(n sort) Given a list $L$ such that $L(\square L) = \square L$, write a program to sort $L$ in linear time and constant space. The only change permitted to $L$ is to swap two items.

§

The problem is $P$, defined as

$$P = L(\square L) = \square L \Rightarrow L' = [0;..#L]$$

The only change permitted to $L$ is swap, defined as

$$\text{swap } i \ j = L := i \rightarrow Lj \ j \rightarrow Li \ | L$$

execution time has to be linear, so that suggests starting an index variable $k$ at 0, and moving up by $k := k + 1$ until $k = \#L$, so that the part of the list before $k$ is in order, and therefore the part of the list from $k$ onward has the right items but may not yet in the right order.

$$P \iff k := 0. \ Q$$

$$Q \iff \begin{cases} \text{if } k = \#L \text{ then } \text{ok} \\ \text{else if } Lk = k \text{ then } k := k + 1. \ Q \\ \text{else swap } (Lk) k. \ Q \end{cases} \text{ fi}$$

To define $Q$, we can look at $P$ for inspiration. Perhaps

$$Q = L(k;..#L) = k;..#L \Rightarrow L' = L[0;..k] ;; [k;..#L]$$

I think that will work. But I think it will be easier to prove the $Q$ refinement if we weaken $Q$ by strengthening its antecedent. I'm going to try

$$Q = L[0;..k] = [0;..k] \land L(k;..#L) = k;..#L \Rightarrow L' = L[0;..k] ;; [k;..#L]$$

This says: if the first part of $L$ is done, and the last part has the right items (but not necessarily in the right order), then we complete the job by leaving the first part of $L$ alone and putting the last part in order.

Proof of $P$ refinement:

$$k := 0. \ Q$$

$$\begin{array}{ll}
k := 0. & L[0;..k] = [0;..k] \land L(k;..#L) = k;..#L \Rightarrow L' = L[0;..k] ;; [k;..#L] \\
\text{Substitution Law} & \text{ simplify} \\
L[0;..0] = [0;..0] \land L(\square L) = \square L \Rightarrow L' = L[0;..0] ;; [0;..#L] \\
\text{Proof of first case of } Q \text{ refinement:} & \text{P} \\
& k = \#L \land \text{ok} \Rightarrow Q \\
& \begin{array}{ll}
& k = \#L \land k' = k \land L' = L \\
& \Rightarrow (L[0;..k] = [0;..k] \land L(k;..#L) = k;..#L \Rightarrow L' = L[0;..k] ;; [k;..#L]) \\
& \text{context} \\
& k = \#L \land k' = k \land L' = L \\
& \Rightarrow (L[0;..#L] = [0;..#L] \land L(#L;..#L) = #L;..#L \Rightarrow L = L[0;..#L] ;; [#L;..#L]) \\
& \text{ simplify} \\
& \top \\
& \text{Proof of middle case of } Q \text{ refinement:} \\
& k = \#L \land Lk = k \land (k := k + 1. \ Q) \\
& \begin{array}{ll}
& k = \#L \land Lk = k \\
& \land (k := k + 1. \ L[0;..k] = [0;..k] \land L(k;..#L) = k;..#L \Rightarrow L' = L[0;..k] ;; [k;..#L]) \\
& \text{ substitution law} \\
& k = \#L \land Lk = k \\
& \land (L[0;..k+1] = [0;..k+1] \land L(k+1;..#L) = k+1;..#L \Rightarrow L' = L[0;..k+1] ;; [k+1;..#L]) \\
& \text{ use context } Lk = k \text{ to simplify the implication}
\end{array}$$

$$Q \iff k := 0. \ Q$$

$$Q \iff \begin{cases} \text{if } k = \#L \text{ then } \text{ok} \\ \text{else if } Lk = k \text{ then } k := k + 1. \ Q \\ \text{else swap } (Lk) k. \ Q \end{cases} \text{ fi}$$
\[ k \# L \land L k = k \land (L[0..k] = [0..k] \land L(k,\#L) = k,\#L) \Rightarrow L' = L[0..k];(k,\#L) \]
\[ k \# L \land L k = k \land Q \]
\[ \Rightarrow Q \]

Proof of last case of \( Q \) refinement:
\[ k \# L \land L k = k \land (\text{swap} (L k) \land Q) \Rightarrow Q \]
\[ k \# L \land L k = k \land (\text{swap} (L k) \land Q) \]
\[ \Rightarrow (L[0..k] = [0..k] \land L(k,\#L) = k,\#L) \Rightarrow L' = L[0..k] ;; [k,\#L] \]

To prove this implication, I'll go from the antecedent on the top line to the consequent on the bottom line.
\[ k \# L \land L k = k \land L[0..k] = [0..k] \land L(k,\#L) = k,\#L \]
\[ \Rightarrow (L = L k \land (k \rightarrow L(L k) | L)) \land L[0..k] = [0..k] \land L(k,\#L) = k,\#L \Rightarrow L' = L[0..k] ;; [k,\#L] \]

This next step is more complicated and less formal than I would like.
In the top line it says \( L[0..k] = [0..k] \), and since each item in the list
occurs once, the items less than \( k \) are used up at indexes less than \( k \).
The top line also says \( L k = k \), therefore \( L k \neq k \). So the swap is swapping
the item at \( k \) with an item at an index greater than \( k \). The swap does not
affect the first part of the list \( L[0..k] \). The swap affects the last part of the
list, but it does not change the bunch of items in the last part of the list
\( L(0..k) \). So the top line, used as context, allows us to simplify the
bottom three lines.
\[ k \# L \land L k = k \land L[0..k] = [0..k] \land L(k,\#L) = k,\#L \]
\[ \Rightarrow L' = L[0..k] ;; [k,\#L] \]

And that completes the last case of the \( Q \) refinement.

Recursive time is bounded by \( 2 \times \# L \). Counting just \( \text{swaps} \), the time is bounded by \( \# L \). To prove time bounds, it is helpful to define
\[ f i = \& j : i = \# L \land L_{j} \]
Then the timing specifications are \( A \) and \( B \), defined as
\[ A = t' \leq t + \# L + f 0 \]
\[ B = t' \leq t + \# L - k + f k \]
With time, the refinements are
\[
A \iff k := 0. \ B
\]
\[
B \iff \begin{cases} 
& \text{if } k = \#L \text{ then } ok \\
& \text{else if } Lk = k \text{ then } k := k+1. \ t := t+1. \ B \\
& \text{else } \text{swap} (Lk) \ k. \ t := t+1. \ B \end{cases}
\]

Proof of \text{A refinement}:
\[
k := 0. \ B
\]
\[
k := 0. \ t' \leq t + \#L - k + f \ k
\]
\[
t' \leq t + \#L - 0 + f \ 0
\]
\[
A
\]

Proof of first case of \text{B refinement}:
\[
k = \#L \land ok \Rightarrow B
\]
\[
k = \#L \land k = k \land L' = L \land t' = t \Rightarrow t' \leq t + \#L - k + f \ k
\]
\[
k = \#L \land k = k \land L' = L \land t' = t \Rightarrow t \leq t + \#L - \#L + f (\#L)
\]
\[
k = \#L \land k = k \land L' = L \land t' = t \Rightarrow 0 \leq \varepsilon j; \#L, \ldots \#L; L j + j
\]
\[
k = \#L \land k = k \land L' = L \land t' = t \Rightarrow 0 \leq 0
\]
\[
\top
\]

Proof of middle case of \text{B refinement}:
\[
k = \#L \land Lk = k \land (k := k+1. \ t := t+1. \ B)
\]
\[
k = \#L \land Lk = k \land (k := k+1. \ t := t+1. \ t' \leq t + \#L - k + f \ k)
\]
\[
k = \#L \land Lk = k \land t' \leq t + 1 + \#L - k - 1 + f (k+1)
\]
\[
k = \#L \land Lk = k \land t' \leq t + \#L - k + f (k+1)
\]
\[
k = \#L \land Lk = k \land t' \leq t + \#L - k + f k
\]
\[
\Rightarrow B
\]

Proof of last case of \text{B refinement}:
\[
k = \#L \land Lk = k \land (\text{swap} (Lk) k. \ t := t+1. \ B)
\]
\[
k = \#L \land Lk = k \land (L := Lk \rightarrow Lk \ | k \rightarrow L(Lk) \ | \ L. \ t := t+1. \ t' \leq t + \#L - k + f \ k)
\]

The next step looks like it should be the Substitution Law. But \(f\) is defined in terms of \(L\). So we have to apply \(f\) first.

\[
k = \#L \land Lk = k \land (L := Lk \rightarrow Lk \ | k \rightarrow L(Lk) \ | \ L. \ t := t+1. \ t' \leq t + \#L - k + f \ k)
\]
\[
\Rightarrow B
\]  

And that completes the last case of the \text{B refinement}. 