1 4F-1 Bookkeeping

- 0 pts Correct

Peer Review ID: 70736538 — 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:

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

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

Answer 4F-2

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

Answer 4F-3

command c: let x = (2 * 3) in y = x + 7
post-condition B: $x > 5$
state σ: $\sigma(x) = 3$

This state σ matches VC(c, B) by the buggy let rule because VC(c, B) is that $e > 5$, and $e = 2 * 3 = 6 > 5$.

state σ': $\sigma'(x) = 3, \sigma'(y) = 13$
However, we see that $\sigma'(x) = 3 < 5$ which does not meet the post-condition B that $\sigma'(x) > 5$.

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).

2 4F-2 VCGen for Let

- 0 pts Correct

Peer Review ID: 70736538 — 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.

Answer 4F-2

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

Answer 4F-3

command c: let x = (2 * 3) in y = x + 7
post-condition B: $x > 5$
state σ: $\sigma(x) = 3$

This state σ matches VC(c, B) by the buggy let rule because VC(c, B) is that $e > 5$, and $e = 2 * 3 = 6 > 5$.

state σ': $\sigma'(x) = 3, \sigma'(y) = 13$
However, we see that $\sigma'(x) = 3 < 5$ which does not meet the post-condition B that $\sigma'(x) > 5$.

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).

3 4F-3 VCGen Mistakes

- 0 pts Correct

Peer Review ID: 70736538 — enter this when you fill out your peer evaluation via gradescope

Answer 4F-4

We use the fact that a do-while loop is essentially the same as executing the command and then a while loop.

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

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

Peer Review ID: 70736538 — enter this when you fill out your peer evaluation via gradescope