Termination Analysis for Bit-Vector Programs

DISS. ETH NO. 19589

Termination Analysis for Bit-Vector Programs

A dissertation submitted to

ETH ZURICH

for the degree of

Doctor of Sciences (Dr. sc. ETH Zurich)

presented by

Christoph Michael Wintersteiger

Dipl.-Ing., Johannes Kepler Universität Linz, Österreich

Date of birth

May 15, 1979

citizen of Austria

accepted on the recommendation of

Prof. Dr. David Basin
Prof. Dr. Daniel Kröning
Dr. Leonardo de Moura

2011

Abstract

Recent advances in software termination analysis have shown that program termination can be decided efficiently for many practically relevant problems, despite the fact that the Halting Problem in general is undecidable. This dissertation presents a new algorithm for termination analysis, called *Compositional Termination Analysis*, which is based on compositional (or transitive) transition invariants. This algorithm depends on an underlying ranking relation synthesis engine and this dissertation presents two such engines that are able to synthesize Bit-Vector ranking relations. This class of ranking relations is especially important for verification of embedded software or for software that interacts with hardware, like device drivers.

Furthermore, a method for certification of decision procedures for quantified Boolean formulae (QBF) is presented; a requirement for one of the ranking relation synthesis methods and many other applications of QBF. Since decision procedures for QBF face performance problems in practice, an alternative and richer logic (quantified Bit-Vector logic with uninterpreted functions) is proposed. This logic enables decision procedures to be more efficient for many practically relevant formulas and at the same time it enables a more convenient and efficient translation of verification and synthesis problems to the input of the decision procedure.

All of the methods described in this dissertation are compared in a substantial experimental evaluation which clearly demonstrates the advantages in runtime or precision of the new methods over existing techniques.

Zusammenfassung

Im Gebiet der Terminierungsanalyse für Software gab es in den letzten Jahren große Fortschritte auf vielen praktisch relevanten Problemen, trotz der Unentscheidbarkeit des Halteproblems im generellen Fall. Diese Dissertation präsentiert einen neuen Algorithmus für Terminierungsanalyse, genannt *Compositional Termination Analysis*, welcher auf compositional (transitiven) Transitionsinvarianten basiert. Dieser Algorithmus hängt von einem externen Algorithmus zur Synthese von Rank-Relationen ab und zwei solche Algorithmen werden vorgestellt. Diese Algorithmen synthetisieren Rank-Relationen für Programme mit Bit-Vector Variablen, einer Klasse von Programmen die besonders im Bereich der Verifikation von embedded und hardware-nahen Software, wie etwa Gerätetreibern, von großer Bedeutung ist.

Des weiteren wird eine Methode zur Zertifizierung von Entscheidungsprozeduren für quantifizierte Boole'sche Formeln (QBF) präsentiert; eine Voraussetzung für eine der Synthesemethoden für Rank-Relationen und viele andere QBF-Anwendungen. Da Entscheidungsprozeduren für QBF in der Praxis Performanceprobleme aufweisen wird eine alternative Logik (quantifizierte Bitvektor-Logik mit uninterpretierten Funktionen) vorgeschlagen. Diese Logik erlaubt effizientere Entscheidungsprozeduren für viele praktisch relevante Probleme, während die Übersetzung von Verifikations- und Syntheseproblemen zur Eingabe der Entscheidungsprozedur vereinfacht wird.

Alle Methoden die in dieser Dissertation beschrieben werden, wurden einer umfangreichen experimentellen Evaluierung unterzogen, welche die Laufzeit- oder Präzisionsvorteile der neuen über vergleichbare existierende Techniken klar aufzeigt.