| | |
|---|---|
| 氏名 | 岡野浩三（おかのこうぞう） |
| 博士の専攻分野の名称 | 博士（工学） |
| 学位記番号 | 第 11970 号 |
| 学位授与年月日 | 平成7年3月23日 |
| 学位授与の要件 | 学位規則第4条第2項該当 |
| 学位論文名 | **順序機械型プログラムの階層的設計と分散実行プログラム群への変換** |
| 論文審査委員 | （主査）<br>教授 谷口 健一<br>（副査）<br>教授 藤井 護　教授 首藤 勝　教授 萩原 兼一 |


## 論文内容の要旨

本論文は，大域変数を表す内部レジスタの同時更新と入出力動作を一状態遷移で行う順序機械型モデルによるプログラムの階層的設計法と分散動作仕様群の自動導出に関する研究をまとめたものである。この順序機械型モデルでは多くの実用システムを記述することができる。一般に高信頼システムを設計する際，抽象レベルから具体レベルに順次詳細化していく方法が有効であり，本研究では，順序機械型モデルに対して以下の二つの研究を行った。

第一に，代数的言語 ＡＳＬを用い，階層的設計の有用な枠組として，拡張射影，到達正当性条件を用いた記述法，及び，これらを用いた記述の詳細化の定義，証明法を提案する。順序機械型の要求記述を自然に行う枠組として拡張射影の概念を導入する。順序機械型プログラムの最上位の要求は，普通，入力系列と出力系列の満たすべき関係のみを指定する。この関係は直接表せないので，補助的な内部レジスタを想定し，入力系列と補助的な内部レジスタ，及び，内部レジスタと出力系列の，それぞれの満たすべき条件を記述し，それらを満たす入力系列と出力系列のすべての組合せとして，この関係を指定する。拡張射影を用いた記述に対する詳細化の正しさの証明法も与える。次に，初期状態から正当な入力系列が与えられたときのみ到達可能な（内部レジスタの状態も含めた）抽象状態において真となる述語（到達正当性条件）を定義し，これを前提条件にして状態遷移の要求記述を行うスタイルを提案する。また到達正当性条件を用いた記述に対する詳細化の正しさの証明法を与える。この証明法における論法，手間等は前提条件を具体的に記述するスタイルと比べほぼ同じである。また，以上の二つをプログラム設計の公開問題である在庫管理の階層的設計に適用した。

第二に，信頼できる通信環境と信頼できない通信環境それぞれに対して，分散システムの動作仕様の導出アルゴリズムを考案した。順序機械型モデルによる単一のプログラムを，複数のノードからなる分散計算システムの抽象的な全体仕様とする。入出力動作を行うゲートと内部レジスタの各ノードへの割り当てを設計者が指定する。この全体仕様と割り当てをアルゴリズムの入力とし，信頼できる通信環境において，与えられた全体仕様とおりに動作し，割り当てを満たす各ノードの動作仕様を出力とする。この際，この導出法で採用している模倣方針のもとで，全体仕様の一状態遷移ごと必要なメッセージの送受信数を最小にする。信頼できない通信環境に対する導出アルゴリズムでは，高々一箇所リンク故障を起こすような通信環境を仮定する。リンク故障によるメッセージ損失を回避し，かつ高速に動作する方法として同一情報を持つ複数のメッセージを異なる経路で送受信する方法をとる。全体仕様の一状態遷移ごと必要なメッセージの送受信数を最小にする。

## 論文審査の結果の要旨

本論文は，多くの実用ソフトウェアシステムが記述できる順序機械型計算モデルを対象に，プログラムの階層的設計法と分散環境で実行されるプログラム群の自動導出に関する研究をまとめている。

代数的言語を用いた階層的設計では，仕様記述の枠組や証明方法が重要である。本論文では，仕様記述の新しい枠組の一つとして，「拡張射影」の概念を提案しており，それを用いると，抽象レベルにおいて，従来記述できなかったプログラムの入出力の満たすべき関係のみを自然に記述できる。さらに，状態遷移による動作の要求記述を行うとき，前提条件として，「正当性条件」を用いる記述スタイルを提案している。「正当性条件」を用いると，要求記述時に，具体的な前提条件をいちいち考慮しなくてもよく，また，成立しない条件を誤って書いて記述全体が意味のないものになる恐れもなくなる。「拡張射影」や「正当性条件」を用いた記述に対して，詳細化が正しいことを証明する有用な方法も与えている。さらに，これらの記述法をプログラム設計の公開問題に適用し，実用的にも有用であることを確認している。

次に，分散システムの全体仕様から，各ノードのプログラムを導出するアルゴリズムを，信頼できるネットワークと信頼できないネットワークそれぞれについて，考案している。導出されるプログラム群で用いているメッセージ交換方式は一般的な場合の実行動作数が最小のものであり，その中で，全体仕様の一状態遷移を模倣するのに必要なメッセージの送受信数が最小のものを求めている。どちらのアルゴリズムでも，実用的な時間内でプログラム群が自動生成できることを実験により示している。

以上の研究成果は，ソフトウェアの階層的設計法，及び分散システムの設計法に関する研究分野の発展に貢献しており，本論文は博士（工学）論文として価値あるものと認める。