312 (frame problem) Suppose there is one nonlocal variable x, and we define $P = x'=0$. Can we prove

$$P \Leftarrow \textbf{new } y\text{: } nat\cdot\ y := 0.\ P.\ x := y$$

The problem is that y was not part of the state space where P was defined, so does P leave y unchanged? Hint: consider the definition of sequential composition. Is it being used properly?

After trying the question, scroll down to the solution.

§ The definition of sequential composition

$$Q.R \;=\; \exists \sigma'' \cdot \langle \sigma' \cdot Q \rangle \sigma'' \wedge \langle \sigma \cdot R \rangle \sigma''$$

assumes that Q and R have the same state space, and identifies the final state of Q with the initial state of R. We have not defined sequential composition of specifications with different state spaces. In this question, we are composing $y := 0$ and P and $x := y$. The two assignments have a state space consisting of variables x and y, but P has a state space consisting of only x. So the composition is not defined.

We can extend our definition of sequential composition to specifications with different state spaces in various ways. One way is to expand the state space of each specification to the union of the spaces, and then make the composition. How should we make the expansion? We could keep $P = x'=0$ in the larger space consisting of x and y. Then

$$\begin{array}{ll}
 & \textbf{new } y\text{: } nat \cdot \; y := 0.\; P.\; x := y \\
= & \exists y, y' \cdot \; y := 0.\; x'=0.\; x := y \qquad \text{subst law on first composition, replace last assignment} \\
= & \exists y, y' \cdot \; x'=0.\; x'=y \wedge y'=y \qquad \text{expand remaining composition} \\
= & \exists y, y', x'', y'' \cdot \; x''=0 \wedge x'=y'' \wedge y'=y'' \\
= & \top
\end{array}$$

which is not strong enough to imply P. In order for the refinement to be a theorem, we must strengthen P in the larger space. Suppose that all added variables are unchanged. Then $P = x'=0 \wedge y'=y$ and

$$\begin{array}{ll}
 & \textbf{new } y\text{: } nat \cdot \; y := 0.\; P.\; x := y \\
= & \exists y, y' \cdot \; y := 0.\; x'=0 \wedge y'=y.\; x := y \\
 & \qquad \text{substitution law on first composition, replace last assignment} \\
= & \exists y, y' \cdot \; x'=0 \wedge y'=0.\; x'=y \wedge y'=y \qquad \text{expand remaining composition} \\
= & \exists y, y', x'', y'' \cdot \; x''=0 \wedge y''=0 \wedge x'=y'' \wedge y'=y'' \\
= & x'=0
\end{array}$$

This time the refinement is a theorem.