平成27年度 情報工学コース卒業研究報告要旨

酒井 研究室	氏　　名	水 谷　慎 之 介
卒業研究題目	配列を入力引数とする関数における不正メモリ参照検出のための分離論理の拡張	

メモリの不正参照がないことを証明する分離論理という検証モデルがある．分離論理とは，プログラムの静的検証法であるホーア論理を，メモリを扱えるように拡張したもので，プログラムの前後で成り立つ事前条件および事後条件を推論規則に基づいて推論する証明系である．例えば，2つのアドレスの指すヒープ（メモリ領域）が重ならないということを表す命題論理式を表明式（事前条件および事後条件）に記述することができる．一般に高信頼性が求められるソフトウェアの検証への応用が期待されている．

C言語では，配列を入力引数とする関数が，関数としては不正なメモリ参照を起こすにもかかわらず，参照したメモリ自体は多次元配列のようにプログラムの実行で確保されているため，セグメントエラーが起こらず不正なメモリ参照に気づかない場合がある．そのような関数では配列の先頭のアドレスのみを関数に渡すため，関数内からはその配列のサイズは不明である．したがって，配列を入力引数とする関数のみを検証するには事前条件にサイズが可変なヒープを記述する必要がある．しかし，分離論理ではサイズが可変なヒープを表現できないため，配列を入力引数とする関数のみを検証することはできない．

本論文では，サイズが可変なヒープを表現できるように分離論理の表明式におけるヒープの記述法および意味論を拡張し，配列を入力引数とする関数の不正なメモリ参照の検出を目指す．そのため，分離論理の表明式の拡張および推論規則の拡張に加え，不正なメモリ参照を検出するための分離論理における反証法を提案し，それを用いることで配列を入力引数とする関数の不正なメモリ参照を検出できる例を示す．

本論文で提案する分離論理のヒープの記述法は正規表現に基づくもので，たとえば，あるアドレスが変数を含む変数多項式で表現される長さのヒープの先頭であるということを記述できる．その他にもヒープの一つのセルに入り得る値の集合をヒープの表現に用いることで，あるアドレスのヒープの中の値が特定の値以外であるということを記述できる．また，推論規則もこれらの拡張に対応できるように拡張する．

また，分離論理における反証の手法としてヒープの存在性に基づく反証の手法を提案する．分離論理において，ヒープの存在性は意味論に含まれており，存在しないヒープを参照するプログラムはエラーを返す．そのため，ホーア論理とは異なり分離論理では，推論の途中であっても事前条件にないヒープの領域を参照する命令が現れると，その時点で反証が成立する．また，分離論理においてループのないプログラムは，推論規則に基づいて表明式が機械的に決まる．一方，ループのあるプログラムはループ不変式を考慮する必要があり機械的に推論を進めることができないため，ループの一回分の処理を条件分岐を用いて展開したプログラムを生成し，そのプログラムの先頭からループの繰り返し部分を実行せずに到達できる命令列で反証が成り立ち，その命令列へ先頭から到達可能な変数割当が存在するとき，反証が成立する．

以上の分離論理の拡張および反証法を用いて，実際にプログラミングの講義で提出された学生のC言語のプログラムを検証する．このプログラムでは，関数が不正なメモリ参照を起こしているが，参照したメモリ自体はプログラム中で確保されているため，セグメントエラーが起こらず実行環境次第では正しい実行結果が出力するため，不正なメモリ参照を発見することは難しい．しかし，本論文の手法を用いることで，このプログラムの不正なメモリ参照を検出できることを示す．