平成 29 年度

修士学位論文

最大充足化ソルバを用いた誤り位置特定手法の近似解法の研究

Study on approximation algorithms of an error localization method using a Max-SAT solver

1205089　　米田裕司

指導教員　　高田喜朗

2018 年 2 月 28 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報システム工学コース

要 旨

最大充足化ソルバを用いた誤り位置特定手法の近似解法の研究

米田裕司

年々，ソフトウェアにはより高度な機能が求められ, プログラムは複雑化している．それに伴いプログラムに潜在する誤りを発見するのが困難になっている．また, ソフトウェアのバグを取り除くのに開発工程のうち多くの時間が費やされており, ソフトウェアの生産性に大きな影響を与えている．

そのため, 誤りを検出する方法としてモデル検査やデータフロー解析などの静的解析手法が研究されてきた．近年, 高速な SAT ソルバ (充足可能性判定器) の開発が進み，プログラムを表す論理式と仕様を表す論理式を生成することでプログラムの正当性を SAT 問題（充足可能性問題）に帰着させ SAT ソルバで検査する有界モデル検査法が知られるようになった．有界モデル検査も含め, 通常のモデル検査法は, エラー箇所及びその箇所までの実行系列を出力する．しかし, エラーの原因となる箇所は通常その実行系列の中のごく一部であり, 誤りを修正するためには利用者が実行系列の中のエラー原因を探さなければいけないという問題がある．

その問題に対して, Jose らは，充足可能性問題の拡張である最大充足化問題に対するソルバを使って, エラー箇所までの実行系列のうち修正するべきプログラム中の誤り位置の候補を特定する手法を提案した．この手法は, 有界モデル検査と同じ手法で命令列を表す論理式を作り, 潜在的な誤りの位置の検出をプログラムの仕様を満たしつつ命令列に対応する論理式をできるだけ満たすという最大充足化問題に帰着させて Max-SAT ソルバ（最大充足化ソルバ）で解くものである．

しかし，最大充足化問題を厳密に解くアルゴリズムは時間計算量が大きく，大きなソフト

ウェアの誤り位置を特定することは難しい.

そこで本研究では，最大充足化問題の近似解法をこの問題に適用することで高速に誤り位置の候補を特定する手法を提案し, 精度を既存手法と比較する.

キーワード　誤り位置特定, 静的解析, モデル検査, SAT ソルバ, Max-SAT ソルバ

Abstract

Study on approximation algorithms of an error localization method using a Max-SAT solver

Yuji YONEDA

More advanced functions are required for software year by year, software is becoming complicated. Accordingly, it is becoming difficult to find potential errors in programs. In recent years, satisfiability solvers, or SAT-solvers, have been actively developed, and high speed SAT-solvers have become available. The bounded model checking (BMC) is a well-known application of SAT-solvers to software verification. It is done by reducing correctness of programs to a satisfiability problem.

When a given program has an error, model checking tools provide the execution path to the location where an assertion fails. However, usually the real error of that program is in a little part of that execution path, and users have to search for the real error location by the themselves.

Jose et al. proposed a method for locating errors in programs, using a Max-SAT solvers, which is an extension of SAT-solvers. This method reduces error location of programs to a Max-SAT problem. This is done by generating logical expressions representing instruction sequences in the same way as the BMC. However, it is time-consuming to strictly solve the Max-SAT problem, and it difficult to identify the error location of a large software by this method. In this research, we propose a method for quickly identifying error location candidates, by applying approximation algorithms of Max-SAT problems. And then, we compare its accuracy with existing methods.

key words Fault localization, Static analysys, Model Checking, SAT Solver, Max-SAT Solver