

# Алгебраические типы данных

# Алгебра на типах данных

Множество	Мощность	Тип	Название
$\emptyset$	0	void	необитаемый
$\{\emptyset\}$	1	unit	одноэлементный
$\{T, F\}$	2	boolean	булевский, двухэлементный
$A \uplus B$	$ \alpha  +  \beta $	Either Alpha Beta	тип-сумма
$A \times B$	$ \alpha  \cdot  \beta $	(Alpha, Beta)	пара, декартово произведение
$B^A$	$ \beta ^{ \alpha }$	Alpha $\rightarrow$ Beta	функциональный

## Пример

*(boolean, A  $\rightarrow$  boolean) соответствует  $2 \cdot (2^A)$*

# Алгебраический тип данных, тип-сумма

## Определение

Отмеченным объединением множеств (дизъюнктивным объединением) назовём:

$$A \uplus B := \{ \langle a, "L" \rangle \mid a \in A \} \cup \{ \langle b, "R" \rangle \mid b \in B \} = \{ a_L \mid a \in A \} \cup \{ b_R \mid b \in B \}$$

## Пример

$$\mathbb{N} \cup \mathbb{N} = \{1, 2, 3, \dots\} \quad \mathbb{N} \uplus \mathbb{N} = \{1_L, 1_R, 2_L, 2_R, 3_L, 3_R, \dots\}$$

$$\mathbb{N} \uplus \mathbb{Z} = \{\dots - 3_R, -2_R, -1_R, 0_R, 1_L, 1_R, 2_L, 2_R, 3_L, 3_R, \dots\}$$

Алгебраический тип данных (тип-сумма) задаётся набором конструкторов, каждому конструктору сопоставляется тип параметра.

## Пример

*boolean* := False / True

$B = \{\emptyset\} \uplus \{\emptyset\}$      $\text{Л} : \emptyset_L$

*angle* := Degrees of int / Radians of real

$A := \mathbb{Z} \uplus \mathbb{R}$

$180^\circ : 180$

## Примеры из языков программирования

```
type angle = record          struct angle {
    case radians : boolean of  bool radians;
        true: (rads: real);    union {
        false: (deg: integer); float rads;
    end;                      int deg;
                              }
};
```

Типичное применение:

```
union {
    short ax;
    struct {
        char al;
        char ah;
    }
};
```

# Списки

- ▶ Список (целых чисел) — алгебраический тип:

```
type list = Nil | Cons of int * list
```

- ▶ Как строим значения:

```
Nil                                     => []  
Cons (5, Nil)                          => [5]  
Cons (3, Cons (4, Cons (5, Nil)))      => [3,4,5]
```

- ▶ Как используем значения:

```
let rec length l = match l with  
  Nil -> 0  
  | Cons (_,lt) -> 1 + length lt
```

## Взглянем немного глубже

Надо научиться строить и разбирать тип

`list = Nil | Cons of int * list:`

$$L = \{\emptyset\} \uplus (\mathbb{Z} \times L)$$

- ▶ Строить. Конструкторы: `Nil`, `Cons` — или левая и правая инъекции  $(In_L, In_R)$ .

$$Nil := In_L() \quad Cons\ a\ b := In_R\ \langle a, b \rangle$$

- ▶ Разбирать.

<code>let rec length l = match l with</code>	<code>match l with</code>
<code>Nil -&gt; 0</code>	<code>  InL p -&gt; 0</code>
<code>  Cons (lh,lt) -&gt; 1 + length lt</code>	<code>  InR p -&gt; 1 + length p</code>

В самом низу — элиминатор `Case`:

`length l := Case l (\p.0) (\p.1 + length (\pi_R p))`

# Алгебраический тип как дизъюнкция

Общие соображения: ВНК-интерпретация.

Интуиционистское исчисление высказываний

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta} \quad \frac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta} \quad \frac{\Gamma \vdash \alpha \vee \beta \quad \Gamma \vdash \alpha \rightarrow \gamma \quad \Gamma \vdash \beta \rightarrow \gamma}{\Gamma \vdash \gamma}$$

Просто-типизированное лямбда исчисление — придумаем названия

$$\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash \text{In}_L A : \alpha \vee \beta} \quad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash \text{In}_R B : \alpha \vee \beta} \quad \frac{\Gamma \vdash X : \alpha \vee \beta \quad \Gamma \vdash L : \alpha \rightarrow \gamma}{\Gamma \vdash \text{Case } X \text{ L } R : \gamma}$$

## Пример

Напомним, если  $\tau = \varphi = \text{unit}$ , то  $\tau \vee \varphi \approx \text{bool}$ .

Тогда  $T^{\tau \vee \varphi} := \text{In}_L()$ ,  $F^{\tau \vee \varphi} := \text{In}_R()$ . И, например,

$\text{Not } x := \text{Case } x (\lambda t. \text{In}_R()) (\lambda t. \text{In}_L())$

## Реализация алгебраического типа

Просто-типизированное лямбда исчисление:

$$\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash \text{In}_L A : \alpha \vee \beta} \quad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash \text{In}_R B : \alpha \vee \beta} \quad \frac{\Gamma \vdash X : \alpha \vee \beta \quad \Gamma \vdash L : \alpha \rightarrow \gamma}{\Gamma \vdash \text{Case } X \text{ L } R : \gamma}$$

Предлагаем такую реализацию:

$$\text{In}_L := \lambda x. \lambda t. \lambda f. t \ x, \quad \text{In}_R := \lambda x. \lambda t. \lambda f. f \ x \quad \text{Case} := \lambda x. \lambda l. \lambda r. x \ l \ r$$
$$\text{Case } (\text{In}_L X^\tau) L^{\tau \rightarrow \gamma} R \rightarrow_\beta (\text{In}_L X) L R = (\lambda t. \lambda f. t \ X) L R \rightarrow_\beta (L \ X)^\gamma$$

А где здесь дизъюнкция? Ожидаем, что  $(\text{In}_L X^\tau) : \tau \vee \varphi$ . А что на деле?

$$X : \tau \vdash \lambda t^{\tau \rightarrow \gamma}. \lambda f^{\varphi \rightarrow \gamma}. t \ X : (\tau \rightarrow \gamma) \rightarrow (\varphi \rightarrow \gamma) \rightarrow \gamma$$

«Если некоторое утверждение  $\gamma$  истинно **всегда**, когда оно следует из истинности  $\tau$  и  $\varphi$  — то либо  $\tau$ , либо  $\varphi$  истинно».

Рассуждение не совсем формально, потому что не хватает **кванторов по утверждениям**, использующимся неявно:

$$\forall \gamma. (\tau \rightarrow \gamma) \rightarrow (\varphi \rightarrow \gamma) \rightarrow \gamma$$



## Примеры алгебраических типов

Булевские значения:

$$T_1 := \text{In}_L() = \lambda t. \lambda f. t \quad F_1 := \text{In}_R() = \lambda t. \lambda f. f \quad \text{If}_1 := \lambda b. \lambda t. \lambda e. b \ t \ e$$

Ну или когда аргумент опущен за ненадобностью:

$$T := \lambda t. \lambda f. t \quad F := \lambda t. \lambda f. f \quad \text{If} := \lambda b. \lambda t. \lambda e. b \ t \ e$$

Списки:

$$\text{Nil} := \text{In}_L 0 \quad \text{Cons } p \ q := \text{In}_R \langle p, q \rangle$$

Тогда  $[1, 3, 5]$  превращается в  $\text{Cons } 1 \ (\text{Cons } 3 \ (\text{Cons } 5 \ \text{Nil}))$ .

Для простоты раскроем полностью  $[1] = \text{Cons } 1 \ \text{Nil}$ :

$$\lambda t. \lambda f. f(\lambda p. p \ (\lambda f. \lambda x. f \ x) \ (\lambda t. \lambda f. t \ (\lambda f. \lambda x. x)))$$

Мощность	Тип	Высказывание
0	$\perp$	необитаемый тип
1	$() : \text{unit}$	одноэлементный тип
$ \alpha  +  \beta $	$\text{Either } A^\alpha B^\beta : \alpha \vee \beta$	тип-сумма, дизъюнкция
$ \alpha  \cdot  \beta $	$(A^\alpha, B^\beta) : \alpha \& \beta$	тип-произведение, конъюнкция
$ \beta ^{ \alpha }$	$\lambda x^\alpha. B : \alpha \rightarrow \beta$	функциональный, импликация

# Мощность множеств

# Отношения

## Определение

$A \times B := \{\langle a, b \rangle \mid a \in A, b \in B\}$

Бинарное отношение —  $R \subseteq A \times B$

Функциональное бинарное отношение (функция)  $R$  — такое, что  $\forall x. x \in A \rightarrow \exists! y. \langle x, y \rangle \in R$

$R$  — инъективная функция, если

$\forall x. \forall y. \langle x, y \rangle \in R \ \& \ \langle y, t \rangle \in R \rightarrow x = y.$

$R$  — сюръективная функция, если  $\forall y. y \in B \rightarrow \exists x. \langle x, y \rangle \in R.$

# Равномощные множества

## Определение

*Множество  $A$  равномощно  $B$  ( $|A| = |B|$ ), если существует биекция  $f : A \rightarrow B$ .*

*Множество  $A$  имеет мощность, не превышающую мощности  $B$  ( $|A| \leq |B|$ ), если существует инъекция  $f : A \rightarrow B$ .*

# Теорема Кантора-Бернштейна

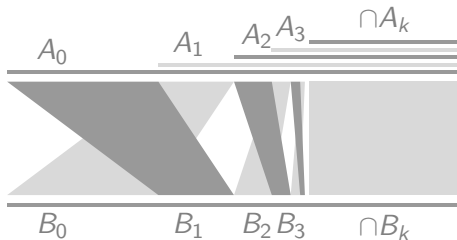
## Теорема

Если  $|A| \leq |B|$  и  $|B| \leq |A|$ , то  $|A| = |B|$ .

Заметим,  $f : A \rightarrow B$ ,  $g : B \rightarrow A$  — инъекции, но не обязательно  $g(f(x)) = x$ .

## Доказательство.

Избавимся от множества  $B$ : пусть  $A_0 = A$ ;  $A_1 = g(B)$ ;  
 $A_{k+2} = g(f(A_k))$ .



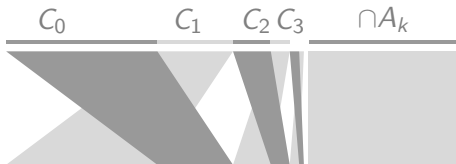
Тогда, если существует  $h : A_0 \rightarrow A_1$  — биекция, то тогда  $g^{-1} \circ h : A \rightarrow B$  — требуемая биекция.



## Построение биекции $h : A_0 \rightarrow A_1$

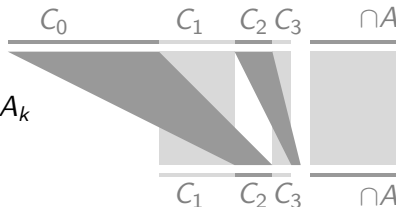
Пусть  $C_k = A_k \setminus A_{k+1}$ . Тогда

$$g(f(C_k)) = g(f(A_k)) \setminus g(f(A_{k+1})) = A_{k+2} \setminus A_{k+3} = C_{k+2}.$$



Тогда определим  $h(x)$  следующим образом:

$$h(x) = \begin{cases} x, & x \in C_{2k+1} \vee x \in \cap A_k \\ g(f(x)), & x \in C_{2k} \end{cases}$$



# Кардинальные числа

## Определение

*Кардинальное число — наименьший ординал, не равномощный никакому меньшему:*

$$\forall x. x \in c \rightarrow |x| < |c|$$

## Теорема

*Конечные ординалы — кардинальные числа.*

## Определение

*Мощность множества ( $|S|$ ) — равномощное ему кардинальное число.*



# Диагональный метод

## Лемма

$$|\mathbb{R}| > |\mathbb{N}|$$

## Доказательство.

Рассмотрим  $a \in (0, 1)$  и десятичную запись:  $0.a_0a_1a_2\dots$ . Пусть существует биективная  $f : \mathbb{N} \rightarrow (0, 1)$ . По функции найдём значение  $\sigma$ , не являющееся образом никакого натурального числа.

$n$	$f(n)$	$f(n)_0$	$f(n)_1$	$f(n)_2$	$f(n)_3$	$f(n)_4$	$f(n)_5$	$\dots$
$n_0$	0.3	3	0	0	0	0	0	$\dots$
$n_1$	$\pi/10$	3	1	4	1	5	9	$\dots$
$n_2$	$1/7$	1	4	2	8	5	7	$\dots$
$\sigma$		8	6	7	$\dots \sigma_k = (f(n_k)_k + 5) \% 10$			



# Теорема Кантора

## Теорема

$$|\mathcal{P}(S)| > |S|$$

## Доказательство.

Пусть  $S = \{a, b, c, \dots\}$

$n$	$a \in f(n)$	$b \in f(n)$	$c \in f(n)$	...
$a$	И	Л	И	
$b$	Л	Л	И	
$c$	И	И	И	
	Л	И	Л	$y \notin f(y)$

Пусть  $f : S \rightarrow \mathcal{P}(S)$  — биекция. Тогда  $\sigma = \{y \in S \mid y \notin f(y)\}$ .  
Пусть  $f(x) = \sigma$ . Но  $x \in f(x)$  тогда и только тогда, когда  $x \notin \sigma$ ,  
то есть  $f(x) \neq \sigma$ . □

О буквах

[https://en.wikipedia.org/wiki/Proto-Sinaitic\\_script](https://en.wikipedia.org/wiki/Proto-Sinaitic_script)

# Иерархии $\aleph_n$ и $\beth_n$

## Определение

$$\aleph_0 := |\omega|; \aleph_{k+1} := \min\{a \mid a - \text{ординал}, \aleph_k < |a|\}$$

## Определение

$$\beth_0 := |\omega|; \beth_{k+1} := |\mathcal{P}(\beth_k)|$$

Континуум-гипотеза (Г.Кантор, 1877):  $\aleph_1 = \beth_1$  (не существует мощности, промежуточной между счётной и континуумом).

Обобщённая континуум-гипотеза:  $\aleph_n = \beth_n$  при всех  $n$ .

## Определение

Утверждение  $\alpha$  противоречит аксиоматике:  $\vdash \alpha$  ведёт к противоречию.

Утверждение  $\alpha$  не зависит от аксиоматики:  $\nvdash \alpha$  и  $\nvdash \neg\alpha$ .

Теорема (О независимости континуум-гипотезы, Дж.Коэн, 1963)

Утверждение  $\aleph_1 = \beth_1$  не зависит от аксиоматики ZFC.

# Примеры мощностей множеств

Пример	мощность
$\omega$	$\aleph_0$
$\omega^2, \omega^\omega$	$\aleph_0$
$\mathbb{R}$	$\beth_1$
все непрерывные функции $\mathbb{R} \rightarrow \mathbb{R}$	$\beth_1$
все функции $\mathbb{R} \rightarrow \mathbb{R}$	$\beth_2$

# Как пересчитать вещественные числа (неформально)?

1. Номер вещественного числа — первое упоминание в литературе, т.е.  $\langle j, y, n, p, r, c \rangle$ :
  - $j$  — гёделев номер названия научного журнала (книги);
  - $y$  — год издания;
  - $n$  — номер;
  - $p$  — страница;
  - $r$  — строка;
  - $c$  — позиция
2. Попробуйте предъявить число  $x$ , не имеющее номера? Это рассуждение сразу даст номер.

# Мощность модели и аксиоматизации

## Определение

*Пусть задана модель  $\langle D, F_n, P_n \rangle$  для некоторой теории первого порядка. Её мощностью будем считать мощность  $D$ .*

## Определение

*Пусть задана формальная теория с аксиомами  $\alpha_n$ . Её мощность — мощность множества  $\{\alpha_n\}$ .*

## Пример

*Формальная арифметика, исчисление предикатов, исчисление высказываний — счётно-аксиоматизируемые.*

# Элементарная подмодель

## Определение

$\mathcal{M}' = \langle D', F'_n, P'_n \rangle$  — элементарная подмодель  $\mathcal{M} = \langle D, F_n, P_n \rangle$ , если:

1.  $D' \subseteq D$ ,  $F'_n, P'_n$  — сужение  $F_n, P_n$  (замкнутое на  $D'$ ).
2.  $\mathcal{M} \models \varphi(x_1, \dots, x_n)$  тогда и только тогда, когда  $\mathcal{M}' \models \varphi(x_1, \dots, x_n)$  при  $x_i \in D'$ .

## Пример

Когда сужение  $\mathcal{M}$  не является элементарной подмоделью?

$\forall x. \exists y. x \neq y$ . Истинно в  $\mathbb{N}$ . Но пусть  $D' = \{0\}$ .



# Теорема Лёвенгейма-Сколема

## Теорема

*Пусть  $T$  — множество всех формул теории первого порядка. Пусть теория имеет некоторую модель  $\mathcal{M}$ . Тогда найдётся элементарная подмодель  $\mathcal{M}'$ , причём  $|\mathcal{M}'| = \max(\aleph_0, |T|)$ .*

## Доказательство.

(Схема доказательства)

1. Построим  $D_0$  — множество всех значений, которые упомянуты в языке теории.
2. Будем последовательно пополнять  $D_i$ :  $D_0 \subseteq D_1 \subseteq D_2 \dots$ , следя за мощностью.  $D' = \cup D_i$ .
3. Покажем, что  $\langle D', F_n, P_n \rangle$  — требуемая подмодель.



## Начальный $D_0$

Пусть  $\{f_k^0\}$  — все 0-местные функциональные символы теории.

1.  $D_0 = \{\llbracket f_k^0 \rrbracket\}$ , если есть хотя бы один  $f_k^0$ .
2. Если таких  $f_k^0$  нет, возьмём какое-нибудь одно значение из  $D$ .

Очевидно,  $|D_0| \leq |T|$ .

## Пополнение $D$

Фиксируем некоторый  $D_k$ . Напомним,  $T$  — множество всех формул теории. Рассмотрим  $\varphi \in T$ .

1.  $\varphi$  не имеет свободных переменных — пропустим.
2.  $\varphi$  имеет хотя бы одну свободную переменную  $y$ .
  - 2.1  $\varphi(y, x_1, \dots, x_n)$  при  $y, x_i \in D_k$  бывает истинным и ложным — ничего не меняем
  - 2.2  $\varphi(y, x_1, \dots, x_n)$  при  $y \in D$  и  $x_i \in D_k$  либо всегда истинен, либо всегда ложен — ничего не меняем
  - 2.3  $\varphi(y, x_1, \dots, x_n)$  при  $y, x_i \in D_k$  тождественно истинен или ложен, но при  $y' \in D \setminus D_k$  отличается — добавим  $y'$  к  $D_{k+1}$ . Вместе добавим всевозможные  $\llbracket \theta(y') \rrbracket$ .

Всего добавили не больше  $|T| \cdot |D_k|$ .

$$|\cup D_i| \leq |T| \cdot |D_k| \cdot |\aleph_0| = \max(|T|, |\aleph_0|)$$

## $\mathcal{M}'$ — элементарная подмодель

Индукцией по структуре формул  $\tau \in T$  покажем, что все формулы можно вычислить, и что  $\llbracket \varphi \rrbracket_{\mathcal{M}'} = \llbracket \varphi \rrbracket_{\mathcal{M}}$ .

1. База, 0 связок.  $\tau \equiv P(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ .  
Если  $x_i \in D'$ , то значит, добавлены на некоторых шагах (максимальный пусть  $t$ ). Поэтому в  $D_{t+1}$  можно вычислить формулу, и её значение сохранилось.
2. Переход. Пусть формулы из  $k$  связок сохраняют значения. Рассмотрим  $\tau$  с  $k + 1$  связкой.
  - 2.1  $\tau \equiv \rho \star \sigma$  — очевидно.
  - 2.2  $\tau \equiv \forall y. \varphi(y, x_1, \dots, x_n)$ . Каждый  $x_i$  добавлен на каком-то шаге — максимум  $t$ . Если  $\varphi(y, x_1, \dots, x_n)$  бывает истинен и ложен при  $y_t, y_f \in D$ , то  $y_t, y_f \in D_{t+1}$  (по построению). Поэтому, если  $\mathcal{M} \not\models \forall y. \varphi(y, x_1, \dots, x_n)$ , то и  $\mathcal{M}' \not\models \forall y. \varphi(y, x_1, \dots, x_n)$ . Если же  $\varphi(y, x_1, \dots, x_n)$  не меняется от  $y$ , то тем более  $\llbracket \varphi \rrbracket_{\mathcal{M}'} = \llbracket \varphi \rrbracket_{\mathcal{M}}$ .
  - 2.3  $\tau \equiv \exists y. \varphi(y, x_1, \dots, x_n)$  — аналогично.

## «Парадокс» Сколема

1. Как известно,  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0$ . Однако, ZFC — теория со счётным количеством формул. Значит, существует счётная модель ZFC, то есть  $|\mathbb{R}| = \aleph_0$ . В чём ошибка?
2. У равенств разный смысл, первое — в предметном языке, второе — в метаязыке.