Proving the Correctness of Disk Paxos in Isabelle/HOL

Mauro Jaskelioff Stephan Merz

April 19, 2020

Abstract

Disk Paxos [GL00] is an algorithm for building arbitrary fault-tolerant distributed systems. The specification of Disk Paxos has been proved correct informally and tested using the TLC model checker, but up to now, it has never been fully formally verified. In this work we have formally verified its correctness using the Isabelle theorem prover and the HOL logic system [NPW02], showing that Isabelle is a practical tool for verifying properties of TLA+ specifications.

Contents

1 Introduction 2

2 The Disk Paxos Algorithm 3
   2.1 Informal description of the algorithm. 4
   2.2 Disk Paxos and its TLA+ Specification 4

3 Translating from TLA+ to Isabelle/HOL 6
   3.1 Typed vs. Untyped 6
   3.2 Primed Variables 8
   3.3 Restructuring the specification 8

4 Structure of the Correctness Proof 9
   4.1 Going from Informal Proofs to Formal Proofs 10

5 Conclusion 11

A TLA+ correctness specification 12

B Disk Paxos Algorithm Specification 13
1 Introduction

Algorithms for fault-tolerant distributed systems were first introduced to implement critical systems. Nevertheless, what good is such an algorithm if it has a design error? We need some kind of guarantee that the algorithm does not have a faulty design. Formal verification of its specification is one such guarantee.

Disk Paxos [GL00] is an algorithm for building arbitrary fault-tolerant distributed systems, that, due to its complexity, is difficult to reason about. It has been proved correct informally, and tested using the TLC model checker [Lam02]. The informal proof is rigorous but, as it is always the case with large informal proofs, it is easy to overlook details. Thus, one of the motivations of this work is to see if such a rigorous proof can be formalized in a contemporary theorem prover.

In [Pac01] part of the correctness proof (invariance of $HInv_1$ and $HInv_3$) was verified using the theorem prover ACL2 [KMM00]. An implicit assumption of this formalization is that all sets are finite, thus overlooking the fact that there is a missing conjunct in the Disk Paxos invariant (see Section 4).

We set the goal of formally verifying Disk Paxos correctness using the theorem prover Isabelle/HOL [NPW02]. In this way, we could gain more confidence in the correctness of Disk Paxos design and, at the same time, learn to what extent can Isabelle be a useful tool for proving the correctness of distributed systems using a real world example.
In Section 2 we give a brief description of the algorithm and its specification. In Section 3 we describe the translation from TLA+ to Isabelle/HOL and the problems that this translation originated. In Section 4 we discuss how our formal proofs relate to the informal ones in [GL00], and in Section 5 we conclude. The entire specification and all formal proofs can be found in the Appendix.

2 The Disk Paxos Algorithm

Disk Paxos is a variant of the classic Paxos algorithm [Lam98] for the implementation of arbitrary fault-tolerant systems with a network of processors and disks. It maintains consistency in the event of any number of non-Byzantine failures. This means that a processor may fail completely or pause for arbitrary long periods and then restart, remembering only that it has failed. A disk may become inaccessible to some or all processors, but it may not be corrupted. We say that a system is stable if all processes are either non-faulty or have failed completely (i.e. there are no new failed processes). Disk Paxos guarantees progress if the system is stable and there is at least one non-faulty processor that can read and write a majority of the disks. Consequently, the fundamental difference between Classic Paxos and Disk Paxos is that the former achieves redundancy by replicating processes while the latter replicates disks. Since disks are usually cheaper than processors, it is possible to obtain more redundancy at a lower cost.

Disk Paxos uses the state machine approach to solve the problem of implementing an arbitrary distributed system. The state machine approach [Sch90] is a general method that reduces this problem to solving a consensus problem. The distributed system is designed as a deterministic state machine that executes a sequence of commands, and a consensus algorithm ensures that, for each n, all processors agree on the n\textsuperscript{th} command. Hence, each processor p starts with an input value (a command), and it may output a value (the command to be executed). The problem is solved if all processors eventually output the same value and this value was a value of input[p] for some p (under certain assumptions, in our case that there exists at least one non-faulty processor that can write and read a majority of disks).

Progress of Disk Paxos relies on progress of a leader-election algorithm. It is easy to make a leader-election algorithm if the system stable, but very hard to devise one that works correctly even if the system is unstable. We are requiring stability to ensure progress, but actually only a weaker requirement is needed: progress of the underlying leader-election algorithm. Disk Paxos ensures that all outputs (if any) will be the same even if the leader-election algorithm fails.
2.1 Informal description of the algorithm.

The consensus algorithm of Disk Paxos is called Disk Synod. In it, each processor has an assigned block on each disk. Also it has a local memory that contains its current block (called the \textit{dblock}), and other state variables (see figure 1). When a process $p$ starts it contains an input value $input[p]$ that will not be modified, except possibly when recovering from a failure.

Disk Synod is structured in two phases, plus one more phase for recovering from failures. In each phase, a processor writes its own block and reads each other processor’s block, on a majority of the disks. The idea is to execute ballots to determine:

\textbf{Phase 1:} whether a processor $p$ can choose its own input value $input[p]$ or must choose some other value. When this phase finishes a value $v$ is chosen.

\textbf{Phase 2:} whether it can commit $v$. When this phase is complete the process has committed value $v$ and can output it (using variable \textit{outpt}).

In either phase, a processor aborts its ballot if it learns that another processor has begun a higher-numbered ballot. The third phase (Phase 0) is for starting the algorithm or recovering from a failure.

In each block, processors maintain three values:

- \textbf{mbal} The current ballot number.
- \textbf{bal} The largest ballot number for which the processor entered phase 2.
- \textbf{inp} The value the processor tried to commit in ballot number \textit{bal}.

For a complete description of the algorithm, see [GL00].

2.2 Disk Paxos and its TLA$^+$ Specification

The specification of Disk Paxos is written in the TLA$^+$ specification language [Lam02]. As it is usual with TLA$^+$, the specification is organized into modules.

The specification of consensus is given in module \textit{Synod}, which can be found in appendix A. In it there are only two variables: \textit{input} and \textit{output}. To formalize the property stating that all processors should choose the same value and that this value should have been an input of a processor, we need variables that represent all past inputs and the value chosen as result. Consequently, an \textit{Inner} submodule is introduced, which adds two variables: \textit{allInput} and \textit{chosen}. Our \textit{Synod} module will be obtained by existentially quantifying these variables of the \textit{Inner} module.

The specification of the algorithm is given in the \textit{HDiskSynod} module. Hence, what we are going to prove is that the (translation to Isabelle/HOL
of the) Inner module is implied by the (translation to Isabelle/HOL of the) algorithm module \textit{HDiskSynod}.

More concretely we have that the specification of the algorithm is:

\[
\text{HDiskSynodSpec} \triangleq HInit \land \square[HNext]_{\langle\text{vars, chosen, allInput}\rangle}
\]

where \textit{HInit} describes the initial state of the algorithm and \textit{HNext} is the action that models all of its state transitions. The variable \textit{vars} is the tuple of all variables used in the algorithm.

Analogously, we have the specification of the Inner module:

\[
\text{ISpec} \triangleq IInit \land \square[INext]_{\langle\text{input, output, chosen, allInput}\rangle}
\]

We define \textit{ivars} = \langle input, output, chosen, allInput \rangle. In order to prove that \textit{HDiskSynodSpec} implies \textit{ISpec}, we follow the structure of the proof given by Gafni and Lamport. We must prove two theorems:

\textbf{THEOREM} R1 \quad HInit \Rightarrow IInit

\textbf{THEOREM} R2 \quad HInit \land \square[HNext]_{\langle\text{vars, chosen, allInput}\rangle} \Rightarrow \square[INext]_{\text{ivars}}

The proof of R1 is trivial. For R2, we use TLA proof rules [Lam02] that show that to prove R2, it suffices to find a state predicate \textit{HInv} for which we can prove:

\textbf{THEOREM} R2a \quad HInit \land \square[HNext]_{\langle\text{vars, chosen, allInput}\rangle} \Rightarrow \Box[HInv]

\textbf{THEOREM} R2b \quad HInv \land HInv' \land HNext \Rightarrow INext \lor (\text{UNCHANGED ivars})

A predicate satisfying \textit{HInv} is said to be an invariant of \textit{HDiskSynodSpec}. To prove R2a, we make \textit{HInv} strong enough to satisfy:
Again, we have TLA proof rules that say that $I_1$ and $I_2$ imply $R2a$. In summary, $R2b$, $I_1$, and $I_2$ together imply $HDiskSynodSpec \Rightarrow ISpec$.

Finding a predicate $HInv$ that is strong enough can be rather difficult. Fortunately, Gafni and Lamport give this predicate. In their paper, they present $HInv$ as a conjunction of 6 predicates $HInv_1, \ldots, HInv_6$, where $HInv_1$ is a simple “type invariant” and the higher-numbered predicates add more and more information. The proof is structured such that the preservation of $HInv_i$ by the algorithm’s next-state relation relies on all $HInv_j$ (for $j \leq i$) being true in the state before the transition. In our proofs we are going to use exactly the same tactic.

Before starting our proofs we have to translate all the specification and theorems above into the formal language of Isabelle/HOL.

### 3 Translating from TLA+ to Isabelle/HOL

The translation from TLA+ to Isabelle/HOL is pretty straightforward as Isabelle/HOL has equivalent counterparts for most of the constructs in TLA+ (some representative examples are shown in table 1). Nevertheless, there are some semantic discrepancies. In the following, we discuss these differences, some of the options that one has when dealing with them, and the reasons for our choices\textsuperscript{1}.

#### 3.1 Typed vs. Untyped

TLA+ is an untyped formalism. However, TLA+ specifications usually have some type information, usually in the form of set membership or set inclusion. When translating these specifications to Isabelle/HOL, which is a typed formalism, one has to invent types that represent these sets of values.

\textsuperscript{1}There is no point in using the existing TLA encoding in Isabelle. Since the encoding is also based on HOL and we only prove safety, we would have gained nothing.
TLA⁺:

\begin{align*}
\text{CONSTANT } & \text{Inputs} \\
\text{NotAnInput} & \triangleq \text{CHOOSE } c : c \notin \text{Inputs} \\
\text{DiskBlock} & \triangleq [mbal : (\text{UNION Ballot}(p) : p \in \text{Proc}) \cup \{0\}, \\
& \quad bal : (\text{UNION Ballot}(p) : p \in \text{Proc}) \cup \{0\}, \\
& \quad inp : \text{Inputs} \cup \{\text{NotAnInput}\}] \\
\end{align*}

Isabelle/HOL:

\texttt{typedef \textit{InputsOrNi}}

\texttt{consts}

\begin{align*}
\text{Inputs} & :: \textit{InputsOrNi} \text{ set} \\
\text{NotAnInput} & :: \textit{InputsOrNi} \\
\end{align*}

\texttt{axioms}

\begin{align*}
\textit{NotAnInput}: \text{NotAnInput} \notin \textit{Inputs} \\
\textit{InputsOrNi}: (\text{UNIV} :: \textit{InputsOrNi} \text{ set}) = \textit{Inputs} \cup \{\text{NotAnInput}\} \\
\end{align*}

\texttt{record}

\begin{align*}
\text{DiskBlock} = \\
\quad mbal :: \text{nat} \\
\quad bal :: \text{nat} \\
\quad inp :: \textit{InputsOrNi} \\
\end{align*}

Figure 2: Untyped TLA⁺ vs. Typed Isabelle/HOL

This process is not automatic and requires some thought to find the right abstractions. Furthermore, simple types may not be expressive enough to represent exactly the set in the specification. In some cases, these sets could be modelled by algebraic datatypes, but this would make the specification more complex and less directly related to the original one. In this work, we have chosen to stick to simple types and add additional axioms to account for their lack of expressiveness.

For example, see figure 2. The type \textit{InputsOrNi} models the members of the set \textit{Inputs}, and the element \textit{NotAnInput}. We record the fact that \textit{NotAnInput} is not in \textit{Inputs}, with axiom \textit{NotAnInput}. Now, looking at the type of the \textit{inp} field of the \textit{DiskBlock} record in the TLA⁺ specification, we see that its type should be \textit{InputsOrNi}. However, this is not the same type as \textit{Inputs} \cup \{\textit{NotAnInput}\}, as nothing prevents the \textit{InputsOrNi} type from having more values. Consequently, we add the axiom \textit{InputsOrNi} to establish that the only values of this type are the ones in \textit{Inputs} and \textit{NotAnInput}.

This example shows the kind of difficulties that can arise when trans-
TLA⁺:

\[ \text{Phase1or2Write}(p, d) \triangleq \]
\[ \land \ phase[p] \in \{1, 2\} \]
\[ \land \ disk'[s] = [\text{disk except } ![d]](p) = \text{dblock}[p] \]
\[ \land \ disksWritten'[s] = [\text{disksWritten except } ![p]] = @ \cup \{d\} \]
\[ \land \ \text{UNCHANGED} \ (\text{input, output, phase, dblock, blocksRead}) \]

Isabelle/HOL:

\[ \text{Phase1or2Write :: state } \Rightarrow \text{state } \Rightarrow \text{Proc } \Rightarrow \text{Disk } \Rightarrow \text{bool} \]
\[ \text{Phase1or2Write } s s' p d \equiv \]
\[ \land \ disk s' = (\text{disk } s) (d := (\text{disk } s d) (p := \text{dblock } s p)) \]
\[ \land \ disksWritten s' = (\text{disksWritten } s) (p := (\text{disksWritten } s p) \cup \{d\}) \]
\[ \land \ inpt s' = inpt s \land \ outpt s' = outpt s \]
\[ \land \ phase s' = phase s \land \ dblock s' = \text{dblock } s \]
\[ \land \ blocksRead s' = \text{blocksRead } s \]

Figure 3: Translation of an action

3.2 Primed Variables

In TLA⁺, to denote the value of a variable in the state resulting from an action, there exists the concept of primed variables. In Isabelle/HOL, there is no built-in notion of state, so we define the state as a record of the variables involved. Instead of defining a “priming” operator, we just define actions as predicates that take any two states, intended to be the previous state and the next state. In this way, \( P s s' \) will be true iff executing an action \( P \) in the \( s \) state could result in the \( s' \) state. In figure 3 we can see how the action \( \text{Phase1or2Write} \) is expressed in TLA⁺ and in Isabelle/HOL.

3.3 Restructuring the specification

There are some minor changes that can be made to specifications to make the proofs in Isabelle easier.

One such change is the elimination of \texttt{let} constructs by making them global definitions. This has two benefits, as it makes it possible to:

- Formulate lemmas that use these definitions.
- Selectively unfold these definitions in proofs, instead of adding \texttt{Let-def} to Isabelle’s simplifier, which unfolds all “let” constructs.

8
Another change that makes proofs easier is to break down actions into simpler actions (e.g. giving separate definitions for subactions corresponding to disjuncts). By making actions smaller, Isabelle has to deal with smaller formulas when we feed the prover with such an action.

For example, \textit{Phase1or2Read} is mainly a big if-then-else. We break it down into two simpler actions:

\[
\text{Phase1or2Read} \triangleq \text{Phase1or2ReadThen} \lor \text{Phase1or2ReadElse}
\]

In \textit{Phase1or2ReadThen} the condition of the if-then-else is present as a state formula (i.e. it is an enabling condition) while in \textit{Phase1or2ReadElse} we add the negation of this condition.

Another example is \textit{HInv2}, which we break down into:

\[
\text{HInv2} \triangleq \text{Inv2a} \land \text{Inv2b} \land \text{Inv2c}
\]

Not only we break it down into three conjuncts but, since these conjuncts are quantifications over some predicate, we give a separate definition for this predicate. For example for \textit{Inv2a}, and after translating to Isabelle/HOL, instead of writing:

\[
\text{Inv2a} s \equiv \forall p. \forall bk \in \text{blocksOf} s p \ldots
\]

we write:

\[
\text{Inv2a-innermost} :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{DiskBlock} \Rightarrow \text{bool}
\]

\[
\text{Inv2a-inner} s p bk \equiv \ldots
\]

\[
\text{Inv2a-inner} :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{bool}
\]

\[
\text{Inv2a-inner} s p \equiv \forall bk \in \text{blocksOf} s p. \text{Inv2a-innermost} s p bk
\]

\[
\text{Inv2a} :: \text{state} \Rightarrow \text{bool}
\]

\[
\text{Inv2a} s \equiv \forall p. \text{Inv2a-inner} s p
\]

Now we can express that we want to obtain the fact

\[
\text{Inv2a-innermost} s q (\text{dblock} s q)
\]

explicitly stating that we are interested in predicate \textit{Inv2a}, but only for some process \( q \) and block (\textit{dblock} \( s q \)).

4 Structure of the Correctness Proof

In [GL00], a specification of correctness and a specification of the algorithm are given. Then, it is proved that the specification of the algorithm implies the specification of correctness. We will do the same for the translated specifications, maintaining the names of theorems and lemmas. It should be noted that only safety properties are given and proved.
4.1 Going from Informal Proofs to Formal Proofs

There are informal proofs for invariants $HInv_3$-$HInv_6$ and for theorem $R2b$ in [GL00]. These informal proofs are written in the structured-proof style that Lamport advocates [Lam95], and are rigorous and quite detailed. We based our formal proofs on these informal proofs, but in many cases a higher level of detail was needed. In some cases, the steps where too big for Isabelle to solve them automatically, and intermediate steps had to be proved first; in other cases, some of the facts relevant to the proofs were omitted in the informal proofs.

As an example of these omissions, the invariant should state that the set $allRdBlks$ is finite. This is needed to choose a block with a maximum ballot number in action $EndPhase1$. Interestingly, this omission cannot be detected with finite-state model checking. As another example, it was omitted that it is necessary to assume that $HInv_4$ and $HInv_5$ hold in the previous state to prove lemma $I2f$.

Although our proofs were based on the informal ones, the high-level structure was often different. When proving that a predicate $I$ was an invariant of $Next$, we preferred proving the invariance of $I$ for each action, rather than a big theorem proving the invariance of $I$ for the $Next$ action. As a consequence, a proof for some actions was often similar to the proof of some other action. For example, the proof of the invariance of $HInv_3$ for the $EndPhase0$ and $Fail$ actions is almost the same. This means we could have made only one proof for the two actions, shortening the length of the complete proof. Nevertheless, proving each action separately could be tackled more easily by Isabelle, as it had fewer facts to deal with, and proving a new lemma was often a simple matter of copy, paste and renaming of definitions. Once the invariance of a given predicate has been proved for each simple action, proving it for the $Next$ action is easy since the $Next$ action is a disjunction of all actions.

The informal proofs start working with $Next$, and then do a case split in which each case implies some action. The structure of the formal proof was copied from the informal one, in the parts where the latter focused on a particular action. This structure could be easily maintained since we used Isabelle’s Isar proof language [Wen02, Nip03], a language for writing human-readable structured proofs.

Lamport’s use of a hierarchical scheme for naming subformulas of a formula would have been very useful, as we have to repeatedly extract subfacts from facts. These proofs were always solved automatically by the auto Isabelle tactic, but made the proofs longer and harder to understand. Automatic naming of subformulas of Isabelle definitions would be a very practical feature.
5 Conclusion

We formally verified the correctness of the Disk Paxos specification in Isabelle/HOL. We found some omissions in the informal proofs, including one that could not have been detected with finite-state model checking, but no outright errors. This formal proof gives us a greater confidence in the correctness of the algorithm.

This work was done in little more than two months, including learning Isabelle from scratch. Consequently, this work can be taken as evidence that formal verification of fault-tolerant distributed algorithms may be feasible for software verification in an industrial context.

Isabelle proved to be a very helpful tool for this kind of verification, although it would have been useful to have Lamport’s naming of subfacts to make proofs shorter and easier to write.

References


A TLA$^+$ correctness specification

---

**MODULE Synod**

EXTENDS Naturals

CONSTANT $N$, Inputs

ASSUME $(N \in \text{Nat}) \land (N > 0)$

Proc $\triangleq 1..N$

NotAnInput $\triangleq$ choose $c : c \notin Inputs$

VARIABLES inputs, output

---

**MODULE Inner**

VARIABLES allInput, chosen

---

$IInit$ $\triangleq \quad \land \: \text{input} \in [\text{Proc} \rightarrow \text{Inputs}]
\land \: \text{output} = [p \in \text{Proc} \mapsto \text{NotAnInput}]
\land \: \text{chosen} = \text{NotAnInput}
\land \: \text{allInput} = \text{input}[p] : p \in \text{Proc}$

$IChoose(p)$ $\triangleq$
\begin{align*}
& \land \: \text{output}[p] = \text{NotAnInput} \\
& \land \: \text{if chosen} = \text{NotAnInput}
\begin{align*}
& \quad \text{then } \text{ip} \in \text{allInput} : \land \: \text{chosen}' = \text{ip} \\
& \quad \quad \land \: \text{output}' = [\text{output except !}[p] = \text{ip}]
\end{align*}
\end{align*}
\begin{align*}
& \quad \text{else } \land \: \text{output}' = [\text{output except !}[p] = \text{chosen}] \\
& \quad \quad \land \: \text{UNCHANGED chosen} \\
& \quad \quad \land \: \text{UNCHANGED } \langle \text{input, allInput} \rangle
\end{align*}

$IFail(p)$ $\triangleq \quad \land \: \text{output}' = [\text{output except !}[p] = \text{NotAnInput}] \\
\begin{align*}
& \quad \land \: \exists \text{ip} \in \text{Inputs} : \land \: \text{input}' = [\text{input except !}[p] = \text{ip}] \\
& \quad \quad \land \: \text{allInput}' = \text{allInput} \cup \{\text{ip}\}
\end{align*}$

$INext$ $\triangleq \exists p \in \text{Proc} : IChoose(p) \lor IFail(p)$

$ISpec$ $\triangleq \quad IInit \land \square [INext]_{\langle \text{input, output, chosen, allInput} \rangle}$

$IS(\text{chosen, allInput})$ $\triangleq \text{INSTANCE Inner}$

$SynodSpec$ $\triangleq \exists \text{chosen, allInput} : IS(\text{chosen, allInput}) \land ISpec$
B Disk Paxos Algorithm Specification

theory DiskPaxos-Model imports Main begin

This is the specification of the Disk Synod algorithm.

typedecl InputsOrNi
typedecl Disk
typedecl Proc

axiomatization
  Inputs :: InputsOrNi set and
  NotAnInput :: InputsOrNi and
  Ballot :: Proc ⇒ nat set and
  IsMajority :: Disk set ⇒ bool

where
  NotAnInput: NotAnInput ∉ Inputs and
  InputsOrNi: (UNIV :: InputsOrNi set) = Inputs ∪ {NotAnInput} and
  Ballot-nzero: ∀ p. 0 ∉ Ballot p and
  Ballot-disj: ∀ p q. p ≠ q → (Ballot p) ∩ (Ballot q) = {} and
  Disk-isMajority: IsMajority(UNIV) and
  majorities-intersect:
    ∀ S T. IsMajority(S) ∧ IsMajority(T) → S ∩ T ≠ {}

lemma ballots-not-zero [simp]:
  b ∈ Ballot p → 0 < b
⟨proof⟩

lemma majority-nonempty [simp]: IsMajority(S) ⇒ S ≠ {}
⟨proof⟩

definition AllBallots :: nat set
  where AllBallots = (UN p. Ballot p)

record
  DiskBlock =
    mbal :: nat
    bal :: nat
    inp :: InputsOrNi

definition InitDB :: DiskBlock
  where InitDB = (mbal = 0, bal = 0, inp = NotAnInput)

record
  BlockProc =
    block :: DiskBlock
    proc :: Proc

record
  state =
\[
inpt :: \text{Proc} \Rightarrow \text{InputsOrNi}
\]
\[
outpt :: \text{Proc} \Rightarrow \text{InputsOrNi}
\]
\[
disk :: \text{Disk} \Rightarrow \text{Proc} \Rightarrow \text{DiskBlock}
\]
\[
dblock :: \text{Proc} \Rightarrow \text{DiskBlock}
\]
\[
phase :: \text{Proc} \Rightarrow \text{nat}
\]
\[
disksWritten :: \text{Proc} \Rightarrow \text{Disk set}
\]
\[
blocksRead :: \text{Proc} \Rightarrow \text{Disk} \Rightarrow \text{BlockProc set}
\]

\[
\text{allInput} :: \text{InputsOrNi set}
\]
\[
\text{chosen} :: \text{InputsOrNi}
\]

\[
definition \text{hasRead} :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{Disk} \Rightarrow \text{Proc} \Rightarrow \text{bool}
\]
\[
\text{where} \quad \text{hasRead} s p d q = (\exists br \in \text{blocksRead} s p d. \text{proc} br = q)
\]

\[
definition \text{allRdBlks} :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{BlockProc set}
\]
\[
\text{where} \quad \text{allRdBlks} s p = (\bigcup d. \text{blocksRead} s p d)
\]

\[
definition \text{allBlocksRead} :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{DiskBlock set}
\]
\[
\text{where} \quad \text{allBlocksRead} s p = \text{block } e (\text{allRdBlks} s p)
\]

\[
definition \text{Init} :: \text{state} \Rightarrow \text{bool}
\]
\[
\text{where} \quad \text{Init} s =
\]
\[
\begin{align*}
& (\text{range } (\text{inpt} s) \subseteq \text{Inputs}) \\
& \& \text{outpt } s = (\lambda p. \text{NotAnInput}) \\
& \& \text{disk } s = (\lambda d p. \text{InitDB}) \\
& \& \text{phase } s = (\lambda p. 0) \\
& \& \text{dblock } s = (\lambda p. \text{InitDB}) \\
& \& \text{disksWritten } s = (\lambda p. \{\}) \\
& \& \text{blocksRead } s = (\lambda p d. \{\})
\end{align*}
\]

\[
definition \text{InitializePhase} :: \text{state} \Rightarrow \text{state} \Rightarrow \text{Proc} \Rightarrow \text{bool}
\]
\[
\text{where} \quad \text{InitializePhase} s s' p =
\]
\[
\begin{align*}
& (\text{disksWritten } s' = (\text{disksWritten } s)(p := \{\})) \\
& \& \text{blocksRead } s' = (\text{blocksRead } s)(p := (\lambda d. \{\}))
\end{align*}
\]

\[
definition \text{StartBallot} :: \text{state} \Rightarrow \text{state} \Rightarrow \text{Proc} \Rightarrow \text{bool}
\]
\[
\text{where} \quad \text{StartBallot} s s' p =
\]
\[
\begin{align*}
& (\text{phase } s p \in \{1,2\}) \\
& \& \text{phase } s' = (\text{phase } s)(p := 1) \\
& \& (\exists b \in \text{Ballot } p. \\
& \quad \text{mbal } (\text{dblock } s p) < b \\
& \quad \& \text{dblock } s' = (\text{dblock } s)(p := (\text{dblock } s p)(\text{mbal} := b \|)) \\
& \& \text{InitializePhase } s s' p \\
& \& \text{inpt } s' = \text{inpt } s \& \text{outpt } s' = \text{outpt } s \& \text{disk } s' = \text{disk } s)
\end{align*}
\]
definition Phase1or2Write :: state ⇒ state ⇒ Proc ⇒ Disk ⇒ bool
where
  Phase1or2Write s s′ p d =  
    (phase s p ∈ {1, 2})  
    ∧ disk s′ = (disk s) (d := (disk s d) (p := dblock s p))  
    ∧ disksWritten s′ = (disksWritten s) (p := (disksWritten s p) ∪ {d})  
    ∧ inpt s′ = inpt s ∧ outpt s′ = outpt s  
    ∧ phase s′ = phase s ∧ dblock s′ = dblock s  
    ∧ blocksRead s′ = blocksRead s)

definition Phase1or2ReadThen :: state ⇒ state ⇒ Proc ⇒ Disk ⇒ Proc ⇒ bool
where
  Phase1or2ReadThen s s′ p d q =  
    (d ∈ disksWritten s p)  
    ∧ mbal(disk s d q) < mbal(dblock s p)  
    ∧ blocksRead s′ = (blocksRead s) (p := (blocksRead s p) (d := (blocksRead s p d) ∪ {\{ block = disk s d q, \  
                    proc = q \}}))  
    ∧ inpt s′ = inpt s ∧ outpt s′ = outpt s  
    ∧ disk s′ = disk s ∧ phase s′ = phase s  
    ∧ dblock s′ = dblock s ∧ disksWritten s′ = disksWritten s)

definition Phase1or2ReadElse :: state ⇒ state ⇒ Proc ⇒ Disk ⇒ Proc ⇒ bool
where
  Phase1or2ReadElse s s′ p d q =  
    (d ∈ disksWritten s p)  
    ∧ StartBallot s s′ p

definition Phase1or2Read :: state ⇒ state ⇒ Proc ⇒ Disk ⇒ Proc ⇒ bool
where
  Phase1or2Read s s′ p d q =  
    (Phase1or2ReadThen s s′ p d q  
    ∨ Phase1or2ReadElse s s′ p d q)

definition blocksSeen :: state ⇒ Proc ⇒ DiskBlock set
where
  blocksSeen s p = allBlocksRead s p ∪ {dblock s p}

definition nonInitBlks :: state ⇒ Proc ⇒ DiskBlock set
where
  nonInitBlks s p = \{ bs . bs ∈ blocksSeen s p ∧ inp bs ∈ Inputs\}

definition maxBlk :: state ⇒ Proc ⇒ DiskBlock
where
  maxBlk s p =  
    (SOME b . b ∈ nonInitBlks s p ∧ (∀ c ∈ nonInitBlks s p. bal c ≤ bal b))

definition EndPhase1 :: state ⇒ state ⇒ Proc ⇒ bool
where
  EndPhase1 s s′ p =  
    (IsMajority \{ d . d ∈ disksWritten s p\)
\( (\forall q \in \text{UNIV} - \{p\}. \text{hasRead} s p d q) \)
\( \land \text{phase} s p = 1 \)
\( \land \text{dblock} s' = (\text{dblock} s) (p := \text{dblock} s p) \)
\( \{ \begin{array}{l}
\text{bal} := \text{mbal}(\text{dblock} s p), \\
\text{inp} := \\
\quad (\text{if nonInitBlks} s p = \{\} \\
\quad \text{then inp} s p \\
\quad \text{else inp} (\text{maxBlk} s p)) \\
\end{array} \}
\)
\( \land \text{outpt} s' = \text{outpt} s \)
\( \land \text{phase} s' = (\text{phase} s) (p := \text{phase} s p + 1) \)
\( \land \text{InitializePhase} s s' p \)
\( \land \text{inpt} s' = \text{inpt} s \land \text{disk} s' = \text{disk} s \)

**definition** \( \text{EndPhase2} :: \text{state} \Rightarrow \text{state} \Rightarrow \text{Proc} \Rightarrow \text{bool} \)
where
\( \text{EndPhase2} s s' p = \)
\( (\text{IsMajority} \{ d . d \in \text{disksWritten} s p \\
\land (\forall q \in \text{UNIV} - \{p\}. \text{hasRead} s p d q) \}) \)
\( \land \text{phase} s p = 2 \)
\( \land \text{outpt} s' = (\text{outpt} s) (p := \text{inp} (\text{dblock} s p)) \)
\( \land \text{dblock} s' = \text{dblock} s \)
\( \land \text{phase} s' = (\text{phase} s) (p := \text{phase} s p + 1) \)
\( \land \text{InitializePhase} s s' p \)
\( \land \text{inpt} s' = \text{inpt} s \land \text{disk} s' = \text{disk} s \)

**definition** \( \text{EndPhase1or2} :: \text{state} \Rightarrow \text{state} \Rightarrow \text{Proc} \Rightarrow \text{bool} \)
where \( \text{EndPhase1or2} s s' p = (\text{EndPhase1} s s' p \lor \text{EndPhase2} s s' p) \)

**definition** \( \text{Fail} :: \text{state} \Rightarrow \text{state} \Rightarrow \text{Proc} \Rightarrow \text{bool} \)
where
\( \text{Fail} s s' p = \)
\( (\exists \text{ip} \in \text{Inputs}. \text{inpt} s' = (\text{inpt} s) (p := \text{ip}) \)
\( \land \text{phase} s' = (\text{phase} s) (p := 0) \)
\( \land \text{dblock} s' = (\text{dblock} s) (p := \text{InitDB}) \)
\( \land \text{outpt} s' = (\text{outpt} s) (p := \text{NotAnInput}) \)
\( \land \text{InitializePhase} s s' p \)
\( \land \text{disk} s' = \text{disk} s \)

**definition** \( \text{Phase0Read} :: \text{state} \Rightarrow \text{state} \Rightarrow \text{Proc} \Rightarrow \text{Disk} \Rightarrow \text{bool} \)
where
\( \text{Phase0Read} s s' p d = \)
\( (\text{phase} s p = 0 \land \text{blocksRead} s' = (\text{blocksRead} s) (p := \text{blocksRead} s p) (d := \text{blocksRead} s p d \cup \{ (\langle \text{block} = \text{disk} s d p, \text{proc} = p \rangle) \})) \)
\( \land \text{inpt} s' = \text{inpt} s \land \text{outpt} s' = \text{outpt} s \land \text{disk} s' = \text{disk} s \land \text{phase} s' = \text{phase} s \land \text{dblock} s' = \text{dblock} s \land \text{disksWritten} s' = \text{disksWritten} s) \)
**definition** EndPhase0 :: state ⇒ state ⇒ Proc ⇒ bool
where
EndPhase0 s s' p =
(phase s p = 0
∧ IsMajority ({d. hasRead s p d})
∧ (∃ b ∈ Ballot p.
   (∀ r ∈ allBlocksRead s p. mbal r < b)
   ∧ dblock s' = (dblock s) ( p:=
      (SOME r. r ∈ allBlocksRead s p
      ∧ (∀ s ∈ allBlocksRead s p. bal s ≤ bal r)) ( mbal := b )))
∧ InitializePhase s s' p
∧ phase s' = (phase s) (p:= 1)
∧ inpt s' = inpt s ∧ outpt s' = outpt s ∧ disk s' = disk s)

**definition** Next :: state ⇒ state ⇒ bool
where
Next s s' = (∃ p.
   StartBallot s s' p
   ∨ (∃ d. Phase0Read s s' p d
   ∨ Phase1or2Write s s' p d
   ∨ (∃ q. q ≠ p ∧ Phase1or2Read s s' p d q))
   ∨ EndPhase1or2 s s' p
   ∨ Fail s s' p
   ∨ EndPhase0 s s' p)

In the following, for each action or state name we name Hname the corresponding action that includes the history part of the HNext action or state predicate that includes history variables.

**definition** HInit :: state ⇒ bool
where
HInit s =
(Init s
& chosen s = NotAnInput
& allInput s = range (inpt s))

HNextPart is the part of the Next action that is concerned with history variables.

**definition** HNextPart :: state ⇒ state ⇒ bool
where
HNextPart s s' =
(chosen s' =
   (if chosen s ≠ NotAnInput ∨ (∀ p. outpt s' p = NotAnInput )
   then chosen s
   else outpt s' (SOME p. outpt s' p ≠ NotAnInput))
   ∧ allInput s' = allInput s ∪ (range (inpt s')))
We add $HNextPart$ to every action (rather than proving that $Next$ maintains the $HInv$ invariant) to make proofs easier.

**definition**

$HPhase1or2ReadThen :: state \Rightarrow state \Rightarrow Proc \Rightarrow Disk \Rightarrow Proc \Rightarrow bool$ where

$HPhase1or2ReadThen s s' p d q = (Phase1or2ReadThen s s' p d q \land HNextPart s s')$

**definition**

$HEndPhase1 :: state \Rightarrow state \Rightarrow Proc \Rightarrow bool$ where

$HEndPhase1 s s' p = (EndPhase1 s s' p \land HNextPart s s')$

**definition**

$HStartBallot :: state \Rightarrow state \Rightarrow Proc \Rightarrow bool$ where

$HStartBallot s s' p = (StartBallot s s' p \land HNextPart s s')$

**definition**

$HPhase1or2Write :: state \Rightarrow state \Rightarrow Proc \Rightarrow Disk \Rightarrow bool$ where

$HPhase1or2Write s s' p d = (Phase1or2Write s s' p d \land HNextPart s s')$

**definition**

$HPhase1or2ReadElse :: state \Rightarrow state \Rightarrow Proc \Rightarrow Disk \Rightarrow Proc \Rightarrow bool$ where

$HPhase1or2ReadElse s s' p d q = (Phase1or2ReadElse s s' p d q \land HNextPart s s')$

**definition**

$HEndPhase2 :: state \Rightarrow state \Rightarrow Proc \Rightarrow bool$ where

$HEndPhase2 s s' p = (EndPhase2 s s' p \land HNextPart s s')$

**definition**

$HFail :: state \Rightarrow state \Rightarrow Proc \Rightarrow bool$ where

$HFail s s' p = (Fail s s' p \land HNextPart s s')$

**definition**

$HPhase0Read :: state \Rightarrow state \Rightarrow Proc \Rightarrow Disk \Rightarrow bool$ where

$HPhase0Read s s' p d = (Phase0Read s s' p d \land HNextPart s s')$

**definition**

$HEndPhase0 :: state \Rightarrow state \Rightarrow Proc \Rightarrow bool$ where

$HEndPhase0 s s' p = (EndPhase0 s s' p \land HNextPart s s')$

Since these definitions are the conjunction of two other definitions declaring them as simplification rules should be harmless.

**declare** $HPhase1or2ReadThen-def [simp]

**declare** $HPhase1or2ReadElse-def [simp]

**declare** $HEndPhase1-def [simp]

**declare** $HStartBallot-def [simp]
C Proof of Disk Paxos’ Invariant

theory DiskPaxos-Inv1 imports DiskPaxos-Model begin

C.1 Invariant 1

This is just a type Invariant.

definition Inv1 :: state ⇒ bool where
Inv1 s = (∀ p.
inpt s p ∈ Inputs ∧ phase s p ≤ 3 ∧ finite (allRdBlks s p))

definition HInv1 :: state ⇒ bool where
HInv1 s = (Inv1 s ∧ allInput s ⊆ Inputs)

declare HInv1-def [simp]

We added the assertion that the set allRdBlksp is finite for every process p; one may therefore choose a block with a maximum ballot number in action EndPhase1.

With the following the lemma, it will be enough to prove Inv1 s’ for every action, without taking the history variables in account.

lemma HNextPart-Inv1: [ HInv1 s; HNextPart s s’; Inv1 s’ ] ⇒ HInv1 s’
⟨proof⟩

theorem HInit-HInv1: HInit s −→ HInv1 s
⟨proof⟩

lemma allRdBlks-finite:
  assumes inv: HInv1 s
  and asm: ∀ p. allRdBlks s’ p ⊆ insert bk (allRdBlks s p)
  shows ∀ p. finite (allRdBlks s’ p)
⟨proof⟩
theorem HPhase1or2ReadThen-HInv1:
assumes inv1: HInv1 s
and act: HPhase1or2ReadThen s s' p d q
shows HInv1 s'
⟨proof⟩

theorem HEndPhase1-HInv1:
assumes inv1: HInv1 s
and act: HEndPhase1 s s' p
shows HInv1 s'
⟨proof⟩

theorem HStartBallot-HInv1:
assumes inv1: HInv1 s
and act: HStartBallot s s' p
shows HInv1 s'
⟨proof⟩

theorem HPhase1or2Write-HInv1:
assumes inv1: HInv1 s
and act: HPhase1or2Write s s' p d
shows HInv1 s'
⟨proof⟩

theorem HPhase1or2ReadElse-HInv1:
assumes act: HPhase1or2ReadElse s s' p d q
and inv1: HInv1 s
shows HInv1 s'
⟨proof⟩

theorem HEndPhase2-HInv1:
assumes inv1: HInv1 s
and act: HEndPhase2 s s' p
shows HInv1 s'
⟨proof⟩

theorem HFail-HInv1:
assumes inv1: HInv1 s
and act: HFail s s' p
shows HInv1 s'
⟨proof⟩

theorem HPhase0Read-HInv1:
assumes inv1: HInv1 s
and act: HPhase0Read s s' p d
shows HInv1 s'
⟨proof⟩

theorem HEndPhase0-HInv1:
assumes inv1: HInv1 s
and act: HEndPhase0 s s' p
shows HInv1 s'

(proof)

declare HInv1-def [simp del]

HInv1 is an invariant of HNext

lemma I2a:
assumes nxt: HNext s s'
and inv: HInv1 s
shows HInv1 s'

(proof)

end

theory DiskPaxos-Inv2 imports DiskPaxos-Inv1 begin

C.2 Invariant 2

The second invariant is split into three main conjuncts called Inv2a, Inv2b, and Inv2c. The main difficulty is in proving the preservation of the first conjunct.

definition rdBy :: state ⇒ Proc ⇒ Proc ⇒ Disk ⇒ BlockProc set
where
rdBy s p q d = {br . br ∈ blocksRead s q d ∧ proc br = p}

definition blocksOf :: state ⇒ Proc ⇒ DiskBlock set
where
blocksOf s p = {dblock s p} ∪ {disk s d p | d . d ∈ UNIV} ∪ {block br | br . br ∈ (UN q d . rdBy s p q d ) }

definition allBlocks :: state ⇒ DiskBlock set
where allBlocks s = (UN p . blocksOf s p)

definition Inv2a-innermost :: state ⇒ Proc ⇒ DiskBlock ⇒ bool
where
Inv2a-innermost s p bk = (mbal bk ∈ (Ballot p) ∪ {0})
∧ bal bk ∈ (Ballot p) ∪ {0}
∧ (bal bk = 0) = (inp bk = NotAnInput)
∧ bal bk ≤ mbal bk
∧ inp bk ∈ (allInput s) ∪ {NotAnInput})
definition Inv2a-inner :: state ⇒ Proc ⇒ bool
  where Inv2a-inner s p = (∀ bk ∈ blocksOf s p. Inv2a-innermost s p bk)

definition Inv2a :: state ⇒ bool
  where Inv2a s = (∀ p. Inv2a-inner s p)

definition Inv2b-inner :: state ⇒ Proc ⇒ Disk ⇒ bool
  where
    Inv2b-inner s p d =
      ((d ∈ disksWritten s p =⇒
        (phase s p ∈ {1,2} ∧ disk s d p = dblock s p))
      ∧ (phase s p ∈ {1,2} =⇒
        (blocksRead s p d ≠ {} =⇒ d ∈ disksWritten s p)
        ∧ ¬ hasRead s p d)))

definition Inv2b :: state ⇒ bool
  where Inv2b s = (∀ p d. Inv2b-inner s p d)

definition Inv2c-inner :: state ⇒ Proc ⇒ bool
  where
    Inv2c-inner s p =
      (((phase s p = 0 =⇒
        (dblock s p = InitDB
        ∧ disksWritten s p = {})
        ∧ (∀ d. ∀ br ∈ blocksRead s p d.
          proc br = p ∧ block br = disk s d p)))
      ∧ (phase s p ≠ 0 =⇒
        (mbal(dblock s p) ∈ Ballot p
        ∧ bal(dblock s p) ∈ Ballot p ∪ {0}
        ∧ (∀ d. ∀ br ∈ blocksRead s p d.
          mbal(block br) < mbal(dblock s p)))
      ∧ (phase s p ∈ {2,3} =⇒ bal(dblock s p) = mbal(dblock s p))
      ∧ outpt s p = (if phase s p = 3 then inp(dblock s p) else NotAnInput)
      ∧ chosen s ∈ allInput s ∪ {NotAnInput}
      ∧ (∀ p. inp s p ∈ allInput s
      ∧ (chosen s = NotAnInput =⇒ outpt s p = NotAnInput)))

definition Inv2c :: state ⇒ bool
  where Inv2c s = (∀ p. Inv2c-inner s p)

definition HInv2 :: state ⇒ bool
  where HInv2 s = (Inv2a s ∧ Inv2b s ∧ Inv2c s)

C.2.1 Proofs of Invariant 2 a

theorem HInit-Inv2a: HInit s =⇒ Inv2a s
(proof)

For every action we define a action-blocksOf lemma. We have two cases: ei-
ther the new blocksOf is included in the old blocksOf, or the new blocksOf is included in the old blocksOf union the new dblock. In the former case the assumption inv will imply the thesis. In the latter, we just have to prove the innermost predicate for the particular case of the new dblock. This particular case is proved in lemma action-Inv2a-dblock.

**lemma** $HPhase1or2ReadThen$-blocksOf:

$\left( HPhase1or2ReadThen \ s \ s' \ p \ d \ q \right) \implies blocksOf \ s' \ r \subseteq blocksOf \ s \ r$

(proof)

**theorem** $HPhase1or2ReadThen$-Inv2a:

assumes inv: Inv2a s

and act: $HPhase1or2ReadThen \ s \ s' \ p \ d \ q$

shows Inv2a s'

(proof)

**lemma** InitializePhase-rdBy:

InitializePhase s s' p \implies rdBy s' pp qq dd \subseteq rdBy s pp qq dd

(proof)

**lemma** $HStartBallot$-blocksOf:

$HStartBallot \ s \ s' \ p \implies blocksOf \ s' \ q \subseteq blocksOf \ s \ q \cup \{dblock \ s' \ q\}$

(proof)

**lemma** $HStartBallot$-Inv2a-dblock:

assumes act: $HStartBallot \ s \ s' \ p$

and inv2a: Inv2a-innermost s p (dblock s p)

shows Inv2a-innermost s' p (dblock s' p)

(proof)

**lemma** $HStartBallot$-Inv2a-dblock-q:

assumes act: $HStartBallot \ s \ s' \ p$

and inv2a: Inv2a-innermost s q (dblock s q)

shows Inv2a-innermost s' q (dblock s' q)

(proof)

**theorem** $HStartBallot$-Inv2a:

assumes inv: Inv2a s

and act: $HStartBallot \ s \ s' \ p$

shows Inv2a s'

(proof)

**lemma** $HPhase1or2Write$-blocksOf:

$\left( HPhase1or2Write \ s \ s' \ p \ d \right) \implies blocksOf \ s' \ r \subseteq blocksOf \ s \ r$

(proof)

**theorem** $HPhase1or2Write$-Inv2a:

assumes inv: Inv2a s

and act: $HPhase1or2Write \ s \ s' \ p \ d$
shows \(\text{Inv2a}\ s\)
\(\langle\text{proof}\rangle\)

**Theorem HPhase1or2ReadElse-Inv2a:**

- **Assumes:** \(\text{inv} : \text{Inv2a}\ s\)
- **And:** \(\text{act} : \text{HPhase1or2ReadElse}\ s\ s\ p d q\)
- **Shows:** \(\text{Inv2a}\ s'\)
\(\langle\text{proof}\rangle\)

**Lemma HEndPhase2-blocksOf:**

\[ [\text{HEndPhase2}\ s\ s'\ p] \implies \text{blocksOf}\ s'\ q \subseteq \text{blocksOf}\ s\ q \]
\(\langle\text{proof}\rangle\)

**Theorem HEndPhase2-Inv2a:**

- **Assumes:** \(\text{inv} : \text{Inv2a}\ s\)
- **And:** \(\text{act} : \text{HEndPhase2}\ s\ s\ p\)
- **Shows:** \(\text{Inv2a}\ s'\)
\(\langle\text{proof}\rangle\)

**Lemma HFail-blocksOf:**

\(\text{HFail}\ s\ s'\ p \implies \text{blocksOf}\ s'\ q \subseteq \text{blocksOf}\ s\ q \cup \{\text{dblock}\ s\ q\}\)
\(\langle\text{proof}\rangle\)

**Lemma HFail-Inv2a-dblock-q:**

- **Assumes:** \(\text{act} : \text{HFail}\ s\ s'\ p\)
- **And:** \(\text{inv} : \text{Inv2a-innermost}\ s\ q\ (\text{dblock}\ s\ q)\)
- **Shows:** \(\text{Inv2a-innermost}\ s'\ q\ (\text{dblock}\ s'\ q)\)
\(\langle\text{proof}\rangle\)

**Theorem HFail-Inv2a:**

- **Assumes:** \(\text{inv} : \text{Inv2a}\ s\)
- **And:** \(\text{act} : \text{HFail}\ s\ s'\ p\)
- **Shows:** \(\text{Inv2a}\ s'\)
\(\langle\text{proof}\rangle\)

**Lemma HPhase0Read-blocksOf:**

\(\text{HPhase0Read}\ s\ s'\ p\ d \implies \text{blocksOf}\ s'\ q \subseteq \text{blocksOf}\ s\ q\)
\(\langle\text{proof}\rangle\)

**Theorem HPhase0Read-Inv2a:**

- **Assumes:** \(\text{inv} : \text{Inv2a}\ s\)
- **And:** \(\text{act} : \text{HPhase0Read}\ s\ s'\ p\ d\)
- **Shows:** \(\text{Inv2a}\ s'\)
\(\langle\text{proof}\rangle\)

**Lemma HEndPhase0-blocksOf:**

\(\text{HEndPhase0}\ s\ s'\ p \implies \text{blocksOf}\ s'\ q \subseteq \text{blocksOf}\ s\ q \cup \{\text{dblock}\ s'\ q\}\)
\(\langle\text{proof}\rangle\)
lemma HEndPhase0-blocksRead:
assumes act: HEndPhase0 s s' p
shows \( \exists d. \text{blocksRead} s p d \neq \{\} \)
⟨proof⟩

EndPhase0 has the additional difficulty of having a choose expression. We prove that there exists an \( x \) such that the predicate of the choose expression holds, and then apply someI: \( \forall x. \exists P x \implies \exists P \) (Eps \( \forall x. \exists P x \)).

lemma HEndPhase0-some:
assumes act: HEndPhase0 s s' p
and inv1: Inv1 s
shows \begin{align*}
(SOME b. b \in \text{allBlocksRead} s p & ) \\
\land (\forall t \in \text{allBlocksRead} s p. \text{bal} t \leq \text{bal} b) \\
\land (\forall t \in \text{allBlocksRead} s p. \text{bal} t \leq \text{bal} (SOME b. b \in \text{allBlocksRead} s p & ) ) \\
\land (\forall t \in \text{allBlocksRead} s p. \text{bal} t \leq \text{bal} b) 
\end{align*}
⟩
⟨proof⟩

lemma HEndPhase0-dblock-allBlocksRead:
assumes act: HEndPhase0 s s' p
and inv1: Inv1 s
shows \( \text{dblock} s' p \in (\lambda x. x (|mbal:= mbal(\text{dblock} s' p)) ) \uplus \text{allBlocksRead} s p \)
⟨proof⟩

lemma HNextPart-allInput-or-NotAnInput:
assumes act: HNextPart s s'
and inv2a: Inv2a-innermost s p
shows \( \text{inp} (\text{dblock} s' p) \in \text{allInput} s' \cup \{\text{NotAnInput}\} \)
⟨proof⟩

lemma HEndPhase0-Inv2a-allBlocksRead:
assumes act: HEndPhase0 s s' p
and inv2a: Inv2a-inner s p
and inv2c: Inv2c-inner s p
shows \( \forall t \in (\lambda x. x (|mbal:= mbal(\text{dblock} s' p)) ) \uplus \text{allBlocksRead} s p. \text{Inv2a-innermost} s p t \)
⟨proof⟩

lemma HEndPhase0-Inv2a-dblock:
assumes act: HEndPhase0 s s' p
and inv1: Inv1 s
and inv2a: Inv2a-inner s p
and inv2c: Inv2c-inner s p
shows Inv2a-innermost s' p (dblock s' p)
⟨proof⟩

lemma HEndPhase0-Inv2a-dblock-q:
assumes act: HEndPhase0 s s' p
and inv1: Inv1 s
and inv2a: Inv2a-inner s q
and inv2c: Inv2c-inner s p
shows Inv2a-innermost s' q (dblock s' q) (proof)

theorem HEndPhase0-Inv2a:
assumes inv: Inv2a s
and act: HEndPhase0 s s' p
and inv1: Inv1 s
and inv2c: Inv2c-inner s p
shows Inv2a s' (proof)

lemma HEndPhase1-blocksOf:
  HEndPhase1 s s' p \Rightarrow blocksOf s' q \subseteq blocksOf s q \cup \{dblock s' q\} (proof)

lemma maxBlk-in-nonInitBlks:
  assumes b: b \in nonInitBlks s p
  and inv1: Inv1 s
  shows maxBlk s p \in nonInitBlks s p
  \land (\forall c \in nonInitBlks s p. bal c \leq bal (maxBlk s p)) (proof)

lemma blocksOf-nonInitBlks:
  (\forall p bk. bk \in blocksOf s p \rightarrow P bk)
  \rightarrow \forall bk \in nonInitBlks s p. P bk (proof)

lemma maxBlk-allInput:
  assumes inv: Inv2a s
  and mbk: maxBlk s p \in nonInitBlks s p
  shows inp (maxBlk s p) \in allInput s (proof)

lemma HEndPhase1-dblock-allInput:
  assumes act: HEndPhase1 s s' p
  and inv1: HInv1 s
  and inv2: Inv2a s
  shows inp': inp (dblock s' p) \in allInput s' (proof)

lemma HEndPhase1-Inv2a-dblock:
  assumes act: HEndPhase1 s s' p
  and inv1: HInv1 s
  and inv2: Inv2a s
  and inv2c: Inv2c-inner s p
lemma HEndPhase1-Inv2a-dblock-q:
  assumes act: HEndPhase1 s s' p
  and inv1: HInv1 s
  and inv: Inv2a s
  and inv2c: Inv2c-inner s p
  shows Inv2a-innermost s' q (dblock s' q)
⟨proof⟩

theorem HEndPhase1-Inv2a:
  assumes act: HEndPhase1 s s' p
  and inv1: HInv1 s
  and inv: Inv2a s
  and inv2c: Inv2c-inner s p
  shows Inv2a s'
⟨proof⟩

C.2.2 Proofs of Invariant 2 b

Invariant 2b is proved automatically, given that we expand the definitions involved.

theorem HInit-Inv2b: HInit s → Inv2b s
⟨proof⟩

theorem HPhase1or2ReadThen-Inv2b:
  [ [ Inv2b s; HPhase1or2ReadThen s s' p d q ] ]
  ⇒ Inv2b s'
⟨proof⟩

theorem HStartBallot-Inv2b:
  [ [ Inv2b s; HStartBallot s s' p ] ]
  ⇒ Inv2b s'
⟨proof⟩

theorem HPhase1or2Write-Inv2b:
  [ [ Inv2b s; HPhase1or2Write s s' p d ] ]
  ⇒ Inv2b s'
⟨proof⟩

theorem HPhase1or2ReadElse-Inv2b:
  [ [ Inv2b s; HPhase1or2ReadElse s s' p d q ] ]
  ⇒ Inv2b s'
⟨proof⟩

theorem HEndPhase1-Inv2b:
  [ [ Inv2b s; HEndPhase1 s s' p ] ] ⇒ Inv2b s'
⟨proof⟩
theorem HFail-Inv2b:
\[
\begin{array}{l}
\text{Inv2b } s; \text{HFail } s \ s' \ p \ \Rightarrow \text{ Inv2b } s'
\end{array}
\]
\[\text{proof}\]

theorem HEndPhase2-Inv2b:
\[
\begin{array}{l}
\text{Inv2b } s; \text{HEndPhase2 } s \ s' \ p \ \Rightarrow \text{ Inv2b } s'
\end{array}
\]
\[\text{proof}\]

theorem HPhase0Read-Inv2b:
\[
\begin{array}{l}
\text{Inv2b } s; \text{HPhase0Read } s \ s' \ p \ d \ \Rightarrow \text{ Inv2b } s'
\end{array}
\]
\[\text{proof}\]

C.2.3 Proofs of Invariant 2 c

theorem HInit-Inv2c: HInit s \(\rightarrow\) Inv2c s
\[\text{proof}\]

lemma HNextPart-Inv2c-chosen:
\[
\begin{array}{l}
\text{assumes } hnp: \text{HNextPart } s \ s' \\
\text{and } \text{inv2c: Inv2c } s \\
\text{and } \text{outpt: } \forall p. \text{ outpt } s' \ p = \begin{cases} 
\text{inp}(\text{dblock } s' \ p) & \text{if phase } s' \ p = 3 \\
\text{NotAnInput} & \text{else}
\end{cases} \\
\text{and } \text{inp-dblk: } \forall p. \text{ inp}(\text{dblock } s' \ p) \in \text{allInput } s' \cup \{\text{NotAnInput}\} \\
\text{shows } \text{chosen } s' \in \text{allInput } s' \cup \{\text{NotAnInput}\}
\end{array}
\]
\[\text{proof}\]

lemma HNextPart-chosen:
\[
\begin{array}{l}
\text{assumes } hnp: \text{HNextPart } s \ s' \\
\text{shows } \text{chosen } s' = \text{NotAnInput} \rightarrow (\forall p. \text{ outpt } s' \ p = \text{NotAnInput})
\end{array}
\]
\[\text{proof}\]

lemma HNextPart-allInput:
\[
\begin{array}{l}
\text{HNextPart } s \ s'; \text{Inv2c } s \ \Rightarrow \forall p. \text{ inpt } s' \ p \in \text{allInput } s'
\end{array}
\]
\[\text{proof}\]

theorem HPhase1or2ReadThen-Inv2c:
\[
\begin{array}{l}
\text{assumes } \text{inv: Inv2c } s \\
\text{and } \text{act: HPhase1or2ReadThen } s \ s' \ p \ d \ q \\
\text{and } \text{inv2a: Inv2a } s \\
\text{shows } \text{Inv2c } s'
\end{array}
\]
\[\text{proof}\]
theorem HStartBallot-Inv2c:
  assumes inv: Inv2c s
  and act: HStartBallot s s' p
  and inv2a: Inv2a s
  shows Inv2c s'  
 ⟨proof⟩

theorem HPhase1or2Write-Inv2c:
  assumes inv: Inv2c s
  and act: HPhase1or2Write s s' p d
  and inv2a: Inv2a s
  shows Inv2c s'  
 ⟨proof⟩

theorem HPhase1or2ReadElse-Inv2c:
  \[ \[ Inv2c s; HPhase1or2ReadElse s s' p d q; Inv2a s \] \implies Inv2c s' \]
 ⟨proof⟩

theorem HEndPhase1-Inv2c:
  assumes inv: Inv2c s
  and act: HEndPhase1 s s' p
  and inv2a: Inv2a s
  and inv1: HInv1 s
  shows Inv2c s'  
 ⟨proof⟩

theorem HEndPhase2-Inv2c:
  assumes inv: Inv2c s
  and act: HEndPhase2 s s' p
  and inv2a: Inv2a s
  shows Inv2c s'  
 ⟨proof⟩

theorem HFail-Inv2c:
  assumes inv: Inv2c s
  and act: HFail s s' p
  and inv2a: Inv2a s
  shows Inv2c s'  
 ⟨proof⟩

theorem HPhase0Read-Inv2c:
  assumes inv: Inv2c s
  and act: HPhase0Read s s' p d
  and inv2a: Inv2a s
  shows Inv2c s'  
 ⟨proof⟩

theorem HEndPhase0-Inv2c:
assumes \text{inv: Inv2c \ s}
and \text{act: HEndPhase0 \ s \ s' \ p}
and \text{inv2a: Inv2a \ s}
and \text{inv1: Inv1 \ s}
shows \text{Inv2c \ s'}

\langle proof \rangle

\text{theorem HInit-HInv2:}
\text{HInit \ s} \implies \text{HInv2 \ s}

\langle proof \rangle

\text{HInv1} \land \text{HInv2} \text{ is an invariant of HNext.}

\text{lemma I2b:}
assumes \text{nxt: HNext \ s \ s'}
and \text{inv: HInv1 \ s} \land \text{HInv2 \ s}
shows \text{HInv2 \ s'}

\langle proof \rangle

end

theory DiskPaxos-Inv3 imports DiskPaxos-Inv2 begin

C.3 Invariant 3

This invariant says that if two processes have read each other’s block from disk \( d \) during their current phases, then at least one of them has read the other’s current block.

definition HInv3-L :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Disk} \Rightarrow \text{bool}
where
\text{HInv3-L \ s \ p \ q \ d} = \text{(phase \ s \ p} \in \{1,2\} \land \text{phase \ s \ q} \in \{1,2\} \land \text{hasRead \ s \ p \ d \ q} \land \text{hasRead \ s \ q \ d \ p)}

definition HInv3-R :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Disk} \Rightarrow \text{bool}
where
\text{HInv3-R \ s \ p \ q \ d} = ( (\text{\{block= dblock \ s \ q, proc= q\}}) \in \text{blocksRead \ s \ p \ d} \lor (\text{\{block= dblock \ s \ p, proc= p\}}) \in \text{blocksRead \ s \ q \ d} )

definition HInv3-inner :: \text{state} \Rightarrow \text{Proc} \Rightarrow \text{Proc} \Rightarrow \text{Disk} \Rightarrow \text{bool}
where
\text{HInv3-inner \ s \ p \ q \ d} = (\text{HInv3-L \ s \ p \ q \ d} \implies \text{HInv3-R \ s \ p \ q \ d})

definition HInv3 :: \text{state} \Rightarrow \text{bool}
where
\text{HInv3 \ s} = (\forall \ p \ q \ d. \text{HInv3-inner \ s \ p \ q \ d})

C.3.1 Proofs of Invariant 3

\text{theorem HInit-HInv3: HInit \ s} \implies \text{HInv3 \ s}
proof

lemma InitPhase-HInv3-p:
[ InitializePhase s s' p; HInv3-L s' p q d ] \implies HInv3-R s' p q d

(proof)

lemma InitPhase-HInv3-q:
[ InitializePhase s s' q; HInv3-L s' p q d ] \implies HInv3-R s' p q d

(proof)

lemma HInv3-L-sym: HInv3-L s p q d \implies HInv3-L s q p d

(proof)

lemma HInv3-R-sym: HInv3-R s p q d \implies HInv3-R s q p d

(proof)

lemma Phase1or2ReadThen-HInv3-pq:
assumes act: Phase1or2ReadThen s s' p d q
and inv-L': HInv3-L s' p q d
and pq: p \neq q
and inv2b: Inv2b s
shows HInv3-R s' p q d

(proof)

lemma Phase1or2ReadThen-HInv3-hasRead:
[ \neg hasRead s pp dd qq;
  Phase1or2ReadThen s s' p d q;
  pp \neq p \lor qq \neq q \lor dd \neq d ]
\implies \neg hasRead s' pp dd qq

(proof)

theorem HPhase1or2ReadThen-HInv3:
assumes act: HPhase1or2ReadThen s s' p d q
and inv: HInv3 s
and pq: p \neq q
and inv2b: Inv2b s
shows HInv3 s'

(proof)

lemma StartBallot-HInv3-p:
[ StartBallot s s' p; HInv3-L s' p q d ]
\implies HInv3-R s' p q d

(proof)

lemma StartBallot-HInv3-q:
[ StartBallot s s' q; HInv3-L s' p q d ]
\implies HInv3-R s' p q d

(proof)
lemma StartBallot-HInv3-nL:
\[
[ \text{StartBallot } s s' t; \neg \text{HInv3-L } s p q d; t \neq p; t \neq q ] \\
\implies \neg \text{HInv3-L } s' p q d
\]
\langle proof \rangle

lemma StartBallot-HInv3-R:
\[
[ \text{StartBallot } s s' t; \text{HInv3-R } s p q d; t \neq p; t \neq q ] \\
\implies \text{HInv3-R } s' p q d
\]
\langle proof \rangle

lemma StartBallot-HInv3-t:
\[
[ \text{StartBallot } s s' t; \text{HInv3-inner } s p q d; t \neq p; t \neq q ] \\
\implies \text{HInv3-inner } s' p q d
\]
\langle proof \rangle

lemma StartBallot-HInv3:
\[
\text{assumes act: StartBallot } s s' t \\
\text{and inv: HInv3-inner } s p q d \\
\text{shows } \text{HInv3-inner } s' p q d
\]
\langle proof \rangle

theorem HStartBallot-HInv3:
\[
[ \text{HStartBallot } s s' p; \text{HInv3 } s ] \\
\implies \text{HInv3 } s'
\]
\langle proof \rangle

theorem HPhase1or2ReadElse-HInv3:
\[
[ \text{HPhase1or2ReadElse } s s' p d q; \text{HInv3 } s ] \\
\implies \text{HInv3 } s'
\]
\langle proof \rangle

theorem HPhase1or2Write-HInv3:
\[
\text{assumes act: HPhase1or2Write } s s' p d \\
\text{and inv: HInv3 } s \\
\text{shows } \text{HInv3 } s'
\]
\langle proof \rangle

lemma EndPhase1-HInv3-p:
\[
[ \text{EndPhase1 } s s' p; \text{HInv3-L } s' p q d ] \\
\implies \text{HInv3-R } s' p q d
\]
\langle proof \rangle

lemma EndPhase1-HInv3-q:
\[
[ \text{EndPhase1 } s s' q; \text{HInv3-L } s' p q d ] \\
\implies \text{HInv3-R } s' p q d
\]
\langle proof \rangle

lemma EndPhase1-HInv3-nL:
\[
[ \text{EndPhase1 } s s' t; \neg \text{HInv3-L } s p q d; t \neq p; t \neq q ] \\
\implies \neg \text{HInv3-L } s' p q d
\]
\langle proof \rangle

lemma EndPhase1-HInv3-R:
\[ \text{lemma EndPhase1-HInv3-t:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase1 s s' t} \\
\text{and inv: HInv3-inner s p q d} \\
\text{shows HInv3-inner s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase1-HInv3:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase1 s s' t} \\
\text{and inv: HInv3-inner s p q d} \\
\text{shows HInv3-inner s' p q d}
\end{array} \]

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

\[ \text{theorem HEndPhase1-HInv3:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase1 s s' t} \\
\text{and inv: HInv3-inner s p q d} \\
\text{shows HInv3-inner s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase2-HInv3-p:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase2 s s' t} \\
\text{and inv: HInv3-L s' p q d} \\
\text{shows HInv3-L s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase2-HInv3-q:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase2 s s' t} \\
\text{and inv: HInv3-L s' p q d} \\
\text{shows HInv3-L s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase2-HInv3-nL:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase2 s s' t} \\
\text{and inv: HInv3-L s' p q d} \\
\text{shows HInv3-L s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase2-HInv3-R:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase2 s s' t} \\
\text{and inv: HInv3-L s' p q d} \\
\text{shows HInv3-L s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase2-HInv3-t:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase2 s s' t} \\
\text{and inv: HInv3-L s' p q d} \\
\text{shows HInv3-L s' p q d}
\end{array} \]

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

\[ \text{lemma EndPhase2-HInv3:} \]
\[ \begin{array}{l}
\text{assumes act: EndPhase2 s s' t} \\
\text{and inv: HInv3-L s' p q d} \\
\text{shows HInv3-L s' p q d}
\end{array} \]

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

\[ \text{theorem HEndPhase2-HInv3:} \]
lemma Fail-HInv3-p:
\[
[\text{Fail } s \ s' \ p \ HInv3 \ s \ L] \implies HInv3 \ s' \ R \ s \ p \ q \ d
\] (proof)

lemma Fail-HInv3-q:
\[
[\text{Fail } s \ s' \ q \ HInv3 \ s \ L] \implies HInv3 \ s' \ R \ s \ p \ q \ d
\] (proof)

lemma Fail-HInv3-nL:
\[
[\text{Fail } s \ s' \ t; \neg HInv3 \ s \ p \ q \ d; \ t \neq p; \ t \neq q]
\implies \neg HInv3 \ s' \ p \ q \ d
\] (proof)

lemma Fail-HInv3-R:
\[
[\text{Fail } s \ s' \ t; HInv3 \ s \ R \ s \ p \ q \ d; t \neq p; t \neq q]
\implies HInv3 \ s' \ R \ s \ p \ q \ d
\] (proof)

lemma Fail-HInv3-t:
\[
[\text{Fail } s \ s' \ t; HInv3-\text{inner } s \ p \ q \ d; t \neq p; t \neq q]
\implies HInv3-\text{inner} \ s' \ p \ q \ d
\] (proof)

lemma Fail-HInv3:
\begin{align*}
&\text{assumes act: Fail } s \ s' \ t \\
&\text{and inv: HInv3-\text{inner } s \ p \ q \ d} \\
&\text{shows HInv3-\text{inner } s' \ p \ q \ d}
\end{align*}
(proof)

theorem HFail-HInv3:
\[
[\text{HFail } s \ s' \ p \ HInv3 \ s \ L] \implies HInv3 \ s' \ p \ q \ d
\] (proof)

theorem HPhase0Read-HInv3:
\begin{align*}
&\text{assumes act: HPhase0Read } s \ s' \ p \ d \\
&\text{and inv: HInv3 } s
\end{align*}
\text{shows HInv3 } s'
(proof)

lemma EndPhase0-HInv3-p:
\[
[\text{EndPhase0 } s \ s' \ p \ HInv3 \ s \ L] \implies HInv3 \ s' \ R \ s \ p \ q \ d
\] (proof)

lemma EndPhase0-HInv3-q:
\[
[\text{EndPhase0 } s \ s' \ q \ HInv3 \ s \ L] \implies HInv3 \ s' \ R \ s \ p \ q \ d
\]
HInv3-R s' p q d

lemma EndPhase0-HInv3-R:
\[
\[ \text{EndPhase0 } s \ s' \ t; \ HInv3-R \ s \ p \ q \ d; \ t \neq p; \ t \neq q \] \implies HInv3-R \ s' \ p \ q \ d
\]

lemma EndPhase0-HInv3-L:
\[
\[ \text{EndPhase0 } s \ s' \ t; \ HInv3-L \ s \ p \ q \ d; \ t \neq p; \ t \neq q \] \implies HInv3-L \ s' \ p \ q \ d
\]

lemma EndPhase0-HInv3-t:
\[
\[ \text{EndPhase0 } s \ s' \ t; \ HInv3-inner \ s \ p \ q \ d; \ t \neq p; \ t \neq q \] \implies HInv3-inner \ s' \ p \ q \ d
\]

lemma EndPhase0-HInv3:
\[
\begin{align*}
\text{assumes} & \quad \text{act: EndPhase0 } s \ s' \ t \\
\text{and} & \quad \text{inv: HInv3-inner } s \ p \ q \ d \\
\text{shows} & \quad \text{HInv3-inner } s' \ p \ q \ d
\end{align*}
\]

theorem HEndPhase0-HInv3:
\[
\begin{align*}
\text{assumes} & \quad \text{nxt: HNext } s \ s' \\
\text{and} & \quad \text{inv: HInv1 } s \land HInv2 \ s \land HInv3 \ s \\
\text{shows} & \quad \text{HInv3 } s' 
\end{align*}
\]

HInv1 \land HInv2 \land HInv3 is an invariant of HNext.

lemma I2c:
\[
\begin{align*}
\text{assumes} & \quad \text{nxt: HNext } s \ s' \\
\text{and} & \quad \text{inv: HInv1 } s \land HInv2 s \land HInv3 s \\
\text{shows} & \quad \text{HInv3 } s' 
\end{align*}
\]

end

theory DiskPaxos-Inv4 imports DiskPaxos-Inv2 begin

C.4 Invariant 4

This invariant expresses relations among mbal and bal values of a processor and of its disk blocks. HInv4a asserts that, when p is not recovering from a failure, its mbal value is at least as large as the bal field of any of its blocks, and at least as large as the mbal field of its block on some disk in any majority set. HInv4b conjunct asserts that, in phase 1, its mbal value is actually greater than the bal field of any of its blocks. HInv4c asserts that, in phase 2, its bal value is the mbal field of all its blocks on some majority
set of disks. \( HInv4d \) asserts that the \( bal \) field of any of its blocks is at most as large as the \( mbal \) field of all its disk blocks on some majority set of disks.

**definition** `MajoritySet` :: Disk set set

where `MajoritySet = \{ D. IsMajority(D) \}

**definition** `HInv4a1` :: state ⇒ Proc ⇒ bool

where `HInv4a1 s p = (∀ bk ∈ blocksOf s p. bal bk ≤ mbal (dblock s p))

**definition** `HInv4a2` :: state ⇒ Proc ⇒ bool

where `HInv4a2 s p = (∀ D ∈ MajoritySet. (∃ d ∈ D. mbal(disk s d p) ≤ mbal(dblock s p)) ∧ bal(disk s d p) ≤ bal(dblock s p)))

**definition** `HInv4a` :: state ⇒ Proc ⇒ bool

where `HInv4a s p = (phase s p ≠ 0 → HInv4a1 s p ∧ HInv4a2 s p)

**definition** `HInv4b` :: state ⇒ Proc ⇒ bool

where `HInv4b s p = (phase s p = 1 → (∀ bk ∈ blocksOf s p. bal bk < mbal(dblock s p)))

**definition** `HInv4c` :: state ⇒ Proc ⇒ bool

where `HInv4c s p = (phase s p ∈ \{ 2, 3 \} → (∃ D ∈ MajoritySet. \∀ d ∈ D. mbal(disk s d p) = bal(dblock s p))

**definition** `HInv4d` :: state ⇒ Proc ⇒ bool

where `HInv4d s p = (∀ bk ∈ blocksOf s p. ∃ D ∈ MajoritySet. bal bk ≤ mbal(disk s d p))

**definition** `HInv4` :: state ⇒ bool

where `HInv4 s = (∀ p. HInv4a s p ∧ HInv4b s p ∧ HInv4c s p ∧ HInv4d s p)

The initial state implies Invariant 4.

**theorem** `HInit-HInv4`: `HInit s ⇒ HInv4 s`

⟨proof⟩

To prove that the actions preserve \( HInv4 \), we do it for one conjunct at a time.

For each action `actionss'q` and conjunct \( x \in a, b, c, d \) of \( HInv4xs'p \), we prove two lemmas. The first lemma `action-HInv4x-p` proves the case of \( p = q \), while lemma `action-HInv4x-q` proves the other case.

### C.4.1 Proofs of Invariant 4a

**lemma** `HStartBallot-HInv4a1`:

**assumes** `act: HStartBallot s s' p` and `inv: HInv4a1 s p` and `inv2a: Inv2a-inner s' p`
shows $HInv4a1 \ s' \ p$

lemma *HStartBallot-HInv4a2*:  
assumes act: $HStartBallot \ s \ s' \ p$  
and inv: $HInv4a2 \ s \ p$  
shows $HInv4a2 \ s' \ p$

(\proof)

lemma *HStartBallot-HInv4a-p*:  
assumes act: $HStartBallot \ s \ s' \ p$  
and inv: $HInv4a \ s \ p$  
and inv2a: $Inv2a-inner \ s' \ p$  
shows $HInv4a \ s' \ p$

(\proof)

lemma *HStartBallot-HInv4a-q*:  
assumes act: $HStartBallot \ s \ s' \ p$  
and inv: $HInv4a \ s \ q$  
and pnq: $p \neq q$  
shows $HInv4a \ s' \ q$

(\proof)

theorem *HStartBallot-HInv4a*:  
assumes act: $HStartBallot \ s \ s' \ p$  
and inv: $HInv4a \ s \ q$  
and inv2a: $Inv2a \ s'$  
shows $HInv4a \ s' \ q$

(\proof)

lemma *Phase1or2Write-HInv4a1*:  
[ $Phase1or2Write \ s \ s' \ p \ d \ ; \ HInv4a1 \ s \ q \ ] \implies HInv4a1 \ s' \ q$

(\proof)

lemma *Phase1or2Write-HInv4a2*:  
[ $Phase1or2Write \ s \ s' \ p \ d \ ; \ HInv4a2 \ s \ q \ ] \implies HInv4a2 \ s' \ q$

(\proof)

theorem *HPhase1or2Write-HInv4a*:  
assumes act: $HPhase1or2Write \ s \ s' \ p \ d$  
and inv: $HInv4a \ s \ q$  
shows $HInv4a \ s' \ q$

(\proof)

lemma *HPhase1or2ReadThen-HInv4a1-p*:  
assumes act: $HPhase1or2ReadThen \ s \ s' \ p \ d \ q$  
and inv: $HInv4a1 \ s \ p$  
shows $HInv4a1 \ s' \ p$

(\proof)
lemma $H_{\text{Phase1or2ReadThen}} - H_{\text{Inv4a2}}$:
\[ [H_{\text{Phase1or2ReadThen}} s s' p d r; H_{\text{Inv4a2}} s q ] \Rightarrow H_{\text{Inv4a2}} s' q \]
(proof)

lemma $H_{\text{Phase1or2ReadThen}} - H_{\text{Inv4a-p}}$:
assumes act: $H_{\text{Phase1or2ReadThen}} s s' p d r$
and inv: $H_{\text{Inv4a}} s p$
and inv2b: $H_{\text{Inv2b}} s$
shows $H_{\text{Inv4a}} s' p$
(proof)

lemma $H_{\text{Phase1or2ReadThen}} - H_{\text{Inv4a-q}}$:
assumes act: $H_{\text{Phase1or2ReadThen}} s s' p d r$
and inv: $H_{\text{Inv4a}} s q$
and $\text{pnq: } p \neq q$
shows $H_{\text{Inv4a}} s' q$
(proof)

theorem $H_{\text{Phase1or2ReadThen}} - H_{\text{Inv4a}}$:
\[ [H_{\text{Phase1or2ReadThen}} s s' p d r; H_{\text{Inv4a}} s q; H_{\text{Inv2b}} s ] \Rightarrow H_{\text{Inv4a}} s' q \]
(proof)

theorem $H_{\text{Phase1or2ReadElse}} - H_{\text{Inv4a}}$:
assumes act: $H_{\text{Phase1or2ReadElse}} s s' p d r$
and inv: $H_{\text{Inv4a}} s q$ and inv2a: $H_{\text{Inv2a}} s'$
shows $H_{\text{Inv4a}} s' q$
(proof)

lemma $H_{\text{EndPhase1}} - H_{\text{Inv4a1}}$:
assumes act: $H_{\text{EndPhase1}} s s' p$
and inv: $H_{\text{Inv4a1}} s p$
shows $H_{\text{Inv4a1}} s' p$
(proof)

lemma $H_{\text{EndPhase1}} - H_{\text{Inv4a2}}$:
assumes act: $H_{\text{EndPhase1}} s s' p$
and inv: $H_{\text{Inv4a2}} s p$
and inv2a: $H_{\text{Inv2a}} s$
shows $H_{\text{Inv4a2}} s' p$
(proof)

lemma $H_{\text{EndPhase1}} - H_{\text{Inv4a-p}}$:
assumes act: $H_{\text{EndPhase1}} s s' p$
and inv: $H_{\text{Inv4a}} s p$
and inv2a: $H_{\text{Inv2a}} s$
shows $H_{\text{Inv4a}} s' p$
(proof)
lemma \textit{HEndPhase1-HInv4a-q}:
assumes act \text{:} HEndPhase1 \ s \ s' \ p
and inv \text{:} HInv4a \ s \ q
and \textit{pnq}: p\neq q
shows HInv4a \ s' \ q
\langle \text{proof} \rangle

theorem \textit{HEndPhase1-HInv4a}:
[ HEndPhase1 \ s \ s' \ p; \ HInv4a \ s \ q; \ Inv2a \ s ] \Rightarrow HInv4a \ s' \ q
\langle \text{proof} \rangle

theorem \textit{HFail-HInv4a}:
[ HFail \ s \ s' \ p; \ HInv4a \ s \ q ] \Rightarrow HInv4a \ s' \ q
\langle \text{proof} \rangle

theorem \textit{HPhase0Read-HInv4a}:
[ HPhase0Read \ s \ s' \ p \ d; \ HInv4a \ s \ q ] \Rightarrow HInv4a \ s' \ q
\langle \text{proof} \rangle

theorem \textit{HEndPhase2-HInv4a}:
[ HEndPhase2 \ s \ s' \ p; \ HInv4a \ s \ q ] \Rightarrow HInv4a \ s' \ q
\langle \text{proof} \rangle

lemma \textit{allSet}:
assumes aPQ: \forall a. \forall r \in P a. Q r \text{ and } rb: rb \in P d
shows Q rb
\langle \text{proof} \rangle

lemma \textit{EndPhase0-44}:
assumes act \text{:} EndPhase0 \ s \ s' \ p
and \textit{bk}: bk \in \text{blocksOf} s \ p
and inv4d: HInv4d \ s \ p
and inv2c: Inv2c-inner \ s \ p
shows \exists d. \exists rb \in \text{blocksRead} s \ p \ d. \ bal bk \leq \text{mbal(block rb)}
\langle \text{proof} \rangle

lemma \textit{HEndPhase0-HInv4a1-p}:
assumes act \text{:} HEndPhase0 \ s \ s' \ p
and inv2a': Inv2a \ s'
and inv2c: Inv2c-inner \ s \ p
and inv4d: HInv4d \ s \ p
shows HInv4a1 \ s' \ p
\langle \text{proof} \rangle

lemma \textit{hasRead-allBlks}:
assumes inv2c: Inv2c-inner \ s \ p
and \textit{phase}: phase \ s \ p = 0
shows (\forall d \in \{d. \text{hasRead} s \ p \ d \ p\}, \text{disk} s \ d \ p \in \text{allBlocksRead} s \ p)
\langle \text{proof} \rangle
lemma $H_{\text{EndPhase0-41}}$:
assumes act: $H_{\text{EndPhase0}} \ s \ s' \ p$
and inv1: Inv1 $s$
and inv2c: Inv2c-inner $s \ p$
shows $\exists \ D \in \text{MajoritySet}. \ \forall \ d \in D. \ \text{mbal}(\text{disk} \ s \ d \ p) \leq \text{mbal}(\text{dblock} \ s' \ p)$
\land \ \text{bal}(\text{disk} \ s \ d \ p) \leq \text{bal}(\text{dblock} \ s' \ p)$
\langle proof \rangle

lemma $\text{Majority-exQ}$:
assumes asm1: $\exists \ D \in \text{MajoritySet}. \ \forall \ d \in D. \ \text{P} \ d$
shows $\forall \ D \in \text{MajoritySet}. \ \exists \ d \in D. \ \text{P} \ d$
\langle proof \rangle

lemma $H_{\text{EndPhase0-HInv4a2-p}}$:
assumes act: $H_{\text{EndPhase0}} \ s \ s' \ p$
and inv1: Inv1 $s$
and inv2c: Inv2c-inner $s \ p$
shows $H_{\text{Inv4a2}} \ s' \ p$
\langle proof \rangle

lemma $H_{\text{EndPhase0-HInv4a-p}}$:
assumes act: $H_{\text{EndPhase0}} \ s \ s' \ p$
and inv2a: Inv2a $s$
and inv2: Inv2c $s$
and inv4d: $H_{\text{Inv4d}} \ s \ p$
and inv1: Inv1 $s$
and inv: $H_{\text{Inv4a}} \ s \ p$
shows $H_{\text{Inv4a}} \ s' \ p$
\langle proof \rangle

lemma $H_{\text{EndPhase0-HInv4a-q}}$:
assumes act: $H_{\text{EndPhase0}} \ s \ s' \ p$
and inv: $H_{\text{Inv4a}} \ s \ q$
and pnq: $p \neq q$
shows $H_{\text{Inv4a}} \ s' \ q$
\langle proof \rangle

theorem $H_{\text{EndPhase0-HInv4a}}$:
\[[ H_{\text{EndPhase0}} \ s' \ p ; \ H_{\text{Inv4a}} \ s \ q ; \ H_{\text{Inv4d}} \ s \ p ; \ Inv2a \ s ; \ Inv1 \ s ; \ Inv2a \ s ; \ Inv2c \ s ] \]
\implies H_{\text{Inv4a}} \ s' \ q$
\langle proof \rangle
c.4.2 Proofs of Invariant 4b

lemma $\text{blocksRead-allBlocksRead}$:
rb $\in$ blocksRead $s \ p \ d \implies \text{block} \ rb \in \text{allBlocksRead} \ s \ p$

40
proof

lemma HEndPhase0-dblock-mbal:
[ HEndPhase0 s s' p ]
\[ \implies \forall \text{br} \in \text{allBlocksRead}\ s\ p.\ \text{mbal}\ br < \text{mbal}(\text{dblock}\ s'\ p) \]

⟨proof⟩

lemma HEndPhase0-HInv4b-p-dblock:
assumes act: HEndPhase0 s s' p
and inv1: Inv1 s
and inv2a: Inv2a s
and inv2c: Inv2c-inner s p
shows bal(dblock s' p) < mbal(dblock s' p)

⟨proof⟩

lemma HEndPhase0-HInv4b-p-blocksOf:
assumes act: HEndPhase0 s s' p
and inv4d: HInv4d s p
and inv2c: Inv2c-inner s p
and bk: bk \in blocksOf s p
shows bal bk < mbal(dblock s' p)

⟨proof⟩

lemma HEndPhase0-HInv4b-p:
assumes act: HEndPhase0 s s' p
and inv4d: HInv4d s p
and inv1: Inv1 s
and inv2a: Inv2a s
and inv2c: Inv2c-inner s p
shows HInv4b s' p

⟨proof⟩

lemma HEndPhase0-HInv4b-q:
assumes act: HEndPhase0 s s' p
and pnq: p \neq q
and inv: HInv4b s q
shows HInv4b s' q

⟨proof⟩

theorem HEndPhase0-HInv4b:
assumes act: HEndPhase0 s s' p
and inv: HInv4b s q
and inv4d: HInv4d s q
and inv1: Inv1 s
and inv2a: Inv2a s
and inv2c: Inv2c-inner s q
shows HInv4b s' q

⟨proof⟩
lemma $H\text{StartBallot-}\text{HInv4b-}p$:
assumes act: $H\text{StartBallot}$ $s$ $s'$ $p$
and inv2a: $\text{Inv2a-innermost}$ $s$ $p$ ($\text{dblock}$ $s$ $p$)
and inv4b: $\text{HInv4b}$ $s$ $p$
shows $\text{HInv4b}$ $s'$ $p$
(proof)

lemma $H\text{StartBallot-}\text{HInv4b-}q$:
assumes act: $H\text{StartBallot}$ $s$ $s'$ $p$
and pnq: $p \neq q$
and inv: $\text{HInv4b}$ $s$ $q$
shows $\text{HInv4b}$ $s'$ $q$
(proof)

theorem $H\text{StartBallot-}\text{HInv4b}$:
assumes act: $H\text{StartBallot}$ $s$ $s'$ $p$
and inv2a: $\text{Inv2a}$ $s$
and inv4b: $\text{HInv4b}$ $s$ $q$
and inv4a: $\text{HInv4a}$ $s$ $p$
shows $\text{HInv4b}$ $s'$ $q$
(proof)

theorem $H\text{Phase1or2Write-}\text{HInv4b}$:
$[ [H\text{Phase1or2Write} \; s \; s' \; d \; q; \; \text{HInv4b} \; s \; q ] \implies \text{HInv4b} \; s' \; q ]$
(proof)

lemma $H\text{Phase1or2ReadThen-}\text{HInv4b-}p$:
assumes act: $H\text{Phase1or2ReadThen}$ $s$ $s'$ $p$ $d$ $q$
and inv: $\text{HInv4b}$ $s$ $p$
shows $\text{HInv4b}$ $s'$ $p$
(proof)

lemma $H\text{Phase1or2ReadThen-}\text{HInv4b-}q$:
assumes act: $H\text{Phase1or2ReadThen}$ $s$ $s'$ $p$ $d$ $r$
and inv: $\text{HInv4b}$ $s$ $q$
and pnq: $p \neq q$
shows $\text{HInv4b}$ $s'$ $q$
(proof)

theorem $H\text{Phase1or2ReadThen-}\text{HInv4b}$:
$[ [H\text{Phase1or2ReadThen} \; s \; s' \; p \; d \; q; \; \text{HInv4b} \; s \; r ] \implies \text{HInv4b} \; s' \; r ]$
(proof)

theorem $H\text{Phase1or2ReadElse-}\text{HInv4b}$:
$[ [H\text{Phase1or2ReadElse} \; s \; s' \; p \; d \; q; \; \text{HInv4b} \; s \; r;$
$\text{Inv2a} \; s; \; \text{HInv4a} \; s \; p ] ]$
$\implies \text{HInv4b} \; s' \; r$

42
lemma HEndPhase1-HInv4b-p:
HEndPhase1 s s' p \implies HInv4b s' p
⟨proof⟩

lemma HEndPhase1-HInv4b-q:
assumes act: HEndPhase1 s s' p
and p\neq q
and inv: HInv4b s q
shows HInv4b s' q
⟨proof⟩

theorem HEndPhase1-HInv4b:
assumes act: HEndPhase1 s s' p
and inv: HInv4b s s' q
shows HInv4b s' q
⟨proof⟩

lemma HEndPhase2-HInv4b-p:
HEndPhase2 s s' p \implies HInv4b s' p
⟨proof⟩

lemma HEndPhase2-HInv4b-q:
assumes act: HEndPhase2 s s' p
and p\neq q
and inv: HInv4b s q
shows HInv4b s' q
⟨proof⟩

theorem HEndPhase2-HInv4b:
assumes act: HEndPhase2 s s' p
and inv: HInv4b s s' q
shows HInv4b s' q
⟨proof⟩

lemma HFail-HInv4b-p:
HFail s s' p \implies HInv4b s' p
⟨proof⟩

lemma HFail-HInv4b-q:
assumes act: HFail s s' p
and p\neq q
and inv: HInv4b s q
shows HInv4b s' q
⟨proof⟩

theorem HFail-HInv4b:
assumes act: HFail s s' p
and inv: Hinv4b s q
shows Hinv4b s' q
(proof)

lemma HPhase0Read-Hinv4b-p:
HPhase0Read s s' p d \implies Hinv4b s' p
(proof)

lemma HPhase0Read-Hinv4b-q:
assumes act: HPhase0Read s s' p d
and pnq: p \neq q
and inv: Hinv4b s q
shows Hinv4b s' q
(proof)

theorem HPhase0Read-Hinv4b:
assumes act: HPhase0Read s s' p d
and inv: Hinv4b s q
shows Hinv4b s' q
(proof)

C.4.3 Proofs of Invariant 4c

lemma HStartBallot-Hinv4c-p:
[ HStartBallot s s' p; Hinv4c s p ] \implies Hinv4c s' p
(proof)

lemma HStartBallot-Hinv4c-q:
assumes act: HStartBallot s s' p
and inv: Hinv4c s q
and pnq: p \neq q
shows Hinv4c s' q
(proof)

theorem HStartBallot-Hinv4c:
[ HStartBallot s s' p; Hinv4c s q ] \implies Hinv4c s' q
(proof)

lemma HPhase1or2Write-Hinv4c-p:
assumes act: HPhase1or2Write s s' p d
and inv: Hinv4c s p
and inv2c: Inv2c s
shows Hinv4c s' p
(proof)

lemma HPhase1or2Write-Hinv4c-q:
assumes act: HPhase1or2Write s s' p d
and inv: Hinv4c s q
and pnq: p \neq q
shows $HInv4c \ s' \ q$

(\textit{proof})

\textbf{theorem} \ HPhase1or2Write-$HInv4c$:
\[
\begin{array}{l}
[ HPhase1or2Write \ s \ s' \ p \ d; \ HInv4c \ s \ q; \ Inv2c \ s ]
\implies HInv4c \ s' \ q
\end{array}
\]

(\textit{proof})

\textbf{lemma} \ HPhase1or2ReadThen-$HInv4c$-p:
\[
\begin{array}{l}
[ HPhase1or2ReadThen \ s \ s' \ p \ d \ q; \ HInv4c \ s \ p ] \implies HInv4c \ s' \ p
\end{array}
\]

(\textit{proof})

\textbf{lemma} \ HPhase1or2ReadThen-$HInv4c$-q:
\begin{itemize}
  \item \textbf{assumes} \ act: \ HPhase1or2ReadThen \ s \ s' \ p \ d \ r
  \item \textbf{and} \ inv: \ HInv4c \ s \ q
  \item \textbf{and} \ pnq: \ p \neq q
\end{itemize}
\textbf{shows} \ HInv4c \ s' \ q

(\textit{proof})

\textbf{theorem} \ HPhase1or2ReadThen-$HInv4c$:
\[
\begin{array}{l}
[ HPhase1or2ReadThen \ s \ s' \ p \ d \ r; \ HInv4c \ s \ q ]
\implies HInv4c \ s' \ q
\end{array}
\]

(\textit{proof})

\textbf{theorem} \ HPhase1or2ReadElse-$HInv4c$:
\[
\begin{array}{l}
[ HPhase1or2ReadElse \ s \ s' \ p \ d \ r; \ HInv4c \ s \ q ] \implies HInv4c \ s' \ q
\end{array}
\]

(\textit{proof})

\textbf{lemma} \ HEndPhase1-$HInv4c$-p:
\begin{itemize}
  \item \textbf{assumes} \ act: \ HEndPhase1 \ s \ s' \ p
  \item \textbf{and} \ inv2b: \ Inv2b \ s
\end{itemize}
\textbf{shows} \ HInv4c \ s' \ p

(\textit{proof})

\textbf{lemma} \ HEndPhase1-$HInv4c$-q:
\begin{itemize}
  \item \textbf{assumes} \ act: \ HEndPhase1 \ s \ s' \ p
  \item \textbf{and} \ inv: \ HInv4c \ s \ q
  \item \textbf{and} \ pnq: \ p \neq q
\end{itemize}
\textbf{shows} \ HInv4c \ s' \ q

(\textit{proof})

\textbf{theorem} \ HEndPhase1-$HInv4c$:
\[
\begin{array}{l}
[ HEndPhase1 \ s \ s' \ p; \ HInv4c \ s \ q; \ Inv2b \ s ] \implies HInv4c \ s' \ q
\end{array}
\]

(\textit{proof})

\textbf{lemma} \ HEndPhase2-$HInv4c$-p:
\[
[ HEndPhase2 \ s \ s' \ p; \ HInv4c \ s \ p ] \implies HInv4c \ s' \ p
\]

(\textit{proof})
lemma HEndPhase2-HInv4c-q:
  assumes act: HEndPhase2 s s' p
  and inv: HInv4c s q
  and pnq: p ≠ q
  shows HInv4c s' q
 ⟨proof⟩

theorem HEndPhase2-HInv4c:
  [ HEndPhase2 s s' p; HInv4c s q] ⇒ HInv4c s' q
 ⟨proof⟩

lemma HFail-HInv4c-p:
  [ HFail s s' p; HInv4c s p] ⇒ HInv4c s' p
 ⟨proof⟩

lemma HFail-HInv4c-q:
  assumes act: HFail s s' p
  and inv: HInv4c s q
  and pnq: p ≠ q
  shows HInv4c s' q
 ⟨proof⟩

theorem HFail-HInv4c:
  [ HFail s s' p; HInv4c s q] ⇒ HInv4c s' q
 ⟨proof⟩

lemma HPhase0Read-HInv4c-p:
  [ HPhase0Read s s' p d; HInv4c s p] ⇒ HInv4c s' p
 ⟨proof⟩

lemma HPhase0Read-HInv4c-q:
  assumes act: HPhase0Read s s' p d
  and inv: HInv4c s q
  and pnq: p ≠ q
  shows HInv4c s' q
 ⟨proof⟩

theorem HPhase0Read-HInv4c:
  [ HPhase0Read s s' p d; HInv4c s q] ⇒ HInv4c s' q
 ⟨proof⟩

lemma HEndPhase0-HInv4c-p:
  [ HEndPhase0 s s' p; HInv4c s p] ⇒ HInv4c s' p
 ⟨proof⟩

lemma HEndPhase0-HInv4c-q:
  assumes act: HEndPhase0 s s' p
  and inv: HInv4c s q
  and pnq: p ≠ q
shows $H_{\text{Inv4c}}(s, q)$

(Proof)

**Theorem HEndPhase0-HInv4c**: \[ [H_{\text{EndPhase0}}(s, s', p); H_{\text{Inv4c}}(s, q)] \implies H_{\text{Inv4c}}(s', q) \]

(Proof)

### C.4.4 Proofs of Invariant 4d

**Lemma HStartBallot-HInv4d-p**:  
*assumes* act: $H_{\text{StartBallot}}(s, s', p)$  
*and* inv: $H_{\text{Inv4d}}(s, p)$  
*shows* $H_{\text{Inv4d}}(s', p)$

(Proof)

**Lemma HStartBallot-HInv4d-q**:  
*assumes* act: $H_{\text{StartBallot}}(s, s', p)$  
*and* inv: $H_{\text{Inv4d}}(s, q)$  
and $p \neq q$  
*shows* $H_{\text{Inv4d}}(s', q)$

(Proof)

**Theorem HStartBallot-HInv4d**: \[ [H_{\text{StartBallot}}(s, s', p); H_{\text{Inv4d}}(s, q)] \implies H_{\text{Inv4d}}(s', q) \]

(Proof)

**Lemma HPhase1or2Write-HInv4d-p**:  
*assumes* act: $H_{\text{Phase1or2Write}}(s, s', p, d)$  
*and* inv: $H_{\text{Inv4d}}(s, p)$  
*and* inv4a: $H_{\text{Inv4a}}(s, p)$  
*shows* $H_{\text{Inv4d}}(s', p)$

(Proof)

**Lemma HPhase1or2Write-HInv4d-q**:  
*assumes* act: $H_{\text{Phase1or2Write}}(s, s', p, d)$  
*and* inv: $H_{\text{Inv4d}}(s, q)$  
and $p \neq q$  
*shows* $H_{\text{Inv4d}}(s', q)$

(Proof)

**Theorem HPhase1or2Write-HInv4d**: \[ [H_{\text{Phase1or2Write}}(s, s', p, d); H_{\text{Inv4d}}(s, q); H_{\text{Inv4a}}(s, p)] \implies H_{\text{Inv4d}}(s', q) \]

(Proof)

**Lemma HPhase1or2ReadThen-HInv4d-p**:  
*assumes* act: $H_{\text{Phase1or2ReadThen}}(s, s', p, d, q)$  
*and* inv: $H_{\text{Inv4d}}(s, p)$  
*shows* $H_{\text{Inv4d}}(s', p)$

(Proof)

47
lemma \texttt{HPhase1or2ReadThen-HInv4d-q}:
\begin{itemize}
    \item \texttt{assumes act: HPhase1or2ReadThen s s' p d r}
    \item \texttt{and inv: HInv4d s q}
    \item \texttt{and p\#q}
\end{itemize}
\texttt{shows HInv4d s' q}
\langle \texttt{proof} \rangle

\texttt{theorem HPhase1or2ReadThen-HInv4d:}
\begin{align*}
\llbracket \text{HPhase1or2ReadThen s s' p d r; HInv4d s q}\rrbracket & \Rightarrow \text{HInv4d s' q}
\end{align*}
\langle \texttt{proof} \rangle

\texttt{theorem HPhase1or2ReadElse-HInv4d:}
\begin{align*}
\llbracket \text{HPhase1or2ReadElse s s' p d r; HInv4d s q}\rrbracket & \Rightarrow \text{HInv4d s' q}
\end{align*}
\langle \texttt{proof} \rangle

lemma \texttt{HEndPhase1-HInv4d-p}:
\begin{itemize}
    \item \texttt{assumes act: HEndPhase1 s s' p}
    \item \texttt{and inv: HInv4d s p}
    \item \texttt{and inv2b: Inv2b s}
    \item \texttt{and inv4c: HInv4c s p}
\end{itemize}
\texttt{shows HInv4d s' p}
\langle \texttt{proof} \rangle

lemma \texttt{HEndPhase1-HInv4d-q}:
\begin{itemize}
    \item \texttt{assumes act: HEndPhase1 s s' p}
    \item \texttt{and inv: HInv4d s q}
    \item \texttt{and p\#q}
\end{itemize}
\texttt{shows HInv4d s' q}
\langle \texttt{proof} \rangle

\texttt{theorem HEndPhase1-HInv4d:}
\begin{align*}
\llbracket \text{HEndPhase1 s s' p; HInv4d s q; Inv2b s; HInv4c s p}\rrbracket & \Rightarrow \text{HInv4d s' q}
\end{align*}
\langle \texttt{proof} \rangle

lemma \texttt{HEndPhase2-HInv4d-p}:
\begin{itemize}
    \item \texttt{assumes act: HEndPhase2 s s' p}
    \item \texttt{and inv: HInv4d s p}
\end{itemize}
\texttt{shows HInv4d s' p}
\langle \texttt{proof} \rangle

lemma \texttt{HEndPhase2-HInv4d-q}:
\begin{itemize}
    \item \texttt{assumes act: HEndPhase2 s s' p}
    \item \texttt{and inv: HInv4d s q}
    \item \texttt{and p\#q}
\end{itemize}
\texttt{shows HInv4d s' q}
\langle \texttt{proof} \rangle
\textbf{theorem} \texttt{HEndPhase2-HInv4d}:
\[
[HEndPhase2 \ s \ s' \ p; \ HInv4d \ s \ q] \implies \ HInv4d \ s' \ q
\langle\text{proof}\rangle
\]

\textbf{lemma} \texttt{HFail-HInv4d-p}:
\begin{itemize}
  \item \textbf{assumes} \ \texttt{act}: \ HFail \ s \ s' \ p
  \item \texttt{and} \ \texttt{inv}: \ HInv4d \ s \ p
  \item \texttt{shows} \ HInv4d \ s' \ p
\end{itemize}
\langle\text{proof}\rangle

\textbf{lemma} \texttt{HFail-HInv4d-q}:
\begin{itemize}
  \item \textbf{assumes} \ \texttt{act}: \ HFail \ s \ s' \ p
  \item \texttt{and} \ \texttt{inv}: \ HInv4d \ s \ q
  \item \texttt{and} \ \texttt{pnq}: \ p \neq q
  \item \texttt{shows} \ HInv4d \ s' \ q
\end{itemize}
\langle\text{proof}\rangle

\textbf{theorem} \texttt{HFail-HInv4d}:
\[
[HFail \ s \ s' \ p; \ HInv4d \ s \ q] \implies \ HInv4d \ s' \ q
\langle\text{proof}\rangle
\]

\textbf{lemma} \texttt{HPhase0Read-HInv4d-p}:
\begin{itemize}
  \item \textbf{assumes} \ \texttt{act}: \ HPhase0Read \ s \ s' \ p \ d
  \item \texttt{and} \ \texttt{inv}: \ HInv4d \ s \ p
  \item \texttt{shows} \ HInv4d \ s' \ p
\end{itemize}
\langle\text{proof}\rangle

\textbf{lemma} \texttt{HPhase0Read-HInv4d-q}:
\begin{itemize}
  \item \textbf{assumes} \ \texttt{act}: \ HPhase0Read \ s \ s' \ p \ d
  \item \texttt{and} \ \texttt{inv}: \ HInv4d \ s \ q
  \item \texttt{and} \ \texttt{pnq}: \ p \neq q
  \item \texttt{shows} \ HInv4d \ s' \ q
\end{itemize}
\langle\text{proof}\rangle

\textbf{theorem} \texttt{HPhase0Read-HInv4d}:
\[
[HPhase0Read \ s \ s' \ p \ d; \ HInv4d \ s \ q] \implies \ HInv4d \ s' \ q
\langle\text{proof}\rangle
\]

\textbf{lemma} \texttt{HEndPhase0-blocksOf2}:
\begin{itemize}
  \item \textbf{assumes} \ \texttt{act}: \ HEndPhase0 \ s \ s' \ p
  \item \texttt{and} \ \texttt{inv2c}: \ Inv2c-inner \ s \ p
  \item \texttt{shows} \ allBlocksRead \ s \ p \subseteq \ blocksOf \ s \ p
\end{itemize}
\langle\text{proof}\rangle

\textbf{lemma} \texttt{HEndPhase0-HInv4d-p}:
\begin{itemize}
  \item \textbf{assumes} \ \texttt{act}: \ HEndPhase0 \ s \ s' \ p
  \item \texttt{and} \ \texttt{inv}: \ HInv4d \ s \ p
  \item \texttt{and} \ \texttt{inv2c}: \ Inv2c \ s
  \item \texttt{and} \ \texttt{inv1}: \ Inv1 \ s
\end{itemize}
lemma HEndPhase0-HInv4d-q:
assumes act: HEndPhase0 s s' p
and inv: HInv4d s q
and pnq: p\neq q
shows HInv4d s' q
(proof)

theorem HEndPhase0-HInv4d:
[ [ HEndPhase0 s s' p; HInv4d s q; Inv2c s; Inv1 s ] ] \Rightarrow HInv4d s' q
(proof)

Since we have already proved HInv2 is an invariant of HNext, HInv1 \land
HInv2 \land HInv4 is also an invariant of HNext.

lemma I2d:
assumes nxt: HNext s s'
and inv: HInv1 s \land HInv2 s \land HInv2 s' \land HInv4 s
shows HInv4 s'
(proof)

end

theory DiskPaxos-Inv5 imports DiskPaxos-Inv3 DiskPaxos-Inv4 begin

C.5 Invariant 5

This invariant asserts that, if a processor p is in phase 2, then either its
bal and inp values satisfy maxBalInp, or else p must eventually abort its
current ballot. Processor p will eventually abort its ballot if there is some
processor q and majority set D such that p has not read q’s block on any
disk D, and all of those blocks have mbal values greater than bal(dblocksp).

definition maxBalInp :: state \Rightarrow nat \Rightarrow InputsOrNi \Rightarrow bool
where maxBalInp s b v = (\forall bk\in allBlocks s. b \leq bal bk \rightarrow inp bk = v)

definition HInv5-inner-R :: state \Rightarrow Proc \Rightarrow bool
where HInv5-inner-R s p =
( maxBalInp s (bal(dblock s p)) (inp(dblock s p))
\lor (\exists D\in MajoritySet. \exists q. (\forall d\in D. bal(dblock s p) < mbal(disk s d q)
\land \neg hasRead s p d q)) )

definition HInv5-inner :: state \Rightarrow Proc \Rightarrow bool
where HInv5-inner s p = ( phase s p = 2 \rightarrow HInv5-inner-R s p)
**definition** $HInv5 :: state \Rightarrow bool$

where $HInv5 \ s = (\forall \ p. \ HInv5-inner \ s \ p)$

### C.5.1 Proof of Invariant 5

The initial state implies Invariant 5.

**theorem** $HInit-HInv5: HInit \ s \Longrightarrow HInv5 \ s$

⟨proof⟩

We will use the notation used in the proofs of invariant 4, and prove the lemma $action-HInv5-p$ and $action-HInv5-q$ for each action, for the cases $p = q$ and $p \neq q$ respectively.

Also, for each action we will define an $action-allBlocks$ lemma in the same way that we defined $blocksOf$ lemmas in the proofs of $HInv2$. Now we prove that for each action the new $allBlocks$ are included in the old $allBlocks$ or, in some cases, included in the old $allBlocks$ union the new $dblock$.

**lemma** $HStartBallot-HInv5-p$:

-assumes act: $HStartBallot \ s \ s' \ p$

-and inv: $HInv5-inner \ s \ p$

-shows $HInv5-inner \ s' \ p$ ⟨proof⟩

**lemma** $HStartBallot-blocksOf-q$:

-assumes act: $HStartBallot \ s \ s' \ p$

-and $p = q$

-shows $blocksOf \ s' q \subseteq blocksOf \ s q$ ⟨proof⟩

**lemma** $HStartBallot-allBlocks$:

-assumes act: $HStartBallot \ s \ s' \ p$

-shows $allBlocks \ s' \subseteq allBlocks \ s \cup \{dblock \ s' \ p\}$ ⟨proof⟩

**lemma** $HStartBallot-HInv5-q1$:

-assumes act: $HStartBallot \ s \ s' \ p$

-and $p = q$

-and $inv5-1$: $maxBalInp \ s \ (bal(dblock \ s \ q)) \ (inp(dblock \ s \ q))$

-shows $maxBalInp \ s' \ (bal(dblock \ s' \ q)) \ (inp(dblock \ s' \ q))$ ⟨proof⟩

**lemma** $HStartBallot-HInv5-q2$:

-assumes act: $HStartBallot \ s \ s' \ p$

-and $p = q$

-and $inv5-2$: $\exists D \in MajoritySet. \ \exists q. \ (\forall d \in D. \ bal(dblock \ s \ d \ q) < mbal(disk \ s \ d \ qq)$

-shows $\exists D \in MajoritySet. \ \exists q. \ (\forall d \in D. \ bal(dblock \ s' \ d \ q) < mbal(disk \ s' \ d \ qq)$

\(\setminus hasRead \ s \ d \ q \ q qq\)

\(\setminus hasRead \ s' \ d \ q \ q qq\)
lemma HStartBallot-HInv5-q:
  assumes act: HStartBallot s s' p
  and inv: HInv5-inner s q
  and pq: p ≠ q
  shows HInv5-inner s' q
⟨proof⟩

theorem HStartBallot-HInv5:
  [[ HStartBallot s s' p; HInv5-inner s q ]] ⇒ HInv5-inner s' q
⟨proof⟩

lemma HPhase1or2Write-HInv5-1:
  assumes act: HPhase1or2Write s s' p d
  and inv5-1: maxBalInp s (bal(dblock s q)) (inp(dblock s q))
  shows maxBalInp s' (bal(dblock s' q)) (inp(dblock s' q))
⟨proof⟩

lemma HPhase1or2Write-HInv5-p2:
  assumes act: HPhase1or2Write s s' p d
  and inv4c: HInv4c s p
  and phase: phase s p = 2
  and inv5-2: ∃ D ∈ MajoritySet. ∃ q. (∀ d ∈ D. bal(dblock s p) < mbal(disk s d q) ∧ ¬ hasRead s p d q)
  shows ∃ D ∈ MajoritySet. ∃ q. (∀ d ∈ D. bal(dblock s' p) < mbal(disk s' d q) ∧ ¬ hasRead s' p d q)
⟨proof⟩

lemma HPhase1or2Write-HInv5-p:
  assumes act: HPhase1or2Write s s' p d
  and inv: HInv5-inner s p
  and inv4: HInv4c s p
  shows HInv5-inner s' p
⟨proof⟩

lemma HPhase1or2Write-allBlocks:
  assumes act: HPhase1or2Write s s' p d
  shows allBlocks s' ⊆ allBlocks s
⟨proof⟩

lemma HPhase1or2Write-HInv5-q2:
  assumes act: HPhase1or2Write s s' p d
  and pq: p ≠ q
  and inv4a: HInv4a s p
  and inv5-2: ∃ D ∈ MajoritySet. ∃ q. (∀ d ∈ D. bal(dblock s q) < mbal(disk s d qq) ∧ ¬ hasRead s q d qq)
\[
\exists D \in \text{MajoritySet. } \exists qq. \left(\forall d \in D. \quad \text{bal}(\text{dblock } s' q) < \text{mbal}(\text{disk } s' d qq) \land \neg \text{hasRead } s' q d qq\right)
\]

\text{lemma } H\text{Phase1or2Write-HInv5-q:}
\begin{align*}
\text{assumes } & \text{act: } H\text{Phase1or2Write } s s' p d \\
\text{and } & \text{inv: } H\text{Inv5-inner } s q \\
\text{and } & \text{inv4a: } H\text{Inv4a } s p \\
\text{and } & \text{pnq: } p \neq q \\
\text{shows } & H\text{Inv5-inner } s' q
\end{align*}

\text{theorem } H\text{Phase1or2Write-HInv5:}
\begin{align*}
[ & H\text{Phase1or2Write } s s' p d; \quad H\text{Inv5-inner } s q; \\
& H\text{Inv4c } s p; \quad H\text{Inv4a } s p ] \implies H\text{Inv5-inner } s' q
\end{align*}

\text{lemma } H\text{Phase1or2ReadThen-HInv5-1:}
\begin{align*}
\text{assumes } & \text{act: } H\text{Phase1or2ReadThen } s s' p d r \\
\text{and } & \text{inv5-1: } \text{maxBalInp } s \left(\text{bal}(\text{dblock } s q)\right) \left(\text{inp}(\text{dblock } s q)\right) \\
\text{shows } & \text{maxBalInp } s' \left(\text{bal}(\text{dblock } s' q)\right) \left(\text{inp}(\text{dblock } s' q)\right)
\end{align*}

\text{lemma } H\text{Phase1or2ReadThen-HInv5-p2:}
\begin{align*}
\text{assumes } & \text{act: } H\text{Phase1or2ReadThen } s s' p d r \\
\text{and } & \text{inv4c: } H\text{Inv4c } s p \\
\text{and } & \text{inv2c: } \text{Inv2c-inner } s p \\
\text{and } & \text{phase: } \text{phase } s p = 2 \\
\text{and } & \text{inv5-2: } \exists D \in \text{MajoritySet. } \exists q. \left(\forall d \in D. \quad \text{bal}(\text{dblock } s p) < \text{mbal}(\text{disk } s d q) \land \neg \text{hasRead } s p d q\right) \\
\text{shows } & \exists D \in \text{MajoritySet. } \exists q. \left(\forall d \in D. \quad \text{bal}(\text{dblock } s' p) < \text{mbal}(\text{disk } s' d q) \land \neg \text{hasRead } s' p d q\right)
\end{align*}

\text{lemma } H\text{Phase1or2ReadThen-HInv5-p:}
\begin{align*}
\text{assumes } & \text{act: } H\text{Phase1or2ReadThen } s s' p d r \\
\text{and } & \text{inv: } H\text{Inv5-inner } s p \\
\text{and } & \text{inv4: } H\text{Inv4c } s p \\
\text{and } & \text{inv2c: } \text{Inv2c } s \\
\text{shows } & H\text{Inv5-inner } s' p
\end{align*}

\text{lemma } H\text{Phase1or2ReadThen-allBlocks:}
\begin{align*}
\text{assumes } & \text{act: } H\text{Phase1or2ReadThen } s s' p d r \\
\text{shows } & \text{allBlocks } s' \subseteq \text{allBlocks } s
\end{align*}

\text{lemma } H\text{Phase1or2ReadThen-HInv5-q2:}
\begin{align*}
\text{assumes } & \text{act: } H\text{Phase1or2ReadThen } s s' p d r
\end{align*}
and \( p \neq q \)
and \( \text{inv4a: } \text{HInv4a } s \ p \)
and \( \text{inv5-2: } \exists D \in \text{MajoritySet}. \exists q q. (\forall d \in D. \ \text{bal}(\text{dblock } s \ q) < \text{mbal}(\text{disk } s \ d \ qq)) \)
and \( \neg \text{hasRead } s \ q \ d \ qq \)
s
shows \( \exists D \in \text{MajoritySet}. \exists q q. \ 
(\forall d \in D. \ \text{bal}(\text{dblock } s' \ q) < \text{mbal}(\text{disk } s' \ d \ qq)) \)
\( \neg \text{hasRead } s' \ q \ d \ qq \)

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

**Lemma HPhase1or2ReadThen-HInv5-q:**
assumes act: HPhase1or2ReadThen \( s \ s' \ p \ d \ r \)
and inv: HInv5-inner \( s \ q \)
and inv4a: HInv4a \( s \ p \)
and \( p \neq q \)
s
shows HInv5-inner \( s' \ q \)
\( \langle \text{proof} \rangle \)

**Theorem HPhase1or2ReadThen-HInv5:**
\[
[ \ 
\text{HPhase1or2ReadThen } s \ s' \ p \ d \ r; \ 
\text{HInv5-inner } s \ q; \ 
\text{Inv2c } s; \ 
\text{HInv4c } s \ p; \ 
\text{HInv4a } s \ p \ ] \ \Rightarrow \ HInv5-inner \ s' \ q
\]
\( \langle \text{proof} \rangle \)

**Theorem HPhase1or2ReadElse-HInv5:**
\[
[ \ 
\text{HPhase1or2ReadElse } s \ s' \ p \ d \ r; \ 
\text{HInv5-inner } s \ q \ ]
\Rightarrow \ HInv5-inner \ s' \ q
\]
\( \langle \text{proof} \rangle \)

**Lemma HEndPhase2-HInv5-p:**
\text{HEndPhase2 } s \ s' \ p \ \Rightarrow \ HInv5-inner \ s' \ p
\( \langle \text{proof} \rangle \)

**Lemma HEndPhase2-allBlocks:**
assumes act: HEndPhase2 \( s \ s' \ p \)
s
shows allBlocks \( s' \subseteq \text{allBlocks } s \)
\( \langle \text{proof} \rangle \)

**Lemma HEndPhase2-HInv5-q1:**
assumes act: HEndPhase2 \( s \ s' \ p \)
and \( p \neq q \)
and \( \text{inv5-1: } \maxBalInp \ s (\text{bal}(\text{dblock } s \ q)) (\text{inp}(\text{dblock } s \ q)) \)
s
shows \( \maxBalInp \ s' (\text{bal}(\text{dblock } s' \ q)) (\text{inp}(\text{dblock } s' \ q)) \)
\( \langle \text{proof} \rangle \)

**Lemma HEndPhase2-HInv5-q2:**
assumes act: HEndPhase2 \( s \ s' \ p \)
and \( p \neq q \)
and \( \text{inv5-2: } \exists D \in \text{MajoritySet}. \exists q q. (\forall d \in D. \ \text{bal}(\text{dblock } s \ q) < \text{mbal}(\text{disk } s \ d \ qq)) \)

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

54
\[ \exists D \in \text{MajoritySet}. \exists q. (\forall d \in D. \text{bal}(\text{dblock } s' q) < \text{mbal}(\text{disk } s' d qq) \land \neg \text{hasRead } s' q d qq) \]

(proof)

**lemma HEndPhase2-HInv5-q:**
- **assumes** act: HEndPhase2 \( s s' p \)
- **and** inv: HInv5-inner \( s q \)
- **and** pnq: \( p \neq q \)
- **shows** HInv5-inner \( s' q \)

(proof)

**theorem HEndPhase2-HInv5:**
\[
[ H\text{EndPhase2} s s' p; \text{HInv5-inner } s q ] \implies \text{HInv5-inner } s' q
\]

(proof)

**lemma HEndPhase1-HInv5-p:**
- **assumes** act: HEndPhase1 \( s s' p \)
- **and** inv4: HInv4 \( s \)
- **and** inv2a: Inv2a \( s \)
- **and** inv2a': Inv2a' \( s' \)
- **and** inv2c: Inv2c \( s \)
- **and** asm4: \( \neg \text{maxBalInp } s' (\text{bal}(\text{dblock } s' p)) (\text{inp}(\text{dblock } s' p)) \)
- **shows** (\( \exists D \in \text{MajoritySet}. \exists q. (\forall d \in D. \text{bal}(\text{dblock } s' p) < \text{mbal}(\text{disk } s' d qq) \land \neg \text{hasRead } s' p d qq))

(proof)

**lemma union-inclusion:**
\[
[ A \subseteq A'; B \subseteq B'] \implies A \cup B \subseteq A' \cup B'
\]

(proof)

**lemma HEndPhase1-blocksOf-q:**
- **assumes** act: HEndPhase1 \( s s' p \)
- **and** pnq: \( p \neq q \)
- **shows** blocksOf \( s' q \subseteq \text{blocksOf } s q \)

(proof)

**lemma HEndPhase1-allBlocks:**
- **assumes** act: HEndPhase1 \( s s' p \)
- **shows** allBlocks \( s' \subseteq \text{allBlocks } s \cup \{ \text{dblock } s' p \} \)

(proof)

**lemma HEndPhase1-HInv5-q:**
- **assumes** act: HEndPhase1 \( s s' p \)
- **and** inv: HInv5 \( s \)
- **and** inv1: Inv1 \( s \)
- **and** inv2a: Inv2a \( s' \)
- **and** inv2a-q: Inv2a' \( s \)
- **and** inv2b: Inv2b \( s \)
- **and** inv2c: Inv2c \( s \)
and \text{i}nv3: \text{HInv3} s
and \text{phase}:' \text{phase} s' q = 2
and \text{pnq}: p \neq q
and asm4: \neg \text{maxBalInp} s' (\text{bal}(\text{dblock} s' q)) (\text{inp}(\text{dblock} s' q))
shows (\exists D \in \text{MajoritySet}. \exists qq. (\forall d \in D. \text{bal}(\text{dblock} s' q) < \text{mbal}(\text{disk} s' d qq) \\
\wedge \neg \text{hasRead} s' q d qq))

⟨proof⟩

\text{theorem HEndPhase1-HInv5:}
\text{assumes act: HEndPhase1 s s' p}
\text{and inv: HInv5 s}
\text{and inv1: Inv1 s}
\text{and inv2a: Inv2a s}
\text{and inv2a': Inv2a s'}
\text{and inv2b: Inv2b s}
\text{and inv2c: Inv2c s}
\text{and inv3: HInv3 s}
\text{and inv4: HInv4 s}
shows HInv5-inner s' q
⟨proof⟩

\text{lemma HFail-HInv5-p:}
\text{HFail s s' p} \implies \text{HInv5-inner s' p}
⟨proof⟩

\text{lemma HFail-blocksOf-q:}
\text{assumes act: HFail s s' p}
\text{and pnq: p \neq q}
\text{shows blocksOf s' q \subseteq blocksOf s q}
⟨proof⟩

\text{lemma HFail-allBlocks:}
\text{assumes act: HFail s s' p}
\text{shows allBlocks s' \subseteq allBlocks s \cup \{d\text{block s' p}\}}
⟨proof⟩

\text{lemma HFail-HInv5-q1:}
\text{assumes act: HFail s s' p}
\text{and pnq: p \neq q}
\text{and inv2a: Inv2a-inner s' q}
\text{and inv5-1: \text{maxBalInp} s (\text{bal}(\text{dblock} s q)) (\text{inp}(\text{dblock} s q))}
\text{shows maxBalInp s' (\text{bal}(\text{dblock} s' q)) (\text{inp}(\text{dblock} s' q))}
⟨proof⟩

\text{lemma HFail-HInv5-q2:}
\text{assumes act: HFail s s' p}
\text{and pnq: p \neq q}
\text{and inv5-2: \exists D \in \text{MajoritySet}. \exists qq. (\forall d \in D. \text{bal}(\text{dblock} s q) < \text{mbal}(\text{disk} s d qq)}
\begin{align*}
& \land \lnot \text{hasRead } s \ q \ d \ qq \\
& \text{shows} \ \exists D \in \text{MajoritySet}. \ \exists qq. \ (\forall d \in D. \ \text{bal}(dblock \ s' \ q) < \text{mbal}(disk \ s' \ d \ qq) \\
& \quad \land \lnot \text{hasRead } s' \ q \ d \ qq) \\
\langle \text{proof} \rangle
\end{align*}

\textbf{lemma} \text{HFail-HInv5-q}:
\textbf{assumes} \text{act}: \text{HFail } s \ s' \ p \\
\text{and} \ \text{inv}: \text{HInv5-inner } s \ q \\
\text{and} \ \text{pnq}: \ p \neq q \\
\text{shows} \ \text{HInv5-inner } s' \ q \\
\langle \text{proof} \rangle

\textbf{theorem} \text{HFail-HInv5}:
[ \text{HFail } s \ s' \ p; \ \text{HInv5-inner } s \ q; \ \text{Inv2a } s' ] \Longrightarrow \text{HInv5-inner } s' \ q \\
\langle \text{proof} \rangle

\textbf{lemma} \text{HPhase0Read-HInv5-p}:
\text{HPhase0Read } s \ s' \ p \ d \ \Longrightarrow \ \text{HInv5-inner } s' \ p \\
\langle \text{proof} \rangle

\textbf{lemma} \text{HPhase0Read-allBlocks}:
\textbf{assumes} \text{act}: \text{HPhase0Read } s \ s' \ p \ d \\
\text{shows} \ \text{allBlocks } s' \subseteq \text{allBlocks } s \\
\langle \text{proof} \rangle

\textbf{lemma} \text{HPhase0Read-HInv5-1}:
\textbf{assumes} \text{act}: \text{HPhase0Read } s \ s' \ p \ d \\
\text{and} \ \text{inv5-1}: \ \text{maxBalInp } s (\text{bal}(dblock \ s \ q)) (\text{inp}(dblock \ s \ q)) \\
\text{shows} \ \text{maxBalInp } s' (\text{bal}(dblock \ s' \ q)) (\text{inp}(dblock \ s' \ q)) \\
\langle \text{proof} \rangle

\textbf{lemma} \text{HPhase0Read-HInv5-q2}:
\textbf{assumes} \text{act}: \text{HPhase0Read } s \ s' \ p \ d \\
\text{and} \ \text{pnq}: \ p \neq q \\
\text{and} \ \text{inv5-2}: \ \exists D \in \text{MajoritySet}. \ \exists qq. \ (\forall d \in D. \ \text{bal}(dblock \ s \ q) < \text{mbal}(disk \ s \ d \ qq) \\
\quad \land \lnot \text{hasRead } s \ q \ d \ qq) \\
\text{shows} \ \exists D \in \text{MajoritySet}. \ \exists qq. \ (\forall d \in D. \ \text{bal}(dblock \ s' \ q) < \text{mbal}(disk \ s' \ d \ qq) \\
\quad \land \lnot \text{hasRead } s' \ q \ d \ qq) \\
\langle \text{proof} \rangle

\textbf{lemma} \text{HPhase0Read-HInv5-q}:
\textbf{assumes} \text{act}: \text{HPhase0Read } s \ s' \ p \ d \\
\text{and} \ \text{inv}: \text{HInv5-inner } s \ q \\
\text{and} \ \text{pnq}: \ p \neq q \\
\text{shows} \ \text{HInv5-inner } s' \ q \\
\langle \text{proof} \rangle

57
**Theorem** $H_{\text{Phase0Read-HInv5}}$:

\[
\begin{array}{l}
[ H_{\text{Phase0Read}} s s' p d; H_{\text{Inv5-inner}} s q ] \implies H_{\text{Inv5-inner}} s' q
\end{array}
\]

(proof)

**Lemma** $H_{\text{EndPhase0-HInv5-p}}$:

\[
H_{\text{EndPhase0}} s s' p \implies H_{\text{Inv5-inner}} s' p
\]

(proof)

**Lemma** $H_{\text{EndPhase0-blocksOf-q}}$:

- **assumes** $\text{act} : H_{\text{EndPhase0}} s s' p$
- $\text{pnq} : p \neq q$
- **shows** $\text{blocksOf} s' q \subseteq \text{blocksOf} s q$

(proof)

**Lemma** $H_{\text{EndPhase0-allBlocks}}$:

- **assumes** $\text{act} : H_{\text{EndPhase0}} s s' p$
- **shows** $\text{allBlocks} s' \subseteq \text{allBlocks} s \cup \{ \text{dblock} s' p \}$

(proof)

**Lemma** $H_{\text{EndPhase0-HInv5-q1}}$:

- **assumes** $\text{act} : H_{\text{EndPhase0}} s s' p$
- $\text{pnq} : p \neq q$
- $\text{inv1} : \text{Inv1} s$
- $\text{inv5-1} : \text{maxBalInp} s (\text{bal}(\text{dblock} s q)) (\text{inp}(\text{dblock} s q))$
- **shows** $\text{maxBalInp} s' (\text{bal}(\text{dblock} s' q)) (\text{inp}(\text{dblock} s' q))$

(proof)

**Lemma** $H_{\text{EndPhase0-HInv5-q2}}$:

- **assumes** $\text{act} : H_{\text{EndPhase0}} s s' p$
- $\text{pnq} : p \neq q$
- $\text{inv5-2} : \exists D \in \text{MajoritySet}. \exists q_0. (\forall d \in D. \text{bal}(\text{dblock} s q) < \text{mbal}(\text{disk} s d qq) \land \neg \text{hasRead} s q d qq)$
- **shows** $\exists D \in \text{MajoritySet}. \exists q_0. (\forall d \in D. \text{bal}(\text{dblock} s' q) < \text{mbal}(\text{disk} s' d qq) \land \neg \text{hasRead} s' q d qq)$

(proof)

**Lemma** $H_{\text{EndPhase0-HInv5-q}}$:

- **assumes** $\text{act} : H_{\text{EndPhase0}} s s' p$
- $\text{inv} : H_{\text{Inv5-inner}} s q$
- $\text{inv1} : \text{Inv1} s$
- $\text{pnq} : p \neq q$
- **shows** $H_{\text{Inv5-inner}} s' q$

(proof)

**Theorem** $H_{\text{EndPhase0-HInv5}}$:

\[
\begin{array}{l}
[ H_{\text{EndPhase0}} s s' p; H_{\text{Inv5-inner}} s q; \text{Inv1} s ] \implies H_{\text{Inv5-inner}} s' q
\end{array}
\]

(proof)

58
HInv1 ∧ HInv2 ∧ HInv3 ∧ HInv4 ∧ HInv5 is an invariant of HNext.

lemma I2e:
assumes next: HNext s s'
and inv: HInv1 s ∧ HInv2 s ∧ HInv2 s' ∧ HInv3 s ∧ HInv4 s ∧ HInv5 s
shows HInv5 s'
⟨proof⟩
end

theory DiskPaxos-Chosen imports DiskPaxos-Inv5 begin

C.6 Lemma I2f

To prove the final conjunct we will use the predicate valueChosen(v). This predicate is true if v is the only possible value that can be chosen as output. It also asserts that, for every disk d in D, if q has already read disksdp, then it has read a block with bal field at least b.

definition valueChosen :: state ⇒ InputsOrNi ⇒ bool
where
valueChosen s v =
(∃ b∈ (UN p. Ballot p).
maxBalInp s b v
∧ (∃ p. ∃ D∈MajoritySet.(∀ d∈D. b ≤ bal(disk s d p)
∧ (∀ q.( phase s q = 1
∧ b ≤ mbal(dblock s q)
∧ hasRead s q d p
) −→ (∃ br∈blocksRead s q d. b ≤ bal(block br)))))
)

lemma HEndPhase1-valueChosen-inp:
assumes act: HEndPhase1 s s' q
and inv2a: Inv2a s
and asm1: b∈ (UN p. Ballot p)
and bk-blocksOf: bk∈blocksOf s r
and bk: bk∈ blocksSeen s q
and b-bal: b ≤ bal bk
and asm3: maxBalInp s b v
and inv1: Inv1 s
shows inp(dblock s' q) = v
⟨proof⟩

lemma HEndPhase1-maxBalInp:
assumes act: HEndPhase1 s s' q
and asm1: b∈ (UN p. Ballot p)
and asm2: D∈MajoritySet
and asm3: maxBalInp s b v
and asm4: ∀ d∈D. b ≤ bal(disk s d p)
\(\forall q. \) ( phase \( s q = 1 \)
\(\land b \leq m\text{bal}(\text{dblock} \ s \ q)\)
\(\land \text{hasRead} \ s \ q \ d \ p\)
\(\rightarrow (\exists \text{br} \in \text{blocksRead} \ s \ q \ d. \ b \leq \text{bal}(\text{block} \ \text{br})))\)

and inv1: Inv1 \(s\)
and inv2a: Inv2a \(s\)
and inv2b: Inv2b \(s\)
shows maxBalImp \(s\) \(b\) \(v\)

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

**lemma** HEndPhase1-valueChosen2:

assumes act: HEndPhase1 \(s\) \(s'\) \(q\)
and asm4: \(\forall d \in D. \ b \leq \text{bal}(\text{disk} \ s \ d \ p)\)
\(\land(\forall q. \) ( phase \( s q = 1 \)
\(\land b \leq m\text{bal}(\text{dblock} \ s \ q)\)
\(\land \text{hasRead} \ s \ q \ d \ p\)
\(\rightarrow (\exists \text{br} \in \text{blocksRead} \ s \ q \ d. \ b \leq \text{bal}(\text{block} \ \text{br})))\)
(is ?P \(s\))

shows ?P \(s'\)

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

**theorem** HEndPhase1-valueChosen:

assumes act: HEndPhase1 \(s\) \(s'\) \(q\)
and vc: valueChosen \(s\) \(v\)
and inv1: Inv1 \(s\)
and inv2a: Inv2a \(s\)
and inv2b: Inv2b \(s\)
and v-input: \(v \in \text{Inputs}\)
shows valueChosen \(s'\) \(v\)

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

**lemma** HStartBallot-maxBalImp:

assumes act: HStartBallot \(s\) \(s'\) \(q\)
and asm3: maxBalImp \(s\) \(b\) \(v\)
shows maxBalImp \(s'\) \(b\) \(v\)

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

**lemma** HStartBallot-valueChosen2:

assumes act: HStartBallot \(s\) \(s'\) \(q\)
and asm4: \(\forall d \in D. \ b \leq \text{bal}(\text{disk} \ s \ d \ p)\)
\(\land(\forall q. \) ( phase \( s q = 1 \)
\(\land b \leq m\text{bal}(\text{dblock} \ s \ q)\)
\(\land \text{hasRead} \ s \ q \ d \ p\)
\(\rightarrow (\exists \text{br} \in \text{blocksRead} \ s \ q \ d. \ b \leq \text{bal}(\text{block} \ \text{br})))\)
(is ?P \(s\))

shows ?P \(s'\)

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

**theorem** HStartBallot-valueChosen:

assumes act: HStartBallot \(s\) \(s'\) \(q\)
and \(vc\): valueChosen \(s\ v\)
and \(v\text{-input}\): \(v \in \text{Inputs}\)
shows valueChosen \(s'\ v\)

\(\text{lemma}\ HPhase1or2Write-maxBalInp:\)
\(\text{assumes}\ act: HPhase1or2Write \(s\ s'\ q\ d\)
\text{and} \(asm3:\ maxBalInp \(s\ b\ v\)
\shows maxBalInp \(s'\ b\ v\)

\(\text{lemma}\ HPhase1or2Write-valueChosen2:\)
\(\text{assumes}\ act: HPhase1or2Write \(s\ s'\ pp\ d\)
\text{and} \(asm2: D \in \text{MajoritySet}\)
\text{and} \(asm4: \forall d \in D.\ b \leq bal(disk \(s\ d\ p\))
\wedge(\forall q.(\text{phase} \(s\ q\ = 1\)
\wedge b \leq mbal(dblock \(s\ q\))
\wedge \text{hasRead} \(s\ q\ d\ p\)
\rightarrow (\exists \text{blocksRead} \(s\ q\ d.\ b \leq bal(block br))) \text{ (is } ?P s\)
\text{and} \(inv4: HInv4a \(s\ pp\)
\shows ?P s'

\(\text{theorem}\ HPhase1or2Write-valueChosen:\)
\(\text{assumes}\ act: HPhase1or2Write \(s\ s'\ q\ d\)
\text{and} \(vc:\ valueChosen \(s\ v\)
\text{and} \(v\text{-input}\): \(v \in \text{Inputs}\)
\text{and} \(inv4: HInv4a \(s\ q\)
\shows valueChosen \(s'\ v\)

\(\text{lemma}\ HPhase1or2ReadThen-maxBalInp:\)
\(\text{assumes}\ act: HPhase1or2ReadThen \(s\ s'\ q\ d\ p\)
\text{and} \(asm3:\ maxBalInp \(s\ b\ v\)
\shows maxBalInp \(s'\ b\ v\)

\(\text{lemma}\ HPhase1or2ReadThen-valueChosen2:\)
\(\text{assumes}\ act: HPhase1or2ReadThen \(s\ s'\ q\ d\ pp\)
\text{and} \(asm4: \forall d \in D.\ b \leq bal(disk \(s\ d\ p\))
\wedge(\forall q.(\text{phase} \(s\ q\ = 1\)
\wedge b \leq mbal(dblock \(s\ q\))
\wedge \text{hasRead} \(s\ q\ d\ p\)
\rightarrow (\exists \text{blocksRead} \(s\ q\ d.\ b \leq bal(block br))) \text{ (is } ?P s\)
\shows ?P s'

\(\text{theorem}\ HPhase1or2ReadThen-valueChosen:\)
assumes act: \text{HPhase1or2ReadThen} s s' q d p 
and vc: valueChosen s v 
and v-input: v \in Inputs 
shows valueChosen s' v

\langle \text{proof} \rangle

\text{theorem HPhase1or2ReadElse-valueChosen:}
[ \text{HPhase1or2ReadElse} s s' p d r; valueChosen s v; v \in Inputs ]
\implies valueChosen s' v 

\langle \text{proof} \rangle

\text{lemma HEndPhase2-maxBalInp:}
assumes act: \text{HEndPhase2} s s' q 
and asm3: maxBalInp s b v 
shows maxBalInp s' b v 

\langle \text{proof} \rangle

\text{lemma HEndPhase2-valueChosen2:}
assumes act: \text{HEndPhase2} s s' q 
and asm4: \forall d \in D. \quad b \leq \text{bal}(disk s d p) 
\land (\forall q. ( \quad \text{phase} s q = 1 
\land b \leq m\text{bal}(\text{dblock} s q) 
\land \text{hasRead} s q d p 
\implies (\exists b'r \in \text{blocksRead} s q d. b \leq \text{bal}(\text{block} b'))) \quad (\text{is} \ ?P s) 
shows ?P s' 

\langle \text{proof} \rangle

\text{theorem HEndPhase2-valueChosen:}
assumes act: \text{HEndPhase2} s s' q 
and vc: valueChosen s v 
and v-input: v \in Inputs 
shows valueChosen s' v 

\langle \text{proof} \rangle

\text{lemma HFail-maxBalInp:}
assumes act: \text{HFail} s s' q 
and asm1: b \in (\text{UN} p, \text{Ballot} p) 
and asm3: maxBalInp s b v 
shows maxBalInp s' b v 

\langle \text{proof} \rangle

\text{lemma HFail-valueChosen2:}
assumes act: \text{HFail} s s' q 
and asm4: \forall d \in D. \quad b \leq \text{bal}(disk s d p) 
\land (\forall q. ( \quad \text{phase} s q = 1 
\land b \leq m\text{bal}(\text{dblock} s q) 
\land \text{hasRead} s q d p 
\implies (\exists b'r \in \text{blocksRead} s q d. b \leq \text{bal}(\text{block} b'))) \quad (\text{is} \ ?P s) 
shows ?P s' 

\langle \text{proof} \rangle

62
\begin{proof}

\textbf{theorem} \texttt{HFail-valueChosen:}
\begin{itemize}
  \item \texttt{assumes} \texttt{act: HFail} \texttt{s} \texttt{s'} \texttt{q}
  \item \texttt{and \ v-c: valueChosen} \texttt{s} \texttt{v}
  \item \texttt{and \ v-input: \ v} \in \texttt{Inputs}
  \item \texttt{shows} \texttt{valueChosen} \texttt{s'} \texttt{v}
\end{itemize}
\end{proof}

\textbf{lemma} \texttt{HPhase0Read-maxBalInp:}
\begin{itemize}
  \item \texttt{assumes} \texttt{act: HPhase0Read} \texttt{s} \texttt{s'} \texttt{q} \texttt{d}
  \item \texttt{and \ asm3: maxBalInp} \texttt{s} \texttt{b} \texttt{v}
  \item \texttt{shows} \texttt{maxBalInp} \texttt{s'} \texttt{b} \texttt{v}
\end{itemize}

\textbf{lemma} \texttt{HPhase0Read-valueChosen2:}
\begin{itemize}
  \item \texttt{assumes} \texttt{act: HPhase0Read} \texttt{s} \texttt{s'} \texttt{q} \texttt{d}
  \item \texttt{and \ asm4:} \forall \texttt{d} \in \texttt{D}. \ b \leq \texttt{bal(disk s d p)}
  \item \texttt{shows} \texttt{?P s'}
\end{itemize}

\textbf{theorem} \texttt{HPhase0Read-valueChosen:}
\begin{itemize}
  \item \texttt{assumes} \texttt{act: HPhase0Read} \texttt{s} \texttt{s'} \texttt{q} \texttt{d}
  \item \texttt{and \ v-c: valueChosen} \texttt{s} \texttt{v}
  \item \texttt{and \ v-input: \ v} \in \texttt{Inputs}
  \item \texttt{shows} \texttt{valueChosen} \texttt{s'} \texttt{v}
\end{itemize}

\textbf{lemma} \texttt{HEndPhase0-maxBalInp:}
\begin{itemize}
  \item \texttt{assumes} \texttt{act: HEndPhase0} \texttt{s} \texttt{s'} \texttt{q}
  \item \texttt{and \ asm3: maxBalInp} \texttt{s} \texttt{b} \texttt{v}
  \item \texttt{and \ inv1: Inv1} \texttt{s}
  \item \texttt{shows} \texttt{maxBalInp} \texttt{s'} \texttt{b} \texttt{v}
\end{itemize}

\textbf{lemma} \texttt{HEndPhase0-valueChosen2:}
\begin{itemize}
  \item \texttt{assumes} \texttt{act: HEndPhase0} \texttt{s} \texttt{s'} \texttt{q}
  \item \texttt{and \ asm4:} \forall \texttt{d} \in \texttt{D}. \ b \leq \texttt{bal(disk s d p)}
  \item \texttt{shows} \texttt{?P s'}
\end{itemize}

\begin{proof}
\end{proof}
theorem HEndPhase0-valueChosen:
  assumes act: HEndPhase0 s s' q
  and vc: valueChosen s v
  and v-input: v ∈ Inputs
  and inv1: Inv1 s
  shows valueChosen s' v
⟨proof⟩
end

theory DiskPaxos-Inv6 imports DiskPaxos-Chosen begin

C.7 Invariant 6

The final conjunct of HInv asserts that, once an output has been chosen, valueChosen(chosen) holds, and each processor’s output equals either chosen or NotAnInput.

definition HInv6 :: state ⇒ bool
where
  HInv6 s = ((chosen s ≠ NotAnInput ⟷ valueChosen s (chosen s))
  ∧ (∀p. outpt s p ∈ {chosen s, NotAnInput}))

theorem HInit-HInv6: HInit s ⟷ HInv6 s
⟨proof⟩

lemma HEndPhase2-Inv6-1:
  assumes act: HEndPhase2 s s' p
  and inv: HInv6 s
  and inv2b: Inv2b s
  and inv2c: Inv2c s
  and inv3: HInv3 s
  and inv5: HInv5-inner s p
  and chosen': chosen s' ≠ NotAnInput
  shows valueChosen s' (chosen s')
⟨proof⟩

lemma valueChosen-equal-case:
  assumes max-v: maxBalInp s b v
  and Dmaj: D ∈ MajoritySet
  and asm-v: ∀d∈D. b ≤ bal (disk s d p)
  and max-w: maxBalInp s ba w
  and Damaj: Da ∈ MajoritySet
  and asm-w: ∀d∈Da. ba ≤ bal (disk s d pa)
  and b-ba: b≤ba
  shows v=w
⟨proof⟩

64
lemma valueChosen-equal:
  assumes v: valueChosen s v
  and w: valueChosen s w
  shows v = w ⟨proof⟩

lemma HEndPhase2-Inv6-2:
  assumes act: HEndPhase2 s s' p and inv: HInv6 s and inv2b: Inv2b s and inv2c: Inv2c s and inv3: HInv3 s and inv5: HInv5-inner s p and asm: outpt s' r ≠ NotAnInput shows outpt s' r = chosen s' ⟨proof⟩

theorem HEndPhase2-Inv6:
  assumes act: HEndPhase2 s s' p and inv: HInv6 s and inv2b: Inv2b s and inv2c: Inv2c s and inv3: HInv3 s and inv5: HInv5-inner s p shows HInv6 s' ⟨proof⟩

lemma outpt-chosen:
  assumes outpt: outpt s = outpt s' and inv2c: Inv2c s and nextp: HNextPart s s' shows chosen s' = chosen s ⟨proof⟩

lemma outpt-Inv6:
  [ outpt s = outpt s'; ∀ p. outpt s p ∈ {chosen s, NotAnInput}; Inv2c s; HNextPart s s' ] ⟹ ∀ p. outpt s' p ∈ {chosen s', NotAnInput} ⟨proof⟩

theorem HStartBallot-Inv6:
  assumes act: HStartBallot s s' p and inv: HInv6 s and inv2c: Inv2c s shows HInv6 s' ⟨proof⟩

theorem HPhase1or2Write-Inv6:
  assumes act: HPhase1or2Write s s' p d and inv: HInv6 s and inv4: HInv4a s p
and \( inv2c: \text{Inv2c} s \)

shows \( \text{HInv6} s' \)

(proof)

**Theorem HPhase1or2ReadThen-Inv6:**

assumes act: \( \text{HPhase1or2ReadThen} s s' p d q \)
and inv: \( \text{HInv6} s \)
and inv2c: \( \text{Inv2c} s \)

shows \( \text{HInv6} s' \)

(proof)

**Theorem HPhase1or2ReadElse-Inv6:**

assumes act: \( \text{HPhase1or2ReadElse} s s' p d q \)
and inv: \( \text{HInv6} s \)
and inv2c: \( \text{Inv2c} s \)

shows \( \text{HInv6} s' \)

(proof)

**Theorem HEndPhase1-Inv6:**

assumes act: \( \text{HEndPhase1} s s' p \)
and inv: \( \text{HInv6} s \)
and inv1: \( \text{Inv1} s \)
and inv2a: \( \text{Inv2a} s \)
and inv2b: \( \text{Inv2b} s \)
and inv2c: \( \text{Inv2c} s \)

shows \( \text{HInv6} s' \)

(proof)

**Lemma outpt-chosen-2:**

assumes outpt: \( \text{outpt} s' = (\text{outpt} s) (p:= \text{NotAnInput}) \)
and inv2c: \( \text{Inv2c} s \)
and nextp: \( \text{HNextPart} s s' \)

shows chosen s = chosen s'

(proof)

**Lemma outpt-HInv6-2:**

assumes outpt: \( \text{outpt} s' = (\text{outpt} s) (p:= \text{NotAnInput}) \)
and inv: \( \forall p. \text{outpt} s p \in \{\text{chosen} s, \text{NotAnInput}\} \)
and inv2c: \( \text{Inv2c} s \)
and nextp: \( \text{HNextPart} s s' \)

shows \( \forall p. \text{outpt} s' p \in \{\text{chosen} s', \text{NotAnInput}\} \)

(proof)

**Theorem HFail-Inv6:**

assumes act: \( \text{HFail} s s' p \)
and inv: \( \text{HInv6} s \)
and inv2c: \( \text{Inv2c} s \)

shows \( \text{HInv6} s' \)

(proof)
theorem HPhase0Read-Inv6:
  assumes act: HPhase0Read s s' p d
  and inv: HInv6 s
  and inv2c: Inv2c s
  shows HInv6 s'
⟨proof⟩

theorem HEndPhase0-Inv6:
  assumes act: HEndPhase0 s s' p
  and inv: HInv6 s
  and inv1: Inv1 s
  and inv2c: Inv2c s
  shows HInv6 s'
⟨proof⟩

HInv1 ∧ HInv2 ∧ HInv2' ∧ HInv3 ∧ HInv4 ∧ HInv5 ∧ HInv6 is an invariant of HNext.

lemma I2f:
  assumes nxt: HNext s s'
  and inv: HInv1 s ∧ HInv2 s ∧ HInv2 s' ∧ HInv3 s ∧ HInv4 s ∧ HInv5 s ∧ HInv6 s
  shows HInv6 s' ⟨proof⟩

end

definition HInv :: state ⇒ bool
where
  HInv s = (HInv1 s ∧ HInv2 s ∧ HInv3 s ∧ HInv4 s ∧ HInv5 s ∧ HInv6 s)

theorem I1:
  HInit s ⟹ HInv s
⟨proof⟩

theorem I2:
  assumes inv: HInv s
  and nxt: HNext s s'
  shows HInv s'
⟨proof⟩
theory DiskPaxos imports DiskPaxos-Invariant begin

C.9 Inner Module

record
Istate =
  iinput :: Proc \Rightarrow InputsOrNi
  ioutput :: Proc \Rightarrow InputsOrNi
  ichosen :: InputsOrNi
  iallInput :: InputsOrNi set

definition IInit :: Istate \Rightarrow bool
where
  IInit s = (range (iinput s) \subseteq Inputs
         \land ioutput s = (\lambda p. NotAnInput)
         \land ichosen s = NotAnInput
         \land iallInput s = range (iinput s))

definition IChoose :: Istate \Rightarrow Istate \Rightarrow Proc \Rightarrow bool
where
  IChoose s s' p = (ioutput s p = NotAnInput
                   \land (if (ichosen s = NotAnInput)
                       then (\exists ip \in iallInput s. ichosen s' = ip
                             \land ioutput s' = (ioutput s) (p := ip))
                       else ( ioutput s' = (ioutput s) (p:= ichosen s)
                             \land ichosen s' = ichosen s))
                   \land iinput s' = iinput s \land iallInput s' = iallInput s)

definition IFail :: Istate \Rightarrow Istate \Rightarrow Proc \Rightarrow bool
where
  IFail s s' p = (ioutput s' = (ioutput s) (p:= NotAnInput)
                  \land (\exists ip \in Inputs. iinput s' = (iinput s)(p:= ip)
                  \land iallInput s' = iallInput s \cup \{ip\})
                  \land ichosen s' = ichosen s)

definition INext :: Istate \Rightarrow Istate \Rightarrow bool
where
  INext s s' = (\exists p. IChoose s s' p \lor IFail s s' p)

definition s2is :: state \Rightarrow Istate
where
  s2is s = (\{iinput = inpt s, ioutput = outpt s, ichosen=chosen s, iallInput = allInput s\)
theorem $R1$:
\[ [HInit s; is = s \text{s} s] \implies HInit is \]

\langle \text{proof} \rangle

theorem $R2b$:
\begin{align*}
\text{assumes} & \quad \text{inv: } HInv s \\
\text{and} & \quad \text{inv': } HInv s' \\
\text{and} & \quad \text{nxt: } HNext s s' \\
\text{and} & \quad \text{srel: } is = s \text{s} s \land is' = s \text{s} s' \\
\text{shows} & \quad (\exists p. IFail is is' p \lor IChoose is is' p) \lor is = is' \\
\end{align*}

\langle \text{proof} \rangle

end