1 5F-1 Bookkeeping

- **0 pts** Correct

2 5F-2

Since we have that $\mathsf{do}_{\mathsf{INV}}\ c\ \mathsf{while}\ b$ is equivalent to $c\ ;\ \mathsf{while}_{\mathsf{INV}}\ b\ \mathsf{do}\ c$ we can simply compose the VCGen for the sequencing command with that for while-do:

$$\text{VC}(\mathsf{do}_{\mathsf{INV}}\ c\ \mathsf{while}\ b, P) = \text{VC}(c, INV \wedge (\forall x_1 ... x_n . INV \implies (b \implies \text{VC}(c, INV) \wedge \neg b \implies P)))$$

(Where the x_i represent all variables modified in c)

3 5F-3

For the stark Hoare rule, let $c = \mathsf{while}\ a \neq 1\ \mathsf{do}\ a := a + 1$, $A = true$, $B = (a = 1)$, $\sigma = \{a : 0\}$, and $\sigma' = \{a : 1\}$. By our operational semantics we then have that $\langle c, \sigma \rangle \Downarrow \sigma'$, and by our semantics of assertions we have that $\sigma \models A$ and $\sigma' \models B$. But since out pre-condition A is logically distinct from our post-condition B, and the stark rule applies only to identical pre- and post-conditions, we cannot apply it to yield $\vdash \{A\}\ c\ \{B\}$.

For the targaryen Hoare rule, let $c = \mathsf{while}\ a \neq 1\ \mathsf{do}\ \{\ \mathsf{if}\ a = 1\ \mathsf{then}\ a := a + 2\ \mathsf{else}\ a := a + 1\ \}$, $A = (a < 2)$, $B = A \vee \neg b = (a < 2) \vee (a = 1) = (a = 1)$, $\sigma = \{a : 0\}$, and $\sigma' = \{a : 1\}$. Similarly to above, the conditions 7, 8, and 9 indicated in the question all hold. It remains then to show that it is not possible to prove that $\vdash \{a < 2\}\ \mathsf{while}\ a \neq 1\ \mathsf{do}\ \{\ \mathsf{if}\ a = 1\ \mathsf{then}\ a := a + 2\ \mathsf{else}\ a := a + 1\}\ \{a = 1\}$, which by the targaryen rule reduces to showing that $\vdash \{a < 2\}\ \mathsf{if}\ a = 1\ \mathsf{then}\ a := a + 2\ \mathsf{else}\ a := a + 1\ \{a < 2\}$.

By inversion the rule applied to conclude the above must be the if rule. By said rule, we'd need to show that (**I**) $\{a < 2 \wedge a = 1\}\ a := a + 2\ \{a < 2\}$ and (**II**) $\{a < 2 \wedge a \neq 1\}\ a := a + 1\ \{a < 2\}$. We can see that (**II**) holds by simplifying the precondition to $a < 1$ and then using consequence: $a < 1 \implies a + 1 < 2$ and $\vdash \{a + 1 < 2\}\ a := a + 1\ \{a < 2\}$, where the last clause holds by the rule for assignment. (**I**) however has no possible derivation, and in fact does not hold; the targaryen rule has left us with insufficient information to conclude the the else branch must necessarily be taken.

2 5F-2 VCGen Do-While

- **0 pts** Correct

2 5F-2

Since we have that $\mathsf{do}_{\mathsf{INV}}\ c\ \mathsf{while}\ b$ is equivalent to $c\ ;\ \mathsf{while}_{\mathsf{INV}}\ b\ \mathsf{do}\ c$ we can simply compose the VCGen for the sequencing command with that for while-do:

$$\text{VC}(\mathsf{do}_{\mathsf{INV}}\ c\ \mathsf{while}\ b, P) = \text{VC}(c, INV \wedge (\forall x_1 ... x_n . INV \implies (b \implies \text{VC}(c, INV) \wedge \neg b \implies P)))$$

(Where the x_i represent all variables modified in c)

3 5F-3

For the stark Hoare rule, let $c = \mathsf{while}\ a \neq 1\ \mathsf{do}\ a := a + 1$, $A = true$, $B = (a = 1)$, $\sigma = \{a : 0\}$, and $\sigma' = \{a : 1\}$. By our operational semantics we then have that $\langle c, \sigma \rangle \Downarrow \sigma'$, and by our semantics of assertions we have that $\sigma \models A$ and $\sigma' \models B$. But since out pre-condition A is logically distinct from our post-condition B, and the stark rule applies only to identical pre- and post-conditions, we cannot apply it to yield $\vdash \{A\}\ c\ \{B\}$.

For the targaryen Hoare rule, let $c = \mathsf{while}\ a \neq 1\ \mathsf{do}\ \{\ \mathsf{if}\ a = 1\ \mathsf{then}\ a := a + 2\ \mathsf{else}\ a := a + 1\ \}$, $A = (a < 2)$, $B = A \vee \neg b = (a < 2) \vee (a = 1) = (a = 1)$, $\sigma = \{a : 0\}$, and $\sigma' = \{a : 1\}$. Similarly to above, the conditions 7, 8, and 9 indicated in the question all hold. It remains then to show that it is not possible to prove that $\vdash \{a < 2\}\ \mathsf{while}\ a \neq 1\ \mathsf{do}\ \{\ \mathsf{if}\ a = 1\ \mathsf{then}\ a := a + 2\ \mathsf{else}\ a := a + 1\}\ \{a = 1\}$, which by the targaryen rule reduces to showing that $\vdash \{a < 2\}\ \mathsf{if}\ a = 1\ \mathsf{then}\ a := a + 2\ \mathsf{else}\ a := a + 1\ \{a < 2\}$.

By inversion the rule applied to conclude the above must be the if rule. By said rule, we'd need to show that (**I**) $\{a < 2 \wedge a = 1\}\ a := a + 2\ \{a < 2\}$ and (**II**) $\{a < 2 \wedge a \neq 1\}\ a := a + 1\ \{a < 2\}$. We can see that (**II**) holds by simplifying the precondition to $a < 1$ and then using consequence: $a < 1 \implies a + 1 < 2$ and $\vdash \{a + 1 < 2\}\ a := a + 1\ \{a < 2\}$, where the last clause holds by the rule for assignment. (**I**) however has no possible derivation, and in fact does not hold; the targaryen rule has left us with insufficient information to conclude the the else branch must necessarily be taken.

3 5F-3 VCGen Mistakes

- **0 pts** Correct