Verification and Visualization of a Consensus Algorithm using TLA^+

Afonso das Neves Fernandes
Faculty of Sciences, University of Porto

Rolando da Silva Martins
Faculty of Sciences, University of Porto

July 1, 2021

In our work, we used TLA^+ to formalize the consensus algorithm used in Ceph (which is based on Paxos). We found that the formalization was useful to clarify how the algorithm works and to prove its correctness. The specification can be found at: `https://github.com/afonsonf/ceph-consensus-spec`.

We also found that the specification could catch real world bugs of the algorithm. To do this we introduced a bug that was previously present in the algorithm and then evaluate if the model checker would catch it, which was found to be successful.

During the formalization of the algorithm, we developed a visualization tool to help understand the algorithm, its bugs, and how the specification could be improved to make it more efficient. The tool accepts for the visualization both state graphs in the dot format and error traces from TLC. The tool can be found at: `https://github.com/afonsonf/tlaplus-graph-explorer`.

We propose to present our findings on formalizing the algorithm and using the visualization tool. This proposal follows the work done by Afonso Fernandes in his Master thesis (still not published).