1 4F-1 Bookkeeping

- **0 pts** Correct

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: Let α be some symbol that is not an IMP variable.

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

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

Solution:

1. Let c be $\mathsf{let}\ x := 2\ \mathsf{in}\ \mathsf{skip}$
2. Let B be $x = 2$.
3. Let $\sigma(\alpha) = 0\ \forall \alpha$
4. In our buggy VC,

$$\begin{array}{rl} \mathrm{VC}(c, B) & = [2/x]\ \mathrm{VC}(\mathsf{skip}, B) \\ & = [2/x]\ B \\ & = [2/x]\ (x = 2) \\ & = (2 = 2) \\ & = \mathsf{true} \end{array}$$

2 4F-2 VCGen for Let

- **0 pts** Correct

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: Let α be some symbol that is not an IMP variable.

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

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

Solution:

1. Let c be $\mathsf{let}\ x := 2\ \mathsf{in}\ \mathsf{skip}$
2. Let B be $x = 2$.
3. Let $\sigma(\alpha) = 0\ \forall \alpha$
4. In our buggy VC,

$$\begin{array}{rl} \mathrm{VC}(c, B) & = [2/x]\ \mathrm{VC}(\mathsf{skip}, B) \\ & = [2/x]\ B \\ & = [2/x]\ (x = 2) \\ & = (2 = 2) \\ & = \mathsf{true} \end{array}$$

and, $\sigma \models \mathsf{true}$

5. $\langle c, \sigma \rangle \Downarrow \sigma$, as our c let command does nothing.
6. However, $\sigma(x) = 0 \neq 2$, so $\sigma \not\models B$

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).

Solution:

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

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

and, $\sigma \models \mathsf{true}$

5. $\langle c, \sigma \rangle \Downarrow \sigma$, as our c let command does nothing.
6. However, $\sigma(x) = 0 \neq 2$, so $\sigma \not\models B$

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).

Solution:

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

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