All subsequent answers should appear after the first page of your submission and may be shared publicly during peer review.

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.

Solution:

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

To arrive at the above rule, we define x_{prev} to be the value of x before the let command, then break the let command into a series of 3 commands, and apply our rules for assigment and commands in series, as shown below.

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

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

Solution:

1. command $c := \mathsf{let}\ x = 5\ \mathsf{in}\ x = 3$
2. post-condition $B := x == 3$
3. state $\sigma := \{(x, 1)\}$
4. $\mathrm{VC}(\mathsf{let}\ x = 5\ \mathsf{in}\ x = 3, x == 3) = (3 == 3)$, and $\sigma \models (3 == 3)$
5. $\langle \mathsf{let}\ x = 5\ \mathsf{in}\ x = 3, \{(x, 1)\}\rangle \Downarrow \{(x, 1)\}$
6. $\{(x, 1)\} \not\models x == 3$

Peer Review ID: 316622200 — enter this when you fill out your peer evaluation via gradescope

Question assigned to the following page: 4

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).

Solution:

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

We use the logic of the for concatenated (semi colon separated) commands and the while to derive the above.

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.

Peer Review ID: 316622200 — enter this when you fill out your peer evaluation via gradescope