Compositional and quantitative approaches in symbolic control

Antoine Girard

CNRS, Laboratoire des Signaux et Systèmes
Gif-sur-Yvette, France

GT VS-CPS
Paris, July, 3rd, 2018
Cyber-physical systems (CPS) consist of physical entities enhanced with computation and communication capabilities, used for monitoring and control purpose.

Design of reliable CPS is challenging, time consuming and costly:

*Innovative approaches to abstraction and architectures that enable seamless integration of control, communication, and computation must be developed for rapid design and deployment of CPS.*

Baheti & Gill, Cyber-physical systems, The impact of control technology, 2011
A programmable CPS should consist of:

- A **high-level language** enabling the specification of the CPS behavior while abstracting computational and physical details;
- An **automated synthesis tool**, based on a model (including description of physical system), generating from a high-level program, controllers enforcing the specified behavior.

We aim at giving strong guarantees on the synthesized controllers:

- **Correct by construction** design through formal controller synthesis techniques.

Rapid and dependable development/evolution of advanced functions of a CPS.
Example - vehicle platoon

\[ \dot{x}_i = v_i, \quad \dot{v}_i = f_i(v_i, u_i), \quad i = 1, 2. \]

High level program

\[
\begin{align*}
0.080 & \leq x_2 - x_1 & \leq 0.100 \\
110 & \leq v_1 & \leq 130 \\
110 & \leq v_2 & \leq 130
\end{align*}
\]

Model based automatic synthesis

CbC controller

\[
\begin{align*}
u_1 &= \ldots \\
u_2 &= \ldots
\end{align*}
\]

Controller not existing/found
Model-based synthesis for CPS from high-level behavioral specifications:
Outline of the talk

1. Brief overview of symbolic control
   - Symbolic control architecture
   - System abstraction and interface
   - High-level specifications and synthesis

2. Compositional synthesis of symbolic controllers
   - Assume-guarantee contracts
   - Overlapping abstractions

3. Quantitative synthesis of symbolic controllers
   - Quantitative safety, reachability and stability
   - Application in compositional synthesis
Symbolic control architecture

\[ \dot{x} = f(x, u, v) \]
\[ y = h(x) \]
Symbolic control architecture

Symbolic model:
- Finite abstraction of the physical system dynamics
- Based on a formal abstraction relation

Symbolic model:

Finite abstraction of the physical system dynamics
Based on a formal abstraction relation
Symbolic control architecture

Interface:

- Low-level controller implementing the formal abstraction relation between the two models
- Makes the physical system and the symbolic model behave similarly
Symbolic control architecture

Symbolic controller:
- High-level controller implementing the advanced functions of the CPS
- Automatic synthesis from high-level specifications, based on the symbolic model
Physical system \( \mathcal{P} \):
\[
x^+ \in F(x, u), \ x \in X, \ u \in U
\]

Symbolic model \( \mathcal{S} \):
\[
q^+ \in T(q, a), \ q \in Q, \ a \in A
\]

- Finite partition (or cover) \( (X_q)_{q \in Q} \) of the state space \( X \)
- Finite subset \( A \) of the input set \( U \)
- Over-approximation of the dynamics by reachability analysis \( (u = a) \)
System abstraction

Physical system $\mathcal{P}$:
$$x^+ \in F(x, u), \ x \in X, \ u \in U$$

Symbolic model $\mathcal{S}$:
$$q^+ \in T(q, a), \ q \in Q, \ a \in A$$

Feedback may reduce non-determinism:
$$u = \mu(a, x, q) = a + K(x - x_q)$$
Formal abstraction relation

- Simulation, bisimulation relations [Park 81, Milner 89], their approximate and alternating versions [Girard & Pappas 07, Pola & Tabuada 09]
- Given a “distance” $d$ between physical and symbolic states:
  e.g. $d(x, q) = \|x - x_q\|

Definition

Let $\varepsilon > 0$, the relation $R = \{(x, q) | x \in X_q\}$ is an alternating $\varepsilon$-approximate simulation relation if for all $(x, q) \in R$:

- $d(x, q) \leq \varepsilon$,
- $\forall a \in A, \exists u \in U, \forall x^+ \in F(x, u), \exists q^+ \in T(q, a)$, s.t. $(x^+, q^+) \in R$.

Interface:

$$
\begin{aligned}
    u & = \mu(a, x, q) \\
    q^+ & \in T(q, a) \cap R(x^+)
\end{aligned}
$$
Control refinement through the interface

Behavioral similarity:

**Theorem**

For all symbolic input sequences \(a(.), (x(0), q(0)) \in R \implies d(x(k), q(k)) \leq \varepsilon, \forall k \in \mathbb{N}.\)
Related work

- **Symbolic dynamics** [Hadamard 1898, Morse & Hedlund 1938...]

- **Partition-based approaches**
  - with feedback [Caines & Wei 1998, Habets et al. 2006, Belta & Habets 2006, Girard & Martin 2012...]


Specifications - safety and reachability

Symbolic model $S$:
$q^+ \in T(q, a), \ q \in Q, \ a \in A, \ q_0 \in Q_0$

Symbolic controller:
$a = C(q)$

Definition
- Given a safe set $Q_s \subseteq Q$, $C$ is a **safety controller** if:
  \[ \forall k \in \mathbb{N}, \ q_k \in Q_s. \]
- Given a target set $Q_t \subseteq Q$, $C$ is a **reachability controller** if:
  \[ \exists k \in \mathbb{N}, \ q_k \in Q_t. \]
Controllable predecessors of a subset $P \subseteq Q$:

$$Pre(P) = \{ q \in Q \mid \exists a \in A, \ T(q, a) \subseteq P \}.$$

Safety synthesis

$$P_0 = Q$$

loop

$$| \quad P_{k+1} = Q_s \cap Pre(P_k)$$

until $P_{k+1} = P_k$

Reachability synthesis

$$P_0 = \emptyset$$

loop

$$| \quad P_{k+1} = Q_t \cup Pre(P_k)$$

until $P_{k+1} = P_k$

- Synthesis through greatest and least fixed point computation
- Termination guaranteed by finiteness of $Q$
Definition

Given a target set $Q_t \subseteq Q$

- $C$ is a **stability controller** if: $\exists j \in N, \forall k \geq j, q_k \in Q_t$.
- $C$ is a **recurrence controller** if: $\forall j \in N, \exists k \geq j, q_k \in Q_t$.

- Synthesis through nested greatest and least fixed point computation
- Termination guaranteed by finiteness of $Q$
Automata-based specifications

- Hybrid automata semantics
- Compute the product of symbolic model and automaton
- Specifications and controllers defined on the product space:
  - safety, reachability...
  - stability and...
  - recurrence
    \[ \Rightarrow \quad \text{Linear Temporal Logic (LTL)} \]
Outline of the talk

1. Brief overview of symbolic control
   - Symbolic control architecture
   - System abstraction and interface
   - High-level specifications and synthesis

2. Compositional synthesis of symbolic controllers
   - Assume-guarantee contracts
   - Overlapping abstractions

3. Quantitative synthesis of symbolic controllers
   - Quantitative safety, reachability and stability
   - Application in compositional synthesis
Towards scalable symbolic control

Symbolic control suffers from **scalability issues** (partition of the state-space, discretization of input set):

- **Intermediate lower-dimensional continuous abstractions**
  

- **Efficient abstraction techniques**
  
  - Optimal abstraction parameters [Weber et al. 2017, Saoud & Girard 2017]
  - Input-based abstraction [Le Corronc et al. 2013, Zamani et al. 2015]

- **Compositional synthesis**
  
  [Dallal & Tabuada 2015, Kim et al. 2015, Meyer et al. 2018]
Interconnected systems:

Subsystem $S_i$:

$$
\begin{cases}
    x_i^+ \in F_i(x_i, x_{M_i}, u_i) \\
    x_i \in X_i, \; u_i \in U_i \\
    x_{M_i} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m)
\end{cases}
$$

Distributed controllers:

$$u_i = C_i(x_i, x_{M_i})$$

Safety specifications:

$$\forall k \in \mathbb{N}, \; x_i(k) \in X_i^s$$

Component-based design:

- Synthesize distributed controllers “locally”
- Objective: improve scalability and modularity
**Assume-guarantee contracts**

- **AG contracts**: properties that a component (subsystem + controller) must guarantee under assumptions on the behavior of its environment (other components).

- **AG contract for component** $i$:

\[
\left\{
\begin{array}{ll}
\text{Assumption}: & \forall k = 0, \ldots, j, \quad x_{Mi}(k) \in X_{Mi}^s \\
\text{Guarantee}: & \forall k = 0, \ldots, j + 1, \quad x_i(k) \in X_i^s
\end{array}
\right.
\]

where $X_{Mi}^s = X_1^s \times \cdots \times X_{i-1}^s \times X_{i+1}^s \times \cdots \times X_m^s$.

**Theorem**

*If all components satisfy their AG contract, then:*

\[
\forall k \in \mathbb{N}, \quad x_i(k) \in X_i^s, \quad i = 1, \ldots, m.
\]
Assume-guarantee synthesis

Local synthesis (at the level of components) of controllers achieving AG contract satisfaction

Fully decentralized control:

System abstraction from component $i$ (assumption):
\[
\begin{align*}
&x_i^+ \in F_i(x_i, X_{M_i}^s, u_i) \\
&x_i \in X_i, \ u_i \in U_i
\end{align*}
\]

Controller $C_i$:
\[u_i = C_i(x_i)\]

Specification (guarantee):
\[\forall k \in \mathbb{N}, \ x_i(k) \in X_i^s\]
Assume-guarantee synthesis

- Safety synthesis using symbolic control techniques

Advantages:
- Reduced dimension (both state and input)  \implies \textbf{Scalability}
- Independence between components  \implies \textbf{Modularity}

Drawbacks:
- No information about other components (state, dynamics)  \implies \textbf{Conservatism}

Compromise between scalability/modularity and conservatism:
- Include partial description of environment for AG synthesis  \implies \textbf{Overlapping abstractions and partially decentralized controllers}
Overlapping abstractions

Partially decentralized control:

System abstraction from component $i$ (assumption):
\[
\begin{align*}
x_i^+ & \in F_i(x_i, x_{N_i}, X_{s_P_i}^s, u_i) \\
x_{N_i}^+ & \in F_{N_i}(x_i, x_{N_i}, X_{P_i}^s, U_{N_i}) \\
x_i & \in X_i, \ x_{N_i} \in X_{N_i}, \ u_i \in U_i
\end{align*}
\]

Controller $C_i$:
\[u_i = C_i(x_i, x_{N_i})\]

Specification (AG contract):
\[
\forall k = 0, \ldots, j, \ x_{N_i}(k) \in X_{N_i}^s \\
\implies \forall k = 0, \ldots, j + 1, \ x_i(k) \in X_i^s
\]
Synthesis with overlapping abstractions

Subtlety – AG contract can be satisfied by:

- enforcing the guarantee, or... falsifying the assumption
- reformulation as a safety synthesis problem
Example - temperature regulation

4-room building:

\[
\begin{array}{cc}
T_1 & T_2 \\
\hline
u_1 & u_2 \\
T_4 & T_3 \\
\hline
u_4 & u_3
\end{array}
\]

Symbolic control synthesis:

- Centralized (C) approach
- Fully decentralized (FD) approach
  - A room is a component
  - No information from other rooms
- Partially decentralized (PD) approach
  - A room is a component
  - Information about neighboring rooms

\[
T^+ = AT + Bu + c
\]

### Example - temperature regulation

<table>
<thead>
<tr>
<th>state symbols (#)</th>
<th>controllable states (%)</th>
<th>CPU times (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C</td>
<td>FD</td>
</tr>
<tr>
<td>625 (= 5^4)</td>
<td>84</td>
<td>0</td>
</tr>
<tr>
<td>10000 (= 10^4)</td>
<td>89</td>
<td>0</td>
</tr>
<tr>
<td>160000 (= 20^4)</td>
<td>91</td>
<td>0</td>
</tr>
</tbody>
</table>

Controllable states for room 4
Asynchronous components

- Discrete-time framework:
  \[ \Rightarrow \text{all controllers need to be synchronized (same period, no skew)} \]

- Asynchronous components:
  - Each component has its own sampling period
  - Inter-sampling behavior matters: continuous-time models and AG contracts

\[
\begin{align*}
\text{Assumption:} & \quad \forall t \in [0, T], \quad x_{M_i}(t) \in X_{M_i}^s \\
\text{Guarantee:} & \quad \forall t \in [0, T + \delta], \quad x_i(t) \in X_i^s \quad \text{with } \delta > 0
\end{align*}
\]

- Computation of symbolic model:
  - Symbolic model describes transitions over a period
  - Inter-sampling behavior analyzed using reachability analysis

\textit{Saoud, Girard & Fribourg, ECC, 2018.}
Outline of the talk

1. Brief overview of symbolic control
   - Symbolic control architecture
   - System abstraction and interface
   - High-level specifications and synthesis

2. Compositional synthesis of symbolic controllers
   - Assume-guarantee contracts
   - Overlapping abstractions

3. Quantitative synthesis of symbolic controllers
   - Quantitative safety, reachability and stability
   - Application in compositional synthesis
Specifications in symbolic control are typically qualitative
  \[\Rightarrow\] hard to reason on robustness!

Robustness margins using symbolic models with additional non-determinism (bounded disturbances)
  [Pola & Tabuada 2009, Liu & Ozay 2014]

Quantitative semantics of specifications
  [Fainekos & Pappas 2009, Donzé & Maler 2010]
  - Input-output stability [Tabuada et al. 2014]
  - Model predictive control [Sadraddini & Belta 2015, Raman et al. 2014]
Quantitative approach to safety and reachability

Safety

Reachability

Signed distance:

\[ d(q, P) = \begin{cases} 
\sup \{ \delta \geq 0 \mid B_\delta(q) \cap P \neq \emptyset \} & \text{if } q \notin P \\ 
- \sup \{ \delta \geq 0 \mid B_\delta(q) \subseteq P \} & \text{if } q \in P 
\end{cases} \]
Quantitative safety synthesis

Optimal control formulation:

\[
\text{Minimize } \sup_{k \in \mathbb{N}} d(q_k, Q_s)
\]

Quantitative safety synthesis

\[
V_0(q) = -\infty
\]

<table>
<thead>
<tr>
<th>Loop</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ V_{k+1}(q) = \max \left( d(q, Q_s), \min_{a \in A} \max_{q' \in T(q,a)} V_k(q') \right) ]</td>
</tr>
</tbody>
</table>

until \( V_{k+1} = V_k \)

- Termination guaranteed by finiteness of \( Q \)
- Extension of the fixed point computation for qualitative synthesis
Quantitative safety synthesis

**Theorem**

*For all $\delta \in \mathbb{R}$, the level set*

$$P^*_\delta = \{ q \in Q | V^*(q) \leq \delta \}$$

*is the maximal safety controllable set for $B_\delta(Q_s)$. Moreover, there exists a controller $C$ such that*

$$\forall k \in \mathbb{N}, \; d(q_k, Q_s) \leq V^*(q_0).$$

- The fixed point of the qualitative approach is given by $P^*_0$
- Computation of a parameterized family of safety controllable sets $P^*_\delta$
- Common safety controller for all the family

A. Girard (CNRS, L2S) Symbolic Control
Quantitative reachability synthesis

Optimal control formulation:

$$\text{Minimize } \inf_{k \in \mathbb{N}} d(q_k, Q_t)$$

Quantitative reachability synthesis

$$V_0(q) = +\infty$$

loop

$$V_{k+1}(q) = \min \left( d(q, Q_t), \min_{a \in A} \max_{q' \in T(q, a)} V_k(q') \right)$$

until $$V_{k+1} = V_k$$

- Termination guaranteed by finiteness of $$Q$$
- Extension of the fixed point computation for qualitative synthesis
Theorem

For all $\delta \in \mathbb{R}$, the level set

$$P^*_\delta = \{ q \in Q | V^*(q) \leq \delta \}$$

is the maximal reachability controllable set for $B_\delta(Q_t)$. Moreover, there exists a controller $C$ such that

$$\exists k \in \mathbb{N}, \ d(q_k, Q_t) \leq V^*(q_0).$$

- The fixed point of the qualitative approach is given by $P^*_0$
- Computation of a parameterized family of reachability controllable sets $P^*_\delta$
- Common reachability controller for all the family
Qualitative stability synthesis

Stability as “reachability then safety”

Quantitative stability synthesis

\[
V_0(q) = -\infty
\]

loop

\[
V_{k+1}(q) = \max \left( d(q, Q_t), \min_{a \in A} \max_{q' \in T(q, a)} V_k(q') \right)
\]

until \( V_{k+1} = V_k \)

\( V^*(q) = V_k(q), \ W_0(q) = +\infty \)

loop

\[
W_{k+1}(q) = \min \left( V^*(q), \min_{a \in A} \max_{q' \in T(q, a)} W_k(q') \right)
\]

until \( W_{k+1} = W_k \)

- Termination guaranteed by finiteness of \( Q \)
- Computation of a parameterized family of stability controllable sets with a common controller

Theorem

There exists a controller \( C \) such that

\[
\exists j \in \mathbb{N}, \forall k \geq j, \ d(q_k, Q_t) \leq W^*(q_0).
\]
Example - DC/DC converter

Model: $\dot{x} = A_p x + b_p, \ p \in \{1, 2\}$
Safety specification: $Q_s = [1.1, 1.6] \times [5.4, 5.9]$

Quantitative safety
(left: value function, right: trajectory)

Eqtami & Girard, ADHS 2018
Example - DC/DC converter

Model: \( \dot{x} = A_p x + b_p, \ p \in \{1, 2\} \)

Reachability specification: \( Q_t = [1.1, 1.6] \times [5.4, 5.9] \)

Quantitative reachability
(left: value function, right: trajectory)
Example - DC/DC converter

Model: \( \dot{x} = A_p x + b_p, \ p \in \{1, 2\} \)

Stability specification: \( Q_t = [1.1, 1.6] \times [5.4, 5.9] \)

Quantitative stability

(left: value function, right: trajectory)
Conclusion

- Symbolic control is a very rich and lively area at the interface between automatic control and computer science.

- It is a rigorous computational approach to controller design from high level specifications, applicable to broad classes of systems.

- Challenging problems include:
  - Scalability and modularity (systems and specifications).
  - Robustness (unmodeled disturbances) and adaptation (uncertain / time-varying parameters).
### Independent Graduate Modules

- **Formal Methods in Control Design - from Discrete Synthesis to Continuous Controllers**
  - Instructor: Cailin A. Belta, Boston University, USA
  - Antoine Girard, CNRS L2S, Univ. Paris-Saclay, France

- **Practical Adaptive Control**
  - Instructor: Anuradha Annaswamy, MIT, USA

- **Neuronal Excitability: Modeling, Control and Interconnection Principles**
  - Instructor: Rodolphe Sepulchre, Univ. Cambridge, UK, Guillaume Drion, Univ. Liège, Belgium, Alessio Franci, UNAM

- **Sliding Mode Control and Observation**
  - Instructor: Christopher Edwards, University of Exeter, UK

- **The Scenario Approach: Making Decisions in an Uncertain World (Systems, Control, Machine Learning)**
  - Instructor: Marco C. Campi, University of Brescia, Italy
  - Simone Garatti, Politecnico di Milano, Italy

- **Stochastic Models in Systems & Synthetic Biology**
  - Instructor: Alessandro Borri & Pasquale Palumbo, CNR-IAS Rome, Italy

- **High-Gain Observers in Nonlinear Feedback Control**
  - Instructor: Hassan K. Khalil, Michigan State University, USA

- **Model-Based Fault Diagnosis - a Linear Synthesis Framework using MATLAB**
  - Instructor: Andreas Varga, retired from German Aerospace Center
  - Daniel Ossmann, German Aerospace Center

- **Computational Issues in Nonlinear Control and Estimation**
  - Instructor: Arthur Krener, Naval Postgraduate School, Monterey CA, USA

- **Energy-Based Control Design to Face the Challenges of Future Power Systems**
  - Instructor: Romeo Ortega, CNRS L2S, Univ. Paris-Saclay, France
  - Johannes Schiffer, University of Leeds, UK

- **Frequency and Nonlinear Control Designs**
  - Instructor: Frédéric Mazenc & Catherine Bonnet, INRIA, Paris-Saclay, France

- **Nonlinear Observers: Applications to Aerial Robotic Systems**
  - Instructor: Robert Mahony & Jochen Trumpf, Australian Nat. Univ
  - Tarek Hamel, CNRS Sophia-Antipolis, France

- **Homogeneity Based Design of Sliding Mode Controllers**
  - Instructor: Leonid Fridman & Jaime Alberto Moreno Pérez
  - Instituto de Ingeniería, UNAM, Mexico

- **Game Theory and Distributed Control**
  - Instructor: Jeff S. Shamma, KAUST, Jeddah, Saudi Arabia
  - Jason R. Marden, Univ. of California, Santa Barbara, USA

- **Model Reduction for Linear and Nonlinear Systems**
  - Instructor: Alessandro Astolfi & Giordano Scarciotti, Imperial College, London, UK

- **Robust and Adaptive Output Regulation of**
  - Instructor: Alberto Isidori, Sapienza Università di Roma, Italy
Many thanks to

Students & postdocs:
- Pierre-Jean Meyer
- Adnane Saoud
- Alina Eqtami
- Vladimir Sinyakov
- Zohra Kader
- Euriell Le Corronc
- Sebti Mouelhi
- Javier Camara

Collaborators:
- Laurent Fribourg
- Gregor Gössler
- Majid Zamani
- Paulo Tabuada
- Giordano Pola
- George Pappas