Exercise 5F-2. VCGen Do-While

$VC(\texttt{do}_{Inv}\ c\ \texttt{while}\ \ b, P)$
$= VC(c; \texttt{while}_{Inv} b\ \texttt{do}\ \ c, P)$
$= VC(c, VC(\texttt{while}_{Inv} b\ \texttt{do}\ \ c, P))$
$= VC(c, Inv \land (\forall x_1, \ldots, x_n. Inv \implies (b \implies VC(c, Inv) \land (\neg b \implies P))))$ where $x_1, \ldots, x_n$ are all the variables modified in c
$= VC(c, Inv) \land VC(c, \forall x_1, \ldots, x_n. Inv \implies (b \implies VC(c, Inv) \land (\neg b \implies P)))$ where $x_1, \ldots, x_n$ are all the variables modified in c

Exercise 5F-3. VCGen Mistakes

1. Name: Stark
2. $A = \{\texttt{true}\}$
3. $B = \{x > 3\}$
4. $\sigma = \{x \mapsto 0\}$
5. $\sigma' = \{x \mapsto 4\}$
6. $c = \ \ \texttt{while}\ \ x \leq 3\ \texttt{do}\ \ x := x + 1$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$ by using the large step operational semantics. Derivation elided.
8. $\{x \mapsto 0\} \vDash x \leq 3$
9. $\{x \mapsto 4\} \vDash x > 3$
10. It is not possible to prove $\vdash \{A\}c\{B\}$ using only the stark rule since we must know that the loop guard is false once the loop terminates. There's no post-condition we can prove about the command $x := x + 1$ that helps us ensure that $x > 3$ even with the rule of consequence.

1. Name: Targaryen
2. $A = \{y \leq 1\}$
3. $B = \{y \leq 1\}$
4. $\sigma = \{x \mapsto 0, y \mapsto 0\}$
5. $\sigma' = \{x \mapsto 2, y \mapsto 1\}$
6. $c = \ \ \texttt{while}\ \ x \leq 1\ \texttt{do}\ \ x := x + 1; y := x$
7. $\langle c, \sigma \rangle \Downarrow \sigma'$ by using the large step operational semantics. Derivation elided.
8. $\{x \mapsto 0, y \mapsto 0\} \vDash \{y \leq 1\}$
9. $\{x \mapsto 2, y \mapsto 1\} \vDash \{y \leq 1\}$
10. It is not possible to prove $\vdash \{A\}c\{B\}$ using only the Targaryen rule since we must know that the loop guard is true to show that $y \leq 1$ remains. There's no way to use the premise of the targaryen rule with $x := x+1; y := x$ to show that $y \leq 1$ since we can't know that $x \leq 1$.