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

$i{:=}\ 0.$
do **exit when** $i{=}\#L.$
    $L\ i := L\ i + 1.$
    exit when $L\ i = 100.$
    $i{:=}\ i{+}1$
od

Write a formal specification, and prove it is refined by the program.

After trying the question, scroll down to the solution.

§ Define k as the first index where $L\,k = 99$, or $\#L$ if there's no such index.

$$\neg(\exists j: 0,..k\cdot\ L\,j = 99) \land (L\,k = 99\ \lor\ k{=}\#L)$$

Now the specification S is

$$\begin{array}{l} \quad(\forall j: 0,..k\cdot L'j = L\,j + 1) \\ \land\ (L\,k = 99 \land L'k{=}100 \land (\forall j: k{+}1,..\#L\cdot L'j = L\,j)\ \ \lor\ \ k{=}\#L) \\ \land\ t' \le t{+}\#L \end{array}$$

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

$$\begin{array}{l} \quad(\forall j: i,..k\cdot L'j = L\,j + 1) \\ \land\ (L\,k = 99 \land L'k{=}100 \land (\forall j: k{+}1,..\#L\cdot L'j = L\,j)\ \ \lor\ \ k{=}\#L) \\ \land\ t' \le t{+}\#L{-}i \end{array}$$

We have two refinements to prove.

$$\begin{array}{l} S\ \Leftarrow\ i{:=}\,0.\ P \\ P\ \Leftarrow\ \textbf{if}\ i{=}\#L\ \textbf{then}\ ok \\ \qquad\quad \textbf{else}\ L{:=}\ i \to (L\,i + 1)\ |\ L.\ \textbf{if}\ L\,i = 100\ \textbf{then}\ ok\ \textbf{else}\ i{:=}\ i{+}1.\ P\ \textbf{fi}\ \textbf{fi} \end{array}$$

The first is easy: replacing i by 0 in P we obtain S. We prove the last refinement by cases. First case.

$$i{=}\#L \land ok\ \Rightarrow\ P \qquad\qquad \text{UNFINISHED}$$

$$=\quad \top$$

Last refinement, last case.

$$i{\ne}\#L \land (L{:=}\ i \to (L\,i + 1)\ |\ L.\ \textbf{if}\ L\,i = 100\ \textbf{then}\ ok\ \textbf{else}\ i{:=}\ i{+}1.\ P\ \textbf{fi})\ \Rightarrow\ P \qquad \text{UNFINISHED}$$

$$=\quad \top$$