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

   Valid

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

   Not valid. $m_{in} = [x = 5] m_{out} = [x = 6]$

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

   Valid

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

   Valid

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

   Valid

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

   Not valid. For every m, $m_{in} = m m_{out} = m$.

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

   Valid

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

   Valid

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

   Valid

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

    Valid

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

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

$$\frac{\dfrac{\vdash Z := X : \{Y = m, X = n\} \Rightarrow \{Y = m, Z = n\} \qquad \vdash X := Y : \{Y = m, Z = n\} \Rightarrow \{X = m, Z = n\}}{\vdash Z := X; X := Y : \{Y = m, X = n\} \Rightarrow \{X = m, Z = n\}} \qquad \vdash Y := Z : \{X = m, Z = n\} \Rightarrow \{X = m, Y = n\}}{\vdash Z := X; X := Y; Y := Z : \{Y = m, X = n\} \Rightarrow \{X = m, Y = n\}}$$

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

$$\frac{X = n \wedge (X > 0) \Rightarrow X + 1 = n + 1 \quad \vdash X = X + 1 : \{X + 1 = n + 1\} \Rightarrow \{X = n + 1\} \quad X = n + 1 \Rightarrow X = n + 1}{\vdash X = X + 1 : \{X = n \wedge X > 0\} \Rightarrow \{X = n + 1\}}$$

$$\frac{X = n \wedge !(X > 0) \Rightarrow \texttt{true} \quad \vdash \texttt{abort} : \{\texttt{true}\} \Rightarrow \{\texttt{false}\} \quad \texttt{false} \Rightarrow X = n + 1}{\vdash \texttt{abort} : \{X = n \wedge !(X > 0)\} \Rightarrow \{X = n + 1\}}$$

$$\frac{\vdash X = X + 1 \{X = n \wedge X > 0\} \Rightarrow \{X = n + 1\} \qquad \vdash \texttt{abort} : \{X = n \wedge !(X > 0)\} \Rightarrow \{X = n + 1\}}{\vdash \texttt{if}\, X > 0\, \texttt{then}\, X = X + 1\, \texttt{else}\, \texttt{abort} : \{X = n\} \Rightarrow \{X = n + 1\}}$$

3)

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

$$\dfrac{\{X > 0\} \Rightarrow \{X > 0\} \qquad \dfrac{\dfrac{\{X > 0 \wedge X \geq 0\} \Rightarrow \{X - 1 \geq 0\} \qquad X := X - 1 : \{X - 1 \geq 0\} \Rightarrow \{X \geq 0\} \qquad \{X \geq 0\} \Rightarrow \{X \geq 0\}\}}{X := X - 1 : \{X > 0 \wedge X \geq 0\} \Rightarrow \{X \geq 0\}\}}{\vdash \texttt{while}\, X > 0\, \texttt{do}\, X := X - 1\, \texttt{end} : \{X > 0\} \Rightarrow \{X \geq 0 \wedge !(X > 0)\}} \qquad \{X \geq 0 \wedge !(X > 0)\} \Rightarrow \{X = 0\}}{\vdash \texttt{while}\, X > 0\, \texttt{do}\, X := X - 1\, \texttt{end} : \{X > 0\} \Rightarrow \{X = 0\}}$$

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

1)

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

Let us call Π the following derivation

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

and let's call Σ the following derivation

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

Then we have a derivation Δ:

$$\dfrac{\Pi \qquad \Sigma}{\vdash X := X + 1; Y := Y + 1 \sim X := X + 1; Y := Y - 1 : \{X\langle 1\rangle + 1 = X\langle 2\rangle + 1 \wedge Y\langle 1\rangle + 1 = -(Y\langle 2\rangle - 1)\} \Rightarrow \{X\langle 1\rangle = X\langle 2\rangle \wedge Y\langle 1\rangle = -Y\langle 2\rangle\}}$$

and we can conclude

$$\dfrac{\{X\langle 1\rangle = X\langle 2\rangle \wedge Y\langle 1\rangle = -Y\langle 2\rangle\} \Rightarrow \{X\langle 1\rangle + 1 = X\langle 2\rangle + 1 \wedge Y\langle 1\rangle + 1 = -(Y\langle 2\rangle - 1)\} \qquad \Delta}{\vdash X := X + 1; Y := Y + 1 \sim X := X + 1; Y := Y - 1 : \{X\langle 1\rangle = X\langle 2\rangle \wedge Y\langle 1\rangle = -Y\langle 2\rangle\} \Rightarrow \{X\langle 1\rangle = X\langle 2\rangle \wedge Y\langle 1\rangle = -Y\langle 2\rangle\}}$$

2)

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

Let us call P the formula $X\langle 1\rangle = X\langle 2\rangle \wedge Z\langle 1\rangle = 0 \wedge Z\langle 2\rangle = 1$ and let us call Π the following

derivation

$$\dfrac{\{X\langle 1\rangle > Z\langle 1\rangle \wedge P\} \Rightarrow \{2 = 1 + 1\} \qquad \dfrac{}{\vdash Z := 2 \sim Z := 1 : \{2 = 1 + 1\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle + 1\}}}{\vdash Z := 2 \sim Z := 1 : \{X\langle 1\rangle > Z\langle 1\rangle \wedge P\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle + 1\}}$$

and let's call Σ the following derivation

$$\dfrac{\{!(X\langle 1\rangle > Z\langle 1\rangle) \wedge P\} \Rightarrow \{1 = 0 + 1\} \qquad \dfrac{}{\vdash Z := 1 \sim Z := 0 :: \{1 = 0 + 1\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle + 1\}}}{\vdash Z := 1 \sim Z := 0 :: \{!(X\langle 1\rangle > Z\langle 1\rangle) \wedge P\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle + 1\}}$$

Let's Ω be the following derivation

$$\dfrac{\{P\} \Rightarrow \{X\langle 1\rangle > Z\langle 1\rangle = X\langle 2\rangle + 1 > Z\langle 2\rangle\} \qquad \Pi \qquad \Sigma}{\begin{array}{c}\vdash \texttt{if}\ X > Z\ \texttt{then}\ Z := 1\ \texttt{else}\ Z := 2 \sim \texttt{if}\ X + 1 > Z\ \texttt{then}\ Z := 0\ \texttt{else}\ Z := 1\\ : \{P\} \Rightarrow \{\texttt{Z}\langle 1\rangle = \texttt{Z}\langle 2\rangle + 1\}\end{array}}$$

Let Ξ be the following derivation

$$\dfrac{\{X\langle 1\rangle = X\langle 2\rangle\} \Rightarrow \{X\langle 1\rangle = X\langle 2\rangle \wedge 0 = 0 \wedge 1 = 1\} \qquad \dfrac{}{\vdash Z := 0 \sim Z := 1 : \{X\langle 1\rangle = X\langle 2\rangle \wedge 0 = 0 \wedge 1 = 1\} \Rightarrow \{P\}}}{\vdash Z := 0 \sim Z := 1 : \{X\langle 1\rangle = X\langle 2\rangle\} \Rightarrow \{P\}}$$

Putting everything together we have:

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

3)

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

Let us use the following formulas

$$\begin{array}{lcl}P_{1,1} & = & X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0 \wedge (X\langle 1\rangle \mod 2 = Z\langle 1\rangle) \wedge (X\langle 2\rangle \mod 2 = Z\langle 2\rangle)\\ P_{1,2} & = & X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0 \wedge (X\langle 1\rangle \mod 2 = Z\langle 1\rangle) \wedge !(X\langle 2\rangle \mod 2 = Z\langle 2\rangle)\\ P_{2,1} & = & X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0 \wedge !(X\langle 1\rangle \mod 2 = Z\langle 1\rangle) \wedge (X\langle 2\rangle \mod 2 = Z\langle 2\rangle)\\ P_{2,2} & = & X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0 \wedge !(X\langle 1\rangle \mod 2 = Z\langle 1\rangle) \wedge !(X\langle 2\rangle \mod 2 = Z\langle 2\rangle)\end{array}$$

and let us call $\Pi_{1,1}$ the following derivation

$$\dfrac{\{P_{1,1}\} \Rightarrow \{1 = 2\} \qquad \dfrac{}{\vdash Z := 1 \sim Z := 2 : \{1 = 2\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}}{\vdash Z := 1 \sim Z := 2 : \{P_{1,1}\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}$$

$\Pi_{1,2}$ the following derivation

$$\dfrac{\{P_{1,2}\} \Rightarrow \{1 = 1\} \qquad \dfrac{}{\vdash Z := 1 \sim Z := 1 : \{1 = 1\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}}{\vdash Z := 1 \sim Z := 1 : \{P_{1,2}\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}$$

$\Pi_{2,1}$ the following derivation

$$\dfrac{\{P_{2,1}\} \Rightarrow \{2 = 2\} \qquad \dfrac{}{\vdash Z := 2 \sim Z := 2 : \{2 = 2\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}}{\vdash Z := 2 \sim Z := 2 : \{P_{2,1}\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}$$

$\Pi_{2,2}$ the following derivation

$$\dfrac{\{P_{2,2}\} \Rightarrow \{2 = 1\} \qquad \dfrac{}{\vdash Z := 2 \sim Z := 1 : \{2 = 1\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}}{\vdash Z := 2 \sim Z := 1 : \{P_{2,2}\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}}$$

Let's Ω_1 be the following derivation

$$\frac{\Pi_{1,1} \qquad \Pi_{2,1}}{\begin{array}{c}\vdash \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 1\,\texttt{else}\,Z := 2 \sim Z := 2 \\ : \{X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0 \wedge (X\langle 2\rangle \mod 2 = Z\langle 2\rangle)\} \Rightarrow \{\texttt{Z}\langle 1\rangle = \texttt{Z}\langle 2\rangle\}\end{array}}$$

Let's Ω_2 be the following derivation

$$\frac{\Pi_{1,2} \qquad \Pi_{2,2}}{\begin{array}{c}\vdash \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 1\,\texttt{else}\,Z := 2 \sim Z := 1 \\ : \{X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0 \wedge !(X\langle 2\rangle \mod 2 = Z\langle 2\rangle)\} \Rightarrow \{\texttt{Z}\langle 1\rangle = \texttt{Z}\langle 2\rangle\}\end{array}}$$

Let Σ be the following derivation:

$$\frac{\Omega_1 \qquad \Omega_2}{\begin{array}{c}\vdash \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 1\,\texttt{else}\,Z := 2 \quad \sim \\ \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 2\,\texttt{else}\,Z := 1 \\ : \{X\langle 1\rangle + 1 = X\langle 2\rangle \wedge Z\langle 1\rangle = Z\langle 2\rangle = 0\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}\end{array}}$$

We can then conclude with the following derivation:

$$\frac{X\langle 1\rangle + 1 = X\langle 2\rangle \Rightarrow X\langle 1\rangle + 1 = X\langle 2\rangle \wedge 0 = 0 = 0 \qquad \dfrac{\Sigma}{\begin{array}{c}\vdash Z := 0; \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 1\,\texttt{else}\,Z := 2 \quad \sim \\ Z := 0; \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 2\,\texttt{else}\,Z := 1 \\ : \{X\langle 1\rangle + 1 = X\langle 2\rangle \wedge 0 = 0 = 0\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}\end{array}}}{\begin{array}{c}\vdash Z := 0; \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 1\,\texttt{else}\,Z := 2 \quad \sim \\ Z := 0; \texttt{if}\,(X \mod 2 = Z)\,\texttt{then}\,Z := 2\,\texttt{else}\,Z := 1 \\ : \{X\langle 1\rangle + 1 = X\langle 2\rangle\} \Rightarrow \{Z\langle 1\rangle = Z\langle 2\rangle\}\end{array}}$$