Assignment 2: Verification

Maxwell Bo 43926871

April 12, 2017

1 Part A

Given

$$pre \triangleq D.len \geqslant max(\{A.len,\ B.len,\ C.len\}) \\ \wedge\ sorted(A)\ \wedge\ sorted(B)\ \wedge\ sorted(C)$$

and

$$post \triangleq D_{[0,r)} = A \cap B \cap C$$

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

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

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

where

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

$\sqsubseteq$ {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: $inv \wedge \neg guard \Rrightarrow post$}

$i, j, k, r := 0, 0, 0, 0;\ i, j, k, r, D : [inv, inv \wedge \neg guard]$

$\because$

$$guard \quad \triangleq \quad (i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len)$$

$$inv \wedge \neg guard \quad \equiv \quad inv \wedge (i = A.len \ \wedge \ j = B.len \ \wedge k = C.len)$$

Assuming $(i = A.len \ \wedge \ j = B.len \ \wedge k = C.len)$ holds, we can show that still

$$inv \wedge (i = A.len \ \wedge \ j = B.len \ \wedge k = C.len) \ \Rrightarrow \ post$$

$\because$

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

$$\begin{array}{lcl} (D_{[0,r)} = A \cap B \cap C) \ \wedge \ (r \in [0, D.len]) & \Rrightarrow & post \\ & \Rrightarrow & D_{[0,r)} = A \cap B \cap C \end{array}$$

$\sqsubseteq$ {Repetition}

$i, j, k, r := 0, 0, 0, 0;$
do $(i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len) \rightarrow$
$\quad i, j, k, r, D : [inv \ \wedge \ guard, \ inv \ \wedge \ (0 \leqslant V < V_0)]$
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: $inv \ \wedge \ guard \Rrightarrow (G_1(i,j) \vee G_2(j,k) \vee G_3(k,i) \vee G_4(i,j,k))$}

$i, j, k, r := 0, 0, 0, 0;$
do $(i \neq A.len \ \vee \ j \neq B.len \ \vee \ k \neq C.len) \rightarrow$
$\quad$ **if** $(A_i > B_j) \rightarrow i, j, k, r, D : [(A_i > B_j) \wedge inv \wedge guard, \ inv \wedge (0 \leqslant V < V_0)]$
$\quad [\!] \ (B_j > C_k) \rightarrow i, j, k, r, D : [(B_j > C_k) \wedge inv \wedge guard, \ inv \wedge (0 \leqslant V < V_0)]$
$\quad [\!] \ C_k > A_i \rightarrow i, j, k, r, D : [C_k > A_i \wedge inv \wedge guard, \ inv \wedge (0 \leqslant V < V_0)]$
$\quad$ **fi** $(A_i = B_j) \wedge (B_j = C_k) \rightarrow i, j, k, r, D : [(A_i = B_j) \wedge (B_j = C_k) \wedge inv \wedge guard, \ inv \wedge (0 \leqslant V < V_0)]$
od

where

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

and $\because$

$G_1(i,j) \vee G_2(j,k) \vee G_3(k,i) \vee G_4(i,j,k)$
$\equiv$ {Expansion of the guard definitions}
$(A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee ((A_i = B_j) \wedge (B_j = C_k))$
$\equiv$ {Transitivity}
$(A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee (A_i = B_j = C_k)$