マルチメディア通信と分散処理 69−15
（１９９５．３．３）

LOTOSを応用した 通信ソフトウェア設計支援環境の研究

坪根 宣宏　　土岐田 義明
(株)高度通信システム研究所

筆者らは、今後一層の規模拡大が予想される通信ソフトウェアの信頼性向上を目指し、ISO標準の形式記述技法LOTOSを応用した通信ソフトウェア設計支援環境ITECSを提案し、開発を進めている。LOTOSは厳密な仕様記述や機械的な仕様検証を可能とする点に優れた特徴を持つ。ITECSはこれらの特徴を活用して信頼性の高い通信ソフトウェアの構築を目指す設計支援環境であるが、その実用化という観点からは大規模なLOTOS仕様に対する機械検証の適用性を評価する課題が残されている。本論文では、この観点からの具体的な評価課題について述べる。

Study of an Integrated Environment for Communication Software Design using LOTOS

Nobuhiro TSUBONE and Yoshiaki TOKITA
Advanced Intelligent Communication System Laboratories

We have proposed and been developing an Integrated Environment for Communication Software Design using LOTOS, which we call ITECS (Integrated Environment for high reliability Communication Software design and development). The purpose of ITECS is to reliably construct larger communication software in future. LOTOS has an excellent feature of enabling rigorous specifications and their verifications by computers. ITECS makes the most of this feature for the purpose. However, we still have some tasks to assess availability of such verifications for large scale LOTOS specifications from a point of view of its practical use. This paper will describe the tasks in detail.

1. はじめに

LOTOS[1]は1989年に国際標準として制定された通信システムの仕様を記述する形式記述技法である。LOTOSの応用研究は、欧州を中心に広く実施されている。筆者らも、4年前よりこの研究を開始し、その一環としてITECS(Integrated Environment for high reliability Communication Software design and development)[2]の開発を行っている。

LOTOSは厳密な仕様記述や機械的な仕様検証を可能とする点に優れた特徴を持つ。しかし今までの研究では、これらの特徴は理論的

な観点から評価されることが多く、交換機や計算機の通信ソフトウェアなど実システム開発への応用という立場から評価されることは少なかった。その中で、形式記述技法の応用研究を行っている欧州のMEDASプロジェクトでは、LOTOSとSDLを実際のシステム開発へ適用することにより、それらの実用性を評価している。その評価の中間報告[3]では、LOTOSやSDLを用いた大規模な仕様に対する機械検証実現の困難性について指摘がある。ただし、その困難性の具体事例については示されていない。この問題はLOTOSの実用化を目指す筆者らにとっては非常に重要であるため、その具体事例を考察し本論文にまとめた次第である。

本論文では、後の議論の準備として、まずLOTOSの意味モデルについて述べる。さらに、ITECSにおけるLOTOSによる機械検証の手法について述べた後、大規模なLOTOS仕様に対する機械検証の適用性に関する評価課題を挙げる。なお、LOTOSの詳細については文献[8][9]を参照されたい。

2. LOTOSの意味モデル

LOTOSで記述された動作の意味はLTS(Labelled Transition Systems)で表現することができる。LTSの定義は次のように与えられる。

定義1　LTS(遷移システム)

LTSは4項組$<S, Act, T, s_0>$である。ここで、Sは状態の集合、Actはアクション(イベント)の集合、$T=\{-act\rightarrow \mid -act\rightarrow \subseteq S\times S, act \in Act\}$は遷移関係の集合、$s_0 \in S$は初期状態である。

一般に一つのLOTOS仕様に対するその意味モデルであるLTSは唯一であるとは限らない。なぜなら、LTSを生成するアルゴリズムの違いにより複数の正しいLTSが存在しうるからである。LTS生成アルゴリズムの違いは、LTSを構成する状態の定義の仕方に自由度があることから生じる。ただし、一つのLOTOS仕様から生成される複数のLTSは当然同一の意味を持つはずである。従って、これらのLTSの間には何らかの等価関係が成立するはずである。本論文では、この等価関係として、LOTOSの標準で採用されている弱双模倣等価の概念を導入する。弱双模倣等価の定義は次のように与えられる。

定義2　弱双模倣等価

$Sys1 = <S_1, Act, T, \sigma_1>$、$Sys2 = <S_2, Act, T, \sigma_2>$を任意の遷移システムとし、$S = S_1 \cup S_2$とする。状態の組$(s_1, s_2) \in R$と、任意の観測可能アクション系列$\rho \in (Act-\{i\})^*$に対して次の条件(a)と(b)が成り立つ時、関係$R \subseteq S\times S$を弱双模倣等価の関係という。

(a)$s_1=\rho\Rightarrow s'_1$である$s'_1\in S$が存在するならば、$s_2=\rho\Rightarrow s'_2$で$(s'_1, s'_2)\in R$である$s'_2\in S$が存在する。

(b)$s_2=\rho\Rightarrow s'_2$である$s'_2\in S$が存在するならば、$s_1=\rho\Rightarrow s'_1$で$(s'_1, s'_2)\in R$である$s'_1\in S$が存在する。

ただし、$(Act-\{i\})^*$は$(Act-\{i\})$に属する要素を組み合せて構成した有限の長さの系列の全体、iは内部アクションを表す。また、$s_1=\rho\Rightarrow s'_1$　は$\rho=\alpha_1\alpha_2\cdots\alpha_n$，　$\alpha_k \in (Act-\{i\})$，$1\leqq k\leqq n$とする時、

$$(-i\rightarrow)^*(-\alpha_1\rightarrow)(-i\rightarrow)^*(-\alpha_2\rightarrow)\cdots$$
$$\cdots(-i\rightarrow)^*(-\alpha_n\rightarrow)(-i\rightarrow)^*$$

なるs_1からs'_1への状態遷移を表す。ここに、$-\alpha_k\rightarrow$は任意の状態間のアクションα_kによる

状態遷移、$(-i\rightarrow)^*$ は内部アクションiによる状態遷移の系列である。$s_2=\rho\Rightarrow s'_2$も同様の意味を持つ。

弱双模倣等価の概念では、LTSでモデル化される複数のシステムが外部観測上、その振る舞いの違いを識別できない時に互いに等価なものとして扱う。

3. ITECSにおけるLOTOSによる機械検証の手法

ITECSでは、LOTOS仕様に対して次の2種類の検証が行える。

(1) LOTOS仕様の時間的性質の検証
- イベントの順序関係やデッドロックの有無などを調べる。[4]

(2)2つのLOTOS仕様間の無矛盾性の検証
- 仕様を詳細化していく際に「下位の仕様が上位の仕様を正しく反映しているか」などを調べる。
- 下記2種類の検証アルゴリズムを提供している。
  - ①弱双模倣等価性 [5]
  - ②模倣関係 [6]

これらの検証は図3.1に示すように直接LOTOSの構文に対して行うのではなく、LOTOSの意味表現であるLTSに対して行う。従って、LOTOS仕様の機械検証を実現するためには、LOTOS仕様の意味を解釈してLTSを生成する機能の実現が不可欠である。LOTOS意味解釈機能に関する研究は文献[7]に見られる。現在筆者らは、ITECSの一機能として、文献[7]の研究成果を拡張したLOTOS意味解釈機能の実現に取り組んでいる。

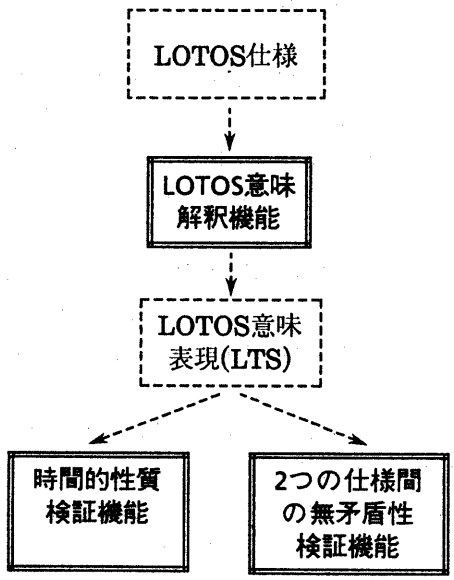

図3.1 ITECSにおけるLOTOS仕様の機械検証手順

4. 大規模仕様に対する機械検証の適用性に関する評価課題

筆者らが考察した範囲では、次に示す2つの課題があると考える。

(1) LOTOS意味解釈機能の信頼性を評価する手段の確立
(2) 大規模なLOTOS仕様における検証に要する計算時間(実用的な範囲に納まるか)

ここでは紙面の都合上、ITECSの実用化にとって特に重要と考えられる(1)の課題とその解決策について述べる。(2)の課題については別の機会に述べることとしたい。

LOTOS意味解釈機能の信頼性を厳密に評価し、その信頼性を確保することがITECS実用化のために特に重要なことは次の例で明確となる。

- 状態数1000個のLTS L1と状態数2000個のLTS L2の無矛盾性を検証する場合でも、

その検証結果は「成立」あるいは「不成立」の1ビットの情報に集約されるが、L1、L2をLOTOS意味解釈機能で生成する際にたとえ1つの状態定義を誤ったとしても、検証結果が反転し、正しい検証結果が得られない可能性がある。

LOTOS意味解釈機能の信頼性を評価するためには、「できる限り多くのLOTOS仕様に対して、そのLOTOS意味解釈機能が生成するLTSの正当性を示すこと」である。さらには、このLOTOS意味解釈機能が大規模仕様に対しても正しく動作することを保証するためには、幾つかの大規模仕様について完全に正しいLTSが生成できることを示さなければならない。

ここで、「大規模仕様」を具体的に定義する必要がある。因みに、筆者らがある交換サービスの接続シーケンスをLOTOSで記述したところ、そのLOTOS仕様の行数は140、対応するLTSの状態数は200であった。この例から考えて、実際の通信システムが記述できる規模は少なくとも数百行の規模と言える。そこで、ここでは「大規模仕様」を少なくとも数百行の規模を持つLOTOS仕様と定義する。

この際問題となるのが、「この規模のLOTOS仕様に対してLOTOS意味解釈機能が生成したLTSの正当性を如何にして示すか」である。この問題の本質は、この判断に機械的な手段が使えないことである。なぜなら、機械的な手段を使おうとすれば、結局はこのLOTOS意味解釈機能に類する機能が必要となり、堂々巡りを起こすからである。詰まるところ人手に頼るしかないのだが、人手の作業により判断することは、筆者らの経験上、その作業量の膨大さから困難と考える。

生成されたLTSの正当性を人手で示すには、そのLTSに示される全ての状態遷移経路が元のLOTOS仕様と完全に一致することを検査することになる。この作業が可能なのは、対象とするLOTOS仕様の規模が高々数十行のものまでである。実際、上記交換サービスのLOTOS仕様に対するLTSの正当性を示すことも困難と考えている。以上述べた課題を整理すると次のようになる。

- 少なくとも数百行の規模を持つLOTOS仕様に対して、生成したLTSの正当性を示す実施可能な手段の確立。

この課題に対する完全な解決策、すなわち少なくとも数百行の規模を持つLOTOS仕様から生成されたLTSの正当性を示す必要かつ十分な条件を生み出す実施可能な確認手段は存在しないと言える。しかし、次のような必要条件を生み出す確認手段は提案できる。

この確認手段では、まず現状信頼性を評価しようとしているLOTOS意味解釈機能とは異なる実装(アルゴリズムとプログラムの両方)に基づくもう1つのLOTOS意味解釈機能を導入(実現)する。さらに、これら2つのLOTOS意味解釈機能を用い、次の手順に基づいてLTSの正当性を示すための必要条件を生み出すことができる。

① 2つのLOTOS意味解釈機能で同一のLOTOS仕様からそれぞれLTSを生成する。
② 筆者らがすでに実現した弱双模倣等価性検証機能(2つの仕様間の無矛盾性検証機能の一つ)を用いて、その2つのLTSの等価性を判定する。
③ ②で等価性が成立すれば、その検証結果は生成された2つのLTSの正当性を示す必要条件となる。一方、②で等価性が不成立であれば、生成された2つのLTSのうち

の少なくとも1つは正当ではない。すなわち、2つのLOTOS意味解釈機能の実装の少なくとも1つに、不具合のあることを意味している。

(図4.1参照)

この手順の③で、「生成された2つのLTSの等価性成立」をLTSの正当性を示す「必要条件」とするのは、もしその2つのLTSが両方とも「正解」であるならば、その2つのLTSが同一のLOTOS仕様から生成されている以上、2.LOTOSの意味モデルで述べたように、それらの間に弱双模倣等価の関係が成立するはずだからである。

「生成された2つのLTSの等価性成立」がLTSの正当性を示す「十分条件」にはならないのは、その2つのLTSが「正解」とは異なる意味モデルで一致することがあり得るからである。換言すれば、2つのLOTOS意味解釈機能の実装の両方に不具合があり、両機能とも誤ったLTSを生成したのだが、偶然にも2つのLTSの意味が等価になるような誤りを作りこんでいたことを意味する。

この必要条件を生み出す確認手段を用いてLOTOS意味解釈機能の動作を評価する場合には、2つのLTSが等価であれば、その対応するLOTOS仕様に対しては正当なLTSが生成できたと判断(すなわち、その1つの評価項目については合格)することになる。もちろん上記のような「偶然」が起きていれば、不具合を見落とすことにはなる。

この「偶然」を少なくする手段としては、"LOTOS意味解釈機能C"を更に導入し、1つのLOTOS仕様から生成された3つのLTSの間に「等価性」が成立する場合を、その「必要条件」とすることも考えられる。同様に、より多くのLOTOS意味解釈機能を導入すれば、この「偶然」の起きる確率を一層少なくすることが可能である。

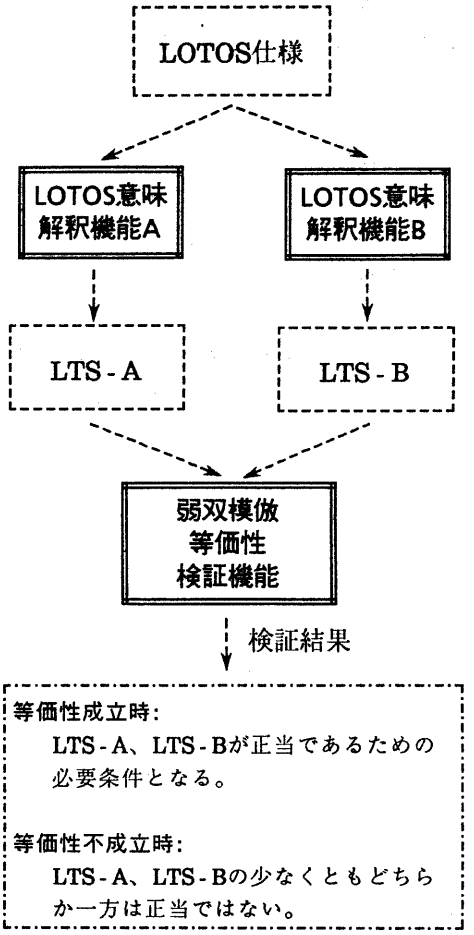

図4.1 LTS正当性の確認手順

生成された2つのLTSが「等価性不成立」の場合には、2つのLOTOS意味解釈機能の少なくともどちらか一方に不具合があることを意味しており、LOTOS意味解釈機能を改修し、信頼性を向上させる契機を与えることができる。

以上述べた確認手段はあくまで「必要条件」を生み出すものであり弱点を有する。しかし、大規模仕様に対するLOTOS意味解釈機能の信頼性を評価する手段は、筆者らの知る限り他には考えられないため、LOTOS意味解

釈機能の信頼性を向上させるという観点からは意義があると思われる。

5. おわりに

以上本論文では、ITECSにおける大規模なLOTOS仕様に対する機械検証の適用性評価に関し、次のことを示した。

LOTOS意味解釈機能の信頼性評価は、2つ以上のLOTOS意味解釈機能を導入することにより実施できること。

今後の課題としては以下のものが挙げられる。

(1) 交換機など実際の通信システムのLOTOSによる仕様記述と検証の実施によるITECSの実証評価

(2) 大規模なLOTOS仕様における検証に要する計算時間の評価

[謝辞]

本研究に当たりご指導をいただいた(株)高度通信システム研究所　顧問　野口　正一氏(東北大学 名誉教授)に深謝いたします。また、本研究の機会を与えていただいた同研究所　緒方　秀夫常務、三菱電機(株)　通信システム研究所　山内　才胤所長、石坂　充弘部長の各氏に謝意を表します。さらに、本論文の執筆に当たり、貴重な意見を寄せてくれた(株)高度通信システム研究所の諸氏に感謝します。

[参考文献]

[1]ISO: "ISO8807: Information processing systems - Open Systems Interconnection - LOTOS - a formal description technique based on the temporal ordering of observational behaviour", (1989)

[2]K. Takahashi, K. Sarashina, K.Yamano, S. Mikami, N. Tsubone and Y. Tokita: "ITECS, An Integrated Environment for Communication Software Design", Proceedings of International Telecommunication Symposium'94,Vol.2 P.1-8

[3]G. León, J. Carracedo, J.C. Moreno, J.C. Yelmo, J.J. Gil, C. Sánchez and F.J. Carrasco: "An Industrial Experience on Development with LOTOS and SDL", Participants' Proceedings of FORTE '93 P.221-236

[4]高橋、土岐田、田中: "A Flexible Verifier for LOTOS Specifications"、電子情報通信学会　1994年春期大会予稿集　B-662

[5]R. Milner : "Communication and Concurrency", Prentice Hall(1989)

[6]山野、太田、高橋: "シミュレーション関係に基づくLOTOS仕様の検証システム"、情報処理学会　マルチメディア通信と分散処理 58-1299(1992)

[7]佐藤、川口、高橋、白鳥、野口: "SAL: LOTOS仕様の意味解析支援系"、情報処理学会　マルチメディア通信と分散処理　46-6(1990)

[8]高橋、神長、白鳥: "LOTOS言語の特質と処理系の現状と動向"、情報処理Vol.31 No.1 P.35-46.(1990)

[9]T. Bolognesi and E. Brinksma : "Introduction to the ISO Specification Language LOTOS", The Formal Description Technique LOTOS Results of ESPRIT/SEDOS project, NORTH-HOLLAND, P.23-73 (1989)