1 4F-1 Bookkeeping

- 0 pts Correct

Peer Review ID: 70896152 — enter this when you fill out your peer evaluation via gradescope

Exercise 4F-2. VCGen for Let [6 points]

Let x_2 be a fresh variable in the following rule.

$$\begin{aligned}
\text{VC}(\text{let } x = e \text{ in } c, B) &= \text{VC}(x_2 := x; x := e; c; x := x_2, B) \\
&= \text{VC}(x_2 := x; x := e; c, \text{VC}(x := x_2, B)) \\
&= \text{VC}(x_2 := x; x := e; c, [x_2/x]B) \\
&= \text{VC}(x_2 := x; x := e, \text{VC}(c, [x_2/x]B)) \\
&= \text{VC}(x_2 := x, \text{VC}(x := e, \text{VC}(c, [x_2/x]B))) \\
&= \text{VC}(x_2 := x, [e/x]\text{VC}(c, [x_2/x]B)) \\
&= [x/x_2][e/x]\text{VC}(c, [x_2/x]B))
\end{aligned}$$

Exercise 4F-3. VCGen Mistakes [6 points]

Considering the following example:

1. $c:$ **let** $x = 1$ **in skip**
2. $B:$ $x > 0$
3. $\sigma:$ $x = 0$

Consider the following situation where we evaluate $\text{VC}(c, B)$ using σ

$$\begin{aligned}
\text{VC}(c, B) &= \text{VC}(\ \textbf{let}\ x = 1\ \textbf{in skip}, B) \\
&= [1/x]\text{VC}(\textbf{skip}, B) \\
&= [1/x]B \\
&= [1/x](x > 0) \\
&= \textbf{True}
\end{aligned}$$

Thus, $\sigma \models \text{VC}(c, B)$ as desired.

Now, let's evaluate σ'.

$$\begin{gathered}
\langle c, \sigma \rangle \Downarrow \sigma' \\
\langle\ \textbf{let}\ x = 1\ \textbf{in skip};, \sigma \rangle \Downarrow \sigma'
\end{gathered}$$

This, consequently gives us $\sigma' = \sigma$ as the command in the *let* does not modify anything. Thus $\sigma' :\ x = 0$.

Now, let's evaluate and show $\sigma' \not\models B$. We know that $\sigma'[x] = 0$. Then, when B checks $x > 0$ it compares $0 > 0$, which is clearly false.

Thus, our let rule is unsound as we have proven a statement that we have just shown is false.

2 4F-2 VCGen for Let

- 0 pts Correct

Peer Review ID: 70896152 — enter this when you fill out your peer evaluation via gradescope

Exercise 4F-2. VCGen for Let [6 points]

Let x_2 be a fresh variable in the following rule.

$$\begin{aligned}
\mathrm{VC}(\text{let } x = e \text{ in } c, B) &= \mathrm{VC}(x_2 := x; x := e; c; x := x_2, B) \\
&= \mathrm{VC}(x_2 := x; x := e; c, \mathrm{VC}(x := x_2, B)) \\
&= \mathrm{VC}(x_2 := x; x := e; c, [x_2/x]B) \\
&= \mathrm{VC}(x_2 := x; x := e, \mathrm{VC}(c, [x_2/x]B)) \\
&= \mathrm{VC}(x_2 := x, \mathrm{VC}(x := e, \mathrm{VC}(c, [x_2/x]B))) \\
&= \mathrm{VC}(x_2 := x, [e/x]\mathrm{VC}(c, [x_2/x]B)) \\
&= [x/x_2][e/x]\mathrm{VC}(c, [x_2/x]B))
\end{aligned}$$

Exercise 4F-3. VCGen Mistakes [6 points]

Considering the following example:

1. $c :$ **let** $x = 1$ **in skip**
2. $B :\ x > 0$
3. $\sigma :\ x = 0$

Consider the following situation where we evaluate $\mathrm{VC}(c, B)$ using σ

$$\begin{aligned}
\mathrm{VC}(c, B) &= \mathrm{VC}(\textbf{ let } x = 1 \textbf{ in skip}, B) \\
&= [1/x]\mathrm{VC}(\textbf{skip}, B) \\
&= [1/x]B \\
&= [1/x](x > 0) \\
&= \textbf{True}
\end{aligned}$$

Thus, $\sigma \vDash \mathrm{VC}(c, B)$ as desired.

Now, let's evaluate σ'.

$$\begin{aligned}
&\langle c, \sigma\rangle \Downarrow \sigma' \\
&\langle \textbf{ let } x = 1 \textbf{ in skip};, \sigma\rangle \Downarrow \sigma'
\end{aligned}$$

This, consequently gives us $\sigma' = \sigma$ as the command in the *let* does not modify anything. Thus $\sigma' :\ x = 0$.

Now, let's evaluate and show $\sigma' \nvDash B$. We know that $\sigma'[x] = 0$. Then, when B checks $x > 0$ it compares $0 > 0$, which is clearly false.

Thus, our let rule is unsound as we have proven a statement that we have just shown is false.

3 4F-3 VCGen Mistakes

- 0 pts Correct

Peer Review ID: 70896152 — enter this when you fill out your peer evaluation via gradescope

Exercise 4F-4. Axiomatic Do-While [6 points]

We just want to somehow encode the information of running c once before we run the while loop stuff. Thus, we have a statement that looks very similar to the while loop rule presented in lecture.

$$\frac{\vdash \{A\}\ c\ \{B\} \qquad \vdash \{B \wedge b\}\ c\ \{B\}}{\vdash \{A\}\ \textbf{do}\ c\ \textbf{while}\ b\ \{B \wedge \neg b\}}$$

Peer Review ID: 70896152 — enter this when you fill out your peer evaluation via gradescope

4 4F-4 Axiomatic Do-While

- 0 pts Correct

Peer Review ID: 70896152 — enter this when you fill out your peer evaluation via gradescope