328 Let L be a variable, L: [*int] . Here is a program to change all the negative items of L to 0 , and otherwise leave L unchanged.

```
for $n$:= 0;..#$L$ do if $L\ n < 0$ then $L$:= $n \rightarrow 0 \mid L$ else $ok$ fi od
```

Write all the specifications and refinements needed to prove that execution of this program does as intended. You do not need to prove the refinements.

After trying the question, scroll down to the solution.

§ The main specification is P , defined as

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

For $0\le n\le \#L$ define $F\,n$ as

$$F\,n \;=\; \#L'=\#L \;\land\; (\forall i\colon 0,..n\cdot\; L'i = L\,i) \;\land\; (\forall i\colon n,..\#L\cdot\; L'i = (L\,i)\uparrow 0)$$

We need to prove

$$P \;\Leftarrow\; F\,0$$

which is easy, and we need to prove

$$F\,n \;\Leftarrow\; n\colon 0,..\#L \;\land\; (\mathbf{if}\; L\,n < 0\; \mathbf{then}\; L{:=}\; n{\rightarrow}0 \mid L\; \mathbf{else}\; ok\; \mathbf{fi}.\;\; F(n{+}1))$$

$$F\,(\#L) \;\Leftarrow\; ok$$

UNFINISHED