MODULE *SendSetUndo*

This module defines a specification *SpecU* which is a variant of the specification *Spec* of module *SendSet*. It adds to the next-state action *Next* of *Spec* an $Undo(S)$ action that removes from y the elements that are in S, where S is an arbitrary non-empty subset of y. The $Undo(S)$ action changes only y, so we consider it to be an internal action. The defintion of *SpecU* is straightforward. It has the same initial predicate and type-correctness invariant as *Spec*.

The specification $\exists\, y : Spec$ and $\exists\, y : SpecU$ are equivalent. The hard part of demonstrating the equivalence is showing that *Spec* implies $\exists\, y : SpecU$. This is done in module *SpecUP*, which adds to *SpecU* a prophecy variable and shows that *SpecUP* implements *Spec* under a suitable refinement mapping.

EXTENDS *SendSet*

$$Undo(S) \triangleq \land\, y' = y \setminus S \\ \land\, x' = x$$

$$NextU \triangleq Next \lor (\exists\, S \in (\text{SUBSET } y) \setminus \{\{\}\} : Undo(S))$$

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

* Modification History
* Last modified Sat *Oct* 22 00:42:56 *PDT* 2016 by *lamport*
* Created *Thu Sep* 15 01:39:08 *PDT* 2016 by *lamport*