Exercise 5F-2

I pick the first option, and present the following formula:

$$VC(\texttt{do}_{Inv}\ \texttt{c while b}) = VC(c, Inv) \land (\forall x_1 x_2, \ldots x_n . Inv \Rightarrow (b \Rightarrow VC(c, Inv) \land \neg b \Rightarrow P))$$

The first $VC(c, Inv)$ models that we wish Inv to hold immediately before the first evaluation of b. The second part says that for every assignment of variables, the invariant should either be mantained by the loop, or, if the loop exits, it should imply our desired postcondition P.

Exercise 5F-3

The first rule I choose is stark, with the following $(A, B, \sigma, \sigma', c)$:

$$A : z = 2$$

$$B : z = 3$$

$$\sigma : \{z = 2\}$$

$$\sigma' : \{z = 3\}$$

c : `while z=2 do z := 3`

It is clear that $\langle c, \sigma \rangle \Downarrow \sigma'$ because the loop body is run exactly once (in fact, this is more of an if statement than a while). Further, we have that $\sigma \models A$ and $\sigma' \models B$ immediately by inspection.

I claim that it is impossible to prove $\vdash \{A\}c\{B\}$ using the stark rule. Suppose otherwise, letting $\{X\}$ be the result of the application of the stark rule. So $\{X\}$ implies $z = 3$, but then we cannot apply the stark rule, as it is not true that $z = 3$ before the execution of c. That is, because the precondition and postcondition of the stark rule are exactly equal, it is unable to handle the change in state from running c.

The second rule I choose is targaryen, with the following $(A, B, \sigma, \sigma', c)$:

$$A : z = 0$$

$$B : z = 3$$

$$\sigma : \{z = 0\}$$

$$\sigma' : \{z = 3\}$$

c : `while z ≤ 2 do z := z + 1`

It is clear that $\langle c, \sigma \rangle \Downarrow \sigma'$, as our loop simply increments z until it reaches 3. As in the previous case, we again have that $\sigma \models A$ and $\sigma' \models B$ by inspection.

I claim it is impossible to prove $\vdash \{A\}c\{B\}$ using the targaryen rule. Note that $\neg b$ is equivalent to $z \geq 3$ in our case. Thus, for the targaryen rule to give us what we want, we need for $\{X\}$ to imply that $z \leq 3$. However, it is impossible to use such an X, as when $z = 3$, running $z := z + 1$ increments z to 4, so $\{X\}$ does not imply itself when running $z := z + 1$. In order to apply targaryen, we must have that $\vdash \{X\}z := z + 1\{X\}$, so X cannot imply $z \leq 3$ and thus $X \wedge \neg b$ cannot imply $z = 3$. So, there is no way to prove $\vdash \{A\}c\{B\}$ using the targaryen rule.