要 旨

シェープ解析を利用した動的データ構造に適した静的解析ツールの構築に関する研究

水野 雄介

近年, ソフトウェアの開発作業においてプログラムが複雑化するにつれて, ソフトウェア製品に潜在する問題を発見することが困難になっている. 潜在的な不具合の検出を支援する手法の一つに静的解析がある.

静的解析とは, プログラムを実行せず, ソースコードの意味上の誤りを解析して不具合部分を発見したり, あるいは改善に役に立つ情報を提供したりすることをいう. 静的解析ツールの一つに AdLint と呼ばれるオープンソースのソフトウェアがある. AdLint は, ソースコードを解析し, 潜在的に不具合となり得る箇所について数多くの警告を出力する. この解析ツールを活用することでコードレビュープロセスの大部分を自動化することが可能になる. しかし, AdLint ではポインタに対する解析が正確ではない. この問題を改良するためにはポインタが指しうる要素についてより詳細に解析する必要がある.

ポインタが指しうる要素を詳細に解析する手法の一つとして, シェープ解析が提案されている. シェープ解析では, 従来のポインタ解析手法とは異なり, ポインタが指しうる要素を一つに要約することなく解析することで, より正確に解析することができる.

本研究では, シェープ解析法を用いて AdLint のポインタに対する解析結果をより正確で有益な情報に変更する.

キーワード　シェープ解析, AdLint, 動的データ構造, TVLA, COINS

Abstract

Development of a static analysis tool using shape analysis suitable for dynamic data structures

Yusuke Mizuno

In recent years, software has become complicated and it has become difficult to discover a potential problem in a software product. Static analysis is one of the techniques to support the detection of the potential problem in a program.

Static analysis detects semantic errors in a source code without executing the code, or it outputs information that is useful for improving the code. AdLint is one of the open-source static analysis tools. Analyzing a source code, AdLint outputs a lot of warnings about potential bugs. This analysis tool can automate most of the code review process. However, AdLint is not accurate at the pointer analysis, and it outputs many false warnings. In dealing with this problem, it is necessary to analyze the element to which a pointer may point.

The shape analysis has been proposed as one of such techniques. The shape analysis provides more accurate analysis than usual pointer analysis, by avoiding summarizing the potential elements to which a pointer may point as a single element.

In this study, we propose a method for improving the analysis result of AdLint about pointers by means of the shape analysis.

key words shape analysis, AdLint, dynamic data structure, TVLA, COINS,