CS 591 G1—Formal Methods in Security and Privacy—Spring 2021

Assignment 3

Due by Wednesday, March 3, at 5pm
Submission Via Gradescope

Exercise 1 For each of the following Hoare Triples, say if it is valid or not, providing a counterexample in the case it is not valid.

1. $X := 8 : \{\texttt{True}\} \Rightarrow \{X = 4 + 4\}$

2. $X := X + 1 : \{X = 4 + 1\} \Rightarrow \{X = 4\}$

3. $X := 5; Y := 0 : \{Y = 0\} \Rightarrow \{X = 5\}$

4. $X := 5 : \{X = 2 \wedge X = 3\} \Rightarrow \{X = 0\}$

5. $\texttt{abort} : \{\texttt{False}\} \Rightarrow \{\texttt{True}\}$

6. $\texttt{skip} : \{\texttt{True}\} \Rightarrow \{\texttt{False}\}$

7. $\texttt{abort} : \{\texttt{True}\} \Rightarrow \{\texttt{False}\}$

8. $\texttt{while true do skip end} : \{\texttt{True}\} \Rightarrow \{\texttt{False}\}$

9. $\texttt{while}\, X > 0\, \texttt{do}\, X := X - 1\, \texttt{end} : \{X > 0\} \Rightarrow \{X = 0\}$

10. $\texttt{while}\, !(X = 5)\, \texttt{do}\, X := X + 1\, \texttt{end} : \{X < 0\} \Rightarrow \{X = 5\}$

Exercise 2 Use the rules of Hoare Logic presented in class to derive formally the following Hoare triples.

1) $\vdash Z := X; X := Y; Y := Z : \{Y = m, X = n\} \Rightarrow \{X = m, Y = n\}$

2) $\vdash \texttt{if}\, X > 0\, \texttt{then}\, X := X + 1\, \texttt{else}\, \texttt{abort} : \{\texttt{X} = \texttt{n}\} \Rightarrow \{\texttt{X} = \texttt{n} + \texttt{1}\}$

3)

$$\vdash \texttt{while}\, X > 0\, \texttt{do}\, X := X - 1\, \texttt{end} : \{X > 0\} \Rightarrow \{X = 0\}$$

Exercise 3 Use the rules of Relational Hoare Logic presented in class to derive formally the following Relational Hoare triples.

1)

$$\vdash X := X + 1; Y := Y + 1 \sim X := X + 1; Y := Y - 1$$
$$: \{X\langle 1\rangle = X\langle 2\rangle \wedge Y\langle 1\rangle = -Y\langle 2\rangle\} \Rightarrow \{X\langle 1\rangle = X\langle 2\rangle \wedge Y\langle 1\rangle = -Y\langle 2\rangle\}$$

2)

$$
\begin{array}{l}
\vdash Z := 0; \texttt{if}\ X > Z\ \texttt{then}\ Z := 1\ \texttt{else}\ Z := 2 \\
\sim \\
Z := 1; \texttt{if}\ X + 1 > Z\ \texttt{then}\ Z := 0\ \texttt{else}\ Z := 1 \\
: \{X\langle 1\rangle = X\langle 2\rangle\} \Rightarrow \{\texttt{Z}\langle 1\rangle = \texttt{Z}\langle 2\rangle + 1\}
\end{array}
$$

3)

$$
\begin{array}{l}
\vdash Z := 0; \texttt{if}\ (X \mod 2 = Z)\ \texttt{then}\ Z := 1\ \texttt{else}\ Z := 2 \\
\sim \\
Z := 0; \texttt{if}\ (X \mod 2 = Z)\ \texttt{then}\ Z := 2\ \texttt{else}\ Z := 1 \\
: \{X\langle 1\rangle + 1 = X\langle 2\rangle\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}
\end{array}
$$