

Лекция

15–16 сентября

Предикаты и доказательства



Предикаты и кванторы

Математику можно определить как предмет, в котором мы никогда не знаем ни того, о чём говорим, ни того, истинно ли то, что мы говорим.

— Бертран Рассел

Зачем нужны кванторы?

«Квадрат любого числа неотрицателен» — это бесконечный перечень фактов:

$$0^2 \geq 0, \quad 1^2 \geq 0, \quad 2^2 \geq 0, \quad \dots$$

Выписать такой перечень целиком нельзя.

Квантор сжимает его в одну строку:

$$\forall x. x^2 \geq 0$$

Сегодня в языке появляются **предикаты** — утверждения с переменной — а также **кванторы** $\forall$ и $\exists$, превращающие их в высказывания.

Предикаты

Высказывание может зависеть от переменной.

Определение 1

Предикат $P(x)$ — это утверждение, истинность которого зависит от значения переменной x .

Определение 2

Предметная область (*domain of discourse*) — множество допустимых значений x .

Подстановка значения

Пример

- Пусть $P(x)$: « x — чётное число».
- Тогда $P(2)$ истинно, а $P(3)$ ложно.
- Предикат $P(x)$ — не высказывание: его истинность определена только после подстановки.

Предикат — шаблон.

Подстановка значения превращает шаблон в высказывание.

Квантор всеобщности

Определение 3

Запись $\forall x. P(x)$ читается «для всех x истинно $P(x)$ ».

Знак $\forall$ — **квантор всеобщности**.

Пример

«Все студенты сдали экзамен» — $\forall x. S(x)$.

Здесь $S(x)$: « x сдал экзамен», а предметная область — студенты.

Для любого натурального x выполнено $x^2 \geq 0$.

«Все сдали экзамен» ложно лишь тогда, когда кто-то не сдал.

В пустой аудитории лгать не о ком — утверждение истинно.

Квантор существования

Определение 4

Запись $\exists x. P(x)$ читается «существует x , для которого истинно $P(x)$ ».

Знак $\exists$ — **квантор существования**.

Пример

«Некоторый студент опоздал»: $\exists x. L(x)$.

Здесь $L(x)$: « x опоздал».

Пример

Существует целое x , для которого $x^2 = 9$: это $x = 3$ или $x = -3$.

Свободные и связанные переменные

Определение 5

Переменная под знаком квантора — **связанная**, вне кванторов — **свободная**.

Область действия квантора — формула, к которой он применяется.

Пример

В $\exists x. (P(x) \wedge Q(y))$ переменная x связана квантором, а y свободна.

Формула со свободной переменной — по-прежнему предикат: её истинность зависит от y .

Отрицание кванторов

Теорема 1 (Отрицание кванторов)

$$\neg(\forall x. P(x)) \equiv \exists x. \neg P(x)$$

$$\neg(\exists x. P(x)) \equiv \forall x. \neg P(x)$$

Доказательство

Первая эквивалентность. $\neg\forall x. P(x)$ истинно ровно когда не все x дают $P(x)$, то есть существует x с ложным $P(x)$ — это $\exists x. \neg P(x)$.

Вторая. $\neg\exists x. P(x)$ значит, что ни один x не даёт $P(x)$, то есть $\forall x. \neg P(x)$.

Отрицание проносится сквозь квантор: квантор меняется, предикат отрицается.

«Не все» — не «все не»

Пример

«Не все студенты сдали экзамен» — это $\exists x. \neg S(x)$: хотя бы один не сдал.

Это не «все не сдали»: $\forall x. \neg S(x)$ означает, что не сдал никто.

Порядок кванторов

Порядок кванторов меняет смысл утверждения.

Пример

1. «Для каждого человека существует мать»: $\forall x \exists y. M(y, x)$.
2. «Существует человек, который мать для всех»: $\exists y \forall x. M(y, x)$.

Здесь $M(y, x)$: « y — мать x ».

Первое утверждение истинно, второе — абсурдно.

Но формально они отличаются только порядком кванторов.

Порядок кванторов над числами

Пример

Над натуральными числами:

$$\forall x \exists y. y > x$$

(истинно: для каждого x годится свой $y = x + 1$)

$$\exists y \forall x. y > x$$

(ложно: числа, большего всех натуральных, нет)

«Для каждого x ищем свой y » и «один y на все x » — разные утверждения.

Ограниченные кванторы

Часто область ясна из контекста: «для всех студентов», «для каждого элемента массива».

Определение 6

- $\forall x \in A. P(x)$ — «для всех x из множества A истинно $P(x)$ ».
- $\exists x \in A. P(x)$ — «существует x из A , для которого истинно $P(x)$ ».

Пример

Пусть $A = \{1, 2, 3\}$.

- $\forall x \in A. x < 5$ истинно: все три элемента меньше 5.
- $\exists x \in A. x > 2$ истинно: подходит $x = 3$.
- $\exists x \in A. x > 3$ ложно: такого элемента в A нет.

Развёртка ограниченных кванторов

Ограниченные кванторы — не новые:

- $\forall x \in A. P(x)$ — это $\forall x. (x \in A) \rightarrow P(x)$,
- $\exists x \in A. P(x)$ — это $\exists x. (x \in A) \wedge P(x)$.

В пустой области «для всех» истинно: посылка $x \in \emptyset$ ложна всегда.

Почему $\rightarrow$ и $\wedge$?

«Все из A обладают P »: вне A ничего не требуется — импликация.

«Существует из A со свойством P »: объект обязан быть и в A , и со свойством — конъюнкция.

Условие « x принадлежит A » — первый мост от логики к множествам.

Отрицание ограниченного квантора

Отрицание ограниченного квантора сохраняет ограничение:

$$\neg(\forall x \in A. P(x)) \equiv \exists x \in A. \neg P(x)$$

Проверьте на $A = \{1, 2, 3\}$ и предикате $P(x)$: « x чётно».

Правильное отрицание — «существует нечётное»: истинно, $x = 1$.

Ошибочное прочтение «все нечётны» ложно: 2 чётно.

Перевод на язык предикатов

Перевод с естественного языка — это выбор области, предикатов и кванторов.

Пример

«Каждый студент знает хотя бы один язык программирования».

Пусть X — студенты, Y — языки программирования, $Z(x, y)$: « x знает y »:

$$\forall x \in X. \exists y \in Y. Z(x, y).$$

Без ограниченных кванторов ограничения уходят в предикаты:

$$\forall x. (S(x) \rightarrow \exists y. (L(y) \wedge Z(x, y))).$$

Здесь $S(x)$: « x — студент», $L(y)$: « y — язык программирования».

Формализация снимает двусмысленность естественного языка.

Отсортированный массив

Пример

«Массив a отсортирован по возрастанию»:

$$\forall i \in \{1, \dots, n - 1\}. a_i \leq a_{i+1}.$$

Без ограниченного квантора диапазон становится посылкой импликации:

$$\forall i. (1 \leq i \leq n - 1) \rightarrow a_i \leq a_{i+1}.$$

Почему до $n - 1$?

Сравнение — со следующим элементом a_{i+1} , а у последнего элемента a_n его нет.

Вне диапазона посылка ложна, и импликация ничего не требует.

Слово «только»

Слово «только» — ловушка перевода: оно меняет направление импликации.

Пример

Пусть $O(x)$: « x — отличник», $S(x)$: « x получает стипендию».

- «Все отличники получают стипендию»: $\forall x. (O(x) \rightarrow S(x))$
(каждый отличник получает)
- «Только отличники получают стипендию»: $\forall x. (S(x) \rightarrow O(x))$
(никто, кроме отличников, стипендию не получает)

Второе не обещает, что каждый отличник получает стипендию — отличников может быть больше, чем стипендий.

«Только A ...» ставит A в консеквент:

«только отличники ...» — это $S \rightarrow O$, а не $O \rightarrow S$.

Единственность

Определение 7 (Единственность)

«Существует единственный x с $P(x)$ » — существование плюс уникальность:

$$\exists x. (P(x) \wedge \forall y. (P(y) \rightarrow y = x)).$$

Пример

Существует единственное чётное простое число — это 2.

«Ровно один» — хотя бы один и не более одного одновременно.

Кванторы и код

Пример

Проверка $\forall i. a_i > 0$ в лучшем языке программирования:

```
a.iter().all(|&v| v > 0)
```

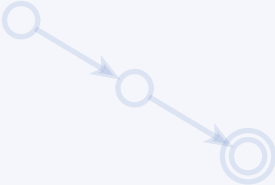
Отрицание меняет `all` на `any` и переворачивает условие:

```
a.iter().any(|&v| v <= 0)
```

Это тот же цикл с ранним выходом на первом нарушителе.

Кванторы — это циклы:

- $\forall$ проходит все элементы,
- $\exists$ останавливается на первом подходящем.



Методы доказательств

Начиная с предметов наиболее простых и легко познаваемых, восходить мало-помалу до познания наиболее сложных.

— Рене Декарт

Что такое доказательство?

- **Доказательство** — цепочка логических шагов.
- Каждый шаг опирается на определения, аксиомы или ранее доказанные факты.
- Цель — показать, что из посылок логически следует заключение.

Доказательство проверяемо: каждый шаг можно проверить.

В этом его отличие от «очевидно» и «по интуиции».

Прямое доказательство

Определение 8

Прямое доказательство импликации $P \rightarrow Q$: предполагаем P и выводим Q цепочкой шагов.

Теорема 2 (Чётность квадрата)

Если целое n чётно, то n^2 чётно.

Доказательство

Пусть n чётно, тогда $n = 2k$ для некоторого целого k .

Возводим в квадрат: $n^2 = 4k^2 = 2(2k^2)$, значит, n^2 делится на 2, то есть чётно.

Нечётность квадрата

Теорема 3

Если целое n нечётно, то n^2 нечётно.

Доказательство

Пусть $n = 2k + 1$, тогда $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ — нечётно.

Каждое целое либо чётно, либо нечётно.

Поэтому чётный квадрат бывает только у чётных чисел: если бы n было нечётно, n^2 было бы нечётно.

Контрапозиция

Определение 9

Импликация $P \rightarrow Q$ эквивалентна своей **контрапозиции**: $\neg Q \rightarrow \neg P$.

Иногда из $\neg Q$ исходить легче, чем из P .

Теорема 4

Если n^2 нечётно, то целое n нечётно.

Доказательство

Напрямую из нечётности n^2 исходить трудно.

Возьмём контрапозицию «если n чётно, то n^2 чётно» — это теорема о чётности квадрата.

Доказательство от противного

Определение 10

Доказательство от противного: предполагаем отрицание утверждения и выводим противоречие.

Не путать с контрапозицией!

- там — прямое доказательство $\neg Q \rightarrow \neg P$,
- здесь — поиск любого противоречия из отрицания цели.

Теорема 5

Число $\sqrt{2}$ иррационально.

Иррациональность корня из двух

Доказательство

Пусть $\sqrt{2} = \frac{a}{b}$ — несократимая дробь.

Возведём в квадрат: $a^2 = 2b^2$, поэтому a^2 чётно, а значит и a чётно — иначе a было бы нечётно и a^2 нечётно. Пишем $a = 2k$.

Тогда $b^2 = 2k^2$, поэтому b чётно тем же рассуждением — дробь $\frac{a}{b}$ сокращается на 2: противоречие с несократимостью.

Разбор случаев

Чтобы доказать утверждение, можно разбить рассуждение на полный набор случаев — вместе они покрывают все возможности.

Теорема 6

Для любых целых x и y выполнено $|x| \cdot |y| = |xy|$.

Доказательство

- Если $x = 0$ или $y = 0$, обе части равны нулю.
- Если x и y одного знака, то $|x||y| = xy = |xy|$.
- Если знаки разные, то $xy < 0$ и $|x||y| = -xy = |xy|$.

Контрпример

Определение 11

Контрпример — один объект, на котором утверждение ложно.

Чтобы опровергнуть утверждение $\forall x. P(x)$, достаточно одного x с $\neg P(x)$.

Пример

Утверждение «все простые числа нечётны» ложно.

Контрпример: число 2 — простое и чётное.

Контрпример — это тест, который валит программу.

Доказать утверждение для всех x — значит показать, что контрпримеров нет.

Доказательство эквивалентности

Определение 12

Чтобы доказать $P \leftrightarrow Q$, доказывают обе импликации: $P \rightarrow Q$ и $Q \rightarrow P$.

Альтернатива — цепочка эквивалентностей от P к Q .

Пример

- Докажем: x чётно тогда и только тогда, когда x^2 чётно.
- Прямое направление — теорема о чётности квадрата.
- Обратное — контрапозицией: если x нечётно, то x^2 нечётно. Значит, чётный квадрат бывает только у чётных.

Две импликации одной эквивалентности удобно доказывать разными методами.

Логические ошибки

Не всякая схема рассуждения корректна.

Две ошибки подстерегают чаще всего.

Определение 13 (Утверждение консеквента (*affirming the consequent*))

Из $P \rightarrow Q$ и Q вывести P — ошибка.

Определение 14 (Отрицание антецедента (*denying the antecedent*))

Из $P \rightarrow Q$ и $\neg P$ вывести $\neg Q$ — ошибка.

Примеры ошибок

Пример

«Если дождь, то земля мокрая».

- Вывод «земля мокрая, значит был дождь» ошибочен: землю могли полить из шланга.
- Вывод «дождя нет, значит земля сухая» тоже ошибочен: без дождя земля не обязана быть сухой.

Импликация работает в одну сторону.



Индукция

*Хотя у этого предложения бесконечное число случаев,
я дам для него весьма короткое доказательство.*

— Блез Паскаль

Принцип математической индукции

Представьте домино: если упала первая кость и каждая роняет следующую, упадут все.

Определение 15

Математическая индукция доказывает утверждение $\forall n \geq n_0. P(n)$ в два шага:

1. **База:** проверить $P(n_0)$.
2. **Шаг:** для произвольного $k \geq n_0$ из $P(k)$ вывести $P(k + 1)$.

Тогда $P(n)$ истинно для всех $n \geq n_0$.

В примерах ниже $n_0 = 1$ и $n_0 = 2$.

Индукция — это бесконечная цепочка прямых доказательств, записанная компактно.

Сумма первых n чисел

Теорема 7

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \text{ для всех } n \geq 1.$$

Доказательство

База: при $n = 1$ обе части равны 1.

Шаг: пусть равенство верно для k , тогда

$$\begin{aligned} 1 + \dots + k + (k + 1) &= \frac{k(k + 1)}{2} + (k + 1) \\ &= \frac{(k + 1)(k + 2)}{2}. \end{aligned}$$

Значит, равенство верно и для $k + 1$ — по принципу индукции оно верно для всех $n \geq 1$.

Сумма кубов

Теорема 8

$1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2$ для всех $n \geq 1$.

Доказательство

База: при $n = 1$ обе части равны 1.

Шаг: пусть равенство верно для k , тогда

$$\begin{aligned} 1^3 + \dots + k^3 + (k+1)^3 &= (1 + \dots + k)^2 + (k+1)^3 \\ &= \frac{(k+1)^2(k+2)^2}{4} \\ &= (1 + \dots + k + (k+1))^2. \end{aligned}$$

Сумма кубов — квадрат суммы первых n чисел: $1^3 + 2^3 + 3^3 = 36 = (1 + 2 + 3)^2$.

Сильная индукция

Определение 16

Сильная индукция:

- **База:** $P(n_0)$.
- **Шаг:** из истинности $P(i)$ для всех $n_0 \leq i < k$ вывести $P(k)$.

Обычная индукция использует в шаге только $P(k)$.

Сильная нужна, когда шагу не хватает одного $P(k)$: в разложении на множители о сомножителях известно лишь то, что они меньше k .

Обычная индукция — частный случай сильной.

Разложение на простые множители

Теорема 9

Каждое целое $n > 1$ разлагается в произведение простых чисел.

Доказательство

База: $n = 2$ — простое число.

Шаг: пусть утверждение верно для всех i , где $2 \leq i < k$.

Если k простое, всё доказано.

Иначе $k = ab$, где $1 < a < k$ и $1 < b < k$.

Оба множителя попадают в диапазон предположения, поэтому оба разлагаются — их произведение даёт разложение k .

«Сильная» — не сильнее

Обычная индукция — частный случай сильной, но по доказательной силе принципы равносильны.

Теорема 10

Всё, что доказывается сильной индукцией, доказывается и обычной.

«Сильная» — про удобство предположения в шаге, а не про то, что она доказывает больше.

Редукция к обычной индукции

Доказательство

Положим $Q(n) = P(n_0) \wedge P(n_0 + 1) \wedge \dots \wedge P(n)$ — «верны все P до n включительно».

База: $Q(n_0)$ — это в точности $P(n_0)$.

Шаг: пусть верно $Q(k - 1)$, то есть все $P(i)$ при $i < k$. Сильный шаг даёт $P(k)$, значит, верно и $Q(k)$.

Обычная индукция доказывает $Q(n)$ для всех n , а из $Q(n)$ следует $P(n)$.

Принцип полной упорядоченности

Определение 17

Принцип полной упорядоченности (*well-ordering principle*): каждое непустое подмножество $\mathbb{N}$ имеет наименьший элемент.

Принцип полной упорядоченности эквивалентен математической индукции.

Почему индукция работает?

Пусть $P(n)$ верно не для всех n .

Тогда множество контрпримеров $S = \{n \in \mathbb{N} \mid \neg P(n)\}$ непусто, и по принципу полной упорядоченности в нём есть наименьший элемент m — первый контрпример.

Первый контрпример невозможен

Обычная: $m > n_0$, значит, $m - 1$ — не контрпример, и шаг из $P(m - 1)$ даёт $P(m)$.

Сильная: все $i < m$ — не контрпримеры, и сильный шаг даёт $P(m)$.

В обоих случаях первый контрпример опровергает сам себя — противоречие.

Наименьшего контрпримера не существует, значит, контрпримеров нет вовсе.

Простой делитель

Теорема 11

Каждое $n \geq 2$ имеет простой делитель.

Доказательство

Пусть нет, и пусть m — наименьший контрпример.

m не простое (иначе делит само себя), значит, $m = ab$ при $1 < a < m$.

По минимальности у a есть простой делитель p — он делит и m . Противоречие.

Индукция и код

- Индукция и рекурсия — одно и то же с разных сторон.
- Корректность рекурсивной функции доказывается индукцией по размеру аргумента.
- Инвариант цикла — индукция по числу итераций.
- Инвариант — это `assert`, который обязан оставаться истинным на каждой итерации.

Пример

- Инвариант линейного поиска: после i итераций элемент не найден среди первых i позиций.
- База $i = 0$ тривиальна, шаг — индукция по i .
- При выходе из цикла инвариант вместе с условием выхода даёт ответ.

Типичные ошибки

Индукция ломается, если база неверна или шаг не работает при всех k .

Пример

Ложное доказательство «все лошади одного цвета».

- База $P(1)$ верна.
- Шаг: возьмём $k + 1$ лошадей, разделим их на две группы по k : в одну не входит первая, в другую — последняя.
- Каждая группа одноцветна по предположению.
- При $k \geq 2$ группы пересекаются, и цвет переносится на всех.
- При $k = 1$ пересечение групп пусто, поэтому цвет не переносится.
- Шаг обязан работать при *всех* k , включая маленькие.

Ошибки индукции живут на границах шага.

Лекция 2: что мы поняли?

- Предикат — шаблон высказывания. $\forall$ и $\exists$ превращают его в высказывание.
- Отрицание проносится сквозь квантор, меняя его. Порядок кванторов меняет смысл.
- Доказательство — проверяемая цепочка шагов: прямо, контрапозиция, от противного, разбор случаев.
- Контрпример опровергает общее утверждение одним объектом.
- Индукция: база и шаг дают утверждение сразу для всех n .
- Язык и инструменты собраны. Следующий шаг — первый тип объектов: множества, говорящие на языке логики.

Вопросы для самопроверки

- Запишите кванторами: «в любом классе есть отличник».
- Запишите и прочитайте по-русски отрицание: $\neg(\exists x \in A. P(x))$.
- Докажите: если n^2 делится на 3, то n делится на 3.
- Найдите контрпример: «все нечётные числа простые».
- Докажите индукцией: $1 + 3 + 5 + \dots + (2n - 1) = n^2$.
- Чем $\forall x \exists y. P(x, y)$ отличается от $\exists y \forall x. P(x, y)$?
- Запишите формулой «только отличники получают стипендию» и её отрицание.

Чтение к следующей паре

- m03 — «Предикаты», «Кванторы», «Отрицание кванторов», «Ограниченные кванторы».
- m01 — «Методы доказательств» (индукция, от противного).
- Флеш-опросник — в начале лекции 3.