

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, $mr\text{run}(A, n_0, m)$, expands to $lr\text{un}(A, n_0, m) \wedge (m < A.\text{len} \Rightarrow A_{n_0} \neq A_m)$. This satisfies the form $Q_1 \wedge Q_2$.

Q_1 was chosen as the invariant, s.t.

$$inv \triangleq lr\text{un}(A, n_0, m)$$

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

$$\begin{aligned} pre &\triangleq lr\text{un}(A, n, n+1) \\ post &\triangleq mr\text{run}(A, n_0, m) \end{aligned}$$

s.t.

$$n, m : [pre, post]$$

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

$$n, m : [pre, inv]; \quad n, m : [inv, post]$$

$$\sqsubseteq \{ \text{Assignment: } pre \Rightarrow inv[m \setminus n+1] \}$$

$$m := n+1; \quad n, m : [inv, post]$$

\therefore

$$\begin{aligned} inv[m \setminus n+1] &\equiv lr\text{un}(A, n_0, m)[m \setminus n+1] \\ &\equiv lr\text{un}(A, n_0, n+1) \end{aligned}$$

\therefore

$$lr\text{un}(A, n, n+1) \Rightarrow lr\text{un}(A, n_0, n+1)$$

$$\sqsubseteq \{ \text{Strengthen post: } inv \wedge \neg guard \Rightarrow post \}$$

$$m := n+1; \quad n, m : [inv, inv \wedge \neg guard]$$

\therefore

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

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

where

$$V \triangleq A.len - m$$

$$\begin{aligned}
\sqsubseteq & \{ \text{Assignment: } inv \wedge guard \Rightarrow (inv \wedge (0 \leq V < V_0))[m \setminus m + 1] \} \\
& m := n + 1; \\
& \mathbf{do} (m < A.len \wedge A_{n_0} = A_m) \rightarrow \\
& \quad m := m + 1 \\
& \mathbf{od}
\end{aligned}$$

\therefore

$$\begin{aligned}
(inv \wedge (0 \leq V < V_0))[m \setminus m + 1] & \equiv (lrun(A, n_0, m) \wedge (0 \leq (A.len - m) < (A.len - m_0)))[m, m_0 \setminus m + 1, m] \\
& \equiv lrun(A, n_0, m + 1) \wedge (0 \leq (A.len - (m + 1)) < (A.len - m))
\end{aligned}$$

\therefore

$$\begin{aligned}
inv \wedge guard & \Rightarrow lrun(A, n_0, m + 1) \wedge (0 \leq (A.len - (m + 1)) < (A.len - m)) \\
lrun(A, n_0, m) \wedge (m < A.len \wedge A_{n_0} = A_m) & \Rightarrow lrun(A, n_0, m + 1) \wedge (0 \leq (A.len - (m + 1)) < (A.len - m))
\end{aligned}$$

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

i.

$$m < A.len \Rightarrow 0 \leq (A.len - (m + 1)) < (A.len - m)$$

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

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

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**.

□

2.

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

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

where

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

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 $A.\text{len}$. We replace $A.\text{len}$ with a program variable i , to create the invariant defined above. We can further derive the negation of our guard to be $(i = A.\text{len})$, such that the guard is $(i \neq A.\text{len})$.

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

\therefore

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

\therefore

$$A.\text{len} > 0 \Rightarrow mrun(A_{[0,1]}, 0, 1) \wedge (\forall p, q \cdot mrun(A_{[0,1]}, p, q) \Rightarrow (1 - 0) \leq (q - p))$$

The first conjunct is intuitively *true*, as the maximal run of an array of $\text{len} = 1$ is itself.

The **LHS** of the implication in the second conjunct is *true* only when $p = 0$ and $q = 1$. The **RHS** is then $(1 - 0) \leq (1 - 0)$. 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

$$A.\text{len} > 0 \Rightarrow \text{true} \wedge \text{true}$$

Let

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

s.t.

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

\therefore

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

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

$$\begin{aligned} &mrun(A_{[0,A.\text{len}]}, \ell, h) \wedge (\forall p, q \cdot mrun(A_{[0,A.\text{len}]}, p, q) \Rightarrow (h - \ell) \leq (q - p)) \\ &\Rightarrow mrun(A, \ell, h) \wedge (\forall p, q \cdot mrun(A, p, q) \Rightarrow (h - \ell) \leq (q - p)) \end{aligned}$$

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

```

 $\sqsubseteq$  {Repetition}
 $i, \ell, h := 1, 0, 1;$ 
do ( $i \neq A.\text{len}$ )  $\rightarrow$ 
     $\ell, h : [inv \wedge guard, inv \wedge (0 \leq V < V_0)]$ 
od

```

where

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