アルゴリズム　23－14
（1991．9．20）

CCS+b: ブロードキャスト型通信機構を追加したCCS

今井祐二　結縁祥治　坂部俊樹　稲垣康善
(名古屋大学 工学部)

あらまし　本稿では基本的通信機構がブロードキャスト型である通信プロセスの形式的体系CCS+bを提案する。CCS+bにおいて、1つの送信プロセスと任意個の受信プロセスが関与し、受信プロセスが存在しない場合でも通信が完結するブロードキャスト型通信をモデル化した。

最初にCCS+bの導出意味論をCCSの導出意味論と同様に与える。さらに、強等価関係、観測等価、観測合同関係を導入し、ブロードキャスト型通信機構を持つプロセスの代数的な意味づけを与える。

CCS+b:Calculus of Communicating Systems with Broadcast

Yuuji Imai　Shoji Yuen　Toshiki Sakabe and Yasuyoshi Inagaki
(Nagoya University)

abstract　In this paper ,we propose a calculus of communicating systems with broadcast, which is called CCS+b. CCS+b models broadcast communication that one sender process and arbitarily many receiver processes participate at one communication action and this action may be completed with no receivers.

We first give a derivation semantics of CCS+b in a same way as CCS's. Then strong equivalence, observation equivalence and observation congruence are introduced to give argebraic semantics of CCS+b which has broadcast communication mechanism.

1 はじめに

通信プロセスの形式的体系の成果は多様な分野に反映されている。通信プロトコルの記述、検証もその1つである。現実のプロトコルを記述検証するためには、現実の世界での通信機構が、モデル化する形式的体系上での通信機構によって自然に表現されることが望ましい。

一方、個人用ワークステーションなどの接続に幅広く用いられているEthernetや、大量の情報を遠隔地に点在した場所へ同時に送ることができる衛星通信などの、いわゆるブロードキャスト型通信機構を持った通信媒体が広く実際に使われており、これらの上でのプロトコルを形式的に記述検証できることの利益は大きい。

ところが同期型通信プロセスの形式的体系として広く用いられているHoareのCSP[1]とMilnerのCCS[2]はブロードキャスト型通信を自然に表現することが難しい。

そこで本稿ではブロードキャスト型通信機構を持つ通信プロセスの形式的体系CCS+bを提案する。この体系を用いると1個以上の任意の個数のエージェントが参加する通信を自然な形で表現することができる。2節ではブロードキャスト型通信機構の明確な特徴づけを行なう。3節でCCS+bの構文規則を導入し、4節で導出意味論を示す。5節ではCCS+bがブロードキャスト型通信を自然に表現していることを示す。6節ではCCS+bの意味論として強等価関係、観測等価関係、観測合同関係を定義する。

2 ブロードキャスト型通信機構

本節ではブロードキャスト型通信機構をCCS,CSPがモデル化する通信機構と比較して特徴づける。

CCS,CSPの表す通信機構は、ともにアクションと言われる基本的かつ不可分な動作によって成り立っている。それぞれの動作は名前づけされている。プロセスが動作を行なうとは、動作と同じ名前のポートにおいて外部環境と通信することである。外部のプロセスの同じ名前のポートとの間で同期通信を行なうことで計算が進行する。

CSP,CCSが表現している通信機構は次のように特徴づけることができる。

CSPの通信機構

- 1度の通信が複数のプロセス間で起こる。
- 1つの名前につき1度の通信で参加するプロセスの集合は,静的に構文的に決定する。
- 1つの名前について決定されたプロセスの集合のすべてのプロセスが動作可能でなければその通信は起こらない。

CCSの通信機構

- 1度の通信が送信ポートを持つプロセス1個、受信ポートを持つプロセス1個の組によって起こる。
- 1つの通信につき送信・受信の各1個以上のプロセスが動作可能でなければ動作は起こらない。

これに対してブロードキャスト型通信機構は次のように特徴づけられる。

Broadcast型の通信機構

- 1度の通信で、送信1個、受信0個以上の任意の数のプロセスで動作が起こる。
- 1つの送信プロセスが、動作可能であれば通信が起こる。

よって、ブロードキャスト型通信機構の基本的動作はCSPの通信機構やCCSの通信機構の基本動作と全く異質のものであり、異なった計算モデルで捉えるのが自然である。

このようなブロードキャスト型通信を自然に表現するために、基本的通信機構がブロードキャスト型通信機構であるような体系CCS+bを提案する。

3 CCS+bの構文

CCS+bでは、通信プロセスはエージェント式と呼ばれる記号列で表現する。

[定義 1]
CCS+bの動作(action)の集合 Act を以下のように定義する。

- $\mathcal{B}$:
  ブロードキャスト受信名(Broadcast name)

の集合
$\mathcal{B}$ の元は受信を表す動作や、ポートにつける名前で ⓐ, ⓑ ... で表現する。

- $\overline{\mathcal{B}}$:
ブロードキャスト送信名 (Broadcast co-name) の集合
$\overline{\mathcal{B}}$ の元は送信を表す動作や、ポートにつける名前である。
$\overline{\mathcal{B}}$ の元は $\mathcal{B}$ の元 ⓐ , ⓑ ... に $\bar{}$ をつけた $\overline{ⓐ}, \overline{ⓑ}$ ... である。
- $Act = \mathcal{B} \cup \overline{\mathcal{B}} \cup \{\tau\}$: 動作の集合
ここで $\tau \notin \mathcal{B} \cup \overline{\mathcal{B}}$ は内部動作を表現する。

□

[定義 2]
$\mathcal{E}$ は、次の条件を満たす最小の集合である。

1. $\alpha \in Act$ かつ $E \in \mathcal{E}$ ならば $\alpha.E \in \mathcal{E}$
2. $E_1, E_2 \in \mathcal{E}$ ならば $E_1|E_2 \in \mathcal{E}$
3. $E_i \in \mathcal{E}(i \in I)$ ならば $\sum_{i\in I} E_i \in \mathcal{E}$
4. $E \in \mathcal{E}, \mathcal{L} \subseteq \mathcal{B}$ ならば $E\backslash L \in \mathcal{E}$

$\mathcal{E}$ の元をエージェント式と呼ぶ。

□

以下では表現を簡単化するために、
$I = \phi$ のとき $\sum_{i\in I} E_i$ を 0 と書き、
$I = \{1 \ldots n\}$ のとき $\sum_{i\in I} E_i$ を $E_1 + \ldots + E_n$ と書く。

4 CCS+b の導出意味論

名前つき遷移系とは、状態集合 S、遷移名集合 T、遷移関係の集合 $\{\xrightarrow{t} \subseteq S \times S | t \in T\}$ からなる系で

$$(S, T, \{\xrightarrow{t} | t \in T\})$$

で表す。$(s_1, s_2) \in \xrightarrow{t}$ である時 $s_1 \xrightarrow{t} s_1$ と書き、状態 s_1 は t で名前づけされた遷移で状態 s_2 になることを表す。

[定義 3] CCS+b のエージェント式に対して名前つき遷移系 *Behave* を次のように定義する。

$$Behave = (\mathcal{E}, Act, \{\xrightarrow{\alpha} | \alpha \in Act\})$$

ここで $\xrightarrow{\alpha} \subseteq \mathcal{E} \times \mathcal{E}$ は以下の推論規則を満足する最小の二項関係である。

$$\mathsf{Act}\ \frac{}{\alpha.E \xrightarrow{\alpha} E}$$

$$\mathsf{Com_1}\ \frac{E \xrightarrow{\alpha} E'}{E|F \xrightarrow{\alpha} E'|F}$$

$$\mathsf{Com_2}\ \frac{F \xrightarrow{\alpha} F'}{E|F \xrightarrow{\alpha} E|F'}$$

$$\mathsf{Com_{31}}\ \frac{E \xrightarrow{ⓛ} E',\ F \xrightarrow{ⓛ} F'}{E|F \xrightarrow{\tau} E'|F'} \text{ if } ⓛ \in \mathcal{B}$$

$$\mathsf{Com_{32}}\ \frac{E \xrightarrow{ⓛ} E',\ F \xrightarrow{\overline{ⓛ}} F'}{E|F \xrightarrow{\tau} E'|F'} \text{ if } ⓛ \in \mathcal{B}$$

$$\mathsf{Com_{33}}\ \frac{E \xrightarrow{\overline{ⓛ}} E',\ F \xrightarrow{ⓛ} F'}{E|F \xrightarrow{\tau} E'|F'} \text{ if } ⓛ \in \mathcal{B}$$

$$\mathsf{Sum}\ \frac{E_j \xrightarrow{\alpha} E'_j}{\sum_{i\in I} E_i \xrightarrow{\alpha} E'_j} \text{ if } j \in I$$

$$\mathsf{Res_1}\ \frac{E \xrightarrow{\alpha} E'}{E\backslash L \xrightarrow{\alpha} E'\backslash L} \text{ if } \alpha \notin L$$

$$\mathsf{Res_2}\ \frac{E \xrightarrow{\overline{ⓛ}} E'}{E\backslash L \xrightarrow{\tau} E'\backslash L} \text{ if } ⓛ \in L$$

□

エージェント式の導出意味論は *Behave* によって定義される。遷移関係 $E \xrightarrow{\alpha} F$ はエージェント式 E が動作 α を行なった後、F というエージェント式になるという振舞いを表す。

5 CCS+b の通信機構

ここではいくつかのエージェント式を例にして、エージェント式が *Behave* でどのような遷移関係を持つかを説明するとともに 2 節で示したブロードキャスト型通信機構が CCS+b でうまく表現できることを示す。

ブロードキャスト型通信機構の特徴を再度示す。

(⋆) 1 度の通信で、送信 1 個、受信 0 個以上の任意の数のプロセスで動作が起こる。

(⊙) 1 つの送信プロセスが、動作可能であれば通信が起こる。

まず特徴 (⋆) を CCS+b が持つことを示すためにエージェント式

$$((\overline{ⓐ}.0 | ⓐ.0) | ⓐ.0)\backslash\{ⓐ\} \qquad (1)$$

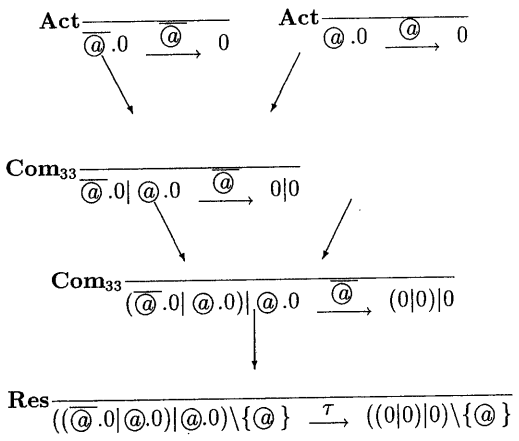
の振舞いを見ていく。

エージェント式 (1) は通信ポート $\overline{@}$ から信号を出力して停止する 1 つのプロセスと、通信ポート @ から信号を入力して停止する 2 つのプロセスが、外部とは @ に関する信号の伝達が制限された世界で並行に動作するプロセスを表現している。

(1) に対して、遷移関係

$$((\overline{@}.0|\ @.0)|\ @.0)\backslash\{@\} \xrightarrow{\tau} ((0|0)|0)\backslash\{@\}$$

が存在する。この遷移関係はは次のように導出される。



この他に $\xrightarrow{\tau}$ で (1) から遷移するエージェント式は 3 個あり、全部で 4 個存在する。

$$((0|\ @.0)|\ @.0)\backslash\{@\} \quad (2)$$

$$((0|0)|\ @.0)\backslash\{@\} \quad (3)$$

$$((0|\ @.0)|0)\backslash\{@\} \quad (4)$$

$$((0|0)|0)\backslash\{@\} \quad (5)$$

それぞれのエージェント式への遷移を直観的に解釈する。

- (2) は送信プロセス $\overline{@}.0$ だけが通信している。これは、送信プロセスが信号を出力したにもかかわらず、受信プロセスが反応しなかったと解釈できる。
- (3)(4) は、2 つの受信プロセス @ .0 のうち一方が、送信プロセス $\overline{@}.0$ と通信し遷移している。送信プロセスの出力した信号が 1 個の受信プロセスによって受信されたと解釈する。
- (5) では 2 つの受信プロセスと送信プロセスが通信している。この場合は出力された 1 つの信号を 2 つの受信プロセスが受信したと解釈できる。

これらから、CCS+b が先に述べた性質 ($\star$) を確かに満たしていることがわかる。

次に CCS+b が特徴 ($\odot$) を持つことを示すためにエージェント式

$$(\overline{@}.0|\ @.0)\backslash\{@\}$$

を考える。この式は直観的には @ を送信して停止するプロセスと、 @ を受信して止まるプロセスが、@ に関して閉じた世界で並行に動くプロセスである。

ここでこれらのプロセスの部分プロセスが何らかの原因で故障し、停止するプロセス 0 に置き換わるとする。

まず送信側プロセス $\overline{@}.0$ が故障して停止するプロセスに変化した場合を考える。

$$(0|\ @.0)\backslash\{@\}$$

この式は遷移関係を持たない。

これに対してプロセス中の受信側プロセス @.0 が故障したとする。

$$(\overline{@}.0|0)\backslash\{@\} \quad (6)$$

この式には遷移関係

$$(\overline{@}.0|0)\backslash\{@\} \xrightarrow{\tau} (0|0)\backslash\{@\}$$

が存在する。

受信動作を起こすプロセスが、存在しないにもかかわらず、送信プロセスが通信可能であるだけで通信が起こっている。

これは、CCS+b が確かに性質 ($\odot$) を満たしていることを意味する。

ちなみに CCS が特徴 ($\star$)($\odot$) を持たないことは以下のように示される。(1) と直観的意味の同じエージェント式

$$((\overline{a}.0|a.0)|a.0)\backslash\{a\}$$

の $\xrightarrow{\tau}$ による遷移は、送信プロセス $\bar{a}.0$ 1個と受信プロセス $a.0$ 1個が通信する場合

$$((0|0)|a.0)\backslash\{a\}$$
$$((0|a.0)|0)\backslash\{a\}$$

しか存在しない。よってCCSは性質 $(\star)$ を持たない。

また直観的意味が(6)に対応するCCSのエージェント式

$$(\bar{a}.0|0)\backslash\{a\}$$

には遷移関係が存在しない。つまり性質 $(\odot)$ はCCSにはない。

6 等価関係による意味論

Behave はCCS+bに動作的意味を与えている。本節でCCS+bにおける3種類の等価関係による意味論を導入する。CCS+bでは、相手が起こす任意の遷移を互いに模倣できる時に、エージェント式が等しいとする立場をとる。CCS+bにおいてもCCS[1]と同様に双模倣という概念を用いて、エージェント式の等価性が定義できる。

6.1 強等価関係

[定義 4]
2項関係 $\mathcal{S} \subseteq \mathcal{E} \times \mathcal{E}$ が強双模倣 (strong bisimilation) であるとは以下の条件を満たすことであると定義する。

$(E, F) \in \mathcal{S}$ ならば、任意の $\alpha \in Act$ について、

1. $E \xrightarrow{\alpha} E'$ ならば、$F \xrightarrow{\alpha} F'$ かつ $(E', F') \in \mathcal{S}$ なる F' が存在する。
2. $F \xrightarrow{\alpha} F'$ ならば、$E \xrightarrow{\alpha} E'$ かつ $(E', F') \in \mathcal{S}$ なる E' が存在する。

□

[定義 5]
エージェント式 E と F が強等価 (strong equivalent) であるとは $(E, F) \in \mathcal{S}$ なる強双模倣 $\mathcal{S}$ が存在することである。この時 $E \sim F$ と書く。

□

2つのプロセスが強等価であるとは直観的には、一方が行なうすべての動作を互いに模倣できることである。

[命題 1]
$\sim$ は等価関係である。

□

強等価関係は演算子 | に関して、交換律と結合律がなり立つ。

[命題 2]

1. $E|F \sim F|E$
2. $E|(F|G) \sim (E|F)|G$

[証明]
2の証明の概略を示す。定義5より、
$\mathcal{S} = \{(E_1|(E_2|E_3), (E_1|E_2)|E_3) | E_1, E_2, E_3 \in \mathcal{E}\}$
が強双模倣であることを証明すればよい。
$E_1|(E_2|E_3) \xrightarrow{\alpha} F$ とする。Com導出規則それぞれに対応した5つの場合分けが考えられ、それぞれの場合がさらにいくつかに場合分けされる。

Case 1 $E_1 \xrightarrow{\alpha} E_1', F \equiv E_1'|(E_2|E_3)$
Case 2 $E_2|E_3 \xrightarrow{\alpha} E_{23}', F \equiv E_1|E_{23}'$
Case 3 $\alpha = \textcircled{l}, E_1 \xrightarrow{\textcircled{l}} E_1', E_2|E_3 \xrightarrow{\textcircled{l}} E_{23}'$
$F \equiv E_1'|E_{23}'$
Case 4 $\alpha = \overline{\textcircled{l}}, E_1 \xrightarrow{\textcircled{l}} E_1', E_2|E_3 \xrightarrow{\overline{\textcircled{l}}} E_{23}'$
$F \equiv E_1'|E_{23}'$
Case 5 $\alpha = \overline{\textcircled{l}}, E_1 \xrightarrow{\overline{\textcircled{l}}} E_1', E_2|E_3 \xrightarrow{\textcircled{l}} E_{23}'$
$F \equiv E_1'|E_{23}'$

それぞれの場合に、
$(E_1|E_2)|E_3 \xrightarrow{\overline{\textcircled{l}}} G$ かつ $F \sim G$ なる G が存在することは容易に示せる。

□

この際 $\mathbf{Com_{31}}$ が、結合律の成立に重要な役割を果たす。それは、

$$E_1 \xrightarrow{\textcircled{l}} E_1', E_2 \xrightarrow{\textcircled{l}} E_2', E_3 \xrightarrow{\overline{\textcircled{l}}} E_3'$$

の条件の元で、図1, 図2の2つの導出が存在することが結合律の成立のためにに必要だからである。

交換律、結合律が成り立つことで、並列演算子によるプロセスの結合は、結合するプロセスの集合が決定できれば結合の仕方には独立に意味が決まる。すなわち送信プロセスの出した信号は演算子"|"で結合されたすべてのプロセスにエージェント式での構造と関係なく全く同じ条件で届くと

考えることができる。

$$E_1 \xrightarrow{\textcircled{l}} E_1', \quad \mathsf{Com}_{32}\ \frac{E_2 \xrightarrow{\textcircled{l}} E_2',\ E_3 \xrightarrow{\overline{\textcircled{l}}} E_3'}{E_2|E_3 \xrightarrow{\overline{\textcircled{l}}} E_2'|E_3'}$$

$$\mathsf{Com}_{32}\ \frac{}{E_1|(E_2|E_3) \xrightarrow{\overline{\textcircled{l}}} E_1'|(E_2'|E_3')}$$

図1 結合律の証明に必要な導出 1

$$\mathsf{Com}_{31}\ \frac{E_1 \xrightarrow{\textcircled{l}} E_1',\ E_2 \xrightarrow{\textcircled{l}} E_2'}{E_1|E_2 \xrightarrow{\textcircled{l}} E_1'|E_2'} \quad E_3 \xrightarrow{\overline{\textcircled{l}}} E_3'$$

$$\mathsf{Com}_{32}\ \frac{}{(E_1|E_2)|E_3 \xrightarrow{\overline{\textcircled{l}}} (E_1'|E_2')|E_3'}$$

図2 結合律の証明に必要な導出 2

次に強等価関係が合同関係であることを示す。

[命題 3]

$E \sim F$ ならば、

1. $\alpha.E \sim \alpha.F$
2. $E|G \sim F|G$
3. $E+G \sim F+G$
4. $E\backslash L \sim F\backslash L$

□

強等価関係が合同関係であるので、演算子によって合成されたエージェント式が表すプロセスの意味は、合成するもとのエージェント式が表すプロセスの意味だけから決まる。

6.2 観測等価関係

$t \in Act^*$ の時 $\hat{t} \in \mathcal{L}$ は t に出現するすべての τ を除いた系列を表す。

$\alpha \in Act$ に対して $E\{\xrightarrow{\tau}\}^* \xrightarrow{\alpha} \{\xrightarrow{\tau}\}^* E'$ の時 $E \overset{\alpha}{\Longrightarrow} E'$ である。特に $\alpha = \tau$ の時 $E \overset{\hat{\tau}}{\Longrightarrow} E$ とする。

[定義 6]

$\mathcal{S} \subseteq \mathcal{E} \times \mathcal{E}$ が弱双模倣 (weak bisimilation) であるとは以下の条件を満たすことであると定義する。

$(E,F) \in \mathcal{S}$ ならば、任意の $\alpha \in Act$ について、

1. $E \xrightarrow{\alpha} E'$ ならば、$F \overset{\hat{\alpha}}{\Longrightarrow} F'$ かつ $(E',F') \in \mathcal{S}$ なる F' が存在する。
2. $F \xrightarrow{\alpha} F'$ ならば、$E \overset{\hat{\alpha}}{\Longrightarrow} E'$ かつ $(E',F') \in \mathcal{S}$ なる E' が存在する。

□

[定義 7]

エージェント式 E と F が観測等価 (observation-equivalent) であるとは $(E,F) \in \mathcal{S}$ なる弱双模倣 $\mathcal{S}$ が存在することである。この時 $E \approx F$ と書く。

□

強等価関係が互いの動作を τ を含めて完全に模倣することを要求しているのに対して、観測等価関係では τ は内部動作を表しており外部から観測できないとし、τ についてはどのように動作するかは無視し、τ 以外の動作の模倣に注目する立場をとる。

[命題 4] $\approx$ は等価関係である。

□

観測等価関係が演算子 $|$ に関して、交換律と結合律を満たす。

[命題 5]

1. $E|F \approx F|E$
2. $E|(F|G) \approx (E|F)|G$

□

観測等価関係は $\sum$ 以外の演算に対しては合同関係である。

[命題 6] $E \approx F$ ならば、

1. $\alpha.E \approx \alpha.F$
2. $E|G \approx F|G$
3. $E\backslash L \approx F\backslash L$

□

ところが観測等価関係は $\sum$ に関して合同関係ではない、すなわち一般に

$E+G \approx F+G$ は成立しない。例えば

$$ⓐ.0 \approx \tau.ⓐ.0$$

であるが、

$$ⓐ.0 + ⓑ.0 \not\approx \tau.ⓐ.0 + ⓑ.0$$

である。

合同関係が成り立たないので強等価関係による意味論では演算子によって合成されたプロセ

スは、もとのエージェント式が表すプロセスからは決まらない。またエージェント式に代入などの代数的な操作ができない。そのような意味論はCCS+bのエージェント式によってプロセスを表現するのには適当とはいえない。

6.3 観測合同関係

6.2節の問題を解決するために、τについての条件を若干加えた関係を導入する。

[定義 8]

$\mathcal{S} \subseteq \mathcal{E} \times \mathcal{E}$が観測合同 (observation conguruent) であるとは以下の条件を満たすことであると定義する。

$(E,F) \in \mathcal{S}$ならば、任意の$\alpha \in Act$について、

1. $E \xrightarrow{\alpha} E'$ ならば、$F \stackrel{\alpha}{\Longrightarrow} F'$ かつ $E' \approx F'$ なる F' が存在する。
2. $F \xrightarrow{\alpha} F'$ ならば、$E \stackrel{\alpha}{\Longrightarrow} E'$ かつ $E' \approx F'$ なる E' が存在する。

この時$E = F$と書く。

□

観測等価関係では、模倣すべき動作がτである時に長さ0のτの系列によって遷移すること、すなわち何も遷移しないことでもτが模倣できたとしてしまう。観測合同では模倣すべき動作の系列の先頭がτであった時に限って、少なくとも1回τで遷移しないと模倣したことにならないという立場をとる。

[命題 7] $=$は等価関係である。

□

$=$は合同関係である。

[命題 8]

$E = F$ならば、

1. $\alpha.E = \alpha.F$
2. $E|G = F|G$
3. $E + G = F + G$
4. $E\backslash L = F\backslash L$

□

7 まとめ

ブロードキャスト型通信機構を表現するための形式的通信プロセス体系としてCCS+bを提案した。この体系では1個以上の任意の数のプロセスが参加する通信を自然な形で表現することができる。

さらに本稿ではCCS+bの意味論として強等価関係、観測等価関係、観測合同関係を導入した。これらの等価関係のもとで$|$について交換律と結合律が成立し、強等価関係、観測合同関係については、合同関係であることが示された。CCS+bのプロセスとは$\mathcal{E}$の強等価関係もしくは観測合同関係での同値分割$\mathcal{E}/\sim, \mathcal{E}/=$の元である。そのどちらをプロセスと意味づけるかは応用に応じて決めることができる。

CCS+bはこれらの意味に基づいて代数的にプロセスを取り扱うことを可能にする。したがって、CCS+bの表現するプロセスモデルはブロードキャスト型通信機構を持つ媒体上でのプロトコルの形式的記述、及びその検証などに適していると思われる。

本稿の定義では有限回数の動作で停止するプロセスしか扱うことはできないが、再帰の記述を導入することで、繰り返しを含む無限回の動作を実行できるプロセスを導入することは今後の課題である。また実際のブロードキャスト型通信媒体上のプロトコルを記述し検証に適用することも今後の課題である。

謝辞

日頃討論いただく研究室の皆様に感謝致します。

参考文献

[1] R.Milner:Communication and Concurrency, Prentice Hall(1989)

[2] C.A.R.Hoare:Communicating Sequential Processes,Prentice Hall(1985)