207 Define a partial order $«$ on pairs of integers as follows:

$$[a; b] « [c; d] \ = \ a<c \land b<d$$

Given n: nat+1 and L: [n*[int; int]] write a program to find the index of a minimal item in L . That is, find j: $\square L$ such that $\neg\exists i\cdot L\,i « L\,j$. The execution time should be n .

After trying the question, scroll down to the solution.

§ Let k: nat+1 and j: $\square L$ be program variables. Let S and P be specifications, defined as

$$S \;=\; \neg\exists i\colon \square L\cdot\ L\,i \ll L\,j'$$
$$P \;=\; \neg(\exists i\colon 0,..k\cdot\ L\,i \ll L\,j) \Rightarrow S$$

The refinements are

$$S \;\Leftarrow\; j:= 0.\ \ k:= 1.\ \ P$$

$P \;\Leftarrow\;$ **if** $k{=}\#L$ **then** ok
else if $L\,k\,0 < L\,j\,0\ \wedge\ L\,k\,1 < L\,j\,1$ **then** $j:= k$
else ok **fi**.
$k:= k{+}1.\ \ P$ **fi**

Proof of the S refinement.

$j:= 0.\ \ k:= 1.\ \ P$ — replace P and then S
$=\ \ j:= 0.\ \ k:= 1.\ \ \neg(\exists i\colon 0,..k\cdot\ L\,i \ll L\,j) \Rightarrow \neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j')$ — substitution law twice
$=\ \ \neg(\exists i\colon 0,..1\cdot\ L\,i \ll L\,0) \Rightarrow \neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j')$ — one element domain
$=\ \ \neg(L\,0 \ll L\,0) \Rightarrow \neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j')$ — $\ll$ is irreflexive
$=\ \ \neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j')$
$=\ \ S$

Proof of the P refinement by cases. First case:

$k{=}\#L \wedge ok \Rightarrow P$ — replace ok and P and then S
$=\ \ k{=}\#L \wedge k'{=}k \wedge j'{=}j \Rightarrow (\neg(\exists i\colon 0,..k\cdot\ L\,i \ll L\,j) \Rightarrow \neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j'))$ — context
$=\ \ k{=}\#L \wedge k'{=}k \wedge j'{=}j \Rightarrow (\neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j') \Rightarrow \neg(\exists i\colon \square L\cdot\ L\,i \ll L\,j'))$ — reflexive $\Rightarrow$
$=\ \ k{=}\#L \wedge k'{=}k \wedge j'{=}j \Rightarrow \top$ — base $\Rightarrow$
$=\ \ \top$

Middle case:

$k{\ne}\#L\ \wedge\ L\,k\,0 < L\,j\,0\ \wedge\ L\,k\,1 < L\,j\,1\ \wedge\ (j:= k.\ \ k:= k{+}1.\ \ P) \Rightarrow P$
definition of $\ll$; replace first P
$=\ \ k{\ne}\#L \wedge L\,k \ll L\,j \wedge (j:= k.\ \ k:= k{+}1.\ \ \neg(\exists i\colon 0,..k\cdot\ L\,i \ll L\,j) \Rightarrow S) \Rightarrow P$
substitution law twice: S does not have j or k in it.
$=\ \ k{\ne}\#L\ \wedge\ L\,k \ll L\,j\ \wedge\ (\neg(\exists i\colon 0,..k{+}1\cdot\ L\,i \ll L\,k) \Rightarrow S) \Rightarrow P$
$=\ \ $UNFINISHED
$=\ \ \top$

Last case:

$k{\ne}\#L \wedge \neg(L\,k\,0 < L\,j\,0\ \wedge\ L\,k\,1 < L\,j\,1) \wedge (ok.\ \ k:= k{+}1.\ \ P) \Rightarrow P$
ok is identity for $.$; definition of $\ll$; replace first P
$=\ \ k{\ne}\#L \wedge \neg(L\,k \ll L\,j) \wedge (k:= k{+}1.\ \ \neg(\exists i\colon 0,..k\cdot\ L\,i \ll L\,j) \Rightarrow S) \Rightarrow P$
substitution law: S does not have k in it.
$=\ \ k{\ne}\#L \wedge \neg(L\,k \ll L\,j) \wedge (\neg(\exists i\colon 0,..k{+}1\cdot\ L\,i \ll L\,j) \Rightarrow S) \Rightarrow P$
$=\ \ $UNFINISHED
$=\ \ \top$