Assignment 2: Verification

Maxwell Bo   43926871

April 12, 2017

1 Part A

Given

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

and

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

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

where

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

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

$\because$

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

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

$\because$

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

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

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

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

$\sqsubseteq$ {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

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

$\sqsubseteq$ {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

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

$(A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee ((A_i = B_j) \wedge (B_j = C_k))$
$\equiv$ {Transitivity}
$(A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee (A_i = B_j = C_k)$
$\equiv$ {TODO}
$\neg\neg((A_i > B_j) \vee (B_j > C_k) \vee (C_k > A_i) \vee (A_i = B_j = C_k))$
$\equiv$ {TODO}
$\neg((A_i \leqslant B_j) \wedge (B_j \leqslant C_k) \wedge (C_k \leqslant A_i) \wedge (A_i \neq B_j \neq C_k))$
$\equiv$ {TODO}
$\neg((A_i = B_j = C_k) \wedge (A_i \neq B_j \neq C_k))$
$\equiv$ {TODO}
$(A_i \neq B_j \neq C_k) \vee (A_i = B_j = C_k)$