【44】

氏名・（本籍）	東野輝夫（ひがしのてるお）
学位の種類	工学博士
学位記番号	第6480号
学位授与の日付	昭和59年3月24日
学位授与の要件	基礎工学研究科　物理系専攻 学位規則第5条第1項該当
学位論文題目	代数的仕様記述の検証に関する研究
論文審査委員	（主査） 教授 嵩　忠雄 （副査） 教授 藤澤 俊男　教授 高島 堅助　教授 都倉 信樹 教授 豊田 順一　教授 鳥居 宏次

論文内容の要旨

本論文は代数的仕様記述の検証に関する研究を2章にまとめたものである。

通常，代数的仕様記述の検証では，与えられた仕様の公理系を項書き換え系とみなして，項を書き換えることにより，検証作業を進めていくが，その検証作業は煩雑である。そのため，項の書き換え等の作業を実行することを目的とする検証支援系が幾つか提案されているが，実際的規模の検証に対しては，機能が十分でないのが現状である。本論文の第1章では，筆者らが作成した代数的仕様検証支援系の概要について述べている。本支援系はAFFIRMシステム等と同様，主として項書き換え系上での検証を支援するシステムであるが，(1)与えられた項書き換え系のChureh－Rosser性や有限停止性を前提としない，(2)プレスブルガー文の真偽判定機能を持つ，(3)記述言語の変更に容易に対応できる，等の特徴を持つ。

従来，項書き換え系上で検証を行う場合，検証が形式的に行える反面，プール代数や整数の性質など基礎的な数学の諸性質についても，すべて検証者が公理として導入しなければならず，検証が煩雑になる等の問題点があった。筆者らの支援系では，プレスブルガーの算術に関する性質（ブール代数や整数の加減算，大小比較に関する幾つかの基本的性質を含む）のみを用いて検証できる部分は，検証が完全に機械的に行えるよう，プレスブルガー文の真偽判定機能を組み込んでいる。この機能は，第2章で述べるHDLC手順の検証等で有効に利用できた。

従来，代数的に書かれた仕様の検証例として引き合いに出されるものは，配列と整数の対で正しくスタックが実現されるか等，非常に簡単なものが多く，実用的な規模の問題に対する検証例がほとんど報告されていない。そこで本論文の第2章では，代数的に記述されたハイレベルデータリンク制御（HD

LC）手順の検証結果について報告する。一般に，HDLC手順のような伝送制御手順（プロトコル）の記述法は，状態遷移図を利用する方法と，プログラム言語を利用する方法とに大別される。前者の記述法を用いた時の検証における問題点は，プロトコルの複雑化に伴い，状態数が急激に増加することであり，後者の問題点は，処理順序の一意的記述により過剰規定に陥り易いことや，利用する言語の意味の形式的定義が複雑であることである。代数的仕様記述法は，状態遷移図等では取り扱いの困難なシーケンス番号やパラメータ値の取り扱いが簡単に記述でき，又，一般のプログラム言語に比べ意味の形式的定義が容易であるなど，上述の欠点を免れ得る有効な手法の1つであると考えられる。

筆者らは，まずHDLC手順の規格を分析し，その結果に基づきHDLC手順を用いて通信を行う通信系を抽象的な順序機械とみなして，その代数的記述を作成した。すなわち，通信系に対し内部構造を陽に持たない抽象的な“状態”を導入し，送信や受信といった動作を“状態遷移関数”として，又，各局の状態変数等を状態からの“出力関数”として導入した。そして，それぞれの状態遷移後における各出力関数の値が，遷移前の状態における各出力関数の値からどのように定まるかを公理として表した。次に，この記述が公理系として“矛盾なく”且つ“不促なく”書かれていることを示すと共に，この記述において成立する幾つかの重要な論理関係式（例えば，通信系全体の動作可能性や1，2次局の状態変数間に成立する関係等）の検証を行った。検証は主として構造的帰納法を用いて行い，検証作業には上述の検証支援系を利用した。

論文の審査結果の要旨

本論文は代数的仕様記述の検証に関する研究を2章にまとめたものである。第1章では，著者が中心となって設計，作成した検証支援系について述べられている。主として項書き換え系上での検証を支援するシステムであるが，項書き換え系が有限停止性をもつための十分条件の判定機能，Knuth-Bendixの完全化法を利用者が適宜介入して効果的に実行する機能，プレスブルガー文の真偽判定機能等をもち，検証例についてこれらの機能が如何に有効であったかが示されている。第2章では，ハイレベルデータリンク制御手順の検証結果が示されている。制御手順の規格を分析し，その結果に基づいて，制御手順を用いて通信を行う通信系を抽象的な順序機械とみなして，その代数的記述を作成し，この記述が矛盾なくかつ不足なく書かれていることを示すと共に，伝送手順において成立すべきいくつかの重要な不変式が実際に成立することを，代数的記述に基づき，構造的帰納法を用いて厳密に示している。これは，伝送制御手順の記述と検証に関して，代数的記述法とくに，抽象的順序機械としての表現法が如何に有効であるかを示している。これらの成果は，プログラムの仕様記述と検証問題に対する大きな貢献であり，博士論文として価値あるものと認める。