

Modul “Kombination von Spezifikationstechniken”

Ziel

Die Lehrveranstaltung bietet eine Einführung in die Spezifikationssprachen Z für Daten, CSP für Prozesse und deren objekt-orientierte Kombination CSP-OZ für reaktive Systeme mit Daten- und Prozessanteilen. Es werden folgende Kenntnisse, Fertigkeiten und Kompetenzen vermittelt:

- Kenntnisse:
Spezifikation von komplexen Daten und Operationen in Z, Typdefinitionen und Schemakalkül von Z, Datenverfeinerung;
Spezifikation von kommunizierenden Prozessen in CSP, operationelle Semantik von CSP, drei abstrakte semantische Modelle für CSP: Trace-Semantik, Failures-Semantik, Failures-Divergences-Semantik, Prozessverfeinerung in diesen Semantiken, FDR Model-Checker für CSP;
kombinierte Spezifikationsmethode CSP-OZ, transformationelle Semantik als CSP-Prozess, Sätze über Verfeinerungen, objekt-orientierte Konzepte von Klassen und Vererbung in CSP-OZ
- Fertigkeiten:
formale Spezifikation von Daten und Prozessen mit Z, CSP und CSP-OZ,
formale Überprüfung von Datenverfeinerungsbeziehungen,
Verifikation von CSP-OZ Spezifikationen mit dem FDR Model-Checker
- Kompetenzen:
Fähigkeit, komplementäre Spezifikationsmethoden zu integrieren

Inhalt

Die Vorlesung greift einen aktuellen Forschungstrend im Bereich der formalen Methoden auf, die Kombination und Integration verschiedener Spezifikationstechniken. Im Vordergrund steht eine konkrete Kombination CSP-OZ der Spezifikationstechniken CSP (Communicating Sequential Processes) für Prozesse und Z bzw. Object-Z für Daten. CSP-OZ ist zur Beschreibung von reaktiven Systemen gedacht.

Zur Vorbereitung werden zunächst die Spezifikationssprachen Z und CSP erklärt. Dann wird die Kombination CSP-OZ mit ihrer prozessorientierten Semantik eingeführt. Es werden die Konzepte der Verfeinerung und Vererbung sowie die Möglichkeit einer automatischen Verifikation einer Teilsprache von CSP-OZ mit dem FDR Model-Checker für CSP diskutiert. Abschließend werden Erweiterungsmöglichkeiten von CSP-OZ zur Spezifikation zeitkritischer Systeme angesprochen, deren Verifikation zur Zeit in der Abteilung erforscht werden.

In den Übungen werden die Inhalte der Vorlesung durch Beispiele vertieft. Insbesondere wird der FDR Model-Checker für CSP erprobt.

Literatur

J. Woodcock and J. Davies. *Using Z – Specification, Refinement, and Proof*. Prentice Hall, 1996 (siehe <http://www.usingz.com>).

A.W. Roscoe. *The Theory and Practice of Concurrency*. Prentice Hall, 1998.

Formal Systems Ltd. *Failures-Divergence Refinement*. FDR2 User Manual, 2003.

C. Fischer. *CSP-OZ: A Combination of Object-Z and CSP*. In H. Bowmann, J. Derrick (Editors). *Formal Methods for Open Object-Based Distributed Systems* (Chapman & Hall, 1997) 423–438.

E.-R. Olderog. *Kombination von Spezifikationstechniken*. Vorlesungsskript Sommersemester 2005, Universität Oldenburg, 2005.