1 5F-1 Bookkeeping

- 0 pts Correct

5F-2

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

5F-3

For the rule $\textsf{stark}$:

$$\begin{aligned} A &= (x = 0) \\ B &= (x \neq 0) \\ \sigma &= [x := 0] \\ \sigma' &= [x := 1] \\ c &= \textsf{while } x = 0 \textsf{ do } x := 1 \end{aligned}$$

This evaluates as shown in the following example with big-step semantics (Aexp and Bexp evaluation omitted for brevity)

$$\dfrac{\dfrac{...}{< x = 0, [x := 0] > \Downarrow \textsf{true}} \quad \dfrac{\dfrac{...}{< x := 1, [x := 0] > \Downarrow [x := 1]} \quad \dfrac{\dfrac{...}{< x = 0, [x := 1] > \Downarrow \textsf{false}}}{< \textsf{while } x = 0 \textsf{ do } x := 1, [x := 1] > \Downarrow [x := 1]}}{< x := 1; \textsf{while } x = 0 \textsf{ do } x := 1, [x := 1] > \Downarrow [x := 1]}}{< \textsf{while } x = 0 \textsf{ do } x := 1, [x := 0] > \Downarrow [x := 1]}$$

But with the condition X as both a precondition and postcondition in the rule, it is not possible for this to be proven using the rule $\textsf{stark}$ unless A and B are eqivalent, which is not the case here. The expression $\{x = 0 \wedge x = 0\}\ x := 1\ \{x = 0\}$ is not provable.

The above example also works for the rule $\textsf{targaryen}$ as the expression $\{x = 0\}\ x := 1\ \{x = 0\}$ is not provable.

Neither of these rules account for the condition X no longer being satisfied after evaluation of c.

2 5F-2 VCGen Do-While

- 0 pts Correct

Peer Review ID: 72806494 — enter this when you fill out your peer evaluation via gradescope

5F-2

$$\mathrm{VC}(\textsf{do } c \textsf{ while } b, B) = Inv \wedge \mathrm{VC}(c, Inv) \wedge (\forall x_1 ... x_n . Inv \rightarrow (b \Rightarrow \mathrm{VC}(c, Inv) \wedge \neg b \Rightarrow B))$$

5F-3

For the rule $\textsf{stark}$:

$$\begin{aligned} A &= (x = 0) \\ B &= (x \neq 0) \\ \sigma &= [x := 0] \\ \sigma' &= [x := 1] \\ c &= \textsf{while } x = 0 \textsf{ do } x := 1 \end{aligned}$$

This evaluates as shown in the following example with big-step semantics (Aexp and Bexp evaluation omitted for brevity)

$$\dfrac{\dfrac{...}{< x = 0, [x := 0] >\Downarrow \textsf{true}} \qquad \dfrac{\dfrac{...}{< x := 1, [x := 0] >\Downarrow [x := 1]} \qquad \dfrac{\dfrac{...}{< x = 0, [x := 1] >\Downarrow \textsf{false}}}{< \textsf{while } x = 0 \textsf{ do } x := 1, [x := 1] >\Downarrow [x := 1]}}{< x := 1; \textsf{while } x = 0 \textsf{ do } x := 1, [x := 1] >\Downarrow [x := 1]}}{< \textsf{while } x = 0 \textsf{ do } x := 1, [x := 0] >\Downarrow [x := 1]}$$

But with the condition X as both a precondition and postcondition in the rule, it is not possible for this to be proven using the rule $\textsf{stark}$ unless A and B are eqivalent, which is not the case here. The expression $\{x = 0 \wedge x = 0\}\ x := 1\ \{x = 0\}$ is not provable.

The above example also works for the rule $\textsf{targaryen}$ as the expression $\{x = 0\}\ x := 1\ \{x = 0\}$ is not provable.

Neither of these rules account for the condition X no longer being satisfied after evaluation of c.

3 5F-3 VCGen Mistakes

- 0 pts Correct

Peer Review ID: 72806494 — enter this when you fill out your peer evaluation via gradescope