Informatik-Oberseminar

Fachgruppe Informatik

Lehrstuhl für Informatik 11

RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

EINLADUNG

Zeit: 04.06.2008, 10.00 Uhr

Ort: AH III, Ahornstr. 55

Referent: Diplom-Informatiker Bastian Schlich
RWTH Aachen University

Titel: Model Checking of Software for Microcontrollers

Abstract:

Software for microcontrollers is getting more and more complex. It is mandatory to extensively analyze their software as errors can lead to severe failures or cause high costs. Model checking is a formal method used to verify whether a system satisfies certain properties. In this talk, a new approach for model checking software for microcontrollers is described, which model checks assembly code instead of an intermediate representation such as C code.

The development of [mc]square, which is a microcontroller assembly code model checker implementing this approach, is detailed. The creation of states is performed by a specific simulator, which is the only hardware-dependent component of [mc]square. Within the simulator, several microcontrollers are modeled accurately.

The presentation describes the modeling of the ATMEL ATmega16 microcontroller and details implemented abstraction techniques, which are used to tackle the state-explosion problem. These abstraction techniques include lazy interrupt evaluation, lazy stack evaluation, delayed nondeterminism, dead variable reduction, and path reduction. Delayed nondeterminism introduces symbolic states, which represent a set of states, into [mc]square while still explicit model checking techniques are used.

Es laden ein: Die Dozenten der Informatik