ISS-P-55

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†　　高田　喜朗†
† 高知工科大学工学研究科

1. はじめに

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[2]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．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，Sagiv らによってシェープ解析[1]が提案されている．

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．

2. AdLint

AdLint は C 言語を対象としたオープンソースの静的解析ツールである．解析は，ソースコードの行単位で行い，各行で起こりうる不具合に関する警告を出力する．ポインタに関する警告では，意図しないアドレスを使用する可能性が高いポインタ型の変数に対する算術演算や，Null になりうるポインタに対する参照を検出して出力する．

3. シェープ解析

シェープ解析は,ポインタを解析する手法の一つであり,連結リストや木構造に関してプログラム実行中に現れる構造を求める手法である.シェープ解析では,ポインタが指しうる要素を一つに要約することなく,指す・指されるの関係が同一のもののみを要約することで,既存の解析手法よりも詳細な情報を提供する．

Sagiv らが提案しているシェープ解析では，要約された要素を必要に応じて複数の要素に分解する処理を加えることで,より正確な解析を可能としている．

本研究ではこのシェープ解析法を実装している既存解析ツール[3]を利用する．この解析ツールでは,ポインタが指しうる要素の状態を表す「述語」と，代入文，比較文などによる述語の解釈の変化を表す関数を用いて解析対象を表し，それらに対して解析を行う．

4. 提案システムの概要

本システムの構成を図 1 に示す．点線で囲まれている箇所は既存ツールを使用し，実線で囲まれている箇所が今回作成したものである．

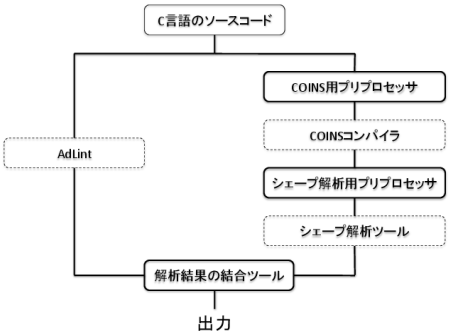

図1. システム全体の概要図

5. 評価

本システムの評価のために，リストの要素の追加・削除・表示を行う C プログラムに対して解析を行った．AdLint では，「値が NULL になることがあるポインタに対して間接参照が行われています．」と警告した箇所が 20 個存在した．本システムでは，その警告の内 11 個が実際のプログラム上では NULL にならないと解析した．一方，実際には NULL にならないにも関わらず本システムで警告を削除できなかった箇所は，5 箇所存在した．また，4 つの関数のポインタ引数が NULL にならないことも出力した．

16 個の誤警告の内 11 個を削除できたこと等より，本システムはある程度有用であると考える．

6. まとめ

本研究では,コンパイラ等では検出できない潜在的な不具合を解析することを目的として,無償で提供されている AdLint とシェープ解析の二つのツールを活用して動的データ構造に適した静的解析ツールを提案した．

参考文献

[1] M.Sagiv et al. Parametric Shape Analysis via 3-Valued Logic, ACM TOPLAS Vol.24, No.3, pp.217-298, May 2002.
[2] オープンソースの静的解析ツール AdLint, http://www.ogis-ri.co.jp/product/1199335_6798.html/.
[3] TVLA Home Page, http://www.cs.tau.ac.il/~tvla/.