

# Mechanised Verification of Paxos-like Consensus Protocols

Anirudh Pillai

January 15, 2018

Thesis advisor: Professor Dr. Ilya Sergey

Anirudh Pillai

# Mechanised Verification of Paxos-like Consensus Protocols

## ABSTRACT

Distributed systems are hard to reason about.

# Acknowledgments

Consectetuer adipiscing elit. Morbi commodo, ipsum sed pharetra gravida, orci magna rhoncus neque, id pulvinar odio lorem non turpis. Nullam sit amet enim. Suspendisse id velit vitae ligula volutpat condimentum. Aliquam erat volutpat. Sed quis velit. Nulla facilisi. Nulla libero. Vivamus pharetra posuere sapien. Nam consectetuer. Sed aliquam, nunc eget euismod ullamcorper, lectus nunc ullamcorper orci, fermentum bibendum enim nibh eget ipsum. Donec porttitor ligula eu dolor. Maecenas vitae nulla consequat libero cursus venenatis. Nam magna enim, accumsan eu, blandit sed, blandit a, eros.

# Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>2</b>
1.1	The Problem . . . . .	3
1.2	Aims and Goals . . . . .	3
1.3	Project Overview . . . . .	3
1.4	Report Overview . . . . .	3
<b>2</b>	<b>CONTEXT</b>	<b>4</b>
2.1	Paxos . . . . .	5
2.2	Coq . . . . .	5
2.3	Disel . . . . .	5
<b>3</b>	<b>REQUIREMENTS AND ANALYSIS</b>	<b>6</b>
3.1	Detailed Problem Statement . . . . .	7
3.2	Requirements . . . . .	7
3.3	Analysis . . . . .	7
<b>4</b>	<b>DESIGN AND IMPLEMENTATION</b>	<b>8</b>
4.1	The Protocol . . . . .	9
4.2	State Transitions . . . . .	9
4.3	Inductive Invariant . . . . .	9
4.4	Client Implementatin . . . . .	9
<b>5</b>	<b>TESTING</b>	<b>10</b>
<b>6</b>	<b>CONCLUSION AND EVALUATION</b>	<b>11</b>
6.1	Summary of Achievements . . . . .	12
6.2	Critical Evaluation . . . . .	12
6.3	Future Work . . . . .	12
6.4	Final Thoughts . . . . .	12
	<b>REFERENCES</b>	<b>13</b>
	<b>APPENDIX A INTERIM REPORT</b>	<b>14</b>

# 1

## Introduction

Talk about some stuff for this chapter.

1.1 THE PROBLEM

1.2 AIMS AND GOALS

1.3 PROJECT OVERVIEW

1.4 REPORT OVERVIEW

# 2

## Context

2.1 PAXOS

2.2 CoQ

2.3 DiSEL



# 3

## Requirements and Analysis

### 3.1 DETAILED PROBLEM STATEMENT

### 3.2 REQUIREMENTS

### 3.3 ANALYSIS

# 4

## Design and Implementation

## 4.1 THE PROTOCOL

## 4.2 STATE TRANSITIONS

## 4.3 INDUCTIVE INVARIANT

## 4.4 CLIENT IMPLEMENTATION

# 5

## Testing

Need to find some form of testing.

# 6

## Conclusion and Evaluation

## 6.1 SUMMARY OF ACHIEVEMENTS

## 6.2 CRITICAL EVALUATION

## 6.3 FUTURE WORK

## 6.4 FINAL THOUGHTS

## References





## Interim Report