1 5F-1 Bookkeeping

- 0 pts Correct

Peer Review ID: 72110660 — enter this when you fill out your peer evaluation via gradescope

Exercise 5F-2

We know that executing $\mathsf{do}_{Inv}\ c\ \mathsf{while}\ b$ is equivalent to executing the inner block c once followed by a regular while_{Inv} command. This means that the verification condition for $\mathsf{do\text{-}while}_{Inv}$ should be very similar to the one for while_{Inv} with the only difference being that the invariant Inv isn't required at the onset, instead we required that Inv be established by executing c. That is, we must have $VC(c, Inv)$ as a precondition. Thus we obtain the following verification condition for $\mathsf{do\text{-}while}_{Inv}$:

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

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

Exercise 5F-3

1. stark
2. Let $A =$ "true".
3. Let $B =$ "$x = 0$".
4. Let σ be such that $\sigma(x) = 0$.
5. Let $\sigma' = \sigma$.
6. Let c be the command while false do skip.
7. We have $\langle c, \sigma\rangle \Downarrow \sigma'$ because the inner block of the while loop never executes (regardless of the value of σ).
8. We have $\sigma \models A$ trivially because everything models true.
9. We have $\sigma' \models B$ because $\sigma'(x) = 0$.
10. We claim that it is impossible to prove $\vdash \{A\}c\{B\}$ with only the stark rule for while. This is because the stark rule only allows us to conclude Hoare triples of the form $\{X\}c\{X\}$ and A is not logically equivalent to B (nor does it even imply B).

    To see this formally, suppose for contradiction that we have a derivation D proving $\{A\}c\{B\}$. By inversion the last rule applied in D must either be the stark rule or the rule of consequence. From above it's clear that the rule must not have been the stark rule. Thus we have that D is of the form

    $$\frac{\vdash A \implies A' \quad D' :: \vdash \{A'\}c\{B'\} \quad \vdash B' \implies B}{\vdash \{A\}c\{B\}}.$$

    Again by inversion we know that the last rule used in D' is the stark rule or the rule of consequence. Without loss of generality we may assume it was the stark rule because successive applications of the rule of consequence can be reduced to a single application. Thus we conclude that $A' = B'$ and thus we have the implication $A \implies A' = B' \implies B$. But this is a contradiction because true does not imply $x = 0$.

2 5F-2 VCGen Do-While

- 0 pts Correct

Exercise 5F-2

We know that executing $\mathsf{do}_{Inv}\ c\ \mathsf{while}\ b$ is equivalent to executing the inner block c once followed by a regular while_{Inv} command. This means that the verification condition for $\mathsf{do\text{-}while}_{Inv}$ should be very similar to the one for while_{Inv} with the only difference being that the invariant Inv isn't required at the onset, instead we required that Inv be established by executing c. That is, we must have $VC(c, Inv)$ as a precondition. Thus we obtain the following verification condition for $\mathsf{do\text{-}while}_{Inv}$:

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

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

Exercise 5F-3

1. stark
2. Let $A =$ "true".
3. Let $B =$ "$x = 0$".
4. Let σ be such that $\sigma(x) = 0$.
5. Let $\sigma' = \sigma$.
6. Let c be the command while false do skip.
7. We have $\langle c, \sigma \rangle \Downarrow \sigma'$ because the inner block of the while loop never executes (regardless of the value of σ).
8. We have $\sigma \models A$ trivially because everything models true.
9. We have $\sigma' \models B$ because $\sigma'(x) = 0$.
10. We claim that it is impossible to prove $\vdash \{A\}c\{B\}$ with only the stark rule for while. This is because the stark rule only allows us to conclude Hoare triples of the form $\{X\}c\{X\}$ and A is not logically equivalent to B (nor does it even imply B).

    To see this formally, suppose for contradiction that we have a derivation D proving $\{A\}c\{B\}$. By inversion the last rule applied in D must either be the stark rule or the rule of consequence. From above it's clear that the rule must not have been the stark rule. Thus we have that D is of the form

    $$\frac{\vdash A \implies A' \quad D' :: \vdash \{A'\}c\{B'\} \quad \vdash B' \implies B}{\vdash \{A\}c\{B\}}.$$

    Again by inversion we know that the last rule used in D' is the stark rule or the rule of consequence. Without loss of generality we may assume it was the stark rule because successive applications of the rule of consequence can be reduced to a single application. Thus we conclude that $A' = B'$ and thus we have the implication $A \implies A' = B' \implies B$. But this is a contradiction because true does not imply $x = 0$.

1. targaryen
2. Let $A =$ "$x \leq 0$".
3. Let $B =$ "$x \leq 1$".
4. Let $\sigma = (x \mapsto 0)$.
5. Let $\sigma' = (x \mapsto 1)$.
6. Let c be the command while $x \leq 0$ do $x := x + 1$.
7. We have $\langle c, \sigma \rangle \Downarrow \sigma'$ because after executing the inner command $x := x + 1$ one time, we'll have $x = 1 > 0$, terminating the loop.
8. We have $\sigma \models A$ because $\sigma(x) = 0 \leq 0$.
9. We have $\sigma' \models B$ because $\sigma'(x) = 1 \leq 1$.
10. We claim that it's not possible to prove $\vdash \{A\}c\{B\}$ with only the targaryen rule for while. This is because the targaryen rule requires us to prove a statement of the form $\vdash \{X\}x := x{+}1\{X\}$, without knowing b is true as a precondition, which is not possible.

    To see this formally, assume for contradiction that D is a derivation proving $\vdash \{A\}c\{B\}$. By inversion the last rule used in D must either be the targaryen rule or the rule of consequence. It cannot be the targaryen rule, however, because B is not of the form $A \wedge \neg b$. Thus we know the last rule was the rule of consequence, so D is of the form

    $$\frac{\vdash A \implies A' \quad D' :: \vdash \{A'\}c\{B'\} \quad \vdash B' \implies B}{\vdash \{A\}c\{B\}}.$$

    First, note that we can see that A' is either "true" or "$x \leq a$" for some constant $a \in \mathbb{Z}$ because those are the only statements that are implied by $x \leq 0$. As in the previous part, we may assume, without loss of generality, that the last rule used in D' is the targaryen rule. This implies that $\vdash \{A'\}x := x + 1\{A'\}$ is proven in the hypothesis for D'. If A' is "$x \leq a$", then this is a contradiction because $x \leq a$ does not imply $x + 1 \leq a$. If A' is simply "true", then this is also a contradiction because then $B' = A' \wedge \neg b =$ "$x > 0$", which does not imply B. This completes the proof that it is not possible to prove $\vdash \{A\}c\{B\}$ with the targaryen rule.

3 5F-3 VCGen Mistakes

- 0 pts Correct