Assignment 2: Verification

Maxwell Bo 43926871

April 12, 2017

1 Part A

Given

$$\begin{aligned} pre &\triangleq D.len \geqslant max(\{A.len,\ B.len,\ C.len\}) \\ &\quad \wedge\ sorted(A)\ \wedge\ sorted(B)\ \wedge\ sorted(C) \end{aligned}$$

and

$$\begin{aligned} post &\triangleq D = A \cap B \cap C \\ &\triangleq D_{[0,D.len)} = A_{[0,A.len)} \cap B_{[0,B.len)} \cap C_{[0,C.len)} \end{aligned}$$

$i, j, k, r, D : [pre, post]$

$\sqsubseteq$ {Composition: middle predicate is inv}

$i, j, k, r, D : [pre, inv];\ i, j, k, r, D : [inv, post]$

where

$$\begin{aligned} inv &\triangleq D_{[0,r)} = A_{[0,i)} \cap B_{[0,j)} \cap C_{[0,k)} \\ &\quad \wedge\ r \in [0, D.len]\ \wedge\ i \in [0, A.len]\ \wedge\ j \in [0, B.len]\ \wedge\ k \in [0, C.len] \end{aligned}$$

$\sqsubseteq$ {Assignment: $pre \Rrightarrow inv[i, j, k, r \backslash 0, 0, 0, 0]$}

$i, j, k, r := 0, 0, 0, 0;\ i, j, k, r, D : [inv, post]$

$\because$

$$\begin{aligned} inv[i, j, k, r \backslash 0, 0, 0, 0] &\equiv D_{[0,0)} = A_{[0,0)} \cap B_{[0,0)} \cap C_{[0,0)} \\ &\quad \wedge\ 0 \in [0, D.len]\ \wedge\ 0 \in [0, A.len]\ \wedge\ 0 \in [0, B.len]\ \wedge\ 0 \in [0, C.len] \\ &\equiv \varnothing = (\varnothing \cap \varnothing \cap \varnothing)\ \wedge\ (\text{true}\ \wedge\ \text{true}\ \wedge\ \text{true}\ \wedge\ \text{true}) \\ &\equiv \varnothing = \varnothing\ \wedge\ \text{true} \\ &\equiv \text{true} \end{aligned}$$

$\sqsubseteq$ {Strengthen post: $inv \wedge \neg(i \neq A.len\ \vee\ j \neq B.len\ \vee\ k \neq C.len) \Rrightarrow post$}

$i, j, k, r := 0, 0, 0, 0;\ i, j, k, r, D : [inv, inv \wedge \neg(i \neq A.len\ \vee\ j \neq B.len\ \vee\ k \neq C.len)]$

$\because$

$$\begin{array}{lcl} inv \wedge \neg(i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len) \Rrightarrow post & \equiv & inv \wedge (i = A.len \ \wedge \ j = B.len \ \wedge k = C.len) \Rrightarrow post \\ & \equiv & TODO \end{array}$$

$((a \wedge b) \Rrightarrow (a \wedge c)) \equiv (b \Rrightarrow c)$

$\sqsubseteq$ {Repetition}

$i, j, k, r := 0, 0, 0, 0;$
do $(i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len) \rightarrow$
$\quad i, j, k, r, D : [inv \ \wedge \ (i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len), \ inv \ \wedge \ (0 \leqslant V < V_0)]$
od

where

$$\begin{array}{rcl} V & \triangleq & (A.len - i) + (B.len - j) + (C.len - k) \\ & \triangleq & (A.len + B.len + C.len) - (i + j + k) \end{array}$$

$\sqsubseteq$ {Selection: $inv \ \wedge \ (i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len) \Rrightarrow (G_1 \vee G_2 \vee G_3 \vee G_4)$}

$i, j, k, r := 0, 0, 0, 0;$
do $(i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len) \rightarrow$
$\quad TODO$
od

where

$$\begin{array}{rcl} G_1 & \triangleq & A_i > B_j \\ G_2 & \triangleq & B_j > C_k \\ G_3 & \triangleq & C_k > A_i \\ G_4 & \triangleq & (A_i = B_j) \wedge (B_j = C_k) \end{array}$$