Assignment 3: Derivation

Maxwell Bo 43926871

May 17, 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. Thus,

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

   (c) Let

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

s.t.

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

$\because$

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

$\therefore$

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

Let

$$guard \triangleq (m < A.\text{len} \wedge A_{n_0} = A_m)$$

s.t.

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

$\because$

$$\begin{aligned}
& inv \wedge \neg guard \Rrightarrow post \\
\equiv\ & \{\text{Expansion of definitions}\} \\
& lrun(A, n_0, m) \wedge \neg(m < A.\text{len} \wedge A_{n_0} = A_m) \Rrightarrow mrun(A, n_0, m) \\
\equiv\ & \{\text{Expansion of functions}\}
\end{aligned}$$

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

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

where

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

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

$\because$

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

$\therefore$

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

Furthermore,

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

is trivially true.

$$lrun(A, n_0, m) \quad \Rrightarrow \quad lrun(A, n_0, m + 1)$$

Reiterating

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

Because $A_{n_0} = A_m$, the $run(A, n_0, m+1)$ holds, noting that $run(A, n_0, m+1)$ describes a run up to, but not including index $m+1$. Thus, we are free to perform the assignment, expanding the *run* range.
All conjuncts hold, and are entailed by the LHS.
□

2.

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

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

where

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

This invariant was chosen as the postcondition refers to a constant A, which can be written $A_{[0,A.\mathrm{len})}$, 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.

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

$\because$

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

$\therefore$

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

The first part of the conjunct is intuitively true, as the maximal run of an array of len $= 1$ is itself.

$\ell := 0;$
do $(m < A.\mathrm{len} \wedge A_{n_0} = A_m) \rightarrow$