

Лекция 20–21 октября

Функции



Функции и отображения

*Функция ненасыщена: она содержит место, которое
заполняется аргументом.*

— Готлоб Фреге

Что такое вычисление?

«Вычислить» — значит взять вход, применить правило и получить выход.

Каждая программа работает именно так.

- Калькулятор.
- Компилятор.
- Поисковая система.

Всё это — функции, применённые к конкретному входу.

Вход, правило и выход — три части любого вычисления.

Функция — математическая абстракция вычисления.

Функция как отношение

Определение 1

Бинарное отношение $f \subseteq A \times B$ называется **функцией** из A в B , если:

- для каждого $a \in A$ найдётся $b \in B$ с $(a, b) \in f$;
- из $(a, b_1) \in f$ и $(a, b_2) \in f$ следует $b_1 = b_2$.

Каждый вход имеет ровно один выход.

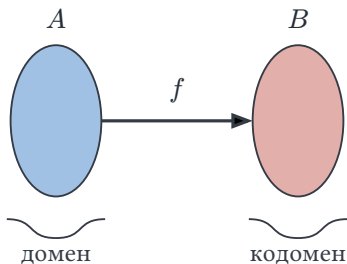
Пример

$A = \{1, 2\}$, $B = \{a, b\}$.

- $f_1 = \{(1, a), (2, b)\}$ — функция.
- $f_2 = \{(1, a), (1, b)\}$ — не функция: входу 1 отвечают два выхода.
- $f_3 = \{(1, a)\}$ — функция на $\{1\}$, но не на $\{1, 2\}$: у входа 2 нет образа.

Части функции

Функция сопоставляет два множества.



- A — область определения (*domain*).
- B — кодомен.
- Образ $f(X)$ — что функция реально производит.
- Прообраз $f^{-1}(Y)$ — какие входы ведут к заданному выходу.

Образ и прообраз

Определение 2

Образ множества $X \subseteq A$:

$$f(X) = \{f(x) \mid x \in X\}.$$

Прообраз множества $Y \subseteq B$:

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Пример

$$f : \{1, 2, 3\} \rightarrow \{a, b\}, f = \{(1, a), (2, b), (3, a)\}.$$

$$f^{-1}(a) = \{1, 3\} \text{ — два входа ведут к } a.$$

$$f^{-1}(b) = \{2\} \text{ — один вход ведёт к } b.$$

Тотальные и частичные функции

Определение 3

- **Тотальная** функция определена для каждого $a \in A$: $f : A \rightarrow B$.
- **Частичная** функция определена лишь на подмножестве A : $f : A \mapsto B$.

Пример

$f(x) = \frac{1}{x}$ частична на $\mathbb{R}$: в точке $x = 0$ не определена.

На суженной области $\mathbb{R} \setminus \{0\}$ та же формула — тотальная функция.

Выбор области определения меняет статус функции.

Сужение превращает частичную функцию в тотальную.

Частичные функции и вычисление

Частичная функция — честная модель вычисления, которое может не завершиться.

- Программа может бросить исключение, уйти в бесконечный цикл, аварийно завершиться.
- Тотальная функция — вычисление, которое всегда завершается.

Проблема остановки спрашивает, завершится ли программа на данном входе, если известно её описание.

Ответ — нет.

Языки с доказанной тотальностью (Coq, Agda) отвергают функции без доказательства того, что вычисление завершается.

График функции

Определение 4

График функции $f : A \rightarrow B$ — множество пар $\{(a, f(a)) \mid a \in A\}$.

Это сама функция, рассматриваемая как бинарное отношение.

Пример

$f(x) = x^2$ на $\{1, 2, 3\}$: график — $\{(1, 1), (2, 4), (3, 9)\}$.

Формула — ещё не функция.

Окружность $x^2 + y^2 = 1$ — формула без функции: при $x = 0$ допустимы два y .

Инъекция

Определение 5

$f : A \rightarrow B$ **инъективна**, если для любых $a_1, a_2 \in A$ из $f(a_1) = f(a_2)$ следует $a_1 = a_2$.

Пример

$f(x) = 2x + 1$ инъективна.

$g(x) = x^2$ не инъективна: $g(2) = g(-2) = 4$.

Инъективность — условие про *разные* входы: из $a_1 \neq a_2$ следует $f(a_1) \neq f(a_2)$, а «каждому входу ровно один выход» — это определение функции.

Для конечных множеств инъекция возможна лишь при $|A| \leq |B|$.

Функция не обязана покрывать весь кодомен: у $f : \{1, 2\} \rightarrow \{a, b, c\}$ с $f(1) = a$, $f(2) = b$ точка c не достигнута — покрытие кодомена отдельное свойство.

Сюръекция

Определение 6

f сюръективна, если каждый элемент кодомена достигается:

$$\forall b \in B. \exists a \in A. f(a) = b.$$

Эквивалентно: $f(A) = B$.

Пример

$f(x) = x^3$ сюръективна на $\mathbb{R}$.

$g(x) = e^x$ не сюръективна: ноль и отрицательные числа недостижимы.

Сюръективность зависит не от формулы, а от кодомена.

e^x сюръективна как отображение $\mathbb{R} \rightarrow \mathbb{R}^+$, но не $\mathbb{R} \rightarrow \mathbb{R}$.

Биекция

Определение 7

f биективна, если она одновременно инъективна и сюръективна.

Пример

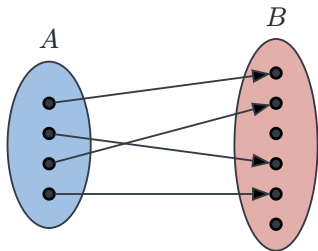
$f : \{1, 2, 3\} \rightarrow \{a, b, c\}$ с $f(1) = a$, $f(2) = b$, $f(3) = c$ — биекция. $g(x) = x^2$ на $\mathbb{R}$ — не биекция: не сюръективна.

Только биекция имеет полноценную обратную функцию:

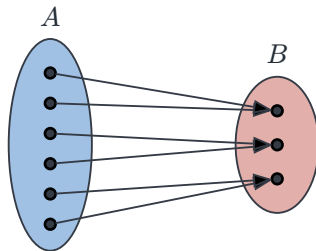
$$f^{-1} \circ f = \text{id}_A \quad \text{и} \quad f \circ f^{-1} = \text{id}_B.$$

Для конечных множеств биекция возможна лишь при $|A| = |B|$.

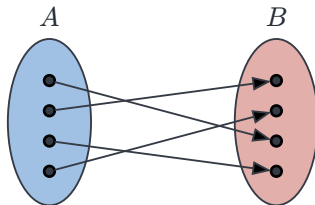
Диаграммы отображений



Инъекция



Сюръекция



Биекция

- Инъекция — каждый выход достигнут не более одного раза.
- Сюръекция — каждый выход достигнут хотя бы один раз.
- Биекция — каждый выход достигнут ровно один раз.

Критерии мощности

Тип	Условие	Мощность	Обратная
Инъекция	$a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)$	$ A \leq B $	левая $g \circ f = \text{id}_A$
Сюръекция	$\forall b \in B. \exists a \in A. f(a) = b$	$ A \geq B $	правая $f \circ g = \text{id}_B$
Биекция	инъекция + сюръекция	$ A = B $	двусторонняя f^{-1}

Для конечных множеств одинакового размера инъекция автоматически биективна.

Для бесконечных — нет: $f(n) = 2n$ инъективна, но не сюръективна.

Как измерять бесконечные множества — следующая лекция.

Прообраз и обратная функция

$f^{-1}(b)$ — **прообраз**: множество всех входов, отображающихся в b .

$f^{-1} : B \rightarrow A$ — **обратная функция**: существует только для биекций.

Пример

$f(x) = x^2$ на $\mathbb{R}$.

$f^{-1}(4) = \{-2, 2\}$ — прообраз, определён всегда.

Обратной функции f^{-1} нет: f не инъективна.

Пример: $f(x) = 2x + 1$

Рассмотрим $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = 2x + 1$.

Пример

Инъективность: из $f(a) = f(b)$ следует $2a + 1 = 2b + 1$, значит $a = b$.

Сюръективность: из $2x + 1 = y$ следует $x = \frac{y-1}{2}$.

Для нечётного y решение целое, для чётного — нет.

На $\mathbb{Z}$ функция инъективна, но не сюръективна: чётные числа недостижимы.

На множестве нечётных чисел $\{2k + 1 \mid k \in \mathbb{Z}\}$ та же формула — биекция.

Инъекция и код

- Кодирование символов (ASCII) и кодирование данных (Base64) инъективны — потому возможно однозначное декодирование.
- Сериализация и десериализация — пара взаимно обратных функций: биекция между объектами и представлениями.
- Криптографические хеши не инъективны: ключей больше, чем отпечатков.

Если $|A| > |B|$, инъекция $f : A \rightarrow B$ невозможна.

Это принцип Дирихле — коллизии неизбежны.

Композиция, образ и прообраз



Если я видел дальше других, то потому, что стоял на плечах гигантов.

— *Исаак Ньютон*

Композиция

Две функции подряд — одна составная: сначала f , затем g .

Определение 8

Композиция $g \circ f$ функций $f : A \rightarrow B$ и $g : B \rightarrow C$:

$$(g \circ f)(a) = g(f(a)).$$

Композиция ассоциативна: $h \circ (g \circ f) = (h \circ g) \circ f$.

Но не коммутативна: $g \circ f \neq f \circ g$ в общем случае.

Пример

$f(x) = x + 1$, $g(x) = x^2$ на $\mathbb{R}$.

$(g \circ f)(x) = (x + 1)^2$, а $(f \circ g)(x) = x^2 + 1$ — порядок имеет значение.

Композиция сохраняет тип

Теорема 1 (Композиция сохраняет свойства)

- Если f и g инъективны, то $g \circ f$ инъективна.
- Если f и g сюръективны, то $g \circ f$ сюръективна.
- Если f и g биективны, то $g \circ f$ биективна.

Доказательство

Инъективность: из $(g \circ f)(a_1) = (g \circ f)(a_2)$ следует $g(f(a_1)) = g(f(a_2))$.

Инъективность g даёт $f(a_1) = f(a_2)$, а f — $a_1 = a_2$.

Сюръективность: $c \in C$ достигается как $g(b)$, а b — как $f(a)$, откуда $(g \circ f)(a) = c$.

Корректность целого выводится из корректности частей — принцип модульной верификации.

Обратная композиции

Теорема 2 (Обратная композиции)

Если $f : A \rightarrow B$ и $g : B \rightarrow C$ биективны, то

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Доказательство

Проверим композицию: $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ \text{id}_B \circ f = \text{id}_A$.

Симметричный подсчёт в другую сторону даёт id_C .

Порядок меняется: «раздеваться» нужно в обратном порядке.

Сначала снять g , затем f .

Композиция и код

- Конвейеры: $x \mid > f \mid > g \mid > h$ — композиция, записанная слева направо.
- Пайплайны в командной строке: `rs | gper` — композиция фильтров.
- Модульная верификация: каждый шаг корректен — корректен и конвейер.

Образ объединения и пересечения

Теорема 3 (Образ и операции)

$$f(A \cup B) = f(A) \cup f(B)$$

$$f(A \cap B) \subseteq f(A) \cap f(B)$$

Доказательство

$y \in f(A \cup B)$, если найдётся $x \in A \cup B$ с $f(x) = y$, то есть $x \in A$ или $x \in B$ — ровно $y \in f(A)$ или $y \in f(B)$.

Для пересечения включение может быть строгим: разные входы сливаются в один выход.

Пример

$f(x) = x^2$: $f(\{-1\} \cap \{1\}) = \emptyset$, но $f(\{-1\}) \cap f(\{1\}) = \{1\}$ — пересечение строгое.

Когда образ точен?

Образ может терять информацию: разные входы сливаются в один выход.

Инъекция запрещает слияния — и сохраняет пересечения.

Прообраз сохраняет всё

Теорема 4 (Прообраз и операции)

$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$$

$$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

$$f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$$

Доказательство

$a \in f^{-1}(C \cup D)$, если $f(a) \in C \cup D$, то есть $f(a) \in C$ или $f(a) \in D$ — ровно $a \in f^{-1}(C)$ или $a \in f^{-1}(D)$.

Остальные тождества — тем же ходом: прообраз дословно повторяет булеву операцию.

Пример

Прообраз сохраняет всё [2]

$$f(x) = x^2: f^{-1}(\{1, 4\}) = \{-2, -1, 1, 2\}.$$

$$\text{Прообраз пересечения точен: } f^{-1}(\{1\} \cap \{4\}) = \emptyset = f^{-1}(\{1\}) \cap f^{-1}(\{4\}).$$

Прообраз коммутирует со всеми булевыми операциями: объединением, пересечением, разностью.

Образ — только с объединением.

Характеристическая функция

Определение 9

Характеристическая функция множества $X \subseteq U$: $\chi_X(x) = 1$ при $x \in X$, иначе 0.

Пример

$U = \{1, \dots, 10\}$, $P = \{2, 3, 5, 7\}$:

$$\sum_{x=1}^{10} \chi_P(x) = 4$$

— количество простых чисел.

$|X| = \sum_{x \in U} \chi_X(x)$ — мощность есть сумма значений характеристической функции.

Битовые маски из лекции о множествах — это χ_X , записанная двоично.

Пол и потолок

Определение 10

$\lfloor x \rfloor$ — наибольшее целое, не превышающее x .

$\lceil x \rceil$ — наименьшее целое, не меньшее x .

Пример

$\lfloor 3.7 \rfloor = 3, \lceil 3.7 \rceil = 4.$

$\lfloor -3.7 \rfloor = -4, \lceil -3.7 \rceil = -3.$

Бинарный поиск делает $\lfloor \log_2 n \rfloor + 1$ сравнений.

Разбиение n элементов на блоки размера k требует $\lceil \frac{n}{k} \rceil$ блоков.

Нотация Айверсона

Определение 11

$[P]$ равно 1, если P истинно, и 0 иначе.

Преобразует логическое условие в алгебраическое выражение.

Пример

Число чётных чисел от 1 до n :

$$\sum_{i=1}^n [i \text{ чётно}] = \left\lfloor \frac{n}{2} \right\rfloor.$$

Число простых, не превышающих n : $\pi(n) = \sum_{k=1}^n [k \text{ простое}]$.

Условие становится частью формулы, а не окружающего текста.

Лямбда-абстракция

Определение 12

Нотация $\lambda x \in A \cdot e(x)$ — **лямбда-абстракция**: функция, отображающая x в $e(x)$, без имени.

Пример

$\lambda x \in \mathbb{R} \cdot x^2 + 2x + 1$ — функция, которая по x выдаёт $x^2 + 2x + 1$.

Подстановка $x = 3$ даёт $9 + 6 + 1 = 16$.

Отображение списка: `map(lambda x: 2*x + 1, [0, 1, 2, 3])` даёт `[1, 3, 5, 7]`.

Имя — лишняя сущность, когда функция используется один раз.

Лекция 7: что мы поняли?

- Функция — отношение, в котором каждый вход имеет ровно один выход. Формула задаёт функцию только вместе с областью определения и кодоменом.
- Инъекция, сюръекция и биекция классифицируют, сколько входов ведёт в один выход. Для конечных множеств это условия на мощности.
- Композиция сохраняет инъективность, сюръективность и биективность — корректность целого из корректности частей.
- Прообраз коммутирует со всеми булевыми операциями, а образ может терять информацию.
- Биекция — совпадение размеров. Для бесконечных множеств она станет инструментом измерения — следующая лекция.

Вопросы для самопроверки

1. Какие из отношений $R \subseteq \{1, 2, 3\} \times \{a, b\}$ являются функциями? $R_1 = \{(1, a), (2, b), (3, a)\}$, $R_2 = \{(1, a), (1, b), (2, a)\}$.
2. Найдите $f(A)$ и $f^{-1}(B)$ для $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$, $A = \{-2, -1, 0, 1, 2\}$, $B = \{0, 1, 4, 9\}$.
3. Приведите пример функции $f : \mathbb{N} \rightarrow \mathbb{N}$, сюръективной, но не инъективной.
4. Докажите: если $g \circ f$ инъективна, то f инъективна.
5. Почему $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, и почему порядок меняется?
6. Почему прообраз сохраняет пересечение, а образ — не всегда?
7. Запишите лямбдой функцию, удваивающую число.

Чтение к следующей паре

- m06 — «Инъекция», «Сюръекция», «Биекция», «Композиция функций», «Образ и прообраз».
- Флеш-опросник — в начале лекции 8.