

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

Ichiro Satoh

概要

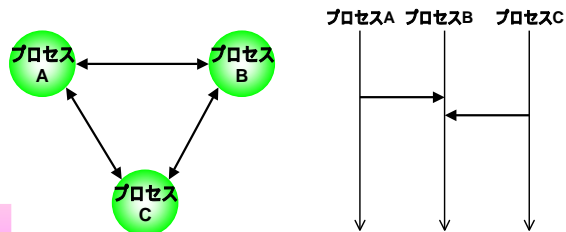
1. プロセス計算
2. CCS
3. 計算

Ichiro Satoh

並列・分散計算は難しい

- 動作箇所が複数
- 非決定性

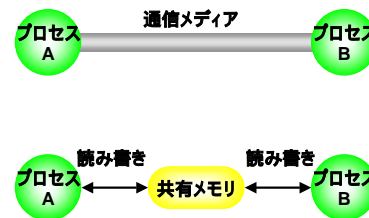
理論的な手法で記述・解析する必要がある。



Ichiro Satoh

通信システムは難しい

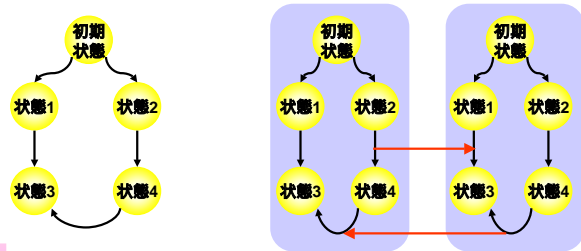
- 送信側と受信側は独立に動作
- 通信プロトコルの接続可能性



Ichiro Satoh

▶ 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

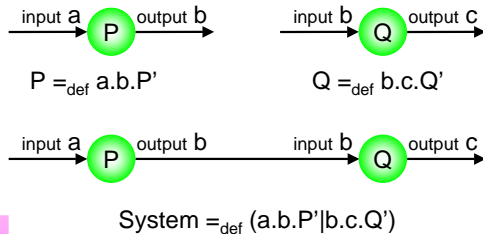
▶ 形式的記述・解析

- 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

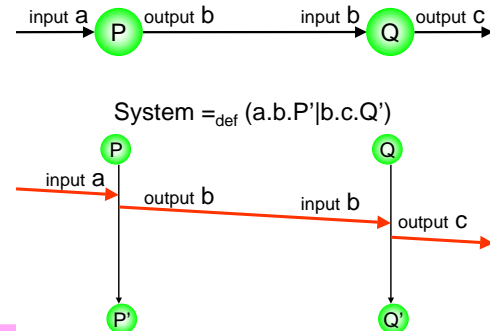
- 通信を状態遷移アクションとするオートマトン
- 同期通信を中心に表現
- 手続き型言語に近い記述性
- 代数的な記述式の関係



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



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

$$a+b = b+a \quad a+(b+c) = (a+b)+c \quad (a+b)c = ac+ab$$

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

状態遷移規則による定義

$$a.P \xrightarrow{a} P \quad \frac{P \xrightarrow{a} P'}{P+Q \xrightarrow{a} P'} \quad \frac{P \xrightarrow{a} P}{P|Q \xrightarrow{a} P'|Q}$$

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 Communicating 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となる時、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)

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

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

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

$$\frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{a}} Q'}{P|Q \xrightarrow{\alpha} P'|Q'}$$

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

$a = b$ のときは非決定的選択

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)

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

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

$$\frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{a}} Q'}{P|Q \xrightarrow{\alpha} P'|Q'}$$

一対一の同期通信

Ichiro Satoh

▶ CCSの動作式例

動作式の例

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

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

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

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

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

Ichiro Satoh

▶ 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 計算に導入:
 双模倣性、試験等価、失敗等価

ただし、 計算の等価性では名前を受け渡しを扱う必要がある

Ichiro Satoh

▶ 双模倣性 (Bisimulation)

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

Ichiro Satoh

▶ プロセスの等価性

双模倣性に基づく代表的な等価関係

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

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

intreeep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

Ichiro Satoh

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

Ichiro Satoh

計算

CCSに通信名(通信ポート名)の受け渡し機構を拡張 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]
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 計算を再定義

Milner [1991年]
多引数(polyadic) 計算

Ichiro Satoh

計算の構文

ただし、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)

$| \overline{xy}.P$ (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 y を受信)

$| P + Q$ (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 の範囲内に制限する)

$| [x = y]P$ (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)

Ichiro Satoh

事象の名前

計算には遷移ラベル:

$\alpha ::= \tau$ 内部計算(外部から観測されない)

$| \overline{xy}$ 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

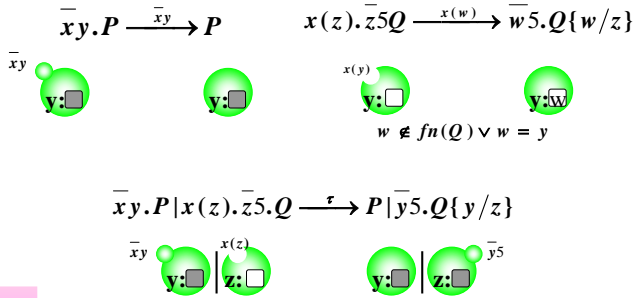
$| x(y)$ 入力ポート x から受け取った名前を束縛名 y と置換

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

Ichiro Satoh

計算の遷移

計算の状態遷移



$fn(P)$ とは P に含まれる未束縛な名前集合

Ichiro Satoh

計算の操作意味論 (構造操作意味論)

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

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

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

$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q} (bn(\alpha) \cap fn(Q) = \emptyset)$ $\frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P'|Q} (bn(\alpha) \cap fn(P) = \emptyset)$

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

$\frac{P \xrightarrow{\bar{x}y} P'}{(y)P \xrightarrow{x(w)} P'\{w/y\}} (y \neq x, w \notin fn(P') \vee w = y)$ $\frac{P \xrightarrow{\alpha} P'}{(x)P \xrightarrow{\alpha} (x)P'} (x \notin n(\alpha))$

$\frac{P \xrightarrow{\alpha} P'}{A \xrightarrow{\alpha} P'} (A =_{def} P)$ + と | は対称

Ichiro Satoh

計算の操作意味論 (通信 1/2)

構造的な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: $x(y).P \xrightarrow{x(w)} P\{w/y\} (w = y \cup w \notin fn(P))$

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

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

yまたはP内の非束縛名に変更可能

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異なるようにと

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

Ichiro Satoh

計算の操作意味論 (通信 2/2)

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

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

遷移例 $\bar{x}y.P | (x(z).Q | R)$

$\bar{x}y.P \xrightarrow{\bar{x}y} P$ $\frac{x(z).Q \xrightarrow{x(w)} Q\{w/z\}}{x(z).Q | R \xrightarrow{x(w)} Q\{w/z\} | R} (w = z \cup w \notin fn(P))$

$\bar{x}y.P | (x(z).Q | R) \xrightarrow{\tau} P | (Q\{w/z\} | R)\{y/w\} (bn(x(w)) \cap fn(Q) = \emptyset)$

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

Ichiro Satoh

▶ 動作式例(1)

計算の動作式の基本例:

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

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

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

$$\xrightarrow{\tau} P|Q\{b/x\}|R\{5/y\}$$

Ichiro Satoh

▶ 計算の遷移

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

OPEN: $\frac{P \xrightarrow{\bar{x}y} P'}{(y)P \xrightarrow{\bar{x}(w)} P'\{w/y\}}$ ($y \neq x$
 $w \notin fn(P') \vee w = y$)
束縛名をスコープ外に出す

CLOSE: $\frac{P \xrightarrow{\bar{x}(w)} P' \quad Q \xrightarrow{x(w)} Q'}{P|Q \xrightarrow{\tau} (w)(P'|Q')}$
束縛名を受け取り、スコープを広げる

Ichiro Satoh

▶ 計算の遷移

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)

計算の動作式の基本例:

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

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

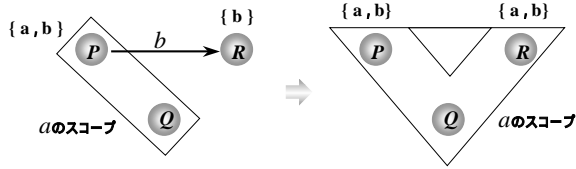
計算では 変換が可能: $(x)(P|Q) = (x')(P\{x'/x\}|Q\{x'/x\})$

Ichiro Satoh

動作式例 (3)

計算の動作式の基本例:

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



Ichiro Satoh

計算の操作意味論 (構造操作意味論)

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

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

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

Ichiro Satoh

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 (計算の 変換に相当)

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

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

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

$$[x = x]P \equiv P$$

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

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

Ichiro Satoh

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 (計算の 変換に相当)

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

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

$$\frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P'|Q} \quad (bn(\alpha) \cap \text{fn}(P) = \emptyset) \quad \frac{P \xrightarrow{\alpha} P'}{(x)P \xrightarrow{\alpha} (x)P'} \quad x \notin n(\alpha)$$

$$\frac{P \xrightarrow{\bar{x}(w)} P' \quad Q \xrightarrow{x(w)} Q'}{P|Q \xrightarrow{\tau} (w)(P'|Q')} \quad \frac{P \xrightarrow{\bar{x}y} P'}{(y)P \xrightarrow{x(w)} P'\{w/y\}} \quad (w \notin \text{fn}(P') \vee w = y)$$

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

Ichiro Satoh

計算の構文(追加)

複製 (Replication)

$$!P \quad !P \equiv P|P!$$

制限 (Restriction)

$$(\nu x)P \quad (\nu x)P \text{ is } (x)P$$

多引数 計算 (Polyadic Calculus)

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

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

$$| \quad (\text{同じ})$$

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

Ichiro Satoh

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

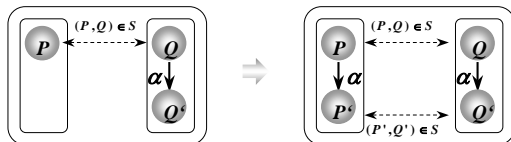
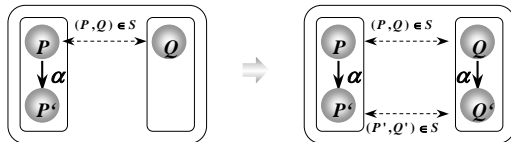
CCSなどのプロセス等価性を 計算に導入:
双模倣性、試験等価、失敗等価

ただし、計算の等価性では名前を受け渡しを扱う必要がある

Ichiro Satoh

双模倣性 (Bisimulation)

$(P, Q) \in S$ とは



Ichiro Satoh

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

Ichiro Satoh

