Supplement Material for the Paper "Synthesis of Maximally Permissive Supervisors for Partially-Observed Discrete-Event Systems"

Xiang Yin, *Student Member, IEEE,* Stéphane Lafortune, *Fellow, IEEE,*

Proof of Theorem IV.2

Proof. ($\Rightarrow$) Suppose that there exists a supervisor S_P for system G such that $\mathcal{L}(S_P/G) \subseteq \mathcal{L}(H)$. Then the most restrictive supervisor S_P^{res}, i.e., $S_P^{res}(s) = E_{uc}, \forall s \in \mathcal{L}(G)$, also generates a sublanguage of $\mathcal{L}(H)$. Let T be the complete BTS obtained by taking $C_T(y) = \{E_{uc}\}, \forall y \in Q_Y^T$. We know that $\mathcal{S}(T) = \{S_P^{res}\}$. Moreover, by Theorem IV.1, we know that $\mathcal{L}(S_P/G) \subseteq \mathcal{L}(H)$ if and only if $\forall s \in \mathcal{L}(S_P/G) : D_I(I(IS_{S_P}^Z(s))) = 1$. So the BTS T considered above satisfies the two conditions in Definition IV.2. Therefore, $\mathcal{AIC}(G)$ at least contains T, which is non-empty.

($\Leftarrow$) Suppose that $\mathcal{AIC}(G)$ is non-empty. Then there exists a supervisor $S_P \in \mathcal{S}(\mathcal{AIC}(G))$ included in the AIC. By Definition III.4 and III.5,, we know that $\forall s \in \mathcal{L}(S_P/G) : IS_{S_P}^Z(s) \in Q_Z^{AICG}$, which implies that $\forall s \in \mathcal{L}(S_P/G) : D_I(I(IS_{S_P}^Z(s))) = 1$ by the definition of the AIC. Therefore, by Theorem IV.1, we know that $\mathcal{L}(S_P/G) \subseteq \mathcal{L}(H)$. □

Proof of Theorem IV.3

Proof. ($\Leftarrow$) Suppose that $L \in \mathcal{L}_{TS}(\mathcal{AIC}(G))$. From Def. III.6, we know that there exists $S_P \in \mathcal{S}(\mathcal{AIC}(G))$ such that $\mathcal{L}(S_P/G) = L$. Thus, L is controllable, observable, prefix-closed and non-empty (by the Controllability and Observability Theorem). From Def. IV.2, we know that all the states of the AIC are legal, i.e., $D_I(I(z)) = 1, \forall z \in Q_Z^{AICG}$. This implies that L is a sublanguage of $\mathcal{L}(H)$ by Theorem IV.1.

($\Rightarrow$) We prove this direction by contradiction. Suppose that L is a non-empty prefix-closed controllable and observable sublanguage of $\mathcal{L}(H)$, and assume it is not generated by $\mathcal{AIC}(G)$. Since L is controllable and observable, there exists a supervisor S_P such that $\mathcal{L}(S_P/G) = L$. Then there exists a BTS T such that $S_P \in \mathcal{S}(T)$. Specifically, we consider the complete BTS T defined as follows: $Q_Y^T := \{y \in I : \exists s \in \mathcal{L}(S_P/G) \text{ s.t. } y = IS_{S_P}^Y(s)\}$, $Q_Z^T := \{z \in I \times \Gamma : \exists s \in \mathcal{L}(S_P/G) \text{ s.t. } z = IS_{S_P}^Z(s)\}$ and for any $y \in Q_Y^T$, $C_T(y) := \{\gamma \in \Gamma : \exists s \in \mathcal{L}(S_P/G) \text{ s.t. } y = IS_{S_P}^Y(s) \wedge \gamma = S_P(s)\}$. Since $L \subseteq \mathcal{L}(H)$, by Theorem IV.1, we know that $\forall z \in Q_Z^T : D_I(I(z)) = 1$. Note that $\mathcal{S}(T)$ may not be a singleton in general, since S_P need not take the same control decision different times it visits the same information state, and $\mathcal{S}(T) = \{S_P\}$ only when $\forall s, t \in \mathcal{L}(S_P/G) : IS_{S_P}^Y(s) = IS_{S_P}^Y(s) \Rightarrow S_P(s) = S_P(t)$. Since L is not generated by $\mathcal{AIC}(G)$, we know that $S_P \notin \mathcal{S}(\mathcal{AIC}(G))$, which implies that there exists a string s, $s \in \mathcal{L}(S_P/G)$, such that $S_P(s) \notin C_{\mathcal{AIC}(G)}(IS_{S_P}^Y(s))$. In this case, the union of T and $\mathcal{AIC}(G)$ is strictly larger than $\mathcal{AIC}(G)$, since control decision $S_P(s)$ is defined at Y-state $IS_{S_P}^Y(s)$ in $T \cup \mathcal{AIC}(G)$ but not in $\mathcal{AIC}(G)$. This contradicts the fact that $\mathcal{AIC}(G)$ is the largest complete and safe subsystem of the TC in the definition of the AIC. Thus, L is generated by $\mathcal{AIC}(G)$. □

Proof of Theorem IV.4

Proof. ($\Rightarrow$) Suppose that $\gamma \in C_{\mathcal{AIC}(G)}(y)$. Since $y \in Q_Y^{AICG}$, by the Def. IV.2, there exists $S_P \in \mathcal{S}(\mathcal{AIC}(G))$ such that $\exists s \in \mathcal{L}(S/G) : IS_{S_P}^Y(s) = y \wedge S_P(s) = \gamma$. Now let us assume that $D_I^e(\text{UR}_\gamma^+(y)) = 0$ and prove this direction by contradiction. Since $\text{UR}_\gamma^+(I(z)) = \text{UR}_\gamma^+(y)$, where $z = h_{YZ}(y, \gamma)$, by Lemma III.1, there exists $w \in \mathcal{L}(S_P/G)$: $f(x_0, w) \in X_e$. This implies that $\exists t \in E_{uc}^* : f(x_0, wt) \notin X_H$. Clearly, st also exists in $\mathcal{L}(S_P/G)$, since all events in t are uncontrollable, which means $\mathcal{L}(S_P/G) \not\subseteq \mathcal{L}(H)$. This is a contradiction, since by Theorem IV.3, $S_P \in \mathcal{S}(\mathcal{AIC}(G))$ implies $\mathcal{L}(S_P/G) \subseteq \mathcal{L}(H)$.

($\Leftarrow$) First, we assume that $y \neq y_0$. Since $y \in Q_Y^{AICG}$, by Definition IV.2, we know that $\exists S \in \mathcal{S}(\mathcal{AIC}(G)), \exists s\sigma \in \mathcal{L}(S/G), \sigma \in E_o : IS_S^Y(s\sigma) = y$. Let us consider a supervisor S' defined as follows:

$$S'(t) = \begin{cases} S(t), & \forall t \in P^{-1}(P(\overline{\{s\}})) \cap \mathcal{L}(G) \\ \gamma, & \forall t \in P^{-1}(P(s\sigma)) \cap \mathcal{L}(G) \\ E_{uc}, & \text{else} \end{cases} \tag{1}$$

By construction, we have that

$$\begin{aligned} &\mathcal{L}(S'/G) = [E_{uc}^* \cap \mathcal{L}(G)] \cup M \cup \\ &[(ME_o \cap \mathcal{L}(S/G))E_{uc}^* \cap \mathcal{L}(G)] \cup \\ &\left[(P^{-1}(P(s\sigma)) \cap \mathcal{L}(S/G))(\gamma \cap E_{uo})^*(\gamma \cap E_o)E_{uc}^* \cap \mathcal{L}(G)\right] \end{aligned} \tag{2}$$

where, $M = P^{-1}(P(\overline{\{s\}})) \cap \mathcal{L}(S/G)$. Since $\mathcal{L}(S/G) \subseteq \mathcal{L}(H)$, we know that M and $E_{uc}^* \cap \mathcal{L}(G)$ are sublanguages of $\mathcal{L}(H)$. Since $\mathcal{L}(S/G)$ is controllable, we know that $(ME_o \cap \mathcal{L}(S/G))E_{uc}^* \cap \mathcal{L}(G) \subseteq \mathcal{L}(S/G)E_{uc}^* \cap \mathcal{L}(G) = \mathcal{L}(S/G) \subseteq \mathcal{L}(H)$. For the last component of (2), since $D_I^e(\text{UR}_\gamma^+(y)) = 1$, by the definition of the extended unobservable reach and the extended specification, we know that $\forall w \in (P^{-1}(P(s\sigma)) \cap \mathcal{L}(S/G))(\gamma \cap E_{uo})^*(\gamma \cap E_o) \cap \mathcal{L}(G), \forall v \in E_{uc}^* : f(x_0, wv) \in X_H$. Therefore, the last component is also a sublanguage of $\mathcal{L}(H)$, which implies that $\mathcal{L}(S'/G) \subseteq \mathcal{L}(H)$. By Theorem IV.3, we know that $S' \in \mathcal{S}(\mathcal{AIC}(G))$. Therefore, $\gamma \in C_{\mathcal{AIC}(G)}(y)$.

Xiang Yin and Stéphane Lafortune are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA. {xiangyin,stephane}@umich.edu.

In the above proof, we assume that $y \neq y_0$. If $y = y_0$, then we can take $\epsilon \in \mathcal{L}(S/G), IS_S^Y(\epsilon) = y_0$ and S' can be constructed by $S'(\epsilon) = \gamma$ and $\forall s \neq \epsilon : S'(s) = E_{uc}$. This will still provide the same result. $\square$