Алгебраические типы данных

Алгебра на типах данных

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

Пример

`(boolean, A -> boolean)` соответствует $2 \cdot (2^A)$

Алгебраический тип данных, тип-сумма

Определение

Отмеченным объединением множеств (дизъюнктным объединением) назовём:

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

Пример

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

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

Пример

boolean := False | True	$B = \{\varnothing\} \uplus \{\varnothing\}$	$Л : \varnothing_L$
angle := Degrees of int | Radians of real	$A := \mathbb{Z} \uplus \mathbb{R}$	$180^\circ : 180_L, \pi_R$

Примеры из языков программирования

```
type angle = record
     case radians : boolean of
         true: (rads: real);
         false: (degs: integer);
     end;
```

```
struct angle {
     bool radians;
     union {
         float rads;
         int degs;
     }
};
```

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`:

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

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

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

- Разбирать.

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

```
match l with
|InL p -> 0
|InR p -> 1 + length (PrR p)
```

В самом низу — элиминатор Case:
$length\ l := Case\ l\ (\lambda p.0)\ (\lambda p.1 + length\ (\pi_R p))$

Алгебраический тип как дизъюнкция

Общие соображения: BHK-интерпретация.
Интуиционистское исчисление высказываний

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

Просто-типизированное лямбда исчисление — придумаем названия

$$\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash In_L A : \alpha \vee \beta} \qquad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash In_R B : \alpha \vee \beta} \qquad \frac{\Gamma \vdash X : \alpha \vee \beta \quad \Gamma \vdash L : \alpha \to \gamma \quad \Gamma \vdash R : \beta \to \gamma}{\Gamma \vdash \text{Case X L R} : \gamma}$$

Пример

Напомним, если $\tau = \varphi = unit$, *то* $\tau \vee \varphi \approx bool$.
Тогда $T^{\tau \vee \varphi} := In_L(), \quad F^{\tau \vee \varphi} := In_R()$. *И, например,*
Not $x :=$ *Case* $x\ (\lambda t.In_R())\ (\lambda t.In_L())$

Реализация алгебраического типа

Просто-типизированное лямбда исчисление:

$$\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash In_L A : \alpha \vee \beta} \qquad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash In_R B : \alpha \vee \beta} \qquad \frac{\Gamma \vdash X : \alpha \vee \beta \quad \Gamma \vdash L : \alpha \to \gamma \quad \Gamma \vdash R : \beta \to \gamma}{\Gamma \vdash \text{Case X L R} : \gamma}$$

Предлагаем такую реализацию:

$$In_L := \lambda x.\lambda t.\lambda f.t\ x, \qquad In_R := \lambda x.\lambda t.\lambda f.f\ x \qquad Case := \lambda x.\lambda l.\lambda r.x\ l\ r$$
$$Case\ (In_L\ X^{\tau})\ L^{\tau\to\gamma}\ R \twoheadrightarrow_{\beta} (In_L\ X)\ L\ R = (\lambda t.\lambda f.t\ X)\ L\ R \twoheadrightarrow_{\beta} (L\ X)^{\gamma}$$

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

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

«Если некоторое утверждение γ истинно всегда, когда оно следует из истинности τ и φ — то либо τ, либо φ истинно». Рассуждение не совсем формально, потому что не хватает кванторов по утверждениям, использующимся неявно:

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

Примеры алгебраических типов

Булевские значения:

$$T_1 := In_L() = \lambda t.\lambda f.t\ () \qquad F_1 := In_R() = \lambda t.\lambda f.f\ () \qquad If_1 := \lambda b.\lambda t.\lambda e.b\ (\lambda p.t)\ (\lambda p.e)$$

Ну или когда аргумент опущен за ненадобностью:

$$T := \lambda t.\lambda f.t \qquad F := \lambda t.\lambda f.f \qquad If := \lambda b.\lambda t.\lambda e.b\ t\ e$$

Списки:

$$Nil := In_L 0 \qquad Cons\ p\ q := In_R\langle p, q\rangle$$

Тогда $[1, 3, 5]$ превращается в $Cons\ 1\ (Cons\ 3\ (Cons\ 5\ Nil))$.
Для простоты раскроем полностью $[1] = Cons\ 1\ Nil$:

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

Мощность	Тип	Высказывание
0	$\bot$	необитаемый тип
1	() : unit	одноэлементный тип
$\|\alpha\| + \|\beta\|$	Either A^α B^β : $\alpha \vee \beta$	тип-сумма, дизъюнкция
$\|\alpha\| \cdot \|\beta\|$	$(A^\alpha, B^\beta) : \alpha \,\&\, \beta$	тип-произведение, конъюнкция
$\|\beta\|^{\|\alpha\|}$	$\lambda x^\alpha.B : \alpha \to \beta$	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*
$\forall x.x \in A \to \exists! y.\langle x, y\rangle \in R$

R — *инъективная функция, если* $\forall x.\forall y.\langle x, t\rangle \in R \;\&\; \langle y, t\rangle \in R \to x = y.$

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

Равномощные множества

Определение

Множество A равномощно B ($|A| = |B|$), если существует биекция $f : A \to B$. Множество A имеет мощность, не превышающую мощности B ($|A| \leq |B|$), если существует инъекция $f : A \to B$.

Теорема Кантора-Бернштейна

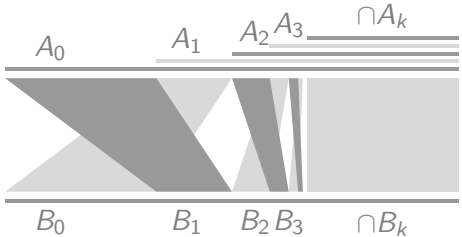
Теорема

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

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

Доказательство.

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

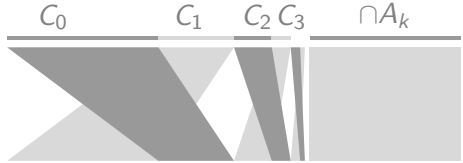


Тогда, если существует $h : A_0 \to A_1$ — биекция, то тогда $g^{-1} \circ h : A \to B$ — требуемая биекция.

□

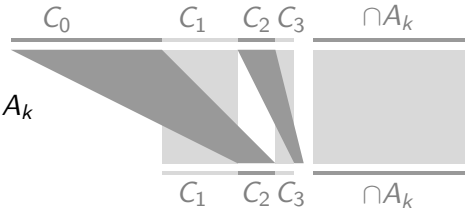
Построение биекции $h : A_0 \to A_1$

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:

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

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: $0.a_0a_1a_2\ldots$. Пусть существует биективная $f : \mathbb{N} \to (0,1)$. По функции найдём значение σ, не являющееся образом никакого натурального числа.

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

□

Теорема Кантора

Теорема

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

Доказательство.

Пусть $S = \{a, b, c, \dots\}$

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

Пусть $f : S \to \mathcal{P}(S)$ — 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

Иерархии $\aleph_n$ и $\beth_n$

Определение

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

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 α *противоречит аксиоматике:* $\vdash \alpha$ *ведёт к противоречию.*
Утверждение α *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
ω	$\aleph_0$
ω^2, ω^ω	$\aleph_0$
$\mathbb{R}$	$\beth_1$
все непрерывные функции $\mathbb{R} \to \mathbb{R}$	$\beth_1$
все функции $\mathbb{R} \to \mathbb{R}$	$\beth_2$

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. Попробуете 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 α_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. $\mathcal{M} \models \varphi(x_1, \ldots, x_n)$ *тогда и только тогда, когда* $\mathcal{M}' \models \varphi(x_1, \ldots, x_n)$ *при* $x_i \in D'$.

Пример

Когда сужение 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: $D_0 \subseteq D_1 \subseteq D_2 \ldots$, 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. $D_0 = \{[\![f_k^0]\!]\}$, 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. φ не имеет свободных переменных — пропустим.
2. φ имеет хотя бы одну свободную переменную y.
   - 2.1 $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ бывает истинным и ложным — ничего не меняем
   - 2.2 $\varphi(y, x_1, \ldots, x_n)$ при $y \in D$ и $x_i \in D_k$ либо всегда истинен, либо всегда ложен — ничего не меняем
   - 2.3 $\varphi(y, x_1, \ldots, x_n)$ 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 $[\![\theta(y')]\!]$.

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 $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.

1. База, 0 связок. $\tau \equiv P(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. 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 τ с $k+1$ связкой.
   - 2.1 $\tau \equiv \rho \star \sigma$ — очевидно.
   - 2.2 $\tau \equiv \forall y.\varphi(y, x_1, \ldots, x_n)$. Каждый x_i добавлен на каком-то шаге — максимум t. Если $\varphi(y, x_1, \ldots, x_n)$ бывает истинен и ложен при $y_t, y_f \in D$, то $y_t, y_f \in D_{t+1}$ (по построению). Поэтому, если $\mathcal{M} \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$, то и $\mathcal{M}' \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$. Если же $\varphi(y, x_1, \ldots, x_n)$ не меняется от y, то тем более $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.
   - 2.3 $\tau \equiv \exists y.\varphi(y, x_1, \ldots, x_n)$ — 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.