平成27年度 情報工学コース卒業研究報告要旨

結縁・中澤 研究室	氏　　名	仲 田　壮 佑
卒業研究題目	帰納的述語を含む分離論理のための 循環証明体系における自動証明	

プログラムは人の手で書かれる以上，しばしばバグを含む．バグはときに重大な問題を引き起こすため，運用前のバグの発見は重要である．プログラムの運用前にプログラムのバグを発見するための枠組みの一つにホーア論理がある．ホーア論理は，プログラムの実行前にプログラムが満たすべき性質を厳密に保証するための枠組みである．より具体的には，事前条件と事後条件を論理式で記述し，事前条件が満たされているときに，プログラムを実行すると事後条件が満たされるということを数学的に証明する．分離論理はホーア論理に対してポインタを操作するコマンドとヒープ状態を表す条件によって拡張したものであり，ヒープへのアクセスを含むプログラムを対象としたプログラム検証のための論理体系となっている．

本研究では，帰納的述語定義を含む分離論理によるプログラム検証の自動化に向けて，論理式の（半）自動証明器を実装した．例えば，あるポインタがリスト構造を指していることを表す述語は帰納的に定義されるが，一般にこのような帰納的に定義された述語を含む論理式の妥当性判定は決定不能である．そこで，Brotherston らの提案した循環証明体系を利用し，証明探索を行う．循環証明体系による証明では通常の推論規則に加えて，特定の条件のもとで証明木に循環を許し，帰納的に定義された述語を含む論理式の証明を行う．

証明探索の際には帰納的述語を定義に従って展開する必要があるが，素朴な方法では適用可能な推論規則の数が爆発的に増加する．そのため，推論規則の性質から適用すべき規則の順序を決定した．さらに，同じ述語を繰り返し展開すると証明探索が有限で止まらないため，述語を展開する回数に上限を定め，展開の順序を様々に変えて証明探索を行うようにし，また，明らかに不要である展開は行なわないようにした．

本研究で実装した証明器を用いて，帰納的述語として様々なリストを含むいくつかの論理式を入力として動作させ，正しい結果が得られることを確認した．さらに論理式が証明可能と判断された場合は，証明器に証明木を出力させ，証明探索によって発見された証明を可視化した．