A coalgebraic approach to supervisory control of partially observed Mealy automata

Jun Kohjina[1], Toshimitsu Ushio[1], Yoshiki Kinoshita[2]

[1]Graduate School of Engineering Science, Osaka University, Japan
[2]National Institute of Advanced Industrial Science and Technology, Japan

CALCO 2011

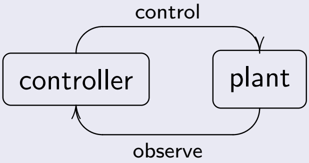
Outline

1. Introduction
2. Supervisory control (not using coalgebra)
3. Coalgebraic formulation
4. Solution to the problem
5. Conclusion

Introduction

Control problem

Given a $\boxed{\text{plant}}$ and a $\boxed{\text{spec}}$, design a $\boxed{\text{controller}}$ such that

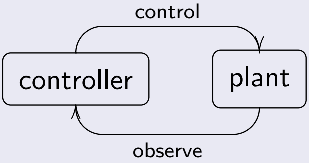


satisfies $\boxed{\text{spec}}$.

Introduction

Control problem

Given a plant and a spec, design a controller such that



satisfies spec.

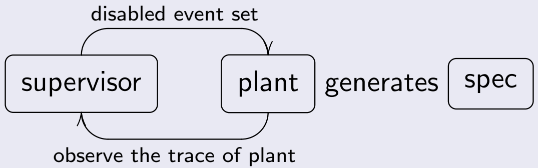
Our interest

- **When does a controller exist?**
- How do we design the controller?

Supervisory control

Control theory for discrete event systems [Ramadge and Wonham 1987]

communication networks, manufacturing systems, traffic systems



plant — deterministic partial automaton (X, A, δ, x_0)

spec — non-empty prefix closed language over A

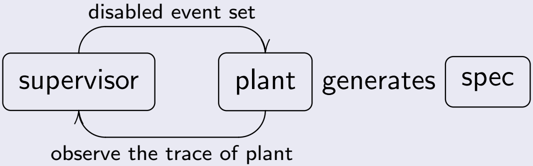
supervisor — function from a trace to a disabled event set

$S : A^* \to \mathcal{P}(A)$

Settings

- **Uncontrollable event** [Ramadge and Wonham 1987]
  event set $A = A_c + A_{uc}$, supervisor $S : A^* \to \mathcal{P}(A_c)$
  - A_c:controllable event set
  - A_{uc}:uncontrollable event set (not disabled by a supervisor)
- **Partial observation** [Ramadge and Wonham 1988, Cieslak et.al 1988]
  event set $A = A_o + A_{uo}$, supervisor $S : (A_o)^* \to \mathcal{P}(A_c)$
  - A_o:observable event set
  - A_{uo}:unobservable event set (not observed by a supervisor)
- **Partially observed Mealy automata** [Takai and Ushio 2009]
  plant modeled by a Mealy automaton
  supervisor $S : (B_o)^* \to \mathcal{P}(A_c)$
  - input event:$A = A_c + A_u$
  - output event:$B = B_o + B_u$

Our approach



plant	$\mathcal{M} \xrightarrow{m} (1 + B \times \mathcal{M})^A$	partial Mealy automaton
spec	$\mathcal{L} \xrightarrow{l} (1 + \mathcal{L})^A$	partial automaton
supervisor	$\mathcal{S} \xrightarrow{\langle o,t \rangle} \mathcal{P}(A_c) \times \mathcal{S}^{B_o}$	Moore automaton

Plant, Spec and Supervisor, coalgebraically

- **Plant** : $\mathcal{M} \xrightarrow{m} (1 + B \times \mathcal{M})^A$

$$\mathcal{M} = \left\{ M : A^* \rightharpoonup B^* \;\middle|\; \begin{array}{c} M \text{ is prefix- and length-preserving.} \\ \mathrm{dom}(M) \neq \emptyset. \end{array} \right\}$$

$m(M)(a) = \text{if } a \in \mathrm{dom}(M) \text{ then } \langle M(a), M_a \rangle \text{ else } \perp.$

where $M_a(w) = \mathsf{tail} \circ M(aw)$.

- **Spec** : $\mathcal{L} \xrightarrow{l} (1 + \mathcal{L})^A$

$\mathcal{L} = \{L \subseteq A^* \mid L \text{ is prefix-closed and nonempty.}\}$

$l(L)(a) = \text{if } a \in L \text{ then } L_a \text{ else } \perp.$

where $L_a := \{w \in A^* \mid aw \in L\}$.

- **Supervisor** : $\mathcal{S} \xrightarrow{\langle o,t \rangle} \mathcal{P}(A_c) \times \mathcal{S}^{B_o}$

$\mathcal{S} = \{S : (B_o)^* \to \mathcal{P}(A_c).\}$

$o(S) = S(\varepsilon),\; t(S)(b) = S_b,$ where $S_b(w) = S(bw)$.

Coinductive definition of supervisory composition

$$
\begin{tikzcd}
\mathcal{S} \times \mathcal{M} \arrow[r, dashed, "\exists!\ /"] \arrow[d, "\mathsf{spv}"'] & \mathcal{L} \arrow[d, "l", "\mathsf{final}"'] \\
(1 + \mathcal{S} \times \mathcal{M})^A \arrow[r, dashed, "(\mathrm{id}_1 + /)^A"'] & (1 + \mathcal{L})^A
\end{tikzcd}
$$

$$
\begin{aligned}
\mathcal{S} &= \{S : (B_o)^* \to \mathcal{P}(A_c)\} \\
\mathcal{M} &= \{M : A^* \rightharpoonup B^* \mid \cdots\} \\
\mathcal{L} &= \{L \subseteq A^* \mid \cdots\}
\end{aligned}
$$

$$
\mathsf{spv}\,\langle S, M\rangle\,(a) =
\begin{cases}
\langle S_b, M_a\rangle & \text{if } M \xrightarrow{a|b} M_a \wedge a \notin o(S) \wedge b \in B_o, \\
\langle S, M_a\rangle & \text{if } M \xrightarrow{a|b} M_a \wedge a \notin o(S) \wedge b \in B_u, \\
\perp & \text{otherwise.}
\end{cases}
$$

$/ : \mathcal{S} \times \mathcal{M} \to \mathcal{L}$ is the supervisory composition.
S/M represents a language generated by the controlled plant.

Formulation of supervisory control problem

Supervisory control problem

Given a plant $M \in \mathcal{M}$ and a specification $K \in \mathcal{L}$, find a supervisor $S \in \mathcal{S}$ satisfying

$$S/M = K.$$

$/ : \mathcal{S} \times \mathcal{M} \to \mathcal{L}$

- $\mathcal{S} = \{S : (B_o)^* \to \mathcal{P}(A_c).\}$
- $\mathcal{M} = \left\{ M : A^* \rightharpoonup B^* \;\middle|\; \begin{array}{c} M \text{ is prefix- and length-preserving} \\ \mathrm{dom}(M) \neq \emptyset. \end{array} \right\}$
- $\mathcal{L} = \{L \subseteq A^* \mid L \text{ is prefix-closed and non-empty.}\}$

Comparison

- Supervised product [Komenda & van Schuppen 2005]

$$(M/N)_a =$$

$$\begin{cases} M_a/N_a & \text{if } M \xrightarrow{a} \wedge N \xrightarrow{a}, \\ \left(\bigcup_{\langle M', M\rangle \in \text{Aux}} M'_a\right)/N_a & \text{if } M \not\xrightarrow{a} \wedge \exists M' \in DK : M' \approx M \text{ s.t. } M' \xrightarrow{a} \wedge N \xrightarrow{a} \wedge a \in A_c \cup A_o, \\ 0/N_a & \text{if } (\forall M' \in DK : M' \approx M) M' \not\xrightarrow{a} \wedge N \xrightarrow{a} \wedge a \in (A_{uc} \cap A_o), \\ M/N_a & \text{if } M \not\xrightarrow{a} \wedge N \xrightarrow{a} \wedge a \in A_{uc} \cap A_{uo}, \\ \emptyset & \text{otherwise.} \end{cases}$$

- Our work

$$\text{spv}\,\langle S, M\rangle\,(a) =$$

$$\begin{cases} \langle S_b, M_a\rangle & \text{if } M \xrightarrow{a|b} M_a \wedge a \notin o(S) \wedge b \in B_o, \\ \langle S, M_a\rangle & \text{if } M \xrightarrow{a|b} M_a \wedge a \notin o(S) \wedge b \in B_u, \\ \perp & \text{otherwise.} \end{cases}$$

$$S(w) = A_c \setminus \{a \in A_c \mid \exists u \in A^* : (K_0 \xrightarrow{ua}) \wedge (P \circ M_0(u) = w)\}$$

Partial bisimulation relation

Definition

Let (X, ξ) and (Y, η) be $(1 + -)^A$-coalgebras.
A partial bisimulation relation is a binary relation $R \subseteq X \times Y$ satisfying (1), (2), and (3).

(1)similarity $\forall a \in A$, $\forall x, x' \in X$, $y \in Y$, $\exists y' \in Y$,

$$x \; R \; y \wedge x \xrightarrow{a} x' \implies y \xrightarrow{a} y' \wedge x' \; R \; y'.$$

(2)controllability $\forall a \in A_u$, $\forall x \in X$, $\forall y, y' \in Y$, $\exists x' \in X$,

$$x \; R \; y \wedge y \xrightarrow{a} y' \implies x \xrightarrow{a} x' \wedge x' \; R \; y'.$$

(3)observability $\forall a \in A_c$, $\forall x \in X$, $\forall y, y' \in Y$, $\exists x' \in X$,

$$x \; R \; y \wedge y \xrightarrow{a} y' \wedge (\exists q \in X, \; (x \approx q) \wedge (q \xrightarrow{a})) \implies x \xrightarrow{a} x' \wedge x' \; R \; y'.$$

$$\approx = \left\{ \langle x, x' \rangle \;\middle|\; \exists w, w' \in A^*, x_0 \xrightarrow{w} x, x_0 \xrightarrow{w'} x', P \circ M(w) = P \circ M(w'). \right\}$$

When does a supervisor exist?

Theorem

Given a plant $M_0 \in \mathcal{M}$ and a specification $K_0 \in \mathcal{L}$, the following two conditions are equivalent.
(1) $\exists S \in \mathcal{S}$, $S/M_0 = K_0$
(2) There exists a partial bisimuration relation $R \subseteq \mathcal{L} \times \mathcal{L}$ *such that* $K_0 \; R \; \mathrm{dom}(M_0)$.

When does a supervisor exist?

Theorem

Given a plant $M_0 \in \mathcal{M}$ and a specification $K_0 \in \mathcal{L}$, the following two conditions are equivalent.
(1) $\exists S \in \mathcal{S},\ S/M_0 = K_0$
(2) There exists a partial bisimuration relation $R \subseteq \mathcal{L} \times \mathcal{L}$ such that $K_0\ R\ \mathrm{dom}(M_0)$.

$(2) \implies (1)$

$$S(w) = A_c \setminus \{a \in A_c \mid \exists u \in A^* : (K_0 \xrightarrow{ua}) \wedge (P \circ M_0(u) = w)\}$$

is a desired supervisor.

Modified normality

Problem

When no supervisor satisfies the specification, find the largest sublanguage of the specification.

- In general, there doesn't exist the largest controllable and observable sublanguage. (not closed under the arbitrary union)
- Therefore, we introduce a notion of *modified normality*. (closed under the arbitrary union)

Modified normality

Problem

When no supervisor satisfies the specification, find the largest sublanguage of the specification.

- In general, there doesn't exist the largest controllable and observable sublanguage. (not closed under the arbitrary union)
- Therefore, we introduce a notion of *modified normality*. (closed under the arbitrary union)

Compute the largest controllable and modified normal sublanguage of the specification.

Controllable and modified normal relation

Definition

Let (X, ξ) and (Y, η) be $(1 + -)^A$-coalgebras.
A *controllable and modified normal relation* is a binary relation $R \subseteq X \times Y$ satisfying (1), (2), and (3).

(1)similarity $\forall a \in A$, $\forall x, x' \in X$, $\forall y \in Y$, $\exists y' \in Y$,

$$x \; R \; y \wedge x \xrightarrow{a} x' \implies y \xrightarrow{a} y' \wedge x' \; R \; y'$$

(2)controllability $\forall a \in A_u$, $\forall x \in X$, $\forall y, y' \in Y$, $\exists x' \in X$,

$$x \; R \; y \wedge y \xrightarrow{a} y' \implies x \xrightarrow{a} x' \wedge x' \; R \; y'$$

(3)modified normality $\forall a \in A_c$, $\forall x \in X$, $\forall y, y' \in Y$, $\exists x' \in X$,

$$x \; R \; y \wedge y \xrightarrow{a} y' \wedge (\exists q \in X, \exists a' \in A, (x \approx q) \wedge (q \xrightarrow{a'})) \implies x \xrightarrow{a} x' \wedge x' \; R \; y'.$$

Properties of modified normality

- controllable and modified normal relation
  $\implies$ partial bisimulation relation
- Let $\{K_i\}_{i \in I}$ be a family of prefix-closed languages.
  $\forall i \in I$, $\exists$controllable and modified normal relation R_i such that $K_i \ R_i \ L$
  $\implies$ $\exists$controllable and modified normal relation R such that $\left(\bigcup_{i \in I} K_i\right) R \ L$.

Supremal controllable and modified normal

Theorem

Let K and L be two prefix closed languages and $\tilde{R}_0$ be the greatest fixpoint of Φ_{R_0}.
$\exists K' \in \mathcal{L}$ such that $K' \subseteq K$ and $\exists$ controllable and modified normal relation R such that $K'\ R\ L$.
$\implies K\ \tilde{R}_0\ L$ and beh $\langle K, L\rangle$ *is the supremal controllable and modified normal sublanguage.*

$$\Phi_{R_0} : \mathcal{P}(R_0) \to \mathcal{P}(R_0),\ R_0 = \{\langle K_w, L_w\rangle \mid w \in K \cap L\}$$

$$\Phi_{R_0}(H) = \left\{ \langle x, y\rangle \in H \;\middle|\; \begin{array}{c} \forall a \in A_u : y \xrightarrow{a} y' \implies x \xrightarrow{a} x' \wedge x'\ H\ y' \text{ and} \\ \forall a \in A_c : y \xrightarrow{a} y' \wedge (\exists q \in X, (q \to) \wedge x \approx_M^{x_0} q) \\ \implies x \xrightarrow{a} x' \wedge x'\ H\ y'. \end{array} \right\}$$

Conclusion

Summary

- Coalgebraic formulation of the supervisory control problem
- Necessary and sufficient condition for the existence of a supervisor
- Algorithm to compute the largest controllable modified normal sublanguage

Future work includes:

- Categorical characterisation of partial bisimulations
- (Non)linear system and hybrid system