324 Given natural list variable L, and index variable i, increase each list item by 1 until you have created list item 100. The program is

```
i:= 0.
do exit when i=#L.
   L i := L i + 1.
   exit when L i = 100.
   i:= i+1
od
```

Add time, write a formal specification, and prove it is refined by the program.

After trying the question, scroll down to the solution.

§ Let t be time. Let S and P be specifications (to be defined later). The program becomes

$S \Leftarrow i{:=}\,0.\ P$

$P \Leftarrow$ **if** $i{=}\#L$ **then** ok
else $L{:=}\ i \rightarrow (L\ i + 1) \mid L.$ **if** $L\ i = 100$ **then** ok
else $i{:=}\ i{+}1.\ t{:=}\ t{+}1.\ P$ **fi fi**

Specification S is

$S \ =\ 0{\le}i'{\le}\#L{=}\#L' \wedge (L'i' = 100 \vee i'{=}\#L)$
$\wedge\ (\forall j{:}\ 0,..i'{\cdot}\ L'j = L\,j + 1 \neq 100)$
$\wedge\ ((\forall j{:}\ i'{+}1,..\#L{\cdot}\ L'j = L\,j) \vee i'{=}\#L)$
$\wedge\ t' = t{+}i'$

Define loop specification P to be like S but from index i rather than from 0.

$P \ =\ 0{\le}i{\le}i'{\le}\#L{=}\#L' \wedge (L'i' = 100 \vee i'{=}\#L)$
$\wedge\ (\forall j{:}\ i,..i'{\cdot}\ L'j = L\,j + 1 \neq 100)$
$\wedge\ ((\forall j{:}\ i'{+}1,..\#L{\cdot}\ L'j = L\,j) \vee i'{=}\#L)$
$\wedge\ t' = t{+}i'{-}i$

Proving the S refinement is easy: replace i by 0 in P and obtain S.
We prove the P refinement by cases. First case.

$i{=}\#L \wedge ok$ UNFINISHED
$\Longrightarrow\ P$

P refinement, middle case.

$i{\neq}\#L \wedge (L{:=}\ i \rightarrow (L\ i + 1) \mid L.\ L\ i = 100 \wedge ok)$
UNFINISHED
$\Longrightarrow\ P$

P refinement, last case.

$i{\neq}\#L \wedge (L{:=}\ i \rightarrow (L\ i + 1) \mid L.\ L\ i \neq 100 \wedge (i{:=}\ i{+}1.\ t{:=}\ t{+}1.\ P))$
UNFINISHED
$\Longrightarrow\ P$