Consensus Protocol: Formal Specification and Verification With TLA+

Mark Johnson
COMP 474

March 17, 2011

1 Print Abstract

TLA stands for Temporal Logic of Actions and it is a logic framework for specifying and reasoning about systems. TLA+ is an extension of TLA, and is a language for specifying systems and tools for verifying the specification. These form a framework and tools for reasoning about systems. As computer scientists we need frameworks and tools for understanding systems. These tools need to be mathematically and scientifically rigorous. Otherwise we are just guessing. The goal of this endeavor is to explore TLA and TLA+ and apply these tools to the creation of a consensus protocol(Lamport 2003).

2 Tweetable Abstract

Application of TLA, TLA+, and related tools to the formal specification and verification of a consensus protocol.

3 Problem Statement and Thesis

When human life or valuable assets are at risk it is important to know that your software is mathematically correct. Because testing is never finished– rather it is only stopped, more scientific methods are needed. This is the role that TLA, TLA+, and related tools can play. These are a methods and tools to formally and mathematically specify a system and use a computer to mechanically verify the correctness of a formal specification. I will use these frameworks to specify and verify a consensus protocol, in order to discover the feasibility of these methods and tools for industrial use.

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. They can be the difference between earning a profit or going bankrupt.

5 Statement of Work and Project Management Plan

I will use "Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers", by Leslie Lamport, as a reference. I will rely heavily on papers written by Lamport, as well as the community resources at www.tlaplus.net. I will produce a formal specification of a consensus protocol, written in the TLA+ language, which I should then be able to mechanically verify with associated software tools, running on a computer.

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.

7 References

1. Lamport, Leslie. A Simple Approach to Specifying Concurrent Systems. Communications of the ACM, 32, 1 (1989), pp. 32-45.
2. Lamport, Leslie. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers". New York: Addison-Wesley, 2003.
3. Fritchie, Scott Lystig. Chain Replication in Theory and in Practice. Proceedings of the 9th ACM SIGPLAN Workshop on Erlang. ACM, 2010, pp. 33-43.

4.