Embedded Systems
2012/13

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

Lecture 7
Construction of Symbolic Models

Maria Domenica Di Benedetto
Giordano Pola
Alessandro Borri
University of L'Aquila

Construction of symbolic models

We now consider **digital control systems**, i.e. control systems where input signals are piecewise constant.

Construction of symbolic models

We now consider **digital control systems**, i.e. control systems where input signals are piecewise constant.

Consider a nonlinear digital control system Σ

$$\dot{x} = f(x,u), \quad x \in R^n,\ u \in R^m$$

and $\tau > 0$, define:

$$T^*_\tau(\Sigma) = (Q, L, \longrightarrow, O, H)$$

where:

- $Q = R^n$
- L is the collection of constant functions $u: [0,\tau] \rightarrow R^m$
- $p \xrightarrow{u} q$, if $x(\tau,p,u)=q$
- $O = R^n$
- H is the identity function

Construction of symbolic models

We now consider **digital control systems**, i.e. control systems where input signals are piecewise constant.

Consider a nonlinear digital control system Σ

$$\dot{x} = f(x,u), \quad x \in R^n,\ u \in R^m$$

and $\tau > 0$, define:

$$T^*_\tau(\Sigma) = (Q, L, \longrightarrow, O, H)$$

where:

- $Q = R^n$
- L is the collection of constant functions $u: [0,\tau] \rightarrow R^m$
- $p \xrightarrow{u} q$, if $x(\tau,p,u)=q$
- $O = R^n$
- H is the identity function

… summarizing

Construction of symbolic models

We now consider **digital control systems**, i.e. control systems where input signals are piecewise constant.

Consider a nonlinear digital control system Σ

$$\dot{x} = f(x,u), \quad x \in R^n,\ u \in R^m$$

and $\tau > 0$, define:

$$T^*_\tau(\Sigma) = (Q, L, \longrightarrow, O, H)$$

where:

- $Q = R^n$
- L is the collection of constant functions $u: [0,\tau] \rightarrow R^m$
- $p \xrightarrow{u} q$, if $x(\tau,p,u)=q$
- $O = R^n$
- H is the identity function

Σ: control system

$\downarrow =$

$T(\Sigma)$: LTS

$\downarrow \geq$

$T_\tau(\Sigma)$: LTS

… summarizing

Construction of symbolic models

We now consider **digital control systems**, i.e. control systems where input signals are piecewise constant.

Consider a nonlinear digital control system Σ

$$\dot{x} = f(x,u), \quad x \in R^n,\ u \in R^m$$

and $\tau > 0$, define:

$$T^*_\tau(\Sigma) = (Q, L, \longrightarrow, O, H)$$

where:

- $Q = R^n$
- L is the collection of constant functions $u: [0,\tau] \to R^m$
- $p \xrightarrow{u} q$, if $x(\tau,p,u)=q$
- $O = R^n$
- H is the identity function

Σ: control system

$=$

$T(\Sigma)$: LTS

$\geq$

$T_\tau(\Sigma)$: LTS

$\geq$

$T^*_\tau(\Sigma)$: LTS

… summarizing

Construction of symbolic models

Consider the following parameters:

- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

Construction of symbolic models

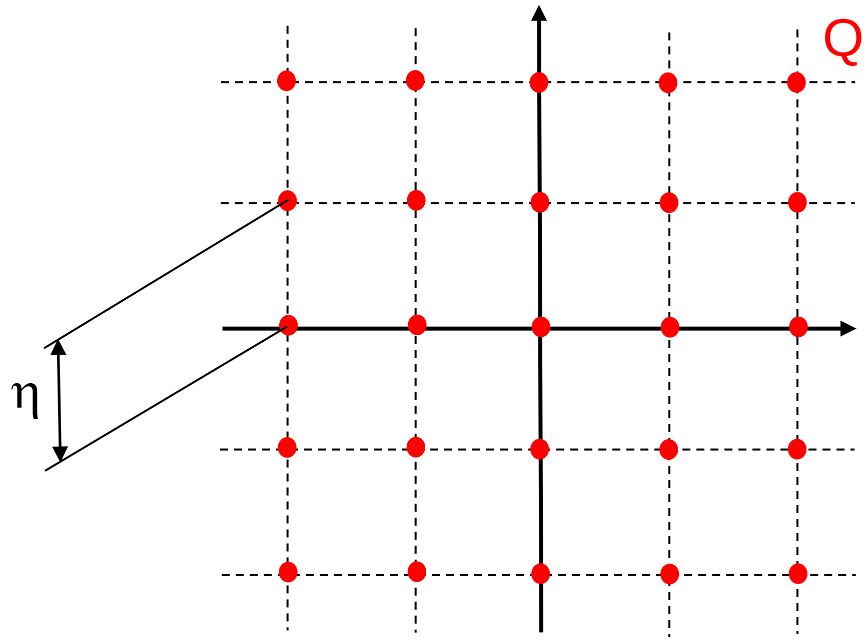
Consider the following parameters:

- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$



Construction of symbolic models

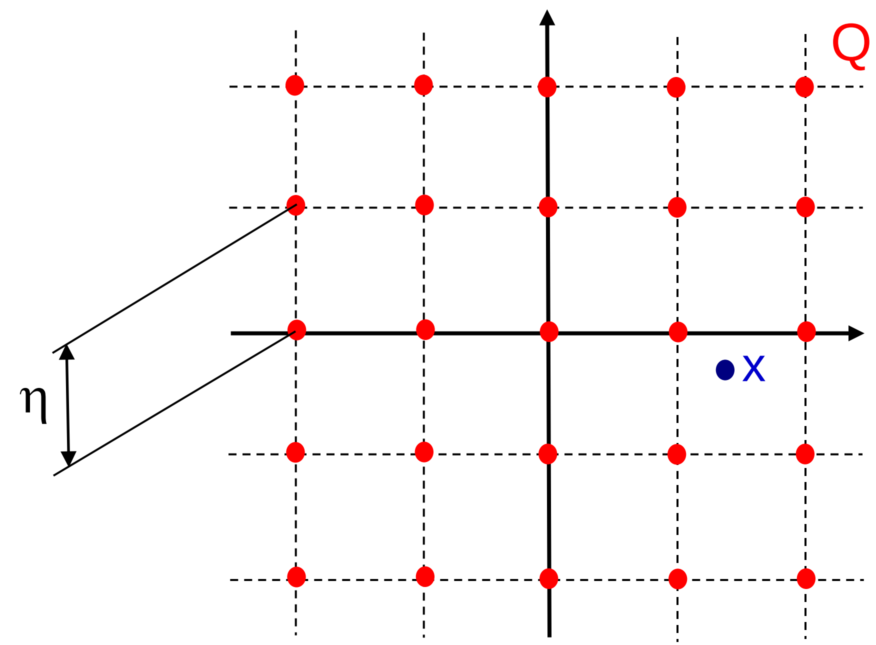
Consider the following parameters:

- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$



Q approximates R^n with precision η

$\forall x \in R^n$

Construction of symbolic models

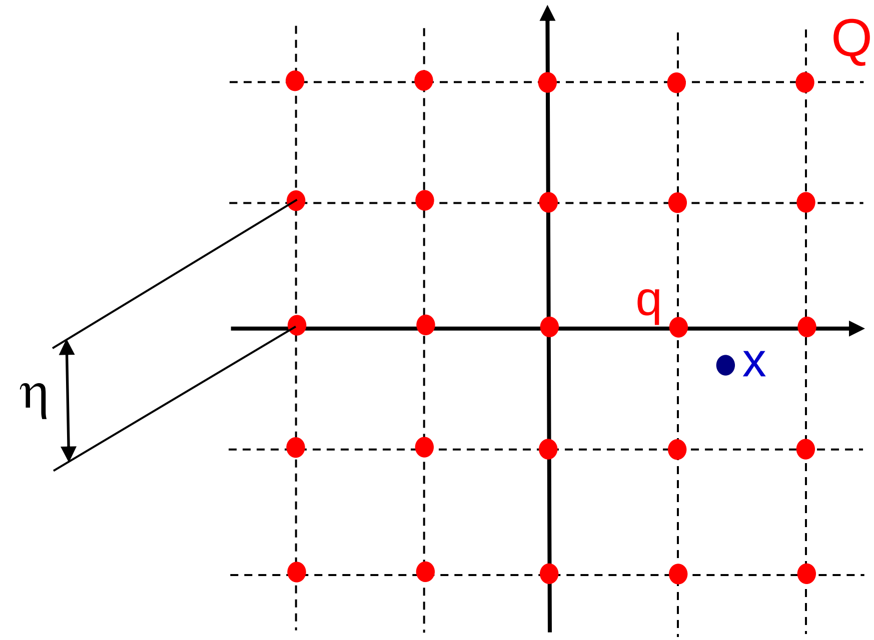
Consider the following parameters:

- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$



Q approximates R^n with precision η

$\forall x \in R^n \quad \exists q \in Q$

Construction of symbolic models

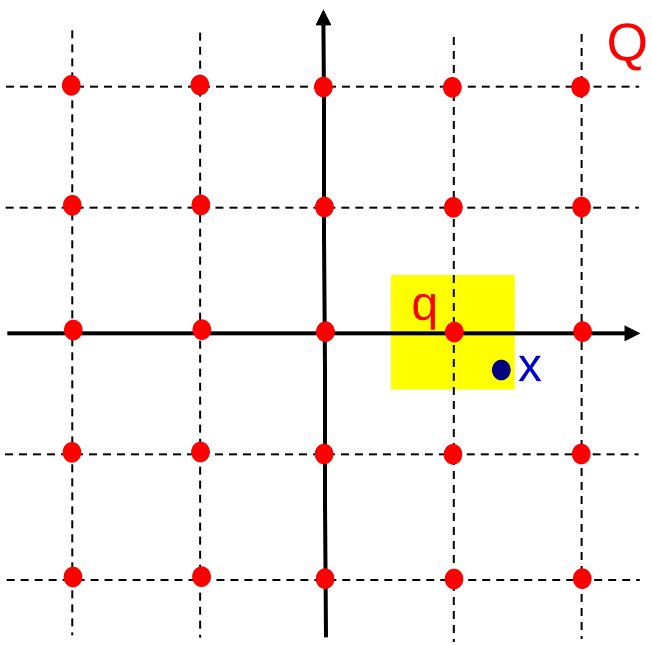
Consider the following parameters:

- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$



Q approximates R^n with precision η

$\forall x \in R^n \quad \exists q \in Q$ s.t. $x \in \mathcal{B}_{[\eta/2[}(q)$

Construction of symbolic models

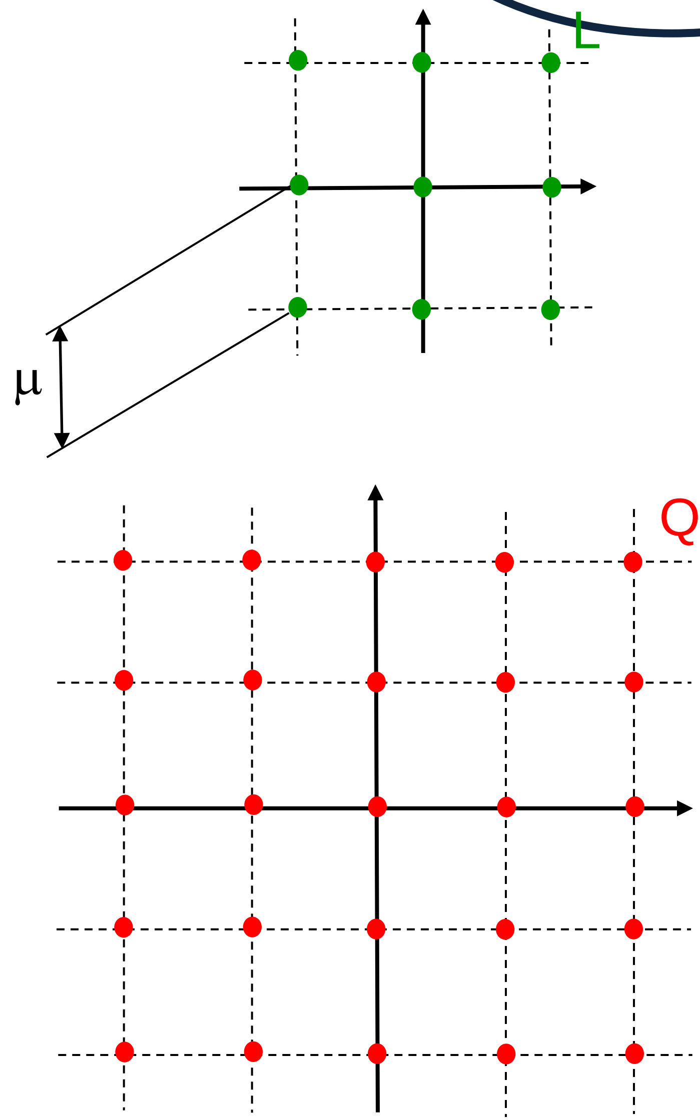
Consider the following parameters:

- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

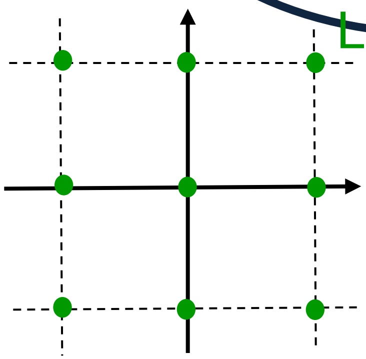
- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$



Construction of symbolic models

Consider the following parameters:

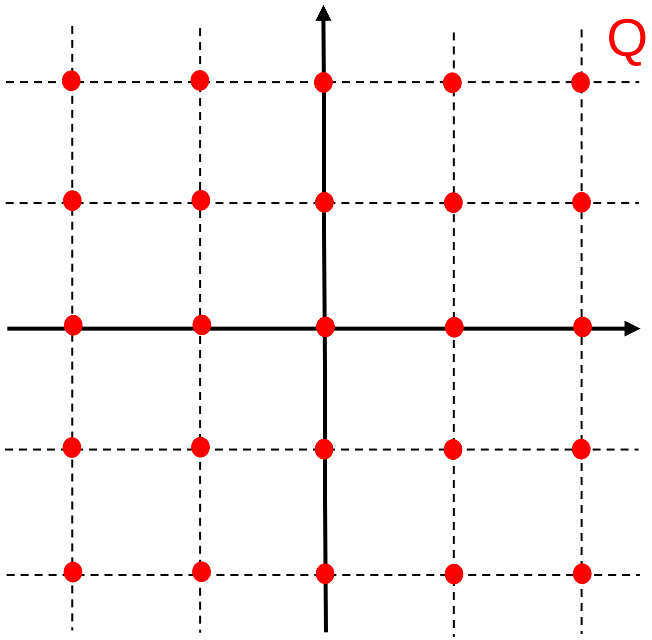
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization



and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function



Labelled transition system $T_{\tau,\eta,\mu}(\Sigma)$ is countable

Construction of symbolic models

Consider the following parameters:

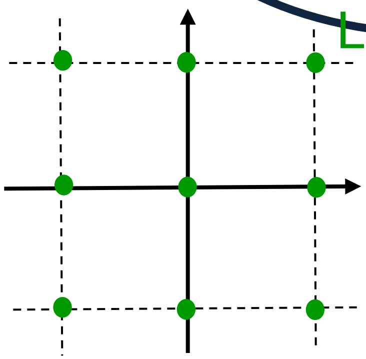
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

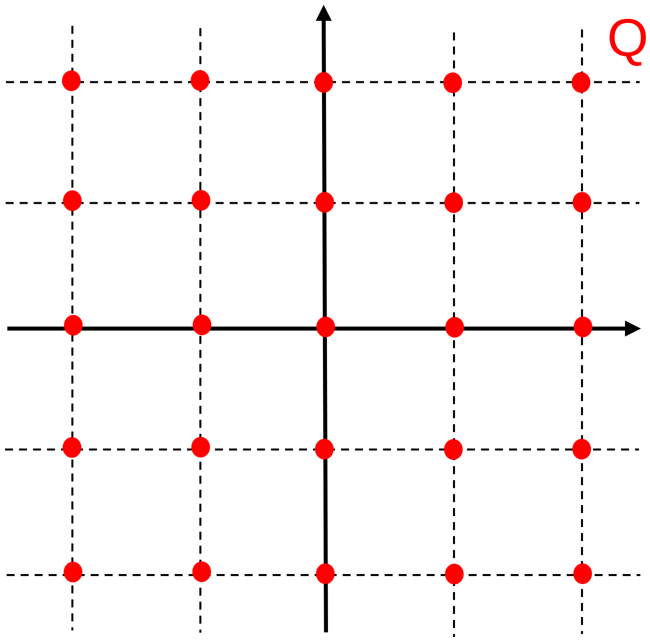
and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

How do I construct this symbolic model ?

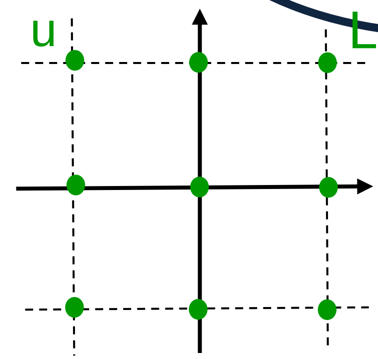




Construction of symbolic models

Consider the following parameters:

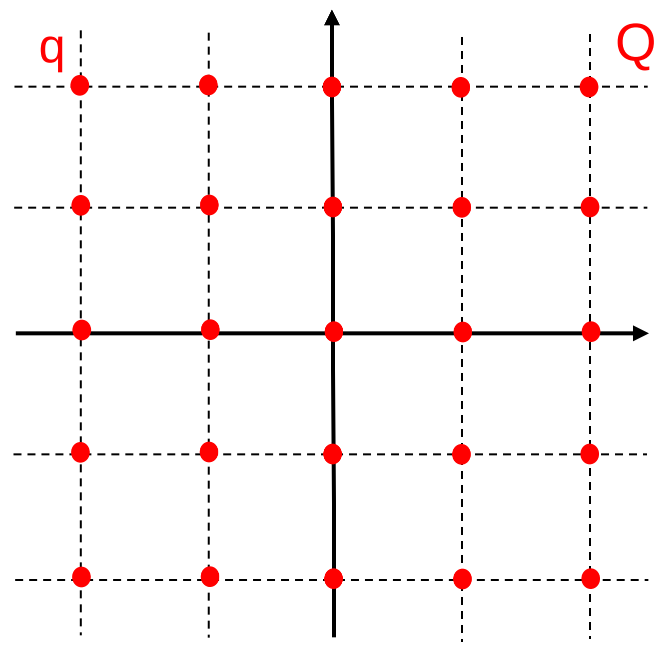
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization



and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

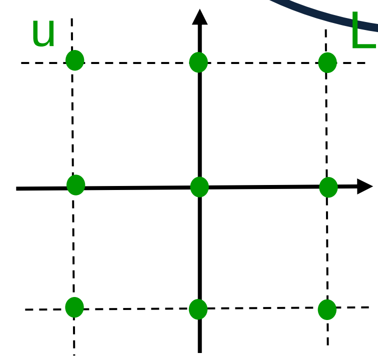
- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function



How do I construct this symbolic model ?

Construction of symbolic models

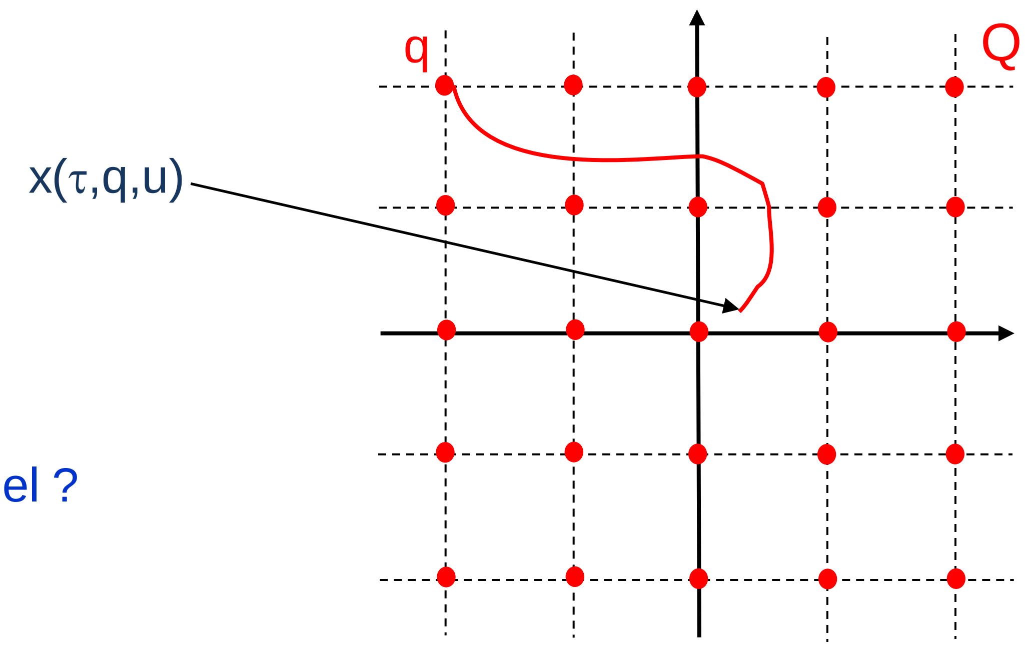
Consider the following parameters:



- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:



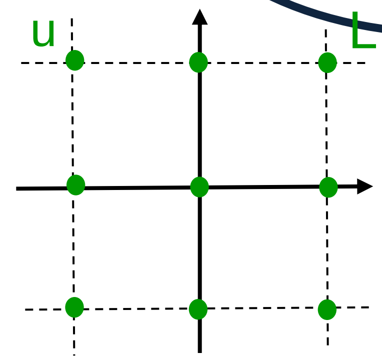
- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

How do I construct this symbolic model ?

Construction of symbolic models

Consider the following parameters:

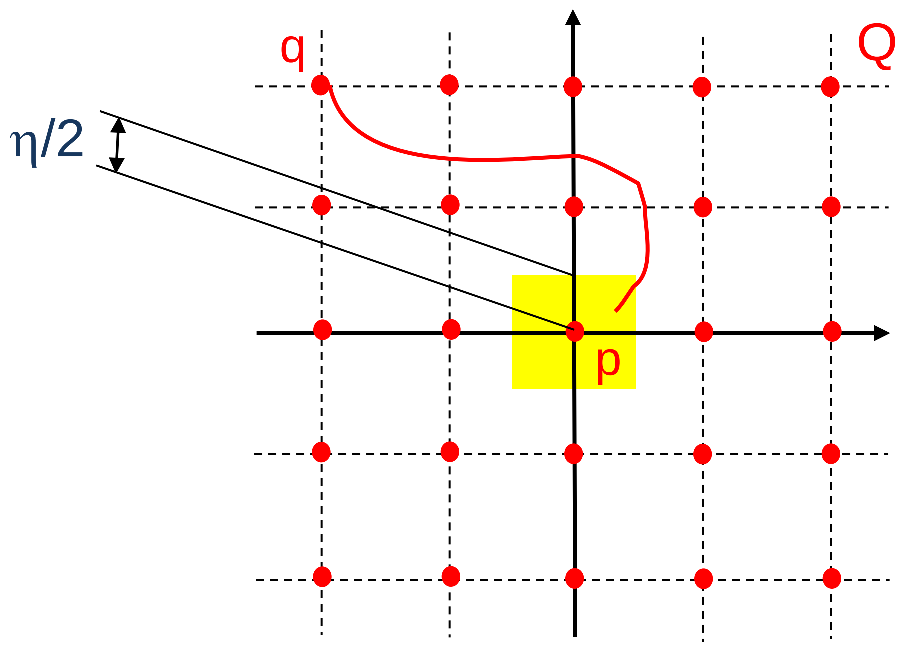
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization



and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

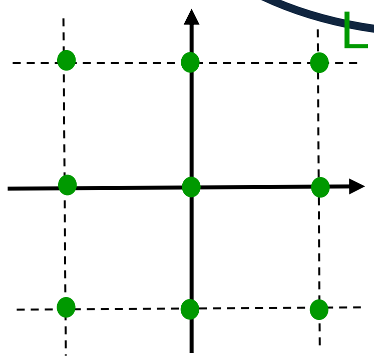


How do I construct this symbolic model ?

Construction of symbolic models

Consider the following parameters:

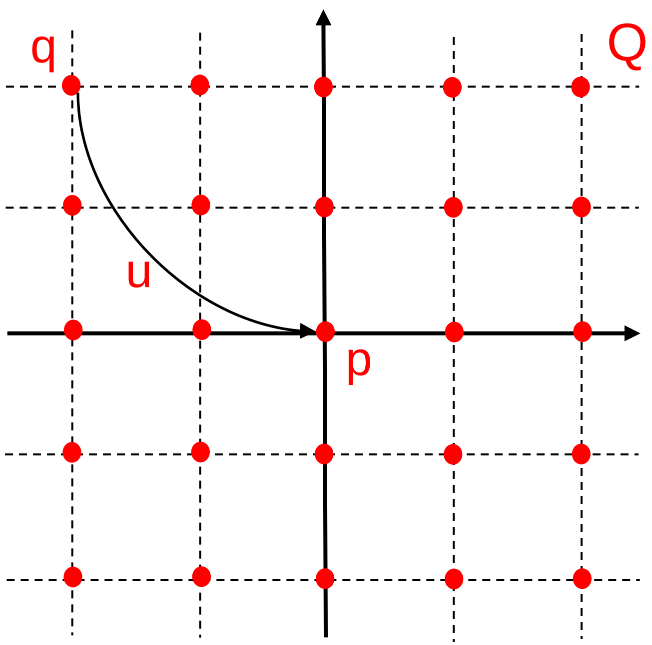
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization



and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [\mathbb{R}^n]_\eta = \eta \mathbb{Z}^n$
- $L = [\mathbb{R}^m]_\mu = \mu \mathbb{Z}^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = \mathbb{R}^n$
- H is the identity function

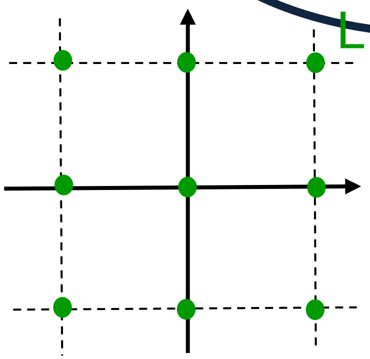


How do I construct this symbolic model ?

Construction of symbolic models

Consider the following parameters:

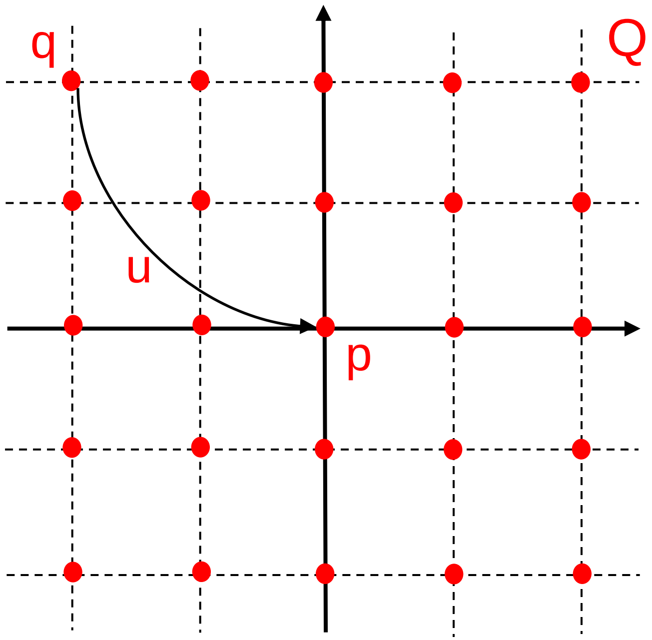
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization



and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [\mathbb{R}^n]_\eta = \eta \mathbb{Z}^n$
- $L = [\mathbb{R}^m]_\mu = \mu \mathbb{Z}^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = \mathbb{R}^n$
- H is the identity function

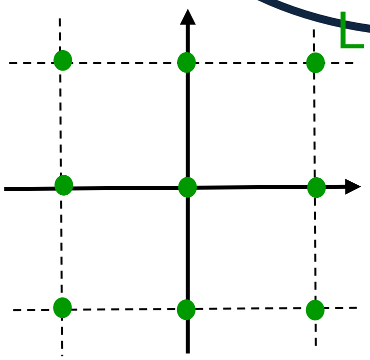


How do I construct this symbolic model ?

Construction of symbolic models

Consider the following parameters:

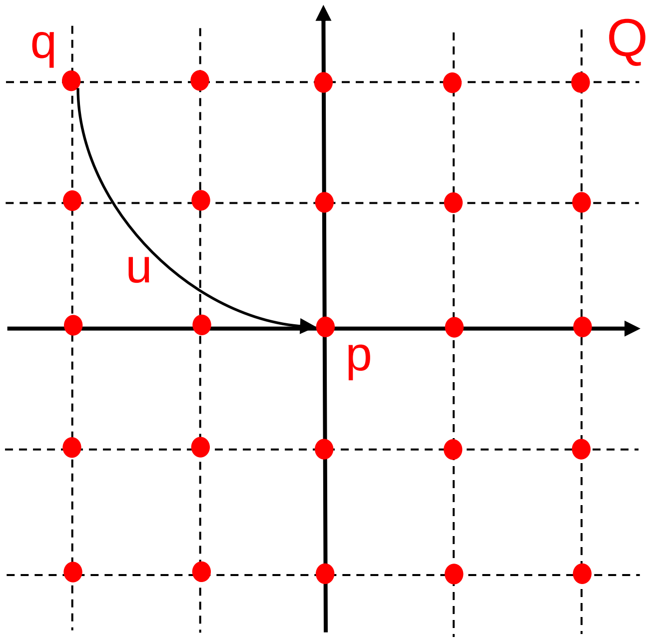
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization



and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

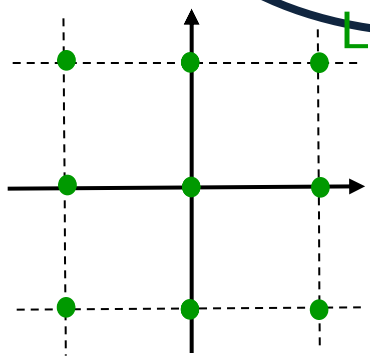
- $Q = [\mathbb{R}^n]_\eta = \eta\, \mathbb{Z}^n$
- $L = [\mathbb{R}^m]_\mu = \mu\, \mathbb{Z}^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = \mathbb{R}^n$
- H is the identity function



How do I construct this symbolic model ?

Construction of symbolic models

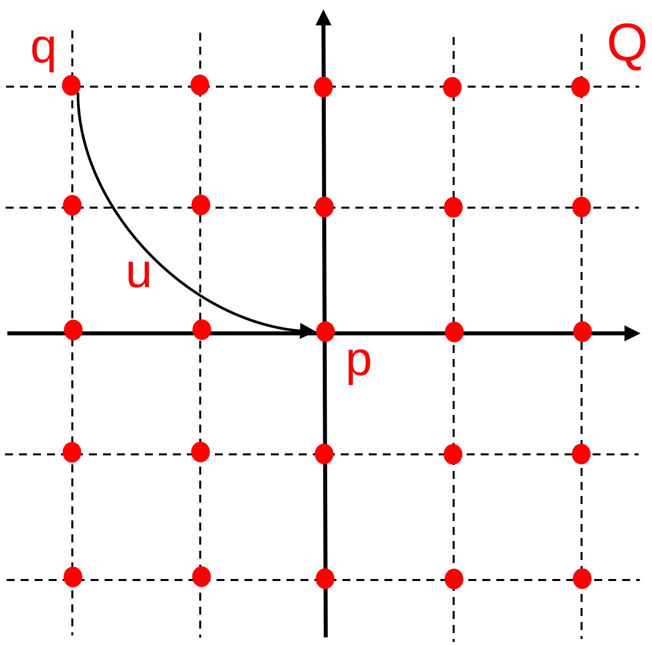
Consider the following parameters:



- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:



- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

How do I construct this symbolic model ?

Construction of symbolic models

Consider the following parameters:

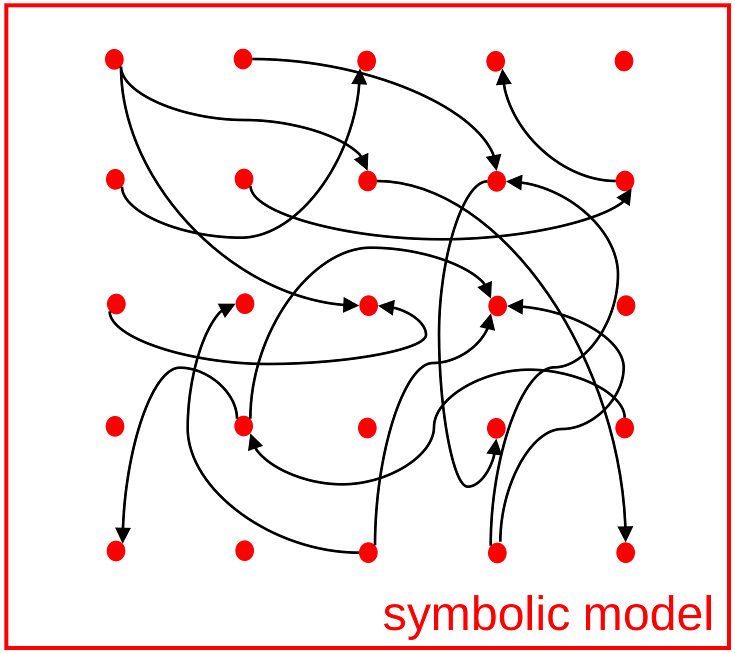
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization

and define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

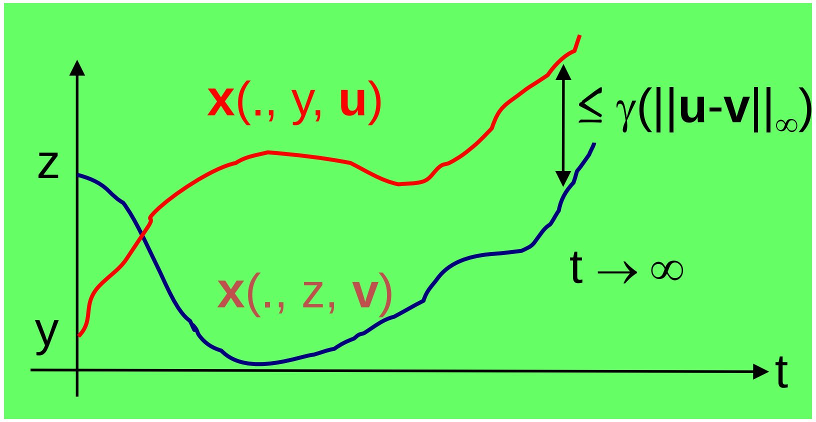
How do I construct this symbolic model ?



Incremental Input-State Stability

A control system $\dot{x} = f(x,u)$ is Incrementally Input-to-State Stable (δ-ISS) if there exist a KL function β and a K_∞ function γ so that for any $t \geq 0$, $y, z \in R^n$ and $\mathbf{u}$, $\mathbf{v}$

$$|| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) || \leq \beta(||y - z||, t) + \gamma(||\mathbf{u} - \mathbf{v}||_\infty)$$



Further details in D. Angeli, A Lyapunov approach to incremental stability properties, IEEE-TAC 02

Incremental Input-State Stability

A control system $\dot{x} = f(x,u)$ is Incrementally Input-to-State Stable (δ-ISS) if there exist a KL function $\boldsymbol{\beta}$ and a K_∞ function γ so that for any $t \geq 0$, $y, z \in R^n$ and **u**, **v**

$$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \boldsymbol{\beta}(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty)$$

Theorem:

A control system $\dot{x} = f(x,u)$ is δ-ISS if there exists a smooth function $V : R^n \times R^n \rightarrow R^+$ and K_∞ functions α_1, α_2, ρ, σ such that:

i) $\alpha_1 (\|x - y\|) \leq V(x, y) \leq \alpha_2 (\|x - y\|)$ for all $x,y \in R^n$

ii) $dV/dx\, f(x,u) + dV/dy\, f(y,v) < - \rho (\|x - y\|) + \sigma (\|u - v\|)$ for all $x,y \in R^n$ and $u,v \in R^m$

Further details from D. Angeli, A Lyapunov approach to incremental stability properties, IEEE-TAC 02

Construction of symbolic models

Theorem Consider a nonlinear digital control system Σ

$$\dot{x} = f(x,u), \quad x \in R^n,\ u \in R^m$$

If Σ is δ-ISS then for any desired precision $\varepsilon > 0$ and for any $\tau, \eta, \mu > 0$ satisfying

$$\beta(\varepsilon,\tau) + \eta / 2 + \gamma(\mu) \leq \varepsilon$$

The labelled transition systems $T^*_{\tau}(\Sigma)$ and $T_{\tau,\eta,\mu}(\Sigma)$ are approximately bisimilar with precision ε.

Construction of symbolic models

Theorem 5.1. *Consider a control system Σ and any desired precision $\varepsilon \in \mathbb{R}^+$. If Σ is δ-ISS then for any $\tau \in \mathbb{R}^+$, $\eta \in \mathbb{R}^+$, and $\mu \in \mathbb{R}^+$ satisfying the following inequality:*

$$\beta(\varepsilon, \tau) + \gamma(\mu) + \eta/2 \le \varepsilon, \tag{17}$$

the transition system $T_{\mathcal{U}_\tau}(\Sigma)$ is ε-bisimilar to $T_{\tau,\eta,\mu}(\Sigma)$.

Before giving the proof of this result we point out that, analogously to condition (8) of Theorem 4.1, there always exist parameters $\tau \in \mathbb{R}^+$, $\eta \in \mathbb{R}^+$, and $\mu \in \mathbb{R}^+$ satisfying condition (17).

Proof. Consider the relation $R \subseteq Q_1 \times Q_2$ defined by $(x, q) \in R$ if and only if $\|x - q\| \le \varepsilon$. By construction $R(Q_1) = Q_2$; since $Q_1 \subseteq \bigcup_{q_2 \in Q_2} \mathcal{B}_{\eta/2}(q_2)$ and by (17), $\eta/2 < \varepsilon$, we have that $R^{-1}(Q_2) = Q_1$. We now show that R is an ε-approximate bisimulation relation between $T_{\mathcal{U}_\tau}(\Sigma)$ and $T_{\tau,\eta,\mu}(\Sigma)$. Consider any $(x, q) \in R$. Condition (i) in Definition 3.2 is satisfied by the definition of R. Let us now show that condition (ii) in Definition 3.2 holds. Consider any $l_1 \in L_1$ and the transition $x \xrightarrow[1]{l_1} y$ in $T_{\mathcal{U}_\tau}(\Sigma)$. Consider a label $l_2 \in L_2$ such that:

$$\|l_1 - l_2\| \le \mu, \tag{18}$$

and set $z = \mathbf{x}(\tau, q, l_2)$. (Notice that such label $l_2 \in L_2$ exists because the assumptions on U make $L_2 = [L_1]_\mu$ non-empty.) For later use notice that since l_1 and l_2 are constant functions, then $\|l_1 - l_2\| = \|l_1 - l_2\|_\infty$. Since $Q_1 \subseteq \bigcup_{q_2 \in [\mathbb{R}^n]_\eta} \mathcal{B}_{\eta/2}(q_2)$, there exists $p \in Q_2$ such that:

$$\|z - p\| \le \eta/2, \tag{19}$$

and therefore $q \xrightarrow[2]{l_2} p$ in $T_{\tau,\eta,\mu}(\Sigma)$. Since Σ is δ-ISS and by (18), (19) and (17), the following chain of inequalities holds:

$$\begin{aligned} \|y - p\| &= \|y - z + z - p\| \le \|y - z\| + \|z - p\| \\ &\le \beta(\|x - q\|, \tau) + \gamma(\|l_1 - l_2\|_\infty) + \eta/2 \\ &\le \beta(\varepsilon, \tau) + \gamma(\mu) + \eta/2 \le \varepsilon. \end{aligned} \tag{20}$$

Hence $(y, p) \in R$ and condition (ii) in Definition 3.2 holds. We now show that also condition (iii) holds. Consider any $(x, q) \in R$, $l_2 \in L_2$ and the transition $q \xrightarrow[2]{l_2} p$ in $T_{\tau,\eta,\mu}(\Sigma)$. By definition of $T_{\tau,\eta,\mu}(\Sigma)$

$$\|z - p\| \le \eta/2, \tag{21}$$

where $z = \mathbf{x}(\tau, q, l_2) \in Q_1$. Choose $l_1 = l_2 \in L_1$ and consider now the transition $x \xrightarrow[1]{l_1} y$ in $T_{\mathcal{U}_\tau}(\Sigma)$. Since Σ is δ-ISS and by (21) and (17), the chain of inequalities in (20) holds. Thus $(y, p) \in R$, which completes the proof. ■

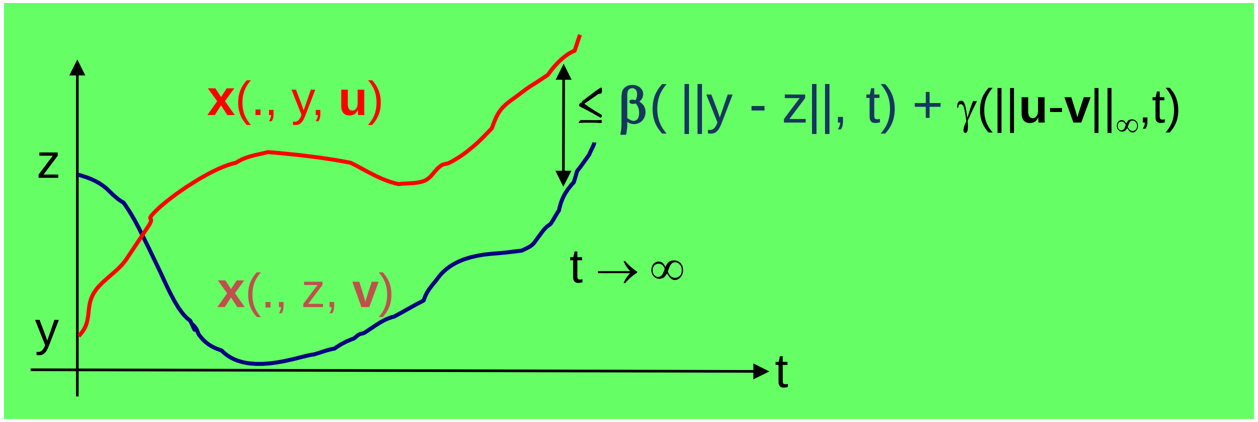
… taken from:

G. Pola, A. Girard, P. Tabuada
Approximately bisimilar symbolic models
for nonlinear control systrenms
Automatica 44 (2008) 2508-2516

Dealing with unstable systems

A control system $\dot{x} = f(x,u)$ is Incrementally Forward Complete (δ-FC) if it is forward complete and there exist continuous functions β and γ such that $\beta(.,s)$ and $\gamma(.,s)$ are K_∞ functions for any $s \in R^+$, and for any $t \geq 0$, for any $y, z \in R^n$ and any **u**, **v**, the following condition is satisfied:

$$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \beta(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty ,t)$$



Further details in Zamani et al., Symbolic Models for Nonlinear Control Systems Without Stability Assumptions, IEEE TAC 12.

Dealing with unstable systems

A control system $\dot{x} = f(x,u)$ is Incrementally Forward Complete (δ-FC) if it is forward complete and there exist continuous functions β and γ such that $\beta(.,s)$ and $\gamma(.,s)$ are K_∞ functions for any $s \in R^+$, and for any $t \geq 0$, for any y, $z \in R^n$ and any **u**, **v**, the following condition is satisfied:

$$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \beta(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty ,t)$$

Properties

- Incremental FC requires the distance between two arbitrary trajectories to be bounded by a continuous function that captures the mismatch between initial conditions and control inputs.
- The class of delta-FC control systems is quite large and includes unstable linear systems.
- Any linear system is delta-FC
- δ-FC is implied by δ-ISS

Further details in Zamani et al., Symbolic Models for Nonlinear Control Systems Without Stability Assumptions, IEEE TAC 12.

Bisimulation equivalence

Given $T_1 = (Q_1, L_1, \longrightarrow_1, O_1, H_1)$ and $T_2 = (Q_2, L_2, \longrightarrow_2, O_2, H_2)$ with $O_1 = O_2$, a relation

$$R \subseteq Q_1 \times Q_2$$

is a ***bisimulation relation*** between T_1 and T_2 if for all $(q_1, q_2) \in R$

- $H_1(q_1) = H_2(q_2)$
- $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 implies existence of $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 so that $(p_1, p_2) \in R$
- $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 implies existence of $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 so that $(p_1, p_2) \in R$

LTSs T_1 and T_2 are ***bisimilar*** if $\pi|_{Q_1}(R) = Q_1$ and $\pi|_{Q_2}(R) = Q_2$

Approximate bisimulation equivalence

Given $T_1 = (Q_1, L_1, \longrightarrow_1, O_1, H_1)$ and $T_2 = (Q_2, L_2, \longrightarrow_2, O_2, H_2)$ with $O_1 = O_2$, and a precision $\varepsilon > 0$, a relation

$$R \subseteq Q_1 \times Q_2$$

is an ***approximate bisimulation relation*** between T_1 and T_2 if for all $(q_1, q_2) \in R$

- $\cancel{H_1(q_1) = H_2(q_2)}$ $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$
- $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 implies existence of $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 so that $(p_1, p_2) \in R$
- $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 implies existence of $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 so that $(p_1, p_2) \in R$

LTSs T_1 and T_2 are ***bisimilar with precision*** ε if $\pi|_{Q_1}(R) = Q_1$ and $\pi|_{Q_2}(R) = Q_2$

We here consider a modified version of bisimulation where outputs need not to coincide but to be close, up to a given precision ε

… is approximate bisimulation equivalence an equivalence relation?

Approximate bisimulation equivalence

Given $T_1 = (Q_1, L_1, \longrightarrow_1, O_1, H_1)$ and $T_2 = (Q_2, L_2, \longrightarrow_2, O_2, H_2)$ with $O_1 = O_2$, and a precision $\varepsilon > 0$, a relation

$$R \subseteq Q_1 \times Q_2$$

is an ***approximate bisimulation relation*** between T_1 and T_2 if for all $(q_1, q_2) \in R$

- $d(\ H_1(q_1), H_2(q_2)\ ) \leq \varepsilon$
- $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 implies existence of $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 so that $(p_1, p_2) \in R$
- $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 implies existence of $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 so that $(p_1, p_2) \in R$

LTSs T_1 and T_2 are ***ε-bisimilar*** if $\pi|_{Q_1}(R) = Q_1$ and $\pi|_{Q_2}(R) = Q_2$

Drawback: **in the presence of non-determinism, this notion can be shown not to capture correctly the robustness requirement of control strategies!**

Alternating approximate bisimulation

Given $T_1 = (Q_1, L_1, \longrightarrow_1, O_1, H_1)$ and $T_2 = (Q_2, L_2, \longrightarrow_2, O_2, H_2)$ with $O_1 = O_2$, and a precision $\varepsilon > 0$, a relation

$$R \subseteq Q_1 \times Q_2$$

is an alternating **approximate bisimulation relation** between T_1 and T_2 if for all $(q_1, q_2) \in R$

- $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$
- for any $l_1 \in L_1$, there exists $l_2 \in L_2$ s.t. the existence of $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 implies the existence of $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 with $(p_1, p_2) \in R$
- for any $l_2 \in L_2$, there exists $l_1 \in L_1$ s.t. the existence of $q_1 \xrightarrow{l_1}_1 p_1$ in T_1 implies the existence of $q_2 \xrightarrow{l_2}_2 p_2$ in T_2 with $(p_1, p_2) \in R$

LTSs T_1 and T_2 are ***AεA-bisimilar*** if $\pi|_{Q_1}(R) = Q_1$ and $\pi|_{Q_2}(R) = Q_2$

From [Alur et al., 1998] symbolic control strategies designed for S_1 can be appropriately transferred to S_2 if the systems are AεA-bisimilar

Symbolic models for δ-FC control systems

Consider the following parameters:

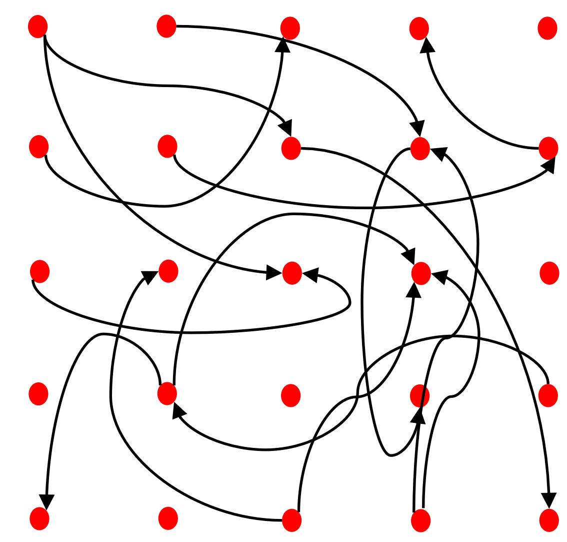
- $\tau > 0$ sampling time
- $\eta > 0$ state space quantization
- $\mu > 0$ input space quantization
- $\theta > 0$ a design parameter

and define $T_{\tau,\eta,\mu,\theta}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $||x(\tau,q,u)-p|| \leq \beta(\theta,\tau) + \gamma(\mu,\tau) + \eta$
- $O = R^n$
- H is the identity function

How do I construct this symbolic model ?



symbolic model

Theorem Consider a nonlinear digital control system Σ

$$\dot{x} = f(x,u), \quad x \in R^n,\ u \in R^m$$

If Σ is δ-FC then for any desired precision $\varepsilon > 0$ and for any $\tau, \eta, \mu, \theta > 0$ satisfying

$$\eta \leq \varepsilon \leq \theta$$

one has:

$$T_{\tau,\eta,\mu,\theta}(\Sigma) \preccurlyeq_{\varepsilon} T^*_{\tau}(\Sigma) \preccurlyeq_{\varepsilon}^{alt} T_{\tau,\eta,\mu,\theta}(\Sigma)$$

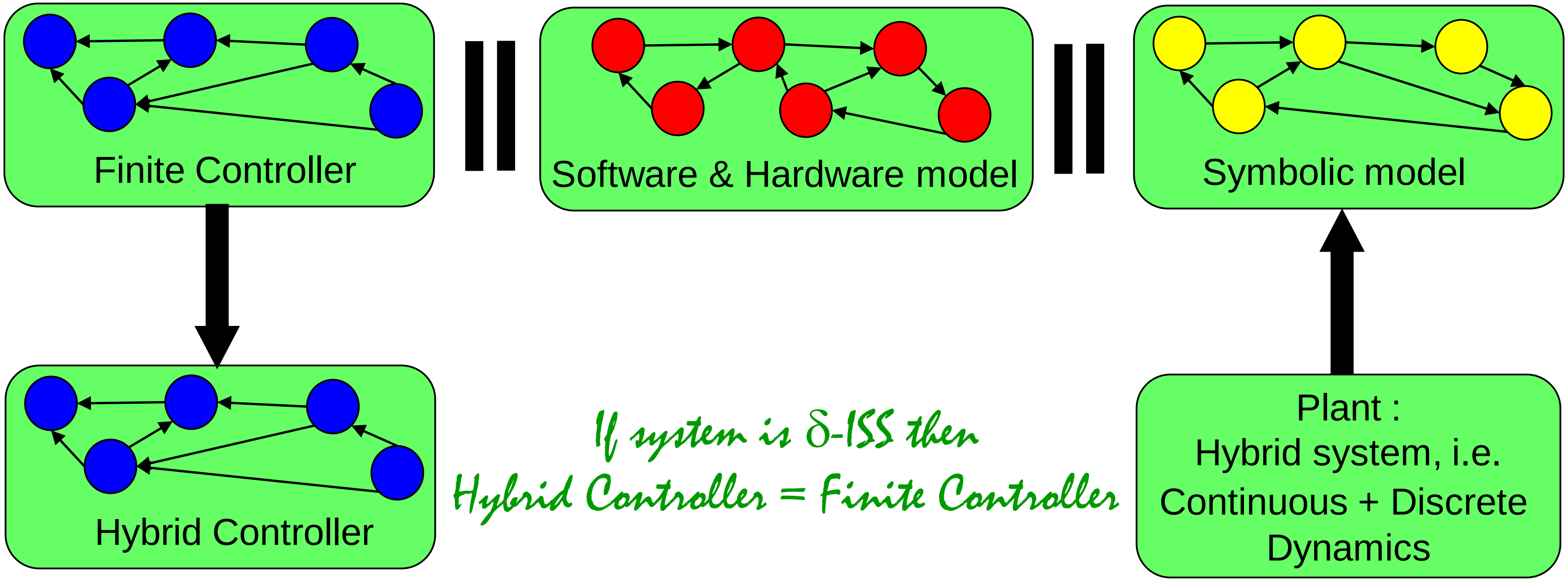
Remark

The previous result implies that any controller synthesized for the finite model $T_{\tau,\eta,\mu,\theta}(\Sigma)$ can be refined to a controller enforcing the same specification on $T^*_{\tau}(\Sigma)$.

Correct-by-Design Embedded Control Software

Synthesis through a three phase process:

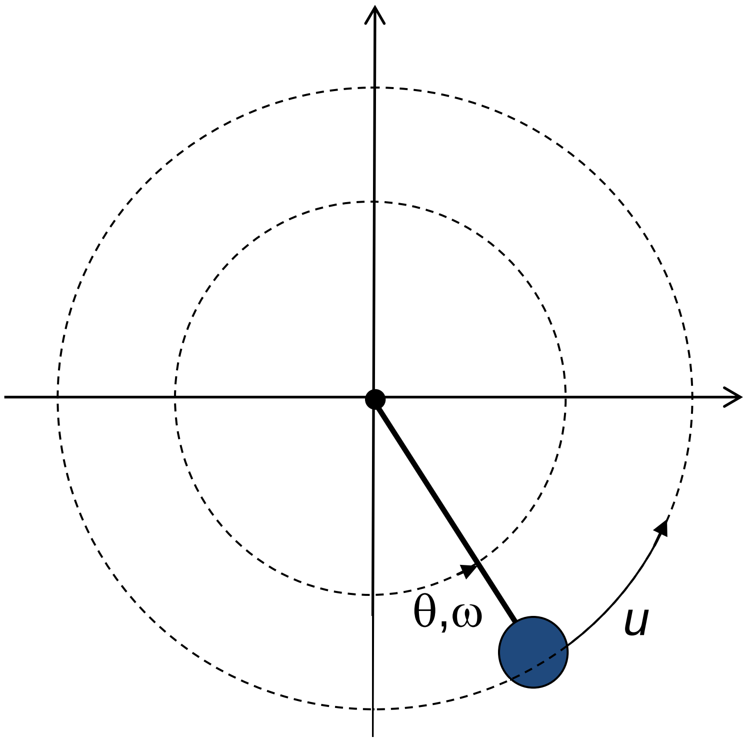
1. Construct the finite model T of the plant system Σ
2. Synthesize a finite controller C solving the specification S on T
3. Synthesize a controller C' for Σ on the basis of C



Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$



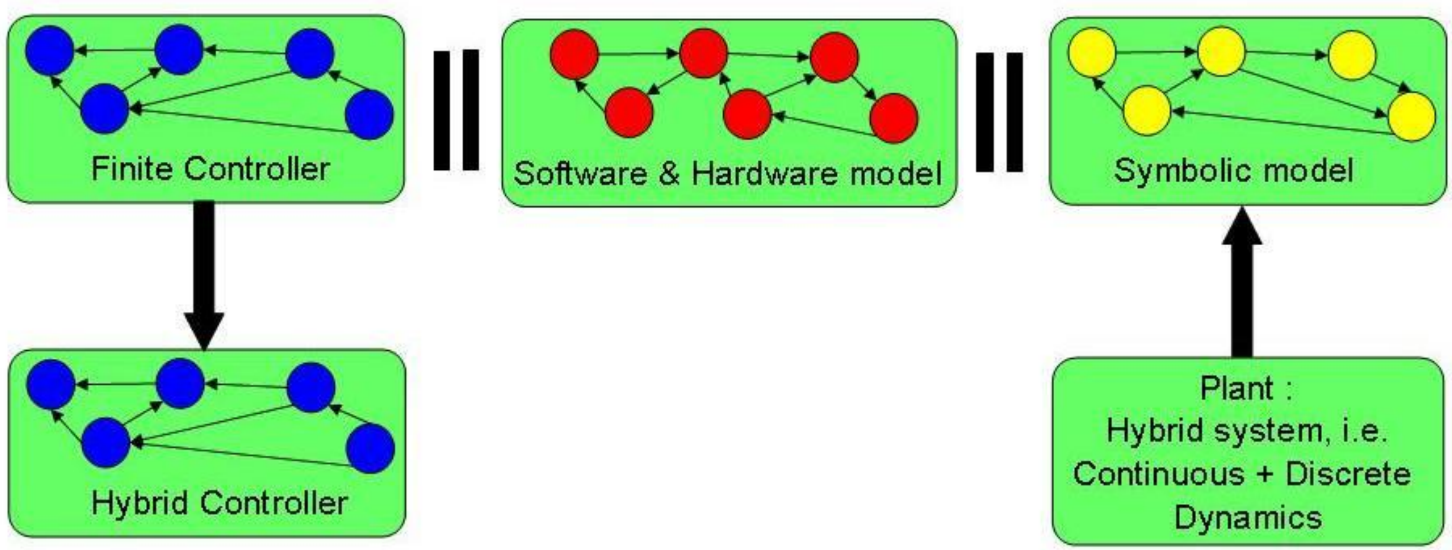
We suppose:

- $g = 9.8$, $l = 5$, $m = 0.5$, $k = 3$
- $u \in U = [-1.5, 1.5]$
- Control signals are piecewise constant
- $(\theta, \omega) \in X = [-1,1] \times [-1,1]$

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

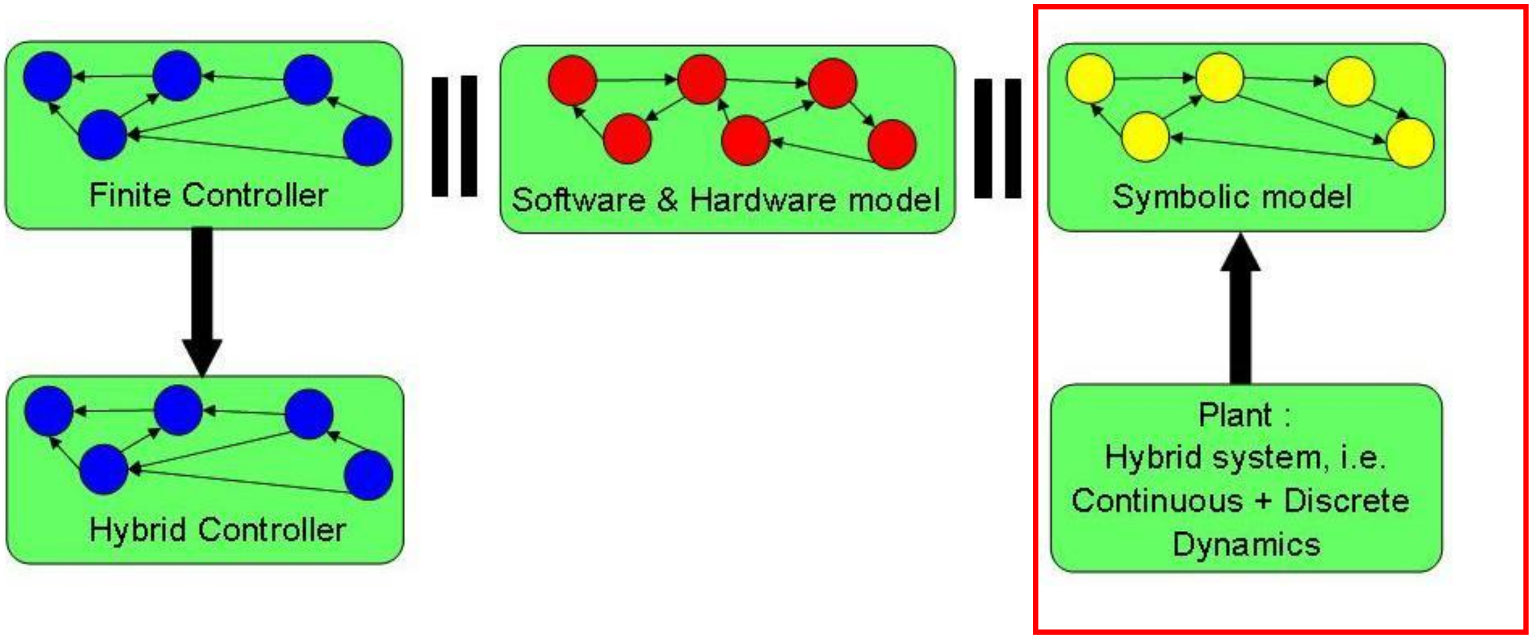
$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$



Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$



Example 1: pendulum

Let us construct a symbolic model for the pendulum control system:

- Check δ-ISS property (directly or by Lyapunov functions)
- Find functions β and γ functions which satisfy

> A control system $\dot{x} = f(x,u)$ is
> ***incrementally input-to-state stable*** (δ-ISS)
> if there exist a KL function β and a K_∞ function γ
> so that for any $t \geq 0$, $y, z \in R^n$ and $\mathbf{u}, \mathbf{v}$
>
> $$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \beta(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty)$$

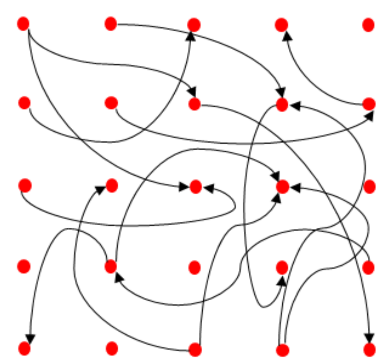
- Choose parameters $\varepsilon, \tau, \eta, \mu$
- Construct the symbolic model

define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

How do I construct this symbolic model ?



symbolic model

Example 1: pendulum

Let us construct a symbolic model for the pendulum control system:

- Check δ-ISS property (directly or by Lyapunov functions)

$$V(x,y) = \frac{1}{2}(x-y)' \begin{bmatrix} \frac{1}{2}\left(\frac{k}{m}\right)^2 & \frac{1}{2}\frac{k}{m} \\ \frac{1}{2}\frac{k}{m} & 1 \end{bmatrix} (x-y).$$

It is possible to show that V satisfies condition (i) of Definition 2.4 with $\alpha_1(r) = 0.49\, r^2$ and $\alpha_2(r) = 18.51\, r^2$. Moreover, by defining for any $z_1, z_2 \in \mathbb{R}$,

$$\zeta(z_1, z_2) = (\sin(z_1) - \sin(z_2))/(z_1 - z_2),$$

one obtains $\zeta_{\min} = \min_{z_1,z_2\in[-1,1]} \zeta(z_1,z_2) = 0.84$ and $\zeta_{\max} = \max_{z_1,z_2\in[-1,1]} \zeta(z_1,z_2) = 1$ and hence:

$$\begin{aligned} \frac{\partial V}{\partial x} f(x,u) + \frac{\partial V}{\partial y} f(y,v) &= -\frac{1}{2}\frac{k}{m}\frac{g}{l}\zeta(x_1,y_1)(x_1-y_1)^2 \\ &\quad - \frac{g}{l}\zeta(x_1,y_1)(x_1-y_1)(x_2-y_2) - \frac{1}{2}\frac{k}{m}(x_2-y_2)^2 \\ &\quad + \left(\frac{1}{2}\frac{k}{m}(x_1-y_1) + x_2 - y_2\right)(u-v) \\ &\le -\frac{1}{2} a \|x-y\|_2^2 + b|u-v|, \qquad (23) \end{aligned}$$

... pendulum is δ-ISS !

Example 1: pendulum

Let us construct a symbolic model for the pendulum control system:

- Check δ-ISS property (directly or by Lyapunov functions)
- Find functions β and γ functions which satisfy

A control system $\dot{x} = f(x,u)$ is ***incrementally input-to-state stable*** (δ-ISS) if there exist a KL function β and a K_∞ function γ so that for any $t \geq 0$, $y, z \in R^n$ and $\mathbf{u}$, $\mathbf{v}$

$$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \beta(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty)$$

Using inequality (23), the definition of V and the comparison lemma (Khalil, 1996), it is possible to show that for any $x, y \in X$, any $\mathbf{u}, \mathbf{v} \in \mathcal{U}$ and any time $t \in \mathbb{R}_0^+$:

$$\|\mathbf{x}(t, x, \mathbf{u}) - \mathbf{x}(t, y, \mathbf{v})\| \leq \beta(\|x - y\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty),$$

where $\beta(r, s) := 6.17\, e^{-2.08\, s} r$ and $\gamma(r) := \sqrt{3.96\, r}$ for any $r, s \in \mathbb{R}$.

Example 1: pendulum

Let us construct a symbolic model for the pendulum control system:

- Check δ-ISS property (directly or by Lyapunov functions)
- Find functions β and γ functions which satisfy

> A control system $\dot{x} = f(x,u)$ is
> ***incrementally input-to-state stable*** (δ-ISS)
> if there exist a KL function β and a K_∞ function γ
> so that for any $t \geq 0$, $y, z \in R^n$ and $\mathbf{u}$, $\mathbf{v}$
>
> $$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \beta(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty)$$

- Choose parameters ε, τ, η, μ

$$6.17 e^{-2.08\tau} \varepsilon + \sqrt{3.96\mu} + \eta / 2 \leq \varepsilon$$

a possible choice is $\varepsilon = 0.25$, $\tau = 2$, $\eta = 0.4$, $\mu = 1.5\ 10^{-4}$

Example 1: pendulum

Let us construct a symbolic model for the pendulum control system:

- Check δ-ISS property (directly or by Lyapunov functions)
- Find functions β and γ functions which satisfy

A control system $\dot{x} = f(x,u)$ is ***incrementally input-to-state stable*** (δ-ISS) if there exist a KL function β and a K_∞ function γ so that for any $t \geq 0$, $y, z \in R^n$ and $\mathbf{u}$, $\mathbf{v}$

$$\| \mathbf{x}(t,y,\mathbf{u}) - \mathbf{x}(t,z,\mathbf{v}) \| \leq \beta(\|y - z\|, t) + \gamma(\|\mathbf{u} - \mathbf{v}\|_\infty)$$

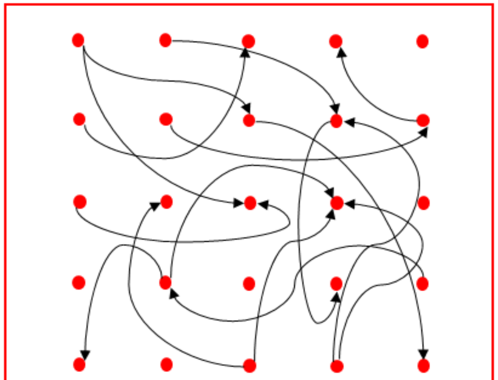
- Choose parameters ε, τ, η, μ
- Construct the symbolic model

define $T_{\tau,\eta,\mu}(\Sigma) = (Q, L, \longrightarrow, O, H)$

where:

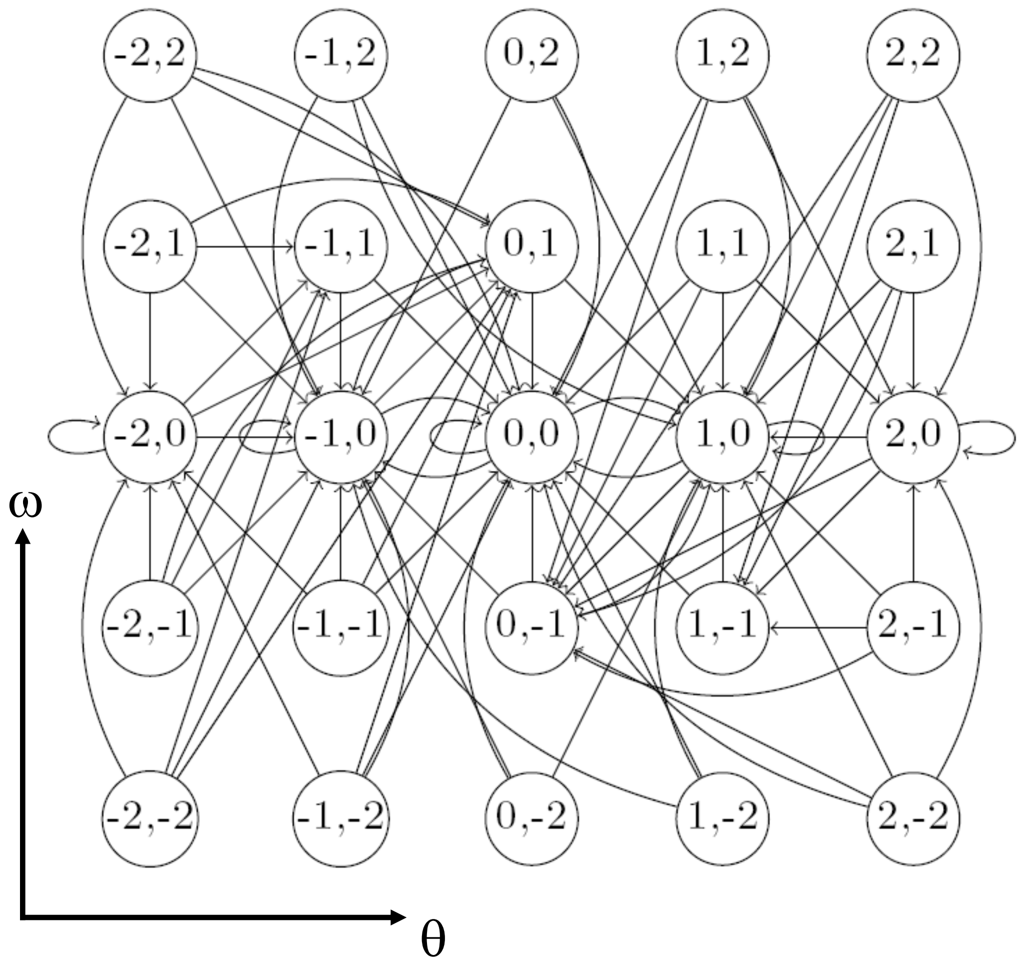
- $Q = [R^n]_\eta = \eta Z^n$
- $L = [R^m]_\mu = \mu Z^m$
- $q \xrightarrow{u} p$, if $x(\tau,q,u) \in \mathcal{B}_{[\eta/2[}(p)$
- $O = R^n$
- H is the identity function

How do I construct this symbolic model ?



Example 1: pendulum

The obtained symbolic model is:

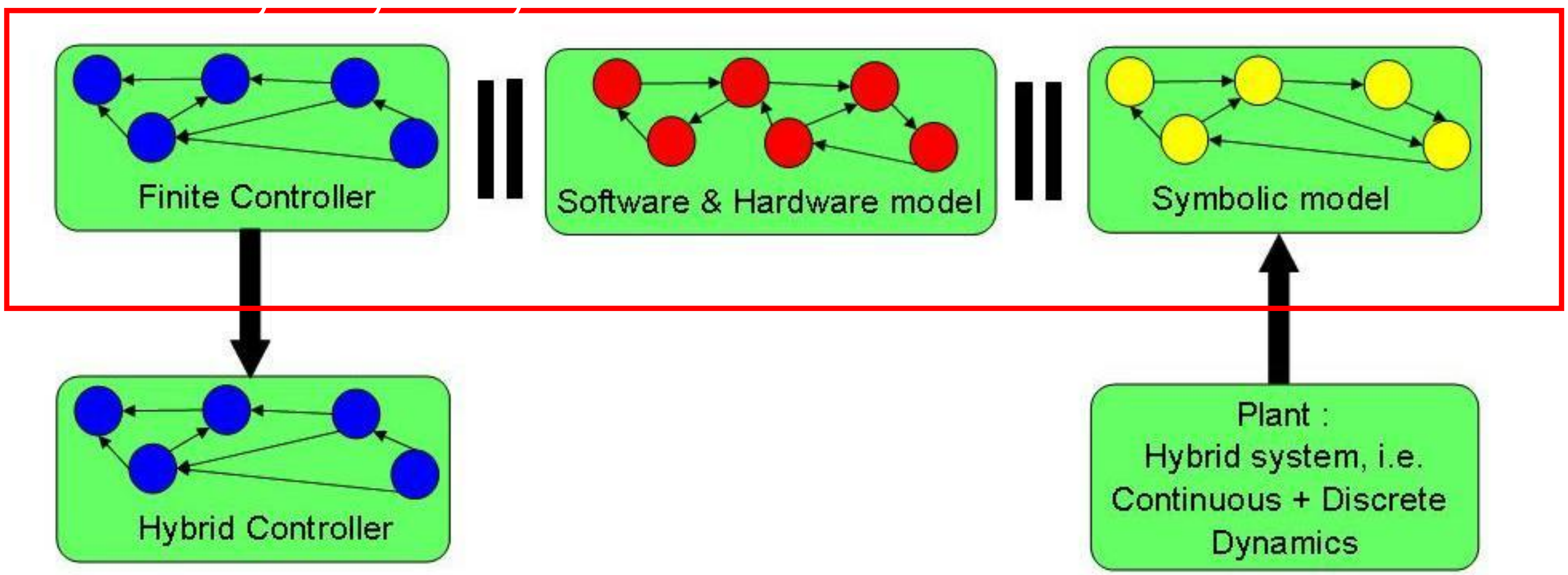


where discrete states (η i, η j) have been labelled by (i, j)

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$



Example 1: pendulum

Let us use the symbolic model for controller synthesis:

Consider a specification given by the concatenation of tasks P_1 and P_2 as follows:

$$P_1, P_1, P_2, P_1, P_1$$

where:

- P_1 requires a periodic orbit from $(\theta, \omega) = (-1, 0)$ to $(0, 0)$
- P_2 requires a periodic orbit from $(\theta, \omega) = (-1, 0)$ to $(1, 0)$

Example 1: pendulum

Let us use the symbolic model for controller synthesis:

Consider a specification given by the concatenation of tasks P_1 and P_2 as follows:

$$P_1, P_1, P_2, P_1, P_1$$

where:

- P_1 requires a periodic orbit from $(\theta, \omega) = (-1, 0)$ to $(0, 0)$
- P_2 requires a periodic orbit from $(\theta, \omega) = (-1, 0)$ to $(1, 0)$

This type of specification is a paradigm for illustrating more complex controller synthesis problems where a task is given by the coordination of smaller tasks.

Example 1: pendulum

Let us use the symbolic model for controller synthesis:

Consider a specification given by the concatenation of tasks P_1 and P_2 as follows:

$$P_1, P_1, P_2, P_1, P_1$$

where:

- P_1 requires a periodic orbit from $(\theta, \omega) = (-1, 0)$ to $(0, 0)$
- P_2 requires a periodic orbit from $(\theta, \omega) = (-1, 0)$ to $(1, 0)$

This type of specification is a paradigm for illustrating more complex controller synthesis problems where a task is given by the coordination of smaller tasks.

Any digital controller enforcing P_1, P_1, P_2, P_1, P_1 in system Σ will result in a hybrid system combining the discrete memory, needed to describe the current task, with the continuous control law enforcing the specification in each task.

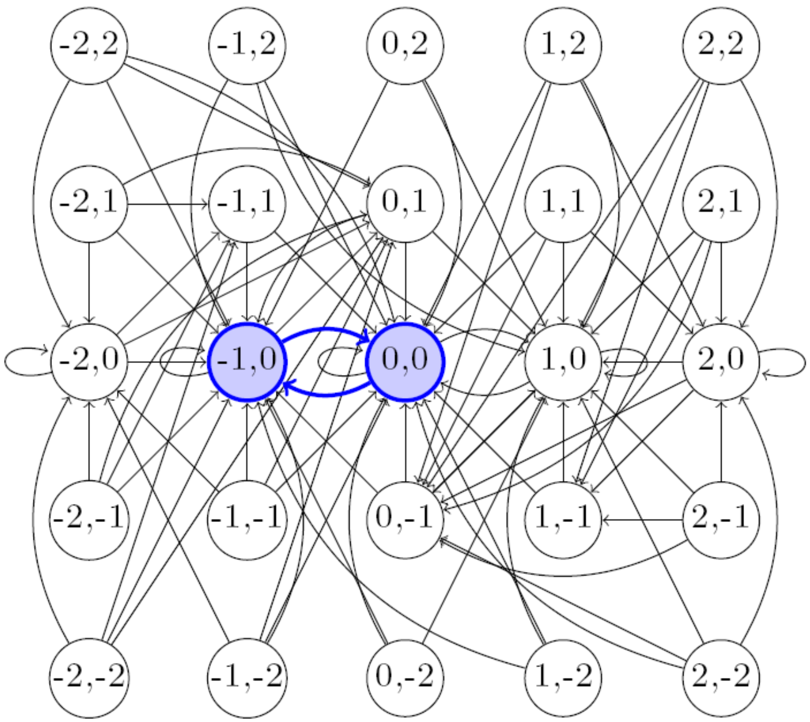
Example 1: pendulum

By exploiting the symbolic model:

One obtains:

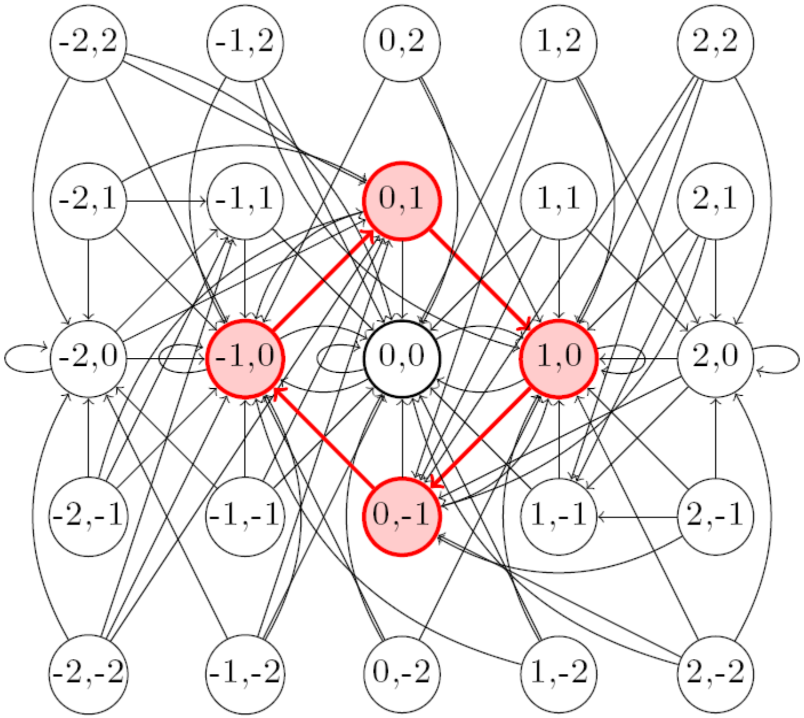
- Specification P_1:

$(-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0)$



Example 1: pendulum

By exploiting the symbolic model:



One obtains:

- Specification P_1:

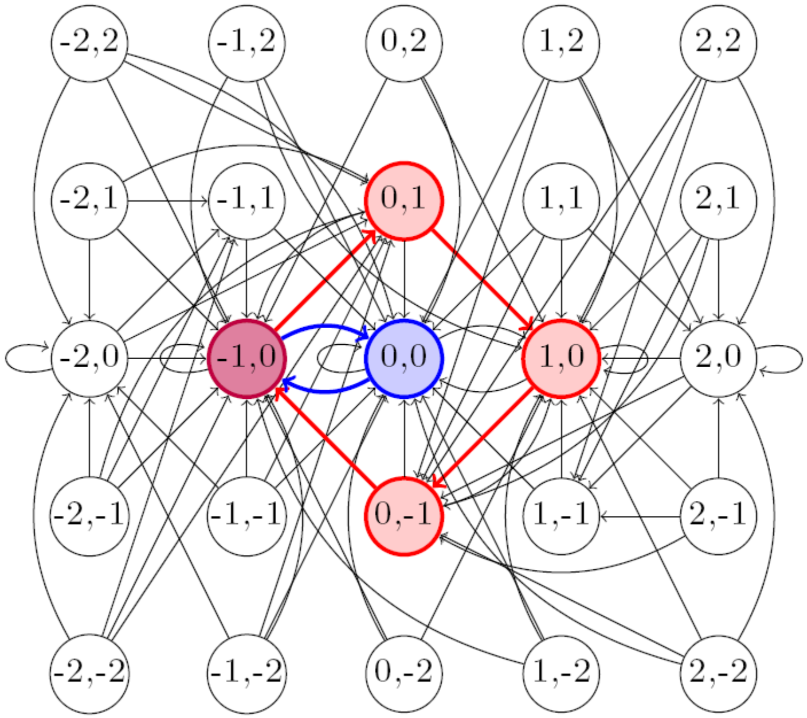
$(-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0)$

- Specification P_2:

$(-1,0) \xrightarrow{1.5} (0,1) \xrightarrow{1.5} (1,0) \xrightarrow{-1.5} (0,-1) \xrightarrow{-0.71} (-1,0)$

Example 1: pendulum

By exploiting the symbolic model:



One obtains:

- Specification P_1:

$(-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0)$

- Specification P_2:

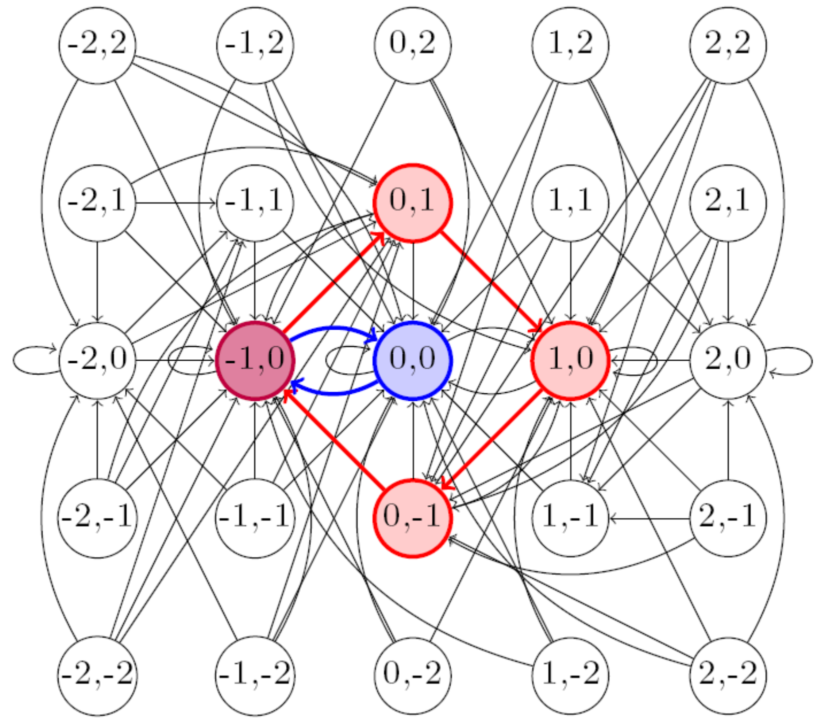
$(-1,0) \xrightarrow{1.5} (0,1) \xrightarrow{1.5} (1,0) \xrightarrow{-1.5} (0,-1) \xrightarrow{-0.71} (-1,0)$

- Overall specification:

$(-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0) \xrightarrow{1.5} (0,1) \xrightarrow{1.5} (1,0) \xrightarrow{-1.5} (0,-1)$
$\xrightarrow{-0.71} (-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0)$

Example 1: pendulum

By exploiting the symbolic model:



One obtains:

- Specification P_1:

$(-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0)$

- Specification P_2:

$(-1,0) \xrightarrow{1.5} (0,1) \xrightarrow{1.5} (1,0) \xrightarrow{-1.5} (0,-1) \xrightarrow{-0.71} (-1,0)$

- Overall specification:

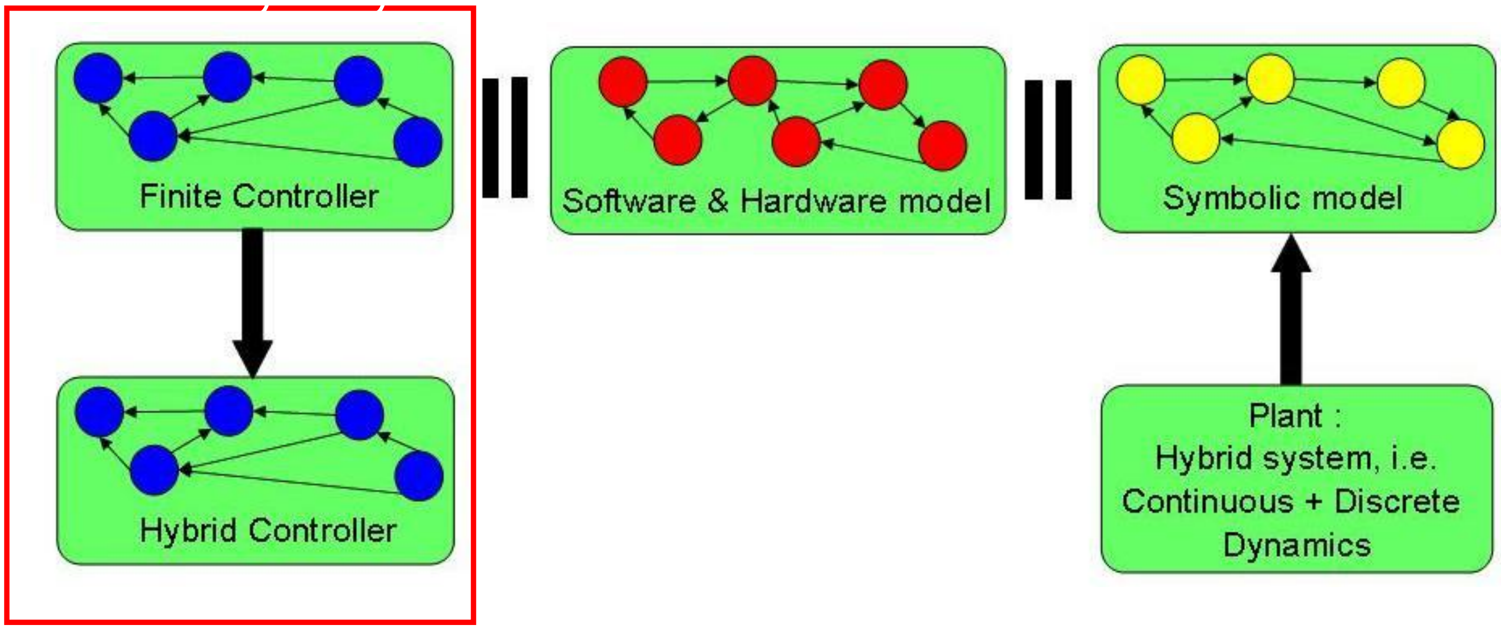
$(-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0) \xrightarrow{1.5} (0,1) \xrightarrow{1.5} (1,0) \xrightarrow{-1.5} (0,-1) \xrightarrow{-0.71} (-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0) \xrightarrow{1.38} (0,0) \xrightarrow{-1.5} (-1,0)$

What does it happen if I apply this control strategy to the original control system?

Example 1: pendulum

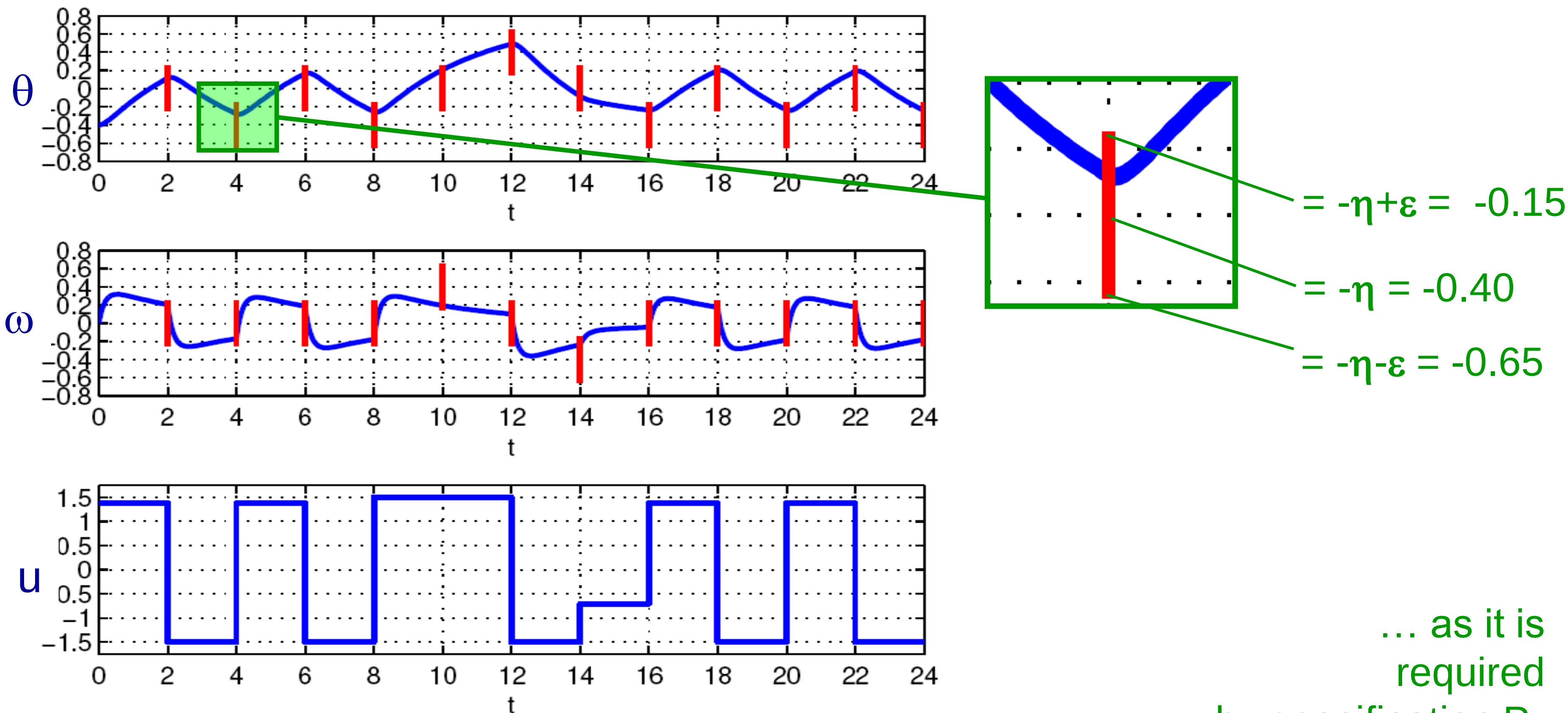
One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$



Example 1: pendulum

Let us apply the control strategy synthesized on the symbolic model $T_{\tau,\eta,\mu}(\Sigma)$ to the continuous system Σ:

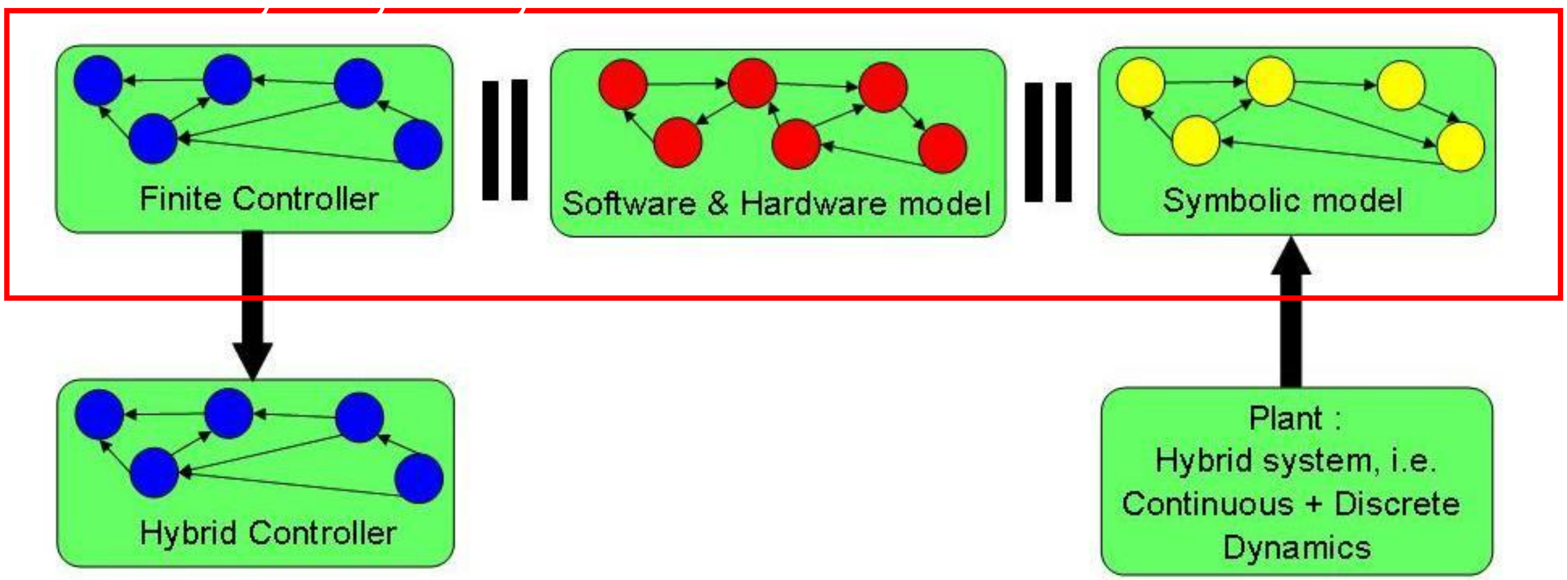


… as it is required by specification P_1 and precision **ε** **!**

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$



… traditional controller synthesis design?

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$

- Σ is feedback linearizable

… traditional controller synthesis design?

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$

- Σ is feedback linearizable
- I can choose two controllers u_1 and u_2 letting the (obtained linear) system satisfying tasks P_1 and P_2

… traditional controller synthesis design?

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$

- Σ is feedback linearizable
- I can choose two controllers u_1 and u_2 letting the (obtained linear) system satisfying tasks P_1 and P_2
- I can concatenate u_1 and u_2

… traditional controller synthesis design?

Example 1: pendulum

One of the simplest mechanical systems studied in the literature is the pendulum:

$$\Sigma : \begin{cases} \dot{\theta} = \omega \\ \dot{\omega} = -\dfrac{g}{l}\sin\theta - \dfrac{k}{m}\omega + \dfrac{1}{ml^2}u \end{cases}$$

- Σ is feedback linearizable
- I can choose two controllers u_1 and u_2 letting the (obtained linear) system satisfying tasks P_1 and P_2
- I can concatenate u_1 and u_2

Disadvantages:

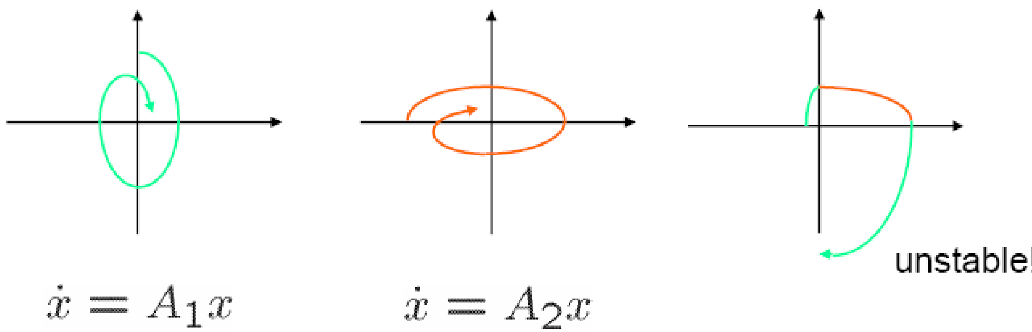
- Feedback linearization is not robust

… traditional controller synthesis design?

Example 1: pendulum

SWITCHING BETWEEN ASYMPTOTICALLY STABLE SYSTEMS

$$\boxed{\dot{x} = A_\sigma x}$$



Disadvantages:

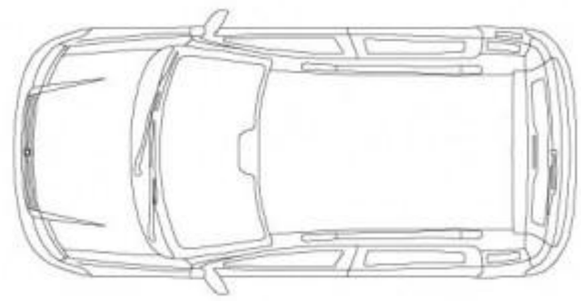
- Feedback linearization is not robust
- Dealing with stability of hybrid systems …

… traditional controller synthesis design?

Example 2: vehicle

A widely used model in the literature is the non-holonomic vehicle model:

$$\Sigma : \begin{cases} \dot{x} = v_0 \dfrac{\cos(\alpha+\theta)}{\cos(\alpha)} \\ \dot{y} = v_0 \dfrac{\sin(\alpha+\theta)}{\cos(\alpha)} \\ \dot{\theta} = \dfrac{v_0}{b} \tan(\delta) \end{cases}$$



with $\alpha = arctan(a \cdot \tan(\delta)/b)$.

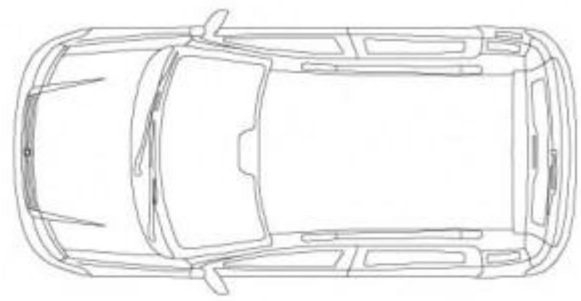
We suppose:

- a = 0.5, b = 1.
- u=(v_0, δ) $\in$ U = [-1,1] x [-1,1]
- Control signals are piecewise constant
- (θ, ω) $\in$ X = [-1,1] x [-1,1]

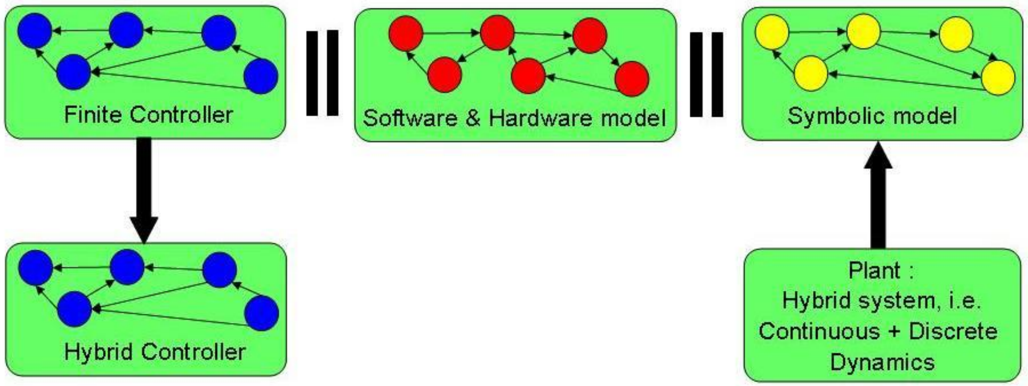
Example 2: vehicle

A widely used model in the literature is the non-holonomic vehicle model:

$$\Sigma : \begin{cases} \dot{x} = v_0 \dfrac{\cos(\alpha+\theta)}{\cos(\alpha)} \\ \dot{y} = v_0 \dfrac{\sin(\alpha+\theta)}{\cos(\alpha)} \\ \dot{\theta} = \dfrac{v_0}{b} \tan(\delta) \end{cases}$$



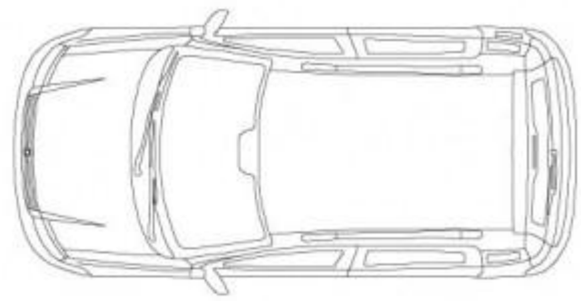
with $\alpha = arctan(a \cdot \tan(\delta)/b)$.



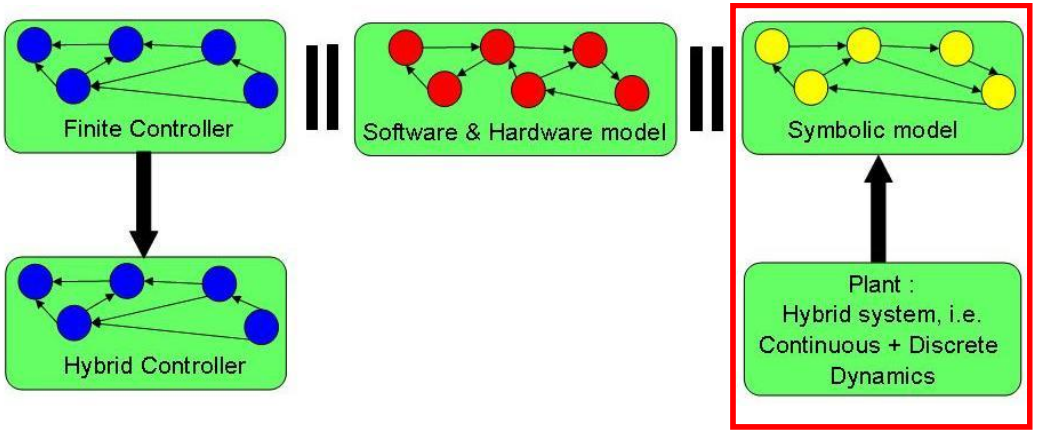
Example 2: vehicle

A widely used model in the literature is the non-holonomic vehicle model:

$$\Sigma : \begin{cases} \dot{x} = v_0 \dfrac{\cos(\alpha+\theta)}{\cos(\alpha)} \\ \dot{y} = v_0 \dfrac{\sin(\alpha+\theta)}{\cos(\alpha)} \\ \dot{\theta} = \dfrac{v_0}{b} \tan(\delta) \end{cases}$$



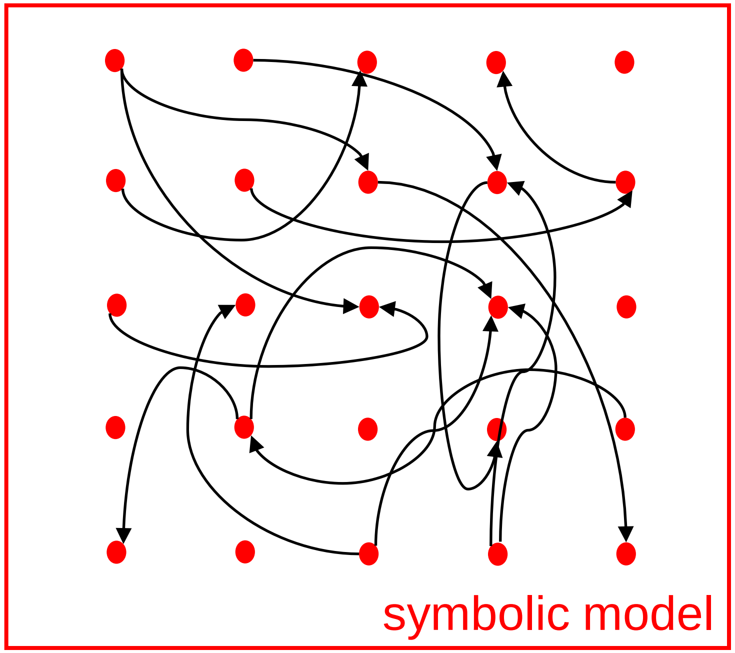
with $\alpha = arctan(a \cdot \tan(\delta)/b)$.



Example 2: vehicle

Let us construct a symbolic model for the vehicle control system:

- We check δ-FC property (the vehicle is not δ-ISS !)
- Find functions β and γ functions which satisfy the definition of δ-FC.
- Choose parameters ε, τ, η, μ, θ.
- Construct the symbolic model



Example 2: vehicle

Let us construct a symbolic model for the vehicle control system:

- We check δ-FC property (the vehicle is not δ-ISS !)
- Find functions β and γ functions which satisfy the definition of δ-FC.
- Choose parameters ε, τ, η, μ, θ.
- Construct the symbolic model

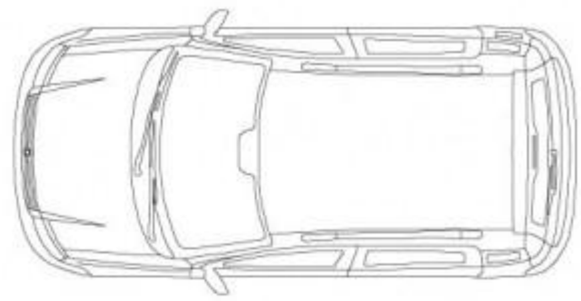
The system is δ-FC with $\beta(r,t) = 1 + 1.267t$

A possible choice is $\varepsilon = 0.2$, $\tau = 0.3$, $\eta = 0.2$, $\mu = 0.3$, $\theta = 0.2$

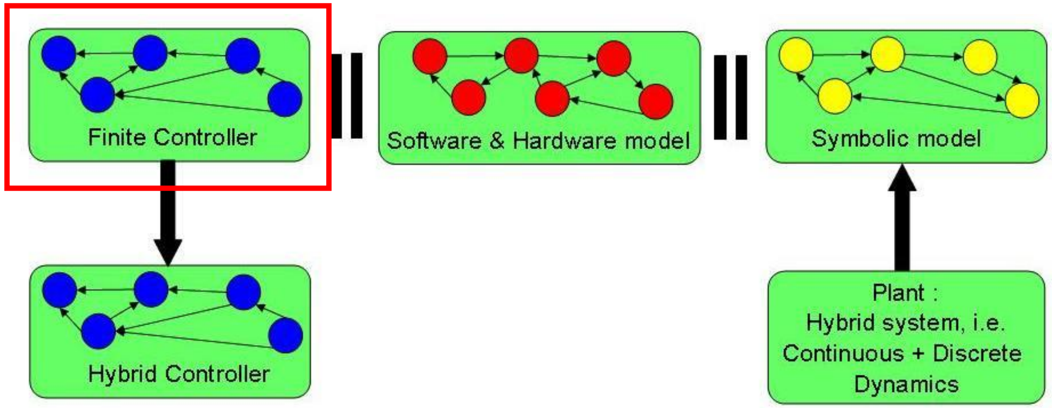
Example 2: vehicle

A widely used model in the literature is the non-holonomic vehicle model:

$$\Sigma : \begin{cases} \dot{x} = v_0 \dfrac{\cos(\alpha+\theta)}{\cos(\alpha)} \\ \dot{y} = v_0 \dfrac{\sin(\alpha+\theta)}{\cos(\alpha)} \\ \dot{\theta} = \dfrac{v_0}{b} \tan(\delta) \end{cases}$$



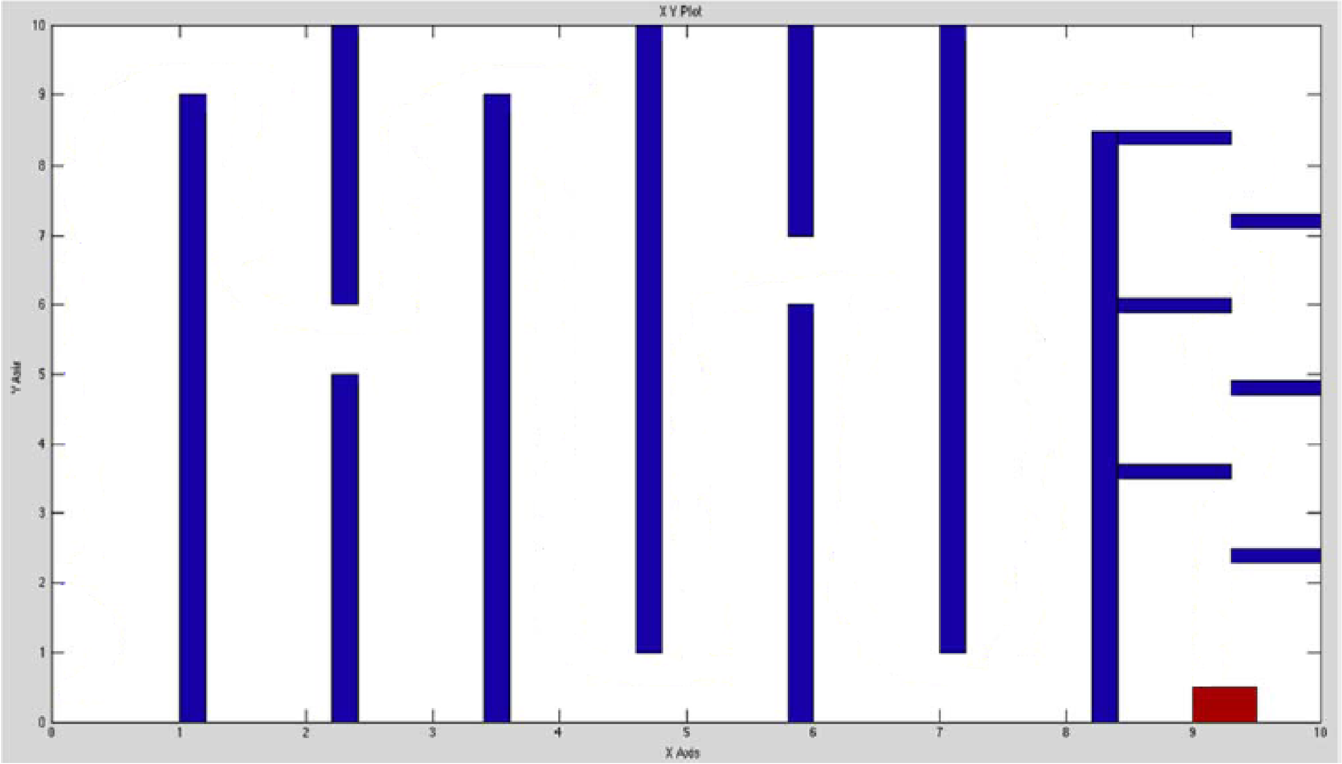
with $\alpha = arctan(a \cdot \tan(\delta)/b)$.



Example 2: vehicle

Let us use the symbolic model for controller synthesis:

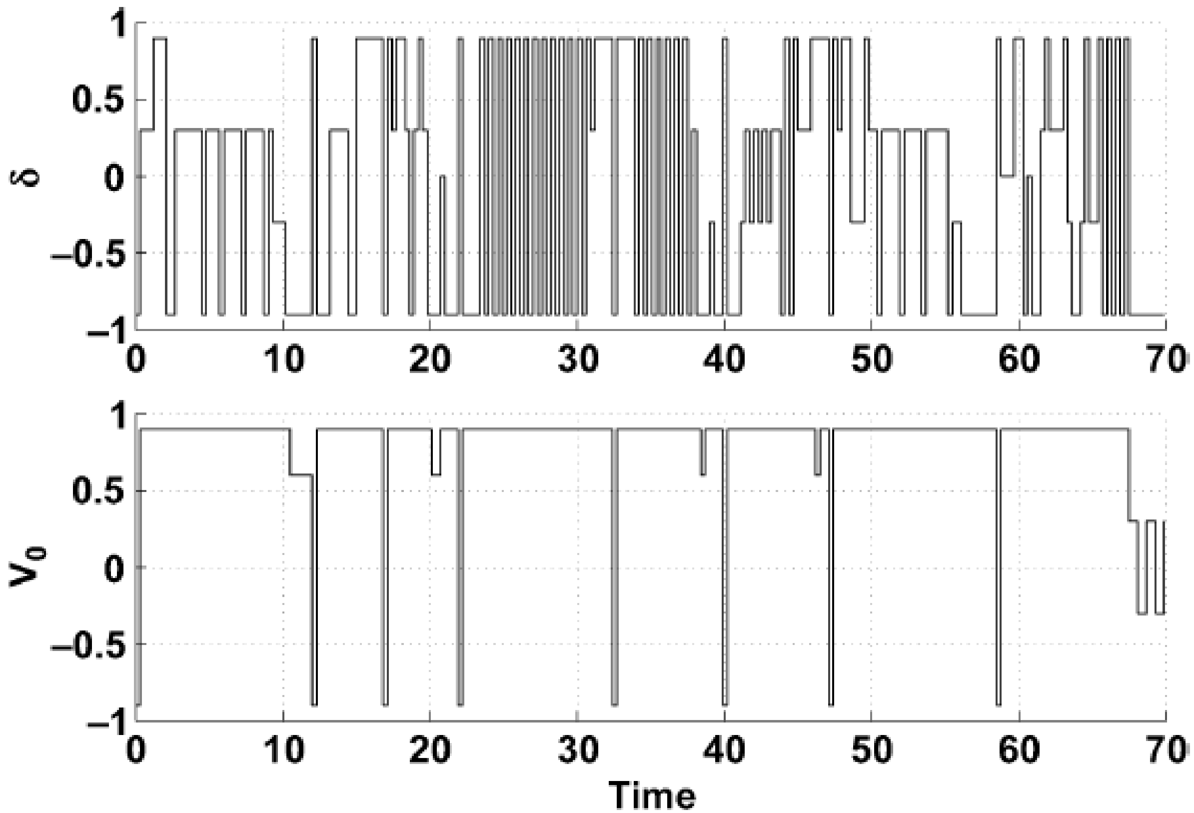
Our objective is to design a controller navigating the vehicle to reach the **target set** (indicated with a red box), while avoiding the **obstacles**, indicated as blue boxes.



Example 2: vehicle

Let us use the symbolic model for controller synthesis:

A controller enforcing the specification was found by exploiting the symbolic model and by using standard algorithms.



Example 2: vehicle

Let us use the symbolic model for controller synthesis:

A controller enforcing the specification was found by exploiting the symbolic model and by using standard algorithms. **The specification is fulfilled!**