# Дискретная математика

КОНСПЕКТЫ ЛЕКЦИЙ
МФТИ и НИУ ВШЭ 2019

Александр Рубцов
alex@rubtsov.su

# Содержание

# Введение

В рамках этого курса мы изучим базовые математические понятия, такие как множества, функции, графы, бинарные отношения. Они важны и нужны для дальнейшего изучения Computer Science, но также являются базой и для чистой математики. С другой стороны, для плодотворного развития в Computer Science нужно понимать, что такое доказательство. Доказательства корректности многих алгоритмов являются по сути доказательствами теорем, поэтому в рамках этого курса мы будем уделять доказательствам особое внимание.

Мы начинаем изучение курса с алгебры логики. С одной стороны, эта тема связана с чистым Computer Science — логика в программировании используется постоянно, хотя бы для задания условий выхода из цикла и условных операторов. С другой стороны, логические законы являются законами для доказательств теорем и для математических рассуждений в целом.

# Лекция 1

# Алгебра логики: введение.

**План:**

1. Высказывания и логические связки.
2. Булевы функции и способы их задания: таблицы истинности, вектор значений, формулы.
3. Законы коммутативности, ассоциативности и дистрибутивности, приоритет операций.
4. Законы поглощения.
5. Равенство булевых функций (и булевых формул). Существенные и фиктивные переменные.

**Ключевые слова:** *высказывание, булева функция, конъюнкция, дизъюнкция, импликация, отрицание (инверсия), эквивалентность, XOR (исключающее или), коммутативность, ассоциативность, дистрибутивность, законы поглощения, существенная переменная, фиктивная переменная.*

---

Мы начинаем наш курс с основ логики, поскольку логика — это цемент для построения математических утверждений и доказательств. Хотя мы и начинаем фактически с изучения правил переписывания логических формул, которые можно выполнять не вдаваясь в суть самих высказываний, дальше эти правила будут использоваться для построения утверждений и доказательств.

Одной из основных целей нашего курса является прививание первокурсникам математической культуры. Математическая культура начинается с работы с формальными определениями, и это влечёт трудности. Формальные определения требуют язык теории множеств и часто при первом изучении формализм мешает содержательному пониманию вещей. Мы решаем эту проблему следующим образом. До введения теории множеств все определения будут неформальными, а после её

изучения мы формализуем уже введённые определения на языке теории множеств. Однако после изучения теории множеств мы не откажемся от неформальных определений перед формальными. Определений в курсе достаточно много, поэтому они часто не выделяются в отдельные блоки, а просто по ходу текста выделяется ***определяемое понятие***. Можно было бы начать изложение с теории множеств, а не логики, но тогда у нас была бы другая проблема — пришлось бы вести изложение без объяснения, что считается доказательством. Надеюсь, мы выбрали меньшее из зол.

Итак, перейдём к изучении основ логики. Алгебра логики оперирует с высказываниями. ***Высказывание*** — это утверждение, которое либо истино, либо ложно. Истинность высказывания $A$ будем обозначать «1», а ложность — «0». В роли $A$ может выступать высказывание «за окном идёт дождь» или «число 7 делится на 6». Заметьте, что утверждение «число $x$ делится на 6» не является высказыванием, в случае если число $x$ не зафиксировано; тогда утверждение зависит от параметра и в зависимости от значения $x$ может меняться истинность этого утверждения. Оговоримся, что утверждение, зависящее от параметра, не считается высказываением даже в случае, когда оно истинно при любом значении параметра: например, «число $x$ делится на 1» — не высказывание.

С помощью логических связок из высказываний можно получать более сложные высказывания, такие как «$A$ и $B$», «$A$ или $B$», «не $A$». Вы знакомы с этими связками со школьной скамьи и знаете, что их называют «конъюнкция», «дизъюнкция» и «отрицание» («инверсия») и обозначают

$$A \wedge B, \qquad A \vee B, \qquad \neg A \text{ или } \bar{A}.$$

Что же такое логические связки? Это функции, которые зависят от набора переменных, принимающих значения 0 или 1 (от набора высказываний). Такие переменные называют ***булевыми переменными***, а функции — ***булевыми функциями***. Есть несколько стандартных способов задания булевой функции. Мы начнём с таблицы истинности.

| $A$ | $B$ | $A \wedge B$ | $A \vee B$ | $A \to B$ | $A \leftrightarrow B$ | $A \oplus B$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 |

Рис. 1.1. задание логических связок таблицами истинности.

Если функция зависит от $k$ переменных, то первые $k$ столбцов соответствуют переменным, а $k+1$-ый столбец — значению функции на соответсвующем наборе значений переменных (все наборы значений перечисляются в строках таблицы). В таблице на рис. 1.1 мы скомпоновали таблицы истинности для нескольких функций в одну таблицу.

Пожалуй, все логические связки имеют естественную интерпретацию, кроме импликации (почему её определяют именно так, мы обсудим позже):

| Обозначение | Смысл | Название |
|---|---|---|
| $A \wedge B$ | «$A$ и $B$» | конъюнкция |
| $A \vee B$ | «$A$ или $B$» | дизъюнкция |
| $\neg A$ | «не $A$» | отрицание |
| $A \to B$ | «из $A$ следует $B$» | импликация |
| $A \leftrightarrow B$ | «$A$ равносильно $B$» | эквивалентность |
| $A \oplus B$ | «либо $A$, либо $B$» | XOR (исключающее или) |

Наборы значений переменных принято перечислять в следующем порядке. Первым идёт набор из одних нулей, а дальше $i$-ый набор является двоичной записью числа $i-1$. Таким образом, всего в таблице истинности $2^k$ строк (именно столько чисел имеют двоичную запись длины $k$).

Благодаря стандартному порядку можно просто задать булеву функцию столбцом её значений:

$$f(x_1) = 10 = \neg x_1, \quad g(x_1, x_2) = 0001 = x_1 \wedge x_2, \quad h(x_1, x_2) = 0110 = x_1 \oplus x_2.$$

Говорят, что функция задана ***вектором значений***.

## 1.1 Задание булевых функций с помощью логических связок (формулами)

Следующий способ задания булевой функции — использовать уже заданные булевы функции для определения более сложных функций. С точки зрения логики, мы используем логические связки для построения более сложных высказываний, например

$$(A \wedge B) \to C.$$

Формулу можно изобразить с помощью дерева, вычисления по которому (после присваивания значений переменным) идут снизу вверх; вообще говоря вычислять значение каждого узла дерева можно параллельно.

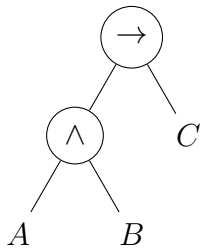


Рис. 1.2. Дерево для формулы $(A \wedge B) \to C$

Скобки используются для указания приоритета операций: в формуле выше следует сначала выполнить конъюнкцию, а затем импликацию. Для удобства записи используют следующие договорённости о приоритете операций:

1) отрицание $\neg$;

2) конъюнкция $\wedge$;

3) дизъюнкция $\vee$ и XOR $\oplus$;

4) импликация $\rightarrow$;

5) эквивалентность $\leftrightarrow$.

Согласно этим договорённостям можно восстановить скобки: самый высокий приоритет у отрицания, самый низкий — у импликации. В случае, если две операции имеют одинаковый приоритет, то считается, что сперва выполняется та, которая стоит левее. Но лучше поставить лишнюю пару скобок, дабы не было непонимания, что мы и будем делать.

**Пример 1.** Расставив скобки для формулы $x_1 \rightarrow \neg x_2 \wedge x_1 \vee x_2$ получим

$$(x_1 \rightarrow (((\neg x_2) \wedge x_1) \vee x_2)).$$

Расставив скобки, согласно приоритету можно преобразовать формулу в дерево, руководствуясь следующими правилами. Если формула состоит только из переменной, то дерево состоит только из одного узла — самой переменной. Если в формуле есть операции, то нужно ззять операцию из внешних скобках и сделать её вершиной дерева; построить деревья для левого и правого операндов и сделать их левым и правым детьми внешней операции соответственно.

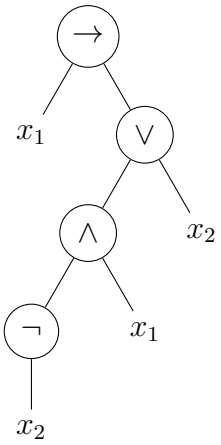


Рис. 1.3. Дерево для формулы из примера 1

## 1.2 Равенство булевых функций и формул. Фиктивные переменные

Один из самых коварных знаков в математике — это знак равенства. Справедливость формулы $x_1 \wedge x_2 = x_2 \wedge x_1$ не вызвает сомнений, ведь можно подставить в неё

всевозможные наборы значений переменных и проверить, что значение левой части всегда равняется значению правой. Разумно было бы сказать, что левая и правая части равенства задают булевы функции, и равенство справедливо, если булевы функции совпадают, но тут есть одна загвоздка. Рассмотрим теперь равенство

$$x_1 \wedge x_2 = x_2 \wedge x_1 \wedge (x_2 \vee \neg x_3). \tag{1}$$

Это равенство также легко проверить подстановкой, но в его левой части записана булева функция от двух аргументов, а в правой — от трёх. От этого можно было бы отмахнуться, сказав, что можно считать, что левая часть равенства задаёт функцию от трёх аргументов, но глядя только на левую часть невозможно предсказать сколько переменных понадобится. Любой, кто хоть раз пробовал писать на C++ понимает, что эта проблема довольно деликатная.

Решение этой проблемы приводит к определению равенства булевых функций, но начнём мы с другого определения. ***Тавтология*** — это булева функция, которая возвращает 1 на любом наборе переменных. Булевы функции $f$ и $g$ ***равны***, если функция $h = (f \leftrightarrow g)$ — тавтология. Определение равенства булевых функций переносится на равенство формул. Если не оговорено противного, то мы считаем, что формула задаёт булеву функцию, зависящую только от переменных, встречающихся в этой формуле.

Обозначим через $g(x_1, x_2, x_3)$ булеву функцию, заданную правой частью формулы (1). Ясно, что значение $g$ не зависит от переменной $x_3$. Благодаря приведённому определению равенства, мы получаем, что $g(x_1, x_2, x_3) = g(x_1, x_2, 0) = g(x_1, x_2, 1)$. В случае, если для булевой функции $f(x_1, \ldots, x_n)$ справедливо равенство

$$f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = f(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n), \tag{2}$$

переменная $x_i$ называется ***фиктивной*** (для функции $f$); в случае, если равенство (2) не выполняется для переменной $x_i$, то она называется ***существенной***.

Заметим, что для доказателсьства существенности переменной $x_i$ достаточно найти в таблице истинности $f$ два набора значений переменных, отличающиеся только значениями $x_i$, на которых $f$ принимает разные значения. Для доказательства же фиктивности, необходимо проверить совпадание значений $f$ на всех таких наборов: равенство (2) выполняется если и только если оно выполняется для всех наборов значений переменных $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.

## 1.3 Логические тождества

Для логических связок выполняется довольно много законов (тождеств). Их справедливость можно проверить с помощью таблиц истинности.

**Законы коммутативности**:

$$x_1 \wedge x_2 = x_2 \wedge x_1, \qquad x_1 \vee x_2 = x_2 \vee x_1, \qquad x_1 \oplus x_2 = x_2 \oplus x_1.$$

**Законы ассоциативности**:

$$x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3.$$

**Законы дистрибутивности:**

- $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
- $A \vee (B \to C) = (A \vee B) \to (A \vee C)$
- $A \to (B \wedge C) = (A \to B) \wedge (A \to C)$
- $A \to (B \vee C) = (A \to B) \vee (A \to C)$
- $A \to (B \to C) = (A \to B) \to (A \to C)$

**Правила поглощения:**

$$A \vee (A \wedge B) = A, \quad A \wedge (A \vee B) = A.$$

**Другие важные свойства:**

- $A \wedge A = A, \quad A \vee A = A$ (идемпотентность)
- $A \wedge \neg A = 0, \quad A \vee \neg A = 1$ (дополнение)
- $A \wedge 0 = 0, \quad A \vee 0 = A$ (универсальные границы)
- $A \wedge 1 = A, \quad A \vee 1 = 1$ (универсальные границы)
- $\neg(\neg A) = A$ (инволютивность)
- $\neg(A \wedge B) = \neg A \vee \neg B, \neg(A \vee B) = \neg A \wedge \neg B$ (законы Моргана)
- $A \to B = \neg A \vee B, \quad A \vee B = \neg A \to B$

Просто чертить таблицы истинности для проверки данных тождеств довольно времязатратно. Приведём пример доказательства тождества через таблицу истинности, не рисуя саму таблицу.

**Пример 2.** Докажем тождество $A \to B = \neg A \vee B$. И импликация и дизъюнкция имеют ровно один ноль среди значений: на наборах $(1, 0)$ и $(0, 0)$ соответственно. Таким образом, заменив в дизъюнкции $A \vee B$ переменную $A$ на её отрицание, мы получим таблицу истинности для импликации.

Многие тождества среди других важных свойств получаются путём подстановки вместо переменной констант.

Тождества, которые мы рассматривали выше, иллюстрируют свойства логических связок. Логических законов за ними сходу не видно. Не такие, например, «закон двойного отрицания» $\neg\neg A = B$ и закон контрапозиции $A \to B = \neg B \to \neg A$.

С осмысленными логическими законами мы познакомимся чуть позже, а пока учимся утилитарно работать с алгеброй логики.

# Лекция 2

# Множества и логика

**План:**

1. Множества и операции над ними
2. Связь алгебры логики и алгебры множеств
    - предикаты
    - юнивёрсум и дополнение
    - законы де Моргана
    - кванторы
    - эквивалентность тождеств алгебры множеств и алгебры логики
    - импликация
    - контрапозиция

---

В математических курсах часто стараются, чтобы всё было достаточно строго определено. Однако, для совсем базовых понятий приходится делать исключение: точки и прямые в школьной геометрии не определяют, а лишь оглашают некоторые их свойства, а в остальном предлагают полагаться на интуицию. Также придётся сделать и нам при изучении множеств.

## 2.1 Множества и операции над ними

Когда говорят, что задано множество $A$, под этим понимают, что $A$ представляет собой совокупность объектов, игнорируя при этом какие либо отношения между этими объектами, в частности порядок; кроме того, один объект не может входить в

множество более одного раза. Конечное множество можно задать явно перечислив его элементы — для этого используют фигурные скобки:

$$\{1, 2, 3, 4, 5\}.$$

Из сказанного выше вытекает, что

$$\{1, 2, 3, 4, 5\} = \{5, 4, 3, 2, 1\} = \{1, 3, 2, 4, 5\} = \{1, 1, 2, 2, 2, 3, 4, 5\}.$$

Два множества ***равны*** друг другу, если их элементы совпадают. В последнем описании множества элементы повторяются: элементы разрешено повторять при перечислении, хотя в множество каждый перечисленный элемент и входит ровно один раз. Количество элементов конечного множества $A$ называют ***мощностью*** $A$ и обозначают через $|A|$: $|\{1, 2, 3\}| = 3$.

В случае описания бесконечных множеств, используют неявное перечисление: так множество $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ состоит из (всех) ***натуральных чисел***. Мы считаем ноль натуральным числом (по этому вопросу среди математиков нет единого мнения), и чтобы не путать читателя обозначаем натуральные числа через $\mathbb{N}_0$; обозначим через $\mathbb{N}_1 = \{1, 2, 3, \ldots\}$ множество ***положительных целых чисел***. Множество ***целых чисел*** $\mathbb{Z}$ часто записывают одним из следующих способов:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{0, 1, -1, 2, -2, \ldots\}$$

Запись «$a \in A$» означает, что объект $a$ ***является элементом*** множества $A$, а запись «$a \notin A$» — отрицание этого условия:

$$3 \in \{1, 2, 3, 4, 5\}, \qquad 2 \notin \{1, 3, 5, \ldots\}.$$

Познакомимся с ещё одной формой записи множеств. Запись

$$A = \{x \mid \text{«условие на } x\text{»}\}$$

означает, что множество $A$ состоит из всех элементов $x$, для которых выполняется условие. Так, запись $\{x \mid x = 2k + 1 \text{ для некоторого } k \in \mathbb{N}\}$ задаёт множество нечётных чисел. Также вместо символа $\mid$ используют двоеточие; эти записи равноправны, а выбор символа часто обусловлен красотой и читаемостью формулы. Определим с помощью такой записи множество ***рациональных чисел***:

$$\mathbb{Q} = \left\{ \frac{m}{n} \,:\, m \in \mathbb{Z},\, n \in \mathbb{N}_1 \right\}.$$

Также введём здесь обозначение для множества ***действительных чисел*** $\mathbb{R}$, аккуратное определение которых даётся в курсе математического анализа.

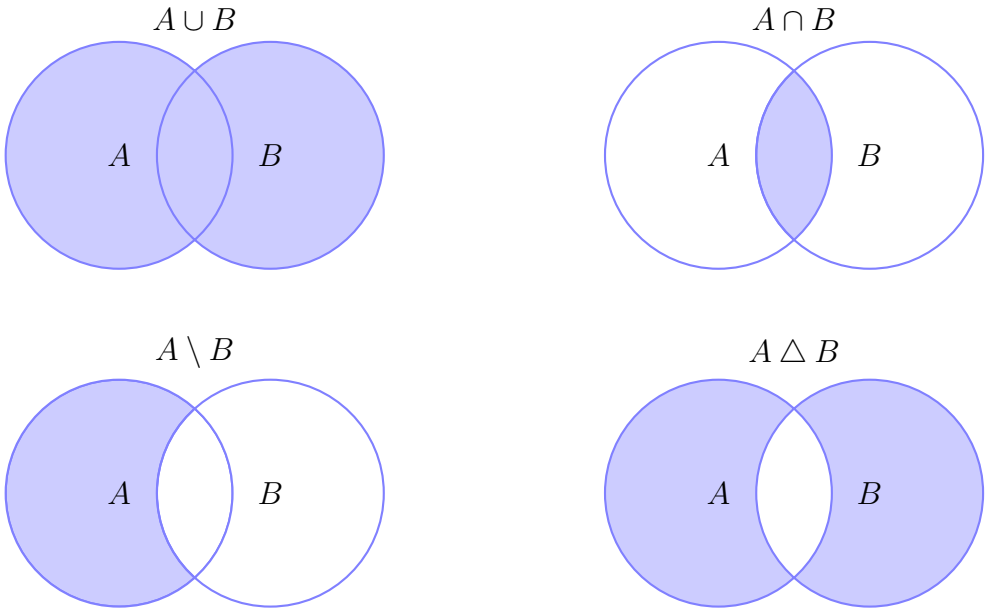


Рис. 2.1. Диаграммы Эйлера-Венна.

Определим теперь операции с множествами:

- объединение $A \cup B$ множеств $A$ и $B$ состоит из элементов, которые принадлежат хотя бы одному из множеств;
- пересечение $A \cap B$ состоит из элементов, которые принадлежат обоим множествам;
- разность $A \setminus B$ состоит из элементов, которые принадлежат $A$, но не принадлежат $B$;
- симметрическая разность $A \triangle B$ состоит из элементов, принадлежащих ровно одному из множеств.

Эти операции иллюстрируют с помощью диаграмм Эйлера-Венна (рис. 2.1).

Говорят, что множество $C$ является ***подмножеством*** множества $D$, если все элементы $C$ принадлежат $D$. Это обозначают $C \subseteq D$. Из картинок видно, что $A \setminus B \subseteq A$. Множество, в котором нет элементов называют ***пустым*** и обозначают $\varnothing$.

**Упражнение 1.** Убедитесь, что $(A \triangle B) \cap (A \cap B) = \varnothing$.

**Упражнение 2.** Убедитесь, что множества $A$ и $B$ равны, тогда и только тогда, когда $A \subseteq B$ и $B \subseteq A$.

**Упражнение 3.** Докажите, что для любых множеств $A$ и $B$ справедлива формула $(A \cup B) \setminus (A \triangle B) = A \cap B$.

## 2.2 Связь с логикой

При изучении алгебры логики, мы имели дело с высказываниями, которые либо истинны, либо ложны. Утверждение $A(x) =$ «$x$ делится на 6» зависит от параметра $x$, а потому таковым не является. Утверждения, зависящие от параметров, называют ***предикатами*** и работать с ними можно точно также как и с обычными высказываниям (можно применять к ним всё те же логические связки). Часто удобно использовать предикаты, зависящие от нескольких параметров: например, $G(x, y) =$ «$x > y$». Число параметров называется ***арностью*** предиката, предикаты арности 1 или ***унарные*** предикаты соответствуют множествам: множеству $A$ соответствует предикат $A(x)$, который истинен тогда и только тогда, когда $x \in A$.

Обратим внимание, что

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\};$$

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\};$$

$$A \setminus B = \{x \mid (x \in A) \wedge \neg(x \in B)\};$$

$$A \triangle B = \{x \mid ((x \in A) \wedge \neg(x \in B)) \vee ((x \in B) \wedge \neg(x \in A))\}.$$

В описании множества $\{x \mid P(x)\}$ условие $P(x)$ — это и есть унарный предикат, задающий множество.

Эта связь объясняет законность рассуждений с картинками (диаграммами Эйлера-Венна). Допустим в диаграмму входят три множества $A$, $B$ и $C$. Каждую область диаграммы можно задать вектором $(a, b, c)$ с компонентами $\{0, 1\}$; значение 1 означает, что $x$ принадлежит соответствующему множеству, а 0, что нет. Так, вектор $(1, 0, 1)$ означает, что $x \in A$, $x \notin B$ и $x \in C$. Сама диаграмма описывает множество $D$, и если область закрашена, то всякий $x$ из этой области принадлежит $D$. Получаем, что диаграммы Эйлера-Венна просто иллюстрируют таблицы истинности.

Многие теоретико-множественные тождества следуют напрямую из тождеств алгебры-логики: тождество

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

равносильно следующему тождеству, в котором $a$ означает «$x \in A$» и т.д.

$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c).$$

### Юнивёрсум и Дополнение

Вы скорее всего уже наслышаны о такой операции с множествами, как дополнение. Но вот каверзный вопрос[1]: принадлежит ли число $\sqrt{2}$ к дополнению множеству чётных чисел? А вот этот стул? Слово «дополнение» буквально означает «до полного», поэтому для этой операции нужно сначала определить «полное множество» — множество из всех объектов, которые мы рассматриваем в рамках наших теоретико-множественных рассуждений. Такое множество называют ***юнивёрсум*** и обозначают $U$.

[1]Если о дополнении вы не слышали, то пропустите этот вопрос.

Множество $\bar{A} = U \setminus A$ называют ***дополнением*** к множеству $A$. Ясно, что $\bar{A}$ — это наименьшее множество, которое нужно добавить к $A$, чтобы получилось множество $U$.

Мы изучаем наивную теорию множеств, которая вообще говоря противоречива. Проблемы возникают, если рассматривать множества всех множеств (см. парадокс Рассела). Для того, чтобы обезопасить себя, достаточно зафиксировать юнивёрсум: если $U$ — множество натуральных (целых неотрицательных) чисел $\mathbb{N}$, целых чисел $\mathbb{Z}$, рациональных чисел $\mathbb{Q}$ или вещественных чисел $\mathbb{R}$, то проблем не будет.

Приведём теперь законы теории множеств, связанные с дополнением и соответствующие им логические законы.

## Законы де Моргана

С помощью диаграмм легко проверить, что $A \cap B = \overline{\bar{A} \cup \bar{B}}$, $A \cup B = \overline{\bar{A} \cap \bar{B}}$. Из связи с таблицами истинности получаем, что $a \wedge b = \neg(\bar{a} \vee \bar{b})$ и $a \vee b = \neg(\bar{a} \wedge \bar{b})$. Эти законы известны как законы де Моргана.

Однако, эти формулы можно обобщить:

$$A_1 \cap A_2 \cap \ldots \cap A_n \cap \ldots = \overline{\bar{A}_1 \cup \bar{A}_2 \cup \ldots \cup \bar{A}_n \cup \ldots} \tag{1}$$

Докажем обобщённую формулу, обозначим левую часть за $X$, а правую за $Y$. Если $x \in X$, то $x$ принадлежит каждому множеству $A_i$, но тогда он не принадлежит ни одному дополнению $\bar{A}_i$, а значит и их объединению. Значит $x$ принадлежит дополнению от объединения дополнений, т.е. $Y$. Мы доказали, что $X \subseteq Y$. Пусть теперь $y \in Y$, тогда $y \notin \overline{Y}$ и потому для каждого $i$ выполняется $y \notin \bar{A}_i$. Но раз $y \notin \bar{A}_i$, то $y \in A_i$ (для каждого $i$), а потому $y \in X$. Отсюда $Y \subseteq X$; как и в первом случае включение справедливо в силу произвольности $y$. Итак, мы доказали, что $X = Y$, что и требовалось. Обратим внимание, что при доказательстве равенства двух множеств требуется доказывать включения в обе стороны! Бывают доказательства, в которых хитрым образом доказывается равенство множеств без доказательств включений по очереди, но это скорее редкость.

Двойственный закон Моргана

$$B_1 \cup B_2 \cup \ldots \cup B_n \cup \ldots = \overline{\bar{B}_1 \cap \bar{B}_2 \cap \ldots \cap \bar{B}_n \cap \ldots}$$

можно доказать аналогично, но можно и вывести из первого закона. Поскольку тождество (1) справедливо для произвольных множеств, заменим в нём $A_i$ на $\bar{B}_i$, снимем двойное дополнение и возьмём дополнения от обеих частей равенств.

## Кванторы

Возможно вы уже познакомились с кванторами в математическом анализе. Вернёмся к утверждениям, зависящим от параметра — предикатам. Часто интересно, истинен ли предикат $A$ при любом $x$. Это утверждение записывают как

$$\forall x A(x),$$

а истинность при хотя бы одном $x$

$$\exists x A(x).$$

Значки $\forall$ и $\exists$ называют ***кванторами*** (всеобщности и существования соответственно).

Кванторы можно интерпретировать как (возможно) бесконечные конъюкции и дизъюнкции элементарных высказываний $A(x)$. Поскольку операции конъюнкция и дизъюнкция коммутативны и ассоциативны, порядок их выполнения не важен. Это приводит к следующему сокращению в формулах:

$$A(1) \wedge A(2) \wedge \dots A(n) = \bigwedge_{i=1}^{n} A(i) = \bigwedge_{i \in \{1,\dots,n\}} A(i).$$

В случае когда порядок операндов важен (например, в произведении матриц), вторая запись интерпретируется как первая, а третья запись вообще говоря некорректна.

В случае произвольной формулы в кванторах, подразумевается что каждая переменная принимает значение из определённого множества, юнивёрсума $U$. В логике удобно считать, что все переменные принимают значения из единственного множества, это легко реализовать технически.

Итак, формально формула в кванторах интерпретируется так:

$$\forall x A(x) = \bigwedge_{x \in U} A(x).$$

К конъюнкции (не обязательно конечной) применим закон Моргана, отсюда получаем, что

$$\neg \forall x A(x) = \overline{\bigwedge_{x \in U} A(x)} = \bigvee_{x \in U} \neg A(x) = \exists x \neg A(x).$$

## Эквивалентность тождеств алгебры логики и алгебры множеств

Тождества алгебры логики переходят в тождества алгебры множеств при замене булевых переменных множествами, а операций алгебры логики на соответсвующие операции алгебры множеств. Переход справедлив и в обратную сторону. Поэтому все преобразования, которые мы изучили, работая с алгеброй логики имеют прямой аналог в алгебре множеств.

Приведём набросок доказательства эквивалентности тождеств в этих алгебрах. Возьмём формулу алгебры множеств и заменим в ней множества $A_i$ на предикаты $A_i(x)$ а операции, на соответствующие логические операции. Добавив перед обеими частями квантор всеобщности по $x$ и заменив равенство на эквивалентность получим выражение вида

$$\forall x((\text{левая часть формулы}) \leftrightarrow (\text{правая часть формулы})).$$

Ясно, что это утверждение истинно для любых предикатов тогда и только тогда, когда изначальная формула алгебры множеств справедлива для любого набора множеств. Также ясно, что это условие выполняется, если заменив теперь предикаты на булевы переменные ($A_i(x)$ на $a_i$) и убрав квантор по $x$, мы получим

тождество в алгебре логики. Если же в результате замены мы получили не тождество, найдётся такой набор переменных, при котором высказывание ложно. Если в этом наборе $a_i = 1$, положим $A_i = 1$, если же $a_i = 0$, положим $A_i = \varnothing$. Выполнив обратную замену от алгебры логики к утверждению в предикатах и к формуле алгебры множеств, получим, что утверждение в предикатах ложно, а формула алгебры множеств не выполняется.

Рассуждения в обратную сторону аналогичны.

Приведём пример построения эквивалентных тождеств алгебры множеств и алгеброй логики с промежуточным шагом формулы с предикатами на примере закона де Моргана.

**Пример 3.**

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\forall x(\neg(A(x) \vee B(x)) \leftrightarrow (\neg A(x) \wedge \neg B(x)))$$

$$\neg(a \vee b) \leftrightarrow \neg a \wedge \neg b$$

## Импликация и множества

На первый взгляд, определение импликации выглядит странно. Почему математики решили, что $0 \to 1 = 1$?! Ответ кроется в связи с теорией множеств. Утверждение «($x$ делится на 6) $\to$ ($x$ делится на 2)$\vee$($x$ делится на 3)» будет считаться теоремой, если оно истинно при всех $x$:

$$\forall x\ D_6(x) \to (D_2(x) \vee D_3(x)).$$

Но утверждение $D_6(x)$ ложно, например, при $x = 4$, а утверждение $D_2(x)$ истинно.

Переведём выссказывание $\forall x\ A(x) \to B(x)$ на язык множеств. Если посылка импликации истинна при некотором $x$, то при этом же $x$ истинно и заключение (иначе, импликация ложно). Если же посылка ложна, то какого бы ни было заключение, импликация истинна. Значит каждый $x$ из $A$ принадлежит также множеству $B$, отсюда получаем, что $A$ — подмножество $B$. Ясно, что $D_6 \subseteq D_2 \cup D_3$.

## Контрапозиция

Логический закон контрапозиции $A \to B = \neg B \to \neg A$ при переводе на язык множеств гласит, что $A \subseteq B \iff \bar{B} \subseteq \bar{A}$. Его часто используют на практике при доказательстве теорем и решении задач: когда нужно доказать следствие $A \to B$, часто вместо него доказывают $\neg B \to \neg A$.

# Лекция 3

# Математические определения, утверждения и доказательства

**План:**

1. Определение, утверждение, теорема, критерий. Запись с помощью формулы первого порядка (неформально).
2. Логический вывод, Modus Ponens
3. Методы доказательств: контрапозиция, индукция, от противного, конструктивные (примеры и контрпримеры), неконструктивные.

**Литература**: [MCS], [Sipser], [Мендельсон]

---

Изучив основы логики и теории множеств мы можем содержательно поговорить о доказательствах. Наш разговор не будет строгим; строгому изложению этого материала отведено место на втором курсе, но изучать доказательства и что-то доказывать при решении задач, нужно уже сейчас.

## 3.1 Определения

***Определения*** описывают объекты и понятия. Если определение записано логической формулой, то оно имеет вид предиката $D(x)$, который истиннен тогда и только тогда, когда $x$, удовлетворяет определению.

**Пример 4.** Множеству $D = \{x \mid x^2 + 2x + 1 = 0\}$ соответствует предикат $D(x)$, который определяет корни многочлена $x^2 + 2x + 1$, т.е. 1 и $-1$.

**Пример 5.** Формула

$$\forall \varepsilon > 0 \; \exists N \in \mathbb{N} : \forall n \geqslant N \; |x_n - a| < \varepsilon$$

Как хорошо известно читателю, определяет предел числовой последовательности. Формально это предикат $D(a, \{x_n\})$, который зависит как от числа $a$, так и от последовательности $\{x_n\}$. Параметры, от которых зависит истинность формулы, не стоят под кванторами.

Определения, данные словами ничуть не хуже определений, данных формулами. На первом курсе последние встречаются чаще, чтобы научить студентов изложению в кванторах. Так, определение предела можно переформулировать словами: «число $a$ — предел последовательности $\{x_n\}$, если любая окрестность числа $a$ содержит все элементы последовательности, начиная с некоторого номера».

## 3.2 Математические утверждения

***Математические утверждения*** — это утверждения, которые либо, истинны либо ложны. В отличие от определений, они не зависят от параметров. Если вы встретили утверждение вида «если последовательность $x_n$ сходится, то она ограничена», то в силу вступает математическое соглашение о том, что в случае отсутствия в утверждении квантора по параметру, нужно поставить квантор всеобщности.

Среди математических утверждений выделяют ***теоремы*** — истинные утверждения. Как правило, теоремами называют значимые математические утверждения. Вспомогательные истинные математических утверждения называют ***леммами***, ***предложениями*** и просто ***утверждениями***.

Истинное утверждение называют ***критерием***, если оно имеет вид

$$\forall x\ (A(x) \leftrightarrow B(x)).$$

Критерии устанавливают необходимое и достаточное условие $B(x)$ для выполнения условия $A(x)$ или, что то же самое, устанавливает эквивалентность определений $A$ и $B$. Например, в математическом анализе критерий Коши устанавливает эквивалентность сходящихся и фундаментальных последовательностей.

Условие $A(x)$ является ***необходимым*** для выполнения $B(x)$, если $\forall x(B(x) \to A(x))$.Симметрично, условие $A(x)$ является ***достаточным***, если $\forall x(A(x) \to B(x))$.Из сказанного вытекает, что $A(x)$ — ***необходимое и достаточное*** условие, если $\forall x(A(x) \leftrightarrow B(x))$.

## 3.3 Доказательства

***Доказательство*** — это логическое рассуждение, которое убеждает в верности математического утверждения любого непредвзятого слушателя (или читателя). У доказательств есть формальное определение в математической логике, но оно требует введение формальных систем и фактически такие доказательства непроверяемы человеком. Математики любят пользоваться приведённым описанием доказательства, но в утилитарном смысле оно слабо годится. Откуда первокурснику знать, убедят ли его аргументы академика? Поэтому помимо философского описания, мы дадим ещё и утилитарное, но для этого нам потребуется сначала описать логический вывод.

## Логический вывод

Представьте, что известна истинность утверждений $A$ и $A \to B$. Из этого можно сразу заключить истинность утверждения $B$, ведь если $B$ ложно, а $A$ истинно, то импликация $A \to B$ ложна. Это правило вывода записывается так:

$$\frac{A, \quad A \to B}{B} \qquad \text{(M.P.)}$$

Это правило вывода называется Modus Ponens (сокращённо M.P.). Запись вывода интерпретируется так: если доказано то, что выше черты, то доказано и то, что ниже черты. По аналогии с импликацией, то что выше черты называют посылкой, а то что ниже — заключением.

Правил вывода можно изобрести много. Например, очевидно

$$\frac{\neg A, \quad A \vee B}{B},$$

но многие такие правила сводятся к Modus Ponens: $A \vee B = \neg A \to B$.

Формально запись

$$\frac{A_1, \quad A_2, \quad \ldots \quad A_n}{B}$$

означает, что

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \to B. \qquad (1)$$

Если известно, что все утверждения $A_i$ истинны, и истинно утверждение (1), то эти факты в совокупности влекут (доказывают) истинность утверждения $B$.

Приведём пример рассуждений с помощью логических выводов.

**Пример 6.** Алису, Вениамина и Сергея вызвали к директору, потому что кто-то из них на перемене разбил окно. Алиса сказала, что ни она, ни Вениамин окно не разбивали. Вениамин сказал, что Алиса не разбивала окно, а это сделал Сергей, а Сергей сказал, что он не разбивал окно и окно разбила Алиса.

Директору известно, что ровно один школьник сказал правду, другой солгал в каждом из утверждений, а третий дал одно истинное, а другое ложное утверждение. Кто же разбил окно?

**Решение.** Обозначим через $A$, $B$, $C$ высказывания «Алиса разбила окно», «Вениамин разбил окно», «Сергей разбил окно». Точно известно, что истинно высказывание

$$A \vee B \vee C.$$

Среди следующих высказываний истинно ровно одно, ещё в одном истинен ровно один конъюнкт, а в оставшемся ложны оба конъюнкта:

$$\neg A \wedge \neg B, \qquad \neg A \wedge C, \qquad \neg C \wedge A.$$

Предположим, что Алиса сказала правду. Тогда истины высказывания $\neg A$ и $\neg B$. Получаем отсюда, что окно разбил Сергей:

$$\frac{\neg A, \quad \neg B, \quad A \vee B \vee C}{C}.$$

Но это невозможно, потому что тогда Вениамин тоже сказал правду:

$$\frac{\neg A, \quad C}{\neg A \wedge C}\ .$$

Предположив, что правду сказал Вениамин, также получим, что окно разбил Сергей, и Алиса тоже сказала правду, что невозможно.

Получается, что правду сказал Сергей и окно разбила Алиса. На этом решение можно было бы закончить, при условии доверия к составителю задачи. Если быть формальными до конца, то нужно проверить оставшиеся условия. Ясно, что Алиса соврала наполовину (ровно одно из её высказываний истинно), а Вениамин соврал в каждом из утверждений. □

В этом примере, мы показали как использовать запись логического вывода и способ рассуждения с помощью этого метода. Если записать условие примера с помощью формулы, то она получится очень длинной, и придётся мучиться с её упрощением. Приведённые рассуждения похожи на реальные доказательства гораздо больше, чем запись условия утверждения в виде булевой формулы и её последующего преобразования.

Формализуем с помощью вывода наши требования к доказательству. Мы считаем логическое рассуждение доказательством, если оно представимо в виде последовательного применения правил вывода, посылки которых либо известные верные утверждения (из нашего курса, параллельных курсов или общеизвестные факты, например из школьной программы), либо уже доказанные утверждения.

Наши требования относятся к сути, а не к форме. Текст на естественном языке, удовлетворяющий им, ничуть не хуже (а часто лучше), чем набор формул с шагами вывода. Но при написании текста нужно понимать, какие утверждения в нём делаются, как они связаны шагами вывода; полезно помогать себе и читателю доказательства, явно выделяя вспомогательные утверждения.

Мы переходим к перечислению различных методов доказательств. Мы формализуем их с помощью правил вывода и приведём примеры.

## Контрапозиция

Закон контрапозиции представим в виде

$$\frac{A \to B}{\neg B \to \neg A}\ .$$

Его смысл становится ясным при переходе на язык множеств (как и его справедливость): $A \subseteq B$ тогда и только тогда, когда $\overline{B} \subseteq \overline{A}$.

Приведём пример его использования.

**Утверждение 1.** *Если число $r$ иррационально, то и число $\sqrt{r}$ иррационально.*

**Доказательство.** Воспользовавшись контрапозицией получим равносильное утверждение:

«Если число $\sqrt{r}$ рационально, то число $r$ рационально.»

Это утверждение доказать нетрудно: если число $\sqrt{r}$ рационально, то $\sqrt{r} = \frac{m}{n}$, отсюда $r = \frac{m^2}{n^2}$ и получаем, что число $r$ рационально по определению. □

## Индукция

Отдельную сложность у студентов (увы, не только первокурсников) вызывают доказательства по индукции.

Доказательство по индукции возможно только тогда, когда доказываемое утверждение зависит от натурального параметра. То есть доказывается утверждение

$$\forall n \in \mathbb{N} : A(n).$$

С помощью правил вывода схему доказательства по индукции можно описать так:

$$\frac{A(0), \quad \forall n : A(n) \to A(n+1)}{\forall n : A(n)}.$$

Первая посылка называется ***базой***, а вторая — ***шагом*** индукции или ***переходом***.

**Пример 7.** Для каждого целого $n > 0$ справедливо

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

## От противного

Мы полагаем, что если утверждение $B$ истинно, то оно не может быть одновременно ложным. Если предположить, что утверждение $A$ ложно и с помощью него доказать, что ложно утверждение $B$, то есть доказать истинность $\neg A \to \neg B$, то в случае, если утверждение $B$ истинно, утверждение $A$ не может быть ложным — иначе бы мы получили истинность $B$ и $\neg B$. Отсюда вытекает способ доказательства от противного, который можно описать как

$$\frac{\neg A \to \neg B, \quad B}{A}.$$

Классический пример такого доказательства — иррациональность числа $\sqrt{2}$.
**Доказательство.** Доказательство от противного. Положим, что $\sqrt{2} = \frac{m}{n}$, где $\frac{m}{n}$ — несократимая дробь, $m \in \mathbb{Z}$, $n \in \mathbb{N}_1$. Тогда $m^2 = 2n^2$, отсюда $m^2$ делится на 2, и $m$ делится на 2, значит $m^2$ делится на 4, и отсюда $n^2$ делится на 2 и $n$ делится на 2. Но тогда и $m$ делится на 2 и $n$ делится на 2, а значит дробь $\frac{m}{n}$ сократима, пришли к противоречию. □

## Примеры и контрпримеры

В случае если утверждение имеет вид $\exists x : A(x)$, его можно доказать, приведя ***пример*** (и доказав справедливость этого примера). Рассмотрим утверждение:

$$\exists n \in \mathbb{N}_1 : \sqrt{n} \in \mathbb{R} \setminus \mathbb{Q},$$

то есть существует натуральное число $n$, корень из которого — иррациональное число. Это утверждение очевидно верно, и для его доказательства достаточно предъявить число $n = 2$ и доказать иррациональность числа $\sqrt{2}$.

Рассмотрим теперь утверждение

$$\forall n \in \mathbb{N}_1 : \sqrt{n} \in \mathbb{R} \setminus \mathbb{Q}.$$

Это утверждение, очевидно, неверно: достаточно взять $n = 4$ и показать, что $\sqrt{4} = 2 \in \mathbb{Q}$. Для опровержения утверждения с квантором всеобщности $\forall x : A(x)$ достаточно привести ***контрпример***, т.е. пример $x$, для которого $A(x) = 0$.

Заметим, что для доказательства утверждений вида $\forall x : A(x)$ одного примера не достаточно. Даже если утверждение $A(x)$ верно при каком-то $x$ или очень многих $x$, даже если их бесконечно много, отсюда ещё не вытекает, что утверждение $A(x)$ верно при всех $x$. Если все $x$ не проверены, то возможно среди не рассмотренных есть контрпример. Но как проверить бесконечно много $x$? Вот несколько рецептов. Провести доказательство утверждения $A(x)$, которое не зависит от выбора $x$. Если $x$ пробегает счётное множество значений (т. е. $\mathbb{N}_0$ или другое множество, элементы которого можно занумеровать натуральными числами), то можно воспользоваться индукцией. Воспользоваться методом доказательства от противного: предположить $\exists x : \neg A(x)$ и прийти к противоречию.

## Неконструктивные доказательства

Утверждение вида $\exists x : A(x)$ не обязательно доказывать приводя пример, хотя это очень желательно, если таковой имеется — наличие примера или контрпримера лучше всего убеждает в справедливости утверждения. Бывает так, что само утверждение доказать проще, чем найти пример и мы приведём здесь такое доказательство.

**Утверждение 2.** *Существуют иррациональные числа $a$ и $b$, такие что число $a^b$ рационально.*

**Доказательство.** Положим, что $a = b = \sqrt{2}$. Если число $(\sqrt{2})^{\sqrt{2}}$ рационально, то утверждение доказано. Если нет, то возьмём $a = (\sqrt{2})^{\sqrt{2}}$, а $b = \sqrt{2}$:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\left(\sqrt{2}\times\sqrt{2}\right)} = \left(\sqrt{2}\right)^{2} = 4.$$

То есть, либо подходит одна пара чисел, либо другая, а какая из — мы не знаем.

Обычно неконструктивные доказательства приводят в некоторое замешательство, особенно при первом знакомстве. Разберёмся со структурой доказательства, формализовав рассуждения.

Само утверждение имеет вид $\exists a, b : A(a, b)$. Мы предположили сначала, что справедливо утверждение $A(\sqrt{2}, \sqrt{2})$, если же оно неверно, то мы доказали, что отсюда вытекает утверждение $A((\sqrt{2})^{\sqrt{2}}, \sqrt{2})$. То есть мы доказали утверждение:

$$\neg A(\sqrt{2}, \sqrt{2}) \to A((\sqrt{2})^{\sqrt{2}}, \sqrt{2}).$$

Перейдя от импликации к дизъюнкции, получаем

$$A(\sqrt{2}, \sqrt{2}) \vee A((\sqrt{2})^{\sqrt{2}}, \sqrt{2}).$$

Доказанная дизъюнкция очевидно влечёт доказываемое утверждение $\exists a, b : A(a, b)$. □

# Таблица обозначений

| Обозначение | Расшифровка | Стр. |
|---|---|---|
| $x \wedge y$ | конъюнкция, логическое И | 4 |
| $x \vee y$ | дизъюнкция, логическое ИЛИ | 4 |
| $\neg x$, $\bar{x}$ | отрицание, инверсия, логическое НЕ | 4 |
| $x \to y$, $x \Rightarrow y$ | импликация, логическое следование | 4 |
| $x \leftrightarrow y$, $x \Leftrightarrow y$ | эквивалентность | 4 |
| $x \oplus y$ | исключающее или, XOR | 4 |
| $f(x_1, x_2) = 0101$ | задание булевой функции вектором значений | 5 |
| $\{1, 2, 3\}$ | описание множества перечислением его элементов | 10 |
| $\{x \mid \ldots\}$, $\{x : \ldots\}$ | описание множества через условие на его элементы | 10 |
| $x \in A$ ($x \notin A$) | $x$ (не) принадлежит множеству $A$ | 10 |
| $\lvert A \rvert$ | мощность (количество элементов) конечного множества $A$ | 10 |
| $\mathbb{N}_0$ | множество натуральных чисел $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ | 10 |
| $\mathbb{N}_1$ | множество положительных целых чисел $\mathbb{N}_1 = \{1, 2, \ldots\}$ | 10 |
| $\mathbb{Z}$ | множество целых чисел | 10 |
| $\mathbb{Q}$ | множество рациональных чисел | 10 |
| $\mathbb{R}$ | множество действительных чисел | 10 |
| $A \cup B$ | объединение множеств | |
| $A \cap B$ | пересечение множеств | |

| | |
|---|---|
| $A \setminus B$ | разность |
| $A \triangle B$ | симметрическая разность |
| $A \subseteq B$ $(A \not\subseteq B)$ | множество $A$ (не) подмножество множества $B$ |
| $A \subsetneq B$ | $A$ собственное подмножество $B$ |
| $A(x)$ | предикат: $A(x) = 1$, если $x \in A$, иначе $A(x) = 0$ |
| $U$ | юнивёрсум |
| $\overline{A}$ | дополнение множества $A$: $\overline{A} = U \setminus A$ |
| $\forall x$ | квантор всеобщности: для любого $x$ |
| $\exists x$ | квантор существования: существует $x$ |
| $\dfrac{A, \quad B}{C}$ | логический вывод: истинность $A$ и $B$ влечёт истинность $C$ |