整数データを含むLOTOS仕様の等価性の証明について

4V−5

李湘東　中田明夫　安本慶一　東野輝夫　谷口健一

大阪大学 基礎工学部 情報工学科

1 まえがき

通信プロトコルなどの分散システムの形式仕様記述言語としてISO(国際標準化機構)においてLOTOS [1] が考案され, 現在までに等価性の判定法や実行系の開発, 適合性試験などに関する多くの研究がなされている. LOTOSにおける意味モデルはラベル付遷移システム (LTS) と呼ばれる有向グラフであり, その有向グラフで与えられたプロセスの実行可能なイベントが表現される. 従来, データを含まないBasic-LOTOSと呼ばれるLOTOSのサブクラスで, そのLTSが有限であるようなクラスに対して, LOTOS仕様の等価性(双模倣等価性) [2] を機械的に判定するアルゴリズムが考案されている[3],[4]. しかしデータを含むクラスに対しては, 未だ有効な判定法が考案されていない. 一般に, 任意のデータを含むFull-LOTOSに対する等価性の判定問題は決定不能である. そこで, 本稿ではまず有限LP-LOTOSと呼ばれるLOTOSのサブクラスを定義し, そのクラスのLOTOS仕様の双模倣等価性を機械的に判定するアルゴリズムを提案する. LP-LOTOSでは, データ型として整数型のデータのみを取り扱い, 整数上の演算を加減算, 大小比較に限定している. 提案する方法では, 従来の状態分割による等価性の判定アルゴリズムを拡張して2つの有限LP-LOTOS仕様の等価性を判定する.

2 諸定義

[定義 2.1 (LP文)]
整数上の変数x,y,... の一次不等式 (等式でもよい), 並びにそれらの論理結合をLP文と呼ぶ.
[定義 2.2 (LP-LOTOS)]
次の条件を満足するLOTOS仕様をLP-LOTOS仕様と呼ぶ.
(1) すべてのガードが1つの変数から成るLP文で表されている.
(2) すべての入力イベントはa?x[Q(x)] の形で表されている. ただしQ(x) は入力変数xのみからなるLP文.
(3) 出力イベント及び内部イベントがない.

また, 実行可能な無限のイベント系列が存在するとき, その仕様を無限LOTOS仕様と呼び, そうでない仕様を有限LOTOS仕様と呼ぶ. 本稿では有限LP-LOTOS仕様を対象に等価性の判定を行う. 次章で有限LP-LOTOSの例を示す. 一般にLOTOS仕様が有限の場合, その仕様を連接";"と選択"[]"オペレータのみを用いた等価なLOTOS仕様に容易に変換することができる. このため, 以下ではこれら2つのオペレータのみを取り扱う.

LP-LOTOSでは内部イベントを取り扱わないので, その等価性は強双模倣等価性に相当する.
[定義 2.3 (強双模倣)]
プロセスの関係Rが強双模倣であるとは, pRq なら, 任意のイベント系列tに対して, 次の2つの条件が成り立つことである. ただし,$p \xrightarrow{t} p'$はpでtを実行するとp'に遷移することをあらわす.
(1) $p \xrightarrow{t} p'$ ならば, あるq'が存在して$q \xrightarrow{t} q'$ かつ $p'Rq'$ を満たす.
(2) $q \xrightarrow{t} q'$ ならば, あるp'が存在して$p \xrightarrow{t} p'$ かつ $p'Rq'$ を満たす.
[定義 2.4 (強双模倣等価性)]
プロセスp,qに対して, ある強双模倣関係Rが存在して, pRqが成り立つとき, pとqは強双模倣等価であるといい, $p \sim q$と書く.

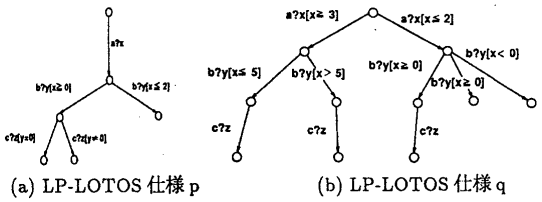
Verification of Equivalence among LOTOS Specifications with Integer Parameters
Xiangdong LI, Akio NAKATA, Keiichi YASUMOTO, Teruo HIGASHINO, Kenichi TANIGUCHI
Department of Information and Computer Sciences,
Faculty of Engineering Science, Osaka University
Toyonaka-shi, 560 Japan

3 等価なLP-LOTOS仕様の例

以下にp~qであるような2つの有限LP-LOTOS仕様の例p, qを紹介する.

```
p:=a?x;((([x ≧ 0]->b?y;([y = 0]->c?z;stop)
                        []([y ≠ 0]->c?z;stop)))
        []([x ≦ 2]->b?y;stop))
q:=(a?x[x ≧ 3];(([x ≦ 5]->b?y;c?z;stop)
                []([x > 5]->b?y;c?z;stop))
  []a?x[x ≦ 2];((([x ≧ 0]->b?y;c?z;stop)
                []([x ≧ 0]->b?y;stop))
                []([x < 0]->b?y;stop)))
```

図1はそれぞれp, qの入力変数やガードを無視してBasic-LOTOSと見なした場合のLTSの各枝にもとの入力変数やガードを付加した有向グラフである.



(a) LP-LOTOS仕様p　(b) LP-LOTOS仕様q

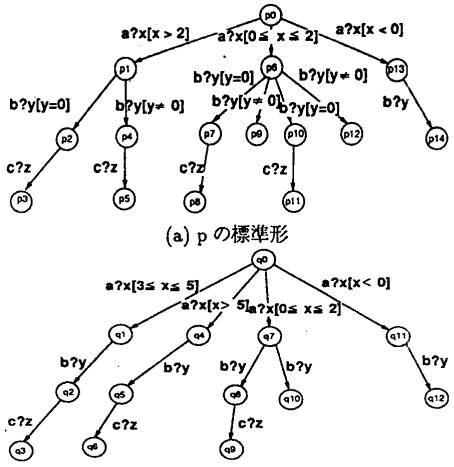
図1 等価なLP-LOTOS仕様の例

4 等価性判定手続き

4.1 有限LP-LOTOS仕様の標準形

等価性を証明するため, 与えられた有限LP-LOTOS仕様を図2のような"標準形"と呼ばれる等価な有限LP-LOTOS仕様に変換する. 標準形の各ノードは元のLTSのノードとそれまでに読み込んだ入力値に関する条件式の対をあらわす. 標準形は次のような手順で生成する.
(1) 変数名の付け替え
図1のようなLTSの一つのノードから複数の入力イベントが出ている場合はそれらの変数名を同じ変数名に置き換える (上のp, qはこの条件を満足する).
(2) ガードの重複部分を分割したLOTOS仕様への変換
例えば, 上のLP-LOTOS仕様pでa?xを実行すると2つのガード[x ≧ 0], [x ≦ 2] によって選択動作が行われる. しかし, 実際に選択動作が行われるのは[x ≧ 0], [x ≦ 2] が共に成り立つ (0 ≦ x ≦ 2) 場合のみであり, x<0の場合や2<xの場合は選択は行われない. そこで, ガードに重複がある場合はそれらを分離する. 各ガードp(x), q(x) はLP文であるので, 重複がある (p(x) and q(x) を満たす解がある) かどうかは決定可能. 重複がある場合, "p(x) and q(x)"と"p(x) and not(q(x))", "not(p(x)) and q(x)"の3つのガードに分割する (充足不能なガードは考慮しない). 3つ以上のガードが重複する場合も同様. 例えば, 図1 (a) のLP-LOTOS仕様pのガードの重複部分を分割すると図3 (a) のようになる.

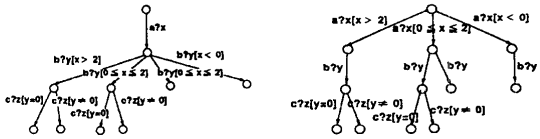
(3) ガードの移動
図3 (a) では入力イベント a?x に相当する枝の子孫の枝に変数 x からなるガードが幾つかあるが, これらのガードの真偽は a?x を実行した時点で定まる. そこで, a?x の実行時にどのガードが成り立つかに応じて条件分けを行う. この際, 上の (2) 同様, ガードに重複がないように条件分けを行う. 例えば, 図3 (a) の LTS の変数 x に関するガードを a?x の実行時に条件分けを行なうように移動すると図3 (b) のようになる. 同様に, 変数 y によるガードの移動を行うと図2 (a) になる. すべての変数について移動が終了すると, 標準形が得られる.



(a) p の標準形

(b) q の標準形

図2 LP-LOTOS 仕様の標準形



(a) ガードの重複部分の分割　　(b) ガードの移動

図3 標準形への変換過程

4.2 標準形の状態の同値類分割

以下に標準形における各状態に対して, 従来の手法と同様な同値類分割を適用する方法を示す. なお, 標準形の LTS の各ノードを状態と呼び, ノード s から s'へ $a?x[P(x)]$ なるラベルの辺がある時,$s- < a?x, P(x) > - > s'$と書く.

アルゴリズム

- input 標準形になっている LTS
- $S \leftarrow$ 標準形におけるすべての状態の集合
- $P_0 \leftarrow \{S\}$
- for $s \in S$ do
  - events$(s) \stackrel{\text{def}}{=} \{(a?x, P_a(x))|$ 状態 s で a が実行可能 $\}$ を求める. ただし,$P_a(x) \stackrel{\text{def}}{=} \bigvee\{P(x)|\exists s' s- < a?x, P(x) > - > s'\}$($\bigvee$は $\{\}$ 内の要素の論理和). 各 $P_a(x)$ は LP 文である.
- 同値関係 $s \sim_1 s' \stackrel{\text{def}}{=}$ (events(s) = events(s')) によって Sを同値類に分割し, その分割を P_1とする.

※ $(a?x, P(x)), (a?y, Q(y)) \in$ events(s) なる LP 文 $P(x), Q(y)$ に対し, $\forall w[P(w) \equiv Q(w)]$ の真偽は決定可能である.

- $k \leftarrow 1$
- while $P_k \neq P_{k-1}$ do
  - let $P_k = \{S_1, \ldots, S_{n_k}\}$
  - for $i := 1$ to n_k do
    - S_iを同値関係$\sim_{k+1}$によって同値類に分割し, その分割を $P_{k+1,i}$とする.
      ただし, $s_1 \sim_{k+1} s_2$とは, 以下の条件がすべて成立することをいう.
      1. $s_1- < a?x, P(x) > - > s'_1$ならば, $s_2- < a?x, Q_l(x) > - > s'_{2,l,m}$かつ $P(x) \wedge Q_l(x)$ が充足可能な任意の lに対して, ある m, jが存在して $s'_1, s'_{2,l,m} \in S_j$
      2. $s_2- < a?x, Q(x) > - > s'_2$ならば, $s_1- < a?x, P_l(x) > - > s'_{1,l,m}$かつ $P_l(x) \wedge Q(x)$ が充足可能な任意の lに対して, ある m, jが存在して $s'_{1,l,m}, s'_2 \in S_j$

      ※ LP-文では $P(x) \wedge Q(x)$ の充足可能性は判定可能.
  - $P_{k+1} \leftarrow \bigcup_{i=1}^{n_k} P_{k+1,i}$
  - $k \leftarrow k+1$
- output P_k

図 2(a),(b) の 2 つの標準形の各状態を同値類分割すると次のようになる.

$P_1 =$ $\{\{p_0, q_0\}, \{p_1, p_6, p_{13}, q_1, q_4, q_7, q_{11}\},$
$\{p_2, p_4, p_7, p_{10}, q_2, q_5, q_8\},$
$\{p_3, p_5, p_8, p_9, p_{11}, p_{12}, p_{14}, q_3, q_6, q_9, q_{10}, q_{12}\}\}$

$P_2 =$ $\{\{p_0, q_0\}, \{p_1, q_1, q_4\}, \{p_6, q_7\}, \{p_{13}, q_{11}\},$
$\{p_2, p_4, p_7, p_{10}, q_2, q_5, q_8\},$
$\{p_3, p_5, p_8, p_9, p_{11}, p_{12}, p_{14}, q_3, q_6, q_9, q_{10}, q_{12}\}\}$

$P_3 = P_2$

p_0, q_0がともに同じ同値類に属するので図 1 の LP-LOTOS 仕様 p,q は強双模倣等価である.

5 あとがき

本稿では, 有限 LP-LOTOS と呼ばれる LOTOS のサブクラスに対して, 双模倣等価性を証明するアルゴリズムを提案した. なお, かけ算を許すと, たとえ有限であっても等価性の判定は決定不能である. 定義 2.2 の制限を緩めることや再帰を含むような (有限でない)LP-LOTOS に拡張することなど, 取り扱えるクラスを広げることが今後の課題である.

参考文献

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

[2] D. Park: "Concurrency and automata on infinite sequences", Proceedings 5th GI Conference , Vol. 104 of Lecture Notes in Computer Science, Springer-Verlag, pp. 167–183 (1981).

[3] P. C. Kanellakis and S. A. Smolka: "CCS expressions, finite state processes, and three problems of equivalence", Information and Computation, **86**, pp. 43–68 (1990).

[4] N. Shiratori, H. Kaminaga, K. Takahashi and S. Noguchi: "A verification method for LOTOS specifications and its application", Protocol Specification, Testing, and Verification, IX , IFIP, Elsevier Science Publishers B.V., pp. 59–70 (1990).