1 4F-1 Bookkeeping

- 0 pts Correct

Peer Review ID: 70567346 — enter this when you fill out your peer evaluation via gradescope

Exercise 4F-2. VCGen for Let [6 points]. In class we gave the following rules for the (backward) verification condition generation of assignment and let:

$$\begin{aligned}
&\mathrm{VC}(c_1; c_2, B) && = \mathrm{VC}(c_1, \mathrm{VC}(c_2, B)) \\
&\mathrm{VC}(x := e, B) && = [e/x]\ B \\
&\mathrm{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) && = [e/x]\ \mathrm{VC}(c, B)
\end{aligned}$$

That rule for let has a bug. Give a correct rule for let.
First unwind let as follow

$$\mathsf{let}\ x = e\ \mathsf{in}\ c = t := x; x := e; c; x := t$$

Therefore

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

Hence the correct rule is

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

2 4F-2 VCGen for Let

- 0 pts Correct

Exercise 4F-3. VCGen Mistakes [6 points]. Given $\{A\}c\{B\}$ we desire that $A \implies \text{VC}(c, B) \implies \text{WP}(c, B)$. We say that our VC rules are *sound* if $\models \{\text{VC}(c, B)\}\ c\ \{B\}$. Demonstrate the unsoundness of the buggy let rule by giving the following six things:

1. a command c and
2. a post-condition B and
3. a state σ such that
4. $\sigma \models \text{VC}(c, B)$ and
5. $\langle c, \sigma \rangle \Downarrow \sigma'$ but
6. $\sigma' \not\models B$.

Demonstration:

1. $c = \textsf{let } x = 5 \textsf{ in skip}$
2. B is $x = 5$
3. $\sigma(x) = 0$
4. $\sigma \models \text{VC}(c, B)$ because $\text{VC}(c, B)$ is $5 = 5$
5. $\langle c, \sigma \rangle \Downarrow \sigma'$, and we know $\sigma'(x) = 0$ based on the property of let
6. $\sigma' \not\models B$ since $\sigma'(x) = 0$ and $\sigma' \not\models x = 5$

Peer Review ID: 70567346 — enter this when you fill out your peer evaluation via gradescope

3 4F-3 VCGen Mistakes

- 0 pts Correct

Peer Review ID: 70567346 — enter this when you fill out your peer evaluation via gradescope

Exercise 4F-4. Axiomatic Do-While [6 points]. Write a sound and complete Hoare rule for do c while b. This statement has the standard semantics (e.g., c is executed at least once, before b is tested).

We know that

$$\textsf{do } c \textsf{ while } b = c;\ \textsf{while do } c$$

Therefore, we can obtain the Hoare rule for do c while b

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

Peer Review ID: 70567346 — enter this when you fill out your peer evaluation via gradescope

4 4F-4 Axiomatic Do-While

- 0 pts Correct

Peer Review ID: 70567346 — enter this when you fill out your peer evaluation via gradescope