ECE 653 - ASSIGNMENT 3

ARSHAD MOMIN

Student ID- 20986176

Email- a5momin@uwaterloo.ca

Question 1 :

Construct a derivation to show the validity of the following Hoare triple:

$\{n \geq 0 \land r = 0 \land i = 0 \land p = 1\}$ P $\{r = 2n - 1\}$

Considering Inductive Invariant as $I = p = 2^i \land r = 2^i - 1 \land i \leq n$

Answer:

Considering below implications:

$$\{\mathbf{n} \geq \mathbf{0} \land \mathbf{r} = \mathbf{0} \land \mathbf{i} = \mathbf{0} \land \mathbf{p} = \mathbf{1}\} \rightarrow I \qquad \{\mathbf{r} = \mathbf{2^n} - \mathbf{1}\} \rightarrow \{\mathbf{I} \land (\mathbf{i} = \mathbf{n})\}$$

$$\frac{\{I\}\mathbf{while}\ !(i = n)\,\mathbf{do}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I \land (i = n)\}}{\{n \geq 0 \land r = 0 \land i = 0 \land p = 1\}\mathbf{while}\ !(i = n)\ \mathbf{do}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{r = 2^n - 1\}}$$

Continuing the above derivation by following inference rule for while loop:

Considering the implications as follows:

$$I \land !(i = n) \rightarrow \{I[r - p\ /\ r, 2 * p\ /\ p\ , r + p\ /r, i + 1\ /i]\}$$

$$\cfrac{\cfrac{\cfrac{\{I[r + p\ /r,\ i + 1\ /i]\}r = r + p\{I[i + 1\ /i]\} \quad \{I[i + i\ /i]\}i = i + 1\{I\}}{\{I \land !(i = n)\}\ r = r - p\{C\} \quad \{C\}\ p = 2 * p\{D\} \quad \{D\}\ r = r + p\{E\} \quad \{E\}i = i + 1\{I\}}}{\{I \land !(i = n)\}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I\}}}{\{I\}\mathbf{while}\ !(i = n)\mathbf{do}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I \land (i = n)\}}$$

Continued:

$$\cfrac{\cfrac{\cfrac{\{I[2 * p\ /\ \ p,\ \ r + p\ /r,\ \ i + 1\ /i]\}p = 2 * p\{I[r + p\ /r,\ \ i + 1\ /i]\}\ \}}{\{I \land !(i = n)\}\ r = r - p\{C\} \quad \{C\}\ p = 2 * p\{D\} \quad \{D\}\ r = r + p\{E\} \quad \{E\}i = i + 1\{I\}}}{\{I \land !(i = n)\}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I\}}}{\{I\}\mathbf{while}\ !(i = n)\mathbf{do}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I \land (i = n)\}}$$

Continued:

$$\cfrac{\cfrac{\cfrac{\{I[r - p\ /\ r\ \ 2 * p\ /\ p\ , r + p\ /r,\ \ i + 1\ /i]\}\ r = r - p\{I[2 * p\ /\ p,\ \ r + p\ /r,\ \ i + 1\ /i]\}}{\{I \land !(i = n)\}\ r = r - p\{C\} \quad \{C\}\ p = 2 * p\{D\} \quad \{D\}\ r = r + p\{E\} \quad \{E\}i = i + 1\{I\}}}{\{I \land !(i = n)\}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I\}}}{\{I\}\mathbf{while}\ !(i = n)\mathbf{do}\ (r = r - p, p = 2 * p, r = r + p, i = i + 1)\{I \land (i = n)\}}$$

Considering the below constraints:

1. $\mathbf{I} \wedge !(\mathbf{i} = \mathbf{n}) \rightarrow \{\mathbf{I}[\mathbf{2} * \mathbf{p} \,/\, \mathbf{p}, \mathbf{r} + \mathbf{p} \,/\mathbf{r}, \mathbf{i} + \mathbf{1} \,/\mathbf{i}]\}$
2. $\{\mathbf{r} = \mathbf{2^n} - \mathbf{1}\} \rightarrow \{\mathbf{I} \wedge (\mathbf{i} = \mathbf{n})\}$

$$\mathbf{I} = \mathbf{p} = \mathbf{2}^{\boldsymbol{i}} \wedge \mathbf{r} = \mathbf{2}^{\boldsymbol{i}} - \mathbf{1} \wedge \mathbf{i} \leq \mathbf{n}$$

1. $\mathbf{I} \wedge !(\mathbf{i} = \mathbf{n}) \rightarrow \mathbf{I} = \mathbf{2} * \mathbf{p} = \mathbf{2^{i+1}} \wedge \mathbf{r} + \mathbf{p} = \mathbf{2^{i+1}} - \mathbf{1} \wedge \mathbf{i} + \mathbf{1} \leq \mathbf{n}$