学位論文要旨

学位論文題目：継続渡し形式の型主導部分評価器における正当性の証明

人間文化創成科学研究科　理学専攻　廣田知子

本論文では，数学的定理の存在証明を定理証明支援システム Coq で定式化することにより，正当性の保証された部分評価器の抽出を行う．部分評価器は，与えられたプログラムを，関数の body 部分も含めてこれ以上簡約出来ない形（正規形）にまで評価するプログラム変換器である．簡約可能な部分は全て評価してくれる為，プログラムを部分評価器に通せば，意味は等価でありながらも元のプログラムよりも実行時間の短いプログラムが生成出来る．実際にユーザが部分評価器を使う際，その部分評価器の正当性が保証されているか否かは，部分評価器を通した後のプログラムの信頼性に大きく関わる．

本論文ではまず，強正規化性定理と評価器が Curry Howard 同型対応の関係にあるという，一般的に良く知られている事実に着目し，限定継続命令 shift/reset 付き λ 計算における強正規化性定理の証明を Coq で定式化することにより，評価器プログラムを抽出する．型システムを定式化するにあたっては，Locally Nameless 手法を用いることによって α 同値問題を回避する．定理の証明は Tait 流の論理述語を用いて行う．しかしながら，この方法で得られた評価器プログラムは非常に複雑であり，この手法を単純に拡張するだけでは実用的な部分評価器を得ることは出来ない．

上の問題を解決するために，本論文では以下の手順を行う．(i) 型主導部分評価器（type-directed partial evaluator，TDPE）と Curry Howard 同型対応となっている（論理述語の）completeness 定理の証明を行う．(ii) (i) の証明から得られる TDPE が正当性定理（TDPE 実行前後で入力値の意味が変化しない）を満たすことを証明する．(iii) (i) と (ii) の証明を Coq で定式化することにより，実用的で，かつ正しさの保証された TDPE プログラムを導出する．

TDPE は他の一般的な部分評価器と異なり，term の中身を全く見ずに計算を行う．そのため，実行が非常に高速であるという特徴を持つ．TDPE に関する先行研究として，Tsushima らは shift/reset 付き TDPE を提案しているが，その正当性に関しては未だ議論がされていなかった．他方で Ilik は Kripke モデルの推論規則に対する completeness 定理の証明から TDPE を抽出する方法を提示しており，shift/reset 付き λ 計算体系における TDPE の抽出も行っているが，そこで扱われている shift/reset は，(Tsushima らが扱っているような）一般的に使われる shift/reset とは異なるものとなっている．そこで，Ilik と Tsushima らの仕事を結びつけることにより，通常の限定継続を扱えるように，Ilik の証明を構築し直す．それにより，Tsushima らの直接形式の shift/reset 付き TDPE を CPS 変換することにより得られる，継続渡し形式（CPS）の shift/reset 付き TDPE を，Coq を用いて抽出する．

しかしながら，上の completeness 定理から得られた TDPE は無限ループが起こらないことは保証されているものの，正当性定理を満たすことは保証されていない．故に本論文では，call-by-name と call-by-value の TDPE における Filinski の正当性定理の証明を Coq

で定式化し，そしてそれら定式化手法を 2CPS に拡張することによって，(CPS 変換された）Tsushima らの shift/reset 付き TDPE の正当性定理を，Coq を用いて証明する．ここで使用する意味論の completeness 定理から得られる TDPE と，上の Kripke 意味論における completeness 定理から得られる TDPE との違いは，使用している意味論が異なるだけで，プログラムの挙動は同じものとなっている．又，型システムの定式化については parametric higher-order abstract syntax（PHOAS）を用いることにより，α 同値問題を回避しつつ非常に簡潔な定式化を実現している．但し PHOAS の higher-order の特性により Coq では証明が困難な性質が存在するため，その性質の証明のみ Coq には載せずに公理として定義する．