輪講 — 論理と計算のしくみ 5.3 型付き λ 計算 (前半)

伊奈 林太郎 (id:tarao)

京都大学 大学院情報学研究科

2012-01-26

参考文献

- 萩谷, 西崎.
  論理と計算のしくみ.
  岩波書店, 2007.
- J. C. Mitchell.
  Foundations for Programming Languages.
  MIT Press, 1996.
- B. C. Pierce.
  Types and Programming Languages.
  MIT Press, 2002.

型理論のアイディア

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

- x は関数のはず

型理論のアイディア

$$(\lambda x^{A \to B}.xx)(\lambda x.xx)$$

- x は関数のはず
  数学のように $A \to B$ の関数だと思ってみる

型理論のアイディア

$$(\lambda x^{A \to B}.xx)(\lambda x.xx)$$

- x は関数のはず
  数学のように $A \to B$ の関数だと思ってみる
- 受け取るのは集合 A の要素

型理論のアイディア

$$(\lambda x^{A \to B}.x\textcolor{red}{x})(\lambda x.xx)$$

- x は関数のはず
  数学のように $A \to B$ の関数だと思ってみる
- 受け取るのは集合 A の要素
- 渡しているのは関数 $A \to B$ ($A \times B$ の部分集合)

型理論のアイディア

$$(\lambda x^{A\to B}.xx)(\lambda x.xx)$$

- x は関数のはず
  数学のように $A \to B$ の関数だと思ってみる
- 受け取るのは集合 A の要素
- 渡しているのは関数 $A \to B$ ($A \times B$ の部分集合)
- $A \to B \in A$ なの? おかしくね?

型理論のアイディア

$$(\lambda x^{A \to B}.xx)(\lambda x.xx)$$

- x は関数のはず
  数学のように $A \to B$ の関数だと思ってみる
- 受け取るのは集合 A の要素
- 渡しているのは関数 $A \to B$ ($A \times B$ の部分集合)
- $A \to B \in A$ なの? おかしくね?
  $\Rightarrow$ 実際おかしいから無限ループする

型理論のアイディア

$$(\lambda x^{A \to B}.xx)(\lambda x.xx)$$

- x は関数のはず
  数学のように $A \to B$ の関数だと思ってみる
- 受け取るのは集合 A の要素
- 渡しているのは関数 $A \to B$ ($A \times B$ の部分集合)
- $A \to B \in A$ なの? おかしくね?
  $\Rightarrow$ 実際おかしいから無限ループする

おかしいものを排除すれば
無限ループしないのでは?

型理論 [1/3] は抽象的な枠組

型を付ける

- 式の使われ方に応じて種類分けする
- この種類のことを型と呼ぶ

型の整合性

- 型の付け方は整合していないといけない
- 同じ式を異なる型として使ってはダメ等

整合性による恩恵

- 使われ方が整合しているので
  おかしなことが起きない
- ということを数学的に証明できる

型理論 [2/3] の具体例

何を型だと思うか

- 関数, 変数の別
- メモリ, プロセス, ロックなどの情報
- セキュリティ上のアクセスレベル
- エスケープ, エンコードされているかどうか

防げるおかしなこと

- 無限ループ, 関数以外の適用
- メモリリーク, デッドロック
- 情報漏洩
- XSS, 文字化け

型理論 [3/3] は魔法ではない

ただし制限もある

- 単純型付 λ 計算は再帰関数を一切書けない
  (ループ禁止だから無限ループしないのは当然)

制限を緩めるには

- 複雑にして頑張る
  - Gödel の System T, Coq
  - 部分型, 多相型, 依存型
- プログラムの一部にだけ性質を保証する
  - OCaml の `let rec`
  - Gradual Typing

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

型

基本型 (α, β, γ)

- プリミティブな型 (`int` とか)
- どんなものがあるかは予め定めておく

単純型 (A, B, C)

$A ::= \alpha \mid A \to A$

単純型に含めることもある

$A ::= \alpha \mid A \to A \mid A \times A \mid A + A$

$\to$ 右結合

$\times, +$ 左結合

型付け [1/2]

各変数の型は固定

x^A と書く

型判断

$\vdash M : A$ 「M の型は A」

型付け規則

$\vdash x^A : A$

$$\frac{\vdash M : B}{\vdash \lambda x^A.M : A \to B} \qquad \frac{\vdash M : A \to B \qquad \vdash N : A}{\vdash MN : B}$$

$$\frac{\vdash M : A \qquad \vdash N : B}{\vdash (M, N) : A \times B} \qquad \frac{\vdash L : A \times B}{\pi_1(L) : A} \qquad \frac{\vdash L : A \times B}{\pi_2(L) : B}$$

型付け [2/2] — 型の整合性

M は型が付く (M is well-typed)

- 型付け規則で $\vdash M : A$ が導ける

型が付かない例

$\lambda x^A . x^A x^A$

型付けの一意性

- 各変数の型が固定なら型付けは一意

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

型保存性 — 示したいこと

- 最終的には「型が付けば○○」と言いたい
- 「○○」は正規化等 $\to_\beta$ に関すること
- $\to_\beta$ の前後で型の付き方は変わらないでほしい

Theorem (主部簡約定理 (subject reduction))

$\vdash M : A$ かつ $M \to_\beta N$ ならば $\vdash N : A$

Theorem (関係 R で一般化版)

$\vdash M : A$ かつ $M \to_\beta N$ ならば, $\vdash N : B$ かつ BRA.

- 上は R が $=$ の場合の話

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

代入補題 [1/2]

Lemma (代入補題)

$\vdash M : A$ かつ x^B かつ $\vdash N : B$ ならば
$\vdash M[x := N] : A$.

代入補題 [2/2] — 証明 [1/3]

証明: M の構造に関する帰納法による

- $M = y$ のとき
  - $y = x$ の場合
    1. 型付け規則と $y = x$ から $\vdash y^B : B$
    2. $\vdash M : A$ なので $B = A$
    3. $M[x := N] = N$
    4. 補題の前提条件と $B = A$ より $\vdash N : A$
  - $y \neq x$ の場合
    1. 型付け規則から y^A のはず
    2. $M[x := N] = y$
    3. 変数の型付け規則を使って $\vdash y^A : A$

代入補題 [2/2] — 証明 [2/3]

証明: M の構造に関する帰納法による

- $M = M_1 M_2$ のとき
  1. 型付け規則から $\vdash M_1 : C \to A$ かつ $\vdash M_2 : C$
  2. IH より $\vdash M_1[x := N] : C \to A$
  3. IH より $\vdash M_2[x := N] : C$
  4. $M_1[x := N]M_2[x := N] = (M_1 M_2)[x := N]$
  5. 適用の型付け規則を使って
     $\vdash (M_1 M_2)[x := N] : A$

代入補題 [2/2] — 証明 [3/3]

証明: M の構造に関する帰納法による

- $M = \lambda y^{A_1}.L$ のとき
  1. 型付け規則から $A = A_1 \to A_2$ かつ $\vdash L : A_2$
  2. $\lambda z^{A_1}.L[y := z] =_\alpha \lambda y^{A_1}.L$ とできるので $y \neq x$ かつ y は N に自由に出現しないとしても一般性を失わない
  3. $\lambda y^{A_1}.L[x := N] = (\lambda y^{A_1}.L)[x := N]$
  4. IH より $\vdash L[x := N] : A_2$
  5. 抽象の型付け規則を使って $\vdash (\lambda y^{A_1}.L)[x := N] : A_1 \to A_2$

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

主部簡約定理 [1/2]

Theorem (主部簡約定理 (subject reduction))

$\vdash M : A$ かつ $M \to_\beta N$ ならば $\vdash N : A$

主部簡約定理 [2/2] — 証明 [1/2]

証明: $M \rightarrow_\beta N$ の導出に関する帰納法による

- **Beta のとき**
  1. $M = (\lambda x^B.M_1)M_2 \rightarrow_\beta M_1[x := M_2] = N$
  2. 型付け規則から $\vdash M_1 : A$ かつ $\vdash M_2 : B$
  3. 代入補題より $\vdash M_1[x := M_2] : A$
- **Lam のとき**
  1. $M = \lambda x^B.L \rightarrow_\beta \lambda x^B.L' = N$ かつ $L \rightarrow_\beta L'$
  2. 型付け規則から $A = B \rightarrow C$ かつ $\vdash L : C$
  3. IH より $\vdash L' : C$
  4. 抽象の型付け規則を使って $\vdash \lambda x^B.L' : B \rightarrow C$

主部簡約定理 [2/2] — 証明 [2/2]

証明: $M \to_\beta N$ の導出に関する帰納法による

- **AppL のとき**
  1. $M = M_1 M_2 \to_\beta M_1' M_2 = N$ かつ $M_1 \to_\beta M_1'$
  2. 型付け規則から $\vdash M_1 : B \to A$ かつ $\vdash M_2 : B$
  3. IH より $\vdash M_1' : B \to A$
  4. 適用の型付け規則を使って $\vdash M_1' M_2 : A$
- **AppR のとき**
  1. $M = M_1 M_2 \to_\beta M_1 M_2' = N$ かつ $M_2 \to_\beta M_2'$
  2. 型付け規則から $\vdash M_1 : B \to A$ かつ $\vdash M_2 : B$
  3. IH より $\vdash M_2' : B$
  4. 適用の型付け規則を使って $\vdash M_1 M_2' : A$

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

やりたいこと [1/4]

すべての無限ループを
生まれる前に消し去りたい

やりたいこと [2/4]

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

- 「型が付いたら無限ループしない」と言いたい
  - 上の例に限れば型が付かないことは既に見た
  - 止まらない項すべてに関して示すには?

やりたいこと [2/4]

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

- 「型が付いたら無限ループしない」と言いたい
  - 上の例に限れば型が付かないことは既に見た
  - 止まらない項すべてに関して示すには?
- そもそも「無限ループ」って何?
  - 無限簡約列があること
  - 評価戦略によってあったりなかったり

やりたいこと [3/4] — 定義 [1/2]

β 正規形

$M \in \mathrm{NF}_\beta \iff M$ は β 簡約で正規形

β 正規形への有限簡約

$$M \Downarrow_\beta N \iff$$
$$M = M_0 \to_\beta M_1 \to_\beta \cdots \to_\beta M_n = N \in \mathrm{NF}_\beta$$

やりたいこと [3/4] — 定義 [2/2]

Definition (弱正規化可能)

型の付いた項 M に対して, ある N が存在して $M \Downarrow_\beta N$.

- 有限簡約列が少なくとも 1 つあるということ
- うまい評価戦略では止まるということ

Definition (強正規化可能 SN)

型の付いた項 M に対して, M から始まる無限簡約列 $M \to_\beta M_1 \to_\beta M_2 \to_\beta \cdots$ が存在しない.

- どんな評価戦略でも止まるということ

やりたいこと [4/4]

評価戦略を固定した場合の正規化可能性

- 簡約列は一通りしかない
- 弱正規化可能 $\Longleftrightarrow$ 強正規化可能

やりたいこと [4/4]

評価戦略を固定した場合の正規化可能性

- 簡約列は一通りしかない
- 弱正規化可能 $\Longleftrightarrow$ 強正規化可能

でもせっかくなので一般の場合で証明

勘所 [1/2]

帰納法で証明できる?

- M, N がともに SN のとき MN は SN?
  - $M = \lambda x.xx$ と $N = \lambda x.xx$ はともに SN
  - $\Omega = MN$ なので適用すると SN ではない
- M, N は型が付かないから大丈夫では?
  - 危険な項すべて型が付かないと言えれば OK
- 「危険な項は型が付かない」こそが強正規化性 $\Rightarrow$ 堂々巡り

勘所 [2/2]

問題点の分析

- $M = \lambda x.xx$ 自体はSNでも MN はSNでない
- 組み合わせると止まらない項は除外したい

組み合わせても止まる項

- M が “止まる項” である条件: MN も “止まる項”

証明方法

1. “止まる項” を項の形で見分ける
   - 制限された形の項はすべて SN
   - どんな項も制限された項に変換できる
   - 型付き項なら変換が SN を保存する
2. “止まる項” を帰納的に集める
   - 集めた項全体 $=$ 型付き項全体を示す

証明方法

1. "止まる項" を項の形で見分ける
   - 制限された形の項はすべて SN
   - どんな項も制限された項に変換できる
   - 型付き項なら変換が SN を保存する
2. "止まる項" を帰納的に集める
   - 集めた項全体 = 型付き項全体を示す

今回は 2 つ目の方法

証明の流れ

1. “止まる項” であることを表す述語を定義
2. “止まる項” の性質を証明
   - 変数は “止まる”
   - “止まる項” は $\rightarrow_\beta$ しても “止まる”
   - $\rightarrow_\beta$ して “止まる” なら元の項も “止まる”
     - ただし元の項の形を制限
3. すべての型付き項は “止まる”

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

論理関係 [1/6] — 定義

述語 R_A

$$\frac{\vdash M : \alpha \qquad M \text{ は SN}}{R_\alpha(M)}$$

$$\frac{\vdash M : A \to B \qquad M \text{ は SN} \qquad \forall N. R_A(N) \Rightarrow R_B(MN)}{R_{A\to B}(M)}$$

- R_A を満たす項は明らかに SN
- R_A を満たす項の集合と
  型 A の項全体の集合が一致すればよい
- cbv に固定するなら
  「M は SN」の代わりに「$M \Downarrow_{cbv} {}^{\exists}N$」

論理関係 [2/6] — 補題5.16 [1/2]

Lemma (5.16)

$0 \leq i \leq n. R_{A_i}(M_i)$ ならば
$R_A(x^{A_1 \to \cdots \to A_n \to A} M_1 \cdots M_n)$.

- 大雑把には $R_A(x^A)$ が成り立つということ
- “止まる項” の条件を反映した強い形

論理関係 [2/6] — 補題5.16 [2/2]

証明: 型 A の構造に関する帰納法

1. $R_{A_i}(M_i)$ より M_i は SN
2. $x^{A_1 \to \cdots \to A_n \to A} M_1 \cdots M_n$ は明らかに SN
3. $R_{A_i}(M_i)$ より $\vdash M_i : A_i$
4. 型付け規則より $\vdash x^{A_1 \to \cdots \to A_n \to \alpha} M_1 \cdots M_n : A$
5. - $A = \alpha$ のとき
     - ただちに $R_A(x^{A_1 \to \cdots \to A_n \to A} M_1 \cdots M_n)$
   - $A = B \to C$ のとき
     1. 任意の $R_B(N)$ なる N について
     2. IH より $R_C(x^{A_1 \to \cdots \to A_n \to B \to C} M_1 \cdots M_n N)$
     3. ゆえに $R_{B \to C}(x^{A_1 \to \cdots \to A_n \to B \to C} M_1 \cdots M_n)$

論理関係 [3/6] — 補題5.15 [1/3]

Lemma (5.15')

$M \to_\beta M'$ のとき $R_A(M)$ **ならば** $R_A(M')$

- $\Longleftarrow$ は成り立たない
  (反例: $M = (\lambda xy.y)(\lambda z.\Omega) \to_\beta \lambda y.y = M'$)
- $\Longleftarrow$ なしでもこの後の証明は可能
- 教科書は $\Longleftarrow$ も成り立つと書いてあるので誤り
  - $\to_{cbv}$ では $\vdash M : A$ を前提に加えれば OK [3]

論理関係 [3/6] — 補題5.15 [2/3]

証明: 型 A の構造に関する帰納法

- $A = \alpha$ のとき
  1. $R_\alpha(M)$ かつ $M \to_\beta M'$
  2. $R_\alpha(M)$ より $\vdash M : \alpha$ かつ M は SN
  3. M' は SN(さもないと M が SN でなくなる)
     - cbv では簡約の一意性をここで使う
  4. 主部簡約定理より $\vdash M' : \alpha$
  5. よって $R_\alpha(M')$

論理関係 [3/6] — 補題5.15 [3/3]

証明: 型 A の構造に関する帰納法

- $A = B \to C$ のとき
  1. $R_{B\to C}(M)$ かつ $M \to_\beta M'$
  2. N を $R_B(N)$ を満たす項とする
  3. $R_{B\to C}(M)$ より $R_C(MN)$
  4. $MN \to_\beta M'N$ なので IH より $R_B(M'N)$
  5. $R_B(M'N)$ なので $M'N$ は SN
  6. M' は SN(さもないと $M'N$ が SN でなくなる)
  7. 主部簡約定理より $\vdash M' : B \to C$
  8. よって $R_{B\to C}(M')$

論理関係 [4/6] — 補題5.17a [1/2]

Lemma (5.17a)

$\vdash M_0 : A_1 \to \cdots A_n \to \alpha$ かつ $R_B(L)$, $R_{A_i}(N_i)$ かつ $R_\alpha(M_0[x^B := L]N_1 \cdots N_n)$ ならば $R_\alpha((\lambda x^B.M_0)LN_1 \cdots N_n)$.

- 教科書には無い補題
- $(\lambda x^B.M_0)LN_1 \cdots N_n$ を $(\lambda x^B.M_0)L\overline{N}$ と略記

論理関係 [4/6] — 補題5.17a [2/2]

証明

1. $R_B(L)$, $R_{A_i}(N_i)$ より $\vdash L : B$, $\vdash N_i : A_i$
2. 型付け規則を使って $\vdash (\lambda x^B.M_0)L\overline{N} : \alpha$
3. $R_B(L)$, $R_{A_i}(N_i)$ より L, N_i は SN
4. $R_\alpha(M_0[x^B := L]\overline{N})$ より $M_0[x^B := L]\overline{N}$ は SN
5. M_0, $\lambda x^B.M_0$ も SN(さもないと矛盾)
6. $M_0 \to_\beta^* M_0'$, $L \to_\beta^* L'$, $N_i \to_\beta^* N_i'$ なる任意の M_0', L', N_i' について
   - $M_0'[x := L']\overline{N'}$ は SN
   - $(\lambda x^B.M_0)L\overline{N} \to_\beta^* M_0'[x := L']\overline{N'}$ は有限簡約
7. なので $(\lambda x^B M_0)L\overline{N}$ も SN
8. ゆえに $R_\alpha((\lambda x^B.M_0)L\overline{N})$

論理関係 [5/6] — 補題5.17b [1/3]

Lemma (5.17b)

$\vdash M_0 : A_1 \to \cdots A_n \to A$ かつ $R_B(L)$, $R_{A_i}(N_i)$ かつ $R_A(M_0[x^B := L]N_1 \cdots N_n)$ ならば $R_A((\lambda x^B.M_0)LN_1 \cdots N_n)$

- 教科書には無い補題
- 補題5.17aの型 α が A に一般化されたもの

論理関係 [5/6] — 補題 5.17b [2/3]

証明: 型 A に関する帰納法

- $A = \alpha$ のとき
  - 補題 5.17a より OK

論理関係 [5/6] — 補題 5.17b [3/3]

証明: 型 A に関する帰納法

- $A = C_1 \to C_2$ のとき
  1. M_1 を $R_{C_1}(M_1)$ を満たす任意の項とする
  2. $R_{C_1 \to C_2}(M_0[x := L]\overline{N})$ より
     - $\vdash M_0[x := L]\overline{N} : C_1 \to C_2$
     - $R_{C_2}(M_0[x := L]\overline{N}M_1)$
  3. IH より $R_{C_2}((\lambda x^B.M_0)L\overline{N}M_1)$
     - $\vdash (\lambda x^B.M_0)L\overline{N}M_1 : C_2$
     - $(\lambda x^B.M_0)L\overline{N}M_1$ は SN
  4. 主部簡約補題より $\vdash (\lambda x^B.M_0)L\overline{N} : C_1 \to C_2$
  5. $(\lambda x^B.M_0)L\overline{N}$ も SN

論理関係 [6/6] — 補題5.17 [1/4]

Lemma (5.17)

$\vdash M : A$ かつ $R_{A_1}(N_1), \ldots, R_{A_n}(N_n)$ ならば $R_A(M[x_1^{A_1} := N_1, \ldots, x_n^{A_n} := N_n])$.

- $x_1^{A_1} := N_1, \ldots, x_n^{A_n} := N_n$ を $\overline{x} := \overline{N}$ と書く

論理関係 [6/6] — 補題 5.17 [2/4]

項 M の構造に関する帰納法

- $M = x_i$ のとき
  1. $M[\overline{x} := \overline{N}] = N_i$
  2. $R_{A_i}(N_i)$ なので成立
- $M = y \neq x_i$ のとき
  1. $M[\overline{x} := \overline{N}] = y^A$
  2. 補題 5.16 より成立

論理関係 [6/6] — 補題5.17 [3/4]

項 M の構造に関する帰納法

- $M = M_1 M_2$ のとき
  1. 型付け規則から $\vdash M_1 : B \to A$ かつ $\vdash M_2 : B$
  2. IH より $R_{B\to A}(M_1[\overline{x} := \overline{N}])$ かつ $R_B(M_2[\overline{x} := \overline{N}])$
  3. $R_{B\to A}$ の定義より $R_A(M_1[\overline{x} := \overline{N}]M_2[\overline{x} := \overline{N}])$
  4. $M_1[\overline{x} := \overline{N}]M_2[\overline{x} := \overline{N}] = (M_1 M_2)[\overline{x} := \overline{N}]$
  5. よって $R_A((M_1 M_2)[\overline{x} := \overline{N}])$

論理関係 [6/6] — 補題5.17 [4/4]

項 M の構造に関する帰納法

- $M = \lambda x^B.M_0$ のとき
  1. 型付け規則から $\vdash M_0 : C$ かつ $A = B \to C$
  2. 代入補題より $\vdash M_0[\overline{x} := \overline{N}] : C$
  3. L を $R_B(L)$ なる任意の項とする
  4. IH より $R_C(M_0[\overline{x} := \overline{N}, x^B := L])$
  5. 補題5.17b より $R_C((\lambda x^B.M_0[\overline{x} := \overline{N}])L)$
  6. $M_0[\overline{x} := \overline{N}, x^B := L]$ は SN なので $\lambda x^B.M_0[\overline{x} := \overline{N}]$ も SN
  7. ゆえに $R_{B\to C}(\lambda x^B.M_0[\overline{x} := \overline{N}])$

単純型付き λ 計算

- 型の整合性 (a), (b)
  - 型
  - 型付け
- 性質 1 — 型保存性 (c)
  - 代入補題
  - 主部簡約定理
- 性質 2 — 正規化可能性 (d)
  - 論理関係
  - 強正規化可能性

強正規化可能性

Theorem (5.18)

正しく型付けされた λ 項は強正規化可能

証明

1. M を $\vdash M : A$ なる項とする
2. 補題 5.17 より $R_A(M)$ が成り立つ
3. ゆえに M は SN

おわり