Supplementary material concerning the paper:

Event Critical-Horizon Opacity

Dan You, *Member, IEEE*, ShouGuang Wang, *Senior Member, IEEE*, MengChu Zhou, *Fellow, IEEE*
Carla Seatzu, *Senior Member, IEEE*

ACRONYMS

靠左 靠左

DES	Discrete Event Systems
DFA	Deterministic Finite-state Automata
UAV	Unmanned Aerial Vehicles

NOMENCLATURE

Σ_s	set of secret events
Σ_F	set of fault events
δ: $X \times \Sigma \to X$	deterministic *transition function*
$L(G)$	the language generated by G
$\Psi(\Sigma')$	set of strings in $L(G)$ ending with an event $e \in \Sigma'$
$\Gamma_K(\sigma)$	*K-step suffix* of $\sigma \in \Sigma^*$
$\mathcal{K}: \Sigma_S \to \mathbb{Z}^+ \cup \{+\infty\}$	a function associating with each secret event a critical horizon
$Seq(x)$	set of all sequences leading from initial state x_0 to state x in system G
$Ver^{\mathcal{K}}(G)$	event critical-horizon opacity verifier
$Ver^{K}(G)$	K-step event-opacity verifier
$Ver^{\infty}(G)$	infinite-step event-opacity verifier
$P_G^{-1}(\omega)$	set of consistent strings of ω in G
$P: \Sigma^* \to \Sigma_o^*$	natural projection

PROOF OF LEMMA 1

1) First, we consider $\epsilon \in L(Ver^{\mathcal{K}}(G))$. Clearly, $|P_G^{-1}(\epsilon)| \neq \emptyset$. By Definition 9, it is $\delta_z(z_0, \epsilon) = z_0 = \{(\Gamma_{Kmax+1}(\sigma), x, l)|(\sigma, x, l) \in UR_{\Sigma_{S(+\infty)}}(\{(\epsilon, x_0, \emptyset)\})\}$. Thus, it is trivial to see that

$$\delta_z(z_0, \epsilon) = \{(\Gamma_{Kmax+1}(\sigma), \delta(x_0, \sigma), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma))| \sigma \in P_G^{-1}(\epsilon)\}.$$

Next, we consider $\omega' \in L(Ver^{\mathcal{K}}(G))$ with $\omega' = \omega v$, where $v \in \Sigma_o$ and $\omega \in L(Ver^{\mathcal{K}}(G))$ satisfying $|P_G^{-1}(\omega)| \neq \emptyset$ and

$$\delta_z(z_0, \omega) = \{(\Gamma_{Kmax+1}(\sigma), \delta(x_0, \sigma), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma))| \sigma \in P_G^{-1}(\omega)\}. \quad (1)$$

Clearly, $\delta_z(z_0, \omega) \neq \emptyset$. Let $z = \delta_z(z_0, \omega)$. By Definition 9, $v \in En_o(z)$ and

$$\delta_z(z, v) = \{(\Gamma_{Kmax+1}(\sigma), x, l)| (\sigma, x, l) \in UR_{\Sigma_{S(+\infty)}}(Next(z, v))\}.$$

Due to (~~3~~ 1), since $v \in En_o(z)$, it follows that

$$\exists \sigma \in P_G^{-1}(\omega), \text{ s.t. } \delta(x_0, \sigma v)! \quad (2)$$

and it holds that

$$Next(z, v) = \{(\Gamma_{Kmax+1}(\sigma)v, \delta(x_0, \sigma v), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma v)) \mid \sigma \in P_G^{-1}(\omega), \delta(x_0, \sigma v)!\}.$$

Furthermore, it is

$$UR_{\Sigma_{S(+\infty)}}(Next(z, v)) = \{(\Gamma_{Kmax+1}(\sigma)\nu u, \delta(x_0, \sigma v u), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma v u)) \mid \sigma \in P_G^{-1}(\omega), u \in \Sigma_u^*, \delta(x_0, \sigma v u)!\}.$$

Trivially, it is

$$\delta z(z, v) = \{(\Gamma_{Kmax+1}(\sigma \nu u), \delta(x_0, \sigma v u), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma v u)) \mid \sigma \in P_G^{-1}(\omega), u \in \Sigma_u^*, \delta(x_0, \sigma v u)!\}. \quad (3)$$

Note that it holds

$$P_G^{-1}(\omega') = P_G^{-1}(\omega v) = \{\sigma v u \mid \sigma \in P_G^{-1}(\omega), u \in \Sigma_u^*, \delta(x_0, \sigma v u)!\}. \quad (4)$$

Thus, $|P_G^{-1}(\omega')| \neq \emptyset$ by (~~4~~ 2). In addition, by (~~5~~ 3) and (~~6~~ 4), it follows

$$\delta_z(z, v) = \{(\Gamma_{Kmax+1}(\sigma'), \delta(x_0, \sigma'), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma')) \mid \sigma' \in P_G^{-1}(\omega')\}.$$

Since $z = \delta_z(z_0, \omega)$ and $\omega' = \omega v$, it is

$$\delta_z(z_0, \omega') = \delta_z(z, v) = \{(\Gamma_{Kmax+1}(\sigma'), \delta(x_0, \sigma'), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma')) \mid \sigma' \in P_G^{-1}(\omega')\}.$$

Consequently, we conclude that

$$\forall \omega \in L(Ver^{\mathcal{K}}(G)), |P_G^{-1}(\omega)| \neq \emptyset \text{ and } \delta_z(z_0, \omega) = \{(\Gamma_{Kmax+1}(\sigma), \delta(x_0, \sigma), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma)) \mid \sigma \in P_G^{-1}(\omega)\}.$$

2) It is proved that $\forall \omega \in L(Ver^{\mathcal{K}}(G))$, $|P_G^{-1}(\omega)| \neq \emptyset$. It means $\forall \omega \in L(Ver^{\mathcal{K}}(G))$, $\omega \in P(L(G))$. Thus, $L(Ver^{\mathcal{K}}(G)) \subseteq P(L(G))$. Next, we prove $L(Ver^{\mathcal{K}}(G)) \supseteq P(L(G))$.

First, we consider $\epsilon \in P(L(G))$. It is clear that $\epsilon \in L(Ver^{\mathcal{K}}(G))$.

Next, we consider $\omega' \in P(L(G))$ s.t. $\omega' = \omega v$, where $v \in \Sigma_o$ and $\omega \in P(L(G)) \wedge \omega \in L(Ver^{\mathcal{K}}(G))$. We prove $\omega' \in L(Ver^{\mathcal{K}}(G))$.

Since $\omega v \in P(L(G))$, $\omega \in P(L(G))$ and $v \in \Sigma_o$, it holds that

$$\exists \sigma \in P_G^{-1}(\omega), \text{ s.t. } \sigma v \in L(G). \tag{5}$$

去掉空的一行

Since $\omega \in L(Ver^{\mathcal{K}}(G))$, there exists $z \in Z$ s.t.

$$\begin{aligned} z = \delta_z(z_0, \omega) = &\{(\Gamma_{Kmax+1}(\sigma), \delta(x_0, \sigma), \eta_{\Sigma_{S(+\infty)}}(\emptyset, \sigma)) \\ &\mid \sigma \in P_G^{-1}(\omega)\}. \end{aligned} \tag{6}$$

Due to (~~7~~5) and (~~8~~6), it is $v \in En_o(z)$. Thus, $\omega' \in L(Ver^{\mathcal{K}}(G))$ since $\omega \in L(Ver^{\mathcal{K}}(G))$.

Consequently, it holds that $\forall \omega \in P(L(G))$, $\omega \in L(Ver^{\mathcal{K}}(G))$, i.e., $L(Ver^{\mathcal{K}}(G)) \supseteq P(L(G))$. Therefore, $P(L(G)) = L(Ver^{\mathcal{K}}(G))$.