```
1  ---------- MODULE Consensus ----------
   This is a trivial specification of consensus. It asserts that the variable chosen , which represents
   the set of values that someone might think has been chosen is initially empty and can be changed
   only by adding a single element to it.
8  EXTENDS Naturals, FiniteSets, TLAPS
9  ------------------------------------------
10 CONSTANTS Values  the set of all values that can be chosen

12 VARIABLES chosen  the set of all values that have been chosen

14 TypeOK ≜
15     ∧  chosen ⊆ Values
16     ∧  IsFiniteSet(chosen)
17 ------------------------------------------
18 Init ≜ chosen = {}

20 Next ≜ ∧ chosen = {}
21        ∧ ∃ v ∈ Values : chosen′ = {v}

23 Spec ≜ Init ∧ □[Next]_chosen
24 ------------------------------------------
25 Inv ≜ Cardinality(chosen) ≤ 1
26     ∧ TypeOK
27     ∧ Cardinality(chosen) ≤ 1

29 THEOREM Spec ⇒ □Inv
30 ⟨1⟩1. Init ⇒ Inv
31   BY DEF Init, Inv
     ⟨2⟩ SUFFICES ASSUME Init
                 PROVE Inv
      OBVIOUS
     ⟨2⟩ QED
      BY DEF Init, Inv
40 ⟨1⟩2. Inv ∧ [Next]_chosen ⇒ Inv′
41   ⟨2⟩ SUFFICES ASSUME Inv,
42                       [Next]_chosen
43               PROVE  Inv′
44     OBVIOUS
45   ⟨2⟩1.CASE Next
46     BY ⟨2⟩1 DEF Inv, Next
47   ⟨2⟩2.CASE UNCHANGED chosen
48     BY ⟨2⟩2 DEF Inv, Next
49   ⟨2⟩3. QED
50     BY ⟨2⟩1, ⟨2⟩2

52 ⟨1⟩3. QED
53   BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec
```

\ * Modification History
\ * Last modified *Tue Jul* 16 13:47:23 *CST* 2019 by *hengxin*
\ * Last modified *Tue Jul* 16 11:26:27 *CST* 2019 by *hengxin*
\ * Last modified *Wed Nov* 21 11:35:33 *PST* 2012 by *lamport*
\ * Created *Mon Nov* 19 15:19:09 *PST* 2012 by *lamport*