Exercises 4.3 (page 300)

5. Use the proof rule for assignment and logical implication as appropriate to show the validity of

   (a) $\vdash_{\mathsf{par}} (\!| x > 0 |\!)\ \mathtt{y = x + 1}\ (\!| y > 1 |\!)$

$$\dfrac{\overset{\checkmark}{\vdash x > 0 \to x + 1 > 1} \qquad \dfrac{-}{(\!| x + 1 > 1 |\!) y = x + 1 (\!| y > 1 |\!)}\ \textit{Assignment}}{(\!| x > 0 |\!) y = x + 1 (\!| y > 1 |\!)}\ \text{Implied}$$

10. Prove the validity of the sequent $\vdash_{\mathsf{par}} (\!| \top |\!)\ P\ (\!| z = \min(x, y) |\!)$, where $\min(x, y)$ is the smalest number of x and y – e.g. $\min(7, 3) = 3$ – and the code of P is given by

$$\begin{array}{l} \textbf{if } (x > y)\ \{ \\ \qquad z = y; \\ \}\ \textbf{else}\ \{ \\ \qquad z = x; \\ \} \end{array}$$

By proof tree:

$$\dfrac{\dfrac{\overset{\checkmark}{\vdash \mathit{true} \wedge x > y \to y = \mathit{min}(x, y)} \qquad \dfrac{-}{(\!| y = \mathit{min}(x, y) |\!) z = y (\!| z = \mathit{min}(x, y) |\!)}\ \text{Assignment}}{(\!| \mathit{true} \wedge x > y |\!) z = y (\!| z = \mathit{min}(x, y) |\!)}\ \text{Implied} \qquad A}{(\!| \mathit{true} |\!) \textbf{if } (x > y) \{ z = y; \}\ \textbf{else}\ \{ z = x; \} (\!| z = \mathit{min}(x, y) |\!)}\ \text{If}$$

$$\dfrac{\dfrac{\overset{\checkmark}{\vdash \mathit{true} \wedge \neg(x > 0) \to x = \mathit{min}(x, y)} \qquad \dfrac{-}{(\!| x = \mathit{min}(x, y) |\!) z = x (\!| z = \mathit{min}(x, y) |\!)}\ \text{Assignment}}{(\!| \mathit{true} \wedge \neg(x > y) |\!) z = x (\!| z = \mathit{min}(x, y) |\!)}\ \text{Implied}}{A}$$

By proof tableaux:

$$\begin{array}{ll}
(\!| \mathit{true} |\!) & \text{Precondition} \\
\textbf{if } (x > y)\ \{ & \\
\qquad (\!| \mathit{true} \wedge x > y |\!) & \text{If} \\
\qquad (\!| y = \mathit{min}(x, y) |\!) & \text{Implied } (\checkmark) \\
\qquad z = y; & \\
\qquad (\!| z = \mathit{min}(x, y) |\!) & \text{Assignment} \\
\}\ \textbf{else}\ \{ & \\
\qquad (\!| \mathit{true} \wedge \neg(x > y) |\!) & \text{If} \\
\qquad (\!| x = \mathit{min}(x, y) |\!) & \text{Implied } (\checkmark) \\
\qquad z = x; & \\
\qquad (\!| z = \mathit{min}(x, y) |\!) & \text{Assignment} \\
\} & \\
(\!| z = \mathit{min}(x, y) |\!) & \text{Postcondition}
\end{array}$$

13. Show that $\vdash_{\mathsf{par}} (\!| x \geq 0 |\!)$ `Copy1` $(\!| x = y |\!)$ is valid, where `Copy1` denotes the code

$$
\begin{array}{l}
a = x; \\
y = 0; \\
\textbf{while } (a \mathrel{!}= 0) \ \{ \\
\qquad y = y + 1; \\
\qquad a = a - 1; \\
\}
\end{array}
$$

The loop invariant is in this case $a + y = x$

Here is a proof tableaux

$$
\begin{array}{ll}
(\!| x \geq 0 |\!) & \text{Precondition} \\
(\!| x + 0 = x |\!) & \text{Implied } (\checkmark) \\
a = x; & \\
(\!| a + 0 = x |\!) & \text{Assignment} \\
y = 0; & \\
(\!| a + y = x |\!) & \text{Assignment} \\
\textbf{while } (a \mathrel{!}= 0) \ \{ & \\
\qquad (\!| a + y = x \wedge a \neq 0 |\!) & \text{Partial-while} \\
\qquad (\!| (a-1) + (y+1) = x |\!) & \text{Implied } (\checkmark) \\
\qquad y = y + 1; & \\
\qquad (\!| (a-1) + y = x |\!) & \text{Assignment} \\
\qquad a = a - 1; & \\
\qquad (\!| a + y = x \ rp & \text{Assignment} \\
\} & \\
(\!| a + y = x \wedge \neg(a \neq 0) |\!) & \text{Partial-while} \\
(\!| x = y |\!) & \text{Implied } \checkmark
\end{array}
$$

We get the following three proof obligations:

$$
\begin{array}{ll}
\vdash x \geq 0 \rightarrow x + 0 = x & \text{holds since } x + 0 = 0 \\
\vdash a + y = x \wedge a \neq 0 \rightarrow (a-1) + (y+1) = x & \text{holds since } (a-1) + (y+1) = a + y \\
\vdash a + y = x \wedge \neg(a \neq 0) \rightarrow x = y & \text{holds since } a + y = y \text{ when } a = 0
\end{array}
$$

14. Show that $\vdash_{\mathsf{par}} (\!| y \geq 0 |\!)$ `Mult1` $(\!| z = x \cdot y |\!)$ is valid, where `Mult1` is:

$$
\begin{array}{l}
a = 0; \\
z = 0; \\
\textbf{while } (a \mathrel{!}= y) \ \{ \\
\qquad z = z + x; \\
\qquad a = a + 1; \\
\}
\end{array}
$$

The proof tableaux is similar to the one in the previous solution, but with the invariant $z = a \cdot x$.