CSU44004-Formal Verification Assignment 2

Leong Kai Ler
15334636

November 19, 2019

$Found = 1 \Rightarrow \exists\, i(0 \leq i < |s| \wedge n = s[i])$
$(\exists\, i(0 \leq i < |s| \wedge n = s[i])) \Rightarrow Found = 1$
$\equiv$
$\forall\, i(0 \leq i < |s| \wedge n = s[i] \Rightarrow Found = 1)$

invariant := $\forall\, i(0 \leq i < ind \not\Rightarrow \neg(n = s[i]))$

$(\!|\ T\ |\!)$
$(\!|\ \neg Memb(s[..0], n)\ |\!)$
ind $:= 0$;
found $:= 0$;
$(\!|\ I_2 \wedge I_3 \wedge \neg Memb(s[..ind], n)\ |\!)$
while(ind$< |s|$ && **found** $= 0)\{$
$(\!|\ I_2 \wedge I_3 \wedge \neg Memb(s[..ind], n) \wedge ind < |s| \wedge found = 0\ |\!)$
$(\!|\ I_2 \wedge I_3 \wedge (s[ind] = n \Rightarrow \neg Memb(s[..ind], n)) \wedge (\neg(s[ind] = n) \Rightarrow \neg Memb(s[..ind + 1], n))\ |\!)$
if(s[ind] $=$ **n)**$\{$
$(\!|\ \neg Memb(s[..ind], n))\ |\!)$
found = 1
$(\!|\ \neg Memb(s[..ind], n))\ |\!)$
$\}$
else$\{$
$(\!|\ \neg Memb(s[..ind + 1], n))\ |\!)$
ind = ind + 1
$(\!|\ \neg Memb(s[..ind], n))\ |\!)$
$\}$
$(\!|\ (I_2 \wedge I_3) \wedge \neg Memb(s[..ind], n))\ |\!)$
$\}$
$(\!|\ I_2 \wedge I_3 \wedge \neg Memb(s[..ind], s) \wedge \neg(ind < |s| \wedge found = 0)\ |\!)$
$(\!|\ \neg(found = 1) \Rightarrow \neg Memb(s, n)\ |\!)$

Memb(s,n) = $\exists\, i(0 \leq i < |s| \wedge s[i] = n)$
Prove:

$$
\begin{aligned}
found = 1 &\Leftrightarrow \exists\, i(0 \leq i < |s| \wedge s[i] = n) \\
\equiv found = 1 &\Leftrightarrow Memb(s, n) \\
\equiv found = 1 &\Rightarrow Memb(s, n) \\
\equiv Memb(s, n) &\Rightarrow found = 1 \\
\equiv \neg(found = 1) &\Rightarrow \neg(Memb(s, n))
\end{aligned}
$$

s = 
Case where n is not in S[..ind] or S.

$$\begin{aligned} I_1 &= \neg Memb(S[..ind], n) \\ &\equiv \forall i(0 \leq i < ind \Rightarrow \neg(s[i] = n) \\ &\equiv \forall i(\neg(0 \leq i < ind) \vee \neg(s[i] = n) \\ &\equiv \forall i \neg(0 \leq i < ind \wedge (s[i] = n) \\ &\equiv \neg \exists(0 \leq i < ind \wedge (s[i] = n) \\ &\equiv \neg Memb(S[..ind], n) \end{aligned}$$

$$\begin{aligned} & \neg Memb(s[..ind], n) \wedge \neg(ind < |s| \wedge found = 0) \\ \Rightarrow\ & \neg Memb(s[..ind], n) \wedge (\neg(ind < |s|) \vee \neg(found = 0)) \\ \Rightarrow\ & \neg(Memb(s[..ind], n) \wedge (\neg(ind < |s|)) \vee (\neg Memb(s[..ind], n) \wedge \neg(found = 0)) \\ \Rightarrow\ & \neg(found = 1) \Rightarrow \neg(Memb(s, n) \end{aligned}$$

Take ¬**found = 0)**:

$$\begin{aligned} I_2 &= (found = 0) \vee (found = 1) \\ I_3 &= 0 \leq ind < |s| \end{aligned}$$

Now, go back and put in the pre- and postconditions.