LONDON'S GLOBAL UNIVERSITY

UCL

Mechanised Verification of Paxos-like Consensus Protocols

Anirudh Pillai

BSc Computer Science

Supervisor: Dr. Ilya Sergey

Submission Date: 30th April 2018

This report is submitted as part requirement for the BSc degree in Computer Science at UCL. It is substantially the result of my own work except where explicitly indicated in the text. The report may be freely copied and distributed provided the source is explicitly acknowledged.

Thesis advisor: Dr. Ilya Sergey Anirudh Pillai

Mechanised Verification of Paxos-like Consensus Protocols

Abstract

Distributed systems have become an integral component of the modern world. Most of these systems power applications with over a million users, thus, the importance of correctly implementing such systems in a way that keeps them up and running and functioning correctly, has never been greater. Despite their widespread use, building correctly functioning distributed systems has remained a notoriously hard challenge.

In this project we use Disel, a framework for *compositional* verification of distributed systems. Recent work has yielded tools that support building verified implementations of the core components of a distributed system, yet, Disel goes beyond them by enabling one to combine the verified implementations of the core components to produce a correct implementation of the entire distributed system. This project aims to use Disel to implement a library of reusable verified distributed components, based on the classical family of fault-tolerant asynchronous Paxos-like consensus protocol, in which a number of participant are supposed to reach an agreement despite the possible failure of a minority of them.

Acknowledgments

Acknowledgements

Contents

1
Introduction

1.1 The Problem

Distributed systems are ubiquitous in the modern world yet correctly implementing such systems is still very hard. Furthermore such systems are composed of various smaller components which in themself are hard to implement correctly. There has been recent work in developing frameworks to verify the implementation of the 'smaller' sub-components but there still remains the problem of checking whether these smaller components, when combined together, achieve the desired goal.

Disel is a framework for compositional verification of distributed protocols built on top of the Coq proof assistant. It allows one to verify the correctness of the implemented components and also to check whether the verified components function correctly when combined together.

Another fundamental problem in the field of distributed computing is to make a set of process achieve consensus on something, for examples, the occurrence of an event or the decision to take some action. The set of distributed computing protocols which tries to solve this problem are termed as consensus protocols. One of these protocols is the Paxos consensus protocol which has numerous variants according to the constraints imposed on the set of processes.

This project involves using Disel to mechanise the proof of the Paxos consensus protocol. We will also be using the code extraction capabilities of Disel to write a client application that uses the verified protocol to make set of distributed processes achieve consensus.

1.2 Aims and Goals

I have highlighted the aims and goals separately. The aims are what I want to achieve out of undertaking this project and the goals are the things that this project tries to achieve.

1.2.1 Aims

1. Learn about distributed computing. I wanted to learn how to reason about and implement distributed programs and the algorithms running on top of them. Working on verifying a popular distributed protocol, will teach me about all the concepts needed to understand such systems. While actually implementing applications using the protocol will teach me how to apply the concepts to the real world.
2. Contribute to open source software. Disel is an open source framework and working on that will enrich my open source contributions and improve my knowledge of the workflow.
3. Learn about formal verification. This was based partly on my interest in the various courses on logic. Using Coq for verification would enable me to apply my theoretical knowledge and use it for implementing and verifying a popular distributed system protocol.

1.2.2 Goals

1. Read about and understand the classical Paxos-like consensus algorithms.
2. Develop state transition systems for the algorithms and identify the invariants that need to be preserved during the operation of the algorithm.
3. Implement a simulation of the protocols in Python.
4. Formulate the implemented protocols in Disel by using the developed state-transition systems.
5. Mechanise the proofs of the identified protocol invariants in Disel/Coq.
6. Add additional communication channels and prove composite invariants.
7. Provide an abstract specification of the protocol, usable by third-party clients.
8. Mechanise a client application of the protocol verified out of the abstract interface.

1.3 Project Overview

During the course of the project we came up with a workflow for using Disel to mechanise proofs of protocols. This workflow is outlined in detail in the Disel section of chapter 2. The main stages in the project were as follows:

- First stage was to read about and understand the various concepts related to distributed computing and more importantly to understand the workings of Paxos-like consensus protocols. Implementing the Python simulation of the algorithm was very helpful in understanding the roles of each of the nodes in the protocol.
- The next stage was to design an adapted protocol that we would prove and to design the state transition diagrams and inductive invariant of that protocol. We also designed the client application that would use the protocol and created a Python simulation of it to ensure that the design functioned correctly.
- The final stage was actually mechanising the proofs in Disel. We first encoded the implementation of the client application and the protocol. Once, the client application functioned correctly, we moved on to writing proofs for it and the encoded protocol.

1.4 Report Overview

In the following chapter we look at various concepts relating to distributed computing and understand the two main components of this project, the Paxos protocol and the Disel framework. Then, with that background information, we look at how we adapted the design of the Paxos protocol and designed safety invariants to detect whether it is functioning correctly. Later, we move on to actually encoding the protocol in Disel and creating a client application that uses the verified protocol. Finally, we evaluate the results of the project and the experience of using the Disel framework and look at areas for future development.

2
Background

This chapter lays down all the previous research which the project builds on. Before going over the design decisions on the project we first need to understand this background information and look at related work to see different approaches used to solve the problem.

2.1 Distributed Systems

A distributed system is a model in which processes running on running different computers, which are connected together in a network, exchange messages to coordinate their action, often resulting in the user thinking of the entire system as one single unified computer. A computer in the distributed system is also alternatively referred to as a processor or a node in the system. Each node in a distributed systems has its own memory.

We will now go over a few concepts of distributed systems which will help us understand the characteristics of the protocols that run on these systems. This will lay down the groundwork for us to understand the Paxos protocol on which this project is based.

2.1.1 Asynchronous Environment

An asynchronous distributed system is one where there are no guarantees about the timing and order in which events occur. The clocks of each of the process in the system can be out of sync and may not be accurate. Therefore, there can be no guarantees about the order in which events occur. Further, messages sent by one process to another can be delayed for an arbitrary period of time.

A protocol running in an asynchronous environment has to account for these conditions in its design and try to achieve its goal without the guarantees of timed events. An asynchronous environment is very common for a real world distributed system but it also makes reasoning about the system harder because of the aforementioned properties.

2.1.2 Fault Tolerance

A fault tolerant distributed system is one which can continue to function correctly despite the failure of some of its components. A 'failure' of a node or 'fault' in a node means any unexpected behaviour from that node, for example, not responding to messages or sending corrupted messages.

Fault tolerance is one of the main reasons for using a distributed system as it increases the chances of your application continuing to functioning correctly and makes it more dependable. As Netflix mention on their blog 'Fault Tolerance is a Requirement, Not a Feature' [1]. With their Netflix API receiving more than 1 billion requests a day, they expect that it is guaranteed that some of the nodes in their distributed system will fail. Using a fault tolerant distributed system they are able to ensure that a small failure in some nodes doesn't hinder the performance of the overall system, hence, enabling them to achieve their uptime metrics.

Fault tolerant distributed system protocols are protocols which achieve their goals despite the failure of some of the nodes of the distributed system they run on. The protocol accounts for the failures and generally specifies the maximum number of failures and the types of failures it can handle before it stops functioning correctly.

2.1.3 State Machine Replication

For a client server model, the easiest way to implement it is to use one single server which handles all the client request. Obviously this isn't the most robust solution as if the single server fails, so does your service. To overcome the problem you use a collection of servers each of which is a replica of the original single server and ensure that each of these 'replicas' fails independently, without effecting the other replicas. This adds more fault tolerance.

State machine replication is method for creating a fault tolerant distributed system by replicating servers and using protocols to coordinate the interactions of these replicated servers with the client. Schneider [2] points out how to use state machine replication to implement fault tolerant services.

A state machine M can be defined as $M = \langle q_0, Q, I, O, \delta, \gamma \rangle$ where
q_0 is the starting state
Q is the set of all possible states.
I is set of all valid inputs
O is the set of all valid outputs
δ is the state transition function, $\delta : I \times Q \rightarrow Q$
γ is the output function, $\gamma : I \times Q \rightarrow O$

The state machine begins in the start state and transitions to other states and produces outputs when it receives the inputs. The transition and output are found using the transition and output functions. A deterministic state machine is one whose state transition and output functions are injective, i.e. multiple copies of the machine when given the same input, pass through the same order of states and produce the same output in the same order.

The method of modelling a distributed system protocol as state transition system was established by Lamport [3] and is very common. It is a critical component of this project as we will see soon when we need to encode our protocol in Disel.

State machine replication involves modelling our single server, from the client server model, and using multiple copies (replicas) of the same deterministic state machine and providing all of them with the input from the client. As long as one of the replicas does not crash, while resolving the request, we can successfully return a response to the client.

2.1.4 Byzantine Fault Tolerance

Byzantine fault tolerance is the most general form of fault tolerance in which any arbitrary form of failure should be defended against. This failure might not just be a node crashing or but could also be some node producing inconsistent output or having corrupted state. A node with a Byzantine fault might also behave 'maliciously', for example, by sending different responses for the same question to different nodes, or it might present itself as failed to some nodes and as functioning to others. It might do this to prevent the distributed algorithm from functioning correctly.

The term comes from the 'Byzantine Generals Problem' by Lamport et al [4] in which a set of nodes must decide on a course of action, but at the same time some of the nodes are 'malfunctioning' and give 'conflicting information to different parts of the system'.

2.1.5 Consensus Protocols

For handling faults in your distributed system you need to have replication. This leads to the problem of making all these replicas agree with each other to keep them consistent. Consensus protocols try to solve this problem.

> Consensus protocols are the family of distributed systems protocols which aim to make a distributed network of processes agree on one result.

These protocols are of interest because of their numerous real world applications. Let us take the example of a distributed database, which is a critical part of almost all large scale real world applications. This distributed database will run over a network of computers and every time you use the database you aren't guaranteed to be served by the same computer.

Suppose you add a file to the database. This action is performed by a node, in the distributed database, that was handling your 'add' request. Later when you want to retrieve the file from the database you might be served by a different node in the distributed database that did not perform the 'add' request. In order for the new node to know that the file exists in the system, you will need to use a consensus protocol which helps all the nodes in the system (which handle user requests) to agree upon the result that the file has been added to the system.

A popular consensus protocol is the blockchain consensus protocol which powers Bitcoin. Pîrlea et al [5] have verified a subset of this protocol in Coq. Other examples of consensus protocols are Raft [6], Stellar Consensus Protocol [7] and Paxos [8], which we look at next.

2.2 Paxos

Having understood the the main concepts behind distributed system protocols, we can now finally get to the protocol at the heart of this project. Paxos is a family of asynchronous, fault tolerant, consensus protocol which achieves consensus in a network of unreliable processes as long as a majority of them don't fail. Paxos was outlined in Lamport's 1998 paper, 'Part Time Parliament' [9].

Paxos is used for state machine replication. Once you have multiple replicas servicing client requests, how do you makes sure that all of these replicas agree on what action to take? The solution is simply to use a consensus protocol like Paxos to make all replicas agree on something. Paxos is heavily used in building software. It has been used at Google to build a fault tolerate database [10] and the Chubby [6] lock service.

Paxos has many variants but the one we will focus on is the one we actually prove in Disel, single decree Paxos, also know as simple Paxos. Simple Paxos is an algorithm that helps a distributed network of processors to achieve consensus. Consensus is achieved when the network of processor agree on a common value.

For simple Paxos, we assume the following assumptions hold about the processors and the environment, in order for the protocol to function correctly.

- Processors communicate between each other by exchanging asynchronous messages between them.
- Processors run at an arbitrary speed and may fail or restart. Handling this relates to the fault tolerant nature of Paxos. Also, we assume that Byzantine faults don't occur. This means that all processors actually work together to try to achieve consensus on a value. There are variants of Paxos which can also handle Byzantine failure buy not simple Paxos. (This can be linked to the 'Practical Byzantine Fault Tolerance' paper, by Castro et al [11], which states that any algorithm handling Byzantine faults must have three phases. Simple Paxos only has two phases.)

As for fault tolerance of Paxos, in order to handle a failure of upto f processors, we need to have a minimum $2f + 1$ processors participating in the algorithm. This means Paxos functions correctly as long as a majority of the processors in the network do not fail. We will see shortly why just a majority needs to be functioning correctly.

A processor participating in simple Paxos, may have one or more of these three different roles - proposer, acceptor or learner.

- **Proposer** - A process acting as a proposer listens for client request and proposes a value which the network of processes tries to agree upon.
- **Acceptor** - acceptors receive proposed values from the proposers and then respond to them stating whether they are in a position to accept the value or not. For a proposed value to be accepted, a majority of all the existing acceptors have to accept the proposed value.

- **Learner** - The learner has to be informed when an acceptor accepts a value. The learner can then figure out when consensus has been achieved by monitoring when a majority of acceptors have accepted the same proposal. Once the acceptors agree on a value, the learner may act on the value by, for example, sending a request to the client informing them about the agreed value.

2.2.1 Choosing a Value

For passing around the value to be chosen from one processor to the other, a processor must send a 'proposal' to the other processor. You can think of a proposal as just a tuple $\langle n, v \rangle$. n is just a natural number associated with a proposal which makes it easy to keep track of all the different proposals and v is the value the value that is being proposed.

A `quorum` of acceptors is a subset of the set of all acceptors and has a length greater than $N/2$ where N is the length of the set of acceptors. A `quorum` is just a set denoting a majority of all the available acceptors.

> Consensus is achieved when a proposal is accepted by a majority of acceptors.

The Algorithm

Simple Paxos runs in rounds until consensus is achieved (a successful round occurs when a majority of acceptors accept a proposal). A successful round of the algorithm has two phases, each of which can be subdivided into parts a, b.

- **Phase 1a: Prepare Request.** A proposer sends a proposal $\langle n, v \rangle$ to each acceptor in any randomly chosen `quorum` of acceptors. This first message that the proposer sends out is called a `prepare request`. This phase can be thought of as the proposer trying to 'prepare' the acceptors to 'accept' a value in the future.

- **Phase 1b: Promise Response.** An acceptor on receiving a prepare request, responds with a `promise response`, if and only if the acceptor has not already sent a promise response with a proposal containing a proposal number n' where $n' > n$.

  A promise response for proposal $\langle n, v \rangle$ is basically a guarantee (a 'promise') that this acceptor will not respond to any messages with proposals that have a proposal number n' where $n' <= n$.

  Thus, if an incoming prepare request has proposal number that is not greater than what the acceptor has already promised earlier, then the acceptor can ignore this prepare request by not responding to it. Although, for speeding up the protocol, the acceptor can send out a `nack response` which tells the proposer to stop trying to achieve consensus with this proposal.

If the acceptor has not already accepted a proposal, then the body of the promise response can be empty, otherwise, the acceptor must include in it the last proposal that it accepted.

- **Phase 2b: Accept Request.** If the proposer successfully receives promise responses from a majority of acceptors, then it can send out an `accept request`. A accept request is a message containing a proposal which tells an acceptor to accept this proposal if it can.

  The proposer creates a new proposal, $\langle n, v' \rangle$ where n is the same as in the proposal which the proposer sent in its prepare request. But, v' is the value from the highest numbered proposal, selected from all the proposals that the proposer receives in the promise responses. If none of the promise responses received by the proposer contain a proposal, the proposer is free to set v' to any value it likes. The proposer then sends this accept request with proposal $\langle n, v' \rangle$ to another `quorum` of acceptors.

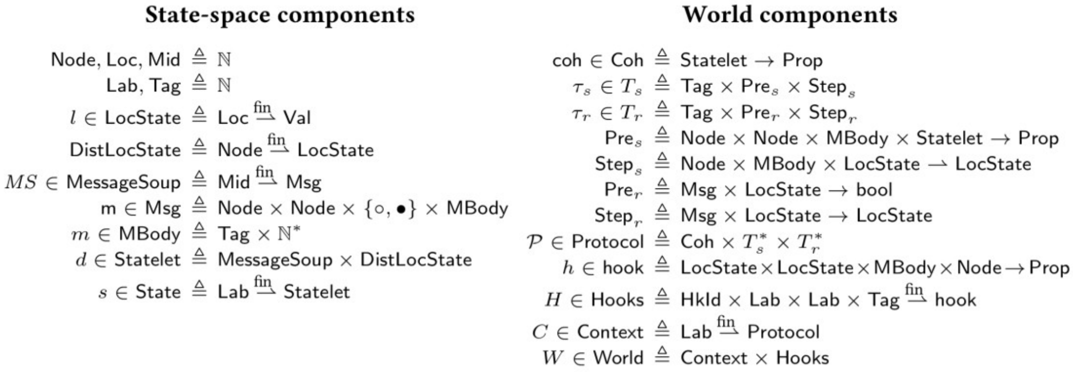
- **Phase 2b: Accepted Response.** Any acceptor that receives the accept request with proposal $\langle n, v \rangle$, responds with an `accepted response` if and only if it hasn't already promised not to respond to any proposals with proposal number n' where $n' >= n$. The `accepted response` is sent to the learner and contains the proposal that was accepted by the acceptor.

2.2.2 Informing learner

When consensus is achieved, a learner must be informed that a majority of acceptors have agreed on a value. There are various ways to do this.

1. Whenever an acceptor accepts a value, it should send the accepted proposal to all the learners (`accepted response`). The learners will then know when a majority of acceptors have accepted the same value.

2. We can have a distinguished learner which informs other learners about the choose value. The acceptors only need to inform this particular learner when they accept a value. This reduces number of messages sent but the distinguished learner becomes the single point of failure and also requires an additional round of sending messages where the distinguished learner informs other learners that a value has been chosen.



State-space components

$$
\begin{aligned}
\mathsf{Node}, \mathsf{Loc}, \mathsf{Mid} &\triangleq \mathbb{N} \\
\mathsf{Lab}, \mathsf{Tag} &\triangleq \mathbb{N} \\
l \in \mathsf{LocState} &\triangleq \mathsf{Loc} \overset{\text{fin}}{\rightharpoonup} \mathsf{Val} \\
\mathsf{DistLocState} &\triangleq \mathsf{Node} \overset{\text{fin}}{\rightharpoonup} \mathsf{LocState} \\
MS \in \mathsf{MessageSoup} &\triangleq \mathsf{Mid} \overset{\text{fin}}{\rightharpoonup} \mathsf{Msg} \\
\mathsf{m} \in \mathsf{Msg} &\triangleq \mathsf{Node} \times \mathsf{Node} \times \{\circ, \bullet\} \times \mathsf{MBody} \\
m \in \mathsf{MBody} &\triangleq \mathsf{Tag} \times \mathbb{N}^* \\
d \in \mathsf{Statelet} &\triangleq \mathsf{MessageSoup} \times \mathsf{DistLocState} \\
s \in \mathsf{State} &\triangleq \mathsf{Lab} \overset{\text{fin}}{\rightharpoonup} \mathsf{Statelet}
\end{aligned}
$$

World components

$$
\begin{aligned}
\mathsf{coh} \in \mathsf{Coh} &\triangleq \mathsf{Statelet} \to \mathsf{Prop} \\
\tau_s \in T_s &\triangleq \mathsf{Tag} \times \mathsf{Pre}_s \times \mathsf{Step}_s \\
\tau_r \in T_r &\triangleq \mathsf{Tag} \times \mathsf{Pre}_r \times \mathsf{Step}_r \\
\mathsf{Pre}_s &\triangleq \mathsf{Node} \times \mathsf{Node} \times \mathsf{MBody} \times \mathsf{Statelet} \to \mathsf{Prop} \\
\mathsf{Step}_s &\triangleq \mathsf{Node} \times \mathsf{MBody} \times \mathsf{LocState} \rightharpoonup \mathsf{LocState} \\
\mathsf{Pre}_r &\triangleq \mathsf{Msg} \times \mathsf{LocState} \to \mathsf{bool} \\
\mathsf{Step}_r &\triangleq \mathsf{Msg} \times \mathsf{LocState} \to \mathsf{LocState} \\
\mathcal{P} \in \mathsf{Protocol} &\triangleq \mathsf{Coh} \times T_s^* \times T_r^* \\
h \in \mathsf{hook} &\triangleq \mathsf{LocState} \times \mathsf{LocState} \times \mathsf{MBody} \times \mathsf{Node} \to \mathsf{Prop} \\
H \in \mathsf{Hooks} &\triangleq \mathsf{HkId} \times \mathsf{Lab} \times \mathsf{Lab} \times \mathsf{Tag} \overset{\text{fin}}{\rightharpoonup} \mathsf{hook} \\
C \in \mathsf{Context} &\triangleq \mathsf{Lab} \overset{\text{fin}}{\rightharpoonup} \mathsf{Protocol} \\
W \in \mathsf{World} &\triangleq \mathsf{Context} \times \mathsf{Hooks}
\end{aligned}
$$

Figure 2.1: Disel's distributed state space and the world components as show in [12]

3. We can use a set of distinguished learners. The acceptors inform these distinguished learners who then inform the other learners. This increases reliability but also increases the number of messages exchanged.

2.3 Disel

Having learnt the concepts behind distributed systems and the Paxos protocol, we can now look at Disel. Disel [12] is a verification framework, built on top of the Coq theorem prover, that enables one to prove the safety properties of a distributed protocol by breaking down the protocol into its state space invariants and its atomic properties. The unique aspect of Disel is that it also allows one to combine these separate verified protocols to create a complete verified system. Additionally, the code extraction properties of Disel enables one to extract the verified runnable OCaml code for the protocols which can be combined with an shim that supplies the implementation of the various primitive operations like sending or receiving a message.

2.3.1 Protocol Encoding

We will now look at how Disel requires the state space of a protocol to be encoded in it. The figure 2.1 shows the distributed state space and the world components in Disel.

As you can see from 2.1, a `statelet` is a component in the protocol and consists of the `MessageSoup` and the `DistLocState`. A message soup is 'finite partial map from unique message identifiers to messages, each of which carries its sender and recipient node ids, the payload m, which includes a tag, and a boolean indicating whether the message is already received or not yet' [12]. While the local state of a node 'maps each node id into protocol-specific piece of local state, represented as a mapping from locations (isomorphic to natural numbers) to specific values' [12].

Additionally, a protocol P in Disel is defined as a tuple of the `Coherence`, the set of send transitions and the set of receive transitions. Let us now look at each of these components in detail.

A `Coherence` is a function that takes in a statelet and returns a proposition indicating whether the statelet is valid or not. Thus, the coherence allows us to impose constraints on the local state of each node and on the message soup.

A transition is defined as a tuple of consisting of the following:

1. Tag - a unique natural number identifier for the message to be sent in the transition.
2. Precondition - The constraints that are imposed on identity of the sender of the message, identity of the receiver is, the message that is being sent and on the local state of the sender/receiver (depending on whether it is a send transition/receive transition).
3. Step function - Describes how the local state of the sender/receiver changes after making the transition.

You can see in the code example below how the step function and pre condition are encoded for sending the `prepare request` in Paxos. `PInit`, `PSentPrep` and `PWaitPrepResp` are some states the proposer can be in.

```
(* Changes in the Node state triggered upon send *)
Definition step_send (s: StateT) (to : nid) (p: proposal): StateT :=
   let: (e, rs) := s in
   match rs with
   ...
   (* Step function for the sending prepare request *)
   | PInit p' ⇒
     if acceptors == [:: to] (* if only one acceptor *)
     then (e, PWaitPrepResp [::] p')
     else (e, PSentPrep [:: to] p')
   ...
   | _ ⇒ (e, rs)
   end.

(* Precondition for send prepare request transition *)
Definition send_prepare_req_prec (p: StateT) (m: payload) :=
  (∃ n psal, p = (n, PInit psal)) ∨
  (∃ n tos psal, p = (n, PSentPrep tos psal)).
```

2.3.2 Protocol to Programs

The state transitions that we implement in the protocol encoding phase, are the first step towards creating executable programs using Disel. We can then use the library of *transition wrappers* provided by Disel that allow one to decorate low level send/receive primitives with the transitions that we have defined. These decorated primitives can later on be used to extract code for executable programs. In Chapter 5, we will dive into the details of how we extracted the code for our client application running Paxos.

The send_action_wrapper wrapper provided by Disel takes a send transition encoded by us and returns a program that will send a message.

```
Program Definition send_prepare_req psal to :=
  act (@send_action_wrapper W paxos p l (prEq paxos)
     (send_prepare_req_trans proposers acceptors) _ psal to).
```

The tryrecv_action_wrapper is similar but the main difference is that in a received transition, we may receive messages from any of the multiple protocols that might be executing at the time. To address this problem, we need to check the tag *t* returned by the receive wrapper and ensure that this tag belongs to the protocol that was specified in the wrapper. In the code example below, we check that the received message is either a promise_resp or a nack_resp both of which belong to the paxos protocol and are valid responses to a prepare_req.

```
(* Non blocking receive *)
Program Definition tryrecv_prepare_resp := act (@tryrecv_action_wrapper W p
     (* filter *)
     (fun k _ t b ⇒ (k == l) && ((t == promise_resp) || (t == nack_resp))) _).
```

If an incoming message matches the conditions specified, the wrapper returns Some(from, m) where *m* is the message and *from* is the sender. Otherwise it returns None.

These low level primitives can then be combined together for specifying the roles of each node in the protocol. We can use the `send_prepare_req` to come up with `send_prepare_req_loop` which every proposer performs when it starts up. These functions can then further be combined together to give the entire implementation of a node. `proposer_round` below is the program that each node acting a proposer executes.

```
Program Definition send_prepare_req_loop e (psal: proposal):
  {(pinit: proposal)}, DHT [p, W]
  (fun i ⇒ loc i = st :→ (e, PInit pinit),
   fun r m ⇒ r = tt ∧
           loc m = st :→ (e, PWaitPrepResp [::] pinit)) :=
  Do (ffix (fun (rec : send_prepare_req_loop_spec e) to_send ⇒
           Do (match to_send with
              | to :: tos ⇒ send_prepare_req psal to ;; rec tos
              | [::] ⇒ ret _ _ tt
              end)) acceptors).

Program Definition proposer_round (psal: proposal):
  {(e : nat)}, DHT [p, W]
  (fun i ⇒ loc i = st :→ (e, PInit psal),
   fun res m ⇒ loc m = st :→ (e.+1, PAbort))
  :=
  Do (e <-- read_round;
     send_prepare_req_loop e psal;;
     recv_promises <-- receive_prepare_resp_loop e;
     check <-- check_promises recv_promises;
     if check
     then send_accept_reqs e (choose_highest_numbered_proposal psal recv_promises)
     else send_accept_reqs e [:: 0; 0]).
    (* If check fails then send an acc_req for (0, 0) which will never be
      accepted by any acceptor *)
```

Once this implementation has been finished in Disel we can use Disel's extraction capabilities to extract the OCaml code for executing the program. (Outlined in Chapter 5)

2.3.3 Inductive Invariant

As many other verification tools for distributed protocols, Disel relies on using inductive invariants to prove the correctness of the protocol. In this section, we look at what are invariants and inductive invariants.

A invariant in a program is a property of a program that always holds true, from the start through to the end of execution of the program. An invariant can be for something more specific like a function or even a loop. The only requirement is the property described by the invariant should always hold before, during and after execution of the part of that code. To put it more formally, 'An invariant of a transition system is a property that is always true, in all of the system's reachable states.' [13].

The problem with using just an invariant like $x > 2$ is that, you may assume that the invariant holds before the execution of the program, but you still do not have a guarantee that this invariant will hold during and after the execution of the program, i.e. hold in any state of the program.

Therefore, we need to make our invariants *inductive*. An inductive invariant of a program, is an invariant which if it holds in a particular state s of the program, it is guaranteed to hold in all states of the program reachable from s. Thus, having an inductive invariant that holds in the start state of a program is much more useful, as we can be sure that the invariant will continue to hold throughout and after the execution of the program.

This means that once you establish an inductive invariant from the given invariants of a protocol and a starting state for the protocol in which the invariant holds, in order to show that the protocol maintains the invariant, you only need to prove the inductive invariant maintains the induction property over any possible state transition in the protocol. This is exactly how you use an inductive invariant in Disel. Developing and encoding the inductive invariant for the protocol in Disel is the way to verify it.

2.4 Related Work

People have attempted to create software for verfying the correctness of distributed systems. IronFleet [14], developed at Microsoft Research, can prove not just safety but also liveness properties of distributed systems and has been used to verify a 'complex implementation of a Paxos-based replicated state machine library'. Verdi [15] is another framework built on top of Coq and has been used to develop the ‘proof of linearizability of the Raft state machine replication algorithm’. Ivy [16] is another tool which makes it much easier to find and prove inductive invariants for the system. Other similar tools are PSync [17] and EventML [18].

3
Requirements and Analysis

3.1 Problem Statement

Having looked at the background information on distributed sytems, consensus protocols and Disel, we can formalise the problem statement for the project. The project aims to mechanise the proof of Paxos-like consensus protocols in Disel. This will involve doing the modelling on the protocol to come up with state transitions and inductive invariants, in order to encode it in Disel. Additionally, we will also implement a client application built on top of the verified protocol that uses Disel's code extraction features.

3.2 Requirements

1. Adapt Paxos for encoding in Disel and devise the state-transition system for this protocol.
2. Develop an inductive invariant for the adapted protocol that ensures the protocol functions correctly by imposing requirements on the global state of the system
3. Implement a simulation of the adapted protocol with the developed state transition system.
4. Mechanise the proof of the adapted protocol in Disel/Coq. Thereby, providing a library of reusable verified distributed components.
5. Mechanise a client application of the protocol verified out of the abstract interface.

3.3 Analysis: Approach to Mechanising Proofs in Disel

Having decided on the requirements we came up with a workflow to mechanise the proof in Disel. Finishing all the stages in the workflow will help us to meet all our requirements.

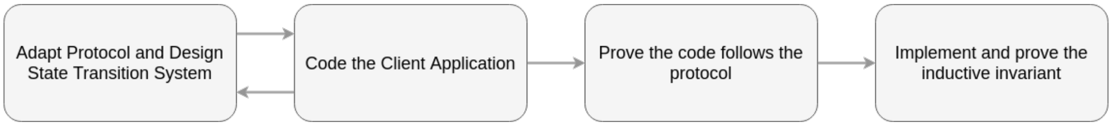

Adapt Protocol and Design State Transition System
Code the Client Application
Prove the code follows the protocol
Implement and prove the inductive invariant

Figure 3.1: Disel Workflow

3.3.1 Adapt protocol and design state transition system

By adapting the protocol we try to focus on the 'core' parts of the protocol and to do away with the 'convenience' parts. For Paxos, this is focusing on the part of the protocol that deals with achieving consensus and not looking at the part where the learner is informed of the decision.

We also need to design state transition systems for the nodes that participate in the protocol. This makes it easier for us to encode the protocol in Disel as we already know which send and receive transitions we will need from each state and thus can easily code the transition wrappers.

In chapter 4, we look go into the details of how we tackled this stage on our way to mechanising the proof of Paxos.

3.3.2 Code the client application

Secondly, we need to think of a client application that uses the implemented protocol. We need to design and implement a client that will demonstrate the properties of the protocol that we want to prove. In case of Paxos, we will design a client where nodes try to acheive consensus on one of the proposals that the proposer is initialised with. This will enabled us to see in action the stages of the protocol that lead to consensus being achieved.

While using Disel, we will often had to cycle between stage 1 and stage 2. This is because while implementing the client, you realise things like, you are missing one state for a node that is required in order for the protocol to progress. There was a case when we saw this while writing the client for Paxos. We realised that we were missing the `PAbort` state for the proposer, which was necessary to signify when a proposer stops participating in the protocol.

The process of cycling between stages 1 and 2 allow us to solidify our adapted protocol. Doing this at an early stage (before starting the proofs) also has the advantage of us not having to rewrite a lot of code that will also break all the proofs relating to the change.

Additionally, implementing the client also helps us identify unnecessary stages and transitions in the adapted protocol which were not needed to implement the client. Reducing the number of states and transitions vastly reduces the amount of things you will need to prove in the later stages.

3.3.3 Prove the code follows the protocol

The next stage involves encoding and proving the protocol and proving that the code for the client actually follows the adapted protocol. Thus, finishing the proofs in this stage gives us confidence that our adapted protocol can actually be used to fulfil the role which our client performs. In case of Paxos, this helped us realise that our adapted protocol can be used to achieve consensus among the acceptors. Finishing this stage means that we have finished the proof of the client. Yet, at this stage we can only be sure that the code follows the protocol.

Reaching this state also gives us relatively strong correctness properties. This because just by ensuring the code follows the protocol, if the protocol we have implemented has already been, we can know that the code will work correctly although we cannot be completely sure until we finish the next stage. In the mechanising of Paxos we were only able to reach till this stage, we designed the inductive invariant but ran out of time to encode it. As the actual protocol we encoded is the simple Paxos algorithm, it still gives us quite a strong correctness as the simple Paxos algorithm has a proof of safety and has also been used to implement real world systems.

3.3.4 Implement and prove the inductive invariant

An inductive invariant is necessary as it helps verify the entire global system. As without it, the code might follow the protocol, but the protocol might itself be broken. In case of Paxos this could be the case that the nodes follow the protocol but they never achieve consensus.

4
Protocol Design and Encoding

This chapter has been split into two parts. First is the 'Modelling' section where look at the design of the adapted protocol, state transitions and inductive invariant for Paxos. We also look at the Python simulator that helped solidify these designs before encoding them in Disel. The latter part of this chapter explains how the adapted protocol was encoded in Disel.

4.1 Modelling

4.1.1 The Adapted Protocol

For mechanising the proof of Paxos in Disel, we followed the approach highlighted in the Disel section of Chapter 3. Applying this approach meant we needed to come up with the state transition system and the inductive invariant for the protocol which we will encode in Disel. Before coming up with these things though, we decided to simplify the actual simple Paxos protocol that we will prove.

The goal of this simplification was to reduce the amount of things that we will need to prove in Disel by focusing on the 'core' parts of the protocol which lead to consensus being achieved. The 'convenience' parts of the protocol, like the sub phase of informing the learner, aren't necessary for consensus being achieved in the global state and can also be proved separately after we have finished proving the 'core' parts of the protocol. Garcia-Perez et al [19] have also showed how the optimizations of a protocol can be verified separately from the 'core' protocol. In their paper, they produce a verified implementation of multi Paxos using their verified implementation of simple Paxos.

In order to adapt the protocol and focus on the 'core' parts, the first thing we did was to do away with the 'Informing the learner' phase of simple Paxos. This is the phase where once an acceptor has accepted a proposal, it then informs a leaner by sending it an accepted request. We decided against proving this because we can use the inductive invariant to check the global state of the system. The inductive invariant allows to check when a majority of acceptors have accepted a proposal and what proposal each of them has accepted. Thus, we can know from the inductive invariant when consensus has been achieved by checking the values of each of the accepted proposals.

Doing away with the learning phase also meant that we did not have to implement a learner. The learner is useful in the actual Paxos implementations as it can detect when consensus is achieved and can then inform the client, its presence does not change how consensus is achieved. Removing the learner simplified our state transition diagram for the protocol as we did not have to account for the states of the learner and also the *Phase2b* transition of the accepted request.

Additionally, we decided to remove some optimisations from the protocol. Optimisations are aspects of the protocol that improve its running time or resource consumption by improving upon the 'mundane' way of doing the same thing. Removing optimisations allowed us to simplify our proofs in Disel.

Firstly, we decided that a proposer, if it fails while trying to achieve consensus with a proposal number (i.e. it receives a nack), it then does not retry with a higher proposal number. Removing this optimisation meant we did not have to deal with the state of a proposer where it changes the proposal number it was initialised with. Removing this optimisation only effects the liveness of the protocol but not its safety, as if a proposer receives a nack, it is just an indication that it will not be able to achieve consensus with the proposal number that it is currently using. Thus, in order for consensus to be achieved, a proposer which is initialised with a higher proposal number will have to successfully get promises from a quorum of acceptors.

Additionally we removed the minor optimisation of choosing a majority for sending requests from the proposer. The proposer instead of choosing a quorum of acceptors for sending a message, chooses the entire set of acceptors. This does not alter the protocol as the entire set of acceptors is a valid quorum of acceptors.

This adapated and simplified protocol allows us to focus on verifying the core logic (the part dealing with achieving consensus) of Paxos. The optimisations and 'conveniece' that we removed can be verified separately after the core logic has been verified.

4.1.2 State Transitions

Having adapted the protocol, we then had to create a state transition system for the nodes in our protocol in order to encode it in Disel. For creating the states, we need to look at what the function of each node is in the protocol at a particular moment and what type of data it holds at that time.

A node should only be able to transition from one state to another when it either receives or sends a message. Therefore, the data held by the node in each state should be enough for it to be able to create the message it wants to send or to be able to correctly process the message it receives.

We tried to minimise the number of states and transitions between them, in order to simplify the proof in Disel. This was important because each state transition has to be shown to hold with the invariant so reducing the state transitions, reduces the number of proofs.

We decided that a node can either be initialised as an acceptor or a proposer. The state transitions of each node will depend upon this initial state, so below we will separately look at the state transition systems for the proposer and the acceptor.

The main difference between the state transition for the acceptor and the proposer is that the acceptor sends and receives messages from a single proposer while a proposer has to send and receive messages from all the acceptors.

Proposer

The proposer starts off in the `PInit` state where it is initialised with a `proposal` (a custom defined data type which is tuple of two natural numbers), $\langle p, v \rangle$. The natural number p is the proposal number and v is the value that the proposer tries to achieve consensus on. This means that the first prepare request this proposer sends will include this proposal $\langle p, v \rangle$.

The proposer then moves to the `PSentPrep` state when it starts to send prepare requests to the acceptors. In this state, the proposer still holds the proposal but additionally now also stores a list of natural numbers, `sent_to`. This list stores the natural number identifiers of the acceptors, this proposer has sent requests to. Whenever it sends a prepare request to an acceptor, it adds the identifier of the acceptor to this list. The proposer remains in the `PSentPrep` state and keeps sending prepare requests until the contents of `sent_to`

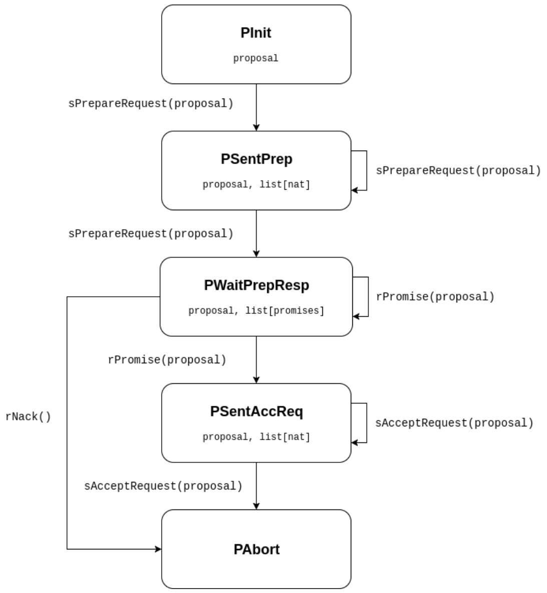


Figure 4.1: proposer State Transition Diagram

become equal to the global list `acceptors` which holds the identifiers of all the acceptors in the system. This means the proposer stays in this state until it has sent a prepare request to every single acceptor in the system.

Once the proposer has sent the last prepare request, it them transitions to the `PWaitPrepResp` state. In this state the proposer again holds a proposal and another list `promises` which is defined as below to be a list of tuples each containing a `nid` (a natural number identifier for a node), a boolean and a `proposal`.

```
Definition promises := seq (nid * bool * proposal).
```

The proposer stays in this state and keeps receiving messages from the acceptor until one of the following two things happen:

1. It receives a nack response from the acceptor. This indicates that the acceptor might already have promised a proposal with a proposal number greater than *p*. This leads to the proposer to transition into the `PAbort` state. In this state the proposer basically gives up trying to achieve consensus using the proposal number *p* that it was initialised with and completely stops sending and receiving messages. Hence, the proposer doesn't need to hold any data in this state.

2. It receives a promise response from every single acceptor. When this happens, the

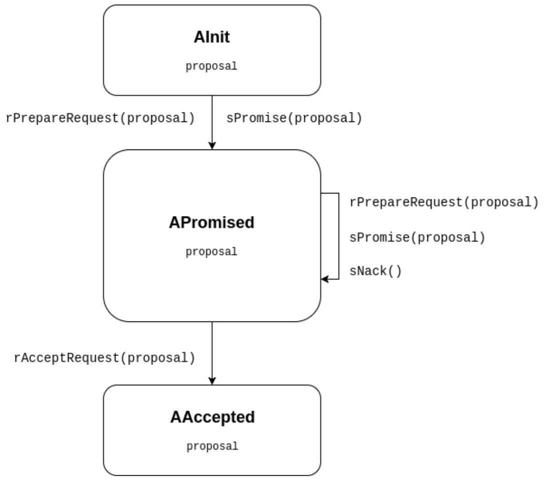


Figure 4.2: acceptor State Transition Diagram

proposer transitions to the `PSentAccReq` state.

When the proposer reaches the `PSentAccReq`, it means it has received a promise from every single acceptor and it can now start sending accept requests to each of the acceptors in the system. In the `PSentAccReq` the proposer again stores a list `sent_to` to keep track of every single acceptor it has already sent the accept request to. It also stores another `proposal` which is has the same proposal number p that the proposer was initialised with but the value v is the the value from the highest numbered proposal it received in a promise response. In the verification section, we will look at how it determines this value by looping over the `promises` list from the `PWaitPrepResp` state. The sending of accept requests works similar to sending prepare requests in the `PSentPrep` state. Finally, when the proposer finishes sending the accept requests to all the acceptors, it transitions to the `PAbort` state where it stops sending and receiving messages.

Acceptor

The acceptor starts off in the `AInit` state. It does not hold any data in this state as it is not sending any messages. It keeps listening for messages and on receiving a prepare request message, it transitions to `APromised` state.

In the `APromised` state, the acceptor holds a `proposal`. This is the highest numbered proposal that it has received so far in a prepare request message. In this state, on receiving a prepare request, if the proposal number of the proposal in the prepare request is greater than the proposal number of the proposal it currently holds, it updates its current state to hold the new proposal but still remains in the `APromised` state. If the proposal number of the proposal in the prepare request is not greater, the acceptor sends a nack response to the proposer who sent the prepare request and does not update its state.

An acceptor in the `APromised` state, on receiving an accept request, if the value of the proposal number of the proposal in the accept request is greater than the proposal number of the proposal that it currently holds, it transitions to the `AAccepted` state where it now holds the new proposal with the greater proposal number. If the proposal number of the new proposal number is not greater, the acceptor remains in the same state.

In the `AAccepted` state, the acceptor stops listening for and responding to messages. This is similar to the `PAbort` state for the proposer.

4.1.3 Inductive Invariant

A critical part of proving our protocol in Disel was designing an inductive invariant for our adapted protocol. The inductive invariant helps ensure the correctness of our adapted protocol enabling us to imposing requirements on the global state of the system. For proving the correctness of Paxos we found that our invariant had to capture when consensus is achieved on a value and also that once consensus is achieved on a particular value, further rounds of the protocol don't change this value.

> Inductive invariant means a property which when it holds for a state s, it will hold for any state s' reachable from s.

The crux of Paxos' correctness lies in the prepare phase where, before sending the accept request, the proposer must first set the value of the proposal, that it wants to propose, to be the value of the highest numbered proposal it receives as a promise. This ensures that when consensus has been achieved on a value 'v', further rounds of the protocol also ensure that consensus will only be achieved on 'v'.

We established two invariants **I1** and **I2** which together form an inductive invariant for our protocol that also proves its safety.

- **I1** simply tries to say that there can only be one unique value associated with a particular proposal number for any proposal that has been accepted.

- **I2** states that once consensus has been achieved on a value v, every higher number proposal accepted by an acceptor also has the value v.

The mathematical representations for the invariants is given by.

- **I1** - $\forall a_i, a_j \in A, \langle p, v_i \rangle \in a_i.accepted \wedge \langle p, v_j \rangle \in a_j.accepted \rightarrow v_i = v_j$.
- **I2** - $\forall a \in A, \forall \langle p_i, v_i \rangle \in a.accepted \rightarrow \forall \langle p_j, v_j \rangle \in a.accepted \wedge p_j > p_i \rightarrow v_j = v_i$.

I1 is preserved because if there are n proposers, they are initialised with a unique proposal number and throughout the running of the adapted protocol, the proposer always uses this unique proposal number for any value that it proposes. Hence, two different proposers never propose a proposal with the same proposal number as they all are initialised with different proposal numbers. Additionally, each proposer only sends one round of accept requests with the same proposal. So as each proposer proposes only one value with a unique proposal number, hus, we can conclude that each accepted proposal will have a unique value associated with a particular proposal number.

For proving that **I2** is preserved, we need to show that once consensus has been achieved on a proposal with value *v* then every other proposal, with a higher proposal number, on which consensus is achieved will also have proposal value set to *v*.

In order for consensus to be achieved on a new proposal, the new proposal first needs to be accepted by an acceptor. So we can reduce the requirement as follows.

$\Rightarrow$ If consensus has been achieved on a proposal $\langle p_1, v_1 \rangle$ then every other proposal $\langle p_2, v_2 \rangle$ accepted by any acceptor, where $p_2 > p_1$, has $v_2 = v_1$.

Further, acceptors can only accept a proposal which has been proposed by a proposer.

$\Rightarrow$ If consensus has been achieved on a proposal $\langle p_1, v_1 \rangle$ then every accept request $\langle p_2, v_2 \rangle$ sent by the proposer with $p_2 > p_1$, has $v_2 = v_1$.

In order to prove the above, let's assume that consensus has been achieved on a proposal $\langle p_1, v_1 \rangle$. (4.1)

After that lets say that the systems achieves consensus on $\langle p_2, v_2 \rangle$ where $p_2 > p_1$ and there does not exist p_x such that consensus has been achieved on a proposal with proposal number p_x where $p_1 < p_x < p_2$.

So from our assumption (4.1), there must be a majority of acceptors such that they have accepted the proposal $\langle p_2, v_2 \rangle$. So we need to show that in $v_2 = v_1$. This is ensured in Paxos because of Phase 1 where the proposer must first get promises from a majority.

So any majority the proposer for p_2, v_2 gets in Phase 1, will have at least one acceptor a that has accepted $\langle p_1, v_1 \rangle$. Paxos also ensures that before sending the accept request for p_2, v_2, the proposer must select the value of the highest numbered proposals which it receives in its promises.

So the acceptor a will send $\langle p_1, v_1 \rangle$ in its promise message to the proposer. As $\langle p_2, v_2 \rangle$ is the only proposal number which has proposal number greater than p_1, the proposer must set $v_2 = v_1$ in its accept request message $\langle p_2, v_2 \rangle$ as v_1 is the value of the highest numbered proposal that it receives as a promise response. Thus, meeting our above requirement.

4.1.4 Simulator

The next step after designing the adapted protocol was to implemented a simulator for it in Python. The simulator was modelled according to Disel, in that each process has send and receive transitions and that each node follows a state transition system. In order to test the protocol, we only used the state transitions we designed in the adapted protocol. The type of messages that each node sends or receives and the data it holds were all taken from the state transition system.

In the code listing below you can see the main body that an acceptor node runs in the simulator. It first checks the type of message and then performs an action depending on its current state. For example, when it receives a `AcceptRequestMessage`, if it is in the `AInit` state then it accepts the proposal, otherwise if it is in the `APromised` state, it first the proposal number of the incoming message (proposal) and accepts the proposal only if the number is greater than the number the acceptor has promised already.

```python
class acceptor(Process):
   ...
   def body(self):
      while True:
         msg = self.get_next_msg()
         p_no, p_val = msg.proposal

         if isinstance(msg, PrepareRequestMessage):
```

```
       if self.state[0] == "AInit":
          self.state = ("APromised", msg.proposal)
          self.send_promise_resp(p_no)
       elif self.state[0] == "APromised":
          promised_no, _ = self.state[1]
          if p_val < promised_no:
             self.send_nack_resp(p_no)
          else:
             self.state = ("APromised", msg.proposal)
             self.send_promise_resp(p_no)
       else:
          self.send_nack_resp(p_no)
    elif isinstance(msg, AcceptRequestMessage):
       if self.state[0] == "AInit":
          self.state = ("AAccepted", msg.proposal)
       else:
          promised_no, _ = self.state[1]
          if p_val >= promised_no:
             self.state = ("AAccepted", msg.proposal)
...
```

Running the simulator and watching it achieve consensus proved that the design of the adapted protocol functioned correctly. Implementing the simulator before encoding the protocol in Disel, not only helped solidify the understanding of the adapted protocol but also helped catch errors in the protocol design early on. This is because, in Disel, we would first have to encode the protocol then implement the client application and then see whether the it functions correctly. Additionally, the simulator can also be used to test the designed inductive invariant. One can write a function that queries the state of each node and prints out a boolean indicating when the inductive invariant is preserved or raise an error otherwise.

4.2 Encoding the protocol in Disel

Having designed the adapted protocol and tested it on a simulator, the next step was to actually encode it in Disel. The most important part was to encode the state transitions of the protocol. In the encoding, we define an inductive type, `RoleState` that stores all the states a node can be in and the data it can hold.

```
(* States of the nodes *)
Inductive RoleState :=
(* proposer States *)
(* Initialised with a proposal (p_no * p_val) *)
| PInit of proposal
(* Sent prepare message to some acceptors at a current stage *)
(* seq nid holds nodes which were sent the message *)
| PSentPrep of seq nid & proposal
(* Received promises/NACKs from acceptors *)
| PWaitPrepResp of promises & proposal
(* Send AcceptRequest *)
| PSentAccReq of seq nid & proposal
(* Finished executing after sending AccReq or not receiving majority*)
| PAbort
(* acceptor states *)
| AInit
(* Holds the highest number promised in the proposal *)
| APromised of proposal
(* Holds the highest number proposal accepted *)
| AAccepted of proposal.
```

The `step` functions were defined next. These functions dictate how the state of a node changes on sending or receiving a message. Below is a code listing from the `step_recv` function which handles the change in state on receiving a message. `s` is the current state of the nodes, `mbody` is the message that is received and `mtag` is the tag of the received message. When the node receives a message in the `APromised` state, it first checks whether it is an prepare request or an accept request. It then checks whether the number of the proposal is greater than the one it has already promised. If it is greater, then the node transitions to `APromised`, but holding a new proposal, or to the `AAccepted` state depending on the type of the incoming message.

```
(* Changes in the Node state triggered upon receive *)
Definition step_recv (s : StateT) (from : nid) (mtag : ttag) (mbody : payload):
  StateT :=
  let: (e, rs) := s in
  let: recv_p_no := head 0 mbody in
  let: recv_p_val := last 0 mbody in
```

```
match rs with
...
| APromised p' ⇒
   let: curr_p_no := head 0 p' in
   let: curr_p_val := last 0 p' in
   if mtag == prepare_req
   then if recv_p_no > curr_p_no (* If received higher number *)
       (* Update promised number by storing new proposal *)
       then (e, APromised mbody)
       else (e, APromised p')
   else (* It's an accept request *)
       if recv_p_no > curr_p_no (* If received higher number *)
       then (e, AAccepted mbody) (* Accept the proposal *)
       else (e, APromised p') (* we'll send nack *)
...
| _ ⇒ s
end.
```

The complete encoding of the adapted protocol can be found in the `PaxosProtocol.v` file.

5
Client Application

As outlined in chapter 2, our approach to using Disel involved first coding the protocol and the client application, and then going on write the proofs. Having the client application working before writing the proofs showed that the design of the adapted protocol worked and could be used to achieve consensus.

In this chapter we look at the implementation of a simple client application that uses the proof of the adapted protocol to create an application where a set of nodes achieve consensus on a value. The chapter first looks at how the client application was designed and encoded in Disel. After which we look into how Disel's `shims` runtime was used to extract the OCaml code for the runnable client application. Then we outline how to extended the client application by writing a wrapper around it. Finally, we look at how the client application was proved in Disel.

5.1 Modelling

The main property that we want to observe from the client is the acceptors achieving consensus on a proposal. This meant we needed to be able to see that a majority of acceptors accepting a protocol and that all of the acceptors in the majority accept the same protocol.

Furthermore, we needed the client application to follow the same state transition system we designed for our adapted protocol. Thus, the correct functioning of the client will give us confidence that our adapted protocol can be proved. This also enables us to catch flaws in our design of the adapted protocol early on and helps us detect things like unnecessary states early on in the process, which makes proving the protocol easier in the later stages.

So our client was simple in that we wanted to initialise two proposers and three acceptors and then see the acceptors achieve consensus. Each proposal that is initialised will only try once to achieve consensus using the proposal number that it is initialised with. If it receives a nack in the process, then it stops and does not retry to achieve consensus with a higher proposal number. As explained in the previous chapter, we choose this 'one shot' process for the proposer in order to focus on just on the part of the protocol where consensus is achieved, i.e. where the proposer accumulates enough promises and then sends out an accept request which then may be accepted by each of the acceptors.

5.2 Encoding client in Disel

Having decided on the design of the client, the next step was to produce a runnable implementation of a proposer and an acceptor which each of the nodes in the protocol can run as programs. Here we will only look at the implementation of the proposer, the implementation of the acceptor follows from that and can be found in the `PaxosAcceptor.v` file.

As a proposer starts off in the `PInit` state, the runnable implementation of a proposer needs to take in a proposal as a parameter which it will use to initialise the proposer with. Below is the main function for the proposer. It first sends out the prepare requests and then starts receiving responses from the acceptors. `check_promises` function checks that none of the responses contain a nack request. If no nacks were received then the proposer sends accept requests to all the acceptors by choosing the value from the highest numbered proposal.

```
Program Definition proposer_round (psal: proposal):
  {(e : nat)}, DHT [p, W]
  (fun i ⇒ loc i = st :→ (e, PInit psal),
   fun res m ⇒ loc m = st :→ (e, PAbort))
  :=
  Do (e <-- read_round;
      send_prepare_req_loop e psal;;
      recv_promises <-- receive_prepare_resp_loop e;
      check <-- check_promises recv_promises;
      if check
      then send_accept_reqs e (choose_highest_numbered_proposal psal recv_promises)
      else send_accept_reqs e [:: 0; 0]).
     (* If check fails then send an acc_req for (0, 0) which will never be
        accepted by any acceptor *)
```

Although, if a nack was received, the proposal still sends accept requests with the proposal $\langle 0, 0 \rangle$. This proposal will never be accepted by any acceptor as its proposal number is not greater than 0. We still need to send these accept requests as both branches of a `if` statement need to have the same type. The distributed Hoare types and the pre and post conditions defined are also show in the code listing. The proposer starts off in the `PInit` state and on finishing the round, ends up in the `PAbort`.

5.3 Extraction

Disel programs can be extracted into their corresponding OCaml definitions. The extracted code contains modules to that define the various node states and transitions. This extracted code can then be used by a shim to create a client application.

In order for the extraction to work, a runnable program needs to be supplied for each of the nodes participating in the protocol. Additionally, each node needs to be given an initial state that satisfied all the imposed invariants.

The `SimplePaxosApp.v` file uses the runnable implementations of the proposer and acceptor and defines the code to instantiate the nodes. The client implementation instantiates two proposers and three acceptors. Each proposer is instantiated with a unique proposal which is required in the `PInit` state (the state in which each proposer starts off in).

Extracting this code using Disel produces the OCaml code that can be used to run each of the nodes. After extracting the code, a shim file (`PaxosMain.ml`) is written that parses the arguments supplied to it and instantiates a program specified for the given node. Compiling the shim file produces the executable (`PaxosMain.d.byte`) which can be supplied with the right arguments to set up execution of one of the nodes participating in the protocol.

The executable was used in a shell script (`paxos.sh`) to instantiate all the different nodes as different processes. Below are the logs produced by one of the proposers (node 2) on running this script. Nodes 3, 4 and 5 are acceptors while node 1 is the other proposer proposing value 1.

```
initial state is: [0 |→ {dstate = [1 |→ [1 |→ <heap>], 3 |→ [1 |→ <heap>],
   4 |→ [1 |→ <heap>], 5 |→ [1 |→ <heap>]]; dsoup = <>}]
World is [0 |→ <protocol with label 0>]
sending msg in protocol 0 with tag = 0, contents = [2; 2] to 3
```

```
World is [0 |→ <protocol with label 0>]
sending msg in protocol 0 with tag = 0, contents = [2; 2] to 4
World is [0 |→ <protocol with label 0>]
sending msg in protocol 0 with tag = 0, contents = [2; 2] to 5
new connection!
done processing new connection from node 3
got msg in protocol 0 with tag = 1, contents = [0; 0] from 3
new connection!
done processing new connection from node 4
got msg in protocol 0 with tag = 1, contents = [0; 0] from 4
new connection!
done processing new connection from node 5
got msg in protocol 0 with tag = 1, contents = [0; 0] from 5
World is [0 |→ <protocol with label 0>]
sending msg in protocol 0 with tag = 3, contents = [2; 2] to 3
World is [0 |→ <protocol with label 0>]
sending msg in protocol 0 with tag = 3, contents = [2; 2] to 4
World is [0 |→ <protocol with label 0>]
sending msg in protocol 0 with tag = 3, contents = [2; 2] to 5
```

The tags identify the messages types. The mapping for the tags is defined in our protocol `PaxosProtocol.v` as follows.

```
Definition prepare_req : nat := 0.
Definition promise_resp : nat := 1.
Definition nack_resp : nat := 2.
Definition accept_req : nat := 3.
```

Thus, the logs show that the proposer first sent out prepare request (`tag = 1`) with the proposal $\langle 2, 2\rangle$ to the three acceptors and received promise responses back from them (`tag = 1`). After this proposer sent out an accept request (`tag = 3`) to each of the acceptors.

5.4 Extending the extracted code

The previous steps helped setup a simple client application but the logs only show what happened at each individual node. Moreover, the important part is to find out when the entire system has achieved consensus, i.e. a majority of acceptors have accepted the same proposal.

One way of making the client do this would be to go back to the Disel code and write the implementation of a learner and define an *accepted* message that will be sent from an acceptor to a learner whenever it accepts a proposal. This learner can then tell us when the entire system has achieved consensus. This method is time consuming because one will have to do all the encoding similar to that for the proposer or acceptor. Although, the final output of this will be a fully verified client where the actions of the learner also adhere to our protocol.

A quicker way to implement the same functionality is to write a wrapper around the extracted code that enables communication with the acceptor. The wrapper can keep checking when each of the acceptors has accepted a proposal and can compare the values in those proposals. Using this the wrapper can 'announce' when the system has achieved consensus. An example wrapper which uses the extracted code is implemented in the `paxos.py` file. Writing such wrappers helps to extend the functionality of the extracted client application and also shows that the client application can be used in other applications where it provides a verified implementation of Paxos.

6
Conclusion and Evaluation

6.1 Summary of Achievements

The project achieved all its goals apart from proving the inductive invariant. The major deliverables were as follows.

1. **The Adapted Protocol**
   We designed the state transition systems for Paxos in order to help encode it in Disel. The state transition systems were also tested on the Python simulator and then encoded in Disel. We also designed the inductive invariant for Paxos that proved its correctness.

2. **Client Application**
   We also created a client application that uses the encoded protocol. The code for the client was extracted using Disel and we successfully wrote wrappers around it as well.

6.2 Critical Evaluation of the project

Firstly, there were also a few places in the project where things were not proved mechanically.

1. **Inductive Invariant**
   We did not mechanise the proof of the designed inductive invariant in Disel. This will enable us to reach the final stage of the previously mentioned Disel workflow, thus, strengthening the proof by completely verifying the adapted protocol.

2. **Learner in Client Application**
   We were successfully able to interface with the extracted code for the client application but writing a wrapper around it. The wrapper basically performed the role of the learner in Paxos and announced when the acceptors had achieved consensus.

> Using the wrapper meant that client application was not fully verified. In order to achieve that, one would have to design and add the state transition system for the learner in the adapted protocol and encode it in Disel.

We were only able to reach the third stage of the Disel workflow by verifying the client application and showing that it follows the adapted protocol and ran out of time to prove the inductive invariant. While this stage does not show that the protocol itself is completely verified, we can still think of it as relatively strong correctness as the protocol is based on the simple Paxos protocol and we have also designed and come up with a proof for its inductive invariant as highlighted in the section 4.1.3. Additionally, simple Paxos already has a proof of correctness provided by Lamport [9].

Furthermore, Although the learner in the client application was not verified, writing the wrapper enabled us to show that it was possible to interface with the code extracted from Disel. This showed that the verified code generated by Disel can be used in other larger application as the verified implementation of a protocol.

The designed adapted protocol and state transition system focused on the 'core' protocol because as previously mentioned, the proof of the 'core' protocol can be used to verify the optimisations. The adapted protocol and state transition system were tested on the Python simulator and the client based on it was also verified. Iterating between the proof of the client and design of the protocol, helped solidify the design and also make it minimal by removing unnecessary state transitions.

6.2.1 Evaluation of Disel

Disel was the critical component of this project and for most purposes, it stacked up very well to meet all the requirements. The experience of encoding in Disel felt very natural. This was because focusing on the 'core' logic of the protocol and then representing it as state transition diagram is quite intuitive. Which then makes encoding it as a `step` function in Disel very easy.

Building the client application showed that one can successfully extract the OCaml code for the verified protocol. Moreover, writing wrappers around the code showed that extracted code can be used as a verified library in other larger applications.

There were numerous instances where, while doing the proofs in Disel ended up revealing flaws in the implementation. One of these situations was when we found a mistake in our proposer implementation within `send_accept_reqs`. Initially, to check whether we received a promise from every single acceptor, we had the condition, `map fst' recv_promises == acceptors`. The problem with this was that it required the promises to be received in the same order from the acceptors with which the acceptors were ordered in the `acceptors` set. We cannot impose such ordering on the messages received, so we had to replace the condition with `perm_eq (map fst' recv_promises) acceptors` that correctly checks whether a promise had been received from every acceptor by checking that the set of acceptors who responded (`map fst' recv_promises`) is a valid permutation of the set of acceptors.

Furthermore, we also found a bug in our acceptor implementation. We came across it when we were not able to prove the post condition of `acceptor_round` as the acceptor was never reaching the `AAccepted` state.

The reason for this was because we when an acceptor receives an `accept_request` we checked if the incoming proposal had a proposal number greater than the one currently held by the proposal, and only then move to the AAccepted state. The fact that we were reading the state of the acceptor after receiving the incoming message meant that by then the acceptor had already transition its state accordingly when it received it and so the proposal number held by it was always equal to the incoming messages proposal. This meant that the acceptor would not send a promise response.

There were also instances where doing the proofs required the pre or post conditions of the transition to be strengthened by case analysing on the the message being sent or received. One example, in the post condition of `resp_to_prepare_req`, is as follows. Initially, the post condition stated that after responding to a `prepare_req`, the acceptor would either go the `APromised` state either holding the proposal it already had or the new proposal it received. The strengthened looks at the received message and checks if the incoming proposal has proposal number greater that the one it has already promised, only then does it transition to the `APromised` state holding the new incoming proposal.

```
(* Initial weaker post condition *)
fun (_ : seq nat) m ⇒ loc m = st :⟶ (e, APromised p_current)
   ∨loc m = st :⟶ (e, APromised p_incoming))

(* Final stronger post condition *)
fun (_ : seq nat) m ⇒
```

```
    if head 0 p_incoming > head 0 p_current
    then loc m = st :-> (e, APromised p_incoming)
    else loc m = st :-> (e, APromised p_current))
```

Catching these bugs shows how useful it is to do the proofs in Disel as they would not have been easily noticed otherwise. There obviously is the drawback that implementation time is increased as one needs to prove every single transition. Furthermore, when the inductive invariant is added, all the transitions need to be show to adhere to it, thus, requiring more time to implement the proofs.

6.3 Future Work

First steps would definitely be to finish mechanising the left out things pointed in the previous section. This will help us reach the final stage in the Disel workflow. After that, it would be possible to try proving the optimisations in Paxos based on the proof of the 'core' protocol. It would also then be possible to use 'Hooks' [12] in Disel to compose the proof with proofs of other verified components.

There are also a few areas for future work in Disel. Finding the inductive invariant for the protocol is much harder task than designing the state transition system. The Disel paper [12] mentioned the prospect of combining Disel with Ivy [16], which would offer assistance in finding the inductive invariant. Another thing, also mentioned in the Disel paper, is the absence of proving the liveness properties in Disel. Hence, the proof of Paxos which we implemented also does not account for liveness whereas tools like IronFleet [14] enable one to also prove liveness. Finally, another aspect of Paxos which we did not look at was its fault tolerance properties. There could be ways to encode it in as a part of the protocol but maybe it might also be possible for Disel to provide an abstraction which can be used to prove the fault tolerance properties of any arbitary protocol.

Bibliography

[1] "Fault tolerance in a high volume, distributed system," https://medium.com/netflix-techblog/fault-tolerance-in-a-high-volume-distributed-system-91ab4faae74a, [Online; accessed 04-April-2018].

[2] F. B. Schneider, "Implementing fault-tolerant services using the state machine approach: A tutorial," *ACM Computing Surveys*, vol. 22, no. 4, pp. 299–319, 1990.

[3] L. Lamport, "The implementation of reliable distributed multiprocess systems," *Computer Networks*, vol. 2, pp. 95–114, 1978.

[4] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[5] G. Pirlea and I. Sergey, "Mechanising blockchain consensus," *Proceedings of 7th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP'18)*, 2018.

[6] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," *Proceedings of USENIX ATC '14: 2014 USENIX Annual Technical Conference*, 2014.

[7] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," https://www.stellar.org/papers/stellar-consensus-protocol.pdf, 2016, [Online; accessed 04-April-2018].

[8] R. V. Renesse and D. Altinbuken, "Paxos made moderately complex," *ACM Computing Surveys*, vol. 47, no. 3, 2015.

[9] L. Lamport, "The part-time parliament," *ACM Transactions on Computer Systems*, pp. 133–169, 1998.

[10] T. Chandra, R. Griesemer, and J. Redstone, "Paxos made live - an engineering perspective," *PODC '07: 26th ACM Symposium on Principles of Distributed Computing*, 2007.

[11] M. Castro and B. Liskov, "Practical byzantine fault tolerance," *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, 1999.

[12] I. Sergey, J. R. Wilcox, and Z. Tatlock, "Programming and proving with distributed protocols," *ACM on Programming Languages*, vol. 2, no. POPL, 2018.

[13] A. Chlipala, "Formal reasoning about programs," http://adam.chlipala.net/frap/frap_book.pdf, [Online; accessed 04-April-2018].

[14] C. Hawblitzel, J. Howell, M. Kapritsos, J. R. Lorch, B. Parno, M. L. Roberts, S. Setty, and B. Zill, "Ironfleet: Proving practical distributed systems correct," *Proceedings of the ACM on Programming Languages*, vol. 2, no. POPL, 2018.

[15] J. R. Wilcox, D. Woos, P. Panchekha, Z. Tatlock, X. Wang, M. D. Ernst, and T. E. Anderson, "Verdi: a framework for implementing and formally verifying distributed systems," *PLDI. ACM*, pp. 357–368, 2015.

[16] O. Padon, K. L. McMillan, A. Panda, M. Sagiv, and S. Shoham, "Ivy: safety verification by interactive generalization," *PLDI. ACM*, pp. 614–630, 2016.

[17] C. Dragoi, T. A. Henzinger, and D. Zufferey, "Psync: a partially synchronous language for fault-tolerant distributed algorithms," *POPL. ACM*, pp. 400–415, 2016.

[18] V. Rahli, D. Guaspari, M. Bickford, and R. L. Constable, "Formal specification, verification, and implementation of fault-tolerant systems using eventml," *AVOCS. EASST*, pp. 400–415, 2015.

[19] A. Garcıa-Perez, A. Gotsman, Y. Meshman, and I. Sergey, "Paxos consensus, deconstructed and abstracted," http://ilyasergey.net/papers/paxos-deconstructed-esop18-extended.pdf, 2018, [Online; accessed 03-April-2018].

A
Project Plan

A.1 Aims

To learn about the family of Paxos-like consensus protocols and then to formulate a proof of their correctness by implementing a library of reusable verified distributed components using Disel. Disel is a framework for compositional verification of distributed protocols, built on top of Coq proof assistant, to verify correctness of the implemented components. Hence, this project will help me learn about the workings of distributed protocols and how to reason about their correctness.

A.2 Objectives

1. Read about and understand the classical Paxos-like consensus algorithms. Develop state transition systems for the algorithms and identify the invariants that need to be preserved during the operation of the algorithm.

2. Implement a simulation of the protocols in Python.

3. Formulate the implemented protocols in Disel by using the developed state-transition systems.

4. Mechanise the proofs of the identified protocol invariants in Disel/Coq.

5. Add additional communication channels and prove composite invariants.

6. Provide an abstract specification of the protocol, usable by third-party clients.

7. Mechanise a client application of the protocol verified out of the abstract interface.

A.3 Expected Deliverables

- Descriptions of the state-transition system and invariants of the Paxos-like Consensus protocols.
- Python implementation of simulations of the Paxos-like Consensus protocols.
- Proofs of correctness of the implemented protocols in Disel. Thereby, providing a library of reusable verified distributed components written in Disel/Coq.

A.4 Work Plan

- Project start to end October (4 weeks).
  - Read about and understand the workings of Paxos-like Consensus protocols.
  - Implement the protocols in Python.
- November start to mid-December (6 weeks).
  - Create state transition diagrams and identify invariants of the protocols.
  - Formulate the protocols in Disel.
  - Prove correctness of the identified protocol invariants in Disel/Coq.
- Mid-December (8 weeks) to mid February.
  - Iterate on the Disel proof to make it more concise.
  - Formulate the abstract interface.
  - Verify a simple client application.
- January start to March end (12 weeks).
  - Submit Interim Report (due in late January).
  - Work on Final Report.

B
Interim Report

B.1 Current Status

Having studied the Paxos protocol in detail, we adapted the protocol for implementing it in Disel. We decided to focus on single decree paxos and to do away with the learner for the first version of the proof in order to prove the part of the protocol where consensus is achieved.

We developed the state transition system for the nodes in the protocol. In Paxos each node can have different roles but we had to split up each role into different states depending on the current data held by the node and the current function of the node in the protocol. We decided on the states each node could be in and how and when it transitions between them. This helped us come up with precondition and postcondition for the state of each node when it transitions on receiving or sending a message. We tried to minimise the number of transitions and the data held in each node's state in order to simplify the proof in Disel.

We also had to come up with an inductive invariant for the protocol such that if the inductive invariant holds in some state then in holds in every state reachable from that state. The inductive invariant was critical as it helped ensure that the protocol functions correctly by imposing requirements on the global state of the system. For proving the correctness of paxos we found that our invariant had to capture when consensus is achieved on a value and also that once consensus is achieved on a particular value, further rounds of the protocol don't change this value. We then also came up with a proof for how this inductive invariant holds in our adapted protocol.

I have also implemented a simulator for Paxos in Python which is modeled according to how Disel works. The simulator is based on a state-transition system like Disel and uses separate processes to simulate different nodes in the distributed system. In the simulator, I implemented our adapted Paxos algorithm, with the state transitions we had decided to use with Disel. The working of the simulator gave us confidence that our state transition system for Paxos will work correctly in Disel.

After studying the Disel paper and looking at similar examples, I implemented the core of the adapted protocol in Disel. I also implemented a client application in Disel. The pre and post conditions from the state transition system helped me to implement the client application in such a way to adhere with the main protocol. Using the extraction feature in Disel and the shims runtime, I successfully extracted a working program of the client application in OCaml.

B.2 Remaining Work

Although, I have implemented the protocol in Disel, I still need to prove that the 'coherence' (the constraints imposed on the local state of each node and the messages exchanged) holds in the protocol. I will need to learn Coq and SSReflect in more detail to be able to finish the proofs and to understand the proofs of other protocols in Disel.

For the client implementation, I still need to prove how the implemented node roles satisfy the pre and post conditions, imposed on the state of the node, by the protocol.

I also need to mechanise the proof of our inductive invariant in Disel and prove how the pre and post conditions of each node hold with respect to the inductive invariant when the node undergoes a state transition on receiving or sending a message.

I aim to finish mechanising the proofs by the end of term (23 March) and also to get most of the project report finished by them, especially the initial sections.

C

Disel Proof Code Listing

C.1 PaxosProtocol.v

```
From mathcomp.ssreflect
Require Import ssreflect ssrbool ssrnat eqtype ssrfun seq.
From mathcomp
Require Import path.
Require Import Eqdep.
Require Import Relation_Operators.
From DiSeL.Heaps
Require Import pred prelude idynamic ordtype finmap pcm unionmap heap coding domain.
From DiSeL.Core
Require Import Freshness State EqTypeX DepMaps Protocols Worlds NetworkSem Rely.
From DiSeL.Core
Require Import Actions Injection Process Always HoareTriples InferenceRules.

Set Implicit Arguments.
Unset Strict Implicit.
Import Prenex Implicits.


Module PaxosProtocol.


Module States.


Definition nid := nat.

(* seq of two elements p_no, p_val *)
Definition proposal := seq nat.
(* Promise -> seq (node * promise/nack * accepted_proposal) *)
Definition promises := seq (nid * bool * proposal).

(* States of the nodes *)
Inductive RoleState :=
(* Proposer States *)
(* Initialised with a proposal (p_no * p_val) *)
| PInit of proposal
(* Sent prepare message to some Acceptors at a current stage *)
(* seq nid holds nodes which were sent the message *)
| PSentPrep of seq nid & proposal
(* Received promises/NACKs from Acceptors *)
| PWaitPrepResp of promises & proposal
(* Send AcceptRequest *)
| PSentAccReq of seq nid & proposal
(* Finished executing after sending AccReq or not receiving majority*)
| PAbort
(* Acceptor states *)
| AInit
(* Holds the highest number promised in the proposal *)
| APromised of proposal
(* Holds the highest number proposal accepted *)
| AAccepted of proposal.

(* Pointer to the state *)
Definition st := ptr_nat 1.

(* Pairing with the current stage of type nat *)
Definition StateT := (nat * RoleState)%type.


End States.

Import States.

Section PaxosProtocol.

(* Proposer nodes *)
Variable proposers : seq nid.
(* Acceptor nodes *)
Variable acceptors : seq nid.
(* Involved nodes *)
Definition nodes := proposers ++ acceptors.


Definition prepare_req : nat := 0.
Definition promise_resp : nat := 1.
Definition nack_resp : nat := 2.
Definition accept_req : nat := 3.


Definition ttag := nat.

Definition tags : seq ttag :=
  [:: prepare_req; promise_resp; nack_resp; accept_req].
```

```
(*** Defining Coherence ***)

(**
Coherence predicate defines the shape of the statelet.
i.e. it components of the local state and message soup properties.
Therefore, we need to write coherence functions for both the
local state and message soup and then combine them to create PaxosCoh.
 *)


(** localCoh constraints the local state of each node. **)
Definition localCoh (n : nid) : Pred heap :=
  [Pred h | valid h ∧∃ (s : StateT), h = st :→ s].

Definition tagFromNode (t : nat) : bool :=
  (t \in [:: prepare_req; accept_req; promise_resp; nack_resp]).

Definition msgFromNode (tms : TaggedMessage) (y : nat) : Prop :=
  let: body := tms_cont tms in ∃ data, body = y :: data.

Definition cohMsg (ms: msg TaggedMessage) (y : nat) : Prop := True.

(** Coherence for the message soup. *)
Definition soupCoh : Pred soup :=
  [Pred s | valid s ∧
         ∀ m ms, find m s = Some ms → ∃ y, cohMsg ms y].

Definition paxos_coh d : Prop :=
  let: dl := dstate d in
  let: ds := dsoup d in
  [∧ soupCoh ds, dom dl =i nodes,
   valid dl &
   ∀ n, n \in nodes → localCoh n (getLocal n d)].

(* Axioms of the coherence predicate *)
Lemma l1 d: paxos_coh d → valid (dstate d).
Proof. by case. Qed.

Lemma l2 d: paxos_coh d → valid (dsoup d).
Proof. by case; case. Qed.

Lemma l3 d: paxos_coh d → dom (dstate d) =i nodes.
Proof. by case. Qed.

(* Wrapping up the coherence predicate *)
Definition PaxosCoh := CohPred (CohPredMixin l1 l2 l3).

Lemma send_soupCoh d m :
   soupCoh (dsoup d) → (∃ y, cohMsg m y) → soupCoh (post_msg (dsoup d) m).1.
Proof.
  move⇒[H1 H2][y]Cm; split⇒[|i ms/=]; first by rewrite valid_fresh.
  rewrite findUnL; last by rewrite valid_fresh.
  case: ifP⇒E; first by move/H2.
   by move/um_findPt_inv⇒[Z G]; subst i m; ∃ y.
Qed.

Lemma trans_updDom this d s :
  this \in nodes → PaxosCoh d → dom (upd this s (dstate d)) =i nodes.
Proof.
  move⇒D C z; rewrite -(cohDom C) domU inE/=.
   by case: ifP⇒///eqP→{z}; rewrite (cohDom C) D; apply: cohVl C.
Qed.

Lemma cohSt n d (C : PaxosCoh d) s:
  find st (getLocal n d) = Some s →
  idyn_tp s = StateT.
Proof.
case: (C)⇒ _ _ _ G; case H: (n \in nodes).
- by move: (G _ H); case⇒V'[s']→; rewrite hfindPt//=; case⇒<-.
rewrite /getLocal; rewrite -(cohDom C) in H.
by case: dom_find H⇒//→; rewrite find0E.
Qed.

Definition getSt n d (C : PaxosCoh d) : StateT :=
  match find st (getLocal n d) as f return _ = f → _ with
  | Some v ⇒ fun epf ⇒ icoerce id (idyn_val v) (cohSt C epf)
  | _ ⇒ fun epf ⇒ (0, AInit)
  end (erefl _).

Lemma locCn n d (C : PaxosCoh d):
  n \in nodes →
  valid (getLocal n d) ∧
  ∃ (s : StateT), getLocal n d = st :→ s.
Proof.
by case: C⇒_ _ _ /(_ n)G; move: G; rewrite /localCoh/=.
Qed.

Lemma getStK n d (C : PaxosCoh d) s :
  getLocal n d = st :→ s → getSt n C = s.
Proof.
move⇒E; rewrite /getSt/=.
move: (cohSt C); rewrite !E/==⇒H.
by apply: ieqc.
Qed.

Lemma getStE n i j C C' (pf : n \in nodes) :
  getLocal n j = getLocal n i → @getSt n j C' = @getSt n i C.
Proof.
case: {-1}(C)⇒_ _ _/(_ _ pf).
move⇒[V][s][E]E'.
rewrite (getStK C E).
by apply: getStK; rewrite E'.
Qed.

Lemma getStE' l i j pf pf' n:
  getLocal n (getStatelet j l) = getLocal n (getStatelet i l) →
  @getSt n (getStatelet j l) pf' = @getSt n (getStatelet i l) pf.
Proof.
Admitted.

(*** State Transitions ***)
Definition fst' (tup: (nat * bool * proposal)%type): nat :=
  match tup with
  | (x, b, props) ⇒ x
  end.

Definition snd' (tup: (nat * bool * proposal)%type): bool :=
  match tup with
  | (x, b, props) ⇒ b
  end.

Fixpoint find_highest_numbered_promise (max_so_far: proposal) (xs: promises):
  proposal :=
  match xs with
  | cons (_, check, p) rest ⇒
    if check && (head 0 p > head 0 max_so_far)
    then find_highest_numbered_promise p rest
    else find_highest_numbered_promise max_so_far rest
  | _ ⇒ max_so_far
 end.

(* Choose value of highest numbered proposal received from acceptors *)
Fixpoint create_proposal_for_acc_req (xs: promises) (p: proposal): proposal :=
  (* All promises received *)
  if (all (fun i ⇒ i) (map snd' xs))
  then
    let: max_proposal := find_highest_numbered_promise [:: 0; 0] xs in
    if perm_eq max_proposal [:: 0; 0]
    then p
    else [:: (head 0 p); (last 0 max_proposal)]
  else [:: 0; 0].

(**
Step Functions

Step function dictactes how the state of the node changes
after performing the send/receive transitions.
*)

(**
Send Transitions:
- Proposer: sPrep, sAccReq
- Acceptor: sPromise, sNack
*)

(* Changes in the Node state triggered upon send *)
Definition step_send (s: StateT) (to : nid) (p: proposal): StateT :=
   let: (e, rs) := s in
   match rs with
   | PInit p' ⇒
     if acceptors == [:: to] (* if only one acceptor *)
     then (e, PWaitPrepResp [::] p')
     else (e, PSentPrep [:: to] p')
   | PSentPrep tos p' ⇒
     if perm_eq (to :: tos) acceptors
     (* If all prepare reqs sent *)
     then (e, PWaitPrepResp [::] p') (* switch to the receiving state *)
     else (e, PSentPrep (to :: tos) p') (* Keep sending *)
   | PSentAccReq tos p' ⇒
     if perm_eq (to :: tos) acceptors
     (* If all accept reqs sent *)
     then (e, PAbort)
     else (e, PSentAccReq (to :: tos) p') (* Keep sending *)
   | _ ⇒ (e, rs)
   end.

(**
Receive Transitions:
- Proposer: rPromise, rNack
- Acceptor: rPrep, rAccReq
 *)

Definition payload := proposal.

(* Changes in the Node state triggered upon receive *)
Definition step_recv (s : StateT) (from : nid) (mtag : ttag) (mbody : payload):
  StateT :=
  let: (e, rs) := s in
  let: p_no := head 0 mbody in
  let: p_val := last 0 mbody in
  match rs with
  | PWaitPrepResp recv_promises p' ⇒
    if (from \in (map fst' recv_promises)) (* If duplicate *)
    then s (* then ignore *)
   else if mtag == nack_resp
       then (e, PAbort) (* Abort if we see nack *)
       else
        let: r_promises := (from, mtag == promise_resp, mbody) :: recv_promises in
        (* if all promises received, we know we don't have nacks *)
        if (perm_eq (map fst' r_promises) acceptors)
        then let: new_p := create_proposal_for_acc_req r_promises p' in
            (e, PSentAccReq [::] new_p)
        else (e, PWaitPrepResp r_promises p') (* keep waiting for promises *)
  | AInit ⇒ (* Promise/Accept first received transition *)
   if mtag == prepare_req
   then (e, APromised mbody)
   else (e, AAccepted mbody)
  | APromised p' ⇒
     let: curr_p_no := head 0 p' in
     let: curr_p_val := last 0 p' in
     if mtag == prepare_req
     then if p_no > curr_p_no (* If received higher number *)
        (* Update promised number by storing new proposal *)
        then (e, APromised mbody)
        else (e, APromised p')
     else (* It's an accept request *)
        if p_no > curr_p_no (* If received higher number *)
        then (e, AAccepted mbody) (* Accept the proposal *)
        else (e, APromised p') (* we'll send nack *)
  | _ ⇒ s
 end.

(*
There should be 4 send-transitions for the node:
- send-prepare-request
- send-accept-request
- send-promise
- send-nack

There should be 4 receive-transitions for the node:
- receive-promise
- receive-nack
- receive-prepare-request
- receive-accept-request
 *)

Section GenericSendTransitions.

Notation coh := PaxosCoh.

Definition Hin this to := (this \in nodes ∧to \in nodes).
Definition mkLocal {T} (sl : T) := st :→ sl.
Check mkLocal.

Variable ptag : ttag.

(* Precondition -- this is the way one can define multiple send-transitions *)
Variable prec : StateT → payload → Prop.

Hypothesis node_prec_safe :
  ∀ this to s m,
   Hin this to → prec s m → cohMsg (Msg (TMsg ptag m) this to true) s.1.

(* Making sure that the precondition is legit *)
Lemma this_in this to : Hin this to → this \in nodes.
Proof.
 by case.
Qed.
```

```
Definition node_safe (this n : nid)
        (d : dstatelet) (msg : payload) :=
 Hin this n ∧
 ∃ (Hp : Hin this n) (C : coh d), prec (getSt this C) msg.

Lemma node_safe_coh this to d m : node_safe this to d m ⟶ coh d.
Proof.
 case.
 move ⇒ in_nodes.
 case.
 move ⇒ in_nodes2.
 case ⇒ coh_d H_coh_d ⇒ //.
Qed.

Lemma node_safe_in this to d m : node_safe this to d m ⟶
                       this \in nodes ∧to \in nodes.
Proof.
 case.
 move ⇒ Hin e_clause ⇒ //.
Qed.

Definition node_step (this to : nid) (d : dstatelet)
        (msg : payload)
        (pf : node_safe this to d msg) :=
 let C := node_safe_coh pf in
 let s := getSt this C in
 Some (mkLocal (step_send s to msg)).

Lemma node_step_coh : s_step_coh_t coh ptag node_step.
Proof.
 move⇒this to d msg pf h[]⟶{h}.
 have C : (coh d) by case: pf⇒?[?][].
 split⇒/=.
 - apply: send_soupCoh; first by case:(node_safe_coh pf).
   ∃ (getSt this C).1.
   case: (pf)⇒ H[C']P /=. move: (conj H P)⇒pf'.
   move: P.
   case ⇒ H2 P.
   move: (node_prec_safe H P). rewrite (proof_irrelevance C H2)/=. done.
 - by apply: trans_updDom⇒//; case: (node_safe_in pf).
 - by rewrite validU; apply: cohVl C.
 move⇒n Ni. rewrite /localCoh/=.
 rewrite /getLocal/=findU; case: ifP⇒B; last by case: C⇒_ _ _/(_ n Ni).
 move/eqP: B⇒Z; subst n⇒/=.
 rewrite (cohVl C)/=; split⇒//.
 move: (step_send _ _ _)⇒ps.
 rewrite ?hvalidPtUn//; last by e∃ _.
Qed.

Lemma node_safe_def this to d msg :
    node_safe this to d msg <⟶
    ∃ b pf, @node_step this to d msg pf = Some b.
Proof.
 split⇒[pf/=|]; last by case⇒?[].
 set b := let C := node_safe_coh pf in
       let s := getSt this C in
       mkLocal (step_send s to msg).
 by ∃ b, pf.
Qed.

Definition node_send_trans :=
 SendTrans node_safe_coh node_safe_in node_safe_def node_step_coh.

End GenericSendTransitions.
```

```
Section SendTransitions.

(* Send prepare request transition *)
Definition send_prepare_req_prec (p: StateT) (m: payload) :=
 (∃ n psal, p = (n, PInit psal)) ∨
 (∃ n tos psal, p = (n, PSentPrep tos psal)).

Program Definition send_prepare_req_trans : send_trans PaxosCoh :=
 @node_send_trans prepare_req send_prepare_req_prec _.
Next Obligation.
 by rewrite /cohMsg.
Qed.

(* Send accept request transition *)
Definition send_accept_req_prec (p: StateT) (m: payload) :=
 (∃ n psal, p = (n, PSentAccReq [::] psal)).

Program Definition send_accept_req_trans : send_trans PaxosCoh :=
 @node_send_trans accept_req send_accept_req_prec _.
Next Obligation.
 by rewrite /cohMsg.
Qed.

(* Send promise response transition *)
Definition send_promise_resp_prec (p: StateT) (m: payload) :=
 (∃ n, p = (n, AInit)) ∨(∃ n psal, p = (n, APromised psal)).

Program Definition send_promise_resp_trans : send_trans PaxosCoh :=
 @node_send_trans promise_resp send_promise_resp_prec _.
Next Obligation.
 by rewrite /cohMsg.
Qed.

(* Send nack response transition *)
Definition send_nack_resp_prec (p: StateT) (m: payload) :=
 ∃ n psal, p = (n, APromised psal).

Program Definition send_nack_resp_trans : send_trans PaxosCoh :=
 @node_send_trans nack_resp send_nack_resp_prec _.
Next Obligation.
 by rewrite /cohMsg.
Qed.

End SendTransitions.

Section GenericReceiveTransitions.

Notation coh := PaxosCoh.

Variable r_tag : ttag.
Variable r_wf : ∀ d, coh d ⟶ nid ⟶ nid ⟶ pred payload.

Definition r_step : receive_step_t coh :=
 fun this (from : nid) (m : proposal) d (pf : coh d) (pt : this \in nodes) ⇒
   let s := getSt this pf in
   mkLocal (step_recv s from r_tag m).

Lemma r_step_coh : r_step_coh_t r_wf r_tag r_step.
Proof.
 move⇒d from this m C pf tms D F Wf T/=.
 rewrite /r_step; case X: (this \in nodes); last first.
 admit.
Admitted.

Definition recv_trans := ReceiveTrans r_step_coh.
```

```
End GenericReceiveTransitions.

Section ReceiveTransitions.

Definition msg_wf d (_ : PaxosCoh d) (this from : nid) :=
  [pred p : payload | true].

(* Got prepare request *)
Definition receive_prepare_req_trans := recv_trans prepare_req msg_wf.

(* Got accept request *)
Definition receive_accept_req_trans := recv_trans accept_req msg_wf.

(* Got promise response *)
Definition receive_promise_resp_trans := recv_trans promise_resp msg_wf.

(* Got nack response *)
Definition receive_nack_resp_trans := recv_trans nack_resp msg_wf.

End ReceiveTransitions.


Section Protocol.

(* Putting it all together *)
Variable l : Label.

(* All send-transitions *)
Definition paxos_sends :=
  [::
    send_prepare_req_trans;
    send_accept_req_trans;
    send_promise_resp_trans;
    send_nack_resp_trans
  ].

(* All receive-transitions *)
Definition paxos_receives :=
  [::
    receive_prepare_req_trans;
    receive_accept_req_trans;
    receive_promise_resp_trans;
    receive_nack_resp_trans
  ].

Program Definition PaxosProtocol : protocol :=
  @Protocol _ l _ paxos_sends paxos_receives _ _.

End Protocol.
End PaxosProtocol.

Module Exports.
Section Exports.

Definition PaxosProtocol := PaxosProtocol.

Definition send_prepare_req_trans := send_prepare_req_trans.
Definition send_accept_req_trans := send_accept_req_trans.
Definition send_promise_resp_trans := send_promise_resp_trans.
Definition send_nack_resp_trans := send_nack_resp_trans.

Definition receive_prepare_req_trans := receive_prepare_req_trans.
Definition receive_accept_req_trans := receive_accept_req_trans.
Definition receive_promise_resp_trans := receive_promise_resp_trans.
Definition receive_nack_resp_trans := receive_nack_resp_trans.

(* Paxos Tags *)
Definition prepare_req := prepare_req.
Definition accept_req := accept_req.
Definition promise_resp := promise_resp.
Definition nack_resp := nack_resp.

(* Getter *)
Definition getSt := getSt.

End Exports.
End Exports.

End PaxosProtocol.

Export PaxosProtocol.States.
Export PaxosProtocol.Exports.
```

C.2 PaxosProposer.v

```
From mathcomp.ssreflect
Require Import ssreflect ssrbool ssrnat eqtype ssrfun seq.
From mathcomp
Require Import path.
Require Import Eqdep.
Require Import Relation_Operators.
From DiSeL.Heaps
Require Import pred prelude idynamic ordtype finmap pcm unionmap heap coding domain.
From DiSeL.Core
Require Import Freshness State EqTypeX DepMaps Protocols Worlds NetworkSem Rely.
From DiSeL.Core
Require Import Actions Injection Process Always HoareTriples InferenceRules.
From DiSeL.Core
Require Import InductiveInv While.
From DiSeL.Examples
Require Import PaxosProtocol.


Module PaxosProposer.
Section PaxosProposer.

Variable l : Label.
Variables (proposers: seq nid) (acceptors: seq nid).
Variable p: nid.

Hypothesis AcceptorsNonEmpty : acceptors != [::].

Check PaxosProtocol.

Definition paxos := PaxosProtocol proposers acceptors l.
Notation W := (mkWorld paxos).

Section ProposerImplementation.

(************** Atomic actions **************)

(* Two send-actions, e -- id of the current era *)
Program Definition send_prepare_req psal to :=
 act (@send_action_wrapper W paxos p l (prEq paxos)
     (send_prepare_req_trans proposers acceptors) _ psal to).
Next Obligation.
 by rewrite InE; do![left|right].
Qed.

Program Definition send_accept_req psal to :=
 act (@send_action_wrapper W paxos p l (prEq paxos)
     (send_accept_req_trans proposers acceptors) _ psal to).
Next Obligation.
 by rewrite !InE; right; left.
Qed.


(* Two receive-actions *)
Program Definition tryrecv_prepare_resp := act (@tryrecv_action_wrapper W p
     (* filter *)
     (fun k _ t b ⇒ (k == l) && ((t == promise_resp) || (t == nack_resp))) _).
Next Obligation.
 by case/andP: H⇒/eqP⟶_; rewrite /ddom gen_domPt inE/=.
Qed.
```

```
(************** Proposer code **************)

(*** Reading internal state ***)
Implicit Arguments PaxosProtocol.PaxosCoh [proposers acceptors].
Notation coh := (@PaxosProtocol.PaxosCoh proposers acceptors).
Notation getS s := (getStatelet s l).
Notation loc i := (getLocal p (getStatelet i l)).

Export PaxosProtocol.

Program Definition read_round:
 {(s: StateT)}, DHT [p, W]
 (fun i ⇒ loc i = st :⟶ s,
  fun r m ⇒ loc m = st :⟶ s ∧
          ∃ (pf : coh (getS m)), r = (getSt p pf).1) :=
 Do (act (@skip_action_wrapper W p l paxos (prEq paxos) _
                        (fun s pf ⇒ (getSt p pf).1))).
Next Obligation.
 apply: ghC.
 move ⇒ s st s_is_st s_in_coh_w.
 apply: act_rule ⇒ j R.
 split ⇒ [|r k m].
   by case: (rely_coh R).
 case⇒/=H1[Cj]Z.
 subst j⇒⟶R'.
 split; first by rewrite (rely_loc' l R') (rely_loc' _ R).
 case: (rely_coh R')⇒_; case⇒_ _ _ _/(_ l)⇒/= pf; rewrite prEq in pf.
 ∃ pf; move: (rely_loc' l R') ⇒/sym E'.
 suff X: getSt p (Actions.safe_local (prEq paxos) H1) = getSt p pf by rewrite X.
 by apply: (getStE' pf _ E').
Qed.

(*******************************************)
(*** Sending out proposals in a loop ***)
(*******************************************)

Definition send_prepare_req_loop_spec (e : nat) := ∀ to_send,
 {(pinit: proposal)}, DHT [p, W]
 (fun i ⇒
    loc i = st :⟶ (e, PInit pinit) ∧
    (perm_eq acceptors to_send ∨
    if to_send == [::]
    then loc i = st :⟶ (e, PWaitPrepResp [::] pinit)
    else ∃ (acptrs : seq nid),
       loc i = st :⟶ (e, PSentPrep acptrs pinit) ∧
       perm_eq acceptors (acptrs ⧺ to_send)),
    fun r m ⇒ r = tt ∧loc m = st :⟶ (e, PWaitPrepResp [::] pinit)).

Program Definition send_prepare_req_loop e (psal: proposal):
 {(pinit: proposal)}, DHT [p, W]
 (fun i ⇒ loc i = st :⟶ (e, PInit pinit),
  fun r m ⇒ r = tt ∧
          loc m = st :⟶ (e, PWaitPrepResp [::] pinit)) :=
 Do (ffix (fun (rec : send_prepare_req_loop_spec e) to_send ⇒
          Do (match to_send with
             | to :: tos ⇒ send_prepare_req psal to ;; rec tos
             | [::] ⇒ ret _ _ tt
             end)) acceptors).
Next Obligation.
 apply: ghC ⇒ i1 p'.
 case⇒[[E1 P1 C1]].
```

```
  case: (to_send)⇒[|x xs]; last first.
  apply: step; apply: act_rule ⇒ j1 R1/=; split⇒[|r k m[Sf]St R2].
  split⇒//=; first by case: (rely_coh R1).
  rewrite /node_safe.
  split.
  split.
  admit. (* what does p \in nodes proposers acceptors mean? *)
  admit.
  split.
  admit. (* again Hin *)
  rewrite /send_prepare_req_prec.
  admit. (* Where do I get coherence from *)
  (* because of inE *)
  (* + rewrite /Actions.can_send /nodes inE eqxx andbC/=. *)
  (* by rewrite -(cohD (proj2 (rely_coh R1)))/ddom gen_domPt inE/=. *)
  admit.
  by rewrite /Actions.filter_hooks um_filt0⇒???/sym/find_some; rewrite dom0 inE.
  admit.
  admit.
Admitted.
Next Obligation.
  apply:ghC⇒i lg E1 _; apply: (gh_ex (g:=lg)).
  apply: call_rule⇒C1. split ⇒ //. by left. done.
Qed.

(*******************************************)
(*** Receiving responses to the proposal ***)
(*******************************************)

(* Ending condition *)
Definition rc_prepare_resp_cond (recv_promises : promises) :=
  ~~ perm_eq (map fst' recv_promises) acceptors.

(* Invariant relates the argument and the shape of the state *)
Definition rc_prepare_resp_inv (e : nat) (psal: proposal): cont (promises) :=
  fun acc i ⇒ loc i = st :→ (e, PWaitPrepResp acc psal).

Program Definition receive_prepare_resp_loop (e : nat):
  {(pinit : proposal)}, DHT [p, W]
  (fun i ⇒ loc i = st :→ (e, PWaitPrepResp [::] pinit),
   fun res m ⇒
      loc m = st :→ (e, PWaitPrepResp res pinit) ∧
      (perm_eq (map fst' res) acceptors))
  :=
  Do _ (@while p W _ _ rc_prepare_resp_cond (rc_prepare_resp_inv e) _
      (fun recv_promises ⇒ Do _ (
        r <-- tryrecv_prepare_resp;
        match r with
        | Some (from, tg, body) ⇒
          if (from \in acceptors) && (from \notin (map fst' recv_promises))
          then ret _ _ ((from, tg == promise_resp, body) :: recv_promises)
          else ret _ _ recv_promises
        | None ⇒ ret _ _ recv_promises
        end
      )) [::]).
Next Obligation.
  by apply: with_spec x.
Defined.
Next Obligation.
  by move:H; rewrite /rc_prepare_resp_inv (rely_loc' _ H0).
Qed.
Next Obligation.
  move ⇒ i [psal] /= [H1 I1].
  apply: step.
  apply: act_rule⇒j R1/=; split; first by case: (rely_coh R1).
```

```
  case⇒[[[from tg] body] k m|k m]; last first.
  - case⇒Sf []Cj[]H; last by case: H⇒[?][?][?][?][?][?][].
   have E: k = j by case: H.
   move: H. subst k⇒_ R2. apply: ret_rule.
   move ⇒ m' R3.
   move ⇒ x [] cond.
   rewrite /rc_prepare_resp_inv.
   by rewrite -(rely_loc' _ R1)-(rely_loc' _ R2)-(rely_loc' _ R3).
  case⇒Sf []Cj[]⇒[|[l'][mid][tms][from'][rt][pf][][E]Hin E1 Hw/=]; first by case.
  case/andP⇒/eqP Z G→{k}[]Z1 Z2 Z3 R2; subst l' from' tg body.
  move: rt pf (coh_s (w:=W) l (s:=j) Cj) Hin R2 E1 Hw G E; rewrite prEq/=.
  move⇒rt pf Cj' Hin R E1 Hw G E.
  have D: rt = receive_prepare_req_trans _ _.
  - case: Hin G⇒/=; first by intuition.
  admit.
  admit.
Admitted.
Next Obligation.
  apply: ghC⇒i pinit E1 C1.
  have Pre: rc_prepare_resp_inv e pinit [::] i by rewrite /rc_prepare_resp_inv/= E1.
  apply: call_rule'⇒[|acc m]; first by ∃ pinit.
  case/(_ pinit Pre)⇒/=H1 H2 Cm; split⇒//; by move/negbNE: H1.
Qed.

Definition read_res (st : StateT) :=
  let: (_, rs) := st in
  match rs with
  | PWaitPrepResp res _ ⇒ res
  | _ ⇒ [::]
  end.

(*******************************************)
(*** Sending accept requests ***)
(*******************************************)

Definition send_accept_req_loop_spec (e : nat) psal := ∀ to_send,
  {(pinit: proposal)}, DHT [p, W]
  (fun i ⇒
    (∃ res,
       [∧ loc i = st :→ (e, PWaitPrepResp res pinit),
       to_send = acceptors &
       perm_eq (map fst' res) acceptors]) ∨
     if to_send == [::]
     then loc i = st :→ (e, PAbort)
     else ∃ (acptrs : seq nid),
      loc i = st :→ (e, PSentAccReq acptrs psal) ∧
      perm_eq acceptors (acptrs ++ to_send),
   fun (r : unit) m ⇒ loc m = st :→ (e, PAbort)).
   (* Aborts after sending all accept requests *)

Program Definition send_accept_req_loop e psal: send_accept_req_loop_spec e psal :=
  fun to_send ⇒
   Do (fix rec to_send :=
        (match to_send with
         | to :: tos ⇒ send_accept_req psal to ;; rec tos
         | [::] ⇒ ret _ _ tt
         end)) to_send.
Next Obligation.
  apply: ghC⇒s1 psal' E1 C1; elim: to_send s1 E1 C1⇒//=.
  - move⇒s1; case; first by case⇒?[]_ Z; rewrite -Z in (AcceptorsNonEmpty).
   move ⇒ E1 _. apply: ret_rule⇒i2 R. by rewrite (rely_loc' _ R).
  move⇒to tos Hi s1 H C1.
  apply: step; apply: act_rule⇒s2 R2/=.
  have Pre: Actions.send_act_safe W (p:=paxos) p l
        (send_accept_req_trans proposers acceptors) [:: e] to s2.
  - split; [by case: (rely_coh R2) | | |]; last first.
   + by rewrite /Actions.filter_hooks um_filt0⇒???/sym/find_some; rewrite dom0 inE.
   (* Because of inE *)
   (* + rewrite /Actions.can_send /nodes inE eqxx andbC/=. *)
   (* by rewrite -(cohD (proj2 (rely_coh R2)))/ddom gen_domPt inE/=. *)
    admit.
   case: (proj2 (rely_coh R2))⇒_ _ _ _/(_ l); rewrite prEq⇒C; split.
   (* Because of inE *)
   (* + split⇒//; case: H; first by case⇒?[_]<-; rewrite inE eqxx. *)
   (* by case⇒ps[_]/perm_eq_mem→; rewrite mem_cat orbC inE eqxx. *)
   admit.
  split.
  admit. (* Because of Hin *)
  admit. (* Don't know why this doesn't work *)


  (* Postcondition *)
  split ⇒ //.
  admit. (* Actions.send_act_safe *)
  move ⇒ body i3 i4[Sf]/=St R3.
  apply: Hi; last by case: (rely_coh R3).
  right; rewrite (rely_loc' _ R3).
  admit.
Admitted.

Program Definition send_accept_reqs e psal:
  {(pinit: proposal)}, DHT [p, W]
  (fun i ⇒ ∃ recv_promises,
       [∧ loc i = st :→ (e, PWaitPrepResp recv_promises pinit) &
        perm_eq (map fst' recv_promises) acceptors],
   fun (r : unit) m ⇒ loc m = st :→ (e, PAbort))
  := Do (send_accept_req_loop e psal acceptors).
Next Obligation.
  apply: ghC⇒i lg[res][H1]H2 H3 C; apply: (gh_ex (g:=lg)).
  apply: call_rule⇒//; first by move⇒_; left; ∃ res.
  done.
Qed.

Lemma equal_rounds (left_state: StateT) (right_state: StateT):
  left_state = right_state → fst left_state = fst right_state.
Proof.
  admit.
Admitted.

(*****************************************************)
(* Full Proposer Implementation *)
(*****************************************************)
Search _ (?X :→ _ = ?X :→ _).
(* This is only ment to be run once for each proposer *)
Program Definition proposer_round (p_init: proposal):
  {(psal: proposal) (e : nat)}, DHT [p, W]
  (fun i ⇒ loc i = st :→ (e, PInit psal),
   fun (_: unit) m ⇒ loc m = st :→ (e, PAbort))
  :=
  Do (e <-- read_round;
      send_prepare_req_loop e p_init;;
      recv_promises <-- receive_prepare_resp_loop e;
      send_accept_reqs e (create_proposal_for_acc_req recv_promises p_init);;
      ret _ _ tt).
Next Obligation.
  move⇒s0/=[psal [e]] E0. apply: step.
  apply: (gh_ex (g := (e, PInit psal))).
  apply: call_rule⇒//e' s1 [E1][pf]→C1.
  (* rewrite !(getStP_K _ E1)⇒{e'}. *)
  (* apply: step; apply: (gh_ex (g := psal)). *)
  (* apply: call_rule⇒//_ s2[_]/=E2 C2. *)
  (* apply: step; apply: (gh_ex (g:=psal)). *)
  (* apply: call_rule⇒//res s3/= [E3 H3] C3. *)
  (* - do![apply: step]; apply: (gh_ex (g:=psal)). *)
  (* apply: call_rule ⇒_. ∃ res. split ⇒ //. *)

  (* move ⇒ s4 E4 C4. *)
  (* apply: ret_rule ⇒ s5 R5 psal' e' E0'. *)
  (* rewrite E0 in E0'. *)

   (* rewrite <- (equal_rounds _ _ (hcancelPtV _ E0')). *)
   (* Found no subterm matching "(e', PInit psal').1" in the current goal. *)
Admitted.

End ProposerImplementation.
End PaxosProposer.

Module Exports.
Section Exports.

Definition proposer_round := proposer_round.

End Exports.
End Exports.

End PaxosProposer.

Export PaxosProposer.Exports.
```

C.3 PaxosAcceptor.v

```
From mathcomp.ssreflect
Require Import ssreflect ssrbool ssrnat eqtype ssrfun seq.
From mathcomp
Require Import path.
Require Import Eqdep.
Require Import Relation_Operators.
From DiSeL.Heaps
Require Import pred prelude idynamic ordtype finmap pcm unionmap heap coding domain.
From DiSeL.Core
Require Import Freshness State EqTypeX DepMaps Protocols Worlds NetworkSem Rely.
From DiSeL.Core
Require Import Actions Injection Process Always HoareTriples InferenceRules.
From DiSeL.Core
Require Import InductiveInv While.
From DiSeL.Examples
Require Import PaxosProtocol.


Module PaxosAcceptor.
Section PaxosAcceptor.

Variable l : Label.
Variables (proposers: seq nid) (acceptors: seq nid).

Variable a: nid.


Definition paxos := PaxosProtocol proposers acceptors l.
Notation W := (mkWorld paxos).

Section AcceptorImplementation.

(************** Atomic actions **************)
(* Two send-actions, e -- id of the current era *)
Program Definition send_promise_resp psal to :=
  act (@send_action_wrapper W paxos a l (prEq paxos)
      (send_promise_resp_trans proposers acceptors) _ psal to).
Next Obligation.
  rewrite !InE. right. right. left. done.
Qed.

Program Definition send_nack_resp psal to :=
  act (@send_action_wrapper W paxos a l (prEq paxos)
      (send_nack_resp_trans proposers acceptors) _ psal to).
Next Obligation.
  rewrite !InE. right. right. right. done.
Qed.


(* Two receive-actions *)
Program Definition tryrecv_prepare_req := act (@tryrecv_action_wrapper W a
    (fun k _ t b ⇒ (k == l) && (t == prepare_req)) _).
Next Obligation.
  by case/andP: H⇒/eqP→_; rewrite /ddom gen_domPt inE/=.
Qed.

Program Definition tryrecv_accept_req :=
  act (@tryrecv_action_wrapper W a
  (fun k _ t b ⇒ (k == l) && (t == accept_req)) _).
Next Obligation.
  by case/andP: H⇒/eqP→_; rewrite /ddom gen_domPt inE/=.
Qed.


(************** Acceptor code **************)

(*** Reading internal state ***)
Implicit Arguments PaxosProtocol.PaxosCoh [proposers acceptors].
Notation coh := (@PaxosProtocol.PaxosCoh proposers acceptors).
Notation getS s := (getStatelet s l).
Notation loc i := (getLocal a (getStatelet i l)).

Export PaxosProtocol.

Program Definition read_round:
  {(s: StateT)}, DHT [a, W]
  (fun i ⇒ loc i = st :→ s,
   fun r m ⇒ loc m = st :→ s ∧
           ∃ (pf : coh (getS m)), r = (getSt a pf).1) :=
  Do (act (@skip_action_wrapper W a l paxos (prEq paxos) _
                        (fun s pf ⇒ (getSt a pf).1))).
Next Obligation.
  apply: ghC.
  move ⇒ s st s_is_st s_in_coh_w.
  apply: act_rule ⇒ j R.
  split ⇒ [|r k m].
   by case: (rely_coh R).
  case⇒/=H1[Cj]Z.
  subst j⇒→R'.
  split; first by rewrite (rely_loc' l R') (rely_loc' _ R).
  case: (rely_coh R')⇒_; case⇒_ _ _ _/(_ l)⇒/= pf; rewrite prEq in pf.
  ∃ pf; move: (rely_loc' l R') ⇒/sym E'.
  suff X: getSt a (Actions.safe_local (prEq paxos) H1) = getSt a pf by rewrite X.
   by apply: (getStE' pf _ E').
Qed.

Program Definition read_state:
  {(s: StateT)}, DHT [a, W]
  (fun i ⇒ loc i = st :→ s,
   fun r m ⇒ loc m = st :→ s ∧
           ∃ (pf : coh (getS m)), r = (getSt a pf).2) :=
  Do (act (@skip_action_wrapper W a l paxos (prEq paxos) _
                        (fun s pf ⇒ (getSt a pf).2))).
Next Obligation.
  apply: ghC.
  move ⇒ s st s_is_st s_in_coh_w.
  apply: act_rule ⇒ j R.
  split ⇒ [|r k m].
   by case: (rely_coh R).
  case⇒/=H1[Cj]Z.
  subst j⇒→R'.
  split; first by rewrite (rely_loc' l R') (rely_loc' _ R).
  case: (rely_coh R')⇒_; case⇒_ _ _ _/(_ l)⇒/= pf; rewrite prEq in pf.
  ∃ pf; move: (rely_loc' l R') ⇒/sym E'.
  suff X: getSt a (Actions.safe_local (prEq paxos) H1) = getSt a pf by rewrite X.
  by apply: (getStE' pf _ E').
Qed.

(* Step 1: Receive prepare req *)

(* Ending condition *)
Definition r_prepare_req_cond (res : option proposal) := res == None.
```

```
(* Invariant relates the argument and the shape of the state *)
Definition r_prepare_req_inv (e : nat) (pinit: proposal): cont (option proposal) :=
  fun res i ⇒
    if res is Some psal
    then loc i = st :→ (e, APromised psal)
    else loc i = st :→ (e, AInit).

(* Loops until it receives a prepare req *)
Program Definition receive_prepare_req_loop (e : nat):
  DHT [a, W]
  (fun i ⇒ loc i = st :→ (e, AInit),
   fun res m ⇒ ∃ psal, (res = Some psal) ∧
       (loc m = st :→ (e, APromised psal)))
  :=
  Do _ (@while a W _ _ r_prepare_req_cond (r_prepare_req_inv e) _
        (fun _ ⇒ Do _ (
           r <-- tryrecv_prepare_req;
           match r with
           | Some (from, tg, body) ⇒ ret _ _ (Some body)
           | None ⇒ ret _ _ None
           end
        )) None).
Next Obligation. by apply: with_spec x. Defined.
Next Obligation. by move:H; rewrite /r_prepare_req_inv (rely_loc' _ H0). Qed.
Next Obligation.
  apply:ghC⇒i1 psal[/eqP→{H}/=E1]C1; apply: step.
  apply: act_rule⇒i2/=R1; split; first by case: (rely_coh R1).
  case⇒[[[from e']d i3 i4]|i3 i4]; last first.
  - case⇒S/=[]?; case; last by case⇒?[?][?][?][?][?][].
    case⇒_ _ Z; subst i3⇒R2; apply: ret_rule⇒i5 R4/=.
    by rewrite (rely_loc' _ R4) (rely_loc' _ R2)(rely_loc' _ R1).
  case⇒Sf[]C2[]⇒[|[l'][mid][tms][from'][rt][pf][][E]Hin E2 Hw/=]; first by case.
  case/andP⇒/eqP Z G→[]Z1 Z2 Z3 R2; subst l' from' e' d.
  move: rt pf (coh_s (w:=W) l (s:=i2) C2) Hin R2 E2 Hw G E; rewrite prEq/=.
  move⇒rt pf Cj' Hin R E2 Hw G E.
  have D: rt = receive_prepare_req_trans _ _.
  - move: Hin G; by do! [case⇒/=; first by move⇒→].
  subst rt⇒{G}.
  have P1: valid (dstate (getS i2))
    by apply: (@cohVl _ coh); case: (Cj')⇒P1 P2 P3 P4; split⇒//=; done.
  have P2: valid i2 by apply: (cohS (proj2 (rely_coh R1))).
  have P3: l \in dom i2 by rewrite -(cohD (proj2 (rely_coh R1)))/ddom gen_domPt inE/=.

  apply: ret_rule⇒//i5 R4.
  - rewrite /r_prepare_req_inv; rewrite (rely_loc' _ R4) (rely_loc' _ R) locE//=.
    rewrite /PaxosProtocol.r_step /=.
    rewrite -(rely_loc' _ R1) in E1.
    rewrite (getStK _ E1).
    by rewrite /step_recv /mkLocal.
Qed.
Next Obligation.
  move ⇒ i1/= E1.
  apply: (gh_ex (g:=([::0; 0]))).
  apply: call_rule ⇒ //r i2 [H1]H2 C2.
  rewrite /r_prepare_req_cond/r_prepare_req_inv in H1 H2.
    by case: r H1 H2 ⇒ //p _; ∃ p.
Qed.

(* Finds the promised number from current state *)
Definition read_promised_number (rs: RoleState): nat :=
  match rs with
  | APromised psal ⇒ head 0 psal
  | _ ⇒ 0
  end.
```

```
Definition read_promised_value (rs: RoleState): nat :=
  match rs with
  | APromised psal ⇒ last 0 psal
  | _ ⇒ 0
  end.

(* Step 2: Respond promise or nack to the proposer *)
Program Definition resp_to_prepare_req (e: nat) (send_promise: bool) (prepare_no: nat)
  (promised_no: nat) (promised_val: nat):
  {(pif: (proposal * proposal))}, DHT [a, W]
   (fun i ⇒ loc i = st :→ (e, APromised pif.1) ∨loc i = st :→ (e, AInit),
    fun (_ : seq nat) m ⇒
      if send_promise
      then loc m = st :→ (e, APromised pif.2)
      else loc m = st :→ (e, APromised pif.1))
  := Do (rs <-- read_state;
         if send_promise
         then send_promise_resp [:: promised_no; promised_val] prepare_no
         else send_nack_resp [:: 0; 0] prepare_no).
Next Obligation.
  apply:ghC⇒i [pinit pfinal]E1 C1.
  have Pre: ∀ i2 proposer_id, network_rely W a i i2 →
        Actions.send_act_safe W (p:=paxos) a l
        (if send_promise
         then send_promise_resp_trans proposers acceptors
         else send_nack_resp_trans proposers acceptors)
        [:: e] proposer_id i2.
  - move⇒i2 pid R1.
    split; first by case: (rely_coh R1).
    case: (proj2 (rely_coh R1))⇒_ _ _ _/(_ l); rewrite (prEq paxos)⇒C.
    case: send_promise.
    split ⇒ //.
    admit.
    rewrite /send_promise_resp_prec.
    rewrite -(rely_loc' _ R1) in E1.
    (* Need inE to work *)
    (* + rewrite /Actions.can_send /nodes inE/= mem_cat Hpin orbC. *)
    (* by rewrite -(cohD (proj2 (rely_coh R1)))/ddom gen_domPt inE/= eqxx. *)

    (* by rewrite /Actions.filter_hooks um_filt0⇒???/sym/find_some; rewrite dom0 inE. *)
Admitted.


(* Ending condition *)
Definition r_acc_req_cond (res : option proposal) := res == None.

(* Invariant relates the argument and the shape of the state *)
Definition r_acc_req_inv (e : nat) (promised: bool) (promised_psal: proposal) (received_psal: proposal): cont (
        option proposal) :=
  fun res i ⇒
    if res is Some received_psal
    then if promised
         then if head 0 promised_psal < head 0 received_psal
           then loc i = st :→ (e, AAccepted received_psal)
           else loc i = st :→ (e, APromised promised_psal)
       else loc i = st :→ (e, AAccepted received_psal)
    else if promised
       then loc i = st :→ (e, APromised promised_psal)
       else loc i = st :→ (e, AInit).

(* Loops until it receives a accept req *)
Program Definition receive_acc_req_loop (e : nat) (promised: bool) (promised_psal: proposal):
  {(pinit: proposal)}, DHT [a, W]
   (fun i ⇒ if promised
             then loc i = st :→ (e, APromised promised_psal)
             else loc i = st :→ (e, AInit),
  fun res m ⇒ ∃ psal, res = Some psal ∧(
    loc m = st :→ (e, APromised promised_psal) ∨
    loc m = st :→ (e, AAccepted psal)
  )) :=
  Do _ (@while a W _ _ r_acc_req_cond (r_acc_req_inv e promised promised_psal) _
        (fun _ ⇒ Do _ (
           r <-- tryrecv_accept_req;
           match r with
           | Some (from, tg, body) ⇒ ret _ _ (Some body)
           | None ⇒ ret _ _ None
           end
        )) None).
Next Obligation. by apply: (with_spec x). Defined.
Next Obligation. by move:H; rewrite /r_acc_req_inv (rely_loc' _ H0). Qed.
Next Obligation.
  apply:ghC⇒i1 psal [/eqP⟶{H}/=E1]C1. apply: step.
  apply: act_rule⇒i2/=R1; split; first by case: (rely_coh R1).
  case⇒[[[from e']v i3 i4]|i3 i4]; last first.
  - case⇒S/=[]?; case; last by case⇒?[?][?][?][?][?][].
    case⇒_ _ Z; subst i3⇒R2; apply: ret_rule⇒i5 R4/=.
    rewrite /r_acc_req_inv/= in E1 *.
    by rewrite (rely_loc' _ R4) (rely_loc' _ R2) (rely_loc' _ R1).
  case⇒Sf[]C2[]⇒[|[l'][mid][tms][from'][rt][pf][][E]Hin E2 Hw/=]; first by case.
  case/andP⇒/eqP Z G⟶[]Z1 Z2 Z3 R2; subst l' from' e' v.
  move: rt pf (coh_s (w:=W) l (s:=i2) C2) Hin R2 E2 Hw G E; rewrite prEq/=.
  move⇒rt pf Cj' Hin R E2 Hw G E.
  have P1: valid (dstate (getS i2))
    by apply: (@cohVl _ coh); case: (Cj')⇒P1 P2 P3 P4; split⇒//=; done.
  have P2: valid i2 by apply: (cohS (proj2 (rely_coh R1))).
  have P3: l \in dom i2 by rewrite-(cohD (proj2 (rely_coh R1)))/ddom gen_domPt inE/=.
  have D: rt = receive_accept_req_trans _ _.
  - by move: Hin G; clear E1; do![case⇒/=; first by move⇒⟶].
  apply: ret_rule⇒//i5 R4.
  - rewrite /r_acc_req_inv (rely_loc' _ R4) (rely_loc' _ R) locE//=.
    case: (promised) E1 E2 D G⇒/=E1 E2; case⇒Z {E2}; subst rt⇒//= _;
    rewrite -(rely_loc' _ R1) in E1;
    rewrite /r_step (getStK _ E1) /step_recv/= /mkLocal.
    case: ifP⇒G1; case: ifP ⇒ //; rewrite G1 ⇒ //.
    done.
Qed.
Next Obligation.
  apply: ghC⇒i1 psal E1 C1/=.
  apply: (gh_ex (g := psal)); apply: call_rule ⇒ //r i2 [H1]H2 C2.
  rewrite /r_acc_req_cond/r_acc_req_inv in H1 H2; case: r H1 H2⇒//b _ i2_AA.
  ∃ b.
  split ⇒ //.
  move: i2_AA.
  case: ifP⇒G1 ⇒ //.
  case: ifP⇒G2.
  by right.
  by left.
  by right.
Qed.

(* Using resp_to_prepare_req 0 as a 'do nothing' transition for now.
As 0 will never be > 0 so the acceptor won't send a promise *)
Program Definition acceptor_round:
  {(ep: nat * proposal)}, DHT [a, W]
  (fun i ⇒ loc i = st :→ (ep.1, AInit),
   fun (_: unit) m ⇒ (
     loc m = st :→ (ep.1, AInit) ∨
     loc m = st :→ (ep.1, APromised ep.2) ∨
     loc m = st :→ (ep.1, AAccepted ep.2)
  )) :=
     Do _ (e <-- read_round;
          (* need to read state here as once it receives the message,
             it already changes state *)
          rs <-- read_state;
          msg <-- receive_prepare_req_loop e;
          (match msg with
           | Some body ⇒
             let: prepare_no := head 0 body in
             let: promised_no := read_promised_number rs in
             let: promised_val := read_promised_value rs in
             resp_to_prepare_req e (promised_no < prepare_no)
               prepare_no promised_no promised_val
           | _ ⇒ resp_to_prepare_req e false 0 0 0 (* results in sending nack *)
          end);;
         rs <-- read_state;
         (match rs with
         (* It's in promised state *)
         | APromised psal ⇒ receive_acc_req_loop e true psal
         (* It hasn't promised anything *)
         | _ ⇒ receive_acc_req_loop e false [:: 0; 0]
         end);;
         ret _ _ tt).
Next Obligation.
  apply: ghC ⇒ i1[e psal]/=E1 C1; apply: step.
  apply: (gh_ex (g:=(e, AInit))); apply: call_rule⇒//e' i2 [E2][pf]⟶C2.
  apply: step.
  apply: (gh_ex (g:=(e, AInit))). apply: call_rule⇒//??[?]??.
  apply: step.
  apply: call_rule; last first.
  move⇒x? _ _. case: x⇒a'. apply: step.
  apply: (gh_ex (g:=([::], [::]))). apply: call_rule; last first.
  move⇒?? _ _. apply: step.
  apply: (gh_ex (g:=(e, AInit))). apply: call_rule; last first.
  move⇒y ? _ _.
  case: y⇒//.
Admitted.


End AcceptorImplementation.
End PaxosAcceptor.

Module Exports.
Section Exports.

Definition acceptor_round := acceptor_round.

End Exports.
End Exports.

End PaxosAcceptor.


Export PaxosAcceptor.Exports.
```

C.4 SimplePaxosApp.v

```
From mathcomp.ssreflect
Require Import ssreflect ssrbool ssrnat eqtype ssrfun seq.
From mathcomp
Require Import path.
Require Import Eqdep.
Require Import Relation_Operators.
From DiSeL.Heaps
Require Import pred prelude ordtype finmap pcm unionmap heap coding domain.
From DiSeL.Core
Require Import State Protocols Worlds NetworkSem Rely.
From DiSeL.Core
Require Import HoareTriples InferenceRules While.
From DiSeL.Examples
Require Import PaxosProtocol PaxosProposer PaxosAcceptor.
From DiSeL.Examples
Require PaxosInductiveInv.

Section SimplePaxosApp.

(*

A simple application to run on the shim implementation.

Check for [Run] tags to find the initial state and the code for the
proposers and the acceptors.

*)

Definition l := 0.
(* Proposer nodes *)
Definition p1 := 1.
Definition p2 := 2.

(* Acceptor nodes *)
Definition a1 := 3.
Definition a2 := 4.
Definition a3 := 5.

Definition proposers := [:: p1].
Definition acceptors := [::a1; a2; a3].

(* Necessary coherence facts *)
Fact AcceptorsNonEmpty : acceptors != [::]. Proof. by []. Qed.

(* Proposers *)
Definition proposer p (pf: acceptors != [::]) psal:=
  proposer_round l proposers acceptors p pf psal.

(* Acceptors *)
Program Definition acceptor a :=
  acceptor_round l proposers acceptors a.

(* Initial distributed state *)
Definition st_ptr := PaxosProtocol.States.st.

Definition init_heap_p psal:= st_ptr :→ (0, PInit psal).
Definition init_heap_a := st_ptr :→ (0, AInit).

Definition init_dstate :=
  p1 \\→ init_heap_p [:: 1; 1] \+
  a1 \\→ init_heap_a \+
  a2 \\→ init_heap_a \+
  a3 \\→ init_heap_a.

Lemma valid_init_dstate : valid init_dstate.
Proof.
  admit.
Admitted.

Notation init_dstatelet := (DStatelet init_dstate Unit).

(* [Run] Initial state to run *)
Definition init_state : state := l \\→ init_dstatelet.


(* Final Safety Facts *)
Notation W := (mkWorld (PaxosProposer.paxos l proposers acceptors)).

Lemma hook_complete_unit (c : context) : hook_complete (c, Unit).
Proof. by move⇒????; rewrite dom0 inE. Qed.

Lemma hooks_consistent_unit (c : context) : hooks_consistent c Unit.
Proof. by move⇒????; rewrite dom0 inE. Qed.

Lemma init_coh : init_state \In Coh W.
Proof. admit. Admitted.

(* [Run] Runnable proposer code *)
Program Definition run_proposer p (AcceptorsNonEmpty: acceptors != [::]) psal:
  DHT [p, _] (
    fun i ⇒ network_rely W p init_state i,
    fun _ m ⇒ ∃ (r : nat),
    getLocal p (getStatelet m l) = st :→ (r, PInit psal))
  := Do (with_inv (PaxosInductiveInv.ii _ _ _) (proposer p AcceptorsNonEmpty psal)).
Next Obligation.
  admit.
Admitted.
Check run_proposer.
(* [Run] Runnable acceptor code *)
Program Definition run_acceptor a:
  DHT [a, _] (
    fun i ⇒ network_rely W a init_state i,
    fun _ m ⇒ ∃ (r : nat),
    getLocal a (getStatelet m l) = st :→ (r, AInit))
  := Do (with_inv (PaxosInductiveInv.ii _ _ _) (acceptor a)).
Next Obligation.
  admit.
Admitted.

Variables (psal_1 psal_2 : proposal).
Variables (p_1 a_1 a_2 a_3: nat).
(* [Run] Runnable nodes *)
Program Definition run_proposer1 := run_proposer p1 AcceptorsNonEmpty psal_1.
Program Definition run_proposer2 := run_proposer p2 AcceptorsNonEmpty psal_2.
Program Definition run_acceptor1 := run_acceptor a_1.
Program Definition run_acceptor2 := run_acceptor a_2.
Program Definition run_acceptor3 := run_acceptor a_3.

End SimplePaxosApp.

(* [Run] Final programs to run with actual arguments supplied *)
```

```
Definition p_runner1 (u : unit) := run_proposer1 [:: 1; 1].
Definition p_runner2 (u : unit) := run_proposer1 [:: 2; 2].

Definition a_runner1 (u : unit) := run_acceptor1 a1.
Definition a_runner2 (u : unit) := run_acceptor2 a2.
Definition a_runner3 (u : unit) := run_acceptor3 a3.
```

C.5 PaxosExtraction.v

```
From DiSeL.Core
Require Import DiSeLExtraction.
From DiSeL.Examples
Require Import SimplePaxosApp.

Cd "extraction".
 Cd "Paxos".
   Separate Extraction DepMaps.DepMaps.dmap init_state p_runner1 p_runner2 a_runner1 a_runner2 a_runner3.
 Cd "..".
Cd "..".
```

C.6 PaxosInductiveInv.v

```
From mathcomp.ssreflect
Require Import ssreflect ssrbool ssrnat eqtype ssrfun seq.
From mathcomp
Require Import path.
Require Import Eqdep.
Require Import Relation_Operators.
From DiSeL.Heaps
Require Import pred prelude idynamic ordtype finmap pcm unionmap.
From DiSeL.Heaps
Require Import heap coding domain.
From DiSeL.Core
Require Import Freshness State EqTypeX Protocols Worlds NetworkSem Rely.
From DiSeL.Core
Require Import Actions Injection Process Always HoareTriples InferenceRules.
From DiSeL.Core
Require Import InductiveInv StatePredicates.
From DiSeL.Examples
Require Import PaxosProtocol.


Set Implicit Arguments.
Unset Strict Implicit.
Import Prenex Implicits.

Section PaxosInductiveInv.

Variable l: Label.

Variable (proposers: seq nid) (acceptors: seq nid).

Definition paxos := PaxosProtocol proposers acceptors l.

(* Take the transitions *)
Notation sts := (snd_trans paxos).
Notation rts := (rcv_trans paxos).

Notation loc z d := (getLocal z d).

Definition role_state (d: dstatelet) (s: StateT) (n: nid): Prop :=
 loc n d = st :→ s.

(*****************************************************)

(* Phase Zero *)
Definition EverythingInit (d : dstatelet) (round : nat): Prop :=
 ∀ n, n \in (proposers ++ acceptors) → (
  (∃ psal, role_state d (round, PInit psal) n)
  ∨role_state d (round, AInit) n).


(* Phase One *)
Definition Phase1a (d: dstatelet) (round: nat) (n: nid): Prop :=
 if n \in acceptors
 then role_state d (round, AInit) n
 else (
  ∃ psal, (role_state d (round, PInit psal) n)
  ∨(∃ sent_to, role_state d (round, PSentPrep psal sent_to) n)
  ∨(∃ promises, role_state d (round, PWaitPrepResp promises psal) n)
 ).

Definition Phase1b (d: dstatelet) (round: nat) (n: nid): Prop :=
 if n \in acceptors
 then ∃ psal, role_state d (round, APromised psal) n
 else ∃ psal,
  ∃ promises, role_state d (round, PWaitPrepResp promises psal) n.

Definition Phase2a (d: dstatelet) (round: nat) (n: nid): Prop :=
 if n \in acceptors
 then (
  role_state d (round, PAbort) n
  ∨∃ psal, (role_state d (round, APromised psal) n)
 )
 else ∃ psal,
  ∃ sent_to, role_state d (round, PSentAccReq sent_to psal) n.

Definition Phase2b (d: dstatelet) (round: nat) (n: nid): Prop :=
 if n \in acceptors
 then ∃ psal, (
  role_state d (round, AAccepted psal) n ∨
  ∀ a, a \in acceptors → role_state d (round, AAccepted psal) a
 )
 else role_state d (round, PAbort) n.

(* TODO: Fix the conditions. This Inv currently isn't checking for anything. *)
Definition Inv (d: dstatelet) :=
 ∃ round,
  EverythingInit d round
  ∨(∀ n, n \in (proposers ++ acceptors) →
     (Phase1a d round n ∨Phase1b d round n
      ∨Phase2a d round n ∨Phase2b d round n)).

(*********************************************************)

Notation Sinv := (@S_inv paxos (fun d _ ⇒ Inv d)).
Notation Rinv := (@R_inv paxos (fun d _ ⇒ Inv d)).
Notation coh d := (coh paxos d).
Notation PI := proof_irrelevance.

(*************************************************************)
(* Send-transitions *)
(*************************************************************)

Program Definition s1: Sinv (send_prepare_req_trans proposers acceptors).
Proof.
 move⇒this to d msg S h/= Hi/=[]T G.
 case: (S)⇒[][/eqP]Z H1[C]. ∃ to.

 (* Init state *)
 right.
 left.
 admit.
Admitted.

Program Definition s2: Sinv (send_accept_req_trans proposers acceptors).
Proof.
 move⇒this to d msg S h/= Hi/=[]T G.
 case: (S)⇒[][/eqP]Z H1[C]. ∃ to.

 (* Init state *)
 right.
 right.
 left.
```

```
  admit.
Admitted.

Program Definition s3: Sinv (send_promise_resp_trans proposers acceptors).
Proof.
  admit.
Admitted.

Program Definition s4: Sinv (send_nack_resp_trans proposers acceptors).
Proof.
  admit.
Admitted.


(**************************************************************)
(* Receive-transitions *)
(**************************************************************)

Program Definition r1: Rinv (receive_prepare_req_trans proposers acceptors).
Proof.
  admit.
Admitted.

Program Definition r2: Rinv (receive_accept_req_trans proposers acceptors).
Proof.
  admit.
Admitted.

Program Definition r3: Rinv (receive_promise_resp_trans proposers acceptors).
Proof.
  admit.
Admitted.

Program Definition r4: Rinv (receive_nack_resp_trans proposers acceptors).
Proof.
  admit.
Admitted.


Definition sts' := [:: SI s1; SI s2; SI s3; SI s4].
Definition rts' := [:: RI r1; RI r2; RI r3; RI r4].

Program Definition ii := @ProtocolWithInvariant.II _ _ sts' rts' _ _.

Definition paxos_with_inv := ProtocolWithIndInv ii.

End PaxosInductiveInv.
```

C.7 paxos.py

```
#!/usr/bin/env python3

import subprocess
import re
import time


proposer1 = "(./PaxosMain.d.byte -me 1 -mode proposer 1 127.0.0.1 8000 2 127.0.0.1 8001 3 127.0.0.1 8002 4
       127.0.0.1 8003 5 127.0.0.1 8004 &) > proposer1.log 2>&1"
proposer2 = "(./PaxosMain.d.byte -me 2 -mode proposer 1 127.0.0.1 8000 2 127.0.0.1 8001 3 127.0.0.1 8002 4
       127.0.0.1 8003 5 127.0.0.1 8004 &) > proposer2.log 2>&1"
acceptor1 = "(./PaxosMain.d.byte -me 3 -mode acceptor 1 127.0.0.1 8000 2 127.0.0.1 8001 3 127.0.0.1 8002 4
       127.0.0.1 8003 5 127.0.0.1 8004 &) > acceptor1.log 2>&1"
acceptor2 = "(./PaxosMain.d.byte -me 4 -mode acceptor 1 127.0.0.1 8000 2 127.0.0.1 8001 3 127.0.0.1 8002 4
       127.0.0.1 8003 5 127.0.0.1 8004 &) > acceptor2.log 2>&1"
acceptor3 = "(./PaxosMain.d.byte -me 5 -mode acceptor 1 127.0.0.1 8000 2 127.0.0.1 8001 3 127.0.0.1 8002 4
       127.0.0.1 8003 5 127.0.0.1 8004 &) > acceptor3.log 2>&1"

a1 = subprocess.Popen(acceptor1, shell=True)
a2 = subprocess.Popen(acceptor2, shell=True)
a3 = subprocess.Popen(acceptor3, shell=True)
p1 = subprocess.Popen(proposer1, shell=True)
p2 = subprocess.Popen(proposer2, shell=True)

consensus_achieved = True
consensus_value = None

exit_codes = [p.wait() for p in [a1, a2, a3]]
print(exit_codes)

# wait for processes to write to files
time.sleep(2)

for i in range(1, 4):
   line = subprocess.check_output(['tail', '-1', "acceptor{0}.log".format(i)])
   line = line.decode("utf-8")
   print(line.rstrip())

   pattern = r"got msg in protocol (\d) with tag = (\d), contents = \[(\d); (\d)\]"
   match = re.match(pattern, line)

   if not match or (consensus_value and consensus_value != match.group(4)):
      print("Error in acceptor %d" % i)
      consensus_achieved = False
      break
   else:
      print("Acceptor %d accepted %s" % (i, match.group(4)))
      consensus_value = match.group(4)

print("=" * 40)

if consensus_achieved:
   print("\nConsesus achieved on value: %s" % consensus_value)
else:
   print("\nConsesus not achieved")
```

D
Simulator Code Listing

D.1 paxos.py

```
#!/usr/bin/env python3

import os
import signal
import sys
import time

from paxos.proposer import Proposer
from paxos.acceptor import Acceptor

NACCEPTORS = 3
NPROPOSERS = 2


class Env:
   """
   Sets up the environment and runs the protocol.
   Initialises each of the nodes in the protocol.

   Attributes:
      :procs holds all the executing processes
   """

   def __init__(self):
      self.procs = {}

   def send_msg(self, dst, msg):
      if dst in self.procs:
         self.procs[dst].deliver(msg)

   def add_proc(self, proc):
      self.procs[proc.id] = proc
      proc.start()

   def remove_proc(self, pid):
      del self.procs[pid]

   def run(self):
      proposers = range(1, NPROPOSERS + 1)
      acceptors = range(NPROPOSERS, NPROPOSERS + NACCEPTORS)

      for i in acceptors:
         pid = "Acceptor %d" % i
         Acceptor(self, i)

      for i in proposers:
         pid = "Proposer %d" % i
         Proposer(self, acceptors, i, i)

   def terminate_handler(self, signal, frame):
      self._graceful_exit()

   def _graceful_exit(self, exit_code=0):
      sys.stdout.flush()
      sys.stderr.flush()
      os._exit(exit_code)


def main():
   e = Env()
   e.run()
   signal.signal(signal.SIGINT, e.terminate_handler)
   signal.signal(signal.SIGTERM, e.terminate_handler)
   signal.pause()


main()
```

D.2 paxos/process.py

```python
import multiprocessing
import threading


class Process(threading.Thread):
   """
   Attributes:
      :state current state of the Acceptor
      :id id of the Acceptor
      :env environment this Acceptor is running in
   """

   def __init__(self, env, id):
      super(Process, self).__init__()
      self.inbox = multiprocessing.Manager().Queue()
      self.env = env
      self.id = id

   def run(self):
      try:
         self.body()
         self.env.remove_proc(self.id)
      except EOFError:
         print("Exiting...")

   def get_next_msg(self):
      return self.inbox.get()

   def send_msg(self, dst, msg):
      self.env.send_msg(dst, msg)

   def deliver(self, msg):
      self.inbox.put(msg)
```

D.3 paxos/message.py

```python
"""
This file defines the Message super class and all the other
types of messages used in the adapted Simple Paxos protocol.
"""


class Message:
   """
   Message super class which all the differnt message types inherit.

   Attributes:
      :src sender of the message
      :proposal proposal contained in the message
   """

   def __init__(self, src, proposal):
      self.src = src
      self.proposal = proposal

   def __str__(self):
      return str(self.__dict__)


class PrepareRequestMessage(Message):
   def __init__(self, src, proposal):
      Message.__init__(self, src, proposal)


class AcceptRequestMessage(Message):
   def __init__(self, src, proposal):
      Message.__init__(self, src, proposal)


class PromiseResponseMessage(Message):
   def __init__(self, src, proposal):
      Message.__init__(self, src, proposal)


class NackResponseMessage(Message):
   def __init__(self, src):
      Message.__init__(self, src, (-1, -1))
```

D.4 paxos/proposer.py

```python
from .process import Process
from .message import AcceptRequestMessage, PrepareRequestMessage, \
    PromiseResponseMessage, NackResponseMessage


class Proposer(Process):
    """
    Implementation of the Proposer in the adapted Simple Paxos protocol.

    Attributes:
        :state current state of the Proposer
        :acceptors set of acceptors in the current environment
        :env environment this Proposer is running in
    """

    def __init__(self, env, acceptors, p_no, p_val):
        Process.__init__(self, env, p_no)
        self.state = ("PInit", p_no, p_val)
        self.acceptors = acceptors
        self.env = env
        self.env.add_proc(self)

    def send_prepare_req(self):
        _, p_no, p_val = self.state
        for acceptor in self.acceptors:
            self.send_msg(
                acceptor,
                PrepareRequestMessage(p_no, (p_no, p_val))
            )

    def send_accept_req(self):
        _, p_no, p_val = self.state
        for acceptor in self.acceptors:
            self.send_msg(
                acceptor,
                AcceptRequestMessage(p_no, (p_no, p_val))
            )

    def body(self):
        _, p_no, p_val = self.state

        self.send_prepare_req()
        self.state = ("PWaitPrepResp", [], p_no, p_val)

        while True:
            msg = self.get_next_msg()
            if isinstance(msg, PromiseResponseMessage):
                if self.state[0] == "PWaitPrepResp":
                    src = msg.src
                    recv_p_no, recv_p_val = msg.proposal
                    recv_promises = self.state[1]

                    if src not in map(lambda x: x[0], recv_promises):
                        recv_promises.append((src, recv_p_no, recv_p_val))
                        if sorted(
                            map(lambda x: x[0], recv_promises)
                        ) == sorted(self.acceptors):
                            recv_promises.sort(key=lambda x: x[1])
                            highest_numbered_value = recv_promises[0][2]
                            self.state = (
                                "PSentAccReq", p_no, highest_numbered_value
                            )
                            self.send_accept_req()
                            print("Exiting proposer", p_no)
                            break
                        else:
                            self.state = (
                                "PWaitPrepResp", recv_promises, p_no, p_val
                            )
            elif isinstance(msg, NackResponseMessage):
                print("Exiting proposer", p_no)
                break
```

D.5 paxos/acceptor.py

```python
from .process import Process
from .message import AcceptRequestMessage, PrepareRequestMessage, \
   PromiseResponseMessage, NackResponseMessage


class Acceptor(Process):
   """
   Implementation of the Acceptor in the adapted Simple Paxos protocol.

   Attributes:
      :state current state of the Acceptor
      :id id of the Acceptor
      :env environment this Acceptor is running in
   """

   def __init__(self, env, id):
      Process.__init__(self, env, id)
      self.state = ("AInit",)
      self.env = env
      self.env.add_proc(self)
      self.id = id

   def send_promise_resp(self, to):
      p_no, p_val = self.state[1]
      self.send_msg(to, PromiseResponseMessage(self.id, (p_no, p_val)))

   def send_nack_resp(self, to):
      self.send_msg(to, NackResponseMessage(self.id))

   def body(self):
      while True:
         msg = self.get_next_msg()
         p_no, p_val = msg.proposal

         if isinstance(msg, PrepareRequestMessage):
            if self.state[0] == "AInit":
               self.state = ("APromised", msg.proposal)
               self.send_promise_resp(p_no)
            elif self.state[0] == "APromised":
               promised_no, _ = self.state[1]
               if p_val < promised_no:
                  self.send_nack_resp(p_no)
               else:
                  self.state = ("APromised", msg.proposal)
                  self.send_promise_resp(p_no)
            else:
               self.send_nack_resp(p_no)
         elif isinstance(msg, AcceptRequestMessage):
            if self.state[0] == "AInit":
               self.state = ("AAccepted", msg.proposal)
            else:
               promised_no, _ = self.state[1]
               if p_val >= promised_no:
                  self.state = ("AAccepted", msg.proposal)
                  print("Node %d has state %s" % (self.id, self.state))
```