Between Testing and Verification: Software Model Checking via Systematic Testing

Patrice Godefroid

Microsoft Research, pg@microsoft.com

Abstract. Dynamic software model checking consists of adapting model checking into a form of systematic testing that is applicable to industrial-size software. Over the last two decades, dozens of tools following this paradigm have been developed for checking concurrent and data-driven software. Compared to traditional software testing, dynamic software model checking provides better coverage, but is more computationally expensive. Compared to more general forms of program verification like interactive theorem proving, this approach provides more limited verification guarantees, but is cheaper due to its higher level of automation. Dynamic software model checking thus offers an attractive practical trade-off between testing and formal verification.

This talk will review 20 years of research on dynamic software model checking. It will highlight some key milestones, applications, and successes. It will also discuss limitations, disappointments, and future work.