# Билеты по матлогике

Игорь Энгель, Полина Чистякова

10 июня 2020 г.

## Содержание

# 1. Равномощность

Это самое начало теории множеств (какое отношение оно имеет к матлогике не очень понятно, но пусть будет).

## 1.1. Билет 01 «Равномощные множества»

Для множеств определено отношение равномощности - «множество $A$ равномощно множеству $B$ » значит, что из одного множества в другое можно построить биекцию. Иными словами это значит, что любому элементу из множества $A$ сопоставляется ровно один элемент из множества $B$.

Пример двух равномощных множеств - в парке гуляют дети. Если каждому ребёнку на входе в парк подарить шарик, то множества детей и шариков в парке будут равномощны (если никакой ребёнок не отпустит/лопнет шарик).

Как у любого отношения у равномощности есть свои свойства. Это отношение эквивалентности. Это значит, что оно

- рефлексивно: «$A$ равномощно $A$»
- симметрично
- транзитивно

**TODO:** Доказательства - АЧИВИДНА **TODO:** Примеры *их там много и они страааашные :c*

## 1.2. Билет 02 «Счётные множества»

Билет не просто маленький, он *крошечный*... В книге просто куча воды. Кажется, на экзамене это не попадётся.

Счётное множество - множество, равномощное множеству натуральных чисел. Иными словами - мы просто «пронумеровали» все элементы множества. Биекция будет означать, что у каждого элемента есть номер (сюръекция), и у каждого элемента не больше одного номера (инъекция).

**TODO:** надо расписать примеры, ага *но мне лень*

Самые простые примеры счётных множеств: само $\mathbb{N}$ или множество значений линейной функции от натуральных чисел. (ещё бывает $\mathbb{Z}$)

Чуть более сложный пример - $\mathbb{Q}$

Но его доказательство - следующий билет с: **TODO:** ссылочка просится :c - можно забить, пусть просится

## 1.3. Билет 0(3+4) «Счётность множества рациональных чисел» + «Счётность объединения счётного количества счётных множеств»

Тут будет ооочень много лемм и теорем, готовьтесь...

**Лемма.**
Объединение двух счётных множеств счётно.

***Доказательство.***
Рассмотрим два счетных множества A и B; каждое из них можно записать в последовательность:

$$a_0, \quad a_1, \quad a_2, \quad ...$$

$$b_0, \quad b_1, \quad b_2, \quad ...$$

Теперь можно поочерёдно брать элементы из первой и второй последовательности и записывать в новую (это даст нам $A \cup B$):

$$a_0, \quad b_0, \quad a_1, \quad b_1, \quad a_2, \quad b_2, \quad a_3, \quad b_3, \quad ...$$

Если $A \cup B = \varnothing$, то мы всё доказали ^^

Если же это не так, то повторяющиеся элементы мы просто не выписываем. □

**Лемма.**
Всякое подмножество счетного множества конечно или счетно.

***Доказательство.***
Пусть у нас есть счётное множество $A$ и его подмножество $A'$. Выпишем множество $A$ в строчку. Затем зачеркнём все элементы, не принадлежащие $A'$. Получим последовательность из всех элементов $A'$: либо конечную (тогда $A'$ конечно), либо бесконечную (тогда $A'$ счётно) □

**Лемма.**
Всякое бесконечное множество содержит счётное подмножество.

***Доказательство.***
Выпишем бесконечную последовательность. Возьмём первый элемент случайно (множество не пусто). Дальше будем каждый раз рассматривать дополнение получившейся послдовательности до изначального множества. Оно никогда не кончится (множество бесконечно), значит, мы всегда сможем выписать новый элемент последовательности. Получили бесконечную последовательность. Значит, у изначального множества есть счётное подмножество. □

**Лемма.**
Множество рациональных чисел $\mathbb{Q}$ счетно

***Доказательство.***
Докажем сначала отдельно про положительные и отрицательные части $\mathbb{Q}$. Тогда по одной из предыдущих лемм их объединение будет счётно.

Неотрицательное рациональное число задается парой чисел — числителем и знаменателем. Числитель может быть произвольным натуральным числом, а знаменатель произвольным положительным натуральным числом. Выпишем все такие числа в виде таблицы, бесконечной вниз и вправо:

$$\begin{array}{cccccc} 0/1 & 1/1 & 2/1 & 3/1 & \dots \\ 0/2 & 1/2 & 2/2 & 3/2 & \dots \\ 0/3 & 1/3 & 2/3 & 3/3 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

В этой таблице выписаны все числа (а некоторые даже повторяются.....)

Числа из этой таблицы теперь уже легко выписать в последовательность. Например, можно идти по диагоналям (вниз-влево). Сначала выпишем единственное число на первой диагонали (0/1), потом два числа на второй (1/1, 0/2), потом три числа на третьей и так далее:

$$0/1, 1/1, 0/2, 2/1, 1/2, 0/3, 3/1, 2/2, 1/3, 0/4, \ldots$$

Другими словами, мы сначала выписываем все числа с суммой числителя и знаменателя 1, потом — с суммой 2, потом 3 и так далее. Если мы встречаем число, которое уже выписывали - просто пропускаем его.

Доказательство для отрицательной части $\mathbb{Q}$ аналогично. □

**Теорема 1.1.**

Объединение конечного или счётного числа конечных или счётных множеств конечно или счётно.

***Доказательство.***

Пусть есть счётное количество счётных множеств $A_1, A_2, A_3, \ldots$. Выпишем их в табличку:

$$\begin{array}{lccccc} A_0: & a_{00} & a_{01} & a_{02} & a_{03} & \ldots \\ A_1: & a_{10} & a_{11} & a_{12} & a_{13} & \ldots \\ A_2: & a_{20} & a_{21} & a_{22} & a_{23} & \ldots \\ A_3: & a_{30} & a_{31} & a_{32} & a_{33} & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

□

**Теорема 1.2.**

Декартово произведение двух счётных множеств A × B счётно.

***Доказательство.***

Декартово произведение - множество упорядоченных пар вида $(a, b) \mid a \in A, b \in B$.

Разделим пары на группы - в каждой группе первый элемент пары совпадает. Тогда получим счётно объединение счётных множеств (у нас будет «$|A|$ штук» множеств по «$|B|$ штук» элементов в каждом) □

## 1.4. Билет 05 «Добавление счётного множества»

**Теорема 1.3.**

Если множество $A$ бесконечно, а множество $B$ конечно или счётно, то множество $A \cup B$ равномощно $A$.

***Доказательство.***

НУО $A \cap B = \varnothing$ - иначе вместо $B$ берём $B \setminus A$.

Мы знаем, что в $A$ есть счётное подмножество $A_0$. Тогда есть биекция из $A_0 \cup B$ в $B$ (потому что оба множества счётные - биекция черз натуральные числа). Тогда есть биекция из $A \cup B = (A \setminus A_0) \cup (A_0 \cup B)$ □

## 1.5. Билет 06 «Равномощность отрезка [0,1] множеству всех бесконечных последовательностей из 0 и 1»

Надеюсь, здесь нужно только то, что в названии билета ( **TODO:** написать всякие интервалы, полуинтервалы и тд - АЧИВИДНА2)

**Теорема 1.4.**
*Вставь сюда название билета*

***Доказательство.***
Мы знаем, что $\forall x \in [0, 1]$ существует запись $x$ в виде бесконечной двоичной дроби. ( **TODO:** сюда бы картинку из samples/...) Но тогда некоторым точкам будут соответсвовать 2 последовательности (например, 0, 1001111... и 0, 101000...). Тогда выкинем все последовательности, заканчивающиеся бесконечным рядом единиц (их счётное число, поэтому так можно) □

## 1.6. Билет 07 «Равномощность квадрата отрезку»

**Теорема 1.5.**
*Название билета*

***Доказательство.***
Мы знаем, что каждому числу из [0, 1] соответствует одна бесконечная последовательность из 0 и 1. Тогда $[0, 1] \times [0, 1]$ соответсвует пара таких последовательностей. Биекция между парой и последовательностью:

$$(a_0a_1a_2a_3\ldots, b_0b_1b_2b_3\ldots) \to a_0b_0a_1b_1a_2b_2a_3b_3...$$ □

## 1.7. Билет 08 «Теорема Кантора (несчётность отрезка)»

**Теорема 1.6.**
Множество бесконечных последовательностей нулей и единиц несчётно.

***Доказательство.***
Пусть оно счётно. Пронумеруеми выпишем:

$$\begin{array}{ccccccc} a_0 & = & a_{00} & a_{01} & a_{02} & a_{03} & \ldots \\ a_1 & = & a_{10} & a_{11} & a_{12} & a_{13} & \ldots \\ a_2 & = & a_{20} & a_{21} & a_{22} & a_{23} & \ldots \\ \vdots & = & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Теперь посмотрим на последовательность, имеющую вид $b_i = 1 - a_{ii}$. Это последовательность из нашего множества. С другой стороны, она не совпадает с любой другой последовательностью (возьмём номер и посмотрим на нужный член). Ой. □

## 1.8. Билет 09 «Теорема Кантора-Бернштейна»

***Определение* 1.1.**
Множество A имеет мощность не большую, чем множество B, если A равномощно некоторому подмножеству множества B (возможно, совпадающему с B).

**Теорема 1.7.**

Если мощность A не больше, чем у B, и одновременно мощность B не больше, чем у A, то A и B равномощны.

***Доказательство.***

Это эквивалентно утверждению: «Если для множеств A и B существует инъекция из A в B и инъекция из B в A, то существует и биекция между A и B.»

*биекция между множеством A и подмножеством множества B = инъекция из A в B*

Нарисуем это!! Слева множество $A$, справа - $B$. И проведём все стрелочки-функции $f$ и $g$. Получим возможно бесконечный ориентированный двудольный граф.

Посмотрим на компоненты связности (если забить на оринтированность). Они бывают либо циклом, либо цепочкой, бесконечной в одну сторону, либо цепочкой, бесконечной в обе стороны.

Почему? Потому что из любой вершины мы точно можем выйти. Но не в любую вершину мы можем войти (отсюда один конец у цепочки). Если мы пришли в вершину, из которой вышли - это цикл,и он конечный, при этом чётной длины. В цикле - у нас целых 2 варианта биекции!! (разделим по функциям). В дважды бесконечной цепочке - тоже. А в лишь однажды бесконечной всё определено за нас :c □

## 1.9. Билет 10 «Теорема Кантора (общая формулировка)»

**Теорема 1.8.**

Никакое множество X не равномощно множеству своих подмножеств.

***Доказательство.***

Пусть не так. Пусть существует биекция $f : X \to 2^X$. Рассмотрим $Y = \{x \mid x \notin f(x)\}$. До противоречия осталось совсем немного! $Y \subset X$. Тогда $\exists y \in X : f(y) = Y$. Тогда

$$y \notin Y \iff y \notin f(y) \text{- потому что} Y = f(y)$$

С другой стороны, тогда $y \in Y$, потому что $Y$ так строился. □

## 1.10. Билет 11 «Операции над мощностями»

Мощности конечных множеств — натуральные числа, и их можно складывать, умножать, возводить в степень.

***Определение* 1.2.**

Сумма мощностей множеств - мощность их объединения (если они не пересекаются) или непересекающихся равномощных им в ином случае.

***Определение* 1.3.**

Произведение мощностей множеств - мощность их Декартового произведения.

***Определение* 1.4.**

Возведение в степень ($|A|^{|B|}$) - мощность множества $A^B = \{f \mid f : B \mapsto A\}$

$$a + b = b + a$$

$$a + (b + c) = (a + b) + c$$

$$a \times b = b \times a$$

$$a \times (b \times c) = (a \times b) \times c$$

$$(a + b) \times c = (a \times c) + (b \times c)$$

Просто поставь нам биекцию вместо равно!

**Теорема 1.9.**

$$a^{b+c} = a^b \times a^c$$

***Доказательство.***

Из чего состоит $A^{B+C}$? Его элементами являются функции со значениями в $A$, определённые на $B+C$. Такая функция состоит из двух частей: своего сужения на $B$ (значения на аргументах из $B$ остаются теми же, остальные отбрасываются) и своего сужения на $C$. Тем самым для каждого элемента множества $A^{B+C}$ мы получаем пару элементов из $A^B$ и $A^C$. Это и будет искомое взаимно однозначное соответствие. □

**TODO:** В книге док-в нет, надо самим писать :c

$$(ab)^c = a^c \times b^c$$

$$(a^b)^c = a^{b \times c}$$

Свойства мощностей:

$$\aleph_0 + n = \aleph_0 \text{ для конечного } n$$

$$\aleph_0 + \aleph_0 = \aleph_0$$

$$\aleph_0 \times \aleph_0 = \aleph_0$$

Какие-то красивые формулы, следующие из свойств операций:

$$\mathfrak{c} \times \mathfrak{c} = 2^{\aleph_0} \times 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$$

$$\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$$

# 2. Частично упорядоченные множества

## 2.1. Билет 12 «Отношение порядка»

***Определение* 2.1.**
Бинарное отношение на множестве $X$ - подмножетсво $R \subset X \times X$

***Определение* 2.2.**
*Отношение частичного порядка* на множестве $X$ - бинарное отношение на множестве $X$, обладающее следующими свойствами:

- *рефлексивность*
- *антисимметричность*
- *транзитивность*

Множество $X$ тогда называется *частично упорядоченным*.

***Определение* 2.3.**
Два элемента $x, y \in X$ называются *сравнимыми*, если $x \geq y$ или $y \geq x$.

***Определение* 2.4.**
Если сравнимы любые 2 элемента из множества $X$ сравнимы, то такое отношение частичного порядка на $X$ называют *линейным*.

***Определение* 2.5.**
Отношение строгого порядка - $x > y \iff x \geq y, x \neq y$

**TODO:** *минимальный* и *максимальный элементы* сюда писать?..

## 2.2. Билет 13 «Примеры упорядоченных множеств»

- Числовые множества с приличным порядком (он ещё и линейный, равняйтесь на него!)
- Пример нелинейного порядка - на множестве $\mathbb{R} \times \mathbb{R}$: $\langle x_1, y_1 \rangle \geq \langle x_2, y_2 \rangle \iff x_1 \geq x_2, y_1 \geq y_2$
- На множестве функций с действительными аргументами и значениями можно ввести частичный порядок, считая, что $f \geq g$, если $f(x) \geq g(x)$ при всех $x \in \mathbb{R}$. Этот порядок не будет линейным.
- На множестве целых положительных чисел можно определить порядок, считая, что $x \geq y$, если $y$ делит $x$. Этот порядок тоже не будет линейным.
- Пусть $U$ — произвольное множество. Тогда на множестве $P(U)$ всех подмножеств множества $U$ отношение включения $\subset$ будет частичным порядком.
- На буквах русского алфавита традиция определяет некоторый порядок (а $<$ б $<$ ... $<$ я). Этот порядок линеен — про любые две буквы можно сказать, какая из них раньше (при необходимости заглянув в словарь).

- На словах русского алфавита определён лексикографический порядок (как в словаре). Формально определить его можно так: если слово $x$ является началом слова $y$, то $x < y$ (например, кант <кантор). Если ни одно из слов не является началом другого, посмотрим на первую по порядку букву, в которой слова отличаются: то слово, где эта буква меньше в алфавитном порядке, и будет меньше. Этот порядок также линеен.

- Отношение равенства также является отношением частичного порядка, для которого никакие два различных элемента не сравнимы.

## 2.3. Билет 14 «Операции над частично упорядоченными множествами»

- Индуцированный порядок: $(\geq_Y) = (\geq) \cap (Y \times Y)$, где $(\geq)$ - частичный порядок на $X, Y \subset X$

- Пусть $X$ и $Y$ — два непересекающихся частично упорядоченных множества. Тогда на их объединении можно определить частичный порядок так: внутри каждого множества элементы сравниваются как раньше, а любой элемент множества $X$ по определению меньше любого элемента $Y$. Это множество естественно обозначить $X + Y$. (Порядок будет линейным, если он был таковым на каждом из множеств.)

  *такое же обозначение есть и для пересекающихся множеств - просто создаём отличающиеся копии элементов, лежащих в обоих множествах*

- Пусть есть $(X, \geq_X), (Y, \geq_Y)$ - два частично упорядоченных множества.

  На произведении $X \times Y$ бывает 2 порядка - покоординатный и лексикографический. **TODO:** на экзамене стоит это расписать

## 2.4. Билет 15 «Изоморфизм частично упорядоченных множеств»

***Определение* 2.6.**

*Изоморфизм* - взаимнооднозначное соответствие, сохраняющее порядок.

Два множества, между которыми существует изоморфизм называются *изоморфными*

**Лемма.**

Отношение «изоморфность» - отношение эквивалентности. Классы эквивалентности называются *порядковыми типами.*

***Доказательство.***

Это отношение рефлексивно (мн-во изоморфно само себе), симметрично (потому что обратная функция биекции - биекция) и транзитивно (каждому элементу соответсвует свой путь до третьего множества) □

**Теорема 2.1.**

Конечные линейно упорядоченные множества из одинакового числа элементов изоморфны.

***Доказательство.***

Всегда можно взять наименьший. Тогда поочереди так можно их вытаскивать и выстроить по порядку (что даёт соответствие с номерами) □

***Определение* 2.7.**

*Автоморфизм* - изоморфизм в себя.

Несколько примеров равномощных, но не изоморфных множеств:

- Отрезок $[0, 1]$ и $\mathbb{R}$ - у одного есть наибольший элемент, а у другого - нет.
- $\mathbb{Z}$ и $\mathbb{Q}$ - потому что соседние должны переходить в соседние.

## 2.5. Билет 16 «Теорема о счётных плотных линейно упорядоченных множествах»

***Определение* 2.8.**

*Соседние* элементы - два сравнимых элемента, между которыми нет третьего.

*Плотное* множество - множество, в котором нет соседних (между любой парой элементов есть третий)

**Теорема 2.2.**

Любые 2 счётных плотных линейных множества без наименьшего и наибольшего элемента изоморфны.

***Доказательство.***

Пусть $X$ и $Y$ — данные нам множества.

Требуемый изоморфизм между ними строится по шагам.

После $n$ шагов у нас есть два $n$-элементных подмножества, элементы которых мы будем называть «охваченными», и изоморфизм между ними.

На очередном шаге мы берём какой-то неохваченный элемент одного из множеств и сравниваем его со всеми охваченными элементами его множества.

Он может оказаться либо меньше всех, либо больше, либо попасть между какими-то двумя. В каждом из случаев мы можем найти неохваченный элемент во втором множестве, находящийся в том же положении (больше всех, между первым и вторым охваченным сверху, между вторым и третьим охваченным сверху и т. п.).

При этом мы пользуемся тем, что у нас нет наименьшего элемента, нет наибольшего и нет соседних элементов, — в зависимости от того, какой из трёх случаев имеет место. После этого мы добавляем выбранные элементы к подмножествам, считая их соответствующими друг другу.

Чтобы в пределе получить изоморфизм между множествами $X$ и $Y$, мы должны позаботиться о том, чтобы все элементы обоих множеств были рано или поздно охвачены. Это можно сделать так:

Поскольку каждое из множеств счётно, пронумеруем его элементы и будем выбирать неохваченный элемент с наименьшим номером (на нечётных шагах — из $X$, на чётных — из $Y$ ).

Это соображение завершает доказательство. □

**Теорема 2.3.**

Всякое счётное линейно упорядоченное множество изоморфно некоторому подмножеству множества $\mathbb{Q}$.

***Доказательство.***

Делаем тоже самое, только выбираем элементы не из обоих множеств, а из первого. □

## 2.6. Билет 17 «Определение цепи, антицепи. Теорема Дилуорса»

***Определение* 2.9.**
Пусть $\langle X, \leqslant \rangle$ - ЧУМ. Цепью называется подмножество $Y \subset X$, такое, что все элементы в $Y$ попарно сравнимы.

***Определение* 2.10.**
Пусть $\langle X, \leqslant \rangle$ - ЧУМ. Цепью называется подмножество $Y \subset X$, такое, что все элементы в $Y$ попарно несравнимы.

**Теорема 2.4** (Теорема Дилуорса)**.**
Для конечного частично упорядоченного множества $X$ размер максимальной антицепи равен минимальному количеству цепей, необходимому чтобы покрыть множество.

***Доказательство*.**
Пусть $A$ - максимальная антицепь в $X$. $|A| = d$.

Покажем, что необходимо $d$ цепей для покрытия:

Пусть покрыли меньше чем $d$ цепями. Тогда, по принципу Дирихле, какая-то цепь содержит хотя-бы два элемента $A$. Но $A$ антицепь, значит они несравнимы. Противоречие.

Покажем что $X$ можно покрыть не более чем $d$ цепями:

Индукция по $|X|$. Для $|X| = 0 \implies X = \varnothing$ тривиально.

Если все элементы $X$ несравнимы, то $X = A$, и единственное все возможные цепи содержат не более одного элемента, так-что для покрытия нужно $d$ цепей.

Пусть $m$ - минимальный элемент $X$, такой, что $\exists a \in X \quad m \leqslant a$, а $M$ - максимальный элемент $S' = \{a \in X \setminus \{m\} \mid m \leqslant a\}$ (это множество точно не пустое, так-как $\exists a \in X \quad m \leqslant a$. Причём, $m \leqslant a \leqslant M \implies m \leqslant M$).

$M$ будет максимальным элементом $X$: Предположим что это не так, тоесть $\exists a \in X \quad M \leqslant a$, тогда по транзитивности $m \leqslant M \leqslant a \implies m \leqslant a \implies a \in S'$, но $M$ - максимальный элемент $S'$, значит $a \leqslant M$ невозможно.

Пусть $T = X \setminus \{m, M\}$. $|T| < |X|$, значит размер поркрытия $T$ не больше чем размер максимальной антицепи в $T$. Так-как $T \subset X$, максимальная антицепь в $T$ имеет размер $\leqslant d$. Если её размер $< d$, добавим к покрытию $T$ цепь $\{m, M\}$, и теорема доказана.

Остаётся случай, когда максимальная антицепь в $T$ имеет размер $d$.

Определим два множества:

$$X^+ = \{x \in X \mid \exists a \in A \quad a \leqslant x\}.$$

$$X^- = \{x \in X \mid \exists a \in A \quad x \leqslant a\}.$$

Заметим, что $X^+ \cup X^- = X$, ведь если какой-то элемент не входит в ни в одно из множеств, то его можно добавить в антицепь $A$, а она максимальна.

Так-же заметим, что $X^+ \cap X^- = A$, по рефлексивнсоти и антисимметричности порядка. Так-как $X^\pm \subset X$, $X^+ \cap X^- \subsetneq X$, то $X^\pm \subsetneq X$ (в $X^+$ должен быть элемент которого нет в $X^-$, значит в $X^-$ нет какого-то элемента из $X$, симметрично для $X^+$ )

Значит, $X^+$ и $X^-$ строго меньше $X$, значит для них выполняется предположение индукции. При этом, размер максимальной антицепи в них ровно $d$ ($A \subset X^\pm \subset X$), значит каждый из них можно покрыть $d$ цепями.

Каждая цепь будет содержать ровно 1 элемент из $A$ (цепь не может содержать больше одного элемента антицепи + принцип Дирихле). При этом, тот элемент будет наименьшем/наибольшим

элементов цепи (по построению множеств). Значит, объединение этих цепей будет цепью в $X$, получилось покрытие $X$ $d$ цепями. $\square$

# 3. Булева логика

## 3.1. Билет 18: «Высказывания и операции. Тавтологии.»

***Определение* 3.1.**
Определим множество «пропозициональных формул» (высказывинй) следующим образом:

- «пропозициональная переменная» является высказыванием
- Если $A$ - высказывание, то $\neg A$ (НЕ $A$) - высказывание.
- Если $A$ и $B$ - высказывания, то $A \wedge B$ ($A$ И $B$), $A \vee B$ ($A$ ИЛИ $B$), $A \to B$ (из $A$ следует $B$) - высказывания.

***Определение* 3.2.**
Пусть высказывание $A$ содержит пропозиональные переменные $x_1, \ldots, x_n$.

Соответствующий высказыванию булевой функцией называется функция $\varphi_A : \mathbb{B}^n \mapsto \mathbb{B}$, где $\mathbb{B} = \{0, 1\} = \mathbb{Z}/2$, заданная индуктивно следующим образом:

| $A$ | $B$ | $A \wedge B$ | $A \vee B$ | $A \to B$ | $\neg A$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 1 |

***Определение* 3.3.**
Тавтологией называется высказывание, соответветсвующия которому функция принимает значение 1 на всех возможных входах.

***Определение* 3.4.** $a \leftrightarrow b = (a \to b) \wedge (b \to a)$

**Пример Примеры тавтологий.**

1. $(p \wedge q) \leftrightarrow (q \wedge p)$
2. $(p \vee q) \leftrightarrow (q \vee p)$
3. $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$
4. $((p \vee q) \vee r) \leftrightarrow (p \vee (q \vee r))$
5. $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$
6. $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$
7. $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
8. $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
9. $(p \vee (p \wedge q)) \leftrightarrow p$
10. $(p \wedge (p \vee q)) \leftrightarrow p$

11. $(p \to q) \leftrightarrow (\neg q \to \neg p)$
12. $p \leftrightarrow \neg\neg p$

**Пример Тоже самое в другой нотации.**

А то об те убиться можно...

1. $pq = qp$
2. $p + q = q + p$
3. $(pq)r = p(qr)$
4. $(p + q) + r = p + (q + r)$
5. $p(q + r) = pq + pr$
6. $p + qr = (p + q)(p + r)$
7. $\overline{p \cdot q} = \overline{p} + \overline{q}$
8. $\overline{p + q} = \overline{p} \cdot \overline{q}$
9. $p + pq = p$
10. $p(p + q) = p$
11. $p \to q = \overline{q} \to \overline{p}$
12. $p = \overline{\overline{p}}$

## 3.2. Билет 19: «Выразимость любой формулы в КНФ и ДНФ»

***Определение* 3.5.**

Формула находится в конъюнктивной нормальной форме (КНФ) если она имеет вид

$$\bigwedge_{i\in\{1,\dots,n\}} \left( \bigvee_{j\in\{1,\dots,m_i\}} \ell_{k_{ij}} \right).$$

Формула находится в дизъюнктивной нормальной форме (ДНФ) если она имеет вид

$$\bigvee_{i\in\{1,\dots,n\}} \left( \bigwedge_{j\in\{1,\dots,m_i\}} \ell_{k_{ij}} \right).$$

Дизъюнктом называется формула вида

$$\bigvee_{j\in\{1,\dots,m\}} \ell_j.$$

Конъюнктом:

$$\bigwedge_{j\in\{1,\dots,m\}} \ell_j.$$

где $\ell_i$ называется литералом, и имеет вид либо $x_i$ либо $\neg x_i$.

**Пример.**

Пример КНФ: $(x_1 \vee x_2 \vee \neg x_5) \wedge (x_3 \vee x_4 \vee x_5)$

Пример ДНФ: $(x_1 \wedge x_4) \vee (x_2 \wedge x_4) \vee \neg x_3$

**Теорема 3.1.**

Любую булеву функцию можно записать в ДНФ.

***Доказательство.***

Возьмём все наборы переменных на которых функция принимает значение 1.

Каждому такому набору сопоставим конъюнкт в который входят все переменные, причём, если во входном наборе переменная имеет значение 1, то она входит как $x_i$, если имеет значение 0, то как $\neg x_i$.

Очевидно, что каждый конъюнкт примет значение 1 только на одном входе, и функция примет значение 1 если хотя-бы один конъюнкт принял значение 1.

□

**Теорема 3.2.**

Любую булеву функцию можно записать в КНФ

***Доказательство.***

Возьмём все наборы переменных на которых функция принимает значение 0.

Каждому такому набору сопоставим дизъюнкт в который переменная $x_i$ входит как литерал $x_i$ если $x_i$ имеет значение 0 и $\neg x_i$ когда $x_i$ имеет значение 1.

Заметим, что такой дизъюнкт выполняется только тогда, кодга строка не совпадает с той, которой он соответствует.

Значит, все дизъюнкты будут выполнены тогда и только тогда, когда функция не принимает значение 0, тоесть, принимает значение 1. □

## 3.3. Билет 20: «Полиномы Жегалкина»

***Определение* 3.6.**

Моном - формула вида

$$1 \wedge \left( \bigwedge_{i \in I} x_i \right).$$

**Пример.**

Примеры мономов: 1, $x_1$, $x_1 x_3$.

***Определение* 3.7.**

Полином Жегалкина - XOR (сумма в $\mathbb{Z}/2$) мономов.

| $a$ | $b$ | $a \oplus b$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

**Пример.**

Примеры полиномов Жегалкина:

$$1 \oplus x_1 \oplus x_1x_2.$$

$$x_1 \oplus x_2 \oplus x_1x_2.$$

**Теорема 3.3.**
Любую булеву функцию можно однозначно записать полиномом Жегалкина.

***Доказательство.***
Докажем существование подходящего полинома:

Выразим основные связки:

$$\neg x = 1 \oplus x$$
$$x_1 \wedge x_2 = x_1 \wedge x_2 \text{ (моном)}$$
$$x_1 \vee x_2 = x_1 \oplus x_2 \oplus x_1x_2$$

Теперь, запишем формулу в ДНФ, раскоре $\vee$, уберём повторяющиеся члены (ессли один член встречается в мономе дважды, то второе вхождение ни на что не влияет и надо оставить одно, если один моном встречается дважды, то он отменяет себя в сложении по модулю 2, и надо убрать оба вхождения).

Докажем единственность:

Всего существует $|\mathbb{B}|^{|\mathbb{B}^n|} = 2^{2^n}$ булевых функций от $n$ переменных.

Заметим, что существует $2^n$ различных мономов - каждый моном либо включает либо не включает одну из $n$ переменных.

Значит, всего существует $2^{2^n}$ различных многочленов Жегалкина от $n$ переменных. По принципу Дирихле, каждой функции соответствует ровно один многочлен, так-как существование хотя-бы одного уже доказано.

□

## 3.4. Билет 21: «Критерий Поста»

***Определение* 3.8.**
Булева функция $f$ называется сохраняющей 0, если

$$f(0, \ldots, 0) = 0.$$

Обозначим множество таких функций $T_0$.

***Определение* 3.9.**
Булева функция $f$ называется сохраняющей 1, если

$$f(1, \ldots, 1) = 1.$$

Обозначим множество таких функций $T_1$.

***Определение* 3.10.**
Булева функция $f$ называется самодвойственной, если

$$f(\neg x_1, \neg x_2, \ldots, \neg x_n) = \neg f(x_1, x_2, \ldots, x_n).$$

Обозначим множество таких функций $S$.

***Определение* 3.11.**

Булева функция $f$ называется монотонной, если

$$f(x_1, \ldots, 0, \ldots, x_n) = 1 \implies f(x_1, \ldots, 1, \ldots, x_n) = 1.$$

(замена 0 на 1 не может изменить результат с 1 на 0).

Обозначим множество таких функций $M$.

***Определение* 3.12.**

Булева функция $f$ называется линейной, если в её полиноме Жегалкина все мономы имеют не более одной переменной.

Обозначим множество таких функций $L$.

***Определение* 3.13.**

Система связок называется полной, если с её помощью можно выразить любую функцию.

**Лемма.**

$\{\neg, \wedge, \vee\}$ - полная система связок.

***Доказательство.***

Можно построить ДНФ. □

**Теорема 3.4** (Критерий Поста)**.**

Система связок $B$ полная тогда и только тогда, когда в ней для каждого из вышеперечисленных классов есть хотя-бы одна функция не входящая в него:

$$\begin{array}{ll} \exists f \in B & f \notin T_0 \\ \exists g \in B & g \notin T_1 \\ \exists h \in B & h \notin S \\ \exists k \in B & k \notin M \\ \exists r \in B & r \notin L \end{array}$$

***Доказательство.***

Необходимость: Если набор содержится в одном из классов, то и все композиции также не выходят за пределы этого класса (легко проверить для каждого из классов в отдельности) и поэтому набор не является полным.

Достаточность:

Рассмотрим функцию $f$. Если $f \in T_1$, то $f(x, \ldots, x) = 1$, иначе $f(x, \ldots, x) = \neg x$.

Рассмотрим функцию $g$. Если $g \in T_0$, то $g(x, \ldots, x) = 0$, инчае $g(x, \ldots, x) = \neg x$.

Мы либо получили $\neg$, либо получили $\{1, 0\}$.

Получим 0 или 1 из $\neg$:

Возьмём функцию $h$. Существует такой набор входов $\varepsilon_i$, что

$$h(\varepsilon_1, \ldots, \varepsilon_n) = h(\neg\varepsilon_1, \ldots, \neg\varepsilon_n).$$

Тогда $h(\varepsilon_1(x), \ldots, \varepsilon_n(x) = h(\varepsilon_1(\neg x), \ldots, \varepsilon_n(\neg x))$, где $\varepsilon_i(x)$ - $x$ если $\varepsilon_i = 1$, иначе $\neg x$.

Тогда такая функция будет константной, другую константу можно получить применив $\neg$.

Получим $\neg$ из $\{0, 1\}$:

Возьмём функцию $k$. Существует такой набор входов $\varepsilon_i$, что

$$k(\varepsilon_1, \ldots, \varepsilon_{i-1}, 0, \varepsilon_{i+1}, \ldots, \varepsilon_n) = 1.$$

$$k(\varepsilon_1, \ldots, \varepsilon_{i-1}, 1, \varepsilon_{i+1}, \ldots, \varepsilon_n) = 0.$$

Тогда $k(\varepsilon_1, \ldots, \varepsilon_{i-1}, x, \varepsilon_{i+1}, \varepsilon_n) = \neg x$.

Теперь точно есть $\{\neg, 0, 1\}$.

У функции $r$ есть хотя-бы один член состоящий из конъюнкции хотя-бы двух переменных. Пусть, без ограничения общности, в нём присутствуют переменные $x_1$, и $x_2$. Тогда

$$r(x_1, x_2, 1, \ldots, 1) = x_1 x_2 [\oplus x_1][\oplus x_2][\oplus 1].$$

Члены в квадратных скобках могут присутствтовать или отсутствовать в зависимости от формулы.

Если присутствует член $\oplus 1$, его можно убрать применив к результату $\neg$.

$$x_1 x_2 = x_1 \wedge x_2.$$

$$x_1 x_2 \oplus x_1 = x_1 \wedge \neg x_2.$$

$$x_1 x_2 \oplus x_2 = \neg x_1 \wedge x_2.$$

$$x_1 x_2 \oplus x_1 \oplus x_2 = x_1 \vee x_2 = \neg\left(\neg x_1 \wedge \neg x_2\right).$$

Заметим, что применяя $\neg$ можно из любого варианта получить $x_1 \wedge x_2$. Значит, мы выразили $\{\neg, \wedge\}$, из этого можно по правилам Де-Моргана выразить $\vee$, значит мы получили полную систему связок. □

## 3.5. Билет 22 «Определение схемы. Размер, глубина схемы»

***Определение* 3.14.**

Схема из функциональных элементов в базисе $B$ с $n$ входами размера $m$ - набор, состоящий из $n$ булевых переменных-*входов* и $m$ булевых переменных-*проводников*. При этом для каждого проводника задана функция из $B$, которая выражает его значение через другие переменные. Циклы запрещены. Один из проводников нарекаем *выходом*.

***Определение* 3.15.**

Глубина схемы - максимальное количество элементов на пути от входа к выходу.

## 3.6. Билет 23 «Теорема о размере схемы в разных базисах»

***Определение* 3.16.**

Базис полный, если любая булева функция может быть задана схемой, состоящей из B-элементов.

***Определение* 3.17.**

*Сложность* булевой функции - минимальный размер схемы, состоящей из B-элементов, которая задаёт эту функцию.

**Теорема 3.5.** $B_1, B_2$ - два полных базиса. Тогда $\exists C \in \mathbb{R} : size_{B_1}(f) \cdot C^{-1} \leq size_{B_2}(f) \leq size_{B_1}(f) \cdot C$

***Доказательство.***

Так как оба базиса полные, можем выразить функции одного базиса через другой. Тогда $C$ - максимальный размер такой схемы. □

## 3.7. Билет 24 «Теорема о наличии функций с большой схемной сложностью»

**Теорема 3.6.**

Пусть $c > 2$. Тогда сложность любой булевой функции $n$ аргументов $\leq c^n$ для всех достаточно больших $n$

***Доказательство.***

*кукарек* Извините

Размер схемы, реализующей ДНФ, с $n$ переменными есть $\mathcal{O}(n2^n)$, поскольку имеется $\leq 2^n$ конъюктов размера $\mathcal{O}(n)$

Заметим что $\mathcal{O}(n2^n) = \mathcal{O}(c^n)$, потому что $c > 2$. □

**Теорема 3.7.**

Пусть $c < 2$. Тогда сложность большинства булевых функций $n$ аргументов $\geq c^n$ для всех достаточно больших $n$

***Доказательство.***

*Замечание: выбор базиса изменяет размер не более, чем в константу раз, поэтому можно рассматривать базис* $\{\wedge, \vee, \neg\}$

Оценим число различных схем размера $N$ с $n$ аргументами. *сейчас будет птичья ферма* **много кукареков**

Каждая такая схема может быть описана последовательностью из $N$ присваиваний, выражающих одну из переменных через предыдущие. Для каждого присваивания есть не более $3(N+n)^2$ вариантов (три типа операций — конъюнкция, дизъюнкция, отрицание, и каждый из не более чем двух аргументов выбирается среди не более чем $N + n$ вариантов). Отсюда легко получить оценку $2^{\mathcal{O}(N \log N)}$ на число всех функций сложности не более $N$ (считая $N > n$). Всего булевых функций с $n$ аргументами имеется $2^{2^n}$. Из сравнения этих формул видно, что что при $c < 2$ и при достаточно больших $n$ булевы функции сложности меньше $c^n$ составляют меньшинство, так как $2^{\mathcal{O}(c^n \log c^n)}$) много меньше $2^{2^n}$ □

## 3.8. Билет 25 «Схема для сравнения чисел»

***WARNING!!! Где-то тут ушёл Игорь, а я могу ооооочень сильно ошибаться. Видите ошибки - пишите мне, пожалуйста***

Схема рекурсивная (отдельно сравниваем левые и правые половины, затем из этого получаем результат).

Будет $2n$ входов и 2 выхода.

Делим числа на 2 половины. Результат функции определяют старшие разряды, если же они равны, смотрим на младшие.

Тогда мы можем 4 бита входа (результаты сравнения половин чисел) и 2 бита выхода реализовать схемой фиксированного размера.

Тогда $T(2n) \leq 2T(n) + c$.

Тогда $T(2^k) \leq c'2^k$

Если размер чисел не степень 2 - добьём нулями.

## 3.9. Билет 26 «Схема размера $\mathcal{O}(n)$ для сложения чисел»

Для вычисления результата в каждом разряде нам нужна схема константного размера (3 бита - перенос и 2 числа - значит, фиксированное количество случаев перебрать). Тогда наша схема будет идти по числам слева направо и вычислять.

## 3.10. Билет 27 «Схема размера $\mathcal{O}(n)$ и $\mathcal{O}(\log n)$ для сложения чисел»

Вычисление битов переноса равносильно сравнению, поэтому нам достаточно научиться параллельно сравнивать все суффиксы чисел.

Результаты сравнения отрезков, длины которых равны степеням 2, нам уже известны из схемы сравнения. Комбинируя их (кусок длины 2 + кусок длины 4 = кусок длины 6), получаем остальные длины.

В общем случае картина такая: после «сужающегося дерева» мы строим «расширяющееся»; за $k$ шагов до конца мы знаем результаты сравнения всех суффиксов, длины которых кратны $2^k$. Это дерево имеет размер $\mathcal{O}(n)$ и глубину $\mathcal{O}(\log n)$

## 3.11. Билет 28 «Схема для функции голосования»

Эта схема имеет нечётное число аргументов и выдаёт тот, которого на входах больше.

На самом деле можно даже вычислить общее число единиц среди входов. Это делается рекурсивно: считаем отдельно для каждой половины, потом складываем. Получается логарифмическое число уровней. На верхнем уровне надо складывать числа размера $\log n$, на следующем — размера $(\log n - 1)$ и так до самого низа, где складываются однобитовые числа (то есть биты входа). Какой средний размер складываемых чисел? Половина вершин в дереве приходится на нижний уровень (числа длины 1), четверть — на следующий (числа длины 2) и т. д. Вспоминая, что ряд $\sum \frac{k}{2^k}$ сходится, видим, что средний размер складываемых чисел есть $\mathcal{O}(1)$ и общий размер схемы есть $\mathcal{O}(n)$. А общая глубина есть $\mathcal{O}(\log n \log\log n)$, так как на каждом из $\log n$ уровней стоит схема глубины $\mathcal{O}(\log\log n)$.

# 4. Исчисление высказываний

## 4.1. Билет 29: «Вывод. Доказательство. Исчисление высказываний»

Исчисление высказываний - формальная система, состоящия из 11 схем аксиом и одного правила вывода.

Формулы исчисления высказываний («утверждения») состоят из формальных переменных а так-же связок $\wedge$ (И), $\vee$ (ИЛИ), $\neg$ (НЕ) и $\to$ (импликация, «следует»).

***Определение* 4.1** (Аксиомы исчисления выссказываний)**.**

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $(A \wedge B) \to A$
4. $(A \wedge B) \to B$
5. $A \to (B \to (A \wedge B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
9. $\neg A \to (A \to B)$
10. $(A \to B) \to ((A \to \neg B) \to \neg A)$
11. $A \vee \neg A$

Это так называемые «схемы аксиом» - на месте $A, B, C$ могут стоять любые формулы исчисления высказываний. Аксиома всегда является теоремой.

***Определение* 4.2** (Modus ponens (MP))**.**
Если $A$ и $A \to B$ - теоремы исчисления высказываний, то $B$ - теорема исчисления высказываний.

***Определение* 4.3** (Вывод)**.**
Выводом называется конечная последовательность формул, в которой каждая либо является аксиомой, либо следует из предыдущих по MP.

***Определение* 4.4** (Вывод из множества формул)**.**
Пусть $\Gamma$ - множество из формул утверждения высказываний.

Выводом из $\Gamma$ называется конечная последовательность формул, в которой каждая либо является аксиомой, либо принадлежит $\Gamma$, либо следует из предыдущих по MP.

Формула $A$ называется выводимой из $\Gamma$ (обозначается $\Gamma \vdash A$) если существует вывод заканчивающийся формулой $A$.

***Определение* 4.5** (Доказательство)**.**
Доказательство формулы $A$ - вывод, в котором $A$ является последней формулой.

## 4.2. Билет 30: «Теорема о корректности исчисления высказываний»

**Теорема 4.1.**
Любая теорема исчисления выссказываний - тавтология.

***Доказательство.***
Не сложно проверить, что все аксиомы - тавтологии.

Докажем корректность MP от противного:

Знаем, что $A$ и $A \to B$ - тавтологии, предположим что $B$ - нет. Возьмём означивание на котором $B$ неверно. Тогда, $A$ верно а $B$ неверно, значит $A \to B$ неверно. Но $A \to B$ - тавтология, значчит оно верно. Противориче. Значит, $B$ - тавтология.

Таким образом, все начальные утверждения - тавтологии, MP сохраняет свойство тавтологии, значит, все теоремы - тавтологии. □

## 4.3. Билет 31: «Теорема о полноте исчисления высказываний»

### 4.3.1. Схема доказательства

- Теорема о полноте
  1. Если $B$ выводится с добавлением либо $A$ либо не $\neg A$ (в обоих случаях), то $B$ выводится без дополнений.
  2. Если булева формула истинна на наборе переменных, то она выводится из истинности соответствующих литералов
     (a) $\{\wedge, \vee, \to, \neg\}$ выводятся из аргументов по таблице истинности
        – Лемма о дедукции для работы с понятием «выводится из»
          i. $D \to D$ - ТИВ
          ii. В одну сторону - добавляем формулу в вывод и MP
          iii. В другую - превращем каждую формулу $C_i$ в выводе в формулу $(A \to C_i)$, и префиксируем её выводом (разбор случаев: $C_i = A$, $C_i \in \Gamma$, $C_i$ - аксиома и $C_i$ выводится из предыдущих (этот самый сложный, через аксиому 2)).
     (b) Индукция по построению

### 4.3.2. Доказательство

Докажем сначала несколько вспомогательных лемм:

**Лемма.**
Для любой формулы $D$, $D \to D$ - ТИВ (теорема исчисления высказываний).

***Доказательство.***

1. Аксиома 2 $(A \to (B \to C) \to ((A \to B) \to (A \to C)))$:
   $\underbrace{D}_{A} \to (\underbrace{(D \to D)}_{B} \to \underbrace{D}_{C}) \to ((\underbrace{D}_{A} \to \underbrace{(D \to D)}_{B}) \to (\underbrace{D}_{A} \to \underbrace{D}_{C}))$
2. Аксиома 1 $(A \to (B \to A))$:
   $\underbrace{D}_{A} \to (\underbrace{(D \to D)}_{B} \to \underbrace{D}_{A})$

3. MP от 1 и 2: $(D \to (D \to D)) \to (D \to D)$
4. Аксиома 1: $A \to (B \to A)$:
   $\underbrace{D}_{A} \to (\underbrace{D}_{B} \to \underbrace{D}_{A})$
5. MP от 3 и 4: $D \to D$ □

**Лемма** (О дедукции (DT))**.**

Пусть $\Gamma \vdash A$ означает «существует вывод формулы $A$ из множества $\Gamma$»

Тогда $\Gamma \vdash (A \to B) \iff \Gamma \cup \{A\} \vdash B$.

***Доказательство.***

Необходимость ( $\Longrightarrow$ ):

Если $\Gamma \vdash (A \to B)$, то и $\Gamma \cup \{A\} \vdash (A \to B)$. Тогда, возьмём вывод формулы $A \to B$ из $\Gamma$, добавим к нему утверждение $A$ (можем добавить, так-как входит в множество из котрого выводим), применим MP к последним двум утвержденям, получим $B$. Значит, существует вывод $B$.

Достаточность ( $\Longleftarrow$ ):

Возьмём вывод формулы $B$ из множества $\Gamma \cup \{A\}$, назовём его $C_i$, заметим, что $C_n = B$.

Тогда, выводом формулы $A \to B$ из $\Gamma$ будет $B_1, (A \to C_1), B_2(A \to C_2), \ldots, B_n, (A \to C_n)$. Тогда, последняя формула - $(A \to B)$.

$B_i$ - такие последовательности, которые позволяют добавлять формулы $(A \to C_i)$ в вывод. Разберём случаи:

1. $C_i = A$ : формула $A \to A$ выводима по предыдущей лемме, тогда $B_i$ - её вывод из аксиом (кроме последней формулы, место котрой займёт сама формула $A \to A$).
2. $C_i \in \Gamma$, либо $C_i$ - аксиома: через аксиому 1: $B_i = C_i, C_i \to (A \to C_i)$. Тогда, $A \to C_i$ получается через MP.
3. $C_i$ выводится из предыдущих по MP: тогда, в оригинальном выводе были формулы $C_j$, $C_j \to C_i$. Значит, в новом выводе будут формулы $A \to C_j$, $A \to (C_j \to C_i)$. выведем из них $A \to C_i$:
   (a) посылка 1: $A \to C_j$
   (b) посылка 2: $A \to (C_j \to C_i)$
   (c) аксиома 2 $((A \to (B \to C)) \to ((A \to B) \to (A \to C))$:
   $(\underbrace{A}_{A} \to (\underbrace{C_j}_{B} \to \underbrace{C_i}_{C})) \to ((\underbrace{A}_{A} \to \underbrace{C_j}_{B}) \to (\underbrace{A}_{A} \to \underbrace{C_i}_{C}))$
   (d) MP от b и c: $(A \to C_j) \to (A \to C_i)$
   (e) MP от a и d: $A \to C_i$.

   Тогда $B_i = a, b, c, d$.

Получили вывод формулы $A \to B$ из множества $\Gamma$. □

**Лемма.**

Следующие утверждения - ТИВ для любых формул $P, Q$:

1. (a) $P, Q \vdash (P \wedge Q)$
   (b) $\neg P, Q \vdash \neg(P \wedge Q)$
   (c) $P, \neg Q \vdash \neg(P \wedge Q)$
   (d) $\neg P, \neg Q \vdash \neg(P \wedge Q)$
2. (a) $P, Q \vdash (P \vee Q)$
   (b) $\neg P, Q \vdash (P \vee Q)$
   (c) $P, \neg Q \vdash (P \vee Q)$
   (d) $\neg P, \neg Q \vdash \neg(P \vee Q)$
3. (a) $P, Q \vdash (P \to Q)$
   (b) $\neg P, Q \vdash (P \to Q)$
   (c) $P, \neg Q \vdash \neg(P \to Q)$
   (d) $\neg P, \neg Q \vdash (P \to Q)$
4. (a) $P \vdash \neg(\neg P)$
   (b) $\neg P \vdash \neg P$

***Доказательство.***

**TODO:** Надеюсь его не надо...Тут просто куча тупых выводов. □

**Лемма.**

Если формула $A$ интерпретированная как булева формула принимает истинное значение при истинности литералов $\ell_1, \ldots, \ell_n$ (если $x$ - формальная переменная, то литерал это либо $x$ либо $\neg x$), то верно что $\ell_1, \ldots, \ell_n \vdash A$, если-же она принимает ложное значение, то верно что $\ell_1, \ldots, \ell_n \vdash \neg A$

***Доказательство.***

Доказательство по индукции. Пусть $\Gamma = \{\ell_1, \ldots, \ell_n\}$.

Будем предпалогать что $A$ принимает истинное значение, для ложного доказательство симметрично ( **TODO:** или надо?).

Если $A$ состоит из одной формальной переменной $x_i$, то раз $A$ истинно, то $x_i$ истинно и присутствует в множестве формул. По лемме мы знаем, что $x_i \to x_i$, и, соответственно $x_i \vdash x_i \implies \Gamma \vdash x_i$.

Если $A = \neg B$, то раз $A$ истинно, то $B$ ложно, значит верно $\Gamma \vdash \neg B$, но $\neg B = A$.

Если $A = B \wedge C$, то раз $A$ истинно, то $B$ и $C$ истинны, значит $\Gamma \vdash B$ и $\Gamma \vdash C$.

1. Вывод 1: $B$
2. Вывод 2: $C$
3. Аксиома 5: $B \to C \to (B \wedge C)$
4. MP 1 и 3: $C \to (B \wedge C)$
5. MP 2 и 4: $B \wedge C$

Если $A = B \vee C$, то раз $A$ истинно то либо $\Gamma \vdash B$ либо $\Gamma \vdash C$. В зависимости от случая, берём либо аксиому 6 либо аксиому 7 и применяем MP. □

**Лемма.**
Для любых формул $A$ и $B$, если $\Gamma \cup \{A\} \vdash B$ и $\Gamma \cup \{\neg A\} \vdash B$, то $\Gamma \vdash B$.

***Доказательство.***
Можем переформулировать теорему с помощью DT как $\{(A \to B), (\neg A \to B)\} \vdash B$

1. посылка 1: $A \to B$
2. посылка 2: $\neg A \to B$
3. аксиома 8 $((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$:
   $(\underbrace{A}_{A} \to \underbrace{B}_{C}) \to ((\underbrace{\neg A}_{B} \to \underbrace{B}_{C}) \to ((\underbrace{A}_{A} \vee \underbrace{\neg A}_{B}) \to \underbrace{B}_{C}))$
4. MP от 1 и 3: $(\neg A \to B) \to ((A \vee \neg A) \to B)$
5. MP от 2 и 4: $(A \vee \neg A) \to B$
6. Аксиома 11: $A \vee \neg A$
7. MP от 5 и 6: $B$ □

**Теорема 4.2.**
Любая тавтология - теорема исчисления высказываний.

***Доказательство.***
Пусть $A$ - тавтология. Тогда она верна на всех наборах литералов.

Возьмём наборы $x_1, \ldots, x_{n-1}, x_n$ и $x_1, \ldots, x_{n-1}, \neg x_n$. На обоих наборах формула истинна, а значит выводится из них.

Но раз она выводится из них, то она выводится из $x_1, \ldots, x_{n-1}$. Аналлогично, она выводится из $x_1, \ldots, \neg x_{n-1}$. Можем повторить $n$ раз, и получить $\varnothing \vdash A$, значит $A$ - ТИВ. □

## 4.4. Билет 32: «Теорема о корректности исчисления высказываний (вторая форма)»

***Определение* 4.6.**
Формула $A$ называется выполнимой, если сущесвует означивание переменных при котором формула $A$ истинна.

***Следствие.***
Формула $A$ тавтология тогда и только тогда, когда $\neg A$ невыполнима.

***Определение* 4.7.**
Множество формул $\Gamma$ называется совместным, если существует означивание переменных при котором все формулы в $\Gamma$ выполнены одновременно

***Определение* 4.8.**
Множество формул $\Gamma$ называется противоречивым если верно $\Gamma \vdash A$ и $\Gamma \vdash \neg A$.

***Следствие.***
Если $\Gamma$ - противоречивое множество, то для любой формулы $B$ верно $\Gamma \vdash B$

***Доказательство.***

1. Посылка 1: $A$
2. Посылка 2: $\neg A$
3. Аксиома 9: $\neg A \to (A \to B)$
4. MP от 2 и 3: $A \to B$
5. MP от 1 и 4: $B$ □

**Теорема 4.3** (Корректность исчисления высказываний (вторая форма))**.**
Любое совместное множество формул непротиворечиво

***Доказательство.***
Пусть $\Gamma$ совместное. Предположим что оно противоречиво.

Тогда $\Gamma \vdash A$ и $\Gamma \vdash \neg A$.

Если все формулы из $\Gamma$ выполняются на каком-то означивании, то и все выводимы из $\Gamma$ формулы выполняются на этом означивании (доказывается индукцией по построению формулы) ( **TODO:** у меня ощущение что на экзе за такое убьют, но в книге ничё больше не написано...).

Значит, должны выполняться одновременно $A$ и $\neg A$. Но такое невозможно, значит $\Gamma$ непротивочво. □

***Следствие.***
Любая теорема исчисления высказыванний - тавтология.

***Доказательство.***
Пусть $A$ - ТИВ. Тогда $\{\neg A\} \vdash A$. Значит, $\{\neg A\}$ противоречиво, а значит несовместно. Значит $A$ - тавтология. □

## 4.5. Билет 33: «Теорема о полноте исчисления высказываний (вторая форма)»

***Определение* 4.9.**
Пусть $V(\Gamma)$ - множество всех формальных переменных участвующих в формулах $\Gamma$.

**Предполагаем что $V(\Gamma)$ не более чем счётно.**

***Определение* 4.10.**
Непротиворечивое множество $\Gamma$ называется полным, если для любой формулы $F$ над переменными из $V(\Gamma)$ верно либо $\Gamma \vdash F$ либо $\Gamma \vdash \neg F$

**Лемма.**
Если $\Gamma$ непротиворечиво, а $\Gamma \cup \{A\}$ противоречиво, то $\Gamma \vdash \neg A$

***Доказательство.***
**TODO:** Книга утверждает что трвивально... □

**Лемма.**
Если $\Gamma$ непротиворечиво, то либо $\Gamma \cup \{A\}$ либо $\Gamma \cup \{\neg A\}$ непротиворечиво.

***Доказательство.***
Прдеположим что оба противоречивы. Тогда $\Gamma \vdash \neg A$ и $\Gamma \vdash \neg(\neg A)$. Но $\Gamma$ непротиворечиво. □

**Лемма.**

Для любого непротиворечивого множества $\Gamma$ существует такое непротиворечивое полное множество $\Delta$, что $\Gamma \subset \Delta$.

***Доказательство.***

$V(\Gamma)$ конечно или счётно, значит формул над $V(\Gamma)$ счётно. Пронумеруем их.

Будем последовательно добавлять либо $F$ либо $\neg F$ к $\Gamma$, в зависимости от того, что будет непротиворечивым.

В результате бесконечного процесса получим полное множество.

Заметим, что оно непротиворечиво: Предположим что не так, $\Gamma \cup X \vdash A$, $\Gamma \cup X \vdash \neg A$. Но так-как вывод $A$ и $\neg A$ содержит только конечно число членов, можно выбрать такое конечное $n$, что после добавления $n$ формул, оба этих вывода возможны. Но тогда противоречиво какое-то конечное количество шагов процесса, сохраняющего непротиворечивость на каждом шаге. □

**Лемма.**

Для любого полного непротиворечивого множества $\Delta$ существует означивание переменных из $V(\Delta)$, при котором все формулы из $\Delta$ истинны.

***Доказательство.***

Для любой переменной $p \in V(\Delta)$, либо $\Delta \vdash p$ либо $\Delta \vdash \neg p$.

Пусть $P = \{p \mid p \in V(\Delta), \quad \Delta \vdash p\} \cup \{\neg p \mid p \in V(\Delta), \quad \Delta \vdash \neg p\}$.

$P$ соответсвует нужному означиванию. При этом, $\Delta \vdash P$. Значит, если $\Delta \cup P$ противоречиво, что $\Delta$ противоречиво, что невозможно. Значит, при означивании $P$ выполняются все формулы в $\Delta$. □

**Теорема 4.4** (Полнота исчисления высказываний (вторая форма))**.**

Любое непротиворечивое множество совместно.

***Доказательство.***

Пусть $\Gamma$ - непротиворечивое множество. Возьмём полное непротиворечивое множество $\Delta$, такое, что $\Gamma \subset \Delta$. Оно совместно, значит и $\Gamma$ совместно. □

***Следствие.***

Любая тавтология - ТИВ.

***Доказательство.***

Пусть $A$ - тавтология. Тогда $\{\neg A\}$ несовместно. Значит оно противоречиво. Значит, $\varnothing \vdash \neg\neg A$, значит $\varnothing \vdash A$. □

## 4.6. Билет 34 «Теорема о компактности. Прмимер с бесконечным двудольным графом.»

**Теорема 4.5** (Теорема о компактности исчисления выссказываний)**.**

Пусть $\Gamma$ - множество формул, каждое конечное подмножество совместно. Тогда $\Gamma$ совместно.

***Доказательство.***

$\Gamma$ совместно если оно непротиворечиво.

Предположим что $\Gamma$ противоречиво.

Рассмотрим выводы формул $A$ и $\neg A$.

Они содержат лишь конечное число формул, значит существует противоречивое конечное подмножество. Но оно не может быть совместным. Противоречие. □

**Теорема 4.6.**

Бесконечный граф двудолен тогда и только тогда, когда каждый конечный подграф двудолен.

***Доказательство.***

Необходимость очевидна: Если есть недвудольный подграф, то в нём есть нечётный цикл, и этот цикл есть в самом графе.

Достаточность:

Сопоставим каждой вершине графа формальную переменную. Каждому ребру $i \to j$ сопоставим утверждение $(\neg x_i \wedge x_j) \vee (x_i \wedge \neg x_j)$.

Множество таких утверждений совместно, если граф двудолен. По теореме о компактности, достаточно проверить только для конечных множеств формул.

Для каждого подмножества $\Gamma'$ возьмём граф содерижащий рёбра соответствующие этим утверждениям, и все инцидентные им вершины. Этот подграф конечем, значит двудолен, значит $\Gamma'$ совместно. □