Exercise 90. *Prove, as claimed in the verification of the synchronous version of TIP, that $\mathcal{I}_4$ is an invariant for Y.*

The linearization of Implementation A of the Tree Identify Protocol TIP consists of the processes $Y(p : \text{Nodelistlist}, s : \text{Statelist})$ that are defined by the following LPE:

$$\left.\begin{aligned} &Y(p : \text{Nodelistlist}, s : \text{Statelist}) \\ &\quad = \sum_{i,j:\text{Node}} \tau \cdot Y(p[i] := p[i] \setminus \{j\}\,,\, s[j] := 1) \\ &\qquad\qquad\qquad \lhd\ j \in p[i] \ \wedge\ p[j] = \{i\} \ \wedge\ s[i] = s[j] = 0 \ \rhd\ \delta \\ &\quad\ + \sum_{i:\text{Node}} \mathit{leader} \cdot Y(p,\, s[i] := 1) \lhd\ \mathit{empty}(p[i]) \ \wedge\ s[i] = 0 \ \rhd \delta \end{aligned}\right\} \tag{1}$$

The exercise refers to the following property for Nodelistlists p and Statelists s:

$$(\mathcal{I}_4(p,s)) : \quad \forall i, j : \text{Node}\ (\, j \in p[i] \ \wedge\ s[i] = 0 \ \Rightarrow\ i \in p[j] \ \wedge\ s[j] = 0\,)$$

Solution (using reasoning by contradiction, as done so in class). We assume that $\mathcal{I}_4$ is not an invariant for the process family $Y(p,s)$, and we will show that that leads to a contradiction. If we succeed in doing so, then we can conclude, by using reasoning in classical logic, that $\mathcal{I}_4$ actually is an invariant.

So let us assume that $Y(p,s) \xrightarrow{x} Y(p',s')$ with $x \in \{\mathit{leader}, \tau\}$ is a step in which $\mathcal{I}_4$ is not preserved. That is, it holds that $\mathcal{I}_4(p,s) = \mathtt{T}$ and $\mathcal{I}_4(p',s') = \mathtt{F}$.

From $\mathcal{I}_4(d') = \mathtt{F}$ we conclude that there exist nodes i_0 and j_0 such that:

$$j_0 \in p'[i_0] \ \wedge\ s'[i_0] = 0 \ \wedge\ (i_0 \notin p'[j_0] \ \vee\ s'[j_0] = 1\,)\,. \tag{2}$$

So we fix nodes i_0 and j_0 with this property. Since in steps of the LPE for Y, states are never set back from 1 to 0, and parent node lists are never enlarged, it follows from (2) that:

$$j_0 \in p[i_0] \ \wedge\ s[i_0] = 0\,. \tag{3}$$

As a consequence of this and of $\mathcal{I}_4(p,s) = \mathtt{T}$ we obtain:

$$j_0 \in p[i_0] \ \wedge\ s[i_0] = 0 \ \wedge\ i \in p[j_0] \ \wedge\ s[j_0] = 0\,. \tag{4}$$

By exploring the two possibilities of why (2) holds we will show now that the situation in which (4) holds before the step $Y(p,s) \xrightarrow{x} Y(p',s')$, and (2) after it, cannot occur.

Case 1: $i_0 \notin p'[j_0]$.

Then since $i_0 \in p[j_0]$ holds due to (4), it follows that i_0 must have been removed from $p[j_0]$ in the step. According to the LPE (1) this step must have been a τ-step, in which also $s[i_0]$ has been set to 1. So $s'[i_0] = 1$. But this contradicts $s'[i_0] = 0$ that holds according to (2).

Case 2: $s'[j_0] = 1$.

Since $s[j_0] = 0$ holds by (4), this means that $s[j_0]$ has been changed from 0 to 1 in the step.

We distinguish the two possible cases in which either $x = \mathit{leader}$ or $x = \tau$ is the action label of the step $Y(p, s) \stackrel{x}{\to} Y(p', s')$.

Case a: $Y(p, s) \stackrel{\mathit{leader}}{\longrightarrow} Y(p', s')$.

As $s[j_0]$ has been switched by this step, it can only have taken place if $p[j_0] = []$. But this contradicts $i_0 \in p[j_0]$, which holds by (4).

Case b: $Y(p, s) \stackrel{\tau}{\to} Y(p', s')$.

As $s[j_0]$ has been changed from 0 to 1 in this step, also $p[j_0] = \{i\}$ must hold for some node i, and $s'[i] = 1$. Since $i_0 \in p[j_0]$ due to (4), it follows that $p[j_0] = \{i_0\}$, and hence also $s'[i_0] = 1$. But that contradicts $s[i_0] = 0$ in (2).

So we have succeeded in showing that the situation in which (4) holds before the step $Y(p, s) \stackrel{x}{\to} Y(p', s')$, and (2) after it, cannot occur.

As this was a consequence of our assumption that $\mathcal{I}_4$ is not an invariant, we have shown that this assumption leads to a contradiction. It follows (on the basis of classical logic) that $\mathcal{I}_4$ is indeed an invariant. $\square$