Proving correctness of MongoRaftReconfig

1 Intro

This note describes our progress on proving that MongoRaftReconfig satisfies State Machine Safety (SMS) (as well as other properties such as Leader Completeness Safety (LCS) and Log Matching Safety (LMS)). Section 2 talks about our work on proving MongoStaticRaft (the base protocol that resembles Raft) and Section 3 talks about our work on proving MongoRaftReconfig.

2 MongoStaticRaft

2.1 Intro

We have finished proving that MongoStaticRaft satisfies SMS and LCS, and we will talk about the details in this section. I will use the abbreviation MSR to refer to MongoStaticRaft with Log Matching (i.e. MSR = MSRLM); I will explicitly mention "MSR without LMS" if needed.

2.2 MSR Protocol

This is discussed in Will's paper. An additional detail is that MSR is similar to Raft, but not identical. Here are two interesting details of note:

1. MSR can only commit log entries at the end of its log
2. Raft considers any log entries earlier than a commit to be committed. We believe that MSR logically abides by this rule, however the *committed* state variable does not keep track of commits that are prior to a log entry that is explicitly committed by a primary. The *committed* state variable is a ghost variable and hence this does not imply an issue in MSR, however it means that we may be able to improve our safety-property-checking by fixing the "holes" in our ghost variable.

2.3 MSR Safety

The inductive invariant we use is called SMS_LC_II (State Machine Safety, Leader Completeness Inductive Invariant). We have proved that SMS_LC_II 1) implies the initial state of MSR, 2) is inductive invariant on the transition relation for MSR, and 3) implies State Machine Safety. Interestingly, SMS_LC_II does *not* imply Log Matching, and does not require the protocol to satisfy Log Matching to hold. We have proved SMS_LC_II for MSR both with and without Log Matching.

2.4 SMS_LC_II Proof Details

2.4.1 Self Referential Proofs

There are a few places where the proofs rely on an "AndNext" property, i.e. the proof references itself or a previous lemma. I will enumerate the places where I do this and breifly describe why it's safe to do so. While [I believe] I've included the self referential proof steps correctly, the proof would be in better form if I cleaned these up. More coming soon.

2.5 MongoRaftReconfig

This is a work in progress, the current status is:

1. Will has created an inductive invariant candidate
2. Ian is working on proving that the candidate is correct in TLAPS, not much progress has been made so far.
3. Will has proved Peterson's algorithm works without any "manual" proof steps. Ian will try to see if this can be done for MongoRaftReconfig as well.