A General Approach for Synthesis of Supervisors for Partially-Observed Discrete-Event Systems

Xiang Yin and Stéphane Lafortune

EECS Department, University of Michigan

19th IFAC WC, August 24-29, 2014, Cape Town, South Africa
Introduction

- Supervisory control under partial observation

\[ S(s) \]

\[ S: E^*_o \rightarrow \Gamma \]

Supervisor

\[ E = E_c \cup E_{uc} = E_o \cup E_{uo} \]

- Supervisor \( S: P(L(G)) \rightarrow \Gamma \), where \( \Gamma := \{ \gamma \in 2^E: E_{uc} \subseteq \gamma \} \)
$G = (X, E, f, x_0)$ is a deterministic FSA

- $X$ is the finite set of states;
- $E$ is the finite set of events;
- $f : X \times E \rightarrow X$ is the partial transition function;
- $x_0$ is the initial state.
System Model

\[ G = (X, E, f, x_0) \] is a deterministic FSA

- \( X \) is the finite set of states;
- \( E \) is the finite set of events;
- \( f : X \times E \rightarrow X \) is the partial transition function;
- \( x_0 \) is the initial state.

- Specification automaton \( H : K = \mathcal{L}(H) \subseteq \mathcal{L}(G) \)
- Assumption: illegality is captured by states \( (w.l.o.g.) \)
  \[ X_H \subseteq X \] is the set of legal states
• Existence Condition: (Controllability and Observability Theorem)

There exists a supervisor such that $\mathcal{L}(S/G) = K$ if and only if $K$ is controllable and observable.
Problem Formulation

• Existence Condition: (Controllability and Observability Theorem)
  There exists a supervisor such that $\mathcal{L}(S/G) = K$ if and only if $K$ is controllable and observable.

• Synthesis Problem: (BSCOP $^{max}$)
  Given a plant $G$ and specification $H$. Find a supervisor $S: E^*_o \rightarrow \Gamma$ such that
  1). $\mathcal{L}(S/G) \subseteq \mathcal{L}(H)$;  \hspace{2cm} \text{(Safety)}
  2). $\mathcal{L}(S/G) \not\subseteq \mathcal{L}(S'/G)$, $\forall$ safe $S'$. \hspace{2cm} \text{(Maximal Permissiveness)}
Literature Survey


(Initial works; Supremal normal solution)
Literature Survey


  (Initial works; Supremal normal solution)


  (Solutions larger than supremal normal)


(Online control; Only for safety specification; A certain class of maximal policies)
Literature Survey


Why we need a new approach?

- Observability is not preserved under union
  - algebraic approach cannot obtain a maximal solution
  - synthesis of maximally-permissive safe and non-blocking supervisor is open

- Solution space may be infinite
  - how to solve optimal control problem?
What is our new approach?

- Bipartite transition system
  - A game structure between the controller and the system
  - Enumerates all (infinite) legal solutions using a finite structure
  - A state-based approach for synthesis
  - Inspired by methodologies in reactive synthesis literature
Information State: a set of states, $I := 2^X$
Bipartite Transition System

Definition. (BTS).
A bipartite transition system $T$ w.r.t. $G$ is a 7-tuple

$$T = (Q_Y, Q_Z, h_{YZ}, h_{ZY}, E, \Gamma, y_0)$$

where

- $Q_Y \subseteq I$ is the set of $Y$-states;
- $Q_Z \subseteq I \times \Gamma$ is the set of $Z$-states so that $z = (I(z), \Gamma(z))$;
- $h_{YZ}: Q_Y \times \Gamma \to Q_Z$ represents the unobservable reach;
- $h_{ZY}: Q^T_Z \times E \to Q_Y$ represents the observation transition;
- $E$ is the set of events of $G$;
- $\Gamma$ is the set of admissible control decisions of $G$;
- $y_0 = \{x_0\}$ is the initial state.

Information State: a set of states, $I := 2^X$
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\} \]

Illegal states = \( X \setminus X_H = \{15\} \)
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, \quad E_o = \{o_1, o_2\} \]

Illegal states = \( X \setminus X_H = \{15\} \)
Bipartite Transition System

$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$

Illegal states $= X \setminus X_H = \{15\}$
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\} \]

Illegal states = \( X \setminus X_H = \{15\} \)
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\} \]

Illegal states = \( X \setminus X_H = \{15\} \)
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\} \]

Illegal states \(X \setminus X_H = \{15\}\)
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\} \]

Illegal states = \( X \setminus X_H = \{15\} \)
Bipartite Transition System

$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states $= X \setminus X_H = \{15\}$
Bipartite Transition System

\[ E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\} \]

Illegal states = \( X \setminus X_H = \{15\} \)
Total Controller
A BTS $T$ that enumerates all control decisions at $Y$ and all observations at $Z$
Total Controller

A BTS $T$ that enumerates *all* control decisions at $Y$ and *all* observations at $Z$

$E_c = \{c_1, c_2\}, \ E_o = \{o_1, o_2\}$

Illegal states = $X \setminus X_H = \{15\}$
Safety Binary function for Information State:

\[ D_I: I \to \{0, 1\} \]

\[ D_I(i) = \begin{cases} 
1, & \text{if } \forall x \in i: x \in X_H \\
0, & \text{otherwise} 
\end{cases} \]
Safety Binary function for Information State:

\[ D_I: I \rightarrow \{0,1\} \]

\[ D_I(i) = \begin{cases} 
1, & \text{if } \forall x \in i: x \in X_H \\
0, & \text{otherwise} 
\end{cases} \]

Safety Binary function for Y and Z-states:

\[ D_Y: I \rightarrow \{0,1\} \text{ and } D_Z: I \times \Gamma \rightarrow \{0,1\} \]

\[ D_Y(y) = \begin{cases} 
1, & \text{if } D_I(y) = 1 \text{ and } \exists \gamma \in \Gamma: D_Z(h_{YZ}(y, \gamma)) = 1 \\
0, & \text{otherwise} 
\end{cases} \]

\[ D_Z(z) = \begin{cases} 
1, & \text{if } D_I(I(z)) = 1 \text{ and } \forall e \in \gamma \cap E_0: D_Y(h_{ZY}(z, e)) = 1 \\
0, & \text{otherwise} 
\end{cases} \]
All Inclusive Controller:

The All Inclusive Controller for $G$

$$\mathcal{AICC}(G) = (Q^\mathcal{AICC}_Y, Q^\mathcal{AICC}_Z, h^\mathcal{AICC}_{YZ}, h^\mathcal{AICC}_{ZY}, E, \Gamma, y_0),$$

is defined as the largest BTS consisting of only safe reachable $Y$ and $Z$-states, and the transitions between them.
All Inclusive Controller

The All Inclusive Controller for $G$

$$\mathcal{AJC}(G) = (Q^AICG, Q_Z^{AICG}, h_{YZ}^{AICG}, h_{ZY}^{AICG}, E, \Gamma, \gamma_0),$$

is defined as the largest BTS consisting of only safe reachable Y and Z-states, and the transitions between them.

$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$
All Inclusive Controller:

The All Inclusive Controller for $G$

$$\mathcal{AIC}(G) = (Q^\text{AICG}_Y, Q^\text{AICG}_Z, h^\text{AICG}_{YZ}, h^\text{AICG}_{ZY}, E, \Gamma, y_0),$$

is defined as the largest BTS consisting of only safe reachable Y and Z-states, and the transitions between them.

$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states $= X \setminus X_H = \{15\}$
Construction of the AIC

- Pruning states from the total controller $O((2^{|X|})^2)$
Construction of the AIC

- Pruning states from the total controller $O((2^{|X|})^2)$
- Our Approach $O(2^{|X|})$
  - Pre-compute the extended specification
  - $V(x) = \infty \iff \exists s \in E_{uc}^*: f(x, s) \in X \setminus X_H$
  - $D_Y(y) = 0 \iff \exists x \in y: V(x) = \infty$
  - Construct the AIC by a DFS
Properties of the AIC

Theorem.
There exists a safe partial observation supervisor if and only if $AIC(G)$ is non-empty.

Theorem.
$$(\bar{L} = L \subseteq \mathcal{L}(H) \land L \text{ is observable} \land L \text{ is controllable}) \iff L \in \mathcal{L}_TS(AIC(G))$$
Properties of the AIC

Theorem.
There exists a safe partial observation supervisor if and only if $\mathcal{AIC}(G)$ is non-empty.

Theorem.

$(\bar{L} = L \subseteq \mathcal{L}(H) \land L$ is observable $\land L$ is controllable $) \iff L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$
Theorem.
There exists a safe partial observation supervisor if and only if $\mathcal{AIC}(G)$ is non-empty.

Theorem.
\[
\overline{L} = L \subseteq \mathcal{L}(H) \land L \text{ is observable } \land L \text{ is controllable} \iff L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))
\]
Theorem.
There exists a safe partial observation supervisor if and only if $\mathcal{AIC}(G)$ is non-empty.

Theorem.
$(\overline{L} = L \subseteq \mathcal{L}(H) \land L$ is observable $\land L$ is controllable$) \iff L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$

The AIC embeds all legal solutions!
Definition. (IS-Based Supervisor)

A partial observation supervisor $S_P$ is said to be information-state-based if

\[
(\forall s, t \in \mathcal{L}(S_P/G))[IS^Y_{SP}(s) = IS^Y_{SP}(t) \Rightarrow S_P(s) = S_P(t)]
\]

X.Yin & S.Lafortune (UMich)
Definition. (IS-Based Supervisor)

A partial observation supervisor $S_P$ is said to be information-state-based if

$$(\forall s, t \in \mathcal{L}(S_P/G))[IS^Y_{S_P}(s) = IS^Y_{S_P}(t) \Rightarrow S_P(s) = S_P(t)]$$

Theorem.

There exists at least one IS-based supervisor $S_I$ such that $\mathcal{L}(S_I/G)$ is a maximal safe, controllable and observable sublanguage.
Definition. (IS-Based Supervisor)

A partial observation supervisor $S_P$ is said to be information-state-based if

$$\forall s, t \in \mathcal{L}(S_P/G)[IS_{S_P}^Y(s) = IS_{S_P}^Y(t) \Rightarrow S_P(s) = S_P(t)]$$

Theorem.

There exists at least one IS-based supervisor $S_I$ such that $\mathcal{L}(S_I/G)$ is a maximal safe, controllable and observable sublanguage.

Our information state is correctly defined for safety specification
Synthesis of Safe and Maximally Permissive Supervisors

Synthesis Step:

1. Build the AIC
2. For any Y-state, pick one local maximal control decision
3. For any Z-state, pick all observations
4. Until reach a terminal state or a state that has been visited
Synthesis of Safe and Maximally Permissive Supervisors

Synthesis Step:
1. Build the AIC
2. For any Y-state, pick one local maximal control decision
3. For any Z-state, pick all observations
4. Until reach a terminal state or a state that has been visited
Synthesis of Safe and Maximally Permissive Supervisors

Synthesis Step:
1. Build the AIC
2. For any Y-state, pick one local maximal control decision
3. For any Z-state, pick all observations
4. Until reach a terminal state or a state that has been visited
Synthesis of Safe and Maximally Permissive Supervisors

Synthesis Step:

1. Build the AIC
2. For any Y-state, pick one local maximal control decision
3. For any Z-state, pick all observations
4. Until reach a terminal state or a state that has been visited
Synthesis Step:

1. Build the AIC
2. For any Y-state, pick one local maximal control decision
3. For any Z-state, pick all observations
4. Until reach a terminal state or a state that has been visited
Synthesis Step:
1. Build the AIC
2. For any Y-state, pick one local maximal control decision
3. For any Z-state, pick all observations
4. Until reach a terminal state or a state that has been visited
Summary

Contribution:

• A new bipartite transition system that captures \textit{all} safe decisions in a \textit{single} finite structure.
• Construction of the AIC
• Properties of the AIC
• Synthesis of supervisors based on the AIC
Summary

Contribution:

• A new bipartite transition system that captures all safe decisions in a single finite structure.
• Construction of the AIC
• Properties of the AIC
• Synthesis of supervisors based on the AIC

Future Work:

• Optimal synthesis problem
• Non-blocking specification
• Decentralized synthesis problem