1N-6

失敗集合モデルによる非同期通信系の等価性定式化*

山中 顕次郎、 堀田英一、伊藤正樹†
NTT ソフトウェア研究所‡

1 はじめに

プロトコル試験、プロトコル合成、階層的な並行プロセス記述などを形式的に扱うためには、システム等価性の定式化が必要である。同期通信系の等価性については、Observation(Bisimulation) Equivalence[1]、Testing Equivalence[2] など多くの研究が有るが、非同期通信系については十分な議論がなされていない。

本稿では、Brookes らの CSP[3, 4] にもとづき、Failure Set(以下失敗集合とよぶ) Equivalence を非同期通信系における等価性に拡張する。

2 CSP の概要

CSP ではプロセス P をアルファベット (αP) と失敗集合 ($failures(P)$) の組で定義するαPは P に関与するイベントの集合であり、失敗集合は (1) 有る状態までのイベントのトレースと、(2) その状態で拒否できるイベントの集合の組、を要素とする集合である。

表 1 に CSP の主な演算子を示す。図 2 に同期並行合成の定義を示す。

図 1: CSP の主な演算子

x:{A}→P	前置	P⊓Q	非決定的選択
P|Q	選択	P\{A}	隠蔽
P||Q	(同期) 並行	P|||Q	インターリーブ
$\mu pF(p)$	再帰	P/s	トレース s 後の P

$$\alpha(P||Q) = \alpha P \cup \alpha Q$$
$$failures(P||Q) = \{(t, X \cup Y) | t \in (\alpha(P||Q))^* \wedge (t \uparrow \alpha P, X) \in failures(P) \wedge (t \uparrow \alpha Q, Y) \in failures(Q)\}$$

$t \uparrow S$はトレース t をイベントの集合 S で制限したもの。

表 1: 同期並行合成の定義

c がチャネル名で v が値のとき、c.v の形のイベントをコミュニケーションと呼ぶ。コミュニケーションと表 2 の略記により、チャネルを介した通信が表現される。

表 2: チャネルから (へ) の入 (出) 力

	記法	意味
入力	$c?x \rightarrow P(x)$	$y : \{y \mid channel(y) = c\} \rightarrow P(message(y))$
出力	$c!a \rightarrow P$	$c.a \rightarrow P$

*) channel(c.v)=c, message(c.v)=v.

簡単な例を図 2に示す。$\mathcal{P}(X)$は X の冪集合である。

$$\alpha a(P) = \alpha c(P) = \alpha d(P) = \mathrm{N}(\text{自然数の集合})$$
$$P \triangleq \mu p\,(a!0 \rightarrow c?x \rightarrow p)$$
$$\{(\varepsilon, X) | X \in \mathcal{P}(\alpha P - \{a.0\})\} \cup$$
$$\{(<a.0>, X) | X \in \mathcal{P}(\alpha P - c\alpha(P))\} \cup \ldots$$
$$\alpha b(Q) = \alpha c(Q) = \alpha d(Q) = \mathrm{N}$$
$$Q \triangleq (d!1 \rightarrow STOP) \sqcap \mu q\,(c!2 \rightarrow b!3 \rightarrow q)$$
$$\{(\varepsilon, X) | X \in \mathcal{P}(\alpha Q - \{d.0\})\} \cup$$
$$\{(<d.0>, X) | X \in \mathcal{P}(\alpha Q)\} \cup$$
$$\{(\varepsilon, X) | X \in \mathcal{P}(\alpha Q - \{c.2\})\} \cup$$
$$\{(<c.2>, X) | X \in \mathcal{P}(\alpha Q - \{b.3\})\} \cup \ldots$$
$$(P||Q)\backslash\{c\alpha(P||Q)\} \triangleq$$
$$STOP \sqcap a!0 \rightarrow STOP \sqcap (a!0 \rightarrow \mu r\,(a!0 \rightarrow b!3 \rightarrow r | b!3 \rightarrow a!0 \rightarrow r)$$
$$= \{(\varepsilon, X) | X \in \mathcal{P}(\alpha(P||Q) - c\alpha(P||Q))\} \cup$$
$$\{(\varepsilon, X) | X \in \mathcal{P}(\alpha(P||Q) - (c\alpha(P||Q) \cup \{a.0\}))\} \cup$$
$$\{(<a.0>, X) | X \in \mathcal{P}(\alpha(P||Q) - c\alpha(P||Q))\} \cup$$
$$\{(<a.0>, X) | X \in \mathcal{P}(\alpha(P||Q) - \{a.0, b.3\})\} \cup$$
$$\{(<a.0, a.0>, X) | X \in \mathcal{P}(\alpha(P||Q) - \{b.3\})\} \cup$$
$$\{(<a.0, b.3>, X) | X \in \mathcal{P}(\alpha(P||Q) - \{a.0\})\} \cup$$
$$\{(<a.0, a.0, b.3>, X) | X \in \mathcal{P}(\alpha(P||Q) - \{a.0, b.3\})\} \cup$$
$$\{(<a.0, b.3, a.0>, X) | X \in \mathcal{P}(\alpha(P||Q) - \{a.0, b.3\})\} \cup \ldots$$
$$\alpha c(P) = \{v | c.v \in \alpha P\}, \quad c\alpha(P) = \{c.v | c.v \in \alpha P\}$$

図 2: CSP の例

3 モデルと非同期通信によるプロセスの観測

モデル

本稿では次のモデルを取り扱う。

- 出力は常に実行可能 (非同期通信性)。
- 信号は必ず受信プロセスに届く (信頼性)。
- 通信路では順序が保たれる (順序保存性)。
- 同じ送受信プロセスをもつ複数の通信路が存在しうる (順序非保存性)。

非同期通信によるプロセスの観測

非同期通信は、バッファプロセスを用いて同期通信系でシミュレートすることが出来る。即ち送信側プロセスとバッファプロセスと受信プロセスとの 3 者の並行合成により、非同期通信下でのシステムが表現できる。無限バッファは CSP では次のプロセス$Buffer$で表現される。

$$Buffer = P(\varepsilon)$$
$$P(\varepsilon) = left?x \rightarrow P(<x>)$$
$$P(<x>\hat{}s) = (left?y \rightarrow P(<x>\hat{}s\hat{}<y>) | right!x \rightarrow P(s))$$

^ はシーケンスの連結を表す。

$left$は入力チャネル、$right$は出力チャネルである。

*An Extension of Failure Set Equivalence for Asynchronously Communicating System

†Kenjiroh Yamanaka, Eiichi Horita, Masaki Itoh
‡NTT Software Laboratories

システム内部の通信は「プロセス間にバッファを入れる」と言う約束で十分である。しかしシステムの等価性を定めるためには外部通信をどのように扱うか、即ち外部からの観測をいかに定めるかが重要である。ここではバッファを送信側のプロセスに並行合成したものを、非同期通信のもとでのプロセスの観測と考える。これは次の理由による。

- バッファにどのような値を蓄積するかを決めるのは送信側のプロセスであり、受信側が決定するのは値の取り出しのタイミングだけであること。
- そのため送信側に合成して考えた方が、プロセスの観測として決定度の高い表現となること。

定義 1 非同期観測
プロセス P の全て出力チャネルに $Buffer$ を並行合成し、P と $Buffer$ 間の通信を隠蔽したものを、P の**非同期観測**と呼び、P^ω で表す。 ■

非同期観測の失敗集合として一致により、非同期通信下での等価性が定義できる。

定義 2 非同期観測同値
プロセス P と Q の非同期観測が失敗集合として等しい時、P と Q は非同期観測同値であるといい、$P =^\omega Q$ で表す。 ■

4 非同期観測・非同期観測同値の性質

以下に非同期観測、及び$=^\omega$の性質を示す。証明は省略する。

定義 3 非同期並行合成
プロセス P,Q の非同期観測 P^ω, Q^ω の並行合成を、P と Q の非同期並行合成といい、$P||^\omega Q$ で表す。

$Buffer$ の性質から非同期観測の性質が導かれる。

命題 1 非同期観測の性質
P の非同期観測 P^ω はプロセスである。P^ω の非同期観測 $(P^\omega)^\omega$ は P^ω と一致する。 ■

命題 2 非同期観測同値の性質
P と Q が失敗集合同値のとき、P と Q は非同期観測同値である。即ち $P=Q$ なら、$P =^\omega Q$ である。 ■

例で示すように、逆は一般には成り立たない。

同値関係 E において次の条件が成り立つ時、E を合同関係という。条件は P を含む任意のコンテキスト F[P] と F での P の出現を Q に置き換えた F[Q] で、E(P,Q) ならば E(F[P],F[Q]) が成り立つ、である。また演算子 O に対し、E(P,Q) ならば E(O(P,...),O(Q,...)) のとき、E を O に関する合同関係と言う。

次の定理は CSP における '=' が並行合成 (||) に関して合同関係であるのに対し、'$=^\omega$' が非同期並行合成 ($||^\omega$) に関して合同であることを示している。これは$=^\omega$が並行システムの階層的な表現の目的に対し妥当性を持つことを表している。

定理 1 $=^\omega$は非同期並行に関して合同
$P =^\omega Q \Rightarrow \forall R\,(P||^\omega R) =^\omega (Q||^\omega R)$ ■

一般に演算子 o が $^\omega$ に関して分配則を満たす、即ち $(o(a,b))^\omega = o(a^\omega, b^\omega)$ ならば、非同期観測同値は o に関して合同関係である。

例 つぎの P,Q,R は非同期観測同値である。

$$\alpha P = \alpha Q = \alpha R = \{A.a, B.b\}$$
$$P = \mu p(A!a \rightarrow B!b \rightarrow p)$$
$$Q = \mu q(B!b \rightarrow A!a \rightarrow q)$$
$$R = \mu r(A!a \rightarrow r | B!b \rightarrow r)$$

同期系で考えると P,Q は交互に A.a,B.b を出力し、R は通信相手の要求に合わせて送信する。非同期観測のもとでは受信タイミングは環境が決定する。このため無限に A.a,B.b を出力する点で同一な P,Q,R は、非同期観測では一致する。 ■

5 まとめと今後の課題

CSP を基本にして、非同期通信系におけるサブシステムの観測、及びその間の等価性を定式化した。またそれらの基本的性質を明らかにした。特に非同期同値な 2 つのシステムは$||^\omega$ で結合されたコンテキスト中で互いに置き換え可能であることを示した。

今後の検討項目を以下に列挙する。

- 合同性について
  合同性を論じるためには、応用に即して演算子を取捨選択する必要がある。これは CSP(失敗集合) 上に非同期性に注目した言語を構成することに相当する。
- 有限バッファの取り扱いについて
  本稿では通信路が無限バッファで表現されるモデルを扱った。実際のプロトコルは有限バッファで実現されるので、有限バッファモデルとの関係を考慮する必要がある。

謝辞

研究の機会を与えて下さった NTT ソフトウェア研究所の市川晴久グループリーダに感謝します。

参考文献

[1] R.Milner, *A Calculus of Communication Systems*, LNCS 92, Springer-Veriag, Berlin, 1980,

[2] R.De Nicola, M.Hennessy, *Testing equivalence for processes*, TCS 34, 1984,

[3] S.D.Brookes, C.A.R.Hoare, A.W.Roscoe, *A Theory of Communicating Sequiential Processes*, JACM 31, 3 (July 84),

[4] C.A.R.Hoare, *Communicating Sequiential Processes*, Prentice-Hall, 1985.