Математическая логика

Ипатов Марк

13 июня 2022 г.

Содержание

1. Множества, мощность множеств

1.1. Равномощные множества и Счётные множества

...тут я ещё не начинал записывать

***Определение* 1.1.** Множества A и B равномощны, если $\exists$ биекция между A и B

Замечание. Равномощность является отношением эквивалентности. Очев.

Возможная, но не совсем корректная трактовка — равномощные множества — содержащие равное количество элементов. Для конечных это действительно верно, а с бесконечными уже не совсем понятно, сколько в них элементов. «Бесконечность»?

***Определение* 1.2.** Множество называется счётным, если оно равномощно множеству натуральных чисел.

Пояснение: мы считаем натуральными числами множество $\{1, 2, 3, \cdots\}$, но никакой разницы с $\{0, 1, 2, 3, \cdots\}$ нет, т.к. существует биекция из одного в другое — $i \to i - 1$.

Пример. Чётные числа — счётное множество. Биекция — $i \to 2 \times i$

Лемма. A, B — счётны $\Rightarrow A \cup B$ — счётно при $A \cap B = \varnothing$.

Доказательство. $\exists f : N \to A \Rightarrow A : \{a_1, a_2, a_3, \cdots\}$

Аналогично $B : \{b_1, b_2, b_3, \cdots\}$

Тогда запишем:

$C : \{a_1, b_1, a_2, b_2, \cdots\}$, $c_{2i-1} = a_i, c_{2i} = b_i$ □

Следствие. $\mathbb{Z}$ — счётно.

Доказательство. $\mathbb{Z} = \{0, 1, 2, \cdots\} \cup \{-1, -2, -3, \cdots\}$, первое равномощно $\mathbb{N}$, как и второе, а значит $\mathbb{Z}$ — счётно по предыдущей лемме. □

Лемма. B — счётное, $A \subset B$, тогда A — конечное или счётное.

Доказательство. B — счётно, тогда можно записать $B : \{b_1, b_2, \cdots\}$

Раз A подмножество, то просто часть элементов отсутствует. Тогда мы пойдём сопоставлять числа оставшимся элементам. Первое оставшееся — 1, второе — 2, и т.д. Тогда или в какой-то момент у нас закончатся оставшиеся числа, т.е. найдётся то, после которого нет оставшихся, и тогда A — конечно, или мы построим биекцию между A и натуральными числами. Это биекция, поскольку это инъекция и сюръекция (мы каждому натуральному поставили число, и всем элементам A что-то одно сопоставили) □

Теорема 1.1 (Лемма)**.** Любое бесконечное множество содержит счётное подмножество.

***Определение* 1.3.** Множество X бесконечно, если $\forall i \in \mathbb{N}$ можно найти i различных элементов из X.

Доказательство. Возьмём элемент из X. Назовём его a_1. Если в X не осталось элементов, значит в нём был всего один элемент. Иначе возьмём из X какой-то другой элемент, назовём его a_2. Если снова не осталось, то было всего два элемента. И так далее, построили $Y = \{a_1, a_2, a_3, \cdots\}$, и $Y \subset X, f : \mathbb{N} \Leftrightarrow Y$. $\square$

Пример. То, что мы нашли счётное подмножество, никак не доказывает счётность исходного множества. Например, мы могли в своём процессе вытащить далеко не все элементы X: Счётное множество, для которого мы таким процессом не докажем счётность: $X = \{1, 2, 3, \cdots\}$, а выбрали из него — $Y = \{2, 4, 6, \cdots\}$.

Пример. Множество $(0, 1)$ не является счётным. Пока что, видимо, без доказательства.

Следствие. Если $A_1, A_2, A_3, \cdots, A_k$ — счётны, то $A_1 \cup A_2 \cup \cdots A_k$ — счётно

Доказательство. Для дизъюнкных уже понимаем: последовательно объединим первое со вторым, результат с третьим, и так далее до k-го. А для недизъюнктных:

Посмотрим на A_1 и $A_2 \setminus A_1$. Оба счётны, а тогда $A_1 \cup A_2 = A_1 \sqcup (A_2 \setminus A_1)$, где оба счётные.

Теперь воспользуемся индукцией по k: База: A_1, A_2 счётны по условию, тогда $A_1 \cup A_2$ тоже счётно. Тогда $(A_1 \cup A_2 \cup A_3 \cdots A_k) = ((\cdots((A_1 \cup A_2) \cup A_3) \cup \cdots) \cup A_k)$, т.е. по сути то же, что и для дизъюнктных. Мы просто свели пересекающиеся к непересекающимся, на самом деле. $\square$

Лемма. $A_1, A_2, \cdots$ — счётное число счётных множеств, т.е. $\forall i \in \mathbb{N} \exists A_i$— счётное множество.

Тогда $A_1 \cup A_2 \cup \cdots$ тоже счётно.

Доказательство. A_1 счётно, тогда $A_1 : \{a_{11}, a_{12}, a_{13}, \cdots\}$. Аналогично $A_2 : \{a_{21}, a_{22}, a_{23}, \cdots\}$ И так далее ещё счётное число строк.

Теперь нам нужно эту таблицу представить в виде последовательности. Будем ходить по диагоналям: $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \cdots$

Утверждение — любой элемент будет выписан. Рассмотрим элемент множества i номер j, тогда оно будет на $i + j$-ой диагонали, а значит его номер точно не будет превышать $(i + j)^2$. Тогда получаем, что любой элемент будет выписан.

Это всё для непересекающихся множеств, а для пересекающихся — давайте просто не выписывать элементы, которые уже выписали. $\square$

Упражнение. $\mathbb{N}, \mathbb{Z}$ — счётны. $[0, 1)$ — несчётно (просто знаем), знаем $\mathbb{R}$ — несчётно. $\mathbb{Q}$ — счётно или нет?

Доказательство. $\mathbb{Q}_+$ счётно. Давайте представим его в виде $A_1 \cup A_2 \cup \cdots$, где $A_i = \{\frac{m}{i} | m \in \mathbb{N}\}$. Так получили, что $\mathbb{Q}_+$ это ровно счётное число счётных множеств. А тогда мы получаем (по предыдущей теореме), что $\mathbb{Q}_+$ счётно. Аналогично получим, что $\mathbb{Q}_-$ тоже счётно, добавим ноль, объединим полученное (два счётных множества и ноль) и получим, что $\mathbb{Q}$ — счётно, ура. $\square$

Лемма. A, B — счётны, тогда $A \times B$ — счётно.

Доказательство. A, B — счётны, тогда $A : \{a_1, a_2, \cdots\}$, $B : \{b_1, b_2, \cdots\}$ Элементы из $A \times B$ выглядят так: (a_i, b_j), тогда давайте запишем следующее:

$A_1 = a_1 \times B = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), \cdots\}$, A_2 аналогично, и так далее. Тогда каждое A_i — счётно, и их счётное число, значит их объединение, которое и есть $A \times B$ счётно, по доказанной лемме. $\square$

1.2. Несчётные множества

Лемма. Пусть A бесконечно, а B — конечно. Тогда $A \cup B$ равномощно A.

Доказательство. B заменим на $B' = B \setminus A$. B' или станет пустым, или останется конечным.

Очевидно, что $A \cup B = A \sqcup B'$

У A есть счётное подмножество $A' = \{a_1, a_2, \cdots\}$, тогда $A = (A \setminus A') \cup A'$.

Хотим построить биекцию между $A = A' \cup (A \setminus A')$ и $A' \cup B' \cup (A \setminus A')$

Часть «$(A \setminus A')$» есть в обеих половинах, а значит между $(A \setminus A')$ слева и $(A \setminus A')$ справа построим тождественную биекцию. Из оставшегося $a_i \in A'$ будем отображать в $b_i \in B'$, если $i \leqslant k$, или в a_{i-k} при $i > k$. Понятно, что это биекция. Таким образом мы возьмём все элементы как из B, так и из A'. □

Замечание. Доказательство можно модифицировать для случая, когда B счётно. Тогда давайте на последнем шаге чётные индексы отображать в $a_{\frac{i}{2}}$, а нечётные — в $b_{\frac{i-1}{2}}$.

Теорема 1.2. Множество X последовательностей (бесконечных) из нулей и единиц не счётно. (Бинарные строки бесконечной длины)

Доказательство. От противного: пусть счётен, тогда есть биекция $f\colon \mathbb{N} \to X$. Тогда выпишем последовательности $f(1), f(2), f(3), \cdots$. А теперь воспользуемся диагональным (методом Кантора): Посмотрим на элемент a_{11}, возьмём элемент $1 - a_{11}$. Затем на элемент a_{22}, возьмём $1 - a_{22}$. И так далее, строим последовательность $1 - a_{ii}$. Получили бесконечную последовательность нулей и единиц, значит она элемент X. Но при этом она не может быть любой i-ой последовательностью, поскольку её i-ый элемент не совпадает с i-ым элементом строки i по тому, как мы строили нашу последовательность. Противоречие. Значит мы не можем вот так вот выписать наши элементы X, значит биекции f не существует. □

Следствие. Множество чисел из отрезка $[0, 1]$ несчётно.

Доказательство. Покажем равномощность множеству X из теоремы. Из бесконечной последовательности число получить легко — припишем слева «0,», а все элементы последовательности запишем слитно. Могло показаться, что получили биекцию, но нет. У нас разные последовательности могут соответствовать одному числу — $0,100000000\cdots$ и $0,011111111\cdots$ — разные последовательности, но являются одним числом. Возьмём две последовательности — $0,a_{11}a_{12}a_{13}\cdots$, $0,a_{21}a_{22}a_{23}\cdots$. Утверждение — они задают одно число тогда и только тогда, когда они имеют совпадающий префикс, а затем у одного числа идёт единица и после только нули, а у второго ноль и затем только единицы. Докажем от противного — пойдём по таким двум числам слева направо и найдём первый момент, когда они отличаются. В одном ноль, во втором единица. Далее всё идёт сколько-то, как мы предсказали (там где ноль — единицы, где единица — нули), затем, раз от противного, что-то пойдёт не так. Тогда в этот момент расхождения с предсказанием можно посмотреть на текущие величины чисел, образованные пройденными префиксами (до момента расхождения с предсказанием включительно) и можно заметить, что на этот момент числа отричаются настолько, что дальше мы даже бесконечностью цифр не сможем сделать расстояние между двумя числами сделать сколь угодно близким к нулю. А числа такого вида это просто суммы некоторых конечных количеств отрицательных степеней двойки, что есть подмножество $\mathbb{Q}$, а значит их счётное число. Можно записать, словно это $\mathbb{Q} \cap [0, 1]$ и ничего не потерять Тогда $X \sim [0, 1] \sqcup (\mathbb{Q} \cap [0, 1])$. Результат пересечения счётен, а значит объединение равномощно бесконечной левой части, т.е. $X \sim [0, 1]$ □

Теперь знаем, что натуральные счётны, чётные счётны, целые счётны, рациональные положительные счётны, просто рациональные счётны. А вот вещественные ($\mathbb{R}$) уже несчётны, т.к. содержат $[0,1]$.

Пример. Множество точек границ треугольника и вписанного круга равномощны, т.к. можно построить биекцию из центра.

Теорема 1.3. $X = [0,1]$ и $Y = [0,1] \times [0,1]$ равномощны (т.е. отрезок равномощен квадрату).

Доказательство. Рассмотрим произвольный элемент из Y. Он представляет из себя пару чисел из $[0,1]$, т.е. две бесконечные битовые строки — x_i и y_1. Тогда давайте построим из этих двух битовых строк новую, забирая элементы из исходных поочерёдно — $x_1y_1x_2y_2\cdots$. Это будет новая битовая строка, так что она лежит в $[0,1]$, но при этом она однозначно соответствует исходной паре битовых строк x_i и y_i. Таким образом мы получили биекцию между множеством пар битовых строк и просто множеством битовых строк, а значит искомые множества равномощны, что и требовалось доказать. □

Теперь давайте вернёмся к теореме о несчётности отрезка $[0,1]$ и докажем это снова, но уже другим способом.

Доказательство. Возьмём множество вложенных отрезков $I_1 \subset I_2 \subset I_3 \subset \cdots, \forall i \in \mathbb{N} I_i \subset [0,1]$. Из матанализа знаем, что пересечение всех этих отрезков непусто.

Теперь предположим, что $[0,1]$ — счётно. Тогда занумеруем все его элементы — $a_1, a_2, \cdots$.

Теперь будем строить систему отрезков. Разобьём $[0,1]$ на три части. Заметим, что a_1 может лежать не больше чем в двух из них, а значит найдётся часть, в которой нет точки a_1. Положим эту часть за I_1. I_1 в свою очередь тоже разобьём на три части, и положим за I_2 ту из них, в которой не лежит точка a_2. И так далее, получим систему вложенных отрезков, причём $a_j \notin I_j$.

Мы знаем, что для множества вложенных отрезков (которые являются подотрезками $[0,1]$) существует точка, лежащая во всех них. Назовём её x. Но тогда, раз мы занумеровали все точки $[0,1]$, то $x = a_j$, но $a_j \notin I_j$, а значит и не лежит в пересечении, противоречие. □

Теперь немного отойдём, видимо, в сторону:

Теорема 1.4 (Кантора-Бернштейна)**.** Пусть A, B — множества, и существуют $f : A \to B$ — инъекция и $g : B \to A$ — тоже инъекция. Тогда существует биекция h между A и B (и, как следствие, множества равномощны)

Доказательство. Давайте построим ориентированный двудольный граф. Вершины левой доли — элементы множества A, левой — множества B. Проведём рёбра соответствующие отображениям ($f(a_1) = b_1$ — проводим ребро из a_1 в b_1, $g(b_2) = a_2$ — проводим ребро из b_2 в a_2). Тогда у нас из каждой вершины точно выходит ребро, и в каждую вершину входит не больше одного ребра (т.к. инъекции).

Что может быть в полученном графе?

1. Циклы
2. Цепочки с началом, но без конца
3. Цепочки без начала и без конца

Цепочек с концом быть не может, т.к. из каждой вершины всё же есть ребро, значит всегда есть, куда идти (ну или замыкаться).

Теперь построим биекцию. Все циклы у нас бывают только чётной длины, т.к. граф двудольный, а значит их можно разбить на пары, которые и положим в биекцию. Для второго случая просто сопоставим первый элемент со вторым, третий с четвёртым и т.д. А для третьего — ткнём в случайное место, и пойдём разбивать на пары, но уже в обе стороны одновременно.

Каждый элемент попадает ровно в один случай из трёх, а значит попадёт в какую-то пару. Вот и биекция. $\square$

Вам доказательство показалось каким-то странным? Хорошо, держите ещё одно:

Доказательство. Положим $A_0 = A, A_1 = g(B) \subset A_0$. Так мы получаем, что g есть биекция между A_1 и B. Положим $A_2 = g(f(A)) \subset g(B) = A_1$. Так получили $A_2 \subset A_1 \subset A_0$, а ещё $g(f(A))$ — биекция между A_0 и A_2. Да и вообще положим $h = g \circ f$. Это будет биекция между A_i и A_{i+2}. Так то нам нужно доказать, что A_0 равномощно A_1, и тогда мы победим, поскольку $A_0 = A$, а A_1 равномощно B.

Введём $C_i = A_i \setminus A_{i+1}$. Заметим, что C_i равномощно C_{i+2}, поскольку $C_{i+2} = A_{i+2} \setminus A_{i+3}, C_i = A_i \setminus A_{i+1}$, а A_i и A_{i+2} равномощны (т.к. есть биекция — h), ровно как равномощны и A_{i+1} с A_{i+3} (по той же причине).

Положим $C = \bigcap A_i$. Тогда:

$$A_0 = \overbrace{(A_0 \setminus A_1)}^{=C_0} \cup \overbrace{(A_1 \setminus A_2)}^{=C_1} \cup \overbrace{(A_2 \setminus A_3)}^{=C_2} \cup \dots \cup C$$
$$A_1 = \underbrace{(A_1 \setminus A_2)}_{=C_1} \cup \underbrace{(A_2 \setminus A_3)}_{=C_2} \cup \dots \cup C$$

Теперь отобразим частями: C в C, C_0 в C_2, C_1 в C_3 и так далее. Мы знаем, что они в парах равномощны, и так мы в итоге построили биекцию, т.к. каждый объект попал в какую-нибудь часть. Всё, ура, A_0 и A_1 равномощны, а значит равномощны и A с B, т.е. есть биекция, ура! $\square$

Теорема 1.5 (Теорема Кантора)**.** Пусть X — множество, а 2^X — множество всех подмножеств X. Тогда X и 2^X не равномощны.

Доказательство. Для конечных это верно, поскольку $\forall k \in \mathbb{N} \cup \{0\} 2^k > k$.

Теперь от противного — пусть $\exists \varphi : X \to 2^X$ и φ — биекция. Возьмём $Z = \{x \in X : x \notin \varphi(x)\}$. Z — какое-то подмножество X, а значит, т.к. φ — биекция, то $\exists z \in X : \varphi(z) = Z$. Посмотрим как расположено z относительно Z: если $z \in Z$, то $z \notin \varphi(z)$, т.е. $z \notin Z$, противоречие (т.к. все переходы двусторонние). $\square$

***Определение* 1.4.** Континуальное множество — множество, равномощное $[0, 1]$. (Ещё возможный вариант: континум — отрезок $[0, 1]$. Или $\mathbb{R}$. Какая разница, они всё равно равномощны).

Заметим, что мы всегда можем «увеличивать» множество: $\mathbb{N} \to 2^{\mathbb{N}} \to 2^{(2^{\mathbb{N}})} \to \cdots$. Как итог — нет «наибольшего» множества.

Теорема 1.6. Не существует множества всех множеств

Доказательство. От противного — пусть существует, обзовём его за X. Тогда рассмотрим 2^X. Тогда $2^X \in X$ (т.к. X это уже множество всех множеств), но $|X| < |2^X|$, противоречие. $\square$

Теорема 1.7. Дизъюнктное объединение двух континуальных множеств континуально

Доказательство. A_1, A_2 изоморфны множеству бесконечных битовых строк. Тогда их объединение будет тоже изоморфно множеству бесконечных битовых строк, поскольку можно просто для любого элемента, если он из A_1 взять его битовую запись и приписать в начало ноль, а если он из A_2, то приписать в начало единицу. Всё, получили все битовые строки и записи для всех элементов, значит объединение континуально. □

Теорема 1.8. Объединение счётного числа континуальных множеств континуально.

Доказательство. Пусть у нас есть набор множеств A_i. Знаем, что A_i изоморфен отрезку $[0,1]$. Тогда давайте просто расположим эти отрезки параллельно друг другу внутри квадрата $[0,1] \times [0,1]$. Мы так можем сделать поскольку можем взять какой-нибудь столбец для A_1, A_2 и т.д., иначе говоря, выбрать счётное подмножество из отрезка $[0,1]$. Всё, тогда имеем $[0,1] \quad A_0$, и $A_0 \subset A_0 \cup A_1 \cup A_2 \cup \dots \subset [0,1] \times [0,1] \quad [0,1]$. Тогда мощность объединения находится между мощностями $[0,1]$ и $[0,1] \times [0,1] \times [0,1]$. Но мощность правого равна мощности левого, а значит искомое объединение — континуально. □

Замечание. Мы не знаем, есть ли что-то больше счётного, но меньше континуального. (Если быть точным, то знаем, что в $ZF(C)$ нельзя доказать ни отсутствие там чего-либо, так и присутствие, но забейте).

1.3. Об операциях над мощностями

Если хотим сложить множества (мощности), то нам нужна мощность следующего множества

$$A \times \{0\} \cup B \times \{1\}$$

О корректности — если выбирать разные множества одной мощности, то можно построить биекцию и не париться.

Коммутативность очевидна, т.е. мощность суммы не изменится от перестановки A и B.

Произведение мощностей, ожидаемо, есть мощность множества $|A \times B|$

С возведением в степень чуть сложнее: пусть $|A| = a, |B| = b$, то $a^b = |A^B|$, где последнее — множество всех функций, действующих из B в A.

Хотим проверить, что $A^{B \sqcup C} = A^B \times A^C$. Имеем $g : B \to A, h : C \to A$, и функция $f : B \cup C \to A$ взаимооднозначно определяет g и h.

Теперь хотим проверить, что $(ab)^c = a^c \times b^c$. Слева имеем $\{f : C \to A \times B\}$, а справа $\{f : C \to A\} \times \{g : C \to B\}$. Но тогда заметим, что функций из первого множества есть две координаты в образе и можно рассмотреть проекции образов на A и на B как две функции, и всё хорошо.

Остаётся $(a^b)^c = a^{b \times c}$. По сути $a^{b \times c}$ это $\{f | f : B \times C \to A\}$. Что плюс-минус есть $f_c(x) = f(x, c)$ — как только мы фиксируем c, у нас c отображается в функцию f_c, которая в свою очередь есть функция $B \to A$, что и написано слева, ура.

Зачем же нам всё это? Ну допустим хотим узнать, чем разно ω^c (ω — мощность счётного множества, c — континуального). Т.е. это есть $f : \mathbb{R} \to \mathbb{N}$. Знаем, что $\omega^c \leqslant c^c = (2^\omega)^c = 2^{\omega \times c} \leqslant 2^{c \times c} = 2^c$, но, в свою очередь $\omega^c \geqslant 2^c$, т.е. искомое множество зажато между 2^c и 2^c

Ну или ещё пример — $c^\omega = (2^\omega)^\omega = 2^{\omega \times \omega} = 2^\omega = c$, но при этом $c^\omega \geqslant 2^\omega$, снова зажали.

2. Частично упорядоченные множества

2.1. Про отношения

***Определение* 2.1.** Пусть есть множество A, и на нём ввели отношение $R \subset A \times A$ (Напоминание — отношение есть подмножество $A \times A$).

R — отношение эквивалентности, если оно удовлетворяет следующим аксиомам:

1. $a \in A(a, a) \in R$ — рефлексивность
2. $a, b \in A, (a, b) \in R \to (b, a) \in R$ — симметричность
3. $a, b, c \in A, (a, b), (b, c) \in R \to (a, c) \in R$ — транзитивность

Это хорошо, но нам оно не нужно, какая досада.

***Определение* 2.2.** Отношение R' называется отношением порядка, если оно удовлетворяет следующим аксиомам:

1. $a \in A(a, a) \in R$ — рефлексивность
2. $a, b \in A, (a, b) \in R, (b, a) \in R \to a = b$ — антисимметричность
3. $a, b, c \in A, (a, b), (b, c) \in R \to (a, c) \in R$ — транзитивность

Обычно для него используют значок, например $\leqslant$. Можно рисовать более закорючно, но мне влом.

***Определение* 2.3.** Частично Упорядоченное Множество — ЧУМ — пара $(X, \leqslant)$ — множество, и отношение порядка на нём.

Теперь про частично упорядоченное множество. Возьмём $(X, \leqslant)$, всё, получили ЧУМ. Простейшие примеры — натуральные, рациональные, действительные числа и операция меньше-или-равно. Можно взять тривиальное отношение — в нём находятся только пары вида $(a, a), a \in X$, т.е. $a \leqslant'' b : a = b$. Ещё отношение порядка — рассмотрим 2^X, с отношением «являться подмножеством». Аксиомы, очевидно, выполняются.

Рассмотрим функции $f : \mathbb{R} \to \mathbb{R}$ и введём отношение порядка $f \leqslant g \Leftrightarrow \forall x \in \mathbb{R} f(x) \leqslant g(x)$. Тут уже явно видно, что бывают несравнимые элементы. Тут, например, это пары функций, у которых на первой половине первая больше второй, а на второй половине — вторая больше первой.

Можно строить по $\leqslant$ и отношение строгого порядка $<$ — $x < y \Leftrightarrow x \leqslant y, x \neq y$. Его аксиомы:

1. $a \in A(a, a) \notin R$ — антирефлексивность
2. $a, b, c \in A, (a, b), (b, c) \in R \to (a, c) \in R$ — транзитивность

А теперь давайте размножать ЧУМы.

Пусть X, Y — ЧУМы. Тогда можно строить:

1. $X \sqcup Y$ — внутри одной доли используется старое отношение, а элементы из разных долей просто несравнимы

2. $X + Y$ — считаем, что любой элемент $X \leqslant$ любого элемента Y. Пример — возьмём натуральные числа и ещё раз натуральные числа. Тогда $5 < 6 < \dots < 1' < 2'$, например.

3. $X \times Y$. Есть два варианта — покоординатно — $(x_1, y_1) \leqslant (x_2, y_2) \Leftrightarrow x_1 \leqslant x_2$ И $y_1 \leqslant y_2$. Второй вариант — лексикографически — $(x_1, y_1) \leqslant (x_2, y_2) \Leftrightarrow (x_1 < x_2)$ ИЛИ $((x_1 = x_2)$ И $(y_1 \leqslant y_2))$

***Определение* 2.4.** ЧУМ — линейный, если $\forall$ два элемента сравнимы.

***Определение* 2.5.** Максимальный элемент — тот, больше которого нет. Наибольший элемент — который больше либо равен всех остальных.

Рассмотрим все подмножества трёхэлементного множества $\{a, b, c\}$. Можно нарисовать картинку, как они расположены, но я пока не гений картинок. В общем, если x наибольший, то он максимальный. В обратную сторону далеко не всегда верно, т.к. иногда можно быть несравнимым с кем-нибудь.

***Определение* 2.6.** X, Y — ЧУМы, $\varphi : X \to Y$ — изоморфизм ЧУМов, тогда и только тогда, когда φ — биекция, и $a \leqslant b \Leftrightarrow \varphi(a) \leqslant \varphi(b)$

Пусть ещё пример — $k \leqslant n$ — k делителеь n. И тут мы вспомним, что можно сужать порядок — резать его множество. Давайте сузим наш порядок на множество $\{1, 2, 3, 6\}$ — порядок делимости.

А ещё давайте рассмотрим $2^{<a,b>}$ — $\{\varnothing, \{a\}, \{b\}, \{a, b\}\}$. Можно показать, что оно изоморфно предыдущему множеству. Пример изоморфных есть, какие примеры не изоморфны?

Изоморфно ли $\mathbb{N}, \leqslant$ и $\mathbb{R}, \leqslant$? Нет, т.к. биекции точно нет, т.к. по мощностям не сходятся множества. Изоморфно ли $\mathbb{N}, \leqslant$ и $\mathbb{Z}, \leqslant$? Нет, т.к. во втором множестве нет наименьшего элемента, а в первом — есть, а наименьший должен переходить в наименьший (выводится довольно понятно, как)

Изоморфно ли $\mathbb{Z}, \leqslant$ и $\mathbb{Q}, \leqslant$? Нет, т.к. давайте возьмём 0 и 1 из $\mathbb{Z}$ и отобразим их куда-либо, получили $\varphi(0), \varphi(1)$. Между ними где-то есть $\frac{\varphi(0)+\varphi(1)}{2}$. Подействуем на него φ^{-1}, получим, что прообраз должен жить в $\mathbb{Z}$ между 0 и 1. Но там никого нет! Значит наше предположение о существовании биекции неверно.

Рассмотрим $(\mathbb{Z}, \leqslant)$ и $(\mathbb{Z} + \mathbb{Z}, \leqslant)$ Рассмотрим 0 и $0'$ во втором, между ними находится бесконечное число элементов. Но рассмотрев прообразы, это какие-то два целых, между ними вся бесконечность должна будет поместиться, но нет, т.к. между двумя целыми конечное число элементов.

***Определение* 2.7.** x, y — соседние, если $x \leqslant y$ и между x и y нет элементов и порядок линейный.

***Определение* 2.8.** Линейный порядок называется плотным, если $\forall x, y, x < y \to \exists z : x < z < y$

Теорема 2.1. Пусть X, Y — ЧУМы. Тогда если они конечные, с линейными порядками, то они изоморфны тогда и только тогда, когда $|X| = |Y|$.

Доказательство. Будем брать наименьшие элементы и попарно отображать их друг в друга и удалять. Отношение относительно минимальных и прочих сохраняется, а на меньшем можем построить дальше по индукции. А если размеры не равны, то мы умерли ещё на этапе биекции. $\square$

Замечание. Важна конечность! Для просто равномощных бесконечных мы уже видели контрпримеры.

Теорема 2.2. Пусть X, Y — счётные ЧУМы, имеют плотный и линейный порядок, и в X и Y нет наибольшего и наименьшего элементов, тогда X изоморфно Y. (такие ЧУМы существуют, например $(\mathbb{Q}, \leqslant)$)

Доказательство. Выпишем подряд $X - - - \{x_i\}$, $Y - - - \{y_i\}$. Отобразим x_1 в y_1. А дальше есть x_2, хотим отобразить куда-то. Отобразим x_2 в такой элемент, который относительно y_1 расположен так же, как x_2 расположен относительно y_1. Такой найдётся, т.к. нет минимума и максимума. После этого аналогично поступим с y_2 (второй в выписанном списке игреков, если он ещё не взят). Затем так же поступим с x_3, но теперь уже смотрим на отношения x_3 с x_1, x_2. Это получится, т.к. нет минимума, максимума и ещё мы плотны. Затем на y_3 и т.д.

Так мы задействуем все элементы из X и Y, и при этом ничего не сломаем из ограничений на отношение порядка, а значит получим изоморфизм ЧУМов, ура. $\square$

3. Высказывания

3.1. Высказывания

Начало пропущено, но оно простое.

Высказывание — утверждение, которое может быть ложным или истинным.

Несложно получить, что из ложного утверждения следует всё, что угодно.

***Определение* 3.1.** Пропозициональная переменная — произвольная переменная, обозначаем x, y, z, могут принимать значения 0 или 1

***Определение* 3.2.** Формула:

1. Пропозициональная переменная является формулой
2. Если A — формула, то $\neg A$ — тоже формула (отрицание)
3. Если есть формулы A, B, то $(A \wedge B), (A \vee B), (A \to B)$ — тоже формулы

Минимальный класс строк, удовлетворяющий $*$ (предыдущей тройке утверждений), называется множеством формул.

Теперь хотим давать значения формулам. Для переменной значение формулы есть просто значение переменной. Отрицание работает как отрицание, логические операции работают согласно таблице истинности (которая очевидна)

Для отсутствия проблем с порядком вычисления у нас есть скобки.

Теорема 3.1. Любая формула допускает единственный разбор.

Доказательство. Когда у нас есть формула, мы однозначно попадаем в один из трёх вариантов. Формально говоря — посмотрим первый символ. Если это переменная, то мы завершаемся, если отрицание — отрицаем и убираем отрицание, если открывающая скобка — то в общем там можно найти операцию, в которой скобочный баланс равен единице и порвать по этой операции и уйти рекурсивно с двумя меньшими строками. □

***Определение* 3.3.** Тавтология — формула, истинная при любых значениях переменных. Например $x \vee \neg x$, или $(p \to q) \vee (q \to p)$

***Определение* 3.4.** Две формулы F_1, F_2 эквивалентны, если F_1 истинно тогда и только тогда, когда F_2 истинно.

На самом деле F_1, F_2 эквивалентны тогда и только тогда, когда $(F_1 \to F_2) \wedge (F_2 \to F_1)$ является тавтологией

***Определение* 3.5.** $A \leftrightarrow B = (A \to B) \wedge (B \to A)$

Теорема 3.2. Следующие формулы являются тавтологиями:

- $(p \wedge q) \leftrightarrow (q \wedge p)$
- $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$

- $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
- $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
- $p \vee (p \wedge q) \leftrightarrow p$
- $p \wedge (p \vee q) \leftrightarrow p$
- $(p \to q) \leftrightarrow (\neg q \to \neg p)$
- $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
- $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

Теорема 3.3. Пускай есть $f : B^n \to B$ (из битовых строк длины n в истину/ложь). Утверждение — любая такая f представляется используя $\wedge, \vee$ и $\neg$, и, мало того, представляется в виде ДНФ: дизъюнктивно-нормальная формула.

***Определение* 3.6.** Конъюнкт — $(x_{i1} \wedge x_{i2} \wedge \neg x_{i3} \wedge \cdots \wedge x_{ik})$ — набор переменных (возможно, с отрицаниями), объединённых логическими И.

***Определение* 3.7.** ДНФ — дизъюнкция конъюнктов — набор конъюнктов, объединённых логическим ИЛИ.

Доказательство. Докажем предыдущую теорему.

Рассмотрим все наборы переменных и значения f на них (рассмотрим таблицу истинности f). Выберем строки, в которых $f = 1$, тогда возьмём переменные оттуда и составим из них конъюнкт — каждую переменную, если она со значением 0, то возьмём в конъюнкт её отрицание, а если со значение 1 — возьмём саму переменную. Тогда полученный конъюнкт будет верен только и только на этом наборе переменных.

Взяв все такие конъюнкты, на наборах переменных которых f истинна, и объединив их через логическое ИЛИ, получим как раз ДНФ, истинную только на тех наборах переменных, на которых была истинна f. $\square$

Пример. Если кто хочет — можете нарисовать тут таблицу истинности для формулы от трёх переменных и построить по ней описанным алгоритмом ДНФ.

***Определение* 3.8.** КНФ — конъюнкция дизъюнктов — набор дизъюнктов (объединений переменных (возможно, с отрицаниями) через $\vee$), объединённых через логическое И (выполняться должны все скобки).

Теорема 3.4. Для любой формулы можно построить КНФ. Строится аналогично, но выбираем строки с нулём.

КНФ/ДНФ не единственны, и построенные нами не обязательно минимальны.

Можно ли используя другие связки тоже выразить всё?

Давайте выразим всё через $1, \oplus, \wedge$.

***Определение* 3.9.** Одночлен Жегалкина — $1, x, x \wedge y, x \wedge y \wedge w$, т.е. без $\oplus$

***Определение* 3.10.** Многочлен Жегалкина: набор одночленов Жегалкина, объединённых $\oplus$

Теорема 3.5. Любая функция $f : B^n \to B$ допускает ровно одно представление в виде полинома Жегалкина.

Существование представления. Мы знаем, что используя $\neg, \vee, \wedge$ можно записать все формулы. А сами эти операции можно выразить следующим образом: $\neg x = x \oplus 1; x \vee y = xy \oplus x \oplus y; x \wedge y = x \wedge y$. А значит для любой формулы можно просто записать её в ДНФ/КНФ, а затем выразить операции через $1, \oplus, \wedge$. После этого всё пораскрывать и порадоваться полученному многочлену Жегалкина. □

Пример. Если сильно нужен — напишите, добавлю. Можете и сами добавить...

Единственность представления. Любой многочлен можно свести к многочлену Жегалкина: $x^2y \oplus xy \oplus xy = xy \oplus xy \oplus xy = xy$. Единственность — при использовании каждого одночлена не более раза. У нас бывает 2^n одночленов (переменная или входит или не входит). Многочлен это набор одночленов, тогда многочленов 2^{2^n}, но и всех функций 2^{2^n}, и при этом каждой функции соответствует хотя-бы один многочлен, а тогда, т.к. функций столько же, сколько и многочленов, каждой функции соответствует ровно один многочлен. □

Пусть у нас есть например произвольная тернарная функция $f(x, y, z)$ и $\wedge$. Можем ли мы представить любую функцию таким интересным набором? Хотим иметь критерий на этот счёт.

***Определение* 3.11.** Введём пять классов функций:

Сохраняющие ноль функции — функция от всех нулей выдаёт ноль. Пример — тождественный ноль, логическое или.

Сохраняющие единицу функции — функция от всех единиц выдаёт единицу. Пример — тождественная единица, логическое или.

Отрицание не является ни сохраняющей единицу, ни сохраняющей ноль.

Монотонные функции — от увеличения (замены нуля на единицу) любого из параметров значение функции не уменьшается.

Линейные функции — те, для которых многочлен Жегалкина состоит только из $\oplus$ переменных и единиц, иначе говоря, в многочлене Жегалкина которых нет слагаемых степени больше единицы.

Самодвойственные — отрицание всех переменных влечёт отрицание значения функции.

Пример. $\wedge$ — сохраняющая ноль, сохраняющая единицу, монотонная, не самодвойственная функция.

Тождественная функция является самодвойственной.

Теорема 3.6 (Теорема Поста)**.** Набор функций является полным (можно представить любую функцию) тогда и только тогда, когда для любого класса из пяти названных существует f_i, не лежащее в этом классе.

Если есть класс, в котором лежат все, то набор не полон. Если нет класса, в котором не лежит хотя-бы одна функция, то мы проиграли, т.к. не сможем выразить какую-либо функцию не из этого класса.

Например, любая комбинация сохраняющих ноль/единицу функций тоже является сохраняющей ноль/единицу функцией, и тогда отрицание мы не выразим.

Аналогично с монотонностью — комбинация монотонных функций монотонна. Изменили увеличили какие-то переменные, функции, в которых они были могли только увеличиться, те функции, в которых эти функции как аргументы тоже могли только увеличиться и так далее... В общем, отрицание снова не получим.

Самодвойственность аналогичным образом проходит внутрь, к аргументам функций, которые если тоже функции, то отрицание тоже пройдёт внутрь и так далее, пока не проотрицаем все аргументы, что и есть самодвойственность.

И с линейностью так же будет, что, в целом очев. Рассмотрим как полиномы Жегалкина, у нас просто нигде не будет $\wedge$, а значит и сам $\wedge$ мы ниоткуда получить не сможем. Ну или не так, хз. $\square$

Если для любого класса есть функция вне него, то набор полон. Заметим, что мы из любой функции умеем получать функцию от одного аргумента: $f'(x) = f(x, x, \cdots, x)$

Функций от одного аргумента четыре штуки — тождественные ноль, единица, идентичная (x) и отрицание $(\neg x)$. Запомним это.

Среди исходных функций есть f_i — функция не сохраняющая ноль. Тогда возьмём соответствующую функцию от одного аргумента: $g(x) = f_i(x, x, \cdots, x)$, которая тоже не сохраняет ноль. Тогда g это или тождественная единица, или отрицание.

Среди исходных функций есть f_j — функция не сохраняющая единицу. По аналогии с предыдущей строкой, получим $h(x)$, которая или тождественный ноль, или отрицание.

Т.е. если возьмём функции не сохраняющие ноль и единицу, то или у нас есть сразу константы 0 и 1, или есть отрицание икса. А теперь хотим получить, что на самом деле есть оба из них. Хотим из одного получать второе, а из второго — первое.

Пусть есть немонотонная функция f_k и константы 0 и 1. Функция немонотонная, значит существует набор переменных a_i, одна из которых — ноль, и на этом наборе функция возвращает 1, а при замене нуля на единицу — возвращает ноль.

Тогда возьмём функцию $g'(x)$, в которой все переменные a_i поставим как константы, а на место нуля/единицы подставим x. Так получили отрицание, если есть 1 и 0.

Теперь хотим из отрицания получить константы. У нас есть несамодвойственная функция f_q, тогда $\exists\{a_i\}$, что $f_q(a_1, a_2, \cdots, a_m) = f_q(\neg a_1, \neg a_2, \cdots, \neg a_m)$. Тогда давайте построим функцию $g''(x)$ как $f_q(x, \neg x, x, \cdots)$, где на позиции i, где $a_i = 1$ стоит x, а на противоположных — $\neg x$. Тогда мы получили функцию, которая что при x, что при $\neg x$ выдаёт одно и то же, т.е. константа. А из одной константы и отрицания можем получить вторую константу.

Теперь к нелинейности. Функция нелинейна если её полином Жегалкина нелинеен. Пусть $f_e(x_1, \cdots, x_m) = x_1 x_2 A(x_3, \cdots, x_m) \oplus x_1 B(x_3, \cdots, x_m) \oplus x_2 C(x_3, \cdots, x_m) \oplus D(x_3, \cdots, x_m)$, где A, B, C, D — произвольные многочлены Жегалкина, может и константы, но A — не тождественный ноль. Тогда можно пообрать такие $x_3, \cdots, x_m$, что $A(\cdots)$ равно единице.

Тогда рассмотрим $f_e(x_1, x_2, a_3, \cdots, a_m) = \cdots$, есть восемь вариантов:

1. $x_1 x_2 \oplus x_1 \oplus x_2 \oplus d$
2. $x_1 x_2 \oplus x_1 \oplus d$
3. $x_1 x_2 \oplus x_2 \oplus d$
4. $x_1 x_2 \oplus d$

Где d — какая-то константа (0 или 1). Но отрицанием можно убрать $\oplus d$. Теперь, если мы получили последнее, то мы получили $\wedge$ — победа. Есть первое, то это $\vee$, что тоже победа. Второе есть $x_1 \wedge \neg x_2$. Но отрицание мы умеем убирать, и так мы снова получим $\wedge$. А третье это буквально второе, с точностью до перестановки переменных. Т.е. мы умеем получать $\wedge$ или $\vee$, а из одного на самом деле умеем получать и второе.

Так мы в итоге получили $0, 1, \neg, \vee, \wedge$, а значит умеем строить любой КНФ/ДНФ, а значит наш набор связок полон. Ура! $\square$

Рассмотрим $f(x_1, x_2, x_3) = ((x_1 \wedge x_2) \oplus (x_3 \vee x_1)) \uparrow (x_1 \wedge x_2)$, где $\uparrow$ — стрелка Пирса. Тогда можно составить схему, которая пока что будет деревом — граф выполнения, где вершины это операции или исходные переменные, а рёбра ведут в переменные или результаты других операций, которые используются в нашей.

А теперь сделаем не дерево, а просто ориентированный ациклический граф, где уберём все дублирования.

***Определение* 3.12.** Схема — ациклический граф, где из листьев — значений входных параметров булевой схемы и вершин — самих булевых операций, вычисляется значение всей булевой функции и подаётся на выход, в корень дерева.

Хотим жить в базисе $\wedge, \vee, \neg$ (у нас будут только такие операции в схеме). Размер схемы — количество внутренних узлов.

***Определение* 3.13.** Схемная сложность функции — размер схемы минимального размера. Да, она зависит от базиса, но сейчас докажем, что:

Теорема 3.7. Схемная сложность в различных базисах отличается не более чем в константу раз.

Доказательство. Пусть есть два базиса (полных набора) — C_1 и C_2. Раз наборы полны, то любая функция из одного набора представима используя функции другого набора. Не умаляя общности возьмём $f \in C_1$ такую, что её представление имеет максимальный размер (количество использованных формул из C_2) C. Тогда любую формулу из C_1 можно выразить не более чем C формулами из C_2, а значит, для любой схемы, построенной в базисе C_1, если заменить каждую блок из C_1 на его представление в C_2, то размер схемы увеличится не более чем в C раз, что и требовалось доказать. $\square$

Теорема 3.8. Пусть $f : B^n \to B$. Тогда

1. $size(f) \leqslant \mathcal{O}(c^n) \forall c > 2$
2. $\forall c < 2 \exists f : size(f) < c^n$

Доказательство. Для первого пункта — построим КНФ, в нём, даже в другом базисе, строим схему размера $n \cdot 2^n$, что меньше, чем любое $(2 + \varepsilon)^n$ начиная с некоторого n.

Для второго пункта пойдём следующим путём:

Заметим, что функций от двух переменных у нас $2^{2^2} = 16$

Пусть у нас n переменных, и N — размер схемы. Несложно понять, что $n \leqslant N$.

Возьмём схему, проведём её топологическую сортировку, чтобы в начале шли сами переменные, а потом — внутренние блоки схемы, где каждый использует только результаты предыдущих. Тогда различных схем размера N не больше $(16(n + N)^2)^N \leqslant (64N^2)^N = (8N)^{2N} = 2^{2N \cdot \log 8N}$. Тепрь пусть $N = c^n$. Тогда получаем $2^{(\log 8c^n) 2c^n} \leqslant 2^{c^n \cdot n \cdot const}$. Заменим левое на нечто большее — $2^{(\log 8^n c^n) 2c^n} \leqslant 2^{c^n \cdot n \cdot \log 8c \cdot 2} < c \cdot 2^{2^n}$.

Так мы каким то образом получили, что есть схемы, вычислимые за $(2+\varepsilon)^n$ но не вычислимые схемой размера $(2 - \varepsilon)^n$. $\square$

А вообще люди не умеют приводить пример функций, которые нельзя вычислить быстрее, чем за $4n$. Парадоксально.

А теперь давайте придумывать схемы. Хотим сложить два числа $x_1x_2\cdots x_n$ и $y_1y_2\cdots y_n$ и получить $z_0z_1\cdots z_n$, если у нас есть $\wedge, \vee, \neg, \oplus, 0, 1$. Понятно, что $z_n = x_n \oplus y_n$. Пусть перенос — c_i. Тогда $c_{n-1} = x_n \wedge y_n$. Тогда $z_{n-1} = x_{n-1} \oplus y_{n-1} \oplus c_{n-1}$. Если кто хочет нарисовать саму схему — будем очень рады. $c_{n-2} = MAJ(x_{n-1}, y_{n-1}, c_{n-1})$, т.е. когда из аргументов есть хотя-бы две единицы. По сути, это $(x_{n-1} \wedge y_{n-1}) \vee (x_{n-1} \wedge c_{n-1}) \vee (y_{n-1} \wedge c_{n-1})$. Но какого размера будет схема? $\mathcal{O}(n)$.

***Определение* 3.14.** Глубина схемы — длина самого длинного пути от входа до выхода. По сути, насколько быстро будут проходить вычисления.

Проблема нашей схемы — её глубина $\mathcal{O}(n)$.

Теорема 3.9. Для сложения n-битных чисел существует схема размера $\mathcal{O}(n)$ и глубины $\mathcal{O}(\log n)$

Для доказательства этой теоремы нам потребуется ещё одна вещь.

Пусть у нас есть два n битных числа $\{x_i\}, \{y_i\}$, хотим понять, какое из них больше. Пусть у нас будут два гейта (внутренние вершины) z_0, z_1 и если выход — два нуля, то $x < y$, если ноль один, то $x = y$, если один один, то $x > y$. Последний вариант игнорируем/ошибка/считаем равенством.

Сделаем схему сравнения рекурсивной. Если искомые два числа состоят из одной цифры, то просто как-нибудь очевидно сравним их и вернём результат. Иначе давайте разобьём числа пополам: $x = x_1x_2$, $y = y_1y_2$, и сравним числа x_1 с y_1 и x_2 с y_2. А дальше нам нужно по четырём битам результата вернуть два бита. Но это мы тоже умеем делать за какую-то константу. Несложно понять, что глубина такой схемы будет логарифм, а размер — $\mathcal{O}(n)$.

Доказательство. Так как же всё-таки составить схему сложения n-битных чисел?

Давайте сначала насчитаем все биты переноса — c_i-ое. Бит переноса c_i равен единице, если число $x_ix_{i+1}\cdots x_n$ больше, чем $1-y_i1-y_{i+1}\cdots 1-y_n$. Утверждается, что можно запустить сравнение один раз и полученными результатами пользоваться, чтобы получить все биты переноса. Всё это за глубину логарифм и сложность $\mathcal{O}(n)$. А получив уже биты переноса можно $\oplus$-ом получить i-ый бит результата (самый старший бит есть просто бит переноса). Ура!

□

Теорема 3.10. Пусть есть $x_1x_2\cdots x_n$ и хотим получить сумму этих n бит и записать их в виде числа $y_1y_2\cdots y_{\log n}$. Это можно сделать схемой размера $\mathcal{O}(n)$ и глубины $\mathcal{O}(\log n \log\log n)$

Пруфов не было и, видимо, не будет. Сорян!

4. Исчисление высказываний

Просто аксиом и утверждений, которые считаются верными недостаточно — мы ничего нового получить не сможем.

***Определение* 4.1.** Правила вывода — как из утверждений получить новые.

Пусть есть последовательность утверждений: $C_1, C_2, C_3, \cdots$. Для каждого C_i есть три варианта — быть аксиомой, быть утверждением, в истинность которого мы верим («дано»), или получено при помощи правил вывода, применённых к $C_1, C_2, \cdots, C_{i-1}$.

Зачем же нам это нужно? Потому что естественный язык может приводить к заблуждениям.

Пример. Cheesburger is better than nothing. Nothing is bettter than eternal happiness. Тогда по транзитивности Cheesburger is better than eternal happiness.

Пример.

1. В этой рамочке содержится как минимум одно неверное утверждение. (Представьте, что вокруг этого и следующего утверждений находится рамочка)
2. Среди нас нет долларовых миллиардеров

Если первое утверждение верно, то неверно второе, т.е. миллиардеры есть, если первое неверно, то в рамочке все верные, но противоречие, т.к. первое — неверное, противоречие.

Эти наглядные примеры показывают необходимость математического языка высказываний, иначе будем попадать в подобные ситуации.

Мы будем рассматривать

4.1. Логика высказываний

Или пропозиционная логика. В ней используются операции $\wedge, \vee, \to, \neg$ и операции над множествами.

Нас интересуют тавтологии — формулы, истинные при любых значениях высказываний.

Какие есть варианты? Можно все тавтологии засунуть в аксиомы и радоваться жизни и ничего больше не делать. Но мы этого не хотим, мы хотим выводить тавтологии из множества аксиом.

У нас будет множество аксиом и единственное правило вывода.

Далее будем считать истинными утверждениями — тавтологии.

Можно говорить про полноту и корректность логики.

***Определение* 4.2.** Корректность — все выводимые утверждения являются тавтологиями (ничего лишнего не выведем)

Полнота — имея аксиомы и правила вывода нужно иметь возможность выводить все верные утверждения (ничего не потеряем)

***Определение* 4.3.** Одиннадцать аксиом исчисления высказываний

1. $A \to (B \to A)$ — Из чего угодно следует истина
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ — Дистрибутивность
3. $A \to (A \vee B)$

4. $B \to (A \lor B)$
5. $(A \to C) \to ((B \to C) \to ((A \lor B) \to C))$
6. $(A \land B) \to A$
7. $(A \land B) \to B$
8. $A \to (B \to (A \land B))$
9. $\neg A \to (A \to B)$ — Из лжи следует что угодно
10. $(A \to B) \to ((A \to \neg B) \to \neg A)$ — Доказательство от противного
11. $A \lor \neg A$ — Аксиома исключённого третьего

***Определение* 4.4.** modus ponens — единственное правило вывода: $\frac{A, A \to B}{B}$

Пример. Можем вывести формулу: $(A \lor B) \to (B \lor A)$

$C_1 = A \to (B \lor A)$, аксиома 4. $C_2 = B \to (B \lor A)$, какая-то другая аксиома с переименованием переменных. Далее в пятую аксиому подставим вместо A — A, вместо B — $(B \lor A)$, вместо C — B, получим $(A \to (B \lor A)) \to ((B \to (B \lor A)) \to ((A \lor B) \to (B \lor A)))$, тогда первая часть это A', а вторая — B'. Но тогда заметим, что левая часть это аксиома, и $A' \to B'$, а значит по правилу вывода получим B'. Он, в свою очередь, тоже распадается на два утверждения, из которых первое актиома, и следствие верно (доказали ранее), а значит по правилу вывода последняя скобка $(A \lor B) \to (B \lor A)$ верна, что и хотели доказать.

Теорема 4.1. Исчисление высказываний корректно

Доказательство.
1. Все аксиомы — тавтологии
2. Пусть $C_1, C_2, \cdots, C_k$ — тавтологии, тогда C_{k+1} — тавтология: или C_{k+1} — аксиома, тогда она тавтология, или получена применением modus ponens к $C_1, \cdots, C_k$. У нас есть C_i — тавтология, и у нас есть $C_i \to C_{k+1}$ — тавтология. Хотим сказать, что тогда C_{k+1} — тавтология. Пусть это не так, тогда есть значения, на которых C_{k+1} равно нулю, но тогда при подстановке таких значений в $C_i \to C_{k+1}$ мы получим, что из истины следует ложь.

□

Лемма. Формула $A \to A$ выводима.

Доказательство. Запишем первую аксиому с подстановкой $A = A, B = (A \to A)$, обозначим за C_1. $C_2 = A \to (A \to A)$, тоже первая аксиома, но с подстановкой $A = A, B = A$. За C_3 возьмём вторую аксиому, с подстановкой $A = A, B = (A \to A), C = A$.

Последнее будет выглядеть как $(A \to ((A \to A) \to A)) \to (A \to (A \to A)) \to ((A \to A))$, первое как $A \to ((A \to A) \to A)$. Применим modus ponens к C_1, C_3, получим $C_4 = (A \to (A \to A)) \to (A \to A)$. Применим modus ponens к C_2, C_4. Получим $C_5 = A \to A$. □

***Определение* 4.5.** Если формулу можно вывести, то будем обозначать $\vdash$

***Определение* 4.6.** $\Gamma \vdash F$, где $F = C_n$, и есть $C_1, C_2, \cdots, C_{n-1}$, где C_i это или аксиома, или формула из Γ, или можно вывести через modus ponens.

Лемма. Лемма о дедукции:

$\Gamma \vdash A \to B \Leftrightarrow \Gamma, A \vdash B$

Доказательство. $\Rightarrow$: $\Gamma, A : \cdots, A \to B, A$, и теперь применим modus ponens к последним и получим B, т.е. $\Gamma, A \vdash B$

$\Leftarrow$: $\Gamma, A \vdash B \Rightarrow \Gamma \vdash A \to B$

Пусть $C_1, C_2, \cdots, C_k = B$. Допишем везде A, получим последовательность $A \to C_1, A \to C_2, \cdots, A \to B$. Хотим показать, что это корректный вывод. Будем делать по индукции, почему можно написать $A \to C + i$: Если $C_i = A$, то получили $A \to A$, что мы уже умеем выводить, если C_i — аксиома, то допишем C_i т.к. это аксиома, а затем допишем $C_i \to (A \to C_i)$, что аксиома, затем применим modus ponens и получим как раз $(A \to C_i)$, если $C_i \in \Gamma$, то то же самое, что и предыдущий пункт, но теперь C_i имеем право писать, т.к. оно из Γ. True если $C_i = MP(C_k, C_j), k, j < i$, и $C_j = C_k \to C_i$. Всё остальное до этого мы уже конвертировали в $A \to C_k, A \to C_j$ и хотим вывести $A \to C_i$. Trueтого есть $A \to C_k, A \to (C_k \to C_i)$, напишем вторую аксиому с подстановкой $A = A, B = C_k, C = C_i$, т.е. $(A \to (C_k \to C_i)) \to ((A \to C_k) \to (A \to C_i))$. Тогда по modus ponens $(A \to C_k) \to (A \to C_i)$, а левая часть уже есть, так что итог — $A \to C_i$.

Ура, мы доказали лемму о дедукции. $\square$

Теперь посмотрим на правило $A \to B \to (A \wedge B)$. По сути это $\varnothing \vdash A \to B \to (A \wedge B)$ что $\Leftrightarrow A \vdash B \to (A \wedge B) \Leftrightarrow A, B \vdash A \wedge B$.

Но зачем же всё это нужно?

Представим, что мы знаем всю теорию групп. В ней три аксиомы: $(ab)c = a(bc), \exists e : ea = ae; \forall a \exists a^{-1} : aa^{-1} = a^{-1}a = e$. Т.е. для доказательства любого факта про группы достаточно знать эти три.

Хотелось бы в математике тоже сформулировать какое-то число аксиом, и чтобы из них всё следовало. Ну вот примерно в этом направлении мы и двигаемся (но вообще это не очень возможно).

А вообще мы это изучаем чтобы дальше ориентироваться в более сложных вещей. Пример из аксиом вещественных чисел: $\forall x > 0 \exists y, z : x = y^2 + z^2$. Тут перебрать уже все значения переменных, в отличии от перебора значений булевых переменных, не получится.

А теперь к булевой логике.

4.2. И ещё правила вывода

Из одиннадцати аксиом и modus ponens можно получить ещё правила вывода, упрощающие жизнь (и домашку):

1. $\Gamma A, B, A \to (B \to (A \wedge B)), B \to (A \wedge B), A \wedge B$, так получили, что $\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$
2. $\Gamma, A \wedge B \vdash (A \wedge B) \to A, A \wedge B, A, (A \wedge B) \to B, B, \cdots, C$, так получили, что $\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$
3. $\Gamma, A, B \vdash A \to (B \to (A \wedge B)), A \wedge B$, так получили, что $\frac{\Gamma, A \wedge B \vdash C}{\Gamma, A, B \vdash C}$
4. $\Gamma \vdash A, A \to B, B$, так получили $\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}$. Ну и обобщение есть, когда у нас больше переменных выводится из Γ
5. $\Gamma \vdash A \to B, A \vdash \neg B, (A \to B) \to ((A \to \neg B) \to \neg A)$, Дважды modus ponens: $\neg A$, так получили $\frac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$
6. $\neg A \to (A \to B), \neg A, A, A \to B, B$, Так получили $\Gamma, A, \neg A \vdash B$
7. $\Gamma, A \vee B \vdash A \to C, B \to C, (A \to C) \to ((B \to C) \to ((A \vee B) \to C)), A \vee B \to C, C$, Так получили $\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$

8. Подставим в 7 A и $\neg A$, получим $\frac{\Gamma, A \vdash C \quad ,|Gamma, \neg A \vdash C}{} Gamma, A \vee \neg A \vdash C$, а аксиому можно из итогов выкинуть и получить $\frac{\Gamma, A \vdash C \quad \Gamma, \neg A \vdash C}{\Gamma \vdash C}$

4.3. И обратно к утверждениям

Утверждение 4.2. $\vdash \neg\neg A \to A$

Доказательство. $\neg\neg A \vdash A$

$A \vee \neg A, \neg\neg A \vdash A$

Подставим A и $\neg A$ к $\neg\neg A$, получим

$A, \neg\neg A \vdash A$ поскольку оно есть среди посылок, $\neg A, \neg\neg A \vdash A$ по правилу вывода из противоречия (шестое). А теперь по седьмому объединили полученные два утверждения. □

Лемма. $A, B \vdash A \wedge B, A \vee B, A \to B$

$A, \neg B \vdash \neg A \wedge B, A \vee B, \neg(A \to B)$

$\neg A, B \vdash \neg(A \wedge B), A \vee B, A \to B$

$\neg A, \neg B \vdash \neg(A \wedge B), \neg(A \vee B), A \to B$

$\neg A \vdash \neg A$

$A \vdash \neg(\neg A)$

В доказательство предыдущего: $A, \neg A \vdash A; A, \neg A \vdash \neg A$

Двенадцать первых утверждений доказываются или через modus ponens, или через правило вывода номер пять (которым можно отрицания получать, выводя противоречие). Конкретные доказательства, увы, упущены.

А вообще её можно было несколько иначе сформулировать: давайте писать $A^x = \begin{cases} A, x = 1 \\ \neg A, x = 0 \end{cases}$

Лемма. $\varphi(A_1, A_2, \cdots, A_k)$ — формула, $f(x_1, x_2, \cdots, x_k)$ — функция, вычисляющая эту формулу

$A_1^{x_1}, A_2^{x_2}, \cdots, A_k^{x_k} \vdash \varphi(A_1, \cdots, A_k)^{f(x_1, \cdots x_k)}$

Пример:

Тогда, подставив туда $\vee$ и единицы получим $A_1^1, A_2^1 \vdash (A_1 \vee A_2)^{1 \vee 1} = a_1 \vee A_2$. Аналогично можно подставлять нули и единицы в произвольных комбинациях с соответсвующими изменениями результата.

Доказательство. Доказывать будем по индукции по сложности построения формулы φ. База: если $\varphi(A_1, \cdots, A_k) = A_i$, то $A_1^{x_1}, \cdots, A_k^{x_k} \vdash A_i^{x_i}$

Переход: $\varphi = \varphi_1(op)\varphi_2$, где φ соответствует f, φ_1 соответствует g, φ_2 соответствует h, а (op) соответствует $\wedge, \vee, \to, \cdots$. Тогда $f(x_1, \cdots, x_k) = g(x_1, \cdots, x_k)(op)h(x_1, \cdots, x_k)$. Знаем (по ИП), что $A_1^{x_1}, \cdots, A_k^{x_k} \vdash \varphi_1(A_1, \cdots, A_k)^{g(x_1, \cdots x_k)}, \varphi_2(A_1, \cdots, A_k)^{h(x_1, \cdots, x_k)}$.

Ну и дальше тут происходило что-тоо особо странное, если честно. Кто помнит и понял — допишите этот момент, пожалуйста. □

Теорема 4.3. Любая тавтология выводима

Доказательство. Возьмём произвольную тавтологию φ. Пускай он зависит от $A_1, A_2, \cdots, A_k$. Умеем выводить $A_1, A_2, \cdots, A_k \vdash \varphi(A_1, \cdots, A_k)^{\varphi(1, \cdots, 1)}; \neg A_1, A_2, \cdots, A_n \vdash \varphi(A_1, \cdots, A_k)^{\varphi(0, 1, \cdots, 1)}; \cdots, \neg A_1,$ $\varphi(A_1, \cdots, A_k)$. Но мы знаем, что φ тавтология, поэтому верхние $\varphi(1/0, 1/0, \cdots, 1/0)$ можно убрать. Заметим, что $A_1, \cdots, A_k \vdash \varphi, \neg A_1, \cdots, A_k \vdash \varphi$, а значит $A_1 \vee \neg A_1, A_2, \cdots, A_k \vdash \varphi$, а значит можно убрать $A_1 \vee \neg A_1$. Останемся с хвостом $A_2, \cdots, A_k \vdash \varphi$, потом к A_2 можно применить похожий трюк, и в итоге останемся с тем, что $\vdash \varphi$, т.е. φ выводится из ИВ. □

А теперь докажем ещё иным способом:

Но сначала введём определения:

***Определение* 4.7.** Множество (/набор) формул Γ — совместно, если $\exists$ набор значений, на котором все формулы из Γ вычисляются в единицу.

***Определение* 4.8.** Γ является противоречивым множеством формул, если $\Gamma \vdash F$ и $\Gamma \vdash \neg F$. Если же Γ не противоречиво, то оно непротиворечиво.

Теорема 4.4. Множество непротиворечиво тогда и только тогда когда оно совместно.

Перед доказательством поймём, почему из него следует полнота и корректность.

Теорема 4.5. Из этого следует теорема о корректности — всё выводимое является тавтологиями

Доказательство. Пусть $\vdash \varphi$, тогда $\neg\varphi$ противоречиво, т.к. $\neg\varphi \vdash \varphi$ и $\neg\varphi \vdash \neg\varphi$. Раз противоречиво, то несовместно. Значит нет набора, на котором оно есть единица, тогда φ от всех наборов равняется единице. Корректность доказана. □

Теорема 4.6. Теорема о полносте — любая тавтология выводится

Доказательство. φ — тавтология, тогда $\neg\varphi$ — несовместно, а тогда оно противоречиво (всё по той же недоказанной теореме). А раз противоречиво. Тогда можно $\vdash \neg\neg\varphi$, т.к. $\neg\varphi \vdash G, \neg\varphi \vdash \neg G$. А тогда $\vdash \neg\neg\varphi, \neg\neg\varphi \to \varphi$ □

Утверждение 4.7. Γ — совместно, тогда Γ непротиворечиво. Пусть $F_1, F_2, \cdots, F_k$ (формул, возможно, бесконечность) $\vdash$. Ну а потом там modus ponens бахаем и пытаемся радоваться жизни, я снова проиграл, кто понял + воспринял — распишите пж.

Утверждение 4.8. Γ — непротиворечиво, тогда Γ — совместно.

Доказательство. Ну там если есть прямые формулы вида $x_1, x_2, \neg x_3$ то для них значения очевидны. True тогда если есть выполняющий набор, то это такой.

А теперь хотим Γ вложить в непротиворечивый Γ', содержащий x_1 или $\neg x_1$. True так последовательно продобавляем для каждой переменной x_i или $\neg x_i$. □

***Определение* 4.9.** Γ — полное, если $\forall\varphi\Gamma \vdash \varphi$ или $\Gamma \vdash \neg\varphi$.

Утверждение 4.9. $\forall\Gamma$ непротиворечивых $\exists$ полное $\Gamma' : \Gamma \subset \Gamma'$ и Γ' — непротиворечиво.

Пусть формул счётное число, тогда выпишем их по порядку. True пойдём по ним в этом порядке. $\Gamma_i = \begin{cases} \Gamma_{i-1} \cup \varphi_i \\ \Gamma_{i-1} \cup \neg\varphi_i \end{cases}$ что Γ_i — непротиворечиво. Хотим получить это, зная, что Γ_{i-1} — непротиворечиво. Пусть $\Gamma_{i-1} \vdash \varphi$, тогда $\Gamma_i = \Gamma_{i-1} \cup \varphi_i$. А если $\Gamma \vdash \neg\varphi_i$, то $\Gamma_i = \Gamma_{i-1} \cup \neg\varphi_i$. А если же ни одно не выводится, то возьмём произвольное, в частности $\Gamma_i = \Gamma - i - 1 \cup \varphi_i$.

Почему не возникло противоречий? Пусть возникли, тоогда $\Gamma_{i-1}, \varphi_i \vdash G$; и $\vdash \neg G$, но тогда просто $\Gamma_{i-1} \vdash \neg\varphi_i$. А мы в третьем случае предположили, что ни то, ни это выводить не умеем, противоречие.

Доказательство. Продолжение предыдущего доказательства: теперь умеем выписывать ещё и все переменные, почему такое означение будет корректным? Узнаем на следующей паре □

Вспомните определение совместного множества формул. И определение противоречивого.

Доказательство. Хотим доказать, что если Γ не противоречиво, то Γ совместно.

Уже щнаем, что можем дополнить Γ до полного. Тогда $\Gamma' \vdash x_1$ или $\Gamma' \vdash \neg x_1$, а значит можно означить все переменные. Осталось понять, почему все формулы будут выполнены.

Пусть есть $\varphi(x_{i_1}, \cdots x_{i_k}) = 0$. У нас была лемма, что $A_1^{x_1}, \cdots A_k^{x_k} \vdash \varphi(A_1, \cdots, A_k)$. Тогда мы можем $\Gamma' \vdash \neg\varphi$. Но при этом $\Gamma' \vdash \varphi$ т.к. $\varphi \in \Gamma'$. Противоречие. Значит были противоречивы. Противоречие. □

Теперь знаем, что Γ не противоречиво $\Leftrightarrow$ Γ совместно

Теорема 4.10. О компактности

Γ совместно $\Leftrightarrow$ совместно любое конечное подмножество формул из Γ

Доказательство. Если Γ совместно, то очевидно и любое конечное подмножество будет совместным.

В обратную сторону от противного. Пусть Γ не совместно. Тогда, по предыдущей теореме, Γ противоречиво. Но тогда $\exists C_1, C_2, \cdots C_k = \varphi$ и $C'_1, C'_2, \cdots, C'_k = \neg\varphi$ Это конечное множество формул (объединение этих двух цепочек). Оно использует только аксиомы и конечное число формул из Γ. А тогда мы получили конечное число формул из Γ, из которых выводится противоречие. Вот и конечное несовместное множество. □

А теперь задача — хотим покрасить плоскость в минимальное число цветов так, чтобы любые две точки на расстоянии один были покрашены в разные цвета. Какое минимальное количество цветов? Понятно, что в девять наверно можно, а в два точно нельзя (равносторонний треугольник со стороной один). Оценку снизу можно предъявить используя конечное число точек.

Вопрос: верно ли, что достаточно только конечных наборов? Точнее, верно ли, что если плоскость можно покрасить не меньше, чем в k цветов, то для $k-1$ цветов будет существовать пример на конечном числе точек?

***Определение* 4.10.** Обобщённый граф — подмножество декартового квадрата вершин. Но вершин теперь может быть бесконечность.

***Определение* 4.11.** Граф двудольный $\Leftrightarrow$ в нём нет нечётных циклов.

Теорема 4.11. Верно ли это для обобщённых графов?

Доказательство. Давайте каждой вершине в нашем обобщённом графе присвоим x_i, где индексируем не обязательно натуральными числами. Если мы означим ей значение 0, то она будет лежать в левой доле, а если 1, то в правой. Тогда двудольность — означить все и проверить, что все рёбра $(x \vee y) \wedge (\neg x \vee \neg y)$. Так мы для каждого ребра создали формулу. Получили набор формул Γ.

По теореме о компактности, Γ совместно, если для любое конечное подможетство совместно. А когда оно может быть несовместно? Когда есть конечный цикл нечётной длины. □

А теперь вернёмся к конечным наборам. Для каждой точки создадим набор переменных. Так для точки (i,j) получили набор $x_1^{i,j}, x_2^{i,j}, \cdots, x_k^{i,j}$. Так хотим, чтобы $x_1 = \cdots x_{p-1} = x_{p+1} = \cdots x_k = 0$ и $x_p = 1$. Т.е. $\bigcup_{p=1}(x_p \wedge \neg x_1 \wedge \neg x_2 \wedge \cdots \wedge \neg x_{p-1} \wedge \neg x_{p+1} \wedge \cdots \wedge \neg x_k)$. Теперь добавим условия на то, что две вершины не могут быть покрашены в один цвет: $\forall p \in [1, k] \neg x_p^{i,j} \vee \neg x_p^{i',j'}$. И снова нам нужно совместное множество формул а значит если оно несовместно, то найдётся несовместное конечное подмножество, по которому набирается контрпример из конечного числа точек.

Шаг в сторону: ШОК КОНТЕНТ: Десятая аксиома выводится из аксиом 1-9 и 11.

Сама аксиома: $(A \to B) \to ((A \to \neg B) \to \neg A)$. Заметим, что она не используется для доказательства леммы о Дедукции. Тогда нам нужно доказать, что $A \to B, A \to \neg B \vdash \neg A$. А ещё у нас было правило разбора случаев. А тогда $(A \to C) \to ((B \to C) \to (A \vee B) \to C)$, и сидим с цепочкой из modus ponens $A \to B, A, B, A \to \neg B, \neg B, B \to (\neg B \to \neg A)$.

А вот аксиому 11 $(A \vee \neg A)$ выкинуть нельзя. Но почему?

А давайте введём **мегалогику**. В ней ещё будет, помимо истины и лжи, мистическое **наверное**.

Сидим с $True, False, Probably$. Хотим доопределить всё так, чтобы старое не сломалось. Хотим доопределить таблицы истинности для случаев, когда они из операндов — наверно.

Тавтологии — те формулы, куда подстановка любых значений из тройки результирует в истину.

Сопоставим $True = 1, False = 0, Probably = \frac{1}{2}$. $x \wedge y = \min(x, y)$. $x \vee y = \max(x, y)$. А ещё $\neg Probably = False, \neg(\not{P}robably) = True$. $True \to x = x, False \to x = True, (Probably \to False) = False, (Probably \to Probably) = True, (Probably \to True) = True$.

Аксиомы с первой по десятую сохраним, они остаются тавтологиями. Но вот одиннадцатая аксиома перестала быть тавтологией: $(Probably \vee \neg Probably) = (Probably \vee False) = Probably$

А теперь предположим, что из первых десяти аксиом выводится одиннадцатая. Тогда пусть есть $C_1, C_2, \cdots, C_k = A \vee \neg A$, где C_i — аксиома или применение modus ponens. Тогда пусть $A = Probably$. Мы знаем, что при modus ponens $(C_k \to C_j)$ истинно. Тавтологии у нас были там все как и в 2-системе, так и в 3-системе, но итоговый вывод не является тавтологиев в 3-системе, противоречие/проблема.

Falseогика, в которой аксиомы с 1 по 10, называется интуиционистской логикой.

Обратно к компактности. Выполняется для любого числа переменных, конечного, счётного, несчётного...

Пусть есть переменные $x_1, \cdots, x_n$. Тут было что-то про выполнимость, классы и 2^{2^n} и про выполнимость класса. Вставить текст.

Пускай переменные $x_1, \cdots, x_n, \cdots$. Теперь рассмотрим какие-то наборы значений этих переменных. Различных наборов значений переменных больше, чем континум $(2^{2^{\mathbb{N}}})$. Пусть $\mathcal{A}$ — набор означиваний. Хотим построить множество формул Γ так, чтобы значение лежало в наборе тогда и только тогда, когда любая формула из Γ вычисляется в истину. Если хотим один набор, то его легко задать, явно описав значения через $x_1, \neg x_2, \cdots$. Но подмножеств формул — континум, а означиваний — больше, чем континум. А тогда существует какой-то набор означиваний, который нельзя задать формулами. Печально!