2F－4　シミュレーション関係を用いた大規模システムの部分検証に関する考察

山野敬一郎　高橋薫　土岐田義明

(株)高度通信システム研究所

1　はじめに

近年、通信システム等の仕様を厳密に記述するために、種々の形式的仕様記述技法(FDT)が提案されている。我々は、このFDTの一つであるLOTOS(ISO8807)を中心とした、通信ソフトウェアの設計支援環境ITECS(InTegrated Environment for Constructing high-reliable Software)[1]を提案し、開発を行っている。ITECSで用いられている仕様検証手法は、上位レベルのLOTOS仕様から下位レベルへと正しく詳細化が行われているかどうか、シミュレーション関係[2][3]の概念を用いて検証するものである。しかし、通信システムの仕様は巨大であり、詳細化仕様全体を一度に検証することは、計算量等の観点から現実的ではない。従って本報告では、段階的な仕様の詳細化と、それに基づいて分割された仕様に対する、部分検証に関する方法論を考察する。

2　仕様設計支援環境: ITECS

現在我々は、通信ソフトウェアの設計支援環境ITECSの開発を行っている。図1に示すように、ITECSではまず図的仕様定義環境を用いて、LOTOS、SDL、MSC等の仕様記述技法による要求仕様を与える。次に、これらの要求仕様をLOTOSに統合し、仕様の検証を行いながら、段階的な詳細化を行う。最終的に、LOTOSによる詳細化仕様を生成し、これをもとに実際のソフトウェアを開発する。

ここで用いられている詳細化および検証の手法は、図2に示すような仕様の詳細化過程に従っている。すなわち、抽象度の高い要求仕様から、抽象度の低い詳細仕様まで、段階的な詳細化を行う。ここで、詳細化の各段階において、以下のような仕様検証手法を適用する。まず、与えられたレベルN仕様をもとに、1段階抽象度を低くしたレベルN+1仕様を定義する。次に、このレベルN+1仕様が、レベルN仕様を正しく詳細化しているか、シミュレーション関係の概念を用いて、文献[4]の判定アルゴリズムにより検証を行う。検証結果が正しければ、さらにこの過程を繰り返す。

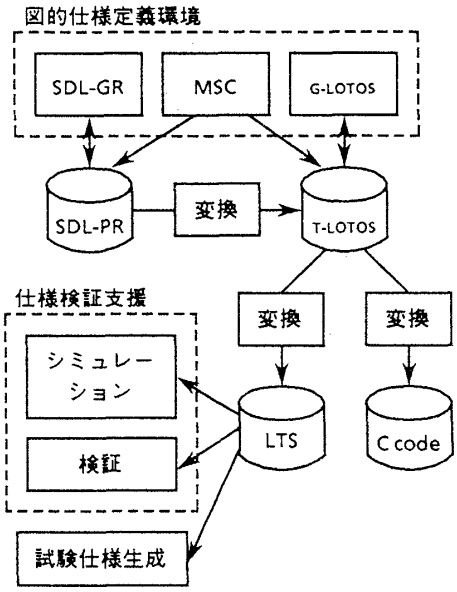

図1　ITECSシステム構成

以上の段階的な詳細化の過程を、与えられた要求仕様をもとに、ソフトウェア仕様として十分な詳細化が行われるまで繰り返す。この結果、最終的に得られる詳細仕様が、与えられた要求仕様を正しく実現していることが保証され、高信頼な通信ソフトウェアの設計支援が可能になると考えられる。

A Partial Verification for Large Systems using the Simulation Relation

Keiichirou YAMANO, Kaoru TAKAHASHI, Yoshiaki TOKITA

Advanced Intelligent Communication System Laboratories

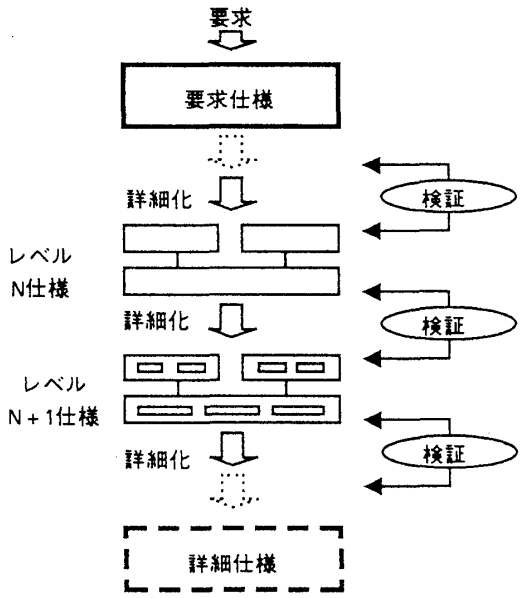

図2　仕様の詳細化過程

3　部分検証に関する考察

前節で述べた、シミュレーション関係を用いた二つの仕様間の検証手法は、仕様の全体の動作確認を行うため、仕様の規模が小さい場合には有効である。一方、詳細化のレベルが進み、仕様が大規模になると、その適用が困難になる。ITECSの対象となる通信ソフトウェアの仕様は、一般的に非常に大規模･複雑であり、詳細化した仕様全体を一度に検証することは、計算量等の観点から現実的ではない。この解決法として、大規模な仕様を分割し、分割された部分的な仕様に対する検証を行うことが考えられる。以下に、この部分検証の考え方を示す。

図3において、仕様の詳細化過程における上位レベルの仕様をSpec Nとする。この仕様を、文献[5]に示す構造化手法によって、機能要素ごとに構造分割し、基本仕様Spec N'とm個の部分仕様Spec $N_{(i)}$ $(1 \leqq i \leqq m)$ を得る。ただしここで、Spec $N_{(i)} \in$ Spec N であり、Spec N' $\cup \Sigma$ Spec $N_{(i)}$ = Spec N である。次に、個々の部分仕様Spec $N_{(i)}$ の詳細化を行い、下位レベルの部分仕様Spec $N+1_{(i)}$ $(1 \leqq i \leqq m)$ を得る。また、基本仕様に関しては、Spec N' = Spec N+1' であるとする。これより、下位レベルの仕様Spec N+1は、個々の詳細化部分仕様を合成したものであり、Spec N+1 = Spec N' $\cup \Sigma$ Spec $N+1_{(i)}$ が得られる。ここで、各部分仕様Spec $N_{(i)}$ に対して、その詳細化仕様Spec $N+1_{(i)}$ とシミュレーション

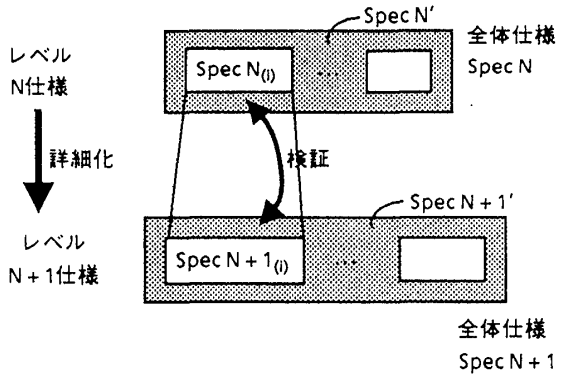

図3　仕様の詳細化と部分検証

関係を適用した検証を行う。最終的に、全ての部分仕様の検証結果が正しければ、詳細化部分仕様を合成した下位レベルの全体仕様Spec N+1も正しく詳細化されていることを確認する。

このように、仕様の詳細化過程において、仕様の構造化分割とシミュレーション関係を用いた部分検証を行うことによって、大規模なシステムの仕様記述においても、効率的な仕様の検証を行うことができると考えられる。

4　おわりに

本報告では、通信ソフトウェア設計支援環境ITECSにおける、仕様の段階的な詳細化とその検証について述べた。さらに、構造化手法による仕様の分割とその検証法に関する考察を行った。この手法の適用により、大規模な通信ソフトウェアの設計においても、効果的な仕様の記述および検証が行えると考えられる。

今後の課題としては、仕様の詳細化過程における、部分検証の定式化と、具体的な分割手法の検討を行う必要がある。

参考文献

[1] 太田 他：“通信ソフトウェア設計支援環境：ITECS(1)-全体構成-,” 情報処理学会第46回全国大会, 6J-2 (1993).

[2] R.Milner : “Communication and Concurrency,” Prentice Hall (1989).

[3] K.Yamano, et al. : “Formal specification and verification of ISDN services in LOTOS,” IEICE Transactions on Communications, E75-B, No.8 (1992).

[4] 高橋 薫, 山野 敬一郎, 太田 正孝：“プロセス仕様の検証のための模倣性判定法,” 電子通信学会論文誌 Vol.J76-D-I, No.1 (1993).

[5] 更科 克幸, 安藤 津芳, 太田 正孝, 高橋 薫：“形式仕様記述言語 G-LOTOS の記述試験,” 情報処理学会 ソフトウェア工学研究会, SE 89-19, pp.147-154 (1992).