1 4F-1 Bookkeeping

- **0 pts** Correct

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.

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

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

2 4F-2 VCGen for Let

- **0 pts** Correct

Let command c be $\mathsf{let}\ x = 2\ \mathsf{in}\ \mathsf{skip}$,
post condition B be $\{x = 2\}$,
and let $\sigma(x) = 4$.
According to the buggy let rule,

$$\begin{aligned} & \sigma \models VC(c, B) \\ = \ & VC(\mathsf{let}\ x = 2\ \mathsf{in}\ \mathsf{skip}, x = 4) \\ = \ & [2/x]\ VC(\mathsf{skip}, x = 4) \\ = \ & VC(\mathsf{skip}, x = 2) \\ = \ & (x = 2) \end{aligned}$$

According to our operational semantics rules in homework 1, when $\sigma(x) = 4$:

$$\frac{\langle 2, \sigma \Downarrow 2\rangle \quad \langle \mathsf{skip}, \sigma[x := 2]\rangle \Downarrow \sigma[x := 2]}{\langle \mathsf{let}\ x = 2\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma[x := 4]}$$

Thus $x = 4$ in σ' while B is $x = 2$. Therefore, $\sigma' \not\models B$.

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

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

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.

3 4F-3 VCGen Mistakes

- **0 pts** Correct

Let command c be $\mathsf{let}\ x = 2\ \mathsf{in}\ \mathsf{skip}$,
post condition B be $\{x = 2\}$,
and let $\sigma(x) = 4$.
According to the buggy let rule,

$$\begin{aligned} & \sigma \models VC(c, B) \\ = \ & VC(\mathsf{let}\ x = 2\ \mathsf{in}\ \mathsf{skip}, x = 4) \\ = \ & [2/x]\ VC(\mathsf{skip}, x = 4) \\ = \ & VC(\mathsf{skip}, x = 2) \\ = \ & (x = 2) \end{aligned}$$

According to our operational semantics rules in homework 1, when $\sigma(x) = 4$:

$$\frac{\langle 2, \sigma \Downarrow 2\rangle \quad \langle \mathsf{skip}, \sigma[x := 2]\rangle \Downarrow \sigma[x := 2]}{\langle \mathsf{let}\ x = 2\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma[x := 4]}$$

Thus $x = 4$ in σ' while B is $x = 2$. Therefore, $\sigma' \not\models B$.

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

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

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.

4 4F-4 Axiomatic Do-While

- **0 pts** Correct