氏　　名	小合　敬之	
学位（専攻分野）	博士（情報学）	
学位記番号	総研大甲第1518号	
学位授与の日付	平成２４年３月２３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	HOLを用いた代入定理の検証	
論文審査委員	主　査	教授　龍田　真
		教授　胡　振江
		教授　佐藤　健
		教授　井上　克巳
		准教授　金沢　誠

論文内容の要旨

本論文では，高階論理証明システムHOLを用いて代入定理を形式化し検証する．代入定理とは，与えられたラムダ項と与えられたいくつかのその変数に対して，任意の弱正規化可能な同じラムダ項を代入してもその項が弱正規化可能であるなら，任意の弱正規化可能な異なるラムダ項を代入してもその項が弱正規化可能であるという2006年に証明された型なしラムダ計算の新しい定理である．これは，原論文では弱正規化可能性に関する代入定理とよばれている．我々は原論文の数学的内容を忠実に形式化する．束縛変数の名前換えの無いラムダ項を扱うために，Homeierのパッケージによって文脈alpha-同値を使用する．本検証の結果，ラムダ計算の新しく重要な定理を検証することができた．

本論文の第1章では，序論として代入定理の検証の概要とその意義，この検証が成す貢献，関連研究，本論文の構成について説明する．先行研究において採られたラムダ計算の形式化の手法について論じる．また，ラムダ計算の定理を検証した先行研究ではChurch-Rosserの定理など良く知られた定理が検証されているのに対して，本論文では最近証明されたラムダ計算の新しく重要な定理を検証したことを述べる．第2章では，予備知識として型無しラムダ計算と高階論理の自動証明システムであるHOLについて説明する．HOLについては，その論理体系と検証コードの文法，定理の検証で用いるgoal，tactic，tacticalについて説明する．第3章では，予備知識として代入定理の数学的記述とその数学的な証明を説明する．代入定理の記述を与え，この定理の証明に導入されたコントロールパスと隣接コントロールパスの概念を導入する．代入定理を証明するための主補題を示し，それを用いて代入定理の証明を与える．第4章では，予備知識として文脈alpha-同値と二種類のラムダ計算について説明する．pure lambda-calculusはpre-lambda-calculusのalpha-同値関係による同値類として定義される．pre-lambda-calculus，文脈alpha-同値とalpha-同値，pure lambda-calculusを順に定義し，lambda calculusにおいてpure lambda-calculusとalpha-同値を導入することの利点と問題点について述べる．また，ラムダ項の代入の定義について説明する．第5章では，第3章と第4章の内容を形式化し，代入定理の形式化を与える．検証の目標となる代入定理の論理式の形式化を与え，弱正規化可能性など検証に必要なラムダ計算に関する概念の形式化を与える．部分項の概念を形式化するために，部分項のindicatorを導入する．コントロールパス，隣接変数出現，隣接コントロールパスなど代入定理の証明のために導入された概念の形式化を与える．特にラムダ項M中の集合Sからの隣接コントロールパスがあることの否定について新たな述語を与えて形式化する．第6章では，代入定理の形式的な証明が得られることを示す．ラムダ計算の概念を形式化した関数や述語について，代入定理の証明で必要な補題を形式化して証明する．また，indicatorによる部分項の表示やコントロールパスなどの代入定理の証明に導入された概念の性質についての補題を形式化して証明する．次に第3章で述べた代入定理の証明に用いた補題を形式化して証明するが，円滑な証明をするために，主補題を変更する．そして代入定理の形式的証明の実行について示し，その実行結果について述べて，コード量および処理時間を記す．第7章では，この研究の解決した問題を論じる．問題解決の第一は，変数の捕捉による困難を解決するために，束縛変数の名前の集合Sに対し，PWN_Sという概念を導入したことである．これは，原論文で使用される永続的弱正規化を置き換え，あるラムダ項がこの性質を

もつことを示すときに，beta-簡約により起こる代入処理を単純化する．第二に，変数代入によりコントロールパスが保たれることを検証するために帰納法に適切な変数を選択する工夫を用いた．この性質の形式的な記述は両方のスタイルのラムダ項を混在させて用いている．我々は記述中に隠された内側の変数を最外部に移動して帰納法を適用する変数として使用する．第三に，隣接コントロールパスの存在の否定を表現するために新たな述語を導入した．隣接コントロールパスの存在の忠実な形式化は暗黙の自由変数条件を正しく表さない．このため，命題の仮定でその否定を使用する場合は，形式的証明が進まなくなる．この問題を解決するために，我々はその否定が自由変数条件を正しく表すような新たな述語を導入する．そして第8章では本研究についてのまとめと今後の研究課題について述べる．

博士論文の審査結果の要旨

本論文は，高階論理証明システムHOLを用いて代入定理を形式化し検証した．代入定理とは，2006年に証明された型なしラムダ計算の新しい定理である．本論文の第1章は序論であり、第2章では，予備知識として型無しラムダ計算と高階論理の自動証明システムであるHOLについて説明する． 第3章では，予備知識として代入定理の数学的記述とその数学的な証明を説明する．代入定理の記述を与え，コントロールパスと隣接コントロールパスの概念を導入する．代入定理を証明するための主補題を示し，それを用いて代入定理の証明を与える．第4章では，予備知識として文脈alpha-同値と二種類のラムダ計算について説明する．第5章では，第3章と第4章の内容を形式化し，代入定理の形式化を与える．検証の目標となる代入定理の論理式の形式化を与え，弱正規化可能性など検証に必要なラムダ計算に関する概念の形式化を与える．コントロールパス，隣接変数出現，隣接コントロールパスなど代入定理の証明のために導入された概念の形式化を与える．特に，与えられた集合からはじまる隣接コントロールパスが存在することの否定について，新たな述語を与えて形式化する． 第6章では，代入定理の形式的な証明が得られることを示す．indicatorによる部分項の表示やコントロールパスなどの概念の性質についての補題を形式化して証明する．次に第3章で述べた代入定理の証明に用いた補題を形式化して証明する．円滑な証明のために，主補題を変更する．代入定理の形式的証明の実行について示し，その実行結果について述べる． 第7章では，この研究の解決した問題を論じる．問題解決の第一は，変数の捕捉による困難を解決するために，束縛変数の名前の集合をパラメターとするパラメター付き永続弱正規化可能性という概念を導入したことである．これは，原論文で使用される永続的弱正規化を置き換え，あるラムダ項がこの性質をもつことを示すときに，beta-簡約により起こる代入処理を単純化する．第二に，変数代入によりコントロールパスが保たれることを検証するために帰納法に適切な変数を選択する工夫を用いた．この性質の形式的な記述は両方のスタイルのラムダ項を混在させて用いている．本論文は記述中に隠された内側の変数を最外部に移動して帰納法を適用する変数として使用する．第三に，隣接コントロールパスの存在の否定を表現するために新たな述語を導入した．隣接コントロールパスの存在の忠実な形式化は暗黙の自由変数条件を正しく表さない．この問題を解決するために，本論文はその否定が自由変数条件を正しく表すような新たな述語を導入する．第8章ではまとめと今後の研究課題について述べる．ラムダ計算の定理を検証する研究は従来からいくつかあるが，いずれも正しいと確信されているよく知られた定理を検証した研究であった．本研究では，最近証明された新しく重要なラムダ計算の定理を検証した点で意義がある．本論文で検証したラムダ計算の定理は，その証明において束縛変数名を陽に用いる必要がある． 先行研究では困難を避けるためアルファ同値を仮定し束縛変数名を使わないで証明できる定理の検証が多かった．本論文では，束縛変数名とアルファ同値の二種類のラムダ計算を混在させて検証を行う必要があり，このような検証の研究は意義がある．以上のように，本論文は，重要なラムダ計算の定理を定理証明システムHOLにより検証し，それを実現するための問題点を解決した研究であり，理論計算機科学の発展および定理検証技術の進歩に対して十分な貢献をした．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．