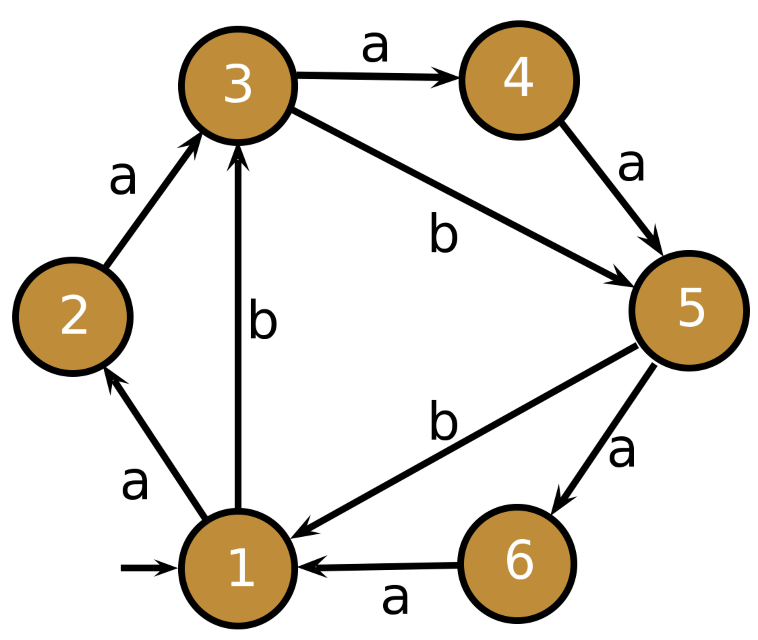
Ensuring Non-Opacity in Discrete Event Systems

Feiyang Lin, FUSRP (Fields Undergraduate Student Research Program) 2018

Introduction

In order to model systems where there are a finite number of states and changes in states after discrete events, the field of discrete event systems uses finite automata, written as a 4-tuple (Q, Σ, δ, q_o) with a corresponding directed graph representation:



A Discrete Event System

- $G = (Q, \Sigma, \delta, q_o)$
- $Q = \{1,2,3,4,5,6\}$, $q_o = 1$
- $\Sigma = \{a, b\}$, $\Sigma^* = \{ab, aabba, ...\}$
- $\delta : Q \times \Sigma^* \to Q$
  e.g. $\delta(1,a) = 2$, $\delta(5, ba) = 2$
- $\delta = \{(1,a,2),(2,a,3),(1,b,3),...\}$ is also the set of directed edges in the graph

- $\delta(q, st) = \delta(\delta(q,s), t)$
- Agent: ability to observe $\delta' \subseteq \delta$, ability to send information according to a policy $com : L(G) \to 2^{\Sigma}$.
- We are interested in an agent's ability to distinguish certain states (opacity) in a system with two agents who are communicating to each other.

Problem Statement

Given a plant $G = (Q, \Sigma, \delta, q_o)$, two agents who can observe $\delta_1, \delta_2 \subseteq \delta$ respectively, the set of secret states Q_L, and the set of non-secret states Q_K. To find a set of observer-based (plant-based) policy implementations $(G_1, G_2, \varphi_1, \varphi_2)$ that are minimal and make the system non-opaque to at least one of the agents with respect to Q_K and Q_L.

Definitions/Theorems

Observation under Communication: Given agents who observe $\delta_1, \delta_2 \subseteq \delta$ and each have policy com_{21}/com_{12}.
Then $\mathcal{C}(com_{21}, com_{12}) := (\theta_{21}, \theta_{12})$ defined as follows:

$$\theta_{ij}(\epsilon) = \epsilon$$

$\forall s \in \Sigma^*, \forall \sigma \in \Sigma,$

$$\theta_{ij}(s\sigma) = \begin{cases} \theta_{ij}(s)\sigma & \text{if } (\delta(q_o,s),\sigma,\delta(q_o,s\sigma)) \in \delta_j \\ & \vee((\delta(q_o,s),\sigma,\delta(q_o,s\sigma)) \in \delta_i \wedge \sigma \in com_{ij}(s)) \\ \theta_{ij}(s) & \text{otherwise} \end{cases}$$

State Estimation $SE^{\theta} : \theta(L(G)) \to Q$ is an agent's estimation of the system's state. Formally,

$$SE^{\theta}(s) = \{q \in Q : \exists t \in L(G), \delta(q_o, t) = q \wedge \theta(t) = s\}$$

Opacity: Given two sets of states $Q_K, Q_L \subseteq Q$, the system is opaque under θ with respect to Q_K and Q_L if

$$\exists s \in L(G), (Q_K \cap SE^{\theta}(s) \neq \emptyset) \wedge (Q_L \cap SE^{\theta}(s) \neq \emptyset),$$

i.e., states in Q_L cannot be distinguished form states in Q_K.

Observer: Given an agent whose observation is characterized by some θ, one can create an *observer* by relabeling all unobservable transitions as ϵ and doing an NFA-DFA transformation.

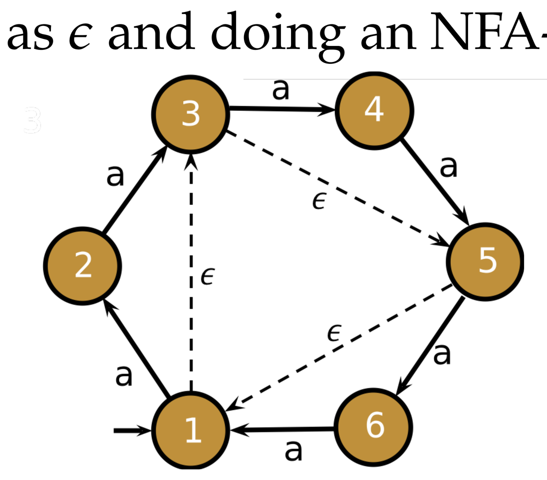


Figure 1: NFA: $(Q, \Sigma, \delta_{\epsilon}, q_o)$
$\delta_1 = \{\text{all transitions by event a}\}$
$\forall s \in L(G), com_{21}(s) = \emptyset$

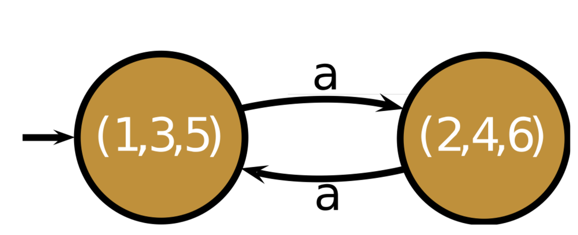


Figure 2: DFA: Observer (X, Σ, ξ, x_o)
$SE^{\theta}(aaa) = \xi(x_o, aaa) = \{2,4,6\}$

Theorem: A state in the observer automaton represents the agent's estimation of the system's current state. Formally,

$$SE^{\theta}(s) = \xi(x_o, s),$$

where ξ is the transition function of the observer.
As a result, a system is opaque under θ iff

$$\exists s \in \theta(L(G)), \xi(x_o, s) \cap Q_L \neq \emptyset \wedge \xi(x_o, s) \cap Q_K \neq \emptyset$$

Constraints

Implementable: A communication policy $com : L(G) \to 2^{\Sigma}$ under θ is implementable if there exists (H, φ) where $H = (Y, \Sigma, \eta, y_o)$ so that $L(H) = \theta(L(G))$, $\varphi : Y \to 2^{\Sigma}$, and for any $s \in L(G)$,

$$com(s) = \varphi(\eta(y_o, \theta(s))).$$

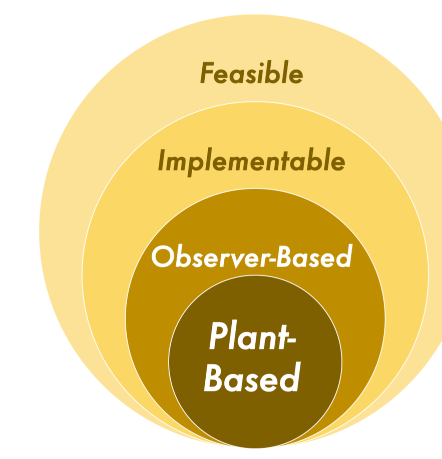


Figure 5: Hierarchy of Different Constraints

Feasibility: A policy $com : L(G) \to 2^{\Sigma}$ is feasible under θ if

$$\forall s, t \in L(G), \theta(s) = \theta(t) \Rightarrow com(s) = com(t).$$

Observer-Based: A pair of communication policies with the finite implementation $(H_1, H_2, \varphi_1, \varphi_2)$ is observer-based if

$$\eta_i(y_{io}, s) = SE^{\theta_{ji}}(s).$$

Plant-Based: A policy (H_i, φ_i) is plant-based if

$$\forall Q \in X_i, \forall q \in Q, (\delta(q,\sigma)! \wedge \sigma \in \varphi_i(Q)) \Rightarrow (q \in Q' \in X_i \Rightarrow \sigma \in \varphi_i(Q'))$$

Challenges

Circular Dependency: What Agent 1 sends to Agent 2 affects what Agent 2 can send. *How can you tell that two policies are feasible with respect to each other?*

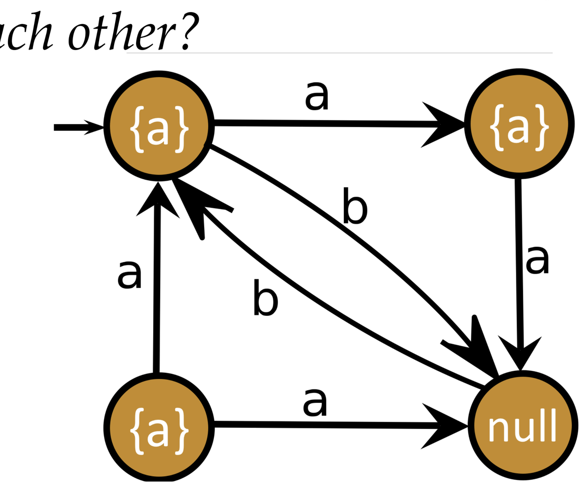


Figure 3: Potential Policy for Agent 1

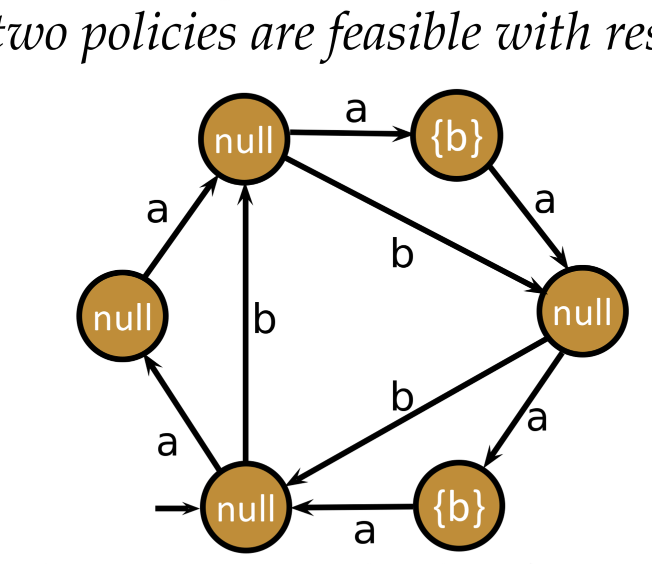


Figure 4: Potential Policy for Agent 2

Results and Conclusions

- Checking Feasibility:
  $\mathcal{R}(H_1, H_2, \varphi_1, \varphi_2) := (X_R, \Sigma, \xi_R, r_o)$ defined as follows:
  $r_o := (q_o, x_{1o}, x_{2o})$, and $\forall c \in \Sigma$ such that $\delta(q,c)!$,

$$\xi_R(r,c) = \begin{cases} (\delta(q,c), \eta_1(Q_a,c), \eta_2(Q_b,c)) & \text{if } c \in o_1(r) \wedge c \in o_2(r) \\ (\delta(q,c), \eta_1(Q_a,c), Q_b) & \text{if } c \in o_1(r) \wedge c \notin o_2(r) \\ (\delta(q,c), Q_a, \eta_2(Q_b,c)) & \text{if } c \notin o_1(r) \wedge c \in o_2(r) \\ (\delta(q,c), Q_a, Q_b) & \text{if } c \notin o_1(r) \wedge c \notin o_2(r) \end{cases}$$

  where

$$r = (q, Q_a, Q_b)$$
$$o_1(q, Q_a, Q_b) := \{c \in \Sigma : (q,c) \in \delta_1 \vee ((q,c) \in \delta_2 \wedge c \in \varphi_2(Q_b))\}$$
$$o_2(q, Q_a, Q_b) := \{c \in \Sigma : (q,c) \in \delta_2 \vee ((q,c) \in \delta_1 \wedge c \in \varphi_1(Q_a))\}$$

  A pair of policies is feasible iff $\delta(q,c)! \Rightarrow \xi_R(r,c)!$ everywhere, i.e. $c \in o_i(r) \Rightarrow \eta_i(Q_x, c)$, in which case we call the "run-through" successful.
- Checking Opacity: Epsilonize ξ_R according to o_1 and o_2 is equivalent to creating the observer
- Algorithm for Finding Plant-Based Solutions: complete and sound, $O(2^{|\delta|}(|Q|^2 \cdot |\Sigma| + |Q|^3))$
- Minimality: guaranteed by enumeration

References

- Rudie, Karen, Stéphane Lafortune, and Feng Lin. ``Minimal communication in a distributed discrete-event system." IEEE transactions on automatic control 48.6 (2003): 957-975.
- Zhang, Bo, Shaolong Shu, and Feng Lin. ``Maximum information release while ensuring opacity in discrete event systems." IEEE Transactions on Automation Science and Engineering 12.3 (2015): 1067-1079.
- Lin, Feng. ``Opacity of discrete event systems and its applications." Automatica 47.3 (2011): 496-503.

Acknowledgments

Thanks to Professor Karen Rudie and Dr. Behnam Behinaein for their guidance during the project. This work was supported by The Fields Institute and NSERC (Canada).

More Information

Email flin@g.hmc.edu
Download the PDF for this poster at https://github.com/feiyanglin/FUSRP-OpacityProjectPoster/releases/latest

Team Members

•Feiyang Lin
•Ende Jin
•Tianchen Tang

Advisor

•Professor Karen Rudie (Queen's University)
•Dr. Behnam Behinaein