

Мотивационный пример про интуиционистскую логику

ВНК-интерпретация — про конструкции, построенные объекты. А пусть конструкция — тип значения, которое может быть вычислено. Тогда:

- ▶ $\alpha \& \beta$ — тип упорядоченной пара значений
- ▶ $\alpha \vee \beta$ — алгебраический тип (тип-сумма)
- ▶ $\alpha \rightarrow \beta$ — тип функций из α в β
- ▶ \perp — значение, не имеющее построения.

Доказательство — значение, *обитающее* в указанном типе. Вот и давайте под доказываем:

$$\vdash 3 : \text{int}$$
$$\vdash \text{fun } x \rightarrow x+1 : \text{int} \rightarrow \text{int}$$

Алгебраический тип (тип-сумма)

Определение

Отмеченное (дизъюнктное) объединение:

$$A \uplus B := \{\langle x, 0 \rangle \mid x \in A\} \cup \{\langle y, 1 \rangle \mid y \in B\}$$

Значение типа $\alpha \vee \beta$ — значение либо типа α , либо типа β , и мы знаем, какого именно. `std::variant` в C++.

Пример

α option — это $\alpha \vee ()$

```
type 'a option = Some of 'a | None
```

```
let print_int_option v = match v with  
  Some x -> print_int x  
  | None   -> print_string "None"
```

```
let csqrt x = if x >= 0. then Some (sqrt x) else None
```

Ложь (необитаемый тип)

Перепишем старый пример чуть иначе:

```
let csqrt x =  
  if x >= 0. then sqrt x  
    else failwith "Cannot compute square root"
```

Какой тип у `csqrt`? Рассмотрим ветки `if`

- ▶ then: $\sqrt{x} : \text{float}$
- ▶ else: `failwith s : \perp` , и поэтому `failwith s : \perp \vdash failwith s : float`

Ветка `else` не возвращает результата — поэтому возвращает любой тип; «из лжи следует всё, что угодно».

Почему мы рассматриваем интуиционистскую логику?

Краткий ответ: семантика аксиомы снятия двойного отрицания сложна и не укладывается в традиционные конструкции языков программирования.

- ▶ Рассмотрим закон снятия двойного отрицания: $M : ((\alpha \rightarrow \perp) \rightarrow \perp) \rightarrow \alpha$.
Необходима отдельная конструкция, поскольку закон не выражается через остальные аксиомы ИИВ. То есть невозможно написать программу с таким типом из рассмотренных выше примитивов (функций, значений, кортежей, алгебраических типов).
- ▶ Попробуем понять, что это за конструкция. Аргумент M — функция $f : (\alpha \rightarrow \perp) \rightarrow \perp$. Функция f , видимо (?), по аргументу $g : \alpha \rightarrow \perp$ угадывает $x : \alpha$ и выполняет вызов $g\ x$. Получается, выражение M должно по функции f как-то угадывать значение x ?
- ▶ Конструкции с таким типом в языках бывают. Например, закон Пирса — как тип для `call/cc` из Scheme. Но это расширение базовых языков.

Изоморфизм Карри-Ховарда

Программа	исчисление высказываний
Выражение	доказательство
Тип выражения	высказывание
Тип функции	импликация
Упорядоченная пара	Конъюнкция
Алгебраический тип	Дизъюнкция
Необитаемый тип	Ложь

Непрерывность

Определение

Функция $f : X \rightarrow Y$ непрерывна, если прообраз любого открытого множества открыт.

Пример

Функция $f : \mathbb{N} \rightarrow \mathbb{R}$ всегда непрерывна (при дискретной топологии на \mathbb{N}), поскольку любое множество в \mathbb{N} открыто.

Компактность

Определение

Будем говорить, что множество компактно, если из любого его открытого покрытия можно выбрать конечное подпокрытие

Пример

Множество $\{0, 1\}$ в дискретной топологии компактно.

Пример

Интервал $(0, 1)$ в \mathbb{R} не компактен — например, рассмотрим покрытие $\{(\varepsilon, 1) \mid \varepsilon \in (0, 1)\}$

Подпространства и связные множества

Определение

Пространство $\langle X_1, \Omega_1 \rangle$ — подпространство пространства $\langle X, \Omega \rangle$, если $X_1 \subseteq X$ и $\Omega_1 = \{A \cap X_1 \mid A \in \Omega\}$.

Пример

$[0, 1]$ с евклидовой топологией на отрезке — подпространство \mathbb{R} . $[0, 0.5)$ открыто в $[0, 1]$, так как $[0, 0.5) = (-0.5, 0.5) \cap [0, 1]$.

Определение

Пространство $\langle X, \Omega \rangle$ связно, если нет $A, B \in \Omega$, что $A \cup B = X$, $A \cap B = \emptyset$ и $A, B \neq \emptyset$.

Пример

Пространство $(0, 1] \cup [2, 3)$ в \mathbb{R} несвязно: возьмём $A = (0, 1]$ и $B = [2, 3)$.

Дискретное топологическое пространство $\langle X, \mathcal{P}(X) \rangle$ несвязно при $|X| > 1$: пусть $a \in X$, тогда $A = \{a\}$ и $B = X \setminus A$.

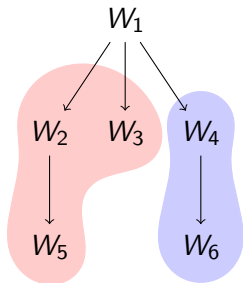
Топология на деревьях

Определение

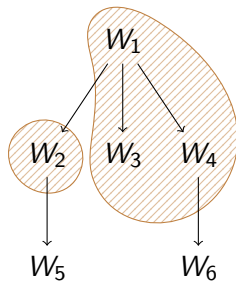
Пусть некоторый лес задан конечным множеством вершин V и отношением (\preceq) , связывающим предков и потомков ($a \preceq b$, если b — потомок a). Тогда подмножество его вершин $X \subseteq V$ назовём открытым, если из $a \in X$ и $a \preceq b$ следует, что $b \in X$.

Пример

Открыты



Не открыты



Связность деревьев

Лемма

Лес связан (является одним деревом) тогда и только тогда, когда соответствующее ему топологическое пространство связно.

Доказательство.

1. Лес связан: пусть не так и найдутся открытые непустые A, B , что $A \cup B = V$ и $A \cap B = \emptyset$. Пусть $v \in V$ — корень дерева и пусть $v \in A$ (для определённости). Тогда $A = \{x \mid v \preceq x\}$ и $B = \emptyset$.
2. Пусть лес топологически связан, но есть несколько разных корней v_1, v_2, \dots, v_k . Возьмём $A_i = \{x \mid v_i \preceq x\}$. Тогда все A_i открыты, непусты, дизъюнкты и $V = \cup A_i$.



Пишем скобки или нет?

Вы как пишете: $\sin x$ или $\sin(x)$?

Пишем скобки или нет?

Вы как пишете: $\sin x$ или $\sin(x)$?

```
int main () {  
    return sizeof 0;  
}
```

Пишем скобки или нет?

Вы как пишете: $\sin x$ или $\sin(x)$?

```
int main () {  
    return sizeof 0;  
}
```

Соглашение о записи:

$$\text{sizeof } \emptyset = \text{sizeof}(\emptyset) = 0$$

но:

$$\text{sizeof}\{\emptyset\} = \text{sizeof}(\{\emptyset\}) = 1$$

Минимальные и максимальные элементы

Определение

Множество нижних граней $X \subseteq \mathcal{U}$: $\text{lwb}_{\mathcal{U}} X = \{y \in \mathcal{U} \mid y \preceq x \text{ при всех } x \in X\}$.

Множество верхних граней $X \subseteq \mathcal{U}$: $\text{upb}_{\mathcal{U}} X = \{y \in \mathcal{U} \mid x \preceq y \text{ при всех } x \in X\}$.

Определение

минимальный ($t \in X$): нет меньшего при всех $y \in X$, $y \preceq t$ влечёт $y = t$

максимальный ($t \in X$): нет большего при всех $y \in X$, $t \preceq y$ влечёт $y = t$

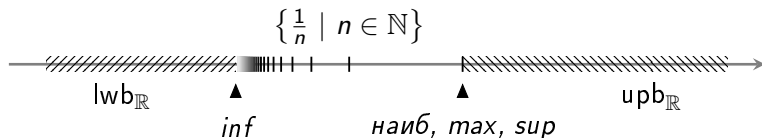
наименьший ($t \in X$): меньше всех при всех $y \in X$ выполнено $t \preceq y$

наибольший ($t \in X$): больше всех при всех $y \in X$ выполнено $y \preceq t$

инфимум: наибольшая нижняя грань $\inf_{\mathcal{U}} X = \text{наиб}(\text{lwb}_{\mathcal{U}} X)$

супремум: наименьшая верхняя грань $\sup_{\mathcal{U}} X = \text{наим}(\text{upb}_{\mathcal{U}} X)$

Пример



Пример: делимость

На \mathbb{N} положим $a \preceq b$, если $b \div a$.

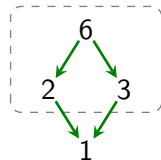
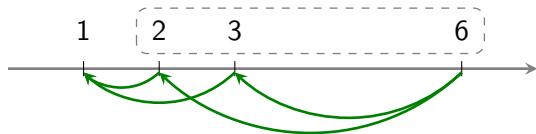
Пример

Множество $\{2, 3, 6\}$

Минимальные: 2, 3 $2 \div x$ влечёт $x = 1$ или $x = 2$, то же про 3

Наименьший: отсутствует $2 \nmid 3$ и $3 \nmid 2$

Инфимум: 1 $1 \preceq x$ при всех $x \in \mathbb{N}$



Пример: делимость

На \mathbb{N} положим $a \preceq b$, если $b \div a$.

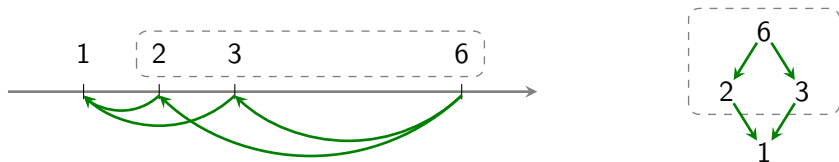
Пример

Множество $\{2, 3, 6\}$

Минимальные: 2, 3 $2 \div x$ влечёт $x = 1$ или $x = 2$, то же про 3

Наименьший: отсутствует $2 \nprec 3$ и $3 \nprec 2$

Инфимум: 1 $1 \preceq x$ при всех $x \in \mathbb{N}$



Пример

Рассмотрим $X = \{1; 1.4; 1.41; 1.414; 1.4142; \dots\}$ — множество десятичных приближений $\sqrt{2}$, $\preceq = \leq$. Тогда $\text{urb}_{\mathbb{Q}} X$ состоит из рациональных чисел, больших $\sqrt{2}$. При этом $\sqrt{2} \notin \text{urb}_{\mathbb{Q}} X$, а значит $\sup_{\mathbb{Q}} X$ не определён.

Пример: внутренность множества

Определение (внутренность множества)

Рассмотрим $\langle X, \Omega \rangle$ и возьмём (\subseteq) как отношение частичного порядка на $\mathcal{P}(X)$. Тогда $A^\circ := \inf_{\Omega}(\{A\})$.

Теорема

A° определена для любого A .

Доказательство.

Пусть $V = \text{lwb}_{\Omega}\{A\} = \{Q \in \Omega \mid Q \subseteq A\}$. Тогда $\inf_{\Omega}\{A\} = \bigcup V$.

Напомним, $\inf_{\mathcal{U}} T = \text{наиб}(\text{lwb}_{\mathcal{U}} T)$.

1. Покажем принадлежность: $\bigcup V \subseteq A$ и $\bigcup V \in \Omega$ как объединение открытых.
2. Покажем, что все из V меньше или равны: пусть $X \in V$, то есть $V = \{X, \dots\}$, тогда $X \subseteq X \cup \dots$, тогда $X \subseteq \bigcup V$



Решётка

Определение

Решёткой называется упорядоченная пара: $\langle X, (\preceq) \rangle$, где X — некоторое множество, а (\preceq) — частичный порядок на X , такой, что для любых $a, b \in X$ определены $a + b = \sup\{a, b\}$ и $a \cdot b = \inf\{a, b\}$.

То есть, $a + b$ — наименьший элемент c , что $a \preceq c$ и $b \preceq c$.

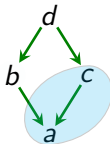
Пример

$\langle \Omega, (\subseteq) \rangle$ — решётка. $\langle \mathbb{N} \setminus \{1\}, (:) \rangle$ — не решётка.

Псевдодополнение

Псевдодополнением $a \rightarrow b$ называется наибольший из $\{x \mid a \cdot x \preceq b\}$.

Пример



$$a \cdot b = a$$

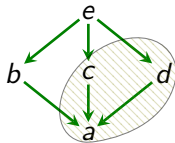
$$b \cdot b = b$$

$$c \cdot b = a$$

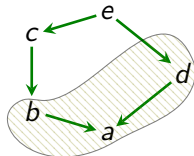
$$d \cdot b = b$$

Здесь $b \rightarrow c = \text{наиб}\{x \mid b \cdot x \preceq c\} = \text{наиб}\{a, c\} = c$

Пример (нет псевдодополнения: алмаз и пентагон)



$$b \rightarrow c = \text{наиб}\{a, c, d\}$$



$$c \rightarrow b = \text{наиб}\{a, b, d\}$$

Особые решётки

Определение

Дистрибутивной решёткой называется такая, что для любых a, b, c выполнено
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Определение

Импликативная решётка — такая, в которой для любых элементов есть псевдодополнение.

Лемма

Любая импликативная решётка — дистрибутивна.

Ноль и один

Определение

0 — наименьший элемент решётки, а 1 — наибольший элемент решётки

Лемма

В любой импликативной решётке $\langle X, (\preceq) \rangle$ есть 1

Доказательство.

Рассмотрим $a \rightarrow a$, тогда $a \rightarrow a = \text{наиб}\{c \mid a \cdot c \preceq a\} = \text{наиб}X = 1$. □

Определение

Импликативная решётка с 0 — псевдобулева алгебра (алгебра Гейтинга). В такой решётке определено $\sim a := a \rightarrow 0$

Определение

Булева алгебра — псевдобулева алгебра, в которой $a + \sim a = 1$ для всех a .

Булева алгебра является булевой алгеброй в смысле решёток

Доказательство.

Символы булевой алгебры: $(\&), (\vee), (\neg), \text{Л}, \text{И}$.

Символы решёток: $(+), (\cdot), (\rightarrow), (\sim), 0, 1$

Упорядочивание: $\text{Л} \leq \text{И}$.

1. $a \& b = \min(a, b)$, $a \vee b = \max(a, b)$ (анализ таблицы истинности), отсюда $a \cdot b = a \& b$ и $a + b = a \vee b$.

2. $a \rightarrow b = \neg a \vee b$, так как:

$$a \rightarrow b = \text{наиб}\{c \mid c \& a \leq b\} = \begin{cases} \neg a, & b = \text{Л} \\ \text{И}, & b = \text{И} \end{cases}$$

3. $0 = \min\{\text{И}, \text{Л}\} = \text{Л}$, $1 = \max\{\text{И}, \text{Л}\} = \text{И}$, $\sim a = a \rightarrow 0 = \neg a \vee \text{Л} = \neg a$.

Заметим, что $a + \sim a = a \vee \neg a = \text{И}$.

Итого: булева алгебра — импликативная решётка с 0 и с $a + \sim a = 1$.



Множества и топологии как решётки

Лемма

$\langle \mathcal{P}(X), (\subseteq) \rangle$ — булева алгебра.

Доказательство.

$a \rightarrow b = \text{наиб}\{c \subseteq X \mid a \cap c \subseteq b\}$. Т.е. наибольшее, не содержащее точек из $a \setminus b$.

Т.е. $X \setminus (a \setminus b)$. То есть $(X \setminus a) \cup b$.

$$a + \sim a = a \cup (X \setminus a) \cup \emptyset = X$$



Лемма

$\langle \Omega, (\subseteq) \rangle$ — псевдобулева алгебра.

Доказательство.

$a \rightarrow b = \text{наиб}\{c \in \Omega \mid a \cap c \subseteq b\}$. Т.е. наибольшее открытое, не содержащее точек из $a \setminus b$. То есть, $(X \setminus (a \setminus b))^\circ$. То есть, $((X \setminus a) \cup b)^\circ$.



Решётки и исчисление высказываний

Определение

Пусть некоторое исчисление высказываний оценивается значениями из некоторой решётки. Назовём оценку согласованной с исчислением, если $\llbracket \alpha \& \beta \rrbracket = \llbracket \alpha \rrbracket \cdot \llbracket \beta \rrbracket$, $\llbracket \alpha \vee \beta \rrbracket = \llbracket \alpha \rrbracket + \llbracket \beta \rrbracket$, $\llbracket \alpha \rightarrow \beta \rrbracket = \llbracket \alpha \rrbracket \rightarrow \llbracket \beta \rrbracket$, $\llbracket \neg \alpha \rrbracket = \sim \llbracket \alpha \rrbracket$, $\llbracket A \& \neg A \rrbracket = 0$, $\llbracket A \rightarrow A \rrbracket = 1$.

Теорема

Любая псевдобулева алгебра, являющаяся согласованной оценкой интуиционистского исчисления высказываний, является его корректной моделью: если $\vdash \alpha$, то $\llbracket \alpha \rrbracket = 1$.

Теорема

Любая булева алгебра, являющаяся согласованной оценкой классического исчисления высказываний, является его корректной моделью: если $\vdash \alpha$, то $\llbracket \alpha \rrbracket = 1$.

Алгебра Линденбаума

Определение

Определим предпорядок на высказываниях: $\alpha \preceq \beta := \alpha \vdash \beta$ в интуиционистском исчислении высказываний. Также $\alpha \approx \beta$, если $\alpha \preceq \beta$ и $\beta \preceq \alpha$.

Определение

Пусть L — множество всех высказываний. Тогда алгебра Линденбаума $\mathcal{L} = L/\approx$.

Теорема

\mathcal{L} — псевдобулева алгебра.

Схема доказательства.

Надо показать, что (\preceq) есть отношение порядка на \mathcal{L} , что $[\alpha \vee \beta]_{\mathcal{L}} = [\alpha]_{\mathcal{L}} + [\beta]_{\mathcal{L}}$, $[\alpha \& \beta]_{\mathcal{L}} = [\alpha]_{\mathcal{L}} \cdot [\beta]_{\mathcal{L}}$, импликация есть псевдодополнение, $[A \& \neg A]_{\mathcal{L}} = 0$, $[\alpha]_{\mathcal{L}} \rightarrow 0 = [\neg \alpha]_{\mathcal{L}}$. □

Полнота псевдобулевых алгебр

Теорема

Пусть $\llbracket \alpha \rrbracket = [\alpha]_{\mathcal{L}}$. Такая оценка интуиционистского исчисления высказываний алгеброй Линденбаума является согласованной.

Теорема

Интуиционистское исчисление высказываний полно в псевдобулевых алгебрах: если $\models \alpha$ во всех псевдобулевых алгебрах, то $\vdash \alpha$.

Доказательство.

Возьмём в качестве модели исчисления алгебру Линденбаума: $\llbracket \alpha \rrbracket = [\alpha]_{\mathcal{L}}$. Пусть $\models \alpha$. Тогда $\llbracket \alpha \rrbracket = 1$ во всех псевдобулевых алгебрах, в том числе и $\llbracket \alpha \rrbracket = 1_{\mathcal{L}}$. То есть $[\alpha]_{\mathcal{L}} = [A \rightarrow A]_{\mathcal{L}}$. То есть $A \rightarrow A \approx \alpha$. Значит, в частности, $A \rightarrow A \vdash \alpha$. Значит, $\vdash \alpha$.

