# Safety control with performance guarantees of cooperative systems using compositional abstractions

**Pierre-Jean Meyer** Antoine Girard Emmanuel Witrant

Université Grenoble-Alpes

ADHS'15, October $16^{th}$ 2015

# Outline

# System description

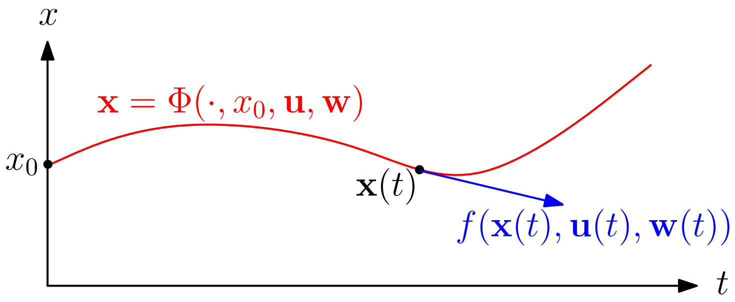
Nonlinear control system:

$$\dot{x} = f(x, u, w)$$

Trajectories:

$$\mathbf{x} = \Phi(\cdot, x_0, \mathbf{u}, \mathbf{w})$$

- $x$: state
- $u$: control input
- $w$: disturbance input
- $\mathbf{x}$, $\mathbf{u}$, $\mathbf{w}$: time functions

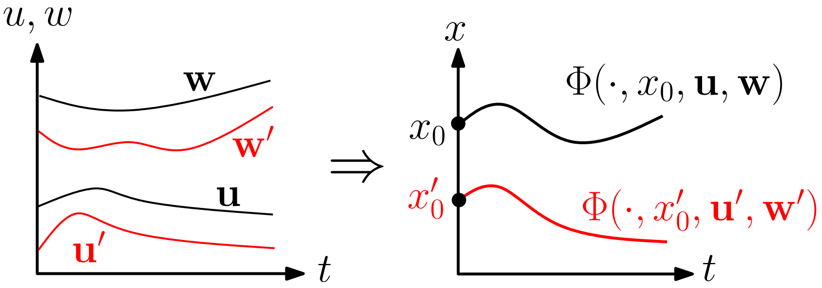


# Cooperative system

## Definition (Cooperativeness)

The system is cooperative if $\Phi$ preserves the componentwise inequality:

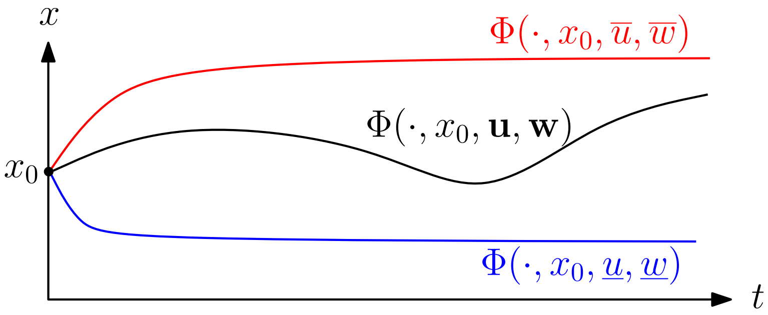
$$\mathbf{u} \geq \mathbf{u}',\ \mathbf{w} \geq \mathbf{w}',\ x_0 \geq x_0' \Rightarrow\ \forall t \geq 0,\ \Phi(t, x, \mathbf{u}, \mathbf{w}) \geq \Phi(t, x', \mathbf{u}', \mathbf{w}')$$



# Bounded inputs

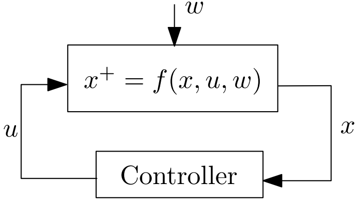
Control and disturbance inputs bounded in intervals:

$$\forall t \geq 0,\ \mathbf{u}(t) \in [\underline{u}, \overline{u}],\ \mathbf{w}(t) \in [\underline{w}, \overline{w}]$$
$$\Longrightarrow$$
$$\forall t \geq 0,\ \Phi(t, x_0, \mathbf{u}, \mathbf{w}) \in [\Phi(t, x_0, \underline{u}, \underline{w}), \Phi(t, x_0, \overline{u}, \overline{w})]$$

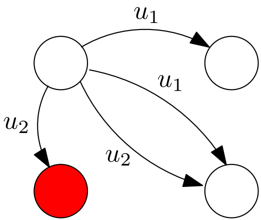


# Outline

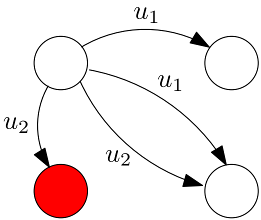
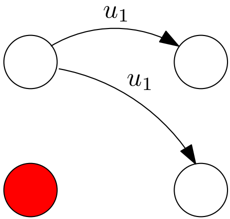
# Abstraction-based synthesis

| | Continuous state | |
|---|---|---|
| Uncontrolled | $x^+ = f(x, u, w)$ | |
| | Synthesis | |
| Controlled |  | |

# Abstraction-based synthesis

| | Continuous state | Discrete state |
|---|---|---|
| Uncontrolled | $x^+ = f(x, u, w)$ Abstraction → |  |
| Controlled | | |

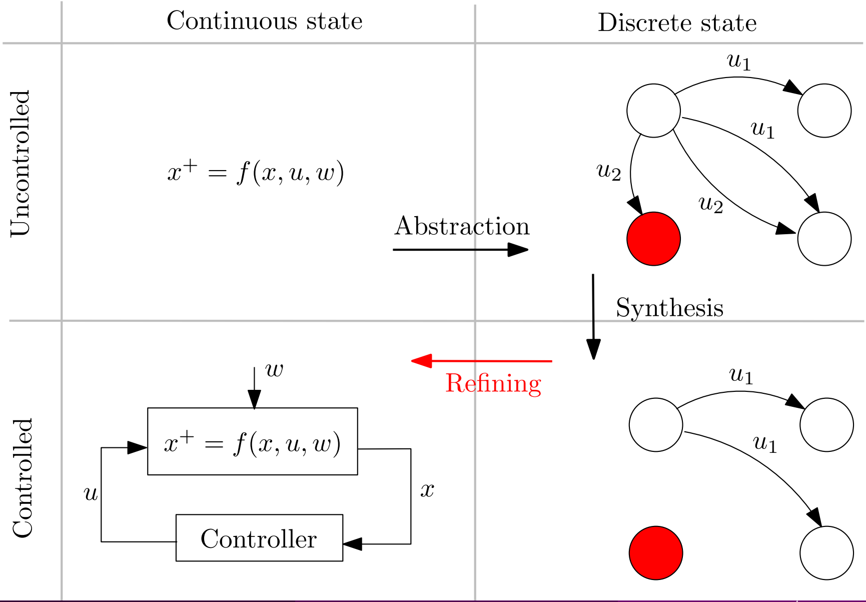
# Abstraction-based synthesis

| | Continuous state | Discrete state |
|---|---|---|
| Uncontrolled | $x^+ = f(x,u,w)$ |  |
| Controlled | |  |

Abstraction $\longrightarrow$

Synthesis $\downarrow$

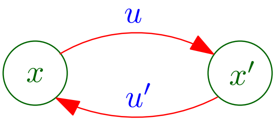
# Abstraction-based synthesis



# Transition systems

$S = (X, U, \longrightarrow)$

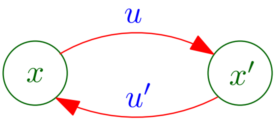
- Set of states $X$
- Set of inputs $U$
- Transition relation $\longrightarrow$
- Trajectories: $x_1 \xrightarrow{u_1} x_2 \xrightarrow{u_2} x_3 \xrightarrow{u_3} \dots$



# Transition systems

$S = (X, U, \longrightarrow)$

- Set of states $X$
- Set of inputs $U$
- Transition relation $\longrightarrow$
- Trajectories: $x_1 \xrightarrow{u_1} x_2 \xrightarrow{u_2} x_3 \xrightarrow{u_3} \dots$



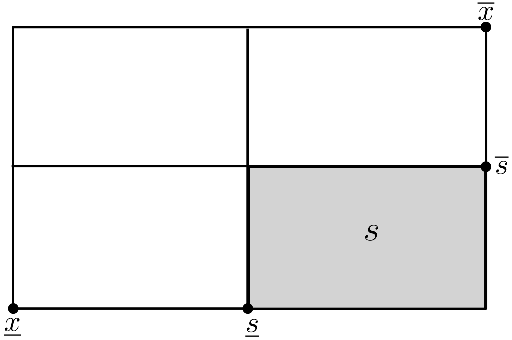

Sampled dynamics (sampling $\tau$)

- $X = \mathbb{R}^n$
- $U = [\underline{u}, \overline{u}]$
- $x \xrightarrow{u} x' \iff \exists \mathbf{w} : [0,\tau] \to [\underline{w}, \overline{w}] \mid x' = \Phi(\tau, x, u, \mathbf{w})$

- Safety specification in $[\underline{x}, \overline{x}] \subseteq \mathbb{R}^n$

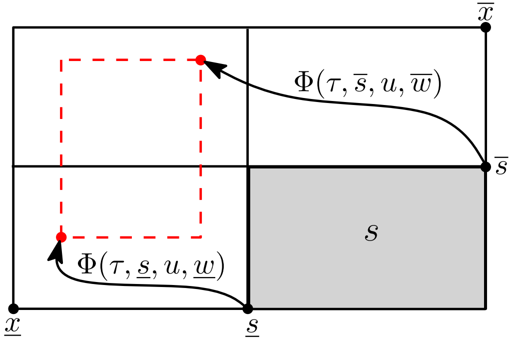
# Abstraction

- Discretization of the control space $[\underline{u}, \overline{u}]$
- Partition $\mathcal{P}$ of the interval $[\underline{x}, \overline{x}]$ into **symbols**



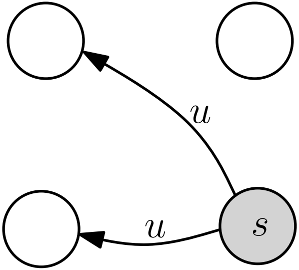
# Abstraction

- Discretization of the control space $[\underline{u}, \overline{u}]$
- Partition $\mathcal{P}$ of the interval $[\underline{x}, \overline{x}]$ into **symbols**
- Over-approximation of the reachable set (cooperativeness)



# Abstraction

- Discretization of the control space $[\underline{u}, \overline{u}]$
- Partition $\mathcal{P}$ of the interval $[\underline{x}, \overline{x}]$ into **symbols**
- Over-approximation of the reachable set (cooperativeness)
- Intersection with the partition




Obtain a finite abstraction $S_a = (X_a, U_a, \underset{a}{\longrightarrow})$

# Alternating simulation

## Definition (Alternating simulation relation)

$H : X \to X_a$ is an alternating simulation relation from $S_a$ to $S$ if:

$$\forall u_a \in U_a,\ \exists u \in U \mid x \xrightarrow{u} x' \text{ in } S \Longrightarrow H(x) \xrightarrow[a]{u_a} H(x') \text{ in } S_a$$

# Alternating simulation

## Definition (Alternating simulation relation)

$H : X \to X_a$ is an alternating simulation relation from $S_a$ to $S$ if:

$$\forall u_a \in U_a,\ \exists u \in U \mid x \xrightarrow{u} x' \text{ in } S \implies H(x) \xrightarrow[a]{u_a} H(x') \text{ in } S_a$$

## Proposition

*The map $H : X \to X_a$ defined by*

$$H(x) = s \iff x \in s$$

*is an alternating simulation relation from $S_a$ to $S$:*

$$\forall u_a \in U_a \subseteq U \mid x \xrightarrow{u_a} x' \textit{ in } S \implies H(x) \xrightarrow[a]{u_a} H(x') \textit{ in } S_a$$

# Safety synthesis

**Specification:** safety of $S_a$ in $\mathcal{P}$ (the partition of the interval $[\underline{x}, \overline{x}]$)

$$F_{\mathcal{P}}(Z) = \{s \in Z \cap \mathcal{P} \mid \exists\ u,\ \forall\ s \xrightarrow[a]{u} s',\ s' \in Z\}$$

# Safety synthesis

**Specification:** safety of $S_a$ in $\mathcal{P}$ (the partition of the interval $[\underline{x}, \overline{x}]$)

$$F_{\mathcal{P}}(Z) = \{s \in Z \cap \mathcal{P} \mid \exists\ u,\ \forall\ s \xrightarrow[a]{u} s',\ s' \in Z\}$$

Fixed-point $Z_a$ of $F_{\mathcal{P}}$ reached in **finite time**
$Z_a$ is the **maximal safe set** for $S_a$, associated with the safety controller:

$$C_a(s) = \{u \mid \forall\ s \xrightarrow[a]{u} s',\ s' \in Z_a\}$$

**Theorem**

*$C_a$ is a safety controller for $S$ in $Z_a$.*

# Performance criterion

Minimize on a trajectory $(x^0, u^0, x^1, u^1, \dots)$ of $S$:

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k)$$

with a cost function $g$ and a **discount factor** $\lambda \in (0, 1)$

# Performance criterion

Minimize on a trajectory $(x^0, u^0, x^1, u^1, \dots)$ of $S$:

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k)$$

with a cost function $g$ and a **discount factor** $\lambda \in (0, 1)$

Cost function on $S_a$: $g_a(s, u) = \max_{x \in s} g(x, u)$
Focus the optimization on a **finite horizon** of $N$ sampling periods
Accurate approximation if $\lambda^{N+1} \ll 1$

# Optimization

Dynamic programming algorithm:

$$J_a^N(s) = \min_{u \in C_a(s)} g_a(s,u)$$

$$J_a^k(s) = \min_{u \in C_a(s)} \left( g_a(s,u) + \lambda \max_{s \xrightarrow[a]{u} s'} J_a^{k+1}(s') \right), \ \forall k < N$$

$J_a^0(s)$ is the **worst-case minimization** of $\sum_{k=0}^{N} \lambda^k g_a(s^k, u^k)$

# Optimization

Dynamic programming algorithm:

$$J_a^N(s) = \min_{u \in C_a(s)} g_a(s,u)$$

$$J_a^k(s) = \min_{u \in C_a(s)} \left( g_a(s,u) + \lambda \max_{s \xrightarrow[a]{u} s'} J_a^{k+1}(s') \right), \ \forall k < N$$

$J_a^0(s)$ is the **worst-case minimization** of $\sum_{k=0}^{N} \lambda^k g_a(s^k, u^k)$

Receding horizon controller:

$$C_a^*(s) = \arg\min_{u \in C_a(s)} \left( g_a(s,u) + \lambda \max_{s \xrightarrow[a]{u} s'} J_a^1(s') \right)$$

# Performance guarantees

## Theorem

*Let $(x^0, u^0, x^1, u^1, \dots)$ be a trajectory of $S$ controlled with $C_a^*$. Let $s^0, s^1, \dots$ such that $x^k \in s^k$, for all $k \in \mathbb{N}$. Then,*

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k) \leq$$

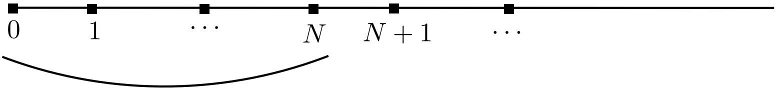
# Performance guarantees

## Theorem

*Let $(x^0, u^0, x^1, u^1, \dots)$ be a trajectory of $S$ controlled with $C_a^*$.*
*Let $s^0, s^1, \dots$ such that $x^k \in s^k$, for all $k \in \mathbb{N}$. Then,*

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k) \leq J_a^0(s^0) +$$

Worst-case minimization on finite horizon:




$$\sum_{k=0}^{N} \lambda^k g_a(s^k, u^k) \leq J_a^0(s^0)$$

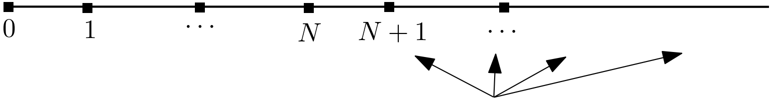
# Performance guarantees

## Theorem

*Let* $(x^0, u^0, x^1, u^1, \dots)$ *be a trajectory of* $S$ *controlled with* $C_a^*$.
*Let* $s^0, s^1, \dots$ *such that* $x^k \in s^k$, *for all* $k \in \mathbb{N}$. *Then,*

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k) \leq J_a^0(s^0) + \frac{\lambda^{N+1}}{1-\lambda} M_a$$

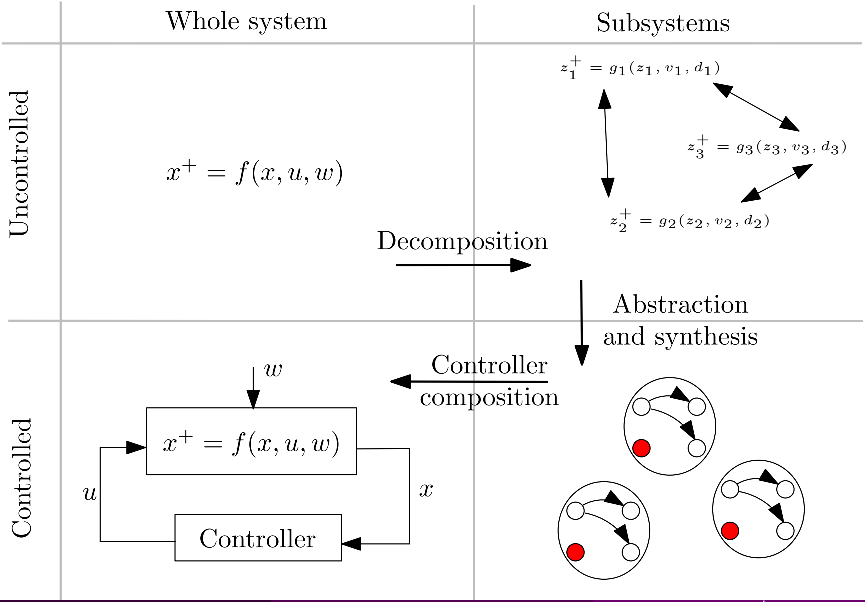
Worst-case minimization of each remaining steps (receding horizon):




$$g_a(s^k, u^k) \leq \max_{s \in Z_a} \min_{u \in C_a(s)} g_a(s,u) = M_a$$

# Outline

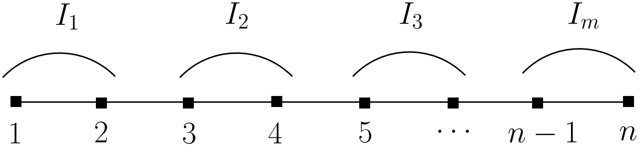
# Compositional synthesis



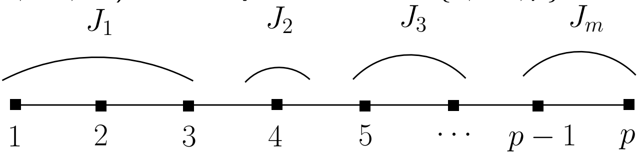
# Decomposition

Decomposition into $m$ subsystems:

Partition $(I_1, \dots, I_m)$ of the **state** dimensions $\{1, \dots, n\}$



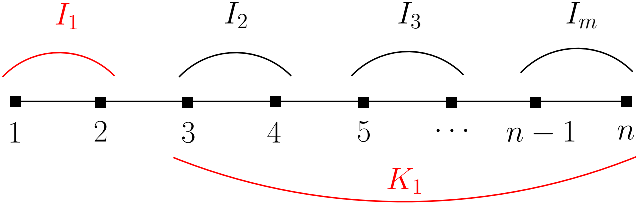

Partition $(J_1, \dots, J_m)$ of the **input** dimensions $\{1, \dots, p\}$



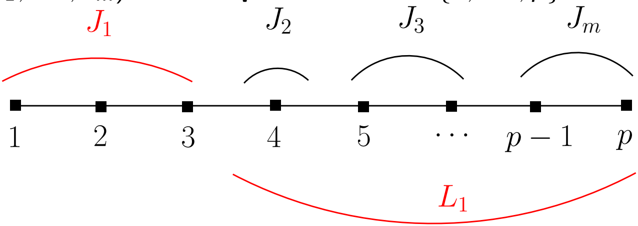
# Decomposition

Decomposition into $m$ subsystems:

Partition $(I_1, \dots, I_m)$ of the **state** dimensions $\{1, \dots, n\}$




Partition $(J_1, \dots, J_m)$ of the **input** dimensions $\{1, \dots, p\}$




Control the states $x_{I_1}$ using the inputs $u_{J_1}$ with disturbances $x_{K_1}$ and $u_{L_1}$

# Abstraction

Symbolic abstraction $S_i = (X_i, U_i, \underset{i}{\longrightarrow})$ of subsystem $i \in \{1, \dots, m\}$:

Classical method, but with an **assume-guarantee obligation**:

**A/G Obligation ($K_i$)**

*Unobserved states:* $x_{K_i} \in [\underline{x}_{K_i}, \overline{x}_{K_i}]$

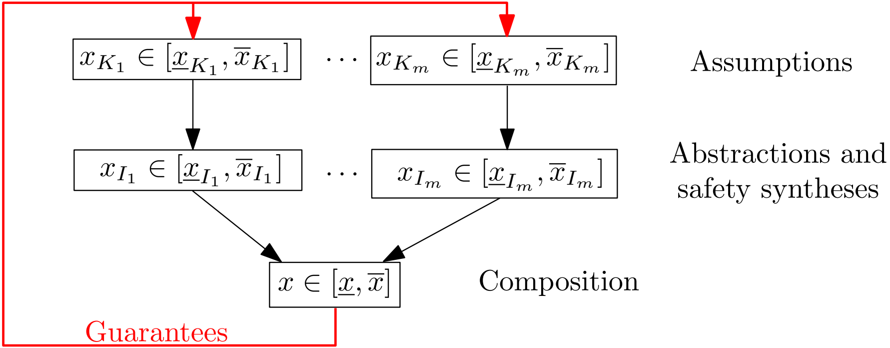
# Abstraction

Symbolic abstraction $S_i = (X_i, U_i, \underset{i}{\longrightarrow})$ of subsystem $i \in \{1, \dots, m\}$:

Classical method, but with an **assume-guarantee obligation**:

## A/G Obligation ($K_i$)

*Unobserved states:* $x_{K_i} \in [\underline{x}_{K_i}, \overline{x}_{K_i}]$



# Synthesis

**Safety synthesis** in the partition of $[\underline{x}_{I_i}, \overline{x}_{I_i}]$:

- maximal safe set: $Z_i \subseteq X_i$
- safety controller: $C_i : Z_i \to 2^{U_i}$

**Performances optimization**:

- cost function $g_i(s_{I_i}, u_{J_i})$, with $g_a(s,u) \leq \sum_{i=1}^{m} g_i(s_{I_i}, u_{J_i})$
- deterministic controller: $C_i^* : Z_i \to U_i$

# Safety

Composition of safe sets and safety controllers:

- $Z_c = Z_1 \times \cdots \times Z_m$
- $\forall s \in Z_c,\ C_c(s) = C_1(s_{I_1}) \times \cdots \times C_m(s_{I_m})$

**Theorem**

*$C_c$ is a safety controller for $S$ in $Z_c$.*

# Safety

Composition of safe sets and safety controllers:

- $Z_c = Z_1 \times \cdots \times Z_m$
- $\forall s \in Z_c,\ C_c(s) = C_1(s_{I_1}) \times \cdots \times C_m(s_{I_m})$

**Theorem**

*$C_c$ is a safety controller for $S$ in $Z_c$.*

**Proposition (Safety comparison)**

*$Z_c \subseteq Z_a$.*

# Performance guarantees

- $\forall s \in Z_c,\ \ C_c^*(s) = (C_1^*(s_{I_1}), \dots, C_m^*(s_{I_m}))$
- Let $M_i = \max\limits_{s_i \in Z_i} \min\limits_{u_i \in C_i(s_i)} g_i(s_i, u_i)$

## Theorem

*Let $(x^0, u^0, x^1, u^1, \dots)$ be a trajectory of $S$ controlled with $C_c^*$. Let $s^0, s^1, \dots$ such that $x^k \in s^k$, for all $k \in \mathbb{N}$. Then,*

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k) \leq \sum_{i=1}^{m} J_i^0(s_{I_i}^0) + \frac{\lambda^{N+1}}{1-\lambda} \sum_{i=1}^{m} M_i$$

# Performance guarantees

- $\forall s \in Z_c,\ \ C_c^*(s) = (C_1^*(s_{I_1}), \dots, C_m^*(s_{I_m}))$
- Let $M_i = \max\limits_{s_i \in Z_i} \min\limits_{u_i \in C_i(s_i)} g_i(s_i, u_i)$

## Theorem

*Let $(x^0, u^0, x^1, u^1, \dots)$ be a trajectory of $S$ controlled with $C_c^*$.*
*Let $s^0, s^1, \dots$ such that $x^k \in s^k$, for all $k \in \mathbb{N}$. Then,*

$$\sum_{k=0}^{+\infty} \lambda^k g(x^k, u^k) \leq \sum_{i=1}^{m} J_i^0(s_{I_i}^0) + \frac{\lambda^{N+1}}{1-\lambda} \sum_{i=1}^{m} M_i$$

## Proposition (Guarantees comparison)

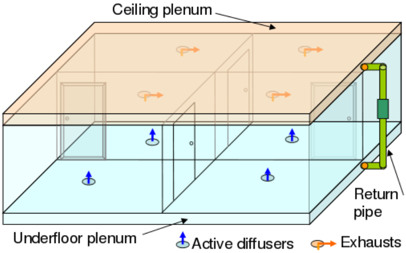
$$\forall s \in Z_c, \qquad J_a^0(s) + \frac{\lambda^{N+1}}{1-\lambda} M_a \leq \sum_{i=1}^{m} J_i^0(s_{I_i}) + \frac{\lambda^{N+1}}{1-\lambda} \sum_{i=1}^{m} M_i$$

# Complexity

- $n$: state space dimension
- $p$: control space dimension
- $\alpha_x \in \mathbb{N}$: number of symbols **per dimension** in the state partition
- $\alpha_u \in \mathbb{N}$: number of controls **per dimension** in the input discretization
- $|\cdot|$: cardinality of a set

| | Method | |
|---|---|---|
| | Centralized | Compositional |
| Complexity | $\alpha_x^n \alpha_u^p$ | $\sum_{i=1}^{m} \alpha_x^{\lvert I_i \rvert} \alpha_u^{\lvert J_i \rvert}$ |

# Complexity example




Application to temperature control

4-room building
Each room equipped with one fan

$n = 4$ states
$p = 4$ control inputs

| | Centralized $(4D)$ | Compositional $(4 * 1D)$ |
|---|---|---|
| Precisions of abstraction | $\alpha_x = 10$ | $\alpha_x = 20$ |
| | $\alpha_u = 4$ | $\alpha_u = 9$ |
| **Computation time** | $> 2$ days | 1.1 second |

# Conclusions and perspectives

The compositional approach provides:

- **Similar** safety and performance results to the centralized method, although **weaker** due to the loss of information
- The possibility of a significant **complexity reduction**
  $\Longrightarrow$ Tradeoff between the accuracy and the complexity reduction

# Conclusions and perspectives

The compositional approach provides:

- **Similar** safety and performance results to the centralized method, although **weaker** due to the loss of information
- The possibility of a significant **complexity reduction**
  $\Longrightarrow$ Tradeoff between the accuracy and the complexity reduction

**Perspectives**

- Extension of the symbolic compositional approach
  - to non-cooperative systems
  - to other specifications than safety
- Adaptive symbolic control framework:
  - measure the disturbance; tight estimation of its future bounds
  - synthesize compositional controller on the more accurate abstraction
  - apply controller until the next measure

  $\Longrightarrow$ increased precision and robustness, local cooperativeness

# Safety control with performance guarantees of cooperative systems using compositional abstractions

**Pierre-Jean Meyer** Antoine Girard Emmanuel Witrant

Université Grenoble-Alpes

ADHS'15, October $16^{th}$ 2015

# Symbolic abstraction

State partition $\mathcal{P}$ of $[\underline{x}, \overline{x}] \subseteq \mathbb{R}^n$ into $\alpha_x$ identical intervals per dimension

$$\mathcal{P} = \left\{ \left[ \underline{s}, \underline{s} + \frac{\overline{x} - \underline{x}}{\alpha_x} \right] \mid \underline{s} \in \left( \underline{x} + \frac{\overline{x} - \underline{x}}{\alpha_x} * \mathbb{Z}^n \right) \cap [\underline{x}, \overline{x}] \right\}$$

Input discretization $U_a$ of $[\underline{u}, \overline{u}] \subseteq \mathbb{R}^p$ into $\alpha_u \geq 2$ values per dimension

$$U_a = \left( \underline{u} + \frac{\overline{u} - \underline{u}}{\alpha_u - 1} * \mathbb{Z}^p \right) \cap [\underline{u}, \overline{u}]$$

# Sampling period

Guidelines for the **viability kernel**[1] (maximal invariant set):

$$2L\tau^2 \sup_{x\in[\underline{x},\overline{x}]} \|f(x,\overline{u},\overline{w})\| \geq \frac{\|\overline{x}-\underline{x}\|}{\alpha_x}$$

- $\tau$: sampling period
- $\frac{\|\overline{x}-\underline{x}\|}{\alpha_x}$: step of the state partition
- $L$: Lipschitz constant
- $\sup_{x\in[\underline{x},\overline{x}]} \|f(x,\overline{u},\overline{w})\|$: supremum of the vector field

[1] P. Saint-Pierre. Approximation of the viability kernel. *Applied Mathematics and Optimization*, 29(2):187–209, 1994.

## Complexity

- $n$: state space dimension
- $p$: control space dimension
- $\alpha_x \in \mathbb{N}$: number of symbols **per dimension** in the state partition
- $\alpha_u \in \mathbb{N}$: number of controls **per dimension** in the input discretization
- $|\cdot|$: cardinality of a set

| | Method | |
|---|---|---|
| | Centralized | Compositional |
| Abstraction (successors computed) | $2\alpha_x^n\alpha_u^p$ | $\sum_{i=1}^{m} 2\alpha_x^{\|I_i\|}\alpha_u^{\|J_i\|}$ |
| Dynamic programming (max iterations) | $N\alpha_x^{2n}\alpha_u^p$ | $\sum_{i=1}^{m} N\alpha_x^{2\|I_i\|}\alpha_u^{\|J_i\|}$ |