Supervisory Control under Partial Observation

Rong Su
Outline

- Motivation
- The Concept of Observability
- Supervisor Synthesis under Partial Observation
- Example
- Conclusions
Three Main Concepts in Control

• Controllability
  – allows you to improve the dynamics of a system by feedback
  – e.g. controllability in the RW supervisory control theory

• Observability
  – allows you to deploy such feedback by using the system's output

• Optimality
  – gives rise to formal methods of control synthesis
  – e.g. supremality in the RW supervisory control theory
Example

\[ \Sigma = \{a, b, c, d\} \]

\[ \Sigma_c = \{b, d\} \]
Example (cont.)

\[ \Sigma = \{a, b, c, d\} \]
\[ \Sigma_c = \{b, d\} \]
Some Intuitions

- Supervisor can only act upon receiving observable events
- Partial observation forces a supervisor to be conservative
- We can enable or disable an unobservable event
Outline

• Motivation
• The Concept of Observability
• Supervisor Synthesis under Partial Observation
• Example
• Conclusions
Observability

- Given $G \in \phi(\Sigma)$, let $\Sigma_o \subseteq \Sigma$ and $P: \Sigma^* \to \Sigma_o^*$ be the natural projection.

- A language $K \subseteq L(G)$ is $(G,P)$-observable, if

\[
(\forall s \in \overline{K})(\forall \sigma \in \Sigma) \ s\sigma \in L(G) \overline{K} \Rightarrow P^{-1}P(s)\sigma \cap \overline{K} = \emptyset
\]

\[\Sigma_o = \{b\}\]
Or equivalently ...

- $K \subseteq L(G)$ is \((G,P)\)-observable, iff for any $s \in K$, $s' \in \Sigma^*$ and $\sigma \in \Sigma$, 
  
  $s\sigma \in L(G) - \bar{K} \land s'\sigma \in L(G) \land P(s) = P(s') \Rightarrow s'\sigma \in L(G) - \bar{K}$

or equivalently,

  $s\sigma \in \bar{K} \land s'\sigma \in L(G) \land P(s) = P(s') \Rightarrow s'\sigma \in \bar{K}$

(Think about why they are equivalent)
Example 1

- $\Sigma = \{a, b, c, d\}$
- $\Sigma_o = \{c\}$
- $K = \{ac, bc\}$

Question: is $K \ (G,P)$-observable? yes
Example 2

- $\Sigma = \{a,b,c,d\}$
- $\Sigma_o = \{c\}$
- $K = \{ac, bc\}$

Question: is $K$ $(G,P)$-observable? **no**
Example 3

- $\Sigma = \{a, b, c, d\}$
- $\Sigma_o = \{a, c\}$
- $K = \{ac, bc\}$

Question: is $K \ (G, P)$-observable? yes
(G,P)-observability is *decidable*. But how?
Procedure of Checking Observability: Step 1

• Let $G = (X, \Sigma, \xi, x_0, X_m)$
• Suppose $K$ is recognized by $A = (Y, \Sigma, \eta, y_0, Y_m)$, i.e. $K = L_m(A)$
• Let $A' = G \times A = (X \times Y, \Sigma, \xi \times \eta, (x_0, y_0), X_m \times Y_m)$
  – Since $K = L(A) \subseteq L(G)$, we have $L(G \times A) = L(A)$
• A state $(x, y) \in X \times Y$ is a boundary state of $A'$ w.r.t. $G$, if
  – $(\exists s \in L(A')) \xi \times \eta((x_0, y_0), s) = (x, y)$, i.e. $(x, y)$ is reachable from $(x_0, y_0)$
  – $(\exists \sigma \in \Sigma) \xi(x, \sigma)! \land \neg \eta(y, \sigma)!$, where “!” denotes “is defined”
• Let $B$ be the collection of all boundary states of $A'$ w.r.t. $G$
  – $B$ is a finite set. (Why?)
Procedure of Checking Observability : Step 2

• For each boundary state \((x,y)\in B\), we define two sets
  
  \[
  T(x,y) := \{ s \in L(A') | \xi \times \eta((x_0,y_0),s) = (x,y) \} \quad (T(x,y) \text{ is regular, why?})
  \]
  
  \[
  \Sigma(x,y) := \{ \sigma \in \Sigma | \xi(x,\sigma)! \land \neg \eta(y,\sigma)! \}
  \]

• Theorem

  \[
P^{-1}P(T(x,y))\Sigma(x,y) \cap \overline{K} = \emptyset
  \]
Example

- $\Sigma = \{a, b, c, d\}$
- $\Sigma_0 = \{c\}$
- $K = \{ac, bc\}$
Example – Step 1

- $\Sigma = \{a, b, c, d\}$
- $\Sigma_o = \{c\}$
- $K = \{ac, bc\}$

$A' = G \times A$

- $B = \{(1,1), (2,2)\}$
Example – Step 2

- For the boundary state (1,1) we have
  - \( T(1,1) = \{b\} \)
  - \( \Sigma(1,1) = \{c\} \)
  - \( P^{-1}P(T(1,1))\Sigma(1,1) \cap \overline{K} = \{bc,ac\} \cap \{ac,ba\} = \{ac\} \neq \emptyset \)

- For the boundary state (2,2) we have
  - \( T(2,2) = \{a\} \)
  - \( \Sigma(2,2) = \{d\} \)
  - \( P^{-1}P(T(2,2))\Sigma(2,2) \cap \overline{K} = \{ad\} \cap \{ac,ba\} = \emptyset \)

\( K \) is not observable w.r.t. \( G \) and \( P \)
Properties of Observable Languages

• Suppose $K_1$ and $K_2$ are closed, observable w.r.t. $G$ and $P$. Then
  – $K_1 \cap K_2$ is observable w.r.t. $G$ and $P$
  – $K_1 \cup K_2$ may not be observable w.r.t. $G$ and $P$

• Given a plant $G$, let
  \[ O(G) := \{ K \subseteq L(G) | K \text{ is closed and observable w.r.t. } G \text{ and } P \} \]

• The partially ordered set (poset) $(O(G), \subseteq)$ is a meet-semi-lattice
  – The greatest element may not exist (i.e. no supremal observable sublanguage)
Example

\[ \Sigma = \{ a, b, c, d, e \} \]
\[ \Sigma_o = \{ c \} \]

- \( K_1 \cap K_2 \) is observable, but \( K_1 \cup K_2 \) is not. (Why?)
Outline

• Motivation
• The Concept of Observability
• Supervisor Synthesis under Partial Observation
• Example
• Conclusions
Main Existence Result

• Theorem 1
  – Let $K \subseteq L_m(G)$ and $K \neq \emptyset$. There exists a proper supervisor iff
    • $K$ is controllable with respect to $G$
    • $K$ is observable with respect to $G$ and $P$
    • $K$ is $L_m(G)$-closed, i.e. $K = \overline{K \cap L_m(G)}$
Supervision under Partial Observation

- Suppose $K$ is controllable, observable and $L_m(G)$-closed.
- Let $A=(Y,\Sigma_o,\eta,y_0,Y_m)$ be the canonical recognizer of $P(K)$.
- We construct a new automaton $S=(Y,\Sigma,\lambda,y_0,Y_m)$ as follow:
  - For any $y \in Y$, an event $\sigma \in \Sigma - \Sigma_o$ is control-relevant w.r.t. $y$ and $K$, if
    $$(\exists s \in \overline{K}) \ \eta(y_0, P(s)) = y \land s \sigma \in \overline{K}$$
  - Let $\Sigma(y)$ be the collection of all events in $\Sigma - \Sigma_o$ control-relevant w.r.t. $y$, $K$
  - We define the transition map $\lambda: Y \times \Sigma \rightarrow Y$ as follows:
    - $\lambda$ is the same as $\eta$ over $Y \times \Sigma_o$
    - For any $y \in Y$ and $\sigma \in \Sigma(y)$, define $\lambda(y, \sigma) := y$ (i.e. selfloop all events of $\Sigma(y)$ at $y$)
    - For all other $(y, \sigma)$ pairs, $\lambda(y, \sigma)$ is undefined
- $S$ is a proper supervisor of $G$ under PO such that $L_m(S/G)=K$
Example

- $\Sigma = \{a, b, c, d\}$
- $\Sigma_0 = \{c\}$
- $K = \{ac, bc\}$

$G$

$K$

$L_m(S/G) = K$?
Difficulty of Synthesis

- Given a plant $G$ and a specification $\text{SPEC}$, let
  
  $\mathcal{O}(G,\text{SPEC}):=\{K \subseteq \mathbb{L}_m(G) \cap \mathbb{L}_m(\text{SPEC}) | K \text{ is controllable and observable}\}$

- Unfortunately, there is no supremal element in $\mathcal{O}(G,\text{SPEC})$. 
Solution 1: A New Supervisory Control Problem

- Given G, suppose we have $A \subseteq E \subseteq L(G)$.

- To synthesize a supervisor $S$ under partial observation such that

$$A \subseteq L(S/G) \subseteq E \quad (*)$$

- Let $O(A) := \{K \supseteq A \mid K \text{ is closed and observable w.r.t. } G \text{ and } P\}$

- Let $C(E) := \{K \subseteq E \mid K \text{ is closed and controllable w.r.t. } G\}$

- Theorem (Feng Lin)
  - Assume $A \neq \emptyset$. The (*) problem has a solution $S$ iff $\inf O(A) \subseteq \sup C(E)$
Solution 2 : The Concept of Normality

- Given $N \subseteq M \subseteq \Sigma^*$, we say $N$ is $(M,P)$-normal if

$$N = M \cap P^{-1}P(N)$$

- In particular, take $N = M \cap P^{-1}(K)$ for any $K \subseteq \Sigma_0^*$. Then $N$ is $(M,P)$-normal.

- $(\forall s_1, s_2 \in M) (s_1, s_2) \in \ker P \iff P(s_1) = P(s_2)$
- $N/\ker P \subseteq M/\ker P$
Properties of Normality

• Let $\mathcal{N}(E ; M) := \{N \subseteq E \mid N \text{ is } (M,P)\text{-normal}\}$ for some $E \subseteq \Sigma^*$
  
  – The poset $(\mathcal{N}(E ; M), \subseteq)$ is a complete lattice

    • The union of $(M,P)$-normal sublanguages is normal (intuitive explanation?)
    • The intersection of $(M,P)$-normal sublanguages is normal (intuitive explanation?)

  – Lin-Brandt formula: $\sup \mathcal{N}(E ; M) = E - P^{-1}P(M - E)$

    • In TCT: $N = \text{Supnorm}(E,M,\text{Null/Image})$

• Let $E \subseteq L_m(G)$, and $\overline{\mathcal{N}}(E ; L(G)):= \{N \subseteq E \mid \overline{N} \text{ is } (L(G),P)\text{-normal}\}$

  – $\overline{\mathcal{N}}(E ; M)$ is closed under arbitrary unions, but not under intersections
Relationship between Normality and Observability

- Let $K \subseteq L_m(G)$. Then

  $\overline{K}$ is $(L(G), P)$-normal $\Rightarrow$ $K$ is observable w.r.t. $G$ and $P$

- Let $\Sigma(K) := \{ \sigma \in \Sigma \mid (\exists s \in \overline{K}) s\sigma \in L(G) - \overline{K} \}$
  - $\Sigma(K)$ is the collection of all boundary events of $K$ w.r.t. $G$

  $K$ is observable w.r.t. $G$, $P \land \Sigma(K) \subseteq \Sigma_o \Rightarrow \overline{K}$ is $(L(G), P)$-normal
Supervisory Control under Normality

- Given a plant $G$ and a specification $E$, let
  \[ \mathcal{C}(G,E) := \{ K \subseteq L_m(G) \cap L_m(E) \mid K \text{ is controllable w.r.t. } G \} \]

- We define a new set
  \[ S(G,E) := \{ K \subseteq \Sigma^* \mid K \in \mathcal{C}(G,E) \land \overline{N}(L_m(E),L(G)) \land L_m(G) \text{-closed} \} \]
  \[ S(G,E) \text{ is nonempty and closed under arbitrary unions. sup } S(G,E) \text{ exists} \]

- Supervisory Control and Observation Problem (SCOP)
  - to compute a proper supervisor $S$ under partial observation such that
    \[ L_m(S/G) = \sup S(G,E) \]
The TCT Procedure for SCOP

• Given a plant $G$ and a specification $E$, let

$$A = \text{Supscop}(E,G,\text{Null/Image})$$

  - $L_m(A) = \sup S(G,E)$
  - Based on $A$, we construct a proper supervisor $S$ under partial observation
    - Why can we do that? Because $\sup S(G,E)$ is controllable and observable
Outline

• Motivation
• The Concept of Observability
• Supervisor Synthesis under Partial Observation
• Example
• Conclusions
Warehouse Collision Control

Traffic Light

Car 1
Receiving Dock

Sensor

Track 1
Track 2
Track 3
Track 4

Dispatching Dock

Car 2
Plant Model

• $\Sigma_1 = \{11, 12, 13, 15\}$, $\Sigma_{1,c} = \{11, 13, 15\}$, $\Sigma_{1,o} = \{11, 15\}$
• $\Sigma_2 = \{21, 22, 23, 25\}$, $\Sigma_{2,c} = \{21, 23, 25\}$, $\Sigma_{2,o} = \{21, 25\}$
Specification

- To avoid collision, $C_1$ and $C_2$ can’t reach the same state together
  - States (1,1), (2,2), (3,3) should be avoided in $C_1 \times C_2$
Synthesis Procedure in TCT

- Create the plant
  \[ G = \text{Sync}(C_1, C_2) \] (25 ; 40)

- Create the specification
  \[ E = \text{mutex}(C_1, C_2, [(1,1), (2,2), (3,3)]) \] (20 ; 24)

- Supervisor Synthesis
  \[ K = \text{Supscop}(E, G, [12,13,22,23]) \] (16 ; 16)
Transition Structure of K
A Proper Supervisor $S$ under Partial Observation

$K = L_m(S/G)$
Some Fact

- Perform the following TCT operation

\[ W = \text{Condat}(G,K) \]

- Only events 11 and 21 are required to be disabled.
- Therefore, we only need one traffic light at Track 1.
A Slight Modification

- \( \Sigma_{1,o} = \{11, 15\} \)
- \( \Sigma_{2,o} = \{21, 25\} \)
- \( \Sigma_{1,o} = \{11, 13\} \)
- \( \Sigma_{2,o} = \{21, 23\} \)
Synthesis Result

- Create the plant
  \[ G = \text{Sync}(C_1, C_2) \]  
  (25 ; 40)

- Create the specification
  \[ E = \text{Mutex}(C_1, C_2, [(1,1), (2,2), (3,3)]) \]  
  (20 ; 24)

- Supervisor Synthesis
  \[ K = \text{Supscop}(E, G, [12, 15, 22, 25]) \]  
  (empty)
  - Explain intuitively why this can happen (homework)
Conclusions

• Partial observation is important for implementation.
  – A supervisor can make a move only based on observations.

• The current observability is not closed under set union.
  – Thus, there is no supremal observable sublanguage (unfortunately).

• Normality is closed under set union.
  – Thus, the supremal normal sublanguage exists.
  – But the concept of normality is too conservative.