

Robust Software Engineering Research Area
Robust Software Engineering Group

COMPOSITIONAL VERIFICATION

HIGHLIGHT: An overview of the Robust Software Engineering (RSE) group's learning-based assume-guarantee verification techniques was presented at the SPIN 2005 workshop in San Francisco, August 22-24. Tools for assume-guarantee reasoning of models and code were also demonstrated. The workshop paper has been published as: Giannakopoulou, D. and Pasareanu, C.S. "Learning-Based Assume-Guarantee Verification." In Proceedings of the 12th International SPIN Workshop on Model Checking of Software, San Francisco, USA, August 2005, LNCS 3639.

RSE researchers have also demonstrated the applicability of their tools and techniques in two NASA test scenarios:

- . Compositional verification techniques captured requirements of the International Space Station related to redundancy management and attitude control handover between the United States and Russian sides. The tools automatically detected two problems that resulted in software change requests, and produced scenarios demonstrating how the problems occurred. Assumption generation techniques were used to suggest a patch for fixing one of problems.

- . Compositional verification achieved 100x savings in memory and 10x savings in time to complete the verification of the MER arbiter (a flight software module from JPL's Mars Exploration Rovers) in the SPIN model checker, as compared to exhaustive verification through model checking with non-compositional algorithms.

BACKGROUND: A key step in achieving scalability in the verification of large software systems is to "divide and conquer"; that is, to break up the verification of a system into smaller tasks that

involve the verification of its components. Assume-guarantee reasoning is a widespread divide-and-conquer approach that uses assumptions as it checks individual components of a system. Assumptions essentially encode expectations that each component has from the rest the system in order to operate correctly. Coming up with the right assumptions is typically a non-trivial manual process, which limits the applicability of this type of reasoning in practice.

Over the last few years, the RSE group has developed a collection of techniques and a supporting toolset for performing assume-guarantee reasoning of software in an automated fashion. The techniques are applicable both at the level of design models and at the level of actual source code. Assumptions are computed automatically, using two main approaches: the first, which received an ACM distinguished paper award in 2002, computes the assumption based on the specification of the component and a required property; the second learns the assumption through queries and counterexamples.

PROGRAM FUNDING: ISS: Exploration Systems Mission Directorate - Software, Intelligent Systems and Modeling (SISM) Program (legacy funding); MER Arbiter: Exploration Systems Mission Directorate - Software, Intelligent Systems and Modeling (SISM) Program Reliable Software Systems Development ICP

POC: Dimitra Giannakopoulou, dimitra@riacs.edu