

発表概要

# Continuation based C を用いたプログラムの検証手法

比嘉 健太<sup>1,a)</sup> 河野 真治<sup>2,b)</sup>

2016年8月10日発表

ソフトウェアが期待される仕様を満たしているか調べることは重要である。特に実際に動作しているソフトウェア自体を検証できるとよい。従来は assert などを用いて検証しているが、モデル検査のような網羅的な検査を行うことはできない。そこでソフトウェアの実行自体を網羅的に行うように変更する。これは計算自体を変更するのでメタ計算となる。本研究ではプログラムを Continuation based C (CbC) で記述する。CbC では Code Segment という単位で処理を記述する。CbC を用いることによりメタ計算は CbC の Code Segment 間に Meta Code Segment を挟むという単純な方法で実現できる。そして、通常計算との切替えも簡単に行うことができる。ここでは、赤黒木を実際の例題として検証した。比較対象として ANSI-C の記号実行を行う CBMC でも検証する。CBMC よりも広い範囲の検査が行えることを確認した。

## Verification Method of Programs Using Continuation based C

YASUTAKA HIGA<sup>1,a)</sup> SHINJI KONO<sup>2,b)</sup>

Presented: August 10, 2016

Checking desirable specifications of software are important. If it checks actual implementations, much better. Currently, assertions in the implementations are used, but it does not verify all possible executions like a model checker. We propose a modification of program executions to do the verification. This kind of modification is called a meta computation. In this study, we describe programs in Continuation based C (CbC). CbC programs are composed of Code Segments. Using CbC, meta computations are easily implemented as an insertion of meta code segment between normal level code segments. Red-black Tree is verified by our method. We also check it with CBMC which executes ANSI-C programs symbolically. Our method covers wider a range of execution of the program.

<sup>1</sup> 琉球大学大学院理工学研究科情報工学専攻  
Information Engineering Course, Graduate School of Engineering and Science, University of the Ryukyus, Okinawa 903-0213, Japan

<sup>2</sup> 琉球大学  
University of the Ryukyus, Okinawa 903-0213, Japan

a) atton@cr.ie.u-ryukyu.ac.jp

b) kono@ie.u-ryukyu.ac.jp