

15F-1 Bookkeeping

- 0 pts Correct

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

$Inv1 \wedge (\forall x_1 \dots x_n. Inv1 \implies VC(c, Inv2)) \wedge (\forall x_1 \dots x_n. Inv2 \implies (b \implies Inv1 \wedge \neg b \implies P))$

Exercise 5F-3. VCGen Mistakes [20 points].

• stark

1. $A = \{y \leq 2\}$
2. $B = \{y = 2\}$
3. $\sigma = \{y = 0\}$
4. $\sigma' = \{y = 2\}$
5. $c = \text{while } y < 2 \text{ do } y = y + 1$
6. it is easy to verify that $\langle c, \sigma \rangle \Downarrow \sigma'$; $\sigma \models A$ and $\sigma' \models B$
7. Let's prove it is impossible to prove $\vdash \{A\} c \{B\}$ given the **stark** rule. We can apply the **stark** rule and conclude that the loop invariant $\{y \leq 2\}$ still persists after the while loop. But because it does not include the fact that the loop guard should be false after the while loop, in our case $\{y \geq 2\}$, there is not enough information for us to further prove that $\{y \leq 2 \wedge y \geq 2\} \implies \{y = 2\}$

• targaryen

1. $A = \{y \leq 2\}$
2. $B = \{y = 2\}$
3. $\sigma = \{y = 0\}$
4. $\sigma' = \{y = 2\}$
5. $c = \text{while } y < 2 \text{ do (if } y < 2 \text{ then } y = y + 1 \text{ else } y = 10)$
6. It is easy to verify that $\langle c, \sigma \rangle \Downarrow \sigma'$; $\sigma \models A$ and $\sigma' \models B$
7. Let's prove it is impossible to prove $\vdash \{A\} c \{B\}$ given the **targaryen** rule. Due to the else branch in our loop body, the loop invariant is persist only when the if condition is true, which happens to be the same with the loop guard. But when reasoning about the loop invariant the **targaryen** rule $\vdash \{X\} c \{X\}$ is missing the part that the loop guard should also be true, thus in our case, it can not exclude the possibility of reaching that else branch that can break our loop invariant. So the **targaryen** rule can not prove in our case that $\vdash \{A\} c \{B\}$.

2 5F-2 VCGen Do-While

- 0 pts Correct

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

$Inv1 \wedge (\forall x_1 \dots x_n. Inv1 \implies VC(c, Inv2)) \wedge (\forall x_1 \dots x_n. Inv2 \implies (b \implies Inv1 \wedge \neg b \implies P))$

Exercise 5F-3. VCGen Mistakes [20 points].

• stark

1. $A = \{y \leq 2\}$
2. $B = \{y = 2\}$
3. $\sigma = \{y = 0\}$
4. $\sigma' = \{y = 2\}$
5. $c = \text{while } y < 2 \text{ do } y = y + 1$
6. it is easy to verify that $\langle c, \sigma \rangle \Downarrow \sigma'$; $\sigma \models A$ and $\sigma' \models B$
7. Let's prove it is impossible to prove $\vdash \{A\} c \{B\}$ given the **stark** rule. We can apply the **stark** rule and conclude that the loop invariant $\{y \leq 2\}$ still persists after the while loop. But because it does not include the fact that the loop guard should be false after the while loop, in our case $\{y \geq 2\}$, there is not enough information for us to further prove that $\{y \leq 2 \wedge y \geq 2\} \implies \{y = 2\}$

• targaryen

1. $A = \{y \leq 2\}$
2. $B = \{y = 2\}$
3. $\sigma = \{y = 0\}$
4. $\sigma' = \{y = 2\}$
5. $c = \text{while } y < 2 \text{ do (if } y < 2 \text{ then } y = y + 1 \text{ else } y = 10)$
6. It is easy to verify that $\langle c, \sigma \rangle \Downarrow \sigma'$; $\sigma \models A$ and $\sigma' \models B$
7. Let's prove it is impossible to prove $\vdash \{A\} c \{B\}$ given the **targaryen** rule. Due to the else branch in our loop body, the loop invariant is persist only when the if condition is true, which happens to be the same with the loop guard. But when reasoning about the loop invariant the **targaryen** rule $\vdash \{X\} c \{X\}$ is missing the part that the loop guard should also be true, thus in our case, it can not exclude the possibility of reaching that else branch that can break our loop invariant. So the **targaryen** rule can not prove in our case that $\vdash \{A\} c \{B\}$.

3 5F-3 VCGen Mistakes

- 0 pts Correct