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.

$$TypeOK \triangleq \land chosen \subseteq Value \\ \land IsFiniteSet(chosen)$$

The initial predicate and next-state relation.

$$Init \triangleq chosen = \{\}$$

$$Next \triangleq \land chosen = \{\} \\ \land \exists\, v \in Value : chosen' = \{v\}$$

The complete spec.

$$Spec \triangleq Init \land \Box[Next]_{chosen}$$

Safety: At most one value is chosen.

$$Inv \triangleq \land TypeOK \\ \land Cardinality(chosen) \leq 1$$

THEOREM $Invariance \triangleq Spec \Rightarrow \Box Inv$ 这块是TLAPS，即TLA proof system

$\langle 1 \rangle 1.$ $Init \Rightarrow Inv$

$\langle 1 \rangle 2.$ $Inv \land [Next]_{chosen} \Rightarrow Inv'$

$\langle 1 \rangle 3.$ QED

  $\langle 2 \rangle 1.$ $Inv \land \Box[Next]_{chosen} \Rightarrow \Box Inv$

    BY $\langle 1 \rangle 2$ and a TLA proof rule

  $\langle 2 \rangle 2.$ QED

    BY $\langle 1 \rangle 1$, $\langle 2 \rangle 1$ and simple logic

---

Liveness: A value is eventually chosen.

$$Success \triangleq \Diamond(chosen \neq \{\})$$

$$LiveSpec \triangleq Spec \land \mathrm{WF}_{chosen}(Next)$$

THEOREM $LivenessTheorem \triangleq LiveSpec \Rightarrow Success$