DISS. ETH NO. 20126

Automatic Verification of Heap Structures with Stereotypes

A dissertation submitted to
ETH Zurich

for the degree of
Doctor of Sciences

presented by
Arsenii Rudich
Master of Computer Science

born May 14, 1982
citizen of Ukraine

accepted on the recommendation of

Prof. Dr. Peter Müller, examiner
Prof. Dr. David Basin, co-examiner
Prof. Dr. Anindya Banerjee, co-examiner

2011

Abstract

This thesis is dedicated to the automatic and formal verification of the heap properties of object oriented programs. Program verification is the check that a given program satisfies given properties. Program verification is called formal if both the semantics of the specifications and the program execution are defined formally as mathematical entities. The verification is called automatic if it is performed automatically without interaction or with limited interaction with a user.

Our approach is targeted towards the verification of the preservation of heap-topological properties. It is also aimed towards the verification of the effects and the frame properties of the program statements.

Automatic verification of heap structures is crucial for the verification of multi-object invariants, the verification of concurrent programs (e.g., absence of race conditions and deadlocks), software engineering (e.g., enabling encapsulation and modular development, handling design patterns), and the verification of security properties (e.g., isolation).

We present a novel approach to the verification of heap structures. Our approach is based on the notion of *stereotypes*. The aim behind a stereotype is to collect in one entity all reusable specifications which are relevant to the heap structure. Stereotypes provide, amongst other information, approximations of the transitive closures of relevant fields; information which is not generally available in a first-order logic. These approximations enable the verification of heap properties in automatic fist order logic theorem provers. The usage of our stereotype based approach has advantages such as reduction of the specification overhead, prevention of specification duplication, the prevention of proof duplication, and the improvement of the readability of the specifications.

To evaluate the stereotype based approach we have specified and verified several design patterns and data structures. All examples are verified in the verification language Boogie. One of the verified examples is the Priority Inheritance Protocol. According to our knowledge it is the first automatic verification of the Priority Inheritance Protocol.

Zusammenfassung

Diese Doktorarbeit ist der automatischen formalen Verifikation von Heap-Eigenschaften objektorientierter Programme gewidmet. Programm-Verifikation ist die Überprüfung, dass ein bestimmtes Programm gegebenen Eigenschaften erfüllt. Programm-Verifikation ist formal, wenn die Semantik der Spezifikation wie auch der Programm-Ausführung mathematisch definiert ist. Die Überprüfung wird als automatisch bezeichnet, wenn sie ohne oder mit begrenzter Interaktion durch einem Benutzer durchgeführt wird.

Unser Ansatz ist auf die Überprüfung der Erhaltung topologischer Heap-Eigenschaften ausgerichtet. Auch die Prüfung von Frame-Conditions ist Ziel dieser Arbeit.

Automatische Überprüfung von Heap-Strukturen ist entscheidend für die Überprüfung eines Verbundes von Objekt-Invarianten, die Überprüfung nebenläufiger Programme (z.B. Fehlen von Race-Conditions und Deadlocks), Software-Engineering Aspekte (z. B. Kapselung, Modularität, Handhabung von Design Patterns), und die Überprüfung Sicherheit-Eigenschaften (z. B. Isolation).

Wir präsentieren einen neuartigen Ansatz zur Überprüfung von Heap-Strukturen. Unser Ansatz basiert auf der Idee von Stereotypen. Das Ziel eines Stereotyps ist, alle wiederverwendbaren Spezifikationen, für die Heap-Struktur zusammenzufassen. Dazu gehören unter anderem die Stereotypen-Annäherungen an die transitive Hülle von entsprechenden Felder in First-Order Logik. Diese Näherungen ermöglichen die Überprüfung von Heap-Eigenschaften mittels automatischer First-Order Logik Theorembeweisern. Die Nutzung unseres Stereotyp Ansatzes bietet Vorteile wie Reduzierung des Spezifikations-Overhead, Vermeidung von doppelter Spezifikationen, Verhinderung von Beweis Vervielfältigung und Verbesserung der Lesbarkeit der Spezifikationen.

Zur Beurteilung der Stereotyp Ansatz haben wir mehrere Design-Patterns und Datenstrukturen spezifiziert und verifiziert. Alle Beispiele sind in der Verifikationssprache Boogie überprüft. Eines der überprüften Beispiele ist das Priority Inheritance Protocol. Nach unserer Kenntnis handelt es sich um die erste automatische Überprüfung dieses Protokolls.