

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:

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $x, y : \text{Int}$ 
 $x, y := 0, 1$ 
do  $x \neq N \rightarrow x, y := x + 1, y + y$  od
 $\{y = 2^N\}$ 

```

Solution: Denote $y = 2^x \wedge x \leq N$ by P . Use P as the invariant and $N - x$ as bound.

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $x, y : \text{Int}$ 
 $x, y := 0, 1$  -- Pf0
 $\{P, \text{bnd} : N - x\}$  -- Pf2
do  $x \neq N \rightarrow \{P \wedge x \neq N\} x, y := x + 1, y + y \{P\}$  od -- Pf1
 $\{y = 2^N\}$  -- Pf3

```

Pf0.

$$\begin{aligned}
 & (y = 2^x \wedge x \leq N)[x, y \setminus 0, 1] \\
 \equiv & 1 = 2^0 \wedge 0 \leq N \\
 \Leftarrow & 0 \leq N.
 \end{aligned}$$

Pf1.

$$\begin{aligned}
 & (y = 2^x \wedge x \leq N)[x, y \setminus x + 1, y + y] \\
 \equiv & y + y = 2^x \wedge x + 1 \leq N \\
 \Leftarrow & y = 2^x \wedge x \leq N \wedge x \neq N.
 \end{aligned}$$

Pf2. It is certainly true that

$$y = 2^x \wedge x \leq N \wedge x \neq N \Rightarrow N - x \geq 0.$$

Furthermore,

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

Pf3. It is immediate that

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

2. Prove the correctness of the following program:

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $y : \text{Int}$ 
 $y := 1$ 
do  $y < N \rightarrow y := y + y$  od
 $\{y \geq N \wedge \langle \exists k : k \geq 0 : y = 2^k \rangle\}$ 

```

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

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $y : \text{Int}$ 
 $y := 1$  -- Pf0
 $\{\langle \exists k : k \geq 0 : y = 2^k \rangle, bnd : N - y\}$  -- Pf1
do  $y < N \rightarrow y := y + y$  od -- Pf2
 $\{y \geq N \wedge \langle \exists k : k \geq 0 : y = 2^k \rangle\}$  -- Pf3

```

Pf₀. We reason:

$$\begin{aligned}
 & \langle \exists k : k \geq 0 : y = 2^k \rangle [y \setminus 1] \\
 \equiv & \langle \exists k : k \geq 0 : 1 = 2^k \rangle \\
 \Leftarrow & \{ \text{range weakening} \} \\
 & \langle \exists k : k = 0 : 1 = 2^k \rangle \\
 \equiv & \{ \text{one-point rule} \} \\
 & 1 = 2^0 \\
 \equiv & \text{True} .
 \end{aligned}$$

Pf₁. Apparently $y < N$ implies $N - y \geq 0$. To prove that the bound decreases, we reason:

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

Pf₂. We reason:

$$\begin{aligned}
 & \langle \exists k : k \geq 0 : y = 2^k \rangle [y \setminus y + y] \\
 \equiv & \langle \exists k : k \geq 0 : y + y = 2^k \rangle \\
 \Leftarrow & \langle \exists k : k \geq 0 : y = 2^k \rangle .
 \end{aligned}$$

Pf₃. Immediate.

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

```

con  $N, M: \text{Int} \{N \geq 0 \wedge M > 0\}$ 
var  $l, r: \text{Int}$ 
 $l, r := 0, N + 1$ 
do  $l + 1 \neq r \rightarrow$ 
  if  $((l + r) / 2) \times M \leq N \rightarrow l := (l + r) / 2$ 
     $| ((l + r) / 2) \times M > N \rightarrow r := (l + r) / 2$ 
  fi
od
 $\{l \times M \leq N < (l + 1) \times M\}$ 

```

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

```

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

```

Pf₀. We reason:

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

Pf₁. We reason:

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

Pf₂. We reason:

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

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

Pf₃. Termination. The invariant guarantees that $r - l \geq 0$. We need show that the bound decreases. For the first branch of **if**,

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

Note that mere $0 \leq l < r$ 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:

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

Pf₄. Certainly, $l \times M \leq N < r \times M$ and $l+1 = r$ implies $l \times M \leq N < (l+1) \times M$.

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

```

con  $N : \text{Int} \{N \geq 1\}$ 
var  $p, x, y : \text{Int}$ 
 $p, x, y := N - 1, 1, 1$ 
 $\{N = x \times y + p \wedge \dots\}$ 
do  $p \neq 0 \rightarrow$ 
  if  $p \bmod x = 0 \rightarrow y, p := y + 1, p - x$ 
     $| p \bmod y = 0 \rightarrow x, p := x + 1, p - y$ 
  fi
od
 $\{x \times y = N\}$ 

```

Solution: If we try reasoning about the first branch:

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

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

We use the invariant

$$P : (N = x \times y + p) \wedge (0 \leq p) \wedge (0 < x) \wedge (0 < y) \wedge (p \bmod x = 0 \vee p \bmod y = 0)$$

and bound p .

```

con  $N : \text{Int} \{N \geq 1\}$ 
var  $p, x, y : \text{Int}$ 
 $p, x, y := N - 1, 1, 1$  -- Pf0
 $\{P, \text{bnd} : p\}$  -- Pf1
do  $p \neq 0 \rightarrow$ 
  if  $p \bmod x = 0 \rightarrow \{P \wedge p \neq 0 \wedge p \bmod x = 0\} y, p := y + 1, p - x \{P\}$  -- Pf2
     $| p \bmod y = 0 \rightarrow \{P \wedge p \neq 0 \wedge p \bmod y = 0\} x, p := x + 1, p - y \{P\}$  -- Pf3
  fi
   $\{P\}$  -- Pf4
od
 $\{x \times y = N\}$  -- Pf5

```

Pf0.

$$\begin{aligned}
& P[p, x, y \setminus N - 1, 1, 1] \\
& \equiv N = 1 + (N - 1) \wedge 0 \leq N - 1 \wedge 0 < 1 \wedge 0 < 1 \wedge ((N - 1) \bmod 1 = 0 \vee (N - 1) \bmod 1 = 0) \\
& \Leftarrow N \geq 1.
\end{aligned}$$

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

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

Similarly with the second branch (omitted).

Pf2. We reason:

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

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) $0 \leq p - x$ follows from $p \neq 0$ and $p \bmod x = 0$ (if $p < x$, $p \bmod x$ would be p);
- (c) $((p - x) \bmod x = 0 \vee (p - x) \bmod (y + 1) = 0)$, being a disjunction, follows from $p \bmod x = 0$.

Pf3. We reason:

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

Pf4. Here we only have to show that $p \bmod x = 0 \vee p \bmod y = 0$, 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:

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $x, y : \text{Int}$ 
 $x, y := 0, 0$ 
do  $x \neq 0 \rightarrow x := x - 1$ 
  |  $y \neq N \rightarrow x, y := x + 1, y + 1$ 
od
 $\{x = 0 \wedge y = N\}$ 

```

Solution: Apparently the negation of the guards equals $x = 0 \wedge y = N$. 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 $-2N$, we add $2N$ to the bound. Thus we pick the bound to be $x + 2 \times (N - y)$.

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

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $x, y : \text{Int}$ 
 $x, y := 0, 0$                                 -- Pf0
 $\{P, bnd : x + 2 \times (N - y)\}$                 -- Pf1
do  $x \neq 0 \rightarrow x := x - 1$                     -- Pf2
    |  $y \neq N \rightarrow x, y := x + 1, y + 1$     -- Pf3
od
 $\{x = 0 \wedge y = N\}$                             -- Pf4

```

Pf0. We reason:

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

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

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

Pf2.

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

Pf3.

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

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:

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $x, y : \text{Int}$ 
 $x, y := 0, 0$ 
do  $x \neq 0 \rightarrow x := x - 1$ 
  |  $y \neq N \rightarrow x, y := N, y + 1$ 
od
 $\{x = 0 \wedge y = N\}$ 

```

Solution: Again, the negation of the guards equals $x = 0 \wedge y = N$ 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 Pf₁ 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:

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

The invariant is only needed for proof of termination.

```

con  $N : \text{Int} \{N \geq 0\}$ 
var  $x, y : \text{Int}$ 
 $x, y := 0, 0$                                 -- Pf0
 $\{P, \text{bnd} : x + (N + 1) \times (N - y)\}$         -- Pf1
do  $x \neq 0 \rightarrow x := x - 1$                     -- Pf2
  |  $y \neq N \rightarrow x, y := N, y + 1$           -- Pf3
od
 $\{x = 0 \wedge y = N\}$                             -- Pf4

```

Pf0. We reason:

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

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

$$\begin{aligned}
& (x + (N + 1) \times (N - y) < C)[x, y \setminus N, y + 1] \\
& \equiv N + (N + 1) \times (N - y - 1) < C \\
& \equiv N + (N + 1) \times (N - y) - (N + 1) < C \\
& \equiv (-1) + (N + 1) \times (N - y) < C \\
& \Leftarrow x + (N + 1) \times (N - y) = C \wedge 0 \leq x .
\end{aligned}$$

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

$$\begin{aligned}
& (x + N \times (N - y) < C)[x, y \setminus N, y + 1] \\
& \equiv N + N \times (N - y - 1) < C \\
& \equiv N + N \times (N - y) - N < C \\
& \equiv N \times (N - y) < C \\
& \not\Leftarrow x + N \times (N - y) = C \wedge 0 \leq x \text{ (since } x \text{ could be 0).}
\end{aligned}$$

Pf2.

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

Pf3.

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

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