Girish Rajani (A20503736)
CS 536: Science of Programming
Homework 5: Loop Invariants and Proof Outlines

1. Minimal and Full Proof Outlines

Task 1.1 (Written, 10 points)

$\{x \geq 0\}$
$i := 0;$
$\{\text{inv } i \leq x \wedge x = i!\}$
while $i < x$ do
  $x := x * i;$
  $i := i + 1$
od
$\{\exists k. x = k!\}$

- Apply rule 9: Add conditions to a loop based on the invariant

$\{x \geq 0\}$
$i := 0;$
$\{\text{inv } i \leq x \wedge x = i!\}$
while $i < x$ do $\{i \leq x \wedge x = i! \wedge i < x\}$
  $x := x * i;$
  $i := i + 1$ $\{i \leq x \wedge x = i!\}$
od $\{i \leq x \wedge x = i! \wedge i \geq x\}$
$\{\exists k. x = k!\}$

We have a proof obligation:
$\{i \leq x \wedge x = i! \wedge i \geq x\} \Rightarrow \{\exists k. x = k!\}$
Since $i \leq x$ and $i \geq x$, we have $x = i$.
$\{x = i \wedge x = i!\} \Rightarrow \{\exists k. x = k!\}$
When $k = i$, this obligation holds because then $x = i! \Rightarrow x = k!$

- Step 1 (two applications): Use wlp to propagate the postcondition of the loop body backwards.

$$\{x \geq 0\}$$

$i := 0;$

$\{inv\ i \leq x \wedge x = i!\}$

while $i < x$ do $\quad \{i \leq x \wedge x = i! \wedge i < x\}$ $\{i+1 \leq x * i \wedge x * i = i+1!\}$

$\quad x := x * i;$ $\quad \{i+1 \leq x \wedge x = i+1!\}$

$\quad i := i + 1$ $\quad \{i \leq x \wedge x = i!\}$

od $\quad \{i \leq x \wedge x = i! \wedge i \geq x\}$

$$\Rightarrow \{\exists k.\ x = k!\}$$

We have a proof obligation:

$$\{i \leq x \wedge x = i! \wedge i < x\} \Rightarrow \{i+1 \leq x * i \wedge x * i = i+1!\}$$

$$i < x \Rightarrow i+1 \leq x \Rightarrow i+1 \leq x * i$$

$$x = i! \not\Rightarrow x * i = i+1!$$

To get $i+1!$, we need $(i+1) * i!$. Since $x = i!$, we instead need $(i+1) * x$ to prove this obligation, but instead, our proof gave $x * i = i+1!$. Hence, it is not provable. This probably means our loop invariant is incorrect.

Perform step 1 again:

$$\{x \geq 0\} \quad \{0 \leq x \wedge x = 0!\}$$

$i := \bar{0};$ $\quad \{i \leq x \wedge x = i!\}$

$\{\text{inv } i \leq x \wedge x = i!\}$

while $i < x$ do $\quad \{i \leq x \wedge x = i! \wedge i < x\} \not\Rightarrow \{i+1 \leq x * i \wedge x * i = i+1!\}$

$\quad x := x * i;$ $\quad \{i+1 \leq x \wedge x = i+1!\}$

$\quad i := i + \bar{1}$ $\quad \{i \leq x \wedge x = i!\}$

od $\quad \{i \leq x \wedge x = i! \wedge i \geq x\}$

$\Rightarrow \{\exists k . x = k!\}$

We have another proof obligation:

$$\{x \geq 0\} \Rightarrow \{0 \leq x \wedge x = 0!\}$$

$$\check{x} = 1$$

Using simplify rule, we can say that:

$$\{x \geq 0\} \Rightarrow \{0 \leq x\}$$

Final completed proof outline:

$\{x \geq 0\}$

$\Rightarrow \{0 \leq x \wedge x = 0!\}$

$i := \bar{0};$ $\quad \{i \leq x \wedge x = i!\}$

$\{\text{inv } i \leq x \wedge x = i!\}$

while $i < x$ do $\quad \{i \leq x \wedge x = i! \wedge i < x\} \not\Rightarrow \{i+1 \leq x * i \wedge x * i = i+1!\}$

$\quad x := x * i;$ $\quad \{i+1 \leq x \wedge x = i+1!\}$

$\quad i := i + \bar{1}$ $\quad \{i \leq x \wedge x = i!\}$

od $\quad \{i \leq x \wedge x = i! \wedge i \geq x\}$

$\Rightarrow \{\exists k . x = k!\}$

Task 1·2 (Written, 12 points)

$\{x \geq 0\}$

$i := \bar{0};$

$r := \bar{1};$

$\{\text{inv } i \leq x \wedge r = i!\}$

while $i < x$ do

$i := i + \bar{1};$

$r := r * i$

od

$\{r = x!\}$

- Apply rule 9: Add conditions to a loop based on the invariant

$\{x \geq 0\}$

$i := \bar{0};$

$r := \bar{1};$

$\{\text{inv } i \leq x \wedge r = i!\}$ $\{i \leq x \wedge r = i! \wedge i < x\}$

while $i < x$ do

$i := i + \bar{1};$ $\{i \leq x \wedge r = i!\}$

$r := r * i$ $\{i \leq x \wedge r = i! \wedge i \geq x\}$

od $\{r = x!\}$

We have a proof obligation:

$\{i \leq x \wedge r = i! \wedge i \geq x\} \Rightarrow \{r = x!\}$

Since $i \leq x \wedge i \geq x$;

$i = x$ so $r = i! \Rightarrow r = x!$

- Step 1 (two applications): Use wlp to propagate the postcondition of the loop body backwards.

$\{x \geq 0\}$

$i := 0;$
$r := 1;$
$\{inv\ i \leq x \wedge r = i!\}$
while $i < x$ do — $\{i \leq x \wedge r = i! \wedge i < x\}$ $\{i+1 \leq x \wedge r * i+1 = i+1!\}$
$i := i+1;$ — $\{i \leq x \wedge r * i = i!\}$
$r := r * i$ — $\{i \leq x \wedge r = i!\}$
od — $\{i \leq x \wedge r = i! \wedge i \geq x\}$

$\Rightarrow \{r = x!\}$

We have a proof obligation:

$\{i \leq x \wedge r = i! \wedge i < x\} \Rightarrow \{i+1 \leq x \wedge r * i+1 = i+1!\}$

$i < x \Rightarrow i+1 \leq x$

Based on factorial rule: $i+1! = i+1 * i!$

since $r = i!$ then $r = i! \Rightarrow i! * i+1 \Rightarrow r * i+1 = i+1!$ hence proven

- Step 1:

$\{x \geq 0\}$ $\{0 \leq x \wedge 1 = 0!\}$

$i := 0;$ — $\{i \leq x \wedge 1 = i!\}$
$r := 1;$ — $\{i \leq x \wedge r = i!\}$
$\{inv\ i \leq x \wedge r = i!\}$
while $i < x$ do — $\{i \leq x \wedge r = i! \wedge i < x\} \Rightarrow \{i+1 \leq x \wedge r * i+1 = i+1!\}$
$i := i+1;$ — $\{i \leq x \wedge r * i = i!\}$
$r := r * i;$ — $\{i \leq x \wedge r = i!\}$
od — $\{i \leq x \wedge r = i! \wedge i \geq x\}$

$\Rightarrow \{r = x!\}$

We have a proof obligation:

$\{x \geq 0\} \Rightarrow \{0 \leq x \wedge 1 = 0!\}$ $\rightarrow T$

$\{x \geq 0\} = \{0 \leq x\}$

Final completed proof outline:

$\{x \geq 0\}$

$\Rightarrow \{0 \leq x \wedge 1 = 0!\}$

$i := 0;$ $\{i \leq x \wedge 1 = i!\}$

$r := 1;$ $\{i \leq x \wedge r = i!\}$

$\{inv\ i \leq x \wedge r = i!\}$

while $i < x$ do $\{i \leq x \wedge r = i! \wedge i < x\} \Rightarrow \{i+1 \leq x \wedge r * i+1 = i+1!\}$

$i := i+1;$ $\{i \leq x \wedge r * i = i!\}$

$r := r * i$ $\{i \leq x \wedge r = i!\}$

od $\{i \leq x \wedge r = i! \wedge i \geq x\}$

$\Rightarrow \{r = x!\}$

Task 3.1

16 hours