発表概要

限定継続命令shift/reset付きλ計算の評価器の抽出

廣田 知子[1,a)]　浅井 健一[1]

2012年3月16日発表

種々の数学的命題を，定理証明系の手法を使って constructive に証明できれば，この証明過程からきわめて信頼性の高いプログラムが自動的に抽出可能であることが一般的に知られている．本発表では，定理証明系 Coq を用いて，let 文および継続を扱う命令 shift/reset 文を含んだ多相の型付きラムダ計算における評価器を抽出する．まず，型システムの定式化は，Aydemir らのライブラリを利用して行った．この定式化において，α-equality の問題を解消するため，変数の名前付けには locally nameless 手法を用いている．次に，上記ラムダ計算が強正規化性の性質を満たすことの constructive な証明を Coq により定式化した．この証明は論理述語を用いて行われている．この証明の定式化により，このラムダ計算における OCaml 言語の評価器プログラムが自動的に抽出された．このプログラムは，入力値の項に型が付くならば，必ずプログラムの実行が無限ループを起こすことなく停止することが保証されている．しかし抽出されたプログラムの構成は複雑で，そのままでは内部の挙動がどうなっているのかを理解することができない．ゆえに，抽出したプログラムを手動で簡単化し，プログラム内部の挙動の解釈を行った．また，本発表では，我々が抽出したプログラムがより有用となりうるための諸点に関しても述べる．

Extraction of Normalizer of Typed Lambda Calculus with Shift/Reset

Noriko Hirota[1,a)]　Kenichi Asai[1]

Presented: March 16, 2012

If various mathematical propositions are constructively proved using a proof assistant, we are able to automatically extract a reliable program from the constructive proof. In this report, we deal with the extraction of the normalizer program of the typed lambda calculus with control operators shift/reset and let-polymorphism using the proof assistant Coq. First, the type system in our study is formalized by fully utilizing the library of Aydemir et al, employing the locally nameless method in order to avoid a complex problem of alpha-renaming. Next, the proof of "strong normalization" on the above lambda calculus has been formalized in Coq by using a particular logical predicate. This formalization leads us to automatically extract the normalizer program in OCaml. An actual implementation of this program is guaranteed to terminate without infinite loop if the input term is well-typed. However, since the program that has been extracted is so complicated to accurately understand its behavior, we have added, by hand, a simplifying process to such extracted program so as to make our interpretation easier. Finally, this report states a couple of points which have to be overcome in order to make our study here more effective and useful.

[1] お茶の水女子大学理学部情報科学科
Department of Information Science, Ochanomizu University, Bunkyo, Tokyo 112–8610, Japan
[a)] hirota.noriko@is.ocha.ac.jp