Let P be the program:

$$\textsf{while } x > 0 \textsf{ do } \{y := x * y; x := x - 1\}$$

We wish to prove that P computes n factorial ($n!$) where we start off in an initial state s such that $s(x) = n$, $n \geq 0$, and $s(y) = 1$.

More precisely, we want to prove:

$$\{x = n \wedge n \geq 0 \wedge y = 1\}\ P\ \{y = n!\}$$

We'll need an invariant for the while loop. Let I be the assertion:

$$(y * x! = n!) \wedge (x \geq 0)$$

This captures the intermediate states – for each iteration of the while loop, we still have to multiply the accumulator y by x, $x - 1$, $x - 2$, ..., 1 which is the same as $n!$. We're going to need the other condition $(x \geq 0)$ to ensure that we get out of the loop.

We want to show that I is indeed an invariant, that is:

$$\{I \wedge x > 0\}\ y := x * y; x := x - 1\ \{I\}$$

or expanding out:

$$\{y * x! = n! \wedge x \geq 0 \wedge x > 0\}\ y := x * y; x := x - 1\ \{y * x! = n! \wedge x \geq 0\}$$

From the assignment rule, working backwards, we have:

$$\{y * (x-1)! = n! \wedge (x-1) \geq 0\}\ x := x - 1\ \{y * x! = n! \wedge x \geq 0\}$$

Again by the assignment rule, we have:

$$\{x * y * (x-1)! = n! \wedge (x-1) \geq 0\}\ y := x * y\ \{y * (x-1)! = n! \wedge (x-1) \geq 0\}$$

So by sequencing, we have:

$$\{x * y * (x-1)! = n! \wedge (x-1) \geq 0\}\ y := x * y; x := x - 1\ \{y * x! = n! \wedge x \geq 0\}$$

Now:

$$\begin{aligned} I \wedge x > 0 \quad &\equiv \quad y * x! = n! \wedge x \geq 0 \wedge x > 0 \\ &\Longrightarrow \quad y * x! = n! \wedge x \geq 1 \\ &\Longrightarrow \quad x * y * (x-1)! = n! \wedge (x-1) \geq 0 \end{aligned}$$

Thus, by the rule of consequence:

$$\{I \wedge x \geq 0\}\ y := x * y; x := x - 1\ \{I\}$$

So I truly is an invariant for the loop. Now applying the rule for while loops, we get:

$$\{I\}\ P\ \{I \wedge \neg(x > 0)\}$$

Clearly, $(x = n) \wedge (n \geq 0) \wedge (y = 1) \implies I$. To see this:

$$\begin{aligned}
(x = n) &\implies x! = n! \\
(y = 1) \wedge (x = n) &\implies y * x! = n! \\
(x = n) \wedge (n \geq 0) &\implies x \geq 0
\end{aligned}$$

So, $(x = n) \wedge (n \geq 0) \wedge (y = 1) \implies (y * x! = n!) \wedge (x \geq 0)$.

In addition:

$$\begin{aligned}
I \wedge \neg(x > 0) \quad &\equiv \quad y * x! = n! \wedge x \geq 0 \wedge \neg(x > 0) \\
&\implies \quad y * x! = n! \wedge x = 0 \\
&\implies \quad y * 0! = y = n!
\end{aligned}$$

So by the rule of consequence, we have:

$$\{x = n \wedge y = 1\} \ P \ \{y = n!\}$$

Tah dah!

Homework

For Wednesday, Oct 1st. Hand in your work in class. Write neatly!

1. Prove using the Hoare rules:

$$\begin{aligned}
&\{1 \leq n\} \\
&\quad p := 0; \\
&\quad c := 1; \\
&\quad \mathsf{while}\ c \leq n\ \mathsf{do}\ (p := p + m; c := c + 1) \\
&\{p = m * n\}
\end{aligned}$$

2. Find an appropriate invariant to use in the while rule for proving the following:

$$\{i = y \wedge x = 1\}\ \mathsf{while}\ \neg(y = 0)\ \mathsf{do}\ (y := y - 1; x := 2 * x)\ \{x = 2^i\}$$