Leveraging Constraint Solvers in Building Reliable Multithreaded Software

Murali Krishna Ramanathan

Indian Institute of Science, Bangalore, India
muralikrishna@csa.iisc.ernet.in
http://drona.csa.iisc.ernet.in/~muralikrishna/

Abstract.   Constraint solvers have been employed successfully in the design of concurrency debugging tools. In this talk, I will share our experience in using them in the context of building thread-safe multithreaded libraries. Detecting concurrency-induced bugs in multithreaded libraries can be challenging due to the intricacies associated with their manifestation. This includes invocation of multiple methods, synthesis of inputs to the methods to reach the failing location, and crafting of thread interleavings that cause the erroneous behavior. Neither fuzzing-based testing techniques nor over-approximate static analyses are well positioned to detect such subtle defects while retaining high accuracy alongside satisfactory coverage.

In this talk, I will present a design of a directed, iterative and scalable testing engine that combines the strengths of static and dynamic analysis to help synthesize concurrent executions to expose complex concurrency-induced bugs. Our engine accepts as input the library, its client (either sequential or concurrent) and a specification of correctness. Then, it iteratively refines the client to generate an execution which can break the input specification. Each iteration step includes statically identifying subgoals towards the goal of failing the specification, generating a plan towards meeting these goals, and merging of the paths traversed dynamically with the plan computed statically via constraint solving to generate a new client. The engine reports full reproduction scenarios, guaranteed to be true, for the bugs it finds. Our evaluation of the prototype tool based on this design resulted in detection of 31 real crashes across 10 classes, including classes from the latest versions of openjdk and google-guava.

This is joint work with Malavika Samak and Omer Tripp.

Biography.   Murali Krishna Ramanathan is an Assistant Professor in CSA at Indian Institute of Science, Bangalore. His research interests broadly span the areas of software engineering, programming languages and scalable system design. Previously, he was affiliated with Coverity and helped build program analysis tools that are widely used in the industry. He received a PhD in Computer Science from Purdue University, USA.