

# ТЕОРЕТИЧЕСКИЕ (“МАЛЫЕ”) ДОМАШНИЕ ЗАДАНИЯ

Теория типов, ИТМО, М3334-М3339, осень 2019 года

## Домашнее задание №1: «знакомство с лямбда-исчислением»

1. Расставьте скобки:

- (a)  $\lambda x.x x \lambda x.x x$
- (b)  $(\lambda x.x x) \lambda x.x x$
- (c)  $\lambda x.(x x) \lambda x.x x$
- (d)  $\lambda f.\lambda x.f f f x$

2. Проведите бета-редукции и приведите выражения к нормальной форме:

- (a)  $(\lambda a.\lambda b.a) (\lambda a.\lambda b.a) (\lambda a.\lambda b.b)$
- (b)  $(\lambda a.\lambda b.a) b$
- (c)  $(\lambda f.\lambda x.f (f x)) (\lambda f.\lambda x.f (f x))$

3. Выразите следующие функции в лямбда-исчислении:

- (a) Or, Xor;
- (b) тернарная операция в Си ( $?:$ );
- (c) isZero (T, если аргумент равен 0, иначе F);
- (d) isEven (T, если аргумент чётный);
- (e) умножение на 2;
- (f) умножение;
- (g) возведение в степень;
- (h) упорядоченная пара. К паре должны прилагаться три лямбда-выражения  $(M, P_l, P_r)$ : выражение  $M$  по двум значениям строит упорядоченную пару, а выражения  $P_l$  и  $P_r$  возвращают первый и второй элемент упорядоченной пары соответственно.

Убедитесь, что для ваших выражений выполнено

$$P_l (M A B) \rightarrow_\beta \dots \rightarrow_\beta A$$

и

$$P_r (M A B) \rightarrow_\beta \dots \rightarrow_\beta B$$

- (i) вычитание 1;
- (j) вычитание;
- (k) сравнение («меньше»);
- (l) деление.

4. Назовём бета-эквивалентностью транзитивное, рефлексивное и симметричное замыкание отношения бета-редукции, будем записывать его как  $(=_\beta)$ . В частности, бета-эквивалентны те термы, которые имеют одинаковую нормальную форму. Также, нетрудно заметить следующее:

- (a)  $And T F =_\beta F$ ;
- (b)  $\Omega =_\beta \Omega$ ;
- (c)  $(\lambda n.\lambda f.\lambda x.n f (f x)) \bar{n} =_\beta \overline{n+1}$ ;
- (d)  $a \neq_\beta b$ .

Мы будем говорить, что лямбда-выражение  $E$  выражает функцию  $f(x_1, \dots, x_k) : \mathbb{N}_0^k \rightarrow \mathbb{N}_0$ , если при любых  $x_1, \dots, x_k \in \mathbb{N}_0$  выполнено

$$E \overline{x_1} \dots \overline{x_k} =_\beta \overline{f(x_1, \dots, x_k)}$$

Какие функции выражают следующие выражения? Ответ обоснуйте.

- (a)  $\lambda t. \lambda n. n \ t;$
- (b)  $\lambda t. \lambda n. \lambda x. n \ (t \ x).$

5. *Ненормализуемым* назовём лямбда-выражение, не имеющее нормальной формы, то есть выражение, для которого нет конечной последовательности бета-редукций, приводящей к нормальной форме. *Сильно нормализуемым* назовём лямбда-выражение, для которого не существует бесконечной последовательности бета-редукций (любая последовательность бета-редукций неизбежно заканчивается нормальной формой, если её продолжать достаточно долго). *Слабо нормализуемым* назовём лямбда-выражение, которое имеет нормальную форму, но существует бесконечная последовательность бета-редукций, которая не приводит его в нормальную форму. Приведите примеры сильно нормализуемого, слабо нормализуемого и ненормализуемого лямбда-выражения.

## Домашнее задание №2: «теорема Чёрча-Россера, Y-комбинатор»

1. *Полное доказательство теоремы Чёрча-Россера.* На лекции был представлен план доказательства теоремы, в котором необходимо заполнить пустоты.
- (a) Покажите, что отношение бета-редукции — подотношение отношения параллельной бета-редукции. В символической записи,  $(\rightarrow_\beta) \subseteq (\Rightarrow_\beta)$ . То есть, если  $A \rightarrow_\beta B$ , то  $A \Rightarrow_\beta B$ .
  - (b) Покажите, что каковы бы ни были термы  $A, P, Q$  и переменная  $x$ , если выполнено  $P \Rightarrow_\beta Q$ , то  $A[x := P] \Rightarrow_\beta A[x := Q]$ . Убедитесь, что это справедливо и если  $x$  не входит свободно в  $A$ .
  - (c) Покажите, что каковы бы ни были термы  $A, B, P, Q$  и переменная  $x$ , если  $A \Rightarrow_\beta B$  и  $P \Rightarrow_\beta Q$ , то  $A[x := P] \Rightarrow_\beta B[x := Q]$ .
  - (d) Покажите, что  $(\Rightarrow_\beta)$  обладает ромбовидным свойством.
  - (e) *Транзитивным и рефлексивным замыканием* отношения  $R \subseteq U^2$  назовём такое отношение  $R^* \subseteq U^2$ , что  $(x, y) \in R^*$  тогда и только тогда, когда существует  $n \in \mathbb{N}$  и последовательность  $a_1, \dots, a_n \in U$ , что:  $a_1 = x, a_n = y$  и  $(a_i, a_{i+1}) \in R$ .  
Покажите, что если  $R$  — некоторое отношение, обладающее ромбовидным свойством, то  $R^*$  тоже обладает ромбовидным свойством.
  - (f) Покажите, что каковы бы ни были отношения  $R$  и  $S$ , если  $R \subseteq S$ , то  $R^* \subseteq S^*$ . В частности, покажите, что  $(\rightarrow_\beta) \subseteq (\Rightarrow_\beta)^*$ .
  - (g) Покажите, что  $(\Rightarrow_\beta)^* \subseteq (\rightarrow_\beta)$ .

На основании доказанных лемм несложно показать утверждение теоремы Чёрча-Россера: из последних пунктов следует, что  $(\Rightarrow_\beta)^* = (\rightarrow_\beta)$ , а из пункта (d) — что это отношение обладает ромбовидным свойством.

2. Реализуйте следующие функции с помощью Y-комбинатора, вычисляющие:

- (a) факториал числа;
- (b)  $n$ -е простое число;
- (c) функцию Аккермана;
- (d) частичный логарифм.

3. *Отмеченным объединением* множеств  $L \uplus R$  назовём множество пар

$$U = \{\langle 1, x \rangle \mid x \in L\} \cup \{\langle 2, y \rangle \mid y \in R\}$$

Соответственно, для данного множества мы можем определить три функции

название	обозначение	определение
левая инъекция	$in_L : L \rightarrow U$	$in_L(x) = \langle 1, x \rangle$
правая инъекция	$in_R : R \rightarrow U$	$in_R(x) = \langle 2, x \rangle$
выбор	$Case : U \times (L \rightarrow X) \times (R \rightarrow X) \rightarrow X$	$Case(u, f, g) = \begin{cases} f(x), & \text{если } u = \langle 1, x \rangle \\ g(x), & \text{если } u = \langle 2, x \rangle \end{cases}$

Говоря простыми словами, инъекции приписывают к значению цифру 1 или 2, получая значение из множества  $U$ , а выбор, основываясь на приписанной цифре, применяет к значению первую или вторую функцию.

Построим аналогичную конструкцию для типов. *Типом-суммой* типов  $L$  и  $R$  (или, иначе, *алгебраическим типом*) назовём тип данных  $U$ , хранящий значения либо типа  $L$ , либо типа  $R$ , причём всегда

точно известно, какого именно (сравните с определением дизъюнкции в интуиционистской логике). С точки зрения теории множеств, множество значений типа  $U$  — отмеченное объединение множеств значений типов  $L$  и  $R$ . Для этого типа существует три базовых операции: две инъекции и выбор. Данный тип данных довольно широко распространён, и присутствует в ограниченном объёме даже в языках Си и Паскаль.

Например, в языке Паскаль с возможно следующее определение (там данная конструкция называется «записью с вариантами»):

```
type value: record
  is_real: boolean;
  case is_real of
    false: (real_value: real);
    true:  (int_value: integer);
  end;
```

Данная запись если `is_real = true` содержит поле `int_value`, а если `false` — поле `real_value`. Реализация данной структуры предполагает, что оба эти поля расположены в одной памяти.

В языке Си аналогом этой структуры является объединение (`union`), однако, явного поля для выбора одного из вариантов там не предусмотрено. В языке Си++ довольно близким аналогом является класс `std::variant` — «безопасное» объединение.

В лямбда-исчислении оказывается возможно реализовать эту конструкцию в чистом математическом виде:

$$\begin{aligned} In_L &= \lambda x. \lambda f. \lambda g. f \ x \\ In_R &= \lambda x. \lambda f. \lambda g. g \ x \\ Case &= \lambda u. \lambda f. \lambda g. u \ f \ g \end{aligned}$$

Также ещё заметим, что список можно представить, как алгебраический тип с двумя вариантами:

- `Nil` (соответствует пустому списку)
- `Cons(h,t)` (соединение головы списка `h` и хвоста `t`)

В частности, можно записать список `[1,2,3]` как `Cons(1,Cons(2,Cons(3,Nil)))`.

В лямбда-исчислении мы можем представить `Cons(h,t)` как правую инъекцию упорядоченной пары  $\langle h, t \rangle$  (так будем обозначать выражение  $\lambda a. a \ h \ t$ ), а `Nil` — как левую инъекцию любого значения, например,  $F$ . Тогда список `[1,2,3]` может быть представлен следующим лямбда-выражением:

$$In_R \ \langle \bar{1}, In_R \ \langle \bar{2}, In_R \ \langle \bar{3}, In_L \ F \rangle \rangle \rangle$$

- Реализуйте конструкции  $In_L$ ,  $In_R$ ,  $Case$  на языках Си, Паскаль и Си++ как можно ближе к формальному определению.
  - Покажите, что  $Case \ (In_L \ \bar{0}) \ (\lambda x. p) \ (\lambda x. q) =_{\beta} p$  и  $Case \ (In_R \ q) \ (\lambda x. p) \ (\lambda x. x) =_{\beta} q$ .
  - Постройте лямбда-выражение, по чётковскому нумералу  $\bar{n}$  возвращающее список `[1,2,3,...,n]`.
  - Постройте лямбда-выражение, по списку возвращающее его длину.
  - Постройте лямбда-выражение, суммирующее список чётковских нумералов.
  - Покажите, как реализовать алгебраический тип на  $n$  вариантов.
  - Покажите, как реализовать обращение списка (функция должна вернуть список в обратном порядке).
4. Чётковские нумералы соответствуют аксиоматике Пеано (числа записываются путём приписываний штрихов — прибавлений единиц). В частности поэтому вся арифметика с ними крайне медленная. А можно ли реализовать их с использованием двоичной записи?
- Предложите, как можно реализовать «логарифмические» нумералы — значения, которые соответствовали бы двоичной записи чисел.
  - Определите операцию преобразования чётковского нумерала в логарифмический.
  - Определите операцию преобразования логарифмического нумерала в чётковский.
  - Определите операцию суммы логарифмических нумералов.
  - Определите операцию ограниченного вычитания единицы из логарифмического нумерала (напомним, ограниченное вычитание возвращает 0, если вычитаемое больше уменьшаемого).

## Домашнее задание №3: «просто типизированное лямбда-исчисление»

1. На прошлой лекции определение параллельной бета-редукции было сформулировано неточно, отчего следующее утверждение не могло быть доказано:

*Покажите, что каковы бы ни были термы  $A, B, P, Q$  и переменная  $x$ , если  $A \Rightarrow_\beta B$  и  $P \Rightarrow_\beta Q$ , то  $A[x := P] \Rightarrow_\beta B[x := Q]$ .*

Однако, данное утверждение можно доказать, если переформулировать параллельную бета-редукцию так.  $A \Rightarrow_\beta B$ , если:

- (a)  $A = x, B = y$  и  $x = y$
- (b)  $A = P Q, B = R S$  и  $P \Rightarrow_\beta R, Q \Rightarrow_\beta S$
- (c)  $A = \lambda x.P, B = \lambda x.Q$  и  $P \Rightarrow_\beta Q$
- (d)  $A = (\lambda x.P) Q, B = R[x := S]$  и  $P \Rightarrow_\beta R, Q \Rightarrow_\beta S$

В связи с этим:

- (a) Докажите утверждение из прошлого домашнего задания при заданном определении.
  - (b) Обладает ли исходное отношение параллельной бета-редукции (заданное на прошлой лекции) ромбовидным свойством? Возможно, вы можете привести для него контрпример?
2. Покажите, что если  $A \rightarrow_\beta B$  и  $\vdash A : \alpha$ , то  $\vdash B : \alpha$ .
  3. Верно ли, что если  $A \rightarrow_\beta B$  и  $\vdash B : \alpha$ , то  $\vdash A : \alpha$ ? Верно ли это свойство для исчисления по Чёрчу?
  4. Покажите, что комбинатор  $\Omega = (\lambda x.x x) (\lambda x.x x)$  не имеет типа.
  5. Покажите, что никакое лямбда-выражение не имеет типа  $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$ .
  6. Докажите следующие утверждения в ИИВ и постройте соответствующие лямбда-выражения согласно изоморфизму Карри-Ховарда:
    - (a)  $\vdash (\alpha \rightarrow \alpha) \rightarrow \alpha \rightarrow \alpha$
    - (b)  $\vdash \alpha \rightarrow \beta \rightarrow \beta$
    - (c)  $\vdash (\alpha \rightarrow \beta) \rightarrow \alpha \rightarrow \beta$
    - (d)  $\vdash (\alpha \rightarrow \alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta)$
    - (e)  $\vdash (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\beta \rightarrow \alpha \rightarrow \gamma)$
    - (f)  $\vdash (\alpha \rightarrow \beta) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$  (аналог контрапозиции)
  7. Каков тип лямбда-выражения для суммы двух чёрчевских нумералов? Ответ поясните.
  8. Заметим, что:

$$\begin{aligned} \vdash S : (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) \\ \vdash K : \alpha \rightarrow \beta \rightarrow \alpha \end{aligned}$$

Как несложно заметить, данные утверждения соответствуют (в смысле изоморфизма Карри-Ховарда) схемам аксиом для импликационного фрагмента интуиционистского исчисления высказываний в гильбертовском стиле. Значит, и доказательство утверждений может быть (согласно изоморфизму) перенесено в лямбда-исчисление.

Гильбертовский стиль, который мы использовали в курсе матлогики, предполагал плоский список высказываний и номера утверждений для подсказок. Однако, мы можем изображать эти доказательства и в виде дерева:

$$\frac{\alpha \rightarrow \alpha \rightarrow \alpha \quad \frac{\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha \quad (\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)}{(\alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)}}{\alpha \rightarrow \alpha}$$

Давайте теперь изобразим вывод типа (для экономии места мы не указываем вывод типов для комбинаторов S и K).

$$\frac{\frac{\vdash K : \alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha \quad \vdash S : (\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)}{\vdash S K : (\alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)}}{\vdash S K K : \alpha \rightarrow \alpha}$$

Осталось заметить, что действительно  $I =_{\beta} S K K$ .

На основе изложенного, постройте доказательства следующих утверждений в гильбертовском стиле и выразите соответствующие выражения с помощью комбинаторов  $S$  и  $K$ :

- (a)  $\alpha \rightarrow \beta \rightarrow \beta$
- (b)  $(\alpha \rightarrow \beta) \rightarrow \alpha \rightarrow \beta$
- (c)  $(\alpha \rightarrow \alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta)$
- (d)  $(\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\beta \rightarrow \alpha \rightarrow \gamma)$

9. В дополнение к базису  $SK$  рассмотрим базис  $BCKW$ :

$$\begin{aligned} B &= \lambda x. \lambda y. \lambda z. x (y z) \\ C &= \lambda x. \lambda y. \lambda z. x z y \\ K &= \lambda x. \lambda y. x \\ W &= \lambda x. \lambda y. x y y \end{aligned}$$

Выведите типы для данных комбинаторов, постройте схемы аксиом для соответствующего гильбертовского исчисления высказываний и покажите, что данное исчисление также позволяет доказать любое утверждение из импликационного фрагмента ИИВ.

## Домашнее задание №4: «выразительная сила $\lambda_{\rightarrow}$ ; три задачи»

1. (Теорема о замкнутости импликационного фрагмента интуиционистского исчисления высказываний) Пусть формулы  $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$  и  $\alpha$  взяты из импликационного фрагмента ИИВ. Покажем, что если  $\Vdash_C \Gamma$  влечёт  $\Vdash_C \alpha$  в любой модели Крипке  $C$ , то тогда  $\Gamma \vdash_{\text{ИФ}} \alpha$ .

Возьмём следующее множество миров:  $W = \{\Delta \mid \Gamma \subseteq \Delta\}$ . Пусть заданы два мира  $w_1, w_2 \in W$ . Договоримся, что  $w_1 \preceq w_2$ , если  $w_1 \subseteq w_2$ . Также договоримся, что если  $w_i \in W$  и  $P$  — некоторая пропозициональная переменная, что  $w_i \Vdash P$ , то  $w_i \Vdash \neg P$ . Напомним, что данной тройки  $\langle W, (\preceq), (\Vdash) \rangle$  достаточно для задания модели Крипке. Тогда рассмотрим следующие задачи:

- (a) Покажите корректность определения модели Крипке: покажите, что если  $w_i \preceq w_j$  и  $w_i \Vdash P$ , то  $w_j \Vdash P$ .
- (b) Покажите, что  $w_i \Vdash \varphi$  тогда и только тогда, когда  $w_i \vdash \varphi$ . *Указание:* Из всего определения моделей Крипке в импликационном фрагменте имеют смысл только определения для переменной и импликации. Поэтому главное содержательное утверждение — показать, что  $w_i \Vdash \psi_1 \rightarrow \psi_2$  тогда и только тогда, когда  $w_i \vdash \psi_1 \rightarrow \psi_2$ . Используйте структурную индукцию и определение оценки импликации в моделях Крипке.
- (c) Пусть  $W = \{\Gamma\}$ . Предъявите пример таких  $\Gamma$  и  $\alpha$ , что  $\Vdash \Gamma$ ,  $\Vdash \alpha$ , но  $\Gamma \not\vdash \alpha$ .
- (d) К сожалению, подобным путём доказать полноту моделей Крипке для ИИВ со всеми связками невозможно. Пусть мы построили аналогичную конструкцию для полного ИИВ. Тогда предложите такие  $\Gamma$  и  $\alpha$ , что при выполненном  $\Vdash \Gamma$  выполнение  $\Vdash \varphi$  не будет влечь  $\Gamma \vdash \varphi$ .

Теперь завершим доказательство: в самом деле, если  $\Vdash_C \Gamma$  влечёт  $\Vdash_C \alpha$  в любой модели Крипке  $C$ , то оно будет выполнено и в построенной выше модели  $\langle W, (\preceq), (\Vdash) \rangle$ . То есть, если  $\Vdash \gamma_1, \dots, \Vdash \gamma_n$ , то  $\Vdash \alpha$ . Значит, по определению импликации в моделях Крипке имеем

$$\Vdash \gamma_1 \rightarrow \dots \rightarrow \gamma_n \rightarrow \alpha$$

Значит, по свойству (b):

$$\vdash \gamma_1 \rightarrow \dots \rightarrow \gamma_n \rightarrow \alpha$$

И по теореме о дедукции получаем искомое  $\Gamma \vdash \alpha$ .

2. Покажите, что функция возведения в степень не является расширенным полиномом.

3. Пусть тип  $\nu = (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ , где  $\alpha$  — это некоторый заранее зафиксированный атомарный тип. Предложите такие лямбда-выражения  $F : \nu \rightarrow \nu \rightarrow \nu$ , что:
- (а) Если  $m, n \in \mathbb{N}_0$ , то  $F_a \overline{m} \overline{n} =_\beta \overline{m + n}$
  - (б) Если  $m, n \in \mathbb{N}_0$ , то  $F_b \overline{m} \overline{n} =_\beta \overline{m \cdot n}$

## Домашнее задание №5: «унификация алгебраических термов»

1. Покажите, что несовместная система не имеет решений. А именно, решений нет, если:
- (а) Если в системе есть уравнение вида  $x = \Theta(x)$ , где  $\Theta(x)$  — некоторый нетривиальный алгебраический терм со свободной переменной  $x$ .
  - (б) Если в системе есть уравнение вида

$$f_n \theta_1 \theta_2 \dots \theta_n = g_m \sigma_1 \sigma_2 \dots \sigma_m$$

где  $f_n \not\equiv g_m$ .

2. Покажите, что следующие операции строят эквивалентную систему уравнений:

- (а) Исключение переменной: из системы

$$\begin{cases} x = \xi \\ \sigma_1 = \theta_1 \\ \dots \\ \sigma_n = \theta_n \end{cases}$$

операция строит систему

$$\begin{cases} x = \xi \\ \sigma_1[x := \xi] = \theta_1[x := \xi] \\ \dots \\ \sigma_n[x := \xi] = \theta_n[x := \xi] \end{cases}$$

- (б) Редукция терма: из системы

$$\begin{cases} f_l \zeta_1 \dots \zeta_l = f_l \eta_1 \dots \eta_l \\ \sigma_1 = \theta_1 \\ \dots \\ \sigma_n = \theta_n \end{cases}$$

операция строит систему

$$\begin{cases} \zeta_1 = \eta_1 \\ \dots \\ \zeta_l = \eta_l \\ \sigma_1 = \theta_1 \\ \dots \\ \sigma_n = \theta_n \end{cases}$$

3. В доказательстве завершаемости алгоритма унификации использовалась лексикографически упорядоченная монотонно убывающая последовательность троек чисел. Однако, точного доказательства конечности этой последовательности не было дано. Покажите, что:
- (а) Не существует бесконечной строго убывающей последовательности упорядоченных троек: таких  $\langle x_i, y_i, z_i \rangle$ ,  $x_i, y_i, z_i \in \mathbb{N}_0$ , что  $\langle x_n, y_n, z_n \rangle > \langle x_{n+1}, y_{n+1}, z_{n+1} \rangle$  при любом  $n$ .
  - (б) Покажите, что любая строго убывающая последовательность ординалов имеет конечную длину.
  - (в) Поясните, почему первый пункт данной задачи является частным случаем второго.
4. При помощи рассказанного на лекции алгоритма найдите типы для следующих лямбда-выражений, или покажите, что у них нет типа:
- (а)  $\lambda x. \lambda y. x$
  - (б)  $\lambda x. \lambda y. \lambda z. x \ z \ (y \ z)$
  - (в)  $(\lambda x. x \ x) \ (\lambda x. x \ x)$
  - (д)  $\lambda f. \lambda x. f \ (f \ x)$
  - (е)  $\lambda m. \lambda n. \lambda f. \lambda x. m \ f \ (n \ f \ x)$

- (f)  $\lambda m. \lambda n. n \ m$
  - (g)  $(\lambda m. \lambda n. n \ m) \ \bar{3} \ \bar{3}$
  - (h)  $(\lambda s. (\lambda m. \lambda n. n \ m) \ s \ s) \ \bar{3}$
  - (i)  $In_L, In_R, Case$
  - (j)  $Pr_L, Pr_R, MkPair$
  - (k) Лямбда-выражение, возвращающее  $T$ , если чётчеревский нумерал равен нулю — иначе  $F$ .
  - (l) Лямбда-выражение, проверяющее чётность чётчеревского нумерала.
5. Покажите, что если алгоритм нашёл тип для выражения, то можно построить доказательство, выводящее этот тип в просто типизированном лямбда-исчислении.
  6. Покажите, что если для некоторого лямбда-выражения имеет тип, то у уравнения в алгебраических терминах, строящегося в алгоритме по выражению, найдётся решение.
  7. Назовём *наиболее общей парой* для лямбда-выражения  $M$  такую пару  $\langle \Gamma, \sigma \rangle$  ( $\Gamma \vdash M : \sigma$ ), что любая другая пара  $\langle \Delta, \tau \rangle$  ( $\Delta \vdash M : \tau$ ) является её частным случаем: существует подстановка  $S$ , что  $\Delta = S(\Gamma)$  и  $\sigma = S(\tau)$ .
    - (a) дайте корректное определение подстановкам на типах и контекстах ( $S(\Gamma)$  и  $S(\tau)$ ), «рукомашенски» использованным выше;
    - (b) покажите, что алгоритм типизации находит наиболее общую пару.

## Домашнее задание №6: «движемся вперёд: полное исчисление высказываний, логика второго порядка»

1. Найдите термы, населяющие указанные ниже типы, постройте доказательство (вывод соответствующего типа), поясните смысл соответствующих следующим лямбда-выражениям программ:
  - (a)  $\alpha \rightarrow \neg \neg \alpha$
  - (b)  $(\alpha \rightarrow \beta) \rightarrow (\neg \beta \rightarrow \neg \alpha)$
  - (c) *Даёшь теорему Гливенко!*  $\neg \neg (\alpha \vee \neg \alpha)$
  - (d)  $\neg \neg (((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha)$
  - (e) *Как вы догадываетесь, обитаем только один из двух вариантов законов Де Моргана, укажите этот вариант и решите задачу для него:  $\alpha \vee \beta \rightarrow \neg(\neg \alpha \ \& \ \neg \beta)$  или  $\neg(\neg \alpha \ \& \ \neg \beta) \rightarrow \alpha \vee \beta$ .*
2. Постройте доказательства в импликационном фрагменте исчисления второго порядка для следующих аксиом полного исчисления:
  - (a) введение конъюнкции;
  - (b) исключение конъюнкции;
  - (c) введение дизъюнкции;
  - (d) исключение дизъюнкции;
  - (e) исключение лжи;
  - (f) введение квантора существования;
  - (g) исключение квантора существования;
  - (h) введение отрицания;
  - (i) исключение отрицания.
3. Существует два различных варианта аксиом для конъюнкции в исчислении высказываний. Один был на лекции, второй приведён ниже:

$$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \ \& \ Q} \quad \frac{\Gamma \vdash P \ \& \ Q \quad \Gamma, P, Q \vdash R}{\Gamma \vdash R}$$

Покажите, что аксиомы конъюнкции в каждом из вариантов исчисления могут быть доказаны как теоремы в другом варианте.

4. Предложите лямбда-выражения в системе F и выведите типы для следующих конструкций нетипизированного лямбда-исчисления:
  - (a)  $T, F$ , исключающее или;
  - (b) чёrchевский нумерал, сложение;
  - (c) возведение в степень чёrchевских нумералов;
  - (d) разность чёrchевских нумералов.

5. Докажите дистрибутивность в логике второго порядка, покажите обитаемость типа и поясните смысл получившейся программы:

$$\forall\alpha.\forall\beta.\forall\gamma.\alpha \vee (\beta \& \gamma) \rightarrow (\alpha \vee \beta) \& (\alpha \vee \gamma)$$

6. Выразимы ли  $\Omega$  или  $Y$  комбинаторы в системе F?
7. Сформулируйте теорему Чёrch-Россера для исчисления второго порядка. Предложите схему её доказательства.

## Домашнее задание №7: «экзистенциальные типы»

1. На лекции были выписаны следующие лямбда-выражения для конструкций с кванторами:

- (a) **pack**  $M, \tau$  **to**  $\exists\alpha.\sigma = \Lambda\beta.\lambda x^{\forall\alpha.\sigma \rightarrow \beta}.x \tau M$
- (b) **abstype**  $\alpha$  **with**  $x : \sigma$  **is**  $M$  **in**  $N^\rho = M \rho (\lambda\alpha.\lambda x^\sigma.N)$

Возможно, в конструкциях есть ошибки — исправьте их и докажите, что данные конструкции удовлетворяют аксиомам, если выразить  $\exists\alpha.P$  как  $\forall\phi.(\forall\alpha.P \rightarrow \phi) \rightarrow \phi$ .

2. Переформулируйте систему F в исчислении по Карри: укажите новые схемы аксиом для квантора всеобщности.
3. Переформулируйте операции **abstype** и **pack** для исчисления по Карри, укажите соответствующие им лямбда-выражения и покажите, что эти выражения соответствуют аксиомам.

## Домашнее задание №8: «типовая система Хиндли-Милнера»

1. Определим отрицание двумя способами:  $\neg\phi = \phi \rightarrow \forall p.p$  и  $\sim\phi = \forall p.\phi \rightarrow p$ .
  - (a) Покажите, что оба отрицания эквивалентны в логике 2 порядка, то есть, что выполнены следующие правила:

$$\frac{\Gamma \vdash \sim\phi}{\Gamma \vdash \neg\phi} \quad \frac{\Gamma \vdash \neg\phi}{\Gamma \vdash \sim\phi}$$

- (b) Покажите, что если  $\Gamma \vdash M : \neg\tau$ , то найдётся такое выражение  $M'$ , что  $\Gamma \vdash M' : \sim\tau$ ; и наоборот, если  $\Gamma \vdash N : \sim\tau$ , то для какого-то  $N'$  выполнено  $\Gamma \vdash N' : \neg\tau$
2. Обозначим минимальный ранг типа  $\tau$  за  $rk(\tau)$ . Приведите пример типа  $\tau$ , что  $rk(\tau) = 3$ .
3. Докажите, что  $rk(\exists x.\phi) > 1$ .
4. Придумайте семейство типов  $\tau_n$ , такое, что  $rk(\tau_n) = n$ .
5. Определим *арифметическую иерархию* на классическом исчислении предикатов второго порядка (сразу упомянем, что данное определение не классическое — традиционно его вводят для исчисления предикатов первого порядка):
  - $\Pi_0 = \Sigma_0$  — все выражения, логически эквивалентные бескванторным выражениям;
  - $\Pi_n, n > 0$  — все выражения, логически эквивалентные выражениям вида  $\forall x.S$ , где  $S \in \Sigma_{n-1}$ ;
  - $\Sigma_n, n > 0$  — все выражения, логически эквивалентные выражениям вида  $\exists x.P$ , где  $P \in \Pi_{n-1}$ .



Заметим, что, например,  $\Pi_3$  состоит из выражений вида  $\forall x.\exists y.\forall z.R$ . Также заметим, что, поскольку к любой формуле можно приписать любые кванторы по свежим переменным и получить формулу, логически эквивалентную исходной, то если  $m < n$ , то  $\Pi_m \subset \Pi_n$  и  $\Sigma_m \subset \Sigma_n$ .

На лекции была высказана гипотеза, что ранг типов для лямбда-выражений в системе F связан с чередованием кванторов. В данной задаче мы предлагаем вам разобраться в этом вопросе:

- (a) Существует ли такая константа  $k$  и такое семейство типов  $\tau_n$ , что  $rk(\tau_n) = n$ , но  $\tau_n \in \Pi_k$
  - (b) Существует ли такая константа  $k$  и такое семейство типов  $\tau_n$ , что  $\tau_n \in \Pi_n \setminus \Pi_{n-1}$ , но  $rk(\tau_n) \leq k$ .
6. Пусть даны две типовых схемы  $\sigma_1$  и  $\sigma_2$ . Придумайте алгоритм проверки того, что  $\sigma_1 \sqsubseteq \sigma_2$ .
7. Напомним, что, по определению,

$$(\text{let } x = E_0 \text{ in } E_1) =_\beta (\lambda x.E_1) E_0$$

На основании этой эквивалентности мы можем для каждого лямбда-выражения  $E'$  в системе НМ сопоставить ему  $\beta$ -эквивалентное выражение  $E$  в системе F.

Пользуясь этой эквивалентностью, найдите выражения в системе НМ для следующих конструкций в системе F, и докажите, что их типы могут быть выведены в системе НМ:

- (a) Булевские значения, функция XOR.
- (b) Чёрчевские нумералы, функция «сумма».
- (c) Возведение в степень (для чёрчевских нумералов).
- (d) Вычитание.
- (e) Деление.

## Домашнее задание №9: «алгоритм W; типовая система НМ»

1. С помощью алгоритма W выведите типы для следующих выражений (или укажите, что выражения не имеют типа):
  - (a)  $a$
  - (b)  $x : \alpha \vdash x$
  - (c)  $\vdash \lambda x.x$
  - (d)  $\vdash \text{let } \bar{1} = \lambda f.\lambda x.f\ x \text{ in } \bar{1}\ \bar{1}$
  - (e)  $\vdash \text{let } s = \lambda f.\lambda x.f\ (f\ x) \text{ in } sq\ (sq\ \bar{1})$
  - (f)  $\vdash \text{let } s = \lambda f.\lambda x.f\ (f\ x) \text{ in } (sq\ sq)\ \bar{1}$
  - (g)  $\vdash \text{let } s = \lambda f.\lambda x.f\ (f\ x) \text{ in } sq\ sq\ sq\ sq\ sq\ sq\ \bar{1}$ ; чему равен результат бета-редукции указанного терма?
2. Рассмотрим типовую систему НМ+Y: система Хиндли-Милнера в которой, по определению,  $\vdash (\lambda f.(\lambda x.f\ (x\ x)))\ (\lambda x.\forall\alpha.(\alpha \rightarrow \alpha) \rightarrow \alpha)$ .
  - (a) Типизируем ли в этой типовой системе  $\Omega = \omega\ \omega$ , где  $\omega = \lambda x.x\ x$ ?
  - (b) Найдите такой терм  $F$ , что  $\vdash F : \perp$ .
  - (c) Найдите такой терм  $E$ , что  $\vdash E : \alpha \vee \neg\alpha$ .
3. Как нетрудно заметить, список — это «параметризованные» числа в аксиоматике Пеано. Число — это длина списка, а к каждому штриху мы присоединяем какое-то значение. Операции добавления и удаления элемента из списка — это операции прибавления и вычитания единицы к числу. Рассмотрим тип «бинарного списка»:

```
type 'a bin_list = Nil | Zero of (('a*'a) bin_list) | One of 'a * (('a*'a) bin_list);;
```

Если бы такое можно было выразить в типовой системе Хиндли-Милнера, то операция добавления элемента к списку записалась бы на языке Окамль вот так (сравните с прибавлением 1 к числу в двоичной системе счисления):

```
let rec add elem lst = match lst with
  Nil -> One (elem,Nil)
  | Zero t1 -> One (elem,t1)
  | One (hd,t1) -> Zero (add (elem,hd) t1)
```

- (a) Какой тип имеет `add` (рекурсивная функция должна уже включать в себя  $Y$ -комбинатор и не требовать никаких дополнительных усилий для вызова)? Считайте, что тип `bin_list 'a` уже как-то задан, и обозначается как  $\tau(\alpha)$ .
- (b) Какой ранг имеет тип этой функции, почему её не скомпилировать в Окамле?
- (c) Предложите функцию для удаления элемента списка (головы).
- (d) Предложите функцию для эффективного соединения двух списков (источник для вдохновения — сложение двух чисел в столбик).
- (e) Предложите функцию для эффективного выделения  $n$ -го элемента из списка.

4. Задан тип «дерево»:

```
type 'a tree = Leaf of 'a | Node of (tree 'a) * (tree 'a);;
```

Задайте тип  $\tau(\alpha)$ :

- (a) Как эквирекурсивный тип (задайте через  $\mu$ -оператор).
- (b) Как изорекурсивный тип (определите функции `roll` и `unroll`, укажите их тип).