Andrew Healy

MSc (by Research) in Computer Science
Supervisors: Dr. James F. Power & Dr. Rosemary Monahan
Principles of Programming Research Group

Title: Implementing a portfolio-solving tactic for Why3

This talk will start by describing recent work in characterising the workload of two SMT (Satisfiability Modulo Theory) solvers Z3 & CVC4. Given a large benchmark suite of programs from various SMT application domains (scheduling, hardware verification, cryptology, etc.), we profiled the dynamic executions of these programs and compared the results to those obtained from a smaller suite of programs specifically designed to test prover capabilities in the software verification domain. Our experimental results showed significant differences in how the two SMT solvers handled verification tasks.

Current work expands on this empirical study by taking the verification status in account (valid, invalid, timeout, etc.) to implement a portfolio-solving tactic for the Why3 verification system. Such a tactic is designed to predict the best-performing prover for the specific verification problem. Recent research has claimed success in applying machine-learning techniques to this problem: by deriving static software metrics, the best-performing prover can be chosen by systems based on Interactive Theorem Provers (ITPs) and Automatic Theorem Provers (ATPs). However, the diversity of input languages and formats for deductive verification using SMT solvers necessitates a new set of verification-based metrics. A series of experiments will investigate if the common input format that the Why3 system provides can be utilised for this purpose.

This material is based on works carried out with funding provided by the Science Foundation Ireland under grant number 11/RFP.1/CMS/3068.