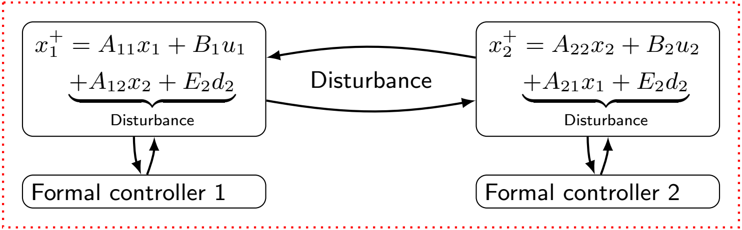
$$\boxed{\begin{bmatrix} x_1^+ \\ x_2^+ \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}}$$

$$\boxed{\begin{aligned} x_1^+ &= A_{11}x_1 + B_1u_1 \\ &\underbrace{+A_{12}x_2 + E_2d_2}_{\text{Disturbance}} \end{aligned}} \quad \underset{\longrightarrow}{\overset{\longleftarrow}{\text{Disturbance}}} \quad \boxed{\begin{aligned} x_2^+ &= A_{22}x_2 + B_2u_2 \\ &\underbrace{+A_{21}x_1 + E_2d_2}_{\text{Disturbance}} \end{aligned}}$$

- Natural decomposition if A_{12} and A_{21} are “small”
- Each subsystem needs to be robust w.r.t. influence from other subsystems

Decomposition of dynamically coupled systems

$$\boxed{\begin{bmatrix} x_1^+ \\ x_2^+ \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}}$$



- Natural decomposition if A_{12} and A_{21} are "small"
- Each subsystem needs to be robust w.r.t. influence from other subsystems

Outline

System description

Discrete time linear system model:

$$x_i^+ = A_{ii}x_i + \sum_{j \neq i} A_{ij}x_j + B_i u_i + E_i d_i$$

- Decomposition given a priori
- Coupling between subsystems
- Unique input and exogenous disturbance for each subsystem

System description

Discrete time linear system model:

$$x_i^+ = A_{ii}x_i + \sum_{j \neq i} A_{ij}x_j + B_i u_i + E_i d_i$$

- Decomposition given a priori
- Coupling between subsystems
- Unique input and exogenous disturbance for each subsystem

Constraints and assumptions:

- Linear input bounds: $H_u^i u_i \leq h_u^i$
- Disturbance assumptions: $-1 \leq H_d^i d_i \leq 1$

Problem statement

Problem (Separable controlled invariance)

Given d dynamically coupled linear subsystems with input, state, and disturbance constraints, find sets $\{\mathcal{X}_i\}_{i=1}^d$ such that

- States are constrained: $\mathcal{X}_i \subset \mathcal{S}_i := \{x_i : H_x^i x_i \leq h_x^i\}$
- $\mathcal{X}_i$ is robustly controlled invariant with respect both to coupling and exogenous disturbance:

$$\forall x_i \in \mathcal{X}_i \;\; \exists u_i \in \mathcal{U}_i \;\; \forall x_j \in \mathcal{X}_j \;\; \forall d_i \in \mathcal{D}_i, \; x_i^+ \in \mathcal{X}_i$$

Problem statement

Problem (Separable controlled invariance)

Given d dynamically coupled linear subsystems with input, state, and disturbance constraints, find sets $\{\mathcal{X}_i\}_{i=1}^d$ such that

- States are constrained: $\mathcal{X}_i \subset \mathcal{S}_i := \{x_i : H_x^i x_i \leq h_x^i\}$
- $\mathcal{X}_i$ is robustly controlled invariant with respect both to coupling and exogenous disturbance:

$$\forall x_i \in \mathcal{X}_i \;\; \exists u_i \in \mathcal{U}_i \;\; \forall x_j \in \mathcal{X}_j \;\; \forall d_i \in \mathcal{D}_i, \;\; x_i^+ \in \mathcal{X}_i$$

We restrict the search to $\mathcal{X}_i$'s that

- Are symmetric zonotopes: $\mathcal{X}_i = \left\{x_i : -\mathbf{1} \leq Z_i H_x^i x_i \leq \mathbf{1}\right\}$
  - Z_i is a given matrix of (arbitrarily many) zonotope generators

Problem statement

Problem (Separable controlled invariance)

Given d dynamically coupled linear subsystems with input, state, and disturbance constraints, find sets $\{\mathcal{X}_i\}_{i=1}^d$ such that

- States are constrained: $\mathcal{X}_i \subset \mathcal{S}_i := \{x_i : H_x^i x_i \leq h_x^i\}$
- $\mathcal{X}_i$ is robustly controlled invariant with respect both to coupling and exogenous disturbance:

$$\forall x_i \in \mathcal{X}_i \;\; \exists u_i \in \mathcal{U}_i \;\; \forall x_j \in \mathcal{X}_j \;\; \forall d_i \in \mathcal{D}_i, \;\; x_i^+ \in \mathcal{X}_i$$

We restrict the search to $\mathcal{X}_i$'s that

- Are symmetric zonotopes: $\mathcal{X}_i = \left\{x_i : -\mathbf{1} \leq Z_i H_x^i x_i \leq \mathbf{1}\right\}$
  - Z_i is a given matrix of (arbitrarily many) zonotope generators
- Can be rendered invariant by a local feedback controller $u_i = \sum_j K_{ij} x_j$
  - Non-zero K_{ij} indicates information availability

Problem features

- Controlled invariant sets $\{\mathcal{X}_i\}_{i=1}^d$ provide an assume guarantee protocol for invariance: system i stays in $\mathcal{X}_i$ as long as system j $(j \neq i)$ stays in $\mathcal{X}_j$
- Enables decoupled formal synthesis for more sophisticated control objectives can be performed within robust controlled invariant sets
- Trade-off: larger sets impose more disturbance on neighboring systems

Outline

Main result

Theorem

If there exist matrices H_x^{-1}, $\hat{K}$, $\Lambda \succ 0$, $D_x^j \succ 0$, Φ_j^{-1}, Γ_j, Ξ_j, Ψ_j, Ω_j^1, Ω_j^2 *with certain structures*[1] *for all* $j = 1, \ldots, \mathcal{N}_x$, *diagonal* $D_s^k \succ 0$ *for all* $k = 1, \ldots, \mathcal{N}_s$, *and diagonal* $D_u^l \succ 0$ *for all* $l = 1, \ldots, \mathcal{N}_u$ *such that a set of linear matrix inequalities hold, then the block diagonal pair* $(H_x, \hat{K} H_x)$ *constitutes a solution to the separable controlled invariance problem when appropriately decomposed.*

- LMI feasibility condition
- $\mathcal{N}_x, \mathcal{N}_s, \mathcal{N}_u$ are the total numbers of zonotope generators, state constraints, and input constraints, respectively
- Size of matrix variables linear in total system dimension

[1] such as block diagonal, symmetric, diagonal

LMI's

$$\left.\begin{aligned}
&\begin{bmatrix} \Xi_j - \Phi_j^{-1} & \Omega_j^1 - \begin{bmatrix} H_x^{-1} & 0 \\ 0 & H_x^{-1} \end{bmatrix} & \Omega_j^2 - \begin{bmatrix} H_x^{-1} & 0 \\ 0 & H_x^{-1} \end{bmatrix} & \Psi_j^T \begin{bmatrix} Z^T e_j \\ Z^T e_j \end{bmatrix} \\ * & 2\begin{bmatrix} \Lambda & 0 \\ 0 & \Lambda \end{bmatrix} - \Gamma_j & \begin{bmatrix} \Lambda & 0 \\ 0 & \Lambda \end{bmatrix} + (\Omega_j^1)^T - \Psi_j & 0 \\ * & * & \Omega_j^2 + (\Omega_j^2)^T - \Xi_j & 0 \\ * & * & * & \lambda_{i(j)} - \mathbf{1}^T D_x^j \mathbf{1} - \mathbf{1}^T D_d^j \mathbf{1} \end{bmatrix} \succ 0 \\
&\begin{bmatrix} \Gamma_j & \Psi_j \\ * & \Xi_j \end{bmatrix} \succ 0 \\
&\begin{bmatrix} Z^T D_x^j Z & 0 & -\frac{1}{2}(H_x^{-T} A^T + \hat{K}^T B^T) & 0, \\ * & D_d^j & 0 & -\frac{1}{2} H_d^{-T} E^T \\ * & & \left[\Phi_j^{-1}\right] & \end{bmatrix} \succ 0
\end{aligned}\right\} \text{(inv.)}$$

$$\begin{bmatrix} Z^T D_s^k Z & -\frac{1}{2} H_x^{-T} H_s^T e_k \\ * & e_k^T h_s - \mathbf{1}^T D_s^k \mathbf{1} \end{bmatrix} \succ 0 \quad \text{(state constraints)}$$

$$\begin{bmatrix} Z^T D_u^l Z & -\frac{1}{2} \hat{K}^T H_u^T e_l \\ * & e_l^T h_u - \mathbf{1}^T D_u^l \mathbf{1} \end{bmatrix} \succ 0 \quad \text{(input constraints)}$$

- Desired variables
- "S Procedure matrices"
- Slack variables

Proof outline

- Ideas borrowed from (Tahir and Jaimoukha, 2015, TAC)

Want to find $\mathcal{X}$ s.t. that $A_K \mathcal{X} \oplus E\mathcal{D} \subset \mathcal{X}$, i.e.,

$$e_j^T Z H_x (A_K x + Ed) - 1 \leq 0$$

for all $x \in \mathcal{X}$, $d \in \mathcal{D}$ and for all $j = 1, \ldots \mathcal{N}_x$.

Proof outline

- Express set membership as quadratic inequality

Lemma

$x \in \mathcal{X} = \{x : -\mathbb{1} \leq ZH_x x \leq \mathbb{1}\}$ *if and only if for all diagonal* $D_x \succ 0$

$$(\mathbb{1} - ZH_x x)^T D_x (\mathbb{1} + ZH_x x) \geq 0.$$

$d \in \mathcal{D} = \{d : -\mathbb{1} \leq H_d d \leq \mathbb{1}\}$ *if and only if for all diagonal* $D_d \succ 0$

$$(\mathbb{1} - H_d d)^T D_d (\mathbb{1} + H_d d) \geq 0.$$

Proof outline

- "For all" quantifiers can be expressed as matrix inequalities using the S Procedure

$$
\begin{aligned}
&e_j^T Z H_x (A_K x + Ed) - 1 \\
&\quad = -(\mathbb{1} - Z H_x x)^T \tilde{D}_x^j (\mathbb{1} + Z H_x x) \\
&\quad -(\mathbb{1} - Z H_d d)^T \tilde{D}_d^j (\mathbb{1} + Z H_d d) \\
&\quad - \begin{bmatrix} x^T & d^T & 1 \end{bmatrix} L_x^j(\tilde{D}_x^j, \tilde{D}_d^j) \begin{bmatrix} x^T & d^T & 1 \end{bmatrix}^T
\end{aligned}
$$

Lemma

$e_j^T Z H_x (A_K x + Ed) - 1 \leq 0$ *for all* $x \in \mathcal{X}$, $d \in \mathcal{D}$ *if and only if there are* $\tilde{D}_x^j \succ 0$, $\tilde{D}_d^j \succ 0$ *s.t.* $L_x^j(\tilde{D}_x^j, \tilde{D}_d^j) \succ 0$

Proof outline

- Use slack variable techniques to eliminate matrix products

Lemma

Let R (sym), Z (sym), A (full) and B (full) be arbitrary matrices. Then the following conditions are equivalent

1. $$\begin{bmatrix} R & AB \\ * & Z \end{bmatrix} \succ 0.$$

2. $$\exists X \text{ (sym)} : \begin{bmatrix} R & A \\ * & X^{-1} \end{bmatrix} \succ 0, \begin{bmatrix} X & B \\ * & Z \end{bmatrix} \succ 0$$

Proof outline

- Use slack variable techniques to eliminate matrix products

Lemma

If there exist Θ (full), Γ (sym) and Ξ (sym) such that

$$\Delta \doteq \begin{bmatrix} \Gamma & Y \\ * & \Xi \end{bmatrix} \succ 0, \quad \begin{bmatrix} Z+\Xi & [-X \ \ I]\Theta & V \\ * & \Theta+\Theta^T-\Delta & 0 \\ * & * & W \end{bmatrix} \succ 0,$$

then

$$\begin{bmatrix} Z+XY+Y^TX^T & V \\ * & W \end{bmatrix} \succ 0.$$

- LMI's are obtained by restricting shape of certain matrices
  - Introduces some conservatism

Outline

Ex 1: Advantage of Zonotopes

Subsystem 1

$$\begin{bmatrix} x_1^+ \\ y_1^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} u_1^x \\ u_2^y \end{bmatrix} + 0.1\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} d_1^x \\ d_1^y \end{bmatrix}$$

Subsystem 2

$$\begin{bmatrix} x_2^+ \\ y_2^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} u_2^x \\ u_2^y \end{bmatrix} + 0.1\begin{bmatrix} x_1 + x_3 \\ y_1 + y_3 \end{bmatrix} + \begin{bmatrix} d_2^x \\ d_2^y \end{bmatrix}$$

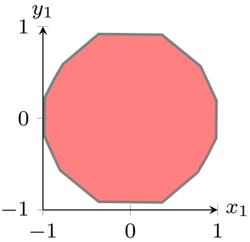
Subsystem 3

$$\begin{bmatrix} x_3^+ \\ y_3^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_3 \\ y_3 \end{bmatrix} + \begin{bmatrix} u_3^x \\ u_3^y \end{bmatrix} + 0.1\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} d_3^x \\ d_3^y \end{bmatrix}$$

Ex 1: Advantage of Zonotopes

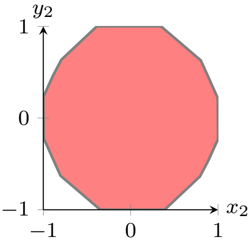
Subsystem 1

$$\begin{bmatrix} x_1^+ \\ y_1^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} u_1^x \\ u_2^y \end{bmatrix} + 0.1\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} d_1^x \\ d_1^y \end{bmatrix}$$



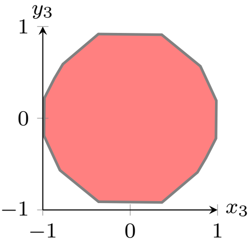
Subsystem 2

$$\begin{bmatrix} x_2^+ \\ y_2^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} u_2^x \\ u_2^y \end{bmatrix} + 0.1\begin{bmatrix} x_1 + x_3 \\ y_1 + y_3 \end{bmatrix} + \begin{bmatrix} d_2^x \\ d_2^y \end{bmatrix}$$



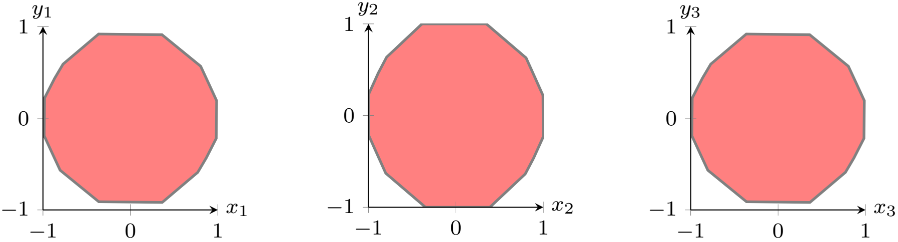
Subsystem 3

$$\begin{bmatrix} x_3^+ \\ y_3^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_3 \\ y_3 \end{bmatrix} + \begin{bmatrix} u_3^x \\ u_3^y \end{bmatrix} + 0.1\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} d_3^x \\ d_3^y \end{bmatrix}$$



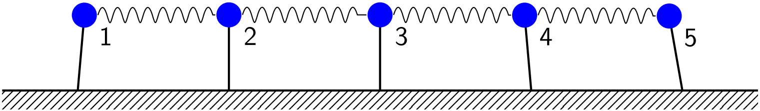
Ex 1: Advantage of Zonotopes

Subsystem 1	Subsystem 2	Subsystem 3
$\begin{bmatrix} x_1^+ \\ y_1^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} u_1^x \\ u_2^y \end{bmatrix} + 0.1\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} d_1^x \\ d_1^y \end{bmatrix}$	$\begin{bmatrix} x_2^+ \\ y_2^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} u_2^x \\ u_2^y \end{bmatrix} + 0.1\begin{bmatrix} x_1 + x_3 \\ y_1 + y_3 \end{bmatrix} + \begin{bmatrix} d_2^x \\ d_2^y \end{bmatrix}$	$\begin{bmatrix} x_3^+ \\ y_3^+ \end{bmatrix} = 0.8R\left(\frac{\pi}{4}\right)\begin{bmatrix} x_3 \\ y_3 \end{bmatrix} + \begin{bmatrix} u_3^x \\ u_3^y \end{bmatrix} + 0.1\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} + \begin{bmatrix} d_3^x \\ d_3^y \end{bmatrix}$



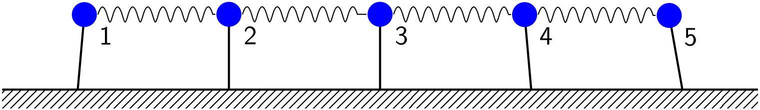
- Infeasible with hyperboxes as in (Tahir and Jaimoukha, 2015, TAC)

Ex 2: Connected inverted pendulums



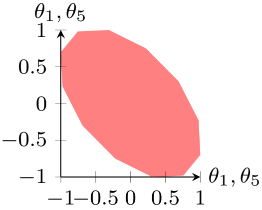
- Appears in literature on decentralized stabilization
- Each pendulum has two states, 10-dimensional system
- Neighbor state sharing

Ex 2: Connected inverted pendulums

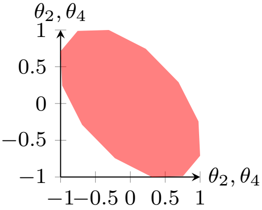


- Appears in literature on decentralized stabilization
- Each pendulum has two states, 10-dimensional system
- Neighbor state sharing

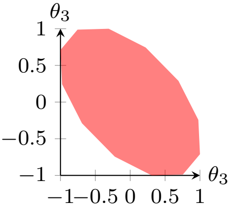
Robust controlled invariant sets:



Pendulums 1,5

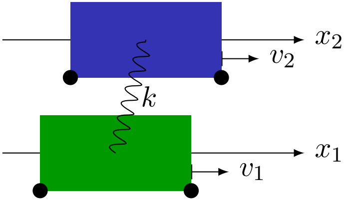


Pendulums 2,4



Pendulum 3

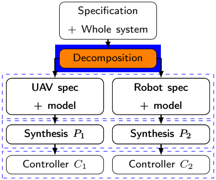
Ex 3: Interconnected ground robot and UAV



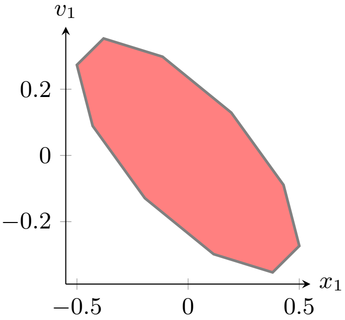
- Toy example of 1D-robots connected by a spring
- Integrator dynamics

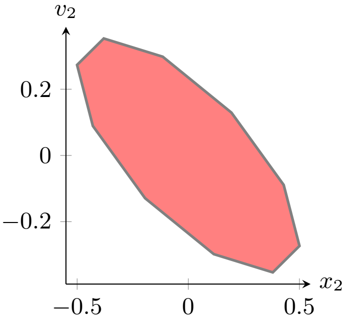
$$
\begin{aligned}
{x_1}^+ &= x_1 && +v_1 \\
{v_1}^+ &= kx_1 && +v_1 - kx_2 \\
{x_2}^+ &= && + x_2 \quad +v_2 \\
{v_2}^+ &= -kx_1 && + kx_2 \quad +v_2
\end{aligned}
$$

Ex 3: Invariant sets

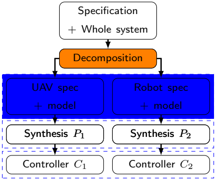


1. Find invariant sets



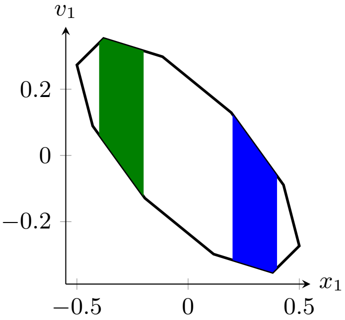


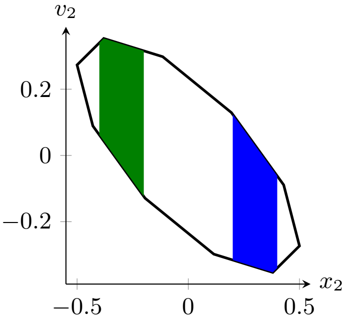
Ex 3: Invariant sets



1. Find invariant sets
2. Do local synthesis for

$$\bigwedge_{i=1}^{2} \Box\Diamond \left(x_i \in {\color{green}\blacksquare}\right) \wedge \Box\Diamond \left(x_i \in {\color{blue}\blacksquare}\right)$$

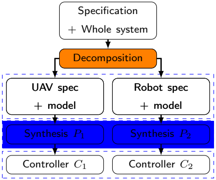


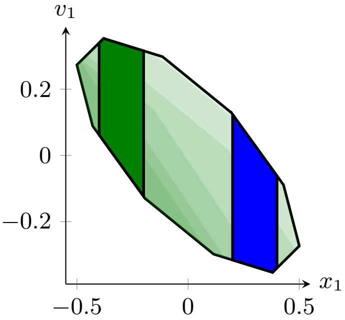


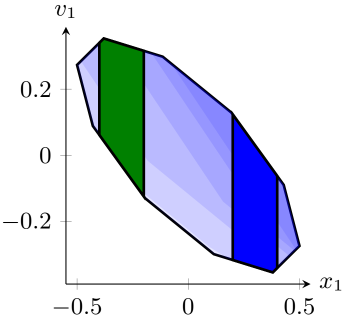
Ex 3: Invariant sets

1. Find invariant sets
2. Do local synthesis for

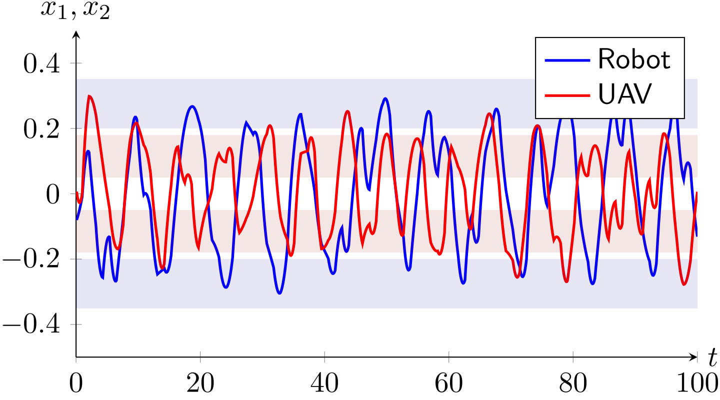
$$\bigwedge_{i=1}^{2} \Box\Diamond (x_i \in \text{green}) \wedge \Box\Diamond (x_i \in \text{blue})$$





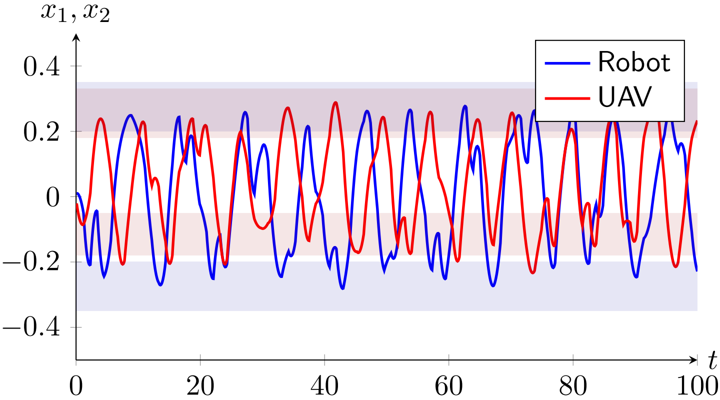


Ex 3: local synthesis



- Visit both green and blue areas infinitely often
- Solving two 2-dimensional problems instead of one 4-dimensional

Ex 3: local synthesis

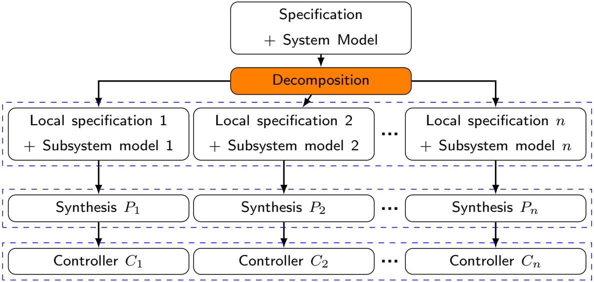


- Can re-synthesize for different specification without re-computing sets

Outline

Main takeaways:

- Decoupled formal synthesis through separable controlled invariant set computation
- Tunable complexity
- Handles input and state constraints, exogenous disturbance
- Flexible w.r.t. information sharing patterns



With compositional correctness guarantees

Main takeaways:

- Decoupled formal synthesis through separable controlled invariant set computation
- Tunable complexity
- Handles input and state constraints, exogenous disturbance
- Flexible w.r.t. information sharing patterns

Future work:

- Exploit sparsity to make LMI solving more efficient
- Application to more realistic systems

Thank you for your attention