30th April 2018 Thesis advisor: Dr. Ilya Sergey

Mechanised Verification of Paxos-like Consensus Protocols

Anirudh Pillai

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 protocols, in which a number of participants are supposed to reach an agreement despite the possible failure of a minority of them.