4F-2. VCGen for Let

Because x is local, any mention of x in the outer postcondition B, once c is done, either makes no sense if x is truly out of scope or refers to some global variable x that is not the same as the local one. Therefore, we need to change the substutition position as follows,

$$VC(\text{let } x = e \text{ in } c, B) = VC([e/x]c, B)$$

4F-3. VCGen Mistakes

Let c be let $x = 0$ in skip, B be $x = 0$ and $\sigma[x] = 3$. Let's calculate the VC(c, B) which is VC(let $x = 0$ in skip, $x = 0$).

$$\begin{aligned} VC(\text{let } x = 0 \text{ in skip}, x = 0) &\equiv [0/x]VC(\text{skip}, x = 0) \\ &\equiv [0/x]x = 0 \\ &\equiv 0 = 0 \\ &\equiv \mathit{true} \end{aligned}$$

And we should also find what is σ'.

$$\begin{aligned} \langle \text{let } x = 0 \text{ in skip}, \sigma \rangle &\to \langle \text{skip; } x := 3, \sigma[x := 0]) \\ &\to \langle x := 3, \sigma(x = 0) \rangle \\ &\to \langle \text{skip}, \sigma(x = 0)[x := 3] \rangle \end{aligned}$$

Then we will have $\sigma'[x] = 3$ after we evaluate the c. Therefore, we have $\sigma \models \mathit{true}$ but $\sigma' \not\models x = 0$. And we can conclude that our VC rule for let is unsound since $\not\models \{VC(c, B)\}\ c\ \{B\}$.

4F-4. Axiomatic Do-While

Here is the Hoare rule for the "do-while" loop. The only difference from the regular while loop here is that we need to have an initial state that first evaluates the c once and then we can apply the loop invariant to the system. Therefore, instead of $A \wedge \neg b \Rightarrow B$ we have $\{A\}\ c\ \{C\}$ and $C \wedge \neg b \Rightarrow B$ and we have the invariant as D.

$$\frac{\vdash \{A\}\ c\ \{C\} \qquad \vdash C \wedge b \Rightarrow D \qquad \vdash \{D\}\ c\ \{C\} \qquad \vdash C \wedge \neg b \Rightarrow B}{\vdash \{A\}\ \text{do } c \text{ while } b\ \{B\}}$$