176 Let L be a variable, L: [*int] . Write a program that changes all the negative items of L to 0 , and otherwise leaves L unchanged.

After trying the question, scroll down to the solution.

§ Let the specification be P, defined as

$$P \;=\; \#L' = \#L \;\wedge\; (\forall i : 0,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$$

Let n be a variable, n: *nat*, and let Q be another specification, defined as

$$Q \;=\; \#L' = \#L \;\wedge\; (\forall i : 0,..n \cdot\; L'i = L\,i) \wedge (\forall i : n,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$$

The program is

$$P \;\Leftarrow\; n := 0.\; Q$$

$$Q \;\Leftarrow\; \textbf{if } n = \#L \textbf{ then } ok$$
$$\textbf{else } \textbf{if } L\,n < 0 \textbf{ then } L := n \rightarrow 0 \mid L \textbf{ else } ok \textbf{ fi}.$$
$$n := n+1.\; Q \textbf{ fi}$$

The assignment $L := n \rightarrow 0 \mid L$ could also be written $L\,n := 0$, but it has to be changed to $L := n \rightarrow 0 \mid L$ before any calculation. Proof of P refinement:

$n := 0.\; Q$ — replace Q and substitute

$= \quad \#L' = \#L \;\wedge\; (\forall i : 0,..0 \cdot\; L'i = L\,i) \wedge (\forall i : 0,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — $\forall$ law

$= \quad \#L' = \#L \;\wedge\; \top \wedge (\forall i : 0,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — base

$= \quad Q$

Proof of Q refinement, by cases. First case:

$n = \#L \wedge ok$ — expand ok

$= \quad n = \#L \wedge L' = L \wedge n' = n$ — conjoin two $\top$s

$= \quad n = \#L \wedge L' = L \wedge n' = n \wedge (\forall i : 0,..\#L \cdot\; L\,i = L\,i) \wedge (\forall i : \#L,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — use context twice, and specialize

$\Longrightarrow \quad Q$

Middle case, after distributing the last line:

$n \neq \#L \wedge L\,n < 0 \wedge (L := n \rightarrow 0 \mid L.\; n := n+1.\; Q)$ — expand Q, substitute

$= \quad n \neq \#L \wedge L\,n < 0 \wedge \#L' = \#L \wedge (\forall i : 0,..n+1 \cdot\; L'i = (n \rightarrow 0 \mid L)i)$ — break up the first $\forall$

$\wedge\; (\forall i : n+1,..\#L \cdot\; L'i = ((n \rightarrow 0 \mid L)i)\uparrow 0)$ — and in the last $\forall$ we have $i \neq n$

$= \quad n \neq \#L \wedge L\,n < 0 \wedge \#L' = \#L \wedge (\forall i : 0,..n \cdot\; L'i = L\,i) \wedge L'n = 0$

$\wedge\; (\forall i : n+1,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — use context $L\,n < 0$ to rewrite 0

$= \quad n \neq \#L \wedge Ln < 0 \wedge \#L' = \#L \wedge (\forall i : 0,..n \cdot\; L'i = L\,i) \wedge L'n = (L\,n)\uparrow 0$

$\wedge\; (\forall i : n+1,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — combine the last two conjuncts, and specialize

$\Longrightarrow \quad Q$

Last case, after distributing the last line:

$n \neq \#L \wedge L\,n \geq 0 \wedge (ok.\; n := n+1.\; Q)$ — expand Q, substitute, ok is identity

$= \quad n \neq \#L \wedge L\,n \geq 0 \wedge \#L' = \#L \wedge (\forall i : 0,..n+1 \cdot L'i = L\,i) \wedge (\forall i : n+1,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — break up the first $\forall$

$= \quad n \neq \#L \wedge L\,n \geq 0 \wedge \#L' = \#L \wedge L'n = L\,n \wedge (\forall i : 0,..n \cdot\; L'i = L\,i)$

$\wedge\; (\forall i : n+1,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — use context $L\,n \geq 0$ to rewrite $L\,n$

$= \quad n \neq \#L \wedge L\,n \geq 0 \wedge \#L' = \#L \wedge L'n = (L\,n)\uparrow 0 \wedge (\forall i : 0,..n \cdot\; L'i = L\,i)$

$\wedge\; (\forall i : n+1,..\#L \cdot\; L'i = (L\,i)\uparrow 0)$ — combine the two conjuncts with $\uparrow$ in them and specialize

$\Longrightarrow \quad Q$

Now here is a **for**-loop solution. Define $F\,i$ as

$$F\,i \;=\; \#L' = \#L \;\wedge\; (\forall j : 0,..i \cdot\; L'j = L\,j) \;\wedge\; (\forall j : i,..\#L \cdot\; L'j = (L\,j)\uparrow 0)$$

Then $P = F\,0$. To prove

$$F\,0 \;\Leftarrow\; \textbf{for } n := 0;..\#L \textbf{ do if } L\,i < 0 \textbf{ then } L := i \rightarrow 0 \mid L \textbf{ else } ok \textbf{ fi od}$$

prove

$$F\,i \;\Leftarrow\; i : 0,..\#L$$
$$\wedge\; (\textbf{ if } L\,i < 0 \textbf{ then } L := i \rightarrow 0 \mid L \textbf{ else } ok \textbf{ fi}.$$
$$\#L' = \#L \;\wedge\; (\forall j : 0,..i+1 \cdot\; L'j = L\,j) \;\wedge\; (\forall j : i+1,..\#L \cdot\; L'j = (L\,j)\uparrow 0))$$

and

$$\#L' = \#L \;\wedge\; (\forall j : 0,..\#L \cdot\; L'j = L\,j) \;\wedge\; (\forall j : \#L,..\#L \cdot\; L'j = (L\,j)\uparrow 0) \;\Leftarrow\; ok$$