

Коллоквиум по дискретной математике №1

10 декабря 2022

Содержание

1	Определения и обозначения	3
1.1	Принцип математической индукции. Принцип полной математической индукции. Принцип наименьшего числа.	3
1.2	Множества, теоретико-множественные операции. Парадокс Рассела.	3
1.3	Бинарные отношения, композиция отношений.	4
1.4	Функции (как частный случай отношений). Образы и прообразы множеств. Обратная функция.	4
1.5	Виды функций: инъекции, сюръекции и биекции.	4
1.6	Отношения эквивалентности. Классы эквивалентности.	4
1.7	Бином Ньютона. Сумма и знакопеременная сумма биномиальных коэффициентов.	4
1.8	Сочетания с повторениями. Количество решений уравнения $x_1 + x_2 + \dots + x_k = n$ в неотрицательных целых числах.	5
1.9	Полиномиальные коэффициенты. Их алгебраический и комбинаторный смысл.	5
1.10	Формулы, полные системы связей, примеры. Дизъюнктивная нормальная форма, СДНФ.	5
1.11	Полином Жегалкина. Теорема о представлении булевой функции полиномом Жегалкина.	6
1.12	Класс линейных функций, лемма о нелинейной функции.	6
1.13	Принцип двойственности, класс самодвойственных функций, лемма о несамодвойственной функции.	6
1.14	Класс монотонных функций, лемма о немонотонной функции.	6
1.15	Критерий Поста полноты системы булевых функций.	6
1.16	Предполные классы	6
1.17	Формула включений–исключений	6
1.18	Равномощные множества. Счетные и континуальные множества. Примеры.	7
1.19	Сравнение мощностей, теорема Кантора.	7
1.20	Теорема Кантора–Бернштейна.	7
1.21	Частично упорядоченные множества: строгий и нестрогий частичные порядки, их связь, линейный порядок	7
1.22	Операции с частично упорядоченными множествами: сумма порядков, покоординатный порядок, лексикографический порядок.	7
1.23	ЛУМ-лемма, теорема Шпернера о размере максимальной антицепи в булевом кубе.	8
1.24	Ориентированные и неориентированные графы. Степени вершин. Лемма о рукопожатиях. Понятия пути, цикла, простого пути, простого цикла.	8
1.25	Отношение достижимости и компоненты связности графа. Неравенство, связывающее число вершин, ребер и компонент связности в графе. Компоненты сильной связности ориентированного графа.	9
1.26	Деревья. Теорема об эквивалентных определениях дерева.	9
1.27	Полное двоичное дерево. Остовное дерево в графе.	9
1.28	Ациклические орграфы, топологическая сортировка.	9
1.29	Эйлеровы циклы в ориентированных и неориентированных графах. Критерий существования эйлерова цикла.	10
1.30	Двудольные графы, критерий двудольности графа. Булев куб.	10
1.31	Теорема Холла.	10
1.32	Паросочетания. Вершинные покрытия. Теорема Кёнига.	10
1.33	Теорема Рамсея. Верхняя оценка чисел Рамсея.	10
2	Доказательства	11
2.1	Применения метода математической индукции: существование 2-цветной раскраски областей на плоскости; неравенство Бернулли; сумма обратных квадратов меньше 2	11
2.2	Эквивалентность принципа математической индукции, принципа полной индукции и принципа наименьшего числа	11
2.3	Числа сочетаний: явная и рекуррентная формула. Треугольник Паскаля. Рекуррентное соотношение для чисел сочетаний. Бином Ньютона. Сумма биномиальных коэффициентов. Знакопеременная сумма биномиальных коэффициентов.	12

2.4	Сочетания с повторениями. Количество решений уравнения $x_1 + x_2 + \dots + x_n = k$ в неотрицательных целых числах.	13
2.5	Полиномиальные коэффициенты. Их алгебраический и комбинаторный смысл.	13
2.6	Формулы, полные системы связок. Полнота системы связок «конъюнкция, дизъюнкция, отрицание». Дизъюнктивная нормальная форма, СДНФ.	14
2.7	Полнота системы связок «XOR, конъюнкция, 1». Теорема о представлении булевой функции полиномом Жегалкина (существование и единственность).	14
2.8	Класс линейных функций, лемма о нелинейной функции. Классы функций, сохраняющих константу. Лемма о функции, не лежащей в классе, сохраняющем константу.	14
2.9	Принцип двойственности, класс самодвойственных функций, лемма о несамодвойственной функции. Класс монотонных функций, лемма о немонотонной функции.	15
2.10	Формула включений-исключений	16
2.11	Подмножество счетного множества конечно или счетно. Во всяком бесконечном множестве есть счетное подмножество. Объединение конечного или счётного числа конечных или счётных множеств конечно или счётно. Декартово произведение конечного числа счетных множеств счетно. Счетность множества конечных последовательностей натуральных чисел.	16
2.12	Если множество A бесконечно, а множество B конечно или счётно, то множество $A \cup B$ равномощно A . Равномощность множеств: бесконечных последовательностей из 0 и 1; вещественных чисел; $[0, 1]$; $[0, 1)$; множества всех подмножеств натуральных чисел. Равномощность отрезка и квадрата.	17
2.13	Несчетность множества бесконечных последовательностей из 0 и 1. Сравнение мощностей, теорема Кантора о сравнении мощности множества и множества всех его подмножеств.	19
2.14	Теорема Кантора – Бернштейна.	19
2.15	ЛУМ-лемма, теорема Шпернера о размере максимальной антицепи в булевом кубе.	19
2.16	Эйлеровы циклы в ориентированных и неориентированных графах. Критерий существования эйлерова цикла.	20
2.17	Двудольные графы, критерий двудольности графа. Пример: булев куб.	21
2.18	Теорема Холла.	22
2.19	Паросочетания. Вершинные покрытия. Теорема Кёнига	22
2.20	Теорема Рамсея. Верхняя оценка чисел Рамсея.	23
3	Задачи из листков	24

1 Определения и обозначения

1.1 Принцип математической индукции. Принцип полной математической индукции. Принцип наименьшего числа.

- Принцип математической индукции:

Пусть есть некоторое утверждение A зависящее от $n \in \mathbb{N}$, которое может быть либо верным, либо ложным, и выполняются следующие условия:

1. $A(1)$ верно (База индукции)
2. $\forall n : A(n) - \text{верно} \Rightarrow A(n+1) \text{ верно.}$ (Шаг индукции)

То $\forall n : A(n) - \text{верно.}$

- Принцип математической индукции (эквивалентная формулировка):

Пусть $S \subseteq \mathbb{N}$ и выполняются следующие условия:

1. $1 \in S$
2. $\forall n \in \mathbb{N} : n \in S \Rightarrow n+1 \in S$

Тогда $S = \mathbb{N}$.

- Принцип полной математической индукции:

Пусть есть некоторое утверждение A зависящее от $n \in \mathbb{N}$, которое может быть либо верным, либо ложным, и выполняются следующие условия:

1. $A(1)$ верно
2. $\forall n : (\forall k < n A(k) - \text{верно}) \Rightarrow A(n+1) \text{ верно.}$

То $\forall n : A(n) - \text{верно.}$

- Принцип наименьшего числа

Пусть $S \subseteq \mathbb{N}$, $S \neq \emptyset \Rightarrow$ в S существует минимальный элемент.

Минимальным элементом множества A называют такое число c , что $\forall a \in A : c \leq a$

1.2 Множества, теоретико-множественные операции. Парадокс Рассела.

- **Определение и некоторые обозначения**

Множеством называют совокупность произвольных объектов

$$X = \{a, b, c\}$$

$a \in X$ – объект a лежит в множестве, $d \notin X$ – объект d не лежит в множестве

Способы задания множества:

1. Явно (списком элементов): $X = \{1, 2, 3\}$
2. Условием: $Y = \{y \in \mathbb{N} \mid y - \text{четно}\}$

\emptyset – пустое множество

2^A – множество всех подмножеств A (в том числе пустое и само A)

- **Операции над множествами**

Пусть A, B – множества. Тогда:

Объединение множеств: $A \cup B = \{x \mid x \in A \vee x \in B\}$

Пересечение множеств: $A \cap B = \{x \mid x \in A \wedge x \in B\}$

Разность множеств: $A \setminus B = \{x \in A \mid x \notin B\}$

Дополнение множества A до B : $\bar{A} = B \setminus A$

Симметрическая разность: $A \triangle B = \{x \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}$

$A \subseteq X \Leftrightarrow \forall x(x \in A \Rightarrow x \in X)$. A – подмножество, X – надмножество.

$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$.

- **Парадокс Рассела**

$$U = \{x \mid x \notin x\}.$$

Вопрос: $U \in U$?

Если да, то по определению U , $U \notin U$. Если нет, то т.к. $U \notin U$, U является элементом себя же. Противоречие.

1.3 Бинарные отношения, композиция отношений.

Бинарное отношение R на множестве $A \times B$ – это $R \subseteq A \times B$ такое, что если $x \in A, y \in B$ и $(x, y) \in R$, элементы находятся в отношении ($R(x, y) = 1, xRy$)

Пример: $\mathbb{R} \times \mathbb{R}, x < y$ – отношение.

Композиция отношений

Пусть $R \subseteq A \times B, S \subseteq B \times C$. Тогда $(S \circ R) \subseteq A \times C: (a, c) \in S \circ R \Leftrightarrow \exists b \in B : (a, b) \in R, (b, c) \in S$ (aRb и bSc).

1.4 Функции (как частный случай отношений). Образы и прообразы множеств. Обратная функция.

Функция f из A в B – это такое отношение $f \subseteq A \times B$, что $\forall a \in A$ в f есть не более одной пары (a, b) , где $b \in B$. Обозначение: $(a, b) \in f$ или $afb \Leftrightarrow f(a) = b$.

Мы рассматриваем частичные функции, то есть они не полностью определены на A . Но

f на A и B тотальна, если $Dom f = A$ (функция определена на всем множестве A). Тогда пишут $f : A \rightarrow B$.

Запись $f : A \rightarrow B$ с подвохом: мы подразумеваем при подобной записи что f тотальна, однако это может быть не так вне нашего курса, будьте бдительны.

Если $X \subseteq A$, то $f(X) = \{b \in B | \exists x \in X : f(x) = b\}$ – **образ** множества A .

Прообраз множества $Y \subseteq B$ $f^{-1}(Y) = \{a \in A | f(a) \in Y\}$.

Пример: $f : \mathbb{R} \rightarrow \mathbb{R} f(x) = x^2$

$f^{-1}(\{0, 1\}) = \{-1, 0, 1\}$

$f(\{0, 1\}) = \{0, 1\}$

Пусть $f : A \rightarrow B$ – биекция. Тогда $f^{-1} : B \rightarrow A$ или **обратная функция к f** определяется как $f^{-1}(b) = a \Leftrightarrow f(a) = b$.

1.5 Виды функций: инъекции, сюръекции и биекции.

Функция $f : A \rightarrow B$ называется инъекцией, если $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

Функция $f : A \rightarrow B$ называется сюръекцией, если $\forall y \in B \exists x, f(x) = y$ (область значений функции есть все множество B).

Функция $f : A \rightarrow B$ называется биекцией, если она одновременно и инъекция, и сюръекция.

1.6 Отношения эквивалентности. Классы эквивалентности.

Отношение R на A называют:

Рефлексивным, если $\forall a \in A, aRa$.

Симметричным, если $\forall a, b \in A, (aRb \Leftrightarrow bRa)$.

Транзитивным, если $\forall a, b, c, (aRb \text{ и } bRc \Rightarrow aRc)$.

Пример: отношение $a < b$ транзитивно, но не рефлексивно и не симметрично. Отношение $a + b = a * b$ симметрично, но не рефлексивно и не транзитивно.

Отношение R на A называют **отношением эквивалентности**, если отношение R рефлексивно, симметрично и транзитивно.

Пример: Отношение $a = b$: рефлексивно ($a = a \forall a \in A$), симметрично ($a = b \Rightarrow b = a \forall a, b \in A$), транзитивно ($a = b, b = c \Rightarrow a = c \forall a, b, c \in A$).

Если R на A – отношение эквивалентности, то множество A можно разбить на классы эквивалентности A_i

Классы эквивалентности – это разбиение множества A отношением эквивалентности R на непересекающиеся классы ($A_i \cap A_j = \emptyset \forall i \neq j, \bigcup_{i \in I} A_i = A$) такое, что $\forall x, y \in A_i xRy$ и $\forall x \in A_i, y \in A_j, i \neq j, \neg xRy$. (то есть если два элемента принадлежат одному классу эквивалентности, они находятся в отношении R и наоборот).

1.7 Бином Ньютона. Сумма и знакочередующаяся сумма биномиальных коэффициентов.

Биномом Ньютона называют формулу для разложения n -й ($n \in \mathbb{N}$) степени суммы двух переменных, а именно:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

Где $\binom{n}{k}$ – число сочетаний без повторений из n по k . Также их называют биномиальными коэффициентами и могут обозначать C_n^k . Верны следующие равенства:

$$\sum_{k=0}^n C_n^k = 2^n$$

$$\sum_{k=0}^n (-1)^k C_n^k = 0$$

1.8 Сочетания с повторениями. Количество решений уравнения $x_1 + x_2 + \dots + x_k = n$ в неотрицательных целых числах.

- Сочетание с повторениями

Сочетанием с повторениями из n элементов по k называют неупорядоченный k -элементный набор, в котором количество каждого элемента может быть произвольным. Их количество обозначается \bar{C}_n^k и равно:

$$\bar{C}_n^k = \binom{n+k-1}{k}$$

- Количество решений уравнения $x_1 + x_2 + \dots + x_k = n, x_i \geq 0, x_i \in \mathbb{Z}$

Замечу, что здесь и в доказательстве количество переменных обозначено k , а сумма n , в отличие от списка билетов (там наоборот).

Количество решений равно $\binom{n+k-1}{n}$

1.9 Полиномиальные коэффициенты. Их алгебраический и комбинаторный смысл.

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{\alpha_1 + \alpha_2 + \dots + \alpha_k = n} \binom{n}{\alpha_1, \dots, \alpha_k} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}$$

Где $\binom{n}{\alpha_1, \alpha_2, \dots, \alpha_k} = \frac{n!}{\alpha_1! \alpha_2! \dots \alpha_k!}$. Это число называют полиномиальным коэффициентом.

Собственно алгебраический смысл - коэффициенты разложения суммы $(x_1 + x_2 + \dots + x_k)^n$.

Комбинаторный смысл - полиномиальный коэффициент равен числу упорядоченных разбиений n -элементного множества на k подмножеств размеров (мощностей) $\alpha_1, \alpha_2, \dots, \alpha_k$

1.10 Формулы, полные системы связок, примеры. Дизъюнктивная нормальная форма, СДНФ.

Связка - это любая булева функция. Вроде как точно связку не определяют, тем не менее, под связками понимают именно булевы функции

Пример множества связок: $F = \{\neg, \wedge, \vee\}$.

Пусть F это множество связок. Тогда, функция $f : \{0, 1\}^n \rightarrow \{0, 1\}$ **выразима в системе связок F** , если \exists формула φ под данной системой F (или f можно выразить через функции системы связок F):

$$\forall (x_1, \dots, x_n) \in \{0, 1\}^n : f(x_1, \dots, x_n) = \varphi(x_1, \dots, x_n)$$

Формула φ строится последовательно:

1. Переменная x_i сама по себе является формулой
2. Переменная $g(\varphi_1, \dots, \varphi_n)$, где $g \in F$ и $\varphi_1, \varphi_2, \dots, \varphi_n$ формулы - тоже формула.
3. Если $\varphi(x_1, x_2, \dots, x_n)$ - формула, то $\varphi(x_1, x_2, \dots, x_n, x_{n+1})$ тоже формула (где x_{n+1} фиктивная переменная, так мы умеем расширять количество аргументов у формулы).

Константы по умолчанию не являются формулами, их надо выражать из связок.

$[F]$ - множество всех булевых функций, выражимых в F (или **замыкание F**)

F - **полная система связок**, если $[F]$ - все булевы функции (P_2).

Пусть $x^a = x$ если $a = 1$ и $\neg x$ если $a = 0$. Тогда:

Конъюнкт - $x_1^{a_1} \wedge x_2^{a_2} \wedge \dots \wedge x_k^{a_k}$

Дизъюнктивная Нормальная Форма (ДНФ) - представление функции $f(x_1, x_2, \dots, x_n)$ как дизъюнкции конъюнктов.

Пример: для функции $(A \vee B) \wedge (C \vee \neg D)$, ДНФ - $A^1 \wedge C^1 \vee A^1 \wedge D^0 \vee B^1 \wedge C^1 \vee B^1 \wedge D^0$

1.11 Полином Жегалкина. Теорема о представлении булевой функции полиномом Жегалкина.

Моном – это выражение вида $x_{i_1} \wedge x_{i_2} \wedge x_{i_k}$.
(0 и 1 – тоже мономы)

Полином Жегалкина – многочлен вида
$$\bigoplus_{(i_1, \dots, i_k), k=0 \dots n} a_{i_1 \dots i_k} x_{i_1} \wedge x_{i_2} \wedge x_{i_k}$$

Пример: $1 \oplus (x \wedge y) \oplus (x \wedge y \wedge z)$

Теорема о представлении булевой функции полиномом Жегалкина: каждую булеву функцию можно однозначно представить в виде полинома Жегалкина.

1.12 Класс линейных функций, лемма о нелинейной функции.

Функция f называется линейной, если $f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$, где $a_i \in \{0, 1\}$

$L = \{f \in P_2 \mid f \text{ – линейная}\}$ – множество всех линейных функций.

Пример: $x_i \in L, x \oplus y \in L, 0, 1 \in L$

$x \wedge y \notin L, x \vee y \notin L$

Лемма о нелинейной функции: Пусть $f(x_1, \dots, x_n) \notin L$. Тогда подставив вместо переменных функции x_1, \dots, x_n 0, x и y можно получить $g(x, y) \notin L$.

Иначе говоря, через любую не линейную функцию на n переменных можно выразить не линейную функцию на двух переменных.

1.13 Принцип двойственности, класс самодвойственных функций, лемма о несамодвойственной функции.

Принцип двойственности:

Пусть $f(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$. Тогда:

$$f^*(x_1, \dots, x_n) = f_0^*(f_1^*(x_1, \dots, x_n), \dots, f_k^*(x_1, \dots, x_n))$$

Функция $f \in P_2$ называется самодвойственной, если $f^* = f$.

$S = \{f \in P_2 \mid f^* = f\}$ – множество всех самодвойственных функций.

Пример: $x \in S, \neg x \in S, x \oplus y \oplus z \in S$

Лемма о несамодвойственной функции:

Пусть $f(x_1, \dots, x_n) \notin S$. Тогда подставляя вместо переменных функции $x, \neg x$, можно получить константу.

1.14 Класс монотонных функций, лемма о немонотонной функции.

Для того, чтобы ввести класс монотонных функций нам нужно ввести понятие порядка на множестве наборов переменных. Скажем, что изначально $0 < 1$. Тогда:

Набор $(\alpha_1, \dots, \alpha_n)$ меньше $(\beta_1, \dots, \beta_n)$, если $\forall i, \alpha_i \leq \beta_i$.

Пример: $(1, 0) \leq (1, 1)$

$(1, 0) \not\leq (0, 1)$ (не сравнимы)

$(0, 1) \not\leq (1, 0)$ (не сравнимы)

$f \in P_2$ **монотонная**, если $\forall \alpha_i, \beta_i, \alpha_i \leq \beta_i \Rightarrow f(\alpha) \leq f(\beta)$

Лемма о немонотонной функции:

Пусть $f(x_1, \dots, x_n) \notin M$. Тогда, подставляя вместо переменных 0, 1, x , можно получить $\neg x$.

1.15 Критерий Поста полноты системы булевых функций.

Критерий Поста: $[F] = P_2 \Leftrightarrow F \notin L, F \notin T_0, F \notin T_1, F \notin S, F \notin M$

Иначе говоря, система связок полная тогда и только тогда, когда для любого класса L, S, T_0, T_1, M в системе связок F есть функция, не лежащая в этом классе.

1.16 Предполные классы

Пусть $F \subseteq P_2$ – замкнутый класс ($[F] = F$)

F – предполный в P_2 , если $F \neq P_2$, но $\forall g \notin F [F \cup g] = P_2$.

1.17 Формула включений–исключений

Пусть A_1, A_2, \dots, A_n – конечные множества. Тогда:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{k=1}^n \sum_{1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}|$$

1.18 Равномощные множества. Счетные и континуальные множества. Примеры.

Равномощные множества. Множества A и B называются равномощными, если $\exists f : A \rightarrow B$ - биекция. $|A| = |B|, A \sim B$

Счетное множество - множество равномощное множеству натуральных чисел \mathbb{N} .

Континуальное множество - множество равномощное множеству действительных чисел \mathbb{R} .

Примеры.

1. $\mathbb{N} \sim \mathbb{N} \cup \{0\}, f(n) = n - 1$
2. $(0, 1) \sim (0, 2), f(x) = 2x$
3. $[a, b] \sim [c, d]$

1.19 Сравнение мощностей, теорема Кантора.

Сравнение мощностей.

$|A| \leq |B|$, если $\exists f : A \rightarrow B$ - инъекция.

$|A| < |B|$, если $A \leq B$ и $A \not\sim B$.

Теорема Кантора:

Пусть X - множество.

Тогда $|X| < |2^X|$.

1.20 Теорема Кантора–Бернштейна.

Пусть $|A| \leq |B|$ и $|A| \geq |B|$, тогда $A \sim B$.

1.21 Частично упорядоченные множества: строгий и нестрогий частичные порядки, их связь, линейный порядок

Говорят, что бинарное отношение R , определенное на множестве P , является **строгим частичным порядком**, если для него выполнены такие свойства:

1. $\forall a \in P, \neg aRa$ (антирефлексивность)
2. $\forall a, b, c \in P, aRb, bRc \Rightarrow aRc$ (транзитивность)

Из транзитивности и антирефлексивности следует то, что отношения строгого порядка не обладают свойством симметричности (aRb и bRa не может выполняться, т.к. тогда по транзитивности $aRb, bRa \Rightarrow aRa$, что противоречит антирефлексивности)

Обычно отношения строгого порядка обозначают как $<$.

Говорят, что бинарное отношение R , определенное на множестве P , является **нестрогим частичным порядком**, если для него выполнены такие свойства:

1. $\forall a \in P, aRa$ (рефлексивность)
2. $\forall a, b \in P, aRb$ и $bRa \Rightarrow a = b$ (антисимметричность)
3. $\forall a, b, c \in P, aRb, bRc \Rightarrow aRc$ (транзитивность)

Обычно отношения нестрогого порядка обозначают как \leq

Связь строгого и нестрогого частичных порядков: Из отношения не строгого порядка на P можно получить отношение строгого порядка на P и наоборот следующим образом

$$\begin{aligned} a \leq b &\Leftrightarrow a < b \text{ или } a = b \\ a < b &\Leftrightarrow a \leq b \text{ и } a \neq b \end{aligned}$$

Множество P называется **частично упорядоченным**, если на нем определен порядок R .

Обозначается как $(P, <_P)$ или (P, \leq_P) для строгого и нестрогого порядков соответственно.

Линейный порядок – это такой порядок (P, \leq_P) , что для любых элементов $x, y \in P$, $x \leq y$ или $y \leq x$. Иначе говоря, в линейном порядке любые два элемента сравнимы.

1.22 Операции с частично упорядоченными множествами: сумма порядков, покомпонентный порядок, лексикографический порядок.

Пусть $(P, \leq_P), (Q, \leq_Q)$ – частично упорядоченные множества. Тогда:

Покомпонентный порядок – это такое частично упорядоченное множество $(P \times Q, \leq_{P \times Q})$, что $(p_1, q_1) \leq_{P \times Q} (p_2, q_2) \Leftrightarrow p_1 \leq_P p_2$ и $q_1 \leq_Q q_2$.

Лексикографический порядок – это такое частично упорядоченное множество $(P \times Q, <_{lex})$, что $(p_1, q_1) <_{lex} (p_2, q_2) \Leftrightarrow p_1 <_P p_2$ или $p_1 = p_2$ и $q_1 <_Q q_2$

Сумма порядков. Определим для множеств P, Q таких, что $P \cap Q = \emptyset$. Пусть $P + Q = P \cup Q$. Тогда на $(P + Q, \leq)$ определен порядок такой, что:

$$x \leq y \Leftrightarrow \begin{cases} x, y \in P, x \leq_P y \\ x, y \in Q, x \leq_Q y \\ x \in P, y \in Q \end{cases}$$

1.23 ЛУМ-лемма, теорема Шпернера о размере максимальной антицепи в булевом кубе.

Отношение порядка на булевом кубе. Вершины булева куба - двоичные слова, тогда, если слово x является подсловом y (с точки зрения единиц), то $x \leq y$ (покоординатное сравнение).

ЛУМ-лемма, или LYM-inequality. Дан булев куб, пусть A в нем - антицепь, a_k - количество элементов в антицепи, в которых ровно k единиц. Тогда утверждается, что выполнено:

$$\sum_{k=0}^n \frac{a_k}{C_n^k} \leq 1$$

Теорема Шпернера. Длина максимальной антицепи в булевом кубе равна $C_n^{\lfloor \frac{n}{2} \rfloor}$.

1.24 Ориентированные и неориентированные графы. Степени вершин. Лемма о рукопожатиях. Понятия пути, цикла, простого пути, простого цикла.

Неориентированный граф - пара множества вершин и множества ребер.

$$G = (V, E), |V| < \infty.$$

$$E \subseteq \{a, b | a, b \in V, a \neq b\}$$

Ориентированный граф - пара множества вершин и множества ребер.

$$G = (V, E), |V| < \infty.$$

$$E \subseteq \{(a, b) | a, b \in V, a \neq b\}$$

Степень вершины - количество ребер исходящих из вершины.

Для неориентированного графа:

$$\deg(v) = |\{e \in E | v \in e\}|$$

Для ориентированного графа:

$$\deg_+(v) = |\{(v, a) \in E | a \in V\}|$$

$$\deg_-(v) = |\{(b, v) \in E | b \in V\}|$$

Лемма о рукопожатиях

Для неориентированного графа:

$$\sum_{v \in V} \deg(v) = 2|E|$$

Для ориентированного графа:

$$\sum_{v \in V} \deg_+(v) = \sum_{v \in V} \deg_-(v) = |E|$$

Смежные вершины. Вершины v_1, v_2 называются смежными, если $\exists e \in E : e = \{v_1, v_2\}$.

Путь - последовательность смежных вершин. $(v_1, v_2, v_3, \dots, v_n)$

Простой путь - путь, в котором все вершины различны.

Цикл - путь, у которого первая и последняя вершины одинаковы.

Простой цикл - путь, у которого совпадают только первая и последняя вершины, длины больше или равной 3.

Длина пути - количество вершин в пути - 1.

1.25 Отношение достижимости и компоненты связности графа. Неравенство, связывающее число вершин, ребер и компонент связности в графе. Компоненты сильной связности ориентированного графа.

Отношение достижимости. Вершина u достижима из вершины v , если \exists путь из v в u . Так же говорят, что вершины v и u - связны ($u \sim v$). Отношение достижимости называют отношением связности.

Отношение сильной связности. u и v - сильно связны, если \exists ориентированный путь $u \rightarrow v$ и \exists ориентированный путь $v \rightarrow u$.

Компонента связности графа. Так как отношение связности является отношением эквивалентности, то множество вершин можно разбить на компоненты - компоненты связности.

Неравенство, связывающее число вершин, ребер и компонент связности в графе.

Количество компонент связности $\geq |V| - |E|$

Компоненты сильной связности ориентированного графа. Так как отношение сильно связности является отношением эквивалентности, то множество вершин ориентированного графа можно разбить на компоненты - компоненты сильной связности.

1.26 Деревья. Теорема об эквивалентных определениях дерева.

Эквивалентные определения дерева:

1. G - минимальный связный граф
2. G - связен и $|E| = |V| - 1$
3. в G между любыми 2 вершинами $\exists!$ простой путь
4. G - связен и в нем нет простых циклов

Обычно дерево обозначают через T .

Предки - все вершины на пути от корня до вершины, не включая саму вершину.

Потомок - вершина, которая не является предком.

Лист - вершина степени 1.

1.27 Полное двоичное дерево. Остовное дерево в графе.

Полное двоичное дерево - дерево, где каждой вершине можно присвоить булевый кортеж и тогда все вершины будут представимы в виде $\bigcup_{k=0}^n \{0,1\}^k$. Тогда ребра будут между вершинами a_1, \dots, a_k и a_1, \dots, a_k, a_{k+1} .

В полном двоичном дереве 2^n листьев.

Остовное дерево в графе. Дан граф $G = (V, E)$. Тогда остовное дерево в G - это $T = (V, E'), E' \subseteq E, T$ - дерево.

1.28 Ациклические орграфы, топологическая сортировка.

Ациклический орграф - орграф, в котором нет циклов.

Топологическая сортировка. Эквивалентные определения:

1. Орграф G - ацикличесен.
2. Все компоненты сильной связности G состоят из 1 вершины.
3. Все вершины G можно пронумеровать числами от 1 до n : если $i \rightarrow j$, то $i < j$.

1.29 Эйлеровы циклы в ориентированных и неориентированных графах. Критерий существования эйлерова цикла.

Цикл (в неориентированном или ориентированном графе) называется эйлеровым, если он проходит по всем рёбрам графа ровно по одному разу (любое ребро соединяет соседние вершины в цикле, и никакое ребро не делает это дважды).

Граф называется эйлеровым, если в нём есть эйлеров цикл.

Есть простой критерий эйлеровости графов и орграфов. Прежде всего заметим, что добавление и удаление изолированных вершин, то есть тех вершин, из которых не выходит и в которые не входит ни одного ребра, не изменяет свойство эйлеровости графа.

Теорема 1. В ориентированном графе без изолированных вершин существует эйлеров цикл тогда и только тогда, когда граф сильно связан и у любой вершины входящая степень равна исходящей.

Теорема 2. Неориентированный граф без вершин нулевой степени содержит эйлеров цикл тогда и только тогда, когда он связан и степени всех вершин чётны.

1.30 Двудольные графы, критерий двудольности графа. Булев куб.

Двудольным графом называется неориентированный граф, в котором вершины можно разделить на две доли — левую и правую, и все рёбра соединяют вершины из разных долей (нет рёбер, соединяющих вершины одной доли). Другими словами, чтобы задать двудольный граф, надо указать два конечных множества L (левую долю) и R (правую долю) и указать, какие вершины левой доли соединены с какими вершинами правой доли.

Критерий двудольности графа. Граф является двудольным тогда и только тогда, когда не содержит в себе циклы нечётной длины.

Булев куб размерности n — это неориентированный граф, вершинами которого являются двоичные слова длины n , а рёбра соединяют слова, отличающиеся в одной позиции.

1.31 Теорема Холла.

Теорема Холла. Если для каждого множества X вершин двудольного графа $G = (L, R, E)$ множество соседей $G(X) \subseteq R$ содержит не меньше, чем $|X|$ вершин, то в графе G есть паросочетания размера $|L|$.

1.32 Паросочетания. Вершинные покрытия. Теорема Кёнига.

Пусть дан граф $G = (V, E)$, **паросочетание** M в G — это множество попарно несмежных рёбер, то есть рёбер, не имеющих общих вершин.

Вершинным покрытием называется такое множество вершин S , что для любого ребра хотя бы один из концов лежит в S . Нетрудно проверить, что дополнение к вершинному покрытию — независимое множество и, наоборот, дополнение к независимому множеству — вершинное покрытие. Для двудольных графов вершинные покрытия оказываются связанными с паросочетаниями.

Теорема Кёнига. В любом двудольном графе максимальный размер паросочетания равен минимальному размеру вершинного покрытия.

1.33 Теорема Рамсея. Верхняя оценка чисел Рамсея.

Теорема Рамсея. Для любых k, n найдётся такое число N_0 , что в любом графе на $N \geq N_0$ вершинах есть или клика размера k , или независимое множество размера n . Минимальное такое N_0 называют **числом Рамсея**, обозначается $R(k, n)$.

2 Доказательства

2.1 Применения метода математической индукции: существование 2-цветной раскраски областей на плоскости; неравенство Бернулли; сумма обратных квадратов меньше 2

- Существование 2-цветной раскраски областей на плоскости

- Утверждение: n прямых делят плоскость на области. $A(n)$ - верно ли, что эти области можно раскрасить в 2 цвета так, чтобы никакие две соседние области не были покрашены в один цвет.

- База:

- Шаг: пусть $A(n)$ - верно, докажем верность $A(n+1)$:

По сути нам дана правильная раскраска плоскости в случае n прямых. Утверждается, что если при добавлении $n+1$ прямой инвертировать цвет всех областей по одну сторону от нее, то мы получим правильную раскраску. Докажем, что любая граница разделяет области разных цветов. Для этого рассмотрим 2 случая:

1. Граница принадлежит какой-либо из старых n прямых. Тогда области, которые она разделяет, лежат по одну сторону от новой прямой. Поэтому поскольку старая раскраска была правильной, то в новой они также будут разного цвета.
2. Граница принадлежит новой $n+1$ прямой. Тогда области, что она разделяет, в старой раскраске были одного цвета, мы инвертируем только одну из них, поэтому получаем 2 разных цвета.

Таким образом $A(n+1)$ верно \Rightarrow индукция верна \Rightarrow исходное утверждение верно.

- Неравенство Бернулли

- Утверждение: $A(n)$ - верно ли, что $(1+x)^n \geq 1+xn$, $x \in \mathbb{R}, x > -1$

- База: $A(1)$: $(1+x)^1 \geq 1+x \cdot 1 \Leftrightarrow 0 \geq 0 \Rightarrow$ база верна

- Шаг: пусть $A(n)$ - верно, докажем верность $A(n+1)$:

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x) \geq (1+xn)(1+x) \geq \\ &\geq (1+xn) + x = 1 + x(n+1)\end{aligned}$$

Таким образом $A(n+1)$ верно \Rightarrow индукция верна \Rightarrow исходное утверждение верно.

- Сумма обратных квадратов меньше 2

- Утверждение: $A(n)$ - верно ли, что $\sum_{k=1}^n \frac{1}{k^2} \leq 2 - \frac{1}{n}$

- База: $A(1)$: $\sum_{k=1}^1 \frac{1}{k^2} = \frac{1}{1} = 1 \leq 2 - 1 \Rightarrow$ база верна

- Шаг: пусть $A(n)$ - верно, докажем верность $A(n+1)$:

$$\sum_{k=1}^{n+1} \frac{1}{k^2} \leq 2 - \frac{1}{n} + \frac{1}{n+1} = 2 - \frac{n^2 + n + 1}{n(n+1)^2} \leq 2 - \frac{n(n+1)}{n(n+1)^2} = 2 - \frac{1}{n+1}$$

Таким образом $A(n+1)$ верно \Rightarrow индукция верна \Rightarrow исходное утверждение верно. Так как $\frac{1}{n} > 0$ получаем:

$$\sum_{k=1}^n \frac{1}{k^2} \leq 2 - \frac{1}{n} < 2$$

2.2 Эквивалентность принципа математической индукции, принципа полной индукции и принципа наименьшего числа

1. ПМИ (принцип математической индукции)

2. ППМИ (принцип полной математической индукции)

3. ПНЧ (принцип наименьшего числа)

Докажем следствия по циклу (из утверждения 1 следует утверждение 2, из $2 \Rightarrow 3$, из $3 \Rightarrow 1$), тогда эквивалентность каждой пары будет доказана.

- ПМИ \Rightarrow ППМИ

Пусть $S \subseteq \mathbb{N}$

$\forall n : (\forall k < n, k \in S) \Rightarrow n \in S$

$X = \{n \mid \forall k < n, k \in S\}$

$1 \in X$

$n \in X \Rightarrow n \in S$

$n \in X \Rightarrow n + 1 \in X \Rightarrow n + 1 \in S$

Тогда по индукции $S = \mathbb{N}$, значит ПМИ \Rightarrow ППМИ, ч.т.д.

- ППМИ \Rightarrow ПНЧ

Рассмотрим $S \subseteq \mathbb{N}$, $S \neq \emptyset$.

Докажем от противного. Пусть в S нет минимального элемента.

$\bar{S} = \mathbb{N} \setminus S = \{n \in \mathbb{N} \mid n \notin S\}$.

Тогда $1 \in \bar{S}$ и $\forall n : (\forall k < n, k \in \bar{S}) \Rightarrow n \in \bar{S}$

По ППМИ получаем $\bar{S} = \mathbb{N} \Rightarrow S = \emptyset \Rightarrow$ противоречие \Rightarrow , значит ППМИ \Rightarrow ПНЧ, ч.т.д.

- ПНЧ \Rightarrow ПМИ

Пусть $S = \{n \in \mathbb{N} \mid A(n) - \text{ложное}\}$ Рассмотрим 2 случая:

1. $S = \emptyset \Rightarrow \forall n \in \mathbb{N} : A(n) - \text{верно}$, ч.т.д.

2. $S \neq \emptyset \Rightarrow \exists \min S$. Обозначим $m = \min S$

Но тогда $m - 1 \notin S \Rightarrow A(m - 1) - \text{верно}$

Но при этом $A(m) - \text{верно} \Rightarrow m \notin S \Rightarrow$ противоречие, значит ПНЧ \Rightarrow ПМИ, ч.т.д.

2.3 Числа сочетаний: явная и рекуррентная формула. Треугольник Паскаля. Рекуррентное соотношение для чисел сочетаний. Бином Ньютона. Сумма биномиальных коэффициентов. Знакопеременная сумма биномиальных коэффициентов.

- Число размещений

$$A_n^k = \frac{n!}{(n-k)!}$$

Количество способов извлечь первый элемент равно n . Удалим его из множества. Количество затем извлечь из оставшихся $n - 1$ объекта второй элемент равно $n - 1$. Продолжим эту процедуру пока не извлечем k элементов. (на последнем шаге количество способов будет равно $n - k + 1$). Применим правило умножения и получим, что количество способов извлечь k произвольных элементов (что и есть неупорядоченный k -элементный набор элементов) из n -элементного множества равно $A_n^k = n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot (n - k + 1) = \frac{n!}{(n-k)!}$.

- Число сочетаний явная формула

$$C_n^k = \frac{n!}{(n-k)!k!}$$

Выпишем все сочетания. Далее заменим каждое на всевозможные его перестановки (то есть $\{a_1, a_2, \dots, a_{k-1}, a_k\} \rightarrow \{\{a_1, a_2, \dots, a_{k-1}, a_k\}, \{a_1, a_2, \dots, a_k, a_{k-1}\}, \dots, \{a_k, a_{k-1}, \dots, a_1\}\}$). Получим всевозможные размещения. Количество способов переставить сочетание размера k равно $k!$ (так как все элементы различные). Таким образом получим $A_n^k = C_n^k \cdot k! \Rightarrow C_n^k = \frac{A_n^k}{k!} = \frac{n!}{(n-k)!k!}$.

- Число сочетаний рекуррентная формула

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

Обозначим первый элемент n -элементного множества за a . Любое сочетание размера k из этого множества либо содержит его, либо не содержит. Число сочетаний размера k не содержащих a равно числу сочетаний размера k из $(n - 1)$ -элементного множества, то есть C_{n-1}^k . Число сочетаний размера k содержащих a равно числу сочетаний размера $(k - 1)$ из $(n - 1)$ -элементного множества, то есть C_{n-1}^{k-1} . В итоге получим:

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

- Бином Ньютона

$$(a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

Очевидно, что $(a+b)^n = \underbrace{(a+b)(a+b)\dots(a+b)}_n$. Пусть мы взяли a из k скобок и b из остальных $n-k$ скобок.

Получим слагаемое вида $a^k b^{n-k}$. Количество способов взять такое слагаемое равно количеству способов выбрать k скобок из которых мы возьмем a (так как если нам известно из каких скобок мы возьмем a , нам известно из каких скобок мы возьмем b). Это количество равно числу сочетаний размера k из n -элементного множества, то есть слагаемое $a^k b^{n-k}$ войдет в итоговое разложение C_n^k раз. Получим:

$$(a+b)^n = C_n^0 \cdot a^0 \cdot b^n + C_n^1 \cdot a^1 \cdot b^{n-1} + \dots + C_n^n \cdot a^n \cdot b^0 = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

- Сумма биномиальных коэффициентов

$$\sum_{k=0}^n C_n^k = 1^0 \cdot 1^n \cdot C_n^0 + 1^1 \cdot 1^{n-1} \cdot C_n^1 + \dots + 1^n \cdot 1^0 \cdot C_n^n = (1+1)^n = 2^n$$

- Знакопеременная сумма биномиальных коэффициентов

$$\sum_{k=0}^n (-1)^k C_n^k = (-1)^0 \cdot 1^n \cdot C_n^0 + (-1)^1 \cdot 1^{n-1} \cdot C_n^1 + \dots + (-1)^n \cdot 1^0 \cdot C_n^n = (-1+1)^n = 0^n = 0$$

2.4 Сочетания с повторениями. Количество решений уравнения $x_1 + x_2 + \dots + x_n = k$ в неотрицательных целых числах.

- Сочетания с повторениями

Обозначим исходное множество за $\{a_1, a_2, \dots, a_n\}$. Пусть у нас есть сочетание с повторениями размера k из этого множества. Сопоставим ему следующую последовательность 0 и 1:

$$\underbrace{1\dots 1}_{{cnt}_{a_1}} 0 \underbrace{1\dots 1}_{{cnt}_{a_2}} 0 \dots \underbrace{1\dots 1}_{{cnt}_{a_n}} 0$$

где cnt_{a_i} - количество элементов a_i в сочетании.

Теперь заметим несколько фактов:

1. Длина такой последовательности равна $n+k-1$, так как сумма всех cnt_{a_i} равна размеру сочетания, то есть k , а количество нулей равно $n-1$.
2. Такое отображение будет биективным, так как два разных сочетания переходят в разные последовательности (если два сочетания не равны, то они различаются хотя бы в одной позиции. Возьмем первую такую позицию, пусть в первом сочетании там стоит a , а во втором b . Тогда при построении двоичной последовательности после $\min(a, b)$ единиц в одной последовательности последует 0, а в другой 1, следовательно не равны) и для любой подходящей последовательности найдется соответствующее ей сочетание.

Поскольку между множествами существует биекция, их мощности равны. Значит количество сочетаний с повторениями равно количеству двоичных последовательностей вышеуказанного вида. А оно равно C_{n+k-1}^k , так как выбрав позиции единиц, мы однозначно можем восстановить позиции нулей. То есть $\overline{C}_n^k = C_{n+k-1}^k$, ч.т.д.

- Количество решений уравнения $x_1 + x_2 + \dots + x_k = n, x_i \geq 0, x_i \in \mathbb{Z}$

Для начала решим аналогичную задачу, но с ограничим $x_i \geq 1$. Применим метод шаров и перегородок. Пусть у нас есть n шаров, расположенных в линию и мы поставили между ними $k-1$ перегородку, причем никакие две перегородки не идут подряд (то есть не разделяют одинаковые пары шаров). Тогда пусть x_i это будет количество шаров до i -й перегородки. Понятно, что тогда выполняется условие $\sum_{i=1}^k x_i = n$. То есть количество решений уравнений сводится к количеству способов расставить перегородки в такой модели. У нас есть $(n-1)$ позиция куда мы можем поставить перегородку и их количество равно $(k-1)$, значит число способов равно C_{n-1}^{k-1} , ч.т.д.

2.5 Полиномиальные коэффициенты. Их алгебраический и комбинаторный смысл.

$$\binom{n}{\alpha_1, \dots, \alpha_k} = \frac{n!}{\alpha_1! \alpha_2! \dots \alpha_k!}$$

Очевидно, что $(x_1 + x_2 + \dots + x_k)^n = \underbrace{(x_1 + \dots + x_k)(x_1 + \dots + x_k) \dots (x_1 + \dots + x_k)}_n$. Пусть из α_i скобок мы выбрали x_i . Получим слагаемое $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}$, причем $\alpha_1 + \alpha_2 + \dots + \alpha_k = n$. Тогда количество способов его выбрать равно произведению количеств способов выбрать каждый x_i . Получим:

$$\binom{n}{\alpha_1, \dots, \alpha_k} = C_n^{\alpha_1} \cdot C_{n-\alpha_1}^{\alpha_2} \cdot C_{n-\alpha_1-\alpha_2}^{\alpha_3} \cdot \dots \cdot C_{n-\alpha_1-\alpha_2-\dots-\alpha_k}^{\alpha_k} =$$

$$= \frac{n!}{\alpha_1!(n-\alpha_1)!} \cdot \frac{(n-\alpha_1)!}{\alpha_2!(n-\alpha_1-\alpha_2)!} \cdot \frac{(n-\alpha_1-\alpha_2)!}{\alpha_3!(n-\alpha_1-\alpha_2-\alpha_3)!} \cdot \dots \cdot \frac{(n-\alpha_1-\dots-\alpha_{k-1})!}{\alpha_k!(n-\alpha_1-\dots-\alpha_k)!} =$$

$$= \frac{n!}{\alpha_1!} \cdot \frac{1}{\alpha_2!} \cdot \dots \cdot \frac{1}{\alpha_k!} = \frac{n!}{\alpha_1!\alpha_2!\dots\alpha_k!}$$

2.6 Формулы, полные системы связок. Полнота системы связок «конъюнкция, дизъюнкция, отрицание». Дизъюнктивная нормальная форма, СДНФ.

Теорема 4.6: $\{\neg, \wedge, \vee\}$ – полная система связок

Доказательство:

Выразим функции f , равные единице только на одном конкретном наборе. Пусть такая функция $f(x_1, x_2, \dots, x_n)$ равна единице на наборе a_1, a_2, \dots, a_n . Тогда $f = y_1 \wedge y_2 \wedge \dots \wedge y_n$, где $y_i = \neg x_i$, если $a_i = 0$ и $y_i = x_i$ иначе.

Обозначим за $x^a = x$ если $a = 1$ и $\neg x$ если $a = 0$.

То есть $f_{a_1, a_2, \dots, a_n}(x_1, \dots, x_n) = x_1^{a_1} \wedge x_2^{a_2} \wedge \dots \wedge x_n^{a_n}$ – функция, которая принимает 1 только на наборе a_1, a_2, \dots, a_n .

Пусть f принимает 1 на некоторых наборах.

$$\text{Тогда } f = \bigvee_{(a_1, \dots, a_n) \in \{0,1\}^n: f(a_1, a_2, \dots, a_n)=1} f_{a_1, a_2, \dots, a_n} = \bigvee_{(a_1, \dots, a_n): f(a)=1} x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$$

Частный случай: тождественный ноль, мы можем его выразить как $x_1 \wedge \neg x_1$.

Вообще, такое представление функции имеет название СДНФ или совершенная дизъюнктивная нормальная форма.

2.7 Полнота системы связок «XOR, конъюнкция, 1». Теорема о представлении булевой функции полиномом Жегалкина (существование и единственность).

2.8 Класс линейных функций, лемма о нелинейной функции. Классы функций, сохраняющих константу. Лемма о функции, не лежащей в классе, сохраняющем константу.

Замкнутость класса линейных функций $[L] = L$

Доказательство: Индукция по построению формулы:

Пусть $f_0(y_1, \dots, y_k), f_1, f_2, \dots, f_k \in L$. Докажем, что $f_0(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)) = g \in L$. Вспомним, что $g = a_0 \oplus a_1 f_1 \oplus a_2 f_2 \oplus \dots \oplus a_k f_k$. Подставим f_i , раскроем скобки, приведем подобные и получим линейную функцию. Получается, что $g \in L$.

Утверждение $L = [\oplus, 1]$

Доказательство: по определению линейной функции.

Лемма о нелинейной функции: Пусть $f(x_1, \dots, x_n) \notin L$. Тогда подставив вместо переменных функции x_1, \dots, x_n 0, x и y можно получить $g(x, y) \notin L$.

Доказательство: $f(x_1, \dots, x_n) = \dots \oplus (x_{i_1} \wedge x_{i_2} \wedge \dots \wedge x_{i_k}) \dots$

Рассмотрим в многочлене Жегалкина мономы с количеством переменных $r \geq 2$: $x_{i_1} \wedge x_{i_2} \wedge \dots \wedge x_{i_r}$. Подставим в x_{i_1} x , а во все остальное y .

$$g(x, y) = x \wedge y \oplus ax \oplus by \oplus c \notin L.$$

Следствие: Пусть $f \notin L$. Тогда $x \wedge y \in \{0, \neg x, f\}$

Доказательство: $g(x, y) = xy \oplus ax \oplus by \oplus c \in \{0, f\}$

Рассмотрим $g(x \oplus b, y \oplus a) = (x \oplus b) \wedge (y \oplus a) \oplus a(x \oplus b) \oplus b(y \oplus a) \oplus c = xy \oplus xa \oplus by \oplus ab \oplus ax \oplus ab \oplus by \oplus ab = xy \oplus ab \oplus c$. Если $ab \oplus c = 0$, то все хорошо и мы получили xy . Иначе $\neg g(x \oplus b, y \oplus a) = xy$.

Класс $T_0 = \{f \in P_2 | f(0, \dots, 0) = 0\}$

Класс $T_1 = \{f \in P_2 | f(1, \dots, 1) = 1\}$

($f \in T_0$ – функция, сохраняющая ноль; $f \in T_1$ – функция, сохраняющая единицу).

Замкнутость классов функций, сохраняющих константу. $[T_0] = T_0$, $[T_1] = T_1$

Доказательство:

Пусть $f_0, f_1, \dots, f_k \in T_0$. Тогда $f_0(f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)) \in T_0$ так, как $f_0(f_1(0, \dots, 0), f_2(0, \dots, 0), \dots, f_k(0, \dots, 0)) = 0$. Аналогично доказывается и для T_1 .

Лемма о функции, не лежащей в классе, сохраняющем константу.

1. Если $f \notin T_0$, тогда $f(x, \dots, x) = \{1, \neg x\}$. (т.к. для $f(0, \dots, 0)$ мы точно знаем что значение равно 1, а для $f(1, \dots, 1)$ множество будет содержать в себе все возможные значения f).

2. Если $f \notin T_1$, тогда $f(x, \dots, x) = \{0, \neg x\}$ (аналогично).

2.9 Принцип двойственности, класс самодвойственных функций, лемма о несамодвойственной функции. Класс монотонных функций, лемма о немонотонной функции.

Класс S

Лемма о принципе двойственности:

Пусть $f(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$. Тогда: $f^*(x_1, \dots, x_n) = f_0^*(f_1^*(x_1, \dots, x_n), \dots, f_k^*(x_1, \dots, x_n))$

Доказательство:

$$\begin{aligned} f^*(x_1, \dots, x_n) &= \neg f(f_1^*(\neg x_1, \dots, \neg x_n), \dots, f_k^*(\neg x_1, \dots, \neg x_n)) = \\ &= \neg f_0(\neg f_1^*(x_1, \dots, x_n), \dots, \neg f_k^*(x_1, \dots, x_n)) = f_0^*(f_1^*(x_1, \dots, x_n), \dots, f_k^*(x_1, \dots, x_n)) \end{aligned}$$

Следствие $[S] = S$

Доказательство: $x_i \in S$

$$f_0, \dots, f_k \in S \Rightarrow f_0(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)) = g(x_1, \dots, x_n) \in S$$

$g^* = g$ по принципу двойственности.

Лемма о несамодвойственной функции:

Пусть $f(x_1, \dots, x_n) \notin S$. Тогда подставляя вместо переменных функции $x, \neg x$, можно получить константу.

Доказательство:

Пусть $f(x_1, \dots, x_n) \neq \neg f(\neg x_1, \dots, \neg x_n)$. Тогда есть какой-то набор $\alpha_1, \dots, \alpha_n \in \{0, 1\}^n$ такой, что: $f(\alpha_1, \dots, \alpha_n) = f(\neg \alpha_1, \dots, \neg \alpha_n)$. Подставим вместо единиц в этом наборе x и вместо нулей $\neg x$. Таким образом, получили новую функцию g от одной переменной. Для неё будет справедливо следующее: $g(1) = f(\alpha_i) = f(\neg \alpha_i) = g(0)$.

Класс M

Для того, чтобы ввести класс монотонных функций нам нужно ввести понятие порядка. Скажем, что изначально $0 < 1$. Тогда: **набор** $(\alpha_1, \dots, \alpha_n)$ **меньше** $(\beta_1, \dots, \beta_n)$, если $\forall i, \alpha_i \leq \beta_i$.

Пример: $(1, 0) \leq (1, 1)$
 $(1, 0) \not\leq (0, 1)$ (не сравнимы)

$(0, 1) \not\leq (1, 0)$ (не сравнимы)

$f \in P_2$ - монотонная, если $\forall \alpha_i, \beta_i : \alpha_i \leq \beta_i \Rightarrow f(\alpha) \leq f(\beta)$

Лемма о замкнутости класса монотонных функций. $[M] = M$

Доказательство: $x_i \in M_i$

$f_0, \dots, f_k \in M, g(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$. Пусть $\alpha = (\alpha_1, \dots, \alpha_n) \leq (\beta_1, \dots, \beta_n) = \beta$. Тогда $\forall 1 \leq i \leq k, f_i(\alpha) \leq f_i(\beta) \Rightarrow f_0(f_i(\alpha)) \leq f_0(f_i(\beta))$.

Лемма о немонотонной функции:

Пусть $f(x_1, \dots, x_n) \notin M$. Тогда, подставляя вместо переменных 0, 1, x , можно получить $\neg x$.

Доказательство: $\exists \alpha = (\alpha_1, \dots, \alpha_n), \exists \beta = (\beta_1, \dots, \beta_n)$ такие, что $\alpha \leq \beta$, но при этом $f(\alpha) = 1, f(\beta) = 0$ (т.к функция $\notin M$).

Построим новую функцию $g(x)$, полученная в результате подставления в x_i значения 0, 1 и x . Рассмотрим две группы индексов i :

1. $\alpha_i = \beta_i$. Тогда поставим в x_i значение α_i .

2. $\alpha_i = 0, \beta_i = 1$. Тогда поставим в x_i переменную x .

При подстановке в x значения 1 получим значение $g(1) = f(\beta) = 0$. При подстановке в x значения 0 получим значение $g(0) = f(\alpha) = 1$. Получим то, что нам было нужно.

2.10 Формула включений-исключений

2.11 Подмножество счетного множества конечно или счетно. Во всяком бесконечном множестве есть счетное подмножество. Объединение конечного или счётного числа конечных или счётных множеств конечно или счётно. Декартово произведение конечного числа счетных множеств счетно. Счетность множества конечных последовательностей натуральных чисел.

Подмножество счетного множества конечно или счетно.

Пусть B - счетно. $A \subseteq B$, тогда A - счетно или конечно.

Доказательство:

Так как B - счетно, то занумеруем все элементы из B и выпишем их в ряд. Теперь вычеркнем все элементы из $B \setminus A$.

$$B : b_1, b_2, b_3, b_4, \dots, b_5, b_6, \dots$$

Остались только элементы из A и это все элементы A , значит мы занумеровали все элементы из A . Чтд

Во всяком бесконечном множестве есть счетное подмножество.

Если A - бесконечное множество, то $\exists B \subseteq A$, что B - счетно.

Доказательство:

$$\exists a_1 \in A \Rightarrow B_1 = \{a_1\}$$

$$\exists a_2 \in A \setminus B_1 \Rightarrow B_2 = \{a_1, a_2\}$$

$$\exists a_3 \in A \setminus B_2 \Rightarrow B_3 = \{a_1, a_2, a_3\}$$

...

$$\exists a_k \in A \setminus B_{k-1} \Rightarrow B_k = \{a_1, a_2, \dots, a_k\}$$

$$B = \bigcup_{i=1}^{\infty} B_i, \text{ очевидно, что } B \text{ - счетно. Чтд}$$

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

Пусть нам дано не более чем счетное количество множеств $A_1, A_2, \dots, A_n, \dots$. Тогда докажем, что их объединение - не более, чем счетно.

Доказательство:

Выпишем в столбец все множества A_1, A_2, \dots , так можно, так как их не более чем, счетно. В строку выпишем элементы этих множеств.

$$\begin{array}{c|cccc} A_1 & a_{11} & a_{12} & a_{13} & \dots \\ A_2 & a_{21} & a_{22} & a_{23} & \dots \\ A_3 & a_{31} & a_{32} & a_{33} & \dots \\ \vdots & \dots & \dots & \dots & \ddots \end{array}$$

Теперь будем набирать элементы по диагоналям, сначала берем с первой, потом со второй и тд. Так мы получим все элементы из A . И они будут занумерованы. Если какие-то элементы совпали, то их можно просто пропустить.

$$A = a_{11}, a_{21}, a_{12}, a_{31}, a_{22}, a_{13}, \dots$$

Ну или можно представить это в виде

$$A = \bigcup_{i=2}^{\infty} \bigcup_{j=1}^{i-1} a_{j(j-i)}$$

Значит A - счетно. Чтд

Декартово произведение конечного числа счетных множеств счетно.

Сначала докажем, что если A, B - счетны. То $A \times B$ - тоже счетно.

Доказательство:

$$A \times B = \{(a, b) | a \in A, b \in B\} = \bigcup_{i=1}^{\infty} \underbrace{A \times \{b_i\}}_{\text{счетное множество}}$$

Но очевидно, что $A \times \{b_i\}$ - счетное множество, так как это просто множество A , к каждому элементу в котором приписали b_i . Значит $A \times B$ - счетное объединение счетных множеств, значит оно счетно.

Но раз $A \times B$ - счетно, то перейдя к равномощным $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ - тоже счетно, значит можно по индукции доказать, что $\forall k \mathbb{N}^k$ - счетно. Чтд

Счетность множества конечных последовательностей натуральных чисел.

Пусть n - длина максимальной последовательности, значит такое множество можно представить в виде $\bigcup_{k=1}^n \mathbb{N}^k$.

$\bigcup_{k=1}^n \mathbb{N}^k$ - счетно, так как это счетное объединение счетных множеств. Кстати, тут \mathbb{N}^k - можно считать за все слова длины k в алфавите \mathbb{N} .

2.12 Если множество A бесконечно, а множество B конечно или счётно, то множество $A \cup B$ равномощно A . Равномощность множеств: бесконечных последовательностей из 0 и 1; вещественных чисел; $[0, 1]$; $[0, 1)$; множества всех подмножеств натуральных чисел. Равномощность отрезка и квадрата.

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

Пусть A - бесконечно, B - не более, чем счетное. Тогда $A \cup B \sim A$.

Доказательство:

$B' = B \setminus A$, B' - не более, чем счетное. Очевидно, что $A \cup B = A \cup B'$, но A и B' - не пересекаются. Так как A - бесконечно, то $\exists C \subseteq A$, C - счетно. Так как $C \cup B'$ - счетно, то $C \sim C \cup B'$. Значит $\exists f: C \rightarrow C \cup B'$ - биекция.

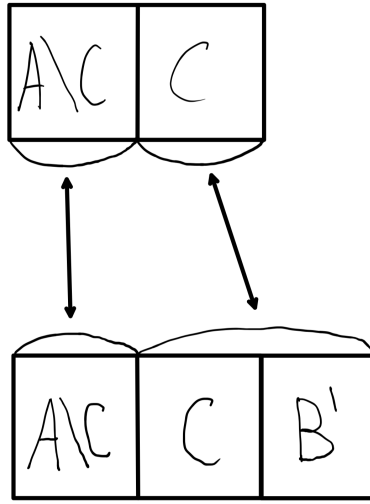


Рис. 1: иллюстрация биекции

Теперь просто построим биекцию $g : A \rightarrow A \cup B'$.

$$g(a) = \begin{cases} f(a), & \text{если } a \in C \\ a, & \text{иначе} \end{cases}$$

Равномощность множеств: $\mathbb{B}^\infty \sim [0, 1) \sim [0, 1] \sim \mathbb{R} \sim 2^{\mathbb{N}}$.

Доказательство $\mathbb{B}^\infty \sim [0, 1)$:

Построим биекцию $f : \mathbb{B}^\infty \rightarrow [0, 1)$. Инициализируем $f(b)$ так:

Пусть $b = b_0 b_1 b_2 \dots$, тогда разделим полуинтервал напополам, если $b_0 = 0$, то перейдем в левую половину и запустимся рекурсивно, если $b_0 = 1$, то вправо. Так мы сможем получить любые числа на полуинтервале $[0, 1)$, но это не будет биекцией, так как некоторые числа можно получить двумя способами. К примеру, $\frac{1}{2}$ будет соответствовать последовательность 01111... и 10000.... Поэтому давайте просто запретим последовательности, которые заканчиваются на бесконечную последовательность 1. Тогда $\mathbb{B}^\infty = \mathbb{B}' \cup Y$, где $Y = \{(* ** * * 0), 1111\dots\}$ - все последовательности, которые заканчиваются на все 1. Но $Y = \bigcup_{k=0}^{\infty} Y_k$, где $Y_k = \{a_1, a_2, \dots, a_{k-1}, 0, 1, 1, 1, \dots\}$, но Y_k - конечно ($|Y_k| = 2^{k-1}$). Значит Y - счетно, а $\mathbb{B}' \sim [0, 1)$, так как мы исключили плохие случаи, то верно, что

$$\mathbb{B}^\infty = \mathbb{B}' \cup Y \sim \mathbb{B}' \sim [0, 1)$$

Доказательство $[0, 1) \sim [0, 1] \sim \mathbb{R}$:

Добавление конечного не меняет мощность, поэтому $[0, 1) \sim [0, 1] \sim (0, 1)$. Заметим, что $(0, 1) \sim (-\frac{\pi}{2}, \frac{\pi}{2})$, тут легко строится биекция $f : (0, 1) \rightarrow (-\frac{\pi}{2}, \frac{\pi}{2})$, $f(x) = x \cdot \pi - \frac{\pi}{2}$. Пусть $g : (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ и $g(x) = \tan x$ - это очевидно биекция, тогда $(-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}$. Значит $[0, 1) \sim [0, 1] \sim (0, 1) \sim (-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}$.

Доказательство $\mathbb{B}^\infty \sim 2^{\mathbb{N}}$:

Тут довольно легко построить биекцию. Пусть дана двоичная последовательность $b = b_1 b_2 b_3 \dots$. Тогда если $b_i = 1$, то мы берем число i в наше подмножество, а если 0, то не берем. При таком кодировании очевидно все подмножества будут различны. Аналогично можно восстановить бинарную последовательность из данного подмножества.

Равномощность отрезка и квадрата.

Было доказано, что $\mathbb{B}^\infty \rightarrow [0, 1]$. Докажем, что $\mathbb{B}^\infty \rightarrow \mathbb{B}^\infty \times \mathbb{B}^\infty$. Построим биекцию $f : (\mathbb{B}^\infty)^2 \rightarrow \mathbb{B}^\infty$, наглядно продемонстрируем работу $f((a, b))$

$$\left. \begin{matrix} a_1 a_2 a_3 a_4 \dots \\ b_1 b_2 b_3 b_4 \dots \end{matrix} \right\} \xrightarrow{f} a_1 b_1 a_2 b_2 a_3 b_3 \dots$$

Значит $[0, 1] \sim \mathbb{B}^\infty \sim (\mathbb{B}^\infty)^2 \sim [0, 1]^2$.

2.13 Несчетность множества бесконечных последовательностей из 0 и 1. Сравнение мощностей, теорема Кантора о сравнении мощности множества и множества всех его подмножеств.

Несчетность множества бесконечных последовательностей из 0 и 1.

Доказательство от противного:

Пусть \mathbb{N} - счетно. Тогда можно каждому натуральному поставить во взаимно-однозначное соответствие бесконечную последовательность из 0 и 1. Тогда выпишем в столбик все натуральные числа, а в строчку к ним припишем соответствующие им последовательности. Тогда у нас не будет последовательностей, которых нет в этой таблице. Воспользуемся диагональным методом Кантора.

1	a_{11}	a_{12}	a_{13}	a_{14}
2	a_{21}	a_{22}	a_{23}	a_{24}
3	a_{31}	a_{32}	a_{33}	a_{34}
4	a_{41}	a_{42}	a_{43}	a_{44}
\vdots	\ddots	...
n	a_{nn}
\vdots

Теперь возьмем все элементы с диагонали и инвертируем их, то есть возьмем обратные к ним, заметим теперь, что мы из каждой последовательности взяли по элементу, и изменили его на обратный, то есть полученная последовательность не равна никакой из таблицы, то есть этой последовательности нет в таблице. Противоречие.

Сравнение мощностей, теорема Кантора о сравнении мощности множества и множества всех его подмножеств.

Пусть X - множество. Тогда $|X| < |2^X|$.

Доказательство:

1) $|X| \leq |2^X|$, так как существует инъекция $f: X \rightarrow 2^X$, $f(x) = \{x\} \in 2^X$.

2) $X \not\sim 2^X$

Докажем от обратного, пусть существует биекция $f: X \rightarrow 2^X$. Пусть $Y = \{x \in X \mid x \notin f(x)\}$. Очевидно, что $Y \subseteq X \Rightarrow Y \in 2^X$. Значит $\exists x \in X: f(x) = Y$.

1. $x \in Y \Rightarrow x \notin f(x) = Y$ - противоречие

2. $x \notin Y \Rightarrow x \in f(x) = Y$ - противоречие

Во все случаях получили противоречие, значит такой биекции нет. Чтд

2.14 Теорема Кантора – Бернштейна.

2.15 LYM-лемма, теорема Шпернера о размере максимальной антицепи в булевом кубе.

LYM-лемма, или LYM-inequality. Дан булев куб, пусть A в нем - антицепь, a_k - количество элементов в антицепи, в которых ровно k единиц. Тогда утверждается, что выполнено:

$$\sum_{k=0}^n \frac{a_k}{C_n^k} \leq 1$$

Доказательство:

Посчитаем количество цепей максимальной длины двумя способами. Для начала разберемся какой длины максимальная цепь. Будем рассматривать элементы цепи в порядке увеличения. Тогда если после x идет y , то x - подслово y , это значит, что в y единицы обязательно в тех же местах что и в x + хотя бы еще одна в других местах. Каждый раз количество единиц в вершины строго увеличивается, а значит, чтобы достичь цепь максимальной длины, нужно увеличивать вес(количество единиц) вершины на 1. Получаем, что максимальная длина цепи $n + 1$.

Посчитаем первым способом количество цепей максимальной длины. Чтобы дойти от 00...0 до 11...1. Нам нужно вставить в каком-то порядке n единиц, причем каждый порядок задает свою цепь. Получаем, что у нас $n!$ вариантов

последовательно вставить единицы, а значит и $n!$ цепей.

Посчитаем вторым способом. Зафиксируем какую-то вершину куба x , вес которой k . Сколько цепей максимальной длины проходит через нее? По тем же соображениям $k! \cdot (n - k)!$, потому что нам нужно каким-то порядком сначала поставлять k заданных единиц, а потом дойти из x до $11\dots 1$, поставив уже $n - k$ единиц.

Тогда сколько цепей максимальной длины проходит через вершины антицепи A ? Заметим тот факт, что через каждую вершину проходят свои уникальные цепи. Пусть это не так, тогда x_1 и x_2 находятся в одной цепи, значит их можно сравнить, значит они не могут быть в одной антицепи. Раз через каждую вершину проходят уникальные цепи максимальной длины, можно выписать неравенство:

$$\sum_{k=0}^n a_k \cdot k! \cdot (n - k)! \leq n!$$

то есть количество уникальных цепей максимальной длины, проходящих через вершины антицепи A не превосходит общего количества цепей максимальной длины. Делим неравенство на правую сторону, получаем то, что и требовалось доказать:

$$\sum_{k=0}^n \frac{a_k}{C_n^k} \leq 1$$

Теорема Шпернера. Длина максимальной антицепи в булевом кубе равна $C_n^{\lfloor \frac{n}{2} \rfloor}$.

Лемма, что $\max_{0 \leq k \leq n} C_n^k = C_n^{\lfloor \frac{n}{2} \rfloor}$. Будет использоваться, но не доказываться.

Доказательство:

Возьмем, то, что мы получили в ЛУМ-лемме и воспользуемся нашей локальной леммой, получим:

$$1 \geq \sum_{k=0}^n \frac{a_k}{C_n^k} \geq \sum_{k=0}^n \frac{a_k}{C_n^{\lfloor \frac{n}{2} \rfloor}} \Rightarrow \sum_{k=0}^n a_k \leq C_n^{\lfloor \frac{n}{2} \rfloor}$$

правая часть неравенства не что иное, как количество элементов в антицепи A .

Доказали, что не больше, как найти пример, где равно. Посмотрим на все вершины весом $\lfloor \frac{n}{2} \rfloor$. Очевидно, что они все несравнимы, а их количество как раз равно $C_n^{\lfloor \frac{n}{2} \rfloor}$. Что и требовалось доказать.

2.16 Эйлеровы циклы в ориентированных и неориентированных графах. Критерий существования эйлерова цикла.

Определение:

Цикл называется эйлеровым, если он проходит по всем рёбрам графа по одному разу (любое ребро входит в цикл, и никакое ребро не входит дважды).

Критерий существования:

Неориентированный граф без вершин нулевой степени содержит эйлеров цикл тогда и только тогда, когда он связан и степени всех вершин чётны.

Ориентированный граф без вершин нулевой степени (в которые не входит и из которых не выходит рёбер) содержит эйлеров цикл тогда и только тогда, когда он сильно связан и у любой вершины входящая степень равна исходящей.

Доказательство:

Будем доказывать параллельно оба варианта теоремы. Пусть сначала эйлеров цикл есть. Тогда он проходит через все вершины (поскольку они имеют ненулевую степень), и по нему можно дойти от любой вершины до любой. Значит, граф связан (сильно связан в ориентированном случае).

Теперь про степени. Возьмём какую-то вершину v , пусть она встречается в цикле k раз. Идя по циклу, мы приходим в неё k раз и уходим k раз, значит, использовали k входящих и k исходящих рёбер. При этом, раз цикл эйлеров, других рёбер у этой вершины нет, так что в ориентированном графе её входящая и исходящая степени равны k , а в

неориентированном графе её степень равна $2k$. Таким образом, в одну сторону критерий доказан.

Рассуждение в обратную сторону чуть сложнее. Будем рассматривать пути, которые не проходят дважды по одному ребру. (Таков, например, путь из одного ребра.) Выберем среди них самый длинный путь

$$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \dots \rightarrow a_{n-1} \rightarrow a_n$$

и покажем, что он является искомым циклом, то есть что $a_1 = a_n$ и что он содержит все рёбра.

В самом деле, если он самый длинный, то добавить к нему ребро $a_n \rightarrow a_{n+1}$ уже нельзя, то есть все выходящие из a_n рёбра уже использованы. Это возможно, лишь если $a_1 = a_n$. В самом деле, если вершина a_n встречалась только внутри пути (пусть она входит k раз внутри пути и ещё раз в конце пути), то мы использовали $k + 1$ входящих рёбер и k выходящих, и больше выходящих нет. Это противоречит равенству входящей и исходящей степени (в ориентированном случае) или чётности степени (в неориентированном случае).

Итак, мы имеем цикл, и осталось доказать, что в него входят все рёбра. В самом деле, если во всех вершинах цикла использованы все рёбра, то из вершин этого цикла нельзя попасть в вершины, не принадлежащие циклу, то есть использованы все вершины (мы предполагаем, что граф связан или сильно связан) и, следовательно, все рёбра. С другой стороны, если из какой-то вершины a_i выходит ребро $a_i \rightarrow v$, то путь можно удлинить до

$$a_i \rightarrow a_{i+1} \rightarrow \dots \rightarrow a_n = a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_i \rightarrow v$$

вопреки нашему выбору (самого длинного пути). Аналогично можно получить противоречие и для входящего ребра $v \rightarrow a_i$, добавив его в начало. (А можно заметить, что если есть неиспользованное входящее ребро, то есть и неиспользованное выходящее.) Это рассуждение было для ориентированного случая, но в неориентированном всё аналогично. Теорема доказана.

Помимо эйлеровых циклов, можно рассматривать *эйлеровы пути* — пути в графе, которые проходят один раз по каждому ребру. (Для неориентированных графов: рисуем картинку, не отрывая карандаша от бумаги, но не обязаны вернуться в исходную точку.) Для них тоже есть критерий: в неориентированном случае нужно, чтобы граф был связан и было не более двух вершин нечётной степени.

2.17 Двудольные графы, критерий двудольности графа. Пример: булев куб.

Определение:

Двудольным графом называется неориентированный граф, в котором можно разбить вершины на две доли — левые и правые, что все рёбра соединяют вершины из разных долей (нет рёбер, соединяющих вершины одной доли).

Критерий двудольности:

Граф двудольный тогда и только тогда, когда он двураскрашиваемый, то есть не содержит циклов нечётной длины.

Очевидно доказать эквивалентность утверждений граф двудольный и граф двураскрашиваемый, так что приведем доказательство того, что в двураскрашиваемом графе нет циклов нечётной длины.

Доказательство:

Докажем сначала, что в двураскрашиваемом графе нет циклов нечётной длины. По контрапозиции, это условие равносильно тому, что если в графе есть цикл нечётной длины, то его нельзя раскрасить в два цвета. Это утверждение легко проверить. Если правильная раскраска есть, то в силу симметрии можно считать, что первая вершина цикла покрашена в цвет 1, тогда вторая вершина покрашена в цвет 2 и так далее, то есть каждая нечётная вершина будет покрашена в цвет 1, а каждая чётная — в цвет 2. Тогда последняя вершина цикла будет покрашена в тот же цвет, что и первая, что невозможно.

Докажем теперь, что если в графе нет циклов нечётной длины, то он двураскрашиваемый. Для этого построим раскраску. Выберем в каждой компоненте связности по вершине s , которую назовём центром, и покрасим её в цвет 2; все вершины на расстоянии (все расстояния и пути подразумеваются минимальными по количеству ребер) 1 от неё покрасим в цвет 1, все вершины на расстоянии 2 — в цвет 2 и так далее: вершины на чётном расстоянии от центра покрасим в цвет 2, а на нечётном в цвет 1.

Предположим, что в результате этой процедуры получилась неправильная раскраска. Это означает, что у некоторого ребра $\{u, v\}$ концы были покрашены в один цвет, а это произошло, если расстояния от центра s некоторой компоненты до вершин u и v имеют одинаковую чётность. Заметим, что если расстояния от центра до u и v не равны, то путь до одной из вершин можно было сократить, проходя через другую вершину (так как расстояния отличаются как минимум на 2). Получаем, что расстояния от центра до v и u равны.

Но тогда путь от центра до v + ребро $\{v, u\}$ + путь от u до центра имеют нечетную длину (пути могут пересекаться, но простоту цикла в теореме ничего не сказано). Получили противоречие.

Булев куб двураскрашиваемый

Будем называть четностью вершины $v = (x_1, \dots, x_n)$ число $\text{parity}(v) = x_1 + \dots + x_n \bmod 2$. Тогда заметим, что если v, u связаны ребром, то $\text{parity}(v) \neq \text{parity}(u)$. Значит если у нас существует цикл нечетной длины k

$$v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_k \rightarrow v_1$$

то, так как четность на каждом шаге меняется, получаем $\text{parity}(v_1) = \text{parity}(v_3) = \dots = \text{parity}(v_k)$, но соседние вершины не могут иметь одну четность. Получаем противоречие.

2.18 Теорема Холла.

Теорема Холла. Если для каждого множества X вершин двудольного графа $G = (L, R, E)$ множество соседей $G(X) \subseteq R$ содержит не меньше вершин, чем X , то в графе G есть паросочетания размера $|L|$

Доказательство:

Полная индукция по количеству элементов в левой доле L .

База индукции. Если в L всего одна вершина x , то у неё есть хотя бы один сосед y в правой доле R по условию теоремы. Получаем паросочетание с ребром $\{x, y\}$.

Шаг индукции. Предположим, что утверждение теоремы выполняется для всех двудольных графов, в которых левая доля содержит меньше n вершин. Рассмотрим граф $G = (L, R, E)$, для которого выполняются условия теоремы и в L ровно n вершин. Разберём два случая.

Первый случай: в левой доле есть такое множество X , для которого $|X| = |G(X)|$. Выделим из графа два подграфа. Первый, G_1 , имеет доли $X, G(X)$ и все рёбра между этими вершинами. Второй, G_2 , имеет доли $L \setminus X, R \setminus G(X)$ и все рёбра между этими вершинами. Для обоих графов выполняются условия теоремы Холла. Для G_1 это очевидно по построению. Докажем выполнение условий теоремы для графа G_2 от противного. Пусть для подмножества $Z \subseteq L \setminus X$ соседей в $R \setminus G(X)$ меньше, чем вершин в Z . Тогда в графе G соседей у множества $X \cup Z$ меньше $|Z \cup X|$ (ведь множества X и Z не пересекаются, а соседей у X ровно $|X|$).

Итак, для G_1, G_2 выполняются условия теоремы, а количество вершин в них меньше n . Поэтому по предположению индукции в каждом из них есть паросочетание размера левой доли. Объединяя эти два паросочетания, получаем искомое паросочетание в G размера $|L|$.

Второй случай: для каждого $X \subseteq L$ выполняется неравенство $|X| < |G(X)|$.

Выберем вершину $a \in L$ и её соседа $b \in R$ (в этом случае соседей у каждой вершины больше одного, нас устроит любой).

Если в графе $G' = ((L \setminus a), (R \setminus b, E'))$, полученном из G выбрасыванием вершин a, b и инцидентных им рёбер, есть паросочетание P размера $n - 1$, то в графе G есть паросочетание размера n : к рёбрам из P добавим ребро $\{a, b\}$.

Если такого паросочетания нет, условие теоремы Холла для G' нарушается в силу индуктивного предположения. Какое-то «особое» множество $X \subseteq L \setminus \{a\}$ имеет мало соседей в $(R \setminus \{b\} : |X| > |G'(X)|$. Но в графе G у множества X есть разве что ещё один сосед b . Поэтому для этого множества выполняется равенство $|X| = |G(X)|$. Это первый случай, который уже рассмотрен выше.

2.19 Паросочетания. Вершинные покрытия. Теорема Кёнига

Теорема Кёнига В любом двудольном графе максимальный размер паросочетания равен минимальному размеру вершинного покрытия.

Доказательство:

В одну сторону легко. Если P - паросочетание в двудольном графе $G = (L, R, E)$, то любое вершинное покрытие содержит хотя бы по одному концу каждого ребра паросочетания и поэтому его размер не меньше размера паросочетания. Значит, минимальный размер вершинного покрытия не меньше максимального размера паросочетания. (Факт верен для любых графов)

Теперь в другую сторону (тут уже верно только для двудольных): рассмотрим минимальное по размеру вершинное покрытие $X \sqcup Y, X \subseteq L, Y \subseteq R$, в графе G . Проверим выполнение условия теоремы Холла для ограничения $G_{X, G(X) \setminus Y}$ графа на множество вершин X в левой доле и множество вершины $G(X) \setminus Y$ в правой доле (оставляем в $G_{X, G(X) \setminus Y}$ только рёбра между указанными вершинами). Пусть $S \subseteq X$.

Множество $(X \setminus S) \sqcup Y \sqcup G_{X, G(X) \setminus Y}(S)$ является вершинным покрытием в G : все рёбра, покрытые вершинами из S , покрыты также либо вершинами из Y , либо соседями вершин из S в правой доле. Поскольку мы выбрали минимальное по размеру вершинное покрытие, $|G_{X, G(X) \setminus Y}(S)| \geq |S|$, что и означает выполнение условия теоремы Холла.

Аналогично проверяется выполнение условия теоремы и для графа $G_{L \setminus X, Y}$, полученного ограничением G на вершины $L \setminus X$ в левой доле и Y в правой доле (так как $X \sqcup Y$ - вершинное покрытие исходного графа, $L \setminus X$ входит в множество соседей Y в левой доле).

По теореме Холла в $G_{X, G(X) \setminus Y}$ есть паросочетание размера $|X|$, а в $G_{L \setminus X, Y}$ есть паросочетание размера $|Y|$. Рёбра этих паросочетаний не совпадают по построению. Значит, объединение этих паросочетаний даёт паросочетание размера $|X| + |Y|$ в графе G . Таким образом, размер максимального паросочетания в G не меньше размера минимального вершинного покрытия.

2.20 Теорема Рамсея. Верхняя оценка чисел Рамсея.

Кликкой называется множество вершин графа, каждая пара которых соединена ребром.

Теорема Рамсея. Для любых k, n найдётся такое число N_0 , что в любом графе на $N \geq N_0$ вершинах есть или клика размера k , или независимое множество размера n .

Ясно, что если утверждение теоремы справедливо для графов на N вершинах, то оно справедливо и для графов с $N' > N$ вершинами. Обозначим через $R(k, n)$ число Рамсея — минимальное количество вершин, для которого справедлива теорема.

Доказательство:

Будем доказывать индукцией по s , что для любой пары чисел k, n такой, что $k + n = s$ справедливо утверждение теоремы.

База индукции $s = 2$ очевидна: $2 = 1 + 1$ — это единственный способ разложить число 2 в сумму целых положительных слагаемых, а одна вершина является одновременно и кликой, и независимым множеством.

Шаг индукции. Предположим, что утверждение выполнено для всех пар (k, n) таких, что $k + n = s$.

Докажем его для пары (k, n) такой, что $k + n = s + 1$. По индуктивному предположению утверждение теоремы выполнено для пар $(k - 1, n)$ и $(k, n - 1)$.

Рассмотрим граф на $N_0 = R(k - 1, n) + R(k, n - 1)$ вершине и возьмём какую-то вершину v этого графа.

Вершин в графе за исключением вершины v ровно $N_0 - 1$ штук. Среди них x соседей и y несоседей.

Докажем, что выполняется хотя бы одно из неравенств

$$x \geq R(k - 1, n)$$

$$y \geq R(k, n - 1)$$

В противном случае выполняются два неравенства

$$x < R(k - 1, n)$$

$$y < R(k, n - 1)$$

из которых следует $x + y \leq R(k - 1, n) - 1 + R(k, n - 1) - 1 = R(k - 1, n) + R(k, n - 1) - 2$.

Получаем противоречие

$$N_0 - 1 = x + y \leq R(k - 1, n) - 1 + R(k, n - 1) - 1 = N_0 - 2$$

Поэтому у вершины v есть $R(k - 1, n)$ соседей или есть $R(k, n - 1)$ несоседей.

Оба случая рассматриваются аналогично.

Первый случай. В индуцированном соседями вершины v подграфе по предположению индукции найдётся клика размера $k - 1$ или независимое множество размера n . В первом варианте добавление вершины v даёт клику в исходном графе размера k , во втором варианте в исходном графе есть независимое множество размера n .

Второй случай. В индуцированном несоседами вершины v подграфе по предположению индукции найдётся клика размера k или независимое множество размера $n - 1$. В первом варианте в исходной графе есть клика размера k , а во втором добавление вершины v даёт независимое множество размера n в исходном графе.

Итак, мы доказали утверждение теоремы и для произвольной пары (k, n) , для которой $k + n = s + 1$. Индуктивный переход доказан, и теорема следует из принципа математической индукции.

3 Задачи из листков