時相論理を用いた試験等価性の特性化

5X－5

山下 健司　米崎 直樹

東京工業大学情報理工学研究科計算工学専攻

1 はじめに

遷移システムを形式的に取り扱うための数学的手法としてプロセス計算がある [3]。プロセス計算では様々な等価性を定義することによって、プロセス式が持つ特定の性質を調べることができる。そのような等価性の一つとして、試験等価性 [4] がある。

試験等価性は、通信を行うことを前提とした等価性で、試験者と呼ばれる特別なプロセス式と通信を行い、その合否判定によって等価性が定義される。

これまでに、それぞれの等価性が持つ本質的な概念を明らかにすることを目的に、等価性の判定問題から論理の同値性判定への還元が行われてきた [2]。

そこで、本論文ではこれまでに試みられていない試験等価性の論理による特性化を行う。ここで提案する論理の特徴は、until 演算子を用いることにより、直観的にかわりやすいモデルを構成することができる点にある。また、試験等価性と同等な失敗等価性 [1] とここで構成した論理式との関係についても言及する。

2 プロセス計算と試験等価性

2.1 プロセス計算

ここで取り扱うプロセス計算は最も基本的なオペレータのみを持つプロセス計算である。すなわち、無動作・アクションプレフィックス・非決定的選択だけからなる。アクションの集合を $\mathcal{A}ct$ とする。

ここで考えるプロセス式の Syntax は

$$p := \mathrm{nil} \mid a.p \mid p_1 + p_2 \quad (a \in \mathcal{A}ct)$$

で表され、プロセス式の意味は次のような遷移規則で与えられる。

$$\frac{}{a.p \xrightarrow{a} p} \qquad \frac{p_j \xrightarrow{a} p'}{\sum_{1 \le i \le n} p_i \xrightarrow{a} p'} \ (1 \le j \le n)$$

Characterization of Testing Equivalence by Temporal Logic
Kenji Yamashita, Naoki Yonezaki
Department of Computer Science, Tokyo Institute of Technology
2-12-1, Oookayama, Meguro-ku Tokyo 152, Japan

2.2 試験等価性

試験等価性の形式的な定義はここでは省略して、直観的な意味を説明する。

試験等価性では各プロセス式を試験する試験者と呼ばれる特別なプロセス式が存在する。試験者は成功を表す特別なアクション ω を実行することができる。試験者はそれぞれのプロセス式 p と同期して、「どのように遷移しても成功する」「成功する遷移がある」「必ず失敗する」のいずれかを結果として返す。

試験等価性には、「成功する場合がある試験者の集合が等しい」ことを意味する may- 等価と「どのように遷移しても成功する試験者の集合が等しい」ことを意味する must- 等価の２つの等価性が存在するが、以下では must- 等価のみを対象とする。

例 2.1 *must-* 等価ではない例

$p = a.(b.nil + c.nil), q = a.b.nil + a.c.nil$ とすると、試験者 $t = a.b.\omega$ は p, q を区別する。p は「どのように遷移しても成功する」が、q は「成功する遷移がある」

3 時相論理による特性化

3.1 時相論理

定義 3.1 時相論理の式の *Syntax* は以下のとおり。

$$F := \bot \mid \overline{a} \mid F_1 \to F_2 \mid \forall\bigcirc F \mid F_1[F_2] \quad (a \in \mathcal{A}ct)$$

ここでは、$\neg, \vee, \wedge, \exists\bigcirc, \langle\,\rangle$ は以下の省略形とする。

$\neg A \equiv A \to \bot, A \vee B \equiv \neg A \to B, A \wedge B \equiv \neg(\neg A \vee \neg B)$

$\exists\bigcirc A \equiv \neg\forall\bigcirc \neg A, A\langle B\rangle \equiv \neg(\neg A[B])$

さらに、次の省略形を用いる。

$$\langle\overline{a}\rangle A \equiv \exists\bigcirc(\overline{a} \wedge A), \quad [\overline{a}]A \equiv \forall\bigcirc(\overline{a} \to A)$$

定義 3.2 時間モデル $M = \langle W, R, m\rangle$ (M は時刻の集合、R は W 上の関係を表す術語、m は各時刻に真となる原始命題の集合を割り当てる関数) が与えられたとき、W の要素の有限系列 z が以下の条件を満たすとき、z は時刻 w_0 における $path$ であるという。

- $z = w_0 w_1 \cdots w_n$ とすると、すべての $0 \le i \le n-1$ について、$w_i R w_{i+1}$ であり、かつすべての $w \in W$ について $w_n R w$ が成り立たない。

定義 3.3 時間モデル M の $w \in W$ で式 F が真であることを、$\overset{M}{w} \models F$ で表し、以下のように定義する。

$\overset{M}{w} \not\models \bot$, $\overset{M}{w} \models \bar{a}$ iff $\bar{a} \in m(w)$

$\overset{M}{w} \models F_1 \to F_2$ iff $\overset{M}{w} \models F_1 \Rightarrow \overset{M}{w} \models F_2$

$\overset{M}{w} \models \forall \bigcirc F$ iff $\forall v \in W.\ (wRv \Rightarrow \overset{M}{v} \models F)$

$\overset{M}{w} \models F_1[F_2]$ iff $z(= w_0 \cdots w_n)$ が w における path であるならば次の条件のどちらかを満す

- $\exists j > 0.(\overset{M}{w_j} \models F_2$ かつ $\forall i\ (0 < i \leq j).\ \overset{M}{w_i} \models F_1)$
- $\overset{M}{w_0} \models F_2$

次の節では、ここで定義した時相論理を用いて試験等価性の特性化を行う。

3.2 試験等価性の特性化

定義 3.4 プロセス式 p に対応する論理式 $(\delta.p)'$ を次のように構成する。δ は $\mathcal{A}ct$ に含まれない特別のアクションとする†。$[[F]], \langle\langle F \rangle\rangle$ はそれぞれ $\overline{F}[F], \overline{F}\langle F \rangle$ の略記。

- $(\mathrm{nil})' \overset{def}{=} [[\forall \bigcirc \bot]]$
- $(p + \mathrm{nil})' \overset{def}{=} (p)'$, $(\mathrm{nil} + p) \overset{def}{=} (p)'$
- $(a_1.p_1 + a_2.p_2 + \cdots + \tau.p_i + \cdots + a_n.p_n)' \overset{def}{=} (a_1.p_1 + a_2.p_2 + \cdots + p_i + \cdots + a_n.p_n)'$
- $(a_1.p_1 + a_2.p_2 + \cdots + a_n.p_n)' \overset{def}{=} [[\bigwedge_{i=1}^{n} [\overline{a_i}](\bigvee_{j \in \{j \mid a_i = a_j\}} (p_j)'' \wedge (\sum_{j \in \{j \mid a_i = a_j\}} p_j)')\ ]]$

複数の規則が適用可能な場合は上にある規則を優先して適用するものとする。

ここで、プロセス式 p が次に実行可能なアクションを表す論理式 $(p)''$ は以下のように定義される。

- $(\mathrm{nil})'' \overset{def}{=} \top$
- $(p + \mathrm{nil})'' \overset{def}{=} (p)''$, $(\mathrm{nil} + p)'' \overset{def}{=} (p)''$
- $(a_1.p_1 + a_2.p_2 + \cdots + \tau.p_i + \cdots + a_n.p_n)'' \overset{def}{=} \bigvee_{i \in \{i \mid a_i = \tau\}} (p_i)''$
- $(a_1.p_1 + \cdots + a_n.p_n)'' \overset{def}{=} \bigwedge_{i=1}^{n} \langle\langle \langle \overline{a_i} \rangle \top \rangle\rangle$

複数の規則が適用可能な場合は上にある方を優先して適用するものとする。

このようにプロセス式から時相論理式への変換を定義した場合、次の定理が成り立つ [5]。

定理 3.5 任意のプロセス式 p, q と、それぞれに対応する論理式 $(\delta.p)', (\delta.q)'$ について、

p, q が *must*-等価 iff 任意の時間モデル M について

$$\overset{M}{w} \models (\delta.p)' \iff \overset{M}{w} \models (\delta.q)'$$

†プロセス式が $\tau.nil + b.nil$ のように τ で分岐している場合に必要

証明の概略

右向きはプロセス式の構成に関する帰納法を用いて証明できる。左向きはその対偶を証明する。すなわち、p, q が must- 等価でないと仮定して、$(\delta.p)', (\delta.q)'$ を区別するモデルを実際に構成することで証明できる。

4 失敗等価性との対応

試験等価性 (must- 等価) と失敗等価性が同等であることはすでに知られている [4]。よって、定理 3.5の系として、前章で構成した論理式は失敗等価性を特性化しているといえる。そこで、前章で構成した論理式からプロセス式の失敗集合を取り出す手続きを与える。

プロセス式 p に対応する論理式 $(\delta.p)'$ が $\bigwedge_{i=1}^{n} \langle\langle \langle \overline{b_i} \rangle \top \rangle\rangle$ という形の部分式を持ち、その部分式に到る様相記号の系列が、$[\overline{\delta}][\overline{a_1}][\overline{a_2}] \cdots [\overline{a_m}]$ であるとき、$(a_1 a_2 \cdots a_m, \{b_1, \cdots, b_n\})$ を要素に加える。

$(\delta.p)'$ が $\top$ という形の部分式を持ち、その部分式に到る様相記号の系列が、$[\overline{\delta}][\overline{a_1}][\overline{a_2}] \cdots [\overline{a_m}]$ であるとき、$(a_1 a_2 \cdots a_m, \phi)$ を要素に加える。

こうしてできた集合を、

$$A(p) = \{(\alpha, A_\alpha) \mid \alpha \in \mathcal{A}ct^*, A_\alpha \in 2^{\mathcal{A}ct}\}$$

として、$A(p)$ から次のような集合 $B(p)$ を作る。

$$B(p) = \{(\alpha, B_\alpha) \mid (\alpha, A_\alpha) \in A(p), B_\alpha \subseteq \mathcal{A}ct - A_\alpha\}$$

このとき、$B(p)$ はプロセス式 p の失敗集合となる。

5 まとめ

本論文では、試験等価性の等価性判定問題を論理の同値性判定問題へと還元する手続きを与えた。また、本論文で構成した論理式からプロセス式の失敗集合を取り出す手続きについても言及した。

参考文献

[1] BERGSTRA, J. A., KLOP, J. W. and OLDEROG, E. R. Readies and failures in the algebra of communicating process, *SIAM journal on Computing*, **17**, 6 (Dec 1988), 1134–1177.

[2] HENNESSY, M. and MILNER, R. Algebraic Laws for Nondeterminism and Concurrency, *Journal of the Association for Computing Machinery*, **32**, 1 (Jan 1985), 137–161.

[3] MILNER, R. A Calculus of Communicating Systems, *Lecture Notes in Computer Science*, **92** (1980).

[4] NICOLA, R. D. and HENNESSY, M. C. B. Testing Equivalences for Processes, *Theoretical Computer Science*, **34**, 1–2 (1984), 83–133.

[5] 山下健司 時相論理による試験等価性の判定法, Master's thesis, 東京工業大学 (1997).