CS536 Science of Programming - Assignment 6

Batkhishig Dulamsurankhor - A20543498

April 21, 2024

Problem 1

Postcondition $x = fac(n)$, precondition $n \geq 0$. Create a loop invariant p by replacing n by variable y in the postcondition.

If we replace n by variable y, we get $x = fac(y)$. Because we need the factorial of the first n natural numbers, we have to intialize $y = 1$ and increment it on each iteration until $y = n$.

$\{$**inv** $p \equiv x = fac(y) \wedge 1 \leq y \leq n\}\{$**bd** $n - y\}$
while $y \neq n$ **do**
 ... make y larger ...
od
$\{x = fac(y) \wedge 1 \leq y \leq n \wedge y = n\}$
$\{x = fac(n)\}$

Problem 2

Create full proof outline under the total correctness.

Let's consider precondition of the loop. From loop invariant, we know that $1 \leq y \leq n$, so that it is logical to start the loop with $y = 1$. x must also be $x = 1$. If one of them starts with 0, then the value of x will never be other than 0.

$\{x = 1 \wedge n \geq 1 \wedge y = 1\}$
$\{$**inv** $p \equiv x = fac(y) \wedge 1 \leq y \leq n\}\{$**bd** $n - y\}$
while $y \neq n$ **do**
 ... make y larger ...
od
$\{x = fac(y) \wedge 1 \leq y \leq n \wedge y = n\}$
$\{x = fac(n)\}$

Loop body.

$\{x = 1 \wedge n \geq 1 \wedge y = 1\}$
$\{$**inv** $p \equiv x = fac(y) \wedge 1 \leq y \leq n\}\{$**bd** $n - y\}$
while $y \neq n$ **do**
 $x := x * (y + 1); y := y + 1;$
od
$\{x = fac(y) \wedge 1 \leq y \leq n \wedge y = n\}$
$\{x = fac(n)\}$

Problem 3

True or False.

a. True. We aim for stronger postcondition.

b. False. Although the statement is the definition of a loop invariant, it doesn't imply a good loop invariant. p can be $p \equiv T$ but it is not a good one.

c. False. There is no algorithm to find bound expressions.

d.

e.

Problem 4

Full proof outline with forward assignment.

First, inner array substitution:
$(b[i])[k/b[j]] \equiv \textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}$

Then, outer array substitution:
$(b[b[i]])[k/b[j]]$

$$\begin{aligned}
&\equiv \textbf{if } ((\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}) = j) \textbf{ then } k \textbf{ else } b[\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}] \textbf{ fi}\\
&\mapsto \textbf{if } (\textbf{if } (i = j) \textbf{ then } k = j \textbf{ else } b[i] = j \textbf{ fi}) \textbf{ then } k \textbf{ else } b[\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}] \textbf{ fi}\\
&\mapsto \textbf{if } (i = j \wedge k = j) \vee (i \neq j \wedge b[i] = j) \textbf{ then } k \textbf{ else } b[\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}] \textbf{ fi}\\
&\mapsto \textbf{if } (i = j \wedge k = j) \vee (i \neq j \wedge b[i] = j) \textbf{ then } k \textbf{ else } (\textbf{if } (i = j) \textbf{ then } b[k] \textbf{ else } b[b[i]] \textbf{ fi}) \textbf{ fi}\\
&\mapsto \textbf{if } (i = j \wedge k = j) \vee (i \neq j \wedge b[i] = j) \textbf{ then } k \textbf{ else if } (i = j) \textbf{ then } b[k] \textbf{ else } b[b[i]] \textbf{ fi}
\end{aligned}$$

Problem 5

Find an optimized precondition p and create full proof outline: $\{p\}b[i] := x; b[j] := y\{b[i] \leq b[j]\}$.

$wp(b[i] := x; b[j] := y, b[i] \leq b[j])$

$$\begin{aligned}
&\equiv wp(b[i] := x, wp(b[j] := y, b[i] \leq b[j]))\\
&\equiv wp(b[i] := x, (b[i] \leq b[j])[y/b[j]])\\
&\equiv wp(b[i] := x, (b[i])[y/b[j]] \leq (b[j])[y/b[j]])\\
&\equiv wp(b[i] := x, (\textbf{if } (i = j) \textbf{ then } y \textbf{ else } b[i] \textbf{ fi}) \leq (\textbf{if } (j = j) \textbf{ then } y \textbf{ else } b[j] \textbf{ fi}))\\
&\mapsto wp(b[i] := x, (\textbf{if } (i = j) \textbf{ then } y \textbf{ else } b[i] \textbf{ fi}) \leq y)\\
&\mapsto wp(b[i] := x, \textbf{if } (i = j) \textbf{ then } y \leq y \textbf{ else } b[i] \leq y \textbf{ fi})\\
&\mapsto wp(b[i] := x, \textbf{if } (i = j) \textbf{ then } T \textbf{ else } b[i] \leq y \textbf{ fi})\\
&\mapsto wp(b[i] := x, (i = j) \vee (b[i] \leq y))\\
&\equiv (i = j \vee (b[i] \leq y))[x/b[i]]\\
&\equiv i = j \vee (b[i])[x/b[i]] \leq y\\
&\equiv i = j \vee (\textbf{if } (i = i) \textbf{ then } x \textbf{ else } b[i] \leq y \textbf{ fi}) \leq y\\
&\mapsto i = j \vee x \leq y
\end{aligned}$$

A valid triple: $\{i = j \vee x \leq y\}b[i] := x; b[j] := y\{b[i] \leq b[j]\}$.

$\{i = j \vee x \leq y\}b[i] := x; b[j] := y\{b[i] \leq b[j]\}$

$$\begin{aligned}
&\equiv \{i = j \vee x \leq y\}b[i] := x\{b[i] \leq y\}b[j] := y\{b[i] \leq b[j]\} && \text{// backward assignment}\\
&\equiv \{i = j \vee x \leq y\}\{x \leq y\}b[i] := x\{b[i] \leq y\}b[j] := y\{b[i] \leq b[j]\} && \text{// backward assignment}
\end{aligned}$$