発表概要

定理証明器によって証明されたCプログラムのマージャ

後藤 裕貴[1,a)]　高橋 和子[1]

2013年1月15日発表

本研究の目的は，ソフトウェア検証過程における定理証明の利用方法の提案と，定理証明の応用領域の拡張である．我々は，ケーススタディとして定理証明器 Isabelle/HOL でシステム仕様を保証した C プログラムマージャを構築する．これは，与えられた 2 つの C プログラムのソースコードに対し，それらを併合し，いくつかの最適化を施した C プログラムソースコードを出力するマージシステムである．また，ここで扱う C プログラムは実際の C 言語の部分集合である．本システムの主要部分は Isabelle/HOL で記述し証明しており，フロントエンドとバックエンドは C プログラムで実装している．本システムは，フロントエンドとバックエンドを備えることで，定理証明器に不慣れなユーザにも使いやすいツールとして提供可能である．証明では，マージ後のプログラムが変数名の重複を含まないこと，改名された関数定義が必ず存在することなど，構文的な正当性のみを対象とした．マージャはソフトウェアテストにおけるテストスイートや，分散開発環境でのプログラムソースの併合などで用いられ，仕様を証明したものを提供することで，これを使って開発されたシステムの信頼性が向上する．また，このマージャを Isabelle/HOL のライブラリとして提供することで，定理証明の応用事例の増加も期待できる．

Certified Merger for C Programs Using a Theorem Prover

Yuki Goto[1,a)]　Kazuko Takahashi[1]

Presented: January 15, 2013

The purpose of this study is to propose a manner of a usage of a theorem prover in software verification process and to expand an application area of theorem proving. As a case study, we construct a certified merger for C programs, which is verified using a theorem prover Isabelle/HOL. It is a merge system that generates a merged code with some optimization of a given pair of C programs. Our target is a subset of a real C language. The main part of the system is both written and proved by Isabelle/HOL. The front-end part and the back-end part are implemented in C. It provides a useful tool for users who are not familiar with theorem provers. We prove several lemmas on syntactical correctness. For example, the merged program includes no duplication of variable names, and there exist the corresponding renamed definitions of functions. Mergers are used for a test program of test suits in the process of software verification or in a distributed environment for software development. The certified merger can improve the reliability of these processes. In addition, if we provide our proof as a library of Isabelle/HOL, more usage of theorem provers is promising.

[1] 関西学院大学理工学部情報科学科
School of Science and Technology, Kwansei Gakuin University, Sanda, Hyogo 669–1337, Japan
[a)] auf75646@kwansei.ac.jp