273 (unique items) 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

$\forall i\colon 1,..\#A\cdot\ A(i-1)<A\ i$

$\forall i\colon 1,..\#B\cdot\ B(i-1)<B\ i$

Let L be a list variable whose final value is the list we want. The specification is S, defined as

$$S\ =\ \ L'(0,..\#L')\ =\ (\S n\colon A(0,..\#A), B(0,..\#B)\cdot\ \neg\ n\colon A(0,..\#A)`B(0,..\#B))$$
$$\wedge\ \ \forall i\colon 1,..\#L'\cdot\ L'(i-1)<L'i$$

Let a and b be natural variables used to index A and B. Now define specification R as

$$R\ =\ \ L'[0;..\#L]\ =\ L$$
$$\wedge\ \ L'(\#L,..\#L')\ =\ (\S n\colon A(a,..\#A), B(b,..\#B)\cdot\ \neg\ n\colon A(a,..\#A)`B(b,..\#B))$$
$$\wedge\ \ \forall i\colon \#L,..\#L'\cdot\ L'(i-1)<L'i$$

The refinements are

$S\ \Leftarrow\ L\!:=[nil].\ \ a\!:=0.\ \ b\!:=0.\ \ R$

$R\ \Leftarrow$ **if** $a=\#A$ **then** $L\!:=L\ ;;\ B[b;..\#B]$
  else if $b=\#B$ **then** $L\!:=L\ ;;\ A[a;..\#A]$
    else if $A\ a = B\ b$ **then** $a\!:=a+1.\ \ b\!:=b+1.\ \ R$
      else if $A\ a > B\ b$ **then** $L\!:=L\ ;;\ B[b].\ \ b\!:=b+1.\ \ R$
        else $L\!:=L\ ;;\ A[a].\ \ a\!:=a+1.\ \ R$ **fi fi fi fi**

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:

$a=\#A\ \wedge (L\!:=L\ ;;\ B[b;..\#B])\ \Rightarrow\ R$ UNFINISHED

$=\ \ \top$

Next case:

$a\ne\#A\ \wedge b=\#B\ \wedge (L\!:=L\ ;;\ A[a;..\#A])\ \Rightarrow\ R$ Same as previous case.

$=\ \ \top$

Next case:

$a\ne\#A\ \wedge b\ne\#B\ \wedge A\ a = B\ b\ \wedge (a\!:=a+1.\ \ b\!:=b+1.\ \ R)\ \Rightarrow\ R$ UNFINISHED

$=\ \ \top$

Next case:

$a\ne\#A\ \wedge b\ne\#B\ \wedge A\ a \ne B\ b\ \wedge A\ a > B\ b\ \wedge (L\!:=L\ ;;\ B[b].\ \ b\!:=b+1.\ \ R)\ \Rightarrow\ R$
UNFINISHED

$=\ \ \top$

Last case:

$a\ne\#A\ \wedge b\ne\#B\ \wedge Aa\ne Bb\ \wedge Aa\le Bb\ \wedge (L\!:=L\ ;;\ A[a].\ \ a\!:=a+1.\ \ R)\ \Rightarrow\ R$
This is just like the previous case.

= T