4N－4

SAL：LOTOS仕様の意味解析支援システム
－目的と概要－

佐藤淳† 川口研治†† 高橋薫†† 白鳥則郎†† 野口正一††

†富士通カストマエンジニアリング

††東北大学電気通信研究所

1. はじめに

システムの仕様化においては、厳密で正確な記述を可能とする形式記述技法(FDT)の導入が望まれる。また、このようなFDTを用いてシステムを仕様化するには、種々の支援環境の開発が重要である。本稿においては、通信システムの仕様化を目的としたFDTの1つであるLOTOS[1]で記述された仕様の意味解析支援システムSAL(Semantic Analyzer of LOTOS Specifications)[2]の目的と概要について述べる。

2. SALの目的

LOTOSの普及に伴い、OSIアーキテクチャを始めとし、種々のシステムのLOTOSによる仕様化が進展してきている。従って、仕様化したシステムの動的意味を解析し、仕様の記述内容の検査などに効果的に役立てる支援システムが重要となる。

SALシステムは、LOTOS仕様の意味であるLTS(ラベル付き遷移システム)のコンパクトな形での導出を支援する。このコンパクトな形のLTSは、本来のLTSに出現するデータ値を一括した形で圧縮表現したものであり、変数をそのままの形で残したLTSである。これをLTSの『中間表現』あるいは『変数付きLTS』と呼ぶ。この中間表現は以下に示すような種々の目的に用いることができる。

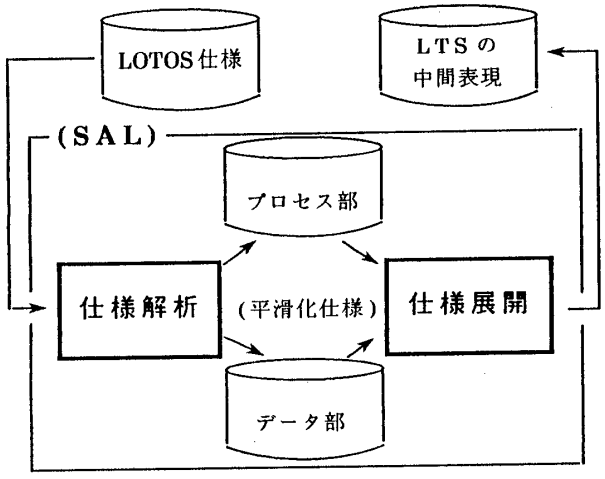

図1 SAL の構成

- 仕様のシミュレーション
  変数をその具体値を用いてインスタンシエートしながら中間表現をトレースすることによって、仕様の意味する動作をシミュレートすることができる。

- 等価性検証
  変数のインスタンシエーションにより中間表現を展開しLTSを求め、それに対して既存の等価性判定法を適用する。

- LOTOS仕様から状態遷移仕様への変換
  Estelle等の状態遷移モデルをランデブー意味論で考えることにより、LOTOS仕様に対応する状態遷移仕様を中間表現から直接に導出できる。

- 自動インプリメンテーション
  中間表現は与えられた仕様中の多数のプロセスを一括して表現したものとなっており、C言語などのプログラムに変換することが容易である。

3. SALの概要

SALシステムは、フル LOTOS 仕様を入力としそれに対応するラベル付き遷移システムの中間表現(変数付きラベル付き遷移システム)を導出する。本システムは現在、具体的にその開発を進行

Outline of the SAL System

Atsushi SATO†, Kenji KAWAGUCHI††, Kaoru TAKAHASHI††, Norio SHIRATORI††,Shoichi NOGUCHI††
†Fujitsu customer engineering LTD
††Research Institute of Electrical Communication,Tohoku University

中であり、全体の構成は図1に示す通り、次の2つの動作フェーズから構成されている。

＜仕様解析フェーズ＞

本フェーズでは、例えば、図2のようなフルLOTOS仕様を入力とし、字句解析、構文解析そして静的意味解析を行い、プロセス部とデータ部に分けて平滑化した仕様を出力する。平滑化仕様には、次のような特徴がある。

(プロセス部)

1. 動作式の前置記法的表現
2. 値宣言へのソート情報の付加

(データ部)

1. データ型の一括した表現
2. 変数名へのソート情報の付加

＜仕様展開フェーズ＞

本フェーズでは、仕様解析フェーズの出力である平滑化仕様を入力とし、LOTOSプロセスの動的意味を与える遷移導出体系(公理と推論規則)を適用し、ユーザとの対話を通して、変数付きラベル付き遷移システムを求める操作を行う。なお、本フェーズで用いている遷移導出体系には、変数と条件を残した形のLTSを求めるためのいくつかの工夫を行っている。その一部を以下に示す。

- 簡略化のためガード、選択述語および値宣言(複合項の場合)の解釈についてはユーザに支援を求める。
- "アクションプレフィクス"の公理の適用において g?y:t;B のような動作式の場合、生起可能なイベントの表現は g?y1:t となり、ソートtの値y1が選択されたことを意味する。
- "一般並列"の推論規則の適用において g!t1;B1|[g]|g!t2;B2 のような動作式の場合、生起可能なイベントの表現は g!t1[t1=t2] となり選択述語を付加した形となる。

図2に示すLOTOS仕様をSALシステムによって解析すると、図3に示すような変数付きラベル付き遷移システムが導出される。図中の○は各状態を示し、矢印は状態の遷移を示す。例えば、初期状態B0からの状態遷移は、ゲートgにおいて環境からソートboolの値x1、ソートnatの値y1とz1を受信し、状態B1に遷移することを表す。状態B1からの状態遷移は、ガード[w(仕様のパラメータ)=x1(環境から受信した値)]がtrueならばゲートhにおいてy1(環境から受信した値)を送信し、状態B2に遷移することを表している。

SALの現バージョンでは、ガード、選択述語および値宣言の解釈をユーザ支援のもとに行っているが、次期バージョンにおいては、項書換えシステム等を利用して自動化を計画している。

```
specification example[g, h](w : bool) : noexit
   type  Boolean   is
      (中略)
   endtype
   type  Nat_numbers    is
      (中略)
   endtype
behaviour
         p0[g, h](w)
where
   process p0[g, h](w : bool) : noexit :=
            g ? x : bool ? y : nat ? z : nat ;
               (   [w=x]      -> p1[g, h](w, y, true)
               [] [w=not(x)] -> p1[g, h](w, z, true))
   where
      process p1[g, h](w:bool,v:nat,s:bool):noexit:=
               [s=true]   -> h ! v ; p0[g, h](not(w))
            [] [not(s)=true]  ->      stop
      endproc
   endproc
endspec
```

図2 LOTOS仕様 (例)

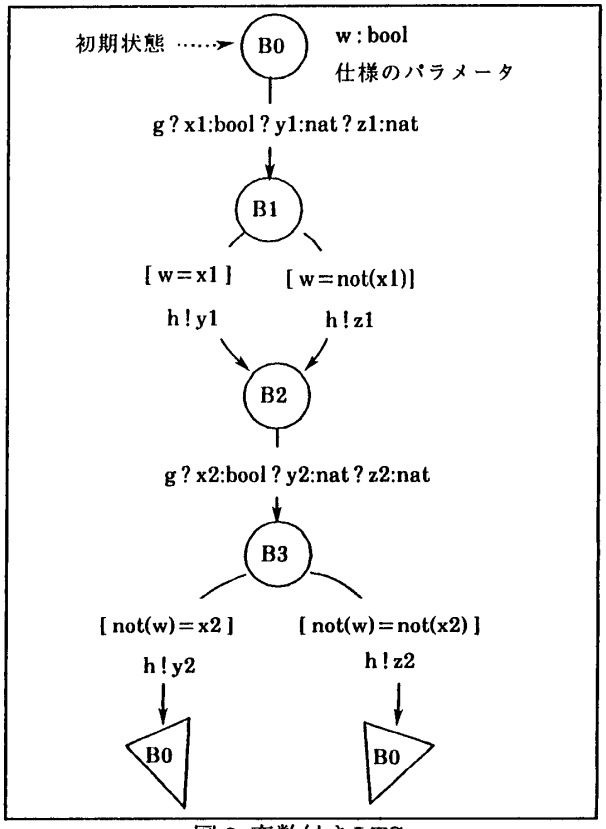

図3 変数付きLTS

参考文献

[1] ISO : " LOTOS －A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour," ISO 8807 (1989).

[2] 高橋:"SAL : LOTOS仕様の意味解析支援システム," 東北大学内部資料(1989).