Formal Methods for the Control of Large-scale Networked Nonlinear Systems with Logic Specifications

Basilica di Santa Maria di Collemaggio, 1287, L'Aquila

Lecture L8
Symbolic models and control for nonlinear systems affected by disturbances and applications

Speaker: Alessandro Borri

What's new?

In this lecture we will consider nonlinear control systems affected by disturbances modeling external unknown inputs and model uncertaintes

Tools:

- Alternating approximate bisimulation
- Functional analysis

Lecture mostly based on:

[Borri et al., IJC12] Borri, A., Pola, G., Di Benedetto, M.D., Symbolic models for nonlinear control systems affected by disturbances, International Journal of Control, 85(10):1422-1432, September 2012

Introduction

- Symbolic models for nonlinear control systems affected by disturbances were first proposed in [Pola & Tabuada, SIAM 2009], but they are difficult to be effectively constructed because they rely upon the knowledge of reachable sets.
- In this lecture, we overcome these difficulties by leveraging results on spline analysis and propose symbolic models that can be effectively constructed.
- Based on these symbolic models, it is possible to design symbolic controllers that are robust with respect to the non-determinism of the model.
- We illustrate robust symbolic control techniques in on vehicle platooning, adaptive cruise control, robot motion planning and control of traffic flow

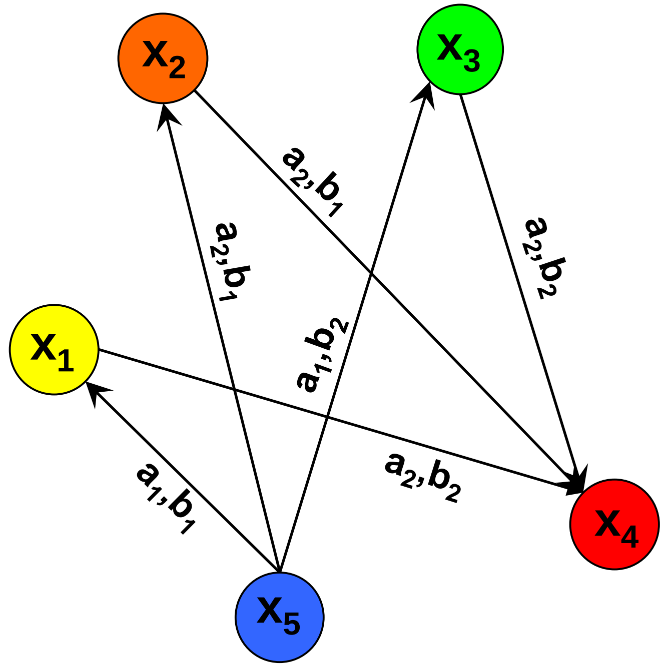
A unified framework for continuous and discrete systems

Definition A **transition system** is a tuple:

$$T = (X, X_0, L, \longrightarrow, X_m, Y, H),$$

consisting of:

- a set of states X
- a set of initial states $X_0 \subseteq X$
- a set of inputs $L = A \times B$, where
  - A is the set of control inputs
  - B is the set of disturbance inputs
- a transition relation $\longrightarrow \subseteq X \times L \times X$
- a set of marked states $X_m \subseteq X$
- a set of outputs Y
- an output function $H: X \rightarrow Y$



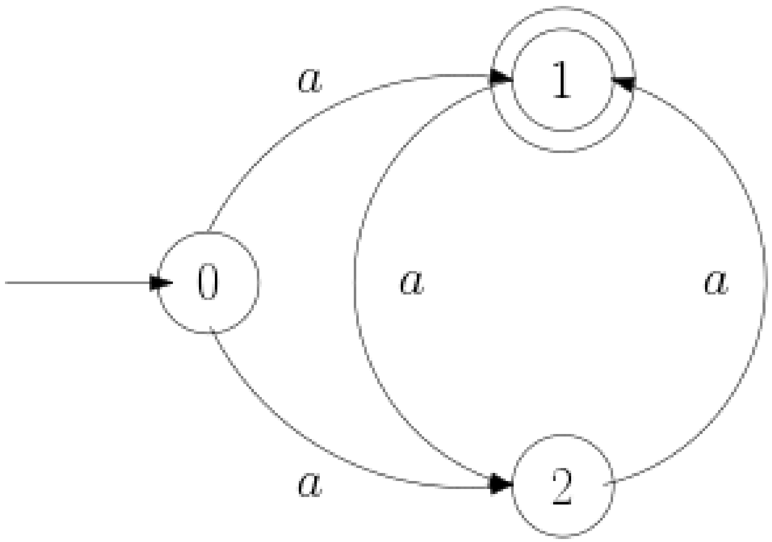
T is said countable if X and L are countable sets

T is said symbolic/finite if X and L are finite sets

T is metric if the output set is equipped with a metric

We will follow standard practice and denote $(x, (a,b), x') \in \longrightarrow$ by $x \xrightarrow{(a,b)} x'$

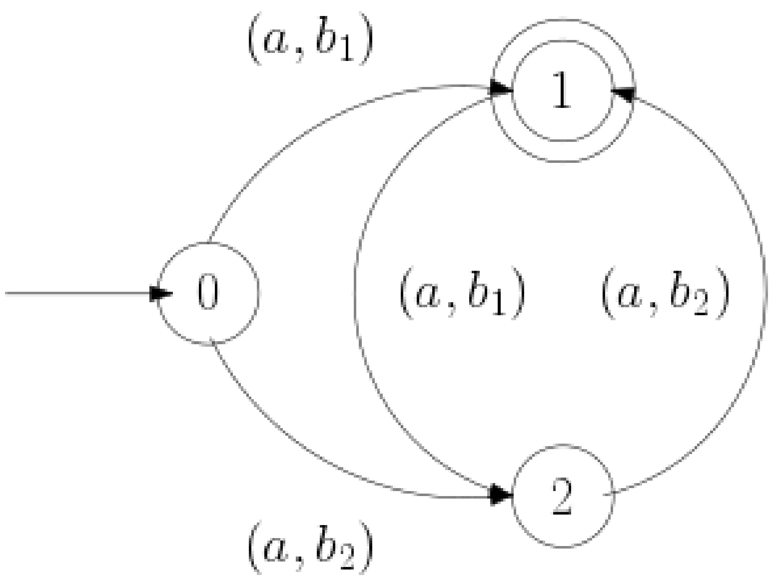
Two equivalent representations for transition systems



$T' = (X, X_0, A, \longrightarrow, X_m, Y, H)$

T' is non-deterministic

The disturbance does not appear explicitly



$T = (X, X_0, A \times B, \longrightarrow, X_m, Y, H)$

T is deterministic

A is the set of control inputs

B is the set of disturbance inputs

In the following, we will use the notation of T because we will compute explicitly an approximation of the set of continuous disturbances

A unified framework for continuous and discrete systems

A **nonlinear control system Σ**

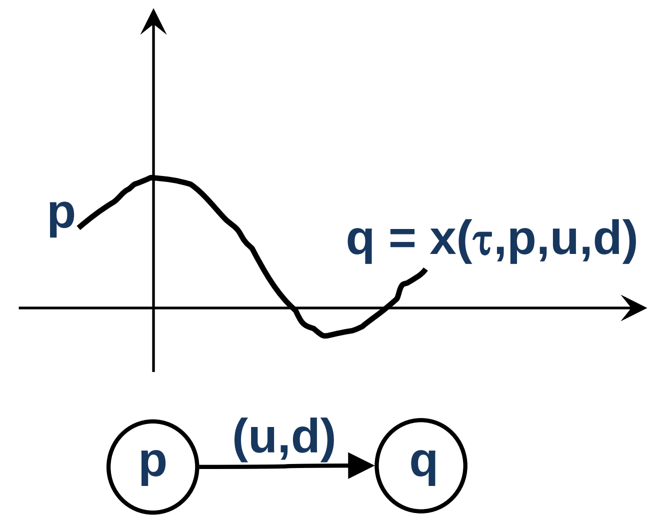
$$dx/dt = f(x,u,d),\ x \in X \subseteq R^n,\ u \in U \subseteq R^m,\ d \in D \subseteq R^l$$

can be modeled by the transition system

$$T(\Sigma) = (X, X_0, \mathcal{U} \times \mathcal{D}, \longrightarrow, X_m, Y, H),$$

where:

- $X_0 = X$
- $\mathcal{U}$ is the collection of control signals $u : R \to U$
- $\mathcal{D}$ is the collection of disturbance signals $u : R \to D$
- $p \xrightarrow{(u,d)} q$, if $x(\tau,p,u,d) = q$ for some $\tau \geq 0$
- $X_m = X$
- $Y = X$
- H is the identity function



$T(\Sigma)$ captures the information contained in Σ but it is not a symbolic model because X, U and D are infinite sets!

Exact equivalence notions

[Milner & Park, 1981] :

Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, a relation

$$R \subseteq X_1 \times X_2$$

is a *simulation relation* from T_1 to T_2 if

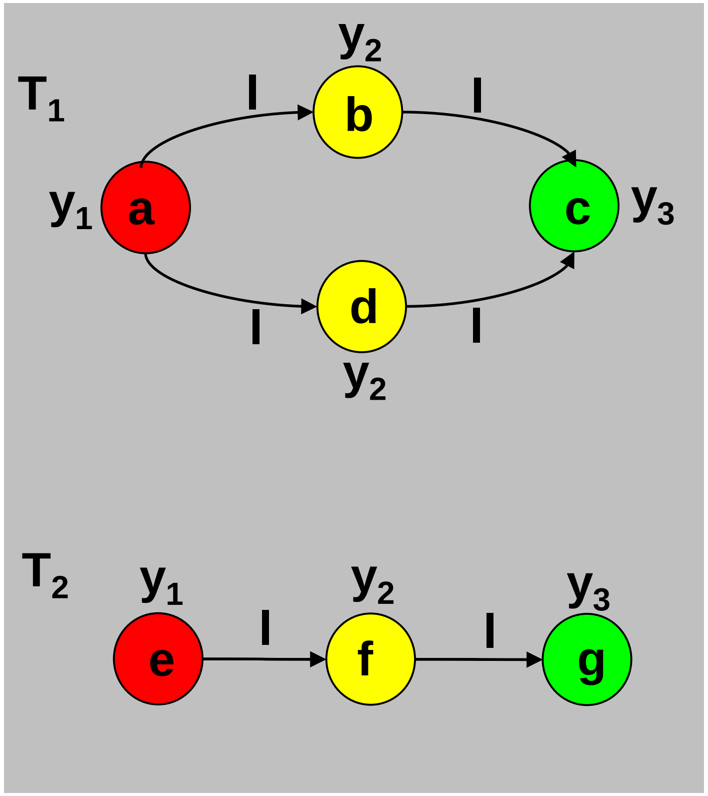
- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R,\ H_1(x_1) = H_2(x_2)$
- $\forall (x_1, x_2) \in R,\ \forall a_1\ \forall b_1\ \exists a_2\ \exists b_2$ such that

$$x_1 \xrightarrow{(a_1,b_1)}_1 p_1 \text{ and } x_2 \xrightarrow{(a_2,b_2)}_2 p_2 \text{ and } (p_1, p_2) \in R$$

R is a bisimulation relation between T_1 and T_2 if

- R is a simulation relation from T_1 to T_2
- R^{-1} is a simulation relation from T_2 to T_1

Transition systems T_1 and T_2 are bisimilar if there exists a *bisimulation relation* between T_1 and T_2



Exact equivalence notions

[Milner & Park, 1981] :

Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, a relation

$$R \subseteq X_1 \times X_2$$

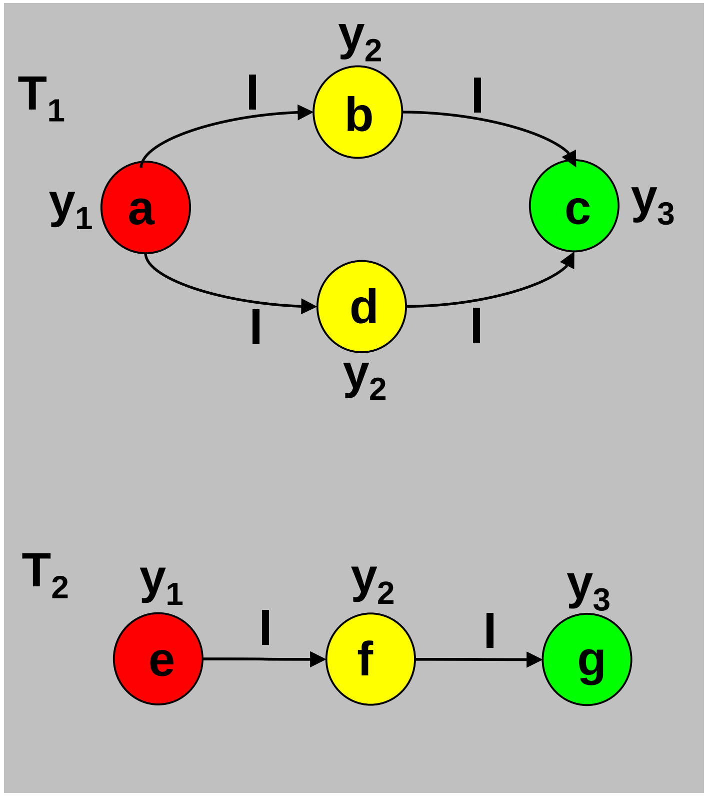
is a *simulation relation* from T_1 to T_2 if

- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R$, $H_1(x_1) = H_2(x_2)$
- $\forall (x_1, x_2) \in R$, $\forall a_1\, \forall b_1\, \exists a_2\, \exists b_2$ such that

  $x_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $x_2 \xrightarrow{(a_2,b_2)}_2 p_2$ and $(p_1, p_2) \in R$

R is a bisimulation relation between T_1 and T_2 if

- R is a simulation relation from T_1 to T_2
- R^{-1} is a simulation relation from T_2 to T_1



Transition systems T_1 and T_2 are bisimilar if there exists a *bisimulation relation* between T_1 and T_2

Approximate equivalence notions

[Girard & Pappas, 2007] :

Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, and an accuracy $\varepsilon > 0$, a relation

$$R \subseteq X_1 \times X_2$$

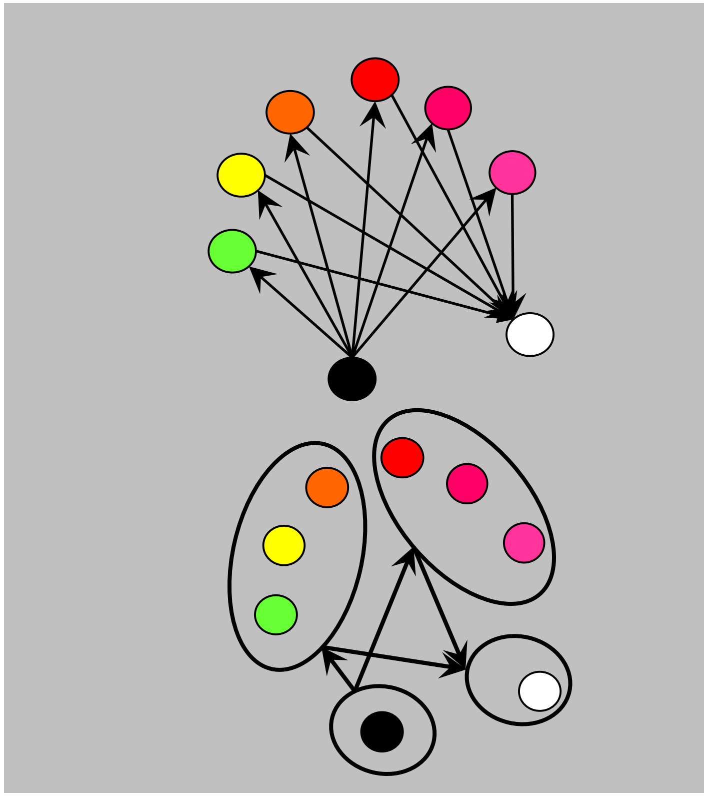
is an ε-*simulation relation* from T_1 to T_2 if

- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R$, $d(H_1(q_1), H_2(q_2)) \le \varepsilon$
- $\forall (x_1, x_2) \in R$, $\forall a_1\, \forall b_1\, \exists a_2\, \exists b_2$ such that

  $x_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $x_2 \xrightarrow{(a_2,b_2)}_2 p_2$ and $(p_1, p_2) \in R$

R is an ε-bisimulation relation between T_1 and T_2 if

- R is an ε-simulation relation from T_1 to T_2
- R^{-1} is an ε-simulation relation from T_2 to T_1



Transition systems T_1 and T_2 are **ε-bisimilar** if there exists an ***ε-bisimulation relation*** between T_1 and T_2

Approximate equivalence notions

[Girard & Pappas, 2007] :

Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, and an accuracy $\varepsilon > 0$, a relation

$$R \subseteq X_1 \times X_2$$

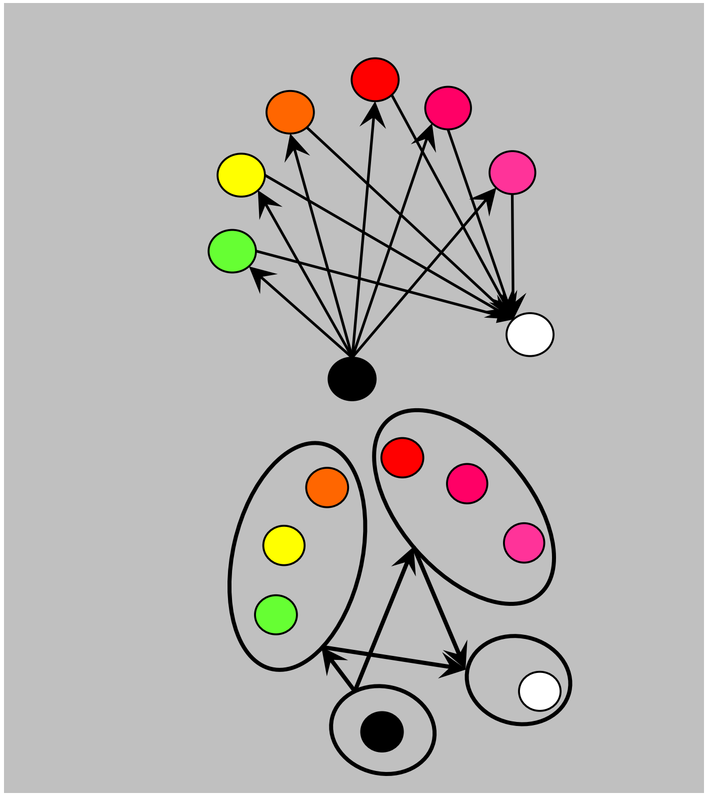
is an ε-*simulation relation* from T_1 to T_2 if

- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R$, $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$
- $\forall (x_1, x_2) \in R$, $\forall a_1\, \forall b_1\, \exists a_2\, \exists b_2$ such that

  $x_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $x_2 \xrightarrow{(a_2,b_2)}_2 p_2$ and $(p_1, p_2) \in R$

R is an ε-bisimulation relation between T_1 and T_2 if

- R is an ε-simulation relation from T_1 to T_2
- R^{-1} is an ε-simulation relation from T_2 to T_1



Drawback: This notion fails to distinguish the different role played by control and disturbance inputs!

Approximate equivalence notions

[Pola & Tabuada, 2009] :

Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, and an accuracy $\varepsilon > 0$, a relation

$$R \subseteq X_1 \times X_2$$

is an AεA-*simulation relation* from T_1 to T_2 if

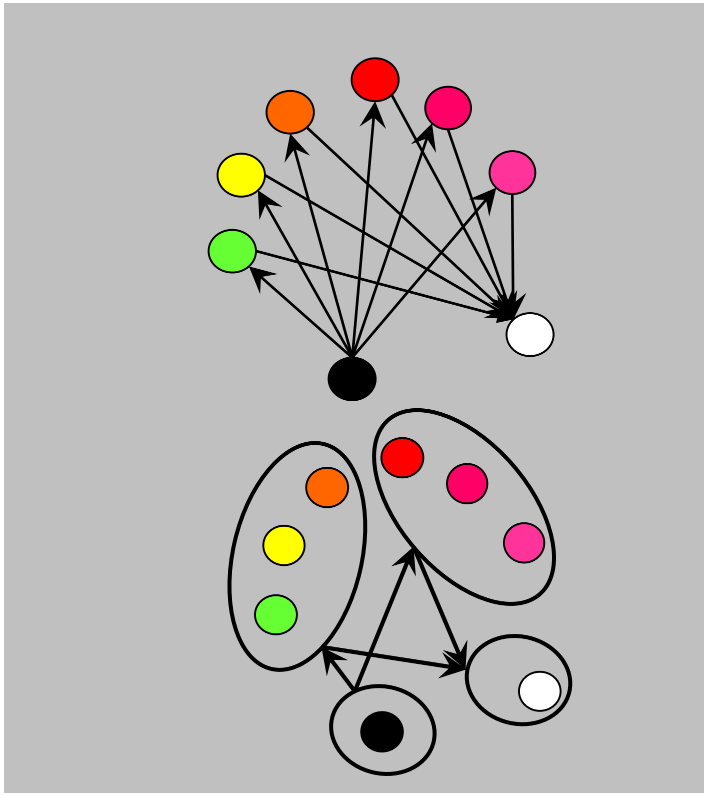
- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R,\ d(H_1(q_1), H_2(q_2)) \leq \varepsilon$
- $\forall (x_1, x_2) \in R$, $\forall a_1 \exists a_2 \forall b_2 \exists b_1$ such that

  $x_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $x_2 \xrightarrow{(a_2,b_2)}_2 p_2$ and $(p_1, p_2) \in R$

R is an AεA-bisimulation relation between T_1 and T_2 if

- R is an AεA-simulation relation from T_1 to T_2
- R^{-1} is an AεA-simulation relation from T_2 to T_1

Transition systems T_1 and T_2 are AεA-bisimilar if there exists an AεA-*bisimulation relation* between T_1 and T_2



Approximate equivalence notions

[Pola & Tabuada, 2009] :

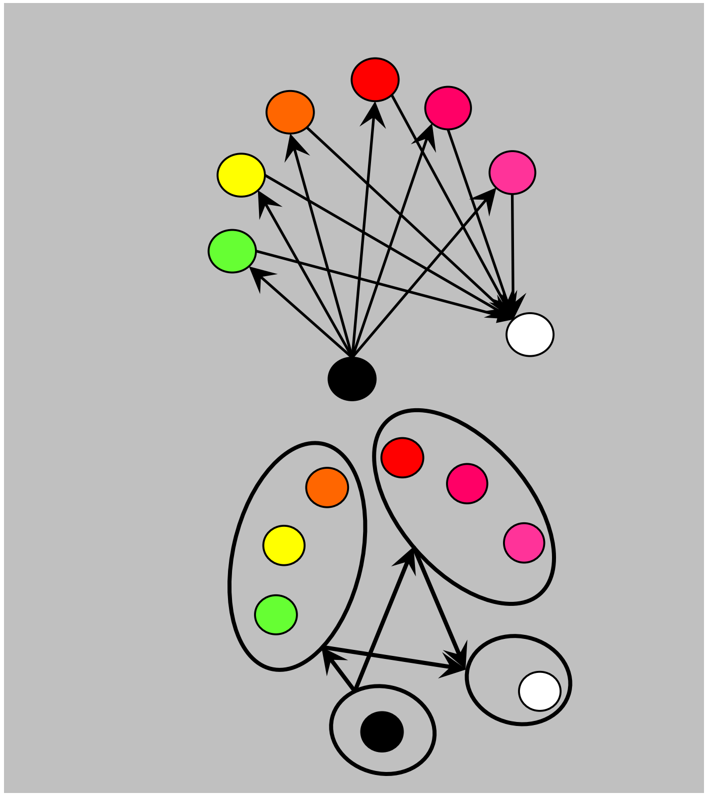
Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, and an accuracy $\varepsilon > 0$, a relation

$$R \subseteq X_1 \times X_2$$

is an $A\varepsilon A$-*simulation relation* from T_1 to T_2 if

- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R$, $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$
- $\forall (x_1, x_2) \in R$, $\forall a_1\, \exists a_2\, \forall b_2\, \exists b_1$ such that

  $x_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $x_2 \xrightarrow{(a_2,b_2)}_2 p_2$ and $(p_1, p_2) \in R$



R is an $A\varepsilon A$-bisimulation relation between T_1 and T_2 if

- R is an $A\varepsilon A$-simulation relation from T_1 to T_2
- R^{-1} is an $A\varepsilon A$-simulation relation from T_2 to T_1

Different role of control and disturbance labels:

- Approximate bisimulation $\forall a_1\, \forall b_1\, \exists a_2\, \exists b_2$

- *Alternating* approximate bisimulation $\forall a_1\, \exists a_2\, \forall b_2\, \exists b_1$

Approximate equivalence notions

[Pola & Tabuada, 2009] :

Given $T_1 = (X_1, X_{01}, A_1 \times B_1, \longrightarrow_1, X_{m1}, Y_1, H_1)$ and $T_2 = (X_2, X_{02}, A_2 \times B_2, \longrightarrow_2, X_{m2}, Y_2, H_2)$ with $Y_1 = Y_2$, and an accuracy $\varepsilon > 0$, a relation

$$R \subseteq X_1 \times X_2$$

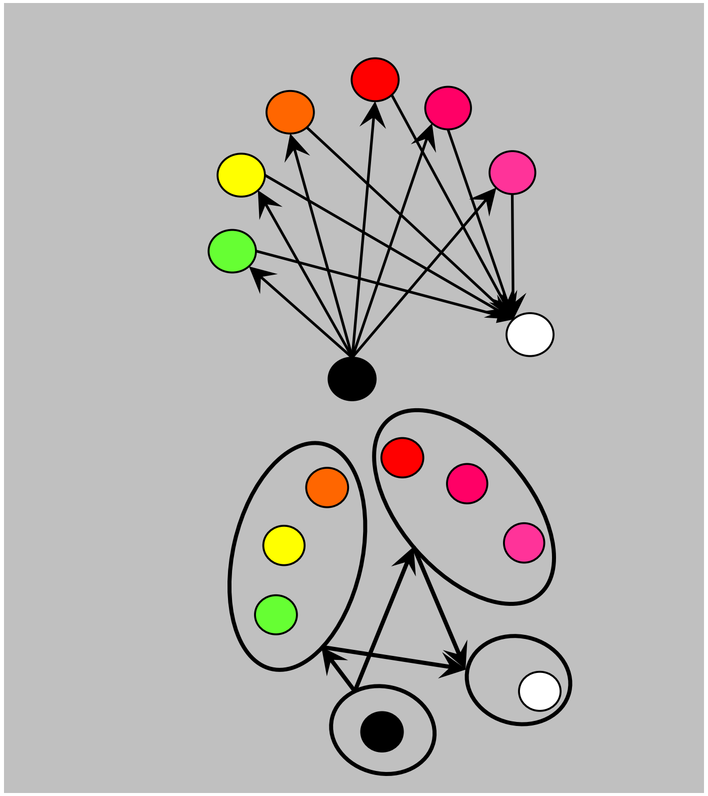
is an AεA-*simulation relation* from T_1 to T_2 if

- $\forall x_1 \in X_{01}, \exists\, x_2 \in X_{02}$ s.t. $(x_1, x_2) \in R$
- $\forall x_1 \in X_{m1}, \exists\, x_2 \in X_{m2}$ s.t. $(x_1, x_2) \in R$
- $\forall (x_1, x_2) \in R,\ d(H_1(q_1), H_2(q_2)) \le \varepsilon$
- $\forall (x_1, x_2) \in R,\ \forall a_1\, \exists a_2\, \forall b_2\, \exists b_1$ such that

  $x_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $x_2 \xrightarrow{(a_2,b_2)}_2 p_2$ and $(p_1, p_2) \in R$

R is an AεA-bisimulation relation between T_1 and T_2 if

- R is an AεA-simulation relation from T_1 to T_2
- R^{-1} is an AεA-simulation relation from T_2 to T_1



From [Alur et al., 1998] symbolic control strategies designed for T_1 *can be appropriately transferred to* T_2 *if the systems are* AεA-bisimilar

Goal: ***construct AεA-bisimilar symbolic models***

Spline approximation of the disturbance space

Assumptions

1. D is radial, i.e. $\rho D \subseteq D$ for any $\rho \in [0,1]$
2. The disturbance functions are bounded ($|d| \leq M$) and Lipschitz continuous with Lipschitz constant κ_d.

Consider the set $\mathcal{D}_\tau$ of the disturbance signals defined on the time interval $[0, \tau]$ for some $\tau > 0$.

Definition

A map $A: R^+ \rightarrow 2^{C^0([0,\tau];D)}$ is a finite inner approximation of $\mathcal{D}_\tau$ if for any desired precision $\lambda > 0$

- $A(\lambda)$ is a finite set
- $A(\lambda) \subseteq \mathcal{D}_\tau$
- $\forall y \in \mathcal{D}_\tau \;\; \exists z \in A(\lambda)$ s.t. $|y - z| \leq \lambda$

Spline approximation of the disturbance space

Approximation scheme

For a given $\lambda > 0$, we define the set $A_{\mathcal{D}_\tau}(\lambda)$ of all functions

$$z(t) := \sum_{i=0}^{N+1} z_i s_i(t), \quad t \in [0,\tau]$$

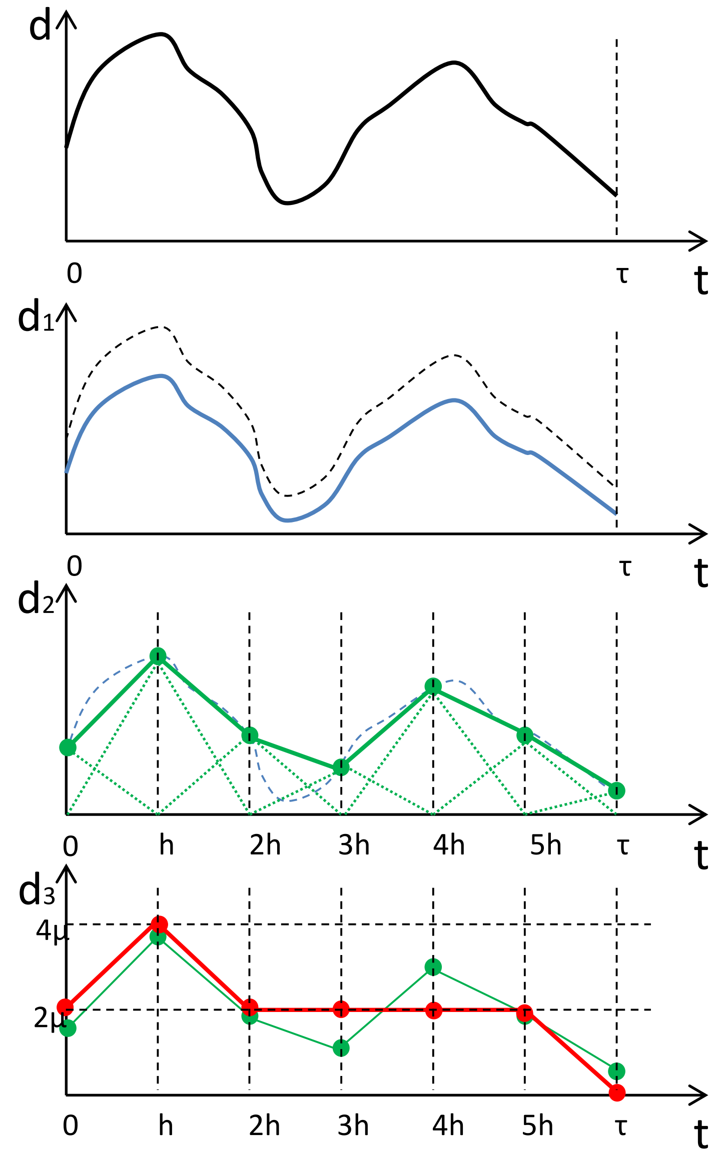
satisfying the following conditions:

- $z_i \in 2\mu\mathbb{Z}^l \cap \rho D$, for $i = 0, \dots, N+1$
- $\| z_{i+1} - z_i \| \leq \kappa\tau/(N+1)$, for $i = 0, \dots, N$

Theorem: The map $A_{\mathcal{D}_\tau}$ is a finite inner approximation of $\mathcal{D}_\tau$

Approximation in 3 steps:

1. $d_1 = \rho d, 0 < \rho < 1$.
2. d_2 is a piecewise-linear function with N+2 samples
3. d_3 is a piecewise-linear function with N+2 ***quantized*** samples



Spline approximation of the disturbance space

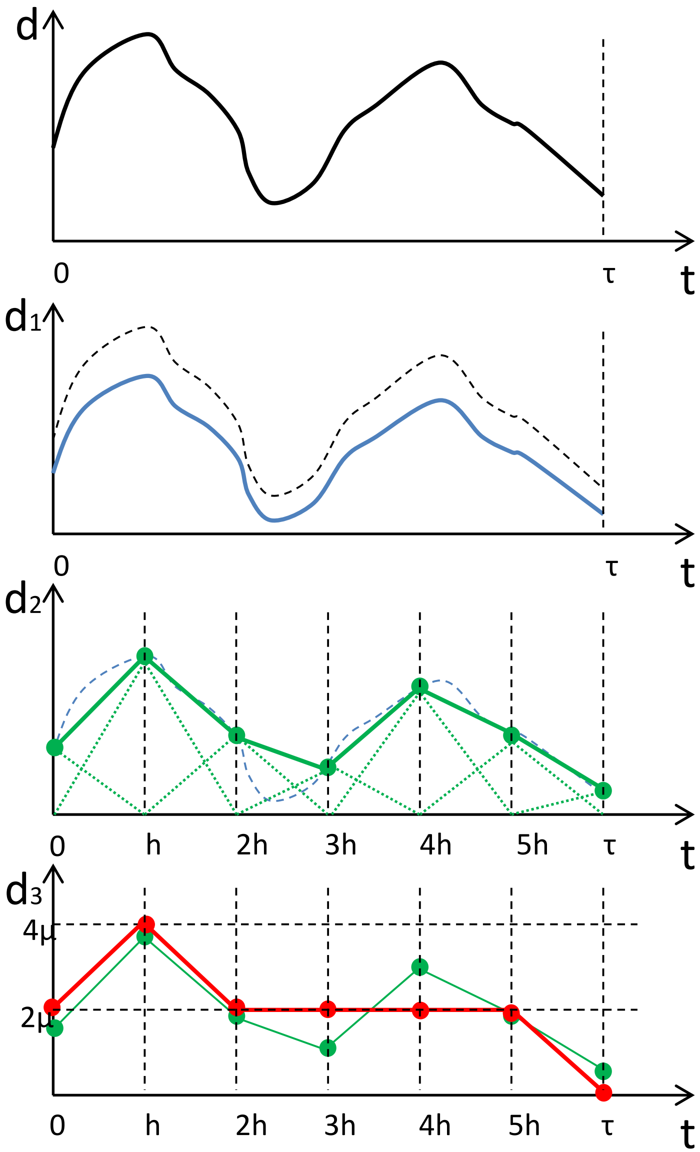
Approximation error:

$$\Lambda\,(\kappa,\tau,M,N,\mu) = (1-\rho)M + (1+\rho)\kappa h + \mu$$

where $\rho = 1 - max\left\{\frac{\mu}{M}, \frac{2\mu(N+1)}{\kappa\tau}\right\}$ and

- κ is the Lipschitz constant
- h = τ /(N+1) is the approximation step
- M is the infinity-norm bound
- N is the number of samples
- μ is the space quantization

Lemma: Given λ, κ, τ, M, there always exist N and μ s.t. $\Lambda\,(\kappa,\tau,M,N,\mu) \leq \lambda$



Incremental Input-to-State-Stability

Definition

Given a nonlinear control system Σ, a smooth function

$$V: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_0^+$$

is said to be a δ-ISS Lyapunov function for Σ if there exist $\lambda \in \mathbb{R}^+$ and K_∞ functions $\alpha_1, \alpha_2, \sigma_u, \sigma_d$ such that, for any $x_1, x_2 \in \mathbb{R}^n$, any $u_1, u_2 \in U$, and any $d_1, d_2 \in D$

1) $\alpha_1(|x_1 - x_2|) \leq V(x_1, x_2) \leq \alpha_2(|x_1 - x_2|)$

2) $\frac{\partial V}{\partial x_1} f(x_1, u_1, d_1) + \frac{\partial V}{\partial x_2} f(x_2, u_2, d_2) \leq -\lambda V(x_1, x_2) + \sigma_u(|u_1 - u_2|) + \sigma_d(|d_1 - d_2|)$

Theorem

A nonlinear control system Σ is δ-ISS if and only if it admits a δ-ISS Lyapunov function

Remark

Backstepping techniques for incremental stabilization are reported in [Zamani & Tabuada, IEEE-TAC 2011]

Time discretization

Consider a nonlinear control system Σ expressed in the form of transition system

$$T(\Sigma) = (X, X_0, \mathcal{U} \times \mathcal{D}, \longrightarrow, X_m, Y, H),$$

and given some $\tau > 0$, define the transition system

$$T_\tau(\Sigma) = (X, X_0, \mathcal{U}_\tau \times \mathcal{D}_\tau, \longrightarrow_\tau, X_m, Y, H),$$

where:

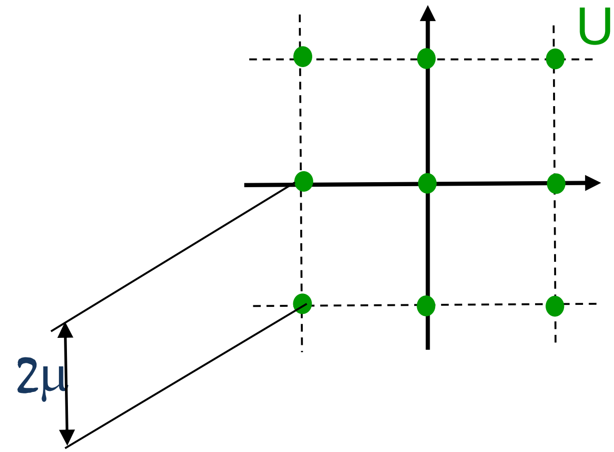
- $\mathcal{U}_\tau \subseteq \mathcal{U}$ is the collection of constant control input functions $u : [0,\tau] \rightarrow U$
- $\mathcal{D}_\tau \subseteq \mathcal{D}$ is the collection of disturbance input functions $d : [0,\tau] \rightarrow D$
- $p \xrightarrow{(u,d)}_\tau q$ if $x(\tau,p,u,d) = q$

$T_\tau(\Sigma)$ can be regarded as the time-discretization of $T(\Sigma)$.
$T_\tau(\Sigma)$ is metric when we regard $Y=X$ as being equipped with the metric

$$\mathrm{d}_Y(p,q) = |p - q|$$

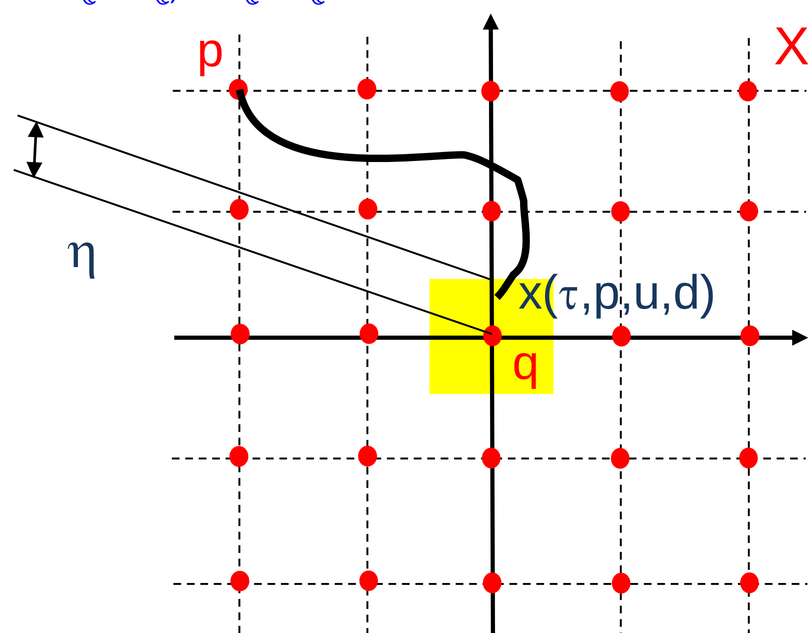
Construction of symbolic models

Consider the following vector $\mathbb{Q} = (\tau, \eta, \mu_u, N_d, \mu_d)$
of quantization parameters, where:



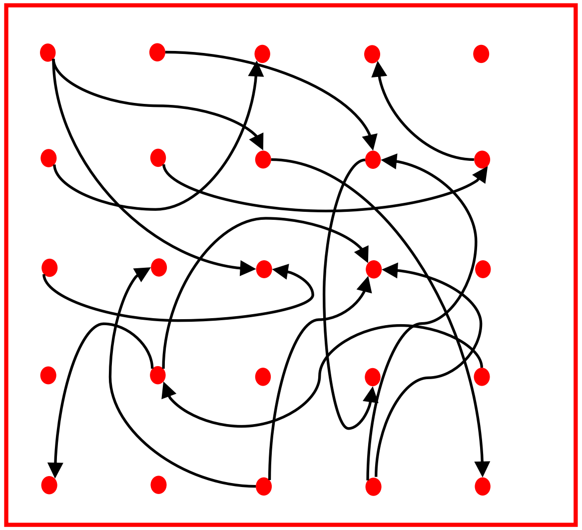
- τ sampling time
- η state space quantization
- μ_u control input space quantization
- N_d number of splines
- μ_d disturbance input space quantization

and define the transition system $T_{\mathbb{Q}}(\Sigma) = (X_{\mathbb{Q}}, X_{\mathbb{Q},0}, L_{\mathbb{Q}}, \longrightarrow_{\mathbb{Q}}, X_{\mathbb{Q},m}, Y_{\mathbb{Q}}, H_{\mathbb{Q}})$,
where:



- $X_{\mathbb{Q}} = 2\eta\mathbb{Z}^n \cap X$
- $X_{\mathbb{Q},0} = X_{\mathbb{Q}}$
- $L_{\mathbb{Q}} = (2\mu_u\mathbb{Z}^m \cap U) \times A_{\mathcal{D}_\tau}(\Lambda(\kappa, \tau, M, N_d, \mu_d))$
- $p \xrightarrow{(u,d)}_{\mathbb{Q}} q$, if $|x(\tau,p,u,d) - q|_\infty \leq \eta$
- $X_{\mathbb{Q},m} = X_{\mathbb{Q}}$
- $Y_{\mathbb{Q}} = X$
- $H_{\mathbb{Q}}$ is the identity function

Construction of symbolic models



Consider the following vector $\mathbb{Q} = (\tau, \eta, \mu_u, N_d, \mu_d)$ of quantization parameters, where:

- τ sampling time
- η state space quantization
- μ_u control input space quantization
- N_d number of splines
- μ_d disturbance input space quantization

and define the transition system $T_{\mathbb{Q}}(\Sigma) = (X_{\mathbb{Q}}, X_{\mathbb{Q},0}, L_{\mathbb{Q}}, \longrightarrow_{\mathbb{Q}}, X_{\mathbb{Q},m}, Y_{\mathbb{Q}}, H_{\mathbb{Q}})$, where:

- $X_{\mathbb{Q}} = 2\eta\mathbb{Z}^n \cap X$
- $X_{\mathbb{Q},0} = X_{\mathbb{Q}}$
- $L_{\mathbb{Q}} = (2\mu_u\mathbb{Z}^m \cap U) \times A_{\mathcal{D}_\tau}(\Lambda(\kappa, \tau, M, N_d, \mu_d))$
- $p \xrightarrow{(u,d)}_{\mathbb{Q}} q$, if $|x(\tau,p,u,d) - q|_\infty \leq \eta$
- $X_{\mathbb{Q},m} = X_{\mathbb{Q}}$
- $Y_{\mathbb{Q}} = X$
- $H_{\mathbb{Q}}$ is the identity function

Remark: $L_{\mathbb{Q}}$ can be effectively computed, hence the symbolic transition system $T_{\mathbb{Q}}(\Sigma)$ can be effectively constructed!

Construction of symbolic models

Theorem

Consider a nonlinear control system Σ and suppose that:

1. There exists a δ-ISS Lyapunov function for Σ, hence there exists $\lambda \in \mathbb{R}^+$ s.t. for any $x_1, x_2 \in \mathbb{R}^n$, any $u_1, u_2 \in U$, and any $d_1, d_2 \in D$

$$\frac{\partial V}{\partial x_1} f(x_1, u_1, d_1) + \frac{\partial V}{\partial x_2} f(x_2, u_2, d_2) \leq -\lambda V(x_1, x_2) + \sigma_u(|u_1 - u_2|) + \sigma_d(|d_1 - d_2|).$$

2. There exists a K_∞ function γ such that $V(x, x') \leq V(x, x'') + \gamma(|x' - x''|)$ for every $x, x', x'' \in X$.

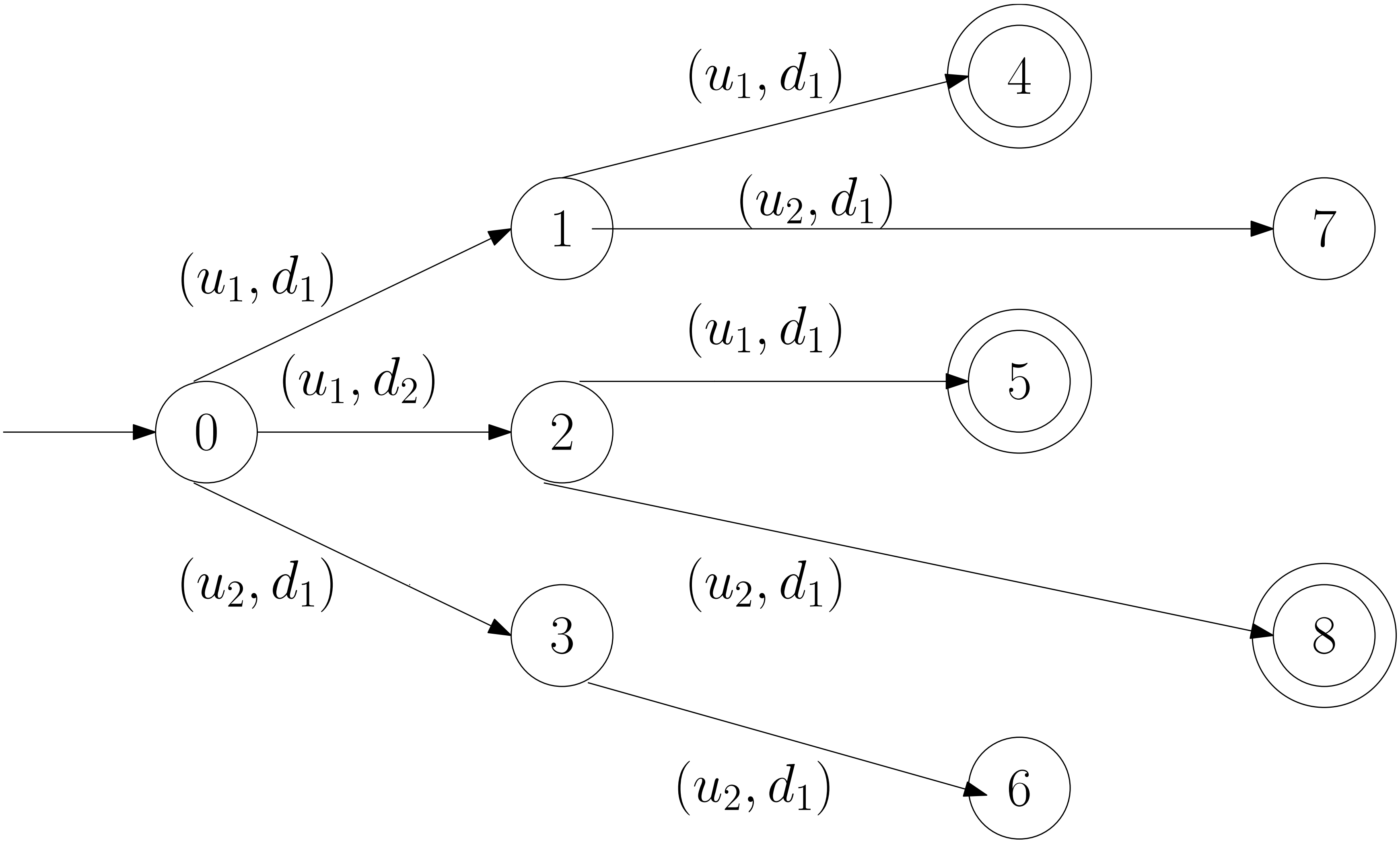
3. The disturbance set D is radial and the disturbance functions are bounded ($|d|_\infty \leq M$) and Lipschitz continuous with uniform Lipschitz constant κ.

Then for any desired precision $\varepsilon > 0$ and any quantization parameters in $\mathbb{Q}$ s.t.

$$\frac{max\{\sigma_u(\mu_u), \sigma_d(\Lambda(\kappa, \tau, M, N_d, \mu_d))\}}{\lambda} + \frac{\gamma(\eta)}{1 - e^{-\lambda\tau}} \leq \alpha_1(\varepsilon)$$

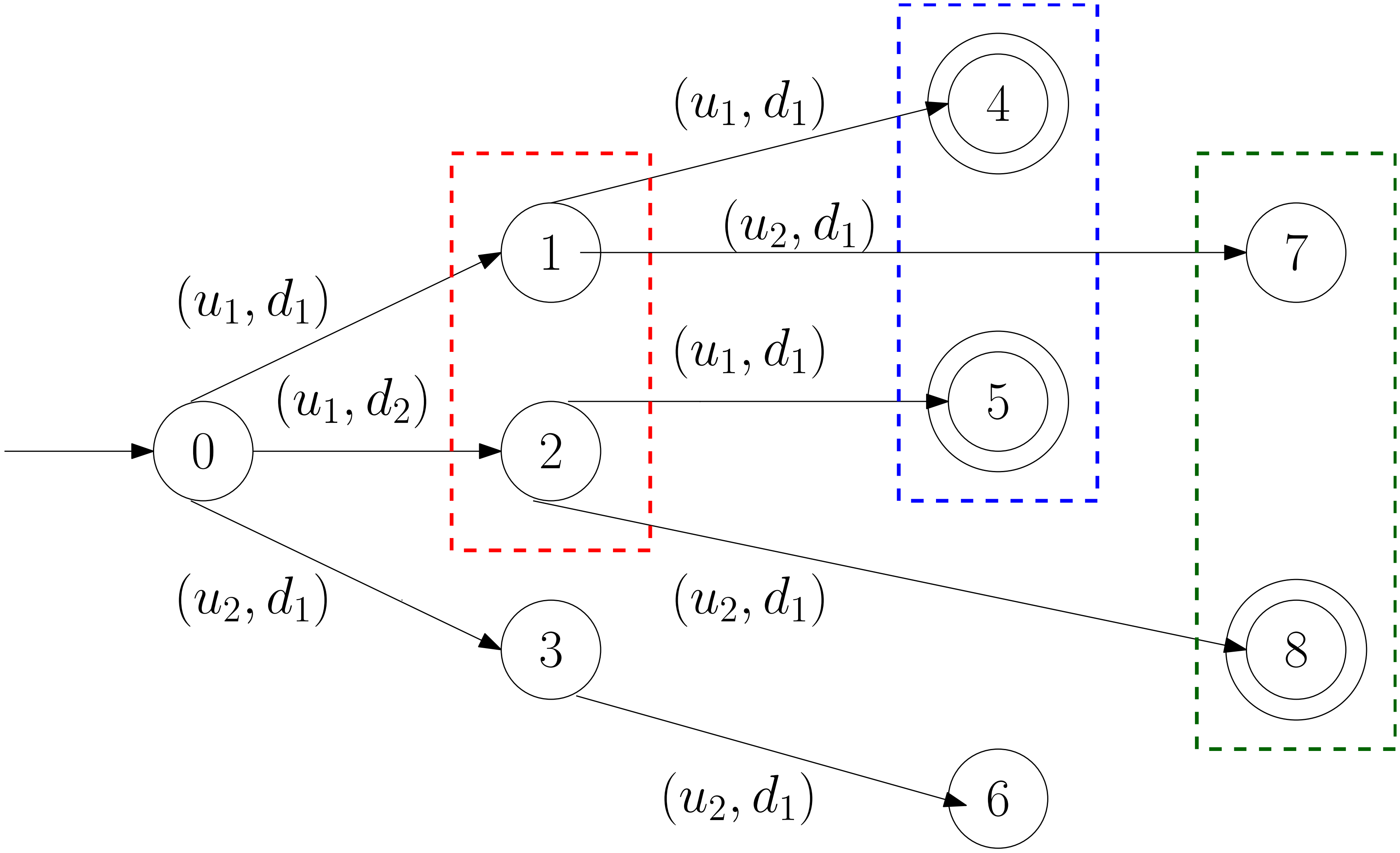
transition systems $T_\tau(\Sigma)$ and $T_{\mathbb{Q}}(\Sigma)$ are *AεA-bisimilar*

Robust control design – a simple example



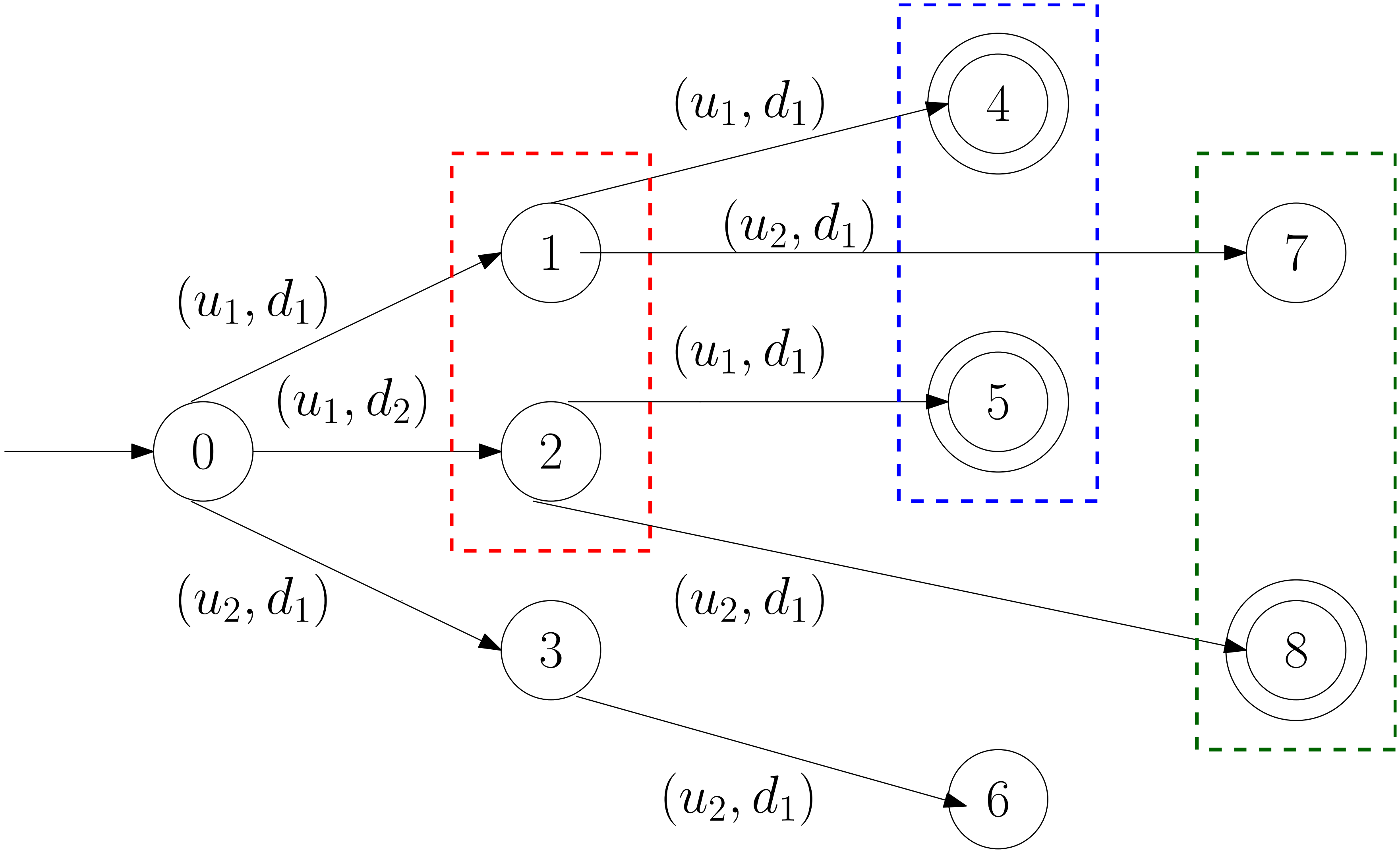
In this transition system, the input u_1 given at initial time can lead the system from the initial state 0 either to state 1 or to state 2.

Robust control design – a simple example



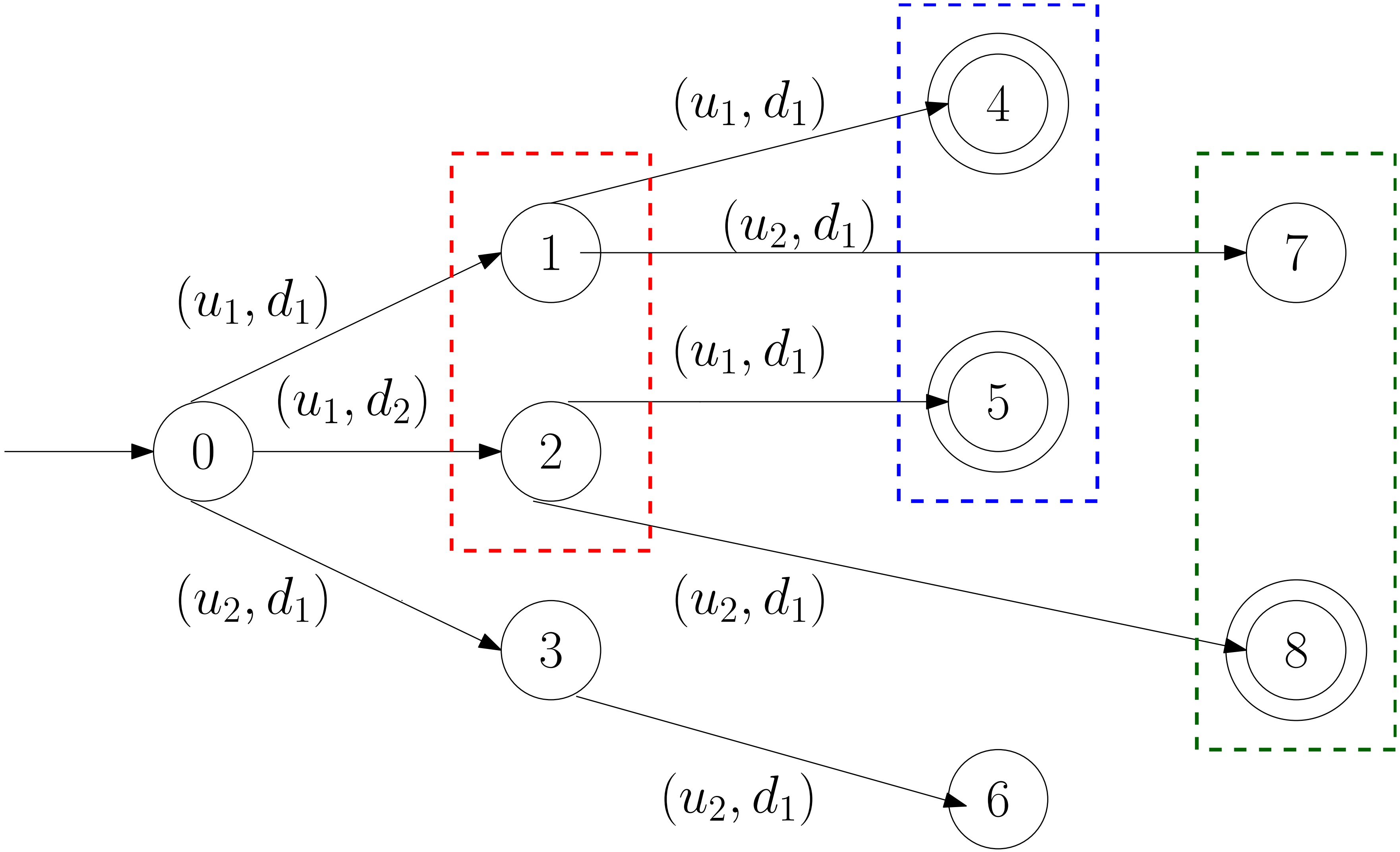
In absence of a state measurement, you cannot distinguish state 1 from 2 at step 1.
Further, you cannot distinguish state 4 from 5 and state 7 from 8 at step 2.

Robust control design – a simple example



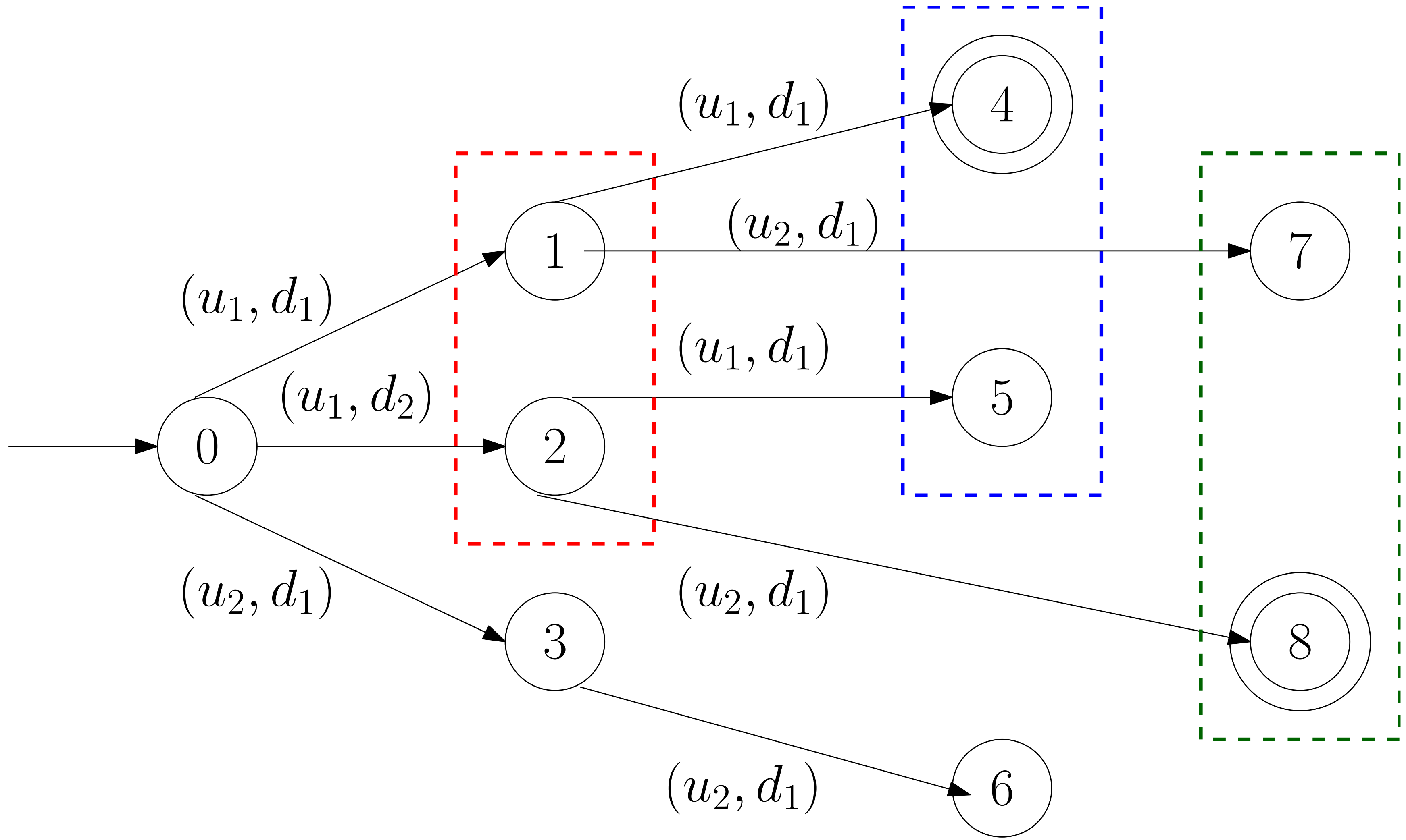
The dashed boxes are called **information sets**: open-loop control strategies cannot distinguish states within the red, blue and green boxes.

Robust control design – a simple example



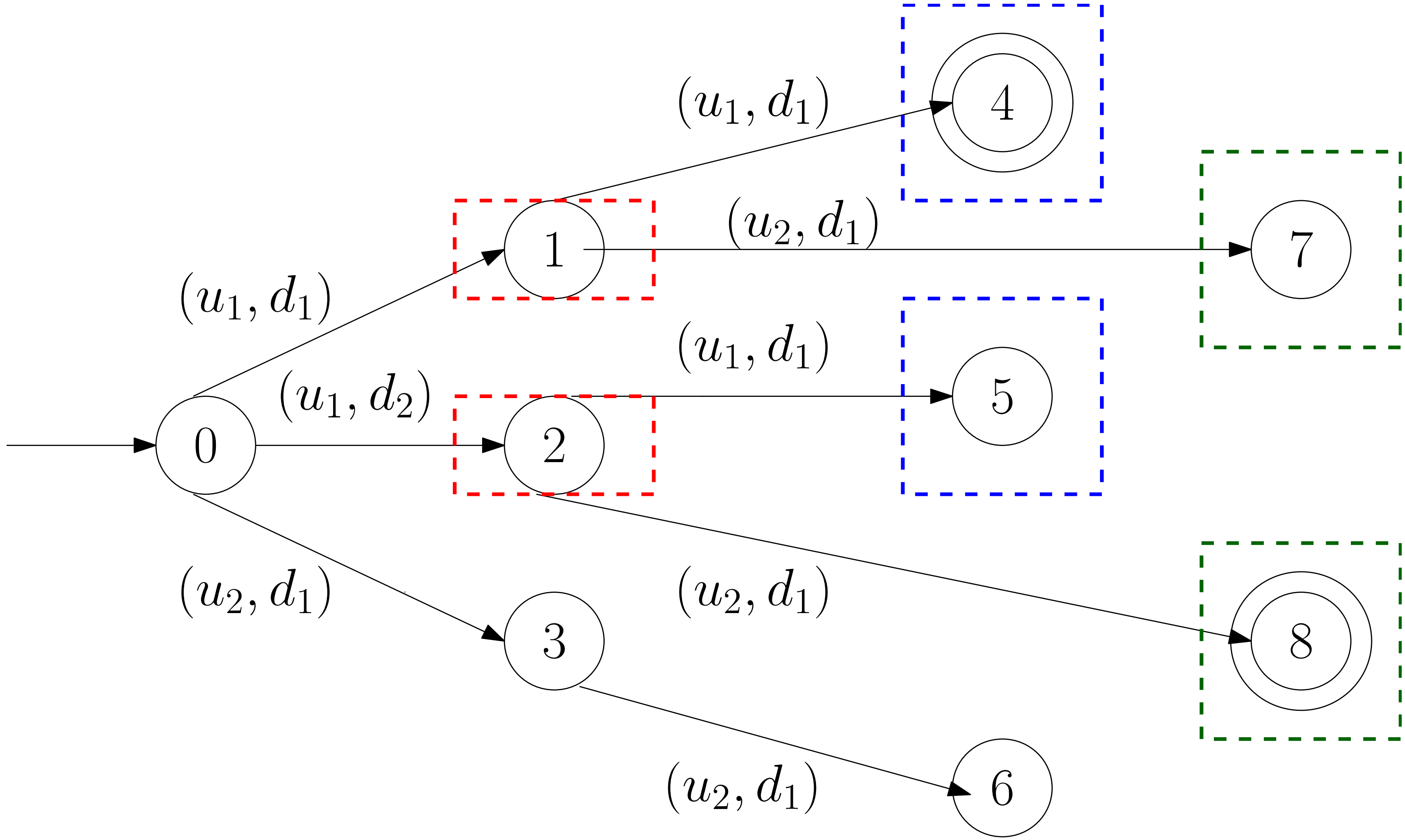
Assume now you need to fulfill a simple specification consisting of reaching a marked state. The sequence of open-loop inputs u_1 (at time 0) and u_1 (at time 1) solves the problem since it reaches the blue set for any disturbance realization.

Robust control design – a simple example



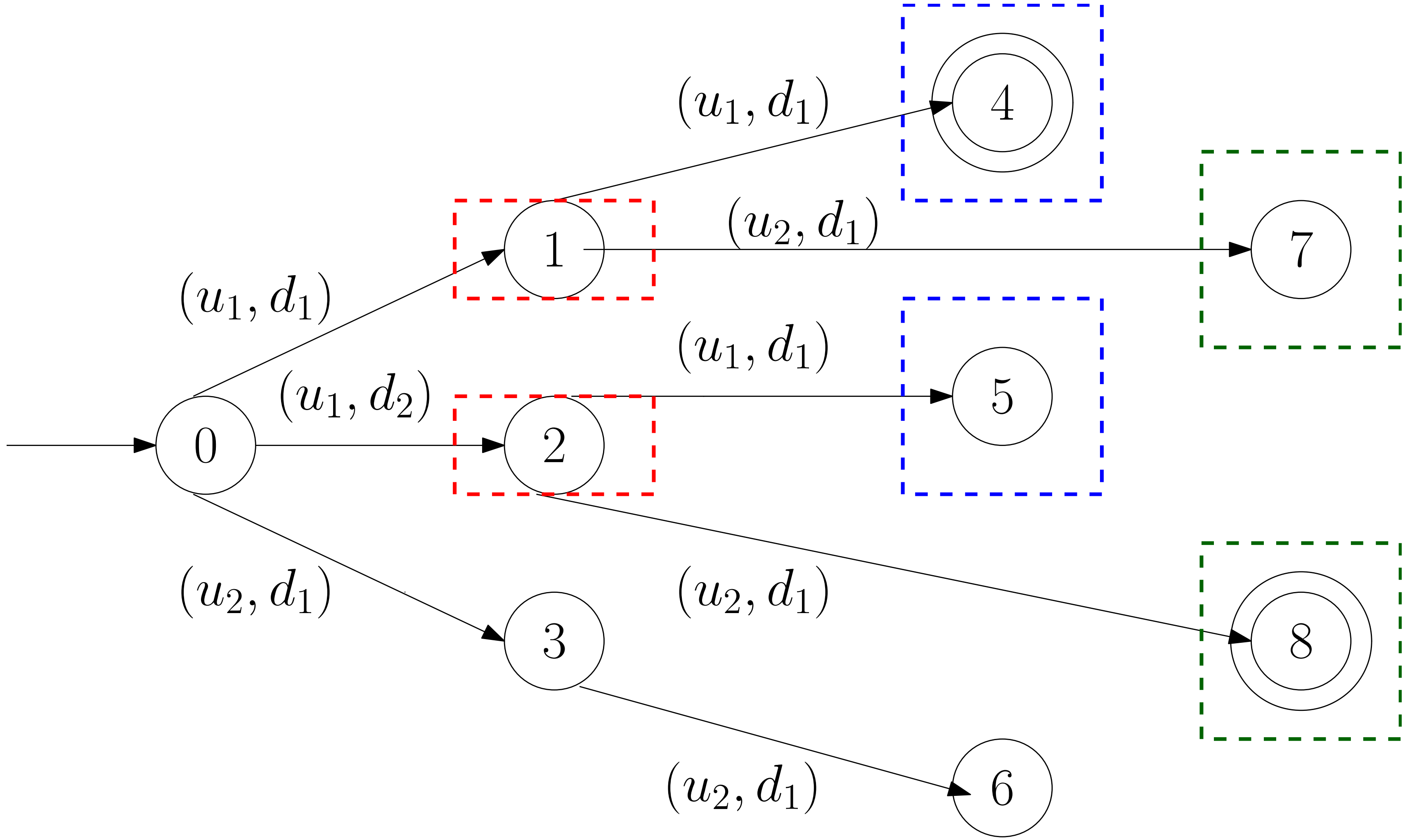
Consider now the more complex case where state 5 is unmarked. Then it is readily seen that any open-loop control strategy cannot solve the problem robustly with respect to all the possible disturbance realizations.

Robust control design – a simple example



Instead, assuming **state feedback**, it is possible to distinguish state 1 from 2 at step 1, and consequently, also all the states at step 2. Notice that now the information sets become singletons (full information).

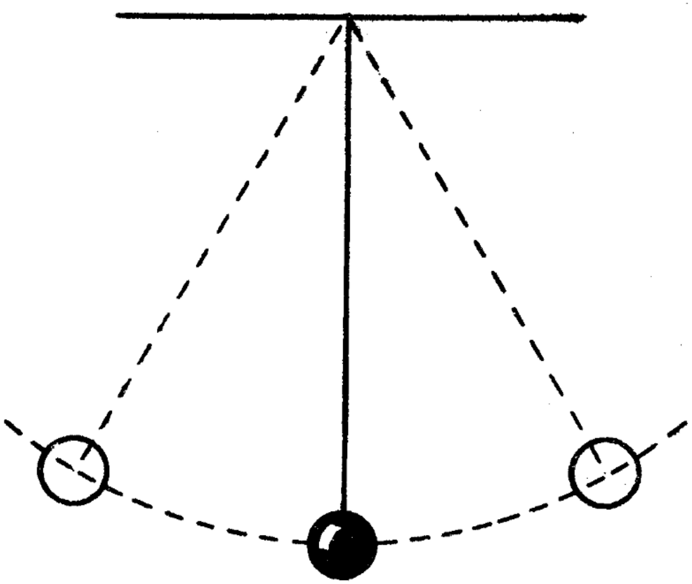
Robust control design – a simple example



Define $k(x)=u_1$ for $x=1$ and $k(x)=u_2$ if $x=2$. It is readily seen that the state-feedback control strategy setting u_1 at step 1, $k(x(1))$ at step 2, where $x(1)$ is the state reached at step 1, **solves the control problem robustly** with respect to all the disturbance realizations.

Example: construction of symbolic models

Pendulum subject to wind



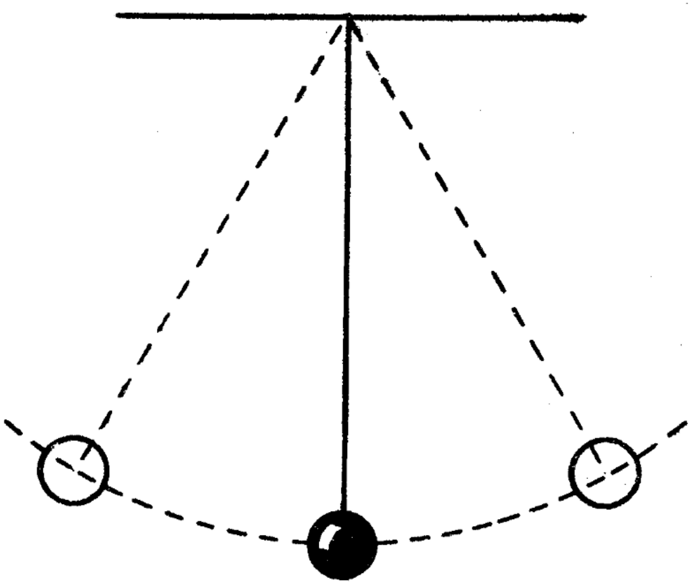
$$\dot{\theta} = \omega$$

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

- θ is the angular position of the point mass
- ω is the angular velocity of the point mass
- u is the applied torque (control input)
- d is the is the (unknown) horizontal acceleration (disturbance)
- g=9.8 is gravity acceleration
- l=0.5 is the length of the rod
- m=0.6 is the mass
- k=2 is the coefficient of rotational friction

Example: construction of symbolic models

Pendulum subject to wind



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

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

State space $X = [-\pi/4, \pi/4] \times [-0.5, 0.5]$

Input space $U = [-1.5, 1.5]$

Disturbance space $D = [-0.01, 0.02]$

Disturbance uniform Lipschitz constant $\kappa_d = 0.002$

Precision requirement $\varepsilon = 0.125$

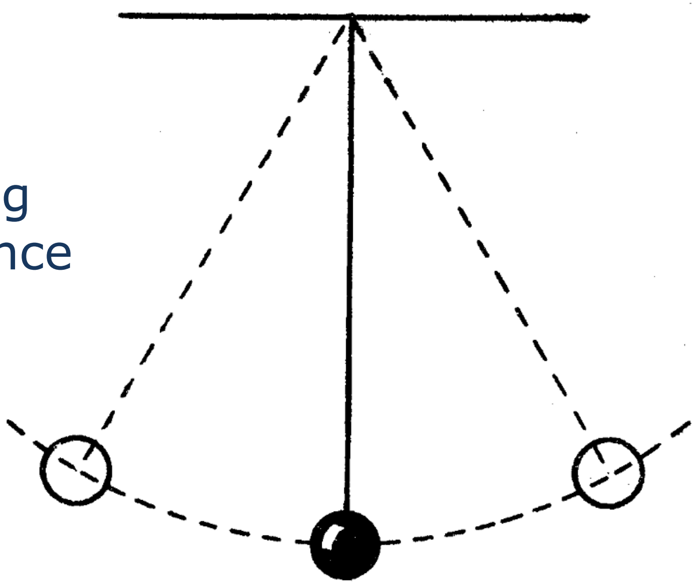
The control system is δ-ISS. We can build a AεA symbolic model with the following choice of quantization parameters

$$\tau = 1, \quad \mu_x = \pi/2000, \quad \mu_u = 0.001, \quad \mu_d = 1.43 \cdot 10^{-4}, \quad N_d = 0, \quad \theta_d = 0.007$$

Example: robust control design

Size of the resulting symbolic model:
159819 states, 1501 control inputs and 6366 disturbance inputs.

Control design problem: satisfy the following specification, independently from the disturbance signal realization:



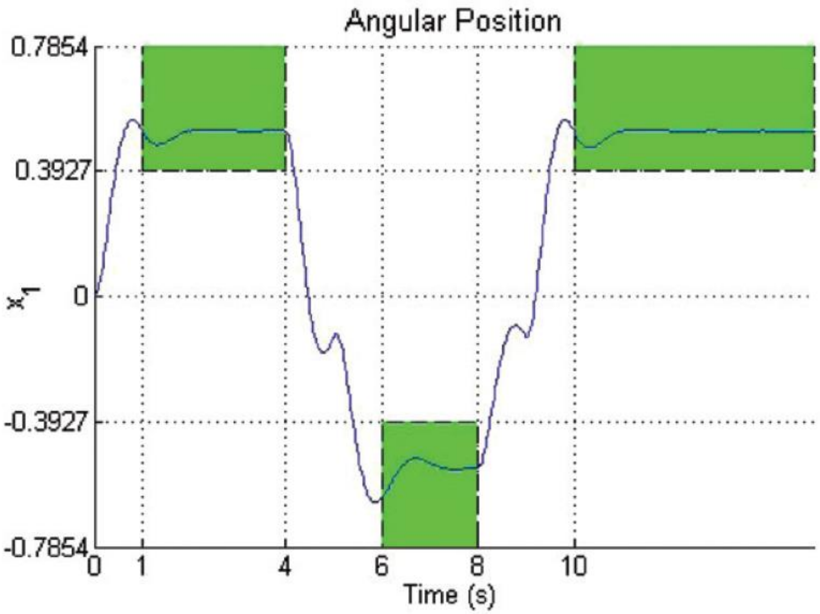
- *starting from* $x_0 = (0,0)$, *reach* $\Omega_1 = \left[\frac{\pi}{8}, \frac{\pi}{4}\right] \times X_2$;
- *stay in* Ω_1 *for a time duration between 2s and 4s;*
- *reach* $\Omega_2 = \left[-\frac{\pi}{4}, -\frac{\pi}{8}\right] \times X_2$;
- *stay in* Ω_2 *for at most 3s;*
- *go back to* Ω_1 *and stay definitively in* Ω_1.

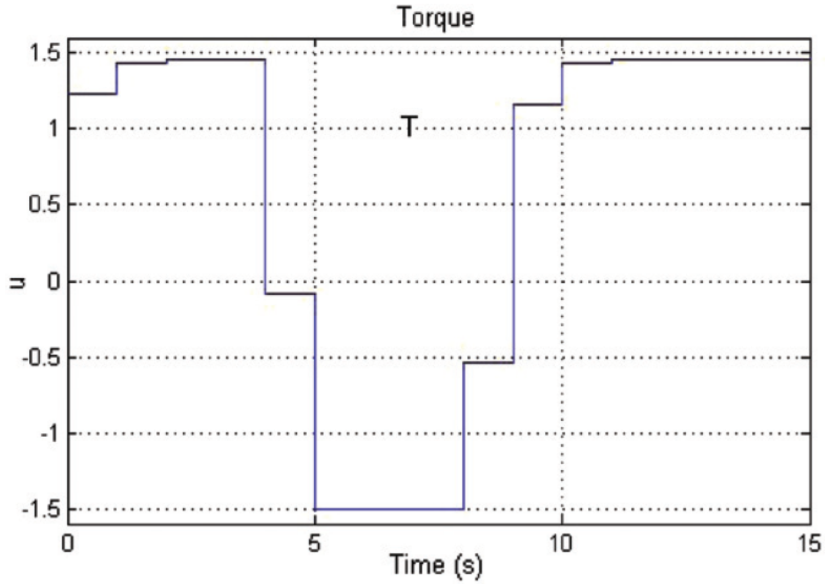
Example: robust control design

Controller synthesis computed by using fixed-point algorithms

Size of the resulting symbolic controller:
716 integers

Computation time:
2681 s.





Application 1: Vehicle Platooning

Application 1: Vehicle Platooning

Heavy Duty Vehicle Model equation

$$m\dot{v} = k_e T - F_{brake} - k_D(d)v^2$$
$$-k_{f_r} cos(\alpha) - k_g sin(\alpha)$$

- m is the mass
- v is the velocity
- T is the net engine torque
- d is the longitudinal distance from the vehicle ahead
- α is the road incline,
- k_e, k_{f_r}, k_g take into account vehicle engine, road friction and gravitational effects,
- $k_D(\cdot)$ is a least-square approximation of the air-drag coefficient.

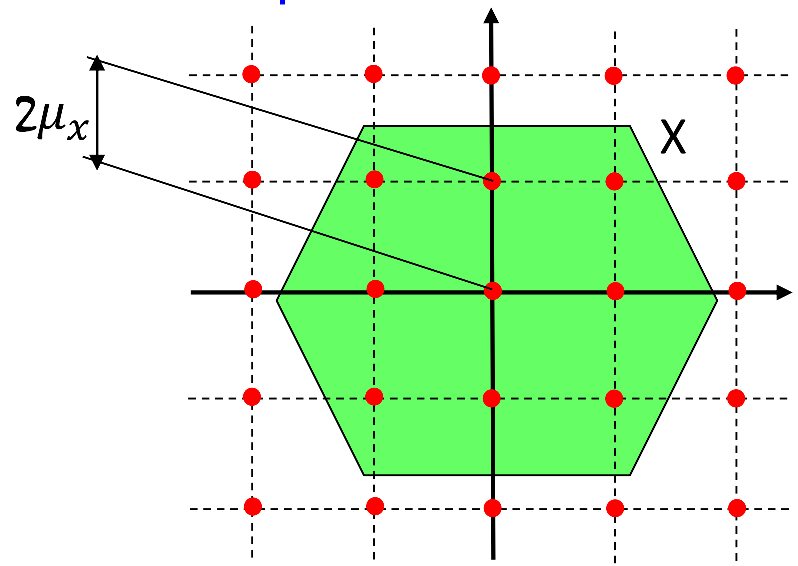
Lecture mostly based on:

[Borri et al., Necsys13] A. Borri, D. V. Dimarogonas, K. H. Johansson, M. D. Di Benedetto, and G. Pola, Decentralized symbolic control of interconnected systems with application to vehicle platooning, Proceedings of NecSys 2013, Koblenz, Germany, pp. 285-292, 2013.

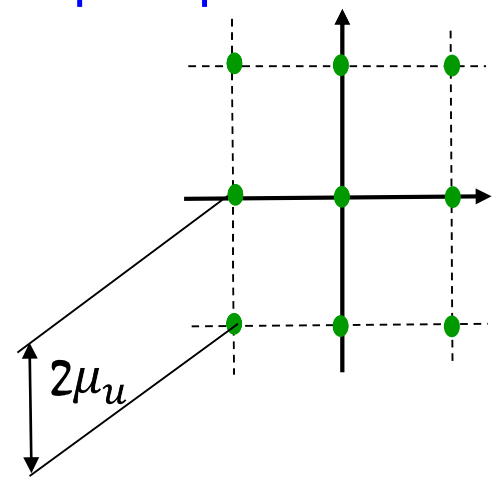
Symbolic control: a review

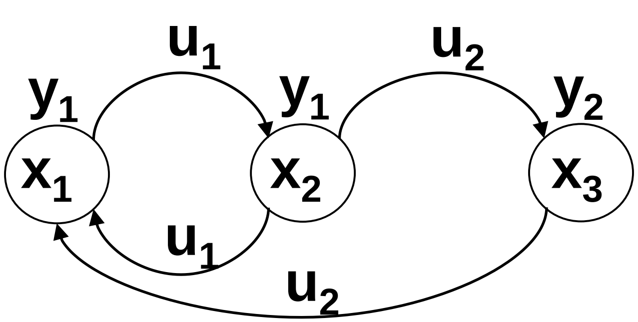
- The continuous system P is formally rewritten in the form of a transition system $\mathrm{T}_{\tau}(\mathrm{P})$ with an infinite number of states and inputs. As you know, this object cannot be built!
- By means of state and input discretization and time sampling, $\mathrm{T}_{\tau}(\mathrm{P})$ can be turned into a symbolic (finite) model $\mathrm{T}_{*}(\mathrm{P})$.

State quantization



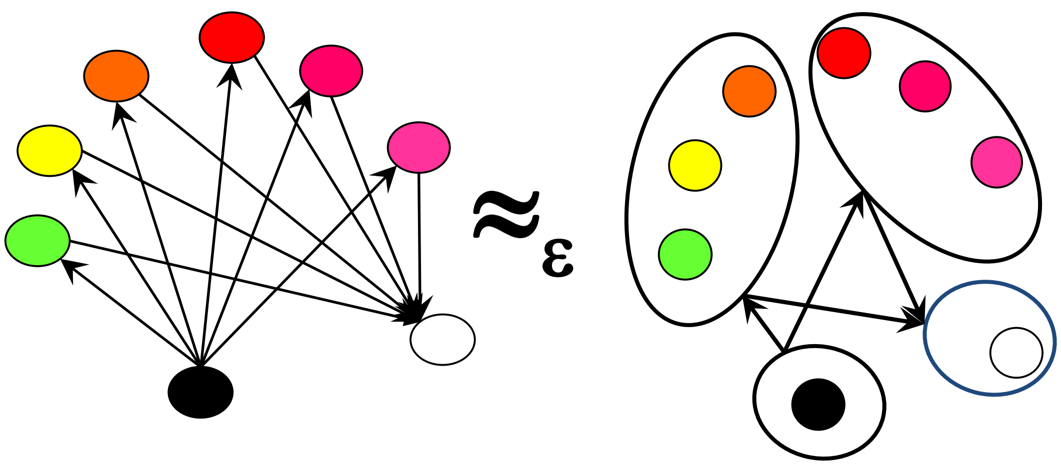
Input quantization





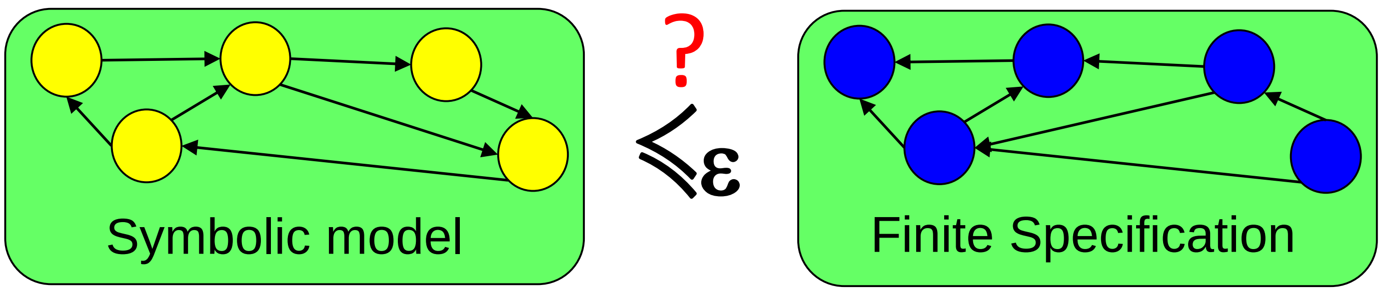
Symbolic control: a review

- The formalism of approximate simulation/bisimulation [Girard-Pappas (2007)] allows to relate the trajectories of the original continuous control system to the corresponding trajectories in the symbolic model, up to a given accuracy ε.
- Exogenous inputs (disturbances) cause the symbolic model to be nondeterministic.

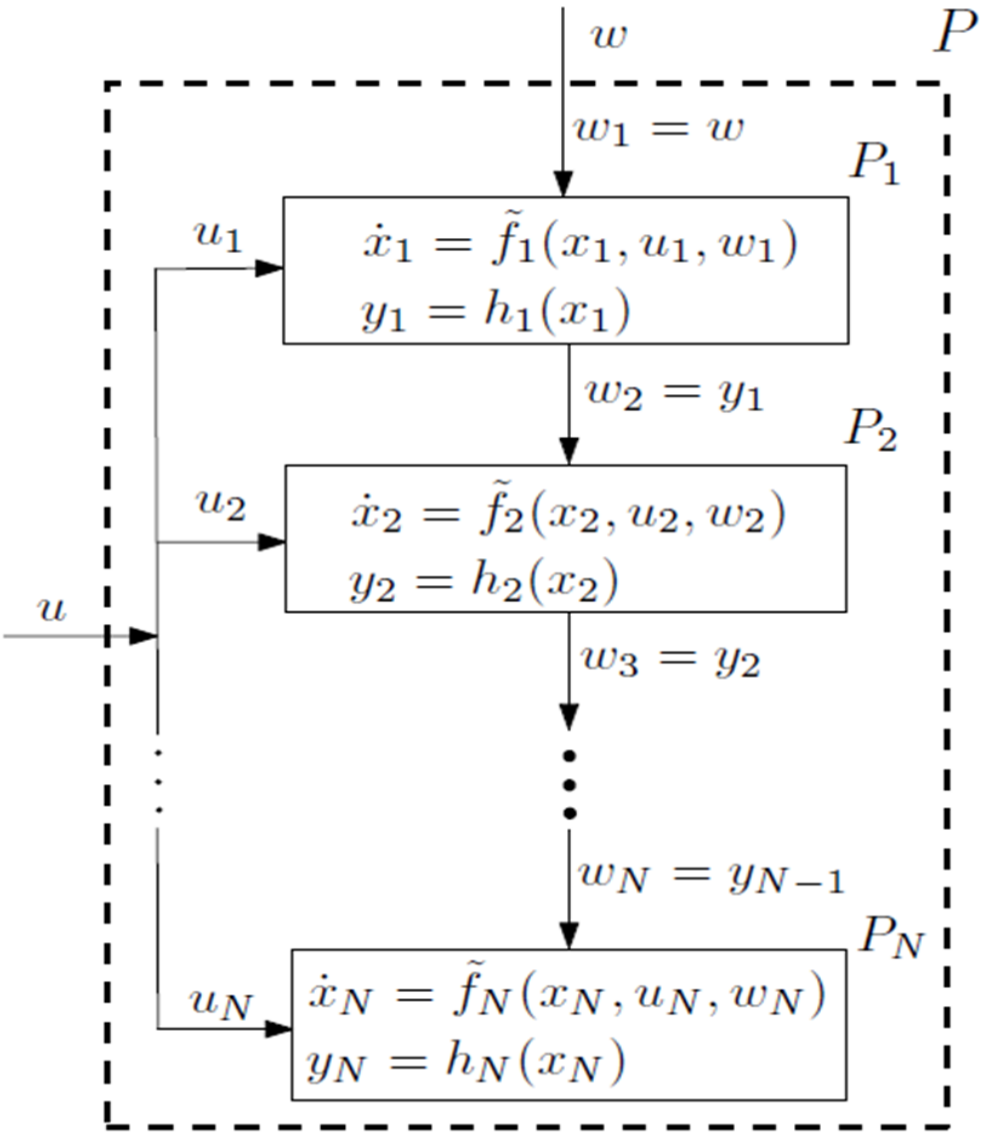


Symbolic control: a review

- Control problems can be expressed in terms of approximate similarity games [Tabuada (2009)], with specifications expressed in the form of finite transition systems.
- Thanks to the concept of alternating approximate simulation (AεA simulation) [Alur et al. (1998), Pola-Tabuada (2009)], the designed symbolic controllers are robust with respect to the non-determinism of the model.



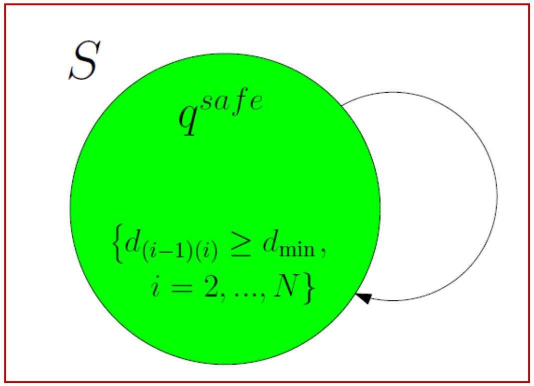
Towards the decentralized symbolic control



Serial interconnection of continuous systems

Global Specification

- **Safety** (no collisions in the platoon)
- **Refinement** problem: minimize global fuel consumption



Main assumptions

- N=6 vehicles
- The *leader* vehicle may reduce his nominal speed due to road speed changes, obstacles… (modeled as **disturbances**)

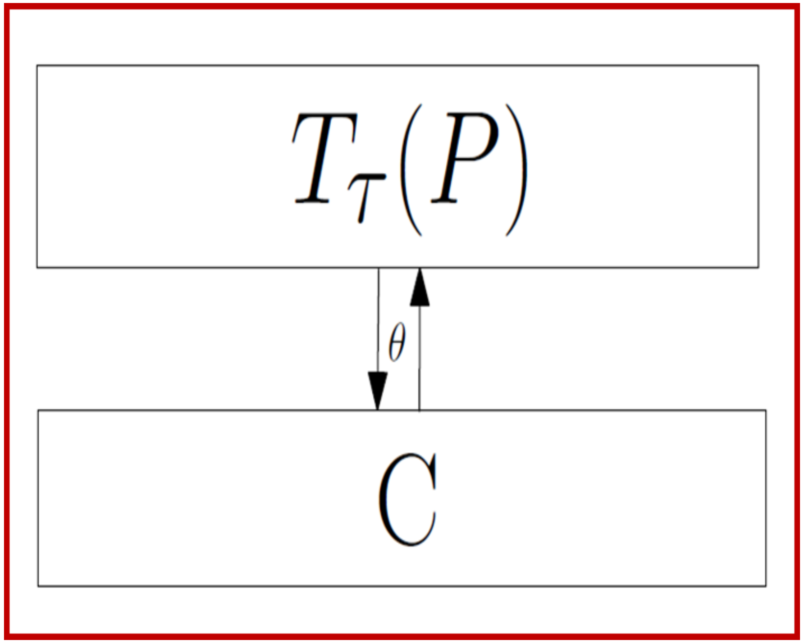
Precision requirement

$\varepsilon = 0.02\ (1\%)$

Centralized Synthesis

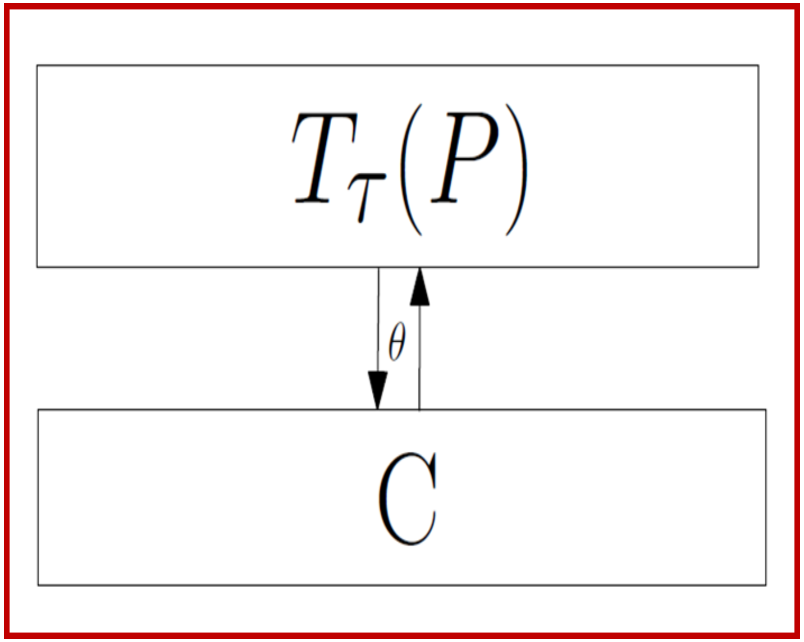
Problem 1. Given a continuous plant P, a specification S, and a desired precision $\varepsilon > 0$, find a sampling time τ, a parameter $\theta>0$, a symbolic controller C and an AθA-simulation relation $\mathcal{R}$ from C to $T_\tau(P)$ s.t. the closed-loop system is ε-simulated by the specification, namely:

$$T_\tau(P) \times_\theta^{\mathcal{R}} C \preccurlyeq_\varepsilon S$$



Control Design

1. Compute the symbolic model $T_*(P)$ of P
2. Compute the maximal sub-transition system C^* of $T_*(P)$ such that:



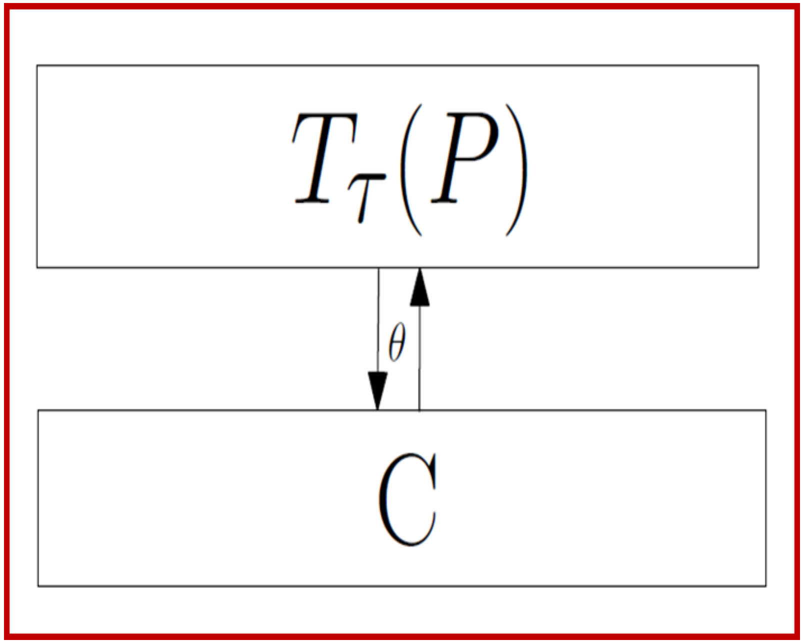
$C^* \preccurlyeq_{\mu_x} S$ **(behavioral inclusion)**
$C^* \preccurlyeq_{\mathbf{0}}^{\boldsymbol{alt}} T_*(P)$ **(robustness requirement)**

Centralized Synthesis

Theorem 1. For any desired precision $\varepsilon > 0$, and any θ, μ_x, $\eta > 0$ s.t.

$$\mu_x \leq \overline{\alpha}^{-1}(\underline{\alpha}(\theta)) \leq \theta \leq \eta$$
$$\mu_x + \theta \leq \varepsilon$$

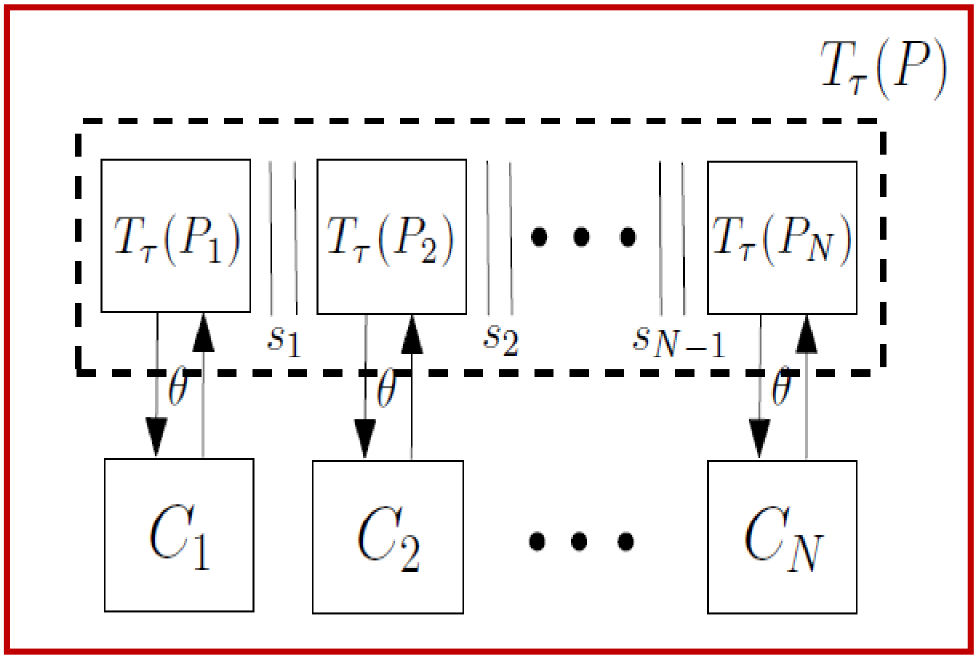
the control problem 1 is solved with $C = C^*$ and with $\mathcal{R} = \mathcal{R}^*$, where $\mathcal{R}^*$ is the maximal A0A-simulation relation from C^* to $T_*(P)$.



Drawback: high computational complexity (exponential with *N*)

Decentralized Synthesis

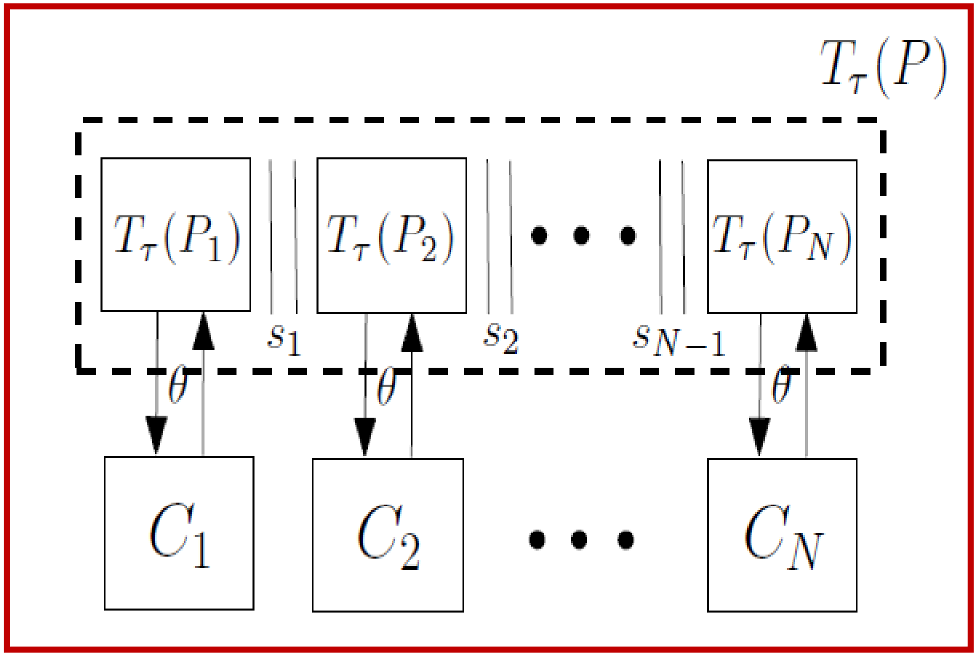
Problem 2. Given a continuous plant P, in the form of serial interconnection of N plants P_i, a specification S, and a desired precision $\varepsilon > 0$, find τ, $\theta > 0$, some symbolic controllers C_i and some AθA-simulation relations $\mathcal{R}_i$ from C_i to $T_\tau(P_i)$ s.t. the closed-loop system is ε-simulated by the specification, namely:



$$\left(T_\tau(P_1) \times_\theta^{\mathcal{R}_1} C_1\right) || \ldots || \left(T_\tau(P_N) \times_\theta^{\mathcal{R}_N} C_N\right) \preccurlyeq_\varepsilon S$$

Control Design.

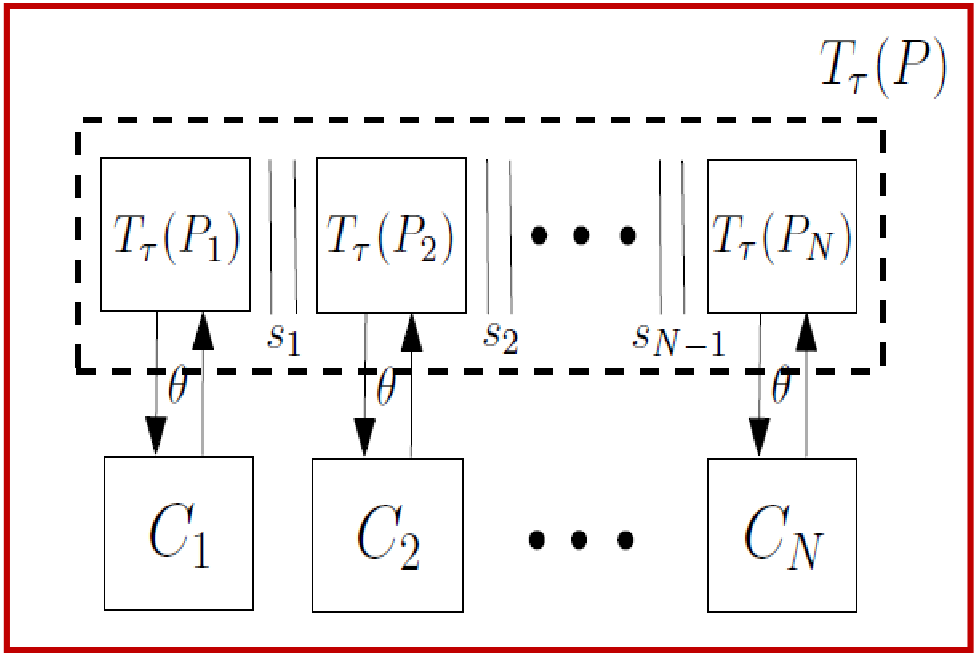
1. The specification S is decomposed into N local specifications S_i s.t.
$$S_1||S_2||\ldots||S_N \preccurlyeq_0 \ S$$
2. Compute the maximal $C_i^* \sqsubseteq T_*(P_i)$ s.t. $C_i^* \preccurlyeq_{\mu_x} S_i$ and $C_i^* \preccurlyeq_{\mathbf{0}}^{alt} T_*(P_i)$, where $T_*(P_i)$ is the symbolic model of P_i.



Theorem 2. For any desired precision $\varepsilon > 0$, and any θ, μ_x, $\eta > 0$ s.t.

$\mu_x \leq \min_i \bar{\alpha}_i^{-1}(\underline{\alpha}_i(\theta)) \leq \theta \leq \eta$
$\mu_x + \theta \leq \varepsilon$

the control problem 2 is solved with $C_i = C_i^*$ and with $\mathcal{R}_i = \mathcal{R}_i^*$, where $\mathcal{R}_i^*$ is the maximal A0A-simulation relation from C_i^* to $T_*(P_i)$, for all *i*.

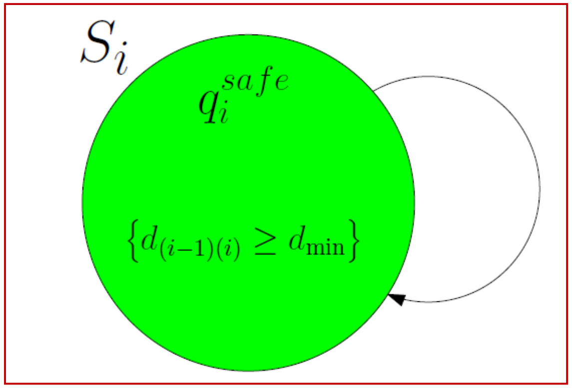


Advantage: low complexity, in particular for identical plants

Centralized vs. decentralized symbolic control

Local Specifications

- **Safety** (no collision with the vehicle ahead)
- **Refinement** problem: minimize local fuel consumption



Space Complexity (estimated)

Centralized approach: $4 \cdot 10^{28}$ states, $4 \cdot 10^{15}$ controls, 401 disturbances (**intractable**)

Decentralized approach : $1.6 \cdot 10^{5}$ states, 401 controls, 401 disturbances (**tractable**)

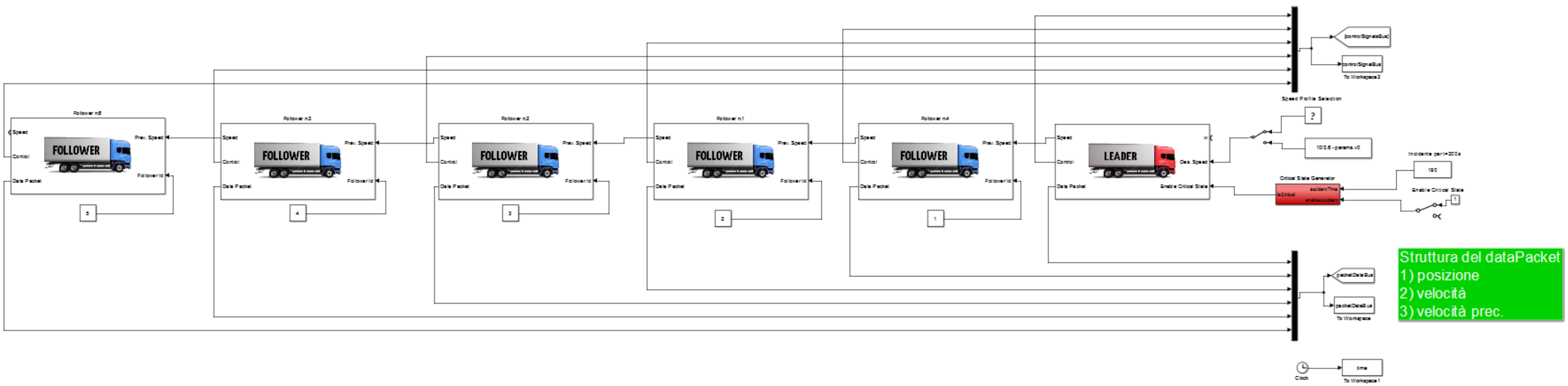
Design parameters

$\theta = 0.01 \quad \tau = 0.2\, s$

$\mu_x = 0.005$

(satisfying Theorems 1-2)

Simulink implementation (by Luigi Rodorigo)



Simulations

Application 2: Symbolic adaptive cruise control

- An alternative approach to the platooning problem it to design Adaptive Cruise Control (ACC) systems independently on each vehicle.
- ACC can be modelled as a hybrid system, with two modes q=1 (no lead car) and q=2 (lead car), where the latter indicates the situation in which a lead car is present within the radar range. Parameter h denotes the distance from the lead car and v_L, a_L the leader velocity and acceleration, when present.

$$q = 1: \quad \boxed{\begin{array}{l} m\dot{v} = F_w - f_0 - f_1 v - f_2 v^2 \\ h \equiv h^{max} \end{array}}$$

$$R_{2,1} \qquad R_{1,2}$$

$$q = 2: \quad \boxed{\begin{array}{l} m\dot{v} = F_w - f_0 - f_1 v - f_2 v^2 \\ \dot{h} = v_L - v \\ \dot{v}_L = a_L \end{array}} \quad R_{2,2}$$

More details in:

[Nilsson et al., CST2016] S. Coogan, M. Arcak, and C. Belta, P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A. D. Ames, J. W. Grizzle, N. Ozay, H. Peng, and P. Tabuada, “Correct-by-construction adaptive cruise control: Two approaches”, IEEE Transactions on Control Systems Technology, 24(4), 1294-1307, 2016.

Application 2: Symbolic adaptive cruise control

First define the time headway $\omega = \frac{h}{v}$.

Requirements (coded in LTL):

1. ACC operates in two modes: the set speed mode and the time gap mode.
2. In set speed mode, a preset desired speed v^{des} eventually needs to be maintained.
3. In time gap mode, a desired time headway ω^{des} to the lead vehicle eventually needs to be maintained, and the time headway needs to satisfy $\omega \geq \omega^{min}$ at all times.
4. The system is in set speed mode if $h \geq v^{des}\omega^{des}$, otherwise it is in time gap mode.
5. Independently of the mode, the input constraint $-0.3mg \leq F_w \leq 0.2mg$ needs to be satisfied at all times.

Application 2: Symbolic adaptive cruise control

Target sets and specification mode sets

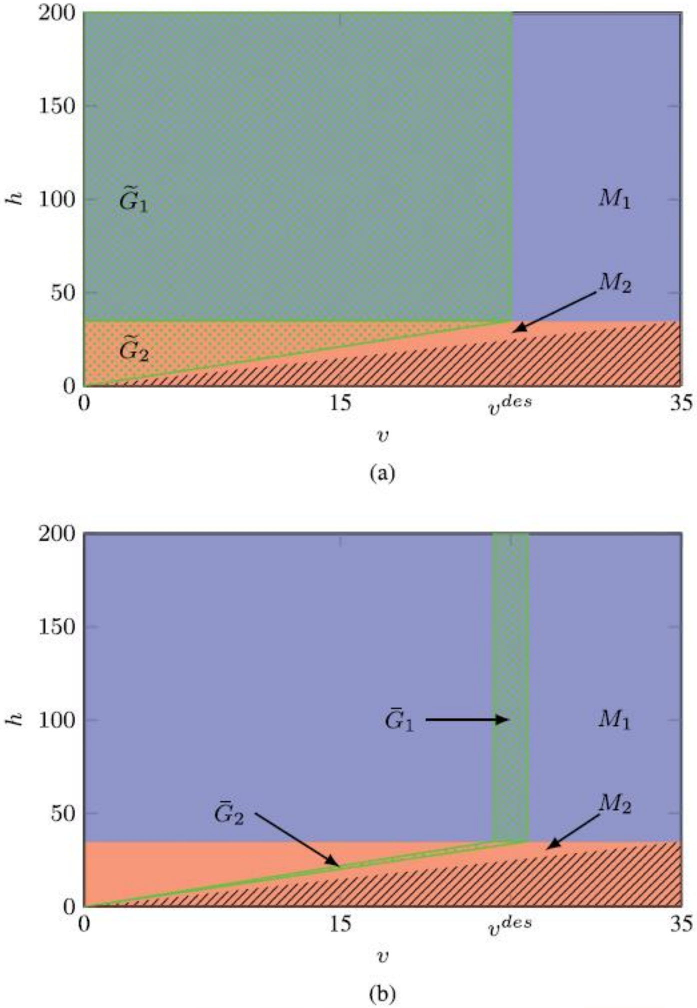
$M_1 = \{(v, h, F_w): v^{des} \leq h/\omega^{des}\}$ set speed
$M_2 = \{(v, h, F_w): v^{des} > h/\omega^{des}\}$ time gap

M_1 and M_2 define the set speed and the time gap modes.

G_1 and G_2 expresses requirements 2 which have to be EVENTUALLY satisfied in set speed mode and time gap mode, respectively.

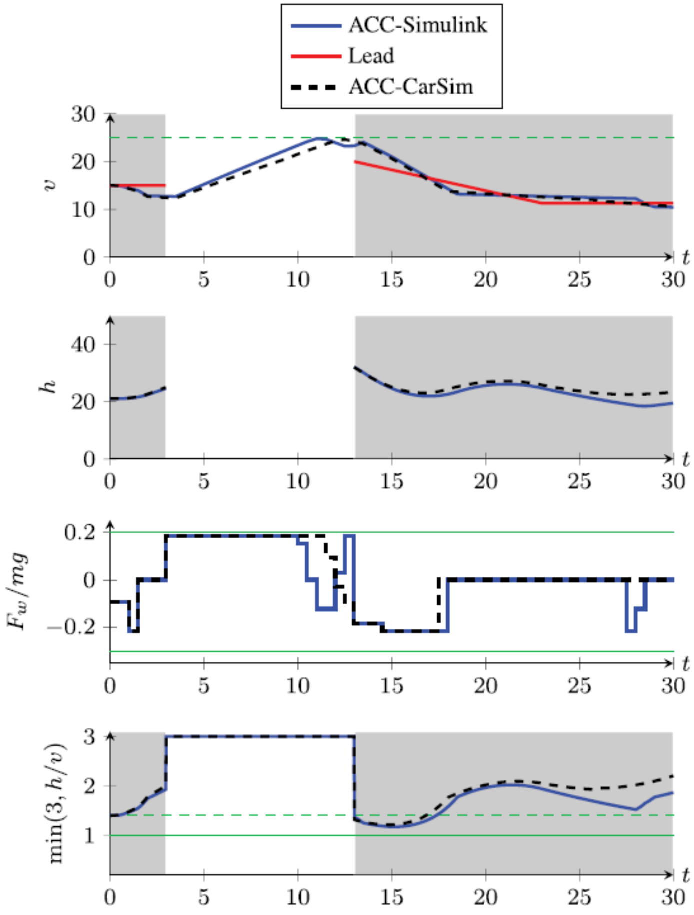
S_1, S_2, S_U are safe sets which need to be ALWAYS satisfied.

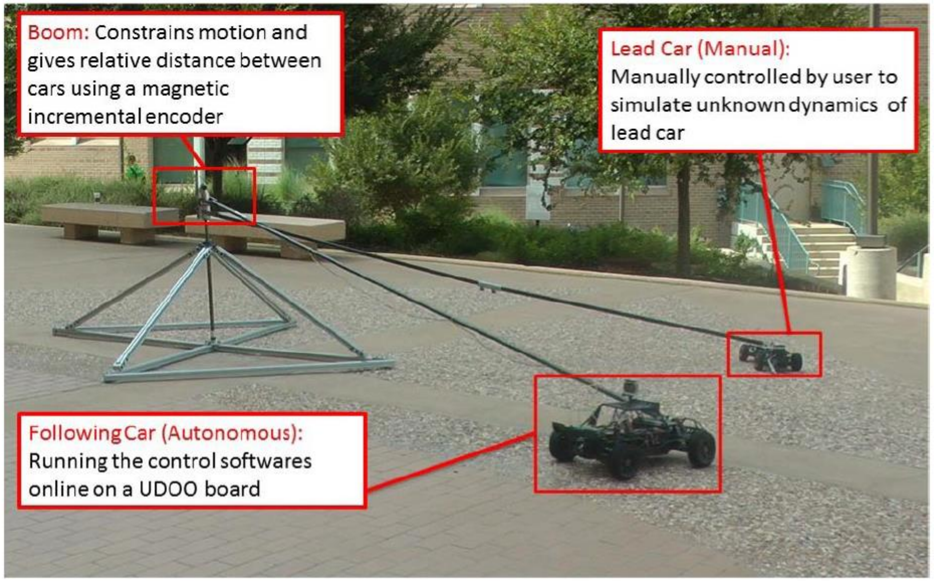
These atomic propositions allow to encode more complex specifications.



Application 2: Symbolic adaptive cruise control

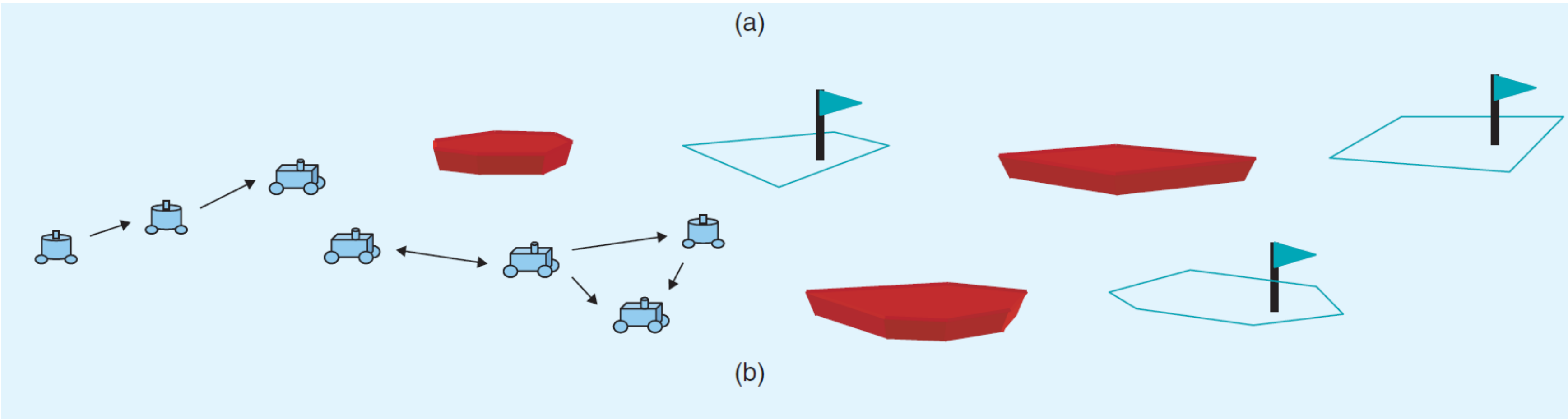
Numerical simulation and physical implementation

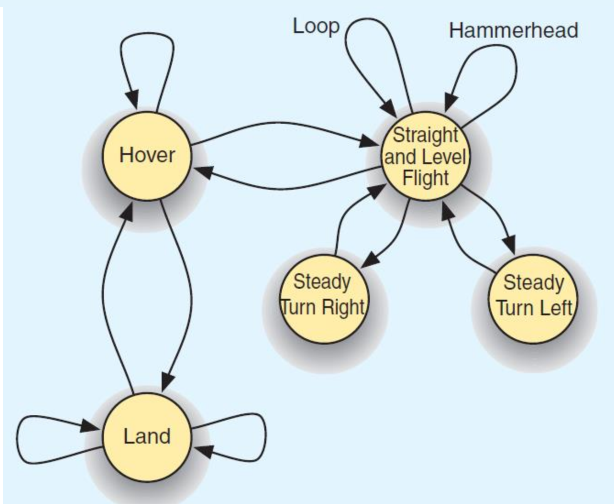


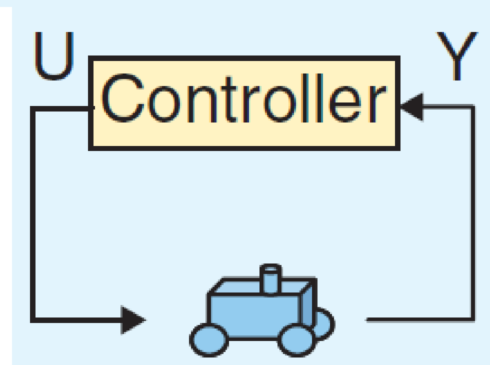


Hardware testbed on which the two controllers were implemented

Application 3: Symbolic robot motion control



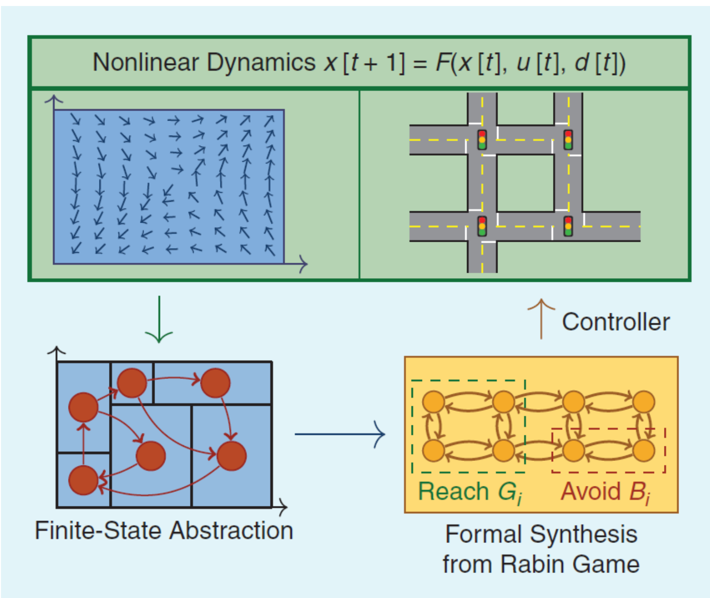


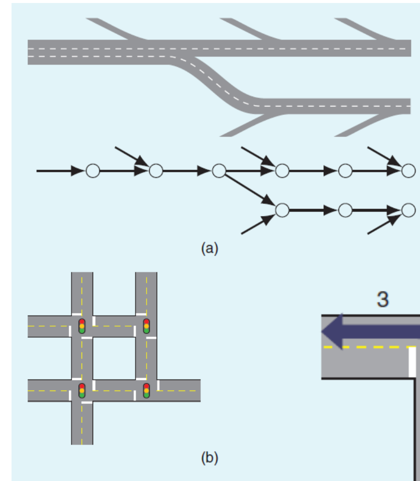


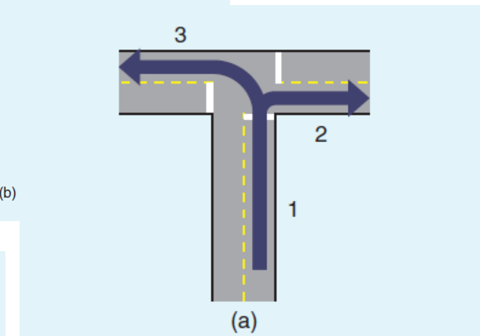
More details in:

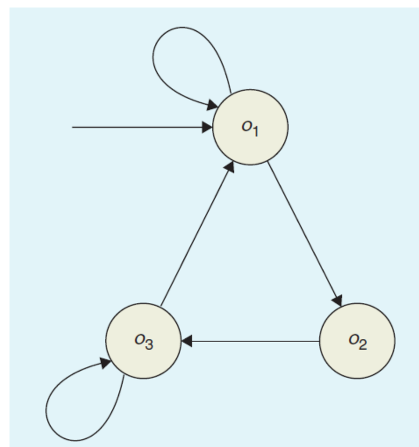
[Belta et al., RAM2007] C. Belta, A. Bicchi, M. Egerstedt, E. Frazzoli, E. Klavins, and G. J. Pappas, “Symbolic planning and control of robot motion”, IEEE Robotics & Automation Magazine, 14(1), 61-70, 2007.

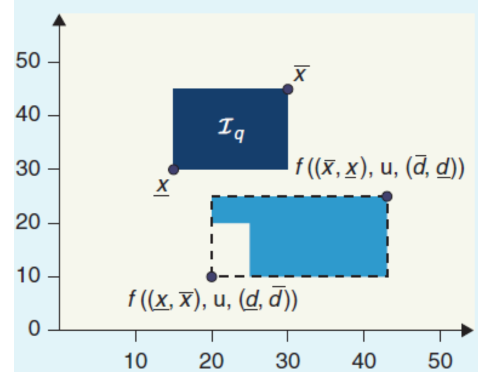
Application 4: Control of Traffic Flow











More details in:

[Coogan et al., CSM2017] S. Coogan, M. Arcak, and C. Belta, “Formal Methods for Control of Traffic Flow”, IEEE Control Systems Magazine, April 2017.