Optimal Sensor Selection for Ensuring Diagnosability in Labeled Bounded Petri Nets

M.P. Cabasino, S. Lafortune, C. Seatzu

In this document the proofs of the theorems, propositions and lemmas of the WODES 2012 paper “Optimal Sensor Selection for Ensuring Diagnosability in Labeled Bounded Petri Nets” are reported.

**Proposition 3.2** Under rules (R1) and (R2), with \(\sigma_1, \sigma_2 \in T^*\), we have that

\[
\mathcal{L}_{init}(\sigma_1) \neq \mathcal{L}_{init}(\sigma_2) \Rightarrow \mathcal{L}_{new}(\sigma_1) \neq \mathcal{L}_{new}(\sigma_2).
\]

**Proof:** We prove the contra-positive. Let

\[
\mathcal{L}_{new}(\sigma_1) = \mathcal{L}_{new}(\sigma_2).
\]

The structure of \(\sigma_1\) and \(\sigma_2\) is as depicted in Figure 1. Transitions that map to \(\varepsilon\) under \(\mathcal{L}_{new}\) necessarily map to \(\varepsilon\) under \(\mathcal{L}_{init}\). Hence, the \(\varepsilon\)-segments between the common label observations of \(\sigma_1\) and \(\sigma_2\) under \(\mathcal{L}_{new}\) in the figure remain \(\varepsilon\)-segments under \(\mathcal{L}_{init}\). Similarly, the common observations of a given label \(\beta \in \mathcal{L}_{init}\) remain the same under \(\mathcal{L}_{init}\) since \(\mathcal{L}_{new}\) does not reuse labels from \(\mathcal{L}_{init}\) by assumption.

We conclude that the only changes in going from \(\mathcal{L}_{new}\) to \(\mathcal{L}_{init}\) in \(\sigma_1\) and \(\sigma_2\) involve common observable labels of the form \(\alpha_t \in \mathcal{L}_{total}\). Clearly, since we have the same label \(\alpha_t\) in both \(\sigma_1\) and \(\sigma_2\) at each “synchronization point” of the sequences of transition labels, then the transition that fires at that point is the same transition \(t\) in both \(\sigma_1\) and \(\sigma_2\). In view of rules (R1) and (R2), we have that:

1. If \(t \in T_{reg}\), then \(\mathcal{L}_{init}(t) = \varepsilon\).
2. If \(t \in T_o\), then \(\mathcal{L}_{init}(t) = \ell \in \mathcal{L}_{init}\).

In either case, the end result is that both sequences \(\sigma_1\) and \(\sigma_2\) have the same label under \(\mathcal{L}_{init}\) at each synchronization point. Overall, we have proved that

\[
\mathcal{L}_{init}(\sigma_1) = \mathcal{L}_{init}(\sigma_2)
\]

which completes the proof.

**Lemma 4.3** Let \(N\) be non-diagnosable under \(\mathcal{L}_{init}\) and consider path \(\sigma_{vn}\) in \(RT_f\). Let \(\mathcal{L}_{new}\) be the same as \(\mathcal{L}_{init}\) except for the relabeling of \(t_i \in T_{reg}\) according to (LO2) or (LO3) and (R1). If \(t_i\) only appears in \(\sigma_{vn}\) in consecutive pairs of the form

\[
(\lambda, \gamma_i)(\gamma'_i, \lambda) \quad \text{or} \quad (\gamma'_i, \lambda)(\lambda, \gamma_i)
\]
where $\gamma_i = t_i$ and $\gamma'_i = t_i$, then $N$ remains non-diagnosable under $L_{new}$.

**Proof:** It suffices to consider that $\sigma_{vn}$ contains a single consecutive pair, say, $\text{pair} = (\lambda, \gamma_i)(\gamma'_i, \lambda)$ with $\gamma_i = t_i$ and $\gamma'_i = t_i$. If we build the new VN under $L_{new}$, then since none of the transitions before or after $\text{pair}$ have had their labels changed, the prefix and suffix of $\sigma_{vn}$ around $\text{pair}$ will be unchanged under $L_{new}$. To build a bad path of the VN under $L_{new}$, we replace $\text{pair}$ by a single transition of the new VN of the form $(\gamma'_i, \gamma_i)$ with label $(L_{new}(t_i), L_{new}(t_i))$. Clearly, since $(\lambda, \gamma_i)(\gamma'_i, \lambda)$ was possible in the original VN, by executing the prefix of $\text{pair}$ we reach the same state in the new VN where $(\gamma'_i, \gamma_i)$ is firable; moreover, it results in the same state as firing $(\lambda, \gamma_i)(\gamma'_i, \lambda)$, implying that the suffix of $\text{pair}$ can be continued unchanged in the new VN. Consequently, we have constructed a bad path in the new VN, proving that the system remains non-diagnosable under $L_{new}$.

**Proposition 4.4** Along every EBP in $RT_f$, there must exist at least one transition which can be relabeled according to the admissible relabeling options (LO1) and (LO2) or (LO3) and associated rules (R1), (R2), (R4).

**Proof:** By contradiction, suppose all transitions in an EBP of $RT_f$ are of the form in (LO4) and (LO5), possibly with consecutive transitions of the form (LO2)-(LO3) [we need this in view of (R4)]. We cannot do anything with (LO5). For the remainder, we can see that even if every single transition (except faulty ones) in that EBP were to be relabeled, the EBP would still exist as the relabeling would maintain equality of projection of the left string of labels with the right string of labels. For pairs of the form $(\lambda, \gamma_i)$ and $(\gamma'_i, \lambda)$, as we saw in the proof of Lemma 4.3, we would get a single pair of the form $(\gamma'_i, \gamma_i)$, for which the same conclusion holds. Hence, we get a contradiction of assumption (A3). In other words, under assumption (A3), it is always possible to implement rules (R1)-(R4).

**Proposition 4.5** Given an EBP $\tilde{\sigma}$ in $RT_f$, that is relabeled according to the admissible relabeling options (LO1) and (LO2) or (LO3) and associated rules (R1), (R2), (R3) and (R4), we have that

$$L_{new}(\sigma'_p\sigma'_s) \neq L_{new}(\sigma_p\sigma_s),$$
where $\sigma'_p, \sigma'_s, \sigma_p$ and $\sigma_s$ are defined as in Definition 4.2.

**Proof:** By Proposition 4.4 we know that along every EBP in $RT_f$ there exists at least one transition that can be relabeled and by rule (R3) we know we have to relabel at least one transition $t \in T_o \cup T_{reg}$ for each EBP.

Let us consider the case in which we relabel an observable transition. According to (LO1), we can either relabel $\gamma'_i \in \sigma'_p \sigma'_s$ or $\gamma_j \in \sigma_p \sigma_s$; since we are introducing in both cases a new label, either $L_{new}(\gamma'_i) = t_i$ or $L_{new}(\gamma_j) = t_j$, this relabeling changes the observable projection of either $\sigma'_p \sigma'_s$ or $\sigma_p \sigma_s$, thus proving the statement.

Let us consider the case in which we relabel an unobservable transition. We can relabel either $\gamma_j$ in $(\lambda, \gamma_j)$ (LO2) or $\gamma'_i$ in $(\gamma'_i, \lambda)$ (LO3) when rule (R3) is satisfied. Let us first consider the case (LO2). In the EBP $(\lambda, \gamma_j)$ can be preceded or followed by $(\lambda, \gamma_k), (\gamma'_i, \lambda), (\gamma'_i, \gamma_i), (\gamma'_i, \gamma_k)$, where $\gamma_k \neq \gamma_j$ (thus consequently $\gamma'_i \neq \gamma_j$) and $L_{init}(\gamma_i) = L_{init}(\gamma_k)$. Since the originally unobservable transition $\gamma_j$ of the faulty net $(N, M_0, L_{new})$ (see Section 4.1) is now observable and labeled $L_{new}(\gamma_j) = t_j$, it cannot be synchronized with the corresponding unobservable transition $\gamma'_j$ of the fault-free net $(N', M'_0, L_{new})$ because (R3) holds, then $L_{new}(\sigma'_p \sigma'_s) \neq L_{new}(\sigma_p \sigma_s)$. The same arguments can be repeated for the case of (LO3).

**Proposition 4.6** If each EBP is relabeled according to the admissible relabeling options (LO1) and (LO2) or (LO3) and associated rules (R1), (R2), (R3) and (R4) then in the Petri net system $(N, M_0, L_{new})$ there are no more EBPs, i.e., the relabeling does not create any new EBP.

**Proof:** By contradiction, assume there is a “new” EBP $\tilde{\sigma}_{new}$ wrt $L_{new}$. Let decompose it in the form:

$$\tilde{\sigma}_{new} = (\sigma'_{new}, \sigma_{new}) = \phi_1(t'_1, t_1) \phi_2(t'_2, t_2) \phi_3(t'_3, t_3) \cdots (t'_k, t_k) \phi_{k+1}$$

where $\phi_i$ with $i \in \{1, \ldots, k + 1\}$ are sequences of transition pairs (possibly empty) that are not relabeled by $L_{new}$, $(t'_i, t_i)$ with $i \in \{1, \ldots, k\}$ are transition pairs that have been relabeled by $L_{new}$, and $\sigma'_{new}$ (resp. $\sigma_{new}$) is the corresponding sequence of transitions in the fault-free (resp. faulty) net $(N', M'_0, L'_{new})$ (resp. $(N, M_0, L_{new})$).

Let us now modify the $(t'_i, t_i)$ elements in $\tilde{\sigma}_{new}$ according to the following rules: if $L_{init}(t_i) \in L_{init}$ keep $(t'_i, t_i)$ as in $\tilde{\sigma}_{new}$, while if $L_{init}(t_i) = \varepsilon$ replace $(t'_i, t_i)$ by $(\lambda, t_i)(t'_i, \lambda)$ (or equivalently by $(t'_i, \lambda)(\lambda, t_i)$). Call the resulting new sequence of transition pairs $\tilde{\sigma}_{new-mod}$.

It follows that $L_{init}(\sigma'_{new-mod}) = L_{init}(\sigma_{new-mod})$, so $\tilde{\sigma}_{new-mod}$ was an EBP wrt $L_{init}$ and since according to relabeling options (LO4) we cannot relabel a transition of type $(t'_i, t_i)$ nor by rule (R4) a consecutive pair $(\lambda, t_i)(t'_i, \lambda)$ (or equivalently $(t'_i, \lambda)(\lambda, t_i)$), this implies we would have had to do relabeling in some $\phi_i$ segment, because by rule (R3) we have to relabel at least one transition in the path from the root to the leaf according to relabeling options (LO1) to (LO3). This leads to a contradiction.

□
**Proposition 4.7** A Petri net system \( \langle N, M_0, \mathcal{L} \rangle \) is diagnosable if the corresponding pruned RT of its VN (called \( RT_f \)) is empty, namely if there do not exist EBPs in \( RT_f \).

**Proof:** By contradiction, suppose that a system is not diagnosable. By definition of diagnosability, this means that there exist two sequences \( \sigma_{nf} \) and \( \sigma_f \) of arbitrarily long length and such that \( t_f \notin \sigma_{nf} \) and \( t_f \in \sigma_f \) and such that \( \mathcal{L}(\sigma_{nf}) = \mathcal{L}(\sigma_f) \). But if there exist two such sequences then there exists an EBP built with a prefix of these sequences. This leads to a contradiction.

**Theorem 4.8** Let \( \langle N, M_0, \mathcal{L}_{init} \rangle \) be non-diagnosable and let \( RT_f^{init} \) be the corresponding pruned RT of its VN. Let \( \mathcal{L}_{new} \) be obtained according to rules (R1), (R2), (R3), (R4) with corresponding relabeling options (LO1), (LO2), (LO3) for elementary bad paths of \( RT_f^{init} \). Then \( \langle N, M_0, \mathcal{L}_{new} \rangle \) is diagnosable.

**Proof:** The proof directly follows by Propositions 3.2, 4.5, 4.6. In fact, by Proposition 3.2 we can state that the new labeling function \( \mathcal{L}_{new} \) keeps distinguishable all sequences that were distinguishable under \( \mathcal{L}_{init} \). By Proposition 4.5 we can state that each EBP in \( RT_f \) can be “broken” if it is relabeled according to the admissible relabeling options (LO1) and (LO2) or (LO3) and the associated rules (R1), (R2), (R3) and (R4). Finally, by Proposition 4.6 we prove that the relabeling of each EBP using (LO1) and (LO2) or (LO3) and the associated rules (R1), (R2), (R3) and (R4) does not create other EBPs. Thus once we have relabeled each EBP (and they are in a finite number due to the unfolding) of \( RT_f \), there are no more EBPs, then by Proposition 4.7 the system is diagnosable.