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

> **Solution:** Try using $x^2 \leqslant N$ as the invariant and $\neg((x+1)^2 > N)$ as the guard. The program:
>
> **con** $N : \mathit{Int}\ \{0 \leqslant N\}$
> **var** $x : \mathit{Int}$
> $x := 0$ -- Pf0
> $\{x^2 \leqslant N, \mathit{bnd} : N - x\}$ -- Pf1
> **do** $(\neg\ ((x+1)^2 > N)) \rightarrow$
> $\quad x := x + 1$ -- Pf2
> **od**
> $\{x^2 \leqslant N \land (x+1)^2 > N\}$ -- Pf3
>
> Pf0. It follows from the assumption that $0^2 \leqslant N$.
>
> Pf1. It's trivial that $N - x$ decreases.
>
> Pf2.
>
> $$\begin{aligned} & (x \leqslant N)[x \backslash x+1] \\ \equiv\ & (x+1)^2 \leqslant N \\ \Leftarrow\ & x^2 \leqslant N \land \neg((x+1)^2 > N). \end{aligned}$$
>
> Pf3. Trivial.

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

(e) $(A = 2 \times b \times x + c)[?\backslash?] \Leftarrow A = b \times x + c$.
(f) $(A = B \times x + B + C)[?\backslash?] \Leftarrow A = B \times x + C$.
(g) $(A = B \times x \,/\, 2 + 2 \times C)[?\backslash?] \Leftarrow A = B \times x + C$.

Solution:

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

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

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

(d) $[x\backslash((x - B) \,/\, 2)]$.

(e) $[x\backslash(x \,/\, 2)]$, $[b\backslash(b \,/\, 2)]$, or $[c\backslash(c - b \times x)]$.

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

(g) $[x\backslash(2 \times x - 2 \times C \,/\, B)]$.

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 $daysInYear : Int \to Int$ 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

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

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:

con $D : Int\ \{0 \leqslant D\}$
var $y, d : Int$
$y, d := 1980, D$ -- Pf0
$\{\langle \Sigma i : 1980 \leqslant i < y : daysInYear\ i \rangle + d = D \wedge 1980 \leqslant y \wedge 0 \leqslant d, bnd : d\}$
do $d \geqslant daysInYear\ y \to$ -- Pf1
  $d := d - daysInYear\ y$ -- Pf2
  $y := y + 1$
od
$\{\langle \Sigma i : 1980 \leqslant i < y : daysInYear\ i \rangle + d = D \wedge 0 \leqslant d < daysInYear\ y\}$ -- Pf3

Pf0.

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

Pf1 That $0 \leqslant d$ follows from the loop invariant, and that d decreases follows from that $daysInYear\ y$ is positive.

Pf2 Assuming $1980 \leqslant y$, consider

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

Therefore,

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

Pf3 Certainly,

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

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

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

Solution:

con $N : Int\ \{N \geqslant 0\}$
con $A :$ **array** $[0..N)$ **of** Int
var $r, n : Int$
$r, n := -\infty, 0$ -- Pf0
$\{r = \langle \uparrow i : 0 \leqslant i < n : A\,[i] \rangle \wedge 0 \leqslant n \leqslant N, bnd : N - n\}$
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.

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

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

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

Pf2.

$$
\begin{aligned}
& ((r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \;\wedge\; 0 \leqslant n \leqslant N)[n \backslash n + 1])[r \backslash r \uparrow a[n]] \\
\equiv \;& r \uparrow a[n] = \langle \uparrow i : 0 \leqslant i < n + 1 : A[i] \rangle \;\wedge\; 0 \leqslant n + 1 \leqslant N \\
\equiv \;& r \uparrow a[n] = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \uparrow A[n] \;\wedge\; 0 \leqslant n + 1 \leqslant N \\
\Leftarrow \;& r = \langle \uparrow i : 0 \leqslant i < n : A[i] \rangle \;\wedge\; 0 \leqslant n \leqslant N \wedge n \neq N \;\; .
\end{aligned}
$$

Pf3. It is immediate that

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

5. Derive a solution for:

   con $N, X : Int \; \{0 \leqslant N\}$
   con $A :$ **array** $[0..N)$ **of** Int
   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:

```
con N, X : Int {0 ⩽ N}
con A : array [0..N) of Int
var r, x, n : Int
r, x, n := 0, 1, 0               -- Pf0
{P, bnd : N − n}
do n ≠ N →                       -- Pf1
   r, x := r + A [n], x × X      -- Pf2
   n := n + 1
od
{r = ⟨Σi : 0 ⩽ i < N : A [i] × X^i⟩}   -- 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

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

Pf2.

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

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.