6K－5 通信ソフトウェア設計支援環境ITECSにおける仕様検証支援 *

山野 敬一郎　土岐田 義明 †

(株)高度通信システム研究所 ‡

1 はじめに

通信ソフトウェア等の開発を行う上で、その設計段階において仕様を誤りなく厳密に記述することが重要視されている。このため、種々の形式記述技法(FDT)が提案され、あわせてその支援環境が開発されている。

現在我々は、通信ソフトウェアの設計を高信頼かつ効率的に支援するための環境として、FDTの一つである*LOTOS*(ISO8807)を中心とした支援環境*ITECS (InTegrated Environment for high reliability Communication Software design)*[1]を提案し、開発を行っている。本稿では、ITECSにおける仕様検証支援環境の紹介を行う。

2 仕様の詳細化過程と検証

通信ソフトウェア等の大規模システムの仕様の開発過程は、図1に示すような仕様の段階的な詳細化過程として位置づけられる。

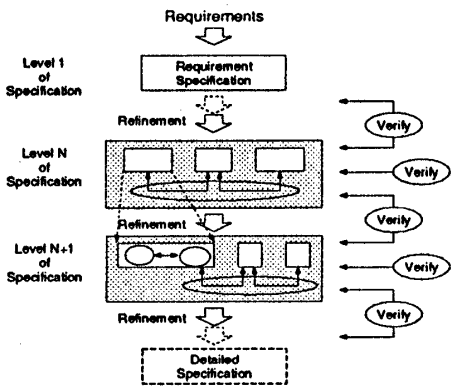

図 1: 仕様の詳細化過程

つまり、ある要求仕様をもとに、それを段階的に詳細化していくことによって詳細設計仕様が得られ、最終的に実際のソフトウェアを開発するという過程である。この過程を高信頼に支援するためには、(i)各詳細化段階における仕様の正当性の検証、つまり仕様が設計者の意図を正しく反映しているかどうかの検証に加えて、(ii)仕様の詳細化過程における仕様間の無矛盾性の検証、つまり詳細化された下位レベルの仕様が上位レベルの要求仕様を正しく実現しているかどうかの検証を行うことが重要となる。

3 ITECSにおける検証支援

ITECSでは、システムの仕様はLOTOSによって記述され、段階的な詳細化が行われる。この過程において、LOTOS仕様の意味導出を行うツールALTAIRと、二種類の検証支援ツールVegaとVenusを用いることにより、LOTOSで記述された仕様に対する上記の仕様検証を実現している。

以下、本稿では特に後者の検証を行うVenusと、LOTOS仕様の検証を行うための前処理として必要なALTAIRについて説明する。

3.1 ALTAIR

一般的に、LOTOSによって記述された仕様を機械的に検証するには、まず対応する意味表現を導出する必要がある。ITECSでは、LOTOSの意味導出ツールであるALTAIRにより、この機能を提供している。

ALTAIRはLOTOS標準に従い、まず入力されたLOTOS仕様の字句解析、構文解析、静的意味解析を行う。次に、そのLOTOS仕様の動的意味を解析し、意味モデルである“遷移システム”を導出する。この導出は対話的あるいは自動的に行われる。遷移システムは一種の状態遷移図であり、状態、状態遷移、状態遷移を起こすアクション(イベント)から構成され、仕様が意味するシステムの動作を表している。付加機能として、ALTAIRは得られた遷移システムをグラフ的に表現することによって、動作をわかり

---

* The Verification Support in ITECS

† Keiichirou YAMANO, Yoshiaki TOKITA

‡ Advanced Intelligent Communication System Labs.

やすく設計者に表示する等の機能も備える。

図2に、ALTAIRの実行画面を示す。

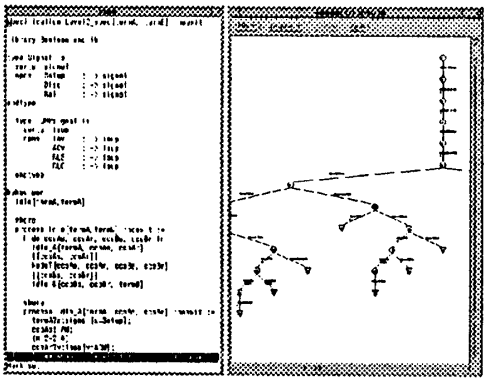

図 2: ALTAIR実行画面

3.2 Venus

Venusは、仕様の詳細化過程における仕様間の無矛盾性の検証を行うツールである。具体的には、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どうかの検証を行う。ITECSにおいて、これらの各レベルの仕様はLOTOSで記述されるため、LOTOSの数学的ベースであるプロセス代数の概念を用いて検証を行うことができる。

まず、仕様の詳細化においてシステムの内部の動作のみが詳細化され、外部的に観測される動作が変化しない場合を考える。このような場合、Venusでは二つのLOTOS仕様間の関係としてよく知られている弱bisimulation等価の概念を用い、無矛盾性の検証を行う。

一方、仕様の詳細化過程では、付加的な情報を加える場合や、複数の上位レベルの仕様を組み合わせて下位レベルの仕様を構成する場合がある。このような場合には、一般的な等価性の概念を適用することができない。従って、Venusでは Simulation 前順序 [2, 3] の概念を用い、無矛盾性の検証を行う。

実際には、Venusでは前述のALTAIRによって導出された遷移システムを対象として検証を行う。つまり、2つのLOTOS仕様にそれぞれ対応する2つの遷移システムを入力すると、決められた判定手続きに従い上記のいずれかの概念に基く検証を実行し、検証結果を出力する。結果は、設計者が実行の際に指定した関係が“成立する”か“否”かで表される。この他にも、検証過程のトレース表示、遷移システム上の関連した状態の強調的なグラフ表示などの機能を有する。これらは分析情報として、仕様のチェックに対して有益な情報となる。

図3に、Venusの実行画面例を示す。

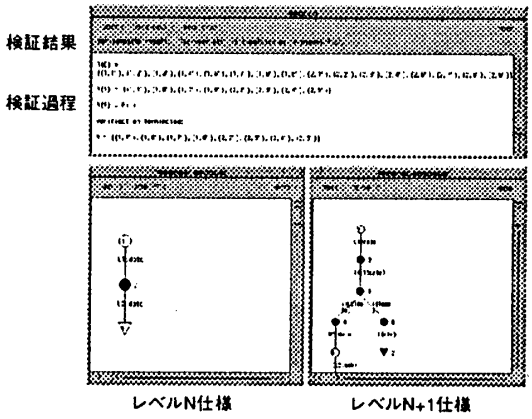

図 3: Venus実行画面

4 おわりに

本稿では、ITECSの仕様検証支援環境としてALTAIRとVenusについて述べた。ALTAIRではLOTOS仕様の意味導出を行い、Venusでは仕様の詳細化過程における仕様間の無矛盾性の検証を行う。これらのツールを用いることによって、最終的に得られる詳細化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。

現在、ISDNの基本呼サービスを例にとり、通信サービスのLOTOSによる仕様化、および仕様検証の適用可能性の検討を行っている。

参考文献

[1] K.Takahashi, et.al.: “ITECS: An Integrated Environment for Communication Software Design,” Proc. of ITS ’94, Vol. II, pp.1-8 (1994).

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

[3] 高橋 薫, 他: “プロセス仕様の検証のための模倣性判定法,” 電子情報通信学会論文誌, Vol.J76-D-I, No.1 (1993).