平成18年度 情報工学コース卒業研究報告要旨

酒井 研究室	氏　　名	田中裕二
卒業研究題目	書換え手法に基づく Cプログラムの検証ツールの実現と その自動化のための考察	

手続き型言語ではホーア理論を利用して関数の正当性 (仕様を満たすか) を検証する方法がある．しかし，ループ不変式や事前条件 · 事後条件を与えるなどのヒューリスティックな作業が必要である．一方，項書き換え系の分野では帰納的定理の証明手法として潜在帰納法や書換え帰納法などが広く研究されている．帰納的定理とは任意の基底頂上で成立する等式であり，2 つの異なる関数が任意の入力に対して同様の出力を返すことは帰納的定理として捉えられる．このため，帰納的定理の証明法は関数型プログラムで定義されている関数の等価性の検証に利用できる．実際，手続き型プログラムを等価な項書き換え系に変換し，帰納的定理の証明法を用いて与えられた仕様との等価性を検証する手法が提案されている．具体的には，真偽判定が決定可能である一回述語論理式を規則の条件に持つ決定可能条件付き項書き換え系（dTRS）の枠組を与え，定めた手続き型言語で書かれたプログラムから，プレスブルガー文を条件部に持つ dTRS（pdTRS）へ変換し，さらに仕様として与える pdTRS の等価性を潜在帰納法を用いて検証する方法である. しかし，潜在帰納法の中で用いられる完備化手続きが pdTRS 上へ拡張されたことで，自動化のための戦略も拡張される必要がある．そのために，人間が手作業で行う検証実験を支援する対話型システムが望まれる．

本研究では，自動検証ツール開発のための実験を支援する対話型システムを実現する．具体的には，構文を制限したC言語の関数（C関数）から pdTRS への変換と，pdTRS の完備化を関数型言語である Standard ML により実装した．さらに，それらにウェブインターフェースを与えることにより，対話型システムとしての利便性を高めた．

完備化は，等式集合と規則集合の対に対して作用する推論規則を順次適用していき，合流性と停止性を持つ書き換え系を導く手続きである．TRS の KB 完備化手続きのような自動化された戦略もあるが，多くの場合は暴走するので，人間が適用すべき推論規則を適宜指定しながら，対話的に作業を進めることも必要である．実装した完備化システムは規則集合，等式集合，さらに適用したい推論規則を記述したファイルを読み込み，推論規則を適用した結果を出力する．また，出力を入力と同じ構文にすることによって，実行時における入力の手間を削減し，対話的処理を容易にしている．

対話的処理のためのウェブインターフェースは入出力のための HTML の作成やファイル処理を行う主要箇所を PHP で，完備化プログラムの実行とその暴走を抑制するためのタイムアウト処理を行う部分を Perl で，さらに必要に応じてインターフェースを動的に表示する部分を JavaScript で実装した．このインターフェースでは，入力と出力を同じ場所に表示させ，等式集合と規則集合に対する対話的処理を繰り返し実行できるようにしている．等式集合と規則集合を編集可能な入力フォームに表示することで，柔軟な検証実験を可能にする．また，C関数の変換のためのウェブインターフェースは PHP のみで実装され，自動的に完備化のウェブインターフェースに結果が入力される．

最後に，非負整数 n において 1 から n までの整数リストの総和を求めるC関数に対して検証実験を行った．この実験でこの手法の効果，自動検証の実現のために解消すべき問題点を抽出する．