1 4F-1 Bookkeeping

- 0 pts Correct

4F-2. A correct rule for let is given by

$$\mathrm{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) = [x/y][e/x]\ \mathrm{VC}(c, [y/x]B),\ \text{where } y \text{ is fresh.}$$

4F-3. The unsoundness of the buggy let rule is apparent from the following:

1. (a command c) $\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}$
2. (a post condition B) $x = 1$
3. (a state σ) $[x := 0]$
4. (that $\sigma \models \mathrm{VC}(c, B)$) Using the buggy let rule and the rule for skip, we see that

   $$\mathrm{VC}(\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, x = 1) = [1/x]VC(\mathsf{skip}, x = 1) = [1/x](x = 1) = (1 = 1) = true,$$

   so indeed

   $$\sigma \models \mathrm{VC}(\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, x = 1).$$

5. (that $\langle c, \sigma\rangle \Downarrow \sigma'$) Applying the operational semantics rule for let and skip, we have the following derivation tree

   $$\frac{\overline{\langle 1, \sigma\rangle \Downarrow 1} \quad \overline{\langle \mathsf{skip}, \sigma[x := 1]\rangle \Downarrow \sigma[x := 1]}}{\langle \mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma[x := 1][x := \sigma(x)]}.$$

   Since $\sigma[x := 1][x := \sigma(x)] = \sigma$, this gives that

   $$\langle \mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma'$$

   with $\sigma' = \sigma$.
6. (that $\sigma' \not\models B$) Since $\sigma'(x) = \sigma(x) = 0$, we see that $\langle x, \sigma'\rangle \Downarrow 0$ and $\langle 1, \sigma'\rangle \Downarrow 1$, thus $0 \neq 1$ implies $\sigma' \not\models (x = 1)$ as desired.

4F-4. We give the following sound and complete Hoare rule for do c while b:

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

Peer Review ID: 67844295 — enter this when you fill out your peer evaluation via gradescope

2 4F-2 VCGen for Let

- 0 pts Correct

4F-2. A correct rule for let is given by

$$\text{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) = [x/y][e/x]\ \text{VC}(c, [y/x]B),\ \text{where } y \text{ is fresh.}$$

4F-3. The unsoundness of the buggy let rule is apparent from the following:

1. (a command c) $\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}$
2. (a post condition B) $x = 1$
3. (a state σ) $[x := 0]$
4. (that $\sigma \models \text{VC}(c, B)$) Using the buggy let rule and the rule for skip, we see that

   $$\text{VC}(\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, x = 1) = [1/x]VC(\mathsf{skip}, x = 1) = [1/x](x = 1) = (1 = 1) = true,$$

   so indeed

   $$\sigma \models \text{VC}(\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, x = 1).$$

5. (that $\langle c, \sigma\rangle \Downarrow \sigma'$) Applying the operational semantics rule for let and skip, we have the following derivation tree

   $$\frac{\overline{\langle 1, \sigma\rangle \Downarrow 1} \quad \overline{\langle \mathsf{skip}, \sigma[x := 1]\rangle \Downarrow \sigma[x := 1]}}{\langle \mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma[x := 1][x := \sigma(x)]}.$$

   Since $\sigma[x := 1][x := \sigma(x)] = \sigma$, this gives that

   $$\langle \mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma'$$

   with $\sigma' = \sigma$.
6. (that $\sigma' \not\models B$) Since $\sigma'(x) = \sigma(x) = 0$, we see that $\langle x, \sigma'\rangle \Downarrow 0$ and $\langle 1, \sigma'\rangle \Downarrow 1$, thus $0 \neq 1$ implies $\sigma' \not\models (x = 1)$ as desired.

4F-4. We give the following sound and complete Hoare rule for do c while b:

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

Peer Review ID: 67844295 — enter this when you fill out your peer evaluation via gradescope

3 4F-3 VCGen Mistakes

- 0 pts Correct

4F-2. A correct rule for let is given by

$$\mathrm{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) = [x/y][e/x]\ \mathrm{VC}(c, [y/x]B),\ \text{where } y \text{ is fresh.}$$

4F-3. The unsoundness of the buggy let rule is apparent from the following:

1. (a command c) $\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}$
2. (a post condition B) $x = 1$
3. (a state σ) $[x := 0]$
4. (that $\sigma \models \mathrm{VC}(c, B)$) Using the buggy let rule and the rule for skip, we see that

   $$\mathrm{VC}(\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, x = 1) = [1/x]VC(\mathsf{skip}, x = 1) = [1/x](x = 1) = (1 = 1) = true,$$

   so indeed

   $$\sigma \models \mathrm{VC}(\mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, x = 1).$$

5. (that $\langle c, \sigma\rangle \Downarrow \sigma'$) Applying the operational semantics rule for let and skip, we have the following derivation tree

   $$\frac{\overline{\langle 1, \sigma\rangle \Downarrow 1} \quad \overline{\langle \mathsf{skip}, \sigma[x := 1]\rangle \Downarrow \sigma[x := 1]}}{\langle \mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma[x := 1][x := \sigma(x)]}.$$

   Since $\sigma[x := 1][x := \sigma(x)] = \sigma$, this gives that

   $$\langle \mathsf{let}\ x = 1\ \mathsf{in}\ \mathsf{skip}, \sigma\rangle \Downarrow \sigma'$$

   with $\sigma' = \sigma$.
6. (that $\sigma' \not\models B$) Since $\sigma'(x) = \sigma(x) = 0$, we see that $\langle x, \sigma'\rangle \Downarrow 0$ and $\langle 1, \sigma'\rangle \Downarrow 1$, thus $0 \neq 1$ implies $\sigma' \not\models (x = 1)$ as desired.

4F-4. We give the following sound and complete Hoare rule for $\mathsf{do}\ c\ \mathsf{while}\ b$:

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

Peer Review ID: 67844295 — enter this when you fill out your peer evaluation via gradescope

4 4F-4 Axiomatic Do-While

- 0 pts Correct