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

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.

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

Loop body:

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

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. True. Since $\neg B$ can imply $e_1 = e_2$, we always have e_1.

e. True. Since $(B \wedge T) \vee (\neg B \wedge B_2) \equiv B \vee (\neg B \wedge B_2) \equiv (B \vee \neg B) \wedge (B \vee B_2) \equiv B \vee B_2$.

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:
$(b[b[i]])[k/b[j]]$

$\equiv \textbf{if } ((\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}) = j) \textbf{ then } k \textbf{ else } b[\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}] \textbf{ fi}$

$\mapsto \textbf{if } (\textbf{if } (i = j) \textbf{ then } k = j \textbf{ else } b[i] = j \textbf{ fi}) \textbf{ then } k \textbf{ else } b[\textbf{if } (i = j) \textbf{ then } k \textbf{ else } b[i] \textbf{ fi}] \textbf{ fi}$

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

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

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

Problem 5

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

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

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

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

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

$\equiv wp(b[i] := x, (\textbf{if } (i = j) \textbf{ then } y \textbf{ else } b[i] \textbf{ fi}) \leq (\textbf{if } (j = j) \textbf{ then } y \textbf{ else } b[j] \textbf{ fi}))$

$\mapsto wp(b[i] := x, (\textbf{if } (i = j) \textbf{ then } y \textbf{ else } b[i] \textbf{ fi}) \leq y)$

$\mapsto wp(b[i] := x, \textbf{if } (i = j) \textbf{ then } y \leq y \textbf{ else } b[i] \leq y \textbf{ fi})$

$\mapsto wp(b[i] := x, \textbf{if } (i = j) \textbf{ then } T \textbf{ else } b[i] \leq y \textbf{ fi})$

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

$\equiv (i = j \vee (b[i] \leq y))[x/b[i]]$

$\equiv i = j \vee (b[i])[x/b[i]] \leq y$

$\equiv i = j \vee (\textbf{if } (i = i) \textbf{ then } x \textbf{ else } b[i] \leq y \textbf{ fi}) \leq y$

$\mapsto i = j \vee x \leq y$

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

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

$\equiv \{i = j \vee x \leq y\}b[i] := x\{b[i] \leq y\}b[j] := y\{b[i] \leq b[j]\}$ // backward assignment

$\equiv \{i = j \vee x \leq y\}\{x \leq y\}b[i] := x\{b[i] \leq y\}b[j] := y\{b[i] \leq b[j]\}$ // backward assignment

Problem 6

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

$$
\begin{aligned}
& wp(b[i] := b[j]; b[j] := b[k], b[i] > b[k]) \\
&\qquad \equiv wp(b[i] := b[j], wp(b[j] := b[k], b[i] > b[k])) \\
&\qquad \equiv wp(b[i] := b[j], (b[i] > b[k])[b[k]/b[j]]) \\
&\qquad \equiv wp(b[i] := b[j], (b[i])[b[k]/b[j]] > b[k][b[k]/b[j]]) \\
&\qquad \equiv wp(b[i] := b[j], (\textbf{if } (i = j) \textbf{ then } b[k] \textbf{ else } b[i] \textbf{ fi}) > (\textbf{if } (k = j) \textbf{ then } b[k] \textbf{ else } b[k] \textbf{ fi})) \\
&\qquad \mapsto wp(b[i] := b[j], (\textbf{if } (i = j) \textbf{ then } b[k] \textbf{ else } b[i] \textbf{ fi}) > b[k]) \\
&\qquad \mapsto wp(b[i] := b[j], \textbf{if } (i = j) \textbf{ then } b[k] > b[k] \textbf{ else } b[i] > b[k] \textbf{ fi}) \\
&\qquad \mapsto wp(b[i] := b[j], \textbf{if } (i = j) \textbf{ then } F \textbf{ else } b[i] > b[k] \textbf{ fi}) \\
&\qquad \mapsto wp(b[i] := b[j], i \neq j \wedge b[i] > b[k]) \\
&\qquad \equiv (i \neq j \wedge b[i] > b[k])[b[j]/b[i]] \\
&\qquad \equiv i \neq j \wedge (b[i])[b[j]/b[i]] > (b[k])[b[j]/b[i]] \\
&\qquad \equiv i \neq j \wedge (\textbf{if } (i = i) \textbf{ then } b[j] \textbf{ else } b[i] \textbf{ fi}) > (\textbf{if } (k = i) \textbf{ then } b[j] \textbf{ else } b[k] \textbf{ fi}) \\
&\qquad \mapsto i \neq j \wedge b[j] > (\textbf{if } (k = i) \textbf{ then } b[j] \textbf{ else } b[k] \textbf{ fi}) \\
&\qquad \mapsto i \neq j \wedge (\textbf{if } (k = i) \textbf{ then } b[j] > b[j] \textbf{ else } b[j] > b[k] \textbf{ fi}) \\
&\qquad \mapsto i \neq j \wedge (\textbf{if } (k = i) \textbf{ then } F \textbf{ else } b[j] > b[k] \textbf{ fi}) \\
&\qquad \mapsto i \neq j \wedge k \neq i \wedge b[j] > b[k]
\end{aligned}
$$

A valid triple: $\{i \neq j \wedge k \neq i \wedge b[j] > b[k]\}b[i] := b[j]; b[j] := b[k]\{b[i] > b[k]\}$.

$\{i \neq j \wedge k \neq i \wedge b[j] > b[k]\}b[i] := b[j]; b[j] := b[k]\{b[i] > b[k]\}$

$\equiv \{i \neq j \wedge k \neq i \wedge b[j] > b[k]\}b[i] := b[j]\{b[i] > b[k]\}b[j] := b[k]\{b[i] > b[k]\}$ // backward assignment

$\equiv \{i \neq j \wedge k \neq i \wedge b[j] > b[k]\}\{b[j] > b[k]\}b[i] := b[j]\{b[i] > b[k]\}b[j] := b[k]\{b[i] > b[k]\}$ // backward assignment

Problem 7

$S \equiv [x := 1 \parallel x := -1]; y := y + x.$

$$
\begin{tikzcd}
& \langle [x := 1 \parallel x := -1]; y := y + x, \sigma \rangle \arrow[dl] \arrow[dr] & \\
\langle [E \parallel x := -1]; y := y + x, \sigma[x \mapsto 1] \rangle \arrow[d] & & \langle [x := 1 \parallel E]; y := y + x, \sigma[x \mapsto -1] \rangle \arrow[d] \\
\langle [E \parallel E]; y := y + x, \sigma[x \mapsto -1] \rangle \arrow[d] & & \langle [E \parallel E]; y := y + x, \sigma[x \mapsto 1] \rangle \arrow[d] \\
\langle [E \parallel E]; E, \sigma[x \mapsto -1][y \mapsto y - 1] \rangle & & \langle [E \parallel E]; E, \sigma[x \mapsto 1][y \mapsto y + 1] \rangle
\end{tikzcd}
$$

$M(S, \sigma) = \{\{x = -1, y = y - 1\}, \{x = 1, y = y + 1\}\}$

Problem 8

$$
\begin{tikzcd}[column sep=tiny]
 & \langle \textbf{while } x < n \textbf{ do } [x \coloneqq x+1 \parallel y \coloneqq y*2] \textbf{ od}, \{x=0, y=1, n=2\}\rangle \arrow[d] & \\
 & \langle [x \coloneqq x+1 \parallel y \coloneqq y*2]; W, \{x=0, y=1, n=2\}\rangle \arrow[dl] \arrow[dr] & \\
\langle [E \parallel y \coloneqq y*2]; W, \{x=1, y=1, n=2\}\rangle \arrow[dr] & & \langle [x \coloneqq x+1 \parallel E]; W, \{x=0, y=2, n=2\}\rangle \arrow[dl] \\
 & \langle [E \parallel E]; W, \{x=1, y=2, n=2\}\rangle \arrow[d] & \\
 & \langle \textbf{while } x < n \textbf{ do } [x \coloneqq x+1 \parallel y \coloneqq y*2] \textbf{ od}, \{x=1, y=2, n=2\}\rangle \arrow[dl] \arrow[dr] & \\
\langle [E \parallel y \coloneqq y*2]; W, \{x=2, y=2, n=2\}\rangle \arrow[dr] & & \langle [x \coloneqq x+1 \parallel E]; W, \{x=1, y=4, n=2\}\rangle \arrow[dl] \\
 & \langle [E \parallel E]; W, \{x=2, y=4, n=2\}\rangle \arrow[d] & \\
 & \langle W, \{x=2, y=4, n=2\}\rangle \arrow[d] & \\
 & \langle E, \{x=2, y=4, n=2\}\rangle &
\end{tikzcd}
$$

$M(W, \sigma) = \{\{x=2, y=4, n=2\}\}$