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) $\{P\}\, x := y; y := x \,\{x = A \wedge y = B\}$.

   (d) $\{P\}\, x := E; x := E \,\{x = E\}$.

Solution:

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

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

(c)
$$
\begin{aligned}
& wp\ (x := y; y := x)\ (x = A \wedge y = B) \\
\Leftrightarrow\ & wp\ (x := y)\ (wp\ (y := x)\ (x = A \wedge y = B)) \\
\Leftrightarrow\ & wp\ (x := y)\ (x = A \wedge x = B) \\
\Leftrightarrow\ & y = A \wedge y = B \\
\Leftrightarrow\ & y = A = B\ \ .
\end{aligned}
$$

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

---

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

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

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

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

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

> **Solution:** The annotated program is
>
> $\{A = x \times y + z\}$
> **if** $\textit{even } x \to \{A = x \times y + z \land \textit{even } x\} \, x, y := x / 2, y \times 2 \, \{A = x \times y + z, \text{Pf}_0\}$
> $\mid \textit{True} \quad \to \{A = x \times y + z\} \, y, z := y - 1, z + y \, \{A = x \times y + z, \text{Pf}_1\}$
> **fi**
> $\{A = x \times y + z, \text{Pf}_2\}$
>
> Pf_0: We reason:
>
> $$(A = x \times y + z)[x, y \backslash x / 2, y \times 2]$$
> $$\Leftrightarrow A = (x / 2) \times (y \times 2) + z$$
> $$\Leftarrow A = x \times y + z \land \textit{even } x \ .$$
>
> Pf_2: We reason:
>
> $$(A = x \times y + z)[y, z \backslash y - 1, z + y]$$
> $$\Leftrightarrow A = x \times (y - 1) + (z + y)$$
> $$\Leftarrow A = x \times y + z \ .$$
>
> Pf_2: Certainly $P \Rightarrow Q \land \textit{True}$ for any P and Q.

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

> **Solution:** The annotated program is
>
> $\{x \times y = 0 \land y \leqslant x\}$
> **if** $y < 0 \to \{x \times y = 0 \land y \leqslant x \land y < 0\} \, y := -y \, \{x < y, \text{Pf}_0\}$
> $\mid y = 0 \to \{x \times y = 0 \land y \leqslant x \land y = 0\} \, x := -1 \, \{x < y, \text{Pf}_1\}$
> **fi**
> $\{x < y, \text{Pf}_2\}$
>
> Pf_0: Note that $x \times y = 0$ equivals $x = 0 \lor y = 0$. Therefore
>
> $$x \times y = 0 \land y \leqslant x \land y < 0$$
> $$\Leftrightarrow (x = 0 \lor y = 0) \land y \leqslant x \land y < 0$$
> $$\Leftrightarrow \quad \{ \text{ distributivity } \}$$
> $$(x = 0 \land y \leqslant x \land y < 0) \lor (y = 0 \land y \leqslant x \land y < 0)$$
> $$\Leftrightarrow \quad \{ \text{ since } (y = 0 \land y \leqslant x \land y < 0) \Leftrightarrow \textit{False} \}$$
> $$x = 0 \land y \leqslant x \land y < 0$$
> $$\Leftrightarrow x = 0 \land y < 0 \ .$$
>
> To prove the Hoare triple we reason:
>
> $$(x < y)[y \backslash - y]$$
> $$\Leftrightarrow x < -y$$
> $$\Leftarrow x = 0 \land y < 0 \ .$$

Pf$_1$: We reason:

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

Pf$_2$: We reason:

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

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

> **var** x : *Int*
> $\{P\}$
> $x := x + 1$
> **if** $x > 0 \to x := x + 1$
> $\mid\ x < 0 \to x := x + 2$
> $\mid\ x = 1 \to skip$
> **fi**
> $\{x \geqslant 1\}$.

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

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

$$
\begin{aligned}
wp\ \text{IF}\ (x \geqslant 1) = &(x > 0 \Rightarrow wp\ (x := x + 1)\ (x \geqslant 1)) \land \\
&(x < 0 \Rightarrow wp\ (x := x + 2)\ (x \geqslant 1)) \land \\
&(x = 1 \Rightarrow wp\ skip\ (x \geqslant 1)) \land \\
&(x > 0 \lor x < 0 \lor x = 1) \quad.
\end{aligned}
$$

We calculate the four conjuncts separately:

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

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

-
$$x = 1 \Rightarrow wp \; skip \; (x \geqslant 1)$$
$$\Leftrightarrow x = 1 \Rightarrow x \geqslant 1$$
$$\Leftrightarrow True \; .$$

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

Therefore,

$$wp \; \text{IF} \; (x \geqslant 1)$$
$$= True \land x \geqslant -1 \land True \land x \neq 0$$
$$= x \geqslant -1 \land x \neq 0 \; .$$

Finally, recall what we want to compute:

$$wp \; (x := x + 1; \text{IF}) \; (x \geqslant 1)$$
$$= wp \; (x := x + 1) \; (wp \; \text{IF} \; (x \geqslant 1))$$
$$= wp \; (x := x + 1) \; (x \geqslant -1 \land x \neq 0)$$
$$= x + 1 \geqslant -1 \land x + 1 \neq 0)$$
$$= x \geqslant -2 \land x \neq -1 \; .$$

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.

$$\textbf{if} \; B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1 \; \textbf{fi}; S$$
$$\textbf{if} \; B_0 \rightarrow S_0; S \mid B_1 \rightarrow S_1; S \; \textbf{fi}$$

Solution:

$$wp \; (\textbf{if} \; B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1 \; \textbf{fi}; S) \; Q$$
$$= \quad \{ \text{ definition of } wp \; \}$$
$$wp \; (\textbf{if} \; B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1 \; \textbf{fi}) \; (wp \; S \; Q)$$
$$= \quad \{ \text{ definition of } wp \; \}$$
$$(B_0 \Rightarrow wp \; S_0 \; (wp \; S \; Q)) \land$$
$$(B_1 \Rightarrow wp \; S_1 \; (wp \; S \; Q)) \land (B_0 \lor B_1)$$
$$= \quad \{ \text{ definition of } wp \; \}$$
$$(B_0 \Rightarrow wp \; (S_0; S) \; Q) \land$$
$$(B_1 \Rightarrow wp \; (S_1; S) \; Q) \land (B_0 \lor B_1)$$
$$= \quad \{ \text{ definition of } wp \; \}$$
$$wp \; (\textbf{if} \; B_0 \rightarrow S_0; S \mid B_1 \rightarrow S_1; S \; \textbf{fi}) \; Q \; .$$

5. Consider the two programs:

$$\text{IF}_0 = \textbf{if} \; B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1 \; \textbf{fi} \; ,$$
$$\text{IF}_1 = \textbf{if} \; B_0 \rightarrow S_0 \mid B_1 \land \neg \; B_0 \rightarrow S_1 \; \textbf{fi} \; .$$

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

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

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

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

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