Математическая логика

Ипатов Марк

20 мая 2022 г.

Содержание

1. Множества, мощность множеств

1.1. Равномощные 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.

***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 $Y \subset X, f : \mathbb{N} \Leftrightarrow Y$. □

Пример. Счётное множество, для которого мы таким процессом не докажем счётность: $X = \{1, 2, 3, \cdots\}$, $Y = \{2, 4, 6, \cdots\}$. Иными словами, мы все элементы из X далеко не обязательно вытащим.

Пример. Множество $(0, 1)$ не является счётным.

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

Доказательство. Для дизъюнкных всё хорошо понятно. Для недизъюнктных:

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

Теперь воспользуемся индукцией по k: База: A_1, A_2 счётны по условию, тогда $A_1 \cup A_2$ тоже счётно. Тогда $(A_1 \cup A_2 \cup A_3 \cdots A_k) = ((\cdots((A_1 \cup A_2) \cup A_3) \cup \cdots) \cup A_k)$ □

Лемма. $A_1, A_2, \cdots$ — счётное число счётных множеств, т.е. для любого $i \exists A_i$.

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. □

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 $A_i = \{\frac{m}{i} | m \in \mathbb{N}\}$. Т.к. любое из $\mathbb{Q}_+$ так представляется, то в такое объединение попадёт всё $\mathbb{Q}_+$. □

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. □

Двигаемся к несчётным множествам.

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

Доказательство. B заменим на $B' = B/A$. 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 $A = (A \ A') \cup A'$.

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

Между частями $(A \setminus A')$ построим тождественную биекцию. А a_i будем отображать в b_i, если $i \leqslant k$, а в a_{i-k} если $i > k$. Понятно, что это биекция. Все элементы возьмём как из B, так и из a_i. □

Замечание. Доказательство можно модифицировать для случая, когда B счётно. Тогда давайте на последнем шаге чётные отображать в a_i, а нечётные — в b_i.

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 один префиксы, а затем у одного числа идёт единица и после только нули, а у второго ноль и затем только единицы. Идём слева направо и найдём первый момент, когда они отличаются. В одном ноль, во втором единица. Далее всё идёт сколько0то, как мы предсказали, затем, что-то разойдётся и там можно оценить, что числа у нас уже отличаются на что-то, что не сможем покрыть дальнейшим. Спасибо Близнецу за успешно закрытую собой доску... Но там в любом случае очев $= D$ А все числа такого вида это просто $\mathbb{Q}$ (или что-то такого рода)((На самом деле оно даже не $\mathbb{Q}$, там только дроби вида сумма какого-то конечного числа отрицательных степеней двойки, что есть подмножество $\mathbb{Q}$)). Тогда $X \equiv [0, 1] \sqcup (\mathbb{Q} \cap [0, 1])$. Результат пересечения счётен, а значит объединение равномощно бесконечной левой части, т.е. $X \equiv [0, 1]$ □

Теперь знаем, что натуральные счётны, чётные счётны, целые счётны, рациональные положительные счётны, просто рациональные счётны. А вот действительные уже несчётны, т.к. содержат $[0, 1]$.

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

ТУТ ПРОПУЩЕНА ЛЕКЦИЯ. ДОСАДНО.

1.2. 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.

Очевидным образом коммутативны.

Произведение мощностей, ожидаемо, мощность произведения множеств.

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 там условно у первых функций есть две координаты, мощно рассмотреть проекции на A и на B и всё будет ок.

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

2. Частично упорядоченные множества

2.1. Про отношение

Пусть есть множество A, и ввели отношение эквивалентности $R \subset A \times A$. Оно должно удовлетворять 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, мы хотим отноешние порядка R' , оно должно удовлетворять 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.

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 $f : \mathbb{R} \to \mathbb{R}, f \leqslant g \Leftrightarrow \forall x \in \mathbb{R} f(x) \leqslant g(x)$. 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 $5 < 6 < \cdots < 1' < 2'$, 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* 2.1.** ЧУМ — линейный, если $\forall$ два элемента сравнимы.

***Определение* 2.2.** 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.

***Определение* 2.3.** X, Y — ЧУМы, $\varphi : X \to Y$ — изоморфизм, тогда и только тогда, когда φ — биекция, и $a \leqslant b \Leftrightarrow \varphi(a) \leqslant \varphi(b)$

Пусть ещё пример — $k \leqslant n$ — k делителей 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. 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* 2.4.** x, y — соседние, есть $x \leqslant y$ и между x и y нет элементов и порядок линейный.

***Определение* 2.5.** Линейный порядок называется плотным, если $\forall x, y, x < y \to \exists z : x < z < y$

Теорема 2.1. X, Y — ЧУМ, если они конечные ЧУМ 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. □

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

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

Доказательство. Выпишем подряд x_i, 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. □

3. Высказывания

3.1. Высказывания

Начало пропущено, но оно простое.

Высказывание — утверждение, которое может быть ложным или истинным.

Тут был кек про Юрия Зайцева и про то, как 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 $(A \cap B), (A \cup B), (A \to B)$ — 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 скобоный 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 $x \cup \neg x$, или $(p \to q) \cup (q \to p)$

***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:

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

- $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$
- $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
- $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
- $p \vee (p \wedge q) \leftrightarrow p$
- $p \wedge (p \vee q) \leftrightarrow p$
- $(p \to q) \leftrightarrow (\not{q} \to \not{p})$
- $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
- $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

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 — $(x_{i1} \wedge x_{i2} \wedge \cdots \wedge x_{ik})$ — набор логических И, возможно с отрицаниями.

***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. □

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 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 — $1, x, x \wedge y, x \wedge y \wedge w$

***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.

Доказательство. 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.

Мы знаем, что используя $\neg, \vee, \wedge$ можно записать все формулы. А сами эти операции можно выразить следующим образом: $\neg x = x \oplus 1; x \vee y = xy \oplus x \oplus y; x \wedge y = x \wedge y$. □

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

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

Займёмся классами функций

***Определение* 3.11.** 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.

Доказательство. 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, но в общем лекция закончилась, теорему доказать не успели.

□

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

Хотим найти функцию не сохраняющую ноль. Тут это только тождественная единица и отрицание икса. Это будет f_i

Теперь хотим $h(x) - - - f_j$ не сохраняющая единицу. Это отрицание или тождественный ноль.

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, среди которых есть ноль, на котором 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.

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 можем получить вторую.

Теперь к нелинейности. Функция нелинейна есть её полином Жегалкина нелинеен. Пусть $f_e(x_1, \cdots, x_m) = x_1x_2A(x_3, \cdots, x_m) \oplus x_1B(x_3, \cdots, x_m) \oplus x_2C(x_3, \cdots, x_m) \oplus D(x_3, \cdots, x_m)$, 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 $f_e(x_1, x_2, a_3, \cdots, a_m$ $\cdots$ восемь вариантов:

1. $x_1x_2 \oplus x_1 \oplus x_2 \oplus d$
2. $x_1x_2 \oplus x_1 \oplus d$
3. $x_1x_2 \oplus x_2 \oplus d$
4. $x_1x_2 \oplus d$

Где d — какая-то константа. Но отрицанием можно убрать $\oplus d$. Теперь, если мы получили последнее, то мы получили $\wedge$ — победа. Есть первое, что 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. □

Рассмотрим $f(x_1, x_2, x_3) = ((x_1 \wedge x_2) \oplus (x_3 \vee x_1))\ (x_1 \wedge x_2)$, где — какая-то бинарная операция (в оригинале — стрелка Пирса). Тогда можно составить схему, пока — дерево — граф выполнения, где вершины — операции или исходные переменные, а рёбра — 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 на практике докажем:

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

Теорема 3.8. $f : B^n \to B$. 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.

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

Пусть у нас n переменных, и N — размер схемы.

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 $2^{(\log 8c^4)2c^n} \leqslant 2^{c^n \cdot n \cdot const}$. 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 $(2-\varepsilon)^n$. □

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 $x_1 x_2 \cdots x_n$ и $y_1 y_2 \cdots y_n$ и получить $z_0 z_1 \cdots z_n$, 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.

Давайте сравним числа $x_1 x_2$ и $y_1 y_2$. Из неравенства между x_1 и y_1 следует неравенство ааа кто здесь между $x_1 x_2$ и $y_1 y_2$. В общем, на первом слое сравниваем единичные цифры, на втором — пары, на третьем — четвёрки подряд идущих блоков и так далее, получаем логарифм слоёв константной глубины. Ну в общем там немного иначе, поправьте кто-нибудь пж. Каждый раз мы сравниваем результаты предыдущих слоёв, а не сравнивать все 4/8/16... битов.

Полученный результат можно использовать для получения бита переноса — бит переноса c_i есть, если число $x_i x_{i+1} \cdots x_n$ больше, чем $1 - y_i 1 - y_{i+1} \cdots 1 - y_n$.

Теорема 3.10. Пусть есть $x_1 x_2 \cdots x_n$ и хотим получить сумму этих n бит и записать их в виде числа $y_1 y_2 \cdots y_{\log n}$. Это можно сделать схемой размера $\mathcal{O}(n)$ и глубины $\mathcal{O}(\log n \log\log n)$

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. $B \to (A \vee B)$
5. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
6. $(A \wedge B) \to A$
7. $(A \wedge B) \to B$
8. $A \to (B \to (A \wedge B))$
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. $A \vee \neg A$ — Аксиома исключённого третьего

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

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

$C_1 = A \to (B \vee A)$, аксиома 4. $C_2 = B \to (B \vee A)$, какая-то другая аксиома с переименованием переменных. Далее в пятую аксиому подставим вместо A — A, вместо B — $(B \vee A)$, вместо C — B, получим $(A \to (B \vee A)) \to ((B \to (B \vee A)) \to ((A \vee B) \to (B \vee A)))$, 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 $(A \vee B) \to (B \vee A)$ 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. И 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 $A \to C_i$. Итого 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 $\Leftrightarrow A \vdash B \to (A \wedge B) \Leftrightarrow A, B \vdash A \wedge B$.