CAV 2022 Protocol Conversion

Ian Dardik

February 11, 2022

1 Introduction

Converting the *MongoLoglessDynamicRaft* protocol from TLA+ to Ivy was a nontrivial exercise. There are two main bottlenecks that we will cover in this note in the sections below.

The two bottlenecks: quorum overlap property, and staying in EPR (ultimately we just trust IC3PO).

2 Conversion

Converting the *MongoLoglessDynamicRaft* protocol from TLA+ to Ivy was a nontrivial exercise. In particular, working within EPR and describing the *Quorum Overlap* property were the two complications we encountered during conversion. We will begin by describing our solution to these two complications, and then describing the conversion.

The *MongoLoglessDynamicRaft* protocol relies on the *Quorum Overlap* property to safely move to new server configurations. The *Quorum Overlap* property is a relation between two confgurations (sets of servers):

Definition 1. *Given two configurations* $c_1, c_2 \in 2^{Server}$*,* c_1 *and* c_2 *exhibit the Quorum Overlap property iff* $\forall Q_1 \in Quorums(c_1), \forall Q_2 \in Quorums(c_2), \exists x \in Server, x \in Q_1 \wedge x \in Q_2$*.*

Unfortunately, this statement naturally contains a $\forall\exists$ edge from the set 2^{Server} to itself, placing the property outside of Stratified EPR (Padon, et al.). While techniques such as *information hiding* exist for fitting an Ivy specification into EPR, we found these techniques to be nontrivial and we are still working to fit MLDR into EPR. To bypass this difficulty, we leveraged the IC3PO tool, which includes a mechanism for checking inductiveness of a property outside of EPR. Working outside of EPR–and more generally, FAU–allowed us to easily encode a powerset module as well as the Quorum Overlap property.

Once we encoded the Quorum Overlap property as a relation, the translation from TLA+ to Ivy was straightforward.