

t イベントによる

3B-6 形式的仕様記述言語 LOTOS への時間概念の導入*

坂田 俊幸

佐伯 元司†

東京工業大学 ‡

1 はじめに

厳密な仕様を記述するために、各種の形式的記述技法 (FDT: Formal Description Techniques) が提案されている。LOTOS[1] もその1つで、ISO (国際標準化機構) で標準化がなされ、実行系も存在する形式的仕様記述言語である。LOTOS の形式的意味モデルはラベルつき付遷移システム (LTS) と呼ばれる有向グラフで与えられ、データを含まない Basic-LOTOS で LTS が有限であるものについては LOTOS 仕様の等価性 (Weak-bisimulation) を機械的に判定するアルゴリズムも考案されている [2]。

しかし、LOTOS ではイベント間の時間の間隔については考慮されていないため delay や wait-until-timeout などの時間に関連した仕様の記述が難しい。このため、LOTOS に時間の概念を導入する試みが多くなされてきている。その方法は時間をイベントとして扱う方法 [3] とタイムスタンプを用いる方法 [4] の大きく2通りに分かれている。後者の方法では時刻をデータとして定義して扱うため、データを扱わないという Basic-LOTOS の枠組を越えている。

本稿では時刻の経過を表す t イベントという特別なイベントを導入する方法で拡張を行なう。この場合、2つの有限 LTS の等価性の判定は Basic-LOTOS で用いられている方法で行なうことができる。

2 拡張 LOTOS

t イベントは時刻の経過を表すイベントである。時刻の経過をイベントとして表すため、時刻は離散的に扱われることになる。

t イベントによってのみ時刻は経過し、他のイベントの生起には時間はかからない。また、時刻の経過は環境によって他のすべてのイベントが生起できない場合にのみ起こり得る。したがって、もし i イベントが生起可能なら必ず時間の経過の前に i イベントは起こることになる。

stop に関しては t イベントも生起しないものとして扱う。この性質は検証に役に立つ。

また、t イベントの生起に関しては以下の性質が成り立つものとする。

$$\forall B_1, B_2, B_3 (B_1 \xrightarrow{t} B_2 \wedge B_1 \xrightarrow{t} B_3 \supset B_2 = B_3)$$

2.1 Syntax

LOTOS の syntax に以下のものを拡張した。

- $(n); B$
- $a\{n\}; B$
- $\text{exit}\{n\}$

ただし、 n は非負整数である。

2.2 Informal Semantics

- $(n); B$
3 単位時間後に B が実行されるという記述は $t; t; t; B$ となるが、これでは扱う時間が大きくなると、記述が長くなり理解しにくくなるので、これを $(3); B$ と書くことにする。これにより、 a が生起してから 100 単位時間後に B が実行されるという記述は $a; (100); B$ と書くことができる。
- $a; B$
action prefix a は生起可能ならすぐに生起してもよい。生起しないまま時刻が経過してもなお生起可能であれば生起する。つまり、生起可能である限り生起するという意味を与える。
- $a\{n\}; B$
 a が生起可能になったなら、すぐに生起しなければならないという記述を $a\{0\}$ で表す。これを用いると $P := a; B$ は $P := a\{0\}; B \parallel (1); P$ で表すことができる。
 a が生起可能になってから n 単位時間だけ待つことができるという記述は $a\{n\}$ で表す。 $a\{3\}; B$ は $a\{0\}; B \parallel (1); a\{0\}; B \parallel (2); a\{0\}; B$ を表している。 n 単位時間経っても生起しない場合は、アクション a はもう生起しない。

2.3 Formal Semantics

$$\begin{array}{l} a; B \xrightarrow{a} B \quad \text{if } \text{name}(a) \neq t \\ a\{n\}; B \xrightarrow{a} B \quad \text{if } \text{name}(a) \neq t \\ \frac{B_1 \xrightarrow{a} B'_1}{B_1 \parallel B_2 \xrightarrow{a} B'_1} \quad \text{if } \text{name}(a) \neq t \\ \frac{B_1 \xrightarrow{a} B'_1 \quad B_2 \xrightarrow{a} B'_2}{B_1 \parallel [G] B_2 \xrightarrow{a} B'_1 \parallel [G] B'_2} \quad \text{if } \text{name}(a) \in G \cup \{\sigma\} \\ \frac{B_1 \xrightarrow{a} B'_1}{B_1 \parallel [G] B_2 \xrightarrow{a} B'_1 \parallel [G] B_2} \quad \text{if } \text{name}(a) \notin G \cup \{\sigma, t\} \end{array}$$

*Timed Extension to LOTOS using t-event

†Toshiyuki Sakata, Motoshi Saeki

‡Tokyo Institute of Technology

$$\begin{array}{l}
a; B \xrightarrow{t} a; B \quad \text{if } \text{name}(a) \neq i \\
a\{n+1\}; B \xrightarrow{t} a\{n\}; B \quad \text{if } \text{name}(a) \neq i \\
(n+1); B \xrightarrow{t} (n); B \\
B_1 \xrightarrow{t} B'_1 \quad B_2 \xrightarrow{t} B'_2 \\
\hline
B_1 \parallel B_2 \xrightarrow{t} B'_1 \parallel B'_2 \\
B_1 \xrightarrow{t} B'_1 \quad B_2 \xrightarrow{t} B'_2 \\
\hline
B_1 \parallel [G] \parallel B_2 \xrightarrow{t} B'_1 \parallel [G] \parallel B'_2
\end{array}$$

3 記述力

以下のように時間に関連した記述が可能である。

- Delay

$$(5); a; B$$

a は 5 単位時間経過後、生起可能となる。

- Timeout

$$(B_1 \parallel (5); \text{exit}) >> B_2$$

5 単位時間以内に B_1 でアクションが起こらなければ B_2 に遷移する。

- Watchdog

$$B_1 [> (5); i; B_2$$

5 単位時間までは B_1 としてふるまい、その後は B_2 に遷移する。(5 単位時間以内に B_1 が終了した場合は終了)

- Spec := P [b] Con
where

$$\begin{array}{l}
P := (1); a; P \parallel (1); b; P \\
\text{Con} := b\{100\}; \text{Con}
\end{array}$$

a, b のいずれかが非決定的に起こるが、必ず 100 単位時間の間に 1 回以上 b が起こる。

4 等価関係

定義 1 $Sys = \langle S, A, T, s_0 \rangle$ を LTS とする。

$s, s' \in S, a_1, \dots, a_n \in A - \{i\}$ とする。

$s \xrightarrow{a_1, a_2, \dots, a_n} s'$ を満たす自然数

$k_0, \dots, k_n$ が存在するとき、

$s \xrightarrow{a_1, \dots, a_n} s'$ と記述する。

定義 2 二項関係 R が Weak Timed Bisimulation 関係にあるとは、もし $s_1, s_2 \in R$ ならば、任意のイベント系列 $\alpha \in (A - \{i\})^*$ に対して、次の 2 つの条件が成り立つことである。

1. $s_1 \xrightarrow{\alpha} s'_1$ ならば、 $s_2 \xrightarrow{\alpha} s'_2$ かつ $\langle s'_1, s'_2 \rangle \in R$ である s'_2 が存在する。
2. $s_2 \xrightarrow{\alpha} s'_2$ ならば、 $s_1 \xrightarrow{\alpha} s'_1$ かつ $\langle s'_1, s'_2 \rangle \in R$ である s'_1 が存在する。

定義 3 $Sys_0 = \langle S_0, A_0, T_0, s_0 \rangle$ と

$Ssy_1 = \langle S_1, A_1, T_1, s_1 \rangle$ が Weak Timed Bisimulation 関係にあるとは、ある Weak Timed Bisimulation 関係 R が存在して $\langle s_0, s_1 \rangle \in R$ が成り立つことである。

この関係は時間も含めた等価関係になっている。

Weak Timed Bisimulation 関係は Parallel Composition, Hiding, Action Prefix, Enabling, Relabeling によっても保存される。

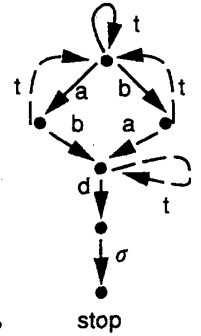
2 つの拡張 LOTOS による仕様記述が LTS の有限のグラフで表現可能なとき、その 2 つが Weak Timed Bisimulation 関係にあるかどうかは判定可能である。

例

Sp1 := hide c in (A[c][B])[c]C
where
A := a; c{0}; exit [] (1); A
B := b; c{0}; exit [] (1); B
C := c; d; exit

Sp2 := a; b{0}; d; exit [] (1); Sp2
[]
b; a{0}; d; exit [] (1); Sp2

この 2 つの仕様は右の LTS に変換でき、等価関係にある。



5 シミュレータ

HIPPO に改良を加え拡張 LOTOS のシミュレータを作成した。拡張が単純なので簡単な改良で済んだ。ただし、choice $x : t \parallel B$ の取り扱いができない。

6 おわりに

本稿では、時間の経過を表す特別なイベントを導入することにより LOTOS への時間概念の導入を行なった。この方法は、タイムスタンプによる方法と比べると記述力は劣るが、単純で扱いやすいと思われる。今後の課題としては、choice も含めた Full LOTOS への拡張、記述実験を行なうことなどが考えられる。

参考文献

- [1] ISO: LOTOS-A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour, IS 8807, 1989
- [2] N. Shiratiri, H. Kaminaga, K. Takahashi, S. Noguchi: A verification method for LOTOS specification and its application, Protocol Specification, Testing, and Verification, IX, 1990
- [3] T. Bolognesi and F. Lucidi: LOTOS-like process algebras with urgent or timed interactions, Formal description techniques 6, 1992
- [4] Contribution on Enhancements to LOTOS, ISO/IEC JTC1/SC21/WG1 N1180, 1992