INFORMATIK-KOLLOQUIUM
AB Programmiersprachen und Übersetzer
Institut für Computersprachen

Einladung

zum Informatik-Kolloquium des
AB Programmiersprachen und Übersetzer am
Dienstag, den 4. September 2012, um 15 Uhr c.t.
in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte)

Es spricht

Dr. Xavier Rival

INRIA Roquencourt / Ecole Normale Supérieure (ENS Paris), Frankreich

über

MemCAD, a Modular Abstract Domain for Reasoning on Memory States

In this talk, we will present the MemCAD analyzer, which relies on a parametric abstract domain for the static analysis by abstract interpretation of programs which manipulate complex and dynamically allocated data-structures. We will set up the foundations for a family of static analyses to compute an over-approximation of the reachable states of programs using such structures, using modular abstractions, which can be adapted to wide families of programs.

Our domain can be parameterized with a set of inductive definitions capturing a set of relevant data-structures and by the choice of an underlying numerical domain. Abstract values can be viewed either as graphs, or as formulas in a subset of separation logic extended with inductive definitions. We will describe the abstraction induced by this domain, and the main static analysis operators. In particular, we will consider the unfolding operator, which allows to refine in a local manner an abstract value, so as to allow precise algorithms for the computation of post-conditions. Then, we will discuss a set of join and widening operators, so as to guarantee the termination of our static analyses.

In the second part of the talk, we will consider several applications of our static analysis. We will show how it can be adapted in order to treat in a precise way specific features of programs written in languages which allow low level memory operations, such as the C language. Then, we will focus on the analysis of programs with recursive procedures and we will introduce a powerful widening operator, which is able to infer accurate inductive definitions to be used to summarize the call-stack of a specific program together with the memory.

Finally, the last part of this talk will focus on recent work to extend the analysis to embedded softwares, which use a custom allocation inside static blocks, and manages their own dynamic structures inside this scope. The reason for this programming pattern is that dynamic memory allocation should not be used in highly critical avionic softwares. It brings new issues for the verification of software by static analysis, which can be addressed using our modular abstraction.

Biography: Xavier Rival studied at Ecole Normale Supérieure (Paris) and obtained his PhD in 2005 from Ecole Polytechnique. He worked as a Post-doctorate researcher at the University of California at Berkeley. He joined INRIA as a Junior Research Scientist in 2007 and he has been a member of the Abstraction group joint with Ecole Normale Supérieure (Paris) and CNRS. He holds a Lecturer position at Ecole Polytechnique since 2009. His main research topic is static analysis of safety critical programs using abstract interpretation techniques, and he took part to the design and implementation of the Astree static analyzer. He also worked on certified compilation. More recently, he started working on static analyses for the verification of memory properties of programs that manipulate complex data-structures. (`http://www.di.ens.fr/~rival/`)

Zu diesem Vortrag lädt der *Arbeitsbereich für Programmiersprachen und Übersetzer am Institut für Computersprachen* herzlich ein.
Tee: 14:30 Uhr in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte).