Assignment 3: Derivation

Maxwell Bo 43926871

May 18, 2017

1. (a) n is a **value** parameter. m is a **result** parameter.

   (b) Our post-condition, $mrun(A, n_0, m)$, expands to $lrun(A, n_0, m) \wedge (m < A.\text{len} \Rightarrow A_{n_0} \neq A_m)$. This satisfies the form $Q_1 \wedge Q_2$. Q_1 was chosen as the invariant.

$$inv \triangleq lrun(A, n_0, m)$$

   Q_2 is chosen as the *negation* of the guard, s.t.

$$\begin{aligned} \neg guard &\triangleq m < A.\text{len} \Rightarrow A_{n_0} \neq A_m \\ guard &\triangleq \neg(m < A.\text{len} \Rightarrow A_{n_0} \neq A_m) \\ &\triangleq \neg(\neg(m < A.\text{len}) \vee (A_{n_0} \neq A_m)) \\ &\triangleq (m < A.\text{len}) \wedge \neg(A_{n_0} \neq A_m) \\ &\triangleq (m < A.\text{len} \wedge A_{n_0} = A_m) \end{aligned}$$

   (c) Let

$$\begin{aligned} pre &\triangleq lrun(A, n, n+1) \\ post &\triangleq mrun(A, n_0, m) \end{aligned}$$

   s.t.

$$\begin{aligned} & n, m : [pre,\ post] \\ \sqsubseteq\ & \{\text{Composition: middle predicate is } inv\} \\ & n, m : [pre,\ inv];\quad n, m : [inv,\ post] \\ \sqsubseteq\ & \{\text{Assignment: } pre \Rrightarrow inv[m \backslash n+1]\} \\ & m := n+1;\quad n, m : [inv,\ post] \end{aligned}$$

   $\because$

$$\begin{aligned} inv[m \backslash n+1] &\equiv lrun(A, n_0, m)[m \backslash n+1] \\ &\equiv lrun(A, n_0, n+1) \end{aligned}$$

   $\therefore$

$$lrun(A, n, n+1) \Rrightarrow lrun(A, n_0, n+1)$$

$$\begin{aligned} \sqsubseteq\ & \{\text{Strengthen post: } inv \wedge \neg guard \Rrightarrow post\} \\ & m := n+1;\quad n, m : [inv,\ inv \wedge \neg guard] \end{aligned}$$

   $\because$

$$
\begin{array}{ll}
& inv \wedge \neg guard \ \Rrightarrow \ post \\
\equiv & \{\text{Expansion of definitions}\} \\
& lrun(A, n_0, m) \wedge \neg(m < A.\text{len} \wedge A_{n_0} = A_m) \ \Rrightarrow \ mrun(A, n_0, m) \\
\equiv & \{\text{Expansion of functions}\} \\
& lrun(A, n_0, m) \wedge \neg(m < A.\text{len} \wedge A_{n_0} = A_m) \ \Rrightarrow \ lrun(A, n_0, m) \wedge (m < A.\text{len} \Rightarrow A_{n_0} \neq A_m) \\
\equiv & \{\text{De Morgan's law - negation of conjunction}\} \\
& lrun(A, n_0, m) \wedge (\neg(m < A.\text{len}) \vee \neg(A_{n_0} = A_m)) \ \Rrightarrow \ lrun(A, n_0, m) \wedge (m < A.\text{len} \Rightarrow A_{n_0} \neq A_m) \\
\equiv & \{P \Rightarrow Q \ \equiv \ \neg P \vee Q\} \\
& lrun(A, n_0, m) \wedge (\neg(m < A.\text{len}) \vee \neg(A_{n_0} = A_m)) \ \Rrightarrow \ lrun(A, n_0, m) \wedge (\neg(m < A.\text{len}) \vee (A_{n_0} \neq A_m)) \\
\equiv & \{\} \\
& \text{true}
\end{array}
$$

$$
\begin{array}{ll}
\sqsubseteq & \{\text{Repetition}\} \\
& \ m := n + 1; \\
& \ \textbf{do } (m < A.\text{len} \wedge A_{n_0} = A_m) \rightarrow \\
& \qquad n, m : [inv \wedge guard,\ inv \wedge (0 \leqslant V < V_0)] \\
& \ \textbf{od}
\end{array}
$$

where

$$V \ \triangleq \ A.\text{len} \ - \ m$$

$$
\begin{array}{ll}
\sqsubseteq & \{\text{Assignment: } inv \wedge guard \ \Rrightarrow \ (inv \wedge (0 \leqslant V < V_0))[m \backslash m + 1]\} \\
& \ m := n + 1; \\
& \ \textbf{do } (m < A.\text{len} \wedge A_{n_0} = A_m) \rightarrow \\
& \qquad m := m + 1 \\
& \ \textbf{od}
\end{array}
$$

$\because$

$$
\begin{array}{rcl}
(inv \wedge (0 \leqslant V < V_0))[m \backslash m + 1] & \equiv & (lrun(A, n_0, m) \wedge (0 \leqslant (A.\text{len} - m) < (A.\text{len} - m_0)))[m, m_0 \backslash m + 1, m] \\
& \equiv & lrun(A, n_0, m + 1) \wedge (0 \leqslant (A.\text{len} - (m + 1)) < (A.\text{len} - m))
\end{array}
$$

$\therefore$

$$
\begin{array}{rcl}
inv \wedge guard & \Rrightarrow & lrun(A, n_0, m + 1) \wedge (0 \leqslant (A.\text{len} - (m + 1)) < (A.\text{len} - m)) \\
lrun(A, n_0, m) \wedge (m < A.\text{len} \wedge A_{n_0} = A_m) & \Rrightarrow & lrun(A, n_0, m + 1) \wedge (0 \leqslant (A.\text{len} - (m + 1)) < (A.\text{len} - m))
\end{array}
$$

To justify this, we need to show that both conjuncts on the **RHS** are entailed by the **LHS**.

i.

$$m < A.\text{len} \ \Rrightarrow \ 0 \leqslant (A.\text{len} - (m + 1)) < (A.\text{len} - m)$$

is trivially *true*. The first conjunct is entailed by the **LHS**.

ii. Reiterating

$$lrun(A, i, j) \ \triangleq \ run(A, i, j) \wedge (i > 0 \Rightarrow A_{i-1} \neq A_i)$$

we can see that

$$lrun(A, n_0, m) \wedge (m < A.\text{len} \wedge A_{n_0} = A_m) \ \Rrightarrow \ lrun(A, n_0, m + 1)$$

holds because

A. $run(A, n_0, m + 1)$ describes a run up to, but not including index $m + 1$. Because we know that $A_{n_0} = A_m$, we are permitted absorb A_m into the run range by incrementing m to $m + 1$.

B. Due to $m < A.len$, A_m describes a valid array access.

The second conjunct is entailed by the **LHS**.

All conjuncts hold, and are entailed by the **LHS**.

$\square$

2.

$$\begin{aligned} pre &\triangleq A.\text{len} > 0 \\ post &\triangleq mrun(A, \ell, h) \land (\forall\, p, q \cdot mrun(A, p, q) \Rightarrow (h - \ell) \leqslant (q - p)) \end{aligned}$$

$$\begin{aligned} & \ell, h : [pre,\ post] \\ \sqsubseteq\ & \{\text{Composition: middle predicate is } inv\} \\ & \ell, h : [pre,\ inv];\quad \ell, h : [inv,\ post] \end{aligned}$$

where

$$inv \triangleq mrun(A_{[0,i)}, \ell, h) \land (\forall\, p, q \cdot mrun(A_{[0,i)}, p, q) \Rightarrow (h - \ell) \leqslant (q - p))$$

This invariant was chosen as the postcondition refers to a constant A, which can be written $A_{[0,A.\text{len})}$, which is of the form A^B, where B is A.len. We replace A.len with a program variable i, to create the invariant defined above. We can further derive the negation of our guard to be ($i = A$.len), such that the guard is ($i \neq A$.len).

$$\begin{aligned} \sqsubseteq\ & \{\text{Assignment: } pre \Rrightarrow inv[i, \ell, h \backslash 1, 0, 1]\} \\ & i, \ell, h := 1, 0, 1;\quad \ell, h : [inv,\ post] \end{aligned}$$

$\because$

$$inv[i, \ell, h \backslash 1, 0, 1] \equiv mrun(A_{[0,1)}, 0, 1) \land (\forall\, p, q \cdot mrun(A_{[0,1)}, p, q) \Rightarrow (1 - 0) \leqslant (q - p))$$

$\therefore$

$$A.\text{len} > 0 \Rrightarrow mrun(A_{[0,1)}, 0, 1) \land (\forall\, p, q \cdot mrun(A_{[0,1)}, p, q) \Rightarrow (1 - 0) \leqslant (q - p))$$

The first conjunct is intuitively *true*, as the maximal run of an array of len $= 1$ is itself.
The **LHS** of the implication in the second conjunct is *true* only when $p = 0$ and $q = 1$. The **RHS** is then $(1 - 0) \leqslant (1 - 0)$. Thus, the implication is *true* for these values of p and q. All other values of p and q cause the **LHS** of the implication to be *false*, and thus the implication to be *true*. Thus, the second conjunct is *true*. Thus, the entailment holds as

$$A.\text{len} > 0 \Rrightarrow \text{true} \land \text{true}$$

Let

$$guard \triangleq (i \neq A.\text{len})$$

s.t.

$$\begin{aligned} \sqsubseteq\ & \{\text{Strengthen post: } inv \land \neg guard \Rrightarrow post\} \\ & i, \ell, h := 1, 0, 1;\quad \ell, h : [inv,\ inv \land \neg guard] \end{aligned}$$

$\because$

$$\begin{aligned} inv \land \neg guard \Rrightarrow post \equiv\ & mrun(A_{[0,i)}, \ell, h) \land (\forall\, p, q \cdot mrun(A_{[0,i)}, p, q) \Rightarrow (h - \ell) \leqslant (q - p)) \land \neg(i \neq A.\text{len}) \\ & \Rrightarrow mrun(A, \ell, h) \land (\forall\, p, q \cdot mrun(A, p, q) \Rightarrow (h - \ell) \leqslant (q - p)) \end{aligned}$$

The third conjunct $\neg(i \neq A.\text{len})$, is equivalent to $i = A$.len. We can absorb this into the first and second conjuncts to give

$$\begin{aligned} & mrun(A_{[0,A.len)}, \ell, h) \land (\forall\, p, q \cdot mrun(A_{[0,A.len)}, p, q) \Rightarrow (h - \ell) \leqslant (q - p)) \\ & \Rrightarrow mrun(A, \ell, h) \land (\forall\, p, q \cdot mrun(A, p, q) \Rightarrow (h - \ell) \leqslant (q - p)) \end{aligned}$$

As $A_{[0,A.len)} \equiv A$, the entailment holds.

$$
\begin{array}{ll}
\sqsubseteq & \{\text{Repetition}\} \\
& i, \ell, h := 1, 0, 1; \\
& \textbf{do } (i \neq A.\text{len}) \rightarrow \\
& \qquad \ell, h : [\mathit{inv} \wedge \mathit{guard},\ \mathit{inv} \wedge (0 \leqslant V < V_0)] \\
& \textbf{od}
\end{array}
$$

where

$$V \triangleq A.\text{len} - i$$