Exercise 4F-2

It seems that the scope of $x := e$ should be within the execution of c, while the given rule is actually the rule for the program $''x := e; c'' \not\equiv ''\texttt{let } x := e \texttt{ in } c''$.

Noticing that

$$''\texttt{let } x := e \texttt{ in } c'' \equiv ''x_0 := x;\ x := e;\ c;\ x := x_0\ '',$$

we have

$$VC(\texttt{let } x := e \texttt{ in } c, B) = [x/x_0][e/x]VC(c, [x_0/x]B),$$

where x_0 is a temporary variable not appearing in the assertion.

The soundness and (relative) completeness of this rule then follow from the soundness and (relative) completeness of the original Hoare Logic.

Another possibility is

$$VC(\texttt{let } x := e \texttt{ in } c, B) = \exists x_0.\ (x = x_0) \wedge [e/x]VC(c, [x_0/x]B)$$

The soundness can be verified by

Proof.

$$\dfrac{\dfrac{\dfrac{}{\langle x,\ \sigma\rangle \Downarrow n_0}\quad\dfrac{}{x = x_0}}{\langle x,\ \sigma\rangle \Downarrow n_0 \quad \langle x_0,\ \sigma\rangle \Downarrow n_0}\quad\dfrac{}{\langle e,\ \sigma\rangle \Downarrow n_1}\quad\dfrac{}{\langle c,\ \sigma[x := n_1]\rangle \Downarrow \sigma' \models [n_0/x]B}}{\langle \texttt{let } x = e \texttt{ in } c,\ \sigma\rangle \Downarrow \sigma'[x := n_0] \models B}\ \texttt{letI}$$

□

while it does not seem to be complete, as the rule assumes some x_0 being in σ.

Question assigned to the following page: 3

Exercise 4F-3

1. $c :=$ ″`let` $x := 1$ `in skip`″;
2. $B := (x = 1)$;
3. $\sigma := \{x \mapsto 0\}$;
4. $$\begin{aligned} VC(c, B) &\iff [1/x]VC(\texttt{skip}, B) \\ &\iff [1/x]B \\ &\iff [1/x](x = 1) \\ &\iff (1 = 1) \\ &\iff \mathsf{True}; \\ \{x \mapsto 0\} &\models \mathsf{True}. \end{aligned}$$
5. $$\begin{aligned} &\langle c, \sigma\rangle \Downarrow \sigma'; \\ &\sigma' = \{x \mapsto 0\}. \end{aligned}$$
6. $$\{x \mapsto 0\} \not\models (x = 1).$$

Question assigned to the following page: 4

Exercise 4F-4

Notice that

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

therefore we have the following rules:

$$\frac{\vdash \{A\}c\{A'\} \qquad \vdash \{A'\}\texttt{while } b \texttt{ do } c\{B\}}{\vdash \{A\}\texttt{do } c \texttt{ while } b\{B\}} \ \texttt{do-while}$$

or

$$VC(\texttt{do } c \texttt{ while } b, B) = VC(c, VC(\texttt{while } b \texttt{ do } c, B)).$$

The soundness and (relative) completeness of this rule then follow from the soundness and (relative) completeness of the original Hoare Logic.