Let $A$ be a sorted list of different integers. Let $B$ be another such list. Write a program to find the sorted list of integers that occur in exactly one of $A$ or $B$.

After trying the question, scroll down to the solution.
We are given
\[ \forall i: 1,..\#A \cdot A(i-1) < A i \]
\[ \forall i: 1,..\#B \cdot B(i-1) < B i \]

Let \( L \) be a list variable whose final value is the list we want. The specification is \( S \), defined as
\[
S = L'(0,..\#L') = (\forall n: A(0,..\#A), B(0,..\#B) \to n: A(0,..\#A)'B(0,..\#B))
\]
\[ \land \forall i: 1,..\#L' \cdot L'(i-1) < L'i \]

Let \( a \) and \( b \) be natural variables used to index \( A \) and \( B \). Now define specification \( R \) as
\[
R = L'[0,..\#L] = L
\]
\[ \land L'(#L,..\#L') = (\forall n: A(a,..\#A), B(b,..\#B) \to n: A(a,..\#A)'B(b,..\#B)) \]
\[ \land \forall i: \#L,..\#L' \cdot L'(i-1) < L'i \]

The refinements are
\[
S \iff L := [nil]. \ a := 0. \ b := 0. \ R
\]
\[
R \iff \begin{cases} 
\text{if } a = \#A \text{ then } L := L ;; B[b,..\#B] \\
\text{else if } b = \#B \text{ then } L := L ;; A[a,..\#A] \\
\text{else if } A \ a = B \ b \text{ then } a := a+1. \ b := b+1. \ R \\
\text{else if } A \ a > B \ b \text{ then } L := L ;; B[b]. \ b := b+1. \ R \\
\text{else } L := L ;; A[a]. \ a := a+1. \ R
\end{cases}
\]

The \( S \) refinement is proven by 3 uses of the Substitution Law. The \( R \) refinement is proven by 5 cases (one for each line). First case:
\[
a = \#A \land (L := L ;; B[b,..\#B]) \Rightarrow R \\
= \top \\
\text{UNFINISHED}
\]

Next case:
\[
a + \#A \land b = \#B \land (L := L ;; A[a,..\#A]) \Rightarrow R \\
= \top \\
\text{Same as previous case.}
\]

Next case:
\[
a + \#A \land b + \#B \land A \ a = B \ b \land (a := a+1. \ b := b+1. \ R) \Rightarrow R \\
= \top \\
\text{UNFINISHED}
\]

Next case:
\[
a + \#A \land b + \#B \land A \ a = B \ b \land A \ a > B \ b \land (L := L ;; B[b]. \ b := b+1. \ R) \Rightarrow R \\
= \top \\
\text{UNFINISHED}
\]

Last case:
\[
a + \#A \land b + \#B \land A a + B b \land A a \leq B b \land (L := L ;; A[a]. \ a := a+1. \ R) \Rightarrow R \\
\text{This is just like the previous case.}
\]