Informatik-Kolloquium

Rheinisch-Westfälische Technische Hochschule Aachen
Lehrstuhl für Informatik II

EINLADUNG

Zeit: Donnerstag, 07. Okt. 1999, 17.00 Uhr
Ort: Raum AH II, Ahornstr.55 (ehem. PH)
Referent: Gerald Luettgen
Institute for Computer Applications in Science and Engineering (ICASE) NASA Langley Research Center Hamtpon, Virginia
Thema: A Semantic Foundation for Heterogeneous Specification Formalisms

Abstract:

Research in the specification and verification of concurrent systems falls into two general categories, the assertional approach and the operational approach. The temporal logic school advocates the assertional approach which employs temporal-logic formulas for system specification, with the semantics of the logic being used as the basis for determining whether or not a system is correct. In contrast, a large part of the process algebra school favors the operational approach. This approach focuses on using a state-machine semantics of process terms as the basis for relating system specifications and implementations via behavioral equivalences and preorders.

In this talk, I present ongoing research by Rance Cleaveland, SUNY at Stony Brook, and myself on the development of a semantic foundation for a heterogeneous specification formalism permitting mixtures of assertional and operational specification styles. The benefits of such a mixed specification formalism are manifold, since it supports the following:

(1) capture of system correctness via refinement, i.e., it enables a sound, gradual transition from abstract, assertional system requirements to concrete, operational system designs;

(2) definition of systems in which some components are or remain only specified as temporal-logic formulas, e.g., when dealing with off-the-shelf components;

(3) consideration of constraints, including fairness constraints, which are imposed by a system's environment or which are known to be true of specific system components.

Technically, we are concerned with assertional specifications using linear-time logics (LTL) and operational specifications using labeled transition systems. Our semantic framework is founded on Buechi automata, which we equip with a behavioral relation based on DeNicola/Hennessy must-testing preorder. We show that this preorder is a conservative extension of the classical must-preorder and that it is "compatible" to the LTL satisfaction relation, i.e., LTL model chekking becomes a special case of preorder checking.

Es laden ein: Die Dozenten der Informatik