Теоретические ("малые") домашние задания

Теория типов, ИТМО, M3334-M3339, 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
   $$P_l\ (M\ A\ B) \to_\beta \cdots \to_\beta A$$
   и
   $$P_r\ (M\ A\ B) \to_\beta \cdots \to_\beta B$$
   (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) $(\lambda n.\lambda f.\lambda x.n\ f\ (f\ x))\ \overline{n} =_\beta \overline{n+1}$;
   (d) $a \neq_\beta b$.

   Мы будем говорить, что лямбда-выражение E выражает функцию $f(x_1, \dots, x_k) : \mathbb{N}_0^k \to \mathbb{N}_0$, 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) $\lambda m.\lambda n.n\ m$;

(b) $\lambda m.\lambda n.\lambda x.n\ (m\ x)$.

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, $(\to_\beta) \subseteq (\rightrightarrows_\beta)$. То есть, если $A \to_\beta B$, то $A \rightrightarrows_\beta B$.

   (b) Покажите, что каковы бы ни были термы A, P, Q и переменная x, если выполнено $P \rightrightarrows_\beta Q$, то $A[x := P] \rightrightarrows_\beta A[x := Q]$. 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 $A \rightrightarrows_\beta B$ и $P \rightrightarrows_\beta Q$, то $A[x := P] \rightrightarrows_\beta B[x := Q]$.

   (d) Покажите, что $(\rightrightarrows_\beta)$ 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 $(\twoheadrightarrow_\beta) \subseteq (\rightrightarrows_\beta)^*$.

   (g) Покажите, что $(\rightrightarrows_\beta)^* \subseteq (\twoheadrightarrow_\beta)$

   На основании доказанных лемм несложно показать утверждение теоремы Чёрча-Россера: из последних пунктов следует, что $(\rightrightarrows_\beta)^* = (\twoheadrightarrow_\beta)$, 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	$in_L : L \to U$	$in_L(x) = \langle 1, x\rangle$
правая инъекция	$in_R : R \to U$	$in_R(x) = \langle 2, x\rangle$
выбор	$Case : U \times (L \to X) \times (R \to X) \to X$	$Case(u, f, g) = \begin{cases} f(x), & \text{если } u = \langle 1, x\rangle \\ g(x), & \text{если } u = \langle 2, x\rangle \end{cases}$

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 фукнцию.

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:

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

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:

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

(a) Реализуйте конструкции In_L, In_R, $Case$ на языках Си, Паскаль и Си++ как можно ближе к формальному определению.

(b) Покажите, что $Case\ (In_L\ \overline{0})\ (\lambda x.p)\ (\lambda x.q) =_\beta p$ и $Case\ (In_R\ q)\ (\lambda x.p)\ (\lambda x.x) =_\beta q$.

(c) Постройте лямбда-выражение, по чёрчевскому нумералу $\overline{n}$ возвращающее список `[1,2,3,...,n]`.

(d) Постройте лямбда-выражение, по списку возвращающее его длину.

(e) Постройте лямбда-выражение, суммирующее список чёрчевских нумералов.

(f) Покажите, как реализовать алгебраический тип на n вариантов.

(g) Покажите, как реализовать обращение списка (функция должна вернуть список в обратном порядке).

4. Чёрчевские 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?

   (a) Предложите, как можно реализовать «логарифмические» нумералы — значения, которые соответствовали бы двоичной записи чисел.

   (b) Определите операцию преобразования чёрчевского нумерала в логарифмический.

   (c) Определите операцию преобразования логарифмического нумерала в чёрчевский.

   (d) Определите операцию суммы логарифмических нумералов.

   (e) 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 $A \rightrightarrows_\beta B$ и $P \rightrightarrows_\beta Q$, то $A[x := P] \rightrightarrows_\beta B[x := Q]$.

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

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

   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 $A \twoheadrightarrow_\beta B$ и $\vdash A : \alpha$, то $\vdash B : \alpha$.

3. Верно ли, что если $A \twoheadrightarrow_\beta B$ 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 $((\alpha \to \beta) \to \alpha) \to \alpha$.

6. Докажите следующие утверждения в ИИВ и постройте соответствующие лямбда-выражения согласно изоморфизму Карри-Ховарда:

   (a) $\vdash (\alpha \to \alpha) \to \alpha \to \alpha$
   (b) $\vdash \alpha \to \beta \to \beta$
   (c) $\vdash (\alpha \to \beta) \to \alpha \to \beta$
   (d) $\vdash (\alpha \to \alpha \to \beta) \to (\alpha \to \beta)$
   (e) $\vdash (\alpha \to \beta \to \gamma) \to (\beta \to \alpha \to \gamma)$
   (f) $\vdash (\alpha \to \beta) \to (\beta \to \gamma) \to (\alpha \to \gamma)$ (аналог контрапозиции)

7. Каков тип лямбда-выражения для суммы двух чёрчевских нумералов? Ответ поясните.

8. Заметим, что:

   $$\begin{array}{l} \vdash S : (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma) \\ \vdash K : \alpha \to \beta \to \alpha \end{array}$$

   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:

   $$\dfrac{\alpha \to \alpha \to \alpha \qquad \dfrac{\alpha \to (\alpha \to \alpha) \to \alpha \qquad (\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to \alpha \to \alpha) \to (\alpha \to \alpha)}{(\alpha \to \alpha \to \alpha) \to (\alpha \to \alpha)}}{\alpha \to \alpha}$$

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

$$\dfrac{\vdash K : \alpha \to \alpha \to \alpha \qquad \dfrac{\vdash K : \alpha \to (\alpha \to \alpha) \to \alpha \quad \vdash S : (\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to \alpha \to \alpha) \to (\alpha \to \alpha)}{\vdash S\ K : (\alpha \to \alpha \to \alpha) \to (\alpha \to \alpha)}}{\vdash S\ K\ K : \alpha \to \alpha}$$

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) $\alpha \to \beta \to \beta$

(b) $(\alpha \to \beta) \to \alpha \to \beta$

(c) $(\alpha \to \alpha \to \beta) \to (\alpha \to \beta)$

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

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 $\lambda_\to$; три задачи»

1. *(Теорема о замкнутости импликационного фрагмента интуиционистского исчисления высказываний)* Пусть формулы $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$ и α 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 $w_i \Vdash P$. 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 $w_i \Vdash \psi_1 \to \psi_2$ тогда и только тогда, когда $w_i \vdash \psi_1 \to \psi_2$. Используйте структурную индукцию и определение оценки импликации в моделях Крипке.

(c) Пусть $W = \{\Gamma\}$. Предъявите пример таких Γ и α, 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 Γ и α, 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 $\Vdash \gamma_1$, ..., $\Vdash \gamma_n$, то $\Vdash \alpha$. Значит, по определению импликации в моделях Крипке имеем

$$\Vdash \gamma_1 \to \dots \to \gamma_n \to \alpha$$

Значит, по свойству (b):

$$\vdash \gamma_1 \to \dots \to \gamma_n \to \alpha$$

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

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

3. Пусть тип $\nu = (\alpha \to \alpha) \to (\alpha \to \alpha)$, где α — это некоторый заранее зафиксированный атомарный тип. Предложите такие лямбда-выражения $F : \nu \to \nu \to \nu$, что:

    (a) Если $m, n \in \mathbb{N}_0$, то $F_a\ \overline{m}\ \overline{n} =_\beta \overline{m + n}$

    (b) Если $m, n \in \mathbb{N}_0$, то $F_b\ \overline{m}\ \overline{n} =_\beta \overline{m \cdot n}$