A Machine-Checked C Implementation of Dijkstra's Shortest Path Algorithm

Short Paper

Anshuman Mohan and Aquinas Hobor

National University of Singapore
{mohan,hobor}@comp.nus.edu.sg

Abstract. We report on a machine-checked proof of correctness for Dijkstra's one-to-all shortest path algorithm. Unlike previous work, we use classic textbook code written in C. Our C code is executable and realistic but also has real-world complications. We prove full functional correctness, and not just program safety. We show that Dijkstra's algorithm suffers from potential overflow issues. The precise bound is nontrivial: we show that the intuitive guess fails, and provide a workable refinement.

Keywords: Dijkstra · verification · Coq