氏　　名	Mahmudul Faisal Al Ameen
学位(専攻分野)	博士(情報学)
学 位 記 番 号	総研大甲第 1889 号
学位授与の日付	平成28年9月28日
学位授与の要件	複合科学研究科　情報学専攻 学位規則第6条第1項該当
学 位 論 文 題 目	Completeness of Verification System with Separation Logic for Recursive Procedures
論 文 審 査 委 員	主　査　教授　龍田 真 准教授　金沢 誠 教授　胡 振江 教授　中島 震 教授　亀山 幸義 筑波大学

(別紙様式 2)
(Separate Form 2)

論文内容の要旨
Summary of thesis contents

第 1 章は，序論であり，研究の動機，主たる結果について述べている．第 2 章は，背景知識として，従来の再帰手続きに対するホーア論理，分離論理を説明している．本論文のホーア論理はペアノ算術を含むため，完全性として相対完全性(以下では単に完全性とよぶ)しか成立ちえないことを説明している．

第 3 章は，再帰手続きに対する新しいホーア論理を構成し，完全性定理を証明した．対象とするプログラミング言語は，代入文，if 文, while 文，skip, 複文，(引数をもたない)手続き呼出しから成る．仕様記述言語は，ペアノ算術とプログラミング言語を含む一階述語論理である．完全であり，かつ分離論理に拡張可能なホーア論理体系を構成することがこの章の研究目的である．従来の再帰手続きに対するホーア論理は，invariance axiom とよばれる公理を含み，これは，分離論理に拡張したときに不健全になる．このため，分離論理と再帰手続きを同時に含むホーア論理を構成するためには，新しいホーア論理体系が必要である．本章ではこれを達成した．

第 4 章，第 5 章が本論文の主たる成果である．第 4 章は，再帰手続きに対する分離論理を含むホーア論理体系(以下では単に再帰手続きに対する分離論理体系とよぶ)を構成し，それを推論規則で表現した．プログラムは，第 3 章で定義されたものと同じものを対象とする．仕様記述言語は，ペアノ算術とプログラミング言語を含む一階述語言語に基づく分離論理であり，分離論理の論理記号としては，空ヒープを表す命題記号，一つのセルからなるヒープを表す述語記号，分離連言，分離含意をもつ分離論理体系である．この論理体系は，第 3 章の結果であるホーア論理体系を分離論理に拡張した論理体系になっている．ホーア論理としては，ホーア論理の通常の推論規則である代入文，複文，if 文，while 文のそれぞれに対する規則，結果規則の他に，メモリセルの生成の文，メモリセルの参照の文，メモリセルの書き換えの文，メモリセルの解放の文，および再帰手続きに対する規則，inv-conj 規則，存在規則をもつ．また，このホーア論理体系は，再帰手続きに対する規則が仮定を削除する操作を含むため，通常のホーア式ではなく，ホーア式を構成要素とするシーケントを基本的判定としている．このシーケントは，前件として仮定となる複数のホーア式をもち，後件として結論となる一つのホーア式をもつ．このため，公理規則，カット規則，weakening 規則もこの体系はもっている．前件はホーア式の集合と考えるため，exchange と contraction に関する規則はもっていない．

第 5 章は，第 4 章で構成した論理体系に対する健全性定理，表現性定理，完全性定理を証明した．健全性定理は，ホーア式がこの論理体系で証明できるならば，このホーア式は標準モデルにおいて真であることを主張する．健全性定理は，手続きを展開するホーア式に対する健全性を証明図の大きさに関する帰納法により証明することにより,証明した.表現性定理は，プログラムと事後条件を表す論理式が与えられたとき，その最弱事前条件を記述する論理式が存在することを主張する．表現性定理は，再帰手続きのない分離論理体系における表現性定理の証明を再帰手続きに拡張することにより，証明した．完全性定理は，健全性定理の逆であり，このホーア式は標準モデルにおいて真であるならば，ホーア式がこの論理体系で証明できることを主張する．完全性定理は，先行研究の再帰手続きのあるホーア論理の完全性証明を分離論理に拡張することにより，証明した．先行研究の再帰手続きのあるホーア論理の完全性証明は，一つしか知られておらず，手続きの性質を完

(別紙様式 2)
(Separate Form 2)

全に記述するホーア式および最強事後条件を用いる証明しか知られていない．これを分離論理に拡張するためには次のような二つの問題と本論文によるその解決が必要であった．第一は，手続きの性質を完全に記述するホーア式が必要であるが，分離論理では，変数の状況だけではなくヒープの状況も記述する必要があった．このため，既存研究にあった現在のヒープをその数表現に対応させる述語を用いて，これを実現した．第二は，分離論理では，abort が起きるため，最強事後条件は一般には存在しない．本論文は，最強事後条件が存在する十分条件として abort-free 条件を見つけ，これを最弱事前条件により記述した．すなわち，与えられたプログラムに対し，事後条件を真にとった最弱事前条件を考える．この最弱事前条件は，表現性定理によりそれを記述する論理式が存在することが保証されている．この最弱事前条件は，プログラムの実行が abort を起こさないことと同等になる．プログラムと事前条件が与えられたとき，その事前条件と abort-free 条件の連言を事前条件とすれば，この条件下ではこのプログラムは abort を起こすことがないため，最強事後条件が定義できる．このようにして abort-free 条件を併用することにより，最強事後条件を用いることができた．

第 6 章は，フレーム規則と論理積規則の許容可能性(addmissibility)についてその性質を証明した．前件のないホーア式に対するフレーム規則は健全かつ許容可能であること，一方で，前件のあるホーア式に対するフレーム規則はすべて許容可能ではなく，そのうち前件を保つフレーム規則は健全であるが，他のフレーム規則は不健全であること，論理積規則は健全だが非許容可能であること，を証明した．第 7 章は結論である．

(別紙様式 3)
(Separate Form 3)

博士論文の審査結果の要旨
Summary of the results of the doctoral thesis screening

本論文は，再帰手続きに対する分離論理体系を構成し，その完全性定理を証明した研究であり，この研究成果はソフトウェア検証の重要な基礎理論を構築したものであり，理論計算機科学および数理論理学に対して十分な貢献をした．また，本論文の研究成果は，査読付き論文雑誌 Theoretical Computer Science に掲載された．このため，本論文が博士論文として学位を与える水準に達していると全員一致で結論した．

また，学位論文に関する口述試験により，本学位申請者が，本学位論文に関連する専門分野および基礎となる分野に関して博士(情報学)の学位の水準に達する学識を有し，十分な学力をもつことが全員一致で確認された．