

# Теория типов

Михайлов Максим

29 октября 2021 г.

# Оглавление

<b>Лекция 1</b>	<b>7 сентября</b>	<b>3</b>
1	Лямбда-исчисление . . . . .	3
1.1	Определение . . . . .	3
1.2	Булево исчисление . . . . .	3
1.3	Числа . . . . .	4
1.4	Типизированное лямбда-исчисление . . . . .	5
1.5	Y-комбинатор и противоречивость нетипизированного $\lambda$ -исчисления .	5
<b>Лекция 2</b>	<b>14 сентября</b>	<b>7</b>
2	Формализация $\lambda$ -исчисления . . . . .	7
<b>Лекция 3</b>	<b>21 сентября</b>	<b>11</b>
3	Просто-типизированное $\lambda$ -исчисление . . . . .	11
3.1	Исчисление по Карри . . . . .	12
3.2	Исчисление по Чёрчу . . . . .	13
<b>Лекция 4</b>	<b>28 сентября</b>	<b>14</b>
3.3	Противоречивость нетипизированного $\lambda$ -исчисления . . . . .	14
4	Изоморфизм Карри-Ховарда . . . . .	15
4.1	Импликационный фрагмент ИИВ . . . . .	15
<b>Лекция 5</b>	<b>5 октября</b>	<b>18</b>
5	Алгебраические термы . . . . .	18
5.1	Эквивалентность уравнений и систем . . . . .	19
5.2	Алгоритм унификации . . . . .	20
5.3	Вывод типов в $\lambda_{\rightarrow}$ . . . . .	20
5.3.1	Построение уравнений . . . . .	21
5.3.2	Разрешение системы . . . . .	21
6	Исчисление предикатов второго порядка . . . . .	21
<b>Лекция 6</b>	<b>12 октября</b>	<b>23</b>
7	Абстрактные типы данных . . . . .	23
<b>Лекция 7</b>	<b>19 октября</b>	<b>24</b>
8	Типовая система Хиндли-Милнера . . . . .	24
8.1	Алгоритм $W$ . . . . .	26

# Лекция 1

## 7 сентября

### 1 Лямбда-исчисление

То, чем мы будем заниматься, можно назвать прикладной матлогикой.

В рамках курса матлогики мы рукомахательно рассмотрели изоморфизм Карри-Ховарда, в этом курсе мы его формализуем. Мы затронем систему типов Хиндли-Милнера (*Haskell*) и язык Arend, основанный на гомотопической теории типов.

#### 1.1 Определение

В 20-30х годах XX века Алонзо Чёрчем была создана альтернатива теории множеств как основе математики — лямбда-исчисление. Основная идея — выбросить из языка все, кроме вызова функций.

В лямбда исчислении есть три конструкции:

- Функция (*абстракция*):  $(\lambda x. A)$
- Применение функции (*аппликация*):  $(A B)$
- Переменная (*атом*):  $x$

Большими буквами начала латинского алфавита мы будем обозначать термы, малыми буквам конца — переменные.  $\lambda$  жадная, как  $\forall$  и  $\exists$  в исчислении предикатов. Аппликация идёт слева направо, т.е.  $\lambda p. p F T = \lambda p. ((p F) T)$

Вычисление происходит с помощью  $\beta$ -редукции, его мы определим позже, общее понимание у нас есть из вводной лекции функционального программирования.

#### 1.2 Булево исчисление

Определим булево исчисление в  $\lambda$ -исчислении:

- $T := \lambda x. \lambda y. x$  — истина
- $F := \lambda x. \lambda y. y$  — ложь
- $\text{Not} := \lambda p. p \ F \ T$

$$\begin{aligned} \text{Not } F &\rightarrow_{\beta} \\ ((\lambda x. \lambda y. y) \ F) \ T &\rightarrow_{\beta} \\ (\lambda y. y) \ T &\rightarrow_{\beta} T \end{aligned}$$

- $\text{And} := \lambda a. \lambda b. a \ b \ F$

And берёт свой второй аргумент, если первый аргумент истина и ложь иначе.

And использует идею **карринга** — функция от 2 аргументов есть функция от первого аргумента, возвращающая другую функцию от второго аргумента.<sup>1</sup> Например, в выражении “((+) 2) 3” ((+) 2) это функция, которая прибавляет к своему аргументу 2.

### 1.3 Числа

Числа в лямбда-исчислении кодируются **нумералами Чёрча**. Это только один из способов кодировки, есть и другие. Общая идея — число  $n$  применяет данную функцию к данному аргументу  $n$  раз.

- $0 = \lambda f. \lambda x. x$
- $1 = \lambda f. \lambda x. f \ x$
- $3 = \lambda f. \lambda x. f \ (f \ (f \ x))$
- $\overline{n+1} = \lambda f. \lambda x. f \ (\overline{n} \ f \ x)$
- $(+1) = \lambda n. \lambda f. \lambda x. n \ f \ (f \ x)$  — функция инкремента.
- $(+) = \lambda a. \lambda b. b \ ((+) \ \overline{1}) \ a$ :  $b$  раз прибавляет единицу к  $a$ .
- $(\cdot) = \lambda a. \lambda b. a \ ((+) \ b) \ \overline{0}$ :  $a$  раз прибавляет  $b$  к 0.

Ходят легенды, что Клини изобрел декремент у зубного врача под действием наркоза. Существует много способов определить декремент различных степеней упоротости.

Рассмотрим декремент, основанный на следующей идее: пусть есть упорядоченная пара  $\langle a, b \rangle$  и функция  $(*) : \langle a, b \rangle \mapsto \langle b, b+1 \rangle$ . Тогда применив  $(*)$   $n$  раз к  $\langle 0, 0 \rangle$  и взяв первый элемент, возьмём первый элемент пары.

<sup>1</sup> Аналогично для  $n$  аргументов.

Упорядоченная пара определяется следующим способом:

$$\text{MkPair} = \lambda a. \lambda b. (\lambda p. p \ a \ b)$$

Можно потрогать эмулятор лямбда-исчисления lci, будет полезно для домашних заданий.

## 1.4 Типизированное лямбда-исчисление

Лямбда-исчисление для нас будет просто языком программирования. Для начала мы его типизируем, потому что нетипизированное лямбда-исчисление противоречиво.

Пусть у каждого выражения  $A$  есть тип  $\tau$ , что обозначается  $A : \tau$ . Также используется некоторый контекст с переменными и их типами, обозначаемый  $M$ . Все вместе это записывается как  $M \vdash A : \tau$ , что напоминает исчисление предикатов.

## 1.5 $Y$ -комбинатор и противоречивость нетипизированного $\lambda$ -исчисления

Мы хотим, чтобы  $\rightarrow_\beta$  сохраняло значения, т.к. иначе мы вообще не можем говорить о равенстве термов.

**Определение.**  $Y := \lambda f. (\lambda x. f \ (x \ x)) (\lambda x. f \ (x \ x))$  —  $Y$ -комбинатор, для него верно  $Y f \approx f(Y f)$ . Такое свойство называется “быть комбинатором неподвижной точки”, т.е. он находит неподвижную точку функции:  $A$  такое, что  $f(A) = A$ .

Пусть мы добавили бинарную операцию  $(\supset)$  — импликацию с некоторыми аксиомами. Оказывается, что доказуемо любое  $A$ . Мы это докажем на последующих лекциях.

$Y$ -комбинатор полезен тем, что позволяет реализовывать рекурсию.

*Пример.* Запишем факториал в неформальном виде:

$$\text{Fact} = \lambda n. \text{If} \ (\text{IsZero } n) \ \bar{1} \ (\text{Fact } (n - 1) \cdot n)$$

На самом деле  $\text{Fact}$  есть неподвижная точка функции

$$\lambda f. \lambda n. \text{If} \ (\text{IsZero } n) \ \bar{1} \ (f \ (n - 1) \cdot n)$$

по определению неподвижной точки функции. Тогда  $\text{Fact}$  это

$$Y(\lambda f. \lambda n. \text{If} \ (\text{IsZero } n) \ \bar{1} \ (f \ (n - 1) \cdot n))$$

У нас появляется проблема: есть выражения, которым мы не можем приписать значение, например

$$Y(\lambda f. \lambda x. f \ (\text{Not } x))$$

Эта проблема происходит из-за того, что наш язык слишком мощный — мы написали решатель любых уравнений, даже тех, у которых нет решения. Логичный выход из этой ситуации — запретить то, из-за чего у нас возникают проблемы. Как запретить  $Y$ ? Оказывается, это позволяют сделать типы — они будут делить выражения на добропорядочные и недобропорядочные.

# Лекция 2

## 14 сентября

### 2 Формализация $\lambda$ -исчисления

**Определение.** Пред- $\lambda$ -терм определяется индуктивно как одно из:

1.  $x$  — переменная
2.  $(L\ L)$  — применение
3.  $(\lambda x.L)$  — абстракция

Почему пред- $\lambda$ -терм? Мы не хотим различать  $\lambda x.x$  и  $\lambda y.y$ .

**Определение.**  $\alpha$ -эквивалентность — обозначается  $A =_\alpha B$  и выполняется, если<sup>1</sup>:

1.  $A \equiv x, B \equiv x$  — одна и та же переменная
2.  $A \equiv P\ Q, B \equiv R\ S, P =_\alpha R, Q =_\alpha S$
3.  $A \equiv \lambda x.P, B \equiv \lambda y.Q$  и существует  $t$  — новая переменная, такая что  $P[x := t] =_\alpha Q[y := t]$

**Определение.** Свобода для подстановки:  $A[x := B]$ , никакое свободное вхождение переменной в  $B$  не станет связанным.

**Определение** ( $\lambda$ -терм). Множество всех  $\lambda$ -термов это  $\Lambda / =_\alpha$

**Определение** ( $\beta$ -редекс). Выражение вида  $(\lambda x.A)\ B$

**Определение** ( $\beta$ -редукция). Обозначается  $A \rightarrow_\beta B$  и выполняется, если выполняется одно из:

1.  $A \equiv P\ Q, B \equiv R\ S$  и либо  $P \rightarrow_\beta R$  и  $Q =_\alpha S$ , либо  $P =_\alpha R$  и  $Q \rightarrow_\beta S$ .

---

<sup>1</sup> И только если.

2.  $A \equiv \lambda x.P, B \equiv \lambda x.Q$  и  $P \rightarrow_\beta Q$

3.  $A \equiv (\lambda x.P) Q, B \equiv P[x := Q]$  и  $Q$  свободно для подстановки.

**Определение.** Придуман Моисеем Шейнфинкелем.

$I := \lambda x.x$  — Identität<sup>2</sup>

**Определение.**

- $K = \lambda x.\lambda y.x$
- $\Omega = \omega \omega$
- $\omega = \lambda x.x x$

*Пример.*



**Определение.**  $R$  обладает ромбовидным свойством (*diamond*), если для любых  $a, b, c$ , таких что:

1.  $aRb, aRc$
2.  $b \neq c$

существует  $d$ :  $bRd$  и  $cRd$ .



*Пример.*  $>$  на  $\mathbb{Z}$  не ромбовидно: для  $a = 3, b = 2, c = 1$  выполнено условие, но  $\nexists d$ .

$>$  на  $\mathbb{R}$  ромбовидно.

---

<sup>2</sup> Тождество (с немецкого)



**Определение** ( $\beta$ -редуцируемость). Рефлексивное, транзитивное замыкание отношения  $\rightarrow_\beta$ , обозначается  $\rightarrow_\beta^*$ .

**Теорема 1** (Чёрча-Россера).  $\beta$ -редуцируемость обладает ромбовидным свойством.

**Определение.**  $\Rightarrow_\beta$  — параллельная  $\beta$ -редукция, выполняется если:

0.  $A =_\alpha B$
1.  $A \equiv P Q, B \equiv R S$  и  $P \Rightarrow_\beta R$  и  $Q \Rightarrow_\beta S$ .
2. Аналогично  $\beta$ -редукции.
3. Аналогично  $\beta$ -редукции.

**Лемма 1.**  $(\Rightarrow_\beta)$  обладает ромбовидным свойством.

**Лемма 2.** Если  $R$  обладает ромбовидным свойством, то  $R^*$  обладает ромбовидным свойством.

*Доказательство.* Две индукции. □

**Лемма 3.**  $(\Rightarrow_\beta) \subseteq (\rightarrow_\beta)$

*Доказательство теоремы Чёрча-Россера.* Заметим, что:

1.  $(\Rightarrow_\beta)^* \subseteq (\rightarrow_\beta)$  — из леммы
2.  $(\rightarrow_\beta) \subseteq (\Rightarrow_\beta)^*$  — из определения
3. Т.к.  $(\Rightarrow_\beta)^*$  обладает р.с., то и  $(\rightarrow_\beta)$  обладает р.с. □

**Следствие 1.1.** У  $\lambda$ -выражения существует не более одной нормальной формы.

*Доказательство.* Пусть  $A$  имеет две нормальные формы:  $A \rightarrow_\beta B, A \rightarrow_\beta C$  и  $B \neq_\alpha C$ . Тогда есть  $D: B \rightarrow_\beta D$  и  $C \rightarrow_\beta D$ . Противоречие. □

**Определение.** Нормальный порядок редукции — редуцируем самый левый редекс.

**Теорема 2.** Если нормальная форма существует, она может быть получена нормальным порядком редукции.

*Примечание.* Нижеследующее объяснение — с практики.

Рассмотрим  $Y f =_\beta f (Y f) =_\beta f (f (Y f)) =_\beta \dots$ . Можно считать, что у  $f$  сколько угодно аргументов, первый аргумент можно считать указателем на свой рекурсивный вызов.

*Пример.* Числа Фибоначчи:

```
fib a b n =  
  if n = 0 then a  
  else fib b (a + b) (n - 1)
```

Здесь решение уравнения заматано под ковер, в  $\lambda$ -исчислении оно видно:

$$\text{Fib} = \lambda f. \lambda a. \lambda b. \lambda n. (\text{IsZero } n) \ a \ (f \ f \ a \ (a + b) \ (n - 1))$$

Здесь  $f$  передается само себе, чтобы иметь ссылку на себя для рекурсивного вызова.

Для работы Fib нужно дать его самому себе: Fib Fib 1 1 10.

# Лекция 3

## 21 сентября

В  $\lambda$ -исчислении можно сделать:

1. Целые числа, где  $\langle a, b \rangle \leftrightarrow a - b$
2. Рациональные числа в виде дробей
3. Матлогику?

Попытки сделать матлогику всегда приводили к парадоксам.

Оказывается, нельзя относиться к любому выражению как к логическому.

*Обозначение.*  $\supset$  — импликация

*Пример.* Рассмотрим комбинатор  $\Phi_A =_\beta A \supset \Phi_A$ . Это  $Y (\lambda f. \lambda a. a \supset f a)$ .

Добавим аксиому  $(A \supset (A \supset B)) \supset (A \supset B)$ . Если такой аксиомы нет, то теория грустная.

Мы также хотим, чтобы если  $X =_\beta Y$ , то  $X \supset Y$ .

Каким-то образом мы получим парадокс.

## 3 Просто-типизированное $\lambda$ -исчисление

**Определение** (типовые переменные).

- $\alpha, \beta, \gamma$  — атомарные
- $\tau, \sigma$  — составные

2 традиции:

1. Исчисление по Чёрчу

## 2. Исчисление по Карри

Мы сначала рассмотрим исчисление по Карри.

### 3.1 Исчисление по Карри

Типизация:  $\Gamma \vdash A : \tau, \Gamma = \{x_1 : \tau_1, x_2 : \tau_2 \dots\}$

Правила:

1.  $\frac{}{\Gamma, x_1 : \tau_1 \vdash x_1 : \tau_1} \text{Ax.}$
2.  $\frac{\Gamma \vdash A : \sigma \rightarrow \tau \quad \Gamma \vdash B : \sigma}{\Gamma \vdash A B : \tau}$
3.  $\frac{\Gamma, x : \tau \vdash A : \sigma}{\Gamma \vdash \lambda x. A : \tau \rightarrow \sigma}$

Пример.

$$\lambda f^{\alpha \rightarrow \alpha}. \lambda x^{\alpha}. f (f x) : (\alpha \rightarrow \alpha) \rightarrow \alpha \rightarrow \alpha$$

Подгоним доказательство под результат:

$$\frac{\frac{\frac{f : \alpha \rightarrow \alpha \vdash f : \alpha \rightarrow \alpha}{f : \alpha \rightarrow \alpha, x : \alpha \vdash f (f x) : \alpha} \quad \frac{\Gamma \vdash f : \alpha \rightarrow \alpha \quad \Gamma \vdash x : \alpha}{\Gamma \vdash f x : \alpha}}{f : \alpha \rightarrow \alpha \vdash \lambda x. f (f x) : \alpha \rightarrow \alpha}}{\lambda f. \lambda x. f (f x) : (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)}$$

**Теорема 3.** Если  $\Gamma \vdash A : \tau$ , то любое подвыражение имеет тип.

*Доказательство.* По индукции по длине.

База. Это правило 1.

Переход. Пусть любое выражение длиной  $< n$  символов обладает искомым свойством. Покажем искомое для  $A : |A| = n$ . Рассмотрим варианты того, по какому правилу доказана типизируемость  $A$ :

1. Второе правило:  $B$  и  $C$  короче  $A$ , следовательно для них искомое верно.
2. Третье правило: аналогично для  $x, B$

□

**Теорема 4** (Subject reduction, о редукции). Если  $\Gamma \vdash A : \sigma$  и  $A \rightarrow_{\beta} B$ , то  $\Gamma \vdash B : \sigma$

Доказательство. Скучно.

Самая интересная часть: рассмотрим  $A \rightarrow_\beta B$ . Случаи:

1.  $\lambda x.A \rightarrow \lambda x.B$  — индукция
2.  $A B$  — индукция
3.  $(\lambda x.A) B \rightarrow A[x := B]$

По теореме о типизации подвыражений,  $(\lambda x^{\tau \rightarrow \sigma}.A^\sigma) B^\tau : \sigma$ . Кроме того, доказывается  $(A[x := B]) : \sigma$ .

□

**Лемма 4.** Если  $\Gamma, x : \tau \vdash A : \sigma, \Gamma \vdash B : \tau$ , то  $\Gamma \vdash A[x := B] : \sigma$

**Теорема 5 (Чёрча-Россера).** Если  $\Gamma \vdash M : \sigma$  и существуют  $N, P : M \rightarrow_\beta N, M \rightarrow_\beta P$ , то найдется такой  $S$ , что  $\Gamma \vdash S : \sigma$  и  $N \rightarrow_\beta S$  и  $P \rightarrow_\beta S$

## 3.2 Исчисление по Чёрчу

Язык:

- $x$  — переменная
- $A B$  — аппликация
- $\lambda x^\tau.P$  — абстракция

**Обозначение.** Когда нужно различить исчисления, будем писать  $\vdash_{\text{ч}}$  или  $\vdash_{\text{к}}$

**Теорема 6.** Если контекст  $\Gamma$  и выражение  $P$  типизируется, то  $\Gamma \vdash_{\text{ч}} P : \sigma$

*Пример.*

$$\vdash_{\text{к}} \lambda x.x : \alpha \rightarrow \alpha$$

$$\vdash_{\text{к}} \lambda x.x : \beta \rightarrow \beta$$

$$\vdash_{\text{ч}} \lambda x^\sigma.x : \sigma \rightarrow \sigma$$

# Лекция 4

## 28 сентября

### 3.3 Противоречивость нетипизированного $\lambda$ -исчисления

???

1. Логические выражения
2. Запрещенные выражения

$Y$  явно нехорошее выражение.  $\Phi_A =_\beta \Phi_A \supset A$

Добавим очевидные аксиомы:

1.  $A =_\beta B$ , то  $\vdash A \supset B, \vdash B \supset A$ . Почему? Потому что мы хотим, чтобы  $\sin 0 = 0$ , а не только  $\sin 0 \rightarrow 0$
2.  $(A \supset A \supset B) \supset (A \supset B)$
3.  $A, A \supset B$ , тогда  $B$

Тогда заметим, что при любом  $A, \vdash A$ :

$$\begin{array}{l}
 \Phi_A \supset \Phi_A \\
 \Phi_A \supset (\Phi_A \supset A) \\
 (\Phi_A \supset (\Phi_A \supset A)) \supset (\Phi_A \supset \Phi_A) \\
 \Phi_A \supset A \\
 \Phi_A \\
 A
 \end{array}$$

## 4 Изоморфизм Карри-Ховарда

$$\begin{array}{c}
 \frac{}{\Gamma, x : \tau \vdash x : \tau} \quad x \notin \Gamma \qquad \frac{}{\Gamma, \tau \vdash \tau} \\
 \\
 \frac{\Gamma \vdash A : \sigma \rightarrow \tau \quad \Gamma \vdash B : \sigma}{\Gamma \vdash AB : \tau} \qquad \frac{\Gamma \vdash \sigma \rightarrow \tau \quad \Gamma \vdash \sigma}{\Gamma \vdash \tau} \\
 \\
 \frac{\Gamma, x : \sigma \vdash A : \tau}{\Gamma \vdash \lambda x. A : \sigma \rightarrow \tau} \quad x \notin \Gamma \qquad \frac{\Gamma, \sigma \vdash \tau}{\Gamma \vdash \sigma \rightarrow \tau}
 \end{array}$$

**Теорема 7** (об изоморфизме Карри-Ховарда).

1.  $\Gamma \vdash_{\lambda \rightarrow} A : \tau$ , то  $|\Gamma| \vdash_{\rightarrow} \tau$
2. Если  $\Delta \vdash_{\rightarrow} \tau$ , то найдутся  $\Gamma, A : |\Gamma| = \Delta, \Gamma \vdash A : \tau$

**Определение.**

$$|\Gamma| := \{\tau \mid x : \tau \in \Gamma\}$$

### 4.1 Импликационный фрагмент ИИВ

У нас есть только импликация.

Есть три правила:  $I_{\rightarrow}, E_{\rightarrow}, A\lambda$ . Будет ли у нас всё работать? Утверждается, что да.

*Обозначение.* Доказуемость в И.Ф. ИИВ будем обозначать  $\Gamma \vdash_{\rightarrow} \tau$

**Определение** (язык И.Ф. ИИВ).

$$\tau ::= \alpha \mid (\tau \rightarrow \tau)$$

**Теорема 8.** Импликационный фрагмент ИИВ замкнут относительно доказуемости: Если  $\Gamma \vdash \tau$  и  $\tau$  содержит только пропозиционные переменные и импликацию, то  $\Gamma \vdash_{\rightarrow} \tau$ . Обратное очевидно верно.

*Доказательство.* Рассмотрим  $\Gamma^*$  — множество формул, замкнутых по доказуемости.

$$\tau \in \Gamma^* \Leftrightarrow \Gamma^* \vdash \tau$$

*Обозначение.*  $\Gamma$  — множество формул, тогда  $\Gamma^*$  — замыкание этого множества по доказуемости, а  $\Gamma^{\rightarrow^*}$  — замыкание по доказуемости в ИФИИВ.

Рассмотрим множество миров:  $\Gamma^{\rightarrow^*} \preceq \Delta^{\rightarrow^*}$ , если  $\Gamma^{\rightarrow^*} \subseteq \Delta^{\rightarrow^*}$ ,  $\Delta^{\rightarrow^*}$  — замкн.,  $\Gamma^* \Vdash \tau$ , если  $\tau \in \Gamma^*$

*Утверждение.*  $\Gamma^*$  образует модель Крипке.

**Определение** (модель Крипке).

1. Множество миров, упорядоченных отношением  $\preceq$
2.  $\Vdash$  такое, что если  $\Gamma \Vdash \alpha$ , то  $\Gamma \preceq \Delta$ , то  $\Delta \Vdash \alpha$ .

Тогда  $\Gamma \Vdash \tau \rightarrow \sigma$  тогда и только тогда, когда в любом  $\Gamma \preceq \Delta$  из  $\Delta \Vdash \tau$ , следует  $\Delta \Vdash \sigma$ .

*Утверждение.*  $\tau \in \Gamma^{\rightarrow*}$  тогда и только тогда, когда  $\Gamma^{\rightarrow*} \vdash_{\text{и}} \tau$

*Доказательство.* Индукция по структуре  $\tau$ .

База.  $\tau \equiv \alpha$

$$\Rightarrow \alpha \in \Gamma^{\rightarrow*}, \text{ то } \alpha \vdash_{\text{и}} \alpha$$

$$\Leftarrow \alpha \vdash_{\text{и}} \alpha, \text{ тогда очевидно } \alpha \in \Gamma^{\rightarrow*}$$

Переход.  $\tau \equiv \delta \rightarrow \pi$

$$\Rightarrow \sigma \rightarrow \pi \in \Gamma^{\rightarrow*}, \text{ то } \Gamma^{\rightarrow*} \vdash_{\rightarrow} \sigma \rightarrow \pi$$

$$\Leftarrow \Gamma^{\rightarrow*} \vdash_{\text{и}} (\sigma \rightarrow \pi). \text{ Значит, } \Gamma^{\rightarrow*} \Vdash \sigma \rightarrow \pi.$$

□

Рассмотрим  $\Gamma^{\rightarrow*} \preceq \Delta : \Delta \Vdash \sigma$ , то  $\Delta \Vdash \pi$ . Значит,  $\Delta \vdash \sigma$ . Значит,  $\sigma \in \Delta$ , т.е.  $\Delta \vdash_{\rightarrow} \sigma$ . Значит,  $\Delta \vdash_{\rightarrow} \pi$  по М.Р., т.к.  $\Gamma^{\rightarrow*} \Vdash \sigma \rightarrow \pi \Rightarrow \Delta \Vdash \sigma \rightarrow \pi \Rightarrow \Delta \vdash_{\rightarrow} \sigma \rightarrow \pi$

*Утверждение.*  $\Gamma \Vdash \tau \Leftrightarrow \Gamma|_{\rightarrow} \tau$

*Доказательство.*

$$\Rightarrow \Gamma \Vdash \tau.$$

$$1. \Gamma \Vdash \alpha, \text{ т.е. } \alpha \in \Gamma, \text{ т.е. } \alpha \vdash_{\rightarrow} \alpha$$

$$2. \Gamma \Vdash \sigma \rightarrow \pi.$$

Рассмотрим  $\Gamma \preceq \Delta$ , причём  $\Delta \Vdash \sigma$ , тогда  $\Delta \Vdash \pi$ . Т.е. по индукционному предположению  $\Delta \vdash_{\rightarrow} \sigma$ . Пусть  $\Delta = \{\Gamma, \sigma\}^*$ . Тогда  $\Gamma, \sigma \vdash_{\rightarrow} \sigma$ .

Тогда  $\Gamma, \sigma \Vdash \pi$  по индукционному предположению и определению  $\Vdash$ . Тогда  $\Gamma, \sigma \vdash_{\rightarrow} \pi$ , т.е.  $\Gamma \vdash_{\rightarrow} \sigma \rightarrow \pi$

$$\Leftarrow \Gamma \vdash_{\rightarrow} \tau, \text{ тогда } \Gamma \Vdash \tau$$

$$1. \tau \equiv \alpha - \text{очевидно.}$$



2.  $\tau \equiv \sigma \rightarrow \pi$ . Дано, что  $\Gamma_{\rightarrow} \vdash \sigma \rightarrow \pi$ .

Пусть  $\Delta \Vdash \sigma$ .  $\Gamma \preceq \Delta$ . Тогда  $\Delta \vdash_{\rightarrow} \sigma$  по индукционному предположению.  $\Gamma \vdash_{\rightarrow} \sigma \rightarrow \pi$ , т.е.  $\Delta \vdash_{\rightarrow} \sigma \rightarrow \pi$ . По М.Р.  $\Delta \vdash_{\rightarrow} \pi$ . По индукционному предположению  $\Delta \Vdash \pi$ . Т.е.  $\Gamma \Vdash \sigma \rightarrow \pi$ . **В лекции было  $\models$ .**

□

Схема доказательства:

1.  $\tau \in \Gamma^*$ , если  $\Gamma^* \vdash_{\text{и}} \tau$
2.  $\Gamma^* \Vdash \tau$
3.  $\Gamma^* \Vdash \tau$  тогда и только тогда, когда  $\Gamma^* \vdash_{\rightarrow} \tau$

□

Обозначение.  $\lambda_{\rightarrow}$  — типизированное  $\lambda$ -исчисление.

1. Обитаемость:  $\overset{?}{\Gamma} \vdash ? : \tau$  — по изоморфизму Карри-Ховарда и теореме об эквивалентности  $\Gamma \vdash \tau$
2. Вывод (реконструкция):  $\Gamma \vdash A : ?$
3. Проверка:  $\Gamma \vdash A : \tau$

Пункты 2 и 3 это одно и то же.

# Лекция 5

## 5 октября

### 5 Алгебраические термы

Определение (алгебраические термы).

$$T ::= \underbrace{a}_{\text{переменная}} \mid \underbrace{f}_{\substack{\text{функциональный} \\ \text{символ}}} T_1 \dots T_n$$

Функциональные символы  $\in F$ , переменные  $\in T$

Пример.  $f (f_2 a b) c$

**Определение.** Подстановка переменных — отображение  $S_0 : V \rightarrow T$ , являющееся тождественным почти всюду<sup>1</sup>, то есть  $\exists$  фиксированные  $a_1 \dots a_n$ , для которых  $S_0$  не тождественна:  $S_0(a_i) = T_i$ , а для  $b \notin \{a_i\}$   $S_0(b) = b$ .

Тогда можно определить определить подстановку  $S : T \rightarrow T$ :

$$S(f T_1 \dots T_n) = f (S(T_1)) (S(T_2)) \dots (S(T_n))$$

$$S(a) = S_0(a)$$

**Определение.** Рассмотрим уравнение  $T_1 = T_2$ . Его **решение** — такая подстановка  $S$ , что  $S(T_1) \equiv S(T_2)$ , где  $\equiv$  обозначается равенство строк.

Пример.

$$\begin{aligned} f a (g b) &= f (g c) d \\ S_0(a) &= g c \quad S_0(d) = g b \\ S(f a (g b)) &= f (g c) (g b) \end{aligned}$$

<sup>1</sup> Кроме конечного количества.

**Определение** (система уравнений).

$$\begin{cases} T_1 = P_1 \\ T_2 = P_2 \\ \vdots \\ T_n = P_n \end{cases}$$

### 5.1 Эквивалентность уравнений и систем

**Определение.** Две системы  $E_1 : \begin{cases} T_1 = P_1 \\ \vdots \\ T_n = P_n \end{cases}$  и  $E_2 : \begin{cases} T'_1 = P'_1 \\ \vdots \\ T'_n = P'_n \end{cases}$  называются эквивалентными, если любое решение системы  $E_1$  подходит к  $E_2$  и наоборот.

*Утверждение.* Для любой системы существует эквивалентное уравнение.

*Доказательство.* Выберем новый  $n$ -местный функциональный символ  $h$ , построим уравнение  $h T_1 \dots T_n = h P_1 \dots P_n$ .  $\square$

**Определение.**

$$(U \circ T)(P) = U(T(P))$$

**Определение.** Определим порядок на подстановках.  $S \preceq T$ , если  $S$  — частный случай  $T$ , т.е.  $\exists U: S = U \circ T$

**Определение.** Наиболее общим решением уравнения  $T = P$  назовём подстановку  $S$ , такую что  $S(T) = S(P)$  и для любой  $S_1: S_1(T) \equiv S_1(P)$  выполнено  $S_1 \preceq S$

**Теорема 9.** У уравнения в алгебраических термах  $T = P$  всегда есть наиболее общее решение, если есть хоть какое-то.

**Определение.** Несовместная система — система с уравнениями вида  $f T_1 \dots T_n = g P_1 \dots P_k$ , где  $f \not\equiv g$ , либо  $x = \dots x \dots$

В OCaml и Haskell это называется “occurs check”.

**Определение.** Система в разрешённой форме — система вида  $\begin{cases} a_1 = T_1 \\ \vdots \\ a_n = T_n \end{cases}$ , где:

1. Все  $a_i$  различны
2.  $T_i$  не содержит  $a_j$  для  $i \neq j$

Альтернативное определение — каждый  $a_i$  входит по одному разу.

## 5.2 Алгоритм унификации

Рассмотрим систему  $\begin{cases} T_1 = P_1 \\ \vdots \\ T_n = P_n \end{cases}$

Применяем одно из следующих:

1.  $x = x$  — отбрасываем.
2.  $T = x$ , где  $T \neq x$ , тогда заменяем на  $x = T$

$$3. \begin{cases} x = P \\ \vdots \\ T_2 = P_2 \\ \vdots \\ T_n = P_n \end{cases} \Rightarrow \begin{cases} T_2[x := P] = P_2[x := P] \\ \vdots \\ T_n[x := P] = P_n[x := P] \\ x = P \end{cases}$$

$$4. f T_1 \dots T_n = f P_1 \dots P_n \Rightarrow \begin{cases} T_1 = P_1 \\ \vdots \\ T_n = P_n \end{cases}$$

**Теорема 10.** Применяя шаги алгоритма унификации, за конечное время можно получить систему либо в разрешенной форме, либо несовместную.

*Доказательство.* Рассмотрим тройку  $\left\langle \begin{matrix} \text{количество} \\ \text{неразрешенных} \\ \text{переменных} \end{matrix}, \begin{matrix} \text{максимальная} \\ \text{сложность} \\ \text{слева} \end{matrix}, \begin{matrix} \text{количество} \\ \text{уравнений} \\ \text{максимальной} \\ \text{сложности} \\ \text{слева} \end{matrix} \right\rangle$ . Сложность — вложенность.

1. Применения правил уменьшают тройку.
2.  $\langle 0, 0, t \rangle$  — система в разрешенной форме.
3. Количество применений правил конечно, т.к. каждая из троек  $\in \omega^3$  и любая последовательность убывающих ординалов конечна.

□

## 5.3 Вывод типов в $\lambda_{\rightarrow}$

$(\rightarrow)$  — 2-местный функциональный символ.

Проведём индукцию по структуре  $\lambda$ -выражения. Результатом разбора будет пара  $\langle \text{система}, \text{тип} \rangle$

### 5.3.1 Построение уравнений

Структура	Комментарий	Система	Тип
$x$	Введём тип $\alpha_x$	$\emptyset$	$\alpha_x$
$A B$	Рекурсивный вызов на $A$ и $B$ даст $\langle E_A, \tau_A \rangle, \langle E_B, \tau_B \rangle$ . Вводим $\beta$ — новый тип.	$E_A, E_B, \tau_B \rightarrow \beta = \tau_A$	$\beta$
$\lambda x.A$	Рекурсивный вызов на $A$ даст $\langle E_A, \tau_A \rangle$ . Берём тип для $x : \alpha_x$ .	$E_A$	$\alpha_x \rightarrow \tau_A$

Несложно заметить, что эти правила соответствуют правилом вывода в типизированном  $\lambda$ -исчислении.

### 5.3.2 Разрешение системы

Это унификация.

*Пример.* Разберём  $B = \lambda x. \overbrace{x}^A$ .

- $E_A = \emptyset, \tau_A = \alpha_x$
- $E_B = \emptyset, \tau_B = \alpha_x \rightarrow \alpha_x$

Разрешим систему уравнений  $\tau_A, \tau_B$ . Оказывается, эта система уже в разрешенной форме. Таким образом,  $\vdash \lambda x.x : \alpha \rightarrow \alpha$ . Контекст пустой, т.к. свободных переменных нет ( $E_A, E_B = \emptyset$ ).

**Определение.** Терм называется **слабо-нормализуемым**, если существует последовательность  $\beta$ -редукций, приводящих его в нормальную форму.

**Определение.** Терм называется **сильно-нормализуемым**, если не существует бесконечной последовательности  $\beta$ -редукций, нигде не приводящая его в нормальную форму.

*Пример.*  $K I \Omega$  — слабо нормализуемый, но не сильно нормализуемый

**Теорема 11.**  $\lambda_{\rightarrow}$  сильно нормализуемо.

*Примечание.* Это сильно ограничивает выразительность  $\lambda_{\rightarrow}$ .

## 6 Исчисление предикатов второго порядка

Второй порядок — это когда переменные есть предикаты.

**Определение (предикат).**

$$\Phi_{\Pi} ::= p \mid \Phi_{\Pi} \cup \Phi_{\Pi} \mid \Phi_{\Pi} \& \Phi_{\Pi} \mid \Phi_{\Pi} \rightarrow \Phi_{\Pi} \mid \forall p. \Phi_{\Pi} \mid \exists p. \Phi_{\Pi}$$

*Утверждение.* Можно выразить:

$$a \& b ::= \forall p. (a \rightarrow b \rightarrow p) \rightarrow p$$

$$a \vee b ::= \forall p. (a \rightarrow p) \rightarrow (b \rightarrow p) \rightarrow p$$

$$\perp ::= \forall p. p$$

$$\exists p. A ::= \forall x. (\forall p. p \rightarrow x) \rightarrow x$$

Это исчисление также называется “Система F”, оно же  $L_2$ .

$$L_2 ::= x \mid \lambda x^\alpha. A \mid P Q \mid P \tau \mid \lambda \alpha. A$$

# Лекция 6

## 12 октября

### 7 Абстрактные типы данных

ООП = АДТ + наследование.

Пример (стек).

$\text{push} : \alpha \rightarrow \alpha \text{ stack} \rightarrow \alpha \text{ stack}$

$\text{pop} : \alpha \text{ stack} \rightarrow (\alpha \cdot \alpha \text{ stack})$

$\text{empty} : \alpha \text{ stack}$

Что мы понимаем под  $\exists \alpha. \varphi$ ?  $\varphi$  — интерфейс и существует где-то в природе тип, который этому интерфейсу соответствует.

Для стека:

$$\exists \alpha. \underbrace{(\eta \rightarrow \alpha \rightarrow \alpha)}_{\text{push}} \& \underbrace{(\alpha \rightarrow \alpha \& \eta)}_{\text{pop}} \& \underbrace{\eta}_{\text{empty}}$$

Правила вывода:

$$\frac{\Gamma \vdash \varphi[x := \theta]}{\exists x. \varphi}$$

$$\frac{\Gamma, \psi \vdash \varphi \quad \Gamma \vdash \exists x. \psi}{\Gamma \vdash \varphi} \quad x \notin \text{FV}(\Gamma)$$

$$\frac{\Gamma \vdash M : \sigma[\alpha := \tau]}{\Gamma \vdash \text{pack } \tau, M \text{ to } \exists \alpha. \sigma : \exists \alpha. \sigma}$$

TBD.

# Лекция 7

## 19 октября

### 8 Типовая система Хиндли-Милнера

Мы рассмотрели две системы типов:

1. Просто типизированное лямбда исчисление: недостаточно выразительно
2. Система F: местами выразительна, местами недостаточно. Кроме того, потеряна разрешимость.

Ограничим излишнюю свободу системы F.

**Определение (ранг типа).** Пусть  $\sigma$  — тип без кванторов.  $R \subset \text{тип} \times \mathbb{N}_0$ , такое что:

1.  $R(\sigma, 0)$
2. Если  $R(\tau, k)$ , то  $R(\forall \alpha. \tau, \max(k, 1))$
3. Если  $R(\tau_0, k)$  и  $R(\tau_1, k + 1)$ , то  $R(\tau_0 \rightarrow \tau_1, k + 1)$ .

*Пример.*

$$R(\alpha, 0) \Rightarrow R(\alpha, 5) \Rightarrow R(\forall \alpha. \alpha, 5)$$

$$R(\alpha \rightarrow \alpha, 0) \Rightarrow R(\forall \alpha. \alpha \rightarrow \alpha, 1)$$

**Определение (Типовая система Хиндли-Милнера).** Рассмотрим  $\lambda$ -исчисление 2 порядка по Карри.

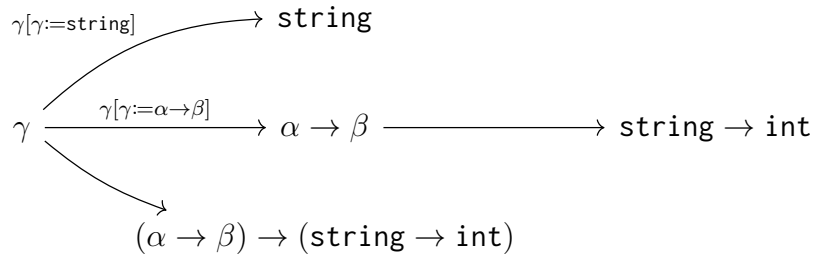
Типы:

1. Типы без кванторов:  $\tau = \alpha \mid (\tau \rightarrow \tau)$
2. Типовые схемы:  $\sigma = \forall \alpha. \sigma \mid \tau$



**Определение** (Отношение “быть частным случаем” (специализация)).  $\sigma_1 \sqsubseteq \sigma_2$  ( $\sigma_2$  — частный случай  $\sigma_1$ ), если  $\sigma_1 \equiv \forall \alpha_1 \dots \forall \alpha_n. \tau_1$ ,  $\sigma_2 \equiv \forall \beta_1 \dots \beta_k. \tau_2[\alpha_1 := \theta_1 \dots \alpha_n := \theta_n]$  и новые  $\beta_1 \dots \beta_k$  не входят свободно в  $\sigma_1$ .

*Пример.*  $\tau \sqsubseteq \text{string}$



*Пример.*

$$\forall \alpha. \alpha \rightarrow \alpha \sqsubseteq \forall \beta. (\beta \rightarrow \beta) \rightarrow (\beta \rightarrow \beta)$$

Правила вывода:

$$\begin{array}{c}
 \frac{}{\Gamma, x : \sigma \vdash x : \sigma} \quad \alpha \notin \text{FV}(\Gamma) \\
 \frac{\Gamma \vdash A : \tau \rightarrow \tau' \quad \Gamma \vdash B : \tau}{\Gamma \vdash A B : \tau'} \\
 \frac{\Gamma, x : \tau \vdash A : \tau'}{\Gamma : \lambda x. A : \tau \rightarrow \tau'} \\
 \frac{\Gamma \vdash A : \sigma \quad \Gamma, x : \sigma \vdash B : \tau}{\Gamma \vdash \text{let } x = A \text{ in } B : \tau} \\
 \frac{\Gamma \vdash A : \sigma' \quad \sigma' \sqsubseteq \sigma}{\Gamma \vdash A : \sigma} \\
 \frac{\Gamma \vdash A : \sigma \quad \alpha \notin \text{FV}(\Gamma)}{\Gamma \vdash A : \forall \alpha. \sigma} \\
 \text{let } x = A \text{ in } B \rightarrow_{\beta} B[x := A]
 \end{array}$$

Казалось бы, `let` похож на  $(\lambda x. B) A$ . Однако, мы разрешаем кванторы в  $A$ .

*Пример.*

$$\begin{array}{l}
 I \equiv \lambda x. x : \forall \alpha. \alpha \rightarrow \alpha \\
 \triangleleft (I \ 1, I \ \text{"a"}) \quad I \ 1 : \text{int}, I \ \text{"a"} : \text{string}
 \end{array}$$

1.

$$\text{let } \underbrace{I = \lambda x. x}_{I : \forall \alpha. \alpha \rightarrow \alpha} \text{ in } (I \ 1, I \ \text{"a"})$$

2. То же самое, но без let:

$$(\lambda i.(i\ 1, i\ "a"))\ (\lambda x.x)$$

В этом варианте тип внутри лямбды без кванторов. В силу этого операцию  $(i\ 1, i\ "a")$  сложно выполнить — нужно угадать, какой тип подставлять.

Эта система очевидно уже, чем System F. Мы её сузили, чтобы получить разрешимость.

## 8.1 Алгоритм $W$

Мы хотим решить  $? \vdash A : ?$ , т.е. найти контекст и тип выражения, притом наиболее общие.

$W(\Gamma, E) \Rightarrow (\tau, S)$  — по контексту и выражению получаем тип и подстановку.

1.  $E \equiv x, x \in \Gamma, x : \sigma_x = \forall \alpha_1 \dots \alpha_n. \tau$ . Тогда введём новые переменные  $\beta_1 \dots \beta_n$  и результатом будет:

$$W(\Gamma, E) = (\forall \beta_1 \dots \beta_n. \tau, \emptyset)$$

2.  $E \equiv \lambda x. P$ . Пусть  $W(\Gamma \cup \{x : \gamma\}, P) = (\tau_P, S_1)$ .

$$W(\Gamma, E) = (S_1(\gamma \rightarrow \tau_P), S_1)$$

3.  $E \equiv P\ Q$ . Введём новый тип  $\gamma$ . Пусть  $\mathcal{U}$  — вызов алгоритма унификации и:

$$W(\Gamma, P) = (\tau_P, S_1) \quad W(S_1\Gamma, Q) = (\tau_Q, S_2) \quad \mathcal{U}(S_2\tau_P, \tau_Q \rightarrow \gamma) = S_3$$

Тогда:

$$W(\Gamma, E) = (S_3\gamma, S_3 \circ S_2 \circ S_1)$$

4.  $E \equiv \text{let } x = P \text{ in } Q$ . Пусть:

$$W(\Gamma, P) = (\tau_P, S_1) \quad W(S_1\Gamma \cup \{x : \forall^1. \tau_f\}, Q) = (S_2, \tau_Q)$$

$$W(\Gamma, E) = (\tau_Q, S_2 \circ S_1)$$

Не дописано

---

<sup>1</sup> Кванторы по всем свободным в  $\tau_f$  переменным.