Exercise 5F-2

[The first option]

Notice that

$$\texttt{do}\ c\ \texttt{while}\ b \equiv c; \texttt{while}\ b\ \texttt{do}\ c,$$
$$(\texttt{while}\ b\ \texttt{do}\ c \equiv \texttt{if}\ b\ \texttt{then}\ \texttt{do}\ c\ \texttt{while}\ b\ \texttt{else}\ \texttt{skip}.)$$

therefore we have the following

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

where $x_1, \ldots, x_n$ are all the variables modified in c (derived from while not defined with $VC(\texttt{while}_{\mathsf{Inv}}\ b\ \texttt{do}\ c, P)$).

Exercise 5F-3

In general, a Hoare rule is supposed to prove more things if it has

- stronger pre-condition of the premise,
- weaker post-condition of the premise,
- weaker pre-condition of the conclusion,
- stronger post-condition of the conclusion.

Comparing with the rule

$$\frac{\vdash \{X \wedge b\}\ c\ \{X\}}{\vdash \{X\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{X \wedge \neg b\}}\ \texttt{while-do}$$

we see that

- Rule stark is not as powerful because the post-condition of the conclusion is weaker;
- Rule targaryen is not as powerful because the pre-condition of the premise is weaker;
- Rule lannister is not as powerful because both the post-condition of the premise and the pre-condition of the conclusion are stronger, and both the pre-condition of the premise and the post-condition of the conclusion are weaker.

- Rule stark

1. Rule stark
2. $A := (x \leq 1)$;
3. $B := (x = 1)$;
4. $\sigma := \{x \mapsto 0\}$;
5. $\sigma' := \{x \mapsto 1\}$;
6. $c :='' \texttt{while}\ x \leq 0\ \texttt{do}\ x := x + 1''$
7. $$\langle'' \texttt{while}\ x \leq 0\ \texttt{do}\ x := x + 1'', \{x \mapsto 0\}\rangle \Downarrow \{x \mapsto 1\};$$
$$\langle c, \sigma\rangle \Downarrow \sigma';$$
8. $$\{x \mapsto 0\} \models (x \leq 1);$$
$$\sigma \models A;$$
9. $$\{x \mapsto 1\} \models (x = 1);$$
$$\sigma' \models B;$$

10. However, with rule stark it's only possible to prove

$$\frac{\vdash \{(x \le 1) \land (x \le 0)\}\ x := x + 1\ \{x \le 1\}}{\vdash \{x \le 1\}\ \texttt{while}\ \ x \le 0\ \ \texttt{do}\ \ x := x + 1\ \{x \le 1\}}\ \texttt{stark}$$

but $\nvdash \{x \le 1\}$ while $x \le 0$ do $x := x+1$ $\{x = 1\}$, as the pre- and post-conditions of the conclusion have to be the same.

- Rule targaryen

1. Rule targaryen
2. $A := (x \le 1)$;
3. $B := (x = 1)$;
4. $\sigma := \{x \mapsto 0\}$;
5. $\sigma' := \{x \mapsto 1\}$;
6. $c :=''$ while $x \le 0$ do $x := x + 1''$
7. $$\langle ''\texttt{while}\ \ x \le 0\ \ \texttt{do}\ \ x := x + 1'', \{x \mapsto 0\}\rangle \Downarrow \{x \mapsto 1\};$$ $$\langle c, \sigma\rangle \Downarrow \sigma';$$
8. $$\{x \mapsto 0\} \models (x \le 1);$$ $$\sigma \models A;$$
9. $$\{x \mapsto 1\} \models (x = 1);$$ $$\sigma' \models B;$$
10. However, with rule targaryen by inversion we see that it's not possible to prove $\vdash \{x \le 1\}$ while $x \le 0$ do $x := x + 1$ $\{x = 1\}$, as

$$\frac{\nvdash \{x \le 1\}\ x := x + 1\ \{x \le 1\}}{\nvdash \{x \le 1\}\ \texttt{while}\ \ x \le 0\ \ \texttt{do}\ \ x := x + 1\ \{(x \le 1) \land (x > 0)\}}\ \texttt{targaryen}$$

where the pre- and post-conditions of the premise have to be the same, which does not hold if $x = 1$; and furthermore we have $(x = 1) \iff (x \le 1) \land (x > 0)$ which excludes the possibilities of applying consequence rules.

- **Rule lannister (optional)**

1. Rule lannister
2. $A := (x \leq 1)$;
3. $B := (x = 1)$;
4. $\sigma := \{x \mapsto 0\}$;
5. $\sigma' := \{x \mapsto 1\}$;
6. $c :='' \texttt{while } x \leq 0 \texttt{ do } x := x + 1''$
7. $$\begin{array}{r}\langle ''\texttt{while } x \leq 0 \texttt{ do } x := x + 1'', \{x \mapsto 0\}\rangle \Downarrow \{x \mapsto 1\};\\ \langle c, \sigma\rangle \Downarrow \sigma';\end{array}$$
8. $$\begin{array}{c}\{x \mapsto 0\} \models (x \leq 1);\\ \sigma \models A;\end{array}$$
9. $$\begin{array}{c}\{x \mapsto 1\} \models (x = 1);\\ \sigma' \models B;\end{array}$$
10. However, with rule lannister by inversion we see that it's not possible to prove $\vdash \{x \leq 1\}$ `while` $x \leq 0$ `do` $x := x + 1$ $\{x = 1\}$, as

    $$\frac{\nvdash \{x \leq 1\}\ x := x + 1\ \{(x \leq 0) \Longrightarrow (x \leq 1) \wedge (x > 0) \Longrightarrow (x = 1)\}}{\nvdash \{(x \leq 0) \Longrightarrow (x \leq 1) \wedge (x > 0) \Longrightarrow (x = 1)\}\ \texttt{while } x \leq 0 \texttt{ do } x := x + 1\ \{x = 1\}}\ \texttt{lannister}$$

    where the premise does not hold if $x = 1$; and furthermore we have $[(x \leq 0) \Longrightarrow (x \leq 1) \wedge (x > 0) \Longrightarrow (x = 1)] \Longleftrightarrow (x \leq 1)$ which excludes the possibilities of applying consequence rules.