平成24年度 情報工学コース卒業研究報告要旨

結縁 研究室	氏　　名	中 村　陽 介
卒業研究題目	プログラム検証器 Depcegar に対する再帰データ構造への拡張	

本研究では, 高階関数型プログラムに対するプログラム検証器である Depcegar に再帰データ構造を扱えるよう拡張した型システムを定義する.

ソフトウェアを安全に開発する手法の一つとして，プログラムの無限の状態に対して網羅的な解析を行いシステムの安全性を保証する，形式手法が提案されている．形式手法の一種である型検査とは，プログラム中に出現する値に型推論を行うことによって，テストを作成しなくとも型の段階でプログラムの一定の安全性を保証するものである．プログラムに対し高精度な型検査を行うためにはプログラムの挙動を詳細に知ることが必要であり，より厳しい条件を含んだ型を利用することが肝要である．既存の型に条件をつける型として，refinement 型が存在する．Refinement 型はプログラム中の値を参照して決定される型であり，型に厳しい条件をつけることが可能となる．

Depcegar は OCaml のサブセットに対するプログラム検証器である．型候補内で型付け可能性を判定し，型付けできない場合を反例として返し，偽反例であれば推論された型を型候補に加えて再び型付け可能かの検証を行う．Depcegar は型に一階述語論理式を含む refinement 型を利用して型検査を行う．Refinement 型は上記のように型に条件を付与できるため，通常の型検査よりも精密な検査が期待できる．しかし Depcegar で使用されている refinement 型では複雑なデータ構造を表現することができず，扱えるプログラムの範囲が狭いことが問題となる．

本研究では，Depcegar で使用されている refinement 型に対し再帰データ構造を扱えるよう型システムの拡張を行い, その健全性を証明する．健全性をもつ型システムによって型付け可能ならば，そのプログラムは正しいといえる．再帰データ構造を拡張することで，既存の refinement 型では扱えなかった型表現ができるようになる．リストや木構造を表すことができ，各要素に型による条件付けができるため精密な型検査を行える．再帰型とは自身を参照する型であり，再帰構造を実現するために不可欠となる．しかし再帰型のみではいつまでも自身を参照することしかできず，複数の要素を組み合わせなければ再帰データ構造を表現することはできないため，ペア型，ヴァリアント型の定義も合わせて必要となる．ペア型は二つの型を組として表す型であり，ヴァリアント型は複数のデータにラベルをつけて管理する型である．これらの型を定義するためそれぞれについて構文規則，型付け規則，評価規則を作成した．最後に，拡張した規則をもとに健全性について証明を行った．