数学基礎論特論
(コンピュータ特別講義 I)
講師 龍田 真

水上 達夫
tatsuo@yl.is.s.u-tokyo.ac.jp

平成 13 年 11 月 1 日

目 次

第1章　序論

型とは何か。　プログラミング言語のデータ型を一般化したもの。

（例）

- Pascal　`var x : integer`，　`y : real`，　`f(x:integer) : real`
- C　`int x`，　`double y`，　`double f(int x)`

関数 f は integer $\rightarrow$ real という型が作れる。これは integer を定義域とし、real を値域とする関数の型。

型理論　型に関する性質を論じるための形式的体系

型理論の意義

1. それ自体面白い
2. プログラミング言語の設計上役に立つ
   - 型の情報を使って、コンパイラによいコードを生成させる
   - 型の誤りをチェックするプログラムにより、プログラムの誤りをチェックできる
   - 型の情報は人間が見て読みやすく書きやすい
3. 強正規化性
4. カリーハワード同型対応

型理論と論理体系によい対応関係が存在する。

型理論	$\longleftrightarrow$	論理体系
型	$\longleftrightarrow$	論理式
項 (プログラム)	$\longleftrightarrow$	証明
簡約 (プログラムの実行)	$\longleftrightarrow$	証明の正規化

第2章　λ 計算の復習

λ 式をプログラムに選んで、その型を論じる。

λ 式の特徴

- 抽象的プログラミング言語
- 簡潔で論理的に扱いやすい
- 十分強力

2.1　λ 計算の定義

可算無限個の変数を表す記号が所与。$x, y, z, \ldots$ で表す。

Def (λ 式)

(1) 変数は λ 式

(2) x が変数、t が λ 式なら $(\lambda x.t)$ は λ 式

(3) a, b が λ 式なら (ab) は λ 式

(例)　$x, \quad \lambda x.x, \quad ((\lambda x.x)y), \quad (\lambda x.(\lambda y.x)), \cdots$

記法

(1) $\lambda x_1, x_2, \cdots x_n.t \equiv (\lambda x_1.(\lambda x_2. \cdots (\lambda x_n.t) \cdots))$

(2) $tt_1 \ldots t_n \equiv (\cdots((tt_1)t_2) \cdots t_n)$

ただし、(2) より (1) を優先して使用する。

$$\begin{aligned} \lambda x.yz &\equiv \lambda x.(yz) \\ &\not\equiv (\lambda x.y)z \end{aligned}$$

前出の例は次のようにして略記できる。

(例)　$x, \quad \lambda x.x, \quad (\lambda x.x)y, \quad \lambda xy.x, \cdots$

(意味)

$\lambda x.t$	$f(x)=t$ となる関数 f
ab	関数 a に引数 b を与えた計算結果 $a(b)$

Def (部分 λ 式)

λ 式 a の部分 b(a 自身も含む) が λ 式であるとき、b を a の部分 λ 式という。

(例)　$\lambda xyz.xz(yz)$ について

$\lambda xyz.xz(yz), \quad \lambda yz.xz(yz), \quad \lambda z.xz(yz), \quad xz(yz), \quad xz, \quad yz, \quad x, \quad y, \quad z$

Def (束縛変数と自由変数)

λ 式 a に変数 x が出現するとする。このとき、a の部分 λ 式 $\lambda x.b$ があって、この変数出現が $\lambda x.b$ 中であるとき、この変数出現は a 中束縛されているという。また、束縛されていないとき、自由であるという。

(例)　$(\lambda x.x^{\bullet}y^{\circ})x^{\circ}$

$^{\bullet}$ は束縛変数、$^{\circ}$ は自由変数

(類似概念)　$\displaystyle\sum_{x=1}^{10}(x^{\bullet}+y^{\circ})+x^{\circ} \quad \int_0^1(x^{\bullet}+y^{\circ})dx+x^{\circ}$

Def (束縛変数の名前換え)

変数 y が $\lambda x.a$ 中に出現しないとする。a 中の自由変数 x を全て y に置き換えた λ 式を a' とする。$\lambda x.a$ と $\lambda y.a'$ を構文上同じであるとみなす。このことを束縛変数の名前変えという。

(例)　$\lambda x.xz \equiv \lambda y.yz$

Def (代入)

λ 式 a, t 変数 x について λ 式 a 中の全ての自由変数 x に λ 式 t を代入した λ 式を $a[x := t]$ で表す。但し、λ 式 t 中の自由変数が λ 式 $a[x := t]$ 中で束縛されていないときだけ代入ができるものとする。これを代入条件という。

(例)

$$\begin{aligned}((\lambda x.xy)x)[y := xx] &\equiv (\lambda z.z(xx))x \\ &\not\equiv (\lambda x.x(xx))x\end{aligned}$$

Def ($FV(t)$)

λ 式 t 中に自由に出現する変数全体を $FV(t)$ で表す。

$$\begin{aligned}FV(x) &= \{x\} \\ FV(\lambda x.t_1) &= FV(t_1) \setminus \{x\} \\ FV(t_1 t_2) &= FV(t_1) \cup FV(t_2)\end{aligned}$$

Def ($a[x_1 := t_1, \cdots, x_n := t_n],\ n \geq 1$)

$a[x_1 := t_1, \cdots, x_n := t_n]$ は λ 式 a の全ての自由変数 x_i に t_i を代入した λ 式 ($0 \leq i \leq n$)。但し、代入条件が満たされているものとする。

2.2　簡約

$\to_\beta$ を次のように定める。

(i) $a_1 \to_\beta a_2$ なら、$\lambda x.a_1 \to_\beta \lambda x.a_2$

(ii) $a_1 \to_\beta a_2$ なら、$a_1 b \to_\beta a_2 b$

(iii) $a_1 \to_\beta a_2$ なら、$ba_1 \to_\beta ba_2$

$(\lambda x.t)$ を λ 抽象、(ab) を λ 適用といい、$a \to_\beta b$ のとき、a が b に 1 ステップ β-簡約されるという。(1-Step β -reduction) また、$(\lambda x.a)b$ の形の λ 式を β-リディックスという。(β-redex)

列 $a \equiv a_1, a_2, \cdots, a_n \equiv b$ ($n \leq 1$) があって、$a_1 \to_\beta a_2 \to_\beta \cdots \to_\beta a_n$ であるとき、$a \twoheadrightarrow_\beta b$ と表す。このことを a が b に β-簡約されるという。(β-reduction)

(例)　$(\lambda x.x)y \to_\beta y$

(意味)　$\to_\beta$ は計算が 1 ステップ進むことを意味する。

λ 式	(意味)
$\lambda x.x$	$f(x) = x$ となる関数 f (恒等関数)
$(\lambda x.x)y$	$\lambda x.x$ の表す関数 f に引数 y を与えた計算結果 $f(y)$

(Remark)　$t \to_\beta u \iff t$ 中の一つの β-redex $(\lambda x.a)b$ を $a[x := b]$ に置き換えて u が得られる

(例)　β-簡約は 1 通りとは限らない。
$(\lambda x.(\lambda y.y)x)z \to_\beta (\lambda x.x)z \to_\beta z$
$(\lambda x.(\lambda y.y)x)z \to_\beta (\lambda y.y)z \to_\beta z$

(例)　計算は必ず停止するとは限らない。(1) は無限ループに、(2) は発散する計算に相当する。

(1) $(\lambda x.xx)(\lambda x.xx) \to_\beta (\lambda x.xx)(\lambda x.xx) \to_\beta \cdots$

(2) $(\lambda x.xxx)(\lambda x.xxx) \to_\beta (\lambda x.xxx)(\lambda x.xxx)(\lambda x.xxx) \to_\beta \cdots$

Def (β-等号)

λ 式の列 $a \equiv a_1, a_2, \cdots, a_n \equiv b$ $(n \geq 1)$ があって、$a_i \to_\beta a_{i+1}$ または $a_{i+1} \to_\beta a_i$ $(1 \leq \forall i < n)$ であるとき、$a =_\beta b$ と書く。

Def (正規形)

$a \to_\beta b$ となる b がないとき、λ 式 a を β-正規形 (normal form) という。

(例)　次は正規形
$x, \quad \lambda x.x, \quad \lambda x.xx$

(Remark)

(1) t が β-正規形 $\iff t$ が β-redex を含まない

(2) t が β-正規形 $\iff t \equiv \lambda x_1 \cdots x_n.xt_1 \cdots t_m$
但し、x は変数, $n, m \geq 0$ $t_1, \cdots, t_m$ β-正規形

(3) β-正規形は計算結果である値を意味する。

2.3　λ 計算の諸性質

Th．(合流性)
$\begin{cases} a \twoheadrightarrow_\beta b \\ a \twoheadrightarrow_\beta c \end{cases}$ なら、λ 式 d があって、$\begin{cases} b \twoheadrightarrow_\beta d \\ c \twoheadrightarrow_\beta d \end{cases}$
合流性は計算結果が計算の道筋によらず、一通りに定まることを保証する。

Def (部分関数)

部分関数 $f : A \hookrightarrow B$ とは、ある $A_1 \subset A$ があって、関数 $f : A_1 \to B$ であること。

Def (λ 表現可能性)

自然数 n について、チャーチ数という λ 式 $\overline{n}$ を次のように定める。

$$\overline{n} = \lambda fx.\underbrace{f(f(\cdots(f(}_{n\text{ 個}}x)\cdots))$$

(例)
$$\overline{0} \equiv \lambda x.x$$
$$\overline{1} \equiv \lambda fx.f(x)$$
$$\overline{2} \equiv \lambda fx.f(f(x))$$

自然数 n を λ 式 $\overline{n}$ で表す。また、λ 式 F が部分関数 $f : N^n \hookrightarrow N$ $(n \geq 0)$ を表現するとは任意の自然数 $m_1, m_2, \cdots, m_n, m$ について

$$f(m_1, m_2, \cdots, m_n) = m \Longleftrightarrow F\overline{m_1}\,\overline{m_2}\cdots\overline{m_n} =_\beta \overline{m}$$

となること。また、部分関数 f が λ 表現可能であるとは、f を表現する λ 式があることである。

Th .　部分帰納関数は λ 表現可能

第 3 章　単純型理論 $\lambda_{\to}$

最も簡単な型理論を例として型理論の一般的な様子を説明する。$\lambda_{\to}$ では型をつけるプログラムは λ 式である。

3.1　$\lambda_{\to}$ の定義

　型理論は一般に項、型、判定、推論規則を定めることにより定義される。ここでは可算無限個の型変数 $\alpha, \beta, \gamma, \cdots$ と変数 $x, y, z, \cdots$ が所与されているとする。

Def ($\lambda_{\to}$ の型)

(1) 型変数は型

(2) A, B が型なら、$(A \to B)$ は型

(例)　次は型である。
$\alpha, \quad (\alpha \to \alpha), \quad (\alpha \to (\beta \to \alpha)),$
$((\alpha \to (\beta \to \alpha)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$

(記法)　次のような略記が可能である。$(n \geq 1)$
$A_1 \to A_2 \to \cdots A_n \to A \equiv (A_1 \to (A_2 \to \cdots (A_n \to A) \cdots))$

(例)　上記の例は次のように略記できる。
$\alpha, \quad \alpha \to \alpha, \quad \alpha \to \beta \to \alpha,$
$(\alpha \to \beta \to \alpha) \to (\alpha \to \beta) \to \alpha \to \gamma$

(意味)　$A \to B$ は型 A のデータを入力として得ると、型 B のデータを出力する関数の型を意味する。

Def ($\lambda_{\to}$ の項)

　$\lambda_{\to}$ の項は λ 式と定める。

Def ($\lambda_\to$ の判定)

$n \geq 0,\quad x_1, \cdots x_n$ は異なる変数、t が項、$A_1, \cdots A_n, A$ が型なら $\vdash$

$$x_1 : A_1, x_2 : A_2, \cdots, x_n : A_n \quad \vdash \quad t : A$$

は判定 (judgement) といい、$x_1 : A_1, x_2 : A_2, \cdots, x_n : A_n$ を文脈 (context) という。

(例)　次は判定である。

- $x : \alpha \quad \vdash \quad x : \alpha$
- $x : \alpha \to \beta \to \gamma,\ y : \alpha \to \beta,\ z : \alpha \quad \vdash \quad xz(yz) : \gamma$

(意味)　$x_1 : A_1, \cdots, x_n : A_n \quad \vdash \quad t : A$ は変数 x_i が型 A_i を持つなら $(1 \leq i \leq n)$、項 t は型 A を持つことを意味する。

(例)

- 変数 x が型 α を持つなら、項 x は型 α をもつ
- 変数 x が型 $\alpha \to \beta \to \gamma$ を持ち、変数 y が型 $\alpha \to \beta$ を持ち、変数 z が型 α を持つなら、項 $xz(yz)$ は型 γ を持つ

Def ($\lambda_\to$ の推論規則)

Γ は文脈、x は変数、f, a, t は項、A, B は型とする。また、Γ 中に $x : A$ が現れることを $(x : A) \in \Gamma$ と略記する。(1), (2), (3) をそれぞれ Assumption, Implication Introduction, Implication Elimination という。

(1) $\dfrac{}{\Gamma \quad \vdash \quad x : A}(ASS) \quad (x : A \in \Gamma)$

(2) $\dfrac{\Gamma, x : A \quad \vdash \quad t : B}{\Gamma \quad \vdash \quad \lambda x.t : A \to B}(\to I)$

(3) $\dfrac{\Gamma \quad \vdash \quad f : A \to B \qquad \Gamma \quad \vdash \quad a : A}{\Gamma \quad \vdash \quad fa : B}(\to E)$

(意味)

(ASS)　x_1 が型 A_1 を持ち、$\cdots$、x_n が型 A_n を持つなら、x_i が型 A_i を持つ

$(\to I)$　$\Gamma, x : A$ を仮定すると、t が B の型をもつことが証明できるなら、Γ を仮定すると、$\lambda x.t$ が $A \to B$ の型をもつことが証明できる。

$(\to E)$ Γ を仮定すると、f が $A \to B$ の型をもつことと、Γ を仮定すると、a が A の型をもつことが証明できるなら、Γ を仮定すると、fa は B の型をもつことが証明できる。

Def ($\lambda_{\to}$ における証明)

$\lambda_{\to}$ における $\Gamma \ \vdash \ t : A$ の証明とは次の図式のこと。

(1) $(x : A) \in \Gamma$ なら

$$\dfrac{}{\Gamma \ \vdash \ x : A}(ASS)$$ は $\Gamma \ \vdash \ x : A$ の証明

(2) P_1 が $\Gamma, x : A \ \vdash \ t : B$ の証明なら、

$$\dfrac{\begin{matrix}\vdots P_1 \\ \Gamma, x : A \ \vdash \ t : B\end{matrix}}{\Gamma \ \vdash \ \lambda x.t : A \to B}(\to I)$$ は $\Gamma \ \vdash \ \lambda x.t : A \to B$ の証明

(3) P_1 が $\Gamma \ \vdash \ f : A \to B$ の証明で、P_2 が $\Gamma \ \vdash \ a : A$ の証明なら、

$$\dfrac{\begin{matrix}\vdots P_1 \\ \Gamma \ \vdash \ f : A \to B\end{matrix} \quad \begin{matrix}\vdots P_2 \\ \Gamma \ \vdash \ a : A\end{matrix}}{\Gamma \ \vdash \ fa : B}(\to E)$$ は $\Gamma \ \vdash \ fa : B$ の証明

(例)

(1) $$\dfrac{\dfrac{}{x : A \ \vdash \ x : A}(ASS)}{\vdash \ \lambda x.x : A \to A}(\to I)$$ は $\vdash \ \lambda x.x : A \to A$ の証明

(2) $$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \ \vdash \ f : A \to A}(ASS) \quad \dfrac{\dfrac{}{\Gamma \ \vdash \ f : A \to A}(ASS) \ \dfrac{}{\Gamma \ \vdash \ x : A}(ASS)}{\Gamma \ \vdash \ fx : A}(\to E)}{f : A \to A, x : A \ \vdash \ f(fx) : A}(\to E)}{f : A \to A \ \vdash \ \lambda x.f(fx) : (A \to A)}(\to I)}{\vdash \ \lambda fx.f(fx) : (A \to A) \to A \to A}(\to I)$$

は $\vdash \ \lambda fx.f(fx) : (A \to A) \to A \to A$ の証明 $(\Gamma = f : A \to A, x : A)$

(記法)　証明中で $\dfrac{}{\Gamma \ \vdash \ x : A}(ASS)$ を $\Gamma \ \vdash \ x : A$ と略記する。また、推論規則名 $(\to I), (\to E)$ を省略してもよい。

(例)　(1) は次のようにして略記できる。

$$\dfrac{x : A \ \vdash \ x : A}{\vdash \ \lambda x.x : A \to A}$$

Def (証明可能)

$\Gamma \vdash t : A$ の証明があるとき、$\Gamma \vdash t : A$ は証明できるという。(”$\Gamma \vdash t : A$ が成り立つ” ”$\Gamma \vdash t : A$ である” などという)

Def (証明の高さ)

証明 P の高さ $|P|$ を次のように定める。

(1) $\dfrac{}{\Gamma \vdash x : A}(ASS)$ の高さは 0

(2) P_1 の高さが n なら

$$\dfrac{\begin{matrix}\vdots P_1 \\ \Gamma, x : A \vdash t : B\end{matrix}}{\Gamma \vdash \lambda x.t : A \to B}(\to I) \text{ の高さは } n+1$$

(3) P_1 の高さが n_1、P_2 の高さが n_2

$$\dfrac{\begin{matrix}\vdots P_1 \\ \Gamma \vdash f : A \to B\end{matrix} \quad \begin{matrix}\vdots P_2 \\ \Gamma \vdash a : A\end{matrix}}{\Gamma \vdash fa : B}(\to E) \text{ の高さは } \max(n_1, n_2) + 1$$

(例)　前の例の (1) の高さは 1、(2) の高さは 4

(Remark)　$|P|$ は証明 P の最大の段数

Prop. 3.1 $\Gamma \vdash t : A$ が証明でき、Γ' は Γ を並び替えたものである $\Longrightarrow$ $\Gamma \vdash t : A$ の証明と同じ高さである $\Gamma' \vdash t : A$ の証明がある。

Proof $\Gamma \vdash t : A$ の証明 P の高さに関する Ind で $|P| = |P'|$ なる $\Gamma \vdash t : A$ の証明 P' が存在することを証明する。最後に使用した推論規則で場合分けを行うと、

(1) (ASS)

P は $\dfrac{}{\Gamma \vdash x : A}(ASS)$　$x : A \in \Gamma$ で表せ、Γ' は Γ の並び換えであるから、$x : A \in \Gamma'$。よって、$\dfrac{}{\Gamma' \vdash x : A}(ASS)$ は $\Gamma' \vdash x : A$ の証明である。これを証明 P' とすればよい。$|P| = |P'| = 0$

(2) $(\to I)$

P は $\dfrac{\begin{matrix}\vdots P_1 \\ \Gamma, x : A \vdash t : B\end{matrix}}{\Gamma \vdash \lambda x.t : A \to B}(\to I)$ と表せ、$|P_1| = |P| - 1$。P_1 に対する IH(帰納法の仮定 Induction Hypothesis) より $\Gamma', x : A \vdash t : B$ の証明

P'_1 があって、$|P_1| = |P'_1|$。$\dfrac{\overset{\vdots P'_1}{\Gamma', x : A \ \vdash \ t : B}}{\Gamma' \ \vdash \ \lambda x.t : A \to B}(\to I)$ を P' とすればよい。$|P'| = |P'_1| + 1 = |P_1| + 1 = |P|$

(3) $(\to E)$

P は $\dfrac{\overset{\vdots P_1}{\Gamma \ \vdash \ f : A \to B} \quad \overset{\vdots P_2}{\Gamma \ \vdash \ a : A}}{\Gamma \ \vdash \ fa : B}(\to E)$ と表せ、証明の高さの定義より、$|P_1| < P, |P_2| < P$。

P_1 に対する IH より、$\Gamma' \ \vdash \ f : A \to B$ の証明 P'_1 があって、$|P_1| = |P'_1|$

P_2 に対する IH より、$\Gamma' \ \vdash \ a : A$ の証明 P'_2 があって、$|P_2| = |P'_2|$

$\dfrac{\overset{\vdots P'_1}{\Gamma' \ \vdash \ f : A \to B} \quad \overset{\vdots P'_2}{\Gamma' \ \vdash \ a : A}}{\Gamma' \ \vdash \ fa : B}(\to E)$ を P' とすればよい。$|P'| = \max(|P'_1|, |P'_2|) + 1 = \max(|P_1|, |P_2|) + 1 = |P|$

(Remark)　判定は文脈を並び換えても証明可能性や証明の高さは変わらない。

Prop. 3.2 $\Gamma, x : A \ \vdash \ t : B \quad x \notin FV(t) \Longrightarrow \Gamma \ \vdash \ t : B$

Proof　$\Gamma \ \vdash \ t : B$ であることを $\Gamma, x : A \ \vdash \ t : B$ の証明 P の高さに関する Ind で証明する。P の最後に使用する推論規則で場合分けを行うと、

(1) (ASS)

P は $\dfrac{}{\Gamma, x : A \ \vdash \ y : B}(ASS) \quad (y : B) \in (\Gamma, x : A)$ と表せる。$x \notin FV(y)$(すなわち $x \neq y$) より $(y : B) \in \Gamma$。よって、$\dfrac{}{\Gamma \ \vdash \ x : B}(ASS)$ は $\Gamma \ \vdash \ x : B$ の証明。

(2) $(\to I)$

P は $\dfrac{\overset{\vdots P_1}{\Gamma, x : A, y : B \ \vdash \ t : C}}{\Gamma, x : A \ \vdash \ \lambda y.t : B \to C}(\to I)$ と表せる。P_1 に Prop.3.1 を使用すると $\Gamma, y : B, x : A \ \vdash \ t : C$ の証明 P'_1 があって $|P'_1| = |P_1| = |P| - 1 < |P|$。

$\Gamma, x : A, y : B$ が文脈なので、$x \not\equiv y$。

また、仮定より $x \notin FV(\lambda y.t)$ であるから

$x \notin FV(\lambda y.t) \cup \{y\} = FV(t)$

よって、 P'_1 に対する IH の仮定が満たされ、$\Gamma, y : B \ \vdash \ t : C$ の証明

Q が存在する。$\dfrac{\begin{matrix}\vdots Q\\ \Gamma, y:B \ \vdash \ t:C\end{matrix}}{\Gamma \ \vdash \ \lambda y.t:B\to C}(\to I)$ は $\Gamma \ \vdash \ \lambda y.t:B\to C$ の証明である。

(3) $(\to E)$

P は $\dfrac{\begin{matrix}\vdots P_1\\ \Gamma, x:A \ \vdash \ f:B\to C\end{matrix} \quad \begin{matrix}\vdots P_2\\ \Gamma, x:A \ \vdash \ a:B\end{matrix}}{\Gamma, x:A \ \vdash \ fa:C}(\to E)$ と表せ、$|P_1|<|P|, |P_2|<|P|$ が成立する。

仮定より $x\notin FV(fa)=FV(f)\cup FV(a)$ であるので

$x\notin FV(f),\quad x\notin FV(a)$

P_1 に対する IH より、$\Gamma \ \vdash \ f:B\to C$ の証明 P_1' が存在する。また、P_2 に対する IH より、$\Gamma \ \vdash \ a:B$ の証明 P_2' が存在する。よって、

$\dfrac{\begin{matrix}\vdots P_1'\\ \Gamma \ \vdash \ f:B\to C\end{matrix} \quad \begin{matrix}\vdots P_2'\\ \Gamma \ \vdash \ a:B\end{matrix}}{\Gamma \ \vdash \ fa:C}(\to E)$ は $\Gamma \ \vdash \ fa:C$ の証明となる。

(Remark)　項 t に現れない変数 x に関する情報 $x:A$ は省いても t に型を付けることができる。

Def (証明の自由変数)

文脈と判定それぞれの自由変数全体を次のように定義する。

$$\begin{aligned} FV(x_1:A_1,\cdots,x_n:A_n) &= \{x_1,\cdots,x_n\} \\ FV(\Gamma \ \vdash \ t:A) &= FV(\Gamma)\cup FV(t) \end{aligned}$$

証明 P の自由変数全体は次のように定義される。

$$FV(P)=\cup FV(J)\quad (J \text{ は } P \text{ 中の判定})$$

Prop. 3.3

$$\begin{matrix}\vdots P\\ \Gamma \ \vdash \ t:A\end{matrix} \quad y\notin FV(P) \Longrightarrow \begin{matrix}\vdots P[x:=y]\\ \Gamma[x:=y] \ \vdash \ t[x:=y]:A\end{matrix}$$

Proof　証明 P の高さに関する Ind で証明する。P の最後に使用する推論規則で場合分けを行うと

(1) (ASS)

P は $\dfrac{}{\Gamma \ \vdash \ z:A}(ASS)\quad (z:A)\in\Gamma$ と表せる。$z\equiv x, z\not\equiv x$ のいずれの場合においても $\dfrac{}{\Gamma[x:=y] \ \vdash \ z[x:=y]:A}(ASS)$ が成立する。

(2) $(\to I)$

P は $\dfrac{\overset{\vdots\, P_1}{\Gamma, z : A \ \vdash \ t : B}}{\Gamma \ \vdash \ \lambda z.t : A \to B}(\to I)$ と表せる。IH for P_1 より

$\overset{\vdots\, P_1[x := y]}{(\Gamma, z : A)[x := y] \ \vdash \ t[x := y] : B}$ となる証明が存在する。

(i) $z \equiv x$ のとき

$$\dfrac{\overset{\vdots\, P_1[x := y]}{\Gamma, y : A \ \vdash \ t[x := y] : B}}{\Gamma \ \vdash \ \lambda y.t[x := y] : A \to B}(\to I)$$

となる証明が存在し、$x \notin FV(\Gamma)$ より

$$\begin{aligned} & \Gamma \ \vdash \ \lambda y.t[x := y] : A \to B \\ = \ & \Gamma \ \vdash \ \lambda x.t : A \to B \\ = \ & \Gamma[x := y] \ \vdash \ (\lambda x.t)[x := y] : A \to B \end{aligned}$$

よって、証明 $P[x := y]$ が成立する。

(ii) $z \not\equiv x$ のとき

$$\dfrac{\overset{\vdots\, P_1[x := y]}{\Gamma[x := y], z : A \ \vdash \ t[x := y] : B}}{\Gamma[x := y] \ \vdash \ \lambda z.t[x := y] : A \to B}(\to I)$$

となる証明が存在し、

$$\begin{aligned} & \Gamma[x := y] \ \vdash \ \lambda z.t[x := y] : A \to B \\ = \ & \Gamma[x := y] \ \vdash \ (\lambda z.t)[x := y] : A \to B \end{aligned}$$

よって、証明 $P[x := y]$ が成立する。

(3) $(\to E)$

$(\to I)$ と同様に証明できる。

Prop. 3.4 $\Gamma \ \vdash \ t : B, \quad x \notin FV(\Gamma) \Longrightarrow \Gamma, x : A \ \vdash \ t : B$

Proof $\Gamma \ \vdash \ t : B$ の証明 P の高さに関する Ind で示す。最後に使用した推論規則で場合分けを行うと、

(1) (ASS)

P は $\dfrac{}{\Gamma \ \vdash \ y : B}(ASS) \quad (y : B) \in \Gamma$ と表せる。

$(y : B) \in (\Gamma, x : A)$ より、次の証明が成立する。

$$\dfrac{}{\Gamma, x : A \ \vdash \ y : B}(ASS)$$

(2) $(\to I)$

P は $\dfrac{\overset{\vdots\, P_1}{\Gamma, y : B \ \vdash \ t : C}}{\Gamma \ \vdash \ \lambda y.t : B \to C}(\to I)$ と表せる。

(i) $x \equiv y$ のとき、Prop. 3.3 から y を別な唯一の変数名に変更し、$x \not\equiv y$ の場合の証明を使用すればよい。

(ii) $x \not\equiv y$ のとき、IH for P_1 より、$\Gamma, y : B, x : A \ \vdash \ t : C$ の証明 P_1' が存在し、Prop. 3.1 より、$\Gamma, x : A, y : B \ \vdash \ t : C$ の証明 P_1'' が存在する。よって、

$$\dfrac{\begin{array}{c}\vdots P_1'' \\ \Gamma, x : A, y : B \ \vdash \ t : C\end{array}}{\Gamma, x : A \ \vdash \ \lambda y.t : B \to C}(\to I)$$

は $\Gamma, x : A \ \vdash \ \lambda y.t : B \to C$ の証明である。

(3) $(\to E)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma \ \vdash \ f : B \to C\end{array} \quad \begin{array}{c}\vdots P_2 \\ \Gamma \ \vdash \ a : B\end{array}}{\Gamma \ \vdash \ fa : C}(\to E)$ と表せる。IH for P_1, IH for P_2 より、

$$\dfrac{\begin{array}{c}\vdots P_1' \\ \Gamma, x : A \ \vdash \ f : B \to C\end{array} \quad \begin{array}{c}\vdots P_2' \\ \Gamma, x : A \ \vdash \ a : B\end{array}}{\Gamma, x : A \ \vdash \ fa : C}(\to E)$$

は $\Gamma, x : A \ \vdash \ fa : C$ の証明である。

Prop. 3.5 $\Gamma \ \vdash \ t : A \Longrightarrow FV(t) \subset FV(\Gamma)$

Proof $\Gamma \ \vdash \ t : A$ の証明 P の高さの Inde で示す。P の最後に使用する推論規則で場合分けを行う。(証明省略)

3.2 Subjection Reduction (SR)

Th . SR $\Gamma \ \vdash \ t : A, \quad t \twoheadrightarrow_{\beta} u \Longrightarrow \Gamma \ \vdash \ u : A$

(Remark) 簡約により型は保存される。

Prop. 3.6 $\Gamma, x : A \ \vdash \ t : B, \quad \Gamma \ \vdash \ a : A \Longrightarrow \Gamma \ \vdash \ t[x := a] : B$

Proof $\Gamma, x : A \ \vdash \ t : B$ の証明 P の高さに関する Ind で示す。最後に使用した推論規則で場合分けを行うと、

(1) (ASS)

(i) $t \equiv x$ のとき

P は $\dfrac{}{\Gamma, x : A \ \vdash \ x : A}(ASS)$ で表され、$A = B, t[x := a] = a$ と仮定より、$\Gamma \ \vdash \ t[x := a] : B$ が成立する。

(ii) $t \not\equiv x$ のとき

P は $\dfrac{}{\Gamma, x : A \ \vdash \ t : B}(ASS) \quad (t : B) \in \Gamma$ で表される。$(t : B) \in \Gamma$ より、$\dfrac{}{\Gamma \ \vdash \ t : B}(ASS)$ が成立する。

(2) $(\to I)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma, x : A, y : B \ \vdash \ t : C\end{array}}{\Gamma, x : A \ \vdash \ \lambda y.t : B \to C}(\to I)$ と表せる。よって、Prop. 3.1 より、

$$\begin{array}{c}\vdots Q_1 \\ \Gamma, y : B, x : A \ \vdash \ t : C\end{array} \qquad (|Q_1| = |P_1| < |P|) \tag{A}$$

となる証明 Q_1 が存在する。また、P の $\Gamma, x : A, y : B$ は文脈より、$x \not\equiv y, y \notin FV(\Gamma)$。よって、$\Gamma \ \vdash \ a : A, y \notin FV(\Gamma)$ と Prop. 3.4 より、

$$\Gamma, y : B \ \vdash \ a : A \tag{B}$$

(A), (B) より、Q_1 の帰納法の仮定が成立し

$$\dfrac{\begin{array}{c}\vdots Q_1' \\ \Gamma, y : B \ \vdash \ t[x := a] : C\end{array}}{\Gamma \ \vdash \ \lambda y.t[x := a] : B \to C}(\to I) \tag{C}$$

また、Prop. 3.6 と $\Gamma \ \vdash \ a : A$ より、$FV(a) \subset FV(\Gamma)$ であり、$y \notin FV(\Gamma)$ より、$y \notin FV(a)$。よって、$x \not\equiv y, y \notin FV(a)$ と (C) より、

$$\dfrac{\begin{array}{c}\vdots Q_1' \\ \Gamma, y : B \ \vdash \ t[x := a] : C\end{array}}{\Gamma \ \vdash \ (\lambda y.t)[x := a] : B \to C}(\to I)$$

が成立する。

(3) $(\to E)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma, x : A \ \vdash \ f : B \to C\end{array} \quad \begin{array}{c}\vdots P_2 \\ \Gamma, x : A \ \vdash \ b : B\end{array}}{\Gamma, x : A \ \vdash \ fb : C}(\to E)$ と表せる。IH for P_1, IH for P_2 より、

$$\dfrac{\begin{array}{c}\vdots P_1' \\ \Gamma \ \vdash \ f[x := a] : B \to C\end{array} \quad \begin{array}{c}\vdots P_2' \\ \Gamma \ \vdash \ b[x := a] : B\end{array}}{\Gamma \ \vdash \ (f[x := a])(b[x := a]) : C} \tag{D}$$

$(f[x := a])(b[x := a]) = (fb)[x := a]$ と (D) より、

$$\dfrac{\begin{array}{c}\vdots P_1' \\ \Gamma \ \vdash \ f[x := a] : B \to C\end{array} \quad \begin{array}{c}\vdots P_2' \\ \Gamma \ \vdash \ b[x := a] : B\end{array}}{\Gamma \ \vdash \ (fb)[x := a] : C}$$

が成立する。

Proof of Th(SR)

$\Gamma \vdash t : A, \quad t \to_\beta u \Longrightarrow \Gamma \vdash u : A$ を $\Gamma \vdash t : A$ の証明 P の高さに関する Ind で示す。最後に使用する推論規則で場合分けを行うと、

(1) (ASS)

P は $\dfrac{}{\Gamma \vdash x : A}(ASS)$ と表せ、$x \to_\beta u$ となる u は存在しない。

(2) $(\to I)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma, x : A \vdash t : B\end{array}}{\Gamma \vdash \lambda x.t : A \to B}(\to I)$ と表せる。よって、$\lambda x.t \to_\beta u$ より、$u \equiv \lambda x.t_1, \quad t \to_\beta t_1$。IH for P_1 より、

$$\dfrac{\begin{array}{c}\vdots P_1' \\ \Gamma, x : A \vdash t_1 : B\end{array}}{\Gamma \vdash \lambda x.t_1 : A \to B}(\to I)$$

$u \equiv \lambda x.t_1$ より、上記の証明は

$$\dfrac{\begin{array}{c}\vdots P_1' \\ \Gamma, x : A \vdash t_1 : B\end{array}}{\Gamma \vdash u : A \to B}(\to I)$$

となり、$\Gamma \vdash u : A \to B$ が証明された。

(3) $(\to E)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma \vdash f : A \to B\end{array} \quad \begin{array}{c}\vdots P_2 \\ \Gamma \vdash a : A\end{array}}{\Gamma \vdash fa : B}(\to E)$ と表せる。$fa \to_\beta u$ の β-簡約が適用される個所で場合分けを行うと、

(i) $u \equiv f_1 a, \quad f \to_\beta f_1$ のとき、IH for P_1 より、

$$\dfrac{\begin{array}{c}\vdots P_1' \\ \Gamma \vdash f_1 : A \to B\end{array} \quad \begin{array}{c}\vdots P_2 \\ \Gamma \vdash a : A\end{array}}{\Gamma \vdash f_1 a : B}(\to E)$$

(ii) $u \equiv f a_1, \quad a \to_\beta a_1$ のとき、上と同様で証明可能。

(iii) $f \equiv \lambda x.b, \quad u \equiv b[x := a]$ のとき、P_1 の最後の推論規則は $(\to I)$ であり、P_1 は

$$\dfrac{\begin{array}{c}\vdots P_3 \\ \Gamma, x : A \vdash b : B\end{array}}{\Gamma \vdash \lambda x.b : A \to B}(\to I)$$

と表せる。よって、P_2 と P_3 を Prop. 3.6 に用いると $\Gamma \vdash b[x := a] : B$ が得られる。u の定義より、$\Gamma \vdash u : B$ が証明された。

これにより、1 ステップ β-簡約の命題が証明された。この命題を複数回適用すると、Th (SR) が証明される。

一般に、他の型理論でも SR が成り立つことが多い。SR はプログラムのデータ型が、プログラムの実行により変わってしまうことがないことを保証している。

3.3　強正規化性 (Strong Normalizability)

Def (t SN)

t SN とは $t \equiv t_0 \to_\beta t_1 \to_\beta \cdots$ となる無限列が存在しないことである。また、t SN のとき、$t \equiv t_0 \to_\beta t_1 \to_\beta \cdots \to_\beta t_n$ となる最大の n を $|t|$ で表す (最大の簡約パス長)。この節では強正規化性定理 ($\Gamma \vdash t : A \Longrightarrow t$ SN) を証明する。

Def (SN)

1. $\wedge$　　λ 式全体
   SN　　SN である λ 式全体
2. $A, B \subset \wedge$ のとき
   $A \to B = \{f \in \wedge |$ 任意の $a \in A$ について $fa \in B\}$
3. $\lambda_{\to}$ の型 A について $[\![A]\!] \subset \wedge$ を次のように定める。
   $[\![\alpha]\!] = \mathbf{SN}$　(α : 型変数)
   $[\![A \to B]\!] = [\![A]\!] \to [\![B]\!]$

(方針)　$t : A$ を解釈すると $[\![t]\!] \in [\![A]\!]$

Def (Saturated Set)

$X \subset \wedge$ が Saturated とは、次が成り立つこと

(sat1)　$X \subset \mathbf{SN}$

(sat2)　x が変数、$t_1, \cdots, t_n$ SN なら $xt_1t_2\cdots t_n \in X$

(sat3)　a SN, $n \geq 0$, t_1 SN, $\cdots, t_n$ SN , $t[x := a]t_1 \cdots t_n \in X$ なら
　　$(\lambda x.t)at_1 \cdots t_n \in X$

Prop. 3.7

(1) $\mathbf{SN}$ *sat*

(2) A, B *sat* $\Longrightarrow A \to B$ *sat*

(3) A が型なら $[\![A]\!]$ *sat*

Proof

(1) (sat1) 定義より自明

(sat2) $n \geq 0,\quad t_1 SN, \cdots, t_n SN \Longrightarrow xt_1 \cdots t_n$ SN であることを $|t_1| + \cdots + |t_n|$ に関する Ind で示す。$xt_1 \cdots x_n \to_\beta u$ となる任意の u について u SN を示す。

$xt_1 \cdots t_n \to_\beta u(u \equiv xt_1 \cdots t_{i-1}t'_i t_{i+1} \cdots t_n,\quad t_i \to_\beta t'_i)$ を仮定すると、$|t'_i| < |t_i|$ より、

$$|t_1| + \cdots + |t_{i-1}| + |t'_i| + |t_{i+1}| + \cdots + |t_n| < |t_1| + \cdots + |t_n|$$

IH より $xt_1 \cdots t_{i-1}t'_i t_{i+1} \cdots t_n$ SN

故に $xt_1 \cdots x_n \to_\beta u$ なら u SN

故に $xt_1 \cdots x_n$ SN

(sat3) $n \geq 0$, a SN, $t[x := a]t_1 \cdots t_n$ SN なら $(\lambda x.t)at_1 \cdots t_n$ SN を $|t[x := a]t_1 \cdots t_n| + |a|$ に関する Ind で示す。$(\lambda x.t)at_1 \cdots t_n \to_\beta u$ を仮定し、u SN を示す。

(i) $u \equiv (\lambda x.t)at_1 \cdots t'_i \cdots t_n,\quad t_i \to_\beta t'_i$ と表せるとき

$$|t[x := a]t_1 \cdots t'_i \cdots t_n| < |t[x := a]t_1 \cdots t_i \cdots t_n| \tag{A}$$

(A) と $t[x := a]t_1 \cdots t_i \cdots t_n$ SN より、

$$t[x := a]t_1 \cdots t'_i \cdots t_n \text{ SN} \tag{B}$$

また、(A) から

$$|t[x := a]t_1 \cdots t'_i \cdots t_n| + |a| < |t[x := a]t_1 \cdots t_i \cdots t_n| + |a| \tag{C}$$

(B), (C) より、帰納法の仮定が満たされ

$(\lambda x.t)at_1 \cdots t'_i \cdots t_n$ SN　(u SN)

(ii) $u \equiv (\lambda x.t)a't_1 \cdots t_n,\quad a \to_\beta a'$ と表せるとき、同上。

(iii) $u \equiv (\lambda x.t')at_1 \cdots t_n,\quad t \to_\beta t'$ と表せるとき、

$$t[x := a]t_1 \cdots t_n \to_\beta t'[x := a]t_1 \cdots t_n \tag{A2}$$

(A2) と $t[x := a]t_1 \cdots t_n$ SN より

$$t'[x := a]t_1 \cdots t_n \text{ SN} \tag{B2}$$

また、(A2) から

$$|t'[x := a]t_1 \cdots t_n| + |a| < |t[x := a]t_1 \cdots t_n| + |a| \tag{C2}$$

(B2), (C2) より、帰納法の仮定が満たされ

$(\lambda x.t')at_1 \cdots t_n$ SN　(u SN)

(iv) $u \equiv t[x := a]t_1 \cdots t_n$ と表せるとき、仮定より、u SN がいえる。

(2) (sat1) $f \in A \to B$ が SN でないと仮定する。すなわち、$f \equiv f_0 \to_\beta f_1 \to_\beta \cdots$ となる無限列が存在すると仮定する。
A(sat1) より、$x \in A$
$fx \in B$,　B(sat1) より、fx SN
一方、$fx \equiv f_0 x \to_\beta f_1 x \to_\beta \cdots$ となる無限列が存在してしまい矛盾する。よって、f は SN。

(sat2) x は変数、t_1 SN, $\cdots$, t_n SN を仮定する。$xt_1 \cdots t_n \in A \to B$ を示すために、$a \in A$ と仮定し、$xt_1 \cdots t_n a \in B$ を示す。
A(sat1) より、a SN。
B(sat2) より、$xt_1 \cdots t_n a \in B$
故に、$\forall a \in A$ について、$xt_1 \cdots t_n a \in B$
故に、$xt_1 \cdots t_n \in A \to B$

(sat3) t_1 SN, $\cdots$, t_n SN, a SN　$t[x := a]t_1 \cdots t_n \in A \to B$ と仮定し、$(\lambda x.t)at_1 \cdots t_n \in A \to B$ を示す。すなわち、$\forall b \in A$ のもとで、$(\lambda x.t)at_1 \cdots t_n b \in B$ を示せばよい。
A(sat1) より、b SN。
B(sat2) より、$t[x := a]t_1 \cdots t_n b \in B$
B(sat3) より、$(\lambda x.t)at_1 \cdots t_n b \in B$
よって、$\forall b \in A$ のもとで、$(\lambda x.t)at_1 \cdots t_n b \in B$ であり、$(\lambda x.t)at_1 \cdots t_n \in A \to B$ が証明された。

(3) 任意の型 A について $[\![A]\!]$ sat であることを、型 A の構成に関する帰納法で示す。

(i) A が型変数 α のとき、
$[\![\alpha]\!]$ =SN　(1) より、sat

(ii) A が $B \to C$ という構成のとき、
$[\![B \to C]\!] = [\![B]\!] \to [\![C]\!]$
IH より、$[\![B]\!], [\![C]\!]$ sat。
(2) より、$[\![B \to C]\!]$ sat であり、A sat。

Def (環境 ρ)

$Vars$ を変数全体の集合と定義し、環境 $\rho : Vars \to \wedge$ を次のように定義する。x を変数とし、$a \in \wedge$ とすると、

$$
\begin{aligned}
(\rho[x := a])(x) &= a \\
(\rho[x := a])(y) &= \rho(y) \quad (x \not\equiv y)
\end{aligned}
$$

また、$t \in \wedge \quad (FV(t) = \{x_1, \cdots, x_n\})$ について

$$[\![t]\!]\rho = t[x_1 := \rho(x_1), \cdots, x_n := \rho(x_n)]$$

$\rho \models t : A$ とは環境 ρ の下で $t : A$ が真のことであり、

$$[\![t]\!]\rho \in [\![A]\!]$$

$\rho \models x_1 : A_1, \cdots, x_n : A_n$ とは環境 ρ の下で文脈 $x_1 : A_1, \cdots, x_n : A_n$ が真のことであり、

$$\rho(x_1) \in [\![A_1]\!], \cdots, \rho(x_n) \in [\![A_n]\!]$$

$\Gamma \models t : A$ とは、任意の環境 ρ について、

$$\rho \models \Gamma \Longrightarrow \rho \models t : A$$

Th．SN

(1) $\Gamma \vdash t : A \Longrightarrow \Gamma \models t : A$

(2) $\Gamma \vdash t : A \Longrightarrow t$ SN

Proof

(1) $\Gamma \vdash t : A$ の証明 P の高さに関する Ind で $\Gamma \models t : A$ を示す。最後に使用した推論規則で場合分けを行うと、

(i) (ASS)

P は $\dfrac{}{\Gamma \vdash x : A}(ASS) \quad (x : A) \in \Gamma$ と表せる。$(x : A) \in \Gamma$ より、$\Gamma \models x : A$ は成立する。

(ii) $(\rightarrow I)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma, x : A \vdash t : B\end{array}}{\Gamma \vdash \lambda x.t : A \rightarrow B}(\rightarrow I)$ と表せる。環境 ρ を固定し、$\rho \models \Gamma$ の仮定の下で、$\rho \models \lambda x.t : A \rightarrow B$ を示す。すなわち、$\forall a \in [\![A]\!]$ について、$([\![(\lambda x.t)]\!]\rho)a \in [\![B]\!]$ を示せばよい。

$FV(\lambda x.t) = \{x_1, \cdots, x_n\}$

とおくと、束縛変数の名前換えと Prop. 3.3 より、

$x \notin FV(\rho(x_1)) \cup \cdots \cup FV(\rho(x_n))$

としてよい。$\Gamma \equiv x_1 : A_1, \cdots, x_n : A_n \quad x_i \not\equiv x$ より、

$\rho[x := a] \ \vDash \ \Gamma, x : A$

また、IH for P_1 より

$\Gamma, x : A \ \vDash \ t : B$

$\therefore \rho[x := a] \ \vDash \ t : B$

$\therefore [\![t]\!](\rho[x := a]) \in [\![B]\!]$

$$\begin{aligned} [\![t]\!](\rho[x := a]) &\equiv t[x := a, x_1 := \rho(x_1), \cdots, x_n := \rho(x_n)] \\ &\equiv t[x_1 = \rho(x_1), \cdots, x_n = \rho(x_n)][x := a] \end{aligned}$$

より、$t[x_1 = \rho(x_1), \cdots, x_n = \rho(x_n)][x := a] \in [\![B]\!]$。

また、B (sat3) より、

$(\lambda x.t[x_1 = \rho(x_1), \cdots, x_n = \rho(x_n)])\, a \in [\![B]\!]$

$(\lambda x.t[x_1 = \rho(x_1), \cdots, x_n = \rho(x_n)])$

$\equiv (\lambda x.t)\,[x_1 = \rho(x_1), \cdots, x_n = \rho(x_n)]$

$\equiv [\![\lambda x.t]\!]\rho$

より、$\forall a \in [\![A]\!]$ について、$([\![\lambda x.t]\!]\rho)a \in [\![B]\!]$

$\therefore [\![\lambda x.t]\!]\rho \in [\![A \to B]\!]$

$\therefore \rho \ \vDash \ \lambda x.t : A \to B$

(iii) $(\to E)$

P は $\dfrac{\begin{array}{c}\vdots P_1 \\ \Gamma \ \vdash \ f : A \to B\end{array} \quad \begin{array}{c}\vdots P_2 \\ \Gamma \ \vdash \ a : A\end{array}}{\Gamma \ \vdash \ fa : B}(\to E)$ と表せる。環境 ρ を固定し、$\rho \ \vDash \ \Gamma$ の仮定の下で、$\rho \ \vdash \ fa : B$ を示す。

IH for P_1 より、$\Gamma \ \vDash \ f : A \to B$

$\therefore [\![f]\!]\rho \in [\![A \to B]\!]$

IH for P_2 より、$\Gamma \ \vDash \ a : A$

$\therefore [\![a]\!]\rho \in [\![A]\!]$

$([\![f]\!]\rho)([\![a]\!]\rho) \in [\![B]\!]$ より、$[\![fa]\!]\rho \in [\![B]\!]$

$\therefore \rho \ \vDash \ fa : B$

(2) $\Gamma \ \vdash \ t : A$ を仮定すると (1) より、$\Gamma \ \vDash \ t : A$。次に環境 ρ を次のように定める。

$\rho(x) = x$　(任意の変数 x)

$\Gamma \equiv x_1 : A_1, \cdots, x_n : A_n$ とおくと Prop. 3.7 の (3) より $[\![A_i]\!]$ は sat。また、$TSET A_i$ sat より、(sat2) より、$x_i \in [\![A_i]\!]$

$\therefore \rho(x_i) = x_i \in [\![A_i]\!]$

よって、$0 \leq i \leq n$ について $\rho \ \vDash \ x_i : A_i$ が成立するから $\rho \ \vDash \ \Gamma$。$\Gamma \ \vDash \ t : A$ より、$\rho \ \vDash \ t : A$。よって、$[\![t]\!]\rho \in [\![A]\!]$。そして、$[\![t]\!]\rho \equiv t$ より、$t \in [\![A]\!]$。

Prop. 3.7 の (3) より $[\![A]\!]$ sat。$[\![A]\!]$ について (sat1) より、$[\![A]\!] \subset$ **SN**。

$\therefore t$ SN

(Remark)

(1) 型が付くことを示せば、プログラムの停止性が示せる。

(2) “SN ならば型が付く” は成り立たない。
(判例) $\lambda x.xx$ は型を持たないが、SN である。

(3) 他の型理論でも SN が成り立つことが多い。

3.4　主型 (principal type)

$\lambda x.x$ の型について考える。

$\vdash \ \lambda x.x : \alpha \to \alpha$

$\vdash \ \lambda x.x : (\alpha \to \beta) \to (\alpha \to \beta)$

つまり、 $\vdash \ \lambda x.x : A \iff$ ある型 B があって、$A \equiv B \to B$
$\lambda x.x$ の主型は $\alpha \to \alpha$ (最も一般的な型)。この節では型が付けば主型があることを示す。

Def (型代入)

TypeVars　型変数全体
Types　型全体
型代入 σ　$\sigma : \mathrm{TypeVars} \to \mathrm{Types}$
型 A, B について、$A = B$ とは $A \equiv B$。
型 A、型代入 σ について A^σ を次のように定める。

$$\begin{aligned} \alpha^\sigma &= \sigma(\alpha) \\ (A \to B)^\sigma &= A^\sigma \to B^\sigma \end{aligned}$$

(記法)　文脈 Γ, Π について、$\Gamma \supset \Pi$ とは、任意の $x : A$ について $(x : A) \in \Pi \Longrightarrow (x : A) \in \Gamma$。また、文脈 $\Gamma \equiv x_1 : A_1, \cdots, x_n : A_N$ について、Γ^σ を次のように定める。

$(x_1 : A_1, \cdots, x_n : A_n)^\sigma = (x_1 : A_1^\sigma, \cdots, x_n : A_n^\sigma)$

Def (主型)

文脈 Γ、項 t、型 A について $\Gamma \ \Vdash \ t : A$ とは次のこと

(1) $\Gamma \ \vdash \ t : A$

(2) $\Pi \ \vdash \ t : B$ なら、型代入 σ があって $B = A^\sigma,\ \Pi \supset \Gamma^\sigma$

このとき、(Γ, A) を t の principal pair という。また、 $\Vdash\ t : A$ のとき、A を t の主型という。

(例) $\lambda x.x$ の主型は $\alpha \to \alpha$

Th．(principal pair の存在)

(1) $\Gamma\ \vdash\ t : A$ なら Π, B があって、$\Pi\ \Vdash\ t : B$

(2) 上の Π, B を t から計算によって得るアルゴリズムが存在する

Prop. 3.8 （主型の存在）

$\vdash\ t : A$ なら t の主型が存在する

Def (型代入の合成)

- 型代入 σ, ρ について $\sigma \circ \rho$ を次のように定義する。

$$\begin{aligned}(\sigma \circ \rho)(\alpha) &= (\sigma(\alpha))^{\rho} \\ A^{\sigma \circ \rho} &= (A^{\sigma})^{\rho}\end{aligned}$$

- $\sigma \leq \rho$ とは、型代入 ρ_1 がって、$\sigma \circ \rho_1 = \rho$
- $\sigma \approx \rho$ とは、$\sigma \leq \rho$ かつ $\rho \leq \sigma$
- 型代入 σ が型 A, B の unifier とは $A^{\sigma} = B^{\sigma}$

(例 1)　$A = (\alpha_1 \to \alpha_2) \to \alpha_3, B = \beta_1 \to (\beta_2 \to \beta_3)$ について、型代入 σ を次のように定めると σ は A, B の unifier となる。

$$\rho(x) = \begin{cases} \alpha_1 \to \alpha_2 & (x = \beta_1) \\ \beta_2 \to \beta_3 & (x = \alpha_3) \\ x & (x \neq \beta_1, x \neq \alpha_3) \end{cases}$$

なぜなら、$A^{\sigma} = B^{\sigma} = (\alpha_1 \to \alpha_2) \to (\beta_2 \to \beta_3)$

(例 2)　$A = \alpha, B = \alpha \to \beta$ とすると A と B の unifier は存在しない。

仮に unifier σ が存在すると仮定すると $A^{\sigma} = B^{\sigma}$
よって、A, B の定義より、$\alpha^{\sigma} = \alpha^{\sigma} \to \beta^{\sigma}$
右辺の文字数 $>$ 左辺の文字数より矛盾する。

Def (mgu)

型代入 σ が型 A, B の most general unifier (mgu) とは次のことである。

(1) $A^\sigma = B^\sigma$

(2) $A^\rho = B^\rho$ ならば $\sigma \leq \rho$

(例)　上の例では、σ は A, B の mgu である。

(Remark)

(1) $\sigma \approx \rho$ なら型変数の名前換えを行うと σ から ρ が得られる。

(2) mgu は $\approx$ を除いて一意的。

Def (unifier)

$A_1, B_1, \cdots, A_n, B_n$ を型、E を列 $(A_1, B_1), \cdots, (A_n, B_n)$ とおくと、σ が E の unifier とは、次のことを満たす。

$A_1^\sigma = B_1^\sigma, \cdots, A_n^\sigma = B_n^\sigma$

このことを $\sigma \models E$ と表す。また σ が E の mgu とは次のことである。

(1) $\sigma \models E$

(2) $\rho \models E$ ならば、$\sigma \leq \rho$

(記法)　$E_1 = (A_1, B_1), \cdots, (A_m, B_m)$, $E_2 = (C_1, D_1), \cdots, (C_n, D_n)$ のとき、$E_1(F, G)E_2$ は次の列を表す。

$(A_1, B_1), \cdots, (A_m, B_m), (F, G), (C_1, D_1), \cdots, (C_n, D_n)$

また、$\alpha_1, \cdots, \alpha_n$ を型変数、$A_1, \cdots, A_n$ を型、σ を型代入とすると、型代入 $\sigma[\alpha_1 := A_1, \cdots, \alpha_n := A_n]$ は次のように定義される。

$$(\sigma[\alpha_1 := A_1, \cdots, \alpha_n := A_n])(x) = \begin{cases} A_i & (x = \alpha_i) \\ \sigma(x) & (x \neq \alpha_i) \end{cases}$$

また、型代入 1 を次のように定義し、

$1(\alpha) = \alpha$　(任意の型変数 α)

$[\alpha_1 := A_1, \cdots, \alpha_n := A_n]$ を $1[\alpha_1 := A_1, \cdots, \alpha_n := A_n]$ の略記と定める。

Lemma

(1) $\sigma \models (\alpha, A) \Longrightarrow [\alpha := A] \circ \sigma = \sigma$

(2) $\sigma \models ((\alpha, A), E) \Longleftrightarrow \sigma \models (\alpha, A)$ かつ $\sigma \models E^{[\alpha := A]}$

Proof

(1) $([\alpha := A] \circ \alpha)(\alpha) = A^\sigma = \alpha^\sigma = \sigma(\alpha)$
$([\alpha := A] \circ \alpha)(\beta) = \sigma(\beta) \quad (\alpha \neq \beta)$

(2) $\Longrightarrow$) 仮定より、$\sigma \ \vDash \ (\alpha, A),\ \sigma \ \vDash \ E$
$\sigma \ \vDash \ (\alpha, A)$ と (1) より $\sigma = [\alpha := A] \circ \sigma$
これと $\sigma \ \vDash \ E$ より $[\alpha := A] \circ \sigma \ \vDash \ E$
$\therefore \sigma \ \vDash \ E^{[\alpha := A]}$

$\Longleftarrow$) $\sigma \ \vDash \ E^{[\alpha := A]}$ より、$[\alpha := A] \circ \sigma \ \vDash \ E$
$\sigma \ \vDash \ (\alpha, A)$ と (1) より $\sigma \ \vDash \ E$
よって、$\sigma \ \vDash \ E$ と $\sigma \ \vDash \ (\alpha, A)$ から $\sigma \ \vDash \ ((\alpha, A), E)$

Prop. 3.9 （mgu の存在）

(1) A と B の unifier があるならば、A と B の mgu が存在する

(2) $A_1, \cdots, A_n, B_1, \cdots, B_n$ を型とするとアルゴリズム unify : $((A_1, B_1), \cdots, (A_n, B_n)) \to \sigma$ or fail を次のように定める。

(a) $\mathrm{Unify}((\alpha, A), E) =$

$$\begin{cases} [\alpha := A] \circ \mathrm{Unify}(E^{[\alpha := A]}) & \text{if } \alpha \notin FV(A),\ \mathrm{Unify}(E^{[\alpha := A]}) \neq \text{fail} \\ \text{fail} & \text{if } \alpha \notin FV(A),\ \mathrm{Unify}(E^{[\alpha := A]}) = \text{fail} \\ \mathrm{Unify}(E) & \text{if } \alpha = A \\ \text{fail} & \text{if } \alpha \neq A, \alpha \in FV(A) \end{cases}$$

(b) $\mathrm{Unify}((A \to B, \alpha), E) = \mathrm{Unify}(((\alpha, A \to B), E))$

(c) $\mathrm{Unify}((A \to B, C \to D), E) = \mathrm{Unify}(((A, C), (B, D), E))$

(d) $\mathrm{Unify}(()) = 1$

このとき、$E = ((A_1, B_1), \cdots, (A_n, B_n))$ とおくと、次が成り立つ。

(2a) E が unifier をもつならば、$\mathrm{Unify}(E)$ は E の mgu

(2b) E が unifier をもたないならば、$\mathrm{Unify}(E)$ は fail

Proof　$|E| =$ (E に出現する変数の個数, E 中の記号数, (A_1 の記号数), $\cdots$, (A_n の記号数)) [1]とし、辞書式順序による $|E|$ に関する Ind で (2a), (2b) を示す。証明の際には、Unify の場合分けと同じ場合分けを行う。

(2a) (a) $E' = ((\alpha, A), E)$ とおき、$\sigma \ \vDash \ E'$ と仮定する。

[1] α, α, β の場合、変数の個数は 2 個

(I) $\alpha \notin FV(A)$ のとき
Lemma. (2) より、$\sigma \models E^{[\alpha:=A]}$
$E^{[\alpha:=A]}$ は E' より変数の個数が少なく $|E^{[\alpha:=A]}| < |E'|$
よって IH より $\mathrm{Unify}(E^{[\alpha:=A]}) = \sigma_1$, σ_1 は $E^{[\alpha:=A]}$ の mgu。
$\therefore \mathrm{Unify}(E') = [\alpha := A] \circ \sigma_1$
$\sigma = [\alpha := A] \circ \sigma_1$ とおき、σ が E' の mgu であることを示す。

(1) $\sigma_1 \models E^{[\alpha:=A]}$ より $[\alpha := A] \circ \sigma_1 \models E$
σ の定義より、$\sigma \models E$
また、$\alpha^\sigma = A^{\sigma_1} = A^\sigma$ より、$\sigma \models (\alpha, A)$
$\therefore \sigma \models E'$

(2) $\tau \models E'$ と仮定し、$\sigma \leq \tau$ を示す。
Lemma. (2) より $\tau \models (\alpha, A)$, $\tau \models E^{[\alpha:=A]}$
σ_1 は $E^{[\alpha:=A]}$ の mgu より、$\sigma_1 \leq \tau$
よって、ある τ_1 があって、$\sigma_1 \circ \tau_1 = \tau$

$$\begin{aligned} \sigma \circ \tau_1 &= [\alpha := A] \circ \sigma_1 \circ \tau_1 \\ &= [\alpha := A] \circ \tau \\ &= \tau \quad (\because \text{Lemma. (1) より}) \end{aligned}$$

よって、$\sigma \leq \tau$ が成り立つ。

(1), (2) より、σ が E' の mgu であることが示された。

(II) $\alpha = A$ のとき
$\sigma \models E'$ を仮定すると、$\mathrm{Unify}(E') = \mathrm{Unify}(E)$
$|E'| > |E|$ より $\mathrm{Unify}(E)$ は mgu より $\mathrm{Unify}(E')$ も mgu。

(III) $\alpha \neq A,\ \alpha \in FV(A)$ のとき
α^σ の文字数 $\neq A^\sigma$ の文字数より、この場合はありえない。

(b) $E_1 = ((A \to B, \alpha), E),\ E_2 = ((\alpha, A \to B), E)$ とおくと
$$\sigma \models E_1 \Longleftrightarrow \sigma \models E_2, \quad |E_1| > |E_2|$$
が成立する。それより、$\sigma \models E_1$ を仮定すると、$\sigma \models E_2$ が成立する。よって、E_2 に対する IH より $\mathrm{Unify}(E_2)$ は E_2 の mgu である。また、それより $\mathrm{Unify}(E_2)$ は E_1 の mgu である。$\mathrm{Unify}(E_1) = \mathrm{Unify}(E_2)$ より、$\mathrm{Unify}(E_1)$ は E_1 の mgu。

(c) $E_1 = ((A \to B, C \to D), E),\ E_2 = ((A, C), (B, D), E)$ とおくと、
$$\sigma \models E_1 \Longleftrightarrow \sigma \models E_2, \quad |E_1| > |E_2|$$
が成立し、以下同様。

(d) 1 は型代入の中で最小であり、$1 \models ()$ は成立する。よって、1 は mgu。

(2b) (a) $E' = ((\alpha, A), E)$ とおき、E' が unifier を持たないと仮定する。

(I) $\alpha \notin FV(A)$ のとき
$\sigma \models E^{[\alpha:=A]}$ と仮定すると、$[\alpha := A] \circ \sigma$ は E' の unifier となり、E' が unifier を持たないという仮定と矛盾する。
$\therefore\ E^{[\alpha:=A]}$ は unifier を持たない。
また、$|E^{[\alpha:=A]}| \leq |E'|$。IH より、$\mathrm{Unify}(E') = \mathrm{fail}$。
$\therefore \mathrm{Unify}(E) = \mathrm{fail}$

(II) $\alpha = A$ のとき
(2a) の (a) の (II) と同様に証明可能。

(III) $\alpha \neq A, \alpha \in FV(A)$ のとき
Unify の定義より、fail。

(b) $E_1 = ((A \to B, \alpha), E), E_2 = ((\alpha, A \to B), E)$ とおき、
(2a) の (b) と同様に証明可能。

(c) $E_1 = ((A \to B, C \to D), E), E_2 = ((A, C), (B, D), E)$ とおき、
(2a) の (c) と同様に証明可能。

(d) 仮定が成立しないために、(2b) は成立する。

(例)　以下のような A, B の unification を求める。
$A = (\alpha_1 \to \alpha_2) \to \alpha_3$
$B = \beta_1 \to \beta_2 \to \beta_3$

$$
\begin{aligned}
\mathrm{Unify}((A, B)) &= \mathrm{Unify}(((\alpha_1 \to \alpha_2) \to \alpha_3, \beta_1 \to \beta_2 \to \beta_3)) \\
&= \mathrm{Unify}((\alpha_1 \to \alpha_2, \beta_1), (\alpha_3, \beta_2 \to \beta_3)) \\
&= \mathrm{Unify}((\beta_1, \alpha_1 \to \alpha_2), (\alpha_3, \beta_2 \to \beta_3)) \\
&= [\beta_1 := \alpha_1 \to \alpha_2] \circ \mathrm{Unify}(\alpha_3, \beta_2 \to \beta_3)) \\
&= [\beta_1 := \alpha_1 \to \alpha_2] \circ [\alpha_3 := \beta_2 \to \beta_3] \circ \mathrm{Unify}() \\
&= [\beta_1 := \alpha_1 \to \alpha_2] \circ [\alpha_3 := \beta_2 \to \beta_3] \\
&= [\beta_1 := \alpha_1 \to \alpha_2,\ \alpha_3 := \beta_2 \to \beta_3]
\end{aligned}
$$

Def $(E(\Gamma, t, A))$

Γ : 文脈、t : 項、A : 型とし、型の対の列 $E(\Gamma, t, A)$ を次のように定める。

(1) $E(\Gamma, x, A) = \begin{cases} (B, A) & \text{if } (x : B) \in \Gamma \\ (A, A \to A) & \text{if } x \notin FV(\Gamma) \end{cases}$

(2) $E(\Gamma, \lambda x.t, A) = (E((\Gamma, x : \alpha), t, \beta), (A, \alpha \to \beta))$　　α, β : fresh variable

(3) $E(\Gamma, fa, A) = (E(\Gamma, f, \alpha \to A), E(\Gamma, a, \alpha))$　　α : fresh variable

Def $(=_V)$

$$\sigma =_V \rho \text{ とは } \forall\alpha \in V \ (V \subset \mathrm{TypeVars}) \quad \sigma(\alpha) = \rho(\alpha)$$

Prop. 3.10 [2]

$$\Gamma^\sigma \ \models \ t : A^\sigma \iff \forall V \subset \mathrm{TypeVars}, \mathrm{V}: \text{ infinite}, V \cap FV(\Gamma, A) = \phi,$$
$$\exists\rho =_{V^C} \sigma(\rho \ \models \ E(\Gamma, t, A))$$

Proof

$\Leftarrow$) $V = FV(\Gamma, A)^C$ とし、t に関する Ind で

$$\sigma \ \models \ E(\Gamma, t, A) \Longrightarrow \Gamma^\sigma \ \vdash \ t : A^\sigma$$

を示す。t に構成で場合分けを行うと、

(1) $t \equiv x$ のとき

(i) $(x, B) \in \Gamma$ となる B が存在するとき

$$E(\Gamma, x, A) = (B, A)$$

よって、$\sigma \ \models \ (B, A)$ より、$B^\sigma = A^\sigma$ が成立する。また、$(x, B) \in \Gamma$ より、$(x, B^\sigma) \in \Gamma^\sigma$ が成立し、$(x : A^\sigma) \in \Gamma^\sigma$

$$\therefore \frac{}{\Gamma^\sigma \ \vdash \ x : A^\sigma}(ASS)$$

(ii) $(x, B) \in \Gamma$ となる B が存在しないとき

$$E(\Gamma, x, A) = (A, A \to A)$$

よって、$\sigma \ \models \ (A, A \to A)$ となるが、これを成立させる型代入 ρ は存在しない。なぜなら、そのような ρ が存在すると仮定すると、

$$A^\rho = A^\rho \to A^\rho$$

より、(左辺の文字数) $\neq$ (右辺の文字数) より矛盾する。

(2) $t \equiv \lambda x.t_1$ のとき

$$E(\Gamma, \lambda x.t_1, A) \quad = \quad (E((\Gamma, x : \alpha), t_1, \beta), (A, \alpha \to \beta))$$
$$(\alpha, \beta : \text{ fresh variable})$$

よって、型代入 ρ の定義より

$$\rho \ \models \ E((\Gamma, x : \alpha), t_1, \beta)$$
$$\rho \ \models \ (A, \alpha \to \beta)$$

IH for t_1 より、

$$(\Gamma, x : \alpha)^\rho \ \vdash \ t_1 : B^\rho$$

$(\Gamma, x : \alpha)^\rho = \Gamma^\rho, x : \alpha^\rho$ より、

$$\frac{\Gamma^\rho, x : \alpha^\rho \ \vdash \ t_1 : B^\rho}{\Gamma^\rho \ \vdash \ \lambda x.t_1 : \alpha^\rho \to \beta^\rho}(\to I)$$

また、$\rho \ \models \ (A, \alpha \to \beta)$ より、$A^\rho = \alpha^\rho \to \beta^\rho$

よって、$\Gamma^\rho \ \vdash \ t : A^\rho$ が成立する。

[2] これにより、型付けと Unify が同値であることが示される

(3) $t \equiv fa$ のとき

$$E(\Gamma, fa, A) \quad = \quad (E(\Gamma, f, \alpha \to A), E(\Gamma, a, \alpha))$$

$(\alpha:$ fresh variable$)$

よって、型代入 ρ の定義より

$\rho \models E(\Gamma, f, \alpha \to A)$

$\rho \models E(\Gamma, a, \alpha)$

IH より $\Gamma^\rho \vdash f : (\alpha \to A)^\rho,\ \Gamma^\rho \vdash a : \alpha^\rho$

$(\alpha \to A)^\rho = \alpha^\rho \to A^\rho$ より

$$\frac{\Gamma^\rho \vdash f : \alpha^\rho \to A^\rho \quad \Gamma^\rho \vdash a : \alpha^\rho}{\Gamma^\rho \vdash fa : A^\rho}(\to E)$$

(1), (2), (3) より $\Gamma^\rho \vdash t : A^\rho$ が成立し、$\sigma =_{FV(\Gamma,A)} \rho$ より $\Gamma^\sigma \vdash t : A^\sigma$

⇒) $\Gamma^\sigma \vdash t : A^\sigma$ の証明 P の高さに関する Ind で示す。最後に使用する推論規則で場合分けを行うと、

(1) (ASS)

P が $\dfrac{}{\Gamma^\sigma \vdash x : A^\sigma}(ASS) \quad (x : A^\sigma) \in \Gamma^\sigma$ と表されるとき、

$(x : B) \in \Gamma, \quad B^\sigma = A^\sigma$

となる B が存在し、$E(\Gamma, x, A) = (B, A)$。$\rho = \sigma$ とすると、

$\rho \models E(\Gamma, x, A)$

(2) $(\to I)$

P が $\dfrac{\Gamma^\sigma, x : B \vdash t : C}{\Gamma^\sigma \vdash \lambda x.t : B \to C}(\to I) \quad (A^\sigma = B \to C)$ と表せるとき

$\alpha, \beta \in V, \alpha \neq \beta$ となる α, β が存在して、

$E(\Gamma, \lambda x.t, A) = (E((\Gamma, x : A), t, \beta), (A, \alpha \to \beta))$

σ_1 を次のように定めると

$$\sigma_1(\gamma) = \begin{cases} B & (\gamma = \alpha) \\ C & (\gamma = \beta) \\ \sigma(\gamma) & (\gamma \neq \alpha, \beta) \end{cases}$$

$\Gamma^\sigma, x : B \vdash t : C$ より

$(\Gamma, x : \alpha)^{\sigma_1} \vdash t : \beta^{\sigma_1}$

また、$V_1 = V - \{\alpha, \beta\}$ と定義すると

$V_1 \cap FV((\Gamma, x : \alpha), \beta) = \phi$

IH for t より

$$\exists \rho =_{V_1^C} \sigma_1, \quad \rho \models E((\Gamma, x : \alpha), t, \beta) \tag{A}$$

また、$(\alpha \to \beta)^\rho = B \to C = A^\sigma = A^{\sigma_1} = A^\rho$ より

$$\rho \models (A, \alpha \to \beta) \tag{B}$$

(A), (B) より、

$$\exists \rho =_{V_1^C} \sigma_1, \quad \rho \ \vDash \ E(\Gamma, \lambda x.t, A) \tag{C}$$

$V^C \subset V_1^C, \alpha, \beta \notin V^C$ より、$\forall r \in V^C, \rho(\gamma) = \sigma_1(\gamma) = \sigma(\gamma)$
よって、$\rho =_{V^C} \sigma$ が成立し、(C) と $\rho =_{V^C} \sigma$ より
$\exists \rho =_{V^C} \sigma_1, \quad \rho \ \vDash \ E(\Gamma, \lambda x.t, A)$

(3) $(\to E)$

P が $\dfrac{\Gamma^\sigma \ \vdash \ f : B \to A^\sigma \quad \Gamma^\sigma \ \vdash \ a : B}{\Gamma^\sigma \ \vdash \ fa : A^\sigma}(\to E)$ と表せるとき、
$\alpha \in V$ が存在して、
$E(\Gamma, fa, A) = (E(\Gamma, f, \alpha \to A), E(\Gamma, a, \alpha))$
V_1, V_2 を次が成り立つように選ぶと、
$V = V_1 + V_2 + \{\alpha\}, \quad V_1, V_2 : \text{infinite}$
$E(\Gamma, f, \alpha \to A) \subset V_1 \cup FV(\Gamma, \alpha \to A)$
$E(\Gamma, a, \alpha) \subset V_2 \cup FV(\Gamma, \alpha)$
型代入 σ_1 を次のように定義すると、
$$\sigma_1(\gamma) = \begin{cases} A & (\gamma = \alpha) \\ \sigma(\gamma) & (\gamma \neq \alpha) \end{cases}$$

(i) $\Gamma^\sigma \ \vdash \ f : B \to A^\sigma$ より $\Gamma^{\sigma_1} \ \vdash \ f : (\alpha \to A)^{\sigma_1}$
また、V_1 について

$$\begin{aligned} V_1 \cup FV(\Gamma, \alpha \to A) &= V_1 \cup \{\alpha\} \cup FV(\Gamma, A) \\ &\subset V \cup FV(\Gamma, A) \\ &= \phi \end{aligned}$$

よって、IH for f より
$\exists \rho_1 =_{V_1^C} \sigma_1, \quad \rho_1 \ \vDash \ E(\Gamma, f, \alpha \to A)$

(ii) $\Gamma^\sigma \ \vdash \ a : B$ より $\Gamma^{\sigma_1} \ \vdash \ a : \alpha^{\sigma_1}$
また、V_2 も V_1 と同様にして、$V_2 \cup FV(\Gamma, \alpha) = \phi$
よって、IH for a より
$\exists \rho_2 =_{V_2^C} \sigma_1, \quad \rho_2 \ \vDash \ E(\Gamma, a, \alpha)$

(i), (ii) より型代入 ρ を次のように定義する。
$$\rho(\gamma) = \begin{cases} \rho_1(\gamma) & (\gamma \in V_1) \\ \rho_2(\gamma) & (\gamma \in V_2) \\ \sigma_1(\gamma) & \text{otherwise} \end{cases}$$
$\forall \gamma \in V^C$ について、$\rho(\gamma) = \sigma_1(\gamma) = \sigma(\gamma)$ より、

$$\rho =_{V^C} \sigma \tag{D}$$

(a) $\gamma \in V_1 \Rightarrow \rho(\gamma) = \rho_1(\gamma)$
$\gamma \in FV(\Gamma, \alpha \to A) \Rightarrow \rho(\gamma) = \sigma_1(\gamma) = \rho_1(\gamma) \quad (\because \sigma_1 =_{V_1^C} \rho_1)$
それゆえ、$\rho =_{V_1 \cup FV(\Gamma, \alpha \to A)} \rho_1$ が成立するので

$$\rho \models E(\Gamma, f, \alpha \to A) \tag{E}$$

(b) $\gamma \in V_2 \Rightarrow \rho(\gamma) = \rho_2(\gamma)$
$\gamma \in FV(\Gamma, \alpha) \Rightarrow \rho(\gamma) = \sigma_1(\gamma) = \rho_2(\gamma) \quad (\because \rho_2 =_{V_2^C} \sigma_1)$
それゆえ、$\rho =_{V_2 \cup FV(\Gamma, \alpha)} \rho_2$ が成立するので

$$\rho \models E(\Gamma, a, \alpha) \tag{F}$$

(c) $(E), (F)$ より、次が成り立つ。

$$\rho \models E(\Gamma, fa, A) \tag{G}$$

(D), (G) より
$\exists \rho =_{V^C} \sigma, \quad \rho \models E(\Gamma, fa, A)$
が証明された。

Def (pp)

項 t に対して、アルゴリズム $pp(t)$ を次のように定義する。$FV(t) = \{x_1, \cdots, x_n\}$ となるとき、$\alpha_1, \cdots, \alpha_n, \alpha$ を異なる型変数とし、$\Gamma = (x_1 : \alpha_1, \cdots, x_n : \alpha_n)$ となる文脈 Γ を作成する。その文脈において、Unify$(E(\Gamma, t, \alpha))$ の結果 Ans の値によって場合分けを行うと

(1) Ans = fail $\Longrightarrow$ $pp(t) =$ fail

(2) Ans = σ $\Longrightarrow$ $pp(t) = (\Gamma^\sigma, \alpha^\sigma)$

Th．principal pair の存在

(1) $\Gamma \vdash t : A$ なら、Π, B が存在して $pp(t) = (\Pi, B)$ かつ $\Pi \models t : B$

(2) $\Gamma \vdash t : A$ となる Π, B が存在しないなら、$pp(t) =$ fail

Proof

(1) $FV(t) = \{x_1, \cdots, x_n\}$ のとき、$\alpha_1, \cdots, \alpha_n, \alpha$ を異なる型変数とし、$\Gamma_0 = (x_1 : \alpha_0, \cdots, x_n : \alpha_n)$, 　Ans = Unify$(E(\Gamma_0, t, \alpha))$ と定義する。Prop.3.1, Prop.3.2 より、$\Gamma = (x_1 : A_1, \cdots, a_n : A_n)$ と表せるとしてもよい。
σ_1 を次のように定義すると

$$\sigma_1(\gamma) = \begin{cases} A_i & (\gamma = \alpha_i, 1 \leq i \leq n) \\ A & (\gamma = \alpha) \\ \gamma & (\gamma \neq \alpha_i, \alpha) \end{cases}$$

$\Gamma \ \vdash \ t : A$ より

$$\Gamma_0^{\sigma_1} \ \vdash \ t : \alpha^{\sigma_1}$$

$V = \mathrm{TypeVar} - \{\alpha_1, \cdots, \alpha_n, \alpha\}$ と定義すると

$$V \cap FV(\Gamma_0, \alpha) = \phi$$

Prop. 3.10 より、

$$\exists \sigma_2 =_{V^C} \sigma_1, \quad \sigma_2 \ \models \ E(\Gamma_0, t, \alpha)$$

よって、$E(\Gamma_0, t, \alpha)$ の unifier(σ_2) が存在し、Ans $= \sigma$ とおくと、Prop. 3.9 より、σ は $E(\Gamma_0, t, \alpha)$ の mgu。そして、$\Pi = \Gamma_0^{\sigma},\ B = \alpha^{\sigma}$ とおくと、

$$pp(t) = (\Pi, B)$$

が成立する。ここから、もう一つの満たすべき性質である $\Pi \ \models \ t : B$ を証明する。

(a) $\sigma \ \models \ E(\Gamma_0, t, \alpha)$ より、$\Gamma_0^{\sigma} \ \vdash \ t : \alpha^{\sigma}$
Π, B の定義より、$\Pi \ \vdash \ B$ が成立する。

(b) $\Gamma' \ \vdash \ t : C$ を仮定すると、Prop.3.1, Prop.3.2 より、$\Gamma' = (x_1 : C_1, \cdots, x_n : C_n)$ と表せるとしてもよい。型代入 ρ_1 を次のように定めると

$$\rho_1(\gamma) = \begin{cases} C_i & (\gamma = \alpha_i, 1 \leq i \leq n) \\ C & (\gamma = \alpha) \\ \gamma & (\gamma \neq \alpha_i, \alpha) \end{cases}$$

$\Gamma' \ \vdash \ t : C$ より、

$$\Gamma_0^{\rho_1} \ \vdash \ t : \alpha^{\rho_1}$$

$V \cap FV(\Gamma_0, \alpha) = \phi$, Prop. 3.10 より、

$$\exists \rho_2 =_{V^C} \rho_1, \quad \rho_2 \ \models \ E(\Gamma_0, t, \alpha)$$

また、σ は mgu より、ある型代入 ρ があって

$$\sigma \circ \rho = \rho_2$$

よって、Π, B の定義より

$$\begin{aligned} \Pi^{\rho} &= (\Gamma_0^{\sigma})^{\rho} = \Gamma_0^{\sigma \circ \rho} = \Gamma_0^{\rho_2} \\ &= \Gamma_0^{\rho_1} = \{x_1 : C_1, \cdots, x_n : C_n\} \\ &\subset \Gamma' \\ B^{\rho} &= (\alpha^{\sigma})^{\rho} = \alpha^{\sigma \circ \rho} = \alpha^{\sigma_2} = \alpha^{\rho_1} = C \end{aligned}$$

(a), (b) より、$\Pi \ \models \ t : B$ が成立する。

(2) $\Gamma \ \vdash \ t : A$ となる Γ, A がないとする。$pp(t) \neq$fail と仮定すると

$$\mathrm{Unify}(E) = \sigma$$

$$\therefore \sigma \ \models \ E(\Gamma, t, A)$$

Prop. 3.10 より、$\Gamma^{\sigma} \ \vdash \ t : A^{\sigma}$ より矛盾。

(例)　$\models \ \lambda x.x : \alpha \to \alpha$ を証明する。$FV(\lambda x.x) = \phi$ より、

$$\begin{aligned}
\mathrm{Ans} &= \mathrm{Unify}(E((), \lambda x.x, \alpha)) \\
&= \mathrm{Unify}(E(x : \alpha_1, x, \alpha 2), (\alpha, \alpha_1 \to \alpha_2)) \\
&= \mathrm{Unify}((\alpha_1, \alpha_2), (\alpha, \alpha_1 \to \alpha_2)) \\
&= [\alpha_1 := \alpha_2] \circ \mathrm{Unify}(\alpha, \alpha_2 \to \alpha_2)) \\
&= [\alpha_1 := \alpha_2] \circ [\alpha := \alpha_2 \to \alpha_2] \circ \mathrm{Unify}(()) \\
&= [\alpha_1 := \alpha_2] \circ [\alpha := \alpha_2 \to \alpha_2] \\
&= [\alpha_1 := \alpha_2,\ \alpha := \alpha_2 \to \alpha_2]
\end{aligned}$$

$\mathrm{Ans} = \sigma$ とおくと、
　$pp(\lambda x.x) = (()^\sigma, \alpha^\sigma) = ((), \alpha_2 \to \alpha_2)$
定理より、 $\models \ \lambda x.x : \alpha_2 \to \alpha_2$

(例)　$y : \alpha \to \beta \ \models \ \lambda x.yx : \alpha \to \beta$ を証明する。$FV(\lambda x.yx) = \{y\}$ より、
文脈 Γ を $(y : \alpha_1)$ と表せ、

$$\begin{aligned}
\mathrm{Ans} &= \mathrm{Unify}(E((y : \alpha_1), \lambda x.yx, \alpha)) \\
&= \mathrm{Unify}(E((y : \alpha_1, x : \alpha_2), yx, \alpha_3), (\alpha, \alpha_2 \to \alpha_3)) \\
&= \mathrm{Unify}(E((y : \alpha_1, x : \alpha_2), y, \alpha_4 \to \alpha_3), \\
&\qquad E((y : \alpha_1, x : \alpha_2), x, \alpha_4), (\alpha, \alpha_2 \to \alpha_3)) \\
&= \mathrm{Unify}((\alpha_1, \alpha_4 \to \alpha_3), (\alpha_2, \alpha_4), (\alpha, \alpha_2 \to \alpha_3)) \\
&= [\alpha_1 := \alpha_4 \to \alpha_3] \circ \mathrm{Unify}((\alpha_2, \alpha_4), (\alpha, \alpha_2 \to \alpha_3)) \\
&= [\alpha_1 := \alpha_4 \to \alpha_3] \circ [\alpha_2 := \alpha_4] \circ \mathrm{Unify}((\alpha, \alpha_4 \to \alpha_3)) \\
&= [\alpha_1 := \alpha_4 \to \alpha_3] \circ [\alpha_2 := \alpha_4] \circ [\alpha := \alpha_4 \to \alpha_3] \circ \mathrm{Unify}(()) \\
&= [\alpha_1 := \alpha_4 \to \alpha_3,\ \alpha_2 := \alpha_4,\ \alpha := \alpha_4 \to \alpha_3]
\end{aligned}$$

$\mathrm{Ans} = \sigma$ とおくと、
　$pp(\lambda x.yx) = (\Gamma^\sigma, \alpha^\sigma) = ((y : \alpha_4 \to \alpha_3), \alpha_4 \to \alpha_3)$
定理より、$y : \alpha_4 \to \alpha_3 \ \models \ \lambda x.yx : \alpha_4 \to \alpha_3$

(例)　$\vdash \ \lambda x.xx : A$ となる型 A は存在しないことを証明する。$FV(\lambda x.xx) = \phi$ より、

$$\begin{aligned}
\mathrm{Ans} &= \mathrm{Unify}(E((), \lambda x.xx, \alpha)) \\
&= \mathrm{Unify}(E((x : \alpha_1), xx, \alpha_2), (\alpha, \alpha_1 \to \alpha_2)) \\
&= \mathrm{Unify}(E((x : \alpha_1), x, \alpha_3 \to \alpha_2), E((x : \alpha_1), x, \alpha_3), (\alpha, \alpha_1 \to \alpha_2)) \\
&= \mathrm{Unify}((\alpha_1, \alpha_3 \to \alpha_2), (\alpha_1, \alpha_3), (\alpha, \alpha_1 \to \alpha_2)) \\
&= [\alpha_1 := \alpha_3 \to \alpha_2] \circ \mathrm{Unify}((\alpha_3 \to \alpha_2, \alpha_3), (\alpha, (\alpha_3 \to \alpha_2) \to \alpha_2)) \\
&= [\alpha_1 := \alpha_3 \to \alpha_2] \circ \mathrm{Unify}((\alpha_3, \alpha_3 \to \alpha_2), (\alpha, (\alpha_3 \to \alpha_2) \to \alpha_2)) \\
&= \mathrm{fail} \qquad (\because \alpha_3 \in FV(\alpha_3 \to \alpha_2))
\end{aligned}$$

$\mathrm{Ans} = \mathrm{fail}$ より

$pp(\lambda x.xx) = \mathrm{fail}$

定理より、 $\vdash \ \lambda x.xx : A$ となる型 A は存在しない。

Def (decidable)

$x_1, \cdots, x_n$ に関する性質 $P(x_1, \cdots, x_n)$ が decidable とは、アルゴリズム $f(x_1, \cdots, x_n)$ があって任意の $x_1, \cdots, x_n$ にていて、次が成り立つことである。

(i) $P(x_1, \cdots, x_n)$ が成立する $\iff f(x_1, \cdots, x_n) = 1$

(ii) $P(x_1, \cdots, x_n)$ が成立しない $\iff f(x_1, \cdots, x_n) = 0$

第4章　MLの型理論

型理論はプログラミング言語の設計に役立つ。

4.1　プログラミング言語ML

特徴　型付ラムダ計算に基づいて作られた。

- 実用的
- 型検査
- 型推論
- 多相型　$\forall\alpha.A$

構文　α を型変数とすると、型、変数、整数、式は次のように定義される。また、ML のプログラムとは式のことである。

型	A	:=	$\alpha \mid \mathrm{int} \mid \mathrm{bool} \mid A \to A$
変数	x		
整数	n	:=	$\cdots \mid \tilde{}1 \mid 0 \mid 1 \mid 2 \mid \cdots$
式	t	:=	$x \mid \mathrm{fn}\ x \to t \mid tt \mid n \mid \mathrm{true} \mid \mathrm{false} \mid$
			$\mathrm{if}\ t\ \mathrm{then}\ t\ \mathrm{else}\ t \mid \mathrm{let\ val}\ x = t\ \mathrm{in}\ t\ \mathrm{end} \mid$
			$t = t \mid t > t \mid t + t \mid t - t \mid t * t \mid t\ \mathrm{div}\ t$

意味

型	int	整数の型 (例) 0:int, 1:int
	bool	論理値の型 (例) true:bool, false:bool
	$A \to B$	関数型
式	$\mathrm{fn}\ x \to t$	$\lambda x.t$ のこと
	$t_1 t_2$	適用 $t_1 t_2$
	$\cdots, \tilde{}1, 0, 1, 2, \cdots$	整数 $\cdots, -1, 0, 1, 2, \cdots$
	true, false	論理値の真、偽
	if t_1 then t_2 else t_3	t_1 が真なら t_2 の値をとり、偽なら t_3 の値をとる
	let val $x = t_1$ in t_2 end	x を t とおいて、t_2 を計算した値が全体の値
	$t_1 = t_2, t_3 > t_4$	整数の等号、不等号
	$t_1 + t_2, t_3 - t_2 \cdots$	加減乗算

Th .

(1) Γ, t, A に関する性質 $\Gamma \ \vdash \ t : A$ は decidable

(2) t に関する性質" ある Γ, A があって、$\Gamma \ \vdash \ t : A$ は decidable

Proof

(1) アルゴリズム $f(\Gamma, t, A)$ を次のように定めればよい。

- (a) $pp(t) = \mathrm{fail}$ なら、$f(\Gamma, t, A) = 0$
- (b) $pp(t) = (\Pi, B)$ なら、
  - (i) 型代入 σ があって、$\Gamma \supset \Pi^\sigma, A = B^\sigma$ となるなら、
    $f(\Gamma, t, A) = 1$
  - (ii) そのような σ がないなら、
    $f(\Gamma, t, A) = 0$

(2) アルゴリズム $f(t)$ を次のように定めればよい。

$$f(t) = \begin{cases} 1 & \text{if } pp(t) = (\Pi, B) \\ 0 & \text{if } pp(t) = \ \text{fail} \end{cases}$$

(Remark)

(1) 判定 $\Gamma \ \vdash \ t : A$ が与えられたとき、それが証明できるかどうかは機械的に判定可能である

(2) 多くの型理論ではそうなっている

(3) λ 式 t が与えられたとき、それが型付けできるかどうかは機械的に判定可能である

一般的に型推論に期待する性質として以下があげられる。

(i) 最も一般的な型を推論してほしい (主型)

(ii) 一般的な方を 2 ヵ所以上の場所においても、異なる型に具体化して使用したい (多相型 $\forall\alpha.A$)

ML はこの性質をもつ。

主型の推論　ML では型推論で主型を推論する。

(例) (`fn x => x`) `true` の型は次のようにして推論される。

1) (`fn x => x`) : 主型 $\alpha \to \alpha$ を推論

2) `bool` : bool を推論

3) (`fn x => x`) `true` : $\alpha = \text{bool}$ を推論

4) (`fn x => x`) : bool $\to$ bool を推論

5) (`fn x => x`) `true` : bool を推論

多相型

```
 e  ≡  let val comp = fn f => fn g => fn x => f(g x) in
       let val add1 = fn x => x + 1 in
       let val neg  = fn x => if x then false else true in
           comp¹ neg neg ((comp² add1 add1 3) = 5)
       end end end
```

`comp`^{1},`comp`^{2} は次のように型付けされる。

`comp`^{1} : `(bool -> bool) -> (bool -> bool) -> bool -> bool`

`comp`^{2} : `(int -> int) -> (int -> int) -> int -> int`

もし、`let val x = t1 in t2 end` は (`fn x => t2`) `t1` と同じ型付けと仮定すると、`e` は型を持たなくなる。ML は `comp` の主型を

$(\alpha \to \beta) \to (\beta \to \gamma) \to \alpha \to \gamma$

`comp` の型を

$\forall\alpha\beta\gamma.(\alpha \to \beta) \to (\beta \to \gamma) \to \alpha \to \gamma$

と推論する

多相型 $\forall\alpha.A$　(α **: 型変数,** A **: 型**)

$f : \forall\alpha : A$ なら、同一プログラム中に f が 2 ヵ所出てくるとき、B_1, B_2 を型として、1 ヶ所では $f\ :\ A[\alpha\ :=\ B_1]$ として型付けし、もう 1 ヶ所では $f : A[\alpha := B_2]$ と型付けできる。

ML では上のような多相型が使えが、そのために以前定義した型付けの意味に次のような変更を付け加える。

- 型付けの直感的意味の修正
  `let val x = t1 in t2 end`
  　`t1` : A_1 かつ
  　A_1 の自由な型変数を $\alpha_1, \cdots, \alpha_n$ とするとき、
  　　$x : \forall\alpha_1.\forall\alpha_2.\cdots.\forall\alpha_n.A_1$ なら `t2` : A
  が成立するならば、上の式は A と型付けされる

- 型付けの直感的意味の追加
  t が $\forall\alpha : A$ と型付けされるならば、t は $A[\alpha := B]$ と型付けされる

(例)

(1) `let val f = fn x => x in f(f) end` は $\alpha \to \alpha$ と型付けされる

(2) `(fn f => f(f))(fn x => x)` は型を持たない

4.2　ML の型理論

以下、変数 $x, y, z, \cdots,$ 型変数 $\alpha, \beta, \gamma, \cdots$ が与えられているとする。

Def (ML の型理論の型)

ML の型	A	$::=$	$\alpha \mid \mathrm{int} \mid \mathrm{bool} \mid A \to A$
ML の型理論の型	σ	$::=$	$A \mid \forall\alpha.\sigma$

(例)

$\mathrm{int} \to \alpha \to (\mathrm{int} \to \alpha \to \alpha) \to \alpha$	ML の型
$\forall\alpha.(\mathrm{int} \to \alpha \to (\mathrm{int} \to \alpha \to \alpha) \to \alpha)$	ML の型理論の型
$(\forall\alpha \to \alpha) \to (\forall\beta \to \beta)$	ML の型理論の型ではない

(記法)　$\forall\alpha_1\alpha_2\cdots\alpha_n.A \equiv \forall\alpha_1.\forall\alpha_2.\cdots.\forall\alpha_n.A$ と略記する。
また、$\forall\alpha$ より $\to$ の方が結合力が強いものとする。

$$\forall\alpha.\alpha \to \beta \equiv \forall\alpha.(\alpha \to \beta)$$

Def (ML の型理論の項)

項は ML のプログラム

Def (ML の型理論の判定)

$n \geq 0,\ x_1, \cdots, x_n$: 変数, $A_1, \cdots, A_n$: ML の型理論の型, t : 項, A : ML の型とするとき、$x_1 : A_1, \cdots, x_n : A_n \ \vdash \ t : A$ が判定である。

Def (ML の型理論の推論規則)

以下では Γ は文脈、$A, B_1, \cdots, B_n, B$: ML の型, $\alpha_1, \cdots, \alpha_n$: 型変数, f, a, t, t_1, t_2, t_3 : 項とする。

- (ASS) $\Gamma \ \vdash \ x : A[\alpha_1 := B_1, \cdots, \alpha_n := B_n]$ 但し、$\Gamma(x) = \forall\alpha_1\cdots\alpha_n.A$

- (Basic)
  $\Gamma \ \vdash \ n : \mathrm{int}$

$$\Gamma \;\vdash\; \text{true}:\ \text{bool}$$

$$\Gamma \;\vdash\; \text{false}:\ \text{bool}$$

$$\frac{\Gamma \;\vdash\; t_1:\ \text{int} \quad \Gamma \;\vdash\; t_2:\ \text{int}}{\Gamma \;\vdash\; t_1+t_2:\ \text{int}}$$ (演算 $-, *$,div の場合も同じ)

$$\frac{\Gamma \;\vdash\; t_1:\ \text{int} \quad \Gamma \;\vdash\; t_2:\ \text{int}}{\Gamma \;\vdash\; t_1=t_2:\ \text{bool}}$$ (演算 $<$ の場合も同じ)

- $(\to I)$ $\dfrac{\Gamma, x:A \;\vdash\; t:B}{\Gamma \;\vdash\; \text{fn } x \Rightarrow t : A \to B}$

- $(\to E)$ $\dfrac{\Gamma \;\vdash\; f:A\to B \quad \Gamma \;\vdash\; a:A}{\Gamma \;\vdash\; fa:B}$

- (If) $\dfrac{\Gamma \;\vdash\; t_1:\text{bool} \quad \Gamma \;\vdash\; t_2:A \quad \Gamma \;\vdash\; t_3:A}{\Gamma \;\vdash\; \text{if } t_1 \text{ then } t_2 \text{ else } t_3 : A}$

- (Let) $\dfrac{\Gamma \;\vdash\; t_1:A \quad \Gamma, x:\forall\overrightarrow{\alpha}.A \;\vdash\; t_2:B}{\Gamma \;\vdash\; \text{let val } x = t_1 \text{ in } t_2 \text{ end } : B}$
  但し、$\overrightarrow{\alpha} = FV(A) - FV(\Gamma)$
  すなわち、$\overrightarrow{\alpha} = \{\alpha_1, \cdots, \alpha_n\}$ と表されるとすると、
  $\overrightarrow{\alpha}.A = \forall\alpha_1\cdots\alpha_n.A$

(意味)　文脈は最右の変数宣言を使う。

- (ASS) $x:\forall\alpha_1\cdots\alpha_n.A$ が変数宣言に入っていたら、任意の型 $B_1,\cdots,B_n$ について $x:A[\alpha_1:=B_1,\cdots,\alpha_n:=B_n]$ と型付けしてもよい

- (Let) $t_1:A$ なら Γ に現れない A の型変数 $\alpha_1,\cdots,\alpha_n$ について、$\forall\alpha_1\cdots\alpha_n.A$ を考えて、“x がこの型をもつなら $t_2:B$” ならば、let 文全体は B の型をもつ

ML の型理論の証明と ML の型理論の判定の証明可能性は今までと同様に可能である。そして判定が証明できるとき、$\Gamma \;\vdash_{ML}\; t:A$ と表す。($\Gamma \;\vdash\; t:A$ と略記することもある)

(例)

(1)　$\vdash_{ML}$　let val $f = $ fn $x \Rightarrow x$ in $f(f)$ end $: \alpha\to\alpha$

$$\dfrac{\dfrac{\dfrac{}{x:\alpha \;\vdash\; x:\alpha}}{\vdash\; \text{fn } x\Rightarrow x : \alpha\to\alpha} \quad \begin{array}{c}\vdots P_1\\ f:\forall\alpha.\alpha\to\alpha \;\vdash\; f(f):\alpha\to\alpha\end{array}}{\vdash\; \text{let val } f = \text{ fn } x\Rightarrow x \text{ in } f(f) \text{ end } : \alpha\to\alpha}\,(\text{Let})$$

$P_1 \equiv$

$$\dfrac{\dfrac{}{f:\forall\alpha.\alpha\to\alpha \;\vdash\; f:(\alpha\to\alpha)\to\alpha\to\alpha} \quad \dfrac{}{f:\forall\alpha.\alpha\to\alpha \;\vdash\; f:\alpha\to\alpha}}{f:\forall\alpha.\alpha\to\alpha \;\vdash\; f(f):\alpha\to\alpha}$$

(2)　$\vdash_{ML}$　(fn $f \Rightarrow f(f)$)(fn $x \Rightarrow x$) : A となる A はない
上記が成立すると仮定すると、B を ML の型とおくと上の判定の証明は次のようにならなくてはならない。

$$\dfrac{\dfrac{\dfrac{\dfrac{B = X \to A}{f : B \ \vdash \ f : X \to A} \quad \dfrac{B = X}{F : B \ \vdash \ f : X}}{f : B \ \vdash \ f(f) : A}}{\vdash \ \text{fn } f \Rightarrow f(f) : B \to A} \qquad \dfrac{\vdots}{\vdash \ \text{fn } x \Rightarrow x : B}}{\vdash \ (\text{fn } f \Rightarrow f(f))(\text{fn } x \Rightarrow x) : A}$$

$B = X \to A,\ B = X$ より上の証明は成立しない。

(3) $e \equiv \cdots$ comp $= \cdots$ (前の例) については、$\vdash_{ML}$　e : bool

4.3　型推論アルゴリズム

ML のプログラムが与えられたとき、その型を推論するアルゴリズムを示し、それが正しいことを証明する。

Def (準備)

- Types　　ML の型
- 1 : TypeVars $\to$ Types
  $1(\alpha) = \alpha$　　(α : 型変数)
- 型代入 σ
  $\{A_1, \cdots, A_n\}^\sigma = \{A_1^\sigma, \cdots, A_n^\sigma\}$
- $\mathrm{Dom}(\sigma) = \{\ \alpha \mid \sigma(\alpha) \neq \alpha\}$
- $\mathrm{Range}(\sigma) = \sigma(\mathrm{Dom}(\sigma))$
- $\mathrm{Dom}(x_1 : A_1, \cdots, x_n : A_n) = \{x_1, \cdots, x_n\}$

Def ($\sigma|_V$)

σ : 型代入、$V \subset$ TypeVars とすると

$$(\sigma|_V)(\alpha) = \begin{cases} \sigma(\alpha) & (\alpha \in V) \\ \alpha & (\alpha \notin V) \end{cases}$$

Def (Typing (Γ, t))

Typing(Γ, t) は型代入と型のペア (σ, A) か fail を返す次のような関数と定義し、Typing$(\Gamma, t) = (\sigma, A)$ なら、Γ^σ　$\vdash$　$t : A$ となると定める。

- $\text{Typing}(\Gamma, x) = \begin{cases} \text{fail} & \text{if } x \notin \text{Dom}(\Gamma) \\ (1, A[\overrightarrow{\alpha} := \overrightarrow{\beta}]) & \text{if } \Gamma(x) = \forall\overrightarrow{\alpha}.A \\ & \overrightarrow{\beta} : \text{fresh type variable}, A : \text{ML の型} \end{cases}$

- $\text{Typing}(\Gamma, \text{fn } x \Rightarrow t) = (\sigma_1|_{FV(\Gamma)}, \alpha^{\sigma_1} \to A_1)$
  $\text{Typing}((\Gamma, x : \alpha), t) = (\sigma_1, A_1) \qquad \alpha : \text{fresh}$

- $\text{Typing}(\Gamma, fa) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3)|_{FV(\Gamma)}, \alpha^{\sigma_3})$
  $\text{Typing}(\Gamma, f) = (\sigma_1, A_1)$
  $\text{Typing}(\Gamma^{\sigma_1}, a) = (\sigma_2, A_2)$
  $\text{Unify}(A_1^{\sigma_2}, A_2 \to \alpha) = \sigma_3 \qquad \alpha : \text{fresh}$

- $\text{Typing}(\Gamma, \text{if } t_1 \text{ then } t_2 \text{ else } t_3) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \sigma_5)|_{FV(\Gamma)}, A_3^{\sigma_4 \circ \sigma_5})$
  $\text{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$
  $\text{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$
  $\text{Typing}(\Gamma^{\sigma_1 \circ \sigma_2}, t_3) = (\sigma_3, A_3)$
  $\text{Unify}(A_1^{\sigma_2 \circ \sigma_3}, \text{ bool}) = \sigma_4$
  $\text{Unify}(A_2^{\sigma_3 \circ \sigma_4}, A_3^{\sigma_4}) = \sigma_5$

- $\text{Typing}(\Gamma, \text{let val } x = t_1 \text{ in } t_2 \text{ end}) = ((\sigma_1 \circ \sigma_2)|_{FV(\Gamma)}, A_2)$
  $\text{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$
  $\text{Typing}((\Gamma^{\sigma_1}, x : \forall\overrightarrow{\alpha}.A_1), t_2) = (\sigma_2, A_2) \qquad \overrightarrow{\alpha} = FV(A_1) - FV(\Gamma^{\sigma_1})$

- $\text{Typing}(\Gamma, t_1 + t_2) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4)|_{FV(\Gamma)}, \text{ int})$
  $\text{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$
  $\text{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$
  $\text{Unify}(A_1^{\sigma_1}, \text{ int}) = \sigma_3$
  $\text{Unify}(A_2^{\sigma_3}, \text{ int}) = \sigma_4$ 　　($-, *,$ div の場合も同様)

- $\text{Typing}(\Gamma, t_1 = t_2) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4)|_{FV(\Gamma)}, \text{ bool})$
  $\text{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$
  $\text{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$
  $\text{Unify}(A_1^{\sigma_1}, \text{ int}) = \sigma_3$
  $\text{Unify}(A_2^{\sigma_3}, \text{ int}) = \sigma_4$ 　　($>$ の場合も同様)

Th .

(1) (τ, B) があって、$\Gamma^\tau \vdash t : B$ なら $\text{Typing}(\Gamma, t) = (\sigma, A)$

(a) $\Gamma^\sigma \vdash t : A$

(b) 任意の (τ_1, B) について、$\Gamma^{\tau_1} \vdash t : B_1$ なら、ρ があって、
$\Gamma^{\sigma \circ \rho} = \Gamma^{\tau_1}, \ A^\rho = B_1$

(Remark)　Typing(Γ, t) は $\lambda_{\rightarrow}$ での $pp(t)$ に近い。
$E(\Gamma, t, A)$, Unify(E) をまとめると、Typing 相当になる。

Lemma

(1) $\Gamma \ \vdash \ t : A$ なら $\Gamma^{\sigma} \ \vdash \ t : A^{\sigma}$

(2) $\Gamma, x : \forall\overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}] \ \vdash \ t : C$
$\overrightarrow{\beta} = FV(A[\overrightarrow{\alpha} := \overrightarrow{B}]) - FV(\Gamma)$
$\overrightarrow{\alpha} = FV(A) - FV(\Gamma)$
なら、$\Gamma, x : \forall\overrightarrow{\alpha}.A \ \vdash \ t : C$

(3) Unify$(E) = \sigma$ なら、Dom(σ), $FV(\mathrm{Range}(\sigma)) \subset FV(E)$

(4) Typing$(\Gamma, t) = (\sigma, A)$ なら、
Dom$(\sigma) \subset FV(\Gamma)$
$FV(\mathrm{Range}(\sigma)), FV(A) \subset FV(\Gamma) +$ FreshVars

Proof [1]

(1) $\Gamma \ \vdash \ t : A$ の証明 P の高さに関する Ind で証明する。最後に使用する推論規則で場合分けを行うと、

- (ASS)
P が $\Gamma \ \vdash \ x : A$ と表せるとき、$A_1, \overrightarrow{B}$: ML の型とすると、
$$\forall\overrightarrow{\alpha}.A_1 \in \Gamma,\ A \equiv A_1[\overrightarrow{\alpha} := \overrightarrow{B}]$$
$\overrightarrow{\alpha}$ の束縛変数の名前換えより、$\overrightarrow{\alpha} \notin \sigma(FV(A_1))$ とできるので、
$$(\forall\overrightarrow{\alpha}.A_1)^{\sigma} = \forall\overrightarrow{\alpha}.A_1^{\sigma}$$
$\forall\overrightarrow{\alpha}.A_1 \in \Gamma$ より、
$$(\forall\overrightarrow{\alpha}.A_1^{\sigma}) \in \Gamma^{\sigma}$$
また、$\overrightarrow{\alpha} \notin \sigma(FV(A_1))$ より、
$$A^{\sigma} = (A_1[\overrightarrow{\alpha} := \overrightarrow{B}])^{\sigma} = (A_1^{\sigma}[\overrightarrow{\alpha} := \overrightarrow{B}^{\sigma}])$$
$$\therefore \Gamma^{\sigma} \ \vdash \ x : A^{\sigma}$$

- $(\rightarrow I)$
P が $\dfrac{\Gamma, x : A \ \vdash \ t : B}{\Gamma \ \vdash \ \mathrm{fn}\ x \Rightarrow t : A \rightarrow B}(\rightarrow I)$ と表せるとき、
IH for t より
$$(\Gamma, x : A)^{\sigma} \ \vdash \ t : B^{\sigma}$$
$(\Gamma, x : A)^{\sigma} = (\Gamma^{\sigma}, x : A^{\sigma})$ より、
$$\frac{\Gamma^{\sigma}, x : A^{\sigma} \ \vdash \ t : B^{\sigma}}{\Gamma^{\sigma} \ \vdash \ \mathrm{fn}\ x \Rightarrow t : A^{\sigma} \rightarrow B^{\sigma}}(\rightarrow I)$$

[1] (3),(4) の証明は省略

$(A \to B)^\sigma = A^\sigma \to B^\sigma$ より、次の証明が成立する。

$$\frac{\Gamma^\sigma, x : A^\sigma \quad \vdash \quad t : B^\sigma}{\Gamma^\sigma \quad \vdash \quad \text{fn } x \Rightarrow t : (A \to B)^\sigma}(\to I)$$

- $(\to E)$, (If), (Basic)
  上と同様に証明可能。

- (Let)
  $$\frac{\Gamma \quad \vdash \quad t_1 : A \quad \Gamma, x : \forall \overrightarrow{\alpha}.A \quad \vdash \quad t_2 : B}{\Gamma \quad \vdash \quad \text{let val } x = t_1 \text{ in } t_2 \text{ end } : B}(\text{Let})$$ と表せるとき、
  IH for t_1 より
  $$\Gamma^\sigma \quad \vdash \quad t_1 : A^\sigma$$
  IH for t_2 より
  $$(\Gamma, x : \forall \overrightarrow{\alpha}.A)^\sigma \quad \vdash \quad t_2 : B^\sigma$$
  $\overrightarrow{\alpha}$ の束縛変数の名前換えより、
  $$\Gamma^\sigma, x : \forall \overrightarrow{\alpha}.A^\sigma \quad \vdash \quad t_2 : B^\sigma$$
  $$\begin{aligned}\overrightarrow{\alpha} &= FV(A) - FV(\Gamma) \\ &= FV(A^\sigma) - FV(\Gamma^\sigma)\end{aligned}$$
  よって、(Let) の推論規則より、次の証明が成立する。
  $$\frac{\Gamma^\sigma \quad \vdash \quad t_1 : A^\sigma \quad \Gamma^\sigma, x : \forall \overrightarrow{\alpha}.A^\sigma \quad \vdash \quad t_2 : B^\sigma}{\Gamma^\sigma \quad \vdash \quad \text{let val } x = t_1 \text{ in } t_2 \text{ end } : B^\sigma}(\text{Let})$$

(2) $\Gamma \quad \vdash \quad t : A$ の証明 P の高さに関する Ind で証明する。最後に使用する推論規則で場合分けを行うと、

- (ASS)
  (i) $\Gamma, x : \forall \overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}] \quad \vdash \quad x : A[\overrightarrow{\alpha} := \overrightarrow{B}][\overrightarrow{\beta} := \overrightarrow{D}]$ で導出されるとき、
  $\overrightarrow{\beta} = \beta_1\beta_2 \cdots \beta_n$ とおくと、$FV(A) - \overrightarrow{\alpha} \subseteq FV(\Gamma)$ より、
  $$\beta_i \notin FV(A) - \overrightarrow{\alpha}$$
  よって、$C = A[\overrightarrow{\alpha} := \overrightarrow{B}][\overrightarrow{\beta} := \overrightarrow{D}] = A[\overrightarrow{\alpha} := \overrightarrow{B}[\overrightarrow{\beta} := \overrightarrow{D}]]$
  また、$\Gamma, x : \forall \overrightarrow{\alpha}.A \quad \vdash \quad x : A[\overrightarrow{\alpha} := \overrightarrow{B}[\overrightarrow{\beta} := \overrightarrow{D}]]$ より、
  $$\Gamma, x : \forall \overrightarrow{\alpha}.A \quad \vdash \quad x : C$$
  (ii) $\Gamma, x : \forall \overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}] \quad \vdash \quad y : D[\overrightarrow{\gamma} := \overrightarrow{E}]$,
  $$(x \not\equiv y), \quad (y : \forall \overrightarrow{\gamma}.D) \in \Gamma$$
  で導出されるとき、明らかに次が成立する $(C = D[\overrightarrow{\gamma} := \overrightarrow{E}])$
  $$\Gamma, x : \forall \overrightarrow{\alpha}.A \quad \vdash \quad y : D[\overrightarrow{\gamma} := \overrightarrow{E}]$$

- $(\to I)$
  $$\frac{\Gamma, x : \forall \overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}], y : D \quad \vdash \quad t : E}{\Gamma, x : \forall \overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}] \quad \vdash \quad \text{fn } y \Rightarrow t : D \to E}(\to I)$$
  で導出されるとき、束縛変数 $\overrightarrow{\alpha}, \overrightarrow{\beta}$ の名前換えより
  $$\overrightarrow{\alpha}, \overrightarrow{\beta} \notin FV(D)$$
  としてもよい。よって $\overrightarrow{\alpha}, \overrightarrow{\beta}$ について

$\overrightarrow{\beta} = FV(A[\overrightarrow{\alpha} := \overrightarrow{B}]) - FV(\Gamma)$
$= FV(A[\overrightarrow{\alpha} := \overrightarrow{B}]) - FV(\Gamma, y : D)$
$\overrightarrow{\alpha} = FV(A) - FV(\Gamma) = FV(A) - FV(\Gamma, y : D)$

が成立するので、IH より

$\Gamma, x : \forall\overrightarrow{\alpha}.A, y : D \quad \vdash \quad t : E$

が成立し、次の証明が成立する。

$$\frac{\Gamma, x : \forall\overrightarrow{\alpha}.A, y : D \quad \vdash \quad t : E}{\Gamma, x : \forall\overrightarrow{\alpha}.A \quad \vdash \quad \text{fn } y \Rightarrow t : D \to E}(\to I)$$

- $(\to E)$, (If), (Basic)
  同様に証明可能。

- (Let)

$$\frac{\begin{matrix}\vdots P_1 \\ \Gamma' \quad \vdash \quad t_1 : D\end{matrix} \quad \begin{matrix}\vdots P_2 \\ \Gamma', y : \forall\overrightarrow{\gamma}.D \quad \vdash \quad t_2 : E\end{matrix}}{\Gamma' \quad \vdash \quad \text{let val } y = t_1 \text{ in } t_2 \text{ end } : E} \text{(Let)}$$

$\Gamma' = \Gamma, x : \forall\overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}]$
$\overrightarrow{\gamma} = FV(D) - FV(\Gamma')$

で導かれるとき、IH for P_1 より、

$$\Gamma, x : \forall\overrightarrow{\alpha}.A \quad \vdash \quad t_1 : D \tag{A}$$

また、$\overrightarrow{\gamma}$ について、次の式より

$FV(x : \forall\overrightarrow{\beta}.A[\overrightarrow{\alpha} := \overrightarrow{B}])$
$= FV(A[\overrightarrow{\alpha} := \overrightarrow{B}]) - \overrightarrow{\beta}$
$\subseteq \overrightarrow{\beta} + FV(\Gamma) - \overrightarrow{\beta}$
$= FV(\Gamma)$

$\overrightarrow{\gamma} = FV(D) - FV(\Gamma') = FV(D) - FV(\Gamma)$ が成立する。よって、上と同様にして、

$FV(y : \forall\overrightarrow{\gamma}.D) \subseteq FV(\Gamma)$

が成立するので、$\overrightarrow{\alpha}, \overrightarrow{\beta}$ について

$\overrightarrow{\alpha} = FV(A) - FV(\Gamma) = FV(A) - FV(\Gamma, y : \forall\overrightarrow{\gamma}.D)$
$\overrightarrow{\beta} = FV(A[\overrightarrow{\alpha} := \overrightarrow{B}]) - FV(\Gamma)$
$= FV(A[\overrightarrow{\alpha} := \overrightarrow{B}]) - FV(\Gamma, y : \forall\overrightarrow{\gamma}.D)$

が成立する。IH for P_2 より

$$\Gamma, x : \forall\overrightarrow{\alpha}.A, y : \forall\overrightarrow{\gamma}.D \quad \vdash \quad t_2 : E \tag{B}$$

また、上の不等号式と同様にして $FV(y : \forall\overrightarrow{\alpha}.A) \subseteq FV(\Gamma)$ が言え、$\overrightarrow{\gamma} = FV(D) - FV(\Gamma)$ より、

$$\overrightarrow{\gamma} = FV(D) - FV(\Gamma, y : \forall\overrightarrow{\alpha}.A) \tag{C}$$

(A), (B), (C) より、次の証明が成立する。

$$\frac{\Gamma, y : \forall\overrightarrow{\alpha}.A \quad \vdash \quad t_1 : D \quad \Gamma, y : \forall\overrightarrow{\alpha}.A, y : \forall\overrightarrow{\gamma}.D \quad \vdash \quad t_2 : E}{\Gamma, y : \forall\overrightarrow{\alpha}.A \quad \vdash \quad \text{let val } y = t_1 \text{ in } t_2 \text{ end } : E} \text{(Let)}$$

Th .

Γ : 文脈、t : 項とする。

(1) τ, B があって、$\Gamma^\tau \ \vdash \ t : B$ なら、$\mathrm{Typing}(\Gamma, t) = (\sigma, A)$。ただし、

(a) $\Gamma^\sigma \ \vdash \ t : A$

(b) 任意の τ, B について、$\Gamma^\tau \ \vdash \ t : B$ なら ρ があって、
$\Gamma^\tau = \Gamma^{\sigma\circ\rho}, \quad B = A^\rho$

(2) $\Gamma^\tau \ \vdash \ t : B$ となる τ, B がないなら、$\mathrm{Typing}(\Gamma, t) = \mathrm{fail}$

Proof　上の定理を証明するには、次のことが成立すればよい。

(A) $\mathrm{Typing}(\Gamma, t) = (\sigma, A)$ なら、$\Gamma^\sigma \ \vdash \ t : A$

(B) $\Gamma^\tau \ \vdash \ t : B$ なら、
$\mathrm{Typing}(\Gamma, t) = (\sigma, A)$ かつ $\exists\rho \quad \Gamma^{\sigma\circ\rho} = \Gamma^\tau, A^\rho = B$

そのことをまず証明する。

(1) $\Gamma^\tau \ \vdash \ t : B$ が成立すると

(a) (B) より $\mathrm{Typing}(\Gamma, t) = (\sigma, A)$ が成立し、(A) より、$\Gamma^\sigma \ \vdash \ t : A$

(b) (B) より明らか。

(2) $\Gamma^\tau \ \vdash \ t : B$ となる τ, D が存在しない場合を考える。仮に $\mathrm{Typing}(\Gamma, t) \neq \mathrm{fail}$ すなわち $\mathrm{Typing}(\Gamma, t) = (\sigma, A)$ となると仮定すると、(A) より矛盾する。

次に (A), (B) を証明することにする。

(A) t の構造に関する Ind で証明する。

- $t \equiv x$ のとき
  $\mathrm{Typing}(\Gamma, x) = (1, A[\overrightarrow{\alpha} := \overrightarrow{\beta}]), \quad (x : \overrightarrow{\alpha}.A) \in \Gamma$
  と表せ、次の証明が成り立つ。

$$\frac{}{\Gamma^1 \ \vdash \ x : A[\overrightarrow{\alpha} := \overrightarrow{\beta}]}(ASS)$$

- $t \equiv \mathrm{fn}\ x \Rightarrow t_1$ のとき
  $\mathrm{Typing}(\Gamma, \ \mathrm{fn}\ x \Rightarrow t_1) = (\sigma_1|_{FV(\Gamma)}, \alpha^{\sigma_1} \to A_1)$
  $\mathrm{Typing}((\Gamma, x : \alpha), t_1) = (\sigma_1, A_1) \quad (\alpha : \text{ fresh })$
  と表せ、IH for t より
  $(\Gamma, x : \alpha)^{\sigma_1} \ \vdash \ t_1 : A_1$
  また、$(\Gamma, x : \alpha)^{\sigma_1} = \Gamma^{\sigma_1}, x : \alpha^{\sigma_1}$ と $\Gamma^\sigma = \Gamma^{\sigma_1}$ より、次の証明が成立する。

$$\frac{\Gamma^\sigma, x : \alpha^{\sigma_1} \ \vdash \ t_1 : A_1}{\Gamma^\sigma \ \vdash \ \mathrm{fn}x \Rightarrow t_1 : \alpha^{\sigma_1} \to A_1}(\to I)$$

- $t \equiv fa$ のとき

$\mathrm{Typing}(\Gamma, fa) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3)|_{FV(\Gamma)}, \alpha^{\sigma_3})$

$\mathrm{Typing}(\Gamma, f) = (\sigma_1, A_1)$

$\mathrm{Typing}(\Gamma^{\sigma_1}, a) = (\sigma_2, A_2)$

$\mathrm{Unify}(A_1^{\sigma_2}, A_2 \to \alpha) = \sigma_3 \qquad \alpha : \mathrm{fresh}$

と表せる。

i) IH for f より、$\Gamma^{\sigma_1} \quad \vdash \quad f : A_1$

Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3} \quad \vdash \quad f : A_1^{\sigma_2 \circ \sigma_3}$

上の定義より、$\Gamma^{\sigma} \quad \vdash \quad f : A_2^{\sigma_3} \to \alpha^{\sigma_3}$

ii) IH for a より、$\Gamma^{\sigma_1 \circ \sigma_2} \quad \vdash \quad a : A_2$

Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3} \quad \vdash \quad a : A_2^{\sigma_3}$

上の定義より、$\Gamma^{\sigma} \quad \vdash \quad a : A_2^{\sigma_3}$

i), ii) より、次の証明が成り立つ。

$$\frac{\Gamma^{\sigma} \quad \vdash \quad f : A_2^{\sigma_3} \to \alpha^{\sigma_3} \qquad \Gamma^{\sigma} \quad \vdash \quad a : A_2^{\sigma_3}}{\Gamma^{\sigma} \quad \vdash \quad fa : \alpha^{\sigma_3}}(\to E)$$

- $t \equiv \mathrm{if}\ t_1\ \mathrm{then}\ t_2\ \mathrm{else}\ t_3$ のとき

$\mathrm{Typing}(\Gamma, \mathrm{if}\ t_1\ \mathrm{then}\ t_2\ \mathrm{else}\ t_3) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \sigma_5)|_{FV(\Gamma)}, A_3^{\sigma_4 \circ \sigma_5})$

$\mathrm{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$

$\mathrm{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$

$\mathrm{Typing}(\Gamma^{\sigma_1 \circ \sigma_2}, t_3) = (\sigma_3, A_3)$

$\mathrm{Unify}(A_1^{\sigma_2 \circ \sigma_3},\ \mathrm{bool}) = \sigma_4$

$\mathrm{Unify}(A_2^{\sigma_3 \circ \sigma_4}, A_3^{\sigma_4}) = \sigma_5$

と表せる。

i) IH for t_1 より、$\Gamma^{\sigma_1} \quad \vdash \quad t_1 : A_1$

Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \sigma_5} \quad \vdash \quad t_1 : A_1^{\sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \sigma_5}$

上の定義より、$\Gamma^{\sigma} \quad \vdash \quad t_1 :\ \mathrm{bool}$

ii) IH for t_2 より、$\Gamma^{\sigma_1 \circ \sigma_2} \quad \vdash \quad t_2 : A_2$

Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \sigma_5} \quad \vdash \quad t_2 : A_2^{\sigma_3 \circ \sigma_4 \circ \sigma_5}$

上の定義より、$\Gamma^{\sigma} \quad \vdash \quad t_2 : A_3^{\sigma_4 \circ \sigma_5}$

iii) IH for t_3 より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3} \quad \vdash \quad t_3 : A_3$

Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \sigma_5} \quad \vdash \quad t_3 : A_3^{\sigma_4 \circ \sigma_5}$

上の定義より、$\Gamma^{\sigma} \quad \vdash \quad t_3 : A_3^{\sigma_4 \circ \sigma_5}$

i), ii) より、次の証明が成り立つ。

$$\frac{\Gamma^{\sigma} \quad \vdash \quad t_1 :\ \mathrm{bool} \qquad \Gamma^{\sigma} \quad \vdash \quad t_2 : A_3^{\sigma_4 \circ \sigma_5} \qquad \Gamma^{\sigma} \quad \vdash \quad t_3 : A_3^{\sigma_4 \circ \sigma_5}}{\Gamma^{\sigma} \quad \vdash \quad \mathrm{if}\ t_1\ \mathrm{then}\ t_2\ \mathrm{else}\ t_3 : A_3^{\sigma_4 \circ \sigma_5}}(\mathrm{If})$$

- $t \equiv \mathrm{let}\ x = t_1\ \mathrm{in}\ t_2\ \mathrm{end}$ のとき

$\mathrm{Typing}(\Gamma, \mathrm{let}\ x = t_1\ \mathrm{in}\ t_2\ \mathrm{end}) = ((\sigma_1 \circ \sigma_2)|_{FV(\Gamma)}, A_2)$

$\mathrm{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$

$\mathrm{Typing}((\Gamma^{\sigma_1}, x : \forall \overrightarrow{\alpha}.A_1), t_2) = (\sigma_2, A_2)$

$\overrightarrow{\alpha} = FV(A_1) - FV(\Gamma^{\sigma_1})$

と表せる。

i) IH for t_1 より、$\Gamma^{\sigma_1} \ \vdash \ t_1 : A_1$
Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2} \ \vdash \ t_1 : A_1^{\sigma_2}$
上の定義より、$\Gamma^{\sigma} \ \vdash \ t_1 : A_1^{\sigma_2}$

ii) IH for t_2 より、$(\Gamma^{\sigma_1}, x : \forall\overrightarrow{\alpha}.A_1)^{\sigma_2} \ \vdash \ t_2 : A_2$
変数名の付け替えにより、$\overrightarrow{\alpha} \notin \mathrm{Dom}(\sigma_2)$
上の定義より、$\Gamma^{\sigma}, x : \forall\overrightarrow{\alpha}.A_1^{\sigma_2} \ \vdash \ t_2 : A$

iii) 変数名の付け替えにより、$\overrightarrow{\alpha} \notin FV(\mathrm{Range}(\sigma_2))$

$$\begin{aligned}\overrightarrow{\alpha} &= FV(A_1) - FV(\Gamma^{\sigma_1}) \\ &= FV(A_1^{\sigma_2}) - FV(\Gamma^{\sigma_1 \circ \sigma_2}) \\ &= FV(A_1^{\sigma_2}) - FV(\Gamma^{\sigma})\end{aligned}$$

i), ii), iii) より、次の証明が成り立つ。

$$\frac{\Gamma^{\sigma} \ \vdash \ t_1 : A_1^{\sigma_2} \quad \Gamma^{\sigma}, x : \forall\overrightarrow{\alpha}.A_1^{\sigma_2} \ \vdash \ t_2 : A_2}{\Gamma^{\sigma} \ \vdash \ \text{let val } x = t_1 \text{ in } t_2 \text{ end } : A_2}(\text{Let})$$

- $t \equiv t_1 + t_2$ のとき

$\mathrm{Typing}(\Gamma, t_1 + t_2) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4)|_{FV(\Gamma)}, \ \mathrm{int})$
$\mathrm{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$
$\mathrm{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$
$\mathrm{Unify}(A_1^{\sigma_1}, \ \mathrm{int}) = \sigma_3$
$\mathrm{Unify}(A_2^{\sigma_3}, \ \mathrm{int}) = \sigma_4$

i) IH for t_1 より、$\Gamma^{\sigma_1} \ \vdash \ t_1 : A_1$
Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4} \ \vdash \ t_1 : A_1^{\sigma_2 \circ \sigma_3 \circ \sigma_4}$
上の定義より、$\Gamma^{\sigma} \ \vdash \ t_1 : \mathrm{int}$

ii) IH for t_2 より、$\Gamma^{\sigma_1 \circ \sigma_2} \ \vdash \ t_2 : A_2$
Lemma (1) より、$\Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4} \ \vdash \ t_2 : A_2^{\sigma_3 \circ \sigma_4}$
上の定義より、$\Gamma^{\sigma} \ \vdash \ t_2 : \mathrm{int}$

i), ii) より次の証明が成り立つ。

$$\frac{\Gamma^{\sigma} \ \vdash \ t_1 : \ \mathrm{int} \quad \Gamma^{\sigma} \ \vdash \ t_2 : \ \mathrm{int}}{\Gamma^{\sigma} \ \vdash \ t_1 + t_2 : \ \mathrm{int}}(\text{Basic})$$

- t が-, *, div, =, > の形で構成されるとき
+の場合と同様に証明可能。

(B) t の構造に関する Ind で証明する。

- $t \equiv x$ のとき、最後に使用する推論規則は

$$\frac{}{\Gamma^{\tau} \ \vdash \ x : B[\overrightarrow{\alpha} := \overrightarrow{C}]}(ASS)$$

$(x : \forall\overrightarrow{\alpha}.B) \in \Gamma^{\tau} \quad B, \overrightarrow{C}$ は ML の型

と表せる。よって、Typing の定義より

$\mathrm{Typing}(\Gamma, x) = (1, B[\overrightarrow{\alpha} := \overrightarrow{\beta}])$ $\quad \overrightarrow{\beta}$: fresh

となる。型代入 ρ を次のように定義すると

$\overrightarrow{\beta} = \beta_1 \cdots \beta_n \quad \overrightarrow{C} = C_1 \cdots C_n$ とおくと

$$\rho(\gamma) = \begin{cases} C_i & (\text{if } \gamma = \beta_i) \\ \tau(\gamma) & (\text{otherwise}) \end{cases}$$

i) $\Gamma^{1 \circ \rho} = \Gamma^{\rho} = \Gamma^{\tau}$

ii) $(B[\overrightarrow{\alpha} := \overrightarrow{\beta}])^{\rho}$
$= B[\alpha_1 := \rho(\beta_1), \cdots, \alpha_n := \rho(\beta_n)]$
$= B[\overrightarrow{\alpha} := \overrightarrow{C}]$

i), ii) より、証明が成立する。

- $t \equiv \mathrm{fn}\ x \Rightarrow t_1$ のとき、最後に使用する推論規則は

$$\frac{\Gamma^{\tau}, x : A \quad \vdash \quad t_1 : B}{\Gamma^{\tau} \quad \vdash \quad \mathrm{fn}\ x \Rightarrow t_1 : A \to B}(\to I)$$

と表せる。そして、

α : fresh

$$\tau_1(\gamma) = \begin{cases} A & (\text{if } \gamma = \alpha) \\ \tau(\gamma) & (\text{otherwise}) \end{cases}$$

と型代入 τ_1 を定義すると

$(\Gamma, x : \alpha)^{\tau_1} \quad \vdash \quad t_1 : B$

が成立し、IH for t_1 より

$\mathrm{Typing}((\Gamma, x : \alpha), t_1) = (\sigma_1, A_1)$

$\exists \rho_1\ (\Gamma, x : \alpha)^{\sigma_1 \circ \rho_1} = (\Gamma, x : \alpha)^{\tau_1},\ A_1^{\rho_1} = B$

よって、Typing の定義より

$\mathrm{Typing}(\Gamma,\ \mathrm{fn}\ x \Rightarrow t_1) = (\sigma_1|_{FV(\Gamma)}, \alpha^{\sigma_1} \to A_1)$

$\sigma = \sigma_1|_{FV(\Gamma)}$ より、次が成立し

i) $\Gamma^{\sigma \circ \rho_1} = \Gamma^{\sigma_1 \circ \rho_1} = \Gamma^{\tau_1} = \Gamma^{\tau}$

ii) $(\alpha^{\sigma_1} \to A_1)^{\rho_1} = \alpha^{\sigma_1 \circ \rho_1} \to A_1^{\rho_1} = \alpha^{\tau_1} \to B = A \to B$

i), ii) から証明が成立する。

- $t \equiv fa$ のとき、最後に使用する推論規則は

$$\frac{\Gamma^{\tau} \quad \vdash \quad f : A \to B \quad \Gamma^{\tau} \quad \vdash \quad a : A}{\Gamma^{\tau} \quad \vdash \quad fa : B}(\to E)$$

と表せる。IH for f より、

$\mathrm{Typing}(\Gamma, f) = (\sigma_1, A_1)$

$\exists \rho_1\ \Gamma^{\sigma_1 \circ \rho_1} = \Gamma^{\tau},\ A_1^{\rho_1} = A \to B$

$\Gamma^{\sigma_1 \circ \rho_1} = \Gamma^{\tau}$ より $(\Gamma^{\sigma_1})^{\rho_1} \quad \vdash \quad a : A$ が成立し、IH for a より、

$\mathrm{Typing}(\Gamma^{\sigma_1}, a) = (\sigma_2, A_2)$

$\exists \rho_2\ \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2} = \Gamma^{\sigma_1 \circ \rho_1},\ A_2^{\rho_2} = A$

よって、ρ_3 を次のように定義すると、

α : fresh

$$V_1 = FV(A_1) - FV(\Gamma^{\sigma_1})$$
$$\rho_3(\gamma) = \begin{cases} B & (\text{if } \gamma = \alpha) \\ \rho_1(\gamma) & (\text{if } \gamma \in V_1) \\ \rho_2(\gamma) & (\text{otherwise}) \end{cases}$$

i) $\gamma \in V_1$ のとき、$\mathrm{Dom}(\sigma_2) \subset FV(\Gamma^{\sigma_1})$ より、$\gamma^{\sigma_2 \circ \rho_3} = \gamma^{\rho_3} = \gamma^{\rho_1}$

$\therefore \sigma_2 \circ \rho_3 =_{V_1} \rho_1$

ii) $\Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_3} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2} = \Gamma^{\sigma_1 \circ \rho_1}$

$\therefore \sigma_2 \circ \rho_3 =_{FV(\Gamma^{\rho_1})} \rho_1$

i),ii) より、$\sigma_2 \circ \rho_3 =_{FV(A_1)} \rho_1$ が成立するので

$A_1^{\sigma_2 \circ \rho_3} = A_1^{\rho_1} = A \to B$

また、Lemma. (4) より、

$(A_2 \to \alpha)^{\rho_3} = A_2^{\rho_3} \to \alpha^{\rho_3} = A_2^{\rho_2} \to B = A \to B$

上記の二式より、$A_1^{\sigma_2 \circ \rho_3} = (A_2 \to \alpha)^{\rho_3}$ が成立し、定理より

$\mathrm{Unify}(A_1^{\sigma_2}, A_2 \to \alpha) = \sigma_3$

$\exists \rho\ \sigma_3 \circ \rho = \rho_3$

よって、Typing の定義より

$\mathrm{Typing}(\Gamma, fa) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3)|_{FV(\Gamma)}, \alpha^{\sigma_3})$

が成立し、次の i), ii) より証明が成立する。

i) $\Gamma^{\sigma \circ \rho} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \rho} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_3} = \Gamma^{\sigma_1 \circ \rho_1} = \Gamma^{\tau}$

ii) $(\alpha^{\sigma_3})^{\rho} = \alpha^{\rho_3} = B$

- $t \equiv$ if t_1 then t_2 else t_3 のとき、最後に使用する推論規則は

$$\frac{\Gamma^{\tau} \vdash t_1 : \mathrm{bool} \quad \Gamma^{\tau} \vdash t_2 : A \quad \Gamma^{\tau} \vdash t_3 : A}{\Gamma^{\tau} \vdash \text{if } t_1 \text{ then } t_2 \text{ else } t_3 : A}(\mathrm{If})$$

と表せる。IH for t_1 より

$\mathrm{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$

$\exists \rho_1\ \Gamma^{\sigma_1 \circ \rho_1} = \Gamma^{\tau},\ A_1^{\rho_1} = \mathrm{bool}$

$\Gamma^{\sigma_1 \circ \rho_1} = \Gamma^{\tau}$ より $\Gamma^{\sigma_1 \circ \rho_1} \vdash t_2 : A$ が成立し、IH for t_2 より、

$\mathrm{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$

$\exists \rho_2\ \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2} = \Gamma^{\sigma_1 \circ \rho_1},\ A_2^{\rho_2} = A$

$\Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2} = \Gamma^{\tau}$ より $\Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2} \vdash t_3 : A$ が成立し、IH for t_3 より、

$\mathrm{Typing}(\Gamma^{\sigma_1 \circ \sigma_2}, t_3) = (\sigma_3, A_3)$

$\exists \rho_3\ \Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \rho_3} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2},\ A_3^{\rho_3} = A$

よって、ρ_4 を次のように定義すると、

$$V_1 = FV(A_1) - FV(\Gamma^{\sigma_1})$$
$$\rho_4(\gamma) = \begin{cases} \rho_1(\gamma) & (\text{if } \gamma \in V_1) \\ \rho_3(\gamma) & (\text{otherwise}) \end{cases}$$

i) $\gamma \in V_1$ のとき、Lemma. (4) より、$\gamma^{\sigma_2 \circ \sigma_3 \circ \rho_4} = \gamma^{\rho_4} = \gamma^{\rho_1}$

$\therefore \sigma_2 \circ \rho_3 \circ \rho_4 =_{V_1} \rho_1$

ii) $\Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\rho_4} = \Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\rho_3} = \Gamma^{\sigma_1\circ\rho_1}$

$\therefore \sigma_2 \circ \rho_3 \circ \rho_4 =_{FV(\Gamma^{\rho_1})} \rho_1$

i),ii) より、$\sigma_2 \circ \sigma_3 \circ \rho_4 =_{FV(A_1)} \rho_1$ が成立するので

$A_1^{\sigma_2\circ\sigma_3\circ\rho_4} = A_1^{\rho_1} = \mathrm{bool}$

それゆえ、定理より

$\mathrm{Unify}(A_1^{\sigma_2\circ\sigma_3}, \mathrm{bool}) = \sigma_4$

$\exists\rho_5\ \sigma_4 \circ \rho_5 = \rho_4$

また上と同様に、ρ_5 を次のように定義すると、

$V_2 = FV(A_2) - FV(\Gamma^{\sigma_1\circ\sigma_2})$

$$\rho_5(\gamma) = \begin{cases} \rho_2(\gamma) & (\text{if } \gamma \in V_2) \\ \rho_5(\gamma) & (\text{otherwise}) \end{cases}$$

i) $\gamma \in V_2$ のとき、Lemma. (4) より、$\gamma^{\sigma_3\circ\sigma_4\circ\rho_6} = \gamma^{\rho_6} = \gamma^{\rho_2}$

ii) $\Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4\circ\rho_6} = \Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4\circ\rho_5} = \Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\rho_4} = \Gamma^{\sigma_1\circ\sigma_2\circ\rho_2}$

$\therefore \sigma_3 \circ \sigma_4 \circ \rho_6 =_{FV(\Gamma^{\sigma_1\circ\sigma_2})} \rho_2$

i),ii) より、$\sigma_3 \circ \sigma_4 \circ \rho_6 =_{FV(A_2)} \rho_2$ が成立するので

$(A_2^{\sigma_3\circ\sigma_4})^{\rho_6} = A_2^{\rho_2} = A$ また、Lemma. (4) より、

$(A_3^{\sigma_4})^{\rho_6} = A_3^{\sigma_4\circ\rho_5} = A_3^{\rho_4} = A_3^{\rho_3} = A$

上記の二式より、$(A_2^{\sigma_3\circ\sigma_4})^{\rho_6} = (A_3^{\sigma_4})^{\rho_6}$ が成立し、定理より

$\mathrm{Unify}(A_2^{\sigma_3\circ\sigma_4}, A_3^{\sigma_4}) = \sigma_5$

$\exists\rho\ \sigma_5 \circ \rho = \rho_6$

よって、Typing の定義より

$\mathrm{Typing}(\Gamma, \mathrm{if}\, t_1\ \mathrm{then}\, t_2\ \mathrm{else}\, t_3) = ((\sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4\circ\sigma_5)|_{FV(\Gamma)}, A_3^{\sigma_4\circ\sigma_5})$

が成立し、次の i), ii) より証明が成立する。

i) $\Gamma^{\sigma\circ\rho} = \Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4\circ\sigma_5\circ\rho} = \Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4\circ\rho_6}$

$= \Gamma^{\sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4\circ\rho_5} = \Gamma^{\tau}$

ii) $(A_3^{\sigma_4\circ\sigma_5})^{\rho} = A_3^{\sigma_4\circ\rho_6} = A$

- $t \equiv \mathrm{let\ val}\ x = t_1\ \mathrm{in}\ t_2\ \mathrm{end}$ のとき、最後に使用する推論規則は

$$\frac{\Gamma^{\tau}\ \vdash\ t_1 : A \quad \Gamma^{\tau}, x : \forall\overrightarrow{\beta}.A\ \vdash\ t_2 : B}{\Gamma^{\tau}\ \vdash\ \mathrm{let\ val}\ x = t_1\ \mathrm{in}\ t_2\ \mathrm{end}\ : B}(\mathrm{Let})$$

と表せる。IH for t_1 より

$\mathrm{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$

$\exists\rho_1\ \Gamma^{\sigma_1\circ\rho_1} = \Gamma^{\tau}, A_1^{\rho_1} = A$

$\overrightarrow{\alpha} = FV(A_1) - FV(\Gamma^{\sigma_1})$ とおくと、$\overrightarrow{\alpha}$ の名前換えより、$\overrightarrow{\alpha} \notin FV(\mathrm{Range}(\rho_1))$ としてもよい。$\overrightarrow{\alpha} = \alpha_1 \cdots \alpha_n$ とおき、ρ_2 を次のように定義すると、

$$\rho_2(\gamma) = \begin{cases} \gamma & (\text{if } \gamma = \alpha_i) \\ \rho_1(\gamma) & (\text{otherwise}) \end{cases}$$

$\overrightarrow{\alpha} \notin FV(\mathrm{Range}(\rho_1))$, $A = A_1^{\rho_1}$, $\Gamma^{\tau} = \Gamma^{\sigma_1\circ\rho_1}$ より、

$A = A_1^{\rho_2}[\overrightarrow{\alpha} := \rho_1(\overrightarrow{\alpha})]$

$\Gamma^{\tau} = \Gamma^{\sigma_1\circ\rho_2}$

$\Gamma^{\tau}, x : \forall\overrightarrow{\beta}.A \quad \vdash \quad t_2 : B$ より、

$$\Gamma^{\sigma_1\circ\rho_2}, x : \forall\overrightarrow{\beta}.A_1^{\rho_2}[\overrightarrow{\alpha} := \rho_1(\overrightarrow{\alpha})] \quad \vdash \quad t_2 : B$$
$$\overrightarrow{\beta} = FV(A_1^{\rho_2}[\overrightarrow{\alpha} := \rho_1(\overrightarrow{\alpha})]) - FV(\Gamma^{\sigma_1\circ\rho_2})$$

$\overrightarrow{\alpha} = FV(A_1) - FV(\Gamma^{\sigma_1})$ と、ρ_2 の定義より、

$$\overrightarrow{\alpha} = FV(A_1^{\rho_2}) - FV(\Gamma^{\sigma_1\circ\rho_2})$$

Lemma. (2) より、

$$\Gamma^{\sigma_1\circ\rho_2}, x : \forall\overrightarrow{\alpha}.A_1^{\rho_2} \quad \vdash \quad t_2 : B$$

$\overrightarrow{\alpha} \notin FV(\mathrm{Range}(\rho_1))$ と ρ_2 の定義より、$\forall\overrightarrow{\alpha}.A_1^{\rho_2} = (\forall\overrightarrow{\alpha}.A_1)^{\rho_2}$ が成立するので、

$$(\Gamma^{\sigma_1}, x : \forall\overrightarrow{\alpha}.A_1)^{\rho_2} \quad \vdash \quad t_2 : B$$

IH for t_2 より、

$$\mathrm{Typing}((\Gamma^{\sigma_1}, x : \forall\overrightarrow{\alpha}.A_1), t_2) = (\sigma_2, A_2)$$
$$\exists\rho\ (\Gamma^{\sigma_1}, x : \forall\overrightarrow{\alpha}.A_1)^{\sigma_2\circ\rho} = (\Gamma^{\sigma_1}, x : \forall\overrightarrow{\alpha}.A_1)^{\rho_2}, A_2^{\rho} = B$$

よって、Typing の定義より

$$\mathrm{Typing}(\Gamma, \text{let val } x = t_1 \text{ in } t_2 \text{ end}) = ((\sigma_1 \circ \sigma_2)|_{FV(\Gamma)}, A_2)$$

が成立し、次の i), ii) より証明が成立する。

i) $\Gamma^{\sigma\circ\rho} = \Gamma^{\sigma_1\circ\sigma_2\circ\rho} = \Gamma^{\sigma_1\circ\rho_2} = \Gamma^{\sigma_1\circ\rho_1} = \Gamma^{\tau}$

ii) $A_2^{\rho} = B$

- $t \equiv t_1 + t_2$ のとき、最後に使用する推論規則は

$$\frac{\Gamma^{\tau} \quad \vdash \quad t_1 : \mathrm{int} \qquad \Gamma^{\tau} \quad \vdash \quad t_2 : \mathrm{int}}{\Gamma^{\tau} \quad \vdash \quad t_1 + t_2 : \mathrm{int}}(\mathrm{Basic})$$

と表せる。IH for t_1 より

$$\mathrm{Typing}(\Gamma, t_1) = (\sigma_1, A_1)$$
$$\exists\rho_1\ \Gamma^{\sigma_1\circ\rho_1} = \Gamma^{\tau}, A_1^{\rho_1} = \mathrm{int}$$

$\Gamma^{\sigma_1\circ\rho_1} = \Gamma^{\tau}$ より、$\Gamma^{\sigma_1\circ\rho_1} \quad \vdash \quad t_2 : \mathrm{int}$ が成立し、IH for t_2 より、

$$\mathrm{Typing}(\Gamma^{\sigma_1}, t_2) = (\sigma_2, A_2)$$
$$\exists\rho_2\ \Gamma^{\sigma_1\circ\sigma_2\circ\rho_2} = \Gamma^{\sigma_1\circ\rho_1}, A_2^{\rho_2} = \mathrm{int}$$

よって、ρ_3 を次のように定義すると、

$$V_1 = FV(A_1) - FV(\Gamma^{\sigma_1})$$
$$\rho_3(\gamma) = \begin{cases} \rho_1(\gamma) & (\text{if } \gamma \in V_1) \\ \rho_2(\gamma) & (\text{otherwise}) \end{cases}$$

i) $\gamma \in V_1$ のとき、Lemma. (4) より、$\gamma^{\sigma_2\circ\rho_3} = \gamma^{\rho_3} = \gamma^{\rho_1}$

$$\therefore \sigma_2 \circ \rho_3 =_{V_1} \rho_1$$

ii) $\Gamma^{\sigma_1\circ\sigma_2\circ\rho_3} = \Gamma^{\sigma_1\circ\sigma_2\circ\rho_2} = \Gamma^{\sigma_1\circ\rho_1}$

$$\therefore \sigma_2 \circ \rho_3 =_{FV(\Gamma^{\sigma_1})} \rho_1$$

i),ii) より、$\sigma_2 \circ \rho_3 =_{FV(A_1)} \rho_1$ が成立するので

$$A_1^{\sigma_2\circ\rho_3} = A_1^{\rho_1} = \mathrm{int}$$

それゆえ、定理より

$$\mathrm{Unify}(A_1^{\sigma_2}, \mathrm{int}) = \sigma_3$$

$\exists \rho_4\ \sigma_3 \circ \rho_4 = \rho_3$

$\gamma \in FV(A_2)$ のとき、$\gamma^{\sigma_3 \circ \rho_4} = \alpha^{\rho_3} = \alpha^{\rho_2}$ より、

$\sigma_3 \circ \rho_4 =_{FV(A_2)} \rho_2$

$\therefore\ A_2^{\sigma_3 \circ \rho_4} = A_2^{\rho_2} = \mathrm{int}$

よって、定理より

$\mathrm{Unify}(A_2^{\sigma_3},\ \mathrm{int}) = \sigma_4$

$\exists \rho\ \sigma_4 \circ \rho = \rho_4$

よって、Typing の定義より

$\mathrm{Typing}(\Gamma, t_1 + t_2) = ((\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4)|_{FV(\Gamma)}, \mathrm{int})$

が成立し、次の i), ii) より証明が成立する。

i) $\Gamma^{\sigma \circ \rho} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 \circ \rho} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \rho_4}$
$= \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_3} = \Gamma^{\sigma_1 \circ \sigma_2 \circ \rho_2} = \Gamma^{\tau}$

ii) $\mathrm{int}^{\rho} = \mathrm{int}$

- t が $-, *, \mathrm{div}, =, <$ で構成されるとき、$t_1 + t_2$ と同様に証明できる。

Corollary　$\Pi \ \vdash\ t : B$ が成立し、Π, B に $\forall$ が出現しないなら、(Γ, A) があって、次が成立する。

(1) $\Gamma \ \vdash\ t : A$

(2) 任意の (Π', B') について、$\Pi' \ \vdash\ t : B'$ が成立し、Π', B' に $\forall$ が出現しないなら、ρ があって、

$A^{\rho} = B'$

$\Gamma^{\rho} \subset \Pi'$

Proof　仮定が成立するとすると

$\Pi \ \vdash\ t : B$

$FV(t) = \{x_1, \cdots, x_n\}$

$\Pi \supset (x_1 : A_1, \cdots, x_n : A_n)$　$A_1, \cdots, A_n$: ML の型

とおけるので、Γ_0, τ を次のように定義すると

$\Gamma_0 = (x_1 : \alpha_1, \cdots, x_n : \alpha_n)$　$\alpha_1, \cdots, \alpha_n$: fresh

$$\tau(\gamma) = \begin{cases} A_i & (\text{if } \gamma = \alpha_i) \\ \gamma & (\text{otherwise}) \end{cases}$$

$\Gamma_0^{\tau} \ \vdash\ t : B$ が成立するので、上の Th より、

$\mathrm{Typing}(\Gamma_0, t) = (\sigma, A_0)$

が成立する。$\Gamma = \Gamma_0^{\sigma}, A = A_0$ とおくと、(1), (2) が証明できることを示す。

(1) Th (1a) より、$\Gamma_0^{\sigma} \ \vdash\ t : A$ が成立する

(2) (2) の仮定が成立するとすると

$\Pi' \ \vdash\ t : B'$

$\Pi' \supset (x_1 : A'_1, \cdots, x_n : A'_n)$

とおけるので、τ' を次のように定義すると

$$\tau'(\gamma) = \begin{cases} A'_i & (\text{if } \gamma = \alpha_i) \\ \gamma & (\text{otherwise}) \end{cases}$$

$\Gamma_0^{\tau'} \quad \vdash \quad t : B'$ が成立するので、Th (1b) より、

$\exists \rho \; \Gamma_0^{\tau'} = \Gamma_0^{\sigma \circ \rho}, B' = A^\rho$

$\Gamma^\rho = \Gamma_0^{\sigma \circ \rho} = \Gamma_0^{\tau'} \subset \Pi'$ より、証明が成立する。

Remark　ML の型理論自体では principal pair の存在は成立しない。

なぜなら、型代入の型を “TypeVars → ML の型理論の型全体” とすると、

$x : \forall \alpha . \alpha \quad \vdash \quad x : \alpha$

$x : \alpha \quad \vdash \quad x : \alpha$

は両方とも型代入による $\leq$ に関して極小であり、principal pair は存在しなくなる。

第 5 章　型理論 F

F は $\forall\alpha.A$ を自然に含むように $\lambda_\rightarrow$ を拡張したもの。

5.1　F の定義

Def (F の型と項)

型変数 : $\alpha, \beta, \cdots,$ 変数 : $x, y, \cdots$ は所与とすると、

型　A　$::= \alpha \mid A \to A \mid \forall\alpha.A$

項　t　$::= x \mid \lambda x : A.t \mid tt \mid \Lambda\alpha.t \mid tA$

記法

$\Lambda\alpha_1 \cdots \alpha_n.t \equiv \Lambda\alpha_1.\Lambda\alpha_2.\cdots.\Lambda\alpha_n.t$

$\forall\alpha_1 \cdots \alpha_n.t \equiv \forall\alpha_1.\forall\alpha_2.\cdots.\forall\alpha_n.t$

$te_1e_2 \cdots e_n \equiv (\cdots((te_1)e_2)\cdots e_n),\quad e_i$: 項または型

ただし、$\forall$ より $\to$ が結合力が強いものとする。

(例)　$\forall\alpha.\alpha \to \alpha \equiv \forall\alpha.(\alpha \to \alpha)$

束縛変数

- $\forall\alpha.A$ では、A 中の自由な型変数 α は、$\forall\alpha$ により束縛される。
- $\lambda x.t$ では、t 中の自由な変数 x は、λx により束縛される。
- $\Lambda\alpha.t$ では、t 中の自由な変数 x は、$\Lambda\alpha$ により束縛される。

(意味)

$t : \forall\alpha.A$	任意の型 B について、$t : A[\alpha := B]$
$\lambda x : A.t$	$\lambda x.t$ と同じ。x の定義域 A が明示されている
$\Lambda\alpha.t$	$f(\alpha) = t$ となる関数 f を意味する
tA	関数 t に型 A を引数として与えたもの $t(A)$

Def (代入)

型 A, B、項 t, a、変数 x、型変数 α について、

$A[\alpha := B]$

$t[x := a]$

$t[\alpha := A]$

により、代入を表す。但し、次の代入条件が成り立つときにだけ代入できるとする。

$A[\alpha := B]$ の代入条件	B 中の自由な型変数が $A[\alpha := B]$ で束縛されないこと
$t[x := a]$ の代入条件	a 中の自由な型変数が $t[x := a]$ で束縛されないこと
	a 中の自由な変数が $t[x := a]$ で束縛されないこと
$t[\alpha := A]$ の代入条件	A 中の自由な型変数が $t[\alpha := A]$ で束縛されないこと

(例)

$(\forall\alpha.\alpha \to \beta)[\beta := \alpha] = \forall\gamma.\gamma \to \alpha$

$(\Lambda\alpha.\lambda x : \alpha.y)[y := \lambda z : \alpha.z] = \Lambda\beta.\lambda x : \beta.\lambda z : \alpha.z$

$(\Lambda\alpha.\lambda x : \alpha \to \beta.x)[\beta := \alpha] = \Lambda\gamma.\lambda x : \gamma \to \alpha.x$

Def (Γ の判定)

$x_1, \cdots, x_n$ を異なる変数、$A_1, \cdots, A_n, A$ を型、t を項とすると、

$x_1 : A_1, \cdots, x_n : A_n \quad \vdash \quad t : A$ が判定

Def (Γ の推論規則)

$$\frac{}{\Gamma \ \vdash \ x : A}(ASS) \quad \text{但し、}(x : A) \in \Gamma$$

$$\frac{\Gamma, x : A \ \vdash \ t : B}{\Gamma \ \vdash \ \lambda x : A.t : A \to B}(\to I)$$

$$\frac{\Gamma \ \vdash \ f : A \to B \quad \Gamma \ \vdash \ a : A}{\Gamma \ \vdash \ fa : B}(\to E)$$

$$\frac{\Gamma \ \vdash \ t : A}{\Gamma \ \vdash \ \Lambda\alpha.t : \forall\alpha.A}(\forall I) \quad \text{但し、}\alpha \notin FV(\Gamma)$$

$$\frac{\Gamma \ \vdash \ t : \forall\alpha.A}{\Gamma \ \vdash \ tB : A[\alpha := B]}(\forall E)$$

判定が証明できるとき、$\Gamma \ \vdash_F \ t : A$ と表す ($\Gamma \ \vdash \ t : A$ と略記可能)

(例)　$\vdash \lambda f:\forall\alpha.\alpha\to\alpha.\Lambda\alpha.f(\alpha\to\alpha)(f\alpha):(\forall\alpha.\alpha\to\alpha)\to\forall\alpha.\alpha\to\alpha$

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{F'\vdash f:\forall\alpha.\alpha\to\alpha}}{F'\vdash f(\alpha\to\alpha):(\alpha\to\alpha)\to\alpha\to\alpha}\quad\dfrac{\overline{F'\vdash f:\forall\alpha.\alpha\to\alpha}}{F'\vdash f\alpha:\alpha\to\alpha}}{F'\vdash f(\alpha\to\alpha)(f\alpha):\alpha\to\alpha}}{f:\forall\alpha.\alpha\to\alpha\vdash\Lambda\alpha.f(\alpha\to\alpha)(f\alpha):\forall\alpha.\alpha\to\alpha}}{\vdash\lambda f:\forall\alpha.\alpha\to\alpha.\Lambda\alpha.f(\alpha\to\alpha)(f\alpha):(\forall\alpha.\alpha\to\alpha)\to\forall\alpha.\alpha\to\alpha}$$

$(F'\equiv f:\forall\alpha.\alpha\to\alpha)$

Def (Γ の項の簡約)

(I) $a\to_\beta b$ を次のように定める。

(1) $(\lambda x:A.b)a\to_\beta b[x:=a]$

(2) $a_1\to_\beta a_2\Rightarrow\lambda x:A.a_1\to_\beta\lambda x:A.a_2$

(3) $a_1\to_\beta a_2\Rightarrow ba_1\to_\beta ba_2$

(4) $a_1\to_\beta a_2\Rightarrow a_1b\to_\beta a_2b$

(5) $a_1\to_\beta a_2\Rightarrow\Lambda\alpha.a_1\to_\beta\Lambda\alpha.a_2$

(6) $a_1\to_\beta a_2\Rightarrow a_1A\to_\beta a_2A$

(II) $a\to_\Lambda b$ を次のように定める

(1) $(\Lambda\alpha.t)A\to_\Lambda t[\alpha:=A]$

(2) $a_1\to_\Lambda a_2\Rightarrow\lambda x:A.a_1\to_\Lambda\lambda x:A.a_2$

(3) $a_1\to_\Lambda a_2\Rightarrow ba_1\to_\Lambda ba_2$

(4) $a_1\to_\Lambda a_2\Rightarrow a_1b\to_\Lambda a_2b$

(5) $a_1\to_\Lambda a_2\Rightarrow\Lambda\alpha.a_1\to_\Lambda\Lambda\alpha.a_2$

(6) $a_1\to_\Lambda a_2\Rightarrow a_1A\to_\Lambda a_2A$

(III) $a\to_{\beta\Lambda} b$ とは、$a\to_\beta b$ かまたは $a\to_\Lambda b$

(IV) $a\twoheadrightarrow_{\beta\Lambda} b$ とは、列 $a_1,\cdots,a_n$ があって、
$a\equiv a_1\to_{\beta\Lambda}a_2\to_{\beta\Lambda}\cdots\to_{\beta\Lambda}a_n\equiv b(n\geq 1)$

5.2　データタイプの表現

一般にプログラミングで用いられる様々なデータタイプが F で表現できる。

論理型 bool

$$\begin{array}{lcl} \text{bool} & \equiv & \forall\alpha.\alpha \to \alpha \to \alpha \\ \text{true} & \equiv & \Lambda\alpha.\lambda x:\alpha.\lambda y:\alpha.x \\ \text{false} & \equiv & \Lambda\alpha.\lambda x:\alpha.\lambda y:\alpha.y \end{array}$$

$\vdash_F$　true : bool ,　$\vdash_F$　false : bool が成立する。なぜなら、

$$\cfrac{\cfrac{\cfrac{\cfrac{}{x:\alpha, y:\alpha \ \vdash \ x:\alpha}(ASS)}{x:\alpha \ \vdash \ \lambda y:\alpha.x:\alpha\to\alpha}(\to I)}{\vdash \ \lambda x:\alpha.\lambda y:\alpha.x:\alpha\to\alpha}(\to I)}{\vdash \ \Lambda\alpha.\lambda x:\alpha.\lambda y:\alpha.x:\forall\alpha.\alpha\to\alpha\to\alpha}(\forall I)$$

また、If は次のように定義できる

$$\text{If} \equiv \Lambda\alpha.\lambda x:\text{bool}\ .\lambda y:\alpha.\lambda z:\alpha.x\alpha yz$$

よって、型は

$$\vdash \ \text{If} : \forall\alpha.\ \text{bool} \to \alpha \to \alpha \to \alpha$$

$$x:\text{bool}\ , y:A, z:A \ \vdash \ \text{If}\ Axyz : A$$

最後の判定は、If x then y else z に相当する。また、If の簡約は次のようになる。

$$\text{If}\ A\ \text{true}\ yz \to_{\beta\Lambda} y$$

$$\text{If}\ A\ \text{false}\ yz \to_{\beta\Lambda} z$$

Prop. 5.1

t nf (Normal Form), $FV(t) = \phi$, $\vdash$ $t : \text{bool}$ なら $t \equiv \text{true}$ または $t \equiv \text{false}$

同様にして、次のものが F で表現できる

ϕ	空の型
A × B	直積型
A + B	直和型
Nat	自然数型
List A	リスト型
$\mu\alpha$.A[α]	再帰型

自然数 Nat

自然数の型

$$\text{Nat} \equiv \forall\alpha.(\alpha\to\alpha)\to\alpha\to\alpha$$

自然数 n を表す F の項 $\overline{n}$

$$\overline{n} \equiv \Lambda\alpha.\lambda f:\alpha\to\alpha.\lambda x:\alpha.f^n x$$

但し　$f^n x \equiv \underbrace{f(f\cdots(f}_{n\text{ 個}}x)\cdots))$

とおくと、$\vdash$　$\overline{n} : \text{Nat}$

- $\mathrm{succ} \equiv \lambda x : \mathrm{Nat}\ .\Lambda\alpha.\lambda y : \alpha \to \alpha.\lambda z : \alpha.y(x\alpha yz)$
  とおくと、
  $\vdash$ succ: Nat $\to$ Nat
  $\mathrm{succ}\ \overline{n} \twoheadrightarrow_{\beta\Lambda} \overline{n+1}$

- $\mathrm{rec} \equiv \Lambda\alpha.\lambda x : \alpha.\lambda y : \mathrm{Nat} \to \alpha \to \alpha.\lambda z : \mathrm{Nat}\ .z\alpha yx$
  とおくと、
  $\vdash$ Rec: $\forall\alpha.\alpha \to (\ \mathrm{Nat} \to \alpha \to \alpha) \to \mathrm{Nat} \to \alpha$
  $x : A, y : \mathrm{Nat} \to A \to A, z : \mathrm{Nat} \quad \vdash \quad \mathrm{Rec}\ Axyz : A$
  $\mathrm{Rec}\ Axy\overline{0} \twoheadrightarrow_{\beta\Lambda} x$
  $\mathrm{Rec}\ Axy\overline{n+1} \twoheadrightarrow_{\beta\Lambda} y\overline{n}(\mathrm{Rec}\ Axy\overline{n})$

Prop. 5.2

$\vdash \quad t : \mathrm{Nat}\ , t$ nf (Normal Form), $Fv(t) = \phi$ なら、n があって $t \equiv \overline{n}$

5.3　F の強正規化性

Th . 2　$\Gamma \ \vdash_F \quad t : A$ なら、t は SN

上の定理を証明するために、関数の定義域に型を明記しない Curry 流に表した F である型理論 F_c[1]でまず証明を行う。

Def (型理論 F_c)

F_c の項	λ 式
F_c の型	F の型と同じ
F_c の判定	$x_1 : A_1, \cdots, x_n : A_n \quad \vdash \quad t : A \quad x_i$ は相異なる
F_c の推論規則	$\lambda_\to$ の 3 つの推論規則 $(ASS), (\to I), (\to E)$ に 次の 2 つ $(\forall I), (\forall E)$ を追加したもの

$$\frac{\Gamma \ \vdash \ t : A}{\Gamma \ \vdash \ t : \forall\alpha.A}(\forall I) \qquad \text{但し、} \alpha \notin FW(\Gamma)$$

$$\frac{\Gamma \ \vdash \ t : \forall\alpha.A}{\Gamma \ \vdash \ t : A[\alpha := B]}(\forall E)$$

(例)　$\vdash_{F_c} \quad (\lambda f.ff)(\lambda x.x) : \forall\alpha.\alpha \to \alpha$

$$P_1 \equiv \cfrac{\cfrac{}{f : \forall\alpha.\alpha \to \alpha \ \vdash \ f : \forall\alpha.\alpha \to \alpha}(ASS)}{f : \forall\alpha.\alpha \to \alpha \ \vdash \ f : (\alpha \to \alpha) \to (\alpha \to \alpha)}(\forall E)$$

$$P_2 \equiv \cfrac{\cfrac{}{f : \forall\alpha.\alpha \to \alpha \ \vdash \ f : \forall\alpha.\alpha \to \alpha}(ASS)}{f : \forall\alpha.\alpha \to \alpha \ \vdash \ f : \alpha \to \alpha}(\forall E)$$

[1] その逆は Church 流

$$P_3 \equiv \dfrac{\dfrac{\dfrac{}{x:\alpha \quad \vdash \quad x:\alpha}(ASS)}{\vdash \quad \lambda x.x:\alpha\to\alpha}(\to I)}{\vdash \quad \lambda x.x:\forall\alpha.\alpha\to\alpha}(\forall I)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{P_1 \quad P_2}{f:\forall\alpha.\alpha\to\alpha \quad \vdash \quad ff:\alpha\to\alpha}(\to E)}{\vdash \quad \lambda f.ff:(\forall\alpha.\alpha\to\alpha)\to\alpha\to\alpha}(\to I) \quad P_3}{\vdash \quad (\lambda f.ff)(\lambda x.x):\alpha\to\alpha}(\to E)}{\vdash \quad (\lambda f.ff)(\lambda x.x):\forall\alpha.\alpha\to\alpha}(\forall I)$$

Th . 1　$\Gamma \quad \vdash_{F_c} \quad t:A$ なら t SN

Def (SAT)

SAT $= \{X \subset \Lambda \mid X$ sat $\}$

Prop. 5.3

$A \subset$ SAT , $A \neq \phi$ なら、$\cap A$ sat

Proof

(sat1) $A \neq \phi$ より、$A_0 \in A$ となる λ 式の集合 A_0 が存在し、A の定義より、A_0 sat が言える。A_0 (sat1) より、$A_0 \subset$ **SN** が言え、それと $\cap A \subset A_0$ より、$\cap A \subset$ **SN** が言える。

(sat2) x を変数とし、$t_1, \cdots, t_n$ SN とすると、$\forall A_i \in A$ について、A_i sat より、(sat2) を使用すると、

$xt_1 \cdots x_n \in A_i$

A の任意の要素 A_i について、上の式が成立するので、次が成り立つ。

$xt_1 \cdots x_n \in \cap A$

(sat3) a SN, $n \geq 0$, $t_1, \cdots, t_n$ SN, $t[x := a]t_1 \cdots t_n \in \cap A$ と仮定すると、$\forall A_i \in A$ について、

$t[x := a]t_1 \cdots t_n \in A_i$

が成立する。A_i sat より、(sat3) を使用すると、

$(\lambda x.t)at_1 \cdots t_n \in A_i$

が成立するので、

$(\lambda x.t)at_1 \cdots t_n \in \cap A$

Def (環境 ρ)

環境 ρ を次のように定義する。

$$\rho : \begin{array}{ccc} \text{Vars} & \to & \Lambda \\ \text{TypeVars} & \to & \text{SAT} \end{array}$$

$$(\rho[x := t])(y) = \begin{cases} t & \text{if } y \equiv x \\ \rho(y) & \text{otherwise} \end{cases}$$

$$(\rho[\alpha := X])(y) = \begin{cases} X & \text{if } y \equiv \alpha \\ \rho(y) & \text{otherwise} \end{cases}$$

型 A、環境 ρ について $[\![A]\!]_\rho$ を次のように定める。

$$\begin{array}{rcl} [\![\alpha]\!]_\rho & = & \rho(\alpha) \\ [\![A \to B]\!]_\rho & = & [\![A]\!]_\rho \to [\![B]\!]_\rho \\ [\![\forall\alpha.A]\!]_\rho & = & \bigcap_{X \in SAT} [\![A]\!]_{(\rho[\alpha:=X])} \end{array}$$

Prop. 5.4

(1) 型 A、環境 ρ について、$[\![A]\!]_\rho$ sat

(2) $[\![A[\alpha := B]]\!]_\rho = [\![A]\!]_{(\rho[\alpha:=[\![B]\!]_\rho])}$

Proof

(1) 型 A に関する帰納法で証明する。

- $\alpha, A \to B$ のとき
  証明省略。
- $\forall\alpha.A$ のとき、
  $$[\![\forall\alpha.A]\!]_\rho = \bigcap_{X \in SAT} [\![A]\!]_{(\rho[\alpha:=X])}$$
  IH for A より、
  $$[\![A]\!]_{(\rho[\alpha:=X])} \text{ sat}$$
  SN $\in$SAT より、
  $$\text{SAT} \neq \phi$$
  Prop. 5.3 より、次が成立する。
  $$\bigcap_{X \in SAT} [\![A]\!]_{(\rho[\alpha:=X])} \text{ sat}$$

(2) 型 A に関する帰納法で証明可能。

Def (環境 ρ)

- ρ : 環境、t : 項のとき、$[\![t]\!]_\rho$ を次のように定義する。
  $$[\![t]\!]_\rho = t[x_1 := \rho(x_1), \cdots, x_n := \rho(x_n)]$$
  但し、$FV(t) = \{x_1, \cdots, x_n\}$

- $\rho \ \models \ t : A$ とは、$[\![t]\!]_\rho \in [\![A]\!]_\rho$
- $\rho \ \models \ x_1 : A_1, \cdots, x_n : A_n$ とは、$\rho(x_i) \in [\![A_i]\!]_\rho \ (1 \le i \le n)$
- $\Gamma \ \models \ t : A$ とは、任意の環境 ρ について、$\rho \ \models \ \Gamma \Rightarrow \rho \ \models \ t : A$

Prop. 5.5 $\Gamma \ \vdash_{F_c} \ t : A \ \Rightarrow \ \Gamma \ \models \ t : A$

Proof $\Gamma \ \vdash \ t : A$ の証明 P に関する帰納法で証明する。最後に使用した推論規則で場合分けを行うと、

- $(ASS), (\to I), (\to E)$ のとき、
  $\lambda_\to$ のときと同様に証明可能。

- $(\forall I)$ のとき、P は

$$\cfrac{\begin{array}{c}\vdots P_1\\ \Gamma \ \vdash \ t : A\end{array}}{\Gamma \ \vdash \ t : \forall\alpha.A}(\forall I)$$

と表せる。環境 ρ を固定し、$\rho \ \models \ \Gamma$ の仮定の下で、$\rho \ \models \ t : \forall\alpha.A$ を示す。$\alpha \notin FV(\Gamma)$ より、任意の X sat について

$\rho[\alpha := X] \ \models \ \Gamma$

また、IH for P_1 より、

$\Gamma \ \models \ t : A$

よって、$\rho[\alpha := X] \ \models \ t : A$ が成立し、

$[\![t]\!]_{\rho[\alpha:=X]} \in [\![A]\!]_{\rho[\alpha:=X]}$

$[\![t]\!]_{\rho[\alpha:=X]} = [\![t]\!]_\rho$ より、任意の X sat について、

$[\![t]\!]_\rho \in [\![A]\!]_{\rho[\alpha:=X]}$

が成り立つ。よって、

$[\![t]\!]_\rho \in \bigcap_{X \in SAT} [\![A]\!]_{\rho[\alpha:=X]}$

$[\![\forall\alpha.A]\!]_\rho$ の定義とから、次の式が成立する。

$\rho \ \models \ t : \forall\alpha.A$

- $(\forall E)$ のとき、P は

$$\cfrac{\begin{array}{c}\vdots P_1\\ \Gamma \ \vdash \ t : \forall\alpha.A\end{array}}{\Gamma \ \vdash \ t : A[\alpha := B]}(\forall E)$$

と表せる。環境 ρ を固定し、$\rho \ \models \ \Gamma$ の仮定の下で、$\rho \ \models \ t : A[\alpha := B]$ を示す。IH for P_1 より、

$\Gamma \ \models \ t : \forall\alpha.A$

上の仮定 $\rho \ \models \ \Gamma$ とから、$\rho \ \models \ t : \forall\alpha.A$ が成立するので、

$[\![t]\!]_\rho \in \bigcap_{X \in SAT} [\![A]\!]_{\rho[\alpha:=X]}$

Prop. 5.4 の (1) より $[\![B]\!]_\rho$ sat が成り立つので、

$[\![t]\!]_\rho \in [\![A]\!]_{\rho[\alpha:=[\![B]\!]_\rho]}$

Prop. 5.4 の (2) より

$$[\![t]\!]_\rho \in [\![A[\alpha := B]]\!]_\rho$$

$$\therefore \rho \models t : A[\alpha := B]$$

Proof　Theorem. 5.3 の証明を行う。

$\Gamma \vdash_{F_c} t : A$ と Prop. 5.5 より、$\Gamma \models t : A$

環境 ρ を次のように定義すると、

$$\rho(X) = X$$

$$\rho(\alpha) = \mathrm{SN}$$

$\Gamma \equiv x_1 : A_1, \cdots, x_n : A_n$ とおくと、Prop. 5.4 の (1) より、$[\![A_i]\!]_\rho$ sat

(sat2) より、$X_i \in [\![A_i]\!]_\rho$

よって、$\rho \models \Gamma$ が成立するので、$\rho \models t : A$

$$\therefore [\![t]\!]_\rho \in [\![A]\!]_\rho$$

$[\![t]\!]_\rho = t$, $[\![A]\!]_\rho$ sat と (sat1) より

$$t \ \mathrm{SN}$$

第6章　まとめ

1. 単純型理論 $\lambda_{\rightarrow}$
   Th. SR
   Th. SN
   Th. principal pair の存在

2. ML の型理論
   多相型
   型検査、型推論
   Th. 型推論アルゴリズム

3. 型理論 F
   $\forall\alpha.A$
   データタイプの表現
   Th. SN

レポート課題　締め切り：9 月末日

1. 型理論 $\lambda_{\rightarrow}$ において、次の λ 式が型をもつときは、型をひとつ例示して、その型をもつことを証明せよ。また、型をもたないときは型をもたないことを証明せよ。

   (1) $Y \equiv \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$

   (2) $X_0 \equiv \lambda x.x(K(K(K(KI))))SK$

   但し、
   $$\begin{array}{rcl} K & \equiv & \lambda xy.x \\ S & \equiv & \lambda xyz.xz(yz) \\ I & \equiv & SKK \end{array}$$

2. 型理論 F において Subject Reduction が成立することを証明せよ。

関連図書

[1] 龍田 真、「型理論」(近代科学社、1992 年)

[2] Editios, S. Abramsky et al, Handbook of Logic in Computer Science Vol 2 (Oxford University Press 1992)

[3] J. Y Girand Proofs and Types (Cambridge University Press 1989)

[4] 大堀 淳、「プログラミング言語の基礎理論」(共立出版 1997 年)