1. Loop Bounds and Proof Outlines

Task 1.1 (Written, 16 points)

Girish Rajan
A20503736
CS 536: Science of Prog
Homework 6

$\{gas_0 = gas \wedge gas > 0 \wedge batt = 0\}$
$\Rightarrow \{0 \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$
$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$

miles := 0;

$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$
{dec ???}
while (gas > 1 ∨ batt > 0) do

$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0 \wedge gas > 1 \vee batt > 0\}$

if batt > 0 then

$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0 \wedge gas > 1 \vee batt > 0 \wedge batt > 0\}$
$\Rightarrow \{miles + 1 \geq gas_0 - (gas + batt - 1) \wedge gas \geq 0 \wedge batt - 1 \geq 0\}$

batt := batt - 1

$\{miles + 1 \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$

else

$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0 \wedge gas > 1 \vee batt > 0 \wedge batt \leq 0\}$
$\Rightarrow \{miles + 1 \geq gas_0 - (gas - 2 + batt + 1) \wedge gas - 2 \geq 0 \wedge batt + 1 \geq 0\}$

gas := gas - 2;

$\{miles + 1 \geq gas_0 - (gas + batt + 1) \wedge gas \geq 0 \wedge batt + 1 \geq 0\}$

batt := batt + 1;

$\{miles + 1 \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$

fi

$\{miles + 1 \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$

miles := miles + 1;

$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$

od

$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0 \wedge gas \leq 1 \wedge batt \leq 0\}$
$\Rightarrow \{miles \geq gas_0 - 1\}$

Expand partial correctness proof outline into proof outline for total correctness using the loop bound:

$\{gas_0 = gas \wedge gas > 0 \wedge batt = 0\}$
$\Rightarrow \{0 \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$
$\{miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$

miles := 0;

$\{inv\ P \triangleq miles \geq gas_0 - (gas + batt) \wedge gas \geq 0 \wedge batt \geq 0\}$
{dec gas + batt}
while (gas > 1 ∨ batt > 0) do

$\{P \wedge gas > 1 \vee batt > 0 \wedge gas + batt = t_0\}$

if batt > 0 then

$\{P \wedge gas > 1 \vee batt > 0 \wedge batt > 0 \wedge gas + batt = t_0\}$
$\Rightarrow \{P \wedge gas + batt - 1 < t_0\}$

batt := batt - 1

$\{P \wedge gas + batt < t_0\}$

else

$\{P \wedge gas \geq 1 \vee batt > 0 \wedge batt \leq 0 \wedge gas + batt = t_0\}$
$\Rightarrow \{P \wedge gas - 2 + batt + 1 < t_0\}$

gas := gas - 2;

$\{P \wedge gas + batt + 1 < t_0\}$

batt := batt + 1

$\{P \wedge gas + batt < t_0\}$

fi

$\{P \wedge gas + batt < t_0\}$

miles := miles + 1;

$\{P \wedge gas + batt < t_0\}$

od

$\{P \wedge gas \leq 1 \wedge batt \leq 0\}$
$\Rightarrow \{miles \geq gas_0 - 1\}$

Task 1.2 (Written, 12 points)

$$[\forall_i \in \mathbb{Z}.(0 \leq i < |a|) \to a[i] \geq 0]$$

```
i := 0;
{inv  i ≤ |a| ∧ i ≥ 0 ∧ ∀k ∈ ℤ. (k ≥ 0 ∧ k < i) → a[k] = 0 }
{dec  |a| - i }
while i < size(a) do
    {inv  i ≥ 0 ∧ i < |a| ∧ a[i] ≥ 0 }
    {dec  a[i] }
    while  a[i] > 0  do
        a[i] := a[i] - 1
    od;
    i := i + 1
od
```

$$[\forall_i \in \mathbb{Z}.(0 \leq i < |a|) \to a[i] = 0]$$

Task 1.2 Explanations

1st bound expression {dec |a| - i};

1. Why $P \Rightarrow t \geq 0$

$i \leq |a| \wedge i \geq 0 \wedge \forall_k \in \mathbb{Z}(k \geq 0 \wedge k < i) \rightarrow a[k] = 0 \Rightarrow |a| - i \geq 0$

i can either be less than or equal to |a| and i can either be greater than or equal to 0.

~~when~~ In three out of four cases when i is less than |a|, equal to 0 or greater than 0, then $|a| - i > 0$ and when i is equal to |a|, then $|a| - i = 0$. This satisfies the above implication and ensures the bound expression is always non-negative.

2. $|a| - i$ decreases at each loop iteration because we see that we have a variable i that increases in the loop body so we subtract it from t but that doesn't work since its negative. So, we add |a| which helps because $i \leq |a|$. This ensures we can't have less than zero iterations left and the loop bound decreases after each iteration.

2nd bound expression {dec a[i]}:

1. Why $P \Rightarrow t \geq 0$

$i \geq 0 \wedge i < |a| \wedge a[i] \geq 0 \Rightarrow a[i] \geq 0$

The first 2 conditions just ensures no errors in array such as index out of bounds so technically, we have $a[i] \geq 0 \Rightarrow a[i] \geq 0$. This ensures that the program terminates.

2. Here our bound expression is a[i] which is a variable that decreases in the loop body. Therefore, by adding this to t, we ensure that the bound expression decreases each loop iteration.

Task 1-3 (Written, 12 points)

a) $\sqrt{t}$ - False (not a valid bound expression)
The $\sqrt{t}$ may give a non integer number which is not allowed and also if t is a perfect square, $\sqrt{t}$ can also be negative which violates the bound expression property.

b) t^2 - True (valid bound expression)
Since t^2 is just an increased t, it will still hold the same properties of t such that $t^2 \geq 0$ and t^2 decreases after each iteration of the loop.

c) $t + i$ - False (not a valid bound expression)
Assuming that i is in the loop body, we should only add i to t if i decreases in the loop body. If i increases in the loop body and we add it to t then, if $i > t$, the bound expression will increase as we do more iterations hence violating the second property.

d) $t + i^2$ - False (not a valid bound expression)
Same reason as above, assuming that i^2 is in the loop body, we should only add i^2 to t if i^2 decreases in the loop body. If $i^2 > t$ and i^2 increases in the loop body by adding i^2 to t, it will cause the bound expression to increase hence violating the second property (number of iterations must decrease as we do more iterations)

e) t + k - Not True (not a valid bound expression)
If k is sufficiently negative then this can cause the loop bound to be < 0 but we can't have less than 0 iterations left so this property is violated.

f) $t + k^2$ - True (valid bound expression)

We can always add a constant to a bound expression and it will still result in a valid bound expression.

2. Weakest Preconditions with Array Assignments

Task 2.1 (Written, 30 points)

a) $wlp(a[\text{if } x = \bar{0} \text{ then } i \text{ else } j] := 1, a[i] = 1)$

$= [\,'/a[\text{if } x = \bar{0} \text{ then } i \text{ else } j]\,]\; a[i] = 1$

$= (\text{if } i = (\text{if } x = \bar{0} \text{ then } i \text{ else } j) \text{ then } 1 \text{ else } a[i]) = 1$

$= \text{if } i = (\text{if } x = \bar{0} \text{ then } i \text{ else } j) \text{ then } 1 = 1 \text{ else } a[i] = 1$

Simplify:

$= \text{if } i = (\text{if } x = \bar{0} \text{ then } i \text{ else } j) \text{ then } T \text{ else } a[i] = 1$

$\Leftrightarrow \quad i = (\text{if } x = \bar{0} \text{ then } i \text{ else } j) \;\vee\; a[i] = 1$

$\Leftrightarrow (\text{if } x = \bar{0} \text{ then } i = i \text{ else } i = j) \vee a[i] = 1$

$= (\text{if } x = \bar{0} \text{ then } T \text{ else } i = j) \vee a[i] = 1$

$\Leftrightarrow (x = 0 \vee i = j) \vee a[i] = 1$

b) $wlp(a[i] := \bar{5},\ a[a[1]] = 5)$

$= [\bar{5}/a[i]]\ (a[a[1]] = 5)$

$= [\bar{5}/a[i]]\ a[a[1]] = [\bar{5}/a[i]]\ 5$

$= [\bar{5}/a[i]]\ a[a[1]] = 5$

$= (\text{if } (\text{if } 1 = i \text{ then } 5 \text{ else } a[1]) = i \text{ then } 5 \text{ else } a[\text{if } 1 = i \text{ then } 5 \text{ else } a[1]]) = 5$

$= \text{if } (\text{if } 1 = i \text{ then } 5 \text{ else } a[1]) = i \text{ then } 5 = 5 \text{ else } a[\text{if } 1 = i \text{ then } 5 \text{ else } a[1]] = 5$

$= \text{if } (\text{if } 1 = i \text{ then } 5 \text{ else } a[1]) = i \text{ then } T \text{ else } a[\text{if } 1 = i \text{ then } 5 \text{ else } a[1]] = 5$

Simplify:

$\Leftrightarrow (\text{if } 1 = i \text{ then } 5 \text{ else } a[1]) = i \ \vee\ a[\text{if } 1 = i \text{ then } 5 \text{ else } a[1]] = 5$

$= (\text{if } 1 = i \text{ then } 5 = i \text{ else } a[1] = i) \vee a[\text{if } 1 = i \text{ then } 5 \text{ else } a[1]] = 5$

$\Leftrightarrow ((1 = i \wedge 5 = i) \vee (1 \neq i \wedge a[1] = i)) \vee a[\text{if } 1 = i \text{ then } 5 \text{ else } a[1]] = 5$

$\Rightarrow ((1 = i \wedge 5 = i) \vee (1 \neq i \wedge a[1] = i)) \vee (\text{if } 1 = i \text{ then } a[5] \text{ else } a[a[1]]) = 5$

$= ((1 = i \wedge 5 = i) \vee (1 \neq i \wedge a[1] = i)) \vee \text{if } 1 = i \text{ then } a[5] = 5 \text{ else } a[a[1]] = 5$

$\Leftarrow ((1 = i \wedge 5 = i) \vee (1 \neq i \wedge a[1] = i)) \vee (1 = i \wedge a[5] = 5) \vee (1 \neq i \wedge a[a[1]] = 5)$

$= (F \vee (1 \neq i \wedge a[1] = i)) \vee (1 = i \wedge a[5] = 5) \vee (1 \neq i \wedge a[a[1]] = 5)$

ID $\Rightarrow$ $(1 \neq i \wedge a[1] = i) \vee (1 = i \wedge a[5] = 5) \vee (1 \neq i \wedge a[a[1]] = 5)$

Dist $\Leftrightarrow$ $((a[1] = i \vee a[a[1]] = 5) \wedge 1 \neq i) \vee (1 = i \wedge a[5] = 5)$

c) $wlp(a[j] := a[i] + 1, a[j] > a[i])$

$= [a[i]+1 / a[j]]\,(a[j] > a[i])$

$= [a[i]+1 / a[j]]\; a[j] > [a[i]+1 / a[j]]\; a[i]$

$= (\text{if } j=j \text{ then } a[i]+1 \text{ else } a[j]) > (\text{if } i=j \text{ then } a[i]+1 \text{ else } a[i])$

$\equiv\!>\; a[i]+1 > \text{if } i=j \text{ then } a[i]+1 \text{ else } a[i]$

$\Leftrightarrow\; \text{if } i=j \text{ then } a[i]+1 > a[i]+1 \text{ else } a[i]+1 > a[i]$

$\Leftrightarrow\; \text{if } i=j \text{ then } F \text{ else } a[i]+1 > a[i]$

$\Leftrightarrow\; i \neq j \wedge a[i]+1 > a[i]$

d) $wlp(i := 5; a[i] := a[i+1], a[i] > 0)$

$= wlp(i := 5, wlp(a[i] := a[i+1], a[i] > 0))$

$wlp(a[i] := a[i+1], a[i] > 0)$

$= [a[i+1]/a[i]]\ a[i] > 0 = [a[i+1]/a[i]]\ a[i] > [a[i+1]/a[i]]\ 0$

$= [a[i+1]/a[i]]\ a[i] > 0$

$= (\text{if } i = i \text{ then } a[i+1] \text{ else } a[i]) > 0$

$= a[i+1] > 0$

$wlp(i := 5, a[i+1] > 0)$

$= [5/i]\ a[i+1] > 0$

$= a[5+1] > 0$

$= a[6] > 0$

e) $wp(i := 5;\ a[i] := a[i+1],\ a[i] > 0)$

$= wlp(i := 5;\ a[i] := a[i+1],\ a[i] > 0) \wedge D(i := 5;\ a[i] = a[i+1])$

$= a[b] > 0 \wedge D(i := 5) \wedge wlp(i := 5,\ D(a[i] := a[i+1]))$

$D(a[e_1] := e_2) = D(e_1) \wedge D(e_2) \wedge 0 \le e_1 < |a|$

$D(a[i] := a[i+1])$

$= D(i) \wedge D(a[i+1]) \wedge 0 \le i < |a|$

$= T \wedge D(i+1) \wedge 0 \le i+1 < |a| \wedge 0 \le i < |a|$

$= T \wedge D(i) + D(1) \wedge 0 \le i+1 < |a| \wedge 0 \le i < |a|$

$= T \wedge T \wedge T \wedge 0 \le i+1 < |a| \wedge 0 \le i < |a|$

$= 0 \le i+1 < |a| \wedge 0 \le i < |a|$

$a[b] > 0 \wedge T \wedge wlp(i := 5,\ 0 \le i+1 < |a| \wedge 0 \le i < |a|)$

$= a[b] > 0 \wedge [5/i]\ 0 \le i+1 < |a| \wedge 0 \le i < |a|$

$= a[b] > 0 \wedge 0 \le 5+1 < |a| \wedge 0 \le 5 < |a|$

$= a[b] > 0 \wedge 0 \le b < |a| \wedge 0 \le 5 < |a|$

f) $wlp(\text{if } i=j \text{ then } j:=j+1 \text{ else } a[j]:=a[i]+1 \text{ fi}, a[j] > a[i])$

$= (i=j \to wlp(j:=j+1, a[j] > a[i])) \wedge (i \neq j \to wlp(a[j]:=a[i]+1, a[j] > a[i]))$

* $wlp(j:=j+1, a[j] > a[i])$

$= [j+1/j]\, a[j] > a[i] = [j+1/j]\, a[j] > [j+1/j]\, a[i]$

$= a[j+1] > a[i]$

* $wlp(a[j]:=a[i]+1, a[j] > a[i])$

$= [a[i]+1 / a[j]]\, a[j] > a[i] = [a[i]+1/a[j]]\, a[j] > [a[i]+1/a[j]]\, a[i]$

$= (\text{if } j=j \text{ then } a[i]+1 \text{ else } a[j]) > (\text{if } i=j \text{ then } a[i]+1 \text{ else } a[i])$

$= (\text{if } T \text{ then } a[i]+1 \text{ else } a[j]) > (\text{if } i=j \text{ then } a[i]+1 \text{ else } a[i])$

$\equiv$ $a[i]+1 > (\text{if } i=j \text{ then } a[i]+1 \text{ else } a[i])$

$\Leftrightarrow$ $\text{if } i=j \text{ then } a[i]+1 > a[i]+1 \text{ else } a[i]+1 > a[i]$

$\Leftrightarrow$ $\text{if } i=j \text{ then } F \text{ else } a[i]+1 > a[i]$

$\Leftrightarrow$ $i \neq j \wedge a[i]+1 > a[i]$

$(i=j \to a[j+1] > a[i]) \wedge (i \neq j \to i \neq j \wedge a[i]+1 > a[i])$

DC $\Leftrightarrow$ $(i \neq j \vee a[j+1] > a[i]) \wedge (i=j \vee i \neq j \wedge a[i]+1 > a[i])$

LEM $\Leftrightarrow$ $(i \neq j \vee a[j+1] > a[i]) \wedge (T \wedge a[i]+1 > a[i])$

ID $\Rightarrow$ $(i \neq j \vee a[j+1] > a[i]) \wedge (a[i]+1 > a[i])$

3 One more wrap-up question

20 hrs