MODULE *Consensus*

The consensus problem requires a set of processes to choose a single value. This module specifies the problem by specifying exactly what the requirements are for choosing a value.

EXTENDS *Naturals*, *FiniteSets*, *TLAPS*

We let the constant parameter *Value* be the set of all values that can be chosen.

CONSTANT *Value*

****

We now specify the safety property of consensus as a trivial algorithm that describes the allowed behaviors of a consensus algorithm. It uses the variable *chosen* to represent the set of all chosen values. The algorithm is trivial; it allows only behaviors that contain a single state-change in which the variable *chosen* is changed from its initial value $\{\}$ to the value $\{v\}$ for an arbitrary value v in *Value*. The algorithm itself does not specify any fairness properties, so it also allows a behavior in which *chosen* is not changed. We could use a translator option to have the translation include a fairness requirement, but we don't bother because it is easy enough to add it by hand to the safety specification that the translator produces.

A real specification of consensus would also include additional variables and actions. In particular, it would have Propose actions in which clients propose values and Learn actions in which clients learn what value has been chosen. It would allow only a proposed value to be chosen. However, the interesting part of a consensus algorithm is the choosing of a single value. We therefore restrict our attention to that aspect of consensus algorithms. In practice, given the algorithm for choosing a value, it is obvious how to implement the Propose and Learn actions.

For convenience, we define the macro *Choose*() that describes the action of changing the value of *chosen* from $\{\}$ to $\{v\}$, for a nondeterministically chosen v in the set *Value*. (There is little reason to encapsulate such a simple action in a macro; however our other specs are easier to read when written with such macros, so we start using them now.) The *when* statement can be executed only when its condition, $chosen = \{\}$, is true. Hence, at most one *Choose*() action can be performed in any execution. The *with* statement executes its body for a nondeterministically chosen v in *Value*. Execution of this statement is enabled only if *Value* is non-empty–something we do not assume at this point because it is not required for the safety part of consensus, which is satisfied if no value is chosen.

We put the *Choose*() action inside a *while* statement that loops forever. Of course, only a single *Choose*() action can be executed. The algorithm stops after executing a *Choose*() action. Technically, the algorithm deadlocks after executing a *Choose*() action because control is at a statement whose execution is never enabled. Formally, termination is simply deadlock that we want to happen. We could just as well have omitted the *while* and let the algorithm terminate. However, adding the *while* loop makes the TLA+ representation of the algorithm a tiny bit simpler.

```
--algorithm Consensus{
  variable chosen = {} ;
  macro Choose( ) { when chosen = {} ;
                    with ( v ∈ Value ) { chosen := {v} } }
   { lbl: while ( TRUE ) { Choose() }
    }
 }
```

The *PlusCal* translator writes the TLA+ translation of this algorithm below. The formula *Spec* is the TLA+ specification described by the algorithm's code. For now, you should just understand its two subformulas *Init* and *Next*. Formula *Init* is the initial predicate and describes all possible initial states of an execution. Formula *Next* is the next-state relation; it describes the possible state changes (changes of the values of variables), where unprimed variables represent their values in the old state and primed variables represent their values in the new state.

****

**** BEGIN TRANSLATION

VARIABLE *chosen*

$vars \triangleq \langle chosen \rangle$

$Init \triangleq$ Global variables

$\quad \land\ chosen = \{\}$

$Next \triangleq \land\ chosen = \{\}$

$\quad \land\ \exists\, v \in Value :$

$\quad\quad chosen' = \{v\}$

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

**** END TRANSLATION

We now prove the safety property that at most one value is chosen. We first define the type-correctness invariant *TypeOK*, and then define *Inv* to be the inductive invariant that asserts *TypeOK* and that the cardinality of the set *chosen* is at most 1. We then prove that, in any behavior satisfying the safety specification *Spec*, the invariant *Inv* is true in all states. This means that at most one value is chosen in any behavior.

$TypeOK \triangleq \land\ chosen \subseteq Value$

$\quad \land\ IsFiniteSet(chosen)$

$Inv \triangleq \land\ TypeOK$

$\quad \land\ Cardinality(chosen) \leq 1$

To prove our theorem, we need the following simple results about the cardinality of finite sets.

AXIOM $EmptySetCardinality \triangleq IsFiniteSet(\{\}) \land Cardinality(\{\}) = 0$

AXIOM $SingletonCardinality \triangleq$

$\quad \forall\, e : IsFiniteSet(\{e\}) \land (Cardinality(\{e\}) = 1)$

Whenever we add an axiom, we should check it with *TLC* to make sure we haven't made any errors. To check axiom *SingletonCardinality*, we must replace the unbounded quantification with a bounded one. We therefore let *TLC* check that the following formula is true.

$SingleCardinalityTest \triangleq$

$\quad \forall\, e \in \text{SUBSET}\ \{\text{“a”}, \text{“b”}, \text{“c”}\} : IsFiniteSet(\{e\}) \land (Cardinality(\{e\}) = 1)$

We now prove that *Inv* is an invariant, meaning that it is true in every state in every behavior. Before trying to prove it, we should first use *TLC* to check that it is true. It's hardly worth bothering to either check or prove the obvious fact that *Inv* is an invariant, but it's a nice tiny exercise. Model checking is instantaneous when *Value* is set to any small finite set.

To understand the following proof, you need to understand the formula *Spec* , which equals

$Init \land \Box[Next]\_vars$

where *vars* is the tuple $\langle chosen, pc \rangle$ of all variables. It is a temporal formula satisfied by a behavior iff the behavior starts in a state satisfying *Init* and such that each step (sequence of states) satisfies $[Next]\_vars$, which equals

$Next \lor (vars' = vars)$

Thus, each step satisfies either *Next* (so it is a step allowed by the next-state relation) or it is a "stuttering step" that leaves all the variables unchanged. The reason why a spec must allow stuttering steps will become apparent when we prove that a consensus algorithm satisfies this specification of consensus.

By default, a definition is not usable in a proof. If the a definition should be usable in the proof of a step, meaning that the prover can expand the definition, then that must be explicitly indicated– usually in the DEF clause of a BY statement. A DEF clause of a USE statement makes the definitions in it usable in the scope of that statement. The following USE statement makes the definition of lbl usable everywhere in the rest of the module. (There is a corresponding HIDE statement that makes definitions unusable in its scope.)

USE DEF lbl

The following lemma asserts that *Inv* is an inductive invariant of the next-state action *Next*. It is the key step in proving that *Inv* is an invariant of (true in every behavior allowed by) specification *Spec*.

LEMMA $InductiveInvariance \triangleq$
$\qquad Inv \land [Next]_{vars} \Rightarrow Inv'$
$\langle 1 \rangle 1.$ SUFFICES ASSUME $Inv,\ [Next]_{vars}$
$\qquad$ PROVE Inv'
$\quad$ OBVIOUS
$\langle 1 \rangle 2.$CASE $Next$
$\quad \langle 2 \rangle 1.$ PICK $v \in Value : chosen' = \{v\}$
$\qquad$ In the following BY proof, $\langle 1 \rangle 2$ denotes the case assumption *Next*
$\qquad$ BY $\langle 1 \rangle 2$ DEF $Next$
$\quad \langle 2 \rangle 2.$ QED
$\qquad$ In the following BY proof, $\langle 1 \rangle 1$ refers to the assumptions
$\qquad$ *Inv* and [*Next*]_*vars*
$\qquad$ BY $\langle 1 \rangle 1,\ \langle 2 \rangle 1,\ SingletonCardinality,\ 1 \leq 1$ DEF $Inv,\ TypeOK,\ Next,\ vars$
$\langle 1 \rangle 4.$CASE $vars' = vars$
$\quad$ BY $\langle 1 \rangle 1,\ \langle 1 \rangle 4$ DEF $Inv,\ TypeOK,\ Next,\ vars$
$\langle 1 \rangle 5.$ QED
$\quad$ BY $\langle 1 \rangle 1,\ \langle 1 \rangle 2,\ \langle 1 \rangle 4$ DEF $Next$

TLAPS does not yet handle temporal logic reasoning. Therefore, proofs of temporal steps are omitted. However, we indicate in comments what we expect the proofs to look like when *TLAPS* does prove temporal formulas.

THEOREM $Invariance \triangleq Spec \Rightarrow \Box Inv$
$\langle 1 \rangle 1.\ \ Init \Rightarrow Inv$
$\quad$ We usually have to use *SimpleArithmetic* to prove facts about numbers,
$\quad$ but $0 \leq 1$ is simple enough that *Isabelle* can prove it by itself.
$\quad$ BY $EmptySetCardinality,\ 0 \leq 1$ DEF $Init,\ Inv,\ TypeOK$

$\langle 1 \rangle 2.$ QED
$\quad \langle 2 \rangle 1.\ Inv \land \Box[Next]_{vars} \Rightarrow \Box Inv$ Typo corrected here 28 *Jun* 2016
$\quad$ BY $InductiveInvariance,\ RuleINV1$

PROOF OMITTED

*RuleInv*1 is defined in the *TLAPS* module by

THEOREM *RuleINV*1 $\triangleq$ ASSUME STATE I, STATE F, ACTION N,
I $\wedge$ $[N]\_F \Rightarrow$ I'
PROVE I $\wedge \Box[N]_F \Rightarrow \Box$I

$\langle 2\rangle 2.$ QED
BY $\langle 1\rangle 1$, $\langle 2\rangle 1$
PROOF OMITTED

We now define *LiveSpec* to be the algorithm's specification with the added fairness condition of weak fairness of the next-state relation, which asserts that execution does not stop if some action is enabled. The temporal formula *Success* asserts that some value is eventually chosen. Below, we prove that *LiveSpec* implies *Success* This means that, in every behavior satisfying *LiveSpec*, some value is chosen.

$LiveSpec \triangleq Spec \wedge \mathrm{WF}_{vars}(Next)$
$Success \triangleq \Diamond(chosen \neq \{\})$

For liveness, we need to assume that there exists at least one value.

ASSUME $ValueNonempty \triangleq Value \neq \{\}$

TLAPS does not yet reason about ENABLED . Therefore, we must omit all proofs that involve ENABLED formulas. To perform as much of the proof as possible, as much as possible we restrict the use of an ENABLED expression to a step asserting that it equals its definition. ENABLED A is true of a state s iff there is a state t such that the step $s \rightarrow t$ satisfies A. It follows from this semantic definition that ENABLED A equals the formula obtained by

1. Expanding all definitions of defined symbols in A until all primes are priming variables.
2. For each primed variable, replacing every instance of that primed variable by a new symbol (the same symbol for each primed variable).
3. Existentially quantifying over those new symbols.

LEMMA $EnabledDef \triangleq$
$TypeOK \Rightarrow$
$((\text{ENABLED } \langle Next\rangle_{vars}) \equiv (chosen = \{\}))$
$\langle 1\rangle$ DEFINE $E \triangleq$
$\exists\, chosenp :$
$\wedge \ \wedge chosen = \{\}$
$\ \ \ \wedge \exists\, v \in Value : chosenp = \{v\}$
$\wedge \ \neg(\langle chosenp\rangle = \langle chosen\rangle)$
$\langle 1\rangle 1.$ $E = \text{ENABLED } \langle Next\rangle_{vars}$
BY DEF *Next*, *vars*
PROOF OMITTED
$\langle 1\rangle 2.$ SUFFICES ASSUME $TypeOK$
PROVE $E = (chosen = \{\})$
BY $\langle 1\rangle 1$
PROOF OMITTED
$\langle 1\rangle 3.$ $E = \exists\, chosenp : E!(chosenp)!1$

BY $\langle 1\rangle 2$ DEF $TypeOK$
$\langle 1\rangle 4.$ $@ = (chosen = \{\})$
BY $\langle 1\rangle 2$, $ValueNonempty$ DEF $TypeOK$
$\langle 1\rangle 5.$ QED
BY $\langle 1\rangle 3$, $\langle 1\rangle 4$

Here is our proof that *Livespec* implies *Success*. It uses the standard TLA proof rules. For example *RuleWF*1 is defined in the *TLAPS* module to be the rule *WF*1 discussed in

```
AUTHOR  = "Leslie Lamport",
TITLE   = "The Temporal Logic of Actions",
JOURNAL = toplas,
volume  = 16,
number  = 3,
YEAR    = 1994,
month   = may,
PAGES   = "872--923"
```

PTL stands for propositional temporal logic reasoning. We expect that, when *TLAPS* handles temporal reasoning, it will use a decision procedure for *PTL*.

THEOREM $LiveSpec \Rightarrow Success$
$\langle 1\rangle 1. \Box Inv \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(Next) \Rightarrow (chosen = \{\} \leadsto chosen \neq \{\})$
$\langle 2\rangle 1.$ SUFFICES $\Box[Next]_{vars} \land \mathrm{WF}_{vars}(Next) \Rightarrow ((Inv \land chosen = \{\}) \leadsto chosen \neq \{\})$
OBVIOUS
PROOF OMITTED
$\langle 2\rangle 2.$ $(Inv \land (chosen = \{\})) \land [Next]_{vars} \Rightarrow ((Inv' \land (chosen' = \{\})) \lor chosen' \neq \{\})$
BY $InductiveInvariance$
$\langle 2\rangle 3.$ $(Inv \land (chosen = \{\})) \land \langle Next\rangle_{vars} \Rightarrow (chosen' \neq \{\})$
BY DEF Inv, $Next$, $vars$
$\langle 2\rangle 4.$ $(Inv \land (chosen = \{\})) \Rightarrow$ ENABLED $\langle Next\rangle_{vars}$
BY $EnabledDef$ DEF Inv
PROOF OMITTED
$\langle 2\rangle 5.$ QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $RuleWF1$
PROOF OMITTED
$\langle 1\rangle 2.$ $(chosen = \{\} \leadsto chosen \neq \{\}) \Rightarrow ((chosen = \{\}) \Rightarrow \Diamond(chosen \neq \{\}))$
OBVIOUS
PROOF OMITTED
$\langle 1\rangle 3.$ QED
BY $Invariance$, $\langle 1\rangle 1$, $\langle 1\rangle 2$ DEF $LiveSpec$, $Spec$, $Init$, $Success$
PROOF OMITTED

The following theorem is used in the refinement proof in module *VoteProof*.

THEOREM $LiveSpecEquals \triangleq$
$LiveSpec \equiv Spec \land (\Box\Diamond\langle Next\rangle_{vars} \lor \Box\Diamond(chosen \neq \{\}))$
$\langle 1\rangle 1. \land Spec \equiv Spec \land \Box TypeOK$
$\land LiveSpec \equiv LiveSpec \land \Box TypeOK$
BY $Invariance$ DEF $LiveSpec$, Inv

PROOF OMITTED

$\langle 1 \rangle 2. \Box \mathit{TypeOK} \Rightarrow ((\Box\Diamond\neg \text{ENABLED } \langle \mathit{Next} \rangle_{\mathit{vars}}) \equiv \Box\Diamond(\mathit{chosen} \neq \{\}))$

$\langle 2 \rangle 1. \Box \mathit{TypeOK} \Rightarrow \Box((\neg \text{ENABLED } \langle \mathit{Next} \rangle_{\mathit{vars}}) \equiv (\mathit{chosen} \neq \{\}))$

BY *EnabledDef*

PROOF OMITTED

$\langle 2 \rangle 2.$ QED

BY $\langle 2 \rangle 1$

PROOF OMITTED

$\langle 1 \rangle 3.$ QED

BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$ DEF *LiveSpec*

PROOF OMITTED

* Modification History

* Last modified Sat *Nov* 16 22:17:07 *CST* 2019 by *hengxin*

* Last modified *Tue Feb* 14 13:35:49 *PST* 2012 by *lamport*

* Last modified *Mon Feb* 07 14:46:59 *PST* 2011 by *lamport*