ABSTRACT
Existing techniques for software Model Checking are divided into Predicate Abstraction (PA) with CounterExample Guided Abstraction Refinement (CEGAR) and Lazy Abstraction With Interpolation (LAWI). CEGAR works by over-approximating the program and refining the over-approximation to rule out infeasible counterexamples. On the other hand, LAWI works by under-approximating a program by a finite unrolling and uses interpolation to generalize a bounded safety proof. The two techniques have clear advantages and limitations, but, until now, have not been integrated into a single verification framework.

In this talk, I will present UFO, a framework that unifies CEGAR and LAWI approaches to leverage both of their advantages. UFO is parameterized by the degree to which over- and under-approximations drive the analysis. In addition to combining LAWI and CEGAR in a unified way, UFO makes several key contributions to both LAWI and CEGAR approaches. At one extreme, UFO is a novel interpolation-based algorithm that generates interpolants to refine multiple program paths using a single SMT solver query. At the other extreme, UFO is a novel CEGAR-based algorithm that uses interpolation to lazily strengthen the abstraction.

UFO has been implemented in the LLVM compiler infrastructure, and is publicly available. It has won 4 gold medals at the 2nd International Software Verification Competition (SV-COMP’13) in the ControlFlowInteger, DeviceDrivers64, ProductLines, and SystemC categories.

This is joint work with Aws Albarghouthi and Marsha Chechik from University of Toronto.

BIO
Arie Gurfinkel received a Ph.D. in Computer Science from the Computer Science Department of University of Toronto in 2007. He is currently a Senior Researcher at the Carnegie Mellon Software Engineering Institute and a Research Scientist at the School of Computer Science at Carnegie Mellon University. His research interests lie in the intersection of formal methods and software engineering, with an emphasis on automated reasoning about software systems. He is a lead developer for a number of automated verification tools including a multi-valued model-checker XChek, a software model-checker Yasm. His most recent tool, UFO, developed in collaboration with University of Toronto has won 4 gold medals at the 2nd International Software Verification Competition (SV-COMP’13).