Consensus Protocol: Formal Specification and Verification With TLA+

Mark Johnson
COMP 474

March 17, 2011

1 Print Abstract

Consensus protocols are well-known and frequently used in many industrial applications. In this protocol, several processes must reach a certain level of agreement regarding state before processing can move forward. The goal of this work is to develop a formal specification for a consensus protocol and verify its correctness using TLA+ and related tools.

2 Tweetable Abstract

Consensus protocol: fromal specification and verification with TLA+.

3 Problem Statement and Thesis

D There is a need for a reliable consensus protocol for distributed systems. Because testing cannot exhaustively reveal all errors, different methods must be used to verify the correctness of the protocol. The techniques of formal specification and verification are needed in order be certain of the correctness of the protocol.

4 Motivation

For critical systems we need a scientifically rigorous method for testing our systems. Scientific techniques can mean the difference between life and death.

5 Statement of Work and Project Management Plan

My project will be based on the book by Leslie Lamport: Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers. I will use it as a guide to my work.

6 Milestones and Deliverables

- System setup and configuration with needed tools.
- Learn the theory and techniques.
- Read background on consensus protocol.
- Develop specification.
- Test the correctness of specification with TLA+ and related tools.