

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) $\{P\} x := x + 1; x := x + 1 \{x \geq 0\}$.
- (b) $\{P\} x := x + y; y := 2 \times x \{y \geq 0\}$.
- (c) $\{P\} x := y; y := x \{x = A \wedge y = B\}$.
- (d) $\{P\} x := E; x := E \{x = E\}$.

Solution:

- (a)
$$\begin{aligned} & wp(x := x + 1; x := x + 1)(x \geq 0) \\ &= wp(x := x + 1)(wp(x := x + 1)(x \geq 0)) \\ &= wp(x := x + 1)(x + 1 \geq 0) \\ &= (x + 1) + 1 \geq 0 \\ &= x \geq -2. \end{aligned}$$
- (b)
$$\begin{aligned} & wp(x := x + y; y := 2 \times x)(y \geq 0) \\ &= wp(x := x + y)(wp(y := 2 \times x)(y \geq 0)) \\ &= wp(x := x + y)(2 \times x \geq 0) \\ &= 2 \times (x + y) \geq 0. \end{aligned}$$
- (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)
$$\begin{aligned} & wp(x := E; x := E)(x = E) \\ &\Leftrightarrow wp(x := E)(wp(x := E)(x = E)) \\ &\Leftrightarrow wp(x := E)((x := E)[x \setminus E]) \\ &\Leftrightarrow wp(x := E)(x = E[x \setminus E]) \\ &\Leftrightarrow (x = E[x \setminus E])[x \setminus E] \\ &\Leftrightarrow E = (E[x \setminus E])[x \setminus E]. \end{aligned}$$

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

- (a) $\{True\} \text{ if } x \geq 1 \rightarrow x := x + 1 \mid x \leq 1 \rightarrow x := x - 1 \text{ fi } \{x \neq 1\}.$
(b) $\{True\} \text{ if } x \geq y \rightarrow \text{skip} \mid y \geq x \rightarrow x, y := y, x \text{ fi } \{x \geq y\}.$
(c) $\{x = 0\} \text{ if } True \rightarrow x := 1 \mid True \rightarrow x := -1 \{x = 1 \vee x = -1\}.$
(d) $\{A = x \times y + z\} \text{ if even } x \rightarrow x, y := x / 2, y \times 2 \mid True \rightarrow y, z := y - 1, z + x \{A = x \times y + z\}.$

Solution: The annotated program is

```

{A = x × y + z}
if even x → {A = x × y + z ∧ even x} x, y := x / 2, y × 2 {A = x × y + z, Pf0}
| True → {A = x × y + z} y, z := y - 1, z + x {A = x × y + z, Pf1}
fi
{A = x × y + z, Pf2}

```

Pf₀: We reason:

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

Pf₂: We reason:

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

Pf₂: Certainly $P \Rightarrow Q \wedge True$ for any P and Q .

- (e) $\{x \times y = 0 \wedge y \leq x\} \text{ if } y < 0 \rightarrow y := -y \mid y = 0 \rightarrow x := -1 \{x < y\}.$

Solution: The annotated program is

```

{x × y = 0 ∧ y ≤ x}
if y < 0 → {x × y = 0 ∧ y ≤ x ∧ y < 0} y := -y {x < y, Pf0}
| y = 0 → {x × y = 0 ∧ y ≤ x ∧ y = 0} x := -1 {x < y, Pf1}
fi
{x < y, Pf2}

```

Pf₀: Note that $x \times y = 0$ equals $x = 0 \vee y = 0$. Therefore

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

To prove the Hoare triple we reason:

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

Pf₁: We reason:

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

Pf₂: We reason:

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

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

```

var  $x : Int$ 
{ $P$ }
 $x := x + 1$ 
if  $x > 0 \rightarrow x := x + 1$ 
  |  $x < 0 \rightarrow x := x + 2$ 
  |  $x = 1 \rightarrow skip$ 
fi
{ $x \geq 1$ } .

```

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

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

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

We calculate the four conjuncts separately:

- $x > 0 \Rightarrow wp(x := x + 1)(x \geq 1)$
 $\Leftrightarrow x > 0 \Rightarrow x + 1 \geq 1$
 $\Leftrightarrow x > 0 \Rightarrow x \geq 0$
 $\Leftrightarrow \text{True} .$
- $x < 0 \Rightarrow wp(x := x + 2)(x \geq 1)$
 $\Leftrightarrow x < 0 \Rightarrow x + 2 \geq 1$
 $\Leftrightarrow x < 0 \Rightarrow x \geq -1$
 $\Leftrightarrow \{ (P \Rightarrow Q) = (\neg P \vee Q) \}$
 $x \geq 0 \vee x \geq -1$
 $\Leftrightarrow x \geq -1 .$

- $$\begin{aligned}
 & x = 1 \Rightarrow wp \text{ skip } (x \geq 1) \\
 & \Leftrightarrow x = 1 \Rightarrow x \geq 1 \\
 & \Leftrightarrow \text{True} .
 \end{aligned}$$
- Furthermore, $x > 0 \vee x < 0 \vee x = 1$ simplifies to $x \neq 0$.

Therefore,

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

Finally, recall what we want to compute:

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

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.

if $B_0 \rightarrow S_0 \mid B_1 \rightarrow S_1$ **fi**; S
if $B_0 \rightarrow S_0; S \mid B_1 \rightarrow S_1; S$ **fi**

Solution:

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

5. Consider the two programs:

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

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

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

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

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

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