A General Approach for Solving Dynamic Sensor Activation Problems for a Class of Properties

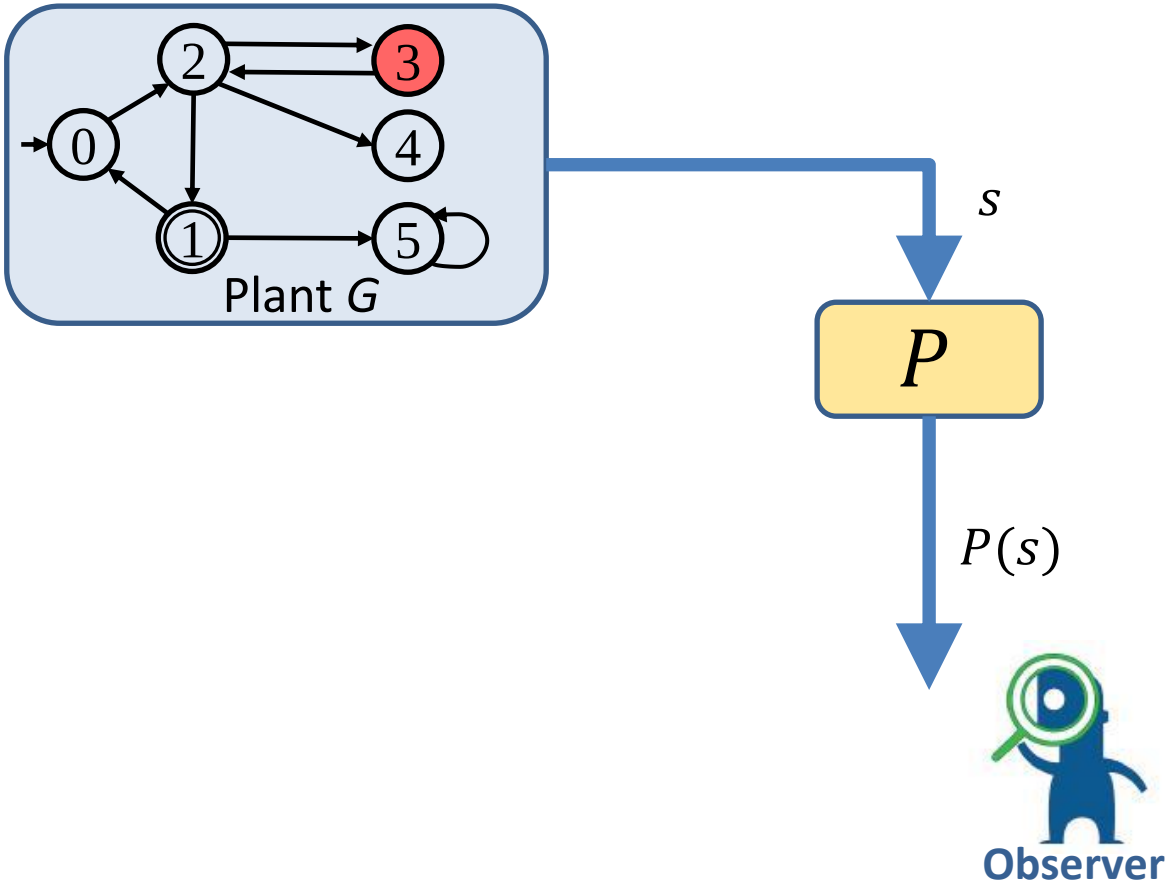
Xiang Yin and Stéphane Lafortune

EECS Department, University of Michigan

54th IEEE CDC, Dec 15-18, 2015, Osaka, Japan

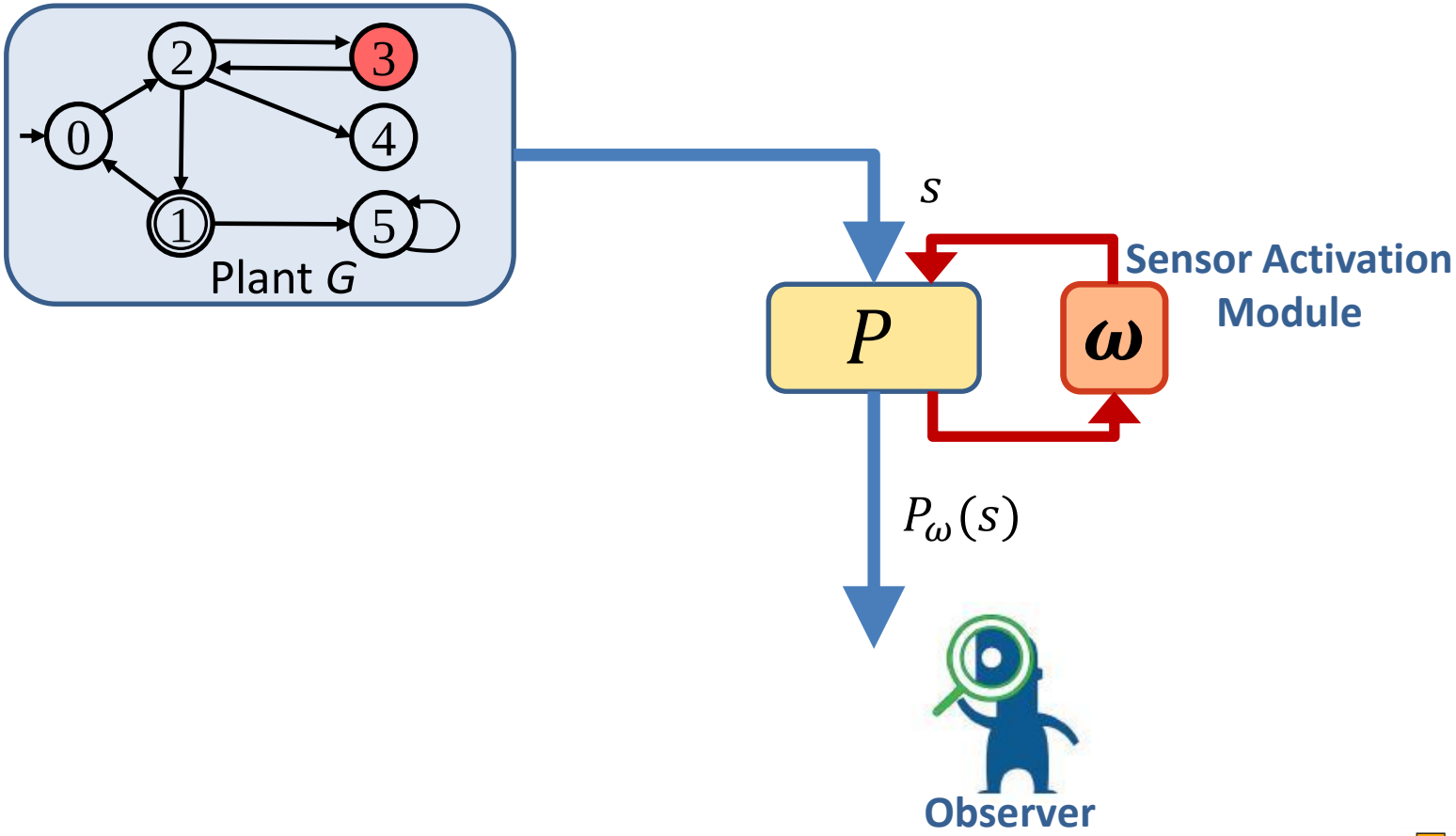
Introduction

- Dynamic Sensor Activation Problem



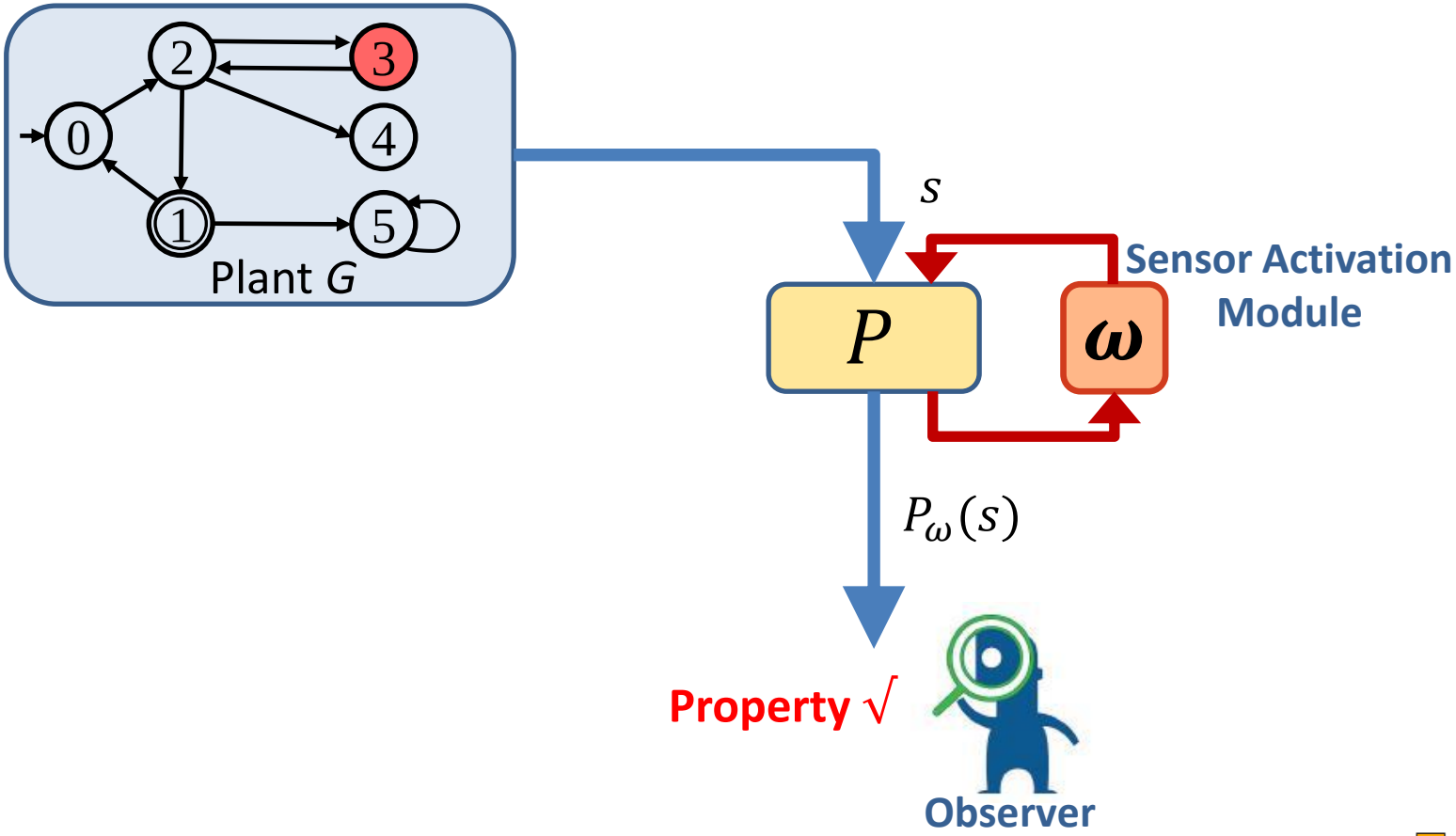
Introduction

- Dynamic Sensor Activation Problem



Introduction

- Dynamic Sensor Activation Problem



System Model

$G = (Q, \Sigma, \delta, q_0)$ is a *deterministic* FSA

- Q is the finite set of states;
- Σ is the finite set of events;
- $\delta: Q \times \Sigma \rightarrow Q$ is the partial transition function;
- q_0 is the initial state

System Model

$G = (Q, \Sigma, \delta, q_0)$ is a *deterministic* FSA

- Q is the finite set of states;
- Σ is the finite set of events;
- $\delta: Q \times \Sigma \to Q$ is the partial transition function;
- q_0 is the initial state

- $\Sigma = \Sigma_o \ \dot{\cup}\ \Sigma_s \ \dot{\cup}\ \Sigma_{uo}$
- A sensing decision is a set of events $\theta \in 2^{\Sigma}$ s.t. $\Sigma_o \subseteq \theta \subseteq \Sigma_o \cup \Sigma_s$
  Θ denotes the set of sensing decisions
- Information mapping $\omega: \mathcal{L}(G) \to \Theta$
  $P_\omega: \mathcal{L}(G) \to (\Sigma_o \cup \Sigma_s)^*$ denotes the corresponding projection
- A sensor activation policy is an information mapping $\omega: \mathcal{L}(G) \to \Theta$ s.t.
  $$\forall s, t \in \mathcal{L}(G): P_\omega(s) = P_\omega(t) \Rightarrow \omega(s) = \omega(t)$$

Information-State-Based Property

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

- **Information-State-Based Property**

Let G be the system automaton and $\omega: \mathcal{L}(G) \to \Theta$ be a sensor activation policy. An IS-based property w.r.t. G is a function

$$\varphi: 2^Q \to \{0,1\}$$

We say that ω satisfies φ w.r.t. G, denoted by $\omega \vDash_G \varphi$, if

$$\forall s \in \mathcal{L}(G): \varphi(\mathcal{E}_\omega^G(s)) = 1$$

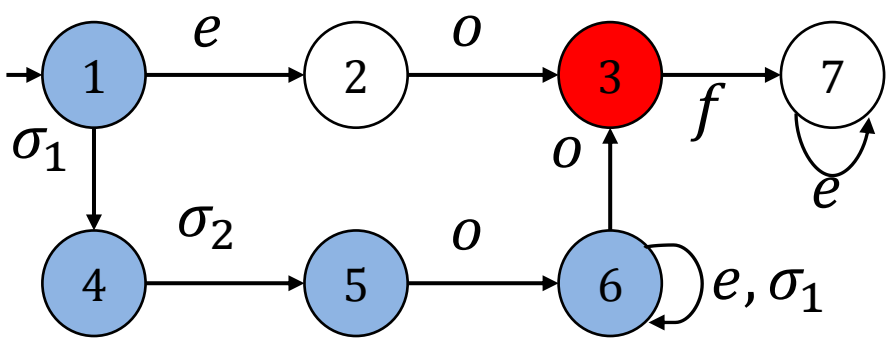
where

$$\mathcal{E}_\omega^G(s) = \{q \in Q: \exists t \in L\ s.t. P_\omega(t) = P_\omega(s) \wedge \delta(q_0, t) = q\}$$

IS-based Properties

- Information-State-Based Properties
  - Opacity: privacy applications
  - Diagnosability: fault detection and isolation
  - Predictability: fault prognosis
  - Detectability: state estimation
  - Anonymity: privacy applications
  - Etc.

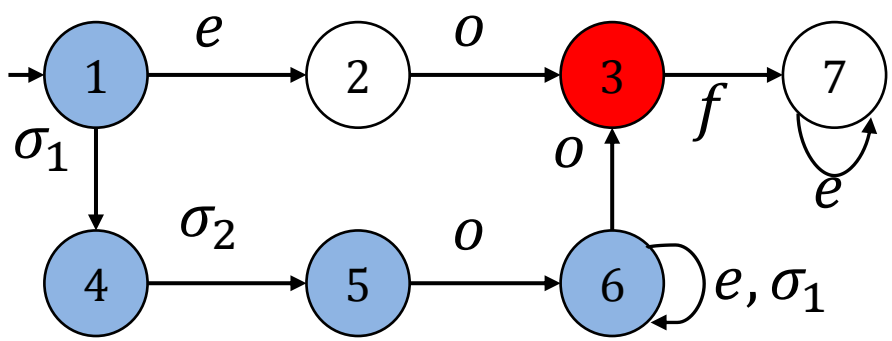
Example 1



- IS-based Property $\varphi: 2^Q \to \{0,1\}$

$$\forall\, i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$$

Example 1



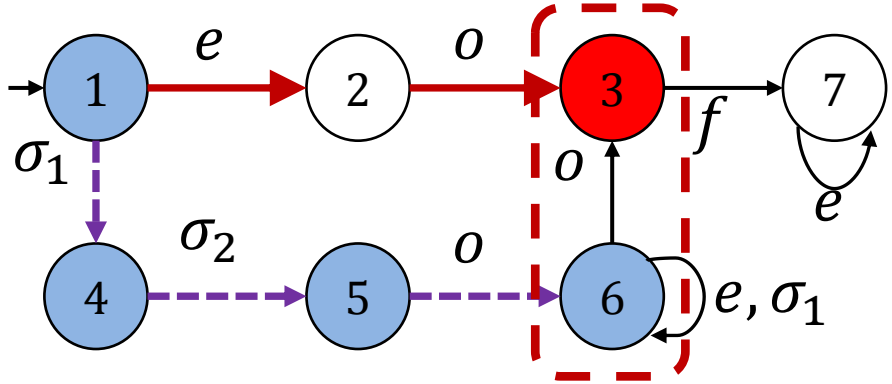
- IS-based Property $\varphi: 2^Q \to \{0,1\}$

$$\forall\, i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$$

- Sensor Activation Policy $\omega: \mathcal{L}(G) \to \Theta$

$$\forall s \in \mathcal{L}(G): \omega(s) = \{o\}$$

Example 1



- IS-based Property $\varphi: 2^Q \to \{0,1\}$

$$\forall\, i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$$

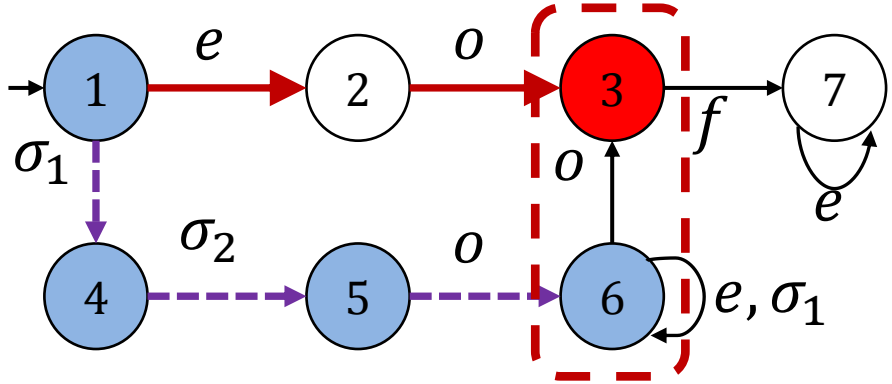
- Sensor Activation Policy $\omega: \mathcal{L}(G) \to \Theta$

$$\forall s \in \mathcal{L}(G): \omega(s) = \{o\}$$

- The IS-based property is not satisfied, i.e., $\omega \nvDash \varphi$

$$\mathcal{E}_\omega^G(eo) = \{\mathbf{3}, \mathbf{6}\}$$

Example 1



- IS-based Property $\varphi: 2^Q \to \{0,1\}$

$$\forall\, i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$$

- Sensor Activation Policy $\omega: \mathcal{L}(G) \to \Theta$

$$\forall s \in \mathcal{L}(G): \omega(s) = \{o\}$$

- The IS-based property is not satisfied, i.e., $\omega \not\models \varphi$

$$\mathcal{E}_\omega^G(eo) = \{\mathbf{3}, \mathbf{6}\}$$

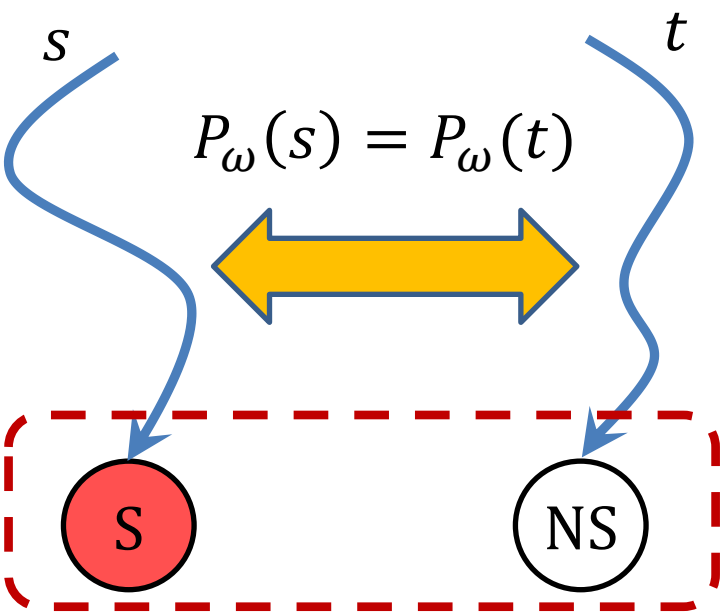
- State-disambiguation problem

Example 2

- IS-based Property $\varphi: 2^Q \to \{0,1\}$

  $\forall\, i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [i \not\subseteq X_{Secret}]$, where $X_{Secret} \subseteq X$

- Opacity problem



Problem Formulation

- Minimal Sensor Activation Problem for IS-Based Properties

Let $G = (Q, \Sigma, \delta, q_0)$ be the system automaton and $\varphi: 2^Q \to \{0,1\}$ be an IS-based property w.r.t. G. Find a sensor activation policy ω such that

(i) $\omega \vDash_G \varphi$ (IS-based Property)

(ii) $\nexists \omega' \in \Omega$ such that $\omega \vDash_G \varphi$ and $\omega' < \omega$. (Minimality)

The *Maximal Sensor Activation Problem* is also defined analogously.

$\omega' < \omega$ is defined in terms of set inclusion.

Literature Review

Dynamic Sensor Activation Problem

- Thorsley, D., & Teneketzis, D. (2007). Active acquisition of information for diagnosis and supervisory control of discrete event systems. Discrete Event Dynamic Systems, 17(4), 531-583.
- Cassez, F., & Tripakis, S. (2008). Fault diagnosis with static and dynamic observers. Fundamenta Informaticae, 88(4), 497-540.
- Wang, W., Lafortune, S., Lin, F., & Girard, A. R. (2010). Minimization of dynamic sensor activation in discrete event systems for the purpose of control. IEEE Transactions on Automatic Control, 55(11), 2447-2461.
- Wang, W., Lafortune, S., Girard, A. R., & Lin, F. (2010). Optimal sensor activation for diagnosing discrete event systems. Automatica, 46(7), 1165-1175.
- Cassez, F., Dubreil, J., & Marchand, H. (2012). Synthesis of opaque systems with static and dynamic masks. Formal Methods in System Design, 40(1), 88-115.
- Shu, S., Huang, Z., & Lin, F. (2013). Online sensor activation for detectability of discrete event systems. IEEE Transactions on Automation Science and Engineering, 10(2), 457-461.
- Dallal, E., & Lafortune, S. (2014). On most permissive observers in dynamic sensor activation problems. Automatic Control, IEEE Transactions on, 59(4), 966-981.
- Sears, D., & Rudie, K. (2015). Minimal sensor activation and minimal communication in discrete-event systems. Discrete Event Dynamic Systems, 1-55.

Literature Review

Dynamic Sensor Activation Problem

- Thorsley, D., & Teneketzis, D. (2007). Active acquisition of information for diagnosis and supervisory control of discrete event systems. Discrete Event Dynamic Systems, 17(4), 531-583.
- Cassez, F., & Tripakis, S. (2008). Fault diagnosis with static and dynamic observers. Fundamenta Informaticae, 88(4), 497-540.
- Wang, W., Lafortune, S., Lin, F., & Girard, A. R. (2010). Minimization of dynamic sensor activation in discrete event systems for the purpose of control. IEEE Transactions on Automatic Control, 55(11), 2447-2461.
- Wang, W., Lafortune, S., Girard, A. R., & Lin, F. (2010). Optimal sensor activation for diagnosing discrete event systems. Automatica, 46(7), 1165-1175.
- Cassez, F., Dubreil, J., & Marchand, H. (2012). Synthesis of opaque systems with static and dynamic masks. Formal Methods in System Design, 40(1), 88-115.
- Shu, S., Huang, Z., & Lin, F. (2013). Online sensor activation for detectability of discrete event systems. IEEE Transactions on Automation Science and Engineering, 10(2), 457-461.
- Dallal, E., & Lafortune, S. (2014). On most permissive observers in dynamic sensor activation problems. Automatic Control, IEEE Transactions on, 59(4), 966-981.
- Sears, D., & Rudie, K. (2015). Minimal sensor activation and minimal communication in discrete-event systems. Discrete Event Dynamic Systems, 1-55.

- **Different approaches for different properties**
- **The sensor activation problems for some properties have not been considered**
- **Need general approach**

Bipartite Dynamic Observer

- Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. G is a 7-tuple $\mathcal{O} = (Q_Y^{\mathcal{O}}, Q_Z^{\mathcal{O}}, h_{YZ}^{\mathcal{O}}, h_{ZY}^{\mathcal{O}}, E, \Gamma, y_0)$

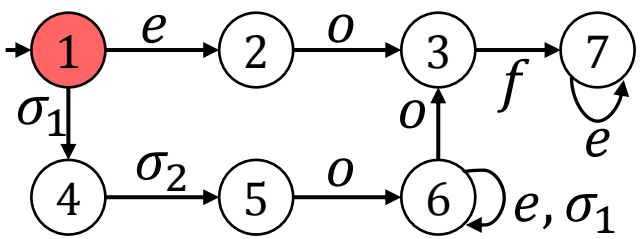
- $Q_Y^{\mathcal{O}} \subseteq I$ is the set of Y-states;
- $Q_Z^{\mathcal{O}} \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^{\mathcal{O}}: Q_Y^{\mathcal{O}} \times \Theta \to Q_Z^{\mathcal{O}}$ represents the unobservable reach;
- $h_{ZY}^{\mathcal{O}}: Q_Z^{\mathcal{O}} \times \Sigma \to Q_Y^{\mathcal{O}}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.

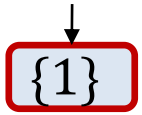
Bipartite Dynamic Observer

- Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. G is a 7-tuple $\mathcal{O} = (Q_Y^{\mathcal{O}}, Q_Z^{\mathcal{O}}, h_{YZ}^{\mathcal{O}}, h_{ZY}^{\mathcal{O}}, E, \Gamma, y_0)$

- $Q_Y^{\mathcal{O}} \subseteq I$ is the set of Y-states;
- $Q_Z^{\mathcal{O}} \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^{\mathcal{O}}: Q_Y^{\mathcal{O}} \times \Theta \to Q_Z^{\mathcal{O}}$ represents the unobservable reach;
- $h_{ZY}^{\mathcal{O}}: Q_Z^{\mathcal{O}} \times \Sigma \to Q_Y^{\mathcal{O}}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.





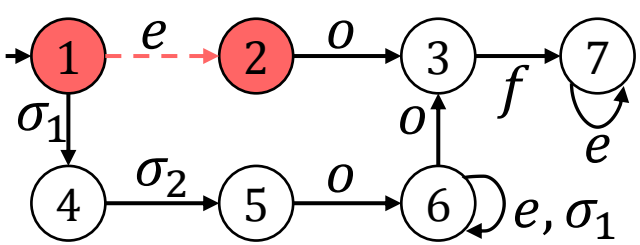
$\Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\}$

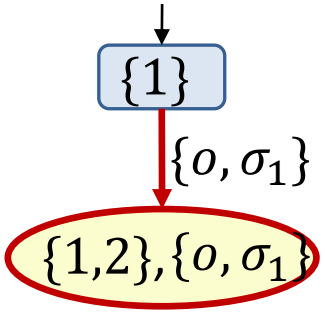
Bipartite Dynamic Observer

- Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. G is a 7-tuple $\mathcal{O} = (Q_Y^{\mathcal{O}}, Q_Z^{\mathcal{O}}, h_{YZ}^{\mathcal{O}}, h_{ZY}^{\mathcal{O}}, E, \Gamma, y_0)$

- $Q_Y^{\mathcal{O}} \subseteq I$ is the set of Y-states;
- $Q_Z^{\mathcal{O}} \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^{\mathcal{O}}: Q_Y^{\mathcal{O}} \times \Theta \to Q_Z^{\mathcal{O}}$ represents the unobservable reach;
- $h_{ZY}^{\mathcal{O}}: Q_Z^{\mathcal{O}} \times \Sigma \to Q_Y^{\mathcal{O}}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.





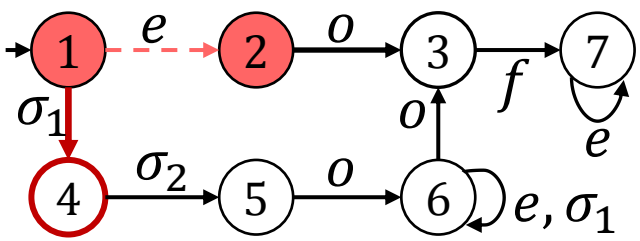
$\Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\}$

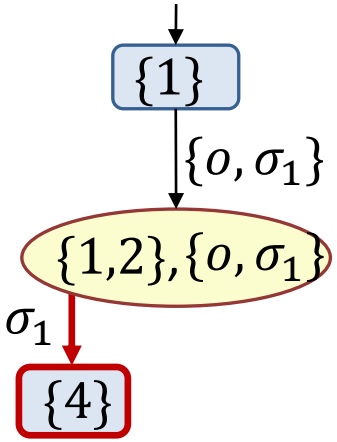
Bipartite Dynamic Observer

- Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. G is a 7-tuple $\mathcal{O} = (Q_Y^{\mathcal{O}}, Q_Z^{\mathcal{O}}, h_{YZ}^{\mathcal{O}}, h_{ZY}^{\mathcal{O}}, E, \Gamma, y_0)$

- $Q_Y^{\mathcal{O}} \subseteq I$ is the set of Y-states;
- $Q_Z^{\mathcal{O}} \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^{\mathcal{O}}: Q_Y^{\mathcal{O}} \times \Theta \to Q_Z^{\mathcal{O}}$ represents the unobservable reach;
- $h_{ZY}^{\mathcal{O}}: Q_Z^{\mathcal{O}} \times \Sigma \to Q_Y^{\mathcal{O}}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.





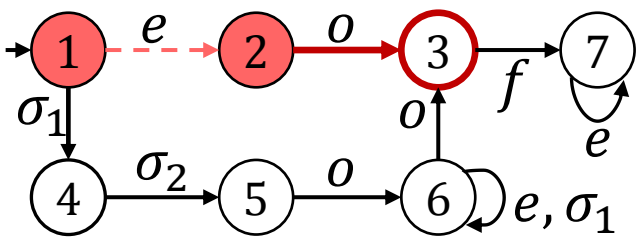
$\Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\}$

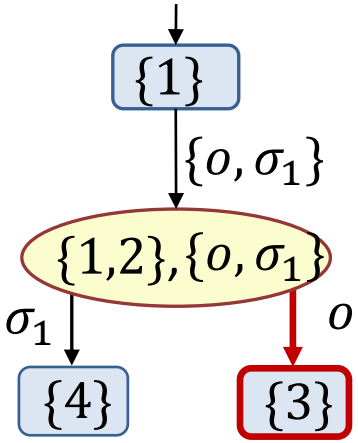
Bipartite Dynamic Observer

- Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. G is a 7-tuple $\mathcal{O} = (Q_Y^{\mathcal{O}}, Q_Z^{\mathcal{O}}, h_{YZ}^{\mathcal{O}}, h_{ZY}^{\mathcal{O}}, E, \Gamma, y_0)$

- $Q_Y^{\mathcal{O}} \subseteq I$ is the set of Y-states;
- $Q_Z^{\mathcal{O}} \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^{\mathcal{O}}: Q_Y^{\mathcal{O}} \times \Theta \to Q_Z^{\mathcal{O}}$ represents the unobservable reach;
- $h_{ZY}^{\mathcal{O}}: Q_Z^{\mathcal{O}} \times \Sigma \to Q_Y^{\mathcal{O}}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.





$\Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\}$

Generalized Most Permissive Observer

- Most Permissive Observer (MPO)

Let $\mathrm{G} = (\mathrm{Q}, \Sigma, \delta, q_0)$ be the system and let $\varphi: 2^Q \to \{0,1\}$ be the IS-based property under consideration. The Most Permissive Observer for φ is the BDO

$$\mathcal{MPO}_\varphi = (Q_Y^{MPO}, Q_Z^{MPO}, h_{YZ}^{MPO}, h_{ZY}^{MPO}, \Sigma, \Theta, y_0)$$

defined as the largest BDO

1. For any $y \in Q_Y^{MPO}$, there exists $\theta \in \Theta$ such that $h_{YZ}^{MPO}(y, \theta)!$;
2. For any $z \in Q_Z^{MPO}$, we have
   2.1. $\big(\forall \sigma \in \Theta(z)\big)\big[(\exists x \in I(z): \delta(x, \sigma)!) \Rightarrow h_{ZY}^{MPO}(z, \sigma)!\big]$;
   2.2. $\varphi\big(I(z)\big) = 1$

Generalized Most Permissive Observer

- Most Permissive Observer (MPO)

Let $G = (Q, \Sigma, \delta, q_0)$ be the system and let $\varphi: 2^Q \to \{0,1\}$ be the IS-based property under consideration. The Most Permissive Observer for φ is the BDO

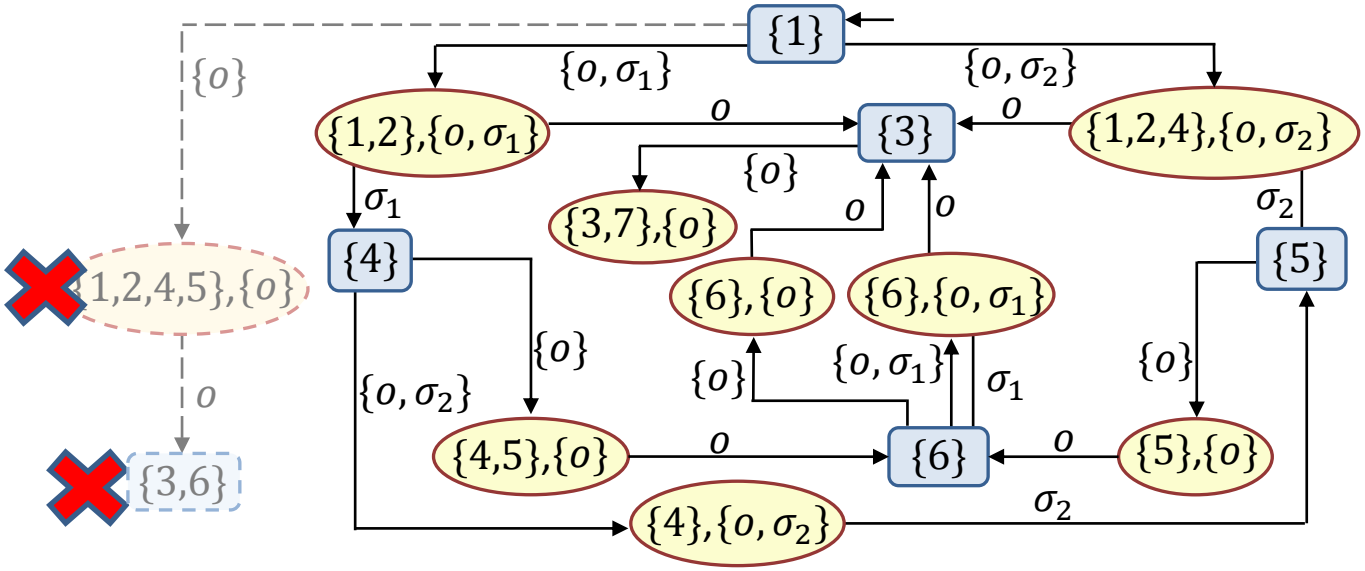
$$\mathcal{MPO}_\varphi = (Q_Y^{MPO}, Q_Z^{MPO}, h_{YZ}^{MPO}, h_{ZY}^{MPO}, \Sigma, \Theta, y_0)$$

defined as the largest BDO

1. For any $y \in Q_Y^{MPO}$, there exists $\theta \in \Theta$ such that $h_{YZ}^{MPO}(y, \theta)!$;
2. For any $z \in Q_Z^{MPO}$, we have
   2.1. $\big(\forall \sigma \in \Theta(z)\big)\big[(\exists x \in I(z): \delta(x, \sigma)!) \Rightarrow h_{ZY}^{MPO}(z, \sigma)!\big]$;
   2.2. $\varphi\big(I(z)\big) = 1$

- MPO for Diagnosability
  Cassez, F., & Tripakis, S. (2008). and Dallal, E., & Lafortune, S. (2014).
- MPO for Opacity
  Cassez, F., Dubreil, J., & Marchand, H. (2012).

Construction of the MPO



- Depth-first search until reach a Z-state violating φ
- Iteratively prune:
  Y-state, from which *all* sensing decisions have been removed
  Z-state, from which *one* observation has been removed

Properties of the MPO

- Theorem

There exists a sensor activation policy ω such that $\omega \vDash_G \varphi$ iff $\mathcal{MPO}_\varphi$ is non-empty.

Properties of the MPO

- Theorem

There exists a sensor activation policy ω such that $\omega \vDash_G \varphi$ iff $\mathcal{MPO}_\varphi$ is non-empty.

- Theorem

$\omega \vDash_G \varphi$ iff ω is included in $\mathcal{MPO}_\varphi$.

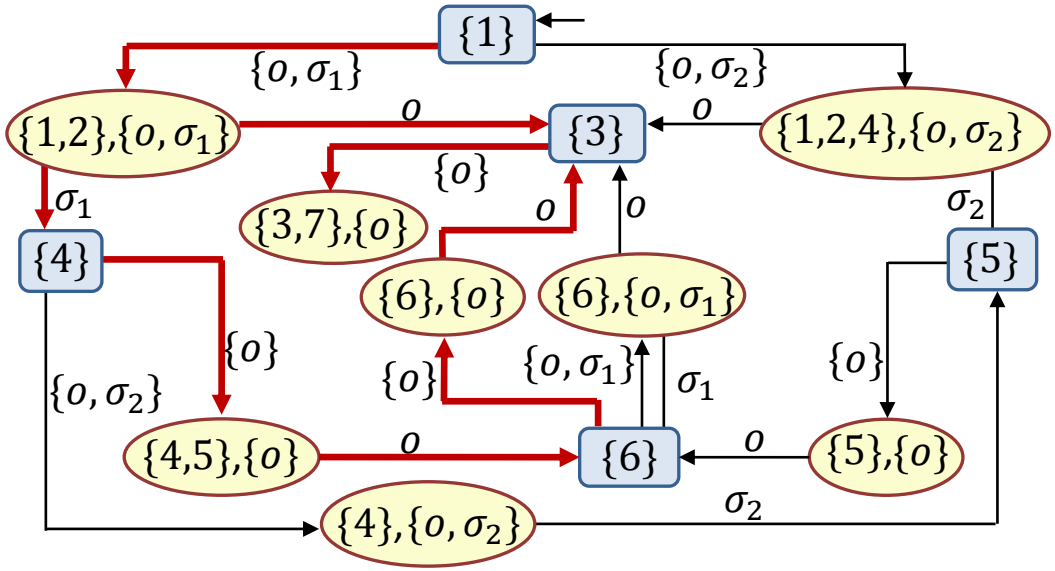
Properties of the MPO

- **Theorem**

There exists a sensor activation policy ω such that $\omega \vDash_G \varphi$ iff $\mathcal{MPO}_\varphi$ is non-empty.

- **Theorem**

$\omega \vDash_G \varphi$ iff ω is included in $\mathcal{MPO}_\varphi$.



Synthesis of Optimal Sensor Activation Policies

- IS-based Sensor Activation Policy

A sensor activation policy ω is said to be *Information-State-based* (or IS-based) if

$$\forall s, t \in \mathcal{L}(G): \mathcal{I}_{\omega}^{Y}(s) = \mathcal{I}_{\omega}^{Y}(t) \Rightarrow \omega(s) = \omega(t)$$

Synthesis of Optimal Sensor Activation Policies

- **IS-based Sensor Activation Policy**

A sensor activation policy ω is said to be *Information-State-based* (or IS-based) if

$$\forall s, t \in \mathcal{L}(G): \mathcal{I}_{\omega}^{Y}(s) = \mathcal{I}_{\omega}^{Y}(t) \Rightarrow \omega(s) = \omega(t)$$

- **Greedy Optimal Sensor Activation Policy**

Suppose that ω is a sensor activation policy such that policy $\omega \vDash_G \varphi$. We say that ω is greedy minimal if

$$\forall s \in \mathcal{L}(G), \forall \theta \in \Theta: h_{YZ}^{MPO}(\mathcal{I}_{\omega}^{Y}(s), \theta)! \Rightarrow \theta \not\subset \omega(s)$$

The notion of *greedy maximality* is defined analogously

Synthesis of Optimal Sensor Activation Policies

- **IS-based Sensor Activation Policy**

A sensor activation policy ω is said to be *Information-State-based* (or IS-based) if

$$\forall s, t \in \mathcal{L}(G): \mathcal{I}_{\omega}^{Y}(s) = \mathcal{I}_{\omega}^{Y}(t) \Rightarrow \omega(s) = \omega(t)$$

- **Greedy Optimal Sensor Activation Policy**

Suppose that ω is a sensor activation policy such that policy $\omega \vDash_G \varphi$. We say that ω is greedy minimal if

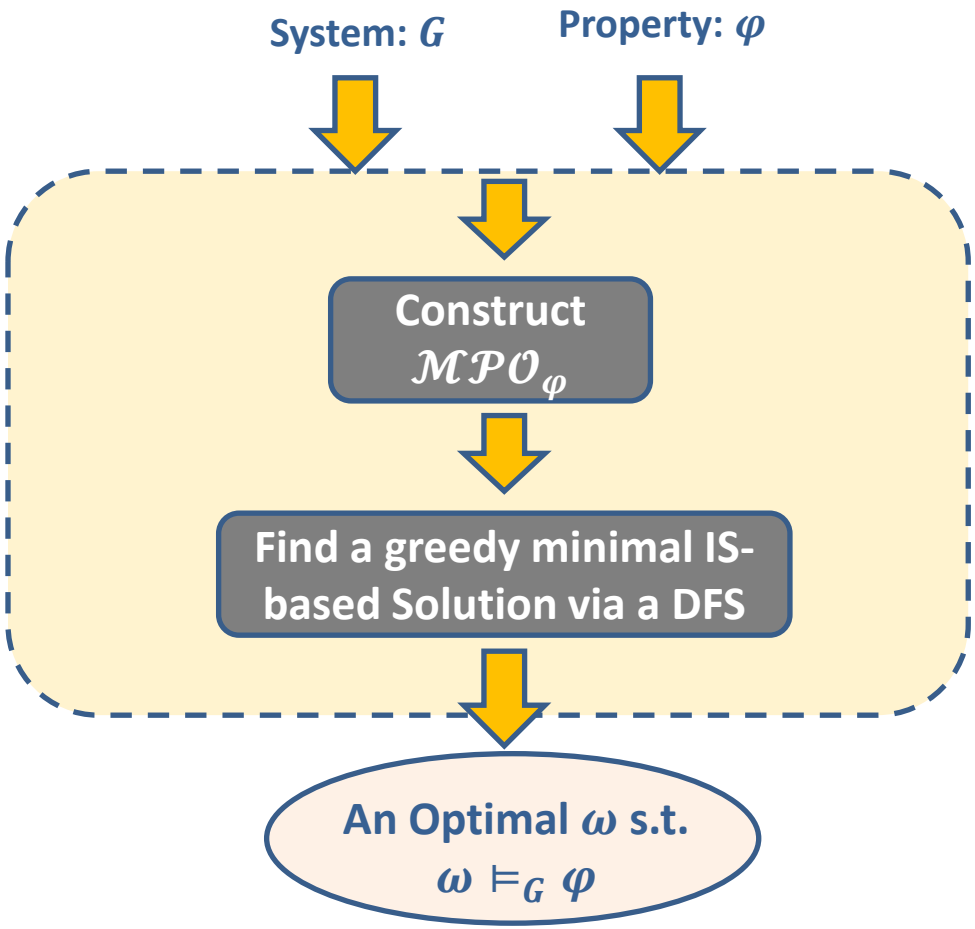
$$\forall s \in \mathcal{L}(G), \forall \theta \in \Theta: h_{YZ}^{MPO}(\mathcal{I}_{\omega}^{Y}(s), \theta)! \Rightarrow \theta \not\subset \omega(s)$$

The notion of *greedy maximality* is defined analogously

- **Theorem**

Let ω be a sensor activation policy such that policy $\omega \vDash_G \varphi$. Then ω is minimal (respectively, maximal) if it is greedy minimal (respectively, greedy maximal).

Synthesis Procedure



IS-based Formulation of Predictability

- **Predictability**

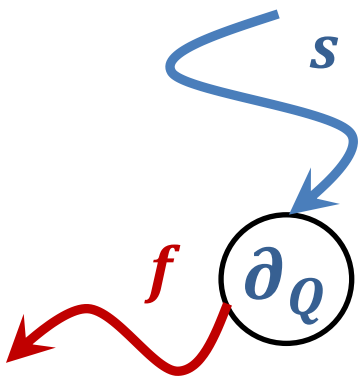
  A live language $\mathcal{L}(G)$ is said to be *predictable* if any fault of the system can be predicted prior to its occurrence with no missed alarm and no false alarm.

- IS-based Predictability $\varphi_{pre}: 2^Q \to \{0,1\}$

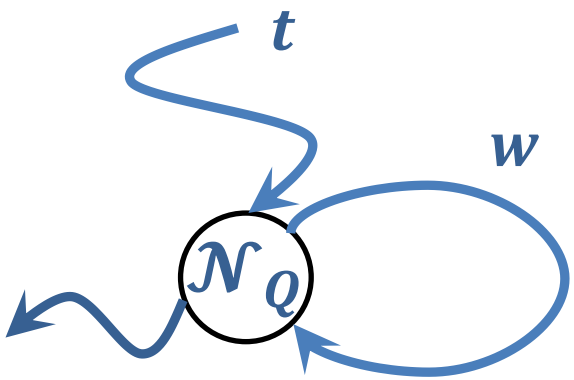
$$\forall\, i \in 2^Q: \left[\varphi_{pre}(i) = 0\right] \Leftrightarrow \left[\exists q, q' \in i: q \in \partial_Q \wedge q' \in \mathcal{N}_Q\right]$$

- **Theorem**

  Let φ_{pre} be the IS-based predictability defined above. For ant sensor activation policy ω, $\mathcal{L}(G)$ is predictable w.r.t. f and ω if and only if $\omega \vDash_G \varphi_{pre}$.

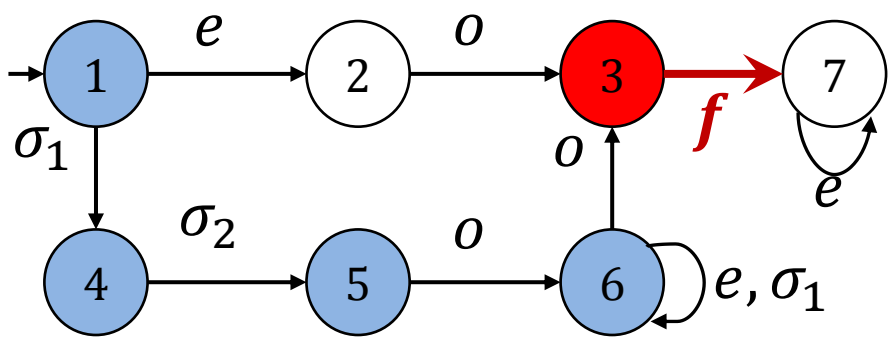


Boundary State [Kumar & Takai, 2010]



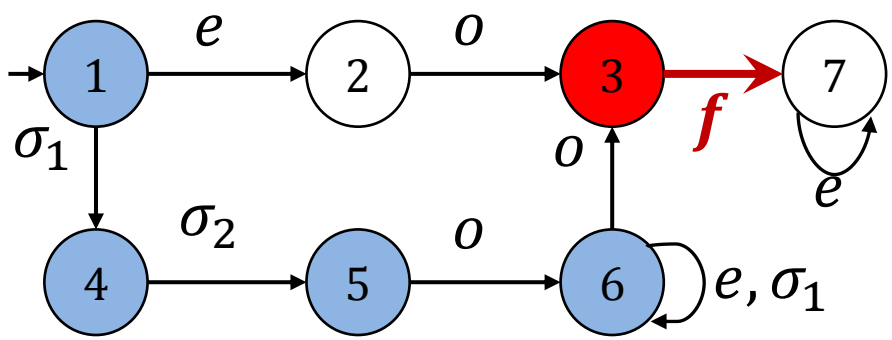
Non-indicator State

Example

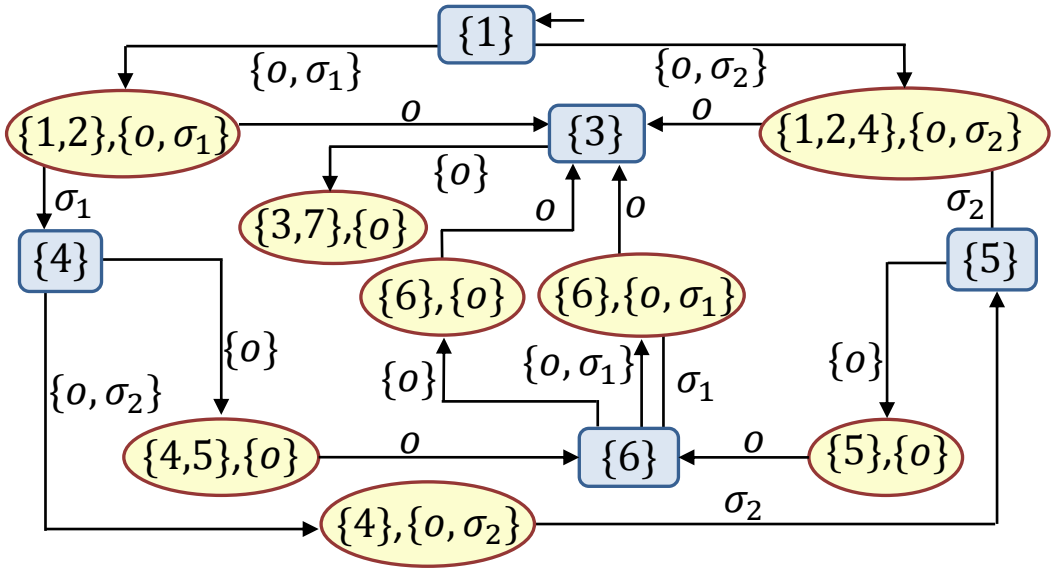


- Boundary states, $\partial_Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1,4,5,6\}$
- $\forall\, i \in 2^Q: \left[\varphi_{pre}(i) = 1\right] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$

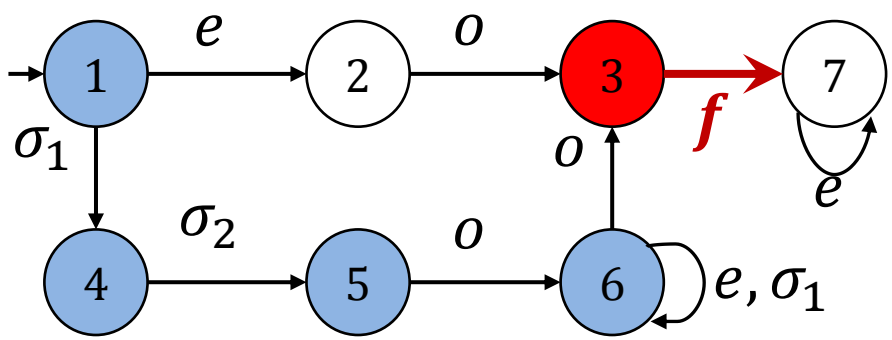
Example



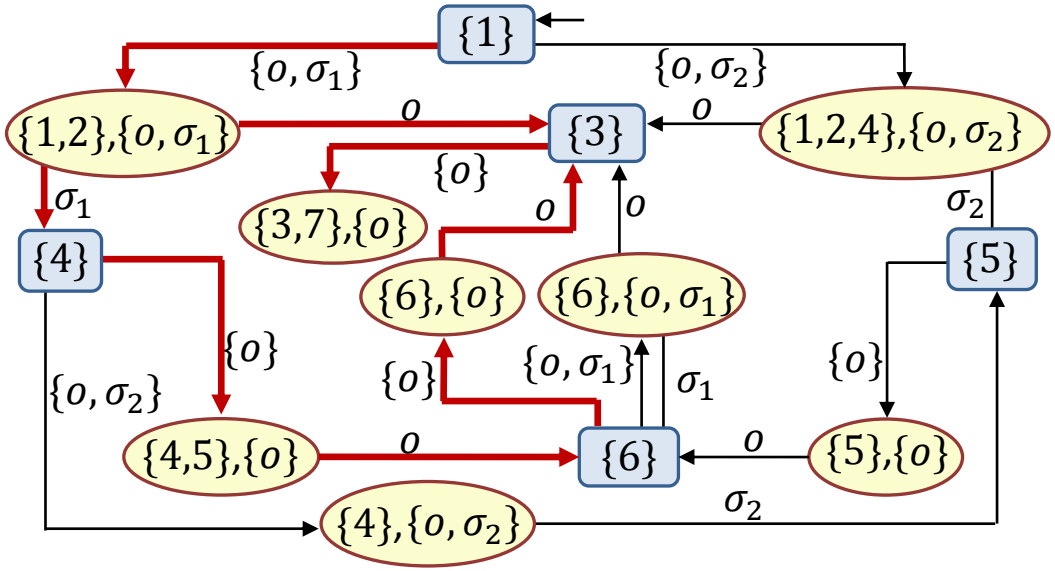
- Boundary states, $\partial_Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1,4,5,6\}$
- $\forall\, i \in 2^Q: [\varphi_{pre}(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$



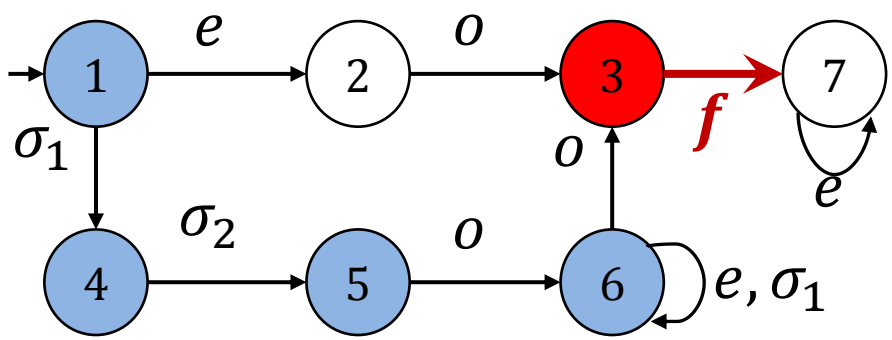
Example



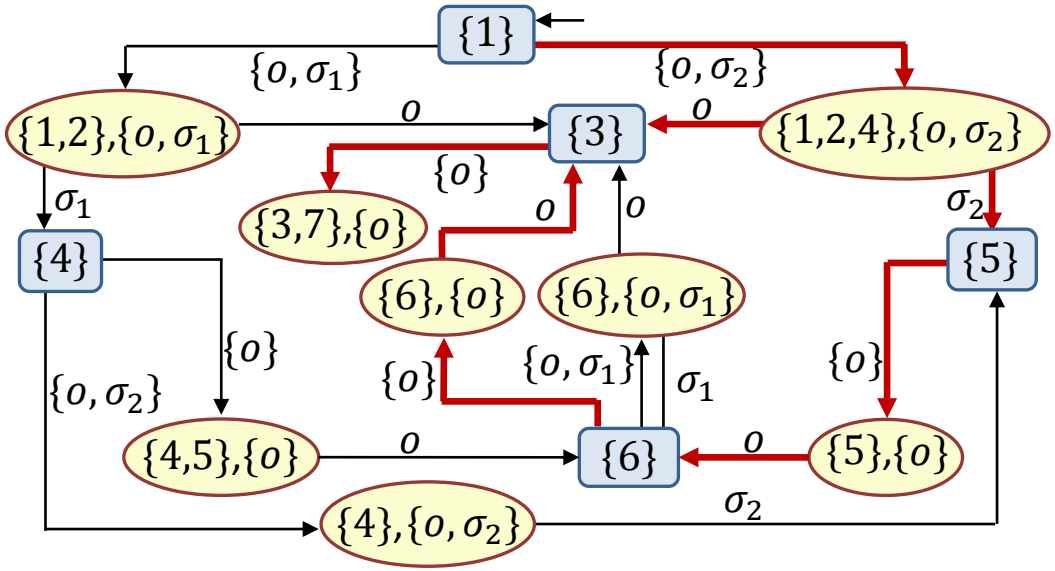
- Boundary states, $\partial_Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1,4,5,6\}$
- $\forall\, i \in 2^Q: [\varphi_{pre}(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$



Example



- Boundary states, $\partial_Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1,4,5,6\}$
- $\forall\, i \in 2^Q: [\varphi_{pre}(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$



Summary

Contributions:

- A general approach for solving dynamic sensor activation problems
- Information-state-based properties: A general class of properties
- Solve previous open problem, e.g., predictability
- Applicable to more *user-defined* properties
- The solution is provably *language-based* minimal