1 5F-1 Bookkeeping

- **0 pts** Correct

Peer Review ID: 72903042 — enter this when you fill out your peer evaluation via gradescope

Exercise 5F-2

I'm choosing the first option, writing the backwards verification condition formula for the command $\texttt{do}_{Inv}\ c\ \texttt{while}\ b$ with respect to the post-condition P. This is very similar to the formula for the normal `while` command, except that the condition when entering the loop is different:

$$\mathrm{VC}(\texttt{do}_{Inv}\ c\ \texttt{while}\ b, P) = VC(c, Inv) \wedge (\forall x_1 ... x_n.\ (b \Rightarrow \mathrm{VC}(c, Inv)) \wedge (\neg b \Rightarrow P))$$

Essentially, we need $\mathrm{VC}(c, Inv)$ to hold at the start, since we'll run c at least once. From there, for all possible states inside the loop, we need to be able to either run the loop again and still have Inv hold, or we need to be able to exit the loop with the post-condition P.

2 5F-2 VCGen Do-While

- **- 0 pts** Correct

Exercise 5F-3

Incompleteness of “stark”

We make the following definitions:

$$\begin{array}{cc} A = (x = 1) & \sigma = \{x = 1\} \\ B = (x = 5) & \sigma' = \{x = 5\} \end{array}$$
$$c = (\texttt{while}\ x < 5\ \texttt{do}\ x := x + 1)$$

Clearly, $\sigma \models A$ and $\sigma' \models B$. And also, if $x = 1$ to start, the while loop will always run until $x = 5$. So $\langle c, \sigma \rangle \Downarrow \sigma'$. However, the “stark” rule only allows us to demonstrate properties about a while loop when the pre- and post-conditions are the same. As such, if we wanted to demonstrate:

$$\vdash \{A\}\ c\ \{B\}$$

Then we would need to find some property X where we could use the rule of consequence alongside the “stark” rule:

$$\frac{\vdash A \Rightarrow X \quad \vdash \{X\}\ c\ \{X\} \quad \vdash X \Rightarrow B}{\vdash \{A\}\ c\ \{B\}}$$

However, there is no such property X where $(x = 1) \Rightarrow X$ and $X \Rightarrow (x = 5)$. So we cannot demonstrate what we want with the “stark” rule, and it must be incomplete.

Incompleteness of “targaryen”

We make the following definitions:

$$A = B = (x = 0 \land y = 0)$$
$$\sigma = \sigma' = \{x = 0, y = 0\}$$
$$c = (\texttt{while}\ y = 1\ \texttt{do}\ x := 1)$$

Clearly, $\sigma \models A$ and $\sigma' \models B$. And since $y = 0$ in σ, the `while` loop body never runs if the starting state is σ, so we have $\langle c, \sigma \rangle \Downarrow \sigma'$. However, using the “targaryen” rule, if we wanted to show:

$$\vdash \{A\}\ c\ \{B\}$$

Which is equivalent to:

$$\vdash \{A\}\ c\ \{A \wedge (y \neq 1)\}$$

Then we would need to demonstrate:

$$\vdash \{A\}\ x := 1\ \{A\}$$

This can't be done, since $A = (x = 0 \wedge y = 0)$ obviously cannot hold if we set $x := 1$. Therefore, the "targaryen" rule is incomplete.

3 5F-3 VCGen Mistakes

- 0 pts Correct