

Programming Languages: Imperative Program Construction

Practicals 5: Loop Constuction I

Shin-Cheng Mu

Autumn Term, 2022

1. Derive a program for the computation of square root.

```

con  $N : \text{Int} \{0 \leq N\}$ 
var  $x : \text{Int}$ 
squareroot
 $\{x^2 \leq N < (x+1)^2\}$  .
    
```

Solution: Try using $x^2 \leq N$ as the invariant and $\neg(N < (x+1)^2)$ as the guard. The program:

```

con  $N : \text{Int} \{0 \leq N\}$ 
var  $x : \text{Int}$ 
 $x := 0$  -- Pf0
 $\{x^2 \leq N, \text{bnd} : N - x\}$  -- Pf1
do  $(\neg(N < (x+1)^2)) \rightarrow$ 
     $x := x + 1$  -- Pf2
od
 $\{x^2 \leq N < (x+1)^2\}$  -- Pf3
    
```

Pf0.

$$\begin{aligned}
 & (x^2 \leq N)[x \setminus 0] \\
 & \equiv 0^2 \leq N \\
 & \equiv 0 \leq N .
 \end{aligned}$$

Pf1. To show that the bound is non-negative:

$$\begin{aligned}
 & 0 \leq N - x \\
 & \equiv x \leq N \\
 & \Leftarrow \{x \leq x^2 \text{ for integer } x\} \\
 & \quad x^2 \leq N \\
 & \Leftarrow x^2 \leq N \wedge \neg(N < (x+1)^2) .
 \end{aligned}$$

To show that the bound decreases:

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

Note: what would happen had we chosen $N - x^2$ as the bound?

$$\begin{aligned} & (x^2 \leq N)[x \setminus x + 1] \\ \text{Pf2. } & \equiv (x + 1)^2 \leq N \\ & \Leftarrow x^2 \leq N \wedge \neg (N < (x + 1)^2) . \end{aligned}$$

Pf3. Certainly,

$$\begin{aligned} & x^2 \leq N \wedge \neg (\neg (N < (x + 1)^2)) \\ & \equiv x^2 \leq N < (x + 1)^2 . \end{aligned}$$

2. Find substitutions (on variables) that satisfy the following implications. (As a convention, variables start with small letters while constants start with capital letters. We assume that all variables and constants are *Int*.)
- (a) $(x = 2 \times E)[? \setminus ?] \Leftarrow x = E$.
 - (b) $(x = 2 \times E + A)[? \setminus ?] \Leftarrow x = E$.
 - (c) $(x = f E)[? \setminus ?] \Leftarrow x = E$, for some function f .
 - (d) $(x = A)[? \setminus ?] \Leftarrow x = 2 \times A + B \wedge \dots$. You may need to discover an additional side condition in place of ... to make the implication valid.
 - (e) $(A = 2 \times b \times x + c)[? \setminus ?] \Leftarrow A = b \times x + c \wedge \dots$. Again you may need an additional condition in
 - (f) $(A = B \times x + B + C)[? \setminus ?] \Leftarrow A = B \times x + C$.
 - (g) $(A = B \times x / 2 + 2 \times C)[? \setminus ?] \Leftarrow A = B \times x + C \wedge \dots$

Solution:

- (a) $[x \setminus 2 \times x]$.
- (b) $[x \setminus 2 \times x + A]$.
- (c) $[x \setminus f x]$.
- (d) One may choose $[x \setminus ((x - B) / 2)]$, and the side condition would be *even* $(x - B)$. That is,

$$\begin{aligned} & (x = A)[x \setminus ((x - B) / 2)] \\ & \equiv (x - B) / 2 = A \\ & \Leftarrow x = 2 \times A + B \wedge \text{even}(x - B) . \end{aligned}$$

- (e) $[x \setminus (x/2)]$ with additional condition *even* x , $[b \setminus (b/2)]$ with additional condition *even* b , or $[c \setminus (c - b \times x)]$.
- (f) $[x \setminus x - 1]$.
- (g) $[x \setminus (2 \times x - 2 \times C / B)]$, with side condition $2 \times C \text{ 'mod' } B = 0$, that is B divides $2 \times C$.

3. **The Zune problem.** Let D be the number of days since 1st January 1980. What is the current year? Assume that there exists a function $\text{daysInYear} : \text{Int} \rightarrow \text{Int}$ such that $\text{daysInYear } i$, with $i \geq 1980$, yields the number of days in year i , which is always a positive number. Derive a program having two variables y and d such that, upon termination, y is the current year, and d is the number of days since the beginning of this year.
- (a) How would you specify the problem? The specification may look like:

```

con  $D : \text{Int} \{0 \leq D\}$ 
var  $y, d : \text{Int}$ 

zune
{???}

```

What would you put as the postcondition? In this postcondition, is 1st January 1980 day 0 or 1?

Solution: One of the possibilities is

$$\langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 0 \leq d < \text{daysInYear } y .$$

This specification implies that 1st January 1980 is day 0 and, days in year i are counted as 0, 1 ... $\text{daysInYear } i - 1$.

(b) Derive the program.

Solution: We choose $\langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 0 \leq d$ as the loop invariant, and $\neg (d < \text{daysInYear } y)$ as guard. During the development we will see that we need $1980 \leq y$ in the invariant, to allow splitting. The resulting program is:

```

con  $D : \text{Int } \{0 \leq D\}$ 
var  $y, d : \text{Int}$ 
 $y, d := 1980, D$  -- Pf0
 $\{ \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 1980 \leq y \wedge 0 \leq d, \text{bnd} : d \}$ 
do  $d \geq \text{daysInYear } y \rightarrow$  -- Pf1
     $d := d - \text{daysInYear } y$  -- Pf2
     $y := y + 1$ 
od
 $\{ \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 0 \leq d < \text{daysInYear } y \}$  -- Pf3

```

Pf0.

$$\begin{aligned}
 & (\langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 1980 \leq y \wedge 0 \leq d)[y, d \setminus 1980, D] \\
 & \equiv \langle \sum i : 1980 \leq i < 1980 : \text{daysInYear } i \rangle + D = D \wedge 1980 \leq 1980 \wedge 0 \leq D \\
 & \equiv 0 + D = D \wedge 0 \leq D \\
 & \equiv 0 \leq D .
 \end{aligned}$$

Pf1. That $0 \leq d$ follows from the loop invariant. To show that d decreases, we need to know that $\text{daysInYear } y$ is always positive:

$$\begin{aligned}
 & ((d < C)[y \setminus y + 1])[d \setminus d - \text{daysInYear } y] \\
 & \equiv d - \text{daysInYear } y < C \\
 & \Leftarrow \{ \text{daysInYear } y \text{ positive} \} \\
 & \quad d = C \\
 & \Leftarrow \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 1980 \leq y \wedge 0 \leq d \wedge d \geq \text{daysInYear } y \wedge d = C .
 \end{aligned}$$

Pf2. Assuming $1980 \leq y$, consider

$$\begin{aligned}
 & \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle[y \setminus y + 1] \\
 & = \langle \sum i : 1980 \leq i < y + 1 : \text{daysInYear } i \rangle \\
 & = \{ \text{since } 1980 \leq y, \text{splitting off } i = y \} \\
 & \quad \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + \text{daysInYear } y .
 \end{aligned}$$

Therefore,

$$\begin{aligned}
 & ((\langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge \\
 & \quad 1980 \leq y \wedge 0 \leq d)[y \setminus y + 1])[d \setminus d - \text{daysInYear } y] \\
 & \equiv \langle \sum i : 1980 \leq i < y + 1 : \text{daysInYear } i \rangle + (d - \text{daysInYear } y) = D \wedge \\
 & \quad 1980 \leq y + 1 \wedge 0 \leq d - \text{daysInYear } y \\
 & \Leftarrow \{ \text{calculation above, } 1980 \leq y + 1 \Leftarrow 1980 \leq y \} \\
 & \quad \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + \text{daysInYear } y + (d - \text{daysInYear } y) = D \wedge \\
 & \quad 1980 \leq y \wedge d \geq \text{daysInYear } y \\
 & \Leftarrow \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 1980 \leq y \wedge 0 \leq d \wedge d \geq \text{daysInYear } y .
 \end{aligned}$$

Pf3. Certainly,

$$\begin{aligned} \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 1980 \leq y \wedge 0 \leq d \wedge \\ \neg (d \geq \text{daysInYear } y) \Rightarrow \\ \langle \sum i : 1980 \leq i < y : \text{daysInYear } i \rangle + d = D \wedge 0 \leq d < \text{daysInYear } y . \end{aligned}$$

4. Assuming that $-\infty$ is the identity element of (\uparrow) . Derive a solution for:

```

con  $N : \text{Int } \{N \geq 0\}$ 
con  $A : \text{array } [0..N] \text{ of } \text{Int}$ 
var  $r : \text{Int}$ 
 $S$ 
 $\{r = \langle \uparrow i : 0 \leq i < N : A[i] \rangle\}$  .

```

Solution:

```

con  $N : \text{Int } \{N \geq 0\}$ 
con  $A : \text{array } [0..N] \text{ of } \text{Int}$ 
var  $r, n : \text{Int}$ 
 $r, n := -\infty, 0$  -- Pf0
 $\{r = \langle \uparrow i : 0 \leq i < n : A[i] \rangle \wedge 0 \leq n \leq N, \text{bnd} : N - n\}$ 
do  $n \neq N \rightarrow$  -- Pf1
   $r := r \uparrow A[n]$  -- Pf2
   $n := n + 1$ 
od
 $\{r = \langle \uparrow i : 0 \leq i < N : A[i] \rangle\}$  -- Pf3

```

Pf0.

$$\begin{aligned} (r = \langle \uparrow i : 0 \leq i < n : A[i] \rangle \wedge 0 \leq n \leq N)[r, n \setminus -\infty, 0] \\ \equiv -\infty = \langle \uparrow i : 0 \leq i < 0 : A[i] \rangle \wedge 0 \leq 0 \leq N \\ \equiv 0 \leq N . \end{aligned}$$

Pf1. Apparently, $0 \leq n \leq N \Rightarrow N - n \geq 0$, and

$$\begin{aligned} ((N - n < C)[n \setminus n + 1])[r \setminus r \uparrow A[n]] \\ \equiv N - (n + 1) < C \\ \Leftarrow N - n = C . \end{aligned}$$

Pf2. We reason:

$$\begin{aligned} ((r = \langle \uparrow i : 0 \leq i < n : A[i] \rangle \wedge 0 \leq n \leq N)[n \setminus n + 1])[r \setminus r \uparrow A[n]] \\ \equiv r \uparrow A[n] = \langle \uparrow i : 0 \leq i < n + 1 : A[i] \rangle \wedge 0 \leq n + 1 \leq N \\ \Leftarrow \{ \text{assuming } 0 \leq n < N, \text{split off } i = n \} \\ r \uparrow A[n] = \langle \uparrow i : 0 \leq i < n : A[i] \rangle \uparrow A[n] \wedge 0 \leq n < N \\ \Leftarrow r = \langle \uparrow i : 0 \leq i < n : A[i] \rangle \wedge 0 \leq n \leq N \wedge n \neq N . \end{aligned}$$

Pf3. It is immediate that

$$\begin{aligned} r = \langle \uparrow i : 0 \leq i < n : A[i] \rangle \wedge 0 \leq n \leq N \wedge n = N \\ \Rightarrow r = \langle \uparrow i : 0 \leq i < N : A[i] \rangle . \end{aligned}$$

5. Derive a solution for:

```

con  $N, X : \text{Int } \{0 \leq N\}$ 
con  $A : \text{array } [0..N) \text{ of } \text{Int}$ 
var  $r : \text{Int}$ 
 $S$ 
 $\{r = \langle \sum i : 0 \leq i < N : A[i] \times X^i \rangle\} .$ 

```

Solution: For efficiency, add a variable x and use the invariant:

$$r = \langle \sum i : 0 \leq i < n : A[i] \times X^i \rangle \wedge x = X^n \wedge 0 \leq n \leq N .$$

Denote it by P . The program:

```

con  $N, X : \text{Int } \{0 \leq N\}$ 
con  $A : \text{array } [0..N) \text{ of } \text{Int}$ 
var  $r, x, n : \text{Int}$ 
 $r, x, n := 0, 1, 0$                                 -- Pf0
 $\{P, bnd : N - n\}$ 
do  $n \neq N \rightarrow$                                      -- Pf1
     $r, x := r + A[n] \times x, x \times X$                 -- Pf2
     $n := n + 1$ 
od
 $\{r = \langle \sum i : 0 \leq i < N : A[i] \times X^i \rangle\}$  -- Pf3

```

Pf0.

$$\begin{aligned}
 &P[r, x, n \setminus 0, 1, 0] \\
 &\equiv 0 = \langle \sum i : 0 \leq i < 0 : A[i] \times X^i \rangle \wedge 1 = X^0 \wedge 0 \leq 0 \leq N \\
 &\Leftarrow 0 \leq N .
 \end{aligned}$$

Pf1. Apparently, $0 \leq n \leq N \Rightarrow N - n \geq 0$, and

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

Pf2. We reason:

$$\begin{aligned}
 &((r = \langle \sum i : 0 \leq i < n : A[i] \times X^i \rangle \wedge x = X^n \wedge 0 \leq n \leq N)[n \setminus n + 1])[r, x \setminus r + A[n] \times x, x \times X] \\
 &\equiv r + A[n] \times x = \langle \sum i : 0 \leq i < n + 1 : A[i] \times X^i \rangle \wedge x \times X = X^{n+1} \wedge 0 \leq n + 1 \leq N \\
 &\Leftarrow \{ \text{assuming } 0 \leq n < N, \text{ split off } i = n \} \\
 &\quad r + A[n] \times x = \langle \sum i : 0 \leq i < n : A[i] \times X^i \rangle + A[n] \times x^n \wedge x \times X = X^{n+1} \wedge 0 \leq n < N \\
 &\Leftarrow r = \langle \sum i : 0 \leq i < n : A[i] \times X^i \rangle \wedge x = X^n \wedge 0 \leq n \leq N \wedge n \neq N .
 \end{aligned}$$

Pf3. It is immediate that

$$\begin{aligned}
 &r = \langle \sum i : 0 \leq i < n : A[i] \times X^i \rangle \wedge x = X^n \wedge 0 \leq n \leq N \wedge n = N \\
 &\Rightarrow r = \langle \sum i : 0 \leq i < N : A[i] \times X^i \rangle .
 \end{aligned}$$

Another possibility, however, is to define for $0 \leq n \leq N$:

$$k\ n = \langle \sum i : n \leq i < N : A[i] \times X^{i-n} \rangle ,$$

use the invariant $r = k\ n \wedge 0 \leq n \leq N$, and decrement n in the loop.