Supplementary document to "Critical Observability Verification and Enforcement of Labeled Petri Nets by Using Basis Markings"

Xuya Cong, *Member, IEEE,* Maria Pia Fanti, *Fellow, IEEE,* Agostino Marcello Mangini, *Member, IEEE,* and Zhiwu Li, *Fellow, IEEE*

Theorem 1: [1] Let $G = (PN, M_0, E, \lambda)$ be an LPN whose unobservable subnet is acyclic. For all $w \in \mathcal{L}(G)$, it holds

$$\begin{aligned}\mathcal{C}(w) &= \bigcup_{M_b \in \mathcal{C}_b(w)} \mathcal{U}(M_b) \\ &= \bigcup_{M_b \in \mathcal{C}_b(w)} \{M \in \mathbb{N}^m | \exists \vec{y}_u \in \mathbb{N}^{n_{uo}} : \\ &\qquad M = M_b + C_u \cdot \vec{y}_u\}.\end{aligned} \tag{1}$$

Theorem 2: [2] Given an LPN G, let $\mathcal{B} = (\mathcal{M}_B, E, \delta, M_0)$ be its BRG. The following two statements are equivalent:

1) There exist a marking M and a firing sequence $\sigma = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \cdots \sigma_{u_n} t_n \sigma_{u_{n+1}}$ with $\sigma_{u_i} \in T_{uo}^*$, $\lambda(\sigma) = e_1 e_2 \cdots e_n$, and $t_j \in T_o$ for all $i \in \{1, 2, \ldots, n+1\}$ and for all $j \in \{1, 2, \ldots, n\}$, such that $M_0[\sigma\rangle M$;

2) There is a path $M_0 \xrightarrow{e_1} M_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} M_n$ in the BRG $\mathcal{B}$ such that $M \in \mathcal{U}(M_n)$.

Definition 1: [3] Let us consider an LPN $G = (PN, M_0, E, \lambda)$ and a set of critical markings C_R. G is said to be *critically observable* if $[\mathcal{C}(w) \subseteq C_R] \vee [\mathcal{C}(w) \subseteq R(PN, M_0) \setminus C_R]$, for all $w \in \mathcal{L}(G)$.

Definition 2: Given an LPN $G = (PN, M_0, E, \lambda)$, its BRG $\mathcal{B} = (\mathcal{M}_B, E, \delta, M_0)$, and a set of critical markings C_R, the set of fully-critical basis markings is defined as $\mathcal{F} = \{M \in \mathcal{M}_B | \mathcal{U}(M) \subseteq C_R\}$, the set of partially-critical basis markings is defined as $\mathcal{P} = \{M \in \mathcal{M}_B | \mathcal{U}(M) \cap C_R \neq \emptyset \wedge \mathcal{U}(M) \setminus C_R \neq \emptyset\}$, and the set of non-critical basis markings is defined as $\mathcal{N} = \{M \in \mathcal{M}_B | \mathcal{U}(M) \cap C_R = \emptyset\}$.

Definition 3: Given an LPN G and a critical marking set C_R, a state $x = (M, M')$ in the twin-BRG of G is said to be critical observability violative if one of the following two conditions holds:

1) $M \in \mathcal{P}$;
2) $M \in \mathcal{F}$ and $M' \in \mathcal{N}$.

Proposition 1: Given an LPN $G = (PN, M_0, E, \lambda)$, its BRG $\mathcal{B} = (\mathcal{M}_B, E, \delta, M_0)$, and a set of critical markings $C_R = \{M_c^1, \ldots, M_c^q\}$, a basis marking $M \in \mathcal{M}_B$ is fully-critical *iff* the integer constraint set (2) is infeasible, a basis marking $M \in \mathcal{M}_B$ is partially-critical *iff* the integer constraint sets (2) and (3) are feasible, and a basis marking $M \in \mathcal{M}_B$ is non-critical *iff* the integer constraint set (3) is infeasible:

$$\begin{cases} \bigwedge\limits_{M_c^k \in C_R} M + C_u \cdot \vec{y}_\sigma \neq M_c^k, \\ M + C_u \cdot \vec{y}_\sigma \geq \vec{0}, \\ \vec{y}_\sigma \in \mathbb{N}^{n_{uo}} \end{cases} \tag{2}$$

$$\begin{cases} \bigvee\limits_{M_c^k \in C_R} M + C_u \cdot \vec{y}_{\sigma'} = M_c^k, \\ M + C_u \cdot \vec{y}_{\sigma'} \geq \vec{0}, \\ \vec{y}_{\sigma'} \in \mathbb{N}^{n_{uo}}. \end{cases} \tag{3}$$

Proof: *(If)* First, if Eq. (2) is infeasible, then there is no marking $M' = M + C_u \cdot \vec{y}_\sigma \notin C_R$ such that $M[\sigma_u\rangle M'$ with $\vec{y}_{\sigma_u} = \vec{y}_\sigma$ by Theorem 1. That is to say, M is a fully-critical basis marking. Second, if Eqs. (2) and (3) are feasible, then there exist two markings $M' = M + C_u \cdot \vec{y}_\sigma \notin C_R$ and $M'' = M + C_u \cdot \vec{y}_{\sigma'} \in C_R$. By Theorem 1, we have $M[\sigma_u\rangle M'$ and $M[\sigma'_u\rangle M''$ with $\vec{y}_{\sigma_u} = \vec{y}_\sigma$ and $\vec{y}_{\sigma'_u} = \vec{y}_{\sigma'}$. Thus, M is a partially-critical basis marking. Third, if Eq. (3) is infeasible, then there is no marking $M'' = M + C_u \cdot \vec{y}_{\sigma'} \in C_R$ such that $M[\sigma'_u\rangle M''$ with $\vec{y}_{\sigma'_u} = \vec{y}_{\sigma'}$ by Theorem 1, i.e., M is a non-critical basis marking.

(Only if) We prove it by contrapositive. First, if Eq. (2) is feasible, then there is a marking $M' = M + C_u \cdot \vec{y}_\sigma \notin C_R$ such that $M[\sigma_u\rangle M'$ with $\vec{y}_{\sigma_u} = \vec{y}_\sigma$ by Theorem 1, which implies that M is not a fully-critical basis marking. Second, if Eq. (2) or Eq. (3) is infeasible, from the if-part of the proof, M is not a partially-critical basis marking. Third, if Eq. (3) is feasible, then there is a marking $M'' = M + C_u \cdot \vec{y}_{\sigma'} \in C_R$ such that $M[\sigma'_u\rangle M''$ with $\vec{y}_{\sigma'_u} = \vec{y}_{\sigma'}$ by Theorem 1. Thus, M is not a non-critical basis marking. □

Proposition 2: Given an LPN $G = (PN, M_0, E, \lambda)$, its BRG $\mathcal{B} = (\mathcal{M}_B, E, \delta, M_0)$, and a set of critical markings C_R, G is critically observable if there is no partially-critical basis marking in the BRG $\mathcal{B}$ of G.

Proof: By contrapositive, suppose that the LPN is not critically observable. It implies that there exists at least one word w such that $\mathcal{C}(w) \cap C_R \neq \emptyset$ and $\mathcal{C}(w) \setminus C_R \neq \emptyset$. Based on Theorems 1 and 2, there exists a path $M_0 \xrightarrow{w} M$ in the BRG such that $M \in \mathcal{C}(w)$ with $\mathcal{U}(M) \cup C_R \neq \emptyset$ and $\mathcal{U}(M) \setminus C_R \neq \emptyset$. Thus, M is a partially-critical basis marking in the BRG. □

X. Cong is with the Youth Innovation Team of Shaanxi Universities, College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710054, China (email: congxuya@163.com).

M. Fanti and A. Mangini are with the Department of Electrical and Information Engineering, Polytechnic of Bari, 70125 Bari, Italy (email: mariapia.fanti@poliba.it; agostinomarcello.mangini@poliba.it).

Z. Li is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China and also with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau. (email: zhwli@xidian.edu.cn).

Proposition 3: Given an LPN $G = (PN, M_0, E, \lambda)$, its twin-BRG $B = (X, E, \delta_{tw}, x_0)$, and a critical marking set C_R, G is critically observable *iff* there is no critical observability violative state in the twin-BRG B of G.

Proof: *(If)* By contrapositive, suppose that G is not critically observable. Then, we have an event sequence w such that $\mathcal{C}(w) \cap C_R \neq \emptyset$ and $\mathcal{C}(w) \cap (R(PN, M_0) \setminus C_R) \neq \emptyset$. There exist two firing sequences σ_1 and σ_2 with the same observation w such that $M_0[\sigma_1\rangle M_2 \in C_R$ and $M_0[\sigma_2\rangle M_2' \notin C_R$. By the construction of the twin-BRG and Theorem 2, there exists a path $x_0 = (M_0, M_0) \xrightarrow{w} x = (M_1, M_1')$ in the twin-BRG such that one of the following two conditions holds: (i) $x_0 \xrightarrow{w} x$, $M_2 \in \mathcal{U}(M_1)$ and $M_2' \in \mathcal{U}(M_1')$ and (ii) $x_0 \xrightarrow{w} x$, $M_2 \in \mathcal{U}(M_1)$ and $M_2' \in \mathcal{U}(M_1)$. Thus, x is a critical observability violative state.

(Only if) By contrapositive, suppose that there exists a critical observability violative state $x = (M_1, M_1')$ in the twin-BRG B. Then, we have the following two cases: (i) $M_1 \in \mathcal{P}$ and (ii) $M_1 \in \mathcal{F}$ and $M_1' \in \mathcal{N}$. For the first case, based on Proposition 2 and the construction of the BRG, we conclude that G is not critically observable. For the second case, we have two paths in the BRG such that $M_0 \xrightarrow{w} M_1$ and $M_0 \xrightarrow{w} M_1'$ based on the construction of the twin-BRG. Moreover, from Definition 3, we know that there exist two markings M_2 and M_2' such that $M_2 \in \mathcal{U}(M_1) \cap C_R$ and $M_2' \in \mathcal{U}(M_1') \setminus C_R$. Based on Theorem 2, the existence of M_2 and M_2' implies that $M_0[\sigma_1\rangle M_2$ and $M_0[\sigma_2\rangle M_2'$ with $\lambda(\sigma_1) = \lambda(\sigma_2) = w$, i.e., $\{M_2, M_2'\} \subseteq \mathcal{C}(w)$. Thus, G is not critically observable. □

REFERENCES

[1] M. P. Cabasino, A. Giua, M. Pocci, and C. Seatzu, "Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems," *Control Eng. Practice*, vol. 19, no. 9, pp. 989–1001, 2011.

[2] Z. Y. Ma, Y. Tong, Z. W. Li, and A. Giua, "Basis marking representation of Petri net reachability spaces and its application to the reachability problem," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1078–1093, Mar. 2017.

[3] T. Masopust, "Critical observability for automata and Petri nets," *IEEE Trans. Autom. Control*, vol. 65, no. 1, pp. 341–346, Jan. 2020.