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:

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

That rule for let has a bug. Give a correct rule for let.

Answer:

$$\mathrm{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) = \exists x.\, (x = e \wedge \mathrm{VC}(c, B)).$$

Exercise 4F-3. VCGen Mistakes [6 points]. Given $\{A\}c\{B\}$ we desire that $A \implies \mathrm{VC}(c, B) \implies \mathrm{WP}(c, B)$. We say that our VC rules are *sound* if $\models \{\mathrm{VC}(c, B)\}\ c\ \{B\}$. 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. $\sigma \models \mathrm{VC}(c, B)$ and
5. $\langle c, \sigma\rangle \Downarrow \sigma'$ but
6. $\sigma' \not\models B$.

Answer:

1. **Command:**
$$c\ =\ \mathsf{let}\ x = 0\ \mathsf{in}\ \mathsf{skip}.$$
2. **Post-condition:**
$$B\ =\ (x = 0).$$
3. **State:** Let σ be a state where the global variable x is 1, i.e., $\sigma(x) = 1$.
4. **Verification Condition Holds:**

Using the buggy rule, we have:

$$\mathrm{VC}(c, B) = [0/x]\mathrm{VC}(\mathsf{skip}, x = 0).$$

Since $\mathrm{VC}(\mathsf{skip}, x = 0) = x = 0$, it follows that:

$$\mathrm{VC}(c, B) = [0/x](x = 0) = (0 = 0),$$

which is a true assertion. Thus, $\sigma \models \mathrm{VC}(c, B)$.

Question assigned to the following page: 4

5. Execution:
The execution of c in σ proceeds by binding a *local* x to 0 and executing skip. After the command, the local binding is discarded, leaving the global x unchanged. That is,

$$\langle c, \sigma \rangle \Downarrow \sigma',$$

with $\sigma'(x) = \sigma(x) = 1$.

6. Post-condition Violated:
The post-condition B requires that $x = 0$. However, in the resulting state σ' we have $x = 1$, so:

$$\sigma' \not\models B.$$

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).

Answer: Assume the loop invariant is I.

$$\frac{A \implies I \quad \{I\}\, c\, \{I\} \quad I \wedge \neg b \implies B}{\{A\}\ \mathsf{do}\ c\ \mathsf{while}\ b\ \{B\}}$$

Submission. Turn in the formal component of the assignment as a single PDF document via the `gradescope` website. Your name and Michigan email address must appear on the first page of your PDF submission but may not appear anywhere else.