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

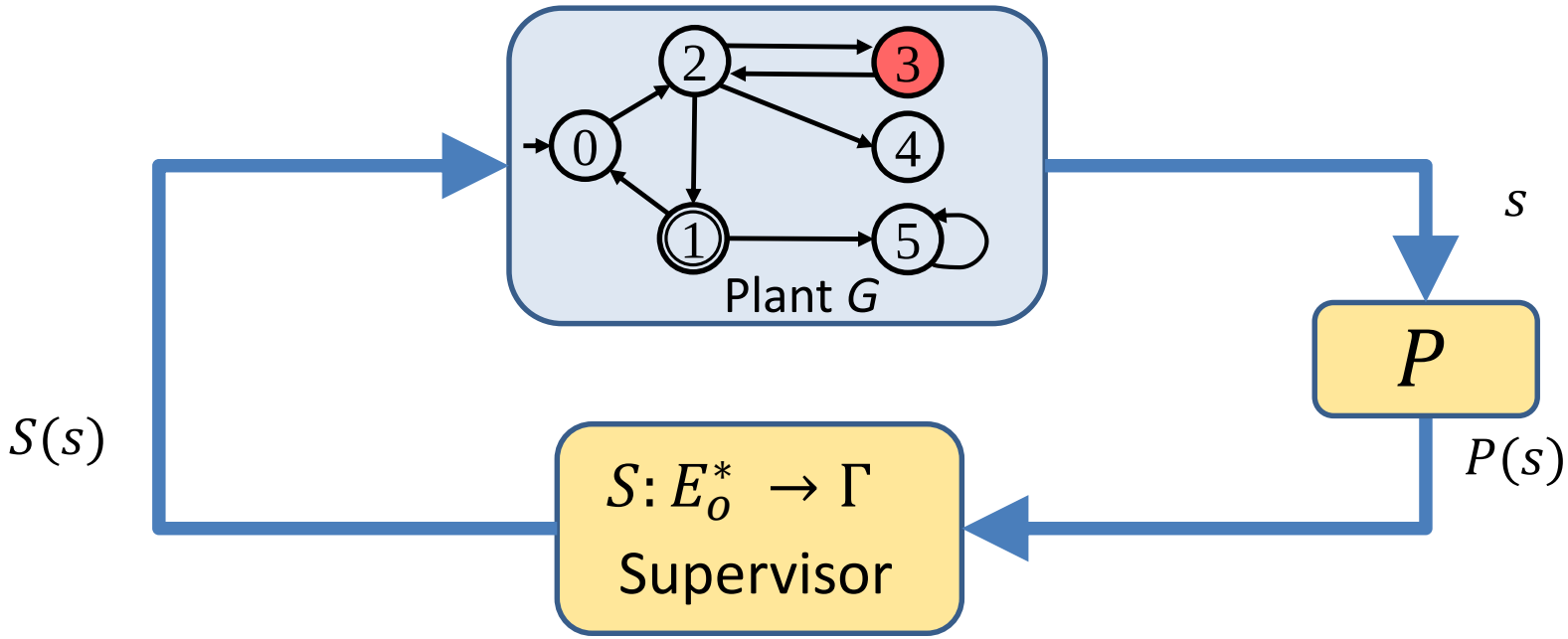
Xiang Yin and Stéphane Lafortune

EECS Department, University of Michigan

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

Introduction

- Supervisory control under partial observation



- $E = E_c \dot{\cup} E_{uc} = E_o \dot{\cup} E_{uo}$
- Supervisor $S: P(\mathcal{L}(G)) \to \Gamma$, where $\Gamma := \{\gamma \in 2^E : E_{uc} \subseteq \gamma\}$

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;
- $f: X \times E \to X$ 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;
- $f: X \times E \to X$ 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

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.

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 $S: E_o^* \to \Gamma$ such that

  1). $\mathcal{L}\,(S/G) \subseteq \mathcal{L}\,(H)$; (Safety)

  2). $\mathcal{L}(S/G) \not\subset \mathcal{L}(S'/G)$, $\forall$ safe S'. (Maximal Permissiveness)

Literature Survey

- F. Lin, and W. M. Wonham. "On observability of discrete-event systems." *Information sciences* 44.3 (1988): 173-198.
- R. Cieslak, et al. "Supervisory control of discrete-event processes with partial observations." *IEEE Transactions on Automatic Control,* 33.3 (1988): 249-260.

(Initial works; Supremal normal solution)

Literature Survey

- F. Lin, and W. M. Wonham. "On observability of discrete-event systems." *Information sciences* 44.3 (1988): 173-198.
- R. Cieslak, et al. "Supervisory control of discrete-event processes with partial observations." *IEEE Transactions on Automatic Control,* 33.3 (1988): 249-260.

(Initial works; Supremal normal solution)

- S. Takai, and T. Ushio. "Effective computation of an $\mathcal{L}_m(G)$-closed, controllable, and observable sublanguage arising in supervisory control." *Systems & Control Letters* 49.3 (2003): 191-200.
- K. Cai, R. Zhang, and W. M. Wonham. "Relative observability of discrete-event Systems and its supremal sublanguages." *IEEE Transactions on Automatic Control,* (2014).

(Solutions larger than supremal normal)

Literature Survey

- Heymann, Michael, and Feng Lin. "On-line control of partially observed discrete event systems." Discrete Event Dynamic Systems 4.3 (1994): 221-236.
- Hadj-Alouane, Nejib Ben, Stéphane Lafortune, and Feng Lin. "Centralized and distributed algorithms for on-line synthesis of maximal control policies under partial observation." Discrete Event Dynamic Systems 6.4 (1996): 379-427.

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

Literature Survey

- Heymann, Michael, and Feng Lin. "On-line control of partially observed discrete event systems." Discrete Event Dynamic Systems 4.3 (1994): 221-236.
- Hadj-Alouane, Nejib Ben, Stéphane Lafortune, and Feng Lin. "Centralized and distributed algorithms for on-line synthesis of maximal control policies under partial observation." Discrete Event Dynamic Systems 6.4 (1996): 379-427.

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

- K. Inan, “Nondeterministic supervision under partial observations,” in 11th International Conference on Analysis and Optimization of Systems: Discrete Event Systems. Springer, (1994): 39–48.

  (Decidability for safe and non-blocking; No synthesis)

- T.-S. Yoo, and S. Lafortune. "Solvability of centralized supervisory control under partial observation." *Discrete Event Dynamic Systems* 16.4 (2006): 527-553.

  (Solvability for safe and non-blocking; No maximality)

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

Bipartite Transition System

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

Bipartite Transition System

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

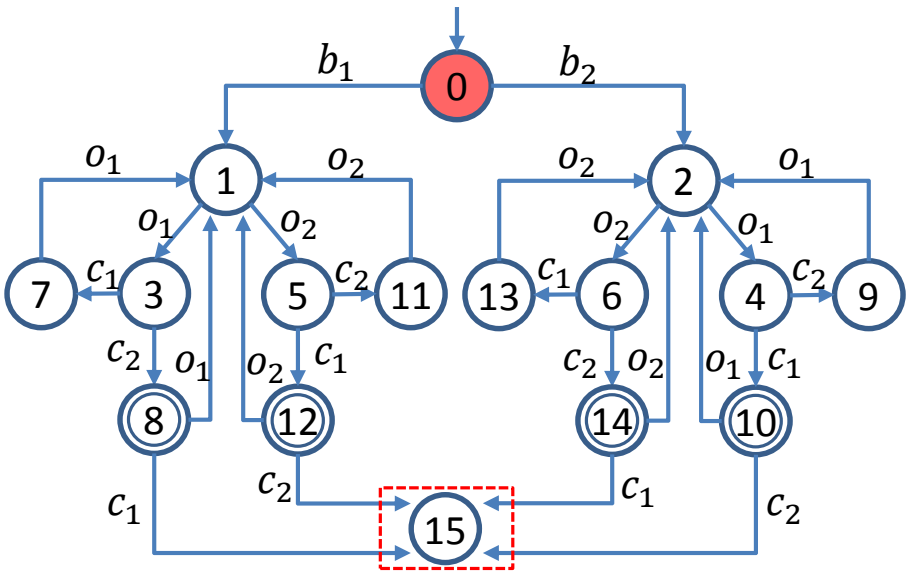
Definition. (BTS).
A bipartite transition system *T* w.r.t. *G* is a 7-tuple

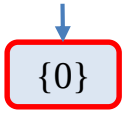
$$T = (Q_Y, Q_Z, h_{YZ}, h_{ZY}, E, \Gamma, y_0)$$

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 $\mathrm{z} = (I(z), \Gamma(z))$;
- $h_{YZ}: Q_Y \times \Gamma \to \mathrm{Q}_Z$ represents the unobservable reach;
- $h_{ZY}: Q_Z^T \times \mathrm{E} \to \mathrm{Q}_Y$ represents the observation transition;
- E is the set of events of G;
- Γ is the set of admissible control decisions of G;
- $y_0 = \{x_0\}$ is the initial state.

Bipartite Transition System

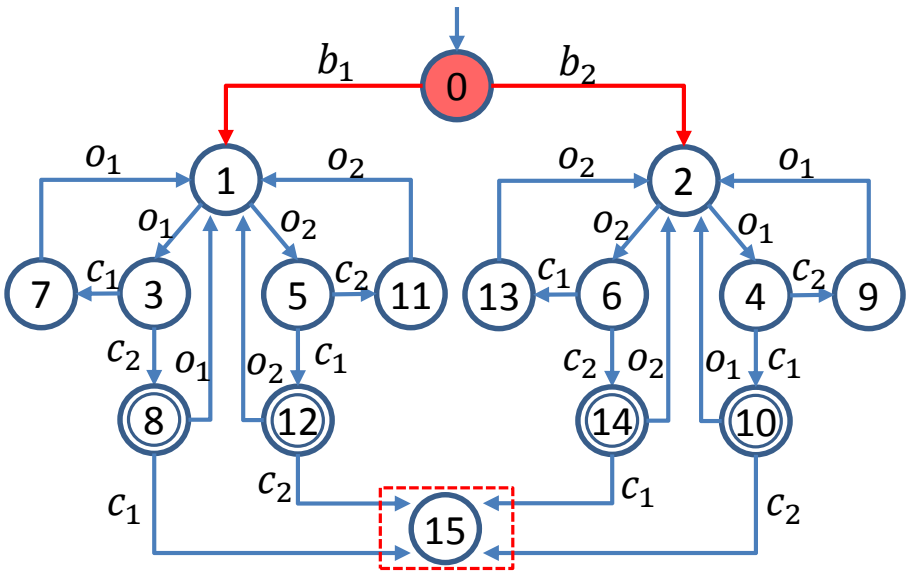


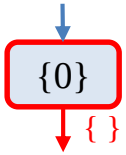


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

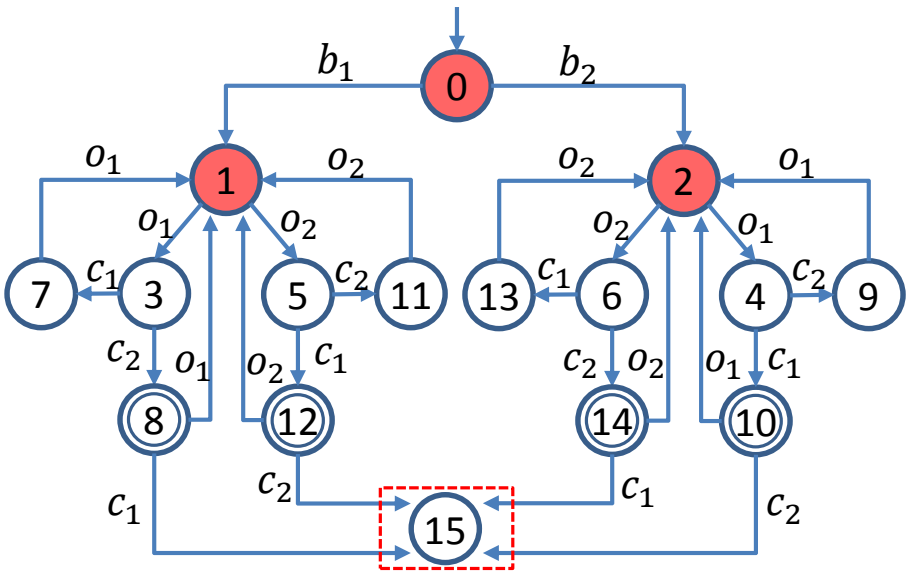


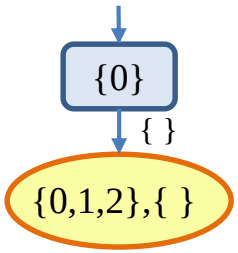


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

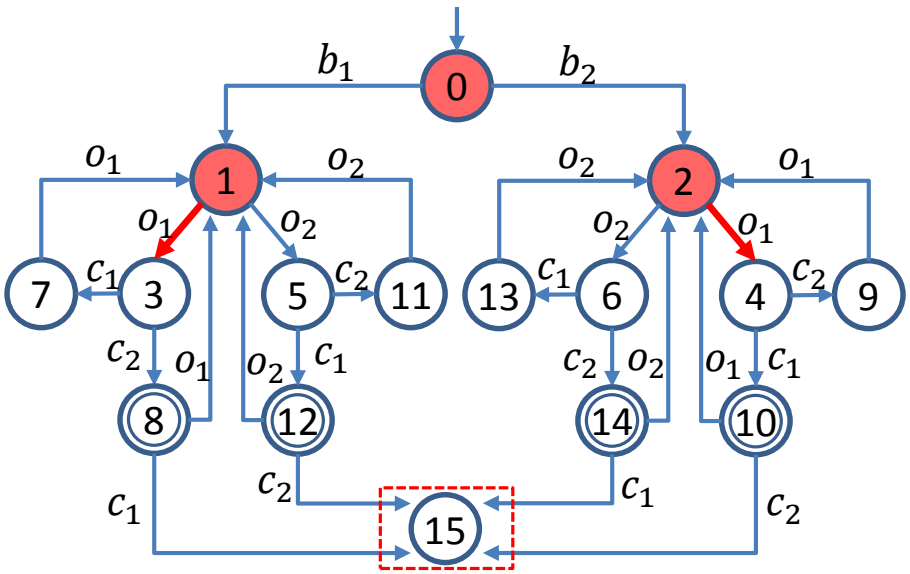


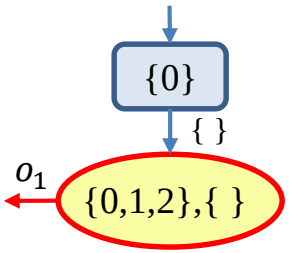


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

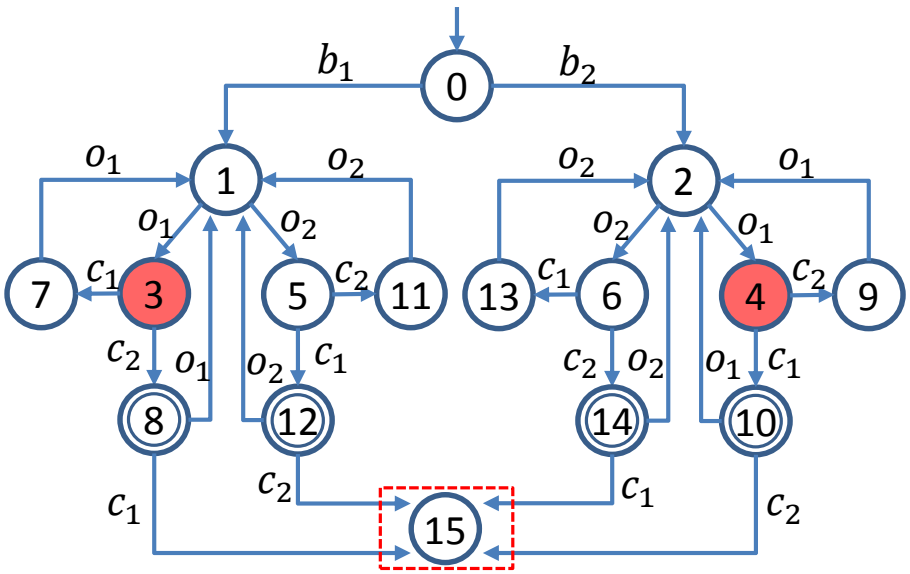


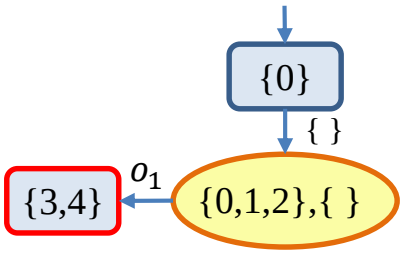


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

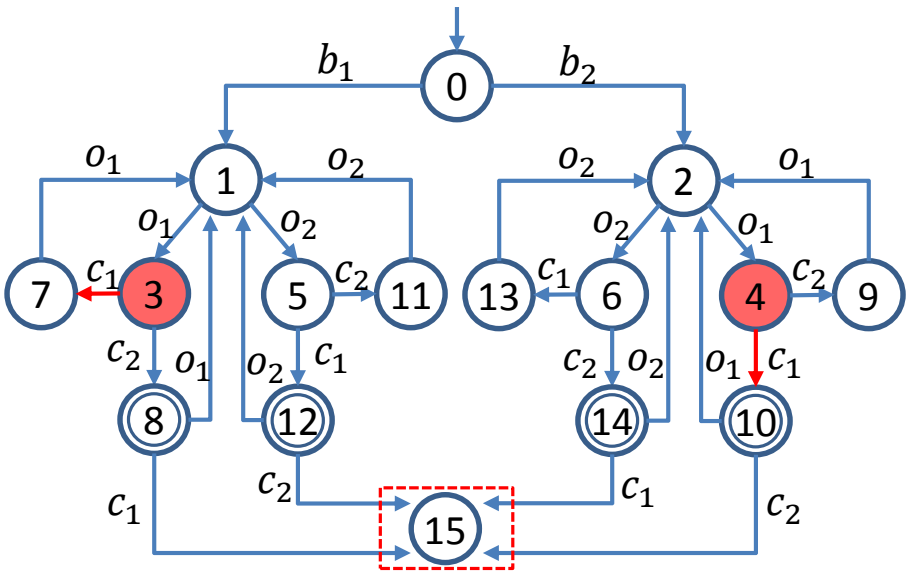


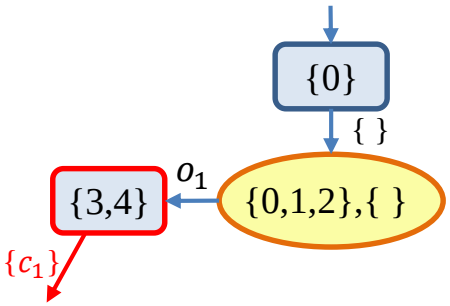


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

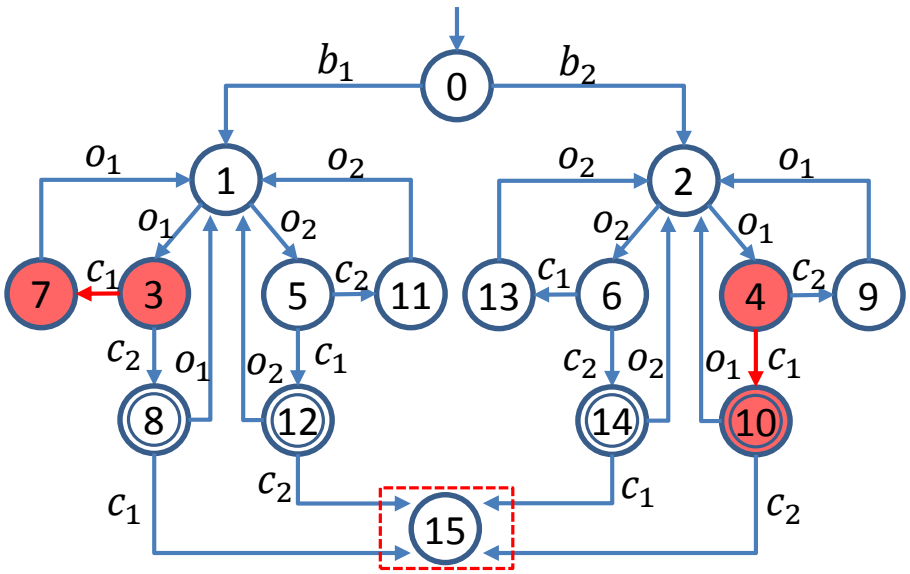


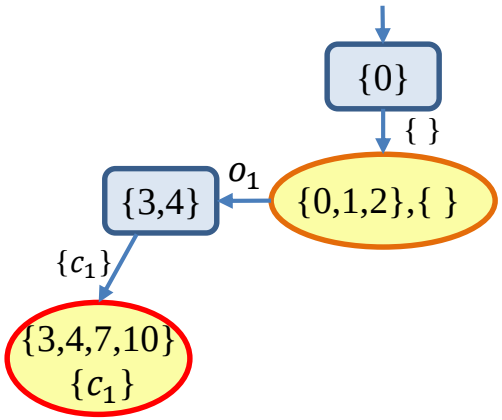


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

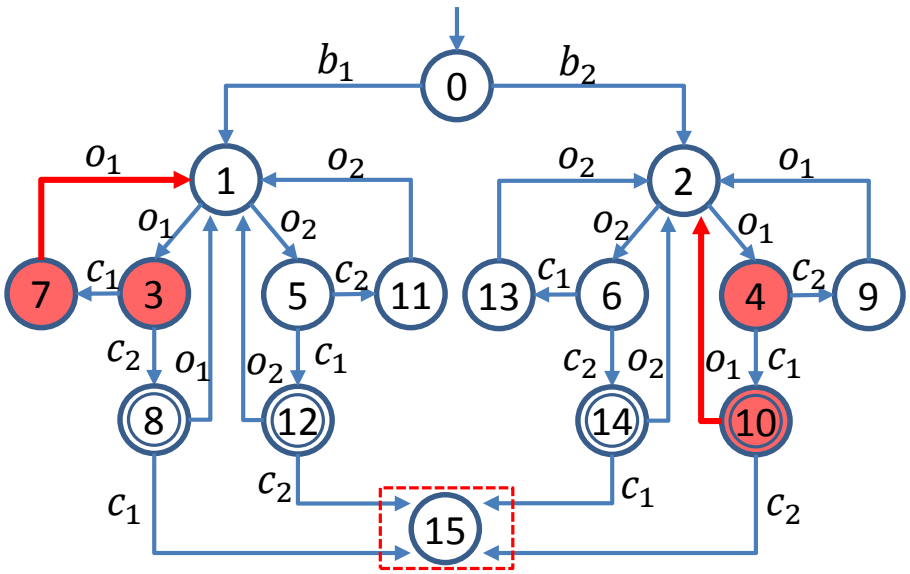


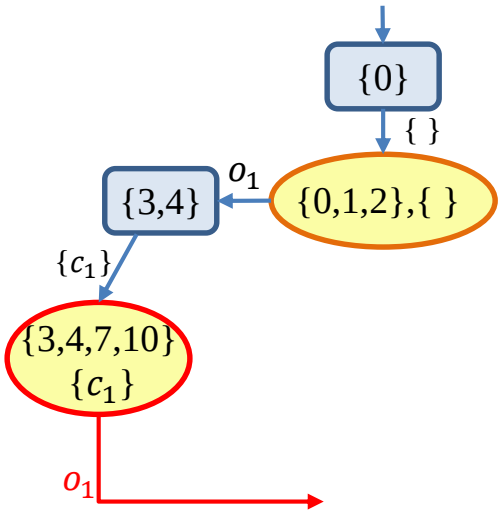


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System

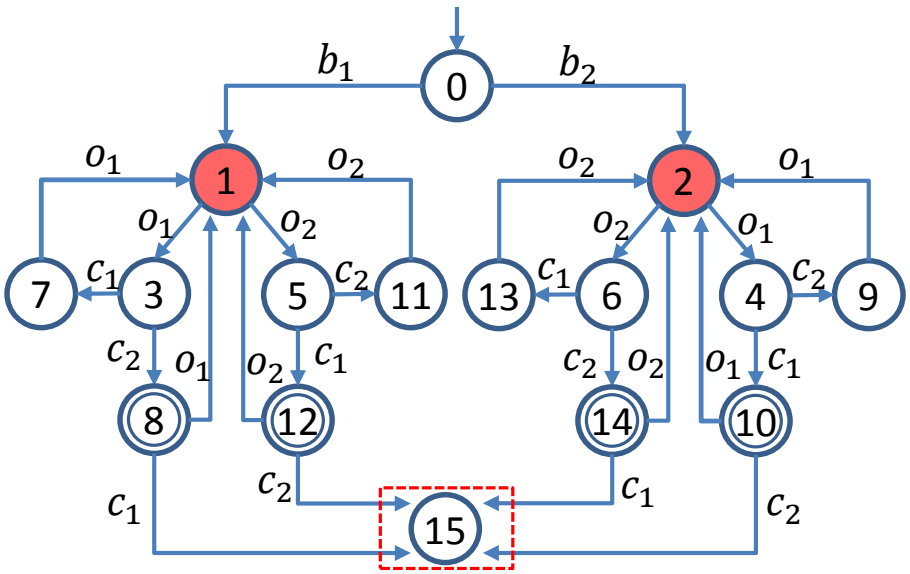


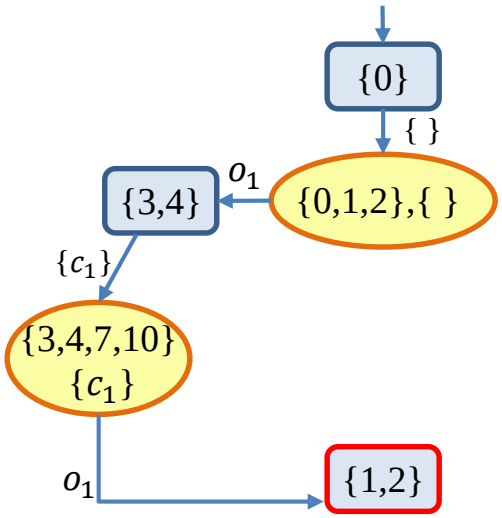


$$E_c = \{c_1, c_2\}, E_o = \{o_1, o_2\}$$

Illegal states$= X \setminus X_H = \{15\}$

Bipartite Transition System





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

Illegal states$= X \setminus X_H = \{15\}$

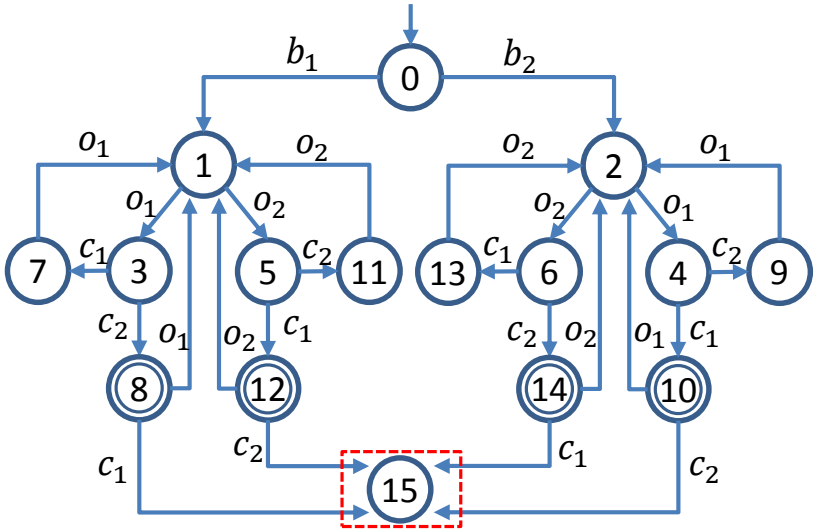
Total Controller

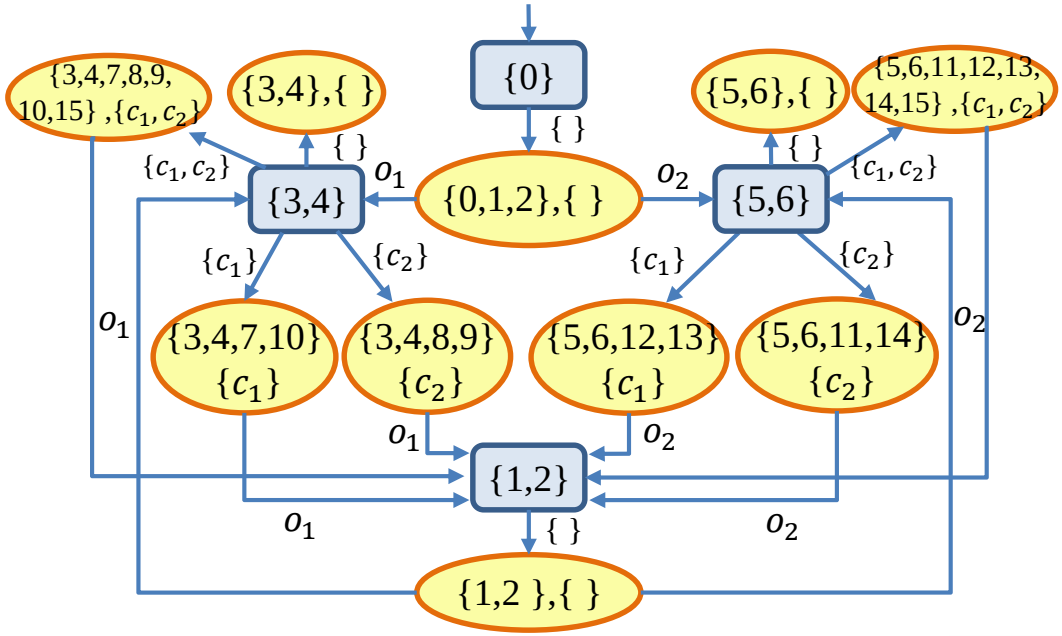
Total Controller

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

Total Controller

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

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

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 Y and Z-states:

$D_Y: I \to \{0,1\}$ and $D_Z: I \times \Gamma \to \{0,1\}$

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

$$D_Z(z) = \begin{cases} 1, & \text{if } D_I(I(z)) = 1 \; and \; \forall e \in \gamma \cap E_o: D_Y\big(h_{ZY}(z,e)\big) = 1 \\ 0, & \text{otherwise} \end{cases}$$

All Inclusive Controller

All Inclusive Controller:

The All Inclusive Controller for G

$$\mathcal{AIC}(G) = (Q_Y^{AICG}, Q_Z^{AICG}, h_{YZ}^{AICG}, h_{ZY}^{AICG}, E, \Gamma, y\_0),$$

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

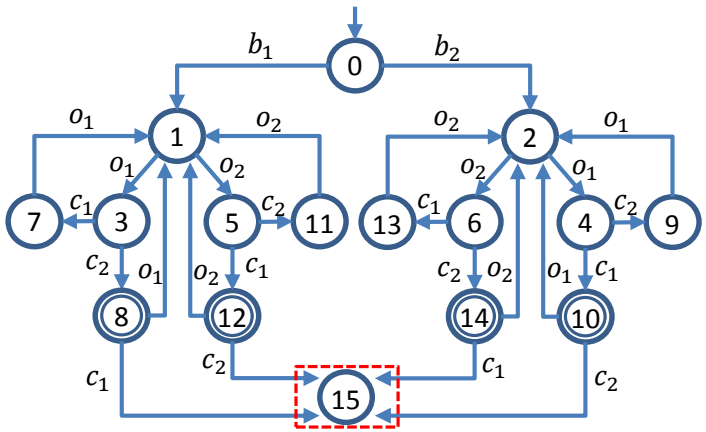
All Inclusive Controller

All Inclusive Controller:

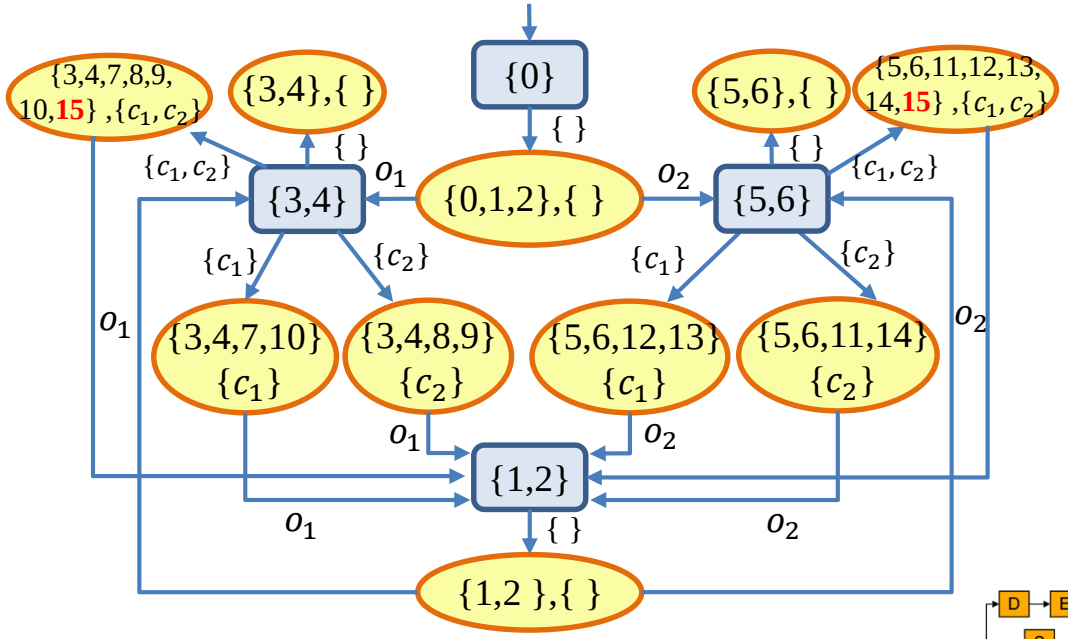
The All Inclusive Controller for G

$$\mathcal{AIC}(G) = (Q_Y^{AICG}, Q_Z^{AICG}, h_{YZ}^{AICG}, h_{ZY}^{AICG}, E, \Gamma, y\_0),$$

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



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



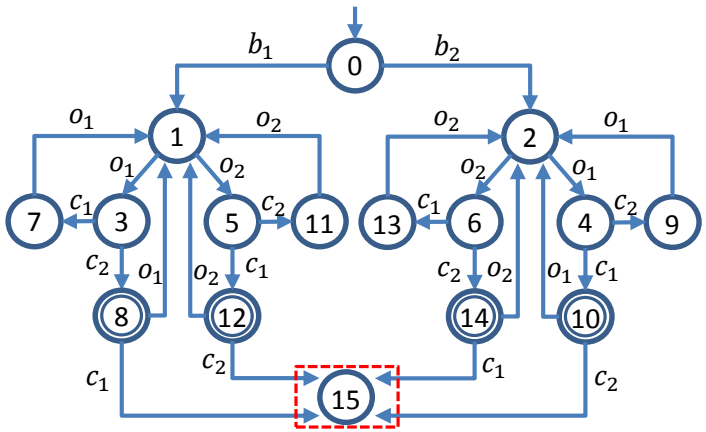
All Inclusive Controller

All Inclusive Controller:

The All Inclusive Controller for G

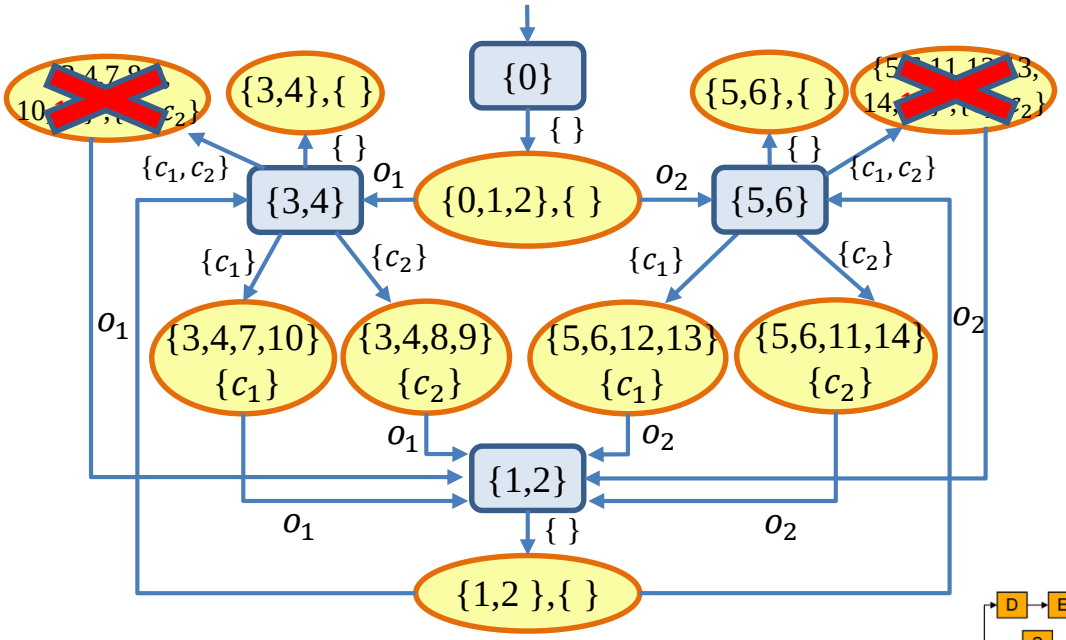
$$\mathcal{AIC}(G) = (Q_Y^{AICG}, Q_Z^{AICG}, h_{YZ}^{AICG}, h_{ZY}^{AICG}, E, \Gamma, y\_0),$$

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

Construction of the AIC

- Pruning states from the total controller $O\left(\left(2^{|X|}\right)^2\right)$

Construction of the AIC

Construction of the AIC

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

Properties of the AIC

Theorem.

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

Theorem.

$$(\bar{L} = L \subseteq \mathcal{L}(H) \wedge L \text{ is observable} \wedge L \text{ is controllable})$$
$$\Leftrightarrow L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$$

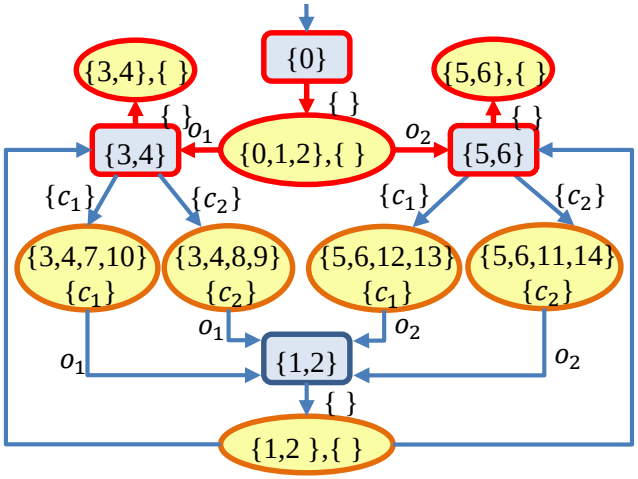
Properties of the AIC

Theorem.

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

Theorem.

$$(\bar{L} = L \subseteq \mathcal{L}(H) \wedge L \text{ is observable} \wedge L \text{ is controllable})$$
$$\Leftrightarrow L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$$



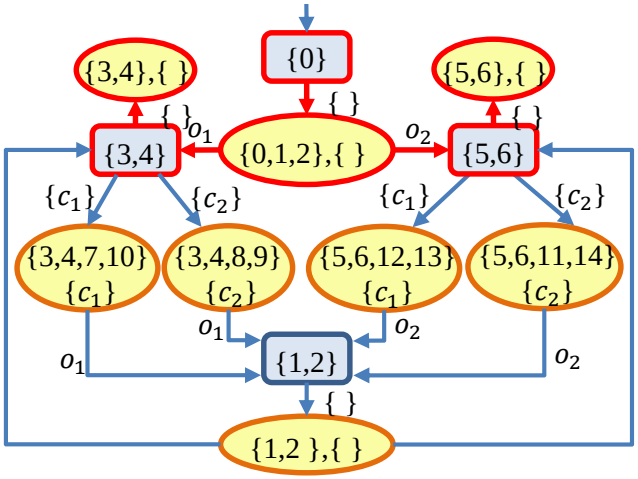
Properties of the AIC

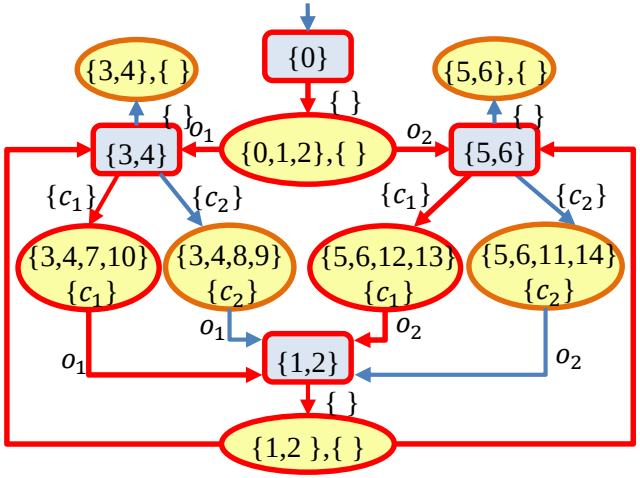
Theorem.

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

Theorem.

$$(\bar{L} = L \subseteq \mathcal{L}(H) \wedge L \text{ is observable} \wedge L \text{ is controllable})$$
$$\Leftrightarrow L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$$





Properties of the AIC

Theorem.

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

Theorem.

$$(\bar{L} = L \subseteq \mathcal{L}(H) \wedge L \text{ is observable} \wedge L \text{ is controllable})$$
$$\Leftrightarrow L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$$

The AIC embeds all legal solutions!

State Based Property of the AIC

Definition. (IS-Based Supervisor)

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

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

State Based Property of the AIC

Definition. (IS-Based Supervisor)

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

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

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.

State Based Property of the AIC

Definition. (IS-Based Supervisor)

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

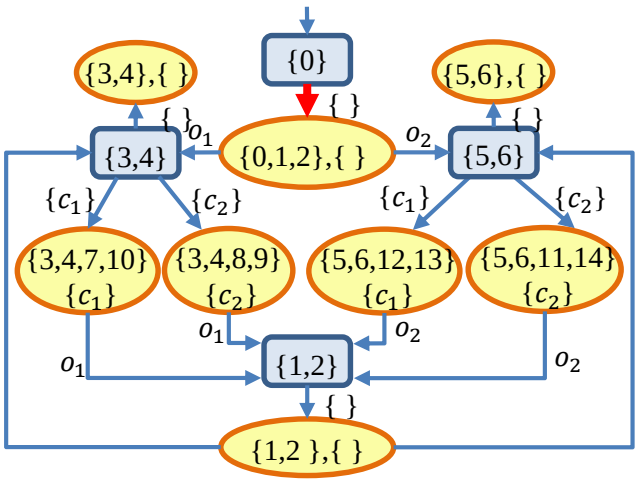
$$\left(\forall s, t \in \mathcal{L}(S_P/G)\right)[IS_{S_P}^{Y}(s) = IS_{S_P}^{Y}(t) \Rightarrow S_P(s) = S_P(t)]$$

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

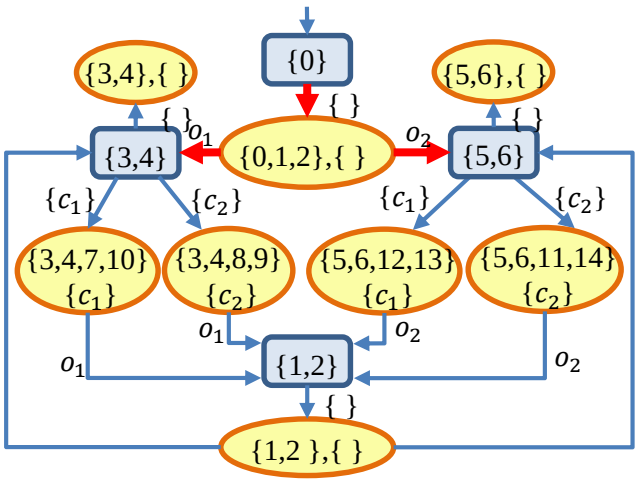
Synthesis of Safe and Maximally Permissive Supervisors



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

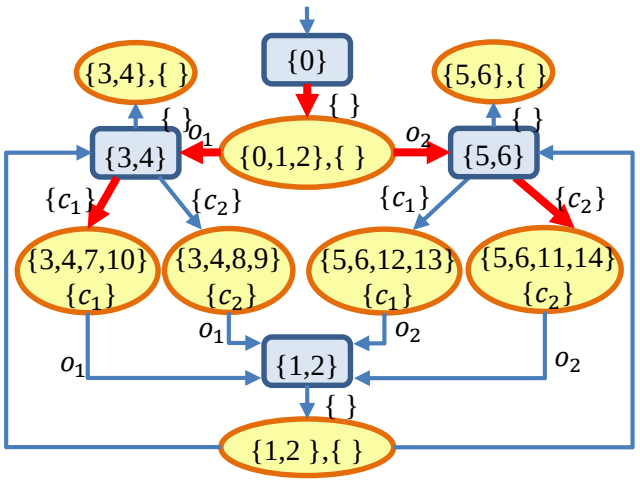
Synthesis of Safe and Maximally Permissive Supervisors



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

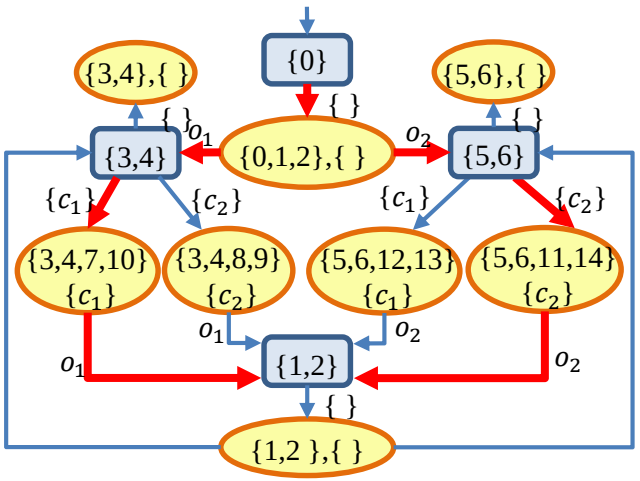
Synthesis of Safe and Maximally Permissive Supervisors



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

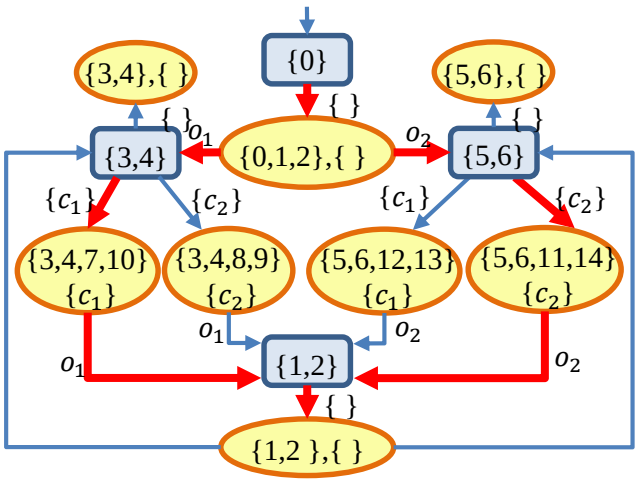
Synthesis of Safe and Maximally Permissive Supervisors



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

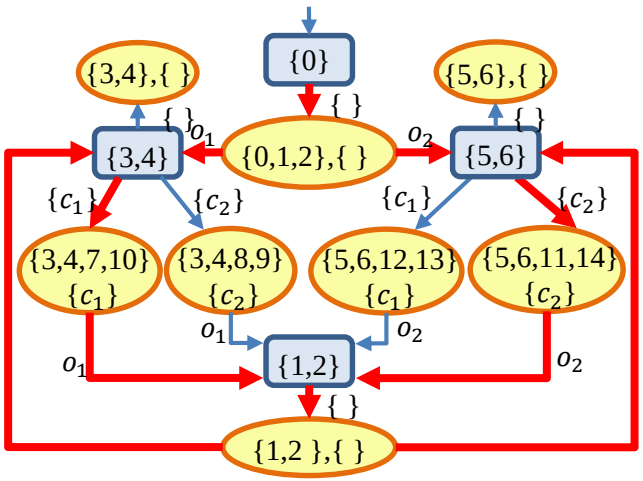
Synthesis of Safe and Maximally Permissive Supervisors



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

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

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