博士（工 学） 能 登 正 人

学 位 論 文 題 名

書換え系の性質の形式的検証に関する研究

学位論文内容の要旨

近年，大規模化の進むソフトウェアに対して，全体的な正しさを保証することは非常に難しい問題であるとされている．そこで，この問題を解決するために，新しいパラダイムに基づくプログラミング言語が次々と提案されている．これらの言語に共通する特徴は，根底にある論理体系が明確に定まっていることである．プログラミングを数学的な枠組みの中に置くことによって，ソフトウェアのメカニズムや性質，計算の意味を明らかにすることができ，厳密に議論することが可能である．

これらの言語のいくつかは，等式系とみなすことができる．等式は，数学をはじめとする科学のさまざまな場面で用いられる．あるときには，与えられた公理からある恒等式が論理的に導かれるかどうかを定めようとし，またあるときには方程式に対してその解を求めることをする．等式を用いたこのような推論はまた，さまざまなコンピュータ応用，たとえば，定理自動証明，代数的仕様記述，関数型言語などの理論的基礎として非常に重要である．

等式系に基づく計算モデルの一つとして，書換え系（抽象書換え系および項書換え系）がある．書換え系は，書換え規則とよばれる左辺から右辺へ向き付けられた等式の集まりであり，与えられた式に対して，その一部をそれと等しい左辺をもつ規則の右辺で置き換える操作を繰り返して式を最も簡単な形にするものである．書換え系にはいくつかの性質があるが，特に重要な性質として停止性と合流性がある．停止性は無限に書換えが続かないことを意味し，合流性は計算結果が一意であることを意味する．停止性と合流性を満たす書換え系は完備であるという．停止性と合流性の検証は一般には決定不能な問題であるが，いくつかの十分条件が知られている．それらの条件を拡張する基礎研究やその応用研究はこの分野で最も重要な研究の一つである．

本論文では，書換え系のこれらの性質を形式的に検証する手法の拡張とその応用を述べている．本論文の構成は，以下のとおりである．

第1章では，本研究の背景および目的について述べている．

第2章では，準備として，書換え系（抽象書換え系および項書換え系）の概要と諸性質について述べている．

第3章では，項書換え系の停止性検証法について述べている．項書換え系の停止性の検証は一般には決定不能な問題であるが，Dershowitz によって提案された単純化順序を用いることにより，一部の（しかし，実用上重要な多くの）項書換え系に対して停止性の形式的検証が可能であることを述べる．本論文では特に，経路順序とよばれる単純化順序の部分クラスに着目する．経路順序は，関数記号の集合上に定義される

優先順位とよばれる半順序と項の構造に基づき，二項の相対的な重さ（大小関係）を比較するものである．この方法は，機械的な手順で二項の比較ができることから実装も容易で，したがって複雑な項にも十分対応し，また前提となる優先順位は項の構造から逆に推論できるなど，自動化という観点から最も有望な方法である．次に，経路順序のうちで特に代表的な（ステータス付き）再帰経路順序（RPOS）について検討する．

第4章では，ステータスの概念を拡張した“拡張ステータス”を提案し，それを適用した経路順序について述べている．ステータスは各関数記号ごとにもっていて，比較すべき二つの項の最外（最左）の関数記号が同一のときの引数の比較方法を示している．ステータスの種類としては，多重集合順序，左辞書式順序，右辞書式順序の3種類あり，慣習的にそれぞれ $mult, left, right$ の記号を用いる．従来の $left, right$ ステータスは，引数の比較する順序を辞書式順序で1引数ずつ比較していたが，拡張ステータスを用いることにより，いくつかの引数をまとめて多重集合順序で比較できるようになっている．本論文では，従来のRPOSよりも検証に成功しやすい拡張ステータス付き再帰経路順序（RPOES）を提案し，それが単純化順序であることを証明し，その有効性について述べている．

第5章では，書換え系の検証理論を用いた応用として，卒業研究の指導などのために学生を大学の各講座（研究室）に配属させる講座配属問題について述べている．本論文では，学生と講座の双方の優先度を考慮して配属を決定するアルゴリズムを考察する．このアルゴリズムには非決定性があるので，解（すなわち配属結果）が一意であるということは自明ではない．そこで，解の一意性を検証するために，このアルゴリズムの停止性と合流性（すなわち完備性）について抽象書換え系の理論を用いて形式的に証明する．

第6章では，本論文の結論および今後の展望について述べている．

学位論文審査の要旨

主　査　教　授　大　内　　東
副　査　教　授　宮　本　衛　市
副　査　教　授　新　保　　勝
副　査　助教授　栗　原　正　仁

学位論文題名

書換え系の性質の形式的検証に関する研究

書換え系は，書換え規則とよばれる左辺から右辺へ向き付けられた等式の集まりであり，与えられた式に対して，その一部をそれとパターン照合する左辺をもつ規則の右辺で置き換える操作を繰り返して式を最も簡単な形にするものである．この分野は計算機基礎理論を支える重要なものの一つとして活発に研究されてきており，定理自動証明，代数的仕様記述，関数型言語などに応用されている．書換え系には満たすことが望まれるいくつかの性質があるが，特に重要なものとして停止性と合流性がある．停止性は無限に計算が続かないこと，合流性は計算結果の一意性を保証する．これらの性質を検証する基礎研究やその応用研究はこの分野で最も重要な研究の一つである．

本論文は，書換え系のこれらの性質を形式的に検証する手法とその応用についてまとめたものであり，その主要な成果は，次の2点に要約される．

1. 従来の停止性検証法では理論的に検証不可能だった問題に対し，拡張ステータスという新しい概念を導入した理論を提案することにより，これを検証可能とした．

2. 非決定性問題の例として講座配属問題を考察の対象とし，抽象書換え系の理論を用いて解の一意性すなわち合流性を形式的に検証している．

本論文は6章から構成されている．

第1章では，本研究の背景および目的について述べている．

第2章では，準備として，書換え系（抽象書換え系および項書換え系）の概要と諸性質について述べている．

第3章では，項書換え系の停止性検証法について述べている．項書換え系の停止性の検証は一般には決定不能な問題であるが，Dershowitz によって提案された単純化順序を用いることにより，一部の（しかし，実用上重要な多くの）項書換え系に対して停止性の形式的検証が可能であることを述べている．本論文では特に，経路順序とよばれる単純化順序の部分クラスに着目している．経路順序は，関数記号の集合上に定義される優先順位とよばれる半順序と項の構造に基づき，二項の相対的な重さ（大小関係）を比較するものである．この方法は，機械的な手順で二項の比較ができることから実装も容易で，したがって複雑な項にも十分対応し，また前提となる優先順位は項の構造から逆に推論できるなど，

自動化という観点から最も有望な方法である．次に，経路順序のうちで特に代表的な（ステータス付き）再帰経路順序（RPOS）について検討している．

第4章では，ステータスの概念を拡張した“拡張ステータス”を提案し，それを適用した経路順序について述べている．ステータスは各関数記号ごとにもっていて，比較すべき二つの項の最外（最左）の関数記号が同一のときの引数の比較方法を示している．ステータスの種類としては，多重集合順序，左辞書式順序，右辞書式順序の3種類あり，慣習的にそれぞれ $mult, left, right$ の記号を用いる．従来の $left, right$ ステータスは，引数の比較する順序を辞書式順序で1引数ずつ比較していたが，拡張ステータスを用いることにより，いくつかの引数をまとめて多重集合順序で比較できるようになっている．本論文では，従来のRPOSよりも検証に成功しやすい拡張ステータス付き再帰経路順序（RPOES）を提案し，それが単純化順序であることを証明し，その有効性について述べている．

第5章では，書換え系の検証理論を用いた応用として，卒業研究の指導などのために学生を大学の各講座（研究室）に配属させる講座配属問題について述べている．本論文では，学生と講座の双方の優先度を考慮して配属を決定するアルゴリズムを考察している．このアルゴリズムには非決定性があるので，解（すなわち配属結果）が一意であるということは自明ではない．そこで，解の一意性を検証するために，このアルゴリズムの停止性と合流性（すなわち完備性）について抽象書換え系の理論を用いて形式的に証明している．

第6章では，本論文の結論および今後の展望について述べている．

これを要するに，著者は，書換え系の最も重要な二つの性質である停止性と合流性の形式的検証について基礎および応用の観点から新たな展開を示し，計算機基礎理論上有益な新知見を得たものであり，システム情報工学の進歩に対して貢献するところ大なるものがある．

よって著者は，北海道大学博士（工学）の学位を授与される資格あるものと認める．