1 5F-1 Bookkeeping

- 0 pts Correct

Peer Review ID: 72793226 — enter this when you fill out your peer evaluation via gradescope

gradescope

Exercise 5F-2. VCGen Do-While.

The following answer is for **option 2**.

According to the description, the statement

$$\mathsf{do}_{Inv1,Inv2}\ c\ \mathsf{while}\ b$$

is equivalent to the sequential statements

$$\mathsf{assert}(Inv1);\ c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c$$

Hence the result is

$$\begin{aligned}
&\mathrm{VC}(\mathsf{do}_{Inv1,Inv2}\ c\ \mathsf{while}\ b, P)\\
&\equiv \mathrm{VC}(\mathsf{assert}(Inv1);\ c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c)\\
&\equiv \mathrm{VC}(\mathsf{assert}(Inv1), \mathrm{VC}(c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c))\\
&\equiv Inv1 \wedge \mathrm{VC}(c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c)\\
&\equiv Inv1 \wedge \mathrm{VC}(c, \mathrm{VC}(\mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c))\\
&\equiv Inv1 \wedge \mathrm{VC}(c, Inv2 \wedge (\forall x_1, \cdots, x_n.\ Inv2 \Rightarrow (b \Rightarrow \mathrm{VC}(c, Inv2) \wedge (\neg b \Rightarrow P))))
\end{aligned}$$

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

Exercise 5F-3. VCGen Mistakes.

stark

1. stark
2. $A = x < 6$
3. $B = x \geq 6$
4. $\sigma(x) = 0$
5. $\sigma'(x) = 6$
6. $c = \mathsf{while}\ x < 6\ \mathsf{do}\ x := 6$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$ since the $\sigma(x) = 0 < 6$ and the loop body just sets x to $6 \geq 6$
8. $\sigma(x) = 0 < 6$ and hence $\sigma \models A$
9. $\sigma'(x) = 6 \geq 6$ and hence $\sigma' \models B$
10. it is not possible to prove $\vdash \{A\}\ c\ \{B\}$

Peer Review ID: 72793226 — enter this when you fill out your peer evaluation via gradescope

2 5F-2 VCGen Do-While

- 0 pts Correct

Exercise 5F-2. VCGen Do-While.

The following answer is for **option 2**.

According to the description, the statement

$$\mathsf{do}_{Inv1,Inv2}\ c\ \mathsf{while}\ b$$

is equivalent to the sequential statements

$$\mathsf{assert}(Inv1);\ c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c$$

Hence the result is

$$\begin{aligned}
&\mathrm{VC}(\mathsf{do}_{Inv1,Inv2}\ c\ \mathsf{while}\ b, P) \\
&\equiv \mathrm{VC}(\mathsf{assert}(Inv1);\ c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c) \\
&\equiv \mathrm{VC}(\mathsf{assert}(Inv1), \mathrm{VC}(c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c)) \\
&\equiv Inv1 \wedge \mathrm{VC}(c;\ \mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c) \\
&\equiv Inv1 \wedge \mathrm{VC}(c, \mathrm{VC}(\mathsf{while}_{Inv2}\ b\ \mathsf{do}\ c)) \\
&\equiv Inv1 \wedge \mathrm{VC}(c, Inv2 \wedge (\forall x_1, \cdots, x_n.\ Inv2 \Rightarrow (b \Rightarrow \mathrm{VC}(c, Inv2) \wedge (\neg b \Rightarrow P))))
\end{aligned}$$

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

Exercise 5F-3. VCGen Mistakes.

stark

1. stark
2. $A = x < 6$
3. $B = x \geq 6$
4. $\sigma(x) = 0$
5. $\sigma'(x) = 6$
6. $c = \mathsf{while}\ x < 6\ \mathsf{do}\ x := 6$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$ since the $\sigma(x) = 0 < 6$ and the loop body just sets x to $6 \geq 6$
8. $\sigma(x) = 0 < 6$ and hence $\sigma \models A$
9. $\sigma'(x) = 6 \geq 6$ and hence $\sigma' \models B$
10. it is not possible to prove $\vdash \{A\}\ c\ \{B\}$

Peer Review ID: 72793226 — enter this when you fill out your peer evaluation via gradescope

We will show that it is not possible to use stark to prove $\{x < 6\}$ while $x < 6$ do $x := 6$ $\{x \geq 6\}$ by contradiction. Suppose it is possible to do so, we have

$$D :: \ \vdash \{x < 6\} \ \textsf{while} \ x < 6 \ \textsf{do} \ x := 6 \ \{x \geq 6\}$$

where D is some derivation. By inversion, the last rule of D must be either stark or the rule of consequence. the last rule was stark, we have that $x < 6$ and $x \geq 6$ have the same form, which is an obvious contradiction. If the last rule was the rule of consequence, we have

$$D :: \frac{\vdash x < 6 \Rightarrow X \quad D' :: \ \vdash \{X\} \ \textsf{while} \ x < 6 \ \textsf{do} \ x := 6 \ \{X\} \quad \vdash X \Rightarrow x \geq 6}{\vdash \{x < 6\} \ \textsf{while} \ x < 6 \ \textsf{do} \ x := 6 \ \{x \geq 6\}}$$

where the last rule of D' was stark. However, such X with $\{x < 6\} \Rightarrow X \wedge X \Rightarrow \{x \geq 6\}$ doesn't exist, which leads to a contradiction.

Hence, it is not possible to use stark to prove $\{A\}$ c $\{B\}$ for the above scenario.

targaryen

1. targaryen
2. $A = x \leq 6$
3. $B = x = 6$
4. $\sigma(x) = 0$
5. $\sigma'(x) = 6$
6. $c =$ while $x < 6$ do $x := x + 1$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$ since $\sigma(x) = 0 < 6$ and the loop body just adds 1 to x until $x = 6$.
8. $\sigma(x) = 0 \leq 6$ and hence $\sigma \models A$
9. $\sigma'(x) = 6 = 6$ and hence $\sigma' \models B$
10. it is not possible to prove $\vdash \{A\}$ c $\{B\}$

We will show that it is not possible to use targaryen to prove $\{x \leq 6\}$ while $x < 6$ do $x := 6$ $\{x = 6\}$ by contradiction. Suppose it is possible to do so, we have

$$D :: \ \vdash \{x \leq 6\} \ \textsf{while} \ x < 6 \ \textsf{do} \ x := x + 1 \ \{x = 6\}$$

where D is some derivation. By inversion, the last rule of D must be either targaryen or the rule of consequence. If the last rule was targaryen, we have $x \leq 6 \wedge \neg(x < 6)$ and $x = 6$ are identical, which is an obvious contradiction. If the last rule was the rule of consequence, we have

Peer Review ID: 72793226 — enter this when you fill out your peer evaluation via gradescope

$$D :: \frac{D_1 ::\ \vdash x \le 6 \Rightarrow X \quad D_2 ::\ \vdash \{X\}\ \textsf{while}\ x < 6\ \textsf{do}\ x := x + 1\ \{X \wedge \neg(x < 6)\} \quad D_3 ::\ \vdash X \wedge \neg(x < 6) \Rightarrow x = 6}{\vdash \{x \le 6\}\ \textsf{while}\ x < 6\ \textsf{do}\ x := x + 1\ \{x = 6\}}$$

where the last rule of D_2 was targaryen. According to D_3 we must have $X \Rightarrow x \le 6$ Together with D_1, we have that X must be $x \le 6$. For D_2, since it used targaryen we must have

$$D_2 :: \frac{D' ::\ \vdash \{x \le 6\}\ x := x + 1\ \{x \le 6\}}{\vdash \{x \le 6\}\ \textsf{while}\ x < 6\ \textsf{do}\ x := x + 1\ \{x \le 6 \wedge \neg(x < 6)\}}$$

However, a sound and complete D' doesn't exist because $x = 6$ is a counterexample.

Hence, it is not possible to use targaryen to prove $\{A\}\ c\ \{B\}$ for the above scenario.

Peer Review ID: 72793226 — enter this when you fill out your peer evaluation via gradescope

3 5F-3 VCGen Mistakes

- 0 pts Correct