1 5F-1 Bookkeeping

- 0 pts Correct

Peer Review ID: 72890627 — enter this when you fill out your peer evaluation via gradescope

Exercise 5F-2. VCGen Do-While [8 points]

We know that **do**. . . **while** is equivalent to executing c once before we check the condition b. Thus we can say

$$\begin{aligned}\textbf{VC}(\ \textbf{do}\ c\ \textbf{while}\ b, \text{Inv}) &= \textbf{VC}(c; \textbf{while}\ b\ \textbf{do}\ c\ , \text{Inv}) \\ &= \textbf{VC}(c, \textbf{VC}(\textbf{while}\ b\ \textbf{do}\ c\ , \text{Inv}))\end{aligned}$$

Then we convert and substitute to get the following

$$\textbf{VC}(\ \textbf{do}_{\text{Inv}}\ c\ \textbf{while}\ b) = \textbf{VC}(c, \text{Inv}) \wedge (\forall x_1 \ldots x_n . \text{Inv} \Rightarrow (b \Rightarrow \textbf{VC}(c, \text{Inv}) \wedge \neg b \Rightarrow B))$$

2 5F-2 VCGen Do-While

- 0 pts Correct

Peer Review ID: 72890627 — enter this when you fill out your peer evaluation via gradescope

VCGen Mistakes [20 points]

We provide two examples of incompleteness for **stark** and **targaryen**

We begin by presenting a counterexample for the completeness of stark.

1. Stark
2. $A : x = 0$
3. $B : x = 2$
4. $\sigma = \{x : 0\}$
5. $\sigma' = \{x : 2\}$
6. $c :$ **while** $x < 2$ **do** $x := x + 1$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$
8. $\sigma \vDash A$
9. $\sigma' \vDash B$
10. It is not possible to prove $\vdash \{A\}\ c\ \{B\}$

First, let's show that this stark rule is provable using the rule of consequence and the correct while rule as presented in lecture

$$\text{Correct While Rule: } \frac{\vdash \{X \wedge b\}\ c\ \{X\}}{\vdash \{X\}\textbf{while } b \textbf{ do } c\ \{X \wedge \neg b\}}$$

$$\text{Rule of Consequence : } \frac{\vdash X' \Rightarrow X \qquad \vdash \{X\}\ c\ \{Y\} \qquad \vdash Y \Rightarrow Y'}{\vdash \{X'\}\ c\ \{Y'\}}$$

.

Due to the constraints of paper space, note that when I write c in the below formula I mean

$$c \equiv \textbf{while } x < 2 \textbf{ do } x := x + 1$$

$$\frac{\vdash \{x = 0\} \Rightarrow \{x \leq 2\} \qquad \vdash \{x \leq 2\}\ c\ \{x \leq 2 \wedge x \not< 2\} \qquad \vdash x \leq 2 \wedge x \not< 2 \Rightarrow x = 2}{\vdash \{x = 0\}\ c\ \{x = 2\}}$$

$$\frac{\vdash \{x \leq 2 \wedge x < 2\} x := x + 1 \{x \leq 2\}}{\vdash \{x \leq 2\} \textbf{while } x < 2 \textbf{ do } x := x + 1 \{x \leq 2 \wedge \not< 2\}}$$

We can observe that all the statements in the consequence line are trivially provable except the middle one. By applying our correct while rule, we can see that it is indeed provable as well. Thus, we say that the correct while rule can prove the example provided by applying the rule of conseuquence.

Now, let's observe what happens if we were to use the stark rule.

$$\text{Incomplete stark Rule: } \frac{\vdash \{X \wedge b\}\ c\ \{X\}}{\vdash \{X\} \textbf{while } b \textbf{ do } c\ \{X\}}$$

We end up with no way to choose X or Y in our rule of consequence such that all of $\vdash \{x = 0\} \Rightarrow X$, $\vdash \{X\}\ c\ \{Y\}$, and $\vdash Y \Rightarrow \{x = 2\}$ can be satisfied. This is because the stark rule will only apply if $X = Y$, and there are no statements X s.t. $x = 0 \Rightarrow X \Rightarrow x = 2$.

Now, we provide a counterexample for the completeness of the targaryen rule.

1. Targaryen
2. $A : x = 0$
3. $B : x = 2$
4. $\sigma = \{x : 0\}$
5. $\sigma' = \{x : 2\}$
6. $c :$ **while** $x < 2$ **do** $x := x + 1$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$
8. $\sigma \vDash A$
9. $\sigma' \vDash B$
10. It is not possible to prove $\vdash \{A\}\ c\ \{B\}$

Since these are the exact same values as provided above, we already know that this is provable using the correct while rule and the consequence rule. Let's observe why the proof fails to work for the incorrect targaryen rule

$$\text{Incomplete targaryen Rule: } \frac{\vdash \{X\}\ c\ \{X\}}{\vdash \{X\}\textbf{while } b \textbf{ do } c\ \{X \land \neg b\}}$$

If we were to attempt the same proof as the correct while rule, we would find that the targaryen rule would not be able to actually prove the while statement. This is because $\nvdash \{x \leq 2\} x := x{+}1 \{x \leq 2\}$. Since x is being incremented, it's possible for it to no longer be ≤ 2. The only way we could guarantee the statement holds after incrementing x is if we were to lower bound x instead. However, that would end up giving us 2 lower bounds on x, which would not be enough to pin x at a specific value of 2.

Peer Review ID: 72890627 — enter this when you fill out your peer evaluation via gradescope

3 5F-3 VCGen Mistakes

- 0 pts Correct

Peer Review ID: 72890627 — enter this when you fill out your peer evaluation via gradescope