INFORMATIK-KOLLOQUIUM
AB Programmiersprachen und Übersetzer
Institut für Computersprachen

computer
languages

Einladung

zum Informatik-Kolloquium des
AB Programmiersprachen und Übersetzer am
Mittwoch, den 4. Feber 2009, um 16:30 Uhr
in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte)

Es spricht

Mădălina Eraşcu, M.Sc.
RISC-Linz, Johannes Kepler University, Linz, Austria

über

Forward Symbolic Execution for Program Verification in *Theorema* System

Abstract: We present a static analysis method for imperative program verification based on forward symbolic execution; given the Hoare triple (Input Specification, Program Body, Output Specification), we want to check whether the program fulfils its specification. The problem of generating the verification conditions is approached using an axiomatic calculus characterizing inference rules for each statement encountered in the program: assignments (including recursive calls), conditionals and abrupt statements (/textttReturn). `While` loops can be simulated using conditionals and recursion. Detailed theoretical aspects of this method are stated in a recent article presented at the 2008 Austrian-Japan Workshop on Symbolic Computation in Software Science. The method is implemented in a prototype framework on top of the computer algebra system Mathematica and uses the existing Theorema imperative language. Our goal is to automatically prove/disprove the verification conditions generated using logical, algebraic and combinatorial techniques. At this aim, we combined logical (natural deduction) and simple algebraic inferences for preprocessing the verification conditions. For further reasoning about the resulting formulae, we will use polynomial algebra algorithms which might (e.g. Cylindrical Algebraic CAD Decomposition works on the theory of real closed fields) or might not (e.g. Groebner basis algorithms works on a commutative ring with 1) need to set an underlying theory. Although CAD method is powerful enough for handling our formulae, it has a high complexity and therefore we avoid to use it until the latest. We will define classes of verification conditions which can be handled by other means and, if possible, hold also in weaker theories than reals.

This is joint work with Tudor Jebelean.

Biography: Mădălina Eraşcu is a 1st year PhD student in the Theorema research group (leader: Bruno Buchberger) at the Research Institute for Symbolic Computation (RISC), Johannes Kepler University of Linz, Austria. She is interested in program analysis using formal methods, computer algebra and automated theorem proving. She holds a M.Sc. from Johannes Kepler University (International School for Informatics), Linz. (`http://www.risc.uni-linz.ac.at/home/merascu`)

Zu diesem Vortrag lädt der *Arbeitsbereich für Programmiersprachen und Übersetzer am Institut für Computersprachen* herzlich ein.
Tee: 16:15 Uhr in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte).