Title

Bridging the Verifiability Gap: Why We Need More From Our Specs and How We Can Get It

Abstract

Formal methods are an essential ingredient in the development of robust and reliable systems. TLA+ is an invaluable tool for developing distributed systems: facilitating precise specifications, providing a mathematical framework for reasoning about and debugging complex concurrent algorithms, and promoting confidence with system designs based in verifiable specifications. With its powerful language and rich toolset, industry can adopt TLA+ to conserve valuable engineering resources by identifying bugs and eliminate design flaws in the earliest phases of software projects. But humans still play a vital role in the implementation of systems designed and verified with TLA+. Within this framework, even the most carefully devised and thoroughly verified system designs are still prone to human coding errors. The correctness of a system ultimately depends on a programmer's ability to produce a correct implementation that strictly adheres to the specification. This "verifiability gap" that persists between TLA+ specifications and real-world implementations could even play a role in limiting industry's adoption of TLA+ for the development of production-grade systems. This talk will explore ways to bridge that gap to enable the development of more stable and reliable systems with TLA+.

During this talk, Jordan will present an overview of relevant research on using formal methods to verify real-world systems and assess the viability of adapting TLA+ to the system verification use case. The talk will explore a variety of techniques that could be adopted for verifying systems with TLA+ and discuss the advantages and limitations of each. Finally, Jordan will provide an in-depth report on the research done at the Open Networking Foundation (ONF) demonstrating the use of TLA+ for trace checking and conformance monitoring of real-world distributed systems running on Kubernetes. The experience gained and lessons learned at ONF will provide users of TLA+ with a technical foundation from which to explore their own system verification solutions, and contributors will gain practical insights into the challenges and limitations encountered in research at ONF. But most importantly, this talk is being delivered to advance a conversation around bridging the gap the remains between TLA+ specifications and their real-world implementations.