Elektronische Prüfungsarbeiten


Analyzing Java in Isabelle/HOL
– Formalization, Type Safety and Hoare Logic –
David von Oheimb

Titel der Arbeit:
Analyzing Java in Isabelle/HOL

Originaluntertitel:
Formalization, Type Safety and Hoare Logic

Übersetzter Titel:
Analyse von Java in Isabelle/HOL

Übersetzter Untertitel:
Formalisierung, Typsicherheit und Hoare-Logik

Autor:
von Oheimb, David

Jahr:
2001

Dokumenttyp:
Dissertation

Institution:
Fakultät für Informatik

Betreuer:
Nipkow, Tobias (Prof. Ph.D.)

Gutachter:
Poetzsch-Heffter, Arnd (Prof. Dr.)

Format:
Text

Sprache:
en

Fachgebiet:
DAT Datenverarbeitung, Informatik

Stichworte:
Java; formalization; operational semantics; type soundness; axiomatic semantics; Isabelle/HOL

SWD Schlagworte:
Java ; Isabelle ; HOL

TU-Systematik:
DAT 362d

Kurzfassung:
This thesis deals with machine-checking a large sublanguage of sequential Java, covering nearly all features, in particular the object-oriented ones. It shows that embedding such a language in a theorem prover and deducing practically important

properties is meanwhile possible and explains in detail how this can be achieved. We formalize the abstract syntax, and the static semantics including the type system and well-formedness conditions, as well as an operational (evaluation) semantics of the language. Based on these definitions, we can express soundness of the type system, an important design goal claimed to be reached by the designers of Java, and prove that type safety holds indeed. Moreover, we give an axiomatic semantics of partial correctness for both statements and (side-effecting) expressions. We prove the soundness of this semantics relative to the operational semantics, and even prove completeness. We further give a small but instructive application example. A direct outcome of this work is the confirmation that the design and specification of Java (or at least the subset considered) is reasonable, yet some omissions in the language specification and possibilities for generalizing the design can be pointed out. The second main contribution is a sound and complete Hoare logic, where the soundness proof for our Hoare logic gives new insights into the role of type safety. To our knowledge, this logic is the first one for an object-oriented language that has been proved complete. By-products of this work are a new general technique for handling side-effecting expressions and their results, the discovery of the strongest possible rule of consequence, and a new rule for flexible handling of mutual recursion. All definitions and proofs have been done fully formally with the interactive theorem prover Isabelle/HOL, representing one of its major applications. This approach guarantees not only rigorous definitions, but also gives maximal confidence in the results obtained. Thus this thesis demonstrates that machine-checking the design of an important non-trivial programming language and conducting meta-theory on it entirely within a theorem proving system has become a reality.

Übersetzte Kurzfassung:

Diese Dissertation behandelt die maschinelle Analyse des (fast vollständigen) sequentiellen Teils der objektorientierten Programmiersprache Java. Wir zeigen, dass die Einbettung einer solchen Sprache in einen Theorembeweiser, in diesem Fall Isabelle/HOL, und der Beweis wichtiger metatheoretischer Eigenschaften inzwischen gut möglich ist. Dazu beschreiben wir detailliert die Formalisierung mit Abstrakter Syntax, Typsystem und der Operationellen Semantik sowie ein Anwendungsbeispiel, geben einen Beweis der Typsicherheit, entwickeln eine Axiomatische Semantik und beweisen deren Korrektheit und Vollständigkeit.

Veröffentlichung:

Universitätsbibliothek der TU München

WWW:

http://mediatum.ub.tum.de/?id=601694

Abgegeben am:

30.11.2000

Mündliche Prüfung:

09.02.2001

Dateigröße:

1179370 bytes

Seiten:

190

Urn:

http://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:91-diss2001020916796

Letzte Änderung:

02.04.2008

Occurences:

- Einrichtungen > Fakultäten > Fakultät für Informatik > Prüfungsarbeiten > Dissertationen
- Elektronische Prüfungsarbeiten > Fachgebiet > Datenverarbeitung, Informatik
- Elektronische Prüfungsarbeiten > Fakultät > Fakultät für Informatik

Entries: