Programming Languages: Imperative Program Construction
Practicals 4: Hoare Logic and Weakest Precondition: Loop

Shin-Cheng Mu

Autumn Term, 2021

1. Prove the correctness of the following program:

$$
\begin{array}{l}
\mathbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\} \\
\mathbf{var}\ \ x, y : \mathit{Int} \\
x, y := 0, 1 \\
\mathbf{do}\ x \neq N \rightarrow x, y := x + 1, y + y\ \mathbf{od} \\
\{y = 2^N\}
\end{array}
$$

Solution: Let $P\lambda equiv\ y = 2\uparrow x\ \tilde{}\backslash\ wedge{\sim}x\lambda leq\ N$. Use P as the invariant and $N - x$ as bound.

$$
\begin{array}{ll}
\mathbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\} & \\
\mathbf{var}\ \ x, y : \mathit{Int} & \\
x, y := 0, 1 & \text{-- Pf0} \\
\{P, \mathit{bnd} : N - x\} & \text{-- Pf2} \\
\mathbf{do}\ x \neq N \rightarrow \{P \wedge x \neq N\}\ x, y := x + 1, y + y\ \{P\}\ \mathbf{od} & \text{-- Pf1} \\
\{y = 2^N\} & \text{-- Pf3}
\end{array}
$$

Pf0.

$$
\begin{array}{ll}
 & (y = 2^x\ \wedge\ x \leqslant N)[x, y \backslash 0, 1] \\
\equiv & 1 = 2^0\ \wedge\ 0 \leqslant N \\
\Leftarrow & 0 \leqslant N\ .
\end{array}
$$

Pf1.

$$
\begin{array}{ll}
 & (y = 2^x\ \wedge\ x \leqslant N)[x, y \backslash x + 1, y + y] \\
\equiv & y + y = 2^x\ \wedge\ x + 1 \leqslant N \\
\Leftarrow & y = 2^x\ \wedge\ x \leqslant N \wedge x \neq N.
\end{array}
$$

Pf2. It is certainly true that

$$y = 2^x\ \wedge\ x \leqslant N \wedge x \neq N\ \ \Rightarrow\ \ N - x \geqslant 0.$$

Furthermore,

$$
\begin{array}{ll}
 & (N - x < C)[x, y \backslash x + 1, y + y] \\
\equiv & N - x - 1 < C \\
\Leftarrow & y = 2^x\ \wedge\ x \leqslant N \wedge x \neq N \wedge N - x = C.
\end{array}
$$

Pf3. It is immediate that

$$y = 2^x\ \wedge\ x \leqslant N \wedge x = N\ \ \Rightarrow\ \ y = 2^N.$$

2. Prove the correctness of the following program:

$$
\begin{array}{l}
\textbf{con } N : \mathit{Int} \ \{N \geqslant 0\} \\
\textbf{var } \ y : \mathit{Int} \\
y := 1 \\
\textbf{do } y < N \rightarrow y := y + y \ \textbf{od} \\
\{y \geqslant N \wedge \langle \exists k : k \geqslant 0 : y = 2^k \rangle\}
\end{array}
$$

Solution: We let the invariant be $\langle \exists k : k \geqslant 0 : y = 2^k \rangle$. The annotated program is:

$$
\begin{array}{ll}
\textbf{con } N : \mathit{Int} \ \{N \geqslant 0\} & \\
\textbf{var } \ y : \mathit{Int} & \\
y := 1 & \text{-- Pf0} \\
\{\langle \exists k : k \geqslant 0 : y = 2^k \rangle, \mathit{bnd} : N - y\} & \text{-- Pf1} \\
\textbf{do } y < N \rightarrow y := y + y \ \textbf{od} & \text{-- Pf2} \\
\{y \geqslant N \wedge \langle \exists k : k \geqslant 0 : y = 2^k \rangle\} & \text{-- Pf3}
\end{array}
$$

Pf_0. We reason:

$$
\begin{array}{cl}
 & \langle \exists k : k \geqslant 0 : y = 2^k \rangle[y \backslash 1] \\
\equiv & \langle \exists k : k \geqslant 0 : 1 = 2^k \rangle \\
\Leftarrow & \quad \{ \text{ range weakening } \} \\
 & \langle \exists k : k = 0 : 1 = 2^k \rangle \\
\equiv & \quad \{ \text{ one-point rule } \} \\
 & 1 = 2^0 \\
\equiv & \mathit{True} \ \ .
\end{array}
$$

Pf_1. Apparently $y < N$ implies $N - y \geqslant 0$. To prove that the bound decreases, we reason:

$$
\begin{array}{cl}
 & (N - y < C)[y \backslash y + y] \\
\equiv & N - (y + y) < C \\
\Leftarrow & N - y = C \wedge y > 0 \\
\Leftarrow & N - y = C \wedge \langle \exists k : k = 0 : 1 = 2^k \rangle \ \ .
\end{array}
$$

Pf_2. We reason:

$$
\begin{array}{cl}
 & \langle \exists k : k \geqslant 0 : y = 2^k \rangle[y \backslash y + y] \\
\equiv & \langle \exists k : k \geqslant 0 : y + y = 2^k \rangle \\
\Leftarrow & \langle \exists k : k \geqslant 0 : y = 2^k \rangle \ \ .
\end{array}
$$

Pf_3. Immediate.

3. Given integers $N \geqslant 0$ and $M > 0$, the following program computes integral division $N \,/\, M$. Prove its correctness.

con $N, M : Int$ $\{N \geqslant 0 \wedge M > 0\}$
var $l, r : Int$

$l, r := 0, N + 1$
do $l + 1 \neq r \rightarrow$
  if $((l + r) / 2) \times M \leqslant N \rightarrow l := (l + r) / 2$
  $|$ $((l + r) / 2) \times M > N \rightarrow r := (l + r) / 2$
  fi
od
$\{l \times M \leqslant N < (l + 1) \times M\}$

Solution: Let $P \equiv l \times M \leqslant N < r \times M \wedge 0 \leqslant l < r$. Use P as the invariant and $r - l$ as bound.

con $N, M : Int$ $\{N \geqslant 0 \wedge M > 0\}$
var $l, r : Int$

$l, r := 0, N + 1$ -- Pf0
$\{l \times M \leqslant N < r \times M \ \wedge \ 0 \leqslant l < r, bnd : r - l\}$ -- Pf3
do $l + 1 \neq r \rightarrow$
  if $((l + r) / 2) \times M \leqslant N \rightarrow l := (l + r) / 2$ -- Pf1
  $|$ $((l + r) / 2) \times M > N \rightarrow r := (l + r) / 2$ -- Pf2
  fi
od -- Pf4
$\{l \times M \leqslant N < (l + 1) \times M\}$

Pf_0. We reason:

$$\begin{aligned}
& (l \times M \leqslant N < r \times M \wedge 0 \leqslant l < r)[l, r \backslash 0, N + 1] \\
\equiv\ & 0 \times M \leqslant N < (N + 1) \times M \wedge 0 \leqslant 0 < N + 1 \\
\Leftarrow\ & 0 < M \wedge 0 \leqslant N \ .
\end{aligned}$$

Pf_1. We reason:

$$\begin{aligned}
& (l \times M \leqslant N < r \times M \ \wedge \ 0 \leqslant l < r)[l \backslash (l + r) / 2] \\
\equiv\ & ((l + r) / 2) \times M \leqslant N < r \times M \ \wedge \ 0 \leqslant (l + r) / 2 < r \\
\Leftarrow\ & l \times M \leqslant N < r \times M \ \wedge \ 0 \leqslant l < r \ \wedge \\
& ((l + r) / 2) \times M \leqslant N \ \wedge \ l + 1 \neq r \ .
\end{aligned}$$

Pf_2. We reason:

$$\begin{aligned}
& (l \times M \leqslant N < r \times M \ \wedge \ 0 \leqslant l < r)[r \backslash (l + r) / 2] \\
\equiv\ & l \times M \leqslant N < ((l + r) / 2) \times M \ \wedge \ 0 \leqslant l < (l + r) / 2 \\
\Leftarrow\ & l \times M \leqslant N < r \times M \ \wedge \ 0 \leqslant l < r \ \wedge \\
& N < ((l + r) / 2) \times M \ \wedge \ l + 1 \neq r \ .
\end{aligned}$$

Note that mere $0 \leqslant l < r$ does not guarantee $l < (l + r) / 2$ in integral division. We need $l + 1 \neq r$ here.

Pf_3. Termination. The invariant guarantees that $r - l \geqslant 0$. We need show that the bound decreases. For the first branch of **if**,

$$\begin{aligned}
& (r - l < C)[l \backslash (l + r) / 2] \\
\equiv\ & r - (l + r) / 2 < C \\
\Leftarrow\ & r - l = C \ \wedge \ l < (l + r) / 2 \\
\equiv\ & \quad \{ \text{ integer arithmetic } \} \\
& r - l = C \ \wedge \ 0 \leqslant l < r \ \wedge \ l + 1 \neq r \ .
\end{aligned}$$

Note that mere $0 \leqslant l < r$ does not guarantee $l < (l + r) / 2$ in integral division and we do need $l + 1 \neq r$ here. For the second branch we reason:

$$\begin{aligned}
& (r - l < C)[r \backslash (l + r) / 2] \\
\equiv\ & ((l + r) / 2) - l < C \\
\Leftarrow\ & r - l = C \ \wedge \ (l + r) / 2 < r \\
\equiv\ & \quad \{ \text{ integer arithmetic } \} \\
& r - l = C \ \wedge \ 0 \leqslant l < r \ .
\end{aligned}$$

Pf_4. Certainly, $l \times M \leqslant N < r \times M$ and $l + 1 = r$ implies $l \times M \leqslant N < (l + 1) \times M$.

4. The following program non-deterministically computes x and y such that $x \times y = N$. Prove:

con $N : Int \ \{N \geqslant 1\}$
var $p, x, y : Int$
$p, x, y := N - 1, 1, 1$
$\{N = x \times y + p \wedge ...\}$
do $p \neq 0 \rightarrow$
  if p **mod** $x = 0 \rightarrow y, p := y + 1, p - x$
    $\mid p$ **mod** $y = 0 \rightarrow x, p := x + 1, p - y$
  fi
od
$\{x \times y = N\}$

Solution: If we try reasoning about the first branch:

$$\begin{aligned}
& (N = x \times y + p)[y, p \backslash y + 1, p - x] \\
\equiv\ & N = x \times (y + 1) + p - x \\
\equiv\ & N = x \times y + p,
\end{aligned}$$

we notice that $N = x \times y + p$ does not need the guard p **mod** x to hold. The guards, however, do play a role in Pf2 to maintain the invariant.

We use the invariant

$$P \ : \ (N = x \times y + p) \ \wedge \ (0 \leqslant p) \ \wedge \ (0 < x) \ \wedge \ (0 < y) \ \wedge \ (p \ \mathbf{mod} \ x = 0 \vee p \ \mathbf{mod} \ y = 0)$$

and bound p.

con $N : Int \ \{N \geqslant 1\}$
var $p, x, y : Int$
$p, x, y := N - 1, 1, 1$ -- Pf0
$\{P, bnd : p\}$ -- Pf1
do $p \neq 0 \rightarrow$
  if p **mod** $x = 0 \rightarrow \{P \wedge p \neq 0 \wedge p \ \mathbf{mod} \ x = 0\}\ y, p := y + 1, p - x \ \{P\}$ -- Pf2
  $\mid p$ **mod** $y = 0 \rightarrow \{P \wedge p \neq 0 \wedge p \ \mathbf{mod} \ y = 0\}\ x, p := x + 1, p - y \ \{P\}$ -- Pf3
  fi
  $\{P\}$ -- Pf4
od
$\{x \times y = N\}$ -- Pf5

Pf0.

$$
\begin{aligned}
& P[p,x,y \backslash N-1,1,1] \\
\equiv\ & N = 1 + (N-1) \wedge 0 \leqslant N-1 \wedge 0 < 1 \wedge 0 < 1 \wedge ((N-1) \mathbf{\ mod\ } 1 = 0 \vee (N-1) \mathbf{\ mod\ } 1 = 0) \\
\Leftarrow\ & N \geqslant 1\ .
\end{aligned}
$$

Pf1. Apparently $P \wedge \neg(p \neq 0) \Rightarrow p \geqslant 0$. The bound p decreases after the assignment $p := p - x$ because $0 < x$. More precisely, for the first branch:

$$
\begin{aligned}
& (p < C)[y,p \backslash y+1, p-x] \\
\equiv\ & p - x < C \\
\Leftarrow\ & p = C \wedge x > 0 \\
\Leftarrow\ & p = C \wedge P \wedge p \neq 0.
\end{aligned}
$$

Similarly with the second branch (omitted).

Pf2. We reason:

$$
\begin{aligned}
& (N = x \times y + p\ \wedge\ 0 \leqslant p\ \wedge\ 0 < x\ \wedge\ 0 < y\ \wedge\ (p \mathbf{\ mod\ } x = 0 \vee p \mathbf{\ mod\ } y = 0))[y,p \backslash y+1, p-x] \\
\equiv\ & N = x \times (y+1) + (p-x)\ \wedge\ 0 \leqslant p - x\ \wedge\ 0 < x\ \wedge\ 0 < y+1 \wedge \\
& \quad ((p-x) \mathbf{\ mod\ } x = 0 \vee (p-x) \mathbf{\ mod\ } (y+1) = 0) \\
\Leftarrow\ & N = x \times y + p\ \wedge\ 0 \leqslant p\ \wedge\ 0 < x\ \wedge\ 0 < y\ \wedge\ (p \mathbf{\ mod\ } x = 0 \vee p \mathbf{\ mod\ } y = 0) \wedge p \mathbf{\ mod\ } x = 0.
\end{aligned}
$$

Examine more closely how the last $\Leftarrow$ holds.

(a) $N = x \times (y+1) + (p-x)$ and $N = x \times y + p$ are equivalent;

(b) $0 \leqslant p - x$ follows from $p \neq 0$ and $p \mathbf{\ mod\ } x = 0$ (if $p < x$, $p \mathbf{\ mod\ } x$ would be p);

(c) $((p-x) \mathbf{\ mod\ } x = 0 \vee (p-x) \mathbf{\ mod\ } (y+1) = 0)$, being a disjunction, follows from $p \mathbf{\ mod\ } x = 0$.

Pf3. We reason:

$$
\begin{aligned}
& (N = x \times y + p\ \wedge\ 0 \leqslant p\ \wedge\ 0 < x\ \wedge\ 0 < y\ \wedge\ (p \mathbf{\ mod\ } x = 0 \vee p \mathbf{\ mod\ } y = 0))[x,p \backslash x+1, p-y] \\
\equiv\ & N = (x+1) \times y + (p-y)\ \wedge\ 0 \leqslant p - y\ \wedge\ 0 < x+1\ \wedge\ 0 < y \wedge \\
& \quad ((p-y) \mathbf{\ mod\ } (x+1) = 0 \vee (p-y) \mathbf{\ mod\ } y = 0) \\
\Leftarrow\ & N = x \times y + p\ \wedge\ 0 \leqslant p\ \wedge\ 0 < x\ \wedge\ 0 < y\ \wedge\ (p \mathbf{\ mod\ } x = 0 \vee p \mathbf{\ mod\ } y = 0) \wedge p \mathbf{\ mod\ } y = 0.
\end{aligned}
$$

Pf4. Here we only have to show that $p \mathbf{\ mod\ } x = 0 \vee p \mathbf{\ mod\ } y = 0$, which is included in the invariant P.

Pf5. Certainly, $P \wedge p = 0 \Rightarrow x \times y = N$.

5. Prove the correctness of the following program:

$\mathbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\}$
$\mathbf{var}\ x, y : \mathit{Int}$
$x, y := 0, 0$
$\mathbf{do}\ x \neq 0\ \rightarrow x := x - 1$
$\mid\ \ y \neq N \rightarrow x, y := x + 1, y + 1$
$\mathbf{od}$
$\{x = 0 \wedge y = N\}$

Solution: Apparently the negation of the guards equivals $x = 0 \wedge y = N$. The difficult part is the proof of termination.

The variable x decreases in one of the branches, therefore we might want to have x in the bound. The variable y increases, therefore we might want $-y$ in the bound. And since each time y increment, x increment too, we weigh y twice as much as x. That gives us $x - 2 \times y$. And since the final value of $x - 2 \times y$ would be $-2\ N$, we add $2\ N$ to the bound. Thus we pick the bound to be $x + 2 \times (N - y)$.

Let the invariant be $P \equiv 0 \leqslant x \wedge 0 \leqslant y \leqslant N$. The annotated program is:

$$
\begin{array}{ll}
\textbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\} & \\
\textbf{var}\ x, y : \mathit{Int} & \\
x, y := 0, 0 & \text{-- Pf0} \\
\{P, \mathit{bnd} : x + 2 \times (N - y)\} & \text{-- Pf1} \\
\textbf{do}\ x \neq 0\ \rightarrow x := x - 1 & \text{-- Pf2} \\
\mid\ \ y \neq N \rightarrow x, y := x + 1, y + 1 & \text{-- Pf3} \\
\textbf{od} & \\
\{x = 0 \wedge y = N\} & \text{-- Pf4}
\end{array}
$$

Pf0. We reason:

$$
\begin{aligned}
& P[x, y \backslash 0, 0] \\
\equiv\ & 0 \leqslant 0 \wedge 0 \leqslant 0 \leqslant N \\
\equiv\ & 0 \leqslant N\ .
\end{aligned}
$$

Pf1. It is immediate that $P \wedge (x \neq 0 \vee y \neq N)$ implies $\mathit{bnd} \geqslant 0$. That the first branch decreases the bound is apparent. For the second branch we reason:

$$
\begin{aligned}
& (x + 2 \times (N - y) < C)[x, y \backslash x + 1, y + 1] \\
\equiv\ & (x + 1) + 2 \times (N - y - 1) < C \\
\equiv\ & x + 2 \times (N - y) + 1 - 2 < C \\
\Leftarrow\ & x + 2 \times (N - y) = C\ .
\end{aligned}
$$

Pf2.

$$
\begin{aligned}
& (0 \leqslant x \wedge 0 \leqslant y \leqslant N)[x \backslash x - 1] \\
\equiv\ & 0 \leqslant x - 1 \wedge 0 \leqslant y \leqslant N \\
\equiv\ & 0 \leqslant x \wedge 0 \leqslant y \leqslant N \wedge x \neq 0.
\end{aligned}
$$

Pf3.

$$
\begin{aligned}
& (0 \leqslant x \wedge 0 \leqslant y \leqslant N)[x, y \backslash x + 1, y + 1] \\
\equiv\ & 0 \leqslant x + 1 \wedge 0 \leqslant y + 1 \leqslant N \\
\Leftarrow\ & 0 \leqslant x \wedge 0 \leqslant y \leqslant N \wedge y \neq N.
\end{aligned}
$$

Pf4. Apparently, $\neg(x \neq 0 \vee y \neq N) \equiv x = 0 \wedge y = N$, and thus $P \wedge \neg(x \neq 0 \vee y \neq N) \Rightarrow x = 0 \wedge y = N$.

6. Prove the correctness of the following program:

$$
\begin{array}{l}
\mathbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\} \\
\mathbf{var}\ x, y : \mathit{Int} \\
x, y := 0, 0 \\
\mathbf{do}\ x \neq 0\ \ \rightarrow x := x - 1 \\
\mid\ \ y \neq N \rightarrow x, y := N, y + 1 \\
\mathbf{od} \\
\{x = 0 \wedge y = N\}
\end{array}
$$

Solution: Again, the negation of the guards equivals $x = 0 \wedge y = N$ and the difficult part is the proof of termination.

Since x decrements in one of the branches, we might want x in the bound. In another branch, $N - y$ decrements. However, x is set to N each time y decrements by 1. To balance that, one possible guess for the bound is $x + N \times (N - y)$. This turns out to be not sufficient (see Pf_1 below) — we need the increment of y to decrease the bound a bit more. The bound we choose turns out to be:

$$x + (N + 1) \times (N - y)\ \ .$$

To prove the bound we use the following P as the loop invariant:

$$P\ \equiv\ 0 \leqslant x \leqslant N \wedge 0 \leqslant y \leqslant N\ \ .$$

The invariant is only needed for proof of termination.

$$
\begin{array}{ll}
\mathbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\} & \\
\mathbf{var}\ x, y : \mathit{Int} & \\
x, y := 0, 0 & \text{-- Pf0} \\
\{P, \mathit{bnd} : x + (N + 1) \times (N - y)\} & \text{-- Pf1} \\
\mathbf{do}\ x \neq 0\ \ \rightarrow x := x - 1 & \text{-- Pf2} \\
\mid\ \ y \neq N \rightarrow x, y := N, y + 1 & \text{-- Pf3} \\
\mathbf{od} & \\
\{x = 0 \wedge y = N\} & \text{-- Pf4}
\end{array}
$$

Pf0. We reason:

$$
\begin{array}{l}
\quad P[x, y \backslash 0, 0] \\
\equiv 0 \leqslant 0 \leqslant N \wedge 0 \leqslant 0 \leqslant N \\
\equiv 0 \leqslant N\ \ .
\end{array}
$$

Pf1. It is immediate that $P \wedge (x \neq 0 \vee y \neq N)$ implies $\mathit{bnd} \geqslant 0$. That the first branch decreases the bound is apparent. For the second branch we reason:

$$
\begin{array}{l}
\quad (x + (N + 1) \times (N - y) < C)[x, y \backslash N, y + 1] \\
\equiv\ N + (N + 1) \times (N - y - 1) < C \\
\equiv\ N + (N + 1) \times (N - y) - (N + 1) < C \\
\equiv\ (-1) + (N + 1) \times (N - y) < C \\
\Leftarrow x + (N + 1) \times (N - y) = C \wedge 0 \leqslant x\ \ .
\end{array}
$$

Note that, had we use $x + N \times (N - y)$ as the bound, the proof would not go through:

$$
\begin{array}{l}
\quad (x + N \times (N - y) < C)[x, y \backslash N, y + 1] \\
\equiv\ N + N \times (N - y - 1) < C \\
\equiv\ N + N \times (N - y) - N < C \\
\equiv\ N \times (N - y) < C \\
\not\Leftarrow x + N \times (N - y) = C \wedge 0 \leqslant x\ \ \text{(since } x \text{ could be 0).}
\end{array}
$$

Pf2.

$$
\begin{aligned}
& (0 \leqslant x \leqslant N \land 0 \leqslant y \leqslant N)[x \backslash x - 1] \\
\equiv\ & 0 \leqslant x - 1 \leqslant N \land 0 \leqslant y \leqslant N \\
\equiv\ & 0 \leqslant x \leqslant N \land 0 \leqslant y \leqslant N \land x \neq 0.
\end{aligned}
$$

Pf3.

$$
\begin{aligned}
& (0 \leqslant x \leqslant N \land 0 \leqslant y \leqslant N)[x, y \backslash N, y + 1] \\
\equiv\ & 0 \leqslant N \leqslant N \land 0 \leqslant y + 1 \leqslant N \\
\Leftarrow\ & 0 \leqslant x \leqslant N \land 0 \leqslant y \leqslant N \land y \neq N.
\end{aligned}
$$

Pf4. Apparently, $\neg(x \neq 0 \lor y \neq N) \equiv x = 0 \land y = N$, and thus $P \land \neg(x \neq 0 \lor y \neq N) \Rightarrow x = 0 \land y = N$.