プロセス等価性の自動証明器の実装

1M－3

鈴木理創　米津光浩　山口文彦　中西正和
慶應義塾大学 理工学部 数理科学科

1. はじめに

プロセスの等価性とは、2つのプロセスが同じような振舞いをすることである。また様々な種類があり、その中から、動作の基本単位であるアクションが全て観測可能な強等価性とそのアクションに外部から観測不能な内部アクションを加えた弱等価性を取り上げる。

2. プロセス代数

プロセス代数 [1](process algebra) とは、現実世界でのプロセスを、構文論的には形式体系として、意味論的には代数としてモデル化した数学的対象である。

3. プロセスの代数的記述

アクションはシステムによって実行される原子的動作の単位であり、外部から観測可能であるとする。以下アクション全体の集合 $\mathcal{A}$ を仮定する。

定義　プロセス動作式

E ::=　x　(プロセス変数)
　　| 0　(無動作プロセス)
　　| $a.E$　(アクションプレフィクス)
　　| $E+E$　(選択)

状態 S でアクション a を実行することができ、a の実行の結果状態 S' に遷移することを

$$S \xrightarrow{a} S'$$

で表す。

遷移規則は次のようなものである。

(1) $a.p \xrightarrow{a} p$

(2) $p \xrightarrow{a} r \Rightarrow p+q \xrightarrow{a} r$, $q \xrightarrow{a} r \Rightarrow p+q \xrightarrow{a} r$

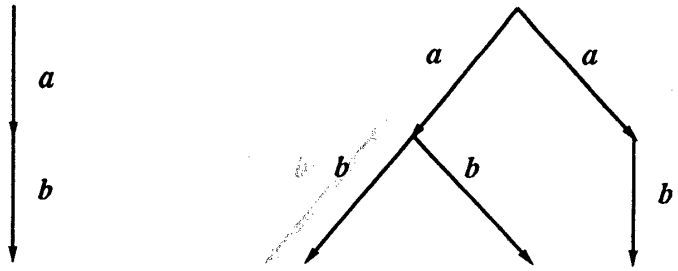

図 1: $p_1 = a.b.0$,　$q_1 = a.(b.0+b.0)+a.b.0$

4. 強等価性

強等価性とは、アクションは全て観測可能であるとした場合の双模倣によるプロセスの等価性であり、次の強双模倣という関係について定義される [1]。

定義　強双模倣

プロセス上の関係 R が**強双模倣** (strong bisimulation) であるとは、pRq ならば $\forall t \in \mathcal{A}^*$ について次の2つの条件が成り立つことである。

(1) $p \xrightarrow{t} p' \Rightarrow \exists q',\ q \xrightarrow{t} q' \ \wedge \ p'Rq'$

(2) $q \xrightarrow{t} q' \Rightarrow \exists p',\ p \xrightarrow{t} p' \ \wedge \ p'Rq'$

等価性判定法

強等価性の判定には、完全な公理系を用いて、標準形に変形する方法を用いる [1]。

プロセスの強等価性に対する公理系

(1) $p+q = q+p$

(2) $p+(q+r) = (p+q)+r$

(3) $p+p = p$

(4) $p+0 = p$

これらの公理系によって、一般のプロセスを標準形に変形できる。

プロセス p が**標準形** (standard form) であるとは、

$$p = a_1.p_1 + \cdots + a_n.p_n$$

Imprementation of a process equivalency prover
Riso SUZUKI　Mitsuhiro YONEZU
Fumihiko YAMAGUCHI　Masakazu NAKANISHI
Department of Mathematics , Faculty of Science and Technology, Keio University 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, Kanagawa 223, Japan

で表される場合である。ここで $a_i \in A$ であり、p_i はまた標準形の形をしているとする。

5. 弱等価性

弱等価性とは、外部から観測不能でしかも制御できないアクション (記号的にτで表し、**内部アクション** (internal action) と呼ぶ) を内部的に実行できるプロセスの等価性であり、次の弱双模倣という関係について定義される [1]。

定義　弱双模倣

プロセス上の関係 R が**弱双模倣** (weak bisimulation) であるとは、pRq ならば、$\forall a \in \mathcal{A} \cup \{\tau\}$ について、次の 2 つの条件が成り立つことである。

(1) $p \stackrel{a}{\Rightarrow} p' \Rightarrow \exists q' \quad , \quad q \stackrel{a}{\Rightarrow} q' \quad \wedge \quad p' R q'$

(2) $q \stackrel{a}{\Rightarrow} q' \Rightarrow \exists p' \quad , \quad p \stackrel{a}{\Rightarrow} p' \quad \wedge \quad p' R q'$

等価性判定法

等価性の判定には、元の遷移システム TSに、次のような遷移集合を付け加えて、新しい遷移システム(元の遷移システムの推移的閉包)TS'を構成する。

$$TS' = \{\stackrel{a}{\rightarrow} \mid \stackrel{a}{\Rightarrow}, a \in \mathcal{A}\}$$

そして、この推移的閉包から、τ を削除する。このようにして得られた遷移システムどうしが強等価であることと、元の遷移システムどうしが弱等価であることは、同値になる [1]。

6. LOTOS 仕様の等価性

ここでは、有限な 2 つの LOTOS 仕様の遷移システムの等価性について考える。

プロセスの LOTOS による表現を動作式 [1][2][3][4] と呼び、次のようにして定義する。

定義　動作式

E ::= **stop**　(プロセスの停止)
| **exit**　(正常終了)
| $a;E$　(アクションプレフィクス)
| $E[]E$　(選択)
| $E|||E$　(非同期並列)
| $E||E$　(同期並列)
| $E|[A]|E$　(並列合成)
| $E[>E$　(割り込み)
| $E >> E$　(逐次合成)
| **hide** A **in** E　(隠蔽)
| $P[g_1, \cdots, g_k](\mathrm{e})$　(プロセス呼びだし)

但し、$a \in Act \cup \{i\}$(Act は全ての観測可能な動作の有限集合)、$A \subset Act$、$k \in \mathbf{N}$、e は式のベクトル。

等価性判定法

LOTOS の等価性の判定は弱等価性の判定に帰着できるので、弱等価の場合と同じようにして等価性の判定を行なうことができる [1][2][3][4]。

7. 結果

プロセス動作式、LOTOS という記述方法と同等な能力を持つプロセスのリスト表現を用いて記述し、プロセス代数を用いた、2 つのプロセスの等価性自動証明器を実装した。例えば、図 1 のような 2 つのプロセスの強等価性は、

```
>(strong '(a b) '(+ (a (+ b b))(a b)))
standard form of first is (A B)
standard form of second is (A B)
strong equivalent
NIL
```

と判定される。

8. 今後の展望

- プロセス動作式の変換システムの設計
- LOTOS のフルセットを用いた場合の等価性の証明

参考文献

[1] 二木厚吉, 富樫敦, 木村成伴, 大蒔和仁ら :「プロセス代数とその応用 第 1 回〜第 11 回」,bit,Vol 23,No.11-12,1991,Vol 24,No.1-8,1992

[2] 神長裕明, 高橋薫, 白鳥則郎, 野口正一:「LOTOS 仕様の等価性とその判定法」, 信学論,D-I,Vol J72-D-I,No.5,1989

[3] 神長裕明, 高橋薫, 白鳥則郎, 野口正一:「LOTOS 仕様の効率的な等価性判定法」, 信学論,D-I,Vol J73-D-I,No.2,1990

[4] 中田明夫, 東野輝夫, 谷口健一,「隣接しない動作間の時間制約を記述するための LOTOS 言語の拡張とその等価性の検証」, コンピュータソフトウェア,Vol.12,No.6,Nov,1995, 岩波書店