Invariance Proof of Algorithm Consensus

Inv is an invariant of algorighm Consensus.

1. $Init \Rightarrow Inv$

PROOF: By the definitions of *Init* and *Inv*, since *Init* implies $chosen = \emptyset$.

2. $Inv \wedge Next \Rightarrow Inv'$

PROOF: By the definitions of *Next* and *Inv*, since *Next* implies *chosen* will contain one element iff $chosen = \emptyset$.

3. Q.E.D

PROOF: By 1, 2.

MODULE *Consensus*

CONSTANT *Value*

VARIABLE *chosen*

$Init \triangleq chosen = \{\}$

$Next \triangleq$

$\quad \wedge chosen = \{\}$

$\quad \wedge \exists\, v \in Value : chosen' = \{v\}$

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

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