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 $N : Int$ $\{0 \leqslant N\}$
   var $x : Int$
   squareroot
   $\{x^2 \leqslant N < (x+1)^2\}$.

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

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

Pf0.

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

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

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

To show that the bound decreases:

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

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

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

Pf3. Certainly,

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

2. For each implication below, find a substitution (on variables) such that the implication holds. Note:

   - Names starting with small letters (x, a, b, etc) are variables, while A, B, and C are constants. E denotes an expression.
   - We assume that all variables and constants are *Int*.
   - For some questions, there could be more than one substitutions that work.

   (a) $(x = 2 \times E)[?\backslash ?] \Leftarrow x = E$, where x does not occur free in E.

   (b) $(x = 2 \times E + A)[?\backslash ?] \Leftarrow x = E$, where x does not occur free in E.

   (c) $(x = f\ E)[?\backslash ?] \Leftarrow x = E$, for some function f. Again, x does not occur free in E.

   (d) $(x = A)[?\backslash ?] \Leftarrow x = 2 \times A + B$.

   (e) $(A = 2 \times b \times x + c)[?\backslash ?] \Leftarrow A = b \times x + c \wedge \ldots$. You may need to discover an additional condition in ... to make the implication valid.

   (f) $(A = B \times x + B + C)[?\backslash ?] \Leftarrow A = B \times x + C$.

   (g) $(A = B \times x\ /\ 2 + 2 \times C)[?\backslash ?] \Leftarrow A = B \times x + C \wedge \ldots$. You will need a side condition. Note that $(\times)$ and $(/)$ are left-associative. That is, $B \times X\ /\ C$ is interpreted as $(B \times X)\ /\ C$.

Solution:

(a) $[x\backslash 2 \times x]$.

(b) $[x\backslash 2 \times x + A]$.

(c) $[x\backslash f\ x]$.

(d) One may choose $[x\backslash((x - B)\ /\ 2)]$. That is,

$$\begin{aligned} & (x = A)[x\backslash((x - B)\ /\ 2)] \\ \equiv\ & (x - B)\ /\ 2 = A \\ \equiv\ & x = 2 \times A + B\ . \end{aligned}$$

Another possibility could be: $[x\backslash(x - A) - B]$:

$$\begin{aligned} & (x = A)[x\backslash(x - A) - B] \\ \equiv\ & (x - A) - B = A \\ \equiv\ & x = 2 \times A + B\ . \end{aligned}$$

(e) One may choose $[x\backslash(x \;/\; 2)]$ with an additional condition *even x*:

$$\begin{array}{ll} & (A = 2 \times b \times x + c)[x\backslash x \;/\; 2] \\ \equiv & A = 2 \times b \times (x \;/\; 2) + c \\ \Leftarrow & A = b \times x + c \wedge even\ x \quad . \end{array}$$

Note that, since $x{:}Int$ and $(/)$ is integral division, we need *even x* to guarantee that $2 \times b \times (x/2) = b \times x$. One could also choose $[b\backslash(b \;/\; 2)]$ with an additional condition *even b*, or $[c\backslash(c - b \times x)]$.

(f) $[x\backslash x - 1]$.

(g) $[x\backslash(2 \times x - 2 \times C \;/\; B)]$, with side condition $2 \times C$ ‘*mod*‘ $B = 0$, that is B divides $2 \times C$:

$$\begin{array}{ll} & (A = B \times x \;/\; 2 + 2 \times C)[x\backslash(2 \times x - 2 \times C \;/\; B)] \\ \equiv & A = B \times (2 \times x - 2 \times C \;/\; B) \;/\; 2 + 2 \times C \\ \equiv & A = (B \times 2 \times x - B \times 2 \times C \;/\; B) \;/\; 2 + 2 \times C \\ \Leftarrow & \quad \{\ B \times X \;/\; B = X \text{ if } B \text{ divides } X\ \} \\ & A = (B \times 2 \times x - 2 \times C) \;/\; 2 + 2 \times C \wedge 2 \times C \text{ ‘}mod\text{‘ } B = 0 \\ \equiv & A = B \times x - C + 2 \times C \wedge 2 \times C \text{ ‘}mod\text{‘ } B = 0 \\ \equiv & A = B \times x + C \wedge 2 \times C \text{ ‘}mod\text{‘ } B = 0 \quad . \end{array}$$

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 $daysInYear : Int \rightarrow Int$ such that $daysInYear\ i$, with $i \geqslant 1980$, 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 $D : Int\ \{0 \leqslant D\}$
var $y, d : Int$

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

$$\langle \Sigma i : 1980 \leqslant i < y : daysInYear\ i \rangle + d = D \wedge 0 \leqslant d < daysInYear\ y \quad .$$

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

(b) Derive the program.

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

$$
\begin{array}{ll}
\textbf{con}\ D : \mathit{Int}\ \{0 \leqslant D\} & \\
\textbf{var}\ y, d : \mathit{Int} & \\
y, d := 1980, D & \text{-- Pf0} \\
\{\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 1980 \leqslant y \wedge 0 \leqslant d, \mathit{bnd} : d\} & \\
\textbf{do}\ d \geqslant \mathit{daysInYear}\ y \rightarrow & \text{-- Pf1} \\
\quad d := d - \mathit{daysInYear}\ y & \text{-- Pf2} \\
\quad y := y + 1 & \\
\textbf{od} & \\
\{\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 0 \leqslant d < \mathit{daysInYear}\ y\} & \text{-- Pf3}
\end{array}
$$

Pf0.

$$
\begin{array}{ll}
 & (\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 1980 \leqslant y \wedge 0 \leqslant d)[y, d \backslash 1980, D] \\
\equiv & \langle \Sigma i : 1980 \leqslant i < 1980 : \mathit{daysInYear}\ i\rangle + D = D \wedge 1980 \leqslant 1980 \wedge 0 \leqslant D \\
\equiv & 0 + D = D \wedge 0 \leqslant D \\
\equiv & 0 \leqslant D\ .
\end{array}
$$

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

$$
\begin{array}{ll}
 & ((d < C)[y \backslash y + 1])[d \backslash d - \mathit{daysInYear}\ y] \\
\equiv & d - \mathit{daysInYear}\ y < C \\
\Leftarrow & \quad \{\ \mathit{daysInYear}\ y \text{ positive }\} \\
 & d = C \\
\Leftarrow & \langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 1980 \leqslant y \wedge 0 \leqslant d \wedge d \geqslant \mathit{daysInYear}\ y \wedge d = C\ .
\end{array}
$$

Pf2. Assuming $1980 \leqslant y$, consider

$$
\begin{array}{ll}
 & \langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle[y \backslash y + 1] \\
= & \langle \Sigma i : 1980 \leqslant i < y + 1 : \mathit{daysInYear}\ i\rangle \\
= & \quad \{\ \text{since } 1980 \leqslant y, \text{ splitting off } i = y\ \} \\
 & \langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + \mathit{daysInYear}\ y\ .
\end{array}
$$

Therefore,

$$
\begin{array}{ll}
 & ((\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge \\
 & \quad 1980 \leqslant y \wedge 0 \leqslant d)[y \backslash y + 1])[d \backslash d - \mathit{daysInYear}\ y] \\
\equiv & \langle \Sigma i : 1980 \leqslant i < y + 1 : \mathit{daysInYear}\ i\rangle + (d - \mathit{daysInYear}\ y) = D \wedge \\
 & \quad 1980 \leqslant y + 1 \wedge 0 \leqslant d - \mathit{daysInYear}\ y \\
\Leftarrow & \quad \{\ \text{calculation above, } 1980 \leqslant y + 1 \Leftarrow 1980 \leqslant y\ \} \\
 & \langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + \mathit{daysInYear}\ y + (d - \mathit{daysInYear}\ y) = D \wedge \\
 & \quad 1980 \leqslant y \wedge d \geqslant \mathit{daysInYear}\ y \\
\Leftarrow & \langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 1980 \leqslant y \wedge 0 \leqslant d \wedge d \geqslant \mathit{daysInYear}\ y\ .
\end{array}
$$

Pf3. Certainly,

$$
\begin{array}{l}
\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 1980 \leqslant y \wedge 0 \leqslant d \wedge \\
\quad \neg\,(d \geqslant \mathit{daysInYear}\ y) \Rightarrow \\
\qquad \langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i\rangle + d = D \wedge 0 \leqslant d < \mathit{daysInYear}\ y\ .
\end{array}
$$

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

$$
\begin{array}{l}
\textbf{con } N : \mathit{Int}\ \{N \geqslant 0\} \\
\textbf{con } A : \textbf{array } [0..N) \textbf{ of } \mathit{Int} \\
\textbf{var } r : \mathit{Int} \\
S \\
\{r = \langle \uparrow i : 0 \leqslant i < N : A[i] \rangle\} \ .
\end{array}
$$

Solution:

$$
\begin{array}{ll}
\textbf{con } N : \mathit{Int}\ \{N \geqslant 0\} & \\
\textbf{con } A : \textbf{array } [0..N) \textbf{ of } \mathit{Int} & \\
\textbf{var } r, n : \mathit{Int} & \\
r, n := -\infty, 0 & \text{-- Pf0} \\
\{r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \wedge 0 \leqslant n \leqslant N, \mathit{bnd} : N - n\} & \\
\textbf{do } n \neq N \rightarrow & \text{-- Pf1} \\
\quad r := r \uparrow A\ [n] & \text{-- Pf2} \\
\quad n := n + 1 & \\
\textbf{od} & \\
\{r = \langle \uparrow i : 0 \leqslant i < N : A[i] \rangle\} & \text{-- Pf3}
\end{array}
$$

Pf0.

$$
\begin{array}{ll}
& (r = \langle \uparrow i : 0 \leqslant i < n : A\ [i] \rangle \wedge 0 \leqslant n \leqslant N)[r, n \backslash -\infty, 0] \\
\equiv & -\infty = \langle \uparrow i : 0 \leqslant i < 0 : A\ [i] \rangle \wedge 0 \leqslant 0 \leqslant N \\
\equiv & 0 \leqslant N \ .
\end{array}
$$

Pf1. Apparently, $0 \leqslant n \leqslant N \Rightarrow N - n \geqslant 0$, and

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

Pf2. We reason:

$$
\begin{array}{ll}
& ((r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \wedge 0 \leqslant n \leqslant N)[n \backslash n + 1])[r \backslash r \uparrow A[n]] \\
\equiv & r \uparrow A[n] = \langle \uparrow i : 0 \leqslant i < n + 1 : A[i] \rangle \wedge 0 \leqslant n + 1 \leqslant N \\
\Leftarrow & \quad \{ \text{ assuming } 0 \leqslant n < N, \text{ split off } i = n \ \} \\
& r \uparrow A[n] = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \uparrow A[n] \wedge 0 \leqslant n < N \\
\Leftarrow & r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \wedge 0 \leqslant n \leqslant N \wedge n \neq N \ .
\end{array}
$$

Pf3. It is immediate that

$$
\begin{array}{l}
r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \ \wedge \ 0 \leqslant n \leqslant N \wedge n = N \\
\quad \Rightarrow r = \langle \uparrow i : 0 \leqslant i < N : A[i] \rangle \ .
\end{array}
$$

5. Derive a solution for:

$\mathbf{con}\ N, X : Int\ \{0 \leqslant N\}$
$\mathbf{con}\ A : \mathbf{array}\ [0..N)\ \mathbf{of}\ Int$
$\mathbf{var}\ r : Int$

S
$\{r = \langle \Sigma i : 0 \leqslant i < N : A\,[\,i\,] \times X^i \rangle\}$.

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

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

Denote it by P. The program:

$\mathbf{con}\ N, X : Int\ \{0 \leqslant N\}$
$\mathbf{con}\ A : \mathbf{array}\ [0..N)\ \mathbf{of}\ Int$
$\mathbf{var}\ r, x, n : Int$

$r, x, n := 0, 1, 0$ -- Pf0
$\{P, bnd : N - n\}$
$\mathbf{do}\ n \neq N \rightarrow$ -- Pf1
  $r, x := r + A\,[\,n\,] \times x, x \times X$ -- Pf2
  $n := n + 1$
$\mathbf{od}$
$\{r = \langle \Sigma i : 0 \leqslant i < N : A\,[\,i\,] \times X^i \rangle\}$ -- Pf3

Pf0.

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

Pf1. Apparently, $0 \leqslant n \leqslant N \Rightarrow N - n \geqslant 0$, and

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

Pf2. We reason:

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

Pf3. It is immediate that

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

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

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

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