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.

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

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

Ans: If we follow the given rule:

1. $c := let\ x = 0\ in\ x = x - 1$
2. $B := x < 0$
3. $\sigma\{x\} = 1$
4. $\sigma \models \mathrm{VC}(c, B)$ as $\models [0/x]\ \mathrm{VC}(x = x - 1, B)$
5. but, $\langle c, \sigma\rangle \Downarrow \sigma' \Rightarrow \sigma'\{x\} = 1$
6. Therefore $\sigma' \not\models B$

Which results in a contradiction. Therefore, given *let* is buggy.

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).

Ans:

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

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.

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

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

Ans: If we follow the given rule:

1. $c := let\ x = 0\ in\ x = x - 1$
2. $B := x < 0$
3. $\sigma\{x\} = 1$
4. $\sigma \models \mathrm{VC}(c, B)$ as $\models [0/x]\ \mathrm{VC}(x = x - 1, B)$
5. but, $\langle c, \sigma\rangle \Downarrow \sigma' \Rightarrow \sigma'\{x\} = 1$
6. Therefore $\sigma' \not\models B$

Which results in a contradiction. Therefore, given *let* is buggy.

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).

Ans:

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

3 4F-3 VCGen Mistakes

- **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.

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

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

Ans: If we follow the given rule:

1. $c := let\ x = 0\ in\ x = x - 1$
2. $B := x < 0$
3. $\sigma\{x\} = 1$
4. $\sigma \models \mathrm{VC}(c, B)$ as $\models [0/x]\ \mathrm{VC}(x = x - 1, B)$
5. but, $\langle c, \sigma\rangle \Downarrow \sigma' \Rightarrow \sigma'\{x\} = 1$
6. Therefore $\sigma' \not\models B$

Which results in a contradiction. Therefore, given *let* is buggy.

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).

Ans:

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

4 4F-4 Axiomatic Do-While

- **0 pts** Correct