Let $P$ be the program:

\[
\text{while } x > 0 \text{ do } \{ y := x \times y; x := x - 1 \}
\]

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:

\[
\{ x = n \land n \geq 0 \land y = 1 \} \ P \ { y = n! } 
\]

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

\[
(y \times x! = n!) \land (x \geq 0)
\]

This captures the intermediate states – for each iteration of the while loop, we still have to multiply the accumulator $y$ by $x$, $x - 1$, $x - 2$, $\ldots$, 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:

\[
\{ I \land x > 0 \} \ y := x \times y; x := x - 1 \ { I } 
\]

or expanding out:

\[
\{ y \times x! = n! \land x \geq 0 \land x > 0 \} \ y := x \times y; x := x - 1 \ { y \times x! = n! \land x \geq 0 } 
\]

From the assignment rule, working backwards, we have:

\[
\{ y \times (x - 1)! = n! \land (x - 1) \geq 0 \} \ y := x \times y; x := x - 1 \ { y \times x! = n! \land x \geq 0 } 
\]

Again by the assignment rule, we have:

\[
\{ x \times y \times (x - 1)! = n! \land (x - 1) \geq 0 \} \ y := x \times y \ { y \times x! = n! \land (x - 1) \geq 0 } 
\]

So by sequencing, we have:

\[
\{ x \times y \times (x - 1)! = n! \land (x - 1) \geq 0 \} \ y := x \times y; x := x - 1 \ { y \times x! = n! \land x \geq 0 } 
\]

Now:

\[
I \land x > 0 \quad \equiv \quad y \times x! = n! \land x \geq 0 \land x > 0 \\
\implies \quad y \times x! = n! \land x \geq 1 \\
\implies \quad x \times y \times (x - 1)! = n! \land (x - 1) \geq 0 
\]

Thus, by the rule of consequence:

\[
\{ I \land x \geq 0 \} \ y := x \times y; x := x - 1 \ { I } 
\]

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

\[
\{ I \} \ P \ { I \land \neg(x > 0) } 
\]
Clearly, \((x = n) \land (n \geq 0) \land (y = 1) \implies I\). To see this:

\[
\begin{align*}
(x = n) & \implies x! = n! \\
(y = 1) \land (x = n) & \implies y \cdot x! = n! \\
(x = n) \land (n \geq 0) & \implies x \geq 0
\end{align*}
\]

So, \((x = n) \land (n \geq 0) \land (y = 1) \implies (y \cdot x! = n!) \land (x \geq 0)\).

In addition:

\[
I \land \lnot(x > 0) \equiv y \cdot x! = n! \land x \geq 0 \land \lnot(x > 0)
\]

\[
\implies y \cdot x! = n! \land x = 0
\]

\[
\implies y \cdot 0! = y = n!
\]

So by the rule of consequence, we have:

\[
\{x = n \land y = 1\} \ P \{y = n!\}
\]

Tah dah!

Homework

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

1. Prove using the Hoare rules:

\[
\begin{align*}
\{1 \leq n\} & \\
\ p := 0; & \\
\ c := 1; & \\
\ \text{while } c \leq n \text{ do } (p := p + m; c := c + 1) & \\
\ \{p = m \cdot n\}
\end{align*}
\]

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

\[
\{i = y \land x = 1\} \ \text{while } \lnot(y = 0) \text{ do } (y := y - 1; x := 2 \cdot x) \ \{x = 2^i\}
\]

2