Programming Languages: Imperative Program Construction
Practicals 1: Non-Looping Constructs and Weakest Precondition

Shin-Cheng Mu

Autumn Term, 2021

1. Determine the weakest P that satisfies
   (a) $\{P\}\; x := x + 1; x := x + 1\; \{x \geqslant 0\}$.
   (b) $\{P\}\; x := x + y; y := 2 \times x\; \{y \geqslant 0\}$.
   (c) $\{P\}\; x := y; y := x\; \{x = A \land y = B\}$.
   (d) $\{P\}\; x := E; x := E\; \{x = E\}$.

Solution:

(a)
$$
\begin{array}{ll}
 & wp\ (x := x + 1; x := x + 1)\ (x \geqslant 0) \\
= & wp\ (x := x + 1)\ (wp\ (x := x + 1)\ (x \geqslant 0)) \\
= & wp\ (x := x + 1)\ (x + 1 \geqslant 0) \\
= & (x + 1) + 1 \geqslant 0 \\
= & x \geqslant -2 \quad .
\end{array}
$$

(b)
$$
\begin{array}{ll}
 & wp\ (x := x + y; y := 2 \times x)\ (y \geqslant 0) \\
= & wp\ (x := x + y)\ (wp\ (y := 2 \times x)\ (y \geqslant 0)) \\
= & wp\ (x := x + y)\ (2 \times x \geqslant 0) \\
= & 2 \times (x + y) \geqslant 0 \quad .
\end{array}
$$

(c)
$$
\begin{array}{ll}
 & wp\ (x := y; y := x)\ (x = A \land y = B) \\
\Leftrightarrow & wp\ (x := y)\ (wp\ (y := x)\ (x = A \land y = B)) \\
\Leftrightarrow & wp\ (x := y)\ (x = A \land x = B) \\
\Leftrightarrow & y = A \land y = B \\
\Leftrightarrow & y = A = B \quad .
\end{array}
$$

(d)
$$
\begin{array}{ll}
 & wp\ (x := E; x := E)\ (x = E) \\
\Leftrightarrow & wp\ (x := E)\ (wp\ (x := E)\ (x = E)) \\
\Leftrightarrow & wp\ (x := E)\ ((x := E)[x \backslash E]) \\
\Leftrightarrow & wp\ (x := E)\ (x = E[x \backslash E]) \\
\Leftrightarrow & (x = E[x \backslash E])[x \backslash E] \\
\Leftrightarrow & E = (E[x \backslash E])[x \backslash E] \quad .
\end{array}
$$

2. Assuming that x, y, and z are integers, prove the following

(a) $\{True\}$ **if** $x \geqslant 1 \to x := x + 1 \mid x \leqslant 1 \to x := x - 1$ **fi** $\{x \neq 1\}$.

(b) $\{True\}$ **if** $x \geqslant y \to skip \mid y \leqslant x \to x, y := y, x$ **fi** $\{x \geqslant y\}$.

(c) $\{x = 0\}$ **if** $True \to x := 1 \mid True \to x := -1$ $\{x = 1 \vee x = -1\}$.

(d) $\{A = x \times y + z\}$ **if** $even\ x \to x, y := x / 2, y \times 2 \mid True \to y, z := y - 1, z + y$ $\{A = x \times y + z\}$.

Solution: The annotated program is

$\{A = x \times y + z\}$
if $even\ x \to \{A = x \times y + z \wedge even\ x\}\ x, y := x / 2, y \times 2\ \{A = x \times y + z, \mathrm{Pf}_0\}$
$\mid\ True \quad \to \{A = x \times y + z\}\ y, z := y - 1, z + y\ \{A = x \times y + z, \mathrm{Pf}_1\}$
fi
$\{A = x \times y + z, \mathrm{Pf}_2\}$

Pf_0: We reason:

$$\begin{aligned} & (A = x \times y + z)[x, y \backslash x / 2, y \times 2] \\ \Leftrightarrow\ & A = (x / 2) \times (y \times 2) + z \\ \Leftarrow\ & A = x \times y + z \wedge even\ x \ \ . \end{aligned}$$

Pf_2: We reason:

$$\begin{aligned} & (A = x \times y + z)[y, z \backslash y - 1, z + y] \\ \Leftrightarrow\ & A = x \times (y - 1) + (z + y) \\ \Leftarrow\ & A = x \times y + z \ \ . \end{aligned}$$

Pf_2: Certainly $P \Rightarrow Q \wedge True$ for any P and Q.

(e) $\{x \times y = 0 \wedge y \leqslant x\}$ **if** $y < 0 \to y := -y \mid y = 0 \to x := -1$ $\{x < y\}$.

Solution: The annotated program is

$\{x \times y = 0 \wedge y \leqslant x\}$
if $y < 0 \to \{x \times y = 0 \wedge y \leqslant x \wedge y < 0\}\ y := -y\ \{x < y, \mathrm{Pf}_0\}$
$\mid\ y = 0 \to \{x \times y = 0 \wedge y \leqslant x \wedge y = 0\}\ x := -1\ \{x < y, \mathrm{Pf}_1\}$
fi
$\{x < y, \mathrm{Pf}_2\}$

Pf_0: Note that $x \times y = 0$ equivals $x = 0 \vee y = 0$. Therefore

$$\begin{aligned} & x \times y = 0 \wedge y \leqslant x \wedge y < 0 \\ \Leftrightarrow\ & (x = 0 \vee y = 0) \wedge y \leqslant x \wedge y < 0 \\ \Leftrightarrow\ & \quad \{ \text{ distributivity } \} \\ & (x = 0 \wedge y \leqslant x \wedge y < 0) \vee (y = 0 \wedge y \leqslant x \wedge y < 0) \\ \Leftrightarrow\ & \quad \{ \text{ since } (y = 0 \wedge y \leqslant x \wedge y < 0) \Leftrightarrow False \ \} \\ & x = 0 \wedge y \leqslant x \wedge y < 0 \\ \Leftrightarrow\ & x = 0 \wedge y < 0 \ \ . \end{aligned}$$

To prove the Hoare triple we reason:

$$\begin{aligned} & (x < y)[y \backslash -y] \\ \Leftrightarrow\ & x < -y \\ \Leftarrow\ & x = 0 \wedge y < 0 \ \ . \end{aligned}$$

Pf$_1$: We reason:

$$
\begin{aligned}
& (x < y)[x \backslash -1] \\
\Leftrightarrow\ & -1 < y \\
\Leftarrow\ & x \times y = 0 \wedge y \leqslant x \wedge y = 0 \ .
\end{aligned}
$$

Pf$_2$: We reason:

$$
\begin{aligned}
& x \times y = 0 \wedge y \leqslant x \\
\Leftrightarrow\ & (x = 0 \vee y = 0) \wedge y \leqslant x \\
\Leftrightarrow\ & \quad \{ \text{ distributivity } \} \\
& (x = 0 \wedge y \leqslant x) \vee (y = 0 \wedge y \leqslant x) \\
\Rightarrow\ & y < 0 \vee y = 0 \ .
\end{aligned}
$$

3. What is the weakest P such that the following holds?

$$
\begin{aligned}
& \textbf{var } x : \mathit{Int} \\
& \{P\} \\
& x := x + 1 \\
& \textbf{if } x > 0 \rightarrow x := x + 1 \\
& \ \mid x < 0 \rightarrow x := x + 2 \\
& \ \mid x = 1 \rightarrow \mathit{skip} \\
& \textbf{fi} \\
& \{x \geqslant 1\} \ .
\end{aligned}
$$

Solution: Denote the **if** statement by IF. The aim is to compute $wp\ (x := x + 1; \mathrm{IF})\ (x \geqslant 1)$.

Recall the definition of wp for **if**. We have

$$
\begin{aligned}
wp\ \mathrm{IF}\ (x \geqslant 1) = {} & (x > 0 \Rightarrow wp\ (x := x + 1)\ (x \geqslant 1)) \wedge \\
& (x < 0 \Rightarrow wp\ (x := x + 2)\ (x \geqslant 1)) \wedge \\
& (x = 1 \Rightarrow wp\ \mathit{skip}\ (x \geqslant 1)) \wedge \\
& (x > 0 \vee x < 0 \vee x = 1) \ .
\end{aligned}
$$

We calculate the four conjuncts separately:

- $$
\begin{aligned}
& x > 0 \Rightarrow wp\ (x := x + 1)\ (x \geqslant 1) \\
\Leftrightarrow\ & x > 0 \Rightarrow x + 1 \geqslant 1 \\
\Leftrightarrow\ & x > 0 \Rightarrow x \geqslant 0 \\
\Leftrightarrow\ & \mathit{True} \ .
\end{aligned}
$$

- $$
\begin{aligned}
& x < 0 \Rightarrow wp\ (x := x + 2)\ (x \geqslant 1) \\
\Leftrightarrow\ & x < 0 \Rightarrow x + 2 \geqslant 1 \\
\Leftrightarrow\ & x < 0 \Rightarrow x \geqslant -1 \\
\Leftrightarrow\ & \quad \{ (P \Rightarrow Q) = (\neg P \vee Q) \} \\
& x \geqslant 0 \vee x \geqslant -1 \\
\Leftrightarrow\ & x \geqslant -1 \ .
\end{aligned}
$$

- $$\begin{aligned} & x = 1 \Rightarrow wp\ skip\ (x \geqslant 1) \\ \Leftrightarrow\ & x = 1 \Rightarrow x \geqslant 1 \\ \Leftrightarrow\ & True\ \ . \end{aligned}$$

- Furthermore, $x > 0 \vee x < 0 \vee x = 1$ simplifies to $x \neq 0$.

Therefore,

$$\begin{aligned} & wp\ \mathsf{IF}\ (x \geqslant 1) \\ =\ & True \wedge x \geqslant -1 \wedge True \wedge x \neq 0 \\ =\ & x \geqslant -1 \wedge x \neq 0\ \ . \end{aligned}$$

Finally, recall what we want to compute:

$$\begin{aligned} & wp\ (x := x + 1; \mathsf{IF})\ (x \geqslant 1) \\ =\ & wp\ (x := x + 1)\ (wp\ \mathsf{IF}\ (x \geqslant 1)) \\ =\ & wp\ (x := x + 1)\ (x \geqslant -1 \wedge x \neq 0) \\ =\ & x + 1 \geqslant -1 \wedge x + 1 \neq 0) \\ =\ & x \geqslant -2 \wedge x \neq -1\ \ . \end{aligned}$$

4. Two programs S_0 and S_1 are equivalent if, for all Q, $wp\ S_0\ Q = wp\ S_1\ Q$. Show that the two following programs are equivalent.

$$\begin{aligned} & \mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1\ \mathbf{fi}; S \\ & \mathbf{if}\ B_0 \rightarrow S_0; S \mid B_1 \rightarrow S_1; S\ \mathbf{fi} \end{aligned}$$

Solution:

$$\begin{aligned} & wp\ (\mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1\ \mathbf{fi}; S)\ Q \\ =\ & \quad \{ \text{ definition of } wp\ \} \\ & wp\ (\mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1\ \mathbf{fi})\ (wp\ S\ Q) \\ =\ & \quad \{ \text{ definition of } wp\ \} \\ & (B_0 \Rightarrow wp\ S_0\ (wp\ S\ Q)) \wedge \\ & (B_1 \Rightarrow wp\ S_1\ (wp\ S\ Q)) \wedge (B_0 \vee B_1) \\ =\ & \quad \{ \text{ definition of } wp\ \} \\ & (B_0 \Rightarrow wp\ (S_0; S)\ Q) \wedge \\ & (B_1 \Rightarrow wp\ (S_1; S)\ Q) \wedge (B_0 \vee B_1) \\ =\ & \quad \{ \text{ definition of } wp\ \} \\ & wp\ (\mathbf{if}\ B_0 \rightarrow S_0; S \mid B_1 \rightarrow S_1; S\ \mathbf{fi})\ Q\ \ . \end{aligned}$$

5. Consider the two programs:

$$\begin{aligned} & \mathsf{IF}_0 = \mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1\ \mathbf{fi}\ \ , \\ & \mathsf{IF}_1 = \mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \wedge \neg B_0 \rightarrow S_1\ \mathbf{fi}\ \ . \end{aligned}$$

Show that for all Q, $wp\ \mathsf{IF}_0\ Q \Rightarrow wp\ \mathsf{IF}_1\ Q$.

Solution: Firstly, we show that $B_0 \vee (B_1 \wedge \neg B_0) = B_0 \vee B_1$.

$$
\begin{aligned}
& \quad B_0 \vee (B_1 \wedge \neg B_0) \\
= & \quad \{ \text{ distributivity } \} \\
& \quad (B_0 \vee B_1) \wedge (B_0 \vee \neg B_0) \\
= & \quad (B_0 \vee B_1) \wedge \mathit{True} \\
= & \quad B_0 \vee B_1 \ .
\end{aligned}
$$

Secondly, recall that

- conjunction is monotonic, that is, $(P_0 \wedge Q) \Rightarrow (P_1 \wedge Q)$ if $P_0 \Rightarrow P_1$;
- implication is anti-monotonic in its first argument, that is $(P_0 \Rightarrow Q) \Rightarrow (P_1 \Rightarrow Q)$ if $P_1 \Rightarrow P_0$.

Therefore we have

$$
\begin{aligned}
& \quad \mathit{wp}\ (\mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1\ \mathbf{fi})\ Q \\
= & \quad (B_0 \Rightarrow \mathit{wp}\ S_0\ Q) \wedge (B_1 \Rightarrow \mathit{wp}\ S_1\ Q) \wedge (B_0 \vee B_1) \\
= & \quad \{ \text{ since } B_0 \vee (B_1 \wedge \neg B_0) = B_0 \vee B_1 \ \} \\
& \quad (B_0 \Rightarrow \mathit{wp}\ S_0\ Q) \wedge (B_1 \Rightarrow \mathit{wp}\ S_1\ Q) \wedge (B_0 \vee (B_1 \wedge \neg B_0)) \\
\Rightarrow & \quad \{ \text{ since } B_1 \wedge \neg B_0 \Rightarrow B_1, \text{(anti-)monotonicity as discussed above. } \} \\
& \quad (B_0 \Rightarrow \mathit{wp}\ S_0\ Q) \wedge (B_1 \wedge \neg B_0 \Rightarrow \mathit{wp}\ S_1\ Q) \wedge (B_0 \vee (B_1 \wedge \neg B_0)) \\
= & \quad \mathit{wp}\ (\mathbf{if}\ B_0 \rightarrow S_0 \mid B_1 \wedge \neg B_0 \rightarrow S_1\ \mathbf{fi})\ Q \ .
\end{aligned}
$$