計算モデル特論

プロセス計算

国立情報学研究所
佐藤一郎
E-mail: ichiro@nii.ac.jp

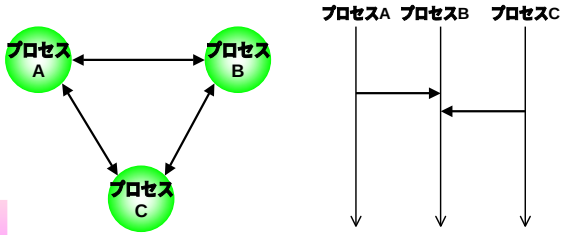
概要

1. プロセス計算
2. CCS
3. π計算

並列･分散計算は難しい

- 動作箇所が複数
- 非決定性

理論的な手法で記述･解析する必要がある。

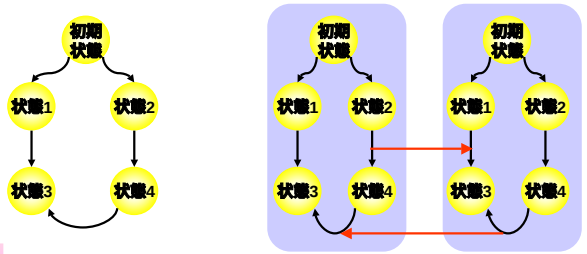


通信システムは難しい

- 送信側と受信側は独立に動作
- 通信プロトコルの接続可能性

オートマトンの並列化

手続き型プログラムは状態遷移図によるモデル化が容易
状態機械（オートマトン）は逐次動作



Ichiro Satoh

形式的記述・解析

- プログラム
- ペトリネット
- プロセス計算（プロセス代数）
- 時相論理

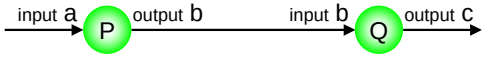
Ichiro Satoh

プロセス計算

- 通信を状態遷移アクションとするオートマトン
- 同期通信を中心に表現
- 手続き型言語に近い記述性
- 代数的な記述式の関係

$P =_{def} a.b.P'$

$Q =_{def} b.c.Q'$

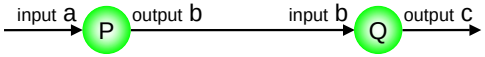


$System =_{def} (a.b.P'|b.c.Q')$

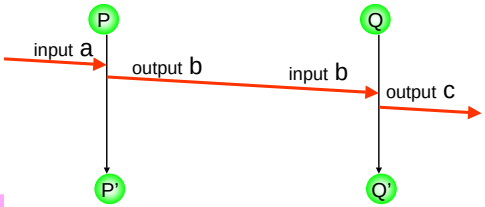
Ichiro Satoh

記述例

- プロセス式＝オートマトン＋通信手順＋プロセス合成



$System =_{def} (a.b.P'|b.c.Q')$



Ichiro Satoh

プロセス計算とは

並行・通信などの処理を含む動作を記述する形式系

代数的規則による定義

a+b = b+a　　a+(b+c) = (a+b)+c　　(a+b)c = ac+ab

a+a = a(ab)c = a(bc)

状態遷移規則による定義

$a.P \xrightarrow{a} P$　　$\dfrac{P \xrightarrow{a} P'}{P+Q \xrightarrow{a} P'}$　　$\dfrac{P \xrightarrow{a} P'}{P \mid Q \xrightarrow{a} P' \mid Q}$

プロセス計算体系の例：CCS、ACP、CSP

プロセス計算をプロセス代数と呼ぶことも多い

Ichiro Satoh

CCS (Calculus of Commucating Systems)

CCSの構文

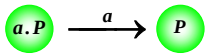
P	$:=$	0	停止プロセス
	|	$a.P$	同期入力 (通信入力aを受信後、Pとなる)
	|	$\bar{a}.P$	同期出力 (通信出力aを送信後、Pとなる)
	|	$\tau.P$	内部計算 (内部計算を実行後、Pとなる)
	|	$P+Q$	選択動作 (PまたはQとなる)
	|	$P\|Q$	並行動作 (PとQが並行に動作できる)
	|	$P \setminus L$	事象制限 (Lに含まれる事象名の外部観測禁止)
	|	A	プロセス定義 (A=Pとなるとき、AをPで置換)

Ichiro Satoh

CCSの遷移

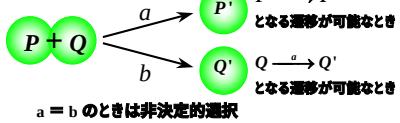
ラベル付き遷移システム (構造的操作意味論)

$\alpha.P \xrightarrow{\alpha} P$



$\dfrac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'}$

$\dfrac{Q \xrightarrow{\alpha} Q'}{P+Q \xrightarrow{\alpha} Q'}$



$\dfrac{P \xrightarrow{\alpha} P'}{P \setminus L \xrightarrow{\alpha} P' \setminus L} (\alpha \notin (L \cup \bar{L}))$

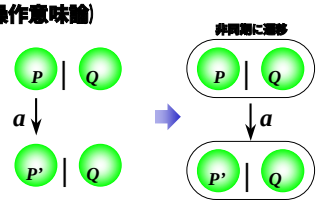
Ichiro Satoh

CCSの遷移

ラベル付き遷移システム (構造的操作意味論)

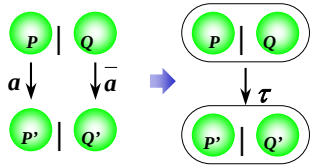
$\dfrac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q}$

$\dfrac{Q \xrightarrow{\alpha} Q'}{P \mid Q \xrightarrow{\alpha} P \mid Q'}$



$\dfrac{P \xrightarrow{a} P' \quad Q \xrightarrow{\bar{a}} Q'}{P|Q \xrightarrow{\tau} P'|Q'}$

一対一の同期通信



Ichiro Satoh

CCSの動作式例

動作式の例

$$a.P + b.Q|\bar{a}.R \xrightarrow{\tau} P|R$$

$$a.P + b.Q|\bar{a}.R \xrightarrow{a} P|\bar{a}.R$$

$$a.P + b.Q|\bar{a}.R \xrightarrow{\bar{a}} a.P + b.P|R$$

$$a.P + b.Q|\bar{a}.R \xrightarrow{b} Q|\bar{a}.R$$

$$(a.P + b.Q|\bar{a}.R)\backslash\{a,b\} \xrightarrow{\tau} (P|R)\backslash\{a,b\}$$

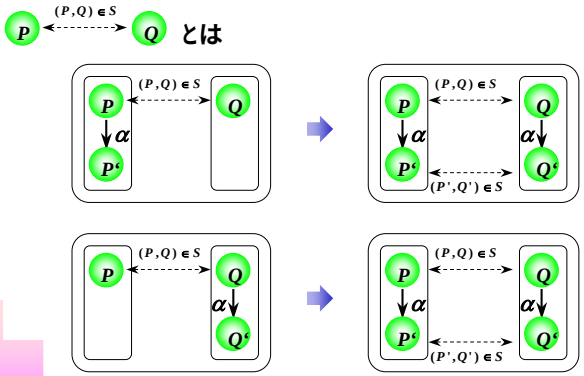
プロセス等価性

プロセス間の等価性
　例：仕様を表したプロセス vs 実装を表したプロセス
　　→ 実装は仕様を満足している

CCSなどのプロセス等価性をπ計算に導入：
　双模倣性、試験等価、失敗等価

ただし、π計算の等価性では名前を受け渡しを扱う必要がある

双模倣性 (Bisimulation)



プロセスの等価性

双模倣性に基づく代表的な等価関係

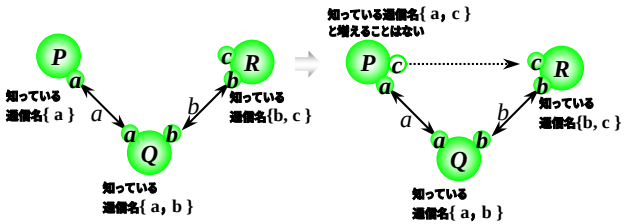
P+0 = P　　P+P = P　　P+Q = Q+P　　(P+Q)+R=P+(Q+R)
P|0 = P　　P|Q = Q|P　　(P|Q)|R = P|(Q|R)

インタリーブ関係 (並列＝非決定性)
a.b.0+b.a.0 = (a.0|b.0)

双模倣性に基づく等価関係により健全かつ完全な公理系が構築可能

CCSの問題点

通信名（ポート名）は静的に決定されている
→ 知らない通信名を介して通信ができない



CCSでは
ポインタ、オブジェクト識別子、動的にリンクが変化する通信ネットワーク
を含むシステムが記述できない

π計算

CCSに通信名（通信ポート名）の受け渡し機構を拡張 → π計算

Engberg,Nielsen[1986年]
通信引数に通信ポート名を導入
Thomsen［1989年］
プロセス受け渡し機構付きCCS（高階CCS）
Milner,Parrow,Walker［1989年］
π計算の提案（構造的操作意味論による定義）
Milner［1990年］
構造合同により簡約系としてπ計算を再定義
Milner[1991年]
多引数（polyadic）π計算

π計算の構文

ただし、π計算には構文構成子が異なる変形が存在する

P	:=	0	（停止したプロセス）
	|	$\overline{x}y.P$	（出力ポートxから引数yを送信）
	|	$x(y).P$	（入力ポートxから値または通信ポート名をyで受信）
	|	$P+Q$	（PまたはQとして振る舞う）
	|	$P\|Q$	（PとQが並行に動作できる）
	|	$(x)P$	（通信ポートxをPのスコープ内に制限する）
	|	$[x=y]P$	（xとyが一致したときのみPとして振る舞う）
	|	A	（A=Pとなるとき、AをPで置換）

事象の名前

π計算には遷移ラベル：

α	::=	τ	内部計算（外部から観測されない）
	|	$\overline{x}y$	束縛されない名前 y を出力ポート x から送信
	|	$\overline{x}(y)$	束縛された名前 y を出力ポート x から送信
	|	$x(y)$	入力ポート x から受け取った名前を束縛名 y と置換

α	$fn(\alpha)$	$bn(\alpha)$	$n(\alpha)$
τ	$\varnothing$	$\varnothing$	$\varnothing$
$\overline{x}y$	$\{x,y\}$	$\varnothing$	$\{x,y\}$
$\overline{x}(y)$	$\{x\}$	$\{y\}$	$\{x,y\}$
$x(y)$	$\{x\}$	$\{y\}$	$\{x,y\}$

π計算の遷移

π計算の状態遷移

$\bar{x}y.P \xrightarrow{\bar{x}y} P$ $\quad x(z).\bar{z}5Q \xrightarrow{x(w)} \bar{w}5.Q\{w/z\}$

$w \notin fn(Q) \vee w = y$

$\bar{x}y.P \mid x(z).\bar{z}5.Q \xrightarrow{\tau} P \mid \bar{y}5.Q\{y/z\}$

$fn(P)$ とは P に含まれる未束縛な名前の集合

Ichiro Satoh

π計算の操作意味論 (構造操作意味論)

構造的操作意味論による定義 $\alpha \in \{\bar{x}y, x(y), \tau\}$

$$\bar{x}y.P \xrightarrow{\bar{x}y} P \qquad x(y).P \xrightarrow{x(w)} P\{w/y\}\left(w = y \cup w \notin fn(P)\right) \qquad \tau.P \xrightarrow{\tau} P$$

$$\frac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'} \qquad \frac{P \xrightarrow{\alpha} P'}{[x=x]P \xrightarrow{\alpha} P'}$$

$$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q}\left(bn(\alpha) \cap fn(Q) = \varnothing\right) \qquad \frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P'|Q}\left(bn(\alpha) \cap fn(P) = \varnothing\right)$$

$$\frac{P \xrightarrow{\bar{x}(w)} P' \quad Q \xrightarrow{x(w)} Q'}{P|Q \xrightarrow{\tau} (w)(P'|Q')} \qquad \frac{P \xrightarrow{\bar{x}y} P' \quad Q \xrightarrow{x(z)} Q'}{P|Q \xrightarrow{\tau} P'|Q'\{y/z\}}$$

$$\frac{P \xrightarrow{\bar{x}y} P'}{(y)P \xrightarrow{\bar{x}(w)} P'\{w/y\}}\left(\begin{array}{c} y \neq x \\ w \notin fn(P') \vee w = y \end{array}\right) \qquad \frac{P \xrightarrow{\alpha} P'}{(x)P \xrightarrow{\alpha} (x)P'}\, x \notin n(\alpha)$$

$$\frac{P \xrightarrow{\alpha} P'}{A \xrightarrow{\alpha} P'}\left(A =_{def} P\right)$$

＋と｜は対称

Ichiro Satoh

π計算の操作意味論 (通信 1/2)

構造的操作意味論による定義 $\alpha \in \{\bar{x}y, x(y), \tau\}$

OUT: $\bar{x}y.P \xrightarrow{\bar{x}y} P$

IN: $x(y).P \xrightarrow{x(w)} P\{w/y\}\left(w = y \cup w \notin fn(P)\right)$

yまたはP内の非束縛名に変更可能

COM: $$\frac{P \xrightarrow{\bar{x}y} P' \qquad Q \xrightarrow{x(z)} Q'}{P|Q \xrightarrow{\tau} P'|Q'\{y/z\}}$$

PAR: $$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q}\left(bn(\alpha) \cap fn(Q) = \varnothing\right)$$

束縛名を受け取るときには、他の並行プロセスの非束縛名と重ならないこと

遷移例 $\bar{x}y.0 \mid x(z).\bar{z}5.0 \xrightarrow{\tau} 0 \mid \bar{y}5.0 \xrightarrow{\bar{y}5} 0 \mid 0$

Ichiro Satoh

π計算の操作意味論 (通信 2/2)

$\bar{x}y.P \xrightarrow{\bar{x}y} P \qquad x(y).P \xrightarrow{x(w)} P\{w/y\}\left(w = y \cup w \notin fn(P)\right)$

$$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q}\left(bn(\alpha) \cap fn(Q) = \varnothing\right) \qquad \frac{P \xrightarrow{\bar{x}y} P' \quad Q \xrightarrow{x(w)} Q'}{P|Q \xrightarrow{\tau} P'|Q'\{y/w\}}$$

遷移例 $\bar{x}y.P \mid (x(z).Q \mid R)$

$$\frac{\bar{x}y.P \xrightarrow{\bar{x}y} P \qquad \dfrac{x(z).Q \xrightarrow{x(w)} Q\{w/z\}}{x(z).Q \mid R \xrightarrow{x(w)} Q\{w/z\} \mid R}\left(\begin{array}{c} w=z \cup w \notin fn(P) \\ bn(x(w)) \cap fn(Q)=\varnothing \end{array}\right)}{\bar{x}y.P \mid (x(z).Q \mid R) \xrightarrow{\tau} P \mid (Q\{w/z\} \mid R)\{y/w\}}$$

$\bar{x}y.P \mid (x(z).Q \mid R) \xrightarrow{\tau} P \mid (Q\{y/z\} \mid R)$ ○

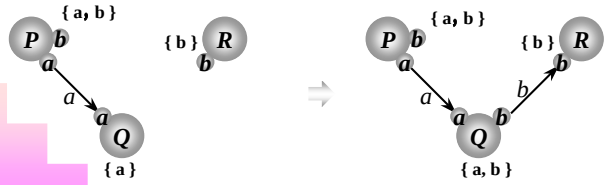
$\xrightarrow{\tau} P \mid (Q \mid R)\{y/z\}$ ×

Ichiro Satoh

動作式例 (1)

π計算の動作式の基本例:

$$\bar{a}b.P|a(x).\bar{x}5.Q|by.R \xrightarrow{\tau} P|(\bar{x}5.Q)\{b/x\}|by.R$$
$$\xrightarrow{\tau} P|(\bar{x}y.Q)\{b/x\}|by.R$$
$$(i.e.\ \ P|\bar{b}5.Q\{b/x\}|by.R)$$
$$\xrightarrow{\tau} P|Q\{b/x\}|R\{5/y\}$$



Ichiro Satoh

π計算の遷移

π計算の状態遷移　　$(x)P$　とは P 内で名前 x を宣言すること

RES: $\dfrac{P \xrightarrow{\alpha} P'}{(x)P \xrightarrow{\alpha} (x)P'}(x \notin n(\alpha))$　通信名がxのときは通信制限
引数がxのときはOPENとCLOSEによる

OPEN: $\dfrac{P \xrightarrow{\bar{x}y} P'}{(y)P \xrightarrow{\bar{x}(w)} P'\{w/y\}}\begin{pmatrix} y \neq x \\ w \notin fn(P') \vee w = y \end{pmatrix}$

束縛名をスコープ外に出す

CLOSE: $\dfrac{P \xrightarrow{\bar{x}(w)} P' \quad Q \xrightarrow{x(w)} Q'}{P|Q \xrightarrow{\tau} (w)(P'|Q')}$

束縛名を受け取り、スコープを広げる

Ichiro Satoh

π計算の遷移

π計算の遷移ラベル

$P \xrightarrow{\tau} P'$　環境と通信を行うことなく P から P' に状態遷移する
τP または P 内通信によって生じる

$P \xrightarrow{x(y)} P'$　リンク x に非束縛名 y を受信し P から P' に状態遷移する
$x(y)$ によって生じる

$P \xrightarrow{\bar{x}y} P'$　リンク x に非束縛名 y を送信し P から P' に状態遷移する
$\bar{x}(y)$ によって生じる

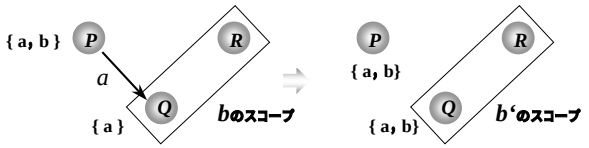
$P \xrightarrow{\bar{x}(y)} P'$　リンク x に束縛名 y を送信し P から P' に状態遷移する
$(y)\bar{x}y$ によって生じる

Ichiro Satoh

動作式例 (2)

π計算の動作式の基本例:

$$\bar{a}b.P|(b)(a(x).Q|R)$$
$$\xrightarrow{\tau} P|(b')(Q\{b'/b\}\{b/x\}|R\{b'/b\})$$



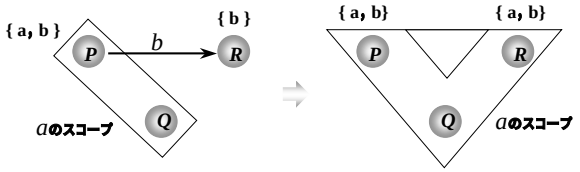
π計算ではα変換が可能:　$(x)(P|Q) = (x')(P\{x'/x\}|Q\{x'/x\})$

Ichiro Satoh

動作式例 (3)

π計算の動作式の基本例:

$$(a)(\bar{b}a.P|Q)|b(x).R \xrightarrow{\tau} (a)(P|Q|R\{a/x\})$$



π計算の操作意味論 (構造操作意味論)

SUM: $\dfrac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'}$

MATCH: $\dfrac{P \xrightarrow{\alpha} P'}{[x=x]P \xrightarrow{\alpha} P'}$

IDE: $\dfrac{P\{\tilde{y}/\tilde{x}\} \xrightarrow{\alpha} P'}{A(\tilde{y}) \xrightarrow{\alpha} P'} (A(\tilde{y}) =_{def} P) \qquad \tilde{y} = y_1 \cdots y_n$

π計算の操作意味論 (構造合同性)

構文的に一致する動作式集合を操作意味論に導入 (λ計算のα変換に相当)

$P|Q \equiv Q|P \quad P|(Q|R) \equiv (P|Q)|R \quad P|0 \equiv P$

$P+Q \equiv Q+P \quad P+(Q+R) \equiv (P+Q)+R \quad P+P \equiv P \quad P+0 \equiv P$

$(x)(y)P \equiv (y)(x)P \quad (x)0 \equiv 0 \quad (x)(P|Q) \equiv P|(x)Q \text{ if } x \notin fn(P)$

$[x=x]P \equiv P$

$A \equiv P(\text{where } A =_{def} P)$

STRUCT: $\dfrac{P \equiv Q \quad P \xrightarrow{\alpha} P' \quad P' \equiv Q'}{Q \xrightarrow{\alpha} Q'}$

π計算の操作意味論 (構造合同性)

構文的に一致する動作式集合を操作意味論に導入 (λ計算のα変換に相当)

$\bar{x}y.P \xrightarrow{\bar{x}y} P \quad x(y).P \xrightarrow{x(w)} P\{w/y\}\left(w = y \cup w \notin fn(P)\right)$

$(\cdots + x(y).P)|(\cdots + \bar{x}z.Q) \xrightarrow{\tau} P\{z/y\}|Q$

$\dfrac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P'|Q}\left(bn(\alpha) \cap fn(P) = \varnothing\right) \qquad \dfrac{P \xrightarrow{\alpha} P'}{(x)P \xrightarrow{\alpha} (x)P'} x \notin n(\alpha)$

$\dfrac{P \xrightarrow{\bar{x}(w)} P' \quad Q \xrightarrow{x(w)} Q'}{P|Q \xrightarrow{\tau} (w)(P'|Q')} \qquad \dfrac{P \xrightarrow{\bar{x}y} P'}{(y)P \xrightarrow{\bar{x}(w)} P'\{w/y\}}\begin{pmatrix} y \neq x \\ w \notin fn(P') \vee w = y \end{pmatrix}$

$\dfrac{P \equiv Q \quad P \xrightarrow{\alpha} P' \quad P' \equiv Q'}{Q \xrightarrow{\alpha} Q'}$

π計算の構文（追加）

複製（Replication）

$!P$　　$!P \equiv P|P!$

制限（Restriction）

$(\nu x)P$　　$(\nu x)P$ is $(x)P$

多引数π計算（Polyadic π Calculus）

$P ::= \bar{x}.[y_1 \cdots y_n]P \quad \bar{x}y_1 \cdots y_n.P$

$\quad | \quad x(y_1 \cdots y_n).P$

$\quad |$ （同じ）

$\bar{x}.[y_1 \cdots y_n]P | x(z_1 \cdots z_n).Q \xrightarrow{\tau} P|Q\{y_1/z_1, \ldots, y_n/z_n\}$

プロセス等価性

プロセス間の等価性

例：仕様を表したプロセス vs 実装を表したプロセス

→ 実装は仕様を満足している

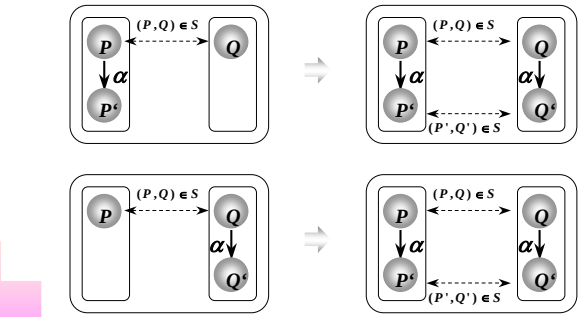
CCSなどのプロセス等価性をπ計算に導入：

双模倣性、試験等価、失敗等価

ただし、π計算の等価性では名前を受け渡しを扱う必要がある

双模倣性（Bisimulation）

$P \overset{(P,Q)\in S}{\cdots\cdots} Q$ とは



Early Bisimulation

早期双模倣関係 $(P,Q) \in S$ とは、任意の通信名a、引数xに対して以下の3条件が成立すること

(1) $P \xrightarrow{\bar{a}x} P' \Rightarrow \exists Q' : Q \xrightarrow{\bar{a}x} Q' \quad and \quad (P',Q') \in S$

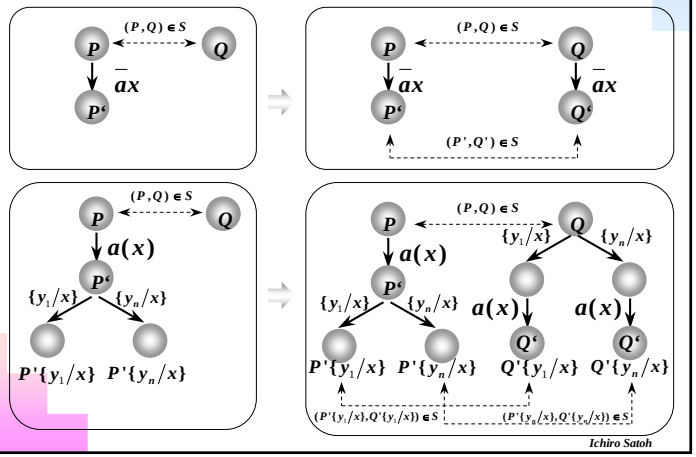
(2) $P \xrightarrow{a(x)} P' \quad and \quad x \notin FN(P,Q) \quad then$

$\exists Q' : Q \xrightarrow{a(x)} Q' \quad and \quad \forall y : (P'\{y/x\}, Q'\{y/x\}) \in S$

(3) S は対称

となる早期双模倣関係 S が存在するとき、$P \sim_E Q$ とし、PとQは早期双模倣であるという

Early Bisimulation $P \overset{(P,Q)\in S}{\longleftrightarrow} Q$ とは



Ichiro Satoh

Late Bisimulation

遅延双模倣関係 $(P,Q) \in S$ とは、任意の通信名a、引数xに対して以下の3条件が成立すること

(1) $P \xrightarrow{\overline{a}x} P' \Rightarrow \exists Q' : Q \xrightarrow{\overline{a}x} Q' \quad and \quad (P',Q') \in S$

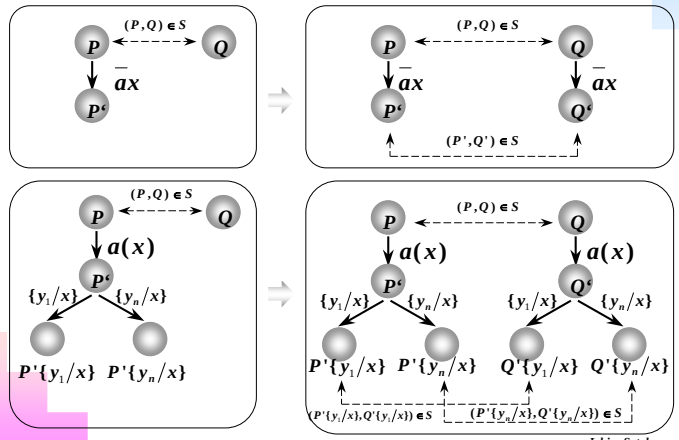
(2) $P \xrightarrow{a(x)} P' \quad and \quad x \notin FN(P,Q) \quad then$
$\forall y, \exists Q' : Q \xrightarrow{a(x)} Q' \quad and \quad (P'\{y/x\}, Q'\{y/x\}) \in S$

(3) S は対称

となる遅延双模倣関係 S が存在するとき、 $P \sim_L Q$ とし、PとQは遅延双模倣であるという

Ichiro Satoh

Late Bisimulation $P \overset{(P,Q)\in S}{\longleftrightarrow} Q$ とは



Ichiro Satoh

最近の研究

- 型理論との融合
  並行計算特有の型理論は存在するのか
- 高階プロセス計算
  プロセスそのものを通信引数として受け渡し
- プログラミング言語の意味論
  関数型プログラミング言語、オブジェクト指向言語の意味論を定式化
- プログラミング言語としての実現
  π計算に基礎におくプログラミング言語処理系の実装
- 非同期通信機構の導入
  同期通信より非同期通信にもとづく方が理論的洗練化が可能？

Ichiro Satoh

π計算の問題点

名前渡し機構は本当に必要なのか？

- 例：通信プロトコルの記述言語：
  プロセス代数はOSIデータリンク層のプロトコルが対象
  データリンク層の通信リンクは固定的
  名前渡し機能は必要はない

- 例：プログラミング言語として利用（例：PICT等）：
  意味論上の制約（ガード付き出力通信、事象の原子性など）の実装は困難
  他の並列・分散プログラミング言語でも十分

検証システムは構築可能なのか（π計算版のCWB等）？
CCSでも検証システムの構築は困難
体系自体が複雑すぎる？

Ichiro Satoh

π計算の問題点

π計算は相互作用系を表す最小の体系なのか？

$P\|Q \quad !P$	Parallelism
$(\nu x)P$	Naming, Restriction, Abstraction
$\bar{x}y.P \quad x(y).P$	Sending, Receiving

しかし、Binding 概念と Guarding 概念が混在

$$\bar{x}y|x(z).P \longrightarrow P\{y/z\}$$

Binding 概念と Guarding 概念の分離 → Action Structure [Milner93]

Ichiro Satoh