```
──────────────────── MODULE Consensus ────────────────────
EXTENDS Naturals, FiniteSets

CONSTANT Value
  The set of all values that can be chosen.

VARIABLE chosen
  The set of all values that have been chosen.

The type-correctness invariant.
TypeOK ≜ ∧ chosen ⊆ Value
         ∧ IsFiniteSet(chosen)

The initial predicate and next-state relation.
Init ≜ chosen = {}

Next ≜ ∧ chosen = {}
       ∧ ∃ v ∈ Value : chosen′ = {v}

The complete spec.
Spec ≜ Init ∧ □[Next]_chosen
──────────────────────────────────────────────────────────
Safety: At most one value is chosen.
Inv ≜ ∧ TypeOK
      ∧ Cardinality(chosen) ≤ 1

THEOREM Invariance ≜ Spec ⇒ □Inv
⟨1⟩1. Init ⇒ Inv
⟨1⟩2. Inv ∧ [Next]_chosen ⇒ Inv′
⟨1⟩3. QED
  ⟨2⟩1. Inv ∧ □[Next]_chosen ⇒ □Inv
     BY ⟨1⟩2  and a TLA proof rule
  ⟨2⟩2. QED
     BY ⟨1⟩1, ⟨2⟩1   and simple logic
──────────────────────────────────────────────────────────
Liveness: A value is eventually chosen.
Success ≜ ◇(chosen ≠ {})
LiveSpec ≜ Spec ∧ WF_chosen(Next)

THEOREM LivenessTheorem ≜ LiveSpec ⇒  Success
──────────────────────────────────────────────────────────
```