MODULE *SendSeqUndo*

This is part of the *SendSeq* example, as explained in the comments in module *SendSeq*. The specification *SpecU* defined here is straightforward, except perhaps for the definition of *RemoveEltFrom*.

EXTENDS *SendSeq*

RemoveElt$(i,\ seq)$ is the sequence obtained from *seq* by removing element number i from it, assuming *seq* is a sequence and $1 \leq i \leq Len(seq)$. (The meaning of *RemoveElt*$(i,\ seq)$ affects the specification only if those assumptions hold. This fact is implicitly checked by *TLC*, which will report an error if checking the spec requires it to evaluate the expression when those assumptions don't hold.) The definition is simple, since a sequence of length n is a function with domain $1 \,..\, n$. However, it's easy to make am "off by one" error in such a definition, so it's a good idea to check it for a few values of i and *seq* using the Evaluate Constant Expression field of the Model Checking Results page.

$$RemoveEltFrom(i,\ seq) \triangleq [j \in 1 \,..\, (Len(seq) - 1) \mapsto \text{IF } j < i \text{ THEN } seq[j] \text{ ELSE } seq[j+1]]$$

$$Undo(i) \triangleq \land\ y' = RemoveEltFrom(i,\ y) \\ \land\ x' = x$$

$$NextU \triangleq Next \lor (\exists\, i \in 1 \,..\, Len(y) : Undo(i))$$

$$SpecU \triangleq Init \land \Box[NextU]_{vars}$$

* Modification History
* Last modified Sat *Oct* 22 00:50:17 *PDT* 2016 by *lamport*
* Created *Thu Sep* 15 02:23:08 *PDT* 2016 by *lamport*