

論文内容の要旨

博士論文題目 Zによるシステム仕様記述のための変換技術に関する基礎的研究

氏名 張 漢明

本論文は、信頼性の高いシステム仕様記述を効率良く作成するために、対象システムのモデル化、およびシステム記述の分析を支援するための形式仕様記述言語Zによる仕様記述の変換技術に関する研究をまとめたものであり、序論と結論を含め八つの章から構成されている。

第一章では、ソフトウェア開発における問題点と課題について議論し、本研究の目的と研究方針、および変換技術の意義を述べるとともに、本論文の内容を概説している。本研究では、変換の対象として、1)システム内部状態のモデルの変換、2)仕様記述の構造の変換、3)システム状態不変条件の記述の変換、4)図式表現と形式的な表現の間の変換について着眼している。

第二章では、本研究の対象として用いている形式仕様記述言語Zの概要と仕様記述の概念を説明するとともに、本論文で具体的な例題として用いている「予約管理システム」の仕様を記述している。

第三章では、システム内部状態のモデルの変換として、二項関係モデルにおける変換技術について述べている。Zにおける二項関係モデルの中でも最も特徴的な全域関数、部分関数、関係の3つの間の対応関係に着眼し、1)全域関数と部分関数の間の変換手法と、2)部分関数と関係の間の変換手法、を提示している。

第四章では、仕様記述の構造の変換として、階層的な機能分割を行う手法について述べている。階層的機能分割とは、階層的な構造を持たないシステムの仕様記述から、階層的に機能分割された仕様記述を得ることである。階層的機能分割では、1)機能分割と、2)階層化の変換手法を提示している。

第五章では、システム状態不変条件の記述の変換として、操作の仕様記述の中に暗黙的に表現されているシステムの内部状態に対する制約を、明示的に表現されたシステム状態不変条件として変換する手法を提示している。

第六章では、図式表現と形式的な表現の間の変換として、構造化ダイアグラムから形式的な表現(Z仕様記述)に変換する手法について述べている。直観的で人間になじみやすい図式表現と形式的な表現との間の関係について着眼し、CASEツールで広く用いられているデータフロー図、および実体関連図の構造化ダイアグラムで表現された記述の分析を行うために、図式表現から形式的な表現への変換手法について議論している。異なった図式表現を統一された形式的な表現(Zで記述)に変換することにより、異種のダイアグラム間の一貫性の検証を可能にしている。

第七章では、仕様記述の過程を分析し、変換を基にした仕様記述のための支援技術、および開発支援環境について議論している。本研究では、仕様記述の過程を、理解、記述、分析の繰り返しであると捉え、仕様記述の書き換えの作業を定式化することにより、仕様記述者がアドホックに行っていた仕様記述の書き換えの作業を改善する。

第八章では、以上の本研究で得られた研究成果についてまとめ、今後の課題を明らかにしている。

氏名	張 漢明
----	------

論文審査結果の要旨

本論文は、ソフトウェアシステムの開発において、対象システムのモデルと仕様記述が試行錯誤を経て得られることに着眼し、仕様記述完成までに至る過程を仕様に対する変換と捉え、その過程を形式仕様記述言語 Z を用いて定式化することを試み、形式仕様記述言語 Z による仕様記述変換技術として、二項関係モデルにおける仕様記述変換、階層的機能分割、システム状態不変条件の変換、図式表現と形式的な表現の間の変換を提案し、その有効性を示したものである。本論文の主な成果は以下に要約される。

1. Z 仕様記述におけるシステム内部状態のモデルとして通常よく利用される全域関数、部分関数、関係の3つの二項関係モデルの特徴を分析することにより、全域関数と部分関数との間の対応関係と、部分関数と関係との間の対応関係を明確にし、それぞれの間の体系的な変換手法を与えた。

2. Z のスキーマ合成の表記を用いて、システム設計において重要な作業の一つである機能分割と階層化の体系的な手法の一つを与えた。階層的機能分割の手法は、機能とデータの分割、および階層間のインタフェースを検討する際の指針を与え、従来、仕様記述者がアドホックに行っていた仕様記述の分割と階層化の作業を改善する効果がある。

3. 操作仕様記述におけるシステム状態不変条件の抽出では、内部状態に影響を与える記述を明示するための変換手法の基礎を与えた。システム状態不変条件は、 Z では状態スキーマとして記述され、システムが満たすべき性質を検討・理解する上で重要な情報である。また、操作の仕様記述がシステム状態と矛盾がないかを検出するためには、システム不変条件を明示する必要がある。本手法は仕様記述の整合性を議論する際の有効な手段の一つである。

4. 実体関連図やデータフロー図の構造化ダイアグラムの図式表現に対する厳密な分析・論証を行うための数学的な基礎づけを与えた。図式表現から形式的な表現への変換技術は、形式的な仕様記述を考える際の直観的な思考を促進し、形式仕様記述の作成を支援するための実用的な手段として利用できる。

5. 図式表現から形式的な仕様記述の変換技術の応用として、統一的な形式的な言語(Z)を用いた仕様記述の上で、異なる図式表現間の一貫性を保証するための手法を与えた。CASEツールで広く用いられている図式表現を対象とした変換手法を提示している点で、実用上評価できる技術である。

以上のように、本論文は、対象システムのモデル化、およびシステム記述の分析を支援するために、形式仕様記述言語 Z による仕様記述変換技術を提案し、仕様記述を構築する際に変換手法を適用することの有効性を示唆したものであり、ソフトウェア開発における形式的手法の分野において、学術上、実際上寄与するところが少なくない。よって本論文は博士(工学)の学位論文として価値あるものと認める。