1 5F-1 Bookkeeping

- **0 pts** Correct

Exercise 5F-2. VCGen Do-While

I chose the first option: Give the (backward) verification condition formula for the command $\underline{\text{do}_{Inv}\ c\ \text{while}\ b}$ with respect to a post-condition P. The invariant Inv is true before each evaluation of the predicate b. Your answer may not be defined in terms of VC(while...).

$$\begin{aligned}\text{VC}(\text{do}_{Inv}\ c\ \text{while}\ b, P) &= \text{VC}(c; \text{while}_{Inv}\ \text{do}\ c, P) \\ &= \text{VC}(c, \text{VC}(\text{while}_{Inv}\ \text{do}\ c, P)) \\ &= \text{VC}(c, Inv \wedge (\forall x_1 \ldots x_n.\, Inv \Rightarrow (b \Rightarrow \text{VC}(c, Inv) \wedge \neg b \Rightarrow P))\end{aligned}$$

where $x_1, \ldots, x_n$ are all the variables modified in c

2 5F-2 VCGen Do-While

- **0 pts** Correct

Exercise 5F-3. VCGen Mistakes

Only the lannister rule is complete. We will show that the other two rules are incomplete by using this example from Lecture 8: $\{x \leq 0\}$ while $x \leq 5$ do $x := x + 1$ $\{x = 6\}$. Breaking it up, we have

- A is $\underline{x \leq 0}$
- B is $\underline{x = 6}$
- $\sigma(x) = 0$
- $\sigma'(x) = 6$
- c is $\underline{\text{while } x \leq 5 \text{ do } x := x + 1}$
- $\langle c, \sigma \rangle \Downarrow \sigma'$ can be verified mathematically
- $\sigma \vDash A$ because $\sigma(x) = 0 \leq 0$
- $\sigma' \vDash B$ because $\sigma'(x) = 6 = 6$

The startk rule and the targaryen are incomplete because it is not possible to use them to prove $\{x \leq 0\}$ while $x \leq 5$ do $x := x + 1$ $\{x = 6\}$. We will show this by contradiction.

The Stark Rule

Assume that the start rule is complete, there exists a derivation D such that

$$D :: \ \{x \leq 0\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{x = 6\}$$

By inversion, the last rule used in D is either the stark rule or the rule of consequence. However, the last rule cannot be the stark rule, because the stark rule requires A and B to be identitcal.

This means that the last rule used must have been the rule of consequence. Then,

$$D :: \ \frac{\vdash x \leq 0 \Rightarrow C1 \quad D1 :: \ \vdash \{C1\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{C2\} \quad \vdash C2 \Rightarrow \{x = 6\}}{\{x \leq 0\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{x = 6\}}$$

Since D1 must be using the stark rule, we have $C1 = C2$. However, we cannot find a $C = C1 = C2$ such that $(x \leq 0) \Rightarrow C \Rightarrow (x = 6)$. A contradiction.

Hence, the stark rule is incomplete.

The Targaryen Rule

Similarly, if the targaryen rule is complete, there exists a derivation D such that

$$D :: \{x \leq 0\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{x = 6\}$$

By inversion, the last rule used in D is either the targaryen rule or the rule of consequence. However, the last rule cannot be the targaryen rule, because the targaryen rule requires B to be $A \wedge \neg b$, and $x = 6$ is not $x \leq 0 \wedge \neg(x \leq 5)$.

This means that the last rule used must have been the rule of consequence.

$$D :: \frac{\vdash x \leq 0 \Rightarrow C1 \quad D1 :: \ \vdash \{C1\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{C2\} \quad \vdash C2 \Rightarrow \{x = 6\}}{\{x \leq 0\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{x = 6\}}$$

Since D1 must be using the targaryen rule, we have

$$D1 :: \frac{\vdash D2 :: \ \{C1\}x := x + 1\{C1\}}{\vdash \{C1\} \text{ while } x \leq 5 \text{ do } x := x + 1 \ \{C2\}},$$

where $C2 = C1 \wedge \neg(x \leq 5)$. However, there is no sound $D2$ that derives $\{C1\}x := x + 1\{C1\}$. A contradiction.

Hence, the targaryen rule is incomplete.

3 5F-3 VCGen Mistakes

- **0 pts** Correct