平成21年度 情報工学コース卒業研究報告要旨

研究室	氏　　名	高 桑　一 也
卒業研究題目	項書換え系への変換による類似した関数の効率的な検証	

変数型上の命令型プログラムの検証手法として，関数型プログラムの計算モデルである書換え系へ命令型プログラムを変換し，定理自動証明により検証する手法がある．定理自動証明とは，等式が与えられた書換え系の帰納的定理であることを証明することであり，2つの関数が計算に関して等価であることの証明に利用できる．しかし，証明の成功には補題式を与えたり簡約の戦略を変えたりするなどの，ユーザの試行錯誤が必要である場合が多い．適切なパラメータを設定しないと手続きが終了しない場合もある．よって，定理証明器を用いた検証はコストが大きいという問題がある．ある1つのプログラムを改良した場合や同じ仕様のプログラムなどの場合には，書換え系に変換するとほとんど同じになる場合がある．このように類似したプログラムの検証には定理自動証明を用いなくてもよい場合があり，その場合には検証コストの削減を期待できる．なお，本論文における類似したプログラムとは，局所変数の名前が異なるもの，制約が構文的に同一ではないが解釈が等しいもの，変数宣言の順番が異なるもの，余分な変数が宣言されているもののような，計算手順には本質的に関係のない差異しかないことをいう．

本論文では，類似したプログラムの等価性を効率的に検証する手法を提案する．まずは，対象を制約付き項書換え系として類似した関数が計算に関して等価であることを保証する条件を示す．片方は仕様を満たす制約付き項書換え系，もう片方は類似した制約付き項書換え系を想定する．関数記号の集合が等価な場合には，引数切り落とし関数を利用した条件を提案する．引数切り落とし関数は，項の引数の並べ替えや切り落としなどを行うことができる．それを用いて，類似した制約付き項書換え系に適用することでもう一方と構文的に等価になるような引数切り落とし関数が存在する場合に，それら2つの制約付き項書換え系が同じ名前で定義された関数の計算に関して等価であることを示す．このとき，仕様を満たす制約付き項書換え系で成立する帰納的定理はもう片方の制約付き項書換え系で帰納的定理となり，類似したプログラムも仕様を満たすことが保証される．

Cプログラムから変換して得られる制約付き項書換え系では，元のプログラムの構造によって内部処理に対応した補助関数の記号が異なる場合がある．このような場合には，条件を満たすような引数切り落とし関数は存在しない．そこで，提案した手法を木準同型写像に拡張する．木準同型写像は，引数切り落とし関数の機能に加えて，項の関数記号の変更も行うことができる．拡張では，関数記号の写像は根に関して単射になるという条件が木準同型写像に要求される．提案した条件を満たす木準同型写像の候補は有限であるので，提案する十分条件は決定可能である．本論文ではさらに，そのような条件を満たす木準同型写像の存在を効率的に判定するアルゴリズムを提案する．

最後に，同じ仕様に従って書かれた複数のCプログラムに対して，本手法による検証を行い，本手法を評価する．具体的には，Cプログラムを制約付き項書換え系に変換し，提案した類似性の十分条件に基づいて分類する実験を行う．本手法を用いて，同じ名前の関数の計算に関して等価といえるプログラムを同じ分類とすることにより，その分類から1つのプログラムを選んでそれらについて定理自動証明を用いた検証を行えば，全プログラムの効率的な検証を期待できる．