Chapter 24 : The longest segment containing at most one zero.

In which we continue to develop our calculational style.

Given f[0..N) of int, $\{0 \le N\}$, we are asked to construct a program to determine the length of the longest segment in f which contains at most one zero.

$$\{f[0..N) \text{ of int contains values}\}$$

$$S$$

$$\{\ r = \langle \uparrow\ i,j : 0 \le i \le j \le N \wedge OZ.i.j : j\text{-}i\ \rangle\}$$

Domain model.

As usual we begin by building a model of the domain.

* (0) $OZ.i.j \quad \equiv \quad \langle + \ k : i \le k < j : g.(f.k)\rangle \quad \le \quad 1 \qquad ,0 \le i \le j \le N$

Where g is defined as follows

$$g.x \quad = \quad 1 \quad \Leftarrow x = 0$$
$$g.x \quad = \quad 0 \quad \Leftarrow x \neq 0$$

Exploiting the empty range and 1-point gives us

\- (1) $OZ.i.i \qquad ,0 \le i \le N$

\- (2) $OZ.i.(i+1) \qquad ,0 \le i < N$

We now consider OZ.i.(j+1) and appeal to associativity. We calculate as follows

$$
\begin{array}{ll}
 & OZ.i.(j+1) \\
= & \quad \{(0)\} \\
 & \langle + \ k : i \le k < j+1 : g.(f.k)\rangle \quad \le \quad 1 \\
= & \quad \{\text{split off } k=j \text{ term}\} \\
 & \langle + \ k : i \le k < j : g.(f.k)\rangle + g.(f.j) \quad \le \quad 1 \\
= & \quad \{\text{case analysis, } f.j \neq 0, \text{ defn. of } g\} \\
 & \langle + \ k : i \le k < j : g.(f.k)\rangle + 0 \quad \le \quad 1 \\
= & \quad \{Id+\} \\
 & \langle + \ k : i \le k < j : g.(f.k)\rangle \quad \le \quad 1 \\
= & \quad \{(0)\} \\
 & OZ.i.j
\end{array}
$$

Thus we have

- (3) $OZ.i.(j+1) \equiv OZ.i.j \Leftarrow f.j \neq 0 \quad ,0 \le i \le j < N$

We now consider the other case.

$$
\begin{array}{ll}
 & OZ.i.(j+1) \\
= & \quad \{(0)\} \\
 & \langle + k : i \le k < j+1 : g.(f.k)\rangle \le 1 \\
= & \quad \{\text{split off } k=j \text{ term}\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle + g.(f.j) \le 1 \\
= & \quad \{\text{case analysis, } f.j = 0\text{, defn. of } g\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle + 1 \le 1 \\
= & \quad \{\text{arithmetic}\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle \le 0 \\
= & \quad \{\text{left-hand term at least zero}\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle = 0 \\
= & \quad \{(5) \text{ see below}\} \\
 & NZ.i.j
\end{array}
$$

Giving

- (4) $OZ.i.(j+1) \equiv NZ.i.j \Leftarrow f.j = 0 \quad ,0 \le i \le j < N$

And we have introduced a new named item

* (5) $NZ.i.j \equiv \langle + k : i \le k < j : g.(f.k)\rangle = 0 \quad ,0 \le i \le j \le N$

From this we can immediately get the following

- (6) $NZ.i.i \quad ,0 \le i \le N$

We once again look to exploit associativity.

$$
\begin{array}{ll}
 & NZ.i.(j+1) \\
= & \quad \{(5)\} \\
 & \langle + k : i \le k < j+1 : g.(f.k)\rangle = 0 \\
= & \quad \{\text{split off } k=j \text{ term}\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle + g.(f.j) = 0 \\
= & \quad \{\text{case analysis, } f.j \neq 0\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle + 1 = 0 \\
= & \quad \{Id+\} \\
 & \langle + k : i \le k < j : g.(f.k)\rangle = 0 \\
= & \quad \{(5)\} \\
 & NZ.i.j
\end{array}
$$

Giving us

- (7) $NZ.i.(j+1) \quad \equiv \quad NZ.i.j \quad \Leftarrow f.j \neq 0 \quad ,0 \leq i \leq j < N$

We consider the other case.

$$
\begin{array}{ll}
 & NZ.i.(j+1) \\
= & \quad \{(5)\} \\
 & \langle + k : i \leq k < j+1 : g.(f.k) \rangle \quad = \quad 0 \\
= & \quad \{\text{split off } k=j \text{ term}\} \\
 & \langle + k : i \leq k < j : g.(f.k) \rangle \ + g.(f.j) \quad = \quad 0 \\
= & \quad \{\text{case analysis, } f.j = 0\} \\
 & \langle + k : i \leq k < j : g.(f.k) \rangle \ + 1 \quad = \quad 0 \\
= & \quad \{\text{arithmetic}\} \\
 & \langle + k : i \leq k < j : g.(f.k) \rangle \quad = \quad -1 \\
= & \quad \{\text{left-hand term must be at least } 0\} \\
 & false
\end{array}
$$

So we have

- (8) $NZ.i.(j+1) \quad \equiv \quad false \quad \Leftarrow f.j = 0 \quad ,0 \leq i \leq j < N$

Now let us return to our postcondition and package up the quantified expression in the postcondition.

* (9) $C.n \quad = \quad \langle \uparrow i,j : 0 \leq i \leq j \leq n \wedge OZ.i.j : j\text{-}i \rangle \quad ,0 \leq n \leq N$

Appealing to the "1 point" rule and (1) gives us

- (10) $C.0 \quad = \quad 0$

In an effort to exploit associativity we calculate as follows

$$
\begin{array}{ll}
 & C.(n+1) \\
= & \quad \{(9)\} \\
 & \langle \uparrow i,j : 0 \leq i \leq j \leq n+1 \wedge OZ.i.j : j\text{-}i \rangle \\
= & \quad \{\text{split off } j = n+1 \text{ term}\} \\
 & \langle \uparrow i,j : 0 \leq i \leq j \leq n \wedge OZ.i.j : j\text{-}i \rangle \uparrow \langle \uparrow i : 0 \leq i \leq n+1 \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \\
= & \quad \{(9)\} \\
 & C.n \uparrow \langle \uparrow i : 0 \leq i \leq n+1 \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \\
= & \quad \{\text{name and conquer}\} \\
 & C.n \uparrow D.(n+1)
\end{array}
$$

- (11) $C.(n+1) \; = \quad C.n \uparrow D.(n+1) \qquad ,0 \le n < N$

* (12) $D.n \; = \quad \langle \uparrow i : 0 \le i \le n \wedge OZ.i.n : n\text{-}i \rangle \qquad ,0 \le n \le N$

An appeal to the "1 point rule" and (1) gives us

- (13) $D.0 \; = \quad 0$

Seeking to exploit associativity, we observe

$$
\begin{array}{ll}
 & D.(n+1) \\
= & \quad \{(12)\} \\
 & \langle \uparrow i : 0 \le i \le n+1 \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \\
= & \quad \{\text{split off } i = n+1 \text{ term}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow (n+1)\text{-}(n+1) \\
= & \quad \{\text{arithmetic}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow 0 \\
 & \quad \{\text{case analysis, } f.n \neq 0 \text{ , (3)}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge OZ.i.n \; : (n+1)\text{-}i \rangle \uparrow 0 \\
= & \quad \{+/\uparrow \text{ for non-empty ranges}\} \\
 & (1 + \langle \uparrow i : 0 \le i \le n \wedge OZ.i.n \; : n\text{-}i \rangle) \uparrow 0 \\
= & \quad \{(12)\} \\
 & (1 + D.n) \uparrow 0
\end{array}
$$

- (14) $D.(n+1) = \quad (1+D.n)\uparrow 0 \qquad \Leftarrow f.n \neq 0 \qquad ,0 \le n < N$

We further observe

$$
\begin{array}{ll}
 & D.(n+1) \\
= & \quad \{(12)\} \\
 & \langle \uparrow i : 0 \le i \le n+1 \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \\
= & \quad \{\text{split off } i = n+1 \text{ term}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow (n+1)\text{-}(n+1) \\
= & \quad \{\text{arithmetic}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge OZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow 0 \\
= & \quad \{\text{case analysis, } f.n = 0, \text{ (4)}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge NZ.i.n : (n+1)\text{-}i \rangle \uparrow 0 \\
= & \quad \{+/\uparrow \text{ for non-empty ranges}\} \\
 & (1 + \langle \uparrow i : 0 \le i \le n \wedge NZ.i.n \; : n\text{-}i \rangle) \uparrow 0 \\
= & \quad \{(16) \text{ below}\} \\
 & (1 + E.n) \uparrow 0
\end{array}
$$

- (15) $D.(n+1) = \quad (1+E.n)\uparrow 0 \qquad \Leftarrow f.n=0 \qquad ,0 \le n < N$

* (16) $E.n \; = \quad \langle \uparrow i : 0 \le i \le n \wedge NZ.i.n \; : n\text{-}i \rangle \qquad ,0 \le n \le N$

By 1-point we get the following

- (17) $E.0 \quad = \quad 0$

We observe

$$
\begin{array}{ll}
 & E.(n+1) \\
= & \qquad \{(16)\} \\
 & \langle \uparrow i : 0 \le i \le n+1 \wedge NZ.i.(n+1) : (n+1)\text{-}i \rangle \\
= & \qquad \{\text{split off } i = n+1 \text{ term}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge NZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow (n+1)\text{-}(n+1) \\
= & \qquad \{\text{arithmetic}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge NZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow 0 \\
 & \qquad \{\text{case analysis, } f.n \ne 0 \text{ , (7)}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge NZ.i.n \ : (n+1)\text{-}i \rangle \uparrow 0 \\
= & \qquad \{+/\uparrow \text{ for non-empty ranges}\} \\
 & (1 + \langle \uparrow i : 0 \le i \le n \wedge OZ.i.n \ : n\text{-}i \rangle) \uparrow 0 \\
= & \qquad \{(16)\} \\
 & (1 + E.n) \uparrow 0
\end{array}
$$

- (18) $E.(n+1) \ = \quad (1+E.n)\uparrow 0 \qquad \Leftarrow f.n \ne 0 \qquad ,0 \le n < N$

We further observe

$$
\begin{array}{ll}
 & E.(n+1) \\
= & \qquad \{(16)\} \\
 & \langle \uparrow i : 0 \le i \le n+1 \wedge NZ.i.(n+1) : (n+1)\text{-}i \rangle \\
= & \qquad \{\text{split off } i = n+1 \text{ term}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge NZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow (n+1)\text{-}(n+1) \\
= & \qquad \{\text{arithmetic}\} \\
 & \langle \uparrow i : 0 \le i \le n \wedge NZ.i.(n+1) : (n+1)\text{-}i \rangle \uparrow 0 \\
= & \qquad \{\text{case analysis, } f.n = 0, (8) \} \\
 & \langle \uparrow i : 0 \le i \le n \wedge \text{false} : (n+1)\text{-}i \rangle \uparrow 0 \\
= & \qquad \{\text{empty range}\} \\
 & Id_{\uparrow} \uparrow 0 \\
= & \qquad \{(ID\uparrow\} \\
 & 0
\end{array}
$$

- (19) $E.(n+1) \ = \quad 0 \qquad \Leftarrow f.n=0 \qquad ,0 \le n < N$

We can now return to the programming task. We rewrite the postcondition as

$$\text{Post} : r = C.n \wedge n = N$$

Invariants.

We choose the following invariants

$$P0 : r = C.n \wedge d = D.n \wedge e = E.n$$
$$P1 : 0 \le n \le N$$

Establish invariants.

$$n, r, d, e := 0, 0, 0, 0$$

Guard

$$n \neq N$$

Variant.

$$N\text{-}n.$$

Loop body.

We observe

$$(n, r, d, e := n+1, U, U', U'').P0$$
$= \quad$ {textual substitution}
$$U = C.(n+1) \wedge U' = D.(n+1) \wedge U'' = E.(n+1)$$
$= \quad$ {(11)}
$$U = C.n \uparrow D.(n+1) \wedge U' = D.(n+1) \wedge U'' = E.(n+1)$$
$= \quad$ {case analysis, $f.n \neq 0$, (14) twice (18)}
$$U = C.n \uparrow (1+D.n)\uparrow 0 \wedge U' = (1+D.n)\uparrow 0 \wedge U'' = (1+E.n)\uparrow 0$$
$= \quad$ {P0}
$$U = r \uparrow (1+d)\uparrow 0 \wedge U' = (1+d)\uparrow 0 \wedge U'' = (1+e)\uparrow 0$$

We further observe

$(n, r, d, e := n+1, U, U', U'').P0$

$=$ {textual substitution}

$U = C.(n+1) \wedge U' = D.(n+1) \wedge U'' = E.(n+1)$

$=$ {(11)}

$U = C.n \uparrow D.(n+1) \wedge U' = D.(n+1) \wedge U'' = E.(n+1)$

$=$ {case analysis, f.n = 0 , (15) twice (19)}

$U = C.n \uparrow (1+E.n)\uparrow 0 \wedge U' = (1+E.n)\uparrow 0 \wedge U'' = 0$

$=$ {P0}

$U = r\uparrow(1 + e) \uparrow 0 \wedge U' = (1 + e) \uparrow 0 \wedge U'' = 0$

Finished program.

```
n, r, d, e := 0, 0, 0, 0
;do n≠N →
        If f.n=0 → n. r. d, e := n+1, r↑(1 + e) ↑0, (1 + e) ↑0, 0
        [] f.n≠0 → n. r. d, e := n+1, r ↑ (1+d)↑0, (1+d)↑0, (1+e)↑0
        fi
od
{ r = C.N }
```