

Assignment 2: Verification

Maxwell Bo 43926871

April 11, 2017

1 Part A

Given

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

and

$$\begin{aligned} post &\triangleq D = A \cap B \cap C \\ &\quad \wedge r \in [0, D.len] \wedge i \in [0, A.len] \wedge j \in [0, B.len] \wedge k \in [0, C.len] \\ &\quad \wedge (i = A.len \vee j = B.len \vee k = C.len) \end{aligned}$$

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

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

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

\therefore

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

$$\sqsubseteq \{ \text{Assignment: } pre \Rightarrow inv[i, j, k, r \setminus 0, 0, 0, 0] \}$$

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

\therefore

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

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

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

∴

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

⊆ {Repetition Rule}

```

i, j, k, r := 0, 0, 0, 0;
do (i ≠ A.len ∨ j ≠ B.len ∨ k ≠ C.len) →
    i, j, k, r, D[inv ∧ (i ≠ A.len ∨ j ≠ B.len ∨ k ≠ C.len), inv ∧ (0 ≤ V < V0)]
od

```