Programming Languages: Imperative Program Construction
Practicals 5: Loop Constuction I

Shin-Cheng Mu

Autumn Term, 2021

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?

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

Pf3. Certainly,

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

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) $(x = 2 \times E)[?\backslash ?] \Leftarrow x = E$.
   (b) $(x = 2 \times E + A)[?\backslash ?] \Leftarrow x = E$.
   (c) $(x = f\ E)[?\backslash ?] \Leftarrow x = E$, for some function f.
   (d) $(x = A)[?\backslash ?] \Leftarrow x = 2 \times A + B \wedge ....$ You may need to discover an additional side condition in place of ... to make the implication valid.
   (e) $(A = 2 \times b \times x + c)[?\backslash ?] \Leftarrow A = b \times x + c \wedge ....$ Again you may need an additional condition in ....
   (f) $(A = B \times x + B + C)[?\backslash ?] \Leftarrow A = B \times x + C$.
   (g) $(A = B \times x\ /\ 2 + 2 \times C)[?\backslash ?] \Leftarrow A = B \times x + C \wedge ....$

Solution:

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

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

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

(d) One may choose $[x\backslash((x - B)\ /\ 2)]$, and the side condition would be *even* $(x - B)$. That is,

$$
\begin{array}{rl}
 & (x = A)[x\backslash((x - B)\ /\ 2)] \\
\equiv & (x - B)\ /\ 2 = A \\
\Leftarrow & x = 2 \times A + B \wedge \mathit{even}\ (x - B) \ .
\end{array}
$$

(e) $[x\backslash(x/2)]$ with additional condition *even* x, $[b\backslash(b/2)]$ with 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 $2 \times C$.

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

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

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

(b) Derive the program.

Solution: We choose $\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i \rangle + d = D \wedge 0 \leqslant d$ as the loop invariant, and $\neg\ (d < \mathit{daysInYear}\ y)$ 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,

$$\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i \rangle + d = D \land 1980 \leqslant y \land 0 \leqslant d \land$$
$$\neg\,(d \geqslant \mathit{daysInYear}\ y) \Rightarrow$$
$$\langle \Sigma i : 1980 \leqslant i < y : \mathit{daysInYear}\ i \rangle + d = D \land 0 \leqslant d < \mathit{daysInYear}\ y \enspace .$$

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

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

Solution:

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

Pf0.

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

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

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

Pf2. We reason:

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

Pf3. It is immediate that

$$\begin{aligned} & r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \ \land\ 0 \leqslant n \leqslant N \land n = N \\ & \quad \Rightarrow r = \langle \uparrow i : 0 \leqslant i < N : A[i] \rangle \enspace . \end{aligned}$$

5. Derive a solution for:

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

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:

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

Pf0.

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

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

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

Pf2. We reason:

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

Pf3. It is immediate that

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

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.