Verifying Fault-Tolerant Distributed Algorithms In
The Heard-Of Model*

Henri Debrat\(^1\) and Stephan Merz\(^2\)
\(^1\) Université de Lorraine & LORIA
\(^2\) Inria Nancy Grand-Est & LORIA
Villers-lès-Nancy, France
August 28, 2014

Distributed computing is inherently based on replication, promising increased tolerance to failures of individual computing nodes or communication channels. Realizing this promise, however, involves quite subtle algorithmic mechanisms, and requires precise statements about the kinds and numbers of faults that an algorithm tolerates (such as process crashes, communication faults or corrupted values). The landmark theorem due to Fischer, Lynch, and Paterson shows that it is impossible to achieve Consensus among \(N\) asynchronously communicating nodes in the presence of even a single permanent failure. Existing solutions must rely on assumptions of “partial synchrony”.

Indeed, there have been numerous misunderstandings on what exactly a given algorithm is supposed to realize in what kinds of environments. Moreover, the abundance of subtly different computational models complicates comparisons between different algorithms. Charron-Bost and Schiper introduced the Heard-Of model for representing algorithms and failure assumptions in a uniform framework, simplifying comparisons between algorithms.

In this contribution, we represent the Heard-Of model in Isabelle/HOL. We define two semantics of runs of algorithms with different unit of atomicity and relate these through a \textit{reduction theorem} that allows us to verify algorithms in the coarse-grained semantics (where proofs are easier) and infer their correctness for the fine-grained one (which corresponds to actual executions). We instantiate the framework by verifying six Consensus algorithms that differ in the underlying algorithmic mechanisms and the kinds of faults they tolerate.

\*Bernadette Charron-Bost introduced us to the Heard-Of model and accompanied this work by suggesting algorithms to study, providing or simplifying hand proofs, and giving most valuable feedback on our formalizations. Mouna Chaouch-Saad contributed an initial draft formalization of the reduction theorem.
7.4 Preliminary Lemmas ........................................ 41
7.5 Boundedness and Monotonicity of Timestamps .......... 44
7.6 Obvious Facts About the Algorithm ...................... 44
7.7 Proof of Integrity ......................................... 47
7.8 Proof of Agreement and Irrevocability .................. 47
7.9 Proof of Termination ..................................... 49
7.10 LastVoting Solves Consensus .......................... 49

8 Verification of the $U_{T,E,\alpha}$ Consensus Algorithm .... 50
  8.1 Model of the Algorithm .................................. 50
  8.2 Communication Predicate for $U_{T,E,\alpha}$ .............. 52
  8.3 The $U_{T,E,\alpha}$ Heard-Of Machine ...................... 53
  8.4 Preliminary Lemmas ..................................... 54
  8.5 Proof of Agreement and Validity ....................... 55
  8.6 Proof of Termination ................................... 57
  8.7 $U_{T,E,\alpha}$ Solves Weak Consensus ................... 58

9 Verification of the $A_{T,E,\alpha}$ Consensus Algorithm ....... 59
  9.1 Model of the Algorithm .................................. 59
  9.2 Communication Predicate for $A_{T,E,\alpha}$ .............. 60
  9.3 The $A_{T,E,\alpha}$ Heard-Of Machine ...................... 61
  9.4 Preliminary Lemmas ..................................... 61
  9.5 Proof of Validity ....................................... 63
  9.6 Proof of Agreement ..................................... 63
  9.7 Proof of Termination ................................... 64
  9.8 $A_{T,E,\alpha}$ Solves Weak Consensus ................... 64

10 Verification of the $EIGByz_f$ Consensus Algorithm ...... 65
  10.1 Tree Data Structure .................................... 65
  10.2 Model of the Algorithm ................................ 66
  10.3 Communication Predicate for $EIGByz_f$ ............... 68
  10.4 The $EIGByz_f$ Heard-Of Machine ...................... 69
  10.5 Preliminary Lemmas .................................... 69
  10.6 Lynch’s Lemmas and Theorems .......................... 72
  10.7 Proof of Agreement, Validity, and Termination ......... 75
  10.8 $EIGByz_f$ Solves Weak Consensus .................... 76

11 Conclusion .................................................. 77
1 Introduction

We are interested in the verification of fault-tolerant distributed algorithms. The archetypical problem in this area is the Consensus problem that requires a set of distributed nodes to achieve agreement on a common value in the presence of faults. Such algorithms are notoriously hard to design and to get right. This is particularly true in the presence of asynchronous communication: the landmark theorem by Fischer, Lynch, and Paterson [9] shows that there is no algorithm solving the Consensus problem for asynchronous systems in the presence of even a single, permanent fault. Existing solutions therefore rely on assumptions of “partial synchrony” [8].

Different computational models, and different concepts for specifying the kinds and numbers of faults such algorithms must tolerate, have been introduced in the literature on distributed computing. This abundance of subtly different notions makes it very difficult to compare different algorithms, and has sometimes even led to misunderstandings and misinterpretations of what an algorithm claims to achieve. The general lack of rigorous, let alone formal, correctness proofs for this class of algorithms makes it even harder to understand the field.

In this contribution, we formalize in Isabelle/HOL the Heard-Of (HO) model, originally introduced by Charron-Bost and Schiper [7]. This model can represent algorithms that operate in communication-closed rounds, which is true of virtually all known fault-tolerant distributed algorithms. Assumptions on failures tolerated by an algorithm are expressed by communication predicates that impose bounds on the set of messages that are not received during executions. Charron-Bost and Schiper show how the known failure hypotheses from the literature can be represented in this format. The Heard-Of model therefore makes an interesting target for formalizing different algorithms, and for proving their correctness, in a uniform way. In particular, different assumptions can be compared, and the suitability of an algorithm for a particular situation can be evaluated.

The HO model has subsequently been extended [3] to encompass algorithms designed to tolerate value (also known as malicious or Byzantine) faults. In the present work, we propose a generic framework in Isabelle/HOL that encompasses the different variants of HO algorithms, including resilience to benign or value faults, as well as coordinated and non-coordinated algorithms.

A fundamental design decision when modeling distributed algorithm is to determine the unit of atomicity. We formally relate in Isabelle two definitions of runs: we first define “coarse-grained” executions, in which entire rounds are executed atomically, and then define “fine-grained” executions that correspond to conventional interleaving representations of asynchronous networks. We formally prove that every fine-grained execution corresponds
to a certain coarse-grained execution, such that every process observes the same sequence of local states in the two executions, up to stuttering. As a corollary, a large class of correctness properties, including Consensus, can be transferred from coarse-grained to fine-grained executions.

We then apply our framework for verifying six different distributed Consensus algorithms w.r.t. their respective communication predicates. The first three algorithms, One-Third Rule, UniformVoting, and LastVoting, tolerate benign failures. The three remaining algorithms, $U_{T,E,\alpha}$, $A_{T,E,\alpha}$, and $EIGByz_f$, are designed to tolerate value failures, and solve a weaker variant of the Consensus problem.


theory HOModel
imports Main
begin

declare split-if-asm [split] — perform default perform case splitting on conditionals

2 Heard-Of Algorithms

2.1 The Consensus Problem

We are interested in the verification of fault-tolerant distributed algorithms. The Consensus problem is paradigmatic in this area. Stated informally, it assumes that all processes participating in the algorithm initially propose some value, and that they may at some point decide some value. It is required that every process eventually decides, and that all processes must decide the same value.

More formally, we represent runs of algorithms as $\omega$-sequences of configurations (vectors of process states). Hence, a run is modeled as a function of type $\text{nat} \Rightarrow \text{proc} \Rightarrow \text{pst}$ where type variables $\text{proc}$ and $\text{pst}$ represent types of processes and process states, respectively. The Consensus property is expressed with respect to a collection $\text{vals}$ of initially proposed values (one per process) and an observer function $\text{dec} : \text{pst} \Rightarrow \text{val option}$ that retrieves the decision (if any) from a process state. The Consensus problem is stated as the conjunction of the following properties:

**Integrity.** Processes can only decide initially proposed values.

**Agreement.** Whenever processes $p$ and $q$ decide, their decision values must be the same. (In particular, process $p$ may never change the value it
decides, which is referred to as Irrevocability.)

**Termination.** Every process decides eventually.

The above properties are sometimes only required of non-faulty processes, since nothing can be required of a faulty process. The Heard-Of model does not attribute faults to processes, and therefore the above formulation is appropriate in this framework.

**type-synonym**

\[(\text{'proc,'pst}) \text{ run} = \text{nat} \Rightarrow \text{'proc} \Rightarrow \text{'pst}\]

**definition**

\[\text{consensus} :: (\text{'proc} \Rightarrow \text{'val}) \Rightarrow (\text{'pst} \Rightarrow \text{'val option}) \Rightarrow (\text{'proc,'pst}) \text{ run} \Rightarrow \text{bool}\]

**where**

\[\text{consensus vals dec rho} \equiv\]

\[
(\forall n p v. \text{ dec } (\text{rho } n p) = \text{Some } v \rightarrow v \in \text{range vals})
\]

\[
\land (\forall m n p q v w. \text{ dec } (\text{rho } m p) = \text{Some } v \land \text{ dec } (\text{rho } n q) = \text{Some } w
\]

\[
\rightarrow v = w)
\]

\[
\land (\forall p. \exists n. \text{ dec } (\text{rho } n p) \neq \text{None})
\]

A variant of the Consensus problem replaces the Integrity requirement by

**Validity.** If all processes initially propose the same value \(v\) then every process may only decide \(v\).

**definition**

\[\text{weak-consensus where}\]

\[\text{weak-consensus vals dec rho} \equiv\]

\[
(\forall v. (\forall p. \text{ vals } p = v) \rightarrow (\forall n p w. \text{ dec } (\text{rho } n p) = \text{Some } w \rightarrow w = v))
\]

\[
\land (\forall m n p q v w. \text{ dec } (\text{rho } m p) = \text{Some } v \land \text{ dec } (\text{rho } n q) = \text{Some } w
\]

\[
\rightarrow v = w)
\]

\[
\land (\forall p. \exists n. \text{ dec } (\text{rho } n p) \neq \text{None})
\]

Clearly, **consensus** implies **weak-consensus**.

**lemma** **consensus-then-weak-consensus:**

**assumes** \[\text{consensus vals dec rho}\]

**shows** \[\text{weak-consensus vals dec rho}\]

(\text{proof})

Over Boolean values (“binary Consensus”), **weak-consensus** implies **consensus**, hence the two problems are equivalent. In fact, this theorem holds more generally whenever at most two different values are proposed initially (i.e., \(\text{card (range vals)} \leq 2\)).

**lemma** **binary-weak-consensus-then-consensus:**

**assumes** \[\text{bc: weak-consensus (vals::'proc} \Rightarrow \text{bool}) \text{ dec rho}\]

**shows** \[\text{consensus vals dec rho}\]

(\text{proof})
The algorithms that we are going to verify solve the Consensus or weak Consensus problem, under different hypotheses about the kinds and number of faults.

### 2.2 A Generic Representation of Heard-Of Algorithms

Charron-Bost and Schiper [7] introduce the Heard-Of (HO) model for representing fault-tolerant distributed algorithms. In this model, algorithms execute in communication-closed rounds: at any round $r$, processes only receive messages that were sent for that round. For every process $p$ and round $r$, the “heard-of set” $HO(p, r)$ denotes the set of processes from which $p$ receives a message in round $r$. Since every process is assumed to send a message to all processes in each round, the complement of $HO(p, r)$ represents the set of faults that may affect $p$ in round $r$ (messages that were not received, e.g. because the sender crashed, because of a network problem etc.).

The HO model expresses hypotheses on the faults tolerated by an algorithm through “communication predicates” that constrain the sets $HO(p, r)$ that may occur during an execution. Charron-Bost and Schiper show that standard fault models can be represented in this form.

The original HO model is sufficient for representing algorithms tolerating benign failures such as process crashes or message loss. A later extension for algorithms tolerating Byzantine (or value) failures [3] adds a second collection of sets $SHO(p, r) \subseteq HO(p, r)$ that contain those processes $q$ from which process $p$ receives the message that $q$ was indeed supposed to send for round $r$ according to the algorithm. In other words, messages from processes in $HO(p, r) \setminus SHO(p, r)$ were corrupted, be it due to errors during message transmission or because of the sender was faulty or lied deliberately. For both benign and Byzantine errors, the HO model registers the fault but does not try to identify the faulty component (i.e., designate the sending or receiving process, or the communication channel as the “culprit”).

Executions of HO algorithms are defined with respect to collections $HO(p, r)$ and $SHO(p, r)$. However, the code of a process does not have access to these sets. In particular, process $p$ has no way of determining if a message it received from another process $q$ corresponds to what $q$ should have sent or if it has been corrupted.

Certain algorithms rely on the assignment of “coordinator” processes for each round. Just as the collections $HO(p, r)$, the definitions assume an external coordinator assignment such that $coord(p, r)$ denotes the coordinator of process $p$ and round $r$. Again, the correctness of algorithms may depend on hypotheses about coordinator assignments – e.g., it may be assumed that processes agree sufficiently often on who the current coordinator is.

The following definitions provide a generic representation of HO and SHO algorithms in Isabelle/HOL. A (coordinated) HO algorithm is described by
the following parameters:

- a finite type 'proc of processes,
- a type 'pst of local process states,
- a type 'msg of messages sent in the course of the algorithm,
- a predicate CinitState such that CinitState p st crd is true precisely of the initial states st of process p, assuming that crd is the initial coordinator of p,
- a function sendMsg where sendMsg r p q st yields the message that process p sends to process q at round r, given its local state st, and
- a predicate CnextState where CnextState r p st msgs crd st' characterizes the successor states st' of process p at round r, given current state st, the vector msgs :: 'proc ⇒ 'msg option of messages that p received at round r (msgs q = None indicates that no message has been received from process q), and process crd as the coordinator for the following round.

Note that every process can store the coordinator for the current round in its local state, and it is therefore not necessary to make the coordinator a parameter of the message sending function sendMsg.

We represent an algorithm by a record as follows.

\[
\text{record}\ ('\text{proc}, '\text{pst}, '\text{msg})\ CHOAlgorithm =
\hspace{1cm}\text{CinitState : 'proc ⇒ 'pst ⇒ 'proc ⇒ bool}
\hspace{1cm}\text{sendMsg : nat ⇒ 'proc ⇒ 'proc ⇒ 'pst ⇒ 'msg}
\hspace{1cm}\text{CnextState : nat ⇒ 'proc ⇒ 'pst ⇒ ('proc ⇒ 'msg option) ⇒ 'proc ⇒ 'pst ⇒ bool}
\]

For non-coordinated HO algorithms, the coordinator argument of functions CinitState and CnextState is irrelevant, and we define utility functions that omit that argument.

\[
\text{definition}\ isNCAlgorithm where
\hspace{1cm}\text{isNCAlgorithm alg ≡}
\hspace{1cm}(\forall p\ st\ crd\ crd'.\ CinitState alg p st crd = CinitState alg p st crd')
\hspace{1cm}\land\ (\forall r\ p\ st\ msgs\ crd\ crd'\ st'.\ CnextState alg r p st msgs crd st' = CnextState alg r p st msgs crd' st')
\]

\[
\text{definition}\ initState where
\hspace{1cm}\text{initState alg p st ≡ CinitState alg p st undefined}
\]

\[
\text{definition}\ nextState where
\hspace{1cm}\text{nextState alg r p st msgs st' ≡ CnextState alg r p st msgs undefined st'}
\]
A *heard-of assignment* associates a set of processes with each process. The following type is used to represent the collections $HO(p, r)$ and $SHO(p, r)$ for fixed round $r$. Similarly, a *coordinator assignment* associates a process (its coordinator) to each process.

**type-synonym**

\[
\text{'proc } HO = \text{'proc } \Rightarrow \text{'proc set}
\]

**type-synonym**

\[
\text{'proc coord } = \text{'proc } \Rightarrow \text{'proc}
\]

An execution of an HO algorithm is defined with respect to HO and SHO assignments that indicate, for every round $r$ and every process $p$, from which sender processes $p$ receives messages (resp., uncorrupted messages) at round $r$.

The following definitions formalize this idea. We define “coarse-grained” executions whose unit of atomicity is the round of execution. At each round, the entire collection of processes performs a transition according to the $CnextState$ function of the algorithm. Consequently, a system state is simply described by a configuration, i.e. a function assigning a process state to every process. This definition of executions may appear surprising for an asynchronous distributed system, but it simplifies system verification, compared to a “fine-grained” execution model that records individual events such as message sending and reception or local transitions. We will justify later why the “coarse-grained” model is sufficient for verifying interesting correctness properties of HO algorithms.

The predicate $CSHOinitConfig$ describes the possible initial configurations for algorithm $A$ (remember that a configuration is a function that assigns local states to every process).

**definition** $CSHOinitConfig$ where

\[
CSHOinitConfig A \ cfg \ (\text{coord} :: \text{'proc coord}) \equiv \forall p. \ CinitState A p (\ cfg \ p) \ (\text{ coord} \ p)
\]

Given the current configuration $cfg$ and the HO and SHO sets $HOp$ and $SHOp$ for process $p$ at round $r$, the function $SHOmsgVectors$ computes the set of possible vectors of messages that process $p$ may receive. For processes $q \notin HOp$, $p$ receives no message (represented as value $None$). For processes $q \in SHOp$, $p$ receives the message that $q$ computed according to the $sendMsg$ function of the algorithm. For the remaining processes $q \in HOp - SHOp$, $p$ may receive some arbitrary value.

**definition** $SHOmsgVectors$ where

\[
SHOmsgVectors A r p \ cfg \ HOp \ SHOp \equiv \\
\{ \mu. \ (\forall q. \ q \in HOp \iff \mu \ q \neq None) \\
\land \ (\forall q. \ q \in SHOp \cap HOp \rightarrow \mu \ q = Some (sendMsg A r q p (cfg \ q))) \}
\]

Predicate $CSHOnextConfig$ uses the preceding function and the algorithm’s $CnextState$ function to characterize the possible successor configurations
in a coarse-grained step, and predicate \texttt{CSHORun} defines (coarse-grained) executions \texttt{rho} of an HO algorithm.

\textbf{definition CSHOnextConfig where}
\begin{align*}
\texttt{CSHOnextConfig A r \; \texttt{cfg} \; \texttt{HO} \; \texttt{SHO} \; \texttt{coord} \; \texttt{cfg}' & \equiv \\
\forall p. \exists \mu \in \texttt{SHOmsgVectors A r p \; \texttt{cfg} \; (HO \; p) \; (SHO \; p)}, \texttt{CnextState A r p \; (cfg \; p) \; \mu \; (coord \; p) \; (cfg' \; p)}
\end{align*}

\textbf{definition CSHORun where}
\begin{align*}
\texttt{CSHORun A \; \texttt{rho} \; \texttt{HOs} \; \texttt{SHOs} \; \texttt{coords} & \equiv \\
\texttt{CHOinitConfig A \; \texttt{rho} \; 0 \; (coords \; 0)} \land (\forall r. \texttt{CSHOnextConfig A r \; (rho \; r) \; (HOs \; r) \; (SHOs \; r) \; (coords \; (Suc \; r))} \\
& \quad \texttt{(rho \; (Suc \; r))})
\end{align*}

For non-coordinated algorithms, the \texttt{coord} arguments of the above functions are irrelevant. We define similar functions that omit that argument, and relate them to the above utility functions for these algorithms.

\textbf{definition HOinitConfig where}
\begin{align*}
\texttt{HOinitConfig A \; \texttt{cfg} & \equiv \texttt{CHOinitConfig A \; \texttt{cfg} \; (\lambda q. \texttt{undefined})} \\
\textbf{lemma HOinitConfig-eq:} \quad \texttt{HOinitConfig A \; \texttt{cfg} = (\forall p. \texttt{initState A p \; (cfg \; p)})}
\end{align*}

\textbf{definition SHOnextConfig where}
\begin{align*}
\texttt{SHOnextConfig A r \; \texttt{cfg} \; \texttt{HO} \; \texttt{SHO} \; \texttt{cfg}' & \equiv \\
\texttt{CSHOnextConfig A r \; \texttt{cfg} \; \texttt{HO} \; \texttt{SHO} \; (\lambda q. \texttt{undefined}) \; \texttt{cfg}'}
\end{align*}

\textbf{lemma SHOnextConfig-eq:}
\begin{align*}
\texttt{SHOnextConfig A r \; \texttt{cfg} \; \texttt{HO} \; \texttt{SHO} \; \texttt{cfg}' & = \\
(\forall p. \exists \mu \in \texttt{SHOmsgVectors A r p \; \texttt{cfg} \; (HO \; p) \; (SHO \; p)}, \texttt{CnextState A r p \; (cfg \; p) \; \mu \; (cfg' \; p)})
\end{align*}

\textbf{definition SHORun where}
\begin{align*}
\texttt{SHORun A \; \texttt{rho} \; \texttt{HOs} \; \texttt{SHOs} & \equiv \\
\texttt{CSHORun A \; \texttt{rho} \; \texttt{HOs} \; \texttt{SHOs} \; (\lambda r \; q. \texttt{undefined})}
\end{align*}

\textbf{lemma SHORun-eq:}
\begin{align*}
\texttt{SHORun A \; \texttt{rho} \; \texttt{HOs} \; \texttt{SHOs} & = \\
(\texttt{HOinitConfig A \; (rho \; 0)} \land (\forall r. \texttt{SHOnextConfig A r \; (rho \; r) \; (HOs \; r) \; (SHOs \; r) \; (rho \; (Suc \; r))}))
\end{align*}

Algorithms designed to tolerate benign failures are not subject to message corruption, and therefore the SHO sets are irrelevant (more formally, each SHO set equals the corresponding HO set). We define corresponding special cases of the definitions of successor configurations and of runs, and prove that these are equivalent to simpler definitions that will be more useful in
proofs. In particular, the vector of messages received by a process in a benign execution is uniquely determined from the current configuration and the HO sets.

**definition** \texttt{HOrcvdMsgs where} \texttt{HOrcvdMsgs A r p HO cfg} \equiv \lambda q. \text{if } q \in \text{HO} \text{ then Some (sendMsg A r q (cfg q)) } \text{else None}

**lemma** \texttt{SHOmsgVectors-HO:} \texttt{SHOmsgVectors A r p HO HO} = \{ \texttt{HOrcvdMsgs A r p HO cfg} \}

With coordinators

**definition** \texttt{CHOnextConfig where} \texttt{CHOnextConfig A r cfg HO coord cfg'} \equiv \texttt{CSHOnextConfig A r cfg HO HO coord cfg'}

**lemma** \texttt{CHOnextConfig-eq:} \texttt{CHOnextConfig A r cfg HO coord cfg'} = \langle \forall p. \text{CnextState A r p (cfg p)} \texttt{(HOrcvdMsgs A r p (HO p) cfg)} (\texttt{coord p}) (\texttt{cfg' p}) \rangle

**definition** \texttt{CHORun where} \texttt{CHORun A rho HOs coords} \equiv \texttt{CSHORun A rho HOs HOs coords}

**lemma** \texttt{CHORun-eq:} \texttt{CHORun A rho HOs coords} = \langle \texttt{HOinitConfig A (rho 0) (coords 0)} \ \wedge \langle \forall r. \texttt{CHOnextConfig A r (rho r) (HOs r) (coords (Suc r)) (rho (Suc r))} \rangle \rangle

Without coordinators

**definition** \texttt{HOnextConfig where} \texttt{HOnextConfig A r cfg HO cfg'} \equiv \texttt{SHOnextConfig A r cfg HO HO cfg'}

**lemma** \texttt{HOnextConfig-eq:} \texttt{HOnextConfig A r cfg HO cfg'} = \langle \forall p. \text{nextState A r p (cfg p)} \texttt{(HOrcvdMsgs A r p (HO p) cfg)} (\texttt{cfg' p}) \rangle

**definition** \texttt{HORun where} \texttt{HORun A rho HOs} \equiv \texttt{SHORun A rho HOs HOs}

**lemma** \texttt{HORun-eq:} \texttt{HORun A rho HOs} = \langle \texttt{HOinitConfig A (rho 0)} \ \wedge \langle \forall r. \texttt{HOnextConfig A r (rho r) (HOs r) (rho (Suc r))} \rangle \rangle
The following derived proof rules are immediate consequences of the definition of \(\text{CHORun}\); they simplify automatic reasoning.

**Lemma CHORun-0:**

- **Assumes:** \(\text{CHORun} \ A \ \rho \ O H \ \text{coords}\)
  
- **And:** \(\forall \text{cfg}. \ \text{CHOinitConfig} \ A \ \text{cfg} \ (\text{coords} \ 0) \implies \ P \ \text{cfg}\)

- **Shows:** \(P \ (\rho \ 0)\)

(\text{proof})

**Lemma CHORun-Suc:**

- **Assumes:** \(\text{CHORun} \ A \ \rho \ O H \ \text{coords}\)
  
- **And:** \(\forall \. \ \text{CHOnextConfig} \ A \ r \ (\rho \ r) \ (H O S \ r) \ (\text{coords} \ (S u c \ r)) \ (\rho \ (S u c \ r)) \implies \ P \ r\)

- **Shows:** \(P \ n\)

(\text{proof})

**Lemma CHORun-induct:**

- **Assumes:** \(\text{run}: \ \text{CHORun} \ A \ \rho \ O H \ \text{coords}\)
  
- **And:** \(\text{init}: \ \text{CHOinitConfig} \ A \ (\rho \ 0) \ (\text{coords} \ 0) \implies \ P \ 0\)
  
- **And:** \(\forall \. [\. [P \ r; \ \text{CHOnextConfig} \ A \ r \ (\rho \ r) \ (H O S \ r) \ (\text{coords} \ (S u c \ r)) \ (\rho \ (S u c \ r))] \implies \ P \ (S u c \ r)\]

- **Shows:** \(P \ n\)

(\text{proof})

Because algorithms will not operate for arbitrary HO, SHO, and coordinator assignments, these are constrained by a communication predicate. For convenience, we split this predicate into a per Round part that is expected to hold at every round and a global part that must hold of the sequence of (S)HO assignments and may thus express liveness assumptions.

In the parlance of [7], a \(\text{HO machine}\) is an HO algorithm augmented with a communication predicate. We therefore define (C)(S)HO machines as the corresponding extensions of the record defining an HO algorithm.

**Record** \(\langle\text{proc}, \ \text{msg}\rangle \ \text{HOMachine} = (\langle\text{proc}, \ \text{msg}\rangle \ \text{CHOAlgorithm} + \ \text{HOcommPerRd} :: (\text{proc HO} \Rightarrow \text{bool}) \ \text{HOcommGlobal} :: (\text{nat} \Rightarrow \text{proc HO}) \Rightarrow \text{bool}\)

**Record** \(\langle\text{proc}, \ \text{msg}\rangle \ \text{CHOMachine} = (\langle\text{proc}, \ \text{msg}\rangle \ \text{CHOAlgorithm} + \ \text{CHOcommPerRd} :: (\text{proc HO} \Rightarrow \text{proc coord} \Rightarrow \text{bool}) \ \text{CHOcommGlobal} :: (\text{nat} \Rightarrow \text{proc HO}) \Rightarrow (\text{nat} \Rightarrow \text{proc coord}) \Rightarrow \text{bool}\)

**Record** \(\langle\text{proc}, \ \text{msg}\rangle \ \text{SHOMachine} = (\langle\text{proc}, \ \text{msg}\rangle \ \text{CHOAlgorithm} + \ \text{SHOcommPerRd} :: (\text{proc HO} \Rightarrow (\text{proc HO}) \Rightarrow \text{bool}) \ \text{SHOcommGlobal} :: (\text{nat} \Rightarrow \text{proc HO}) \Rightarrow (\text{nat} \Rightarrow \text{proc HO}) \Rightarrow \text{bool}\)

**Record** \(\langle\text{proc}, \ \text{msg}\rangle \ \text{CSHOMachine} = (\langle\text{proc}, \ \text{msg}\rangle \ \text{CHOAlgorithm} + \ \text{CSHOcommPerRd} :: (\text{proc HO} \Rightarrow (\text{proc HO}) \Rightarrow \text{proc coord} \Rightarrow \text{bool}) \ \text{CSHOcommGlobal} :: (\text{nat} \Rightarrow \text{proc HO}) \Rightarrow (\text{nat} \Rightarrow \text{proc HO}) \Rightarrow (\text{nat} \Rightarrow \text{proc coord}) \Rightarrow \text{bool}\)

12
3 Reduction Theorem

We have defined the semantics of HO algorithms such that rounds are executed atomically, by all processes. This definition is surprising for a model of asynchronous distributed algorithms since it models a synchronous execution of rounds. However, it simplifies representing and reasoning about the algorithms. For example, the communication network does not have to be modeled explicitly, since the possible sets of messages received by processes can be computed from the global configuration and the collections of HO and SHO sets.

We will now define a more conventional “fine-grained” semantics where communication is modeled explicitly and rounds of processes can be arbitrarily interleaved (subject to the constraints of the communication predicates). We will then establish a reduction theorem that shows that for every fine-grained run there exists an equivalent round-based (“coarse-grained”) run in the sense that the two runs exhibit the same sequences of local states of all processes, modulo stuttering. We prove the reduction theorem for the most general class of coordinated SHO algorithms. It is easy to see that the theorem equally holds for the special cases of uncoordinated or HO algorithms, and since we have in fact defined these classes of algorithms from the more general ones, we can directly apply the general theorem.

As a corollary, interesting properties remain valid in the fine-grained semantics if they hold in the coarse-grained semantics. It is therefore enough to verify such properties in the coarse-grained semantics, which is much easier to reason about. The essential restriction is that properties may not depend on states of different processes occurring simultaneously. (For example, the coarse-grained semantics ensures by definition that all processes execute the same round at any instant, which is obviously not true of the fine-grained semantics.) We claim that all “reasonable” properties of fault-tolerant distributed algorithms are preserved by our reduction. For example, the Consensus (and Weak Consensus) problems fall into this class.

The proofs follow Chaouch-Saad et al. [4], where the reduction theorem was proved for uncoordinated HO algorithms.

3.1 Fine-Grained Semantics

In the fine-grained semantics, a run of an HO algorithm is represented as an $\omega$-sequence of system configurations. Each configuration is represented as a
record carrying the following information:

- for every process $p$, the current round that process $p$ is executing,
- the local state of every process,
- for every process $p$, the set of processes to which $p$ has already sent a message for the current round,
- for all processes $p$ and $q$, the message (if any) that $p$ has received from $q$ for the round that $p$ is currently executing, and
- the set of messages in transit, represented as triples of the form $(p, r, q, m)$ meaning that process $p$ sent message $m$ to process $q$ for round $r$, but $q$ has not yet received that message.

As explained earlier, the coordinators of processes are not recorded in the configuration, but algorithms may record them as part of the process states.

record $(\text{'pst}, \text{'proc}, \text{'msg}) \text{ config } =$
\begin{align*}
\text{round} & : \text{'proc } \Rightarrow \text{nat} \\
\text{state} & : \text{'proc } \Rightarrow \text{'pst} \\
\text{sent} & : \text{'proc } \Rightarrow \text{'proc set} \\
\text{rcvd} & : \text{'proc } \Rightarrow \text{'proc } \Rightarrow \text{'msg } \text{ option} \\
\text{network} & : (\text{'proc }^\ast \text{nat }^\ast \text{'proc }^\ast \text{'msg}) \text{ set}
\end{align*}

\textbf{type-synonym} $(\text{'pst}, \text{'proc}, \text{'msg}) \text{ fgrun } = \text{nat } \Rightarrow (\text{'pst}, \text{'proc}, \text{'msg}) \text{ config}$

In an initial configuration for an algorithm, the local state of every process satisfies the algorithm’s initial-state predicate, and all other components have obvious default values.

\textbf{definition} \text{fg-init-config where}
\begin{align*}
\text{fg-init-config} \ A \ (\text{config}:=(\text{'pst}\text{, 'proc}, \text{'msg}) \text{ config}) \ (\text{coord}:=(\text{'proc coord}) \equiv \\
\text{round config } = (\lambda p. \ 0) \\
\land \ (\forall p. \ \text{CinitState } A \ p \ (\text{state config } p) \ (\text{coord } p)) \\
\land \ \text{sent config } = (\lambda p. \ \{\}) \\
\land \ \text{rcvd config } = (\lambda q. \ \text{None}) \\
\land \ \text{network config } = \{\}
\end{align*}

In the fine-grained semantics, we have three types of transitions due to

- some process sending a message,
- some process receiving a message, and
- some process executing a local transition.

The following definition models process $p$ sending a message to process $q$. The transition is enabled if $p$ has not yet sent any message to $q$ for the
current round. The message to be sent is computed according to the algorithm’s `sendMsg` function. The effect of the transition is to add \( q \) to the `sent` component of the configuration and the message quadruple to the `network` component.

**definition fg-send-msg where**

\[
fg-send-msg A p q \text{config config}' \equiv \\
q \notin (\text{sent config } p) \\
\land \text{config}' = \text{config } (p := \text{sent config } p \cup \{ q \}) \\
\land \text{network} := \text{network config } \cup \\
\{(p, \text{round config } p, q, \\
\text{sendMsg } A \text{(round config } p) \ p \ q \text{(state config } p)\}) \}
\]

The following definition models the reception of a message by process \( p \) from process \( q \). The action is enabled if \( q \) is in the heard-of set \( HO \) of process \( p \) for the current round, and if the network contains some message from \( q \) to \( p \) for the round that \( p \) is currently executing. W.l.o.g., we model message corruption at reception: if \( q \) is not in \( p \)’s \( SHO \) set (parameter \( SHO \)), then an arbitrary value \( m' \) is received instead of \( m \).

**definition fg-rcv-msg where**

\[
fg-rcv-msg p q HO SHO \text{config config}' \equiv \\
\exists m m'. (q, (\text{round config } p), p, m) \in \text{network config} \\
\land q \in HO \\
\land \text{config}' = \text{config } \} \\
\land \text{rcvd} := (\text{rcvd config } p := (\text{rcvd config } p) (q := \\
\text{if } q \in SHO \text{ then Some } m \\text{ else Some } m'), \\
\text{network} := \text{network config } \setminus \{(q, \text{round config } p, p, m)\} \} \\
\]

Finally, we consider local state transition of process \( p \). A local transition is enabled only after \( p \) has sent all messages for its current round and has received all messages that it is supposed to receive according to its current \( HO \) set (parameter \( HO \)). The local state is updated according to the algorithm’s \( CnextState \) relation, which may depend on the coordinator \( crd \) of the following round. The round of process \( p \) is incremented, and the `sent` and `rcvd` components for process \( p \) are reset to initial values for the new round.

**definition fg-local where**

\[
fg-local A p HO crd \text{config config}' \equiv \\
\text{sent config } p = \text{UNIV} \\
\land \text{dom (rcvd config } p) = HO \\
\land (\exists s. \text{CnextState } A \text{(round config } p) \ p \text{(state config } p) \ (\text{rcvd config } p) \ crd \ s) \\
\land \text{config}' = \text{config } \} \\
\land \text{round} := (\text{round config } p := \text{Suc (round config } p)), \\
\text{state} := (\text{state config } p := s), \\
\text{sent} := (\text{sent config } p := \{\}), \\
\text{rcvd} := (\text{rcvd config } p := \lambda q. \text{None} ))
\]
The next-state relation for process \( p \) is just the disjunction of the above three types of transitions.

**Definition** \( \text{fg-next-config} \) where

\[
\text{fg-next-config} \ A \ p \ \text{HO} \ \text{SHO} \ \text{crd} \ \text{config} \ \text{config}' \equiv \\
(\exists q. \ \text{fg-send-msg} \ A \ p \ q \ \text{config} \ \text{config}') \\
\lor (\exists q. \ \text{fg-rce-msg} \ p \ q \ \text{HO} \ \text{SHO} \ \text{config} \ \text{config}') \\
\lor \text{fg-local} \ A \ p \ \text{HO} \ \text{crd} \ \text{config} \ \text{config}'
\]

Fine-grained runs are infinite sequences of configurations that start in an initial configuration and where each step corresponds to some process sending a message, receiving a message or performing a local step. We also require that every process eventually executes every round – note that this condition is implicit in the definition of coarse-grained runs.

**Definition** \( \text{fg-run} \) where

\[
\text{fg-run} \ A \ \rho \ \text{HOs} \ \text{SHOs} \ \text{coords} \equiv \\
\text{fg-init-config} \ A \ (\rho \ 0) \ (\text{coords} \ 0) \\
\land (\forall i. \ \exists p. \ \text{fg-next-config} \ A \ p \\
\quad (\text{HOs} \ (\text{round} \ (\rho \ i) \ p) \ p) \\
\quad (\text{SHOs} \ (\text{round} \ (\rho \ i) \ p) \ p) \\
\quad (\text{coords} \ (\text{round} \ (\rho (\text{Suc} \ i)) \ p) \ p) \\
\quad (\rho \ i) \ (\rho (\text{Suc} \ i))) \\
\land (\forall p \ r. \ \exists n. \ \text{round} \ (\rho \ n) \ p = r)
\]

The following function computes at which “time point” (index in the fine-grained computation) process \( p \) starts executing round \( r \). This function plays an important role in the correspondence between the two semantics, and in the subsequent proofs.

**Definition** \( \text{fg-start-round} \) where

\[
\text{fg-start-round} \ \rho \ p \ r \equiv \text{LEAST} \ (n::\text{nat}). \ \text{round} \ (\rho \ n) \ p = r
\]

### 3.2 Properties of the Fine-Grained Semantics

In preparation for the proof of the reduction theorem, we establish a number of consequences of the above definitions.

Process states change only when round numbers change during a fine-grained run.

**Lemma** \( \text{fg-state-change} \):

- **Assumes** \( \rho: \ \text{fg-run} \ A \ \rho \ \text{HOs} \ \text{SHOs} \ \text{coords} \)
- **And** \( \text{rd}: \ \text{round} \ (\rho (\text{Suc} \ n)) \ p = \text{round} \ (\rho \ n) \ p \)
- **Shows** \( \text{state} \ (\rho (\text{Suc} \ n)) \ p = \text{state} \ (\rho \ n) \ p \)

**Proof**

Round numbers never decrease.

**Lemma** \( \text{fg-round-numbers-increase} \):

- **Assumes** \( \rho: \ \text{fg-run} \ A \ \rho \ \text{HOs} \ \text{SHOs} \ \text{coords} \) and \( n: \ n \leq m \)
shows \( \text{round} (\rho n) \ p \leq \text{round} (\rho m) \ p \)

\(\langle\text{proof}\rangle\)

Combining the two preceding lemmas, it follows that the local states of process \(p\) at two configurations are the same if these configurations have the same round number.

\textbf{lemma fg-same-round-same-state:}

\textbf{assumes} \(\rho:\text{fg-run} \ A \ \rho \ HOs \ \SHOs \ \text{coords}\) and \(r_d: \text{round} (\rho m) \ p = \text{round} (\rho n) \ p\)

\textbf{shows} \(\text{state} (\rho m) \ p = \text{state} (\rho n) \ p\)

\(\langle\text{proof}\rangle\)

Since every process executes every round, function \textit{fg-startRound} is well-defined. We also list a few facts about \textit{fg-startRound} that will be used to show that it is a “stuttering sampling function”, a notion introduced in the theories about stuttering equivalence.

\textbf{lemma fg-start-round:}

\textbf{assumes} \(\text{fg-run} \ A \ \rho \ HOs \ \SHOs \ \text{coords}\)

\textbf{shows} \(\text{round} (\rho (\text{fg-start-round} \ (\rho p \ r))) \ p = r\)

\(\langle\text{proof}\rangle\)

\textbf{lemma fg-start-round-smallest:}

\textbf{assumes} \(\text{round} (\rho k) \ p = r\)

\textbf{shows} \(\text{fg-start-round} \ rho \ p \ r \leq (k::\text{nat})\)

\(\langle\text{proof}\rangle\)

\textbf{lemma fg-start-round-later:}

\textbf{assumes} \(\rho:\text{fg-run} \ A \ \rho \ HOs \ \SHOs \ \text{coords}\) and \(r: \text{round} (\rho n) \ p = r\) and \(r' : r < r'\)

\textbf{shows} \(n < \text{fg-start-round} \ rho \ p \ r' \ \text{(is} \ < \ ?\text{start})\)

\(\langle\text{proof}\rangle\)

\textbf{lemma fg-start-round-0:}

\textbf{assumes} \(\rho:\text{fg-run} \ A \ \rho \ HOs \ \SHOs \ \text{coords}\)

\textbf{shows} \(\text{fg-start-round} \ rho \ p \ 0 = 0\)

\(\langle\text{proof}\rangle\)

\textbf{lemma fg-start-round-strict-mono:}

\textbf{assumes} \(\rho:\text{fg-run} \ A \ \rho \ HOs \ \SHOs \ \text{coords}\)

\textbf{shows} \(\text{strict-mono} (\text{fg-start-round} \ rho \ p)\)

\(\langle\text{proof}\rangle\)

Process \(p\) is at round \(r\) at all configurations between the start of round \(r\) and the start of round \(r+1\). By lemma \textit{fg-same-round-same-state}, this implies that the local state of process \(p\) is the same at all these configurations.

\textbf{lemma fg-round-between-start-rounds:}

\textbf{assumes} \(\rho:\text{fg-run} \ A \ \rho \ HOs \ \SHOs \ \text{coords}\) and \(1: \text{fg-start-round} \ rho \ p \ r \leq n\)
and 2: \( n < \text{fg-start-round}\ \rho\ p \ (\text{Suc } r) \)
shows \( \text{round} \ \rho\ n \ p = r \) (is \( ?\text{rd} = r \))

(\text{proof})

For any process \( p \) and round \( r \) there is some instant \( n \) where \( p \) executes a local transition from round \( r \). In fact, \( n+1 \) marks the start of round \( r+1 \).

**Lemma fg-local-transition-from-round:**
assumes rho: fg-run A rho HOs SHOs coords
obtains \( n \) where \( \text{round} \ \rho\ n \ p = r \)
and \( \text{fg-start-round}\ \rho\ p \ (\text{Suc } r) = \text{Suc } n \)
and \( \text{fg-local}\ A \ p \ (\text{HOs} \ r \ p) \ (\text{COORDS} \ (\text{Suc } r) \ p) \ (\rho\ n) \ (\rho\ (\text{Suc } n)) \)

(\text{proof})

We now prove two invariants asserted in [4]. The first one states that any message \( m \) in transit from process \( p \) to process \( q \) for round \( r \) corresponds to the message computed by \( p \) for \( q \), given \( p \)'s state at its \( r \)th local transition.

**Lemma fg-invariant1:**
assumes rho: fg-run A rho HOs SHOs coords
and \( m: (p,r,q,m) \in \text{network} \ (\rho\ n) \ (\text{is } ?\text{msg} \ n) \)
shows \( m = \text{sendMsg} \ A \ r \ p \ q \ (\text{state} \ (\rho\ (\text{fg-start-round} \ \rho\ p \ r)) \ p) \)

(\text{proof})

The second invariant states that if process \( q \) received message \( m \) from process \( p \), then (a) \( p \) is in \( q \)'s HO set for that round \( m \), and (b) if \( p \) is moreover in \( q \)'s SHO set, then \( m \) is the message that \( p \) computed at the start of that round.

**Lemma fg-invariant2a:**
assumes rho: fg-run A rho HOs SHOs coords
and \( m: \text{rcvd} \ (\rho\ n) \ q \ p = \text{Some} \ m \) (is \( ?\text{rcvd} \ n) \)
shows \( p \in \text{HOs} \ (\text{round} \ (\rho\ n) \ q) \ q \)
(is \( p \in \text{HOs} \ (\text{?rd } n) \ q \) is \( ?\text{P} \ n) \)

(\text{proof})

**Lemma fg-invariant2b:**
assumes rho: fg-run A rho HOs SHOs coords
and \( m: \text{rcvd} \ (\rho\ n) \ q \ p = \text{Some} \ m \) (is \( ?\text{rcvd} \ n) \)
and sho: \( p \in \text{SHOs} \ (\text{round} \ (\rho\ n) \ q) \ q \) (is \( p \in \text{SHOs} \ (\text{?rd } n) \ q) \)
sows \( m = \text{sendMsg} \ A \ (\text{?rd } n) \ p \ q \)
(is \( ?\text{P} \ n) \)

(\text{proof})

### 3.3 From Fine-Grained to Coarse-Grained Runs

The reduction theorem asserts that for any fine-grained run \( \rho \) there is a coarse-grained run such that every process sees the same sequence of local states in the two runs, modulo stuttering. In other words, no process can locally distinguish the two runs.

18
Given fine-grained run \( \rho \), the corresponding coarse-grained run \( \sigma \) is defined as the sequence of state vectors at the beginning of every round. Notice in particular that the local states \( \sigma r p \) and \( \sigma r q \) of two different processes \( p \) and \( q \) appear at different instants in the original run \( \rho \). Nevertheless, we prove that \( \sigma \) is a coarse-grained run of the algorithm for the same HO, SHO, and coordinator assignments. By definition (and the fact that local states remain equal between \( fg\text{-}start\text{-}round \) instants), the sequences of process states in \( \rho \) and \( \sigma \) are easily seen to be stuttering equivalent, and this will be formally stated below.

**Definition** coarse-run where
\[
\text{coarse-run } \rho \rightarrow p \equiv \text{state } (\rho \ (fg\text{-}start\text{-}round \rho \ p \ r)) p
\]

**Theorem** reduction:

- **Assumes** \( \rho : fg\text{-}run A \rho HOs SHOs coords \)
- **Shows** CSHORun A (coarse-run \( \rho \)) HOs SHOs coords
  
  (is CSHORun - \( ?cr \) - -)

(\text{proof})

### 3.4 Locally Similar Runs and Local Properties

We say that two sequences of configurations (vectors of process states) are **locally similar** if for every process the sequences of its process states are stuttering equivalent. Observe that different stuttering reduction may be applied for every process, hence the original sequences of configurations need not be stuttering equivalent and can indeed differ wildly in the combinations of local states that occur. A property of a sequence of configurations is called **local** if it is insensitive to local similarity.

**Definition** locally-similar where
\[
\text{locally-similar } (\sigma :: \text{nat} \Rightarrow \text{proc} \Rightarrow \text{pst}) \rightarrow (\forall p :: \text{proc}. (\lambda n. \sigma n p) \approx (\lambda n. \tau n p))
\]

**Definition** local-property where
\[
\text{local-property } P \equiv (\forall \sigma \tau. \text{locally-similar } \sigma \tau \rightarrow P \sigma \rightarrow P \tau)
\]

Local similarity is an equivalence relation.

**Lemma** locally-similar-refl: locally-similar \( \sigma \ \sigma \)
(\text{proof})

**Lemma** locally-similar-sym: locally-similar \( \sigma \ \tau \Rightarrow \text{locally-similar } \tau \ \sigma \)
(\text{proof})

**Lemma** locally-similar-trans [trans]:
\[
\text{locally-similar } \varrho \ \sigma \Rightarrow \text{locally-similar } \sigma \ \tau \Rightarrow \text{locally-similar } \varrho \ \tau
\]
(\text{proof})
lemma local-property-eq:
  local-property P = (∀ σ τ. locally-similar σ τ → P σ = P τ)
⟨proof⟩

Consider any fine-grained run rho. The projection of rho to vectors of process states is locally similar to the coarse-grained run computed from rho.

lemma coarse-run-locally-similar:
  assumes rho: fg-run A rho HOs SHOs coords
  shows locally-similar (state ◦ rho) (coarse-run rho)
⟨proof⟩

Therefore, in order to verify a local property P for a fine-grained run over given HO, SHO, and coord collections, it is enough to show that P holds for all coarse-grained runs for these same collections. Indeed, one may restrict attention to coarse-grained runs whose initial states agree with that of the given fine-grained run.

theorem local-property-reduction:
  assumes rho: fg-run A rho HOs SHOs coords
  and P: local-property P
  and coarse-correct:
    \[ ∀ crho. [ CSHORun A crho HOs SHOs coords; crho 0 = state (rho 0)] \implies P crho \]
  shows P (state ◦ rho)
⟨proof⟩

3.5 Consensus as a Local Property

Consensus and Weak Consensus are local properties and can therefore be verified just over coarse-grained runs, according to theorem local-property-reduction.

lemma integrity-is-local:
  assumes sim: locally-similar σ τ
  and val: \[ ∀ n. dec (σ n p) = Some v \implies v \in range vals \]
  and dec: dec (τ n p) = Some v
  shows v \in range vals
⟨proof⟩

lemma validity-is-local:
  assumes sim: locally-similar σ τ
  and val: \[ ∀ n. dec (σ n p) = Some w \implies w = v \]
  and dec: dec (τ n p) = Some w
  shows w = v
⟨proof⟩

lemma agreement-is-local:
  assumes sim: locally-similar σ τ
and \( \forall m \, n. \, [\text{dec} \, (\sigma \, m \, p) = \text{Some} \, v; \, \text{dec} \, (\sigma \, n \, q) = \text{Some} \, w] \implies v = w \)

and \( \forall v. \, \text{dec} \, (\tau \, m \, p) = \text{Some} \, v \) and \( \forall w. \, \text{dec} \, (\tau \, n \, q) = \text{Some} \, w \)

shows \( v = w \)

\( \langle \text{proof} \rangle \)

\textbf{lemma} \( \text{termination-is-local} \):
\begin{align*}
\text{assumes} & \quad \text{sim}: \, \text{locally-similar} \, \sigma \, \tau \\
\text{and} & \quad \text{trm}: \, \text{dec} \, (\sigma \, m \, p) = \text{Some} \, v \\
\text{shows} & \quad \exists n. \, \text{dec} \, (\tau \, n \, p) = \text{Some} \, v
\end{align*}

\( \langle \text{proof} \rangle \)

\textbf{theorem} \( \text{consensus-is-local} \): \( \text{local-property} \) (\( \text{consensus} \, \text{vals} \, \text{dec} \))

\( \langle \text{proof} \rangle \)

\textbf{theorem} \( \text{weak-consensus-is-local} \): \( \text{local-property} \) (\( \text{weak-consensus} \, \text{vals} \, \text{dec} \))

\( \langle \text{proof} \rangle \)

\textbf{end}

\textbf{theory} \( \text{Majorities} \)

\textbf{imports} \( \text{Main} \)

\textbf{begin}

\section{Utility Lemmas About Majorities}

Consensus algorithms usually ensure that a majority of processes proposes the same value before taking a decision, and we provide a few utility lemmas for reasoning about majorities.

Any two subsets \( S \) and \( T \) of a finite set \( E \) such that the sum of their cardinalities is larger than the size of \( E \) have a non-empty intersection.

\textbf{lemma} \( \text{abs-majorities-intersect} \):
\begin{align*}
\text{assumes} & \quad \text{crd}: \, \text{card} \, E < \text{card} \, S + \text{card} \, T \\
\text{and} & \quad s: \, S \subseteq E \quad \text{and} \quad t: \, T \subseteq E \quad \text{and} \quad e: \, \text{finite} \, E \\
\text{shows} & \quad S \cap T \neq \{\}
\end{align*}

\( \langle \text{proof} \rangle \)

\textbf{lemma} \( \text{abs-majoritiesE} \):
\begin{align*}
\text{assumes} & \quad \text{crd}: \, \text{card} \, E < \text{card} \, S + \text{card} \, T \\
\text{and} & \quad s: \, S \subseteq E \quad \text{and} \quad t: \, T \subseteq E \quad \text{and} \quad e: \, \text{finite} \, E \\
\text{obtains} & \quad p \, \text{where} \quad p \in S \quad \text{and} \quad p \in T
\end{align*}

\( \langle \text{proof} \rangle \)

Special case: both sets \( S \) and \( T \) are majorities.

\textbf{lemma} \( \text{abs-majoritiesE'} \):
\begin{align*}
\text{assumes} & \quad \text{Smaj}: \, \text{card} \, S > (\text{card} \, E) \, \text{div} \, 2 \quad \text{and} \quad \text{Tmaj}: \, \text{card} \, T > (\text{card} \, E) \, \text{div} \, 2 \\
\text{and} & \quad s: \, S \subseteq E \quad \text{and} \quad t: \, T \subseteq E \quad \text{and} \quad e: \, \text{finite} \, E \\
\text{obtains} & \quad p \, \text{where} \quad p \in S \quad \text{and} \quad p \in T
\end{align*}

\( \langle \text{proof} \rangle \)
We restate the above theorems for the case where the base type is finite (taking $E$ as the universal set).

**lemma** majorities-intersect:
- **assumes** crd: card (UNIV::('a::finite) set) < card (S::'a set) + card T
- **shows** $S \cap T \neq \{\}$

**lemma** majoritiesE:
- **assumes** crd: card (UNIV::('a::finite) set) < card (S::'a set) + card (T::'a set)
- **obtains** $p$ **where** $p \in S$ and $p \in T$

**lemma** majoritiesE':
- **assumes** $S$: card (S::('a::finite) set) > (card (UNIV::'a set)) div 2
- **and** $T$: card (T::'a set) > (card (UNIV::'a set)) div 2
- **obtains** $p$ **where** $p \in S$ and $p \in T$

5 **Verification of the One-Third Rule Consensus Algorithm**

We now apply the framework introduced so far to the verification of concrete algorithms, starting with algorithm **One-Third Rule**, which is one of the simplest algorithms presented in [7]. Nevertheless, the algorithm has some interesting characteristics: it ensures safety (i.e., the Integrity and Agreement) properties in the presence of arbitrary benign faults, and if everything works perfectly, it terminates in just two rounds. **One-Third Rule** is an uncoordinated algorithm tolerating benign faults, hence SHO or coordinator sets do not play a role in its definition.

5.1 **Model of the Algorithm**

We begin by introducing an anonymous type of processes of finite cardinality that will instantiate the type variable 'proc of the generic HO model.

**typedef** Proc — the set of processes

**axiomatization** where Proc-finite: OFCLASS(Proc, finite-class)

**instance** Proc :: finite (proof)
The state of each process consists of two fields: \( x \) holds the current value proposed by the process and \( \text{decide} \) the value (if any, hence the option type) it has decided.

```plaintext
record 'val pstate =
  x :: 'val
  decide :: 'val option
```

The initial value of field \( x \) is unconstrained, but no decision has been taken initially.

```plaintext
definition OTR-initState where
  OTR-initState p st \equiv \text{decide} st = \text{None}
```

Given a vector \( \text{msgs} \) of values (possibly null) received from each process, \( \text{HOV} \text{msgs} v \) denotes the set of processes from which value \( v \) was received.

```plaintext
definition \text{HOV} :: (\text{Proc} \Rightarrow 'val option) \Rightarrow 'val \Rightarrow \text{Proc set} where
  \text{HOV} \text{msgs} v \equiv \{ q . \text{msgs} q = \text{Some} v \}
```

\( \text{MFR} \text{msgs} v \) ("most frequently received") holds for vector \( \text{msgs} \) if no value has been received more frequently than \( v \).

Some such value always exists, since there is only a finite set of processes and thus a finite set of possible cardinalities of the sets \( \text{HOV} \text{msgs} v \).

```plaintext
definition \text{MFR} :: (\text{Proc} \Rightarrow 'val option) \Rightarrow 'val \Rightarrow \text{bool} where
  \text{MFR} \text{msgs} v \equiv \forall w. \text{card} (\text{HOV} \text{msgs} w) \leq \text{card} (\text{HOV} \text{msgs} v)
```

```plaintext
lemma \text{MFR}-exists: \exists v. \text{MFR} \text{msgs} v
⟨proof⟩
```

Also, if a process has heard from at least one other process, the most frequently received values are among the received messages.

```plaintext
lemma \text{MFR-in-msgs:}
  assumes \text{HO}:\text{HOs} m p \neq \{\}
  and v: \text{MFR} (\text{HOrcvdMsgs} \text{OTR-M} m p (\text{HOs} m p) (\rho m)) v
  (is MFR ?\text{msgs} v)
  shows \exists q \in \text{HOs} m p. v = \text{the (?msgs} q)
⟨proof⟩
```

\( \text{TwoThirds} \text{msgs} v \) holds if value \( v \) has been received from more than 2/3 of all processes.

```plaintext
definition \text{TwoThirds} where
  \text{TwoThirds} \text{msgs} v \equiv (2 \times N) \div 3 < \text{card} (\text{HOV} \text{msgs} v)
```

The next-state relation of algorithm \textbf{One-Third Rule} for every process is defined as follows: if the process has received values from more than 2/3 of
all processes, the $x$ field is set to the smallest among the most frequently received values, and the process decides value $v$ if it received $v$ from more than $2/3$ of all processes. If $p$ hasn’t heard from more than $2/3$ of all processes, the state remains unchanged. (Note that Some is the constructor of the option datatype, whereas $\epsilon$ is Hilbert’s choice operator.) We require the type of values to be linearly ordered so that the minimum is guaranteed to be well-defined.

**Definition**

$\text{OTR-nextState}$

$\text{OTR-nextState} \ r \ p \ (\text{st}::(\text{val}::\text{linorder}) \ pstate) \ \text{msgs} \ \text{st}' \ \equiv$

if $(2*N) \ \text{div} \ 3 < \text{card} \ \{q. \text{msgs} \ q \neq \text{None}\}$
then $\text{st}' = \emptyset \ x = \text{Min} \ \{v. \text{MFR} \ \text{msgs} \ v\}$,

$\text{decide} = (\text{if} \ (\exists \ v. \text{TwoThirds} \ \text{msgs} \ v) $
then Some $(\epsilon \ v. \text{TwoThirds} \ \text{msgs} \ v)$
else decide $\text{st}) \ \}$$
else $\text{st}' = \text{st}$

The message sending function is very simple: at every round, every process sends its current proposal (field $x$ of its local state) to all processes.

**Definition**

$\text{OTR-sendMsg}$

$\text{OTR-sendMsg} \ r \ p \ q \ \text{st} \ \equiv \ x \ \text{st}$

### 5.2 Communication Predicate for One-Third Rule

We now define the communication predicate for the One-Third Rule algorithm to be correct. It requires that, infinitely often, there is a round where all processes receive messages from the same set $\Pi$ of processes where $\Pi$ contains more than two thirds of all processes. The “per-round” part of the communication predicate is trivial.

**Definition**

$\text{OTR-commPerRd}$

$\text{OTR-commPerRd} \ HOs \ \equiv \ \text{True}$

**Definition**

$\text{OTR-commGlobal}$

$\text{OTR-commGlobal} \ \equiv$

$\forall r. \exists r0. \Pi. r0 \geq r \land (\forall p. \text{HOs} \ r0 \ p = \Pi) \land \text{card} \ \Pi > (2*N) \ \text{div} \ 3$

### 5.3 The One-Third Rule Heard-Of Machine

We now define the HO machine for the One-Third Rule algorithm by assembling the algorithm definition and its communication-predicate. Because this is an uncoordinated algorithm, the $\text{crd}$ arguments of the initial- and next-state predicates are unused.

**Definition**

$\text{OTR-HOMachine}$

$\text{OTR-HOMachine} =$

$\emptyset \ \text{CinitState} \ = \ (\lambda \ p \ \text{st} \ \text{crd}. \ \text{OTR-initState} \ p \ \text{st}),$

$\text{sendMsg} \ = \ \text{OTR-sendMsg},$

$\text{CnextState} \ = \ (\lambda \ r \ p \ \text{msgs} \ \text{crd} \ \text{st}'. \ \text{OTR-nextState} \ r \ p \ \text{msgs} \ \text{st}')$, 24
\[ \text{HOcommPerRd} = OTR\text{-commPerRd}, \]
\[ \text{HOcommGlobal} = OTR\text{-commGlobal} \]

**abbreviation** \( OTR \equiv OTR\text{-HOMachine} \vdash (\text{Proc}, 'val::linorder\text{ pstate, 'val}) \text{HOMachine} \)

end

theory OneThirdRuleProof

imports OneThirdRuleDefs ../Reduction ../Majorities

begin

We prove that One-Third Rule solves the Consensus problem under the communication predicate defined above. The proof is split into proofs of the Integrity, Agreement, and Termination properties.

5.4 Proof of Integrity

Showing integrity of the algorithm is a simple, if slightly tedious exercise in invariant reasoning. The following inductive invariant asserts that the values of the \( x \) and \( \text{decide} \) fields of the process states are limited to the \( x \) values present in the initial states since the algorithm does not introduce any new values.

**definition** \( VInv \) where

\[ VInv \rho n \equiv \]
\[ \text{let xinit } = (\text{range } (x \circ (\rho 0))) \]
\[ \text{in range } (x \circ (\rho n)) \subseteq xinit \]
\[ \land \text{range } (\text{decide } \circ (\rho n)) \subseteq \{\text{None}\} \cup (\text{Some ' xinit}) \]

**lemma** \( \text{vinv-invariant:} \)
\[ \text{assumes run: } \text{HORun } OTR\text{-M } \rho \text{ HOs} \]
\[ \text{shows } VInv \rho n \]

(proof)

Integrity is an immediate consequence.

**theorem** \( OTR\text{-integrity:} \)
\[ \text{assumes run: } \text{HORun } OTR\text{-M } \rho \text{ HOs and } \text{dec: } \text{decide } (\rho n p) = \text{Some } v \]
\[ \text{shows } \exists q. \ v = x (\rho 0 q) \]

(proof)

5.5 Proof of Agreement

The following lemma \( A1 \) asserts that if process \( p \) decides in a round on a value \( v \) then more than 2/3 of all processes have \( v \) as their \( x \) value in their local state.

We show a few simple lemmas in preparation.

**lemma** \( \text{nextState-change:} \)
\[ \text{assumes } \text{HORun } OTR\text{-M } \rho \text{ HOs} \]
and \( \neg ((2+N) \mod 3 < \text{card } \{ q. (\text{HOrcvdMsgs OTR-M n p (HOs n p) (rho n)) q \neq \text{None}\}) \}

shows rho (Suc n) p = rho n p

\langle proof \rangle

lemma nextState-decide:
\begin{itemize}
  \item assumes run: HORun OTR-M rho HOs
  \item and chg: decide (rho (Suc n) p) \neq decide (rho n p)
  \item shows TwoThirds (HOrcvdMsgs OTR-M n p (HOs n p) (rho n))
  \quad (\text{the (decide (rho (Suc n) p)))}
\end{itemize}

\langle proof \rangle

The following lemma A2 contains the crucial correctness argument: if more than 2/3 of all processes send \( v \) and process \( p \) hears from more than 2/3 of all processes then the \( x \) field of \( p \) will be updated to \( v \).

\begin{itemize}
  \item assumes run: HORun OTR-M rho HOs
  \item and HO: \( (2*N) \mod 3 < \text{card } \{ q. \text{HOrcvdMsgs OTR-M n p (HOs n p) (rho n)} q \neq \text{None} \} \}
  \item and maj: \( (2*N) \mod 3 < \text{card } \{ q. x (\text{rho n} q) = v \} \}
  \item shows \( x (\text{rho (Suc n) p}) = v \)
\end{itemize}

\langle proof \rangle

Therefore, once more than two thirds of the processes hold \( v \) in their \( x \) field, this will remain true forever.

\begin{itemize}
  \item assumes run: HORun OTR-M rho HOs
  \item and n: \( (2*N) \mod 3 < \text{card } \{ q. x (\text{rho n} q) = v \} \) (is ?twothird n)
  \item shows ?twothird (n+k)
\end{itemize}

\langle proof \rangle

It now follows that once a process has decided on some value \( v \), more than two thirds of all processes continue to hold \( v \) in their \( x \) field.

\begin{itemize}
  \item assumes run: HORun OTR-M rho HOs
  \item and dec: decide (rho n p) = Some v (is ?dec n)
  \item shows \( \forall k. (2*N) \mod 3 < \text{card } \{ q. x (\text{rho (n+k)} q) = v \}
  \quad (\text{is} \forall k. ?twothird (n+k))\}
\end{itemize}

\langle proof \rangle

The Agreement property follows easily from lemma A4: if processes \( p \) and \( q \) decide values \( v \) and \( w \), respectively, then more than two thirds of the
processes must propose \( v \) and more than two thirds must propose \( w \). Because these two majorities must have an intersection, we must have \( v = w \).

We first prove an “asymmetric” version of the agreement property before deriving the general agreement theorem.

**Lemma A5:**
- assumes \( \text{HORun OTR-M rho HOs} \)
- and \( p : \text{decide (rho n p)} = \text{Some v} \)
- and \( p' : \text{decide (rho (n+k) p')} = \text{Some w} \)
- shows \( v = w \)

\langle proof \rangle

**Theorem OTR-agreement:**
- assumes \( \text{HORun OTR-M rho HOs} \)
- and \( p : \text{decide (rho n p)} = \text{Some v} \)
- and \( p' : \text{decide (rho m p')} = \text{Some w} \)
- shows \( v = w \)

\langle proof \rangle

### 5.6 Proof of Termination

We now show that every process must eventually decide. The idea of the proof is to observe that the communication predicate guarantees the existence of two uniform rounds where every process hears from the same two-thirds majority of processes. The first such round serves to ensure that all \( x \) fields hold the same value, the second round copies that value into all decision fields.

Lemma A2 is instrumental in this proof.

**Theorem OTR-termination:**
- assumes \( \text{HORun OTR-M rho HOs} \)
  - and \( \text{commG: HOcommGlobal OTR-M HOs} \)
- shows \( \exists r v. \text{decide (rho r p)} = \text{Some v} \)

\langle proof \rangle

### 5.7 One-Third Rule Solves Consensus

Summing up, all (coarse-grained) runs of One-Third Rule for HO collections that satisfy the communication predicate satisfy the Consensus property.

**Theorem OTR-consensus:**
- assumes \( \text{run: HORun OTR-M rho HOs} \) and \( \text{commG: HOcommGlobal OTR-M HOs} \)
- shows consensus \((x \circ (\text{rho 0})) \text{ decide rho}\)

\langle proof \rangle

By the reduction theorem, the correctness of the algorithm also follows for fine-grained runs of the algorithm. It would be much more tedious to establish this theorem directly.
theorem OTR-consensus-fg:
  assumes run: fg-run OTR-M rho HOs HOs (λr q. undefined)
  and commG: HOcommGlobal OTR-M HOs
  shows consensus (λp. x (state (rho 0) p)) decide (state o rho)
    (is consensus ?inits - -)
  ⟨proof⟩
end

theory UvDefs
imports ..../HOModel
begin

6 Verification of the UniformVoting Consensus Algorithm

Algorithm UniformVoting is presented in [7]. It can be considered as a
deterministic version of Ben-Or’s well-known probabilistic Consensus algo-
rithm [2]. We formalize in Isabelle the correctness proof given in [7], using
the framework of theory HOModel.

6.1 Model of the Algorithm

We begin by introducing an anonymous type of processes of finite cardinality
that will instantiate the type variable ‘proc of the generic HO model.
typedecl Proc — the set of processes
axiomatization where Proc-finite: OFCLASS(Proc, finite-class)
instance Proc :: finite ⟨proof⟩

abbreviation
  N ≡ card (UNIV::Proc set) — number of processes

The algorithm proceeds in phases of 2 rounds each (we call steps the in-
dividual rounds that constitute a phase). The following utility functions
compute the phase and step of a round, given the round number.
abbreviation nSteps ≡ 2

definition phase where phase (r::nat) ≡ r div nSteps
definition step where step (r::nat) ≡ r mod nSteps

The following record models the local state of a process.
record 'val pstate =
  x :: 'val — current value held by process
  vote :: 'val option — value the process voted for, if any
  decide :: 'val option — value the process has decided on, if any
Possible messages sent during the execution of the algorithm, and characteristic predicates to distinguish types of messages.

```plaintext
datatype 'val msg = Val 'val | ValVote 'val 'val option | Null — dummy message in case nothing needs to be sent

definition isValVote where isValVote m ≡ ∃ z v. m = ValVote z v

definition isVal where isVal m ≡ ∃ v. m = Val v
```

Selector functions to retrieve components of messages. These functions have a meaningful result only when the message is of appropriate kind.

```plaintext
fun getvote where getvote (ValVote z v) = v

fun getval where getval (ValVote z v) = z
| getval (Val z) = z
```

The \( x \) field of the initial state is unconstrained, all other fields are initialized appropriately.

```plaintext
definition UV-initState where UV-initState p st ≡ (vote st = None) ∧ (decide st = None)
```

We separately define the transition predicates and the send functions for each step and later combine them to define the overall next-state relation.

```plaintext
definition msgRcvd where — processes from which some message was received
msgRcvd (msgs::Proc ↭ 'val msg) = { q . msgs q ≠ None}

definition smallestValRcvd where
smallestValRcvd (msgs::Proc ↭ ('val::linorder) msg) ≡ Min { v. ∃ q. msgs q = Some (Val v)}
```

In step 0, each process sends its current \( x \) value. It updates its \( x \) field to the smallest value it has received. If the process has received the same value \( v \) from all processes from which it has heard, it updates its \( vote \) field to \( v \).

```plaintext
definition send0 where
send0 r p q st ≡ Val (x st)

definition next0 where
next0 r p st (msgs::Proc ↭ ('val::linorder) msg) st' ≡
(∃ v. (∀ q ∈ msgRcvd msgs. msgs q = Some (Val v)) ∧ st' = st [] vote := Some v, x := smallestValRcvd msgs ) ∨ ¬(∃ v. ∀ q ∈ msgRcvd msgs. msgs q = Some (Val v)) ∧ st' = st [] x := smallestValRcvd msgs )
```

29
In step 1, each process sends its current $x$ and $vote$ values.

**definition** send1 where

$send1 \ r \ p \ q \ st \equiv ValVote \ (x \ st) \ (vote \ st)$

**definition** valVoteRcvd where

— processes from which values and votes were received

$valVoteRcvd \ (msgs :: \ Proc -> 'val \ msg) \equiv \{ \ q . \ \exists \ v . \ msgs \ q = Some \ (ValVote \ v \ None) \}$

**definition** smallestValNoVoteRcvd where

$smallestValNoVoteRcvd \ (msgs :: \ Proc -> 'val \ msg) \equiv \{ \ v . \ \exists \ q . \ msgs \ q = Some \ (ValVote \ v \ None) \}$

**definition** someVoteRcvd where

— set of processes from which some vote was received

$someVoteRcvd \ (msgs :: \ Proc -> 'val \ msg) \equiv \{ \ q . \ q \in \ msgRcvd \ msgs \land isValVote \ (the \ (msgs \ q)) \land getvote \ (the \ (msgs \ q)) \neq None \}$

**definition** identicalVoteRcvd where

$identicalVoteRcvd \ (msgs :: \ Proc -> 'val \ msg) \ v \equiv \forall \ q . \ isValVote \ (the \ (msgs \ q)) \land getvote \ (the \ (msgs \ q)) = Some \ v$

**definition** x-update where

$x-update \ st \ msgs \ st' \equiv \exists \ q . \ \exists \ v \ . \ someVoteRcvd \ msgs . \ x \ st' = the \ (getvote \ (the \ (msgs \ q))) \land \ smallestValNoVoteRcvd \ msgs = \{ \}$ \land \ x \ st' = smallestValNoVoteRcvd \ msgs$

**definition** dec-update where

$dec-update \ st \ msgs \ st' \equiv \exists \ v \ . \ identicalVoteRcvd \ msgs \ v \land decide \ st' = Some \ v \lor \neg \exists \ v . \ identicalVoteRcvd \ msgs \ v \land decide \ st' = decide \ st$

**definition** next1 where

$next1 \ r \ p \ st \ msgs \ st' \equiv x-update \ st \ msgs \ st' \land \ dec-update \ st \ msgs \ st' \land \ vote \ st' = None$

The overall send function and next-state relation are simply obtained as the composition of the individual relations defined above.

**definition** UV-sendMsg where

$UV-sendMsg \ (r :: nat) \equiv if \ step \ r = 0 \ then \ send0 \ r \ else \ send1 \ r$

**definition** UV-nextState where

$UV-nextState \ r \equiv if \ step \ r = 0 \ then \ next0 \ r \ else \ next1 \ r$
6.2 Communication Predicate for *UniformVoting*

We now define the communication predicate for the *UniformVoting* algorithm to be correct.

The round-by-round predicate requires that for any two processes there is always one process heard by both of them. In other words, no “split rounds” occur during the execution of the algorithm [7]. Note that in particular, heard-of sets are never empty.

**definition** `UV-commPerRd` where

\[
UV-commPerRd \ HOrs \equiv \forall p, q. \ \exists p, q. \ HOrs p \cap HOrs q
\]

The global predicate requires the existence of a (space-)uniform round during which the heard-of sets of all processes are equal. (Observe that [7] requires infinitely many uniform rounds, but the correctness proof uses just one such round.)

**definition** `UV-commGlobal` where

\[
UV-commGlobal \ HOs \equiv \exists r. \ \forall p, q. \ HOs r p = HOs r q
\]

6.3 The *UniformVoting* Heard-Of Machine

We now define the HO machine for *Uniform Voting* by assembling the algorithm definition and its communication predicate. Notice that the coordinator arguments for the initialization and transition functions are unused since *UniformVoting* is not a coordinated algorithm.

**definition** `UV-HOMachine` where

\[
UV-HOMachine = (\lambda p st crd. \ UV-initState p st), \ UV-sendMsg, \ UV-nextState r p st msgs st' = UV-nextState r p st msgs st', \ HOcommPerRd = UV-commPerRd, \ HOcommGlobal = UV-commGlobal
\]

**abbreviation**

\[
UV-M \equiv (UV-HOMachine::(Proc, 'val::linorder pstate, 'val msg) HOMachine)
\]

end

theory *UvProof*

imports *UvDefs* ../Reduction

begin

6.4 Preliminary Lemmas

At any round, given two processes \( p \) and \( q \), there is always some process which is heard by both of them, and from which \( p \) and \( q \) have received the same message.
lemma some-common-msg:
  assumes HOcommPerRd UV-M (HOs r)
  shows \( \exists pq. \ pq \in \text{msgRcvd} (\text{HOrcvdMsgs} UV-M r p (\text{HOs} r p) (\text{rho} r)) \land \ pq \in \text{msgRcvd} (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) \land \ (\text{HOrcvdMsgs} UV-M r p (\text{HOs} r p) (\text{rho} r)) \ pq = (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) \ pq \)
⟨proof⟩

When executing step 0, the minimum received value is always well defined.

lemma minval-step0:
  assumes com: HOcommPerRd UV-M (HOs r) and s0: step r = 0
  shows smallestValRcvd (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) \in \{ v. \ \exists p. \ (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) p = \text{Some} (\text{Val} v) \}
  (is smallestValRcvd ?msgs \in ?vals)
⟨proof⟩

When executing step 1 and no vote has been received, the minimum among values received in messages carrying no vote is well defined.

lemma minval-step1:
  assumes com: HOcommPerRd UV-M (HOs r) and s1: step r \neq 0 and now: someVoteRcvd (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) = \{\}
  shows smallestValNoVoteRcvd (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) \in \{ v . \ \exists p. \ (\text{HOrcvdMsgs} UV-M r q (\text{HOs} r q) (\text{rho} r)) p = \text{Some} (\text{ValVote} v \text{ None}) \}
  (is smallestValNoVoteRcvd ?msgs \in ?vals)
⟨proof⟩

The vote field is reset every time a new phase begins.

lemma reset-vote:
  assumes run: HORun UV-M rho HOs and s0: step r = 0
  shows vote (\text{rho} r \ p) = \text{None}
⟨proof⟩

Processes only vote for the value they hold in their x field.

lemma x-vote-eq:
  assumes run: HORun UV-M rho HOs and com: \( \forall r. \ \text{HOcommPerRd} UV-M (\text{HOs} r) \) and vote: vote (\text{rho} r p) = \text{Some} v
  shows v = x (\text{rho} r p)
⟨proof⟩

6.5 Proof of Irrevocability, Agreement and Integrity

A decision can only be taken in the second round of a phase.

lemma decide-step:
  assumes run: HORun UV-M rho HOs and decide: decide (\text{rho} (\text{Suc} r) p) \neq decide (\text{rho} r p)
  shows step r = 1
No process ever decides \textit{None}.

\textbf{lemma} decide-nonnull:
\begin{itemize}
\item \textbf{assumes} \text{run: HORun UV-M rho HOs}
\item \text{and} \text{decide: decide (rho (Suc r) p) \neq decide (rho r p)}
\item \text{shows} \text{decide (rho (Suc r) p) \neq None}
\end{itemize}

\texttt{(proof)}

If some process \(p\) votes for \(v\) at some round \(r\), then any message that \(p\) received in \(r\) was holding \(v\) as a value.

\textbf{lemma} msgs-unanimity:
\begin{itemize}
\item \textbf{assumes} \text{run: HORun UV-M rho HOs}
\item \text{and} \text{vote: vote (rho (Suc r) p) = Some v}
\item \text{and} \text{q: q \in msgRcvd (HOrcvdMsgs UV-M r p (HOs r p) (rho r))}
\item \text{is - \in msgRcvd ?msgs}
\item \text{shows} \text{getval (the (?msgs q)) = v}
\end{itemize}

\texttt{(proof)}

Any two processes can only vote for the same value.

\textbf{lemma} vote-agreement:
\begin{itemize}
\item \textbf{assumes} \text{run: HORun UV-M rho HOs}
\item \text{and} \text{com: \forall r. HOcommPerRd UV-M (HOs r)}
\item \text{and} \text{p: vote (rho r p) = Some v}
\item \text{and} \text{q: vote (rho r q) = Some w}
\item \text{shows} \text{v = w}
\end{itemize}

\texttt{(proof)}

If a process decides value \(v\) then all processes must have \(v\) in their \(x\) fields.

\textbf{lemma} decide-equals-x:
\begin{itemize}
\item \textbf{assumes} \text{run: HORun UV-M rho HOs}
\item \text{and} \text{com: \forall r. HOcommPerRd UV-M (HOs r)}
\item \text{and} \text{decide: decide (rho (Suc r) p) \neq decide (rho r p)}
\item \text{and} \text{decval: decide (rho (Suc r) p) = Some v}
\item \text{shows} \text{x (rho (Suc r) q) = v}
\end{itemize}

\texttt{(proof)}

If at some point all processes hold value \(v\) in their \(x\) fields, then this will still be the case at the next step.

\textbf{lemma} same-x-stable:
\begin{itemize}
\item \textbf{assumes} \text{run: HORun UV-M rho HOs}
\item \text{and} \text{comm: \forall r. HOcommPerRd UV-M (HOs r)}
\item \text{x: p. x (rho r p) = v}
\item \text{shows} \text{x (rho (Suc r) q) = v}
\end{itemize}

\texttt{(proof)}

Combining the last two lemmas, it follows that as soon as some process decides value \(v\), all processes hold \(v\) in their \(x\) fields.
lemma safety-argument:
  assumes run: HORun UV-M rho HOs
  and com: ∀ r. HOcommPerRd UV-M (HOs r)
  and decide: decide (rho (Suc r) p) ≠ decide (rho r p)
  and decval: decide (rho (Suc r) p) = Some v
  shows x (rho (Suc r+k) q) = v
⟨proof⟩

Any process that holds a non-null decision value has made a decision sometime in the past.

lemma decided-then-past-decision:
  assumes run: HORun UV-M rho HOs
  and dec: decide (rho n p) = Some v
  shows ∃ m<n. decide (rho (Suc m) p) ≠ decide (rho m p)
  ∧ decide (rho (Suc m) p) = Some v
⟨proof⟩

We can now prove the safety properties of the algorithm, and start with proving Integrity.

lemma x-values-initial:
  assumes run: HORun UV-M rho HOs
  and com: ∀ r. HOcommPerRd UV-M (HOs r)
  shows ∃ q. x (rho r p) = x (rho 0 q)
⟨proof⟩

theorem uv-integrity:
  assumes run: HORun UV-M rho HOs
  and com: ∀ r. HOcommPerRd UV-M (HOs r)
  and dec: decide (rho m p) = Some v
  shows ∃ q. v = x (rho 0 q)
⟨proof⟩

We now turn to Agreement.

lemma two-decisions-agree:
  assumes run: HORun UV-M rho HOs
  and com: ∀ r. HOcommPerRd UV-M (HOs r)
  and decidep: decide (rho (Suc r) p) ≠ decide (rho r p)
  and decvalp: decide (rho (Suc r) p) = Some v
  and decideq: decide (rho (Suc (r+k)) q) ≠ decide (rho (r+k) q)
  and decvalq: decide (rho (Suc (r+k)) q) = Some w
  shows v = w
⟨proof⟩

theorem uv-agreement:
  assumes run: HORun UV-M rho HOs
  and com: ∀ r. HOcommPerRd UV-M (HOs r)
  and p: decide (rho m p) = Some v
  and q: decide (rho n q) = Some w
shows \( v = w \)

(proof)

Irrevocability is a consequence of Agreement and the fact that no process can decide None.

**Theorem uv-irrevocability:**
- **Assumes** \( \text{run}: \text{HORun} \ UV-M \ rho \ HOs \)
- and \( \text{com}: \forall r. \text{HOcommPerRd} \ UV-M \ (HOs \ r) \)
- and \( p: \text{decide} \ (\rho \ m \ p) = \text{Some} \ v \)
- **Shows** \( \text{decide} \ (\rho \ (m+n) \ p) = \text{Some} \ v \)

(proof)

### 6.6 Proof of Termination

Two processes having the same Heard-Of set at some round will hold the same value in their \( x \) variable at the next round.

**Lemma hoeq-xeq:**
- **Assumes** \( \text{run}: \text{HORun} \ UV-M \ rho \ HOs \)
- and \( \text{com}: \forall r. \text{HOcommPerRd} \ UV-M \ (HOs \ r) \)
- and \( \text{hoeq}: \text{HOs} \ r \ p = \text{HOs} \ r \ q \)
- **Shows** \( x \ (\rho \ (\text{Suc} \ r) \ p) = x \ (\rho \ (\text{Suc} \ r) \ q) \)

(proof)

We now prove that UniformVoting terminates.

**Theorem uv-termination:**
- **Assumes** \( \text{run}: \text{HORun} \ UV-M \ rho \ HOs \)
- and \( \text{comR}: \forall r. \text{HOcommPerRd} \ UV-M \ (HOs \ r) \)
- and \( \text{comG}: \text{HOcommGlobal} \ UV-M \ HOs \)
- **Shows** \( \exists r v. \text{decide} \ (\rho \ r \ p) = \text{Some} \ v \)

(proof)

### 6.7 UniformVoting Solves Consensus

Summing up, all (coarse-grained) runs of UniformVoting for HO collections that satisfy the communication predicate satisfy the Consensus property.

**Theorem uv-consensus:**
- **Assumes** \( \text{run}: \text{HORun} \ UV-M \ rho \ HOs \)
- and \( \text{comR}: \forall r. \text{HOcommPerRd} \ UV-M \ (HOs \ r) \)
- and \( \text{comG}: \text{HOcommGlobal} \ UV-M \ HOs \)
- **Shows** \( \text{consensus} \ (x \circ (\rho \ 0)) \ \text{decide} \ \rho \)

(proof)

By the reduction theorem, the correctness of the algorithm carries over to the fine-grained model of runs.

**Theorem uv-consensus-fg:**
- **Assumes** \( \text{run}: \text{fg-run} \ UV-M \ rho \ HOs \ HOs \)
- and \( \text{comR}: \forall r. \text{HOcommPerRd} \ UV-M \ (HOs \ r) \)

35
and \textit{commG} \textit{HOcommGlobal UV-M HOs}

shows consensus (λp. x (state (rho 0) p)) decide (state o rho)
(is consensus ?inits -)
⟨proof⟩

end
theory LastVotingDefs
imports ../HOModel
begin

7 Verification of the \textit{LastVoting} Consensus Algorithm

The \textit{LastVoting} algorithm can be considered as a representation of Lamport’s Paxos consensus algorithm [11] in the Heard-Of model. It is a coordinated algorithm designed to tolerate benign failures. Following [7], we formalize its proof of correctness in Isabelle, using the framework of theory HOModel.

7.1 Model of the Algorithm

We begin by introducing an anonymous type of processes of finite cardinality that will instantiate the type variable \’\textit{proc} of the generic CHO model.

typedecl Proc — the set of processes
axiomatization where Proc-finite: OFCLASS(Proc, finite-class)
instance Proc :: finite ⟨proof⟩

abbreviation
\( N \equiv \text{card} (\text{UNIV::Proc set}) \) — number of processes

The algorithm proceeds in \textit{phases} of 4 rounds each (we call \textit{steps} the individual rounds that constitute a phase). The following utility functions compute the phase and step of a round, given the round number.

definition phase where phase (r::nat) \equiv r \text{ div } 4

definition step where step (r::nat) \equiv r \text{ mod } 4

lemma phase-zero [simp]: phase 0 = 0
⟨proof⟩

lemma step-zero [simp]: step 0 = 0
⟨proof⟩

lemma phase-step: (phase r \* 4) + step r = r
⟨proof⟩
The following record models the local state of a process.

```plaintext
record 'val pstate =
  x :: 'val — current value held by process
vote :: 'val option — value the process voted for, if any
commit :: bool — did the process commit to the vote?
ready :: bool — for coordinators: did the round finish successfully?
timestamp :: nat — time stamp of current value
decide :: 'val option — value the process has decided on, if any
coordΦ :: Proc — coordinator for current phase
```

Possible messages sent during the execution of the algorithm.

```plaintext
datatype 'val msg =
  ValStamp 'val nat
| Vote 'val
| Ack
| Null — dummy message in case nothing needs to be sent
```

Characteristic predicates on messages.

```plaintext
definition isValStamp where isValStamp m ≡ ∃v ts. m = ValStamp v ts

definition isVote where isVote m ≡ ∃v. m = Vote v

definition isAck where isAck m ≡ m = Ack
```

Selector functions to retrieve components of messages. These functions have a meaningful result only when the message is of an appropriate kind.

```plaintext
fun val where
  val (ValStamp v ts) = v
| val (Vote v) = v

fun stamp where
  stamp (ValStamp v ts) = ts
```

The `x` field of the initial state is unconstrained, all other fields are initialized appropriately.

```plaintext
definition LV-initState where
  LV-initState p st crd ≡
  vote st = None
∧ ¬(commit st)
∧ ¬(ready st)
∧ timestamp st = 0
∧ decide st = None
∧ coordΦ st = crd
```

We separately define the transition predicates and the send functions for each step and later combine them to define the overall next-state relation.

— processes from which values and timestamps were received
definition \textit{valStampsRcvd} \ where
definition \textit{valStampsRcvd} (msgs :: Proc \to 'val \ msg) \equiv
\{ q . \exists v \ ts. \ msgs \ q = \text{Some} \ (\text{ValStamp} \ v \ ts)\}

definition \textit{highestStampRcvd} \ where
definition \textit{highestStampRcvd} \equiv
\text{Max} \ \{ ts . \exists q v. (msgs::Proc \to 'val \ msg) \ q = \text{Some} \ (\text{ValStamp} \ v \ ts)\}

In step 0, each process sends its current \(x\) and \(timestamp\) values to its coordinator.

A process that considers itself to be a coordinator updates its \(vote\) field if it has received messages from a majority of processes. It then sets its \(\text{commT}\) field to true.

definition \textit{send0} \ where
definition \textit{next0} \ where
definition \textit{send1} \ where
definition \textit{next1} \ where

definition \textit{send2} \ where

definition \textit{acksRcvd} \ where

— processes from which an acknowledgement was received
acksRcvd (msgs :: Proc \rightarrow \text{'val msg}) \equiv
\{ q . msgs q \neq \text{None} \land isAck (\text{the} (msgs q)) \}

**Definition next2 where**

\[
\text{next2} \; r \; p \; st \; msgs \; crd \; st' \equiv
\begin{align*}
&\text{if } p = \text{coord}\Phi \; st \land \text{card} (\text{acksRcvd} \; msgs) > N \div 2 \\
&\quad \text{then } st' = st (\{ \text{ready} := \text{True} \}) \\
&\quad \text{else } st' = st
\end{align*}
\]

In step 3, coordinators that are ready send their vote to all processes. Processes that received a vote from their coordinator decide on that value. Coordinators reset their ready and commit fields to false. All processes reset the coordinators as indicated by the parameter of the operator.

**Definition send3 where**

\[
\text{send3} \; r \; p \; q \; st \equiv
\begin{align*}
&\text{if } p = \text{coord}\Phi \; st \land \text{ready } st \text{ then Vote } (\text{the} (\text{vote } st)) \text{ else Null}
\end{align*}
\]

**Definition next3 where**

\[
\text{next3} \; r \; p \; st \; msgs \; crd \; st' \equiv
\begin{align*}
&\text{if } \text{msgs} (\text{coord}\Phi \; st) \neq \text{None} \land \text{isVote} (\text{the} (\text{msgs} (\text{coord}\Phi \; st))) \\
&\quad \text{then } \text{decide } st' = \text{Some} (\text{val} (\text{the} (\text{msgs} (\text{coord}\Phi \; st)))) \\
&\quad \text{else } \text{decide } st' = \text{decide } st \\
&\quad \land (\text{if } p = \text{coord}\Phi \; st \\
&\quad \quad \text{then } \neg (\text{ready } st') \land \neg (\text{commit } st') \\
&\quad \quad \text{else } \text{ready } st' = \text{ready } st \land \text{commit } st' = \text{commit } st) \\
&\quad \land x \; st' = x \; st \\
&\quad \land \text{vote } st' = \text{vote } st \\
&\quad \land \text{timestamp } st' = \text{timestamp } st \\
&\quad \land \text{coord}\Phi \; st' = \text{crd}
\end{align*}
\]

The overall send function and next-state relation are simply obtained as the composition of the individual relations defined above.

**Definition LV-sendMsg :: nat \Rightarrow Proc \Rightarrow Proc \Rightarrow \text{'val pstate} \Rightarrow \text{'val msg where**

\[
\text{LV-sendMsg} \; (r::\text{nat}) \equiv
\begin{align*}
&\text{if } \text{step } r = 0 \text{ then send0 } r \\
&\text{else if } \text{step } r = 1 \text{ then send1 } r \\
&\text{else if } \text{step } r = 2 \text{ then send2 } r \\
&\text{else send3 } r
\end{align*}
\]

**Definition LV-nextState :: nat \Rightarrow Proc \Rightarrow \text{'val pstate} \Rightarrow (Proc \Rightarrow \text{'val msg) \Rightarrow Proc \Rightarrow \text{'val pstate} \Rightarrow \text{bool where**

\[
\text{LV-nextState} \; r \equiv
\begin{align*}
&\text{if } \text{step } r = 0 \text{ then next0 } r \\
&\text{else if } \text{step } r = 1 \text{ then next1 } r \\
&\text{else if } \text{step } r = 2 \text{ then next2 } r \\
&\text{else next3 } r
\end{align*}
\]

39
7.2 Communication Predicate for LastVoting

We now define the communication predicate that will be assumed for the correctness proof of the LastVoting algorithm. The “per-round” part is trivial: integrity and agreement are always ensured.

For the “global” part, Charron-Bost and Schiper propose a predicate that requires the existence of infinitely many phases $ph$ such that:

- all processes agree on the same coordinator $c$,
- $c$ hears from a strict majority of processes in steps 0 and 2 of phase $ph$,
- every process hears from $c$ in steps 1 and 3 (this is slightly weaker than the predicate that appears in [7], but obviously sufficient).

Instead of requiring infinitely many such phases, we only assume the existence of one such phase (Charron-Bost and Schiper note that this is enough.)

**definition**

\[LV\text{-}commPerRd\] where

\[LV\text{-}commPerRd\ r\ (HO::Proc\ HO) (coord::Proc\ coord) \equiv True\]

**definition**

\[LV\text{-}commGlobal\] where

\[LV\text{-}commGlobal\ HOs\ coords \equiv \exists \, ph:not.\ \exists \, c::Proc.\]

\[(\forall \, p.\ coords\ (4*ph)\ p = c)\]

\[\land \, \text{card}\ (HOs\ (4*ph)\ c) > N\ \text{div}\ 2\]

\[\land \, \text{card}\ (HOs\ (4*ph+2)\ c) > N\ \text{div}\ 2\]

\[\land \, (\forall \, p.\ c \in HOs\ (4*ph+1)\ p \cap HOs\ (4*ph+3)\ p)\]

7.3 The LastVoting Heard-Of Machine

We now define the coordinated HO machine for the LastVoting algorithm by assembling the algorithm definition and its communication-predicate.

**definition** \[LV\text{-}CHO\text{Machine}\] where

\[LV\text{-}CHO\text{Machine} \equiv\]

\[
\langle \text{CinitState = LV\text{-}initState, }\]

\[
\text{sendMsg = LV\text{-}sendMsg, }\]

\[
\text{CnextState = LV\text{-}nextState, }\]

\[
\text{CHOcommPerRd = LV\text{-}commPerRd, }\]

\[
\text{CHOcommGlobal = LV\text{-}commGlobal }\rangle\]

**abbreviation**

\[LV\text{-}M \equiv (LV\text{-}CHO\text{Machine}::(Proc,'val\ pstate,'val\ msg)\ CHO\text{Machine})\]

end
theory LastVotingProof
imports LastVotingDefs ../Majorities ../Reduction
begin

7.4 Preliminary Lemmas

We begin by proving some simple lemmas about the utility functions used in the model of LastVoting. We also specialize the induction rules of the generic CHO model for this particular algorithm.

lemma timeStampsRcvdFinite:
  finite {ts . ∃ q v. (msgs::Proc → ′val msg) q = Some (ValStamp v ts)}
  ⟨proof⟩

lemma highestStampRcvd-exists:
  assumes nempty: valStampsRcvd msgs ≠ {}
  obtains p v where msgs p = Some (ValStamp v (highestStampRcvd msgs))
  ⟨proof⟩

lemma highestStampRcvd-max:
  assumes msgs p = Some (ValStamp v ts)
  shows ts ≤ highestStampRcvd msgs
  ⟨proof⟩

lemma phase-Suc:
  phase (Suc r) = (if step r = 3 then Suc (phase r)
  else phase r)
  ⟨proof⟩

Many proofs are by induction on runs of the LastVoting algorithm, and we derive a specific induction rule to support these proofs.

lemma LV-induct:
  assumes run: CHORun LV-M rho HOs coords
  and init: ∀ p. CinitState LV-M p (rho 0 p) (coords 0 p) → P 0
  and step0: ∀ r.
  [ step r = 0; P r; phase (Suc r) = phase r; step (Suc r) = 1;
  ∀ p. next0 r p (rho r p)
  (HOrcvdMsgs LV-M r p (HOs r p) (rho r))
  (coords (Suc r) p)
  (rho (Suc r) p) ]
  → P (Suc r)
  and step1: ∀ r.
  [ step r = 1; P r; phase (Suc r) = phase r; step (Suc r) = 2;
  ∀ p. next1 r p (rho r p)
  (HOrcvdMsgs LV-M r p (HOs r p) (rho r))
  (coords (Suc r) p)
  (rho (Suc r) p) ]
  → P (Suc r)

41
and step2: \( \forall r. \)
\[
\begin{align*}
\text{[ } & \text{step } r = 2; \ P r; \ \text{phase } (\text{Suc } r) = \text{phase } r; \ \text{step } (\text{Suc } r) = 3; \\
& \forall p. \ \text{next2 } r \ p (\rho r, r) \\
& \quad (\text{HOrcvdMsgs } LV-M \ r \ p \ (\text{HOs } r \ p) \ (\rho r)) \\
& \quad \text{(coords } (\text{Suc } r) \ p) \\
& \quad (\rho (\text{Suc } r) \ p) \]\end{align*}
\]
\( \implies P (\text{Suc } r) \)

and step3: \( \forall r. \)
\[
\begin{align*}
\text{[ } & \text{step } r = 3; \ P r; \ \text{phase } (\text{Suc } r) = \text{Suc } (\text{phase } r); \ \text{step } (\text{Suc } r) = 0; \\
& \forall p. \ \text{next3 } r \ p (\rho r, r) \\
& \quad (\text{HOrcvdMsgs } LV-M \ r \ p \ (\text{HOs } r \ p) \ (\rho r)) \\
& \quad \text{(coords } (\text{Suc } r) \ p) \\
& \quad (\rho (\text{Suc } r) \ p) \]\end{align*}
\]
\( \implies P (\text{Suc } r) \)

shows \( P \ n \)

(proof)

The following rule similarly establishes a property of two successive configurations of a run by case distinction on the step that was executed.

**Lemma LV-Suc:**

assumes run: \( \text{CHORun } LV-M \ \rho \ \text{HOs } \text{coords} \)

and step0: \[ \text{[ } \text{step } r = 0; \ \text{step } (\text{Suc } r) = 1; \ \text{phase } (\text{Suc } r) = \text{phase } r; \]
\[ \forall p. \ \text{next0 } r \ p (\rho r, r) \\
\quad (\text{HOrcvdMsgs } LV-M \ r \ p \ (\text{HOs } r \ p) \ (\rho r)) \\
\quad \text{(coords } (\text{Suc } r) \ p) \ (\rho (\text{Suc } r) \ p) \]\end{align*}
\( \implies P r \)

and step1: \[ \text{[ } \text{step } r = 1; \ \text{step } (\text{Suc } r) = 2; \ \text{phase } (\text{Suc } r) = \text{phase } r; \]
\[ \forall p. \ \text{next1 } r \ p (\rho r, r) \\
\quad (\text{HOrcvdMsgs } LV-M \ r \ p \ (\text{HOs } r \ p) \ (\rho r)) \\
\quad \text{(coords } (\text{Suc } r) \ p) \ (\rho (\text{Suc } r) \ p) \]\end{align*}
\( \implies P r \)

and step2: \[ \text{[ } \text{step } r = 2; \ \text{step } (\text{Suc } r) = 3; \ \text{phase } (\text{Suc } r) = \text{phase } r; \]
\[ \forall p. \ \text{next2 } r \ p (\rho r, r) \\
\quad (\text{HOrcvdMsgs } LV-M \ r \ p \ (\text{HOs } r \ p) \ (\rho r)) \\
\quad \text{(coords } (\text{Suc } r) \ p) \ (\rho (\text{Suc } r) \ p) \]\end{align*}
\( \implies P r \)

and step3: \[ \text{[ } \text{step } r = 3; \ \text{step } (\text{Suc } r) = 0; \ \text{phase } (\text{Suc } r) = \text{Suc } (\text{phase } r); \]
\[ \forall p. \ \text{next3 } r \ p (\rho r, r) \\
\quad (\text{HOrcvdMsgs } LV-M \ r \ p \ (\text{HOs } r \ p) \ (\rho r)) \\
\quad \text{(coords } (\text{Suc } r) \ p) \ (\rho (\text{Suc } r) \ p) \]\end{align*}
\( \implies P r \)

shows \( P \ n \)

(proof)

Sometimes the assertion to prove talks about a specific process and follows from the next-state relation of that particular process. We prove corresponding variants of the induction and case-distinction rules. When these variants are applicable, they help automating the Isabelle proof.

**Lemma LV-induct’:**
assumes run: CHORun LV-M rho HOs coords
and init: CinitState LV-M p (rho 0 p) (coords 0 p) \implies P \ p \ 0
and step0: \forall r.  \[ \begin{align*}
step r &= 0; \\
(P \ p r; \ \text{phase} (Suc \ r) &= \text{phase} r; \ step (Suc \ r) &= 1; \\
next0 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ (Suc \ r)
\end{align*} \]
and step1: \forall r.  \[ \begin{align*}
step r &= 1; \\
(P \ p r; \ \text{phase} (Suc \ r) &= \text{phase} r; \ step (Suc \ r) &= 2; \\
next1 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ (Suc \ r)
\end{align*} \]
and step2: \forall r.  \[ \begin{align*}
step r &= 2; \\
(P \ p r; \ \text{phase} (Suc \ r) &= \text{phase} r; \ step (Suc \ r) &= 3; \\
next2 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ (Suc \ r)
\end{align*} \]
and step3: \forall r.  \[ \begin{align*}
step r &= 3; \\
(P \ p r; \ \text{phase} (Suc \ r) &= \text{Suc} \ (phase r); \ step (Suc \ r) &= 0; \\
next3 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ (Suc \ r)
\end{align*} \]
shows P \ p \ n

(proof)

lemma LV-Suc':

assumes run: CHORun LV-M rho HOs coords
and step0: \[ \begin{align*}
\text{step} r &= 0; \ \text{step} (Suc \ r) &= 1; \ \text{phase} (Suc \ r) &= \text{phase} r; \\
\text{next}0 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ r
\end{align*} \]
and step1: \[ \begin{align*}
\text{step} r &= 1; \ \text{step} (Suc \ r) &= 2; \ \text{phase} (Suc \ r) &= \text{phase} r; \\
\text{next}1 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ r
\end{align*} \]
and step2: \[ \begin{align*}
\text{step} r &= 2; \ \text{step} (Suc \ r) &= 3; \ \text{phase} (Suc \ r) &= \text{phase} r; \\
\text{next}2 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ r
\end{align*} \]
and step3: \[ \begin{align*}
\text{step} r &= 3; \ \text{step} (Suc \ r) &= 0; \ \text{phase} (Suc \ r) &= \text{Suc} \ (phase r); \\
\text{next}3 r p (rho r p) &\left( \begin{array}{l}
(HOrcvdMsgs LV-M r p (HOs r p) (rho r)) \\
(coords (Suc r) p) (rho (Suc r) p)
\end{array} \right) \\
\implies P \ p \ r
\end{align*} \]
shows P \ p \ r
7.5 Boundedness and Monotonicity of Timestamps

The timestamp of any process is bounded by the current phase.

**lemma** LV-timestamp-bounded:
*assumes* run: CHORun LV-M rho HOs coords
*shows* timestamp (rho n p) \( \leq \) (if step n < 2 then phase n else Suc (phase n))
(is ?P p n)

(proof)

Moreover, timestamps can only grow over time.

**lemma** LV-timestamp-increasing:
*assumes* run: CHORun LV-M rho HOs coords
*shows* timestamp (rho n p) \( \leq \) timestamp (rho (Suc n) p)
(is ?P p n is ?ts \leq -)

(proof)

**lemma** LV-timestamp-monotonic:
*assumes* run: CHORun LV-M rho HOs coords and le: m \( \leq \) n
*shows* timestamp (rho m p) \( \leq \) timestamp (rho n p)
(is ?ts m \leq -)

(proof)

The following definition collects the set of processes whose timestamp is beyond a given bound at a system state.

**definition** procsBeyondTS where
procsBeyondTS ts cfg \equiv \{ p . ts \leq timestamp (cfg p) \}

Since timestamps grow monotonically, so does the set of processes that are beyond a certain bound.

**lemma** procsBeyondTS-monotonic:
*assumes* run: CHORun LV-M rho HOs coords and p: p \in procsBeyondTS ts (rho m) and le: m \( \leq \) n
*shows* p \in procsBeyondTS ts (rho n)

(proof)

7.6 Obvious Facts About the Algorithm

The following lemmas state some very obvious facts that follow “immediately” from the definition of the algorithm. We could prove them in one fell swoop by defining a big invariant, but it appears more readable to prove them separately.

Coordinators change only at step 3.

**lemma** notStep3EqualCoord:
*assumes* run: CHORun LV-M rho HOs coords and stp:step r \neq 3

44
\( \text{shows } \text{coord}(\rho \text{ (Suc } r \text{) } p) = \text{coord}(\rho \text{ r } p) \text{ (is } \rho \text{ p r) } \)
\langle \text{proof} \rangle

**Lemma coordinators:**

**Assumes** run: CHORun LV-M rho HOs coords

**Shows** \( \text{coord}(\rho \text{ r } p) = \text{coords}(4 \ast \text{phase } r) \text{ p} \)
\langle \text{proof} \rangle

Votes only change at step 0.

**Lemma notStep0EqualVote** [rule-format]:

**Assumes** run: CHORun LV-M rho HOs coords

**Shows** \( \text{step } r \neq 0 \rightarrow \text{vote}(\rho \text{ (Suc } r \text{) } p) = \text{vote}(\rho \text{ r } p) \text{ (is } \rho \text{ p r) } \)
\langle \text{proof} \rangle

Commit status only changes at steps 0 and 3.

**Lemma notStep03EqualCommit** [rule-format]:

**Assumes** run: CHORun LV-M rho HOs coords

**Shows** \( \text{step } r \neq 0 \land \text{step } r \neq 3 \rightarrow \text{commt}(\rho \text{ (Suc } r \text{) } p) = \text{commt}(\rho \text{ r } p) \text{ (is } \rho \text{ p r) } \)
\langle \text{proof} \rangle

Timestamps only change at step 1.

**Lemma notStep1EqualTimestamp** [rule-format]:

**Assumes** run: CHORun LV-M rho HOs coords

**Shows** \( \text{step } r \neq 1 \rightarrow \text{timestamp}(\rho \text{ (Suc } r \text{) } p) = \text{timestamp}(\rho \text{ r } p) \text{ (is } \rho \text{ p r) } \)
\langle \text{proof} \rangle

The \( x \) field only changes at step 1.

**Lemma notStep1EqualX** [rule-format]:

**Assumes** run: CHORun LV-M rho HOs coords

**Shows** \( \text{step } r \neq 1 \rightarrow \text{x}(\rho \text{ (Suc } r \text{) } p) = \text{x}(\rho \text{ r } p) \text{ (is } \rho \text{ p r) } \)
\langle \text{proof} \rangle

A process \( p \) has its \textit{commit} flag set only if the following conditions hold:

- the step number is at least 1,
- \( p \) considers itself to be the coordinator,
- \( p \) has a non-null \textit{vote},
- a majority of processes consider \( p \) as their coordinator.

**Lemma commitE:**

**Assumes** run: CHORun LV-M rho HOs coords and \textit{cmt}: \textit{commt}(\rho \text{ r } p)\text{ and \textit{conds}}: \[ 1 \leq \text{step } r; \text{coord}(\rho \text{ r } p) = p; \text{vote}(\rho \text{ r } p) \neq \text{None}; \text{card} \{ q : \text{coord}(\rho \text{ r } q) = p \} > N \div 2 \]
\[ \implies A \]
shows A
(proof)

A process has a current timestamp only if:

• it is at step 2 or beyond,
• its coordinator has committed,
• its $x$ value is the vote of its coordinator.

**lemma** currentTimestampE:
**assumes** run: CHORun LV-M rho HOs coords
and ts: timestamp (rho r p) = Suc (phase r)
and conds: \[ 2 \leq \text{step } r; \]
\[ \text{commit (rho r (coord}\Phi (\text{rho r p}))); \]
\[ x (\text{rho r p}) = \text{the (vote (rho r (coord}\Phi (\text{rho r p})))) \]
\[ \implies A \]

shows A
(proof)

If a process $p$ has its ready bit set then:

• it is at step 3,
• it considers itself to be the coordinator of that phase and
• a majority of processes considers $p$ to be the coordinator and has a current timestamp.

**lemma** readyE:
**assumes** run: CHORun LV-M rho HOs coords and rdy: ready (rho r p)
and conds: \[ \text{step } r = 3; \text{coord}\Phi (\text{rho r p}) = p; \]
\[ \text{card } \{ q : \text{coord}\Phi (\text{rho r q}) = p \}
\[ \land \text{timestamp (rho r q) = Suc (phase r)} \} > N \text{div 2} \]
\[ \implies P \]

shows P
(proof)

A process decides only if the following conditions hold:

• it is at step 3,
• its coordinator votes for the value the process decides on,
• the coordinator has its ready and commit bits set.

**lemma** decisionE:
**assumes** run: CHORun LV-M rho HOs coords
and dec: decide (rho (Suc r) p) $\neq$ decide (rho r p)
and conds: \[
\begin{align*}
& \text{step } r = 3; \\
& \text{decide } (\rho \ (\text{Suc } r) \ p) = \text{Some } (\text{the } (\text{vote } (\rho \ r \ (\text{coord}\Phi \ (\rho \ r \ p))))); \\
& \text{ready } (\rho \ r \ (\text{coord}\Phi \ (\rho \ r \ p))); \text{comm } (\rho \ r \ (\text{coord}\Phi \ (\rho \ r \ p)))
\end{align*}
\] 
shows \( P \)

\begin{proof}
\end{proof}

7.7 Proof of Integrity

Integrity is proved using a standard invariance argument that asserts that only values present in the initial state appear in the relevant fields.

\textbf{lemma lv-integrityInvariant:}
\begin{itemize}
\item \textbf{assumes} run: CHORun LV-M rho HOs coords
\item and inv: \[
\begin{align*}
& \text{range } (x \circ (\rho n)) \subseteq \text{range } (x \circ (\rho 0)); \\
& \text{range } (\text{vote } \circ (\rho n)) \subseteq \{ \text{None} \} \cup \text{Some ' range } (x \circ (\rho 0)); \\
& \text{range } (\text{decide } \circ (\rho n)) \subseteq \{ \text{None} \} \cup \text{Some ' range } (x \circ (\rho 0))
\end{align*}
\] 
\item \textbf{shows} \( A \)
\end{itemize}

\begin{proof}
\end{proof}

Integrity now follows immediately.

\textbf{theorem lv-integrity:}
\begin{itemize}
\item \textbf{assumes} run: CHORun LV-M rho HOs coords
\item and dec: \text{decide } (\rho \ n \ p) = \text{Some } v
\item \textbf{shows} \( \exists q. \ v = x \ (\rho \ 0 \ q) \)
\end{itemize}

\begin{proof}
\end{proof}

7.8 Proof of Agreement and Irrevocability

The following lemmas closely follow a hand proof provided by Bernadette Charron-Bost.

If a process decides, then a majority of processes have a current timestamp.

\textbf{lemma decisionThenMajorityBeyondTS:}
\begin{itemize}
\item \textbf{assumes} run: CHORun LV-M rho HOs coords
\item and \text{dec: } \text{decide } (\rho \ (\text{Suc } r) \ p) \neq \text{decide } (\rho \ r \ p)
\item \textbf{shows} card \ (\text{procsBeyondTS } (\text{Suc } \ (\text{phase } r)) \ (\rho \ r)) > \frac{N}{2}\)
\end{itemize}

\begin{proof}
\end{proof}

No two different processes have their \textit{commit} flag set at any state.

\textbf{lemma committedProcsEqual:}
\begin{itemize}
\item \textbf{assumes} run: CHORun LV-M rho HOs coords
\item and \text{cmt: } \text{comm } (\rho \ r \ p) \ \text{and } \text{cmt' } \text{comm } (\rho \ r \ p')
\item \textbf{shows} \( p = p' \)
\end{itemize}

\begin{proof}
\end{proof}

No two different processes have their \textit{ready} flag set at any state.
lemma readyProcsEqual:
  assumes run: CHORun LV-M rho HOs coords
  and rdy: ready (rho r p) and rdy': ready (rho r p')
  shows p = p'
⟨proof⟩
The following lemma asserts that whenever a process p commits at a state
where a majority of processes have a timestamp beyond ts, then p votes for
a value held by some process whose timestamp is beyond ts.

lemma commitThenVoteRecent:
  assumes run: CHORun LV-M rho HOs coords
  and maj: card (procsBeyondTS ts (rho r)) > N div 2
  and cmt: commit (rho r p)
  shows \exists q \in procsBeyondTS ts (rho r). vote (rho r p) = Some (x (rho r q))
  (is ?Q r)
⟨proof⟩
The following lemma gives the crucial argument for agreement: after some
process p has decided, all processes whose timestamp is beyond the times-
tamp at the point of decision contain the decision value in their x field.

lemma XOfTimestampBeyondDecision:
  assumes run: CHORun LV-M rho HOs coords
  and dec: decide (rho (Suc r) p) ≠ decide (rho r p)
  shows \forall q \in procsBeyondTS (Suc (phase r)) (rho (r+k)).
  x (rho (r+k) q) = the (decide (rho (Suc r) p))
  (is \forall q \in ?bynd k. - = ?v is ?P p k)
⟨proof⟩
We are now in position to prove Agreement: if some process decides at step
r and another (or possibly the same) process decides at step r+k then they
decide the same value.

lemma laterProcessDecidesSameValue:
  assumes run: CHORun LV-M rho HOs coords
  and p: decide (rho (Suc r) p) ≠ decide (rho r p)
  and q: decide (rho (Suc (r+k)) q) ≠ decide (rho (r+k) q)
  shows decide (rho (Suc (r+k)) q) = decide (rho (Suc r) p)
⟨proof⟩
A process that holds some decision v has decided v sometime in the past.

lemma decisionNonNullThenDecided:
  assumes run: CHORun LV-M rho HOs coords
  and dec: decide (rho n p) = Some v
  shows \exists m<n, decide (rho (Suc m) p) ≠ decide (rho m p)
  ∧ decide (rho (Suc m) p) = Some v
⟨proof⟩
Irrevocability and Agreement are straightforward consequences of the two
preceding lemmas.
7.9 Proof of Termination

The proof of termination relies on the communication predicate, which stipulates the existence of some phase during which there is a single coordinator that (a) receives a majority of messages and (b) is heard by everybody. Therefore, all processes successfully execute the protocol, deciding at step 3 of that phase.

7.10 LastVoting Solves Consensus

Summing up, all (coarse-grained) runs of LastVoting for HO collections that satisfy the communication predicate satisfy the Consensus property.
8 Verification of the $U_{T,E,\alpha}$ Consensus Algorithm

Algorithm $U_{T,E,\alpha}$ is presented in [3]. It is an uncoordinated algorithm that tolerates value (a.k.a. Byzantine) faults, and can be understood as a variant of Uniform Voting. The parameters $T$, $E$, and $\alpha$ appear as thresholds of the algorithm and in the communication predicates. Their values can be chosen within certain bounds in order to adapt the algorithm to the characteristics of different systems.

We formalize in Isabelle the correctness proof of the algorithm that appears in [3], using the framework of theory $HOModel$.

8.1 Model of the Algorithm

We begin by introducing an anonymous type of processes of finite cardinality that will instantiate the type variable $'proc$ of the generic HO model.

```isar
typedec Proc — the set of processes
axiomatization where Proc-finite: OFCLASS(Proc, finite-class)
instance Proc :: finite
```  

abbreviation

$N \equiv \text{card}(\text{UNIV}::\text{Proc set})$ — number of processes

The algorithm proceeds in phases of 2 rounds each (we call steps the individual rounds that constitute a phase). The following utility functions compute the phase and step of a round, given the round number.

```isar
abbreviation
nSteps \equiv 2

definition phase where phase (r::nat) \equiv r \div nSteps

definition step where step (r::nat) \equiv r \mod nSteps
```  

lemma phase-zero [simp]: phase 0 = 0
(proof)

lemma step-zero [simp]: step 0 = 0
(proof)

lemma phase-step: (phase r + nSteps) + step r = r
(proof)

The following record models the local state of a process.

record $'val p\text{state} =$

$x :: 'val$ — current value held by process

50
vote :: 'val option  — value the process voted for, if any
decide :: 'val option  — value the process has decided on, if any

Possible messages sent during the execution of the algorithm.

datatype 'val msg =
  Val 'val
| Vote 'val option

The \( x \) field of the initial state is unconstrained, all other fields are initialized appropriately.

definition Ute-initState where
  Ute-initState p st ≡
  (vote st = None) ∧ (decide st = None)

The following locale introduces the parameters used for the \( U_{T,E,\alpha} \) algorithm and their constraints [3].

locale ute-parameters =
  fixes \( \alpha :: \text{nat} \) and \( T :: \text{nat} \) and \( E :: \text{nat} \)
  assumes \( \text{majE}: 2*E \geq N + 2*\alpha \)
  and \( \text{majT}: 2*T \geq N + 2*\alpha \)
  and \( \text{EltN}: E < N \)
  and \( \text{TltN}: T < N \)
begin

Simple consequences of the above parameter constraints.

lemma alpha-lt-N: \( \alpha < N \)
⟨proof⟩

lemma alpha-lt-T: \( \alpha < T \)
⟨proof⟩

lemma alpha-lt-E: \( \alpha < E \)
⟨proof⟩

We separately define the transition predicates and the send functions for each step and later combine them to define the overall next-state relation.

In step 0, each process sends its current \( x \). If it receives the value \( v \) more than \( T \) times, it votes for \( v \), otherwise it doesn’t vote.

definition
  send0 :: nat ⇒ Proc ⇒ Proc ⇒ 'val pstate ⇒ 'val msg
where
  send0 r p q st ≡ Val (x st)

definition
  next0 :: nat ⇒ Proc ⇒ 'val pstate ⇒ (Proc ⇒ 'val msg option)
  ⇒ 'val pstate ⇒ bool
where
In step 1, each process sends its current vote. If it receives more than \( \alpha \) votes for a given value \( v \), it sets its \( x \) field to \( v \), else it sets \( x \) to a default value.

If the process receives more than \( E \) votes for \( v \), it decides \( v \), otherwise it leaves its decision unchanged.

**Definition**

\[
\text{send1} :: \text{nat} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \\
\text{where}
\]

\[
\text{send1} \ r \ p \ q \ s \ t \equiv \text{Vote} (\text{vote } s)
\]

**Definition**

\[
\text{next1} :: \text{nat} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \\
\text{where}
\]

\[
\text{next1} \ r \ p \ q \ s \ t \equiv \begin{cases}
( \exists v. \ \text{card} \{q. \text{msgs} q = \text{Some } (\text{Vote } \text{Some } v)\} > \alpha \land s' = v) \\
\lor (\neg (\exists v. \ \text{card} \{q. \text{msgs} q = \text{Some } (\text{Vote } \text{Some } v)\} > \alpha) \\
\land x' = \text{undefined}) \\
\land (\exists v. \ \text{card} \{q. \text{msgs} q = \text{Some } (\text{Vote } \text{Some } v)\} > E \land \text{decide } s' = \text{Some } v) \\
\lor (\neg (\exists v. \ \text{card} \{q. \text{msgs} q = \text{Some } (\text{Vote } \text{Some } v)\} > E) \\
\land \text{decide } s' = \text{decide } s)
\end{cases}
\]

The overall send function and next-state relation are simply obtained as the composition of the individual relations defined above.

**Definition**

\[
Ute-\text{sendMsg} :: \text{nat} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \\
\text{where}
\]

\[
Ute-\text{sendMsg}(r::\text{nat}) \equiv \text{if step } r = 0 \text{ then } \text{send0 } r \text{ else } \text{send1 } r
\]

**Definition**

\[
Ute-\text{nextState} :: \text{nat} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \\
\text{where}
\]

\[
Ute-\text{nextState}(r::\text{nat}) \equiv \text{if step } r = 0 \text{ then } \text{next0 } r \text{ else } \text{next1 } r
\]

### 8.2 Communication Predicate for \( U_{T,E,\alpha} \)

Following [3], we now define the communication predicate for the \( U_{T,E,\alpha} \) algorithm to be correct.

The round-by-round predicate stipulates the following conditions:

- no process may receive more than \( \alpha \) corrupted messages, and
• every process should receive more than \( \text{max}(T, N + 2\alpha - E - 1) \) correct messages.

[3] also requires that every process should receive more than \( \alpha \) correct messages, but this is implied, since \( T > \alpha \) (cf. lemma \( \text{alpha-lt-T} \)).

definition \( \text{Ute-commPerRd} \) where
\[
\text{Ute-commPerRd} \equiv \forall p. \text{card} (\text{HOs} p - \text{SHO} p) \leq \alpha
\land \text{card} (\text{SHO} p \cap \text{HO} p) > N + 2\alpha - E - 1
\land \text{card} (\text{SHO} p \cap \text{HO} p) > T
\]

The global communication predicate requires there exists some phase \( \Phi \) such that:

• all HO and SHO sets of all processes are equal in the second step of phase \( \Phi \), i.e. all processes receive messages from the same set of processes, and none of these messages is corrupted,

• every process receives more than \( T \) correct messages in the first step of phase \( \Phi + 1 \), and

• every process receives more than \( E \) correct messages in the second step of phase \( \Phi + 1 \).

The predicate in the article [3] requires infinitely many such phases, but one is clearly enough.

definition \( \text{Ute-commGlobal} \) where
\[
\text{Ute-commGlobal} \equiv \exists \Phi. ((\forall p. \text{card} (\text{SHO} p \cap \text{HO} p) > T)
\land (\forall p. \text{card} (\text{SHO} (\text{Suc} r) p \cap \text{HO} (\text{Suc} r) p) > E))
\]

8.3 The \( \mathcal{U}_{T,E,\alpha} \) Heard-Of Machine

We now define the coordinated HO machine for the \( \mathcal{U}_{T,E,\alpha} \) algorithm by assembling the algorithm definition and its communication-predicate.

definition \( \text{Ute-SHOMachine} \) where
\[
\text{Ute-SHOMachine} = (\langle \text{CinitState} = (\lambda p \text{ st crd}. \text{Ute-initState} p \text{ st}),
\text{sendMsg} = \text{Ute-sendMsg},
\text{CnextState} = (\lambda r p \text{ st msgs st}. \text{Ute-nextState} r p \text{ st msgs st'}),
\text{SHOcommPerRd} = \text{Ute-commPerRd},
\text{SHOcommGlobal} = \text{Ute-commGlobal}
\rangle)
\]

abbreviation
8.4 Preliminary Lemmas

Processes can make a vote only at first round of each phase.

**lemma vote-step:**

assumes **nextState Ute-M r p** (rho r p) mu (rho (Suc r) p)
and vote (rho (Suc r) p) \neq None

shows step r = 0

(proof)

Processes can make a new decision only at second round of each phase.

**lemma decide-step:**

assumes run: SHORun Ute-M rho HOs SHOs
and d1: decide (rho r p) \neq Some v
and d2: decide (rho (Suc r) p) = Some v

shows step r \neq 0

(proof)

**lemma unique-majority-E:**

assumes majv: card \{qq::Proc. F qq = Some m\} > E
and majw: card \{qq::Proc. F qq = Some m'\} > E

shows m = m'

(proof)

**lemma unique-majority-E-\alpha:**

assumes majv: card \{qq::Proc. F qq = m\} > E - \alpha
and majw: card \{qq::Proc. F qq = m'\} > E - \alpha

shows m = m'

(proof)

**lemma unique-majority-T:**

assumes majv: card \{qq::Proc. F qq = Some m\} > T
and majw: card \{qq::Proc. F qq = Some m'\} > T

shows m = m'

(proof)

No two processes may vote for different values in the same round.

**lemma common-vote:**
assumes usafe: SHOcommPerRd Ute-M HO SHO and nxtp: nextState Ute-M r p (rho r p) µp (rho (Suc r) p) and mup: µp ∈ SHOmsgVectors Ute-M r p (rho r) (SHO p) and nxtp: nextState Ute-M r q (rho r q) µq (rho (Suc r) q) and muq: µq ∈ SHOmsgVectors Ute-M r q (rho r) (SHO q) and vp: vote (rho (Suc r) p) = Some vp and vq: vote (rho (Suc r) q) = Some vq shows vp = vq

⟨proof⟩

No decision may be taken by a process unless it received enough messages holding the same value.

lemma decide-with-threshold-E:
assumes run: SHORun Ute-M rho HOs SHOs and usafe: SHOcommPerRd Ute-M (HOs r) (SHOs r) and d1: decide (rho r p) ≠ Some v and d2: decide (rho (Suc r) p) = Some v shows card \{q. sendMsg Ute-M r q p (rho r q) = Vote (Some v)\} > E − α ⟨proof⟩

8.5 Proof of Agreement and Validity

If more than \(E − α\) messages holding \(v\) are sent to some process \(p\) at round \(r\), then every process \(pp\) correctly receives more than \(α\) such messages.

lemma common-x-argument-1:
assumes usafe: SHOcommPerRd Ute-M (HOs (Suc r)) (SHOs (Suc r)) and threshold: card \{q. sendMsg Ute-M (Suc r) q p (rho (Suc r) q) = Vote (Some v)\} > E − α (is card (?msgs p v) > -) shows card (?msgs pp v \cap (SHOs (Suc r) pp \cap HOs (Suc r) pp)) > α ⟨proof⟩

If more than \(E − α\) messages holding \(v\) are sent to \(p\) at some round \(r\), then any process \(pp\) will set its \(x\) to value \(v\) in \(r\).

lemma common-x-argument-2:
assumes run: SHORun Ute-M rho HOs SHOs and usafe: \(∀r.\) SHOcommPerRd Ute-M (HOs r) (SHOs r) and nxtp: nextState Ute-M (Suc r) pp (rho (Suc r) pp) µpp (rho (Suc (Suc r)) pp) and mupp: µpp ∈ SHOmsgVectors Ute-M (Suc r) pp (rho (Suc r)) (HOs (Suc r) pp) (SHOs (Suc r) pp) and threshold: card \{q. sendMsg Ute-M (Suc r) q p (rho (Suc r) q) = Vote (Some v)\} > E − α (is card (?sent p v) > -) shows x (rho (Suc (Suc r)) pp) = v ⟨proof⟩
Inductive argument for the agreement and validity theorems.

**Lemma** safety-inductive-argument:
- **assumes** run: \texttt{SHORun Ute-M rho HOs SHOs}
- **and** comm: \( \forall r. \texttt{SHOcommPerRd Ute-M (HOs r) (SHOs r)} \)
- **and** \( \text{ih} : E - \alpha < \text{card } \{ q. \text{sendMsg Ute-M } r' q p (\rho r' q) = \text{Vote } (\text{Some } v) \} \)
- **and** \( \text{stp1} : \text{step } r' = \text{Suc } 0 \)
- **shows** \( E - \alpha < \text{card } \{ q. \text{sendMsg Ute-M (Suc (Suc } r')) q p (\rho (\text{Suc (Suc } r')) q) = \text{Vote } (\text{Some } v) \} \)

\[ \langle \text{proof} \rangle \]

A process that holds some decision \( v \) has decided \( v \) sometime in the past.

**Lemma** decisionNonNullThenDecided:
- **assumes** run: \texttt{SHORun Ute-M rho HOs SHOs}
- **and** \( \text{dv1} : \text{decide } (\rho (\text{Suc } r) p1) = \text{Some } v \)
- **and** \( \text{dn2} : \text{decide } (\rho (r+k) p2) = \text{Some } v2 \)
- **and** \( \text{dv2} : \text{decide } (\rho (\text{Suc (Suc } r+k)) p2) = \text{Some } v2 \)
- **shows** \( v2 = v1 \)

\[ \langle \text{proof} \rangle \]

The Agreement property is an immediate consequence of the two preceding lemmas.

**Theorem** ute-agreement:
- **assumes** run: \texttt{SHORun Ute-M rho HOs SHOs}
- **and** comm: \( \forall r. \texttt{SHOcommPerRd Ute-M (HOs r) (SHOs r)} \)
- **and** \( \text{p} : \text{decide } (\rho m p) = \text{Some } v \)
- **and** \( \text{q} : \text{decide } (\rho n q) = \text{Some } w \)
- **shows** \( v = w \)

\[ \langle \text{proof} \rangle \]

Main lemma for the proof of the Validity property.

**Lemma** validity-argument:
- **assumes** run: \texttt{SHORun Ute-M rho HOs SHOs}
- **and** comm: \( \forall r. \texttt{SHOcommPerRd Ute-M (HOs r) (SHOs r)} \)
- **and** \( \text{init: } \forall p, x ((\rho 0) p) = v \)
- **and** \( \text{dw: decide } (\rho r p) = \text{Some } w \)
- **and** \( \text{stp: step } r' = \text{Suc } 0 \)
- **shows** \( \text{card } \{ q. \text{sendMsg Ute-M } r' q p (\rho r' q) = \text{Vote } (\text{Some } v) \} > E - \alpha \)
The following theorem shows the Validity property of algorithm $U_{T,E,\alpha}$.

**Theorem ute-validity:**
- **assumes** run: $\text{SHORun Ute-M } \rho \text{ HOsh SHOs}$
- and comm: $\forall r. \text{SHOcommPerRd Ute-M } (\text{HOs } r) (\text{SHOs } r)$
- and $\text{init: } \forall p. x (\rho 0 p) = v$
- and $\text{dw: } \text{decide } (\rho r p) = \text{Some } w$

shows $v = w$

### 8.6 Proof of Termination

At the second round of a phase that satisfies the conditions expressed in the global communication predicate, processes update their $x$ variable with the value $v$ they receive in more than $\alpha$ messages.

**Lemma set-x-from-vote:**
- **assumes** run: $\text{SHORun Ute-M } \rho \text{ HOsh SHOs}$
- and comm: $\text{SHOcommPerRd Ute-M } (\text{HOs } r) (\text{SHOs } r)$
- and $\text{stp: } \text{step } (\text{Suc } r) = \text{Suc } 0$
- and $\pi: \forall p. \text{HOs } (\text{Suc } r) p = \text{SHOs } (\text{Suc } r) p$
- and $\text{nxt: } \text{nextState Ute-M } (\text{Suc } r) p (\rho (\text{Suc } r) p) \mu (\rho (\text{Suc } r) p)$
- and $\mu: \mu \in \text{SHOmsgVectors Ute-M } (\text{Suc } r) p (\rho (\text{Suc } r) p) (\text{HOs } (\text{Suc } r) p) (\text{SHOs } (\text{Suc } r) p)$
- and $\text{vp: } \alpha < \text{card } \{ q. \mu q = \text{Some } (\text{Vote } (\text{Some } v)) \}$

shows $x ((\rho (\text{Suc } r)) p) = v$

Assume that HO and SHO sets are uniform at the second step of some phase. Then at the subsequent round there exists some value $v$ such that any received message which is not corrupted holds $v$.

**Lemma termination-argument-1:**
- **assumes** run: $\text{SHORun Ute-M } \rho \text{ HOsh SHOs}$
- and comm: $\text{SHOcommPerRd Ute-M } (\text{HOs } r) (\text{SHOs } r)$
- and $\text{stp: } \text{step } (\text{Suc } r) = \text{Suc } 0$
- and $\pi: \forall p. \pi 0 = \text{HOs } (\text{Suc } r) p$ $\land$ $\pi 0 = \text{SHOs } (\text{Suc } r) p$

obtains $v$ where

$\forall p \mu p' q.$

$[ q \in \text{SHOs } (\text{Suc } r) p \cap \text{HOs } (\text{Suc } r) p; \mu p' \in \text{SHOmsgVectors Ute-M } (\text{Suc } r) p (\rho (\text{Suc } r) p) (\text{HOs } (\text{Suc } r) p) (\text{SHOs } (\text{Suc } r) p)$

$\Rightarrow \mu p' q = (\text{Some } (\text{Val } v))$

If a process $p$ votes $v$ at some round $r$, then all messages received by $p$ in $r$ that are not corrupted hold $v$.

**Lemma termination-argument-2:**
assumes \( mup: \mu p \in \text{SHOmsgVectors Ute-M} (\text{Suc } r) \ p \ \rho (\text{Suc } r) \ p \)
\((\text{HOs} (\text{Suc } r) \ p) \ \rho (\text{SHO} (\text{Suc } r) \ p) \)
and \( \text{nxtq}: \text{nextState Ute-M} r \ q \ \rho (\text{Suc } r) \ q \ \mu q (\text{Suc } r) \ q \)
and \( \text{vq}: \text{vote} (\rho (\text{Suc } r) \ q) = \text{Some } v \)
and \( \text{qsho}: q \in \text{SHO} (\text{Suc } r) \ p \ \cap \text{HO} (\text{Suc } r) \ p \)
shows \( \mu p q = \text{Some } (\text{Vote} \ (\text{Some } v)) \)

\( \text{⟨proof} \rangle \)

We now prove the Termination property.

\textbf{theorem} ute-termination:
assumes \( \text{run}: \text{SHORun Ute-M} \ \rho \ \text{HOs} \ \text{SHOs} \)
and \( \text{commR}: \forall r. \text{SHOcommPerRd Ute-M} \ (\text{HOs } r) \ (\text{SHOs } r) \)
and \( \text{commG}: \text{SHOcommGlobal Ute-M} \ \text{HOs} \ \text{SHOs} \)
shows \( \exists r \ v. \ \text{decide} \ (\rho r p) = \text{Some } v \)
\( \text{⟨proof} \rangle \)

\(8.7\ \mathcal{U}_{T,E,\alpha} \text{ Solves Weak Consensus} \)

Summing up, all (coarse-grained) runs of \( \mathcal{U}_{T,E,\alpha} \) for HO and SHO collections that satisfy the communication predicate satisfy the Weak Consensus property.

\textbf{theorem} ute-weak-consensus:
assumes \( \text{run}: \text{SHORun Ute-M} \ \rho \ \text{HOs} \ \text{SHOs} \)
and \( \text{commR}: \forall r. \text{SHOcommPerRd Ute-M} \ (\text{HOs } r) \ (\text{SHOs } r) \)
and \( \text{commG}: \text{SHOcommGlobal Ute-M} \ \text{HOs} \ \text{SHOs} \)
shows \( \text{weak-consensus} (x \circ (\rho 0)) \ \text{decide } \rho \)
\( \text{⟨proof} \rangle \)

By the reduction theorem, the correctness of the algorithm carries over to the fine-grained model of runs.

\textbf{theorem} ute-weak-consensus-fg:
assumes \( \text{run}: \text{fg-run Ute-M} \ \rho \ \text{HOs} \ \text{SHOs} (\lambda r q. \text{undefined}) \)
and \( \text{commR}: \forall r. \text{SHOcommPerRd Ute-M} \ (\text{HOs } r) \ (\text{SHOs } r) \)
and \( \text{commG}: \text{SHOcommGlobal Ute-M} \ \text{HOs} \ \text{SHOs} \)
shows \( \text{weak-consensus} (\lambda p. x (\text{state}(\rho 0) p)) \ \text{decide } (\text{state } \circ \rho) \)
\( \text{(is weak-consensus ?inits - -)} \)
\( \text{⟨proof} \rangle \)

\( \text{end} \quad \text{— context ute-parameters} \)
\( \text{end} \)
\textbf{theory} AteDefs
\textbf{imports} ../HOModel
\textbf{begin}
9 Verification of the $\mathcal{A}_{T,E,\alpha}$ Consensus algorithm

Algorithm $\mathcal{A}_{T,E,\alpha}$ is presented in [3]. Like $\mathcal{U}_{T,E,\alpha}$, it is an uncoordinated algorithm that tolerates value faults, and it is parameterized by values $T$, $E$, and $\alpha$ that serve a similar function as in $\mathcal{U}_{T,E,\alpha}$, allowing the algorithm to be adapted to the characteristics of different systems. $\mathcal{A}_{T,E,\alpha}$ can be understood as a variant of OneThirdRule tolerating Byzantine faults.

We formalize in Isabelle the correctness proof of the algorithm that appears in [3], using the framework of theory $\text{HOModel}$.

9.1 Model of the Algorithm

We begin by introducing an anonymous type of processes of finite cardinality that will instantiate the type variable `$\text{proc}$` of the generic HO model.

\begin{verbatim}
typedecl Proc — the set of processes
axiomatization where Proc-finite: OFCLASS(Proc, finite-class)
instance Proc :: finite ⟨proof⟩

abbreviation
  $N \equiv \text{card} \ (\text{UNIV}::\text{Proc \ set})$ — number of processes

The following record models the local state of a process.

record $\text{'val \ pstate}$
  $x :: \text{'val}$ — current value held by process
  decide :: $\text{'val \ option}$ — value the process has decided on, if any

The $x$ field of the initial state is unconstrained, but no decision has yet been taken.

definition $\text{Ate-initState}$ where
  $\text{Ate-initState \ p \ st} \equiv (\text{decide \ st} = \text{None})$

The following locale introduces the parameters used for the $\mathcal{A}_{T,E,\alpha}$ algorithm and their constraints [3].

locale $\text{ate-parameters}$ =
  fixes $\alpha :: \text{nat}$ and $T :: \text{nat}$ and $E :: \text{nat}$
  assumes $\text{TNaE:} T \geq 2 * (N + 2 * \alpha - E)$
    and $\text{TNtN:} T < N$
    and $\text{EtN:} E < N$

begin

The following are consequences of the assumptions on the parameters.

lemma $\text{majE:} 2 * (E - \alpha) \geq N$
⟨proof⟩

lemma $\text{Egta:} E > \alpha$

59
\[ \text{proof} \]

**Lemma Tge2a**: \( T \geq 2 \ast \alpha \)

\[ \text{proof} \]

At every round, each process sends its current \( x \). If it received more than \( T \) messages, it selects the smallest value and store it in \( x \). As in algorithm *OneThirdRule*, we therefore require values to be linearly ordered.

If more than \( E \) messages holding the same value are received, the process decides that value.

**Definition** *mostOftenRcvd* where

\[
\text{mostOftenRcvd} \text{ (msgs::Proc } \Rightarrow \text{ 'val option) } \equiv \\
\{ v. \forall w. \text{ card } \{ qq. \text{ msgs qq } = \text{ Some } w \} \leq \text{ card } \{ qq. \text{ msgs qq } = \text{ Some } v \}\}
\]

**Definition**

\[ \text{Ate-sendMsg :: nat } \Rightarrow \text{ Proc } \Rightarrow \text{ Proc } \Rightarrow \text{ 'val pstate } \Rightarrow \text{ 'val} \]

\[ \text{where} \]

\[ \text{Ate-sendMsg r p q st } \equiv x st \]

**Definition**

\[ \text{Ate-nextState :: nat } \Rightarrow \text{ Proc } \Rightarrow (\text{'val::linorder } \text{ pstate } \Rightarrow (\text{Proc } \Rightarrow \text{'val option}) } \Rightarrow \text{'val pstate } \Rightarrow \text{ bool} \]

\[ \text{where} \]

\[ \text{Ate-nextState r p st msgs st’ } \equiv \]

\[ \text{if card } \{ q. \text{ msgs q } \neq \text{ None} \} > T \]

\[ \text{then } x st’ = \text{Min } (\text{mostOftenRcvd msgs}) \]

\[ \text{else } x st’ = x st \]

\[ \wedge (\exists v. \text{ card } \{ q. \text{ msgs q } = \text{ Some } v \} > E \wedge \text{decide st’ } = \text{Some } v) \]

\[ \vee \neg (\exists v. \text{ card } \{ q. \text{ msgs q } = \text{ Some } v \} > E) \]

\[ \wedge \text{decide st’ } = \text{decide st} \]

### 9.2 Communication Predicate for \( A_{T,E,\alpha} \)

Following [3], we now define the communication predicate for the \( A_{T,E,\alpha} \) algorithm. The round-by-round predicate requires that no process may receive more than \( \alpha \) corrupted messages at any round.

**Definition** *Ate-commPerRd* where

\[ \text{Ate-commPerRd HOrs SHOrs } \equiv \]

\[ \forall p. \text{ card } (\text{HOrs p } - \text{SHOrs p}) \leq \alpha \]

The global communication predicate stipulates the three following conditions:

- for every process \( p \) there are infinitely many rounds where \( p \) receives more than \( T \) messages,
- for every process \( p \) there are infinitely many rounds where \( p \) receives more than \( E \) uncorrupted messages,
• and there are infinitely many rounds in which more than $E - \alpha$ processes receive uncorrupted messages from the same set of processes, which contains more than $T$ processes.

**definition**

\[ \text{Ate-commGlobal where} \]

\[ \text{Ate-commGlobal HOs SHOs} \equiv \]

\[ (\forall r p. \exists r' > r. \text{card (HOs } r' p) > T) \]
\[ \land (\forall r p. \exists r' > r. \text{card (SHOs } r' p \cap \text{HOs } r' p) > E) \]
\[ \land (\forall r. \exists r' > r. \exists \pi_1 \pi_2. \]
\[ \text{card } \pi_1 > E - \alpha \]
\[ \land \text{card } \pi_2 > T \]
\[ \land (\forall p \in \pi_1. \text{HOs } r' p = \pi_2 \land \text{SHOs } r' p \cap \text{HOs } r' p = \pi_2) \]

**9.3 The $\mathcal{A}_{T,E,\alpha}$ Heard-Of Machine**

We now define the non-coordinated SHO machine for the $\mathcal{A}_{T,E,\alpha}$ algorithm by assembling the algorithm definition and its communication-predicate.

**definition** \( \text{Ate-SHOMachine where} \)

\( \text{Ate-SHOMachine} = (\lambda C \text{initState} = (\lambda p \text{ st crd. Ate-initState } p (\text{st::('val::linorder) pstate})), \text{sendMsg} = \text{Ate-sendMsg}, \text{CnextState} = (\lambda r p \text{ st msgs crd st'}. \text{Ate-nextState } r p \text{ st msgs st'}), \text{SHOcommPerRd} = (\text{Ate-commPerRd:: Proc HO } \Rightarrow \text{Proc HO } \Rightarrow \text{bool}), \text{SHOcommGlobal} = \text{Ate-commGlobal}) \)

**abbreviation**

\( \text{Ate-M} \equiv (\text{Ate-SHOMachine::(Proc, 'val::linorder pstate, 'val) SHOMachine}) \)

end — locale \( \text{ate-parameters} \)

end
t
do
t
theory \( \text{AteProof} \)
imports \( \text{AteDefs } ..\text{/Reduction} \)
begind
context \( \text{ate-parameters} \)
begind

**9.4 Preliminary Lemmas**

If a process newly decides value \( v \) at some round, then it received more than \( E - \alpha \) messages holding \( v \) at this round.

**lemma** \( \text{decide-sent-msgs-threshold} : \)
  assumes \( \text{run: SHORun } \text{Ate-M } \rho \text{ HOs SHOs} \)
  and \( \text{comm: SHOcommPerRd } \text{Ate-M} (\text{HOs } r) (\text{SHOs } r) \)

61
and \( \text{wvp}: \text{decide} (\rho \ r \ p) \neq \text{Some} \ v \)
and \( \text{vvp}: \text{decide} (\rho \ (\text{Suc} \ r) \ p) = \text{Some} \ v \)
shows \( \text{card} \ \{q.\ \text{sendMsg} \ \text{Ate-M} \ r \ qq \ p (\rho \ r \ qq) = v\} > E - \alpha \)
\( \langle \text{proof} \rangle \)

If more than \( E - \alpha \) processes send a value \( v \) to some process \( q \) at some round, then \( q \) will receive at least \( N + 2*\alpha - E \) messages holding \( v \) at this round.

lemma \( \text{other-values-received}: \)
assumes \( \text{comm}: \text{SHOcommPerRd} \ Ate-M \ (\text{HOs} \ r) \ (\text{SHOs} \ r) \)
and \( \text{nxt}: \text{nextState} \ Ate-M \ r \ q \ (\rho \ r \ q) \ \mu q \ ((\rho \ (\text{Suc} \ r)) \ q) \)
and \( \text{muq}: \mu q \in \text{SHOmsgVectors} \ Ate-M \ r \ q \ (\rho \ r) \ (\text{HOs} \ r \ q) \ (\text{SHOs} \ r \ q) \)
and \( \text{vsent}: \text{card} \ \{q.\ \text{sendMsg} \ Ate-M \ r \ qq \ q (\rho \ r \ qq) = v\} > E - \alpha \)
(\( \text{is} \ \text{card} \ ?\text{vsent} > -\))
shows \( \text{card} \ \{(q.\ \mu q \ qq \neq \text{Some} \ v) \cap \text{HOs} \ r \ qq\} \leq N + 2*\alpha - E \)
\( \langle \text{proof} \rangle \)

If more than \( E - \alpha \) processes send a value \( v \) to some process \( q \) at some round \( r \), and if \( q \) receives more than \( T \) messages in \( r \), then \( v \) is the most frequently received value by \( q \) in \( r \).

lemma \( \text{mostOftenRcvd-v}: \)
assumes \( \text{comm}: \text{SHOcommPerRd} \ Ate-M \ (\text{HOs} \ r) \ (\text{SHOs} \ r) \)
and \( \text{nxt}: \text{nextState} \ Ate-M \ r \ q \ (\rho \ r \ q) \ \mu q \ ((\rho \ (\text{Suc} \ r)) \ q) \)
and \( \text{muq}: \mu q \in \text{SHOmsgVectors} \ Ate-M \ r \ q \ (\rho \ r) \ (\text{HOs} \ r \ q) \ (\text{SHOs} \ r \ q) \)
and \( \text{threshold-T}: \text{card} \ \{q.\ \mu q \ qq \neq \text{None}\} > T \)
and \( \text{threshold-E}: \text{card} \ \{q.\ \text{sendMsg} \ Ate-M \ r \ qq \ q (\rho \ r \ qq) = v\} > E - \alpha \)
shows \( \text{mostOftenRcvd} \ \mu q = \{v\} \)
\( \langle \text{proof} \rangle \)

If at some round more than \( E - \alpha \) processes have their \( x \) variable set to \( v \), then this is also true at next round.

lemma \( \text{common-x-induct}: \)
assumes \( \text{run}: \text{SHORun} \ Ate-M \ \rho \ \text{HOs} \ \text{SHOs} \)
and \( \text{comm}: \text{SHOcommPerRd} \ Ate-M \ (\text{HOs} \ (r+k)) \ (\text{SHOs} \ (r+k)) \)
and \( \text{dh}: \text{card} \ \{qq.\ x \ (\rho \ (r + k) \ qq) = v\} > E - \alpha \)
shows \( \text{card} \ \{qq.\ x \ (\rho \ (r + \text{Suc} \ k) \ qq) = v\} > E - \alpha \)
\( \langle \text{proof} \rangle \)

Whenever some process newly decides value \( v \), then any process that updates its \( x \) variable will set it to \( v \).

lemma \( \text{common-x}: \)
assumes \( \text{run}: \text{SHORun} \ Ate-M \ \rho \ \text{HOs} \ \text{SHOs} \)
and \( \text{comm}: \forall \ r. \ \text{SHOcommPerRd} \ (\text{Ate-M::}(\text{Proc}, \text{val::linorder pstate}, \text{val}) \ \text{SHOMachine}) \)
\( \ (\text{HOs} \ r) \ (\text{SHOs} \ r) \)
and \( \text{d1}: \text{decide} (\rho \ r \ p) \neq \text{Some} \ v \)
and \( \text{d2}: \text{decide} (\rho \ (\text{Suc} \ r) \ p) = \text{Some} \ v \)
and \( \text{update}: \ x \ (\rho \ (r + \text{Suc} \ k) \ q) \neq x \ (\rho \ (r + k) \ q) \)

62
\[ x (\rho (r + \text{Suc} k) q) = v \]

(proof)

A process that holds some decision \( v \) has decided \( v \) sometime in the past.

\textbf{lemma} \( \text{decisionNonNullThenDecided} \):
\begin{align*}
\text{assumes} \quad & \text{run: SHORun Ate-M \ rho \ HOs SHOs} \\
\text{and} \quad & \text{dec: decide (\rho n p) = Some v}
\end{align*}
\begin{align*}
\text{obtains} \quad & m \quad \text{where} \quad m < n \\
\text{and} \quad & \text{decide (\rho m p) \neq Some v} \\
\text{and} \quad & \text{decide (\rho (\text{Suc} m) p) = Some v}
\end{align*}

(proof)

\section*{9.5 Proof of Validity}

Validity asserts that if all processes were initialized with the same value, then no other value may ever be decided.

\textbf{theorem} \( \text{ate-validity} \):
\begin{align*}
\text{assumes} \quad & \text{run: SHORun Ate-M \ rho \ HOs SHOs} \\
\text{and} \quad & \text{comm:} \forall r. \ SHOcommPerRd Ate-M (\text{HOs} r) (\text{SHOs} r) \\
\text{and} \quad & \text{init:} \forall q. \ x (\rho 0 q) = v \\
\text{and} \quad & \text{dp:} \quad \text{decide (\rho r p) = Some w}
\end{align*}
\begin{align*}
\text{shows} \quad & w = v
\end{align*}

(proof)

\section*{9.6 Proof of Agreement}

If two processes decide at the same round, they decide the same value.

\textbf{lemma} \( \text{common-decision} \):
\begin{align*}
\text{assumes} \quad & \text{run: SHORun Ate-M \ rho \ HOs SHOs} \\
\text{and} \quad & \text{comm:} \forall r. \ SHOcommPerRd Ate-M (\text{HOs} r) (\text{SHOs} r) \\
\text{and} \quad & \text{ndp:} \quad \text{decide (\rho r p) \neq Some v} \\
\text{and} \quad & \text{dvp:} \quad \text{decide (\rho (\text{Suc} r) p) = Some v} \\
\text{and} \quad & \text{ndq:} \quad \text{decide (\rho r q) \neq Some w} \\
\text{and} \quad & \text{dwp:} \quad \text{decide (\rho (\text{Suc} r) q) = Some w}
\end{align*}
\begin{align*}
\text{shows} \quad & w = v
\end{align*}

(proof)

If process \( p \) decides at step \( r \) and process \( q \) decides at some later step \( r+k \) then \( p \) and \( q \) decide the same value.

\textbf{lemma} \( \text{laterProcessDecidesSameValue} \):
\begin{align*}
\text{assumes} \quad & \text{run: SHORun Ate-M \ rho \ HOs SHOs} \\
\text{and} \quad & \text{comm:} \forall r. \ SHOcommPerRd Ate-M (\text{HOs} r) (\text{SHOs} r) \\
\text{and} \quad & \text{nd1:} \quad \text{decide (\rho r p) \neq Some v} \\
\text{and} \quad & \text{d1:} \quad \text{decide (\rho (\text{Suc} r) p) = Some v} \\
\text{and} \quad & \text{nd2:} \quad \text{decide (\rho (r+k) q) \neq Some w} \\
\text{and} \quad & \text{d2:} \quad \text{decide (\rho (\text{Suc} (r+k)) q) = Some w}
\end{align*}
\begin{align*}
\text{shows} \quad & w = v
\end{align*}
The Agreement property is now an immediate consequence.

\[ \text{theorem } \text{ate-agreement}: \]
\[ \begin{align*}
  \text{assumes } & \text{run: } \text{SHORun } \text{Ate-M } \rho \text{ HO}s \text{ SHO}s \\
  \text{and } & \text{comm: } \forall r. \text{ SHOcommPerRd } \text{Ate-M } (\text{HOs } r) \ (\text{SHO}s \ r) \\
  \text{and } & p: \text{ decide } (\rho \ m \ p) = \text{Some } v \\
  \text{and } & q: \text{ decide } (\rho \ n \ q) = \text{Some } w \\
  \text{shows } & w = v
\end{align*} \]

\[ \langle \text{proof} \rangle \]

9.7 Proof of Termination

We now prove that every process must eventually decide, given the global and round-by-round communication predicates.

\[ \text{theorem } \text{ate-termination}: \]
\[ \begin{align*}
  \text{assumes } & \text{run: } \text{SHORun } \text{Ate-M } \rho \text{ HO}s \text{ SHO}s \\
  \text{and } & \text{commR: } \forall r. (\text{SHOcommPerRd}::((\text{Proc}, \text{'val::linorder pstate, 'val}) \text{SHOMachine})) \\
    & \Rightarrow (\text{Proc } \text{HO}) \Rightarrow (\text{Proc } \text{HO}) \Rightarrow \text{bool} \\
  \text{and } & \text{commG: } \text{SHOcommGlobal } \text{Ate-M } \text{HO}s \text{ SHO}s \\
  \text{shows } & \exists r \ v. \text{ decide } (\rho \ r \ p) = \text{Some } v
\end{align*} \]

\[ \langle \text{proof} \rangle \]

9.8 \( \mathcal{A}_{T,E,\alpha} \) Solves Weak Consensus

Summing up, all (coarse-grained) runs of \( \mathcal{A}_{T,E,\alpha} \) for HO and SHO collections that satisfy the communication predicate satisfy the Weak Consensus property.

\[ \text{theorem } \text{ate-weak-consensus}: \]
\[ \begin{align*}
  \text{assumes } & \text{run: } \text{SHORun } \text{Ate-M } \rho \text{ HO}s \text{ SHO}s \\
  \text{and } & \text{commR: } \forall r. \text{ SHOcommPerRd } \text{Ate-M } (\text{HOs } r) \ (\text{SHO}s \ r) \\
  \text{and } & \text{commG: } \text{SHOcommGlobal } \text{Ate-M } \text{HO}s \text{ SHO}s \\
  \text{shows } & \text{weak-consensus } (x \circ (\rho \ 0)) \text{ decide } \rho
\end{align*} \]

\[ \langle \text{proof} \rangle \]

By the reduction theorem, the correctness of the algorithm carries over to the fine-grained model of runs.

\[ \text{theorem } \text{ate-weak-consensus-fg}: \]
\[ \begin{align*}
  \text{assumes } & \text{run: } \text{fg-run } \text{Ate-M } \rho \text{ HO}s \text{ SHO}s \ (\lambda r. q. \text{undefined}) \\
  \text{and } & \text{commR: } \forall r. \text{ SHOcommPerRd } \text{Ate-M } (\text{HOs } r) \ (\text{SHO}s \ r) \\
  \text{and } & \text{commG: } \text{SHOcommGlobal } \text{Ate-M } \text{HO}s \text{ SHO}s \\
  \text{shows } & \text{weak-consensus } (\lambda p. x \ (\text{state } (\rho \ 0) \ p)) \text{ decide } (\text{state } \circ \rho) \\
    & \text{is } \text{weak-consensus } ?\text{init}ls \ -
\end{align*} \]

\[ \langle \text{proof} \rangle \]
10 Verification of the \( EIGByz_f \) Consensus Algorithm

Lynch [12] presents \( EIGByz_f \), a version of the exponential information gathering algorithm tolerating Byzantine faults, that works in \( f \) rounds, and that was originally introduced in [1].

We begin by introducing an anonymous type of processes of finite cardinality that will instantiate the type variable \( 'proc \) of the generic HO model.

\textbf{typedecl} Proc — the set of processes

\textbf{axiomatization where} Proc-finite: OFCLASS(Proc, finite-class)

\textbf{instance} Proc :: finite \langle proof \rangle

\textbf{abbreviation}

\( N \equiv \text{card (UNIV::Proc set)} \) — number of processes

The algorithm is parameterized by \( f \), which represents the number of rounds and the height of the tree data structure (see below).

\textbf{axiomatization} \( f :: \text{nat} \)
\textbf{where} \( f < N \)

10.1 Tree Data Structure

The algorithm relies on propagating information about the initially proposed values among all the processes. This information is stored in trees whose branches are labeled by lists of (distinct) processes. For example, the interpretation of an entry \([p,q] \mapsto \text{Some } v\) is that the current process had heard from process \( q \) that it had heard from process \( p \) that its proposed value is \( v \). The value initially proposed by the process itself is stored at the root of the tree.

We introduce the type of \textit{labels}, which encapsulate lists of distinct process identifiers and whose length is at most \( f+1 \).

\textbf{definition} \( \text{Label = \{xs::Proc list. length xs \leq Suc f \land distinct xs\}} \)

\textbf{typedef} \( \text{Label = Label} \langle \text{proof} \rangle \)

There is a finite number of different labels.

\textbf{lemma} \( \text{finite-Label: finite Label} \)
\( \langle \text{proof} \rangle \)

\textbf{lemma finite-UNIV-Label:} finite \((\text{UNIV}::\text{Label set})\)
\(\langle \text{proof} \rangle \)

\textbf{lemma finite-Label-set [iff]:} finite \((S :: \text{Label set})\)
\(\langle \text{proof} \rangle \)

Utility functions on labels.

\textbf{definition root-node where}
\[ \text{root-node} \equiv \text{Abs-Label} [] \]

\textbf{definition length-lbl where}
\[ \text{length-lbl } l \equiv \text{length} \left( \text{Rep-Label } l \right) \]

\textbf{lemma length-lbl [intro]:} \(\text{length-lbl } l \leq \text{Suc } f\)
\(\langle \text{proof} \rangle \)

\textbf{definition is-leaf where}
\[ \text{is-leaf } l \equiv \text{length-lbl } l = \text{Suc } f \]

\textbf{definition last-lbl where}
\[ \text{last-lbl } l \equiv \text{last} \left( \text{Rep-Label } l \right) \]

\textbf{definition butlast-lbl where}
\[ \text{butlast-lbl } l \equiv \text{Abs-Label} \left( \text{butlast} \left( \text{Rep-Label } l \right) \right) \]

\textbf{definition set-lbl where}
\[ \text{set-lbl } l = \text{set} \left( \text{Rep-Label } l \right) \]

The children of a non-leaf label are all possible extensions of that label.

\textbf{definition children where}
\[ \text{children } l \equiv \]
\[ \text{if } \text{is-leaf } l \]
\[ \text{then } \{ \} \]
\[ \text{else } \{ \text{Abs-Label} \left( \text{Rep-Label } l \otimes [p] \right) | p \cdot p \notin \text{set-lbl } l \} \]

\subsection{10.2 Model of the Algorithm}

The following record models the local state of a process.

\textbf{record } 'val pstate =
\[ \text{vals :: Label } \Rightarrow '\text{val option} \]
\[ \text{newvals :: Label } \Rightarrow '\text{val} \]
\[ \text{decide :: 'val option} \]

Initially, no values are assigned to non-root labels, and an arbitrary value is assigned to the root: that value is interpreted as the initial proposal of the process. No decision has yet been taken, and the \textit{newvals} field is unconstrained.
\textbf{definition} \textit{EIG-initState} \textbf{where}
\[\text{EIG-initState } p \text{ st } \equiv \]
\[\forall l . \ (\text{vals st } l = \text{None}) = (l \neq \text{root-node}) \land \ \text{decide st } = \text{None}\]

\textbf{type-synonym} \begin{math} 'val \ Msg = Label \Rightarrow 'val \ option \end{math}

At every round, every process sends its current \textit{vals} tree to all processes. In fact, only the level of the tree corresponding to the round number is used (cf. definition of \textit{extend-vals} below).

\textbf{definition} \textit{EIG-sendMsg} \textbf{where}
\[\text{EIG-sendMsg } r \ p \ q \text{ st } \equiv \]

During the first \(f - 1\) rounds, every process extends its tree \textit{vals} according to the values received in the round. No decision is taken.

\textbf{definition} \textit{extend-vals} \textbf{where}
\[\text{extend-vals } r \ p \text{ st } \text{msgs st'} \equiv \]
\[\text{vals st'} = (\lambda l . \]
\[\text{if length-lbl } l = \text{Suc } r \land \text{msgs (last-lbl } l ) \neq \text{None} \]
\[\text{then (the (msgs (last-lbl } l ))) (\text{butlast-lbl } l ) \]
\[\text{else if length-lbl } l = \text{Suc } r \land \text{msgs (last-lbl } l ) = \text{None} \text{ then None} \]
\[\text{else vals st } l )\]

\textbf{definition} \textit{next-main} \textbf{where}
\[\text{next-main } r \ p \text{ st } \text{msgs st'} \equiv \text{extend-vals } r \ p \text{ st } \text{msgs st'} \land \text{decide st'} = \text{None}\]

In the final round, in addition to extending the tree as described previously, processes construct the tree \textit{newvals}, starting at the leaves. The values at the leaves are copied from \textit{vals}, except that missing values \textit{None} are replaced by the default value \textit{undefined}. Moving up, if there exists a majority value among the children, it is assigned to the parent node, otherwise the parent node receives the default value \textit{undefined}. The decision is set to the value computed for the root of the tree.

\textbf{fun} \textit{fixupval} :: \begin{math} 'val \ option \Rightarrow 'val \end{math}
\[\text{fixupval None } = \text{undefined} \|
\text{fixupval } (\text{Some } v ) = v\]

\textbf{definition} \textit{has-majority} :: \begin{math} 'val \Rightarrow (a \Rightarrow 'val) \Rightarrow 'a \ set \Rightarrow bool \end{math}
\[\text{has-majority } v \ g \ S \equiv \text{card } \{ e \in S . \ g \ e = v \} > (\text{card } S ) \text{ div } 2\]

\textbf{definition} \textit{check-newvals} :: \begin{math} 'val \ pstate \Rightarrow bool \end{math}
\[\text{check-newvals } st \equiv \]
\[\forall l . \ \text{is-leaf } l \land \text{newvals st } l = \text{fixupval } (\text{vals st } l) \land \]
\[\forall (\exists w . \ \text{has-majority } w \ (\text{newvals st }) \ (\text{children } l ) \land \text{newvals st } l = w) \land \]
\[\forall (\exists w . \ \text{has-majority } w \ (\text{newvals st }) \ (\text{children } l )) \land \]
\[\text{newvals st } l = \text{undefined})\]
The overall next-state relation is defined such that every process applies `nextMain` during rounds 0, . . . , \( f - 1 \), and applies `nextEnd` during round \( f \). After that, the algorithm terminates and nothing changes anymore.

**definition** \( EIG\text{-nextState} \) where

\[
EIG\text{-nextState} \ r \equiv
\begin{cases}
  \text{next-main} \ r & \text{if } r < f \\
  \text{next-end} \ r & \text{if } r = f \\
  \left( \lambda p \ st \ msgs \ st' . \ st' = st \right) & \text{else}
\end{cases}
\]

### 10.3 Communication Predicate for \( EIG\text{Byz}_f \)

The secure kernel \( SKr \) w.r.t. given HO and SHO collections consists of the process from which every process receives the correct message.

**definition** \( SKr : \text{Proc HO} \Rightarrow \text{Proc HO} \Rightarrow \text{Proc set} \) where

\[
SKr \ HO \ SHO \equiv \{ q . \forall p. \ q \in HO \ p \cap \ SHO \ p \}
\]

The secure kernel \( SK \) of an entire execution (i.e., for sequences of HO and SHO collections) is the intersection of the secure kernels for all rounds. Obviously, only the first \( f \) rounds really matter, since the algorithm terminates after that.

**definition** \( SK : (\text{nat} \Rightarrow \text{Proc HO}) \Rightarrow (\text{nat} \Rightarrow \text{Proc HO}) \Rightarrow \text{Proc set} \) where

\[
SK \ HOs \ SHOs \equiv \{ q . \forall r. \ q \in SKr (HOs \ r) (SHOs \ r) \}
\]

The round-by-round predicate requires that the secure kernel at every round contains more than \((N+f) \div 2\) processes.

**definition** \( EIG\text{-commPerRd} \) where

\[
EIG\text{-commPerRd} \ HO \ SHO \equiv \text{card} (SKr \ HO \ SHO) > (N + f) \div 2
\]

The global predicate requires that the secure kernel for the entire execution contains at least \( N - f \) processes. Messages from these processes are always correctly received by all processes.

**definition** \( EIG\text{-commGlobal} \) where

\[
EIG\text{-commGlobal} \ HOs \ SHOs \equiv \text{card} (SK \ HOs \ SHOs) \geq N - f
\]

The above communication predicates differ from Lynch’s presentation of \( EIG\text{Byz}_f \). In fact, the algorithm was originally designed for synchronous systems with reliable links and at most \( f \) faulty processes. In such a system, every process receives the correct message from at least the non-faulty processes at every round, and therefore the global predicate \( EIG\text{-commGlobal} \)
is satisfied. The standard correctness proof assumes that $N > 3f$, and therefore $N - f > (N + f) \div 2$. Since moreover, for any $r$, we obviously have
\[
\left( \bigcap_{p \in \Pi, r' \in \mathbb{N}} \text{SHO}(p, r') \right) \subseteq \left( \bigcap_{p \in \Pi} \text{SHO}(p, r) \right),
\]
it follows that any execution of $EIGByz_f$ where $N > 3f$ also satisfies $EIG\text{-commPerRd}$ at any round. The standard correctness hypotheses thus imply our communication predicates.

However, our proof shows that $EIGByz_f$ can indeed tolerate more transient faults than the standard bound can express. For example, consider the case where $N = 5$ and $f = 2$. Our predicates are satisfied in executions where two processes exhibit transient faults, but never fail simultaneously. Indeed, in such an execution, every process receives four correct messages at every round, hence $EIG\text{-commPerRd}$ always holds. Also, $EIG\text{-commGlobal}$ is satisfied because there are three processes from which every process receives the correct messages at all rounds. By our correctness proof, it follows that $EIGByz_f$ then achieves Consensus, unlike what one could expect from the standard correctness predicate. This observation underlines the interest of expressing assumptions about transient faults, as in the HO model.

### 10.4 The $EIGByz_f$ Heard-Of Machine

We now define the non-coordinated SHO machine for $EIGByz_f$ by assembling the algorithm definition and its communication-predicate.

**definition** $EIG\text{-SHOMachine}$ **where**

$EIG\text{-SHOMachine} = (\langle CinitState = (\lambda \ p \ st \ \text{crd}. \ EIG\text{-initState} \ p \ st), \hspace{1cm}
\text{sendMsg} = EIG\text{-sendMsg}, \hspace{1cm}
\text{CnextState} = (\lambda \ r \ p \ st \ \text{msgs} \ \text{crd} \ st'. \ EIG\text{-nextState} \ r \ p \ st \ \text{msgs} \ st'), \hspace{1cm}
\text{SHOcommPerRd} = EIG\text{-commPerRd}, \hspace{1cm}
\text{SHOcommGlobal} = EIG\text{-commGlobal} \rangle)$

**abbreviation** $EIG-M \equiv (EIG\text{-SHOMachine}::(\text{Proc}, 'val \ pstate, 'val \ Msg) \ SHOMachine)$

**end**

**theory** $EigbyzProof$

**imports** $EigbyzDefs .. Majorities .. Reduction$

**begin**

### 10.5 Preliminary Lemmas

Some technical lemmas about labels and trees.
lemma not-leaf-length:
  assumes l: ¬(is-leaf l)
  shows length-lbl l ≤ f

lemma nil-is-Label: [] ∈ Label

lemma card-set-lbl: card (set-lbl l) = length-lbl l

lemma Rep-Label-root-node [simp]: Rep-Label root-node = []

lemma root-node-length [simp]: length-lbl root-node = 0

lemma root-node-not-leaf: ¬(is-leaf root-node)

Removing the last element of a non-root label gives a label.

lemma butlast-rep-in-label:
  assumes l:l ≠ root-node
  shows butlast (Rep-Label l) ∈ Label

The label of a child is well-formed.

lemma Rep-Label-append:
  assumes l: ¬(is-leaf l)
  shows (Rep-Label l @ [p] ∈ Label) = (p ∉ set-lbl l)

The label of a child is the label of the parent, extended by a process.

lemma label-children:
  assumes c: c ∈ children l
  shows ∃ p. p ∉ set-lbl l ∧ Rep-Label c = Rep-Label l @ [p]

The label of any child node is one longer than the label of its parent.

lemma children-length:
  assumes l ∈ children h
  shows length-lbl l = Suc (length-lbl h)

The root node is never a child.

lemma children-not-root:
  assumes root-node ∈ children l
shows $P$

(proof)

The label of a child with the last element removed is the label of the parent.

**lemma** children-butlast-lbl:

assumes $c \in \text{children } l$

shows butlast-lbl $c = l$

(proof)

The root node is not a child, and it is the only such node.

**lemma** root-iff-no-child: $(l = \text{root-node}) = (\forall l'. l \notin \text{children } l')$

(proof)

If some label $l$ is not a leaf, then the set of processes that appear at the end of the labels of its children is the set of all processes that do not appear in $l$.

**lemma** children-last-set:

assumes $l: \neg (\text{is-leaf } l)$

shows last-lbl $'$ (children $l$) = \text{UNIV} - \text{set-lbl } l$

(proof)

The function returning the last element of a label is injective on the set of children of some given label.

**lemma** last-lbl-inj-on-children: inj-on last-lbl (children $l$)

(proof)

The number of children of any non-leaf label $l$ is the number of processes that do not appear in $l$.

**lemma** card-children:

assumes $\neg (\text{is-leaf } l)$

shows $\text{card} \ (\text{children } l) = N - \text{length-lbl } l$

(proof)

Suppose a non-root label $l'$ of length $r+1$ ending in $q$, and suppose that $q$ is well heard by process $p$ in round $r$. Then the value with which $p$ decorates $l$ is the one that $q$ associates to the parent of $l$.

**lemma** sho-correct-vals:

assumes run: SHORun EIG-M rho HOs SHOs

and $l': l' \in \text{children } l$

and shop: last-lbl $l' \in \text{SHOs} \ (\text{length-lbl } l) \ p \cap \text{HOs} \ (\text{length-lbl } l) \ p$

(is $?q \in \text{SHOs} \ (\text{?len } l) \ p \cap -$)

shows $\text{vals} \ (\text{rho} \ (\text{?len } l') \ p) \ l' = \text{vals} \ (\text{rho} \ (\text{?len } l) \ ?q) \ l$

(proof)

A process fixes the value $\text{vals } l$ of a label at state $\text{length-lbl } l$, and then never modifies the value.

**lemma** keep-vals:

assumes run: SHORun EIG-M rho HOs SHOs
shows \( vals(\rho(length-lbl l + n) p) l = vals(\rho(length-lbl l) p) l \)

\( (is \ ?v n = ?v) \)

\((proof)\)

### 10.6 Lynch’s Lemmas and Theorems

If some process is safely heard by all processes at round \( r \), then all processes agree on the value associated to labels of length \( r+1 \) ending in that process.

**Lemma Lynch-6-15:**

- **Assumes** run: \( SHORun\ EIG-M\ rho\ HOs\ SHOs \)
- and \( l': l' \in children l \)
- and skr: \( last-lbl l' \in SKr(HOs(length-lbl l))(SHOs(length-lbl l)) \)
- **Shows** \( vals(\rho(length-lbl l') p) l' = vals(\rho(length-lbl l) q) l' \)

\((proof)\)

Suppose that \( l \) is a non-root label whose last element was well heard by all processes at round \( r \), and that \( l' \) is a child of \( l \) corresponding to process \( q \) that is also well heard by all processes at round \( r+1 \). Then the values associated with \( l \) and \( l' \) by any process \( p \) are identical.

**Lemma Lynch-6-16-a:**

- **Assumes** run: \( SHORun\ EIG-M\ rho\ HOs\ SHOs \)
- and \( l: l \in children t \)
- and skrl: \( last-lbl l \in SKr(HOs(length-lbl t))(SHOs(length-lbl t)) \)
- and \( l': l' \in children l \)
- and skrl': \( last-lbl l' \in SKr(HOs(length-lbl l))(SHOs(length-lbl l)) \)
- **Shows** \( vals(\rho(length-lbl l') p) l' = vals(\rho(length-lbl l) p) l \)

\((proof)\)

For any non-leaf label \( l \), more than half of its children end with a process that is well heard by everyone at round \( length-lbl l \).

**Lemma Lynch-6-16-c:**

- **Assumes** \( commR: EIG-commPerRd(HOs(length-lbl l))(SHOs(length-lbl l)) \)
- and \( l: \neg(is-leaf l) \)
- **Shows** \( card\ \{l' \in children l. last-lbl l' \in SKr(HOs \ ?r) (SHOs \ ?r)\} > card\ (children l) \ div\ 2 \)

\((proof)\)

If \( l \) is a non-leaf label such that all of its children corresponding to well-heard processes at round \( length-lbl l \) have a uniform newvals decoration at round \( f+1 \), then \( l \) itself is decorated with that same value.

**Lemma newvals-skr-uniform:**

- **Assumes** run: \( SHORun\ EIG-M\ rho\ HOs\ SHOs \)
- and \( commR: EIG-commPerRd(HOs(length-lbl l))(SHOs(length-lbl l)) \)
- \( (is\ EIG-commPerRd(HOs \ ?r) -) \)
- and \( notleaf: \neg(is-leaf l) \)

72
and unif: ∃l′ ∈ children l. last-lbl l′ ∈ SKr (HOs (length-lbl t)) (SHOs (length-lbl t))
⇒ newvals (ρ (Suc f) p) l′ = v

shows newvals (ρ (Suc f) p) l = v
⟨proof⟩

A node whose label l ends with a process which is well heard at round length-lbl t will have its newvals field set (at round f + 1) to the “fixed-up” value given by vals.

lemma lynch-6-16-d:
assumes run: SHORun EIG-M ρ HOs SHOs
and commR: ∀r. EIG-commPerRd (HOs r) (SHOs r)
and notroot: l ∈ children t
and skr: last-lbl l ∈ SKr (HOs (length-lbl t)) (SHOs (length-lbl t))
(is - ∈ SKr (HOs (?len t)) -)
shows newvals (ρ (Suc f) p) l = fixupval (vals (ρ (?) p) l)
(is ?P l)
⟨proof⟩

Following Lynch [12], we introduce some more useful concepts for reasoning about the data structure.

A label is common if all processes agree on the final value it is decorated with.

definition common where
common ρ l ≡ ∀p q. newvals (ρ (Suc f) p) l = newvals (ρ (Suc f) q) l

The subtrees of a given label are all its possible extensions.

definition subtrees where
subtrees h ≡ {l. ∃t. Rep-Label l = (Rep-Label h) @ t}

lemma children-in-subtree:
assumes l ∈ children h
shows l ∈ subtrees h
⟨proof⟩

lemma subtrees-refl [iff]: l ∈ subtrees l
⟨proof⟩

lemma subtrees-root [iff]: l ∈ subtrees root-node
⟨proof⟩

lemma subtrees-trans:
assumes l'' ∈ subtrees l' and l' ∈ subtrees l
shows l'' ∈ subtrees l
⟨proof⟩

73
lemma subtrees-antisym:
assumes \( l \in \text{subtrees} \ l' \) and \( l' \in \text{subtrees} \ l \)
shows \( l' = l \)
(proof)

lemma subtrees-tree:
assumes \( l', l \in \text{subtrees} \ l' \) and \( l' \in \text{subtrees} \ l'' \)
shows \( l'' \in \text{subtrees} \ l' \) \( \lor \) \( l' \in \text{subtrees} \ l'' \)
(proof)

lemma subtrees-cases:
assumes \( l', l \in \text{subtrees} \ l \)
and \( \text{self} : l' = l \implies P \)
and \( \text{child} : \bigwedge_c. \left[ c \in \text{children} \ l; l' \in \text{subtrees} \ c \right] \implies P \)
shows \( P \)
(proof)

lemma subtrees-leaf:
assumes \( l : \text{is-leaf} \ l \) and \( l', l \in \text{subtrees} \ l \)
shows \( l' = l \)
(proof)

lemma children-subtrees-equal:
assumes \( c : c \in \text{children} \ l \) and \( c' : c' \in \text{children} \ l \)
and \( \text{sub} : c' \in \text{subtrees} \ c \)
shows \( c' = c \)
(proof)

A set \( C \) of labels is a subcovering w.r.t. label \( l \) if for all leaf subtrees \( s \) of \( l \) there exists some label \( h \in C \) such that \( s \) is a subtree of \( h \) and \( h \) is a subtree of \( l \).

definition subcovering where
subcovering \( C \ l \equiv \forall s \in \text{subtrees} \ l. \text{is-leaf} \ s \implies \left( \exists h \in C. h \in \text{subtrees} \ l \land s \in \text{subtrees} \ h \right) \right) \)

A covering is a subcovering w.r.t. the root node.

abbreviation covering where
covering \( C \equiv \text{subcovering} \ C \ \text{root-node} \)

The set of labels whose last element is well heard by all processes throughout the execution forms a covering, and all these labels are common.

lemma lynch-6-18-a:
assumes \( \text{SHORun} \ EIG-M \ rho \ HOs \ SHOs \)
and \( \forall r. \ EIG-\text{commPerRd} \ (HOs \ r) \ (SHOs \ r) \)
and \( l \in \text{children} \ t \)
and \( \text{last-lbl} \ l \in \text{SKr} \ (HOs \ (\text{length-lbl} \ t)) \ (SHOs \ (\text{length-lbl} \ t)) \)
shows \( \text{common} \ \rho \ l \)
(proof)
lemma lynch-6-18-b:
assumes run: SHORun EIG-M rho HOs SHOs
and commG: EIG-commGlobal HOs SHOs
and commR: \( \forall r. \) EIG-commPerRd (HOs r) (SHOs r)
shows covering \{l. \exists t. l \in children t \land last-lbl l \in (SK HOs SHOs)\}
⟨proof⟩

If \( C \) covers the subtree rooted at label \( l \) and if \( l \notin C \) then \( C \) also covers subtrees rooted at \( l \)'s children.

lemma lynch-6-19-a:
assumes cov: subcovering C l
and l: l \notin C
and e: e \in children l
shows subcovering C e
⟨proof⟩

If there is a subcovering \( C \) for a label \( l \) such that all labels in \( C \) are common, then \( l \) itself is common as well.

lemma lynch-6-19-b:
assumes run: SHORun EIG-M rho HOs SHOs
and cov: subcovering C l
and com: \( \forall l'. l' \in C. \) common rho l'
shows common rho l
⟨proof⟩

The root of the tree is a common node.

lemma lynch-6-20:
assumes run: SHORun EIG-M rho HOs SHOs
and commG: EIG-commGlobal HOs SHOs
and commR: \( \forall r. \) EIG-commPerRd (HOs r) (SHOs r)
shows common rho root-node
⟨proof⟩

A decision is taken only at state \( f+1 \) and then stays stable.

lemma decide:
assumes run: SHORun EIG-M rho HOs SHOs
shows decide (rho r p) =
(\text{if } r < \text{Suc } f \text{ then } \text{None}
  \text{else Some } (\text{newvals } (\text{rho } (\text{Suc } f) p) \text{ root-node}))
(\text{is } ?P r)
⟨proof⟩

10.7 Proof of Agreement, Validity, and Termination

The Agreement property is an immediate consequence of lemma lynch-6-20.

theorem Agreement:
assumes run: SHORun EIG-M ρho HOs SHOs
  and commG: EIG-commGlobal HOs SHOs
  and commR: ∀ r. EIG-commPerRd (HOs r) (SHOs r)
  and p: decide (ρho m p) = Some v
  and q: decide (ρho n q) = Some w
shows v = w
⟨proof⟩

We now show the Validity property: if all processes initially propose the same value v, then no other value may be decided.

By lemma sho-correct-vals, value v must propagate to all children of the root that are well heard at round 0, and lemma lynch-6-16-d implies that v is the value assigned to all these children by newvals. Finally, lemma newvals-skr-uniform lets us conclude.

theorem Validity:
  assumes run: SHORun EIG-M ρho HOs SHOs
  and commR: ∀ r. EIG-commPerRd (HOs r) (SHOs r)
  and initv: ∀ q. the (vals (ρho 0 q) root-node) = v
  and dp: decide (ρho r p) = Some w
shows v = w
⟨proof⟩

Termination is trivial for EIGByzf.

theorem Termination:
  assumes SHORun EIG-M ρho HOs SHOs
  shows ∃ r v. decide (ρho r p) = Some v
⟨proof⟩

10.8 EIGByzf Solves Weak Consensus

Summing up, all (coarse-grained) runs of EIGByzf for HO and SHO collections that satisfy the communication predicate satisfy the Weak Consensus property.

theorem eig-weak-consensus:
  assumes run: SHORun EIG-M ρho HOs SHOs
  and commR: ∀ r. EIG-commPerRd (HOs r) (SHOs r)
  and commG: EIG-commGlobal HOs SHOs
  shows weak-consensus (λp. the (vals (ρho 0 p) root-node)) decide ρho
⟨proof⟩

By the reduction theorem, the correctness of the algorithm carries over to the fine-grained model of runs.

theorem eig-weak-consensus-fg:
  assumes run: fg-run EIG-M ρho HOs SHOs (λx q. undefined)
  and commR: ∀ r. EIG-commPerRd (HOs r) (SHOs r)
  and commG: EIG-commGlobal HOs SHOs
  shows weak-consensus (λp. the (vals (state (ρho 0) p) root-node))
decide \( \text{state} \circ \rho \)

(is weak-consensus ?init - -)

⟨proof⟩

end

11 Conclusion

In this contribution we have formalized the Heard-Of model in the proof assistant Isabelle/HOL. We have established a formal framework, in which fault-tolerant distributed algorithms can be represented, and that caters for different variants (benign or malicious faults, coordinated and uncoordinated algorithms). We have formally proved a reduction theorem that relates fine-grained (asynchronous) interleaving executions and coarse-grained executions, in which an entire round constitutes the unit of atomicity. As a corollary, many correctness properties, including Consensus, can be transferred from the coarse-grained to the fine-grained representation.

We have applied this framework to give formal proofs in Isabelle/HOL for six different Consensus algorithms known from the literature. Thanks to the reduction theorem, it is enough to verify the algorithms over coarse-grained runs, and this keeps the effort manageable. For example, our LastVoting algorithm is similar to the DiskPaxos algorithm verified in [10], but our proof here is an order of magnitude shorter, although we prove safety and liveness properties, whereas only safety was considered in [10].

We also emphasize that the uniform characterization of fault assumptions via communication predicates in the HO model lets us consider the effects of transient failures, contrary to standard models that consider only permanent failures. For example, our correctness proof for the EIGByz algorithm establishes a stronger result than that claimed by the designers of the algorithm. The uniform presentation also paves the way towards comparing assumptions of different algorithms.

The encoding of the HO model as Isabelle/HOL theories is quite straightforward, and we find our Isar proofs quite readable, although they necessarily contain the full details that are often glossed over in textbook presentations. We believe that our framework allows algorithm designers to study different fault-tolerant distributed algorithms, their assumptions, and their proofs, in a clear, rigorous and uniform way.
References


