

14F-1 Bookkeeping

- 0 pts Correct

Exercise 4F-2. VCGen for Let

VCGen for the let presented in the Exercise 4F-2 has a bug because it does not consider the original value of x in the let rule. So, assume that there is a fresh variable called $temp$ which stores the original value of x . Then, if we can express $VC(\text{let } x = e \text{ in } c, B)$ using the fresh variable $temp$ and simplify it, then it will be as a following:

$$\begin{aligned} & VC(\text{let } x = e \text{ in } c, B) \\ &= VC(\text{temp} = x; x = e; c; x = \text{temp}, B) \\ &= VC(\text{temp} = x, VC(x = e; c; x = \text{temp}, B)) \\ &= [x / \text{temp}] VC(x = e; c; x = \text{temp}, B) \\ &= [x / \text{temp}] VC(x = e, VC(c; x = \text{temp}, B)) \\ &= [x / \text{temp}] [e / x] VC(c; x = \text{temp}, B) \\ &= [x / \text{temp}] [e / x] VC(c, VC(x = \text{temp}, B)) \\ &= [x / \text{temp}] [e / x] VC(c, [\text{temp} / x] B) \end{aligned}$$

Therefore, as a result, the correct VCGen for let should be $[x / \text{temp}] [e / x] VC(c, [\text{temp} / x] B)$.

2 4F-2 VCGen for Let

- 0 pts Correct

Exercise 4F-3. VCGen Mistakes

1. A command c is $\text{let } x = j \text{ in skip}$, where j is an arbitrary integer, and
2. a post-condition B is $x = j$, and
3. a state σ such that $\sigma(x) = i$, where i is an arbitrary integer and $i \neq j$.
4. Then, $\sigma \models \text{VC}(c, B)$ because $\text{VC}(c, B)$ is j .
5. $\langle c, \sigma \rangle \Downarrow \sigma_1$, but $\sigma_1(x) = i$ because x needs to be reassigned with its original value after let rule.
6. Therefore, $\sigma_1 \not\models B$ because $\sigma_1(x) = i$ but the post-condition B is $x = j$.

Because the buggy rule does not recover x with its original value after the let rule, it is problematic.

3 4F-3 VCGen Mistakes

- 0 pts Correct

Exercise 4F-4. Axiomatic Do-While

Because c is executed at least once, before b is tested as described in the Exercise 4F-4, we can express $\text{do } c \text{ while } b$ into the following way: $\text{do } c \text{ while } b = c; \text{ while } b \text{ do } c$. Therefore, by using the following way, we can write a sound and complete Hoare rule for $\text{do } c \text{ while } b$ as below.

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

4 4F-4 Axiomatic Do-While

- 0 pts Correct