Exercise 90. Prove, as claimed in the verification of the synchronous version of TIP, that $I_4$ is an invariant for $Y$.

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

$$
Y(p : Nodelistlist, s : Statelist) = \sum_{i,j : Node} \tau \cdot Y(p[i] := p[i] \setminus \{j\}, s[j] := 1) \quad \text{if } j \in p[i] \land p[j] = \{i\} \land s[i] = s[j] = 0 \triangleright \delta \\
+ \sum_{i : Node} \text{leader} \cdot Y(p, s[i] := 1) \triangleright \text{empty}(p[i]) \land s[i] = 0 \triangleright \delta \tag{1}
$$

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

$$(I_4(p, s)) : \forall i, j : Node \ (j \in p[i] \land s[i] = 0 \Rightarrow i \in p[j] \land s[j] = 0)$$

Solution (using reasoning by contradiction, as done so in class). We assume that $I_4$ 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 $I_4$ actually is an invariant.

So let us assume that $Y(p, s) \xrightarrow{x} Y(p', s')$ with $x \in \{\text{leader}, \tau\}$ is a step in which $I_4$ is not preserved. That is, it holds that $I_4(p, s) = T$ and $I_4(p', s') = F$.

From $I_4(d') = F$ we conclude that there exist nodes $i_0$ and $j_0$ such that:

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

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:

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

As a consequence of this and of $I_4(p, s) = T$ we obtain:

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

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 $\tau$-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 \( x = \text{leader} \) or \( x = \tau \) is the action label of the step \( Y(p, s) \xrightarrow{x} Y(p', s') \).

**Case a:** \( Y(p, s) \xrightarrow{\text{leader}} Y(p', s') \).

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:** \( Y(p, s) \xrightarrow{\tau} Y(p', s') \).

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 \( Y(p, s) \xrightarrow{x} Y(p', s') \), and (2) after it, cannot occur.

As this was a consequence of our assumption that \( I_4 \) is not an invariant, we have shown that this assumption leads to a contradiction. It follows (on the basis of classical logic) that \( I_4 \) is indeed an invariant. \( \square \)