CS 142 Homework Set # 2

Timur Kuzhagaliyev
UID: 2079376

① $\{x \geq 2\}$ $x := x - y + 3$ $\{x + y \geq 0\}$

$\equiv$ {assignment axiom}

$x \geqslant 2 \Rightarrow x - y + y + 3 \geqslant 0$

$\equiv \{-y + y = 0\}$

$x \geqslant 2 \Rightarrow x + 3 \geqslant 0$

$\equiv \{x + 3 \geqslant 0 \Rightarrow x \geqslant -3\}$

$x \geqslant 2 \Rightarrow x \geqslant -3$

$\equiv \{2 > -3\}$

true Q.E.D.

② Constants:

a) {False} next {Q}

$\equiv$ {definition of next}

$(\forall a :: \{false\}\ a\ \{Q\})$

$\equiv$ {definition of a Hoare triple}

$(\forall a :: false \Rightarrow Q_a)$

$\equiv$ {definition of $\Rightarrow$}

$(\forall a :: true)$

$\equiv$ {definition of $\forall$}

true

2 b) Similar to a):

$\{P\}$ next true

$\equiv$ {def. of next, Hoare triple}

$(\forall a :: P \Rightarrow true)$

$\equiv$ {def. of $\Rightarrow$, $\forall$}

true

c) Similar to a), b):

true next false

$\equiv$ {Def. of next, Hoare triple}

$(\forall a :: true \Rightarrow false)$

$\equiv$ {Def. of $\Rightarrow$, $\forall$}

false

Junctivity

a) $(P_1 \text{ next } Q_1) \wedge (P_2 \text{ next } Q_2)$

$\equiv$ {def. of next twice}

$(\forall a :: \{P_1\}\, a\, \{Q_1\}) \wedge (\forall a :: \{P_2\}\, a\, \{Q_2\})$

$\equiv$ {def. of $\forall$, associativity and commutativity of $\wedge$}

$(\forall a :: (\{P_1\}\, a\, \{Q_1\}) \wedge (\{P_2\}\, a\, \{Q_2\}))$

$\Rightarrow$ {conjunction rule}

$(\forall a :: \{P_1 \wedge P_2\}\, a\, \{Q_1 \wedge Q_2\})$

$\equiv$ {def. of next}

$\{P_1 \wedge P_2\}$ next $(Q_1 \wedge Q_2)$ Q.E.D

② cont. b) Similar to a):

$(P_1 \text{ next } Q_1) \wedge (P_2 \text{ next } Q_2)$

$\equiv$ { def of next twice, def of $\forall$, $\wedge$ }

$(\forall a :: (\{P_1\}\ a\ \{Q_1\}) \wedge (\{P_2\}\ a\ \{Q_2\}))$

$\Rightarrow$ { disjunction rule }

$(\forall a :: \{P_1 \vee P_2\}\ a\ \{Q_1 \vee Q_2\})$

$\equiv$ { def. of next }

$(P_1 \vee P_2) \text{ next } (Q_1 \vee Q_2)$ Q.E.D.

Weakening:

a) $(P \text{ next } Q) \wedge [Q \Rightarrow Q']$

$\equiv$ { def. of next }

$(\forall a :: \{P\}\ a\ \{Q\}) \wedge [Q \Rightarrow Q']$

$\equiv$ { def. of $\forall$, $\wedge$ }

$(\forall a :: (\{P\}\ a\ \{Q\}) \wedge [Q \Rightarrow Q'])$

$\equiv$ { def. of Hoare triple, $\Rightarrow$ }

$(\forall a :: (\neg P \vee Q_a) \wedge [Q \Rightarrow Q'])$

$\equiv$ { distribution law }

$(\forall a :: (\neg P \wedge [Q \Rightarrow Q']) \vee (Q_a \wedge [Q \Rightarrow Q']))$

$\Rightarrow$ { prediate calculus, modus ponens }

$(\forall a :: \neg P \vee Q'_a)$

$\equiv$ { def of $\Rightarrow$, Hoare triple, next }

$P \text{ next } Q'$ Q.E.D.

③ a) $\text{stable}(P) \wedge \text{stable}(Q)$

$\equiv$ { def. of stable and next twice }

$(\forall a :: \{P\}\, a\, \{P\}) \wedge (\forall a :: \{Q\}\, a\, \{Q\})$

$\equiv$ { def of $\forall$ twice, def of $\wedge$, def of $\forall$ in reverse }

$(\forall a :: (\{P\}\, a\, \{P\}) \wedge (\{Q\}\, a\, \{Q\}))$

$\Rightarrow$ { conjunction rule }

$(\forall a :: \{P \wedge Q\}\, a\, \{P \wedge Q\})$

$\equiv$ { def. of next, stable }

$\text{stable}(P \wedge Q)$ Q.E.D

b) Similar to a):

$\text{stable}(P) \wedge \text{stable}(Q)$

$\equiv$ { see above }

$(\forall a :: (\{P\}\, a\, \{P\}) \wedge (\{Q\}\, a\, \{Q\}))$

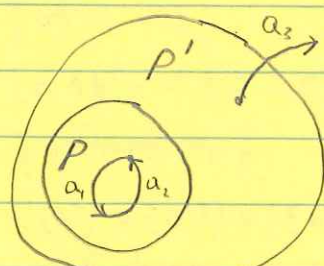
$\Rightarrow$ { disjunction rule }

$(\forall a :: \{P \vee Q\}\, a\, \{P \vee Q\}$

$\equiv$ { def of next, stable }

$\text{stable}(P \vee Q)$ Q.E.D

c) False, consider the following example:



Clearly P is stable and $P \Rightarrow P'$, but a_3 would take us out of P' so P' is not stable.

④ Notation: p' is the new value of p after application of the current action.

a) Recall that: $$V = \frac{\sum_{i=0}^{N-1}(x_i - A)^2}{N-1} = \frac{(x_0 - A)^2 + (x_1 - A)^2 + \sum_{i=2}^{N-1}(x_i - A)^2}{N-1}$$

where $$A = \frac{\sum_{i=0}^{N-1} x_i}{N} = \frac{x_0 + x_1 + \sum_{i=2}^{N-1} x_i}{N}$$

Note that in both cases the order of summation doesn't matter, so x_0 and x_1 could represent any 2 distinct x_j's.

Let $x_0' = x_1' = \frac{x_0 + x_1}{2}$, then $$A' = \frac{x_0' + x_1' + \sum_{i=2}^{N-1} x_i}{N}$$

$$= \frac{2\left(\frac{x_0 + x_1}{2}\right) + \sum_{i=2}^{N-1} x_i}{N}$$

$$= \frac{x_0 + x_1 + \sum_{i=2}^{N-1} x_i}{N}$$

$$= A \quad (I)$$

$\therefore A' = A$, i.e. average is unchanged after application of our iteration action.

Formally:

$$\{A = K\}\ x_i, x_j := \left(\frac{(x_i + x_j)}{2}, \frac{(x_i + x_j)}{2}\right) \{A' = K\}$$

*Note: K is arbitrary, <u>not</u> related to K in the next part.

$\equiv$ {Def of A, assignment axiom}

$$\frac{x_i + x_j + \sum_{p=2}^{N-1} x_p}{N} = K \Rightarrow \frac{2\left(\frac{x_i + x_j}{2}\right) + \sum_{p=2}^{N-1} x_p}{N} = K$$

$\equiv$ {Using result (I)}

$A = K \Rightarrow A = K$

$\equiv$ {Def. of $\Rightarrow$}

true

follows

stable $\{A = K\}$

$\equiv$ {def. of stable, next}

$(\forall a :: \{A = K\}\ a\ \{A = K\})$

$\equiv$ {proof earlier, def of $\forall$}

true

④ a) cont.

Note that $(x_j - A)^2 = x_j^2 - 2Ax_j + A^2$

Hence $(x_0 - A)^2 + (x_1 - A)^2 = x_0^2 - 2Ax_0 + A^2 + x_1^2 - 2Ax_1 + A^2$

$$= (x_0^2 + x_1^2) - 2A(x_0 + x_1) + 2A^2$$

Set $x_0' = x_1' = \frac{x_0 + x_1}{2}$

Then $(x_0' - A)^2 + (x_1' - A)^2 = 2\left(\frac{x_1 + x_0}{2}\right)^2 - 2A\left(2\left(\frac{x_0 + x_1}{2}\right)\right) + 2A^2$

$$= \frac{(x_0 + x_1)^2}{2} - 2A(x_0 + x_1) + 2A^2$$

Hence $V - V' = \underbrace{(x_0^2 + x_1^2)}_{a} - \underbrace{\frac{(x_0 + x_1)^2}{2}}_{b}$

Note that both a and b are increasing functions but a grows faster than b, hence $(x_0^2 + x_1^2) \geq \frac{(x_0 + x_1)^2}{2}$ with equality iff. $x_0 = x_1$

$\therefore$ $V' \leq V$, i.e. variance never increases. (II)

Formally:

$\text{stable}(V \leq K)$

$\equiv$ {Def of stable, next}

$(\forall a :: \{V \leq K\}\ a\ \{V \leq K\})$

$\equiv$ {Def. of program}

$\{V \leq K\}\ x_i, x_j := \frac{(x_i + x_j)}{2}, \frac{(x_i + x_j)}{2}\ \{V \leq K\}$

$\equiv$ {Assignment axiom, def of V and V'}

$V \leq K \Rightarrow V' \leq K$

$\equiv$ {$V' \leq V$ by result (II), predicate calculus}

true

④ b)

$$\{x_i \neq x_j \wedge V=K\}\ x_i, x_j := \frac{(x_i + x_j)}{2}, \frac{(x_i + x_j)}{2}\ \{V<K\}$$

$\equiv$ {assignment axiom, definition of V'}

$x_i \neq x_j \wedge V=K \Rightarrow V' < K$

$\equiv$ {Result Ⅱ, predicate calculus}

true

⑤ a)

Notation: To make the notation easier to read I will define $\ell : \mathbb{R}_{\geq}\times N \times N \longrightarrow \mathbb{B}$

s.t. $\ell(\underset{\text{any } \mathbb{R}}{\underline{D[j,k]}}, j, k) = \begin{cases} \text{true} & \text{if } \exists \text{ path from } j \text{ to } k \text{ of length } D[j,k] \\ \text{false} & \text{otherwise} \end{cases}$

Additionally, let:

$$E \equiv (\forall j,k :: D[j,k] \leq W[j,k])$$

$$L \equiv (\forall j,k :: \ell(D[j,k], j, k))$$

Need to prove: invariant $(E \wedge L)$

initially $(E \wedge L)$:

$D = W$

$\Rightarrow$ {$D[j,k] = W[j,k]$ and $\ell(W[j,k], j, k)$ holds by definition of W}

$E \wedge L$

⑤ a) cont.

stable (E)

$\equiv$ {def. of stable and next}

$(\forall a :: \{E\}\ a\ \{E\})$

$\equiv$ {def. of program}

$\{E\}\ D[i,k] > D[i,j] + D[j,k] \longrightarrow D[i,k] := D[i,j] + D[j,k]\ \{E\}$

$\equiv$ {assignment axiom}

$\left(E \wedge (D[i,k] > D[i,j] + D[j,k]) \Rightarrow E^{D[i,k]}_{D[i,j]+D[j,k]}\right) \wedge \left(E \wedge \neg(D[i,k] > D[i,j] + D[j,k]) \Rightarrow E\right)$

$\Leftarrow$ {Antecedent strengthening of $\Rightarrow$}

$\left(E \wedge (D[i,k] > D[i,j] + D[j,k]) \Rightarrow E^{D[i,k]}_{D[i,j]+D[j,k]}\right) \wedge (E \Rightarrow E)$

$\equiv$ {Def of $\Rightarrow$ and $\wedge$}

$E \wedge (D[i,k] > D[i,j] + D[j,k]) \Rightarrow E^{D[i,k]}_{D[i,j]+D[j,k]}$

$\equiv$ {Old value of $D[i,k]$ was $\leq W[i,k]$, and new value is smaller than old one so by predicate calculus E holds with new value}

true

stable (L)

$\Leftarrow$ {Follow steps from stable (E) proof replacing E with L}

$L \wedge (D[i,k] > D[i,j] + D[j,k]) \Rightarrow L^{D[i,k]}_{D[i,j]+D[j,k]}$

$\equiv$ {Since $\ell(D[i,j], i, j)$ and $\ell(D[j,k], j, k)$ hold, and $i \to j$ ends where $j \to k$ starts, $\ell(D[i,j] + D[j,k], i, k)$ must also hold, hence implication holds}

true

By result in ③ a), $stable(E) \wedge stable(L) \Rightarrow Stable(E \wedge L)$

$\therefore$ Invariant $(E \wedge L)$ Q.E.D

⑤ 6) The program will be in a fixed point when for all actions either the guard is deactivated or assignment doesn't change the state.

From def. of our program we can conclude that for any i, j, k if $D[i,k] \leq D[i,j] + D[j,k]$ holds we'll be in a fixed point.

Let $F \equiv \left(D[i,k] \leq D[i,j] + D[j,k] \right)$

$$
\begin{aligned}
& \text{stable}\,(F) \\
\equiv \quad & \{\text{Def. of stable, next}\} \\
& \left(\forall a :: \{F\}\ a\ \{F\} \right) \\
\equiv \quad & \{\text{Def. of program, def of } F\} \\
& \{F\}\ \neg F \longrightarrow D[i,k] := D[i,j] + D[j,k]\ \{F\} \\
\equiv \quad & \{\text{Assignment axiom}\} \\
& \left(F \wedge \neg F \Rightarrow F^{D[i,k]}_{D[i,j]+D[j,k]} \right) \wedge \left(F \wedge F \Rightarrow F \right) \\
\equiv \quad & \{\text{Def. of } \wedge \text{ twice}\} \\
& \left(\textit{false} \Rightarrow F^{D[i,k]}_{D[i,j]+D[j,k]} \right) \wedge \left(F \Rightarrow F \right) \\
\equiv \quad & \{\text{Def. of } \Rightarrow \text{ and } \wedge) \\
& \text{true}
\end{aligned}
$$