Ramya Krishnan

A20506653

1. Loop Bounds and proof outlines

Task 1.1

$\{gas_0 = gas \wedge gas > 0 \wedge batt = 0\}$

miles := $\bar{0}$;

$\{inv\ P \triangleq gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0\}$

$\{gas_0 = gas \wedge gas > 0 \wedge batt = 0 \wedge miles = 0\}$ → $\{P\}$ → 1

$\{dec\ gas + batt\}$

while (gas > 1 ∨ batt > 0) do

$\{P \wedge gas + batt = m_0 \wedge (gas > 1 \vee batt > 0)\}$

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

$\{\exists miles_0 [miles_0 / miles] P \wedge gas + batt = m_0 \wedge (gas > 1 \vee batt > 0) \wedge miles = [miles_0 / miles] miles + 1\}$ → 2

if batt > 0 then

$\Rightarrow \{P \wedge batt > 0\ gas + batt = m_0\}$ → 3

batt := batt − $\bar{1}$

$\Rightarrow \{[batt - 1 / batt] P \wedge gas + batt + \dots < m_0\}$

$\{P \wedge gas + batt < m_0\}$

else

$\{P \wedge batt \leq 0\ \wedge\ gas + batt = m_0\}$ → 4

gas := gas − $\bar{2}$;

$\Rightarrow \{[gas - 2 / gas][batt + 1 / batt] P \wedge gas - 2 + batt + 1 < m_0\}$

batt := batt + $\bar{1}$

$\{[batt + 1 / batt] P \wedge gas + batt < m_0\}$

$\{P \wedge gas + batt < m_0\}$

fi

od

$\{P \wedge (gas \leq 1 \wedge batt \leq 0)\}$ → 5

$\Rightarrow [miles \geq gas_0 - 1]$

1. $\{gas_0 = gas \wedge gas > 0 \wedge batt = 0 \wedge miles = 0\} \Rightarrow$ (Is provable)

$\Rightarrow \{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0\}$

lets substitute $batt = 0$ & $miles = 0$, $gas_0 = gas$

$gas_0 + 0 + 0 = gas_0 \wedge gas \geq 0 \wedge 0 \geq 0$

$gas_0 = gas_0 \wedge gas \geq 0$

$gas \geq 0$ since $gas > 0 \Rightarrow gas \geq 0$

with this, we can prove the above statement.

2. $\{\exists miles_0 \, [miles_0 / miles] \, P \wedge gas + batt = m_0 \wedge (gas > 1 \vee batt > 0) \wedge miles = [miles_0 / miles] \, miles + 1\} \Rightarrow$

$gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge batt > 0 \wedge gas + batt = m_0 \Rightarrow$ (Is provable)

lets substitute $batt = 1$ & $gas = 0$

$\exists miles_0 \; 1 + miles_0 = gas_0 \wedge 0 \geq 0 \wedge 1 \geq 0 \wedge 0 + 1 = m_0 \wedge (0 > 1 \vee 1 > 0) \wedge miles = miles_0 + 1 \Rightarrow 0 + 1 + miles = gas_0 \wedge 0 \geq 0 \wedge 1 > 0 \wedge 0 + 1 = m_0$

$\exists miles_0 \; 1 + miles_0 = gas_0 \wedge 1 = m_0 \wedge (F \vee T) \wedge miles = miles_0 + 1 \Rightarrow 1 + miles = gas_0 \wedge 1 = m_0$

$\exists miles_0 \; 1 + miles_0 = gas_0 \wedge 1 = m_0 \wedge miles = miles_0 + 1 \Rightarrow 1 + miles = gas_0 \wedge 1 = m_0$

with this, we can prove the above statement.

3. $\{gas + batt + miles = gas_0 \wedge gas \geq 0 \; batt \geq 0 \wedge batt > 0 \wedge$
$gas + batt = m_0\} \Rightarrow \{[batt - 1 \mid batt] \; gas + batt +$
$miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge gas + batt - 1 < m_0\}$
(Is provable)

$\{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge batt > 0$
$\wedge \; gas + batt = m_0\} \Rightarrow \{gas + batt - 1 + miles = gas_0 \wedge$
$gas \geq 0 \wedge batt - 1 \geq 0 \wedge gas + batt - 1 < m_0\}$

$\{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt > 0 \wedge gas + batt =$
$m_0\} \Rightarrow \{gas + batt + miles = gas_0 + 1 \wedge gas \geq 0 \wedge$
$batt \geq 1 \wedge gas + batt - 1 < m_0\}$

lets substitute $gas = 0$ & $batt = 1$

$\{1 + miles = gas_0 \wedge 0 \geq 0 \wedge 1 > 0 \wedge 0 + 1 = m_0\} \Rightarrow$
$\{1 + miles = gas_0 + 1 \wedge 0 \geq 0 \wedge 1 \geq 1 \wedge 0 + 1 - 1 < m_0\}$

$\{1 + miles = gas_0 \wedge 1 = m_0\} \Rightarrow \{1 + miles = gas_0 + 1 \wedge$
$0 < m_0\}$

with this, we can prove the above statement.

4. $\{P \wedge batt \leq 0 \wedge gas + batt = m_0\} \Rightarrow \{[gas - 2/gas][batt + 1/batt]$
$P \wedge gas - 2 + batt + 1 < m_0\} \Rightarrow$ (Provable)

$\{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge batt \leq 0 \wedge$
$gas + batt = m_0\} \Rightarrow \{[gas - 2/gas][batt + 1/batt]$
$gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge gas + batt$
$+ 1 < m_0\}$

$\{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge batt \leq 0$
$\wedge\ gas + batt = m_0\} \Rightarrow \{gas - 2 + batt + 1 + miles =$
$gas_0 \wedge gas - 2 \geq 0 \wedge batt + 1 \geq 0 \wedge gas - 2 + batt + 1 < m_0\}$

$\{gas + miles = gas_0 \wedge gas \geq 0 \wedge gas = m_0\} \Rightarrow \{gas + batt - 1$
$+ miles = gas_0 \wedge gas - 2 \geq 0 \wedge batt + 1 \geq 0 \wedge gas +$
$batt - 1 < m_0\}$

$\{m_0 + miles = gas_0 \wedge m_0 \geq 0\} = \{gas + batt - 1 + miles =$
$gas_0 \wedge gas - 2 \geq 0 \wedge batt + 1 \geq 0 \wedge gas + batt - 1 < m_0\}$

lets substitute $gas = m_0$ and $batt = 0$

$\{m_0 - 1 + miles = gas_0 \wedge m_0 - 2 \geq 0 \wedge m_0 - 1 < m_0\}$

~~$m_0 - 1 < m_0$~~

now, $m_0 - 1 < m_0$

now, $\{m_0 + miles = gas_0 \wedge m_0 \geq 0\} \Rightarrow \{m_0 + miles = gas_0 +$
$1 \wedge m_0 \geq 2\}$

With this, we can prove the above statement

5. $\{P \wedge gas \leq 1 \wedge batt \leq 0\} \Rightarrow [miles \geq gas_0 - 1] \Rightarrow$ (Is provable)

$\{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \wedge$
$gas \leq 1 \wedge batt \leq 0\} \Rightarrow [miles \geq gas_0 - 1]$

$\{gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt = 0 \wedge$
$gas \leq 1\} \Rightarrow [miles \geq gas_0 - 1]$

$\{gas + miles = gas_0 \wedge gas \geq 0 \wedge gas \leq 1\} \Rightarrow [miles \geq gas_0 - 1]$

Since gas $\leq$ o we have 2 options gas = 0 & gas = 1

lets sub, gas = 0

$\{miles = gas_0\} \Rightarrow [miles \geq gas_0 - 1]$

$gas_0 \geq gas_0 - 1$

lets sub, gas = 1

$\{1 + miles = gas_0\} \Rightarrow [miles \geq gas_0 - 1]$

$\{miles = gas_0 - 1\} \Rightarrow [miles \geq gas_0 - 1]$

With this, we can prove the above statement.

6. $P \rightarrow gas + batt \geq 0$ $\Rightarrow$ (Is provable)

$gas + batt + miles = gas_0 \wedge gas \geq 0 \wedge batt \geq 0 \rightarrow$

$gas + batt \geq 0$

By proving all the execution, we have proved the program termination and total Correctness.

Task 1.2

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

$i := 0;$

$\{inv\ \forall_j \in \mathbb{Z}. (0 \leq j < i) \rightarrow a[j] = 0 \wedge \forall_k \in \mathbb{Z}. (i \leq k < |a|) \rightarrow a[k] \geq 0\}$

$\{dec\ |a| - i\}$

while $i < size(a)$ do

$\{inv\ \forall_i \in Z.(0 \le i < |a|) \to a[i] \ge 0\}$

$\{dec\ a[i]\}$

while $a[i] > 0$ do

$a[i] := a[i] - 1$

od ;

$i := i + 1$

od

$[\forall_i \in Z.(0 \le i < |a|) \to a[i] = 0]$

For outer loop Bound $\{dec\ |a| - i\}$

1. Non_negative

From the loop variant we can see, $\forall_j \in Z\ (0 \le j < i)$ which implies i is non-negative. And $\forall_k \in Z.\ (i \le k < |a|)$ implies i is less than $|a|$.

Hence the outer loop bound is always non-negative.

2. From the program, we know size of a is constant and $i := i + 1$. Therefore the ~~difference~~ $|a| - i$ is decrosing at every iteration.

For inner loop Bound { dec 'a[i] }

1. Non - negative

From the loop invariant we can see $a[i] \geq 0$ which implies a[i] is non-negative.
Hence the inner loop bound is always non-negative.

2. From the program, we know a[i] is decreased by 1 at every iteration until a[i] is equal to 0.
Therefore the expression ~~dec a~~ {dec a[i]} is decreasing at every iteration.

Task 1.3

Here t is Variable, k is Constant and t is valid bound expression.

a. $\sqrt{t}$ → Not Valid

Even though t is a valid bound expression, $\sqrt{t}$ not necessarily be decreasing. example, for integers 5 & 4 the $\sqrt{t}$ is 2. So even when value changed it didn't always decreasing. Hence it is not valid.

b. $t^2 \rightarrow$ It is valid.

t^2 is always non-negative and decreasing depending on the value/integer. Hence it is a valid.

c. $t + i \rightarrow$ Not Valid

As per given assumption i is a variable, so it can be negative. So there is a possibility that $t+i < 0$.

Hence it is not Valid.

d. $t + i^2 \rightarrow$ Not Valid

Since i is variable, depending on i the expression $t + i^2$ may not be decreasing, always but rather increasing. For example, $t = 1$ & $i = 2$ then $1+4 = 5$ and in next iteration if we assume $t = 2$ & $i = 3$ then $2 + 9 = 11$ which is increasing.

Hence it is invalid

e. $t + k \rightarrow$ Not Valid

with the assumption, it is clear that k can be negative and $t + k < 0$. Hence it is invalid.

f. $t + K^2 \rightarrow$ Valid.

From the assumption K is constant and K^2 will be positive. So when we add positive constant and t (valid bound) the expression is Valid.

2. Weakest Precondition with Array Assignments.

Task 2.1

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

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

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

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

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

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

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

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

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

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

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

b) $wlp\left(a[i] := 5,\ a[a[1]] = 5\right)$

$= \left[5/a[i]\right]\left(a[a[1]] = 5\right)$

$= \left[5/a[i]\right] a[a[1]] = \left[5/a[i]\right] 5$

$= \left(\text{if } e_2 = i \text{ then } 5 \text{ else } a[e_2]\right) = 5$ $\quad \ni e_2 = \left[5/a[i]\right](a[1])$

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

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

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

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

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

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

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

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

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

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

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

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

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

$= \text{if } i=j \text{ then } F \text{ else } T$

$= \neg(i=j) \wedge T$

$= i \neq j$

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

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

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

$$= wlp\left(i:=5, \left[{}^{a[i+1]}/_{a[i]}\right](a[i]) > \left[{}^{a[i+1]}/_{a[i]}\right](0)\right)$$

$$= wlp(i:=5, (\text{if } i=i \text{ then } a[i+1] \text{ else } a[i]) > 0))$$

$$= wlp(i:=5, (\text{if } T \text{ then } a[i+1] \text{ else } a[i]) > 0)$$

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

$$= \left[{}^{5}/_{i}\right](a[i+1] > 0)$$

$$= \left[{}^{5}/_{i}\right](a[i+1]) > \left[{}^{5}/_{i}\right](0)$$

$$= a[5+1] > 0$$

$$= a[6] > 0$$

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

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

From above we know the result of wlp, $a[6] > 0$.

lets Calculate D,

$D(i := 5 ;\ a[i] := a[i+1])$

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

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

$= T \wedge T \wedge wlp(i := 5,\ D(i) \wedge 0 \leq i < |a| \wedge$

$D(i+1) \wedge 0 \leq (i+1) < |a|$

$= wlp(i := 5,\ T \wedge 0 \leq i < |a| \wedge D(i) \wedge D(1) \wedge$

$0 \leq (i+1) < |a|$

$= wlp(i := 5,\ T \wedge 0 \leq i < |a| \wedge T \wedge T \wedge 0 \leq (i+1) < |a|$

$= wlp(i := 5,\ 0 \leq i < |a| \wedge 0 \leq (i+1) < |a|)$

$= [5/i](0 \leq i < |a| \wedge 0 \leq (i+1) < |a|)$

$= 0 \leq 5 < |a| \wedge 0 \leq 6 < |a|$

Combining both we get,

$= 0 \leq 5 < |a| \wedge 0 \leq 6 < |a| \wedge a[6] > 0$

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

$a[j] > a[i])$

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

$(\neg(i=j) \rightarrow wlp(a[j]:=a[i]+1, a[j] > a[i]))$

lets Calculate ~~then~~ first part,

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

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

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

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

lets Calculate second part;

$(\neg(i=j) \rightarrow wlp(a[j]:=a[i]+1, a[j] > a[i]))$

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

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

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

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

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

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

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

$$= \neg(i=j) \rightarrow (\neg(i=j) \wedge T)$$

$$= \neg(i=j) \rightarrow \neg(i=j)$$

$$= T$$

Combining both,

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

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

$$= i=j \rightarrow (a[j+1] > a[i]) \wedge T$$

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

9.

It took me 7-8 hours to finish this.