

## 通信システムの形式的仕様記述言語の教育支援システムの設計

朴 炳昊\* 李 殷碩\*\* 白鳥 則郎\*

\*東北大学電気通信研究所/情報科学研究科

\*\*韓国成均館大学工科大学情報工学科

形式記述技法(FDT: Formal Description Technique)の一つであるLOTOSは、通信システムの仕様を曖昧なく厳密に記述するための手段を提供する。しかしながら、LOTOSは一般に学習性や理解性に難が言われており、このため、LOTOSの利用と普及が遅々と進まないのが現状である。このようなLOTOSの利用者を増やすためには、特に初心者向けの有効的かつ効率のよい教育支援が行える教育支援環境の構築が必要になる。

本稿ではユーザにLOTOSの構文などの単片的知識だけではなく、仕様記述法など応用的知識を効率的に学習させるために新たに筆者らが提案する等価検証方法に基づき、エラーの検索及びそれに基づく修正支援方法などを備えた教育支援システムについて述べる。

## Design for Education Support System of Specification Language for Communication System

Byung-ho Park\*, Eun-seok Lee\*\* and Norio Shiratori\*

\*Research Institute of Electrical Communication /  
Graduate School of Information Sciences, Tohoku University  
2-1-1, katahira, Aoba-ku, sendai, 980-77, Japan

\*\*Department of information Engineering, Faculty of Engineering,  
Sung-Kyun-Kwan Univ., Seoul, Korea

LOTOS, which is one of the FDTs(Formal Description Techniques), is used to describe communication systems unambiguously and precisely. But due to its poor learnability and understandability, there are a few experts in LOTOS. Therefore, it is important to design a user-friendly LOTOS education support system for non-expert.

In this paper, we propose an education support system for LOTOS toward non-expert users. In this system, we diagnose and correct errors by using a new equal verification method, and explain what kind of error has occurred and indicate the place where it has occurred on the specification.

## 1. はじめに

近年、通信システムの大規模化・複雑化により、分散された複数のコンピュータ間での協調作業(CSCW: Cooperative Support for Computer Work)による通信ソフトウェア開発や製品開発などが盛んに行われている。このような協調作業を行うためには、通信仕様が厳密でかつ曖昧性がないことが求められており、形式記述技法(FDT: Formal Description Technique)はそのための有効的な表現手段を提供する。しかし一般に、FDTは形式的で数学的根拠を用いて記述するので、従来の非形式的記述技法、すなわち、自然言語や図形、表などと比べるとその内容が分かりにくく、また初心者にとって学習しづらいなどの問題点が指摘されている。このため、FDTの普及は十分ではなく、専門家の数も少ないのが現状である。FDTの重要性を考えると、初心者はもちろん、FDTを完全に理解していないユーザのための教育支援環境の構築が重要な課題とされている。

本研究では、国際標準化されているFDTの中で、特にその形式性及び厳密性から注目されているLOTOSを対象とし、LOTOSの学習性及び理解性を向上するため、ユーザフレンドリなコミュニケーションを通じたLOTOSの教育支援環境を構築する。本支援環境では、学習者による解答は本稿で提案する誤り分類法により誤った知識が診断され、これに基づき、解答の誤っている箇所を指摘することで最終的にはLOTOSの完全な知識を学習させ、より多くのユーザにLOTOSによる仕様記述ができるようにすることを目指す。

本稿の構成は、2章で、提案する教育支援システムの概要について述べ、3章で、提案システムで用いられる最簡形LTSを用いた二つの通信システム間での誤り検出法と教育支援法について述べる。4章では具体的な適用例を通じての応用とその評価等について述べる。5章は結論である。

## 2 形式的仕様記述言語に基づいた教育支援システム

### 2.1. LOTOS (1)

#### 2.1.1 本稿で用いるLOTOSの演算子

本稿で用いるシステム(プロセス)は以下のように定義される。

定義2.1 プロセス(Process)は以下のように帰納

的に定義される。

- (1) stopはプロセスである。
- (2)  $P$ がプロセスのとき $a;P$ はプロセスである。
- (3)  $P$ と $Q$ がプロセスのとき、 $P \square Q$ はプロセスである。 □

上で定義されたプロセスはLOTOSにより定義されるそのサブセットである。

ここでのプロセスの定義により、LOTOSの再帰を含まない全てのプロセスと強等価なプロセスを表現することが可能である。

プロセスはその意味をラベル付き遷移システム(LTS: Labelled Transition System)によって与えられる。

LOTOSはその意味表現としてLTSを持っている。

定義2.2 LTSは4項組 $\langle S, A, \rightarrow, s_0 \rangle$ である。

ここで、 $S$ は状態の空でない有限集合であり、 $A$ はアクションの有限集合で、 $\rightarrow$ は状態間の遷移関係であり、 $\rightarrow \subseteq S \times A \times S$ として定義される。

また、 $s_0 \in S$ は初期状態である。 □

$(s, a, s') \in \rightarrow$ のとき、 $s \xrightarrow{a} s'$ と書く。

従って、 $\rightarrow = \cup_{a \in A} \{ \xrightarrow{a} \mid \xrightarrow{a} \subseteq S \times S \}$ と書くことができる。

定義2.3 プロセス間の遷移関係は以下で導出される。

$$\frac{}{a;P \xrightarrow{a} P} \quad \frac{P \xrightarrow{a} P'}{P \square Q \xrightarrow{a} P'} \quad \frac{Q \xrightarrow{a} Q'}{P \square Q \xrightarrow{a} P'}$$

□

#### 2.1.2 LOTOSで許す等価関係の範囲

LOTOSにおけるプロセス間の等価性は観測による等価性が用いられる。すなわち、二つのプロセスを外から観測したとき、両者の振舞いが区別できないなら、これらのプロセスは等価であるとされる。

#### 2.1.3 最簡形LTS

二つのプロセス(正解と学習者のLTS間)の同一レベルでの集合演算により誤りを検索するため一番簡略されたただ一つのLTSが必要される。

定義2.4 状態が有限(FTS: Final Transition Systems)の最簡形LTS(3)

LTSが有限である場合(FTS)に、FTS Sysに対して、Sysと弱等価なFTSの中で、状態と遷移の数が一番最少のものをSysの最簡形と呼ぶ。 □

上の定義に基づいて考察すると、ある通信システムを記述するとき、Text-LOTOSによる記述方法は多数存在し、またこれをLTSで表現しても各々のText-

LOTOSに対応しているLTSは弱等価 [2,5] 概念に基づいて考えているため、そのLTSは無限に存在する。ここでのFTSの最簡形LTSは弱等価概念に基づいて一番簡略されたLTSで表現しているため、強等価 [2,5] の交換律(communitive law)のみ許したら、FTSの最簡形LTSは一意に定まる。(図1)

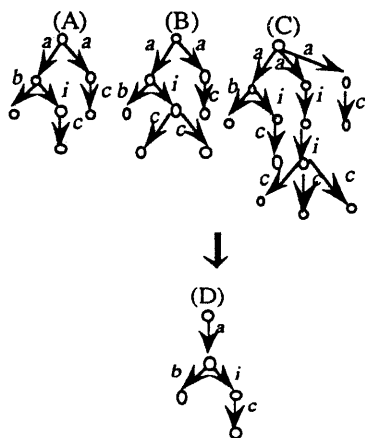


図1. (A)~(D)は弱等価性に基づくお互いに等価関係であるが、最簡形LTSで表現したら(D)になる。

## 2.2 LOTOS教育支援システムの構成

本節では、LOTOS教育支援システムを構成する各モジュールについて述べる。(図2)

### (1) 教授機構

このモジュールは、本教育システムと学習者との入出力の制御と教育方法を保持している部分である。まず、問題領域に関する知識、すなわち、問題及び正解に関する知識を用いてユーザに適切な問題を提示する。学習者がText LOTOS表現で仕様を入力すると、(1)のLTS変換機構により学習者に入力された仕様をLTS表現で表示する。また、(2)の誤り検出機構から検索された誤りを(1)のところで、LTS表現上での誤りを表示させる。さらにこれを利用して、Text LOTOS表現上で誤り箇所を表示する。

### (2) LTS変換機構

このモジュールでは、Text LOTOS表現の仕様からLTS表現への変換を行う。その際、構文エラー検索も行う。また、LTS表現の最簡形への変換も行う。

### (3) 誤り検出機構

このモジュールでは、(1)で学習者に与えた問題に対する解答と問題の正答とを比較し、誤りの検出及び誤り箇所の指摘を行う。この具体的な方法は

次節以降で述べる。

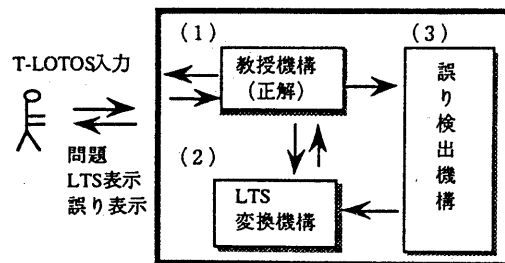


図2. 本LOTOS教育支援システムの構成

## 3 LTSを用いた二つの通信システム間での誤り検出法と教育支援法

### 3.1 誤りの分類

学習者の誤りに対する修正支援は教育支援研究の最重要課題の一つである。学習者の学習過程の観察可能なアウトプットは、練習問題を解いている際に学習者が行うパフォーマンスである。誤答データは、学習者が問題を解決しようとした場合生じるエラーパフォーマンスに関する伝統的な測度である。

本論文では、学習者の誤りを大きく分けて単純(mistake)エラーと知識欠如(lack of knowledge)エラーの二つに分類する。

単純エラーとは、学習者が起こしがちな学習者の単純ミスにより生じるエラーを意味する。例えば、キーボード操作ミスにより構文エラー(二重オペレータ入力、括弧の半欠落など)やアクション名の間違った入力がこれに相当する。

知識欠如エラーは、ある問題を解決しようとしたとき、そのための知識の欠如や忘却のため学習者が持っている他の知識の混同(不完全な知識)したり、誤って導かれた知識を適用したためなどの様々な原因により生じるエラーである。ここでは知識欠如エラーを以下の三つに細分化する。

- (1) 余りエラー(excess error)
- (2) 欠落エラー(shortage error)
- (3) 順序関係エラー(sequential error)

この三つのエラーのプロセスに対する具体的な定義は次節で行う。

また、本論文で対象としているエラーの範囲は単純エラーの構文エラー及び知識欠如エラーに限定している。

### 3.2 誤り検出法

#### 3.2.1 誤り検出のための諸定義

学生が入力したデータにおける誤りを検出、分類するために必要な幾つかの定義を導入する。

誤り検出は、プロセスに対して深さの概念を導入し、学習者の解答と正解のプロセスを深さ毎に区切って比較することで行われる。プロセスの深さは次のように定義される。

**定義3.1** あるプロセス $P$ に対し、 $P$ から $k$  ( $\geq 0$ ) 回遷移を行った (サブ) プロセスを $P$ における深さ $k \geq 1$ のアクションセットを深さ $k$ の (サブ) プロセスと呼ぶ。一般に深さ $k$ の (サブ) プロセスは一意に定まらない。 □

**定義3.2** プロセス $P$ のサクセッサ (successor)  $\text{succ}(P)$ は $P$ から遷移可能なアクションのマルチ集合である。すなわち、

$$\text{succ}(P) = \{a \mid \exists P', P \xrightarrow{a} P'\}$$

ただし、 $\text{succ}(P)$ に同じアクションが $n$ 個 ( $n \geq 0$ ) 含まれるときは、 $P$ から $n$ 種類のプロセスに遷移可能であり、それらは互いに強等価にならない。 □

**定義3.3** プロセス $P$ に対する深さ $k$  ( $\geq 1$ ) のアクション集合 $\text{action\_set } k(P)$ は次のように定義される。但し、 $\cup_M$ はマルチ集合での和集合を示す。

$$\text{action\_set } k(P) = \cup_M \text{succ}(Q)$$

ここで $Q$ は $P$ の深さ $k-1$ のプロセスを表す。 □  
明らかに $\text{action\_set } 0(P) = \text{succ}(P)$ である。

まず、知識の欠如または忘却により生じる欠落エラーを定義する。欠落エラーは同一レベル及び相違レベルエラーに分類される。

**定義3.3** 同一レベルでの欠落エラー (shortage error at same level)

ある深さ $k$ で、正答のプロセス $P$ のアクション集合に含まれるアクションが学習者解答のプロセス $Q$ のアクション集合に含まれないとき、すなわち

$$\text{action\_set } k(P) -_M \text{action\_set } k(Q) \neq \emptyset$$

( $-_M$ はマルチ集合での差集合)

であるとき、同一レベルでの欠落エラーがあるとす。 □

図3に同一レベルでの欠落エラーの例を示す。

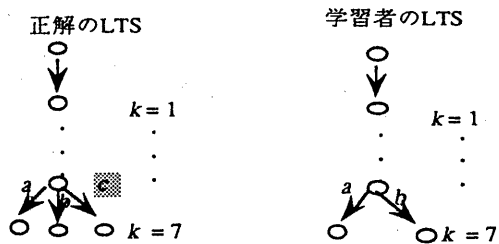


図3. 同一レベルでの欠落エラー

**定義3.4** 相違レベルでの欠落エラー (shortage error at different level)

正解のプロセス $P$ は深さが $k$ 以上の深さのプロセスが存在するのに対し、学習者のプロセス $Q$ は深さが $k$ までのプロセスしか存在しない場合、すなわち、ある $k$ に対して、 $\text{action\_set } k+1(P) \neq \emptyset$ かつ

$\text{action\_set } k+1(Q) = \emptyset$ のとき、相違レベルでの欠落エラーがあるとす。 □

次に、余りエラーを定義する。余りエラーは同一レベル及び相違レベルエラーに分類される。

**定義3.5** 同一レベルでの余りエラー (excess error at same level)

ある深さ $k$ で、正答のプロセス $P$ のアクション集合に含まれないアクションが学習者による解答のプロセス $Q$ のアクション集合に含まれるとき、すなわち

$$\text{action\_set } k(Q) -_M \text{action\_set } k(P) \neq \emptyset$$

( $-_M$ はマルチ集合での差集合) であるとき、同一レベルでの余りエラーがあるとす。 □

同一レベルでの余りエラーの例を図4に示す。

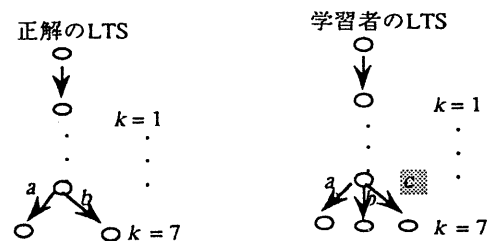


図4. 同一レベルでの余りエラー

**定義3.6** 相違レベルでの余りエラー (excess error at different level)

正解のプロセス $P$ に深さ $k$ までサブプロセスしかないのに対し、学習者のプロセス $Q$ は $k+1$ 以上の深さのプロセスが存在する場合、すなわち、ある $k$ に対して $\text{action\_set } k+1(P) = \emptyset$ かつ $\text{action\_set } k+1(Q)$

$\neq \emptyset$  のとき、相違レベルでの余りエラーがあるとする。

正解のプロセスと学習者による解答のプロセスのアクション集合が全ての深さで一致していても、両者のプロセスは強等価にはならない。例えば、図5のような場合が典型的な例である。これは、アクションを行なう順序に誤りがあったために生じるエラーであり、学習者が自分が持っている他の知識との混同を起こしたり、誤って導出された知識を適用した場合に生じる順序関係エラーに相当する。以下では、順序関係エラーを定義するために必要な諸定義を行う。

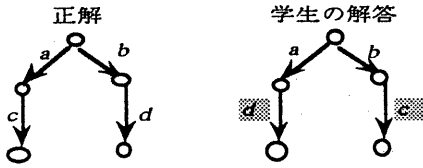


図5. 順序関係のエラー

定義3.7 ( $1\_Trace P(R)$ )  $P$  をプロセス  $R$  を  $P$  の深さ  $n$  ( $\geq 2$ ) のあるサブプロセスとする。このとき、 $1\_Trace P(R) = (a, b)$  と定義する。

ただし、 $a, b \in Act$ ,  $\exists R', R''$

$P \xrightarrow{a} R' \xrightarrow{b} R''$  である。

定義3.8 ( $1\_Trace\_setn(P)$ )  $P$  の深さ  $n$  ( $\geq 2$ ) の任意のプロセス  $R$  における  $1\_Trace P(R)$  のマルチ集合を  $1\_Trace\_set n(P)$  とする。すなわち、

$1\_Trace\_set n(P) = \{(a, b) \mid (a, b) = 1\_Trace P(R)\}$

ただし、 $R$  は  $P$  の深さ  $n$  のサブプロセス

定義3.9 ( $m\_Ans\_StP(R)$ )  $P$  をプロセス、 $R$  を  $P$  の深さ  $n$  ( $\geq m$ ) のあるサブプロセスであるとする。このとき、 $R$  をサブプロセスに持つ  $P$  の深さ  $n - m$  のサブプロセスを  $m\_Ans\_StP(R)$  と書く。すなわち、

$m\_Ans\_StP(R) = R'$  である。ここで、

$P \xrightarrow{a} R' \xrightarrow{b} R''$  である。

定義3.10 ( $m\_Ans\_St\_setn(P)$ )  $P$  の深さ  $n$  ( $\geq m$ ) の任意のサブプロセス  $R$  の  $m\_Ans\_StP(R)$  のマルチ集合を  $m\_Ans\_St\_setn(P)$  とする。すなわち、

$m\_Ans\_St\_setn(P) = \{P' \mid P' = m\_Ans\_StP(R), R \text{ は } P \text{ の深さ } n \text{ のサブプロセス}\}$

定義3.11 (順序関係のエラー (sequential error)) 正答のプロセスを  $P$ 、学習者による解答のプロセスを  $Q$  とし、 $P$  と  $Q$  の深さに対して、アクション集合はそ

れぞれ一致するとする。このとき、ある深さ  $n$  で

$1\_Trace\_set k(P) \neq 1\_Trace\_set k(Q)$  のとき、

または、ある  $m$  に対して

$m\_Ans\_St\_setn(P) \neq m\_Ans\_St\_setn(Q)$

のとき、順序関係にエラーがあるという。

ここで、 $A \neq \sim B$  とは、 $f: A \rightarrow B$  なる全単射のマルチ集合上の写像  $f$  があり、

$\forall a \in A, a \sim f(a)$  を満たすことを示す。

順序関係のエラーは、 $1\_Trace\_set k(P)$  と  $1\_Trace\_set k(Q)$  を比較するだけでは不十分である。例えば、図6のような例では任意の  $n$  に対して、 $1\_Trace\_set k(P) = 1\_Trace\_set k(Q)$  であるが、 $P \neq Q$  である。このため、 $m\_Ans\_St\_setn(P)$  と  $m\_Ans\_St\_setn(Q)$  の比較を行う必要がある。学習者の解答のプロセスからのエラーの検出は正解のプロセスと解答のプロセスの各々の最簡形を比較し、解答のプロセスに欠落エラー、余りエラー及び順序関係エラーがないかどうかを調べることで行う。

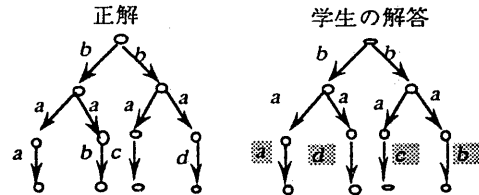


図6. 順序関係のエラー

## 4 応用と評価

### 4.1 実装

本教育支援システムの構築のための開発環境は次の通りである。

試作にあたっては、sunワークステーション上で、C言語とx-windowを用いて実装を行った。また、T-LOTOS表現からLTS表現への変換のため、さらに yacc と lex を利用している。

### 4.2 応用例と評価

#### 4.2.1 応用例

本システムを学部4年生の学生実験に用いた。応用例は通信システムにおける典型的な一例として通信システムの基本要素であるダブルバッファを記述するものである。

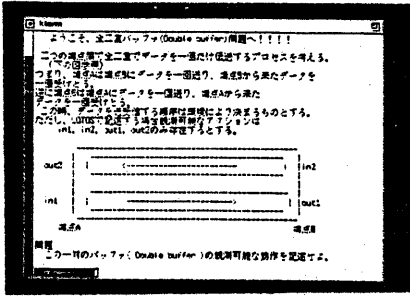


図7. 2重バッファ問題提示画面

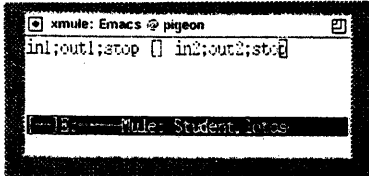


図8. 学習者の入力画面

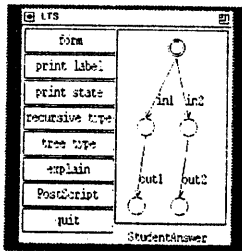


図9. 学習者のLTS画面

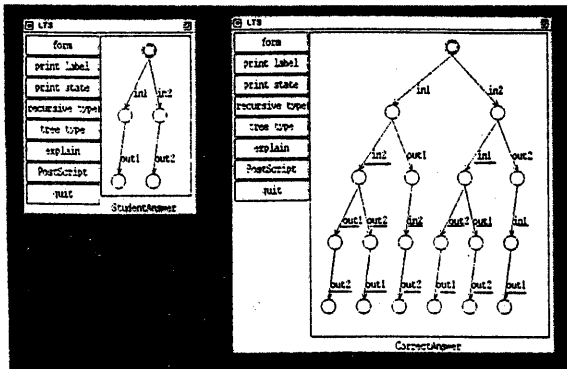


図10. 検索されたエラーをLTS上での表示

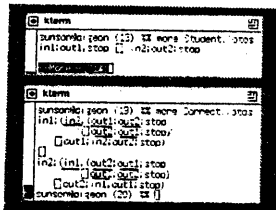


図11. 検索されたエラーをT-LOTOS上での表示

#### 4.2.2 評価

本稿では、誤りの分類（余りエラー、欠落エラー、順序関係エラー）と同定に基づく教育支援により、学習者の誤りのより正確な推定と効果的な教育支援が可能になった。

また、総合的な支援法とユーザフレンドリーな支援環境の提供により視覚的でユーザフレンドリーなインタラクションを通じた親和性の高い教育支援環境が実現された。これにより、より多くのユーザにLOTOSの学習性と理解性が向上期待される。

#### 5 まとめ

通信システムの仕様記述言語の一つであるLOTOSの教育支援システムを提供した。

また、学習者が持っている誤りの同定とそれに基づく支援のため学習者の起こしがちな誤りを分類した。

今後の課題としては、より多くの学生実験を通じて、定量的評価を行う。またさらに、教育効果をあげるためにシステムの改善と拡張及び学習者モデル導入による知的支援があげられる。

#### [ 参考文献 ]

- [1] ISO:Information Processing Systems Open Systems Interconnection LOTOS A Formal Description Technique based on the Temporal Ordering of Observational Behaviour, ISO 8807 (1989)
- [2] Robin, M., "Communication and Concurrency", Prentice Hall (1989)
- [3] Shiratori, N., H. Kaminaga, K. Takahashi and S. Noguchi, "A Verification Method for LOTOS Specifications and its application, Protocol, Specification, Testing and Verification" IX North-Holland, pp59-70 (1990)
- [4] Tommaso, B., Ed Brinksma, "Introduction to the ISO Specification Language LOTOS", Computer Networks and ISDN Systems 14, pp25-59 (1987)
- [5] Tommaso, B., S. Smolka, "Fundamental Results for the Verification of Observational Equivalence: a Survey", Protocol Specification, Testing, and Verification VII", North Holland, pp165-179 (1987)