協調型言語における試験等価性と失敗等価性の関係とモデル検査への適用

大塚　寛†

愛媛大学理工学研究科†

1. 概要

本講演者は並列プログラムの作成において、各プロセス間の通信の仕様を CSP[1]で与え、この詳細化を経て、最終的には協調型言語[2]の枠組みによる実装を行っている。CSP では主に失敗集合によってプロセスに意味を与えるが、試験等価性[3]の立場からは、軌跡等価性と may 試験等価性の間に、失敗集合等価性と must 試験等価性の間に関係がある。ここではこれらの関係を協調型言語の枠組みの中で拡張して得られた関係を報告する。

2. 協調型言語

協調型言語による並列プロセス間の通信とは、タプル空間と呼ばれる永続的な領域を媒介とした非同期通信である。通信されるメッセージはラベルとデータの組であるが、ここではデータは考慮せず、また同期型のプリミティブ $out(v)$, $in(v)$, $rd(v)$ のみを扱う。協調型言語による並列プロセスの動作を記述する遷移関係はプロセスだけでなく、タプル空間の変化にも着目する。

2.1 プロセス代数

ラベルの集合 Σ に対しアクションの集合 A を以下で定義する。ただし $\tau \notin \Sigma$ である。

$$A := \{out(v), in(v), rd(v) \mid v \in \Sigma\} \cup \{\tau\}$$

プロセス表現を並列プロセスが基本プロセスの内部に現れないように定義する。$a \in A$, $L \subseteq \Sigma$ とするとき、

$$P ::= S \mid P \| P \mid P \mid [L] \mid P \mid P \setminus L$$

$$S ::= x \mid 0 \mid a.S \mid S + S \mid \mu x.S$$

プロセス表現に出現する再帰プロセス表現がすべてガード的で、かつ閉じているものをプロセスと呼び、プロセス P と Σ の元から成るマルチセット M の組 $\langle P, M \rangle$ を様相と呼ぶ。マルチセット M に要素 v を追加,削除する操作をそれぞれ $M+v$, $M-v$ で表す。このとき、様相に対する遷移関係 $\longrightarrow$ を次の遷移規則で生成される最小の関係で定義する。

$$\frac{}{\langle \tau.P, M \rangle \xrightarrow{\tau} \langle P, M \rangle}$$

$$\frac{}{\langle in(v).P, M \rangle \xrightarrow{in(v)} \langle P, M - v \rangle} \quad (v \in M)$$

$$\frac{}{\langle out(v).P, M \rangle \xrightarrow{out(v)} \langle P, M + v \rangle}$$

$$\frac{}{\langle rd(v).P, M \rangle \xrightarrow{rd(v)} \langle P, M \rangle} \quad (v \in M)$$

$$\frac{\langle P, M \rangle \xrightarrow{a} \langle P', M' \rangle}{\langle P + Q, M \rangle \xrightarrow{a} \langle P', M' \rangle} \quad + \text{ は可換}$$

$$\frac{\langle P\{\mu x.P / x\}, M \rangle \xrightarrow{a} \langle P', M' \rangle}{\langle \mu x.P, M \rangle \xrightarrow{a} \langle P', M' \rangle}$$

$$\frac{\langle P, M \rangle \xrightarrow{a} \langle P', M' \rangle}{\langle P \| Q, M \rangle \xrightarrow{a} \langle P' \| Q, M' \rangle} \quad \|, |[L]| \text{ は可換}$$

$$\frac{\langle P, M \rangle \xrightarrow{a} \langle P', M' \rangle}{\langle P |[L]| Q, M \rangle \xrightarrow{a} \langle P' |[L]| Q, M' \rangle}$$

$$\frac{\langle P, M \rangle \xrightarrow{a} \langle P', M' \rangle}{\langle P \setminus L, M \rangle \xrightarrow{a} \langle P' \setminus L, M' \rangle} \quad label(a) \notin L \ \vee \ a = \tau$$

ここではマルチセットの操作が不可能な場合は、プロセスの遷移は起きないものとする。

2.2 プロセスの traces, initials, refusals

プロセス P の意味とは、様相 $\langle P, \phi \rangle$ を初期状態とする遷移システムであり、P の軌跡の集合 $traces(P)$ とは、$\langle P, \phi \rangle$ の軌跡の集合

$$traces(\langle P, \phi \rangle) = \{t \mid \exists s'\, s.t. \langle P, \phi \rangle \xrightarrow{t} s'\}$$

のことである。この定義は CSP のそれと同じく軌跡の条件を満す。プロセス P, Q がトレース等価（$traces(P) = traces(Q)$）であることを $P \sim_{tr} Q$ と書く。

プロセスの拒絶集合とは、内部動作によって実行可能なアクションが無いプロセスに遷移する状況を表わすもので、様相上では次のように定義される。Σ の各元の任意の多重度を許すマルチセットを U として、様相 $\langle P, M \rangle$ およびプロ

Testing Equivalence and Failure Equivalence in Coordination Languages and Their Application to Model Checking

†Hiroshi Ohtsuka, Graduate School of Science and Engineering (Dept. of Science), Ehime University

セス P の実行可能なアクションを

$initials(\langle P,M\rangle) = \{a \in A \mid \exists s'\, s.t. \langle P,M\rangle \xrightarrow{a} s'\}$

$initials(P) = initials(\langle P,U\rangle)$

とするとき、$\langle P,M\rangle$ の拒絶集合を

$refusals(\langle P,M\rangle) = \{X \subseteq Act \mid \exists \langle Q,N\rangle\, s.t.$

$\langle P,M\rangle \xrightarrow{\tau} \langle Q,N\rangle \wedge initials(Q) \cap X = \phi\}$

と定義する。これは CSP のそれと同じく拒絶集合の条件を満す。

以上を元に CSP の失敗集合が構成される。

3. プロセスの試験

「プロセス P をテストプロセス T を用いてインターフェイス L の下で試験を行う」ためにいくつか準備をする。まず Σ を L と $H = \Sigma - L$ に分割する。また分割を q とするとき、L_q, H_q と書く。プロセス T が L_q テストとは、$\alpha T = L_q \cup \{\omega\}$ かつ、L_q のアクションによる軌跡 t による T のどのような t-導出も L_q のアクションで拒絶されないこと、である。ここで q は Σ の分割、ω は成功を表す新たなアクションである。またすべての L_q テストからなる集合を $TEST_{L_q}$ と書く。

$t \in traces(P)$ が $successful$ を次で定める。

$\exists s'\, s.t. \langle P,\phi\rangle \xrightarrow{t} s' \wedge s' \xrightarrow{\omega}$

3.1 may_q 試験と等価性

P と $T \in TEST_{L_q}$ に対し、$P\, may_q\, T$ を

$\exists t \in traces((P \mid [L_q] \mid T) \setminus L_q)\ s.t.\ successful$

とする。このときプロセス P, Q が may_q 試験等価（$P \equiv_{may_q} Q$）であるとは

$\forall t \in TEST_{L_q}\ P\, may_q\, T \Leftrightarrow Q\, may_q\, T$

上の定義は次の意味で標準的な may 試験および may 試験等価性[3]の一般化である。

$P\, may\, T \Leftrightarrow Q\, may_{q_0}\, T,\ P \equiv_{may} Q \Leftrightarrow P \equiv_{may_{q_0}} Q$

ここに分割 q_0 は $L_{q_0} = \Sigma, H_{q_0} = \phi$、すなわち $P\, may\, T$ とは $(P \mid [\Sigma] \mid T) \setminus \Sigma$ が（アクションが外部から観測可能な CSP のプロセスの意味[4]で）成功する可能性がある事である。

may_q 試験については、次が成り立つことが示せた。プロセス P, Q と Σ の分割 q, r に対し、

$P \equiv_{may_q} Q \wedge L_r \subseteq L_q \Rightarrow P \equiv_{may_r} Q$

$P \equiv_{may_q} Q \Leftrightarrow P \setminus H_q \sim_{tr} Q \setminus H_q$

3.2 $must_q$ 試験と等価性

まず $\Sigma = L_q \cup H_q$ を次のように拒絶の有無で細分する。$L_q = LN_q \cup LR_q$, $H_q = HN_q \cup HR_q$ とし、拒絶されない部分を $N_q = LN_q \cup HN_q$、拒絶され得る部分を $R_q = LR_q \cup HR_q$ とする。

$t \in traces(P)$ が $complete\ w.r.t.\ N \subseteq \Sigma$ とは、t が無限かまたは、t が有限でかつ

$P \xrightarrow{t} Q \Rightarrow Q \not\xrightarrow{\tau} \wedge Q \not\xrightarrow{b}\quad (b \in N)$

とする。このとき P と $T \in TEST_{LN_q}$ に対し、$P\, must_q\, T$ を次で定める。

$\forall t \in traces((P \mid [L_q] \mid T) \setminus L_q)\ \ complete$

$w.r.t.\ LN_q \subseteq \Sigma\ s.t.\ successful$

このときプロセス P, Q が $must_q$ 試験等価（$P \equiv_{must_q} Q$）であるとは

$\forall T \in TEST_{LN_q}\ P\, must_q\, T \Leftrightarrow Q\, must_q\, T$

これらの定義も may_q 試験と同様の意味で、標準的な $must$ 試験および $must$ 試験等価性[3]の一般化である。

$must_q$ 試験については、次が成り立つことが示せた。プロセス P, Q と Σ の分割 q, r に対し、

$P \equiv_{must_q} Q \wedge L_r \subseteq L_q \Rightarrow P \equiv_{must_r} Q$,

$P \equiv_{must_q} Q \wedge H_r = H_q \wedge LR_r \subseteq LR_q$

$\Rightarrow P \equiv_{must_r} Q$

4. 課題

現在 $must_q$ 試験において、$must$ 試験等価性と失敗集合等価性との関係に対応する関係を考察中であり、特にこの関係を導出するためのテストプロセスを構成することが課題である。

参考文献

[1] C.A.R. Hoare, Communicating Sequential Processes, Prentice Hall, 1985

[2] D. Gelernter, Generative Communication in Linda. ACM Trans. Prog. Lang. Syst. 7, 1(Jan.), pp.80-112, 1985

[3] M. Hennessy, Algebraic Theory of Processes, MIT Press, 1988

[4] S. Schneider, Concurrent and Real-time Systems, The CSP Approach. Wiley, 2000