All subsequent answers should appear after the first page of your submission and may be shared publicly during peer review.

Exercise 5F-2. VCGen Do-While [8 points]. Choose exactly *one* of the two options below. (If you are not certain, pick the first. The answers end up being equivalent, but the first may be easier to grasp for some students and the second easier to grasp for others.)

- Give the (backward) verification condition formula for the command $\mathsf{do}_{\mathit{Inv}}\ c\ \mathsf{while}\ b$ with respect to a post-condition P. The invariant *Inv* is true before each evaluation of the predicate b. Your answer may not be defined in terms of VC(while...).

  Solution: $\mathsf{do}_{\mathit{Inv}}\ c\ \mathsf{while}\ b$ is equivalent to $c; \mathsf{while}_{\mathit{Inv}}\ b\ \mathsf{do}\ c$, so

  $$\begin{aligned}&\mathrm{VC}(\mathsf{do}_{\mathit{Inv}}\ c\ \mathsf{while}\ b, P)\\ &= \mathrm{VC}(c; \mathsf{while}_{\mathit{Inv}}\ b\ \mathsf{do}\ , P)\\ &= \mathrm{VC}(c, \mathit{Inv} \wedge (\forall x_1 \ldots x_n . \mathit{Inv} \implies (e \implies \mathrm{VC}(c, \mathit{Inv}) \wedge \neg e \implies P)))\end{aligned}$$

- Give the (backward) verification condition formula for the command $\mathsf{do}_{\mathit{Inv1},\mathit{Inv2}}\ c\ \mathsf{while}\ b$ with respect to a post-condition P. The invariant *Inv1* is true before c is first executed. The invariant *Inv2* is true before each evaluation of the loop predicate b. Your answer may not be defined in terms of VC(while...).

Exercise 5F-3. VCGen Mistakes [20 points]. Consider the following three alternate while Hoare rules (named $\mathsf{lannister}$, stark, and $\mathsf{targaryen}$):

$$\frac{\vdash \{X\}\ c\ \{b \implies X \ \wedge\ \neg b \implies Y\}}{\vdash \{b \implies X \ \wedge\ \neg b \implies Y\}\ \mathsf{while}\ b\ \mathsf{do}\ c\ \{Y\}}\ \mathsf{lannister} \qquad \frac{\vdash \{X \ \wedge\ b\}\ c\ \{X\}}{\vdash \{X\}\ \mathsf{while}\ b\ \mathsf{do}\ c\ \{X\}}\ \mathsf{stark}$$

$$\frac{\vdash \{X\}\ c\ \{X\}}{\vdash \{X\}\ \mathsf{while}\ b\ \mathsf{do}\ c\ \{X \ \wedge\ \neg b\}}\ \mathsf{targaryen}$$

All three rules are sound but incomplete. Choose **two** incomplete rules. For each chosen rule provide the following:

1. the name of the rule and
2. A and
3. B and
4. σ and
5. σ' and
6. c such that
7. $\langle c, \sigma\rangle \Downarrow \sigma'$ and
8. $\sigma \models A$ and
9. $\sigma' \models B$ but
10. it is not possible to prove $\vdash \{A\}\ c\ \{B\}$.

Solution 1:

1. targaryen
2. $A := \{x \leq 6\}$,
3. $B := \{x = 6\}$,
4. $\sigma : x \mapsto 0$,
5. $\sigma' : x \mapsto 6$,
6. $c :=\ \mathsf{while}\ x \leq 5\ \mathsf{do}\ x := x + 1$
7. we have $\langle c, \sigma\rangle \Downarrow \sigma'$ according to operational semantics
8. we have $\sigma \models A$

9. we have $\sigma' \models B$

10. Note that $(x = 6) \equiv (x \leq 6) \wedge \neg(x \leq 5)$. To derive $\{x \leq 6\}$ $\textsf{while}$ $x \leq 5$ $\textsf{do}$ $x := x + 1\{(x \leq 6) \wedge \neg(x \leq 5)\}$, the targaryen rule requires the premise $\{x \leq 6\}$ $x := x + 1$ $\{x \leq 6\}$. We will show that this premise is not provable.

    If the premise is provable, i.e., $\vdash \{x \leq 6\}$ $x := x + 1$ $\{x \leq 6\}$, then by soundness theorem, we have that $\{x \leq 6\} \implies wp(x := x+1, x \leq 6)$, suggesting that $x \leq 6 \implies x \leq 5$, which clearly does not hold. Therefore, the premise is not provable. As a result, $\{A\}$ c $\{B\}$ is also not provable.

Solution 2:

1. stark

2. $A := \{x \leq 6\}$,

3. $B := \{x = 6\}$,

4. $\sigma : x \mapsto 0$,

5. $\sigma' : x \mapsto 6$,

6. $c :=$ $\textsf{while}$ $x \leq 5$ $\textsf{do}$ $x := x + 1$

7. we have $\langle c, \sigma \rangle \Downarrow \sigma'$ according to operational semantics

8. we have $\sigma \models A$

9. we have $\sigma' \models B$

10. In order to prove $\{x \leq 6\}$ $\textsf{while}$ $x \leq 5$ $\textsf{do}$ $x := x + 1$ $\{x = 6\}$, we need to use stark to prove some $\{X\}$ $\textsf{while}$ $x \leq 5$ $\textsf{do}$ $x := x + 1$ $\{X\}$ for some X such that $\vdash x \leq 6 \implies X$ and $\vdash X \implies x = 6$, so we can use the rule of consequence to prove the desired $\{A\}$ c $\{B\}$. If such X exists, we will have $\vdash x \leq 6 \implies x = 6$, which clearly does not hold. As a result, $\{A\}$ c $\{B\}$ is not provable.