Assignment 2: Verification

Maxwell Bo 43926871

April 12, 2017

1 Part A

Given

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

and

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

$$\begin{aligned} & i, j, k, r, D : [pre, post] \\ \sqsubseteq\ & \{\text{Composition: middle predicate is } inv\} \\ & i, j, k, r, D : [pre, inv];\ i, j, k, r, D : [inv, post] \end{aligned}$$

where

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

$$\begin{aligned} \sqsubseteq\ & \{\text{Assignment: } pre \Rrightarrow inv[i, j, k, r \backslash 0, 0, 0, 0]\} \\ & i, j, k, r := 0, 0, 0, 0;\ i, j, k, r, D : [inv, post] \end{aligned}$$

$\because$

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

$$\begin{aligned} \sqsubseteq\ & \{\text{Strengthen post: } inv \wedge \neg(i \neq A.len\ \vee\ j \neq B.len\ \vee\ k \neq C.len) \Rrightarrow post\} \\ & i, j, k, r := 0, 0, 0, 0;\ i, j, k, r, D : [inv, inv \wedge \neg(i \neq A.len\ \vee\ j \neq B.len\ \vee\ k \neq C.len)] \end{aligned}$$

$\because$

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

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

$\sqsubseteq$ {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

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

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

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

where

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

$$
\begin{aligned}
& (A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee ((A_i = B_j) \wedge (B_j = C_k)) \\
\equiv \quad & \{\text{Transitivity}\} \\
& (A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee (A_i = B_j = C_k) \\
\equiv \quad & \{\text{TODO}\} \\
& \neg\neg((A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee (A_i = B_j = C_k)) \\
\equiv \quad & \{\text{TODO}\} \\
& \neg((A_i \leqslant B_j) \wedge (B_j \leqslant C_k) \wedge (C_k \leqslant A_i) \wedge (A_i \neq B_j \neq C_k)) \\
\equiv \quad & \{\text{TODO}\} \\
& \neg((A_i = B_j = C_k) \wedge (A_i \neq B_j \neq C_k)) \\
\equiv \quad & \{\text{TODO}\} \\
& (A_i \neq B_j \neq C_k) \vee (A_i = B_j = C_k)
\end{aligned}
$$

This predicate holds true for arbritary A, B and C, iff