

# 計算モデルの数理 I: 計算

胡 振江

東京大学計数工学科

2008 年度

## 復習: 3年の「プログラムの数理」

関数プログラミング:

- プログラム: 式 + 関数の定義
- 計算: 式の簡約
- 計算の結果: 式の正規形

その理論背景は?

## 参考資料

- 井田哲雄, 「計算モデルの基礎理論」(第4章), 岩波講座ソフトウェア科学 12, 岩波書店, 1991年, 3700円. (ISBN4-00-010352-0)
- H.P.Barendregt, "The lambda calculus: its syntax and semantics", Studies in logic and the foundations of mathematics, v.103, North-Holland, 1984. (ISBN 044487 5085).
- 高橋正子, 「計算論 - 計算可能性とラムダ計算」, コンピュータサイエンス大学講座 24, 近代科学社, 1991年, 3500円. (ISBN 4-7649-0184-6)

# 計算モデル

計算を理論的・抽象的に考察するための数理モデル

- 機械モデル ( Turing 機械 )
- 関数モデル
- 論理モデル
- 書き換えモデル
- 代数モデル
- オートマトン

## 関数モデル

関数を用いて計算の概念を正確に捉えるモデル

- 帰納的関数の理論

計算可能な関数 = もっとも基本的な関数 + これらの関数の組み合わせ

- ラムダ計算

- ▶ 計算可能な関数：ラムダ項

- ▶ 計算：ラムダ項の簡約

## 計算の歴史的背景

### 1930 年代、Church

- ラムダ計算の基礎を与えた。
- 計算の概念を明確にし、計算可能性に対する一つの答えを与えた。

1950 年代、McCarthy ラムダ計算に基づくプログラミング言語 Lisp を提案した。

### 1960 年代、Landin

ラムダ計算によって Algol60 の意味が与えられた。

### 1970 年代、Scott

表示的意味論：ラムダ計算と、ラムダ計算を介してプログラム集合的意味を与え、計算機科学の全般に大きな影響を与えている。

### 1970 年代の後半

関数型言語に関する研究が盛んになった

現在: 標準的な関数型言語: ML, Haskell

## 基本的なアイデア

- 抽象化による関数の定義:

$$\lambda x.x + 1$$

$$\lambda x.(\lambda y.x + y)$$

- 関数適用:

$$(\lambda x.x + 1) 5 \Rightarrow 5 + 1$$

## 計算の言語

**Definition 1** (項)  $\mathcal{V}$  を可算無限個の変数の集合とする。項の集合  $\Lambda$  を次の条件 (1) ~ (3) を満たす最小の集合と定義する。

$$(1) \quad x \in \mathcal{V} \Rightarrow x \in \Lambda \quad (\text{変数})$$

$$(2) \quad M, N \in \Lambda \Rightarrow (MN) \in \Lambda \quad (\text{関数適用})$$

$$(3) \quad M \in \Lambda, x \in \mathcal{V} \Rightarrow (\lambda x.M) \in \Lambda \quad (\text{抽象化})$$

□

$\langle \text{項} \rangle ::= \langle \text{変数} \rangle \mid (\langle \text{項} \rangle \langle \text{項} \rangle) \mid (\langle \text{変数} \rangle . \langle \text{項} \rangle)$

問題: 正しい 項はどれ?

$(\lambda x. (\lambda y. (x y)))$

$(\lambda. (x y))$

$x$

$((x y) z)$

$(\lambda x. (x.y))$

$((\lambda x. (x x)) (\lambda x. (x x)))$

$(x (\lambda y. z))$

$(y (\lambda y))$

## 項の略記規則

- 最外側の括弧ははずしてよい.

$$((\lambda x.(x x)) (\lambda x.(x x))) \Rightarrow (\lambda x.(x x))(\lambda x.(x x))$$

- 関数適用操作は左結合.

$$((\dots (M_1 M_2) \dots) M_n) \Rightarrow M_1 M_2 \dots M_n$$

- 多重抽象化.

$$(\lambda x_1.(\dots (\lambda x_n.M) \dots)) \Rightarrow \lambda x_1 \dots x_n.M$$

問題 :  $(\lambda x.(\lambda y.((x\ y)\ (z\ u))))$  の略記表現は？

## 部分項

項の構造を調べるときによく用いる概念である。

**Definition 2 (部分項)** 項の部分項を次のように帰納的に定義する。

1.  $x \in \mathcal{V}$  の部分項は  $x$  である。
2.  $(M N)$  の部分項は  $M$  の部分項,  $N$  の部分項, および  $(M N)$  である。
3.  $(\lambda x.M)$  の部分項は  $M$  の部分項と  $(\lambda x.M)$  である。

□

項  $M$  の部分項とは,  $M$  を構成する ( $M$  自体を含む) 項のことをいう。  $M$  自体を除いた  $M$  の部分項を  $M$  の真部分項という。

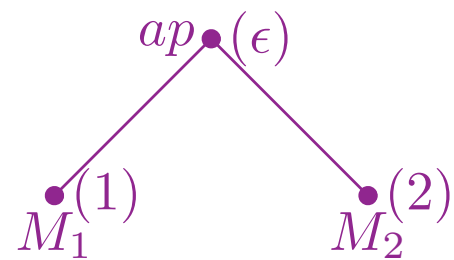
**問題:**  $(\lambda x y.x) (\lambda y.x) z$  のすべての部分項を求めよ。

## 項を表わすラベル付き木

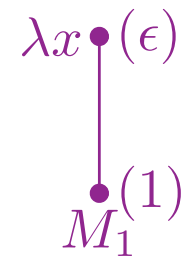
変数:

$$x \bullet (\epsilon)$$

関数適用:



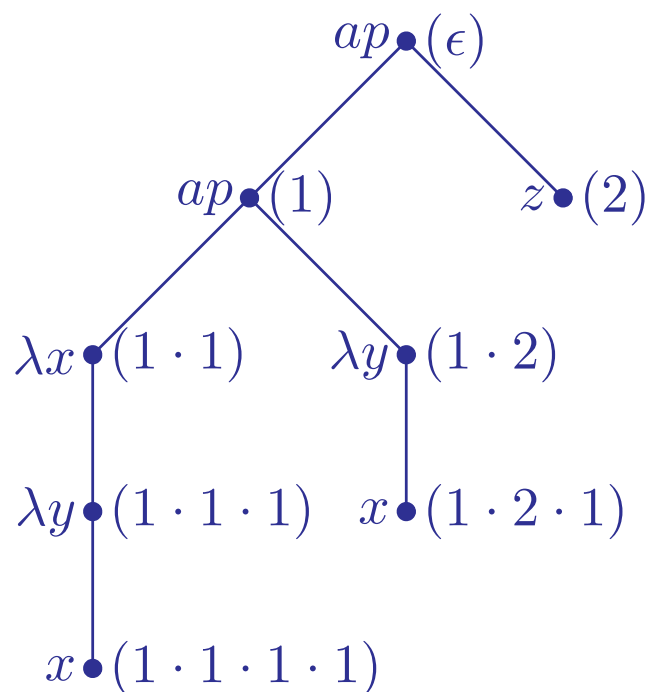
抽象化:



## 出現位置

ノードの出現位置はルートからの数字列で表現される．例： $(1 \cdot 1 \cdot 2)$ ．ルートの位置が  $\epsilon$  で表現される． $\epsilon \cdot i = i \cdot \epsilon$  が成立する．

例： $(\lambda x y.x)$   $(\lambda y.x)$   $z$  のラベル付き木



## 出現位置の集合

**Definition 3 (出現位置の集合)**  $\forall M \in \Lambda$  に対して, 出現位置の集合  $\mathcal{O}(M)$  を次のように帰納的に定義する.

1.  $M = x$  のとき

$$\mathcal{O}(M) = \{\epsilon\}$$

2.  $M = M_1 M_2$  のとき

$$\mathcal{O}(M) = \{\epsilon\} \cup \{i \cdot u \mid u \in \mathcal{O}(M_i), i = 1, 2\}$$

3.  $M = \lambda x.M_1$  のとき

$$\mathcal{O}(M) = \{\epsilon\} \cup \{1 \cdot u \mid u \in \mathcal{O}(M_1)\}$$



$M/u$ : 出現位置  $u \in \mathcal{O}(M)$  における部分項を表わす .

$$M/\epsilon = M$$

$$(M_1 M_2)/i \cdot u = M_i/u, \quad \{ i=1,2 \}$$

$$(\lambda x.M_1)/1 \cdot u = M_1/u$$

位置上の順序  $u \leq v$ :  $v$  を根とする木が  $u$  を根とする木に含まれている .

$$u \leq v \stackrel{def}{=} \exists w, v = u \cdot w$$

## 自由変数・束縛変数

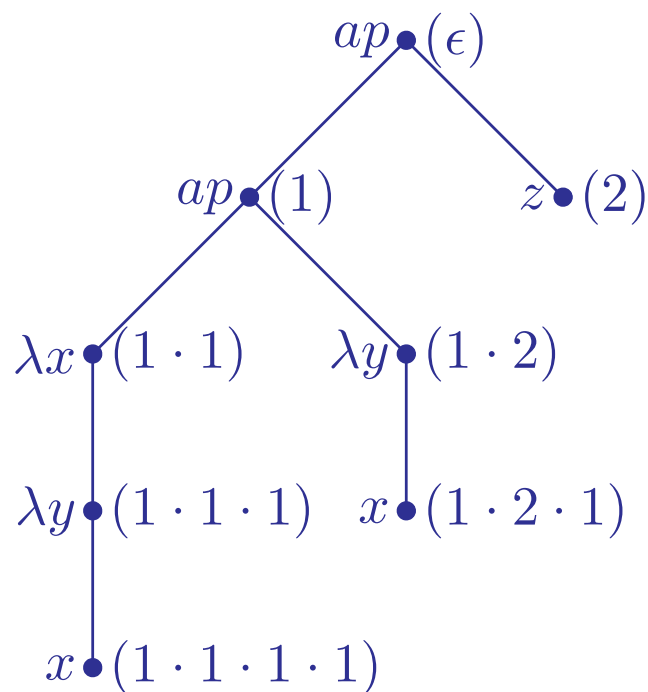
**Definition 4 (自由変数)** 任意の項  $M$  に含まれる変数  $x$  , すなわち ,  
 $\exists u \in \mathcal{O}(M), M/u = x$  , 次の条件を満たすとき ,  $M$  において自由であるという .

$$\forall v \in \mathcal{O}(M), [v < u \Rightarrow M/v \not\equiv \lambda x.(M/v \cdot 1)]$$

**Definition 5 (束縛変数)** 任意の項  $M$  に含まれる変数  $x$  , すなわち ,  
 $\exists u \in \mathcal{O}(M), M/u = x$  , 次の条件を満たすとき ,  $M$  において束縛であるという .

$$\exists v \in \mathcal{O}(M), [v < u \wedge M/v \equiv \lambda x.(M/v \cdot 1)]$$

問題:  $(\lambda x y.x) (\lambda y.x) z$  中のすべての自由変数と束縛変数を求めよ.



問題: 項  $M$  に含まれるすべての自由変数の集合を求める関数  $FV(M)$  を定義せよ.

## 束縛変数の名前変更

$\lambda x.M$  を  $f(x) = M$  となる関数を表現するものと考えられる。

$f(x) = x + 5$  も,  $f(y) = y + 5$  も定義している関数  $f$  は同じものである。  
これに従えば,

$$\lambda x.M \equiv \lambda y.M'$$

ただし,  $M'$  は  $M$  の自由変数  $x$  をすべて  $y$  で置き換えて得られた 項とする。

$$M' \equiv M[x := y]$$

例 :

$$\begin{aligned}\lambda x.x &\equiv \lambda y.y \\ \lambda x.plus\ x\ x &\equiv \lambda y.plus\ y\ y\end{aligned}$$

## 自由変数の代入

$M[x := N]$ :  $M$  に含まれるすべての  $M$  における自由変数  $x$  に  $N$  を代入して得られる項を表わす .

$$\begin{aligned}
 y[x := N] &\equiv \begin{cases} N & \text{if } x \equiv y \\ y & \text{otherwise} \end{cases} \\
 (M_1 M_2)[x := N] &\equiv M_1[x := N] M_2[x := N] \\
 (\lambda y.M_1)[x := N] &\equiv \lambda y.M_1[x := N] \quad \text{if } y \neq x \wedge y \notin \mathcal{FV}(N) \\
 &\quad \text{(by renaming)}
 \end{aligned}$$

注意 : 代入によって ,  $N$  の自由変数が  $M$  の部分項で束縛されることがない .

問題 :  $(\lambda y.x y)[x := \lambda w.y w]$  を求めよ .

## 代入補題

**Lemma 1 (代入補題)**  $\forall L, M, N \in \Lambda$  に対して,  $x \neq y$  かつ  $x \notin \mathcal{FV}(L)$  のとき,

$$M[x := N][y := L] \equiv M[y := L][x := N[y := L]]$$

**問題:** 項の構造に関する帰納法で代入補題を証明せよ.

証明 :  $M$  の構造に関する帰納法で証明する .

- $M = x$ .

$$\begin{aligned} LHS &= x[x := N][y := L] \\ &= N[y := L] \end{aligned}$$

$$\begin{aligned} RHS &= x[y := L][x := N[y := L]] \\ &= x[x := N[y := L]] \\ &= N[y := L] \end{aligned}$$

- $M = y.$

$$\begin{aligned} LHS &= y[x := N][y := L] \\ &= y[y := L] \\ &= L \end{aligned}$$

$$\begin{aligned} RHS &= y[y := L][x := N[y := L]] \\ &= L[x := N[y := L]] \quad \{ x \notin \mathcal{FV}(L) \} \\ &= L \end{aligned}$$

- $M = z, z \neq x \wedge z \neq y.$

$$\begin{aligned} LHS &= z[x := N][y := L] \\ &= z[y := L] \\ &= z \end{aligned}$$

$$\begin{aligned} RHS &= z[y := L][x := N[y := L]] \\ &= z[x := N[y := L]] \\ &= z \end{aligned}$$

- $M = (M_1 \ M_2)$ .

$$\begin{aligned} LHS &= (M_1 \ M_2)[x := N][y := L] \\ &= (M_1[x := N] \ M_2[x := N])[y := L] \\ &= M_1[x := N][y := L] \ M_2[x := N][y := L] \\ &= \{ \text{inductive hypothesis} \} \\ &\quad M_1[y := L][x := N[y := L]] \ M_2[y := L][x := N[y := L]] \\ &= (M_1[y := L] \ M_2[y := L])[x := N[y := L]] \\ &= (M_1 \ M_2)[y := L][x := N[y := L]] \\ &= RHS \end{aligned}$$

- $M = \lambda z.M', z \neq x \wedge z \neq y.$

$$\begin{aligned} LHS &= (\lambda z.M')[x := N][y := L] \\ &= (\lambda z.M'[x := N])[y := L] \\ &= \lambda z.M'[x := N][y := L] \\ &= \{ \text{inductive hypothesis} \} \\ &\quad \lambda z.M'[y := L][x := N[y := L]] \\ &= (\lambda z.M'[y := L])[x := N[y := L]] \\ &= (\lambda z.M')[y := L][x := N[y := L]] \\ &= RHS \end{aligned}$$

## コンビネータ

これからの議論で重要な役割を果たす特別な 項 .

**Definition 6 (コンビネータ)** 自由変数を含まない 項をコンビネータ (combinator) という . 重要なコンビネータには以下のものがある .

$$\begin{aligned} \mathbf{I} &\equiv \lambda x . x \\ \mathbf{K} &\equiv \lambda x y . x \\ \mathbf{F} &\equiv \lambda x y . y \\ \mathbf{S} &\equiv \lambda x y z . x z (y z) \\ \mathbf{B} &\equiv \lambda x y z . x (y z) \\ \mathbf{C} &\equiv \lambda x y z . x z y \\ \mathbf{Q} &\equiv (\lambda x . x x) (\lambda x . x x) \end{aligned}$$

## $\beta$ 簡約

項の集合  $\Lambda$  の上の二項関係を厳密に定義する .

### Definition 7 ( $\beta$ 簡約)

1.  $\Lambda$  上の二項関係  $\beta$  を次のように定義する .

$$\beta = \{ \langle (\lambda x.P)Q, P[x := Q] \rangle \mid P, Q \in \Lambda \}$$

2. 関係  $\beta$  より誘導される 1 ステップ  $\beta$  簡約  $\rightarrow_\beta$  を次の条件を満たす最小の関係と定義する .

(a)  $\langle M, N \rangle \in \beta \Rightarrow M \rightarrow_\beta N$

(b)  $M \rightarrow_\beta N \Rightarrow \forall L \in \Lambda, \forall x \in \mathcal{V},$

- $LM \rightarrow_\beta LN$
- $ML \rightarrow_\beta NL$
- $\lambda x.M \rightarrow_\beta \lambda x.N.$

例:

$$\begin{aligned} \mathbf{II} &\equiv (\lambda x.x) I \\ &\rightarrow_{\beta} \mathbf{I} \end{aligned}$$

$$\begin{aligned} \mathbf{KI(II)} &\equiv (\lambda x y.x)\mathbf{I(II)} \\ &\rightarrow_{\beta} (\lambda y.\mathbf{I})(\mathbf{II}) \\ &\rightarrow_{\beta} \mathbf{I} \end{aligned}$$

問題 :  $\mathbf{SKK}$  の  $\beta$  簡約経路を示せ .

**Lemma 2 (両立性 (compatibility))**

$$\forall u \in \mathcal{O}(M), N_1 \rightarrow_{\beta} N_2 \Rightarrow M[u \leftarrow N_1] \rightarrow_{\beta} M[u \leftarrow N_2]$$

$\twoheadrightarrow_{\beta}$ :  $\rightarrow_{\beta}$  の 0 回以上の繰り返しを表わす .

## 同値関係

次の条件を満たす二項関係  $\mathbf{R}$  を同値関係と呼ぶ。

(i)  $a \mathbf{R} a$

(ii)  $a \mathbf{R} b \Rightarrow b \mathbf{R} a$

(iii)  $a \mathbf{R} b, b \mathbf{R} c \Rightarrow a \mathbf{R} c$

**Definition 8 (関係  $=_{\beta}$ )**

$=_{\beta}$  を次の条件を満たす  $\Lambda$  上の最小の二項関係と定義する。任意の項  $L, M, N$  に対して,

1.  $M \rightarrow_{\beta} N \Rightarrow M =_{\beta} N$
2.  $M =_{\beta} N \Rightarrow N =_{\beta} M$
3.  $M =_{\beta} N$  かつ  $N =_{\beta} L \Rightarrow M =_{\beta} L$

**問題：**  $=_{\beta}$  が同値関係であることを証明せよ。

## 正規形

**Definition 9** ( $\beta$  可簡約項 ( $\beta$ -redex))

$P, Q$  を任意の項とする.  $(\lambda x. P) Q$  なる形の項を可簡約項 ( $\beta$ -redex) という.

例:  $(\lambda x. x y) z w$

**Definition 10** ( $\beta$  正規形)

部分項に  $\beta$  可簡約項を含まない項を  $\beta$  正規形という.

例:  $z y w$

**Definition 11 (正規形を持つ)**

$M =_{\beta} N$  かつ  $N$  が  $\beta$  正規形であるとき、 $M$  は  $\beta$  正規形を持つという。

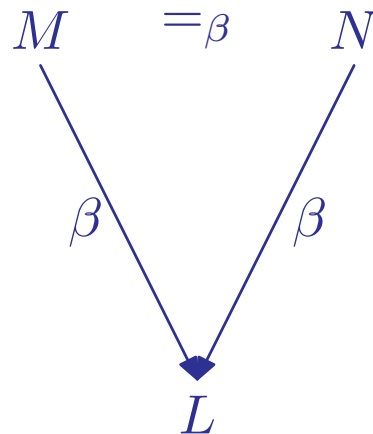
**問題:** 次の項は  $\beta$  正規形を持つか？

- $(\lambda x. x y) z w$
- $\Omega \equiv (\lambda x. x x) (\lambda x. x x)$
- **K I  $\Omega$**

## Church-Rosser 定理

Theorem 3 (Church-Rosser 定理, CR 性)

$$\forall M, N \in \Lambda. [M =_{\beta} N \Rightarrow \exists L \in \Lambda. [M \rightarrow_{\beta} L \wedge N \rightarrow_{\beta} L]]$$



**Corollary 4**  $\beta$  正規形が唯一である .

証明 : 背理法で証明する . 二つの正規形  $N_1, N_2$  ( $N_1 \neq N_2$ ) があるとする .

$N_1 =_{\beta} N_2$  と CR 性により ,

$$\exists L \in \Lambda. [N_1 \twoheadrightarrow_{\beta} L \wedge N_2 \twoheadrightarrow_{\beta} L]$$

となる .  $N_1$  と  $N_2$  が正規形であるため , 矛盾 .

## 合流性 (Congruence)

### Definition 12 (合流性)

$$\begin{aligned} &\forall M, M_1, M_2 \in \Lambda, \\ &\quad M \twoheadrightarrow_{\beta} M_1 \wedge M \twoheadrightarrow_{\beta} M_2 \\ &\quad \Rightarrow \exists M_3 \in \Lambda, M_1 \twoheadrightarrow_{\beta} M_3 \wedge M_2 \twoheadrightarrow_{\beta} M_3 \end{aligned}$$

**Theorem 5**

$\rightarrow_\beta$  が CR 性をもつ  $\Leftrightarrow \rightarrow_\beta$  が合流性をもつ .

[証明]

( $\Rightarrow$ ) :  $\forall M, M_1, M_2 \in \Lambda, M \twoheadrightarrow_\beta M_1 \wedge M \twoheadrightarrow_\beta M_2$  とする .

$=_\beta$  の定義より ,  $M =_\beta M_1 \wedge M =_\beta M_2$  である .

従って ,  $M_1 =_\beta M_2$  である .

CR 性より ,  $\exists M_3 \in \Lambda, M_1 \twoheadrightarrow_\beta M_3 \wedge M_2 \twoheadrightarrow_\beta M_3$ .

( $\Leftarrow$ ) :  $M =_\beta N$  の定義に沿った帰納法による .

1.  $M \twoheadrightarrow_\beta N \Rightarrow M =_\beta N$  の場合 :?
2.  $N =_\beta M \Rightarrow M =_\beta N$  の場合 :?
3.  $M =_\beta N'$  かつ  $N' =_\beta N \Rightarrow M =_\beta N$  の場合 :?

## 簡約の方法と戦略

どの位置にある簡約項を簡約するかによって，次の簡約方法が考えられる．

- 最左簡約：可簡約項の中で最も左にある可簡約項から簡約する方法．
- 内部簡約：可簡約項の中で最も中にある可簡約項から簡約する方法．

## 最左簡約例

$$\begin{aligned} & x \left( \underline{(\lambda u v w. u w (v w)) (I x) (I (I I)) z} \right) \\ = & x \left( \underline{(\lambda v w. (I x) w (v w)) (I (I I)) z} \right) \\ = & x \left( \underline{(\lambda w. (I x) w ((I (I I)) w)) z} \right) \\ = & x \left( \underline{(I x) z ((I (I I)) z)} \right) \\ = & x \left( x z \left( \underline{(I (I I)) z} \right) \right) \\ = & x \left( x z \left( \underline{(I I) z} \right) \right) \\ = & x \left( x z \left( \underline{I z} \right) \right) \\ = & x \left( x z z \right) \end{aligned}$$

## 正規化簡約戦略

### Definition 13 (正規化戦略)

$\beta$  正規形をもつ任意の項  $M$  に対して, 有限個の簡約ステップで正規形を求めることができる簡約戦略を正規化簡約戦略という.

Theorem 6 最左簡約戦略は正規化戦略である.

## 項による計算のコーディング

- ブール計算

$$\mathit{true} \equiv \lambda t f. t$$

$$\mathit{false} \equiv \lambda t f. f$$

$$\mathit{test} \equiv \lambda l m n. l m n$$

問題：次の項の正規形を求めよ．

$$\mathit{and} \equiv \lambda b c. \mathit{test} b c \mathit{false}$$

$$\mathit{or} \equiv \lambda b c. \mathit{test} b \mathit{true} c$$

問題： $\mathit{and} \mathit{true} \mathit{true} =_{\beta} \mathit{true}$  を証明せよ．

- 組

$$\mathit{pair} \equiv \lambda f s b. b f s$$

$$\mathit{fst} \equiv \lambda p. p \mathit{true}$$

$$\mathit{snd} \equiv \lambda p. p \mathit{false}$$

問題 :  $\mathit{fst} (\mathit{pair} v w) =_{\beta} v$  を証明せよ .

- Church numbers:

$$0 \quad \equiv \quad \lambda s z. z$$

$$1 \quad \equiv \quad \lambda s z. s z$$

$$n \quad \equiv \quad \lambda s z. s (s \dots (s z) \dots)$$

$$succ \quad \equiv \quad \lambda n s z. s (n s z)$$

$$plus \quad \equiv \quad \lambda m n s z. m s (n s z)$$

$$times \quad \equiv \quad \lambda m n. m (plus n) 0$$

$$exp \quad \equiv \quad \lambda m n. n m$$

## レポート課題

次の演習問題を解いて，5月12日（月）までに提出してください．提出先は胡のポストです．氏名と学生証番号を記入し忘れないでください．

問1  $M[x := N][x := L] \equiv M[x := N[x := L]]$  を証明せよ．

問2  $(\lambda x y. (\lambda l w. w w) x y) (\mathbf{S} a) (\mathbf{K} \mathbf{I})$  を最左簡約戦略で  $\beta$  正規形までの簡約を示せ．

問3  $\text{snd} (\text{pair } v w) =_{\beta} w$  を証明せよ．

問4  $\text{fix } f \equiv (\lambda x. f(x x))(\lambda x. f(x x))$  とする． $\text{fix } f =_{\beta} f(\text{fix } f)$  を証明せよ．