卒業論文

タイトル

08-222021　長谷川 慧

指導教員　森畑明昌 准教授

2024 年 1 月

東京大学教養学部学際科学科総合情報学コース

概要

ここに概要を書く.

目次

第 1 章

はじめに

プログラム検証とは、プログラムの正しさを (半) 自動的に証明する試みのことである。具体的には、プログラムとその仕様を入力として受け取り、そのプログラムが仕様を満たしているかどうかを判定し、仮に仕様を満たしていなければ反例とともに結果を出力する。

検証を行うにあたって、通常はプログラムの不変条件を発見することが重要となる。不変条件とは、プログラムの実行を通して常に成り立つ性質のことであり、プログラム中の変数に関する述語として表される。例えば、

関係的検証とは、複数のプログラムの関係という形で表される仕様 (関係的検証) を検証するプログラム検証の一分野である。通常の検証と比較すると、プログラムと仕様を受け取ってプログラムが仕様を満たすかどうかを判定する点は共通しているが、対象とするプログラムが複数であり、仕様がそれらの関係という形で表される点が異なる。関係的検証においても不変条件を発見することが鍵となるが、一般に関係的検証問題を解くのに役立つ不変条件は複数のプログラムの変数に関する述語となるので、探索空間が比較的大きくなる傾向があるところに難しさがある。

関係的検証のアプローチとしては、

Unno らは、既存の CHC(制約つきホーン節) を用いた制約ベースのアプローチを拡張し、不変条件以外にいくつかの unpredicated な述語を追加することで、従来の手法では解くことが難しかった関係的仕様の検証に成功した。この研究の artifact である PCSAT は、プログラムを不変条件といくつかの unpredicated な述語が含まれる制約式に変換し、それを SAT ソルバに入力することで検証を行う。

PCSAT を用いた検証や PCSAT の性能評価は Unno ら以外に十分には行われていない。また、PCSAT 用のベンチマークは、9 つの仕様に対してのみ行われている上に、基本的な算術・論理演算から成る単純なプログラムに限られており関数や配列を含むようなプログラムは含まれていない。さらに、Unno らの研究で示されたアプローチは複雑であるため、PCSAT の応用性を予測するのは困難である。

以上を踏まえて、PCSAT の性能調査を行った。まず、Unno らの研究で用いられたベンチマークを使って PCSAT の追試を行った。その結果、ベンチマークのうちいくつかの問題 については解くことができないことがわかった。これを受けて、解けなかった問題についてはベ

ンチマークに自作のヒントを追加し、検証に成功した。次に、自作の関係的検証問題を 3 つ作成し、それを PCSAT で解くことができるかを調査した。ここでも解くことができなかった問題があったので、その問題についてはヒントを追加し、検証に成功した。ここまでの検証問題はベンチマークにあるような単純な計算のみからなるものであったが、PCSAT の応用性を確かめるために配列から読み取った値を用いるプログラムの関係的検証を試みた。これについては、配列を関数とみなした上で関数を interpreted な述語変数に変換することで、PCSAT に解ける問題に帰着させ、ヒントを追加することで検証に成功した。

本論文の構成は以下の通りである。まず、2 章で関係的検証の説明と既存手法について述べる。次に、3 章で本研究で行った実験の概要について述べる。続いて 4 章において 3 章で行った実験の結果を考察し、5 章で本研究のまとめと今後の課題について述べる。

第 2 章

先行研究

2.1 Relasional verifiation

2.2 Unno ら

第 3 章

方法・実験

第 4 章

考察

第 5 章

おわりに

参考文献