Дискретная математика

КОНСПЕКТЫ ЛЕКЦИЙ
МФТИ 2020

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.*

Литература: [1], [2]

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.

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)

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

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.

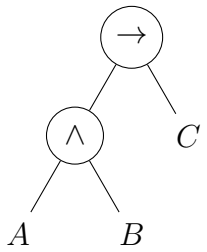

Рис. 1.2. Дерево для формулы $(A \wedge B) \to C$

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 $\to$;

5) эквивалентность $\leftrightarrow$.

Согласно этим договорённостям можно восстановить скобки: самый высокий приоритет у отрицания, самый низкий — у эквивалентности. 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 $x_1 \to \neg x_2 \wedge x_1 \vee x_2$ получим

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

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.

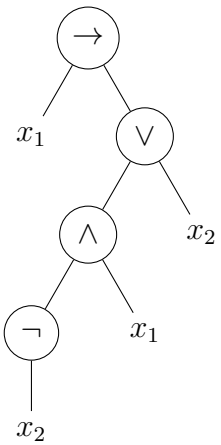

Рис. 1.3. Дерево для формулы из примера 1

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 вызывает 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

Литература: [1], [3]

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 $\{x \mid x = 2k + 1 \text{ для некоторого } k \in \mathbb{N}_0\}$ 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.

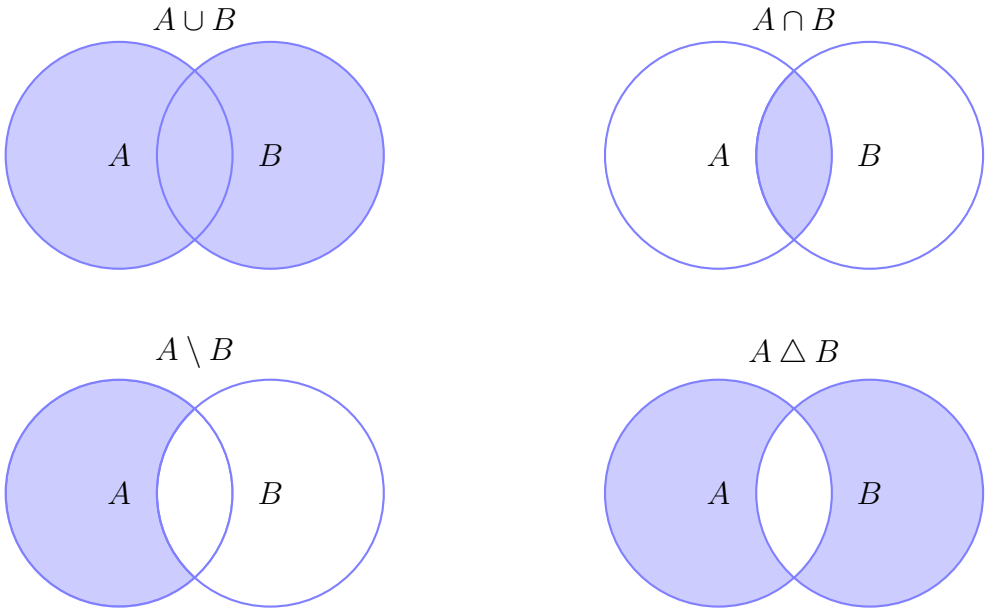

Рис. 2.1. Диаграммы Эйлера-Венна.

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 $\mathbb{N}_0$, 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. Методы доказательств: контрапозиция, индукция, от противного, конструктивные (примеры и контрпримеры), неконструктивные.
3. Границы применимости: парадокс Рассела.

Литература: [4], [5], [6], [1]

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.

Пример 5. Формула

$$\forall \varepsilon > 0 \; \exists N \in \mathbb{N}_1 : \forall n \geqslant N \; |x_n - a| < \varepsilon$$

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.

Рассмотрим утверждения вида

$$\forall x(A(x) \to B(x)) \tag{1}$$

Условие $B(x)$ является ***необходимым*** для выполнения $A(x)$, а условие $A(x)$ является ***достаточным*** для выполнения $B(x)$. Условие $A(x)$ считатеся более ***сильным***, чем $B(x)$, а $B(x)$ считается более ***слабым***, чем $A(x)$.

Смысл этих определений вытекает из определения импликации, напомним что уравнение (1) на языке множеств означает, что $A \subseteq B$, где A и B множества, соответствующие предикатам ($A = \{x \mid A(x)\}$). Отсюда вытекает, что условие $B(x)$ выполняется всегда, когда выполняется $A(x)$, отсюда $A(x)$ — достаточное условие; если условие $A(x)$ выполняется, то всегда выполняется и $B(x)$, отсюда $B(x)$ — необходимое условие. Условие $A(x)$ считается сильнее условия $B(x)$, потому что все условия, которые следуют из выполнения $B(x)$, также следуют и из выполнения $A(x)$:

$$\{C(x) \mid \forall x(A(x) \to C(x))\} \supseteq \{C(x) \mid \forall x(B(x) \to C(x))\}.$$

Отметим также, что в случае теорем вида $\forall x(A(x) \to C(x))$ и $\forall x(B(x) \to C(x))$ вторая теорема считается сильнее первой, потому что в ней условие $C(x)$ следует из более слабого условия $B(x)$.

3.3 Доказательства

Доказательство — это логическое рассуждение, которое убеждает в верности математического утверждения любого непредвзятого слушателя (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. В формальной логике у этого правила есть своё имя (Modus Ponens), а у правил вывода есть специальная запись:

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

Запись 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. Мы не будем уделять внимание разным правилам вывода и акцентировать внимание на этой записи — мы привели их здесь, чтобы описать общие идеи.

Первая состоит в том, что если известна истинность какого-то сложного (составного) логического высказывания, то используя преобразования формул или логические рассуждения можно доказать истинность или ложность частей этого выссказывания, вплоть до элементарных высказываний (логических переменных). Например, пусть известно, что следующее высказывание истинно

$$(\neg A) \wedge (A \vee B) \tag{2}$$

Отсюда сразу следует, что истинны операнды конъюнкции: $\neg A$ и $A \vee B$. Из истинности первого операнда следует, что $A = 0$, а из этого факта и истинности второго операнда следует $B = 1$. В процессе решения задач и доказательства теорем, не обязательно известна истинность сложного выссказывания, как правило известна истинность нескольких фактов, например $\neg A$ и $A \vee B$, из которых можно составить сложное высказывание (2) и с помощью логических преобразований получить

результаты, которые мы получили, но в то же время можно и не составлять формулу (2), а использовть логическое рассуждение. Поэтому в логике, полученное нами правило вывода записали бы так:

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

Отметим, что это правило вывода, как и многие другие, сводится 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

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \to B. \tag{3}$$

Если известно, что все утверждения A_i истинны, и истинно утверждение (3), то эти факты в совокупности влекут (доказывают) истинность утверждения B.

В этой части лекции мы использовали форму (формулы записи логического вывода), чтобы раскрыть суть. При доказательстве на каждом шаге у вас есть множество (список) истинных утверждений. Часть из них берётся из условия доказываемого утверждения, часть — факты из курса, а какую-то часть вы уже доказали. Используя логические рассуждения (преобразования, логические тождества, таблицы истинности) вы можете доказать истинность новых рассуждений, и расширить тем самым этот список. Расширять список нужно до тех пор, пока в нём не окажется доказываемое утверждение. Описанный процесс и является нашим ***требованием к доказательствам***. При работе с доказательствами (решении задач) нужно следовать сути этого метода, а не форме записи логического вывода, которая вторична.

Приведём пример.

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. □

Заметим, что если записать условие примера с помощью формулы, то она получится очень длинной, и придётся мучиться с её упрощением. При доказательствах следует использовать логику по сути, а не пытаться всё формализовать излишне, если это путает дело.

Повторим, что наши требования к доказательствам (решениям) 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, и какая между ними логическая связь; полезно помогать себе и читателю доказательства, явно выделяя вспомогательные утверждения.

Когда много доказательств используют одну и ту же структуру (опираются на одинаковую тавтологию), выделяют метод доказательства. Мы переходим к перечислению различных методов доказательств и примерам их применения.

Контрапозиция

Закон контрапозиции основан на тавтологии

$$(A \to B) \leftrightarrow (\neg B \to \neg A).$$

Он гласит, что утверждение $A \to B$ равносильно (контрапозитивному) утверждению $\neg B \to \neg A$, поэтому если требуется доказать первое, вместо него достаточно доказать последнее.

Смысл закона контрапозиции 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

$$\forall n \in \mathbb{N}_0 : A(n).$$

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

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

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

Заметим, что в случае утверждений, записанных формулой с кванторами (такие формулы называют формулы первого порядка), проверить истинность утверждения не всегда просто. Описанную с помощью вывода тавтологию

$$A(0) \wedge \forall n \, \big(A(n) \to A(n+1)\big) \to \forall n \, A(n)$$

либо причисляют к аксиомам (утверждениям, истинным по определению), либо выводят из других аксиом. Поэтому простого и достаточно строгого обоснования метода математической индукции дать не получится. Неформальное обоснование метода фактически опирается на сам метод: ясно, что если утверждения $A(0)$ и $A(0) \to A(1)$ истинны, то по M.P. получаем, что и утверждение $A(1)$ истинно, а далее по индукции, т. е. при фиксированном n и истинных $A(n)$ и $A(n) \to A(n+1)$ получаем истинность $A(n+1)$.

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

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

Доказательство. Обозначим доказываемое равенство через $A(n)$ и докажем его по индукции. Оговоримся сразу, что без ограничения общности можно считать, что база начинается не обязательно с нуля, как в этом примере, потому что вместо доказательства справедливости утверждения $A(n)$ с единицы можно было бы доказывать утверждение $B(m) = A(m+1)$ с нуля.

База: при $n = 1$ утверждение $A(1)$ утверждает равенство $1 = 1^2$, которое справедливо. Докажем переход; утверждение $A(n+1)$ гласит

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

Считая утверждение $A(n)$ верным, получаем цепочку равенств

$$\underbrace{1 + 3 + 5 + \cdots + (2n-1)}_{=n^2 \text{ по утверждению } A(n)} + (2n+1) = n^2 + 2n + 1 = (n+1)^2,$$

которая доказывает утверждение $A(n+1)$. □

Более подробному изложению индукции и связанных с нею проблемам посвящена первая глава книги [1].

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:

$$\exists n \in \mathbb{N}_0 : \sqrt{n} \in \mathbb{R} \setminus \mathbb{Q},$$

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

$$\forall n \in \mathbb{N}_0 : \sqrt{n} \in \mathbb{R} \setminus \mathbb{Q}.$$

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 $b = \sqrt{2}$:

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

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 $\exists a, b : A(a, b)$. □

3.4 Границы применимости

Хорошо известно, что у физических теорий есть границы применимости: при больших скоростях законы Ньютоновской механики становятся неприменимы, и требуется использовать теорию относительности, а в микромире нужна квантовая механика. Удивительно, но границы применимости есть и у логики, а точнее у теории множеств. За две последние лекции вы должны были убедиться, что эти области тесно связаны.

Мы изучили наивную теорию множеств (не заботились об аксиоматических определениях), которая вообще говоря неверна, и в качестве иллюстрации этого часто приводят парадокс Рассела, известный также как парадокс брадобрея, который звучит так.

Есть деревня, в которой бреется каждый мужчина. При этом либо каждый мужчина бреется сам, либо его бреет единственный в деревне брадобрей (парикмахер). Таким образом, брадобрей бреет тех и только тех мужчин, которые не

бреются сами. Парадокс состоит в том, что бреет ли себя брадобрей? Если да, то он бреется сам, значит брадобрей, то есть он же, брить себя не должен. Если он не бреется сам, то его обязан брить брадобрей.

На язык теории множеств этот парадокс переводится так. «Содержит ли себя множество, которое содержит в качестве элемента каждое множество, которое не содержит себя (в качестве элемента)?» И в случае ответа «да», и в случае ответа «нет» приходим к противоречию.

Как же нам вести доказательства, если мы используем наивную теорию множеств, которая вообще говоря противоречива? Хорошие новости состоят в том, что с момента обнаружения проблем, математики занимались формализацией теории множеств, разработали формальную логику, и мы можем использовать плоды их трудов для наших скромных целей. Как видно, проблемы парадокса начинаются когда мы рассматриваем неограниченный юнивёрсум (множество всех множеств в принципе). В наших рассуждениях мы всюду будем использовать ограниченные и довольно скромные (по мощности) юнивёрсумы. Поэтому подход к доказательствам, принятый в нашем курсе безопасен для наших целей.

Лекция 4

Графы I. Простые неориентированные графы

План:

1. Определение неориентированных графов
2. Степень вершины. Сумма степеней вершин — удвоенное количество рёбер.
    - Число людей, сделавших нечётное число рукопожатий, чётно.
3. Теоретико множественные операции с графами. Определение подграфа
4. Определение путей и циклов (через подграфы)
5. Связные графы и компоненты связности (через подграфы)

Литература: [7], [8], [1]

Мы переходим сейчас к изучению графов по двум причинам. Во-первых, графы иллюстрируют как можно легко ввести новые определения пользуясь аппаратом теории множеств, а во вторых графы — прекрасный полигон для упражнений в доказательствах.

Неформально определение графа легко объяснить с помощью картинок: нарисуем точки, соединим их линиями и получим тем самым граф. Сразу нужно оговориться, что пересечения линий смысла не несут и то, что мы соединяем линиями только разные точки, и каждую пару точек соединяем линией не более одного раза.

Понятие графа легко формализовать с помощью теории множеств. Точки образуют множество ***вершин*** V (произвольное множество любой природы), а линии формализуются как его двухэлементные подмножества $\{u, v\}$, которые образуют множество рёбер E. Поскольку в каждое ребро состоит ровно из двух

элементов, то нет рёбер из вершины в себя, они бы имели вид $\{v\}$, такие рёбра называются ***петлями***; поскольку множество содержит каждый элемент не более одного раза, то двух рёбер между одной и той же парой вершин быть не может, такие рёбра называют ***кратными*** или ***параллельными***.

Введём вспомогательное обозначение. Обозначим через $\binom{A}{2}$ все двухэлементные подмножества множества A, т. е.

$$\binom{A}{2} = \{\{a, b\} \mid a, b \in A,\ a \neq b\}.$$

Формализуем определение графа. (Простой, неориентированный) ***граф*** G — состоит из множества ***вершин*** V и ***рёбер*** $E \subseteq \binom{V}{2}$; формально, граф — это упорядоченная пара $G = (V, E)$. Будем ссылаться на множество вершин и множество рёбер графа G через $V(G)$ и $E(G)$, даже если при определении графа G множества вершин и множество рёбер были обозначены другими буквами. Если множества вершин V и рёбер E заданы, то граф на них обозначают $G(V, E)$, это обозначение используют также чтобы быстро ввести множество вершин и множество рёбер графа: запись $H(W, I)$ означает, что $W = V(H), I = E(H)$.

Если не оговорено противного, то под графом мы понимаем простой неориентированный граф. ***Простой*** означает, что в графе нет петель и кратных рёбер, а ***неориентированный***, что рёбра графа не имеют направлений. В случае если заменить в графе линии на стрелки, т. е. ребро — упорядоченная пара вершин, то получится ***ориентированный граф***. Заметим, что множество вершин графа может вообще говоря быть бесконечным или пустым, но если не оговорено противного, то мы считаем, что множество вершин конечно и непусто.

4.1 Вершины, рёбра степени вершин

Зафиксируем граф $G(V, E)$. Вершины u и v называются ***смежными*** или ***соседями***, если они образуют ребро: $\{u, v\} \in E$. Рёбра e и f называются ***смежными***, если они имеют общую вершину: $e \cap f \neq \varnothing$. Вершина v ***инцидента*** ребру e, если $u \in e$. Вершины u и v, инцидентные ребру e, называются его ***концами***; говорят, что e ***соединяет*** u и v. Рёбра часто записывают сокращённо: uv вместо $\{u, v\}$.

Степенью вершины v называется число смежных с v рёбер и обозначается $d(v)$.

Теорема 1. $\sum\limits_{u \in V} d(u) = 2|E|$.

Доказательство. В левой сумме ребро $\{u, v\}$ было подсчитано два раза: один раз в слагаемом $d(u)$, а в другой раз в слагаемом $d(v)$. □

Из теоремы сразу вытекает следующее следствие:

Следствие 1. *В любом графе число вершин нечётной степени чётно.*

Доказательство. В правой части равенства (из условия теоремы) стоит чётное число. Вычтем из обеих частей равенства все чётные степени вершин и получим, что в левой части осталась сумма нечётных степеней вершин, а в правой — чётное число. □

Это тривиальное следствие позволяет доказывать следующие странные утверждения, такие как «число людей в этой аудитории, пожавших с утра руки нечётному числу людей (в этой аудитории), чётно».

4.2 Базовые графы

Приведём примеры графов, которые встречаются в теории графов так часто, что получили собственные имена.

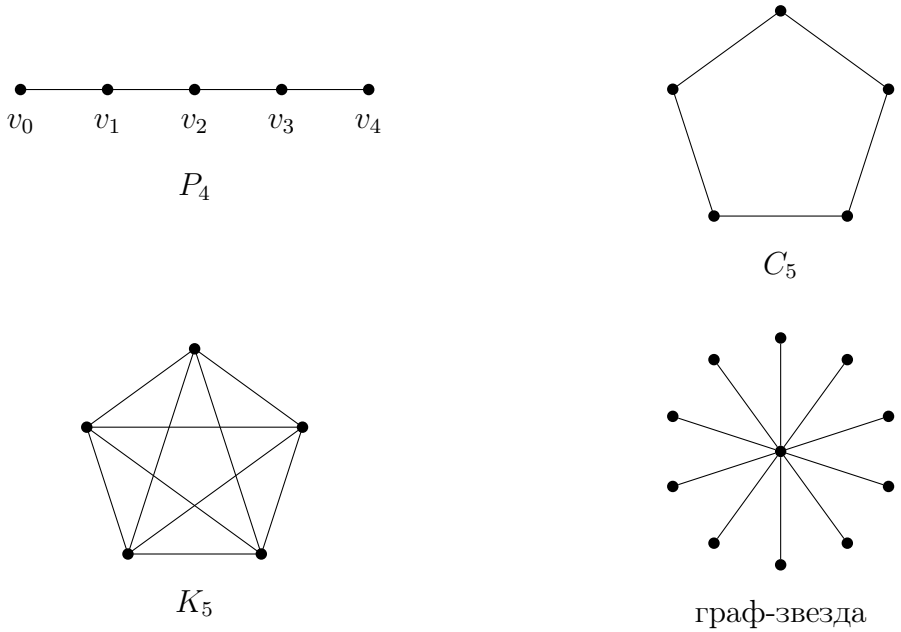

Рис. 4.1. Базовые графы

Граф-путь P_n, $n \geqslant 0$ состоит из вершин $\{v_0, v_1, \ldots, v_n\}$ и рёбер $\{v_i, v_{i+1}\}$. ***Длина пути*** — это число рёбер в пути, которых в графе P_n ровно n (поэтому нумерация вершин графа начинается с нуля); вершина v_0 называется ***началом пути***, а вершина v_n — ***концом пути***. Заметим, что граф P_0 состоит из одной вершины и не имеет рёбер и полноправно считается путём длины 0. Мы называем графом-путём любой граф, представимый в описанном виде (природа множества вершин нас не интересует), это относится и к остальным графам с картинки.

Граф-цикл C_n, $n \geqslant 3$ состоит из вершин $v_1, \ldots, v_n$ и рёбер $\{v_i, v_{i+1}\}$, а также $\{v_n, v_1\}$. Как и в случае пути, длина цикла — это количество рёбер в цикле.

Полный граф $K_n(V, E)$, $n \geqslant 1$ состоит из n вершин и имеет всевозможные рёбра: $E = \binom{V}{2}$.

Граф-зведа состоит из выделенной вершины, соединённой рёбрами со всеми остальными вершинами (больше рёбер в этом графе нет).

Пустой граф не содержит ни вершин, ни рёбер: $V = E = \varnothing$ и обозначается как $\varnothing$. Во всех утверждениях о графах мы полагаем, что граф G не пуст; пустой граф удобно использовать в формулах, например, чтобы кратко сказать, что графы G и H не имеют общих вершин и рёбер.

Обратим внимание, что если граф подпадает под одно из определений выше, то это вовсе не означает, что он не попадает под другое. Так граф-путь P_1 является одновременно графом-звездой, а граф-цикл C_3, ***треугольник***, является также полным графом K_3.

4.3 Теоретико-множественные операции с графами. Подграфы

Операции из теории множеств переносятся на графы естественным образом. Определим операции объединение, пересечение и дополнение графов, с помощью графов $G(V, E)$ и $H(W, I)$:

$$G \cup H = (V \cup W,\, E \cup I), \quad G \cap H = (V \cap W,\, E \cap I), \quad \overline{G} = \left(V,\, \binom{V}{2} \setminus E\right).$$

Операции объединения и пересечения определены естественным образом, а дополнение графа G — это минимальный граф $\overline{G}$ на том же множестве вершин, который при объединении с G даёт полный граф. Под минимальностью понимается, что из $\overline{G}$ нельзя удалить ребро и получить граф, который в объединении с G даст полный граф, это условие равносильно $E(G) \cap E(\overline{G}) = \varnothing$.

На рисунке 4.2 пример теоретико-множественных операций со знакомыми графами.

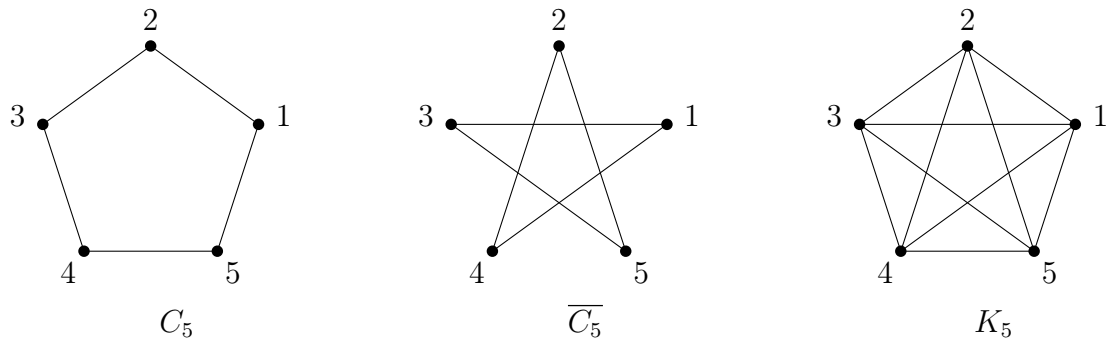

Рис. 4.2. Объединение графа и его дополнения даёт полный граф

Объединив граф C_5 с его дополнением получается граф K_5. При работе с теоретико-множественными операциями важно явно описать множество вершин каждого графа. Так, если бы у второго графа на картинке вместо вершин $\{1, 2, \ldots, 5\}$ были вершины $\{a, b, \ldots, e\}$, то в результате объединения получился бы другой граф. Также напомним, что обозначения вида C_n обозначают, что какой-то граф является графом-циклом. Так, граф $\overline{C_5}$ на картинке является графом C_5 — проверьте это перенумеровав его вершины.

Мы не определили на графах теоретико-множественную операцию разности (и соответственно симметрическую разность), потому что в зависимости от нужд требуется либо удалять из одного графа рёбра другого вместе с вершинами, либо вершины нужно оставить; чтобы не было путаницы мы будем явно указывать какую разность используем оперируя множествами вершин и рёбер, избегая сокращений.

Подграфы

Граф $H(W, I)$ называется ***подграфом*** графа $G(V, E)$, если $W \subseteq V$ и $I \subseteq E$. Другими словами, граф H получается из графа G удалением рёбер и вершин (вместе со смежными рёбрами). Это обозначают $H \subseteq G$. Мы используем определение подграфа, также известное как ***рёберный подграф***.

Формально, граф G является своим подграфом; чтобы подчеркнуть, что подграф H не совпадает с G используют обозначение $H \subsetneq G$; в этом случае подграф H называют ***собственным*** подграфом графа G.

Среди подграфов есть важный частный случай. Пусть $U \subseteq V$; подграф H графа G, состоящий из вершин U и содержащий все рёбра, которые есть в G называется ***индуцированным*** (множеством U); формально $H = \left(U, E \cap \binom{U}{2}\right)$. Для подграфа графа G индуцированного множеством U используют обозначение $G[U]$. По-умолчанию под подграфами мы подразумеваем рёберные подграфы.

С помощью понятия подграфа и базовых графов вводится ряд важных определений. Подграф H графа G называется

- ***путём*** из вершины u в вершину v, если H — это граф-путь P_n с началом в u и концом в v;
- ***циклом***, если H — это граф-цикл C_n;
- ***кликой***, если H — это полный граф K_n.

Множество $U \subseteq V(G)$ называется ***независимым***, если в индуцированном U подграфе нет рёбер, то есть $G[U] = \overline{K_n}$. Другими словами, никакие две вершины множества U не соединены ребром в графе G (это эквивалентное определение).

Перед следующим определением напомним, что формально объект обладает свойством $\mathcal{H}$, если он принадлежит множеству, определяемому этим свойством, которое мы обозначаем также, то есть $\mathcal{H} = \{x \mid \mathcal{H}(x)\}$; свойство формализовано через предикат $\mathcal{H}(x)$.

Пусть $\mathcal{H}$ — это некоторое свойство графов; обозначим через $\mathcal{H}_G$ все подграфы графа G, обладающие свойством $\mathcal{H}$. Подграф $H \subseteq G, H \in \mathcal{H}_G$ называется ***максимальным*** среди подграфов со свойством $\mathcal{H}$, если не существует подграфа $H' \in \mathcal{H}_G$, такого что $H \subsetneq H'$ и $H' \subsetneq G$.

Пример 8. Рассмотрим граф K_5 на рис. 4.2. Рассмотрим свойство «быть циклом». Любой подграф графа K_5, являющийся циклом будет максимальным циклом, потому что добавлением вершин и рёбер в цикл, нельзя получить другой цикл; таким образом графы C_5 и $\overline{C_5}$ на рис. 4.2 являются максимальными циклами графа K_5.

Рассмотрим свойство «быть кликой». Максимальной кликой будет только сам граф K_5, потому что какую бы другую клику мы не взяли, например $K_5[\{1, 2, 3, 4\}]$, её можно превратить в клику большего размера, добавив остальные вершины и рёбра: $K_5[\{1, 2, 3, 4\}] \subsetneq K_5[\{1, 2, 3, 4, 5\}] = K_5$.

Рассмотрим свойством «быть кликой чётного размера». Любая клика графа K_5 на четырёх вершинах, например $K_5[\{1, 2, 3, 4\}]$, будет максимальной кликой чётного размера, а любая клика размера два (ребро) хоть и будет обладать этим свойством, максимальной кликой чётного размера не будет.

4.4 Связность

Вершина u называется ***достижимой*** из v, если есть путь из v в u. Граф G называется ***связным***, если любая его вершина достижима из любой другой. Простая аналогия для понятия связности — города и дороги. Если V — множество городов, а E — множество дорог, то связность графа означает, что из любого города можно добраться до любого другого. Даже в реальной жизни граф автодорог может быть несвязным, в частности несвязен граф автодорог России — Калининградская область отрезана от России странами Европы.

Поэтому, при анализе дорожных сетей интересны ***компоненты связности*** — максимально связные подграфы графа G. То есть, H — компонента связности графа G, если $H \subseteq G$, H — связный граф и не существует связного подграфа $H' \subseteq G$, такого что $H \subsetneq H'$.

Очевидно, что компонента связности всегда индуцированный подграф, поэтому компоненту связности часто определяют как максимальное по включению подмножество вершин $U \subseteq V$, в котором каждая вершина достижима друг из друга. Заметим, что это определение не эквивалентно используемому нами, поскольку второе дано в терминах подграфов, а первое — в терминах подмножеств множества вершин, хотя между ними и есть взаимно однозначное соответствие: $U \mapsto G[U]$.

Любой граф является объединением его компонент связности. Изучив позже отношения эквивалентности, мы докажем, что компоненты связности либо не пересекаются, либо совпадают, то есть, если $H_1, \ldots, H_m$ — компоненты связности графа G, то

$$G = H_1 \cup H_2 \cup \ldots \cup H_m, \quad H_i \cap H_j = \varnothing.$$

Пока этим фактом можно пользоваться без доказательства; попробуйте доказать это утверждение самостоятельно. Компонента связности может состоять из одной вершины; в этом случае вершина имеет степень ноль и называется ***изолированной***.

Более подробно о связности мы поговорим на следующей лекции. На этой мы докажем следующую лемму.

Лемма 1. *Пусть $G(V, E)$ — связный граф и ребро e лежит на цикле; тогда граф $G' = (V, E \setminus \{e\})$ связный. То есть, удаление ребра цикла не нарушает связность.*

Перед доказательством введём вспомогательные обозначения. Пусть P и Q — пути в графе G, x, y — вершины, лежащие на пути P, а y и z — вершины, лежащие на пути Q. Обозначим через xPy — подпуть пути P, начинающийся с вершины x и заканчивающийся в вершине y; считаем, что вершины $p_0, p_1, \ldots, p_n$ пути P упорядочены так, что $x = p_i$, $y = p_j$, $i < j$ и соответственно $xPy = p_iPp_j$ — путь на вершинах $p_i, \ldots, p_j$. Если в результате объединения путей xPy и yQz получится путь, то мы обозначаем этот путь через $xPyQz$. Это обозначение переносится и на объединение нескольких путей, а если пути P и Q имеют единственную общую вершину — общий конец, то путь, получившийся их объединением обозначим через PQ.

Доказательство леммы 1. Пусть ребро e лежит в подграфе-цикле C. Обозначим через $Q \subseteq C$ подграф-путь, получающийся из C удалением ребра e (с сохранением

его концов). Зафиксируем все пути между всеми парами вершин перед удалением e и рассмотрим путь P с началом в вершине w и концом в вершине z.

Если ребро e не лежит на пути P, то после его удаления этот путь не пострадает. Если же e лежит на пути, то превратим этот путь в другой путь с помощью пути Q. Упорядочим вершины P; пусть вершина x — первая общая вершина путей P и Q (ближайшая к w, возможно сама w), а y — последняя общая вершина путей P и Q (ближайшая к z, быть может сама z). Вершины x и y определены, потому что пути P и Q имеют хотя бы две общие вершины — концы ребра e.

Докажем, что $wPxQyPz$ — путь, соединяющий вершины w и z, и не проходящий через ребро e. Действительно, пути wPx и xQy не имеют общих вершин, кроме x, поскольку иначе в пути P нашлась бы вершина ближе к w, чем x, которая была бы общая с путём Q, что противоречит выбору x; симметрично пути xQy и yPz не имеют общих вершин, кроме y (иначе нашлась бы общая вершина ближе к z, чем y); пути wPx и yPz не имеют общих вершин, поскольку это непересекающиеся подпути пути P.

Итак, мы доказали, что после удаления ребра e в графе по-прежнему останутся пути между всеми парами вершин, т. е. граф останется связным. □

Список литературы

1. Лекции по дискретной математике / М. Вялый, В. Подольский, А. Рубцов, Д. Шварц, А. Шень. — Черновик: https://publications.hse.ru/mirror/pubs/share/direct/393719078.pdf, 2020.
2. *Журавлёв Ю. И.*, *Флёров Ю. А.*, *Федько О. С.* Дискретный Анализ. Комбинаторика. Алгебра логики. Теория графов. — М.: МФТИ, 2012.
3. *Биркгоф Г.*, *Барти Т.* Современная прикладная алгебра. — Издательство "Мир", 1976.
4. *Lehman E.*, *Leighton F. T.*, *Meyer A. R.* Mathematics for Computer Science. — United Kingdom : Samurai Media Limited, 2017. — URL: https://courses.csail.mit.edu/6.042/spring17/mcs.pdf.
5. *Sipser M.* Introduction to the Theory of Computation. — Third. — Boston, MA : Course Technology, 2013. — ISBN 113318779X.
6. *Мендельсон Э.* Введение в математическую логику: — УРСС, 2010. — ISBN 9785397013871.
7. *Дистель Р.* Теория графов. — Новосибирск: Институт математики, 2002.
8. *Lovasz L.*, *Vesztergombi K.* Discrete Mathematics. Lecture Notes, Yale University. — 1999. — URL: http://www.cs.elte.hu/~lovasz/dmbook.ps.
9. *Зуев Ю.* По океану дискретной математике: От перечислительной комбинаторики до современной криптографии. Т.1: Основные структуры. Методы перечисления. Булевы функции. — М.: Книжный дом «ЛИБРОКОМ», 2012.
10. *Зуев Ю.* По океану дискретной математике: От перечислительной комбинаторики до современной криптографии. Т.2: Графы. Алгоритмы. Коды, блоксхемы, шифры. — М.: Книжный дом «ЛИБРОКОМ», 2012.
11. *Яблонский С.* Введение в дискретную математику. — М.: Высшая школа, 2003.
12. *Грэхем Р.*, *Кнут Д.*, *Паташник О.* Конкретная математика. Математические основы информатики. — Вильямс, 2010.
13. *Харари Ф.* Теория графов. Изд. 2-е. — М.: Эдиториал УРРС, 2003.
14. *Андерсон Д. А.* Дискретная математика и комбинаторика. — М.: Вильямс, 2003.

15. Сборник задач по дискретному анализу. Комбинаторика. Элементы алгебры логики. Теория графов / Ю. И. Журавлёв, Ю. А. Флёров, О. С. Федько, Т. М. Дадашев. — М.: МФТИ, 2004.