氏　名（本　籍）	郷　健太郎（熊本県）
学位の種類	博　士（情報科学）
学位記番号	情博第14号
学位授与年月日	平成8年3月26日
学位授与の要件	学位規則第4条第1項該当
研究科，専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	**段階的詳細化に基づく通信システムの仕様記述に関する研究**
論文審査委員	（主査） 東北大学教授　白鳥　則郎　　東北大学教授　根元　義章 東北大学教授　牧野　正三

論　文　内　容　要　旨

高品質・高信頼な情報通信システムを構成するうえで，その開発工程の初期段階に相当するシステムの仕様記述工程は，極めて重要な役割を持つ。特に，仕様記述工程において誤りを含むような仕様を記述した場合，その仕様が与える影響は開発工程の下流工程にまで及ぶ。したがって，仕様記述工程において，システムの仕様を系統的に設計するための手法を導入することが必要となる。しかしながら，このような手法は十分には確立されていない。本論文は，段階的詳細化に基づく情報通信システムの仕様記述に有効な，仕様の分割法と変更法の詳細な研究を行なった結果をまとめたものであり，全編6章から成る。

第1章は序論であり，本研究の背景と目的について述べている。

第2章では，形式記述技法について概括している。まず，形式記述技法の背景について述べ，システム設計工程におけるその利点と欠点を詳細に論じている。特に，ISOにより標準化されている形式記述技法LOTOS（Language Of Temporal Ordering Specification）を対象とし，その特徴を構文と意味の観点から述べている。次に，LOTOSを含めた一般のプロセス代数仕様の意味表現として採用されているラベル付き遷移システム（LTS：Labelled Transition System）について，その形式的定義を述べている。さらに，仕様における等価性の概念について，仕様間の強双模倣等価と弱双模倣等価について述べている。

第3章では，LOTOS仕様の系統的な分割法を構成することを目的に，次の2項目を提案している。(1)仕様を構成するアクション集合の分割をもとに，分割の前後で仕様の動的振舞いの等価性を保つような分割法を構成する。(2)等価性を保つために，分割された仕様において同期しなければならないアクション集合を規定した仕様を自動合成する。

まず，LOTOSにおける仕様の分割問題を定式化する。LOTOS仕様の分割問題はLOTOS仕様の記述スタイルの観点から，2つの異った記述スタイルの間のスタイル変換問題とみなすことができる。すなわち，ここでのLOTOS仕様の分割法とは，システムの内部構造を記述しないモノリシックスタイルの仕様を，システムの個別的な機能の制約を表現したプロセスを並列オペレータで合成した形式で仕様を成す制約指向スタイルへ自動変換する記述スタイル変換法に相当する。

次に，この問題を解決する系統的な分割法を構成している。分割法に対する入力は，(a)モノリシックスタイルのLOTOS仕様と(b)この仕様を構成するアクション集合の分割の2項目である。これらの入力に対し，分割法は(b)の集合を基準にして(a)の仕様を分割する。さらに，この分割法の特徴は，分割後の仕様が並列合成オペレータを使って結合されたときに，これが(a)の仕様と強双模倣等になるように制約を与える仕様を導出する点にある。

続いて，本章で構成した分割法の持つ諸性質について議論している。この過程から最終的に，構成した分割法に対する分割前の仕様と，分割後の仕様を並列合成した仕様が強双模倣等価関係を保つことを証明した。すなわちこの分割法では，分割前の仕様の正当性を分割後の仕様においても完全に保存する。これは，特に高信頼システムを設計するうえで有効である。

第4章では，次の2つの観点からラベル付き遷移システム上での分割法を構成している。(1)前章で構成したLOTOSに対する分割法の適用領域を拡大し，一般のプロセス代数仕様に適用可能な分割法を構成する。(2)前章で与えた仕様に関する制限を取り除く。

ここで(2)に関して，第3章で構成した分割法は，分割可能な仕様に対して次のような3つの制限与えている。(a)記述されている各アクションは互いに違う名前を持つ，(b)プロセスの外部から観測不可能な内部アクションを記述しない，(c)再帰構造を持たない。本章では，分割法を仕様に関するこれらの3つの制限に対応して3つの段階に分け，その制限を段階的に削除し，最終的に制限のない仕様に対する分割法を構成している。

まず第1段階では，(3)の制限を取り除いた仕様に対する分割法を構成する。具体的には第3章で構成したLOTOS仕様上での分割法の戦略をLTS上に移したうえで分割法を構成している。この分割法は以下に続く段階の基礎となる分割法である。

次に第2段階では，第1段階で構成した分割法を効果的に利用し，(2)と(3)の制限を取り除いた仕様に対する分割法を構成する。(2)の制限を取り除いた場合に，第1段階の分割法による分割の前後で仕様の等価性を保つためには，アクションの望ましくない非決定性の出現が問題となる。この非決定性を決定性に書換えるために，分割前のプロセスの各状態の性質と分割後のプロセスにおける対応する状態の性質を分類し，各項目に応じた適切なプロセスの書換えを行なっている。この処理により，分割の前後で仕様の等価性を保つことが可能になった。

最後に第3段階では，第2段階までに構成した分割法を利用し，すべての制限を取り除いた仕様に対する分割法を構成する。具体的には，内部アクションに関する前処理と後処理を第2段階の分割法に加えることで，第3段階の分割法としている。内部アクションは，観測可能なアクションと異なり，他のアクションとの同期なしで生起する。この性質を考慮すると，内部アクションを含むプロセスの分割として，次のような戦略が考えられる。まず入力仕様からすべての内部アクションを取り除く。この操作は，内部アクションがラベル付けされた遷移の前状態と後状態を同じ状態とみなすことで実現できる。こうして得られたプロセスに対して第2段階の分割法を適用する。結果として得られたプロセスに対し，これらの並列合成が入力仕様と等価になるような適切な状態に内部アクションの遷移を挿入する。以上の操作を実現しているのが第3段階の分割法である。

本章では，以上の各段階ごとに，構成した分割法に対する分割前の仕様と分割後の仕様を並列合成した仕様が，強双模倣等価関係を保つことを証明した。これは，分割法の実用上重要な結果である。

第5章では，段階的詳細化に適した仕様の変更法について考察している。

まず，設計工程の初期段階における要求の変更に柔軟に対処する方法として，ソフトウェアのやわらかい開発法と呼ぶ枠組を構成している。これは，「やわらかいシステム」の適応性を実現するための基盤技術として位置付けられる。具体的には，要求仕様の変更に対して，システム仕様がそれを充足しない場合に，既存のシステム仕様を効果的に再利用し，変更後の要求仕様を充足するような仕様を構成するための理論的枠組である。

次に，その応用として，情報通信システムのサービス仕様の変更に対するプロトコル仕様の自動変更法を提案している。

本章では，まず通信システムをLTSでモデル化する。そして，LTSで表現された通信システムのサービス仕様における変更要求を，複数のLTSの組で表現されたプロトコル仕様に反映させるという手法を実現している。本章の研究のシナリオは次のとおりである。既存のサービス仕様と，あるプロトコル合成法によって合成されたプロトコル仕様を仮定する。これらの間には弱双模倣関係が成立しているとする。いまサービスに対して新たな要求が加えられ，サービス仕様が修正されたとする。本章で構成する手法の目的は，この修正後のサービス仕様から再度プロトコル仕様を合成することなく，既存のプロトコル仕様を修正することで，修正後のサービス仕様と弱双模倣等価なプロトコル仕様を構成することである。

サービス仕様の変更の種類は次の2つに大別される。(1)追加：仕様に情報を加えること，(2)削除：仕様から情報を

一部取り除くこと。これらの変更をサービス仕様で実現するにあたり，次の2つの理由から，仕様の追加変更部分が既存の仕様から独立したコンポーネントであるのが望ましい。(a)新しいコンポーネントを単独で論理検証することができる。(b)既存の仕様が実装されていた場合に，変更部分だけを独立に実装できる。

本章では，並列合成オペレータを使い，まずサービス仕様において追加変更目標を並行プロセスとして，すなわち既存のサービス仕様とは独立のコンポーネントとして表現する手法を与え，次にこの並行プロセス相当する変更をプロトコル仕様において実現する手法を与える。さらにサービス仕様における削除変更目標を実現するために，LTS 上でアクションの隠蔽オペレータを定義し，このオペレータを効果的に用いてプロトコル仕様での変更を実現している。

以上の手法によって変更されたプロトコル仕様は，サービス仕様で保証されている正当性を保存する。そのため本手法は，高信頼システムの設計工程における要求仕様の円滑な変更や拡張に有効となる興味深い知見である。

第6章は結論であり，本研究で得られた結果を総括している。

以上，本論文の結果は，形式仕様の段階的詳細化を効果的に進めるための基盤として，仕様の正当性を保存する系統的な仕様の分割法と変更法という信頼できる手法を提供する。これらの手法を導入することで，仕様の分割・変更作業にともなう仕様の検証作業の負担を軽減することができる。その結果，システム開発における生産性の大幅な向上が期待できる。

審 査 結 果 の 要 旨

近年，情報通信システムの利用者の増加にともない，システムに対する利用者要求は多種多様化している。これらの要求を満足させるため，必然的にシステムは大規模・複雑化しているが，高品質・高信頼システムの仕様を設計するための手法は，十分には確立されていない。そこで筆者は，段階的詳細化に基づく情報通信システムの仕様記述に有効な仕様の分割法と変更法の詳細な研究を行なった。本論文はその成果をまとめたものであり，全編6章から成る。

第1章は序論である。

第2章では，本論文で対象としている形式記述言語LOTOS，および，その意味表現であるラベル付き遷移システムについて述べている。さらに，形式仕様における等価性の概念について述べている。

第3章では，LOTOSにおける仕様の分割問題を定式化し，その問題を解決する系統的な分割法を構成している。さらにこの分割法が，分割の前後における仕様の等価性を保存することを証明している。この結果は，本分割法を用いた仕様分割の正当性を保証しているため，特に信頼性の高いシステムを設計する上で有効である。

第4章では，前章で構成したLOTOSに対する分割法の適用領域を拡大し，また，前章で与えた仕様に関する制限を除いたラベル付き遷移システム上での分割法を構成している。ここでは分割法を仕様に関する3つの制限に対応して3つの段階に分け，その制限を段階的に削除し，最終的に制限のない仕様に対する分割法を構成している。これは実用上重要な結果である。

第5章では，段階的詳細化に適した仕様の変更法について考察している。具体的には，設計工程の初期段階における要求の変更に柔軟に対処する方法として，ソフトウェアのやわらかい開発法と呼ぶ枠組を構成している。また，その応用として，情報通信システムのサービス仕様の変更に対するプロトコル仕様の自動変更法を提案している。この手法によって変更されたプロトコル仕様は，サービス仕様で保証されている正当性を保存する。そのため本手法は，高信頼システムの設計工程における要求仕様の円滑な変更や拡張に有効となる興味深い知見である。

第6章は結論である。

以上要するに本論文は，段階的詳細化に基づく情報通信システムの仕様記述に有効な基盤技術として，仕様の分割法と変更法についての理論的研究を行ない，高品質・高信頼な情報通信システムを構築するための有用な知見を与えたものであり，情報基礎科学の発展に寄与するところが少なくない。

よって，本論文は博士（情報科学）の学位論文として合格と認める。