

Model Checking, Program Analysis, and Constraint Databases

Dr. Supratik Mukhopadhyay,
Utah State University

Abstract

Bugs in unverified (software) systems can cause disasters ranging from rebooting a PC to the failure of a space mission. Model checking is an automatic technique for verifying systems in which a desired behavior of a system is verified over the model of the system through exhaustive enumeration of all states reachable by the system and the behaviors that traverse through them. Program analysis refers to the technique(s) of automatically ascertaining information about a program without actually running the program. Constraint databases tightly integrate database and constraint solving methods thereby bridging the gap between efficient, declarative database programming and efficient constraint solving.

We establish connections between the seemingly different fields of model checking for infinite state systems, program analysis and constraint databases. This connection allows us to derive uniformly solutions to a large number of problems in verification of software. In particular, we derive uniformly, symbolic and (in most cases) local algorithms for interprocedural dataflow analysis, points-to analysis, aliasing analysis, automatic checking of array bound violation and other memory errors in C programs as well as automatic verification of safety and liveness properties of embedded software. I will also show how to seamlessly integrate deductive reasoning and abstract interpretation techniques within our methodology. The combined "framework" is used to derive "lightweight" tools for automatically verifying (rather falsifying = finding bugs in) software. I will share my experiences in developing and using a tool based on the described methodology for automatically discovering bugs in C programs. In particular, the framework has been used to discover critical bugs in an NSA-funded secure personal access control system deployed in a nuclear power plant as well as in the popular LEDA package used in industry. This research is partially funded by a grant from the National Science Foundation

Biography

Dr. Supratik Mukhopadhyay is an Assistant Professor in Computer Science at the Utah State University. His research interests lie in the fields of software engineering and programming languages. In these areas, he has received more than \$2 millions in research funding over the past few years from federal agencies like the NSF and the ONR as well as from state agencies and industry. Dr. Mukhopadhyay did his doctoral research at the Max Planck Institute for Computer Science in Germany.