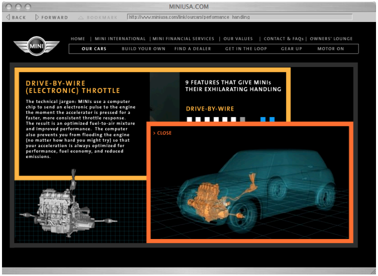
On the synthesis of correct-by-design embedded control software

Paulo Tabuada

Cyber-Physical Systems Laboratory
Department of Electrical Engineering
University of California at Los Angeles

Introduction

Examples of networked embedded control systems



Introduction

Examples of networked embedded control systems

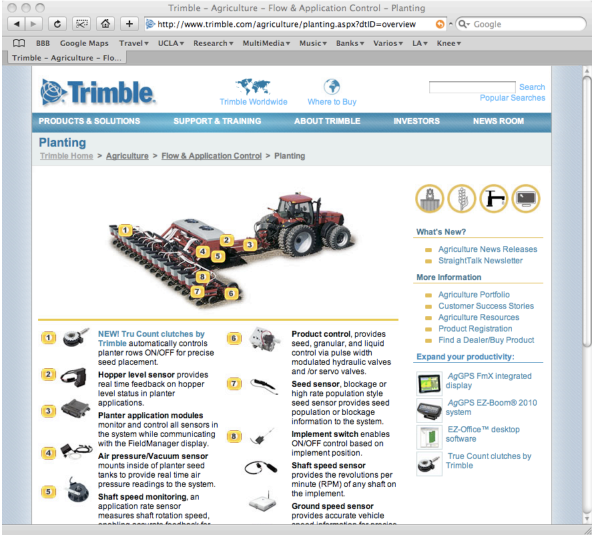
The OneWireless Plant

Honeywell's innovative OneWireless™ solutions turn valuable data into knowledge, helping plants:

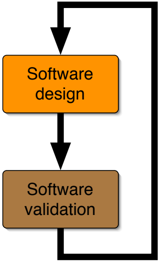
- Keep people, plants and the environment safe
- Improve plant and asset reliability
- Optimize through efficient employees, equipment and processes

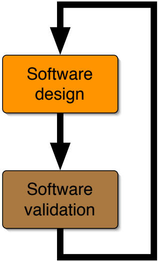
Introduction

Examples of networked embedded control systems



How are embedded control systems designed today?

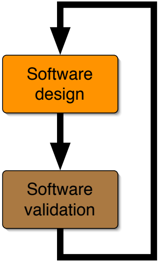




This iterative scheme has several drawbacks:

- Validation by extensive simulation and testing
  increases our confidence in the software but fails to provide adequate guarantees of correct operation and performance;
- Formal verification
  is currently limited to finite state systems and thus cannot be used to verify properties depending on continuous components;
- Extensive validation is time consuming thus
  increasing the cost and time-to-market of embedded software.

Introduction
Existing paradigm



This iterative scheme has several drawbacks:

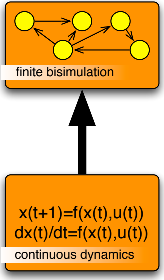
- Validation by extensive simulation and testing
  increases our confidence in the software but fails to provide adequate guarantees of correct operation and performance;
- Formal verification
  is currently limited to finite state systems and thus cannot be used to verify properties depending on continuous components;
- Extensive validation is time consuming thus
  increasing the cost and time-to-market of embedded software.

Some of these disadvantages can be mitigated by adopting a *correct-by-design* approach to the development of embedded control software.

Correct-by-design synthesis

A three step approach

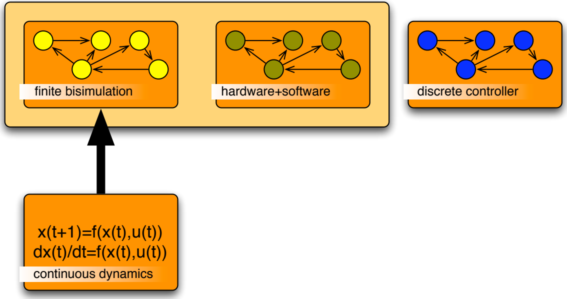
I shall adopt a three step approach to the synthesis of correct-by-design embedded control software.



Correct-by-design synthesis

A three step approach

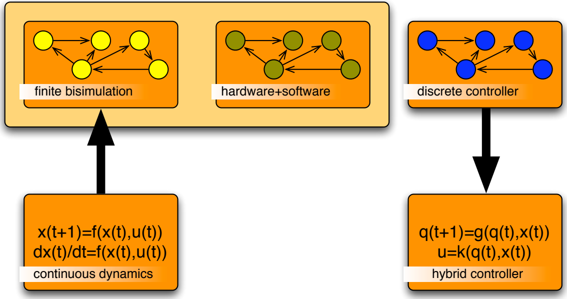
I shall adopt a three step approach to the synthesis of correct-by-design embedded control software.



Correct-by-design synthesis

A three step approach

I shall adopt a three step approach to the synthesis of correct-by-design embedded control software.



CyPhyLab UCLA

Correct-by-design synthesis

A three step approach

Ultimately, I would like to:

1. Specify the continuous dynamics;
2. Specify the software+hardware platform;
3. Define the specification;
4. Obtain embedded code enforcing the specification for the continuous dynamics on the given software+hardware platform.

Correct-by-design synthesis

A three step approach

Ultimately, I would like to:

1. Specify the continuous dynamics;
2. Specify the software+hardware platform;
3. Define the specification;
4. Obtain embedded code enforcing the specification for the continuous dynamics on the given software+hardware platform.

This is a long term goal. Nevertheless, several key ingredients of the proposed approach are already available. In this talk I will focus on one such ingredient:

Existence of finite approximate bisimulations for control systems.

CyPhyLab UCLA

Key ingredients

Control systems as transition systems

Definition

A transition system is a quintuple $T = (Q, L, \longrightarrow, O, H)$, consisting of:

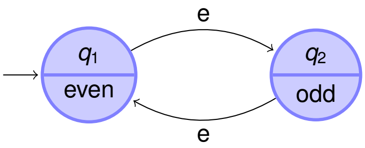
- A set of states Q;
- A set of inputs L;
- A transition relation $\longrightarrow \subseteq Q \times L \times Q$;
- An output set O;
- An output function $H : Q \to O$.

Definition

A transition system is a quintuple $T = (Q, L, \longrightarrow, O, H)$, consisting of:

- A set of states Q;
- A set of inputs L;
- A transition relation $\longrightarrow \subseteq Q \times L \times Q$;
- An output set O;
- An output function $H : Q \to O$.

```
a:=4
b:=1
while a>0
 a:=a+b
end while
```



Can we regard control systems as transition systems?

Definition

A *control system* is a quadruple $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$, where:

- $\mathbb{R}^n$ is the state space;
- $U \subseteq \mathbb{R}^m$ is the input space;
- $\mathcal{U}$ is "nice" subset of the set of all functions of time from intervals of the form $]a, b[\subseteq \mathbb{R}$ to U with $a < 0$ and $b > 0$;
- $f : \mathbb{R}^n \times U \to \mathbb{R}^n$ is a "nice" continuous map.

Can we regard control systems as transition systems?

Definition

A *control system* is a quadruple $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$, where:

- $\mathbb{R}^n$ is the state space;
- $U \subseteq \mathbb{R}^m$ is the input space;
- $\mathcal{U}$ is "nice" subset of the set of all functions of time from intervals of the form $]a, b[\subseteq \mathbb{R}$ to U with $a < 0$ and $b > 0$;
- $f : \mathbb{R}^n \times U \to \mathbb{R}^n$ is a "nice" continuous map.

A "nice" curve $\mathbf{x} :]a, b[\to \mathbb{R}^n$ is said to be a *trajectory* of Σ if there exists $\mathbf{u} \in \mathcal{U}$ satisfying $\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{u}(t))$, for almost all $t \in\,]a, b[$.

Key ingredients

Control systems as transition systems

Given a control system $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$ and sampling time $\tau \in \mathbb{R}^+$, define the transition system:

$$T_\tau(\Sigma) := (Q, L, \longrightarrow, O, H),$$

where:

- $Q = \mathbb{R}^n$;
- L is the set of all the curves in $\mathcal{U}$ of duration τ;
- $q \xrightarrow{\mathbf{u}} p$ if $\mathbf{x}(\tau, q, \mathbf{u}) = p$;
- $O = \mathbb{R}^n$;
- $H = 1_{\mathbb{R}^n}$.

The output set $O = \mathbb{R}^n$ is equipped with the metric $\mathbf{d}(p, q) = \|p - q\|$.

CyPhyLab UCLA

Given a control system $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$ and sampling time $\tau \in \mathbb{R}^+$, define the transition system:

$$T_\tau(\Sigma) := (Q, L, \longrightarrow, O, H),$$

where:

- $Q = \mathbb{R}^n$;
- L is the set of all the curves in $\mathcal{U}$ of duration τ;
- $q \xrightarrow{\mathbf{u}} p$ if $\mathbf{x}(\tau, q, \mathbf{u}) = p$;
- $O = \mathbb{R}^n$;
- $H = 1_{\mathbb{R}^n}$.

The output set $O = \mathbb{R}^n$ is equipped with the metric $\mathbf{d}(p, q) = \|p - q\|$.

Can we replace $T_\tau(\Sigma)$ with an equivalent and yet finite transition system?

Key ingredients

Approximate (bi)simulation

The usual notion of (bi)simulation requires exact matching of outputs.

Definition

Let $T_1 = (Q_1, L_1, \xrightarrow[1]{}, O, H_1)$ and $T_2 = (Q_2, L_2, \xrightarrow[2]{}, O, H_2)$ be transition systems with the same output space O. A relation $R \subseteq Q_1 \times Q_2$ is said to be a simulation relation from T_1 to T_2 if $(p_1, p_2) \in R$ implies:

1. $H(p_1) = H(p_2)$;
2. $p_1 \xrightarrow[1]{l_1} q_1$ imply the existence of $q_2 \in Q_2$ such that $p_2 \xrightarrow[2]{l_2} q_2$ with $(q_1, q_2) \in R$.

CyPhyLab UCLA

The usual notion of (bi)simulation requires exact matching of outputs.

Definition

Let $T_1 = (Q_1, L_1, \xrightarrow[1]{}, O, H_1)$ and $T_2 = (Q_2, L_2, \xrightarrow[2]{}, O, H_2)$ be transition systems with the same output space O. A relation $R \subseteq Q_1 \times Q_2$ is said to be a simulation relation from T_1 to T_2 if $(p_1, p_2) \in R$ implies:

1. $H(p_1) = H(p_2)$;
2. $p_1 \xrightarrow[1]{l_1} q_1$ imply the existence of $q_2 \in Q_2$ such that $p_2 \xrightarrow[2]{l_2} q_2$ with $(q_1, q_2) \in R$.

Relation R is said to be a bisimulation relation between T_1 and T_2 if, in addition to 1. and 2., $(p_1, p_2) \in R$ also implies:

3. $p_2 \xrightarrow[2]{l_2} q_2$ imply the existence of $q_1 \in Q_1$ such that $p_1 \xrightarrow[1]{l_1} q_1$ with $(q_1, q_2) \in R$.

Relaxing the equality constraint $H(p_1) = H(p_2)$ leads to approximate (bi)simulation.

Definition (Girard and Pappas 2005, Tabuada 2005)

Let $T_1 = (Q_1, L_1, \underset{1}{\longrightarrow}, O, H_1)$ and $T_2 = (Q_2, L_2, \underset{2}{\longrightarrow}, O, H_2)$ be metric transition systems with the same output space O and let $\varepsilon \in \mathbb{R}^+$. A relation $R \subseteq Q_1 \times Q_2$ is said to be a ε-approximate simulation relation from T_1 to T_2 if $(p_1, p_2) \in R$ implies:

1. $\mathbf{d}(H(p_1), H(p_2)) \leq \varepsilon$;
2. $p_1 \xrightarrow[1]{l_1} q_1$ imply the existence of $q_2 \in Q_2$ such that $p_2 \xrightarrow[2]{l_2} q_2$ with $(q_1, q_2) \in R$.

Relaxing the equality constraint $H(p_1) = H(p_2)$ leads to approximate (bi)simulation.

Definition (Girard and Pappas 2005, Tabuada 2005)

Let $T_1 = (Q_1, L_1, \underset{1}{\longrightarrow}, O, H_1)$ and $T_2 = (Q_2, L_2, \underset{2}{\longrightarrow}, O, H_2)$ be metric transition systems with the same output space O and let $\varepsilon \in \mathbb{R}^+$. A relation $R \subseteq Q_1 \times Q_2$ is said to be a ε-approximate simulation relation from T_1 to T_2 if $(p_1, p_2) \in R$ implies:

1. $\mathbf{d}(H(p_1), H(p_2)) \leq \varepsilon$;
2. $p_1 \overset{l_1}{\underset{1}{\longrightarrow}} q_1$ imply the existence of $q_2 \in Q_2$ such that $p_2 \overset{l_2}{\underset{2}{\longrightarrow}} q_2$ with $(q_1, q_2) \in R$.

Relation R is said to be a bisimulation relation between T_1 and T_2 if, in addition to 1. and 2., $(p_1, p_2) \in R$ also implies:

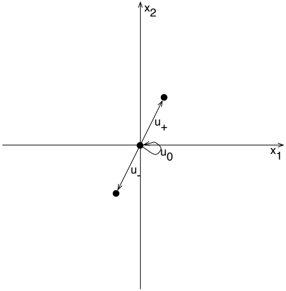
3. $p_2 \overset{l_2}{\underset{2}{\longrightarrow}} q_2$ imply the existence of $q_1 \in Q_1$ such that $p_1 \overset{l_1}{\underset{1}{\longrightarrow}} q_1$ with $(q_1, q_2) \in R$.

Key ingredients

A simple idea

$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= u\end{aligned}$$

$$\begin{aligned}\mathrm{U} &= \{u_-, u_0, u_+\}\\ u_-(t) &= -1 \quad \forall t \in [0,1]\\ u_0(t) &= 0 \quad \forall t \in [0,1]\\ u_+(t) &= 1 \quad \forall t \in [0,1]\end{aligned}$$

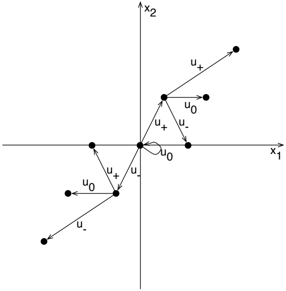


Key ingredients

A simple idea

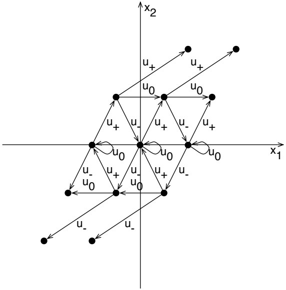
$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= u\end{aligned}$$

$$\begin{aligned}\mathbb{U} &= \{u_-, u_0, u_+\}\\ u_-(t) &= -1 \quad \forall t \in [0,1]\\ u_0(t) &= 0 \quad \forall t \in [0,1]\\ u_+(t) &= 1 \quad \forall t \in [0,1]\end{aligned}$$



$$\dot{x}_1 = x_2$$
$$\dot{x}_2 = u$$

$$\mathbb{U} = \{u_-, u_0, u_+\}$$
$$u_-(t) = -1 \quad \forall t \in [0,1]$$
$$u_0(t) = 0 \quad \forall t \in [0,1]$$
$$u_+(t) = 1 \quad \forall t \in [0,1]$$

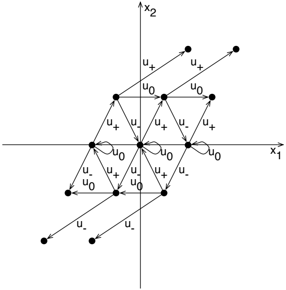


Key ingredients

A simple idea

$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= u\end{aligned}$$

$$\begin{aligned}\mathrm{U} &= \{u_-, u_0, u_+\}\\ u_-(t) &= -1 \quad \forall t \in [0,1]\\ u_0(t) &= 0 \quad \forall t \in [0,1]\\ u_+(t) &= 1 \quad \forall t \in [0,1]\end{aligned}$$



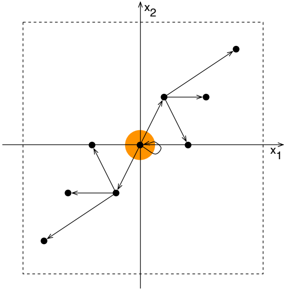
Can we extrapolate from this finite transition system?

Key ingredients

A simple idea

$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= u\end{aligned}$$

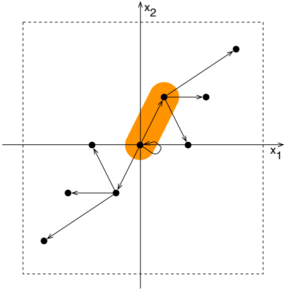
$$\begin{aligned}\mathtt{U} &= \{u_-, u_0, u_+\}\\ u_-(t) &= -1 \quad \forall t \in [0,1]\\ u_0(t) &= 0 \quad \forall t \in [0,1]\\ u_+(t) &= 1 \quad \forall t \in [0,1]\end{aligned}$$



Yes, provided that we know how to robustify it!

$$
\begin{aligned}
\dot{x}_1 &= x_2 \\
\dot{x}_2 &= u
\end{aligned}
$$

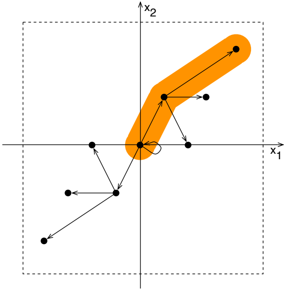
$$
\begin{aligned}
\mathbb{U} &= \{u_-, u_0, u_+\} \\
u_-(t) &= -1 \quad \forall t \in [0,1] \\
u_0(t) &= 0 \quad \forall t \in [0,1] \\
u_+(t) &= 1 \quad \forall t \in [0,1]
\end{aligned}
$$



Yes, provided that we know how to robustify it!

$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= u\end{aligned}$$

$$\begin{aligned}\mathbb{U} &= \{u_-, u_0, u_+\}\\ u_-(t) &= -1 \quad \forall t \in [0,1]\\ u_0(t) &= 0 \quad \forall t \in [0,1]\\ u_+(t) &= 1 \quad \forall t \in [0,1]\end{aligned}$$



Yes, provided that we know how to robustify it!

Key ingredients

Incremental stability

Definition (δ-GAS)

A control system Σ is *incrementally globally asymptotically stable* (δ–GAS) if it is forward complete and there exist a $\mathcal{KL}^a$ function β such that for any $t \in \mathbb{R}_0^+$, any $x, y \in \mathbb{R}^n$ and any $\mathbf{u} \in \mathcal{U}$ the following condition is satisfied:

$$\|\mathbf{x}(t, x, \mathbf{u}) - \mathbf{x}(t, y, \mathbf{u})\| \leq \beta(\|x - y\|, t).$$

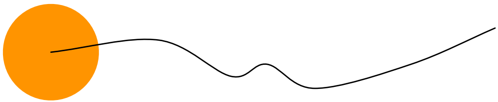
[a] A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}_\infty$ if, for each fixed s, the map $\beta(r, s)$ is strictly increasing, $\beta(0, s) = 0$ and $\beta(r, s) \to \infty$ as $r \to \infty$, and for each fixed r, the map $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \to 0$ as $s \to \infty$.

Definition (δ-GAS)

A control system Σ is *incrementally globally asymptotically stable* (δ–GAS) if it is forward complete and there exist a $\mathcal{KL}^a$ function β such that for any $t \in \mathbb{R}_0^+$, any $x, y \in \mathbb{R}^n$ and any $\mathbf{u} \in \mathcal{U}$ the following condition is satisfied:

$$\|\mathbf{x}(t, x, \mathbf{u}) - \mathbf{x}(t, y, \mathbf{u})\| \leq \beta(\|x - y\|, t).$$

[a] A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}_\infty$ if, for each fixed s, the map $\beta(r, s)$ is strictly increasing, $\beta(0, s) = 0$ and $\beta(r, s) \to \infty$ as $r \to \infty$, and for each fixed r, the map $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \to 0$ as $s \to \infty$.

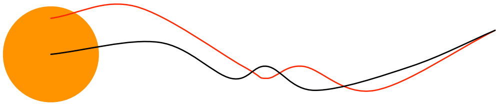


Definition (δ-GAS)

A control system Σ is *incrementally globally asymptotically stable* (δ–GAS) if it is forward complete and there exist a $\mathcal{KL}$[a] function β such that for any $t \in \mathbb{R}_0^+$, any $x, y \in \mathbb{R}^n$ and any $\mathbf{u} \in \mathcal{U}$ the following condition is satisfied:

$$\|\mathbf{x}(t, x, \mathbf{u}) - \mathbf{x}(t, y, \mathbf{u})\| \leq \beta(\|x - y\|, t).$$

[a] A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}_\infty$ if, for each fixed s, the map $\beta(r, s)$ is strictly increasing, $\beta(0, s) = 0$ and $\beta(r, s) \to \infty$ as $r \to \infty$, and for each fixed r, the map $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \to 0$ as $s \to \infty$.

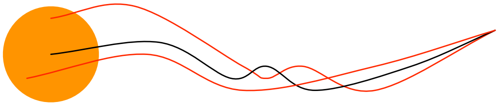


Definition (δ-GAS)

A control system Σ is *incrementally globally asymptotically stable* (δ–GAS) if it is forward complete and there exist a $\mathcal{KL}^a$ function β such that for any $t \in \mathbb{R}_0^+$, any $x, y \in \mathbb{R}^n$ and any $\mathbf{u} \in \mathcal{U}$ the following condition is satisfied:

$$\|\mathbf{x}(t, x, \mathbf{u}) - \mathbf{x}(t, y, \mathbf{u})\| \leq \beta(\|x - y\|, t).$$

[a] A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}_\infty$ if, for each fixed s, the map $\beta(r, s)$ is strictly increasing, $\beta(0, s) = 0$ and $\beta(r, s) \to \infty$ as $r \to \infty$, and for each fixed r, the map $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \to 0$ as $s \to \infty$.

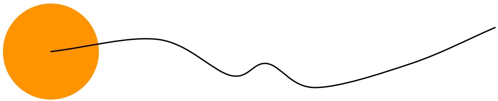


Definition (δ-ISS)

A control system Σ is *incrementally input–to–state stable* (δ–ISS) if it is forward complete and there exist a $\mathcal{KL}$ function β and a $\mathcal{K}_\infty$[a] function γ such that for any $t \in \mathbb{R}_0^+$, any $x, y \in \mathbb{R}^n$ and any $\mathbf{u}, \mathbf{v} \in \mathcal{U}$ the following condition is satisfied:

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

[a] A continuous function $\gamma : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{K}_\infty$ if γ is strictly increasing, $\gamma(0) = 0$ and $\gamma(r) \to \infty$ as $r \to \infty$.

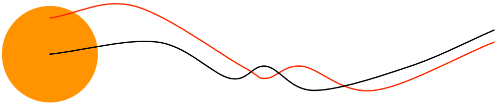


Definition (δ-ISS)

A control system Σ is *incrementally input–to–state stable* (δ–ISS) if it is forward complete and there exist a $\mathcal{KL}$ function β and a $\mathcal{K}_\infty$[a] function γ such that for any $t \in \mathbb{R}_0^+$, any $x, y \in \mathbb{R}^n$ and any $\mathbf{u}, \mathbf{v} \in \mathcal{U}$ the following condition is satisfied:

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

[a] A continuous function $\gamma : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{K}_\infty$ if γ is strictly increasing, $\gamma(0) = 0$ and $\gamma(r) \to \infty$ as $r \to \infty$.



Key ingredients

Incremental stability

1. For linear control systems, that is, $\dot{x} = Ax + Bu$, both δ-GAS and δ-ISS are equivalent to stability of A (all the eigenvalues of A have negative real part);
2. In the nonlinear case, by restricting attention to a compact set, GAS implies δ-GAS and ISS implies δ-ISS;
3. Both δ-GAS and δ-ISS admit Lyapunov characterizations.

Given a control system $\Sigma = (\mathbb{R}^n, U, \mathcal{U}, f)$, a time quantization $\tau \in \mathbb{R}^+$, a space quantization $\eta \in \mathbb{R}^+$, and an input quantization $\mathtt{U}_\tau \subseteq \mathcal{U}$, define the transition system:

$$T_{\eta\mathtt{U}_\tau}(\Sigma) := (Q_{\eta\mathtt{U}_\tau}, L, \xrightarrow[\eta\mathtt{U}_\tau]{}, O, H),$$

where:

- $Q_{\eta\mathtt{U}_\tau} = [\mathbb{R}^n]_\eta$;
- $L = \mathtt{U}_\tau$;
- $q \xrightarrow[\eta\mathtt{U}_\tau]{\mathbf{u}} p$ if $\|\mathbf{x}(\tau, q, \mathbf{u}) - p\| \leq \frac{\eta}{2}$;
- $O = \mathbb{R}^n$;
- $H = 1_{\mathbb{R}^n}$.

Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$, for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.

Main results

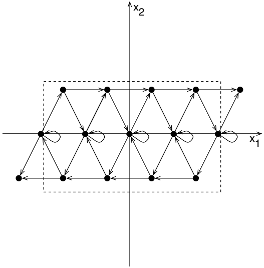
Existence of approximate simulations

Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$, for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.



Main results

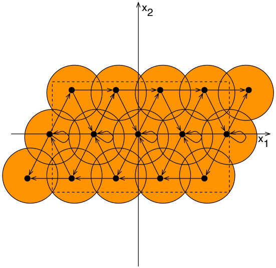
Existence of approximate simulations

Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$, for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.



Main results

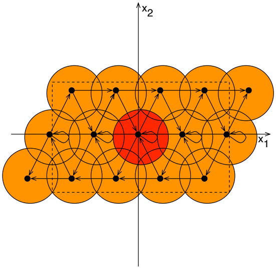
Existence of approximate simulations

Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$, for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.

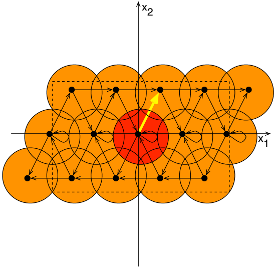


Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$, for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.



Main results

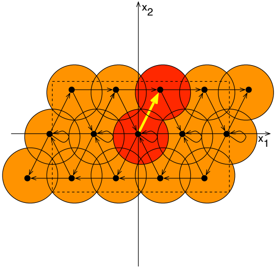
Existence of approximate simulations

Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$, for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.



Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$ for any $\mathrm{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathrm{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathrm{U}_\tau}) = \mathbb{R}^n$.

Under the assumptions of the previous theorem, there exists a countable set of control quanta U_τ rendering $T_{\eta \mathrm{U}_\tau}(\Sigma)$ ε-approximate bisimilar to $T_\tau(\Sigma)$.

Theorem

Let Σ be a control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-GAS, then for any $\tau \in \mathbb{R}^+$ for any $\mathtt{U}_\tau \subseteq \mathcal{U}$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} \leq \varepsilon$$

there exists an ε-approximate simulation relation R from $T_{\eta \mathtt{U}_\tau}(\Sigma)$ to $T_\tau(\Sigma)$ satisfying $R(Q_{\eta \mathtt{U}_\tau}) = \mathbb{R}^n$.

Under the assumptions of the previous theorem, there exists a countable set of control quanta $\mathtt{U}_\tau$ rendering $T_{\eta \mathtt{U}_\tau}(\Sigma)$ ε-approximate bisimilar to $T_\tau(\Sigma)$.

But how do we compute $\mathtt{U}_\tau$?

Theorem

Let Σ be a digital control system and let $\varepsilon \in \mathbb{R}^+$ be any desired precision. If Σ is δ-ISS, then for any $\tau \in \mathbb{R}^+$, for $\mathbb{U}(\tau) = [U]_\mu$, and for any $\eta \in \mathbb{R}^+$ satisfying the following inequality:

$$\beta(\varepsilon, \tau) + \frac{\eta}{2} + \gamma(\mu) \leq \varepsilon$$

there exists an ε-approximate bisimulation relation R between $T_{\eta \mathbb{U}_\tau}(\Sigma)$ and $T_\tau(\Sigma)$.

CyPhyLab UCLA

Example

A non-holonomic robot

Let us consider the simplest nonholonomic robot:

$$\dot{x} = v\cos\theta \quad (1)$$

$$\dot{y} = v\sin\theta \quad (2)$$

$$\dot{\theta} = \omega \quad (3)$$

and construct a finite abstraction by working on $[-2,2] \times [-2,2] \times [0,2\pi]$ and by considering constant input curves of duration $3s$ and assuming values on $\{0,1\} \times \{-1.1,-1,1,1.1\}$.

Example

A non-holonomic robot

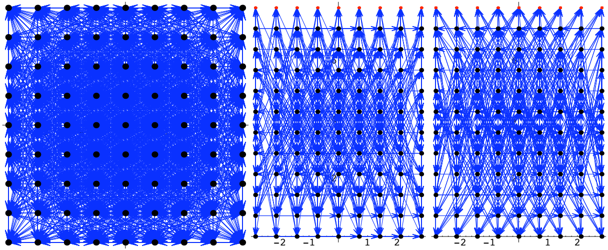
Let us consider the simplest nonholonomic robot:

$$\dot{x} = v \cos \theta \tag{1}$$

$$\dot{y} = v \sin \theta \tag{2}$$

$$\dot{\theta} = \omega \tag{3}$$

and construct a finite abstraction by working on $[-2, 2] \times [-2, 2] \times [0, 2\pi]$ and by considering constant input curves of duration $3s$ and assuming values on $\{0, 1\} \times \{-1.1, -1, 1, 1.1\}$.



Example

A non-holonomic robot

Periodic orbits: find a periodic orbit passing through the origin.

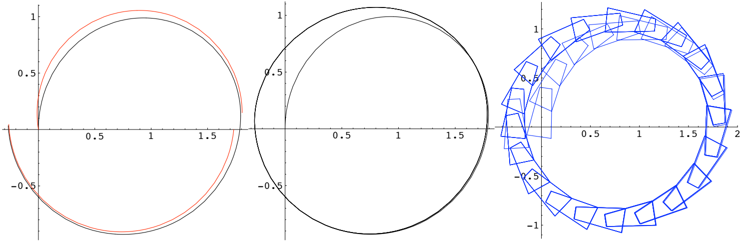
Example

A non-holonomic robot

Periodic orbits: find a periodic orbit passing through the origin.

Searching on the discrete abstraction we obtain:

$$(0,0,0.55\pi) \xrightarrow{(1,-1.1)} (1.73,0,1.47\pi) \xrightarrow{(1,-1)} (0,0,0.55\pi)$$



Example

A non-holonomic robot

Language specifications: execute periodic orbits according to the sequence

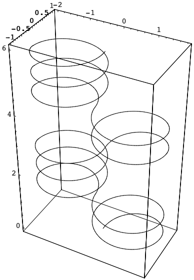
$$\text{right}\rightarrow\text{right}\rightarrow\text{left}\rightarrow\text{left}\rightarrow\text{left}\rightarrow\text{right}\rightarrow\text{right}\rightarrow\text{left}\rightarrow\text{left}\rightarrow\text{left}.$$

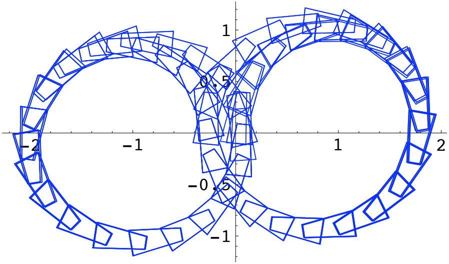
Example

A non-holonomic robot

Language specifications: execute periodic orbits according to the sequence

right→right→left→left→left→right→right→left→left→left.





Example

A non-holonomic robot

Switching specifications.

rotate clockwise

rotate counter-clockwise

either clockwise or counter-clockwise

Example

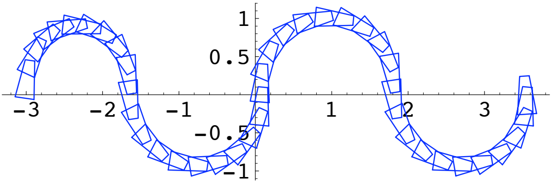
A non-holonomic robot

Switching specifications.

rotate clockwise

rotate counter-clockwise

either clockwise or counter-clockwise



Example

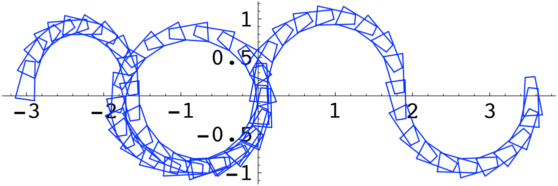
A non-holonomic robot

Switching specifications.

rotate clockwise

rotate counter-clockwise

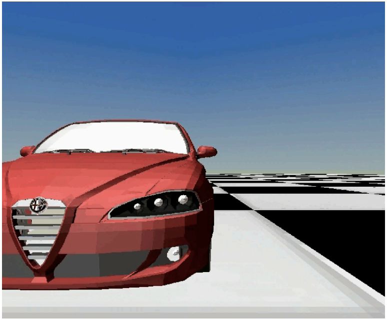
either clockwise or counter-clockwise



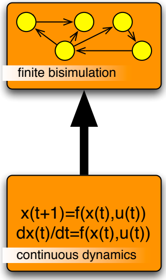
CyPhyLab UCLA

Example
A non-holonomic robot

Interaction with discrete signals.



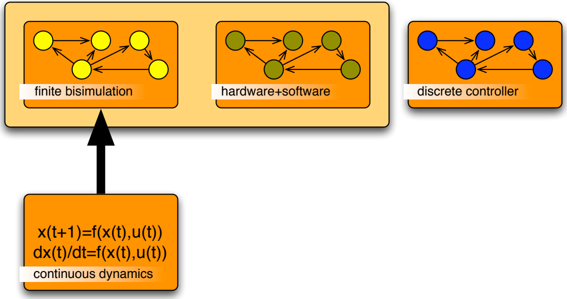
Putting the pieces together
Abstraction



- The abstraction step can be done for a reasonable class of control systems;
- Recent results eliminate the stability assumption by ensuring only the existence of approximate alternating simulation relations;
- Multi-resolution quantization and other techniques can be used to reduce the size of the abstractions.

Putting the pieces together

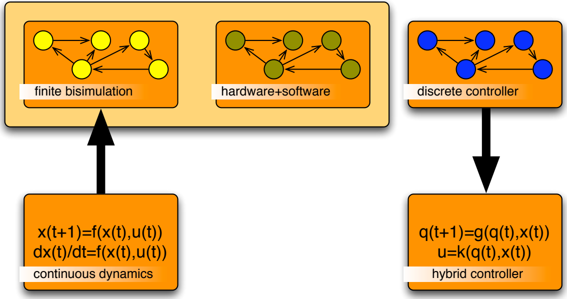
Synthesis of discrete controllers



- Synthesis of controllers based on language specifications can be done by resorting to supervisory control or algorithmic game theory;
- Synthesis of controllers based on (bi)simulation specifications can be done by modifying existing algorithms for the construction of (bi)simulations;
- Incorporating timing considerations is crucial to address real-time issues.

Putting the pieces together

Controller refinement



- The refinement of discrete to hybrid controllers is based on the approximate bisimulation relation between the discrete abstraction and the continuous plant;
- The hybrid controller is a formal model for embedded code. Automated code generation from this model is conceptually simple;
- Correctness of operation depends on real-time scheduling and many other considerations.

Questions?

Many questions remain open and much work is to be done before we can synthesize correct-by-design embedded control software.

The ingredients, however, are becoming available.

Questions?

Many questions remain open and much work is to be done before we can synthesize correct-by-design embedded control software.

The ingredients, however, are becoming available.

The work described in this talk was the result of:

- the dedication of my students and postdocs: Giordano Pola (now Assistant Professor at University of L'Aquila), Manuel Mazo Jr., and Anna Davitian;
- the inspiring discussions with my collaborators: Aaron Ames, Antoine Girard, Agung Julius, Rupak Majumdar, and George Pappas;
- the financial support from the National Science Foundation.

For papers and more information:

`http://www.cyphylab.ee.ucla.edu/`

`http://www.ee.ucla.edu/∼tabuada`