

ДИСКРЕТНАЯ МАТЕМАТИКА

(i)

Вики-страница

ФЗ МАХ 10 + зачима
компьютер мах 10 + доп. задачи
экзамен мах 10

0,259
0,259
0,402

1-2 модуль

$$0,2(\text{одз-2}) + 0,2 \cdot \text{ФЗ} + 0,2 \cdot \text{ком} + 0,4 \cdot \text{экз}$$

3-4 модуль

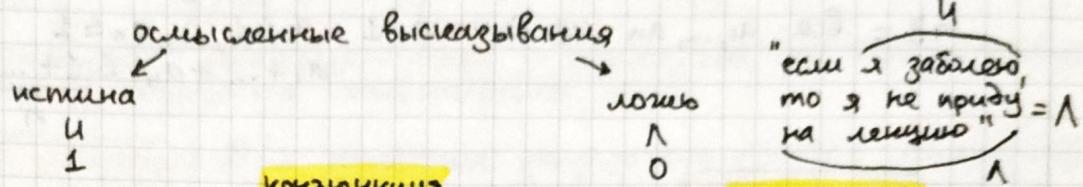
логические связи: и ($\wedge, \&$), или ($\vee, 1$), следует (\rightarrow)

таблица истинности

A	B	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \equiv B$	\bar{A}
0	0	0	0	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	0	0
1	1	1	1	1	1	0

ПРИОРИТЕТ ОПЕРАЦИЙ:

1. \neg
2. \wedge
3. \vee
4. $\rightarrow, \equiv, \text{etc}$

равносильность (\equiv, \leftrightarrow), отрицание (\neg) $\neg A = \bar{A}$

тавтология — высказывание, истинное при всех значениях переменных (в таблице истинности всегда 1)

$$\frac{A \quad A \rightarrow B}{B} \text{ modus ponens}$$

$$A \wedge (A \rightarrow B) \rightarrow B$$

пример тавтологии

Разбор случаев: $A \equiv A_1 \wedge \dots \wedge A_n$

$$A \vee B \equiv B \vee A$$

$$A \wedge B \equiv B \wedge A$$

перестановочная
коммутативность

$$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$

ассоциативность

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

$$\begin{array}{l} \Rightarrow A=1 \\ \quad B \vee C=1 \end{array}$$

если $A=B=1$, то $A \wedge B=1$ если $A \wedge C=1$, то

$$A=1, C=1$$

$$B \vee C=1 \quad A \wedge (B \vee C)=1$$

противоречие: $A \wedge \neg A=0$ всегда

$$(A \wedge \bar{A}) \rightarrow B = 1 \text{ всегда}$$

"если x на ФКН и x не на ФКН, то бы на РИМКИ"

Закон контрапозиции

$$(A \rightarrow B) \equiv (\bar{B} \rightarrow \bar{A})$$

$$A \rightarrow B \equiv \bar{A} \vee B \equiv \bar{B} \vee \bar{A} \equiv B \vee \bar{A}$$

AB: $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$ - тавтология

Если $\underbrace{a_1 + \dots + a_n}_A > n$, то $\underbrace{\text{какое-то из } a_1, \dots, a_n}_{B}$ больше 1,

$$\neg B = \text{все } a_1, \dots, a_n \text{ не больше 1} \quad a_1 \leq 1, \dots, a_n \leq 1 \\ a_1 + \dots + a_n \leq \underbrace{1 + \dots + 1}_n = n$$

Множества

Множество - совокупность объектов однотой природы.
2 множества равны, если в них одни и те же элементы.

$$\{1, 2, 3\} = \{2, 1, 3\} = \{1, 1, 1, 1, 2, 3, 3\} = A$$

$$A = B \Rightarrow \forall x \ x \in A \equiv x \in B \quad 1 \in A \quad 1 \notin A$$

$A \subseteq B$: A - подмножество B $\forall x \ x \in A \rightarrow x \in B$

$$x \in A$$

$$A \subseteq B$$

$$\begin{aligned} 1 &\notin \{\{1\}\} & \{\{1\}\} &\neq \{\{1, 1\}\} \\ \{1\} &\subset \{\{1\}\} & \{\{1\}\} &\subseteq \{\{1\}\} \\ \{1\} &\neq \{\{1\}\} \end{aligned}$$

Пустое множество \emptyset . Все пустые множества равны.

$$x \in A \cap B \equiv (x \in A) \wedge (x \in B)$$

$$x \in A \cup B \equiv (x \in A) \vee (x \in B)$$

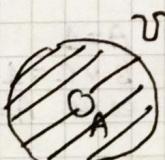
$$x \in A \setminus B \equiv (x \in A) \wedge (x \notin B)$$

$$x \in A \Delta B \equiv ((x \in A) \wedge (x \notin B)) \vee ((x \notin A) \wedge (x \in B))$$

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

$$x \in \bar{A} \equiv (x \notin A)$$

\emptyset только при использовании $\bar{A} = U \setminus A$



$$(A \cap B) \setminus C \equiv (A \setminus C) \cap B$$

$$\forall x: x \in (A \cap B) \setminus C \equiv x \in (A \setminus C) \cap B \Rightarrow (\alpha \wedge \beta) \wedge \gamma \wedge \neg \gamma \wedge \neg \beta \equiv (\alpha \wedge \gamma) \wedge \beta$$

$$x \in A \cap B \wedge x \notin C \equiv x \in A \setminus C \wedge x \in B \equiv \alpha \wedge \neg \gamma \wedge \beta$$

$$(\underbrace{x \in A \wedge x \in B}_{\alpha} \wedge \underbrace{x \notin C}_{\gamma}) \wedge \underbrace{x \in B}_{\beta} \equiv (\underbrace{x \in A}_{\alpha} \wedge \underbrace{x \notin C}_{\gamma}) \wedge x \in B$$

Множество конечно, если его элементы можно пересчитать:
 $A = \{a_1, a_2, \dots, a_n\}$ $\forall i \in A \exists i!$, и - размерность множества
 $n = |A|$. Количество элементов в последовательности - её длина.

Будем называть целые непрерывателные числа натуральными.
Последовательности равны, если их длины равны и все $i \in \mathbb{N}$
соответствующие элементы равны:

$$(1) = (1, 1) \quad (2, 1) = (1, 2) \\ \{1\} = \{1, 1\} \quad \{2, 1\} = \{1, 2\}$$

(Пересчитываемая) канингоморика - раздел, где мы подсчитываем
элементы в конечных множествах.

|Правило суммы| Для конечных непересекающихся множеств
 $|A \cup B| = |A| + |B|$ ($A \cap B = \emptyset$) выполняется равенство

$$2 \begin{array}{|c|c|c|} \hline & & \\ \hline \end{array} 5 \quad \text{Декартово произведение множеств } A \times B \\ \text{У } (a, b) - \text{ упорядоченные пары, где } A \ni a, B \ni b. \\ \text{Пример } \emptyset \times \mathbb{N} = \emptyset$$

|Правило произведения| Для конечных множеств A, B
выполняется равенство $|A \times B| = |A| \cdot |B|$

Для бесконечных множеств:

$$(1, (1, 2)) \in \mathbb{N} \times (\mathbb{N} \times \mathbb{N}), \text{ но } \notin (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \quad \mathbb{N} \times \mathbb{N} \times \mathbb{N} = \mathbb{N}^3$$

последовательность

|Больше тавтологий|

Транзитивность импликации:

$$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$$

Доказательство от противного:

$$((\neg A \rightarrow (B \wedge \neg B)) \rightarrow A \equiv \neg \neg A \rightarrow A \equiv A \rightarrow A)$$

$$\boxed{\neg(A \wedge B) \equiv \neg A \vee \neg B} \quad \boxed{\neg(A \vee B) \equiv \neg A \wedge \neg B}$$

запоны Де Моргана

"для всех x ", $\forall x A(x)$ - квантор всеобщности
"существует x , что..." $\exists x A(x)$ - квантор существования

$$\forall x \in A B(x) \cdot \quad \exists x \in A B(x) \\ \forall x (x \in A \rightarrow B(x)) \quad \exists x (x \in A \wedge B(x))$$

МАТЕМАТИЧЕСКАЯ ИНДУКЦИЯ

Принцип математической индукции. Пусть для последовательности утверждений $A_0, A_1, A_2, \dots, A_n, \dots$ заменяется на натуральными числами, верны утверждения.

База индукции: A_0 истинно

Шаг индукции: $A_n \rightarrow A_{n+1}$ истинно для любого n .
Последнюю инициализацию A_0 называем индуктивным предположением.

$\Rightarrow A_n$ истинно для любого n

$$(A(0) \wedge \forall n (A(n) \rightarrow A(n+1))) \rightarrow \forall n A(n)$$

$$\begin{aligned} A_0 &= 1 \\ A_0 \rightarrow A_1 &= 1 \\ A_1 \rightarrow A_2 &= 1 \\ \vdots \\ A_n \rightarrow A_{n+1} &= 1 \end{aligned}$$

- ♦ есть начало
- ♦ до любого числа можно дойти

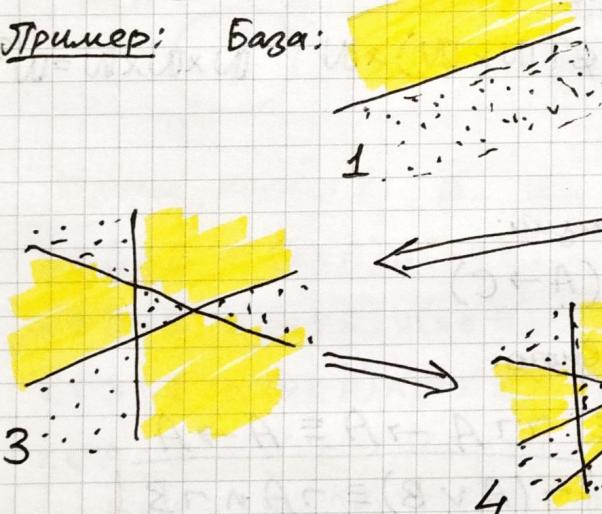
Пример: $\forall n \geq 1 : 1 + 2 + \dots + n = \frac{n(n+1)}{2}$

База: $A_1 = 1 = \frac{1 \cdot (1+1)}{2}$

Предположим, что A_n верно \Rightarrow

$$\begin{aligned} 1 + 2 + \dots + n &= \frac{n(n+1)}{2} \Rightarrow 1 + 2 + \dots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \\ &= \frac{(n+2)(n+1)}{2} = A_{n+1} \Rightarrow A_n \text{ верно } \forall n \end{aligned}$$

Пример: База:



Добавим прямоуголь:



переворачиваем одну сторону в противоположную
сторону

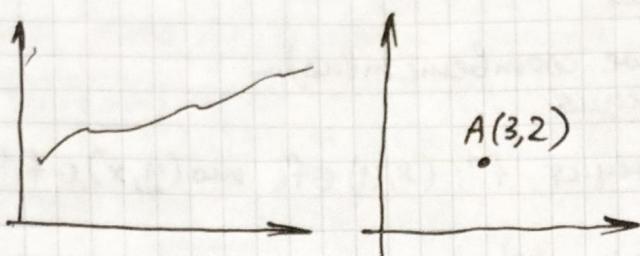
$$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow \dots$$

$$A_n \leftrightarrow A_{n+1}$$

Принцип полной математической индукции

Для последовательности утверждений $A_0, A_1, A_2, \dots, A_n, \dots$, где $n \in \mathbb{N}$ из $A_i \Rightarrow \forall i < n \Rightarrow A_n = 1 \Rightarrow A_n = 1 \forall n$

$$\boxed{\forall n ((\forall k < n : A(k)) \rightarrow A(n)) \rightarrow \forall n A(n)}$$

Функция $A \rightarrow B$ 

$$(a, b) = (c, d) \Leftrightarrow a=c, b=d$$

$$(a, b) := \{\{a\}, \{a, b\}\}$$

$$a=b \quad (a, a) = \{\{a\}\}$$

(c, d) - тоже 1-элементное множество $= \{\{c\}\} \Rightarrow a=c$

$a \neq b \Rightarrow (c, d)$ - тоже 2-х элементное множество

$$\begin{array}{l} \{a\} = \{c\} (\neq \{c, d\}) \\ a=c \end{array} \quad \begin{array}{l} \{a, b\} = \{c, d\} \\ b=d \end{array}$$

R на множестве A : $R \subseteq A \times A$

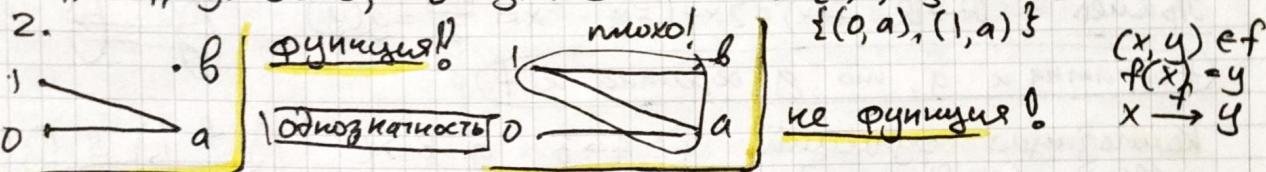
Бинарное отношение - $x R y \quad (x, y) \in R$

\mathbb{N}^2 отношение " $<$ ": $x < y \quad 2 < 3 \quad (2, 3) \in \mathbb{N}^2$

Функция $f: A \rightarrow B$ - это бинарное отношение на $A \times B$ ($f \subseteq A \times B$),

$$\therefore (x, y_1) \in f \text{ и } (x, y_2) \in f \Rightarrow y_1 = y_2$$

A - аргументы, B - значения $A = \{0, 1, 2\} \quad B = \{a, b\}$



1 **Dom (domain)** $f = f: x \in A: \exists y \in B \quad (x, y) \in f$
 $\underline{\text{Dom}}f \subseteq A$ $\underline{\text{Dom}}f = A$ - f -точечная, всюду определенная
 $\underline{\text{Dom}}f \neq A$ - f -частичная

x	0	1	2
$f(x)$	a	a	

Начальный отрезок натурального ряда:

$$[n] = \{x \in \mathbb{N}: x < n\} = \{0, 1, \dots, n-1\} - n \text{ чисел}$$

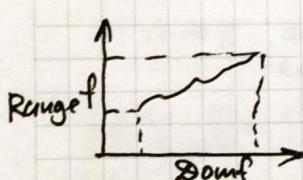
Конечная последовательность (слово) длины n в алфавите A

$$\begin{array}{|c|c|c|c|c|} \hline x & 0 & 1 & \dots & n-1 \\ \hline f(x) & f(0) & f(1) & & f(n-1) \\ \hline \end{array} \quad \text{Бесконечная последовательность}$$

в алфавите A : точечная функция $f: \mathbb{N} \rightarrow A$

$\{0\} = \emptyset$ **Множество значений**: $\underline{\text{Range}}f = \{y \in B: \exists x \in A, (x, y) \in f\}$

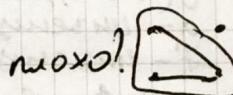
$$f = \{(0, a), (1, a)\} \quad \underline{\text{Range}}f = \{a\} \quad \{0, 1, 2\} \rightarrow \{a, b\} \quad \underline{\text{Range}}f \subseteq B$$



Инъективная функция (инъекция) - точечная функция $f: A \rightarrow B$ $\therefore x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

$$f(x) = x^3 \text{ на } \mathbb{N}$$



$f(x)^2$ - инъекция $\mathbb{N} \rightarrow \mathbb{N}$
не инъекция $\mathbb{Z} \rightarrow \mathbb{Z}$

не инъекция

Сюръективная функция (суръекция) - точечная функция $f: A \rightarrow B$ $\therefore \underline{\text{Range}}f = B$ $\forall y \in B \quad \exists x \in A \quad (x, y) \in f$

или такого



множ!

$$f(x) = x^3 \quad \mathbb{N} \rightarrow \mathbb{N} \quad [f(x)=z]$$

$$f(x) = x^3 \quad \mathbb{R} \rightarrow \mathbb{R} - \text{суръекция}$$

$$f(x) = x^2 \quad \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = -1 \quad \mathbb{R} \rightarrow \mathbb{R}_{>0}$$

f

сюръекция

Биекция (взаимно-однозначное соответствие) —
— и сюръекция, и инъекция

f -биекция. Обратная функция $f^{-1}: (x, y) \in f$, то $(y, x) \in f^{-1}$
 $f: A \rightarrow B \quad f^{-1}: B \rightarrow A$

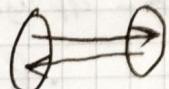
f^{-1} -функция: $(y_1, x_1), (y_2, x_1) \in f^{-1} \Rightarrow x_1 = x_2$
 $(x_1, y_1), (x_2, y_1) \in f \Rightarrow x_1 = x_2 \quad f$ -инъекция

f^{-1} -тотальна: $\forall y \in B \exists x \in A (y, x) \in f^{-1}$
 $\forall y \in B \exists x \in A (x, y) \in f \quad f$ -сюръекция

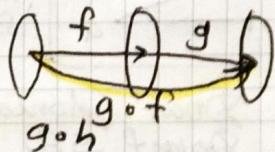
f^{-1} -инъекция: $(y_1, x), (y_2, x) \in f^{-1} \Rightarrow y_1 = y_2$
 $(x, y_1), (x, y_2) \in f \Rightarrow y_1 = y_2 \quad f$ -функция

f^{-1} -сюръекция: $\forall x \in A \exists y \in B (y, x) \in f^{-1}$
 $\forall x \in A \exists y \in B (x, y) \in f \quad f$ -тотальна

Пример $f: \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = 2x + 1 = y \quad x = \frac{y-1}{2} = g(y)$

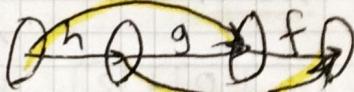


(f обратна к g , то g обратна к f)



Композиции функций: $f: A \rightarrow B \quad g: B \rightarrow C$
 $g(f(x)) = (g \circ f)(x) \quad \exists y \in B \quad (x, y) \in f \quad (y, z) \in g$
 $g \circ f$ — это не пойти что

Ассоциативность: $(f \circ g) \circ h = f \circ (g \circ h)$



Композиции сохраняет классы функций:
(инъективность, сюръективность, биективность). $f \circ g$

Лемма $f: A \rightarrow B, g: B \rightarrow C$

- ① f, g — инъекции $\Rightarrow g \circ f$ — тоже инъекция
- ② f, g — сюръекции $\Rightarrow g \circ f$ — сюръекция
- ③ f, g — биекции $\Rightarrow g \circ f$ — биекция
- ④ f, g — тотальны $\Rightarrow g \circ f$ — тотальная

Док-во: ① $(g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow x_1 = x_2$

$$g(f(x_2)) = g(f(x_1))$$

g — инъекция $\Rightarrow f(x_1) = f(x_2)$

f — инъекция $\Rightarrow x_1 = x_2$

② $\forall z \in C: \exists y \in B \quad g(y) = z \quad f$ -сюръекция $\Rightarrow \exists x \in A \quad f(x) = y \quad \exists x \in A$
 $\therefore f(x) = y$ по опр. композиции $(g \circ f)(x) = g(f(x)) = z \Rightarrow$
 $g \circ f$ — сюръекция

Принцип Дирихле (принцип Крашев) Если $k > n$ и k то хотя бы в одной клетке сидят хотя бы 2 крашка.

Теорема Если $k > n$, r_1, \dots, r_n - натуральные числа и $r_1 + \dots + r_n = k$, то $\exists i, r_i \geq 1$.

Proof. От противного: пусть $\forall i, r_i \leq 1$ сложим все неравенства, $r_1 + \dots + r_n \leq n$ т.к. $r_1 + \dots + r_n = k$, то $k \leq n \Rightarrow$ противоречие, q.e.d.

Конечные множества Множество называется конечным, если для некоторого $n \in \mathbb{N}$ \exists биекция $f: [n] \rightarrow A$, где n - множество множества. $|A| = n$

Теорема (корректность определения конечности множества). Пусть $f: [n] \rightarrow A$ и $g: [m] \rightarrow A$ - две биекции $\Rightarrow n = m$

Proof. От противного. Suppose $n \neq m$. let $n > m \Rightarrow$ $\exists g^{-1}: A \mapsto [m]$ and $g^{-1} \circ f: [n] \rightarrow [m]$ - биекция $[n]$ - крашки, а $[m]$ - птицы. $n > m \Rightarrow$ в какой-то клетке сидят два крашка $\Rightarrow \exists i, j \in [n]: g^{-1} \circ f(i) = g^{-1} \circ f(j)$ \Rightarrow противоречие, q.e.d.

ОБРАЗ Пусть $X \subseteq A$ - подмножество A . f сопоставляет ему образ $f[X] \subseteq B \subseteq X$. То определено $f[X]$ состоит из тех элементов B , которые являются значениями элементов из X :

$$f[X] = \{b \in B \mid \exists x \in X: b = f(x)\} \quad \text{если } X = A \Rightarrow f[A] = \text{Range}(f)$$

Пример. f из $A = \{1, 2, 3, 4\}$

$$\begin{array}{c|cccc} x & 1 & 2 & 3 & 4 \\ f(x) & 1 & 2 & 2 & \end{array}$$

Если $X = \{1, 2\} \Rightarrow f[X] = \{1, 2\}$

$$X = \{3, 4\} \Rightarrow f[X] = \{2\}$$

ПРООБРАЗ $Y \subseteq B$. Тогда предобраз $f^{-1}[Y]$ состоит из тех элементов A , которые лежат в Y :

$$f^{-1}[Y] = \{a \in A \mid f(a) \in Y\} \quad f^{-1}[B] = \text{Dom}(f)$$

Пример. $Y = \{2\}$ $f^{-1}[Y] = \{2, 3\}$ $Y = \{3, 4\} \Rightarrow f^{-1}[Y] = \emptyset$

$f: A \rightarrow B$ ~~если~~ f -инъекция, если $f^{-1}[B] = A$,
если $f[A] = B$, то f -сюръекция

$$|f^{-1}[Y]| = \sum_{b \in Y} |f^{-1}\{b\}|$$

СРАВНЕНИЕ КОНЕЧНЫХ МНОЖЕСТВ

Лемма Для конечных функций из конечного множества в конечное выполняются такие свойства:

- ① если $f: A \rightarrow B$ инъекция $\Rightarrow |A| \leq |B|$;
- ② если $f: A \rightarrow B$ сюръекция $\Rightarrow |A| \geq |B|$;
- ③ если $f: A \rightarrow B$ биекция $\Rightarrow |A| = |B|$.

Proof. $a_i, i \in B$ - количество элементов $A \subseteq A \therefore f(a) = i$
 f -инъекция $\Rightarrow a_i \leq 1 \forall i \in B \Rightarrow$ Аналогично для f -сюръекции
 $|A| = \sum_{i \in B} a_i \leq \sum_{i \in B} 1 = |B|$ $|A| = \sum_{i \in B} a_i \geq \sum_{i \in B} 1 = |B|$

[Лемма] Для монотонных функций из конечного множества
 в седл выполнены свойства:

① если $f: A \rightarrow A$ инъекция, то f -сюръекция;

② если $f: A \rightarrow A$ сюръекция, то f -инъекция.

Proof f -инъекция $\Rightarrow |f[A]| = |A| = n \Rightarrow f$ -сюръекция
 Let f -сюръекция. $|f^{-1}[A]| = |\{x \in A \mid f(x) \in A\}|$
 $|f^{-1}(A)| = \sum_{b \in A} |f^{-1}\{b\}|$. Since f -сюръекция $\Rightarrow |f^{-1}\{b\}| \geq 1 \Rightarrow$
 $\Rightarrow |f^{-1}\{b\}| = 1 \Rightarrow f$ -инъекция

ПОДСЧЕТЫ СЛОВ И ФУНКЦИЙ

Правило суммы для несвязных попарно непересекающихся множеств:

если $A_i \cap A_j = \emptyset$ для всех $1 \leq i < j \leq n$, то $|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$

Правило произведения для несвязных множеств:

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$$

Размещение

$$A_n^k = n(n-1)(n-2) \cdots (n-k+1) = \frac{n!}{(n-k)!}$$

$$P_n = n! \quad (\text{частный случай } A_n^k)$$

Перестановка множества A - любая биекция $f: A \rightarrow A$,
 их количество P_n .

количество инъекций из k -элементного множества в n -элементное.

Сочетание (неупорядоченные

выборки) - из n по k - подмножество n -элементного множества, где k элементов.

$$C_n^k \cdot k! = A_n^k$$

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

$$\binom{n}{k}$$

03.10.23 ЛЕКУЧА-5.

X -множество и элементов
 $P(X)$ -множество его подмножеств

Биклическая $A \subseteq X \mapsto \chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \in X \setminus A \end{cases}$

$A = B \Leftrightarrow A \Delta B = \emptyset \Leftrightarrow \chi_A(x) = \chi_B(x) \quad \chi_A: X \rightarrow \{0, 1\}$ 2^n
 монотонные

Сколько существует слов из 0 и 1 длины n с ровно k единицами?

k -элементные подмножества n -элементного множества

Теорема $C_n^0 + C_n^1 + \dots + C_n^n = 2^n$

$$(x+y)^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$$(x+y)^n = \binom{n}{0}y^n + \binom{n}{1}y^{n-1}x + \dots + \binom{n}{n-1}yx^{n-1} + \binom{n}{n}x^n$$

x и y — 2^n слоговых символов в алфавите $\{x, y\}$. Эквивалентно ли это C_n^k , т.е.?

$$x=y=1 \quad 2^n = (1+1)^n = C_n^0 + C_n^1 + \dots + C_n^n$$

если $k=n$ или $k<0$, то $C_n^k=0$

$$C_n^k = \binom{n}{k}$$

Proof

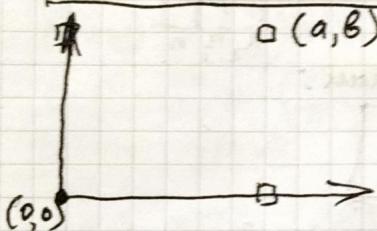
если $k>n$ или $k<0$, то $C_n^k=0$

ТРЕУГОЛЬНИК ПАСКАЛЯ

$$\begin{aligned} n=0 \\ n=1 \\ n=2 \\ n=3 \\ n=4 \\ n=5 \end{aligned}$$

			1			
			1	1		
			1	2	1	
			1	3	3	1
			1	4	6	4
			1	5	10	10
			1	6	15	10
			1	7	21	15
			1	8	28	21

МОНОТОНИЕ ПУТЕЙ В КВАДРАНТЕ



Путь — последовательность целочисленных точек $(x, y) \xrightarrow{(x+1, y)} \xrightarrow{(x, y+1)}$

$T(a, b)$ — количество путей из $(0, 0)$ в (a, b) .

$$2 \text{ группы путей: } \uparrow \text{ или } \rightarrow \quad T(a, b) = T(a, b-1) + T(a-1, b)$$

$$T(a, b) = ? \quad T(a, b-1) \quad T(a-1, b) \quad T(0, 0) = 1 \quad T(0, b) = 1$$

Теорема $T(a, b) = \binom{a+b}{a}$ $(0, 0) \rightarrow (a, b)$ $a+b$ ходов
 $\rightarrow a$ ходов $\uparrow b$ ходов

Протокол движения: $\rightarrow \rightarrow \uparrow \uparrow \rightarrow \dots$ слово из $a+b$ символов
 b алфавите $\{\rightarrow, \uparrow\}$ с a запятыми \rightarrow

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

$$C_n^k = T(k, n-k) = T(k-1, n-k) + T(k, n-k-1) = C_{n-1}^{k-1} + C_{n-1}^k$$

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

\times n элементов
 $\times \in A$ $k-1$ элементов из $n-1$ C_{n-1}^{k-1}
 $\times \notin A$ k элементов из $n-1$ C_{n-1}^k

Свойство Строки треугольника Паскаля симметричны относительно середины.

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

Число k -элементных подмножеств n -элементного множества равно числу его $(n-k)$ -элементных подмножеств

$A \subseteq X \xrightarrow{k} X \setminus A$ "быть выбраным и знатим 'не быть
не выбраным'"

 $(x+y)^n = (y+x)^n \quad x^k y^{n-k}$

Путь по прямой: \Rightarrow путь
многомонотонный

Разрешимы ходы нек (любые ходы) $T(n) - ?$

$$0 \dots n \quad i=0, \dots, n-1 \quad T(n) = T(0) + T(1) + \dots + T(n-1)$$

$$T(1)=1 \quad T(2)=2 \quad T(3)=4 \quad T(4)=8 \dots T(n)=2^{n-1} \quad n \geq 1$$

Теорема $T(n)=2^{n-1}, \quad n \geq 1$

Proof база: $n=1 \quad T(1)=1=2^{1-1}$

$$\text{шаг: } T(n+1) = T(0) + T(1) + \dots + T(n-1) + T(n) = 2T(n) = 2^n = \\ = 2^{n+1} \quad (\text{по предположению индукции}), \quad q.e.d.$$

2^{n-1} , количество слов длины $n-1$ в алфавите $\{0, 1\}$

слово \leftrightarrow маршрут (мы заходим в клетки, где написана 1)

Разрешим ходы на 1 или на 2 клетки:

$H(n)$ - число маршрутов \Rightarrow

$$H(n) = H(n-1) + H(n-2) \quad H(0)=1 \quad H(1)=1$$

- рекуррентная формула для чисел Фибоначчи:

$$F_{n+2} = F_n + F_{n+1} \quad H_n = F_{n+1} \quad \varphi = \frac{1+\sqrt{5}}{2} \quad \varphi' = \frac{1-\sqrt{5}}{2}$$

Формула Бине $F_n = \frac{\varphi^n - \varphi'^n}{\sqrt{5}}$ **База** $n=0$: $F_0 = \frac{\varphi^0 - \varphi'^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0$

$$n=1: \quad F_1 = \frac{\varphi^1 - \varphi'^1}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1$$

Изл $A(0) \wedge A(1) \wedge \forall n (A(n) \wedge A(n+1) \rightarrow A(n+2)) \rightarrow \forall n A(n)$

$$A(0) \wedge A(1) \rightarrow A(2)$$

$$A(1) \wedge A(2) \rightarrow A(3)$$

$$F_{n+2} = F_{n+1} + F_n = \frac{\varphi^{n+1} - \varphi'^{n+1}}{\sqrt{5}} + \frac{\varphi^n - \varphi'^n}{\sqrt{5}} = \frac{\varphi^n(\varphi+1) - \varphi'^n(\varphi+1)}{\sqrt{5}} = \\ = \frac{\varphi^{n+2} - \varphi'^{n+2}}{\sqrt{5}}$$

Теорема Сумма чисел в n -ой строке треугольника Паскаля равна 2^n .

$$C_n^0 + C_n^1 + \dots + C_n^n = 2^n$$

Теорема В первой половине треугольника Паскаля числа возрастают, а во второй убывают.

$$\binom{n}{k} > \binom{n}{k-1} \Leftrightarrow \frac{n!}{k!(n-k)!} > \frac{n!}{(k-1)!(n-k+1)!} \Leftrightarrow \frac{1}{k} > \frac{1}{n-k+1} \Leftrightarrow n-k+1 > k \Leftrightarrow n+1 > 2k \quad (k \text{ лежит в первой половине})$$

Теорема $\left(\frac{2n}{n}\right) > \frac{2^{2n}}{2n+1}$

самый большой в строке $n > 0$

$\left(\frac{2n}{0}\right) + \left(\frac{2n}{1}\right) + \dots + \left(\frac{2n}{2n}\right) = 2^{2n}$

также $2n+1$ слагаемых \Rightarrow самое большое $\geq \frac{2^{2n}}{2n+1}$

Теорема А-и-элементное множество. Тогда подмножества с чётным числом элементов столько же, сколько и с нечётным.

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots$$

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \dots + (-1)^n \binom{n}{n} = 0$$

$$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \dots + \binom{n}{n} y^n \quad \begin{matrix} x=1 \\ y=-1 \end{matrix}$$

$$0 = (1-1)^n = \binom{n}{0} 1^n + \binom{n}{1} 1^{n-1} (-1) + \dots + \binom{n}{n} (-1)^n$$

$$|A|=n \quad |B|=k \quad \text{точечных функций } A \rightarrow B? \quad \begin{matrix} A \rightarrow B? \leftarrow K^n \\ A=B=\emptyset \quad 0^0=1, \text{ и.к. 1 функция} \end{matrix} \quad B^A$$

$$SEA \quad x \subseteq A \quad S \notin X \quad x \leftrightarrow X \cup \{S\}$$

подмножества A разделились на пары, если в x чётное число элементов, то в $X \cup \{S\}$, нечётное

$(x_1 + \dots + x_k)^n$ слагающие: $x_1^{a_1} \dots x_k^{a_k}$ $a_1, \dots, a_k \in \mathbb{N}$
набор (a_1, \dots, a_k) однозначно определяет monom $x_1^{a_1} \dots x_k^{a_k} \quad x_1^{a_1} \dots x_k^{a_k} = [x^\alpha] \quad (\text{обозн.})$

$$(x_1 + \dots + x_k)^n = \sum_{\substack{\alpha=a_1, \dots, a_k \\ a_1+\dots+a_k=n}} \binom{n}{\alpha} x^\alpha \quad k=2: \quad \binom{n}{\alpha} - \text{биномиальный коэффициент}$$

$\binom{n}{\alpha} - \text{мультиномиальный коэффициент}$

Чему они равны?

$$\boxed{\binom{n}{a_1 \dots a_k} = \frac{n!}{a_1! \dots a_k!}}$$

Док-бот1 $x_1 x_2 x_3 x_1 \dots$ — каждое слагающее $\binom{n}{\alpha}$ — перед x^α

a_1 переменная $x_1 \Rightarrow \binom{n}{\alpha} =$ количество слов из n букв, a_1 переменных $x_1 \dots x_k \Rightarrow \binom{n}{\alpha} =$ количество слов из n букв x_1, \dots, x_k , a_1 буква x_1, \dots, a_k буква x_k

если все буквы разные, то всего $n!$ букв $a_1! \dots a_k!$ перестановок x_1
 $a_1! \dots a_k!$ раз посчитано каждое слово $\frac{n!}{a_1! \dots a_k!}$

Доказательство Сколько способов выбрать a_1 места для x_1 ?

$$\frac{(n)(n-a_1)}{a_1!} \cdot \dots \cdot \frac{(n-a_1-\dots-a_{k-1})}{a_k!} = \frac{n!}{a_1!(n-a_1)!} \frac{(n-a_1)!}{a_2!(n-a_1-a_2)!} \cdots \frac{(a_k)!}{a_k!(0)!} = \binom{n}{k} = \binom{n}{k, n-k}$$

Пример 3 человека делают 6 дней \Rightarrow $A, B, C -$ люди

$$A, B, A, B, B, B = \binom{6}{2, 2, 2} = \frac{6!}{2!2!2!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 2 \cdot 2!} = 90$$

$$(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k} \quad n+1 \text{ слагаемых}$$

$$(x_1 + \dots + x_n)^k = \sum_{\alpha} \binom{n}{\alpha} x^{\alpha} \quad \text{сколько слагаемых?}$$

$n=3, k=3$ 3 буквы одинаковые; 3 буквы разные: $\frac{3+1}{6} = 10$

$$x_1^{a_1} \cdots x_n^{a_n} \quad (a_1, \dots, a_n) \quad a_1 + \dots + a_n = k.$$

Сколько решений в натуральных числах?

$\binom{n}{k}$ - число сочетаний с повторениями

$\binom{n}{k}$ - число k -элементных подмножеств n -элементного множества

n -элементное множество t_1, t_2, \dots, t_n
 k местам раздамь
 n людям
 a_1 - первому, ...; a_n - n -ому

k -элементное мульти множество
 порядок не важен,
 но израинство
 вхождения важно!

$$n=7, k=7$$



$$a_1=0 \quad a_2=2 \quad a_3=0 \quad a_4=2 \quad a_5=0 \quad a_6=1 \quad a_7=2$$

k места для маркеров, $k-1$ места для палочек
 решения уравнения $a_1 + \dots + a_n = k \Leftrightarrow$ расстановка

Теорема $\binom{n}{k} = \binom{n+k-1}{k}$

$k-1$ палочки
 $n+k-1$ мест
 к маркеров и $n-1$ палочек

Задача сколько многочленов из n членов из k ?

a_1, \dots, a_n - члены (целые, многочленные) $a_1 + \dots + a_n = k \Rightarrow$

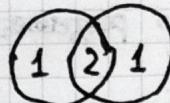
$$\underbrace{(l_1-1)}_{a_1} + \dots + \underbrace{(l_{n-1}-1)}_{a_n} = k-n \quad |0| \quad n+k-1 \text{ членов}$$

$$\Rightarrow \binom{k-1}{n-1} \quad \binom{k-n}{n-1} = \binom{k-n+n-1}{n-1}$$

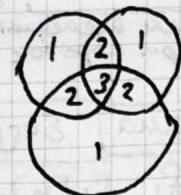
K выбрать $k-1$ число \Rightarrow

$$A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$$

Теорема $|A \cup B| = |A| + |B| - |A \cap B|$
 формула вычитаний и исключений для 2 множеств



Теорема $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$



Теорема $|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} |A_1 \cap \dots \cap A_n|$

$$U \ni A \quad \chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \in U \setminus A = \bar{A} \end{cases} \quad \chi_A(x) \cdot \chi_B(x) = \chi_{A \cap B}(x) \quad \chi_{\bar{A}}(x) = 1 - \chi_A(x)$$

$$A \cup B = \overline{\overline{A} \cap \overline{B}} \quad \chi_{A \cup B}(x) = \min(\chi_A(x) + \chi_B(x), 1)$$

$$\chi_{A \cup B}(x) = 1 - (1 - \chi_A(x))(1 - \chi_B(x)) = \chi_A(x) + \chi_B(x) - \chi_{A \cap B}(x) \quad + (-1)^{n+1} \chi_{A_1 \cap \dots \cap A_n}(x)$$

$$\chi_{A_1 \cup \dots \cup A_n}(x) = 1 - (1 - \chi_{A_1}(x)) \cdot \dots \cdot (1 - \chi_{A_n}(x)) = \sum_{i=1}^n \chi_{A_i}(x) - \sum_{1 \leq i < j \leq n} \chi_{A_i \cap A_j}(x) + \dots +$$

$|A| = \sum_{x \in U} \chi_A(x)$ просуммируем по всем $x \in U$ — будем **формула вычитаний-исключений**

Функций: $n \rightarrow k^{(k+1)^n}$

множественных функций: $n \rightarrow k^{k^n}$

инъекций $n \rightarrow k!$

дискретных $n \rightarrow n!$

сторонних $n \rightarrow k?$

$$k(k-1) \cdots (k-n+1) = \frac{k!}{n!}$$

Сколько не-сторонних?
 (3 элементов в k -элементном множестве
 без прообраза)

$[n] \rightarrow [k] = \{0, 1, \dots, k-1\}$
 $A(i)$ — множество функций т.ч. прообраз $\{i\}$ пуст.

$A(0) \cup A(1) \cup \dots \cup A(k-1)$ — множество не-сторонних

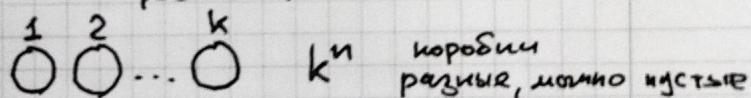
$$|A(0)| = (k-1)^n \quad |A(0) \cap A(1)| = (k-2)^n \quad |A(i_1) \cap \dots \cap A(i_p)| = (k-p)^n$$

$$|A(0) \cup A(1) \cup \dots \cup A(k-1)| = \sum_{i=0}^{k-1} |A(i)| - \sum_{0 \leq i < j \leq k-1} |A(i) \cap A(j)| + \dots =$$

$$= k(k-1)^n - \binom{k}{2}(k-2)^n + \binom{k}{3}(k-3)^n - \dots + (-1)^{k+1} \binom{k}{k}(k-k)^n$$

$$\text{Surj}(n, k) = 1 \cdot k^n - k \cdot (k-1)^n + \binom{k}{2} (k-2)^n - \dots = \sum_{p=0}^k (-1)^p \binom{k}{p} (k-p)^n$$

n -элементное множество
 k классов



k^n коробки
 различные, можно пустые

коробки однотипные, пустые нельзя

p_1 коробка с 1 элементом, p_2 коробка с 2 элементами, $\Phi(n, k)$

p_1 коробка с n элементами

$$p_1 + \dots + p_n = k$$

$$p_1 \cdot 1 + p_2 \cdot 2 + \dots + p_n \cdot n = n$$

$$\left(\begin{array}{c} n \\ 1, 1, 2, 2, \dots \end{array} \right)$$

пустые коробки разные:

n элементов в классы: $\frac{1}{p_1} \cdot 1, \frac{2}{p_2} \cdot 2, \dots$

$$\frac{n!}{(1!)^{p_1} (2!)^{p_2} \dots (n!)^{p_n}}$$

Коробки-то ~~одинаковые~~ одинаковые!

$$\frac{n!}{(1!)^{e_1} \cdots (n!)^{e_n} e_1! \cdots e_n!}$$

меньше или
равно коробкам

меньше или
равно коробкам

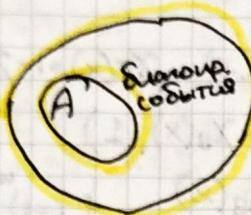
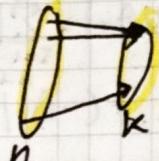
$$\Phi(n, k) = \sum_{\substack{e_1, \dots, e_n \\ e_1 + \dots + e_n = k}} \frac{n!}{(1!)^{e_1} \cdots (n!)^{e_n} e_1! \cdots e_n!}$$

запись

$e_1, \dots, e_n \geq 0$

Теорема $\text{Surj}(n, k) = k! \cdot \Phi(n, k)$

Proof: $f: [n] \rightarrow [k]$ - сюръекция
из n -х коробок - образ $i \in [k]$



$$\frac{|A|}{|U|}$$

Задача: каждый взят случайную штучку (и говяжью)
вероятность: каждый взят случайную штучку

$2, \dots, n$ и $n!$ - всего
 a_1, a_2, \dots, a_n $i \neq a_i$ переси без неподвижных точек

$B(i)$ - это $i = a_i$, $|B(i) \cup \dots \cup B(n)|$ - все перестановки с неподвижными точками

$$|B(i)| = (n-1)! \quad |B(i) \cap B(j)| = (n-2)! \quad |B(i_1) \cap \dots \cap B(i_k)| = (n-k)!$$

$$|B(i) \cup \dots \cup B(n)| = \sum_{i=1}^n |B(i)| - \sum_{1 \leq i < j \leq n} |B(i) \cap B(j)| + \dots = n(n-1)! - \binom{n}{2}(n-2)! + \dots =$$

$$= \sum_{k=1}^n \binom{n}{k} (n-k)! (-1)^{k+1}$$

вероятность = $\frac{n! + \sum_{k=1}^n (-1)^k \binom{n}{k} (n-k)!}{n!} =$

$$= 1 + \sum_{k=1}^n (-1)^k \cdot \frac{1}{k!} = 1 + \sum_{k=0}^n \frac{(-1)^k}{k!} e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

ЛЕКУЧИЙ-8. 24.10.23

Определение бесконечное множество - которое не является конечным (не имеет с отрезком \mathbb{N})

A, B - конечные множества

$$f: A \rightarrow B - \text{бихоломия} \Rightarrow |A| = |B| \quad A \text{-бесконечно}$$

$$f: A \rightarrow B - \text{инъекция} \Rightarrow |A| \leq |B| \quad |A| - ?$$

$|A| = |B|$ (A и B равнозначны), если \exists бихоломия $f: A \rightarrow B$

$|A| \leq |B|$ (множество A меньше или равно множеству B),
если \exists инъекция $f: A \rightarrow B$

$$g: A \rightarrow f[A] \subseteq B$$

Эквивалентность $C \subseteq B$ и бихоломия $g: A \rightarrow C$

$|A| < |B|$: \exists инъекция $f: A \rightarrow B$, которая не бихоломия

$|\mathbb{N}| = |\mathbb{N}|$: $f(x) = x$, при этом $f: \mathbb{N} \rightarrow \mathbb{N}$ - инъекция, но бихоломия?

$|A| < |B|$: $|A| \leq |B|$ и неверно $|A| = |B|$

Свойства \subseteq :

① рефлексивность $|A| = |A|$
 ② $|A| = |B|, |B| = |C| \Rightarrow |A| = |C|$ — транзитивность
 $f: A \rightarrow B, g: B \rightarrow C \quad g \circ f: A \rightarrow C$ — тоже биекция

③ симметричность: $|A| = |B|$, то $|B| = |A|$
 $f: A \rightarrow B \quad f^{-1}: B \rightarrow A$ — тоже биекция

Свойства \subseteq

- ① рефлексивность $|A| \leq |A|$
 ② транзитивность: $|A| \leq |B|, |B| \leq |C| \Rightarrow |A| \leq |C|$
 ③ антисимметричность: $|A| \leq |B|, |B| \leq |A| \Rightarrow |A| = |B| \Rightarrow$
 $\exists f: A \rightarrow B \quad g: B \rightarrow A \quad h: A \rightarrow B$
 инъекция инъекция биекция

Определение Множество называется **счётным**, если оно равномощно \mathbb{N} .

\mathbb{N} — счётно; чётные числа $2\mathbb{N}, f(x) = 2x$
 квадраты натуральных чисел: $f(x) = x^2$

Теорема \mathbb{Z} счётно.

Док-во: $\begin{array}{ccccccc} 0 & 1 & -1 & 2 & -2 & 3 & -3 \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \dots \end{array}$

$\{a_0, a_1, a_2, \dots\}$ счётно
 все элементы множества присутствуют, причём ровно единицы

Теорема a_0, a_1, a_2, \dots — все элементы множества A присутствуют $\Rightarrow A$ счётно или конечно

Док-во вычеркиваем дубли

A, B конечны, $f: A \rightarrow B$ — сюръекция $\Rightarrow |B| \leq |A|$

Теорема A счётно, $f: A \rightarrow B$ — сюръекция $\Rightarrow B$ счётно или конечно

Док-во: a_0, a_1, a_2, \dots
 $f(a_0), f(a_1), f(a_2), \dots$ — все элементы B присутствуют.

Теорема любое подмножество счётного множества A конечно или счётно

Док-во: a_0, a_1, a_2, \dots
 $B \subseteq A$, оставим в последовательности элементы B

Теорема A — бесконечное множество $\Rightarrow A$ содержит счётное подмножество B

$|B| \leq |A|$
 по опред. биекция

$\exists a_0 \in A, a_1 \in A, a_1 \neq a_0$

$a_2 \in A, a_2 \neq a_1, \neq a_0 \dots$

; и так далее

$B = \{a_0, a_1, a_2, \dots\}$ — счётно \Rightarrow
 они все разные

Теорема объединение 2-х счётных множеств счётно

Доказ. a_0, a_1, a_2, \dots b_0, b_1, b_2, \dots если есть дубли, выбросим их и останется ω элементов
 $f: \mathbb{N} \rightarrow A$, $g: \mathbb{N} \rightarrow B$ биекция
 $h: \mathbb{N} \rightarrow A \cup B$ биекция (формула)
($A \cap B = \emptyset$)

Теорема объединение конечного или счётного числа конечных или счётных множеств конечно или счётно;

Доказ. A_0, A_1, A_2, \dots не забыть выбросить дубли

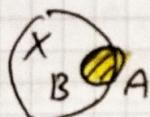
~~$\begin{array}{cccccc} a_{00} & a_{01} & a_{02} & a_{03} & \dots & a_0 \\ a_{10} & a_{11} & a_{12} & a_{13} & \dots & a_1 \\ a_{20} & a_{21} & a_{22} & a_{23} & \dots & a_2 \end{array}$~~

Следствие A, B счётны $\Rightarrow A \times B$ счётно

$B = \{b_0, b_1, b_2, \dots\}$ $A \times \{b_0\}$ счётно $A \times B = \bigcup_{i \in \mathbb{N}} (A \times \{b_i\})$ - счётное объединение счётных множеств
Эбманье $f: \mathbb{N} \rightarrow A$
 $g: \mathbb{N} \rightarrow A \times \{b_0\}$
 $g(i) = (f(i), b_0)$

Теорема X -бесконечно, A -конечно или счётно $\Rightarrow |X \cup A| = |X|$

Доказ. будем считать, что $X \setminus A$
 $A \setminus X \subseteq A$ - тоже конечно или счётно
 $\exists B \subseteq X$, B -счётно, $B \cup A$ счётно $\Rightarrow |B \cup A| = |B|$
 $f: B \cup A \rightarrow A$ -биекция
 $g(x) = \begin{cases} f(x), & x \in B \cup A \\ x, & \text{иначе} \end{cases}$ - биекция
 $X \cup A \rightarrow X$



Теорема \mathbb{Q} счётно

конечно или счётно

Доказ. $f(\langle p, q \rangle) = \frac{p}{q}$ по индукции
 \mathbb{N}^2 счётно $\Rightarrow \mathbb{N}^k$ счётно
 $k = 1, 2, 3, \dots$

$\mathbb{Z} \times (\mathbb{N} \setminus \{0\}) \rightarrow \mathbb{Q}$ - борзыеобраз

$|\mathbb{N}^{k+1}| = |\mathbb{N} \times \mathbb{N}^k| \xrightarrow{(x_1, \dots, x_{k+1}) \rightarrow (x_1, (x_2, \dots, x_{k+1}))}$

Множество всех конечных последовательностей натуральных чисел: $\mathbb{N}^0 \cup \mathbb{N}^1 \cup \mathbb{N}^2 \cup \mathbb{N}^3 \cup \dots$
конечно \uparrow счётны \uparrow

Теорема Множество бесконечных последовательностей 0 и 1 несчётно ($\Rightarrow \mathbb{N}^\mathbb{N}$ несчётно)

Доказ. от противного: пусть оно счётно \Rightarrow Эбманье

$f: \mathbb{N} \rightarrow 2^\mathbb{N}$ $f(0): a_0 a_1 a_2 \dots$

$f(1): a_{10} a_{11} a_{12} \dots$

$f(2): a_{20} a_{21} a_{22} \dots$

$f(n): b_0 b_1 b_2 \dots$ $b_i = 1 - a_{ii}$ $a_{ii} = 0 \Rightarrow b_i = 1$
 $a_{ii} = 1 \Rightarrow b_i = 0$

Определение Множество имеет мощность континуума, если оно равномощно множеству $\{0, 1\}^{\mathbb{N}}$.

A^B - множество totальных функций $B \rightarrow A$
последовательности из 0 и 1: totальная функция $\mathbb{N} \rightarrow \{0, 1\}$

$P(\mathbb{N})$ - множество всех подмножеств \mathbb{N}

$$\{0, 1\}^{\mathbb{N}} \text{-бинарный} \quad \overbrace{\dots}^A \quad A \leftrightarrow \chi_A \in \{0, 1\}^{\mathbb{N}}$$

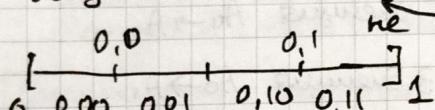
A - счётно $\Rightarrow P(A)$ - континуально

$\begin{array}{c} a_0, a_1, a_2, \dots \\ B \subseteq \mathbb{N} \\ i \in B \end{array} \rightarrow$ подмножество A

$a_i \in \text{подмнож}$

Теорема $[0, 1]$ имеет мощность континуума

бесконечное число \rightarrow двоичная запись - не функция



двоичные записи 0, ...

\downarrow бинарная
последовательность из $\{0, 1\}^{\mathbb{N}}$

\Rightarrow двоичных записей континуум

$$\frac{1}{2} = 0,1000\dots = 0,011\dots$$

не имеющие двоичные записи

\downarrow бинарный

бесконечные числа

x -бесс.

A -счётно

Сколько "иных" двоичных записей?
 $0, \dots 0111 \dots = 0, \dots 100 \dots$,
их счётное множество

и не имеющие континуум $\Rightarrow (x|)$ -континуум

Следствие $(0, 1)$ и $[0, 1]$ - континуальны

Следствие $a < b, (a, b)$ - континуалы

Следствие \mathbb{R} -континуально

$$f: (0, 1) \rightarrow (a, b)$$

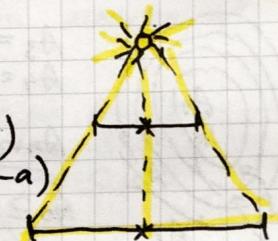
$$f(x) = a + x(b-a)$$

$$f(x) =$$

$$1(\mathbb{R}) = 1(0, 1)$$

$$f(x) = \tan x$$

$$(-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$$



$$|A| = |\mathbb{N}| \Rightarrow |P(A)| = |P(\mathbb{N})|$$

Теорема $|A_1| = |A_2|, |B_1| = |B_2| \Rightarrow |A_1 \times B_1| = |A_2 \times B_2|$

\exists бинария $f: A_1 \rightarrow A_2$ и $g: B_1 \rightarrow B_2$

хотя $h: A_1 \times B_1 \rightarrow A_2 \times B_2$

$$(x, y) \in A_1 \times B_1,$$

$$h(x, y) = (f(x), g(y))$$

$$h(x_1, y_1) = h(x_2, y_2)$$

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

$$g(y_1) = g(y_2) \Rightarrow y_1 = y_2$$

$$h(x, y) = (a, b)$$

$x = f^{-1}(a), y = g^{-1}(b) \Rightarrow h$ -сторецир

Утверждение $|\{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}$

$$\in \{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}} \rightarrow (x_0, y_0, x_1, y_1, \dots) \in \{0, 1\}^{\mathbb{N}}$$

Теорема $|A| = |A_1|, |B| = |B_2| \Rightarrow |A_1 \times B_2| = |A_2 \times B_1|$

Теорема $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}| \quad |\mathbb{R}^k| = |\mathbb{R}|$ симметрия

Теорема $|\mathbb{R}^\mathbb{N}| = |\mathbb{R}|$

Это доказательство $\varphi: \mathbb{R} \rightarrow \{0, 1\}^\mathbb{N}$
 $\mathbb{R}^\mathbb{N} \ni (a_0, a_1, a_2, \dots) \xrightarrow{\text{доказательство}} (\varphi(a_0), \varphi(a_1), \varphi(a_2), \dots) \in (\{0, 1\}^\mathbb{N})^\mathbb{N}$

$$(\{0, 1\}^\mathbb{N})^\mathbb{N} \rightarrow \{0, 1\}^\mathbb{N}$$

$$\downarrow \varphi^{-1}$$

$$\mathbb{R}$$

$$\begin{aligned}\varphi(a_0) &= a_{00} \quad a_{01} \quad a_{02} \dots \\ \varphi(a_1) &= a_{10} \quad a_{11} \quad a_{12} \dots \\ \varphi(a_2) &= a_{20} \quad a_{21} \quad a_{22} \dots\end{aligned}$$

Теорема Кантора - Бернштейна

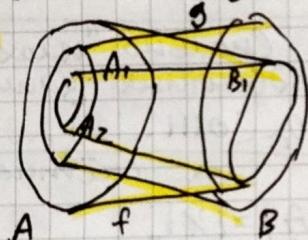
$|A| \leq |B|, |B| \leq |A| \Rightarrow |A| = |B|$
 Э инъекция, Э инъекция
 $A \rightarrow B \quad B \rightarrow A$ симметрия

Теорема-2 $A_0 \supseteq A_1 \supseteq A_2, |A_0| = |A_2| \Rightarrow |A_0| = |A_1| = |A_2|$

(1 \Rightarrow 2) $A = A_0, B = A_1, f_1: A_0 \rightarrow A_1$ - это доказательство $A_0 \rightarrow A_2$
 симметрия

$g: A_1 \rightarrow A_0, g(x) = x$ - инъекция \Rightarrow 3 доказательство $A_0 \rightarrow A_1$

(2 \Rightarrow 1)



$$\begin{aligned}A_1 &= g[B] & B_1 &= f[A] \\ A_2 &= g[B_1] = (g \circ f)[A] \\ g \circ f: A_0 &\rightarrow A_2 - \text{доказательство} \Rightarrow \\ \Rightarrow |A_0| &= |A_1| = |A_2| \quad (g\text{-доказательство}) \Rightarrow \\ \Rightarrow |A_0| &= |B|\end{aligned}$$

Доказательство-2 $f: A_0 \rightarrow A_2$ - доказательство

$$\begin{aligned}A_3 &= f[A_1] & C_i &= A_i \setminus A_{i+1} \\ A_4 &= f[A_2] & C &= \bigcap_{i=0}^{\infty} A_i \\ A_{n+2} &= f[A_n] & \uparrow & \\ A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq A_4 \supseteq \dots & \xrightarrow{f} \xrightarrow{f} \xrightarrow{f} \xrightarrow{f} \end{aligned}$$

$g := \begin{cases} f(x), & \text{если } x \in C_2 \\ x, & \text{иначе} \end{cases}$

Факт $X \subseteq Y$
 \downarrow
 $f[X] = f[Y]$

$$A_0 = C_0 \cup C_1 \cup C_2 \cup C_3 \cup \dots \cup C$$

все эти множества не пересекаются

$f: C_i \rightarrow C_{i+2}$ - доказательство

$$A_0 = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup \dots \cup C$$

$$A_1 = \xrightarrow{f} C_1 \cup C_2 \cup C_3 \cup C_4 \cup \dots \cup C$$

Пример $\mathbb{N}^\mathbb{N}$ компактно
 $\{0, 1\}^\mathbb{N} \subseteq \mathbb{N}^\mathbb{N} \subseteq \mathbb{R}^\mathbb{N}$, компактно

Теорема X не равносильно $\mathcal{P}(X)$

(Кантор)
 Для противного, пусть f -доказательство, $X \rightarrow \mathcal{P}(X)$

$$Y = \{x \in X : x \notin f(x)\} \subseteq X$$

$x \in Y \Leftrightarrow x \notin f(x)$ для любого $x \in X$

$\exists z \in X, f(z) = Y$ (т.к. f -доказательство)

$x \in f(z) \Leftrightarrow x \notin f(x)$ \Rightarrow противоречие

$z \in f(z) \Leftrightarrow z \notin f(x)$

Следствие 1 $|x| < |P(x)|$

Эквивалентно $x \rightarrow \{x\}$
то есть вложим по Кантору

Следствие 2 пусть $|x| = n \in \mathbb{N}$, $n < 2^n$

Следствие 3 не существует множества всех множеств

пусть \mathcal{U} -множество всех множеств

$$P(\mathcal{U}) \subseteq \mathcal{U}$$

$$|P(\mathcal{U})| \leq |\mathcal{U}|$$

$$|\mathcal{U}| < |P(\mathcal{U})|$$

ЛЕКУНИЯ-10. 14.11.23

Определение Бинарное отношение на множествах $A \cup B$
- подмножество $A \times B$.

бинарное отношение на множестве - подмножество $A \times A$.

R_1 и R_2 на множествах A и B :

$$R_1 \cup R_2, R_1 \cap R_2, R_1 \setminus R_2, R_1 = (A \times B) \setminus R_1$$

Функций-частичный случай

$$\text{Dom } R = \{x \in A \mid \exists y \in B \quad (x, y) \in R\}$$

$$\text{Range } R = \{y \in B \mid \exists x \in A \quad (x, y) \in R\}$$

$$A = \{1, 2, 3, 4\}$$

$$B = \{1, 2, 3\}$$

$$R = \{(1, 1), (1, 2),$$

$$(2, 2), (4, 1)\}$$

$$\text{Dom } R = \{1, 2, 4\}, \text{ Range } R = \{1, 2\}$$

Определение Обратное отношение -

$$R^{-1} = \{(y, x) \mid (x, y) \in R\} \text{ на множествах } B \text{ и } A.$$

$\text{Dom } R^{-1} = \text{Range } R, \text{ Range } R^{-1} = \text{Dom } R$ $g(f(x)) = (g \circ f)(x)$
 R_1 на множествах $A \cup B, R_2$ на множествах $B \cup C$
 $R_2 \circ R_1 = \{(a, c) \mid \exists b \in B \quad (a, b) \in R_1 \wedge (b, c) \in R_2\}$ на множествах $A \cup C$

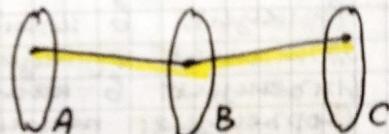
Пример $R - "x > y"$ на \mathbb{N} R^{-1}

$(a, b) \in R^{-1}, R^{-1} - "b \text{ больше } a"$

$R_1 - "x - \text{мужчина } y", R_2 - "y - \text{дочь } z" \Rightarrow$

$R_2 \circ R_1 \ni (x, z) \Rightarrow x - \text{мужчина/женщина } y, z$

$R_1 \circ R_2 \quad a - \text{дочь } b, b - \text{мужчина } z \Rightarrow "z - \text{жена или жена } a"$



Свойства

$$1. (R^{-1})^{-1} = R$$

$$2. (T \circ R) \circ S = T \circ (R \circ S)$$

$$3. (S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

$$(x, y) \in (S \circ R) \Rightarrow \exists z (y, z) \in R, (z, x) \in S$$

$(y, x) \in S \circ R$

S - на $A \cup B$

R - на $B \cup C$

T - на $C \cup D$

стационарное: $A \times A$

пустое:

$$id_A : \{(x, x) \mid x \in A\}$$

Определение

рефлексивное: $\forall x \in A \quad (x, x) \in R$

$$id_A \subseteq R$$

Определение

антирефлексивное: $\forall x \in A \quad (x, x) \in R \Rightarrow id_A \cap R = \emptyset$

симметрическое: $\forall x, y \in A \quad (x, y) \in R \Rightarrow (y, x) \in R \Rightarrow R = R^{-1}$

анисимметрическое: $\forall x, y \in A \quad (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$

$$R \cap R^{-1} \subseteq id_A$$

транзитивность: $\forall x, y, z, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R \Rightarrow R^2 \subseteq R$

$$R^2 = R \circ R$$

Доказательство $\Rightarrow R^2 \subseteq R \quad (x, z) \in R^2 \Rightarrow \exists y (x, y) \in R, (y, z) \in R$

$\Rightarrow (x, z) \in R, \text{ т.е. } R^2 \subseteq R$

$\Leftarrow (x, y) \in R, (y, z) \in R, \text{ по определению композиции } (x, z) \in R^2 \subseteq R,$

т.е. $(x, z) \in R$ - проверим транзитивность

рефлексивность + антирефлексивность: $A = \emptyset, R = \emptyset$

симметрическость + анисимметрическость: $A - \text{такое}, R \subseteq id_A$

\emptyset - транзитивность, $\{(a, b)\}$ - транзитивность

Пример $A = \{1, 2, 3, 4\}$
 $R = \{(1, 1), (1, 2), (3, 1), (3, 4), (4, 3)\}$

$$A = \{a_1, \dots, a_4\} \quad B = \{b_1, \dots, b_4\}$$

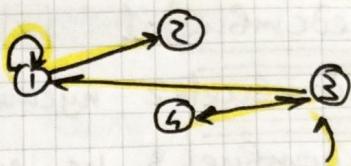
$a_i \begin{pmatrix} & \\ & B \\ & \end{pmatrix}$ 1 на месте $(i, j) \Leftrightarrow (a_i, b_j) \in R$, иначе 0

R^T -транспонированная матрица

R -матрица A , S -матрица B

SOR -матрица AB , заменили все $n > 1$ на 1

$$(-)(|) = \begin{pmatrix} c_{ij} \\ | \end{pmatrix}_i \quad c_{ij} = \sum_k a_{ik} b_{kj} \quad (x_i, x_j) \in SOR \Leftrightarrow \exists k (x_i, x_k) \in R, (x_k, x_j) \in S$$
 $c_{ij} \geq 0 \Leftrightarrow \begin{cases} a_{ik}=1 \\ b_{kj}=1 \end{cases}$



$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Матрицы и виды отношений

Рефлексивно:

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

Антирефлексивно:

$$\begin{pmatrix} 0 & & \\ & 0 & \\ & & 0 \end{pmatrix}$$

Симметрично:

$$\begin{pmatrix} & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

Анисимметрично:

$$\begin{pmatrix} & & \\ & 0 & 1 \\ 0 & & 0 \end{pmatrix}$$

Транзитивность:

A -матрица R \Rightarrow нет ли та же, \Rightarrow нет \Rightarrow транзитивна
 A^2 , заменим на 1, \Rightarrow что у A^2 стоит 1 \Rightarrow 1 та же, где у A 0 \Rightarrow да \Rightarrow нет транзитивна

Руками: в каждой строке ≤ 1 единица

Моментная формула: $\frac{1}{1} = 1$ единица

Инверсия: в каждой строке ≤ 1 единица + моментная

Сортировка: моментность + в каждой строке ≥ 1 единица

Определение

транзитивное замыкание - R -б/о на множ A .

$\exists x \frac{1}{1} = R^*$ - транзитивное

отношение, $R \subseteq R^*$, любое транзитивное отношение T ,
если $R \subseteq T$, то $R^* \subseteq T$

R : "x - родитель y" R^* : "x - предок y"

R : "x = y + 1" на N R^* : "x \gg y"

① если R -транзитивно, то $R^* = R$

② $R^{**} = R^*$, R^* -транзитивно

Лемма

R_i - все транзитивны, $i \in I \neq \emptyset \Rightarrow \bigcap_i R_i$ - транзитивно

$$(x, y), (y, z) \in \bigcap_i R_i \quad (x, y), (y, z) \in R_i \quad (x, z) \in \bigcap_i R_i \quad (x, y) \in \bigcap_i R_i$$

Теорема

R^* существует всегда

Доказ. все R_i -транзитивны и $R \in R_i$ наличие в этой паре

$\bigcap_i R_i$ - транзитивно, $R \subseteq \bigcap_i R_i$

любое транзитивное $T \supseteq R$, $T = R_i$ для некоторых i , $\bigcap_i R_i \subseteq T$

Теорема

$$R^* = R \cup R^2 \cup R^3 \cup \dots \cup R^n \cup \dots = T$$

$$R \subseteq T, T \text{-транзитивно}, (x, y), (y, z) \in T \quad (x, z) \in R^* \quad (x, z) \in T$$

$$(x, z) \in R^{n+1} = R^n \circ R^n$$

$T \subseteq R^*$ база: $R \subseteq R^{n+1}$ шаг: пусть $R^n \subseteq R^* \Rightarrow R^{n+1} \subseteq R^*$
 $(x, z) \in R$ $(x, y) \in R^n, (y, z) \in R$ $(x, z) \in R^*$ по
 Лекция-11 21.11.23

Граф — конечное множество вершин и рёбра соединяют разные вершины.

Простые неориентированные графы: нет петель, нет спиралей, нет изолированных рёбер.

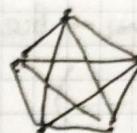
Луны:



Цикл:



Полный граф:



V — множество вершин
 E — множество рёбер состоящих из 2-элемент. подмножеств из $\{v_i, v_j\} \in E \quad \forall i, j \in V$
 смежные, соседние вершины
 ребро инцидентно вершинам v_i, v_j
 v_i, v_j — концы ребра $\{v_i, v_j\}$

Матрица смежности $\delta_1, \dots, \delta_n$

v_1, v_2, \dots, v_m	v_1, v_2, \dots, v_m
v_1	1
v_2	
\vdots	
v_n	

$$\delta_{i,j} = 1 \Leftrightarrow (v_i, v_j) \in E$$

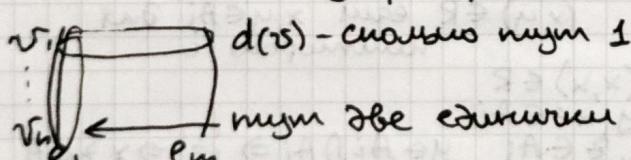
e_1, e_2, \dots, e_n	e_1, e_2, \dots, e_n
v_1	1
v_2	
\vdots	
v_n	1

$$e_i = (v_j, v_k) \quad (j, i) = 1, (k, i) = 1$$

Граф — анимироффлексивное симметричное бинарное отношение.

Степень вершины $d(v)$ — число рёбер из неё идёт

Теорема Сумма степеней вершин равна удвоенному числу рёбер.



Ки — полный граф на n вершинах:
 $n-1$ — степень каждой вершины
 $\frac{n(n-1)}{2} = C_n^2$

Существует ли граф, в котором 77 вершин, где степень каждой $= 15$. $77 \cdot 15 / 2 \neq$ не существует.

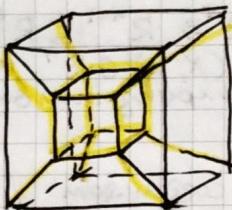
Лемма о рукоопомажах В графе число вершин с чётными степенями — чётное.

$$d(v_1) + d(v_2) + \dots + d(v_n) — чётное$$

+ чётное не меняет чётность
 + нечётное меняет чётность

Будь куб: вершины $\{0, 1\}^n$
 одно слово получается из
 другого заменой ровно 1 символа.

$d(v) = n$
 сумма степеней $= 2^n \cdot n$
 рёбер: $2^{n-1} \cdot n$



гиперкуб (4 измерения)
в нем связанные.

Путь в графе — последовательность вершин v_0, \dots, v_n , каждая из которых соединена ребром со следующей.

$\{v_i, v_{i+1}\} \in E \quad \forall i=0, \dots, n-1$
длина пути $v_0 \dots v_n$ — число и
 v_i, v_j — связанные, если существует путь
с началом v_i и концом v_j

Граф **связан** — любые две вершины

n вершин
0 рёбер $n > 1$ — не связан

Вершин — все перестановки из n элементов $S_n : n!$

(..., ..., ..., ..., ...) $\rightarrow (4, 3, 2, 6, 1, 5) \rightarrow (6, 2, 3, 4, 1, 5)$. Граф связан:
разбором $(\dots, \dots) \rightarrow (1, \dots, n) \rightarrow (\dots, \dots)$

$(x_1, \dots, x_{i-1}, \dots, x_{i+1}, \dots, x_n) \rightarrow (x_{i-1}, \dots, x_i, x_{i+1}, \dots, x_n) \rightarrow$
 $\rightarrow (x_n, \dots, x_{i+1}, x_i, \dots, x_{i-1}, x_i) \Rightarrow$ далее по индукции

Отношение достижимости $R \subseteq V \times V$: $(u, v) \in R$, если они связанные

→ **рефлексивно**: $(u, u) \in R$, u — путь

→ **симметрично**: $(u, v) \in R \Rightarrow (v, u) \in R$ $u \dots v$ — путь

→ **транзитивно**: $(u, v) \in R, (v, w) \in R \Rightarrow (u, w) \in R$ $u \dots v, v \dots w$ — путь $u \dots v \dots w$ — путь

Граф $G \rightarrow$ бинарное отношение A_G

$(v, u) \in A_G \Leftrightarrow \{v, u\} \in E$

R — **отношение достижимости** — транзитивное замыкание $A_G \cup id_V$

T — **отношение транзитивного замыкания** $T \cup T^2 \cup T^3 \cup \dots$

$$id_V = T^0 \quad R = id_V \cup A_G \cup A_G^2 \cup A_G^3 \cup \dots$$

Отношение эквивалентности — рефл., симм., транзитивн.

- достижимость

- равенство ($=$)

$A = \bigcup_i A_i$, $A_i \cap A_j = \emptyset$ ($i \neq j$) $(x, y) \in R$ если $x, y \in A_i$ для некоторого i

→ **рефлексивность**: $x, x \in A_i$ $(x, x) \in R$

→ **симметричность**: $x, y \in A_i$ $y, x \in A_i$

→ **транзитивность**: $x, y \in A_i, y, z \in A_j$ $y \in A_i \cap A_j \Rightarrow i=j \Rightarrow x, z \in A$

Теорема | любое отношение эквивалентности R разбивает множество A на классы эквивалентности, они не пересекаются, $(x, y) \in R \Leftrightarrow$ они лежат в одном классе

Доказ.: $x \in A \mapsto C(x) = \{y \in A : x R y\}$

① $\bigcup_{x \in A} C(x) = A$ $x \in C(x)$ по рефлексивности

② $C(x) \cap C(y)$ либо не пересекаются, либо совпадают.

пусть они пересекаются, т.е. существует $z \in C(x) \cap C(y)$

$x R z$ и $y R z \Rightarrow z R y \Rightarrow x R y \Rightarrow y \in C(x)$

или $x R z$ и $y R z \Rightarrow z R x \Rightarrow y R x \Rightarrow x R y$

таким образом $x R y$, т.е. $x \in C(y)$

таким образом $y \in C(x)$

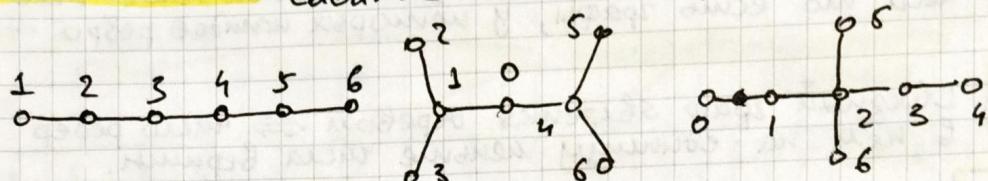
$C_y \subseteq C(x)$

$C(x) \subseteq C(y)$

Компонента связности: $\{C(x) : x \in U\}$ — компоненты связности

ЛЕКУНИЯ-12 28.11.23

Определение Дерево - это такой связный граф, что выделывание любого его ребра даёт несвязный граф.



Определение Мост — такое ребро в графе, что его удаление увеличивает количество компонент связности. Деревья — связные графы, каждое ребро которых — мост. Примитивные графы, у которых каждое ребро является мостом, называются лесами.

Определение **Цикл** — замкнутый путь по графу. **Простой цикл** — цикл, в котором все вершины различны. (аналогично для **простого пути**)

Принцип наименьшего члена любое бесконечное подмножество натуральных чисел содержит наименьший элемент.

Утверждение Если две вершины x и y связанные в графе G , то в этом графе существует простой путь с началом x и концом y .

Теорема Следующие свойства простых неориентированных графов равносильны:

Следствие | Следующие свойства связных простых неориентиро-
ванных графов равносильны!

- ① граф — дерево
- ② для любых двух вершин u, v существует единственный простой путь из u в v
- ③ нет простых циклов длины больше 2.

Задача 60: $\exists \Rightarrow \exists$ ~ $\neg \exists \Rightarrow \neg \exists$ нужно в G есть Ct , $t > 2$
 вершины но и $v_1 \in Ct$ соседние $\Rightarrow \exists$ хотя бы 2 вершины
 с концами в этих вершинах.

$\neg(1) \Rightarrow \neg(3)$ пусть ребро e можно удалить и число компонент связности не увеличится $\Rightarrow G' = G - e$
 x и y связаны $\Rightarrow G'$ есть простой путь и в G есть простой цикл.

$\neg(2) \Rightarrow \neg(1)$ Пусть между \bar{x} и \bar{y} есть два простых пути (x_0, x_1, \dots, x_r) и (y_0, y_1, \dots, y_s) . $x_0 = y_0 = \bar{x}$, $x_r = y_s = \bar{y}$. Возьмём максимальное возможное начало: $\max i, x_i = y_i$. $0 \leq j \leq i \Rightarrow x_{i+j} \neq y_{i+j}$ и $\{x_i, x_{i+1}\} \notin E$ но $\{x_i, x_{i+1}\} \subseteq E$. $\{x_i, x_{i+1}\}$ — не мост (x_i, x_{i+1} остаются в одном компоненте связности) \Rightarrow общее количество мостов не изменяется.

Числоматическое число графа G , где n -количество вершин, m -количество рёбер, а количество компонент связности c .

$$r(G) = m - n + c$$

Теорема Графы, у которых числоматическое число

равно 0 — леса, то есть графы, у которых каждое ребро — мост.

Следствие Связный граф является деревом \Leftrightarrow число рёбер в нём на единицу меньше числа вершин.

Утверждение Пусть граф $G' = G + e$ получается из графа G добавлением ребра $e = \{x, y\}$ к множеству рёбер, а вершины y нет тут.

Пусть $r(G) = r(G')$, если концы ребра x, y лежат в разных компонентах связности графа G и $r(G') = r(G) + 1$, иначе

Доказательство: x, y лежат в одной компоненте связности с графа G \Rightarrow их количество не изменилось \Rightarrow число увеличилось на 1. Иначе в общество досчитанности добавляется $C(y)$, т.к. в G' вершина y изолирована из $x \Rightarrow C(x) = C(y) = C(x) \cup C(y) \Rightarrow$ количество компонент связности уменьшилось на 1, а количество рёбер увеличилось на 1 $\Rightarrow r(G) = r(G')$, ч.т.д.

Доказательство теоремы: индукция по числу рёбер графа

Лемма Числоматическое число графа неотрицательное.

Доказательство: (индукция) пусть $r(G) \geq 0 \quad \forall G$ с $< k$ рёбрами, $k > 0$. $\forall G'$ с k рёбрами и мостом $e = \{x, y\} \Rightarrow r(G' - e) \geq 0$; где a $r(G' - e) \geq 0$ — предположение индукции

Пусть теорема выполняется для G с $< k$ рёбрами, $k > 0$. Если $r(G) > 0$, то найдётся ребро-мост $\Rightarrow G$ -лес. Пусть G -лес \Rightarrow в G -е нет простых цепей длины > 2 , т.к. в такой цепи — проходит и в G $\Rightarrow G$ -е лес. Это индукция $r(G - e) = 0$, но e -мост $\Rightarrow r(G) = r(G - e) = 0$, ч.т.д.

Определение Вершины степени 0 — изолированные, а степени 1 — висячие.

Теорема В дереве с хотя бы двумя вершинами \exists хотя бы две висячие вершины

Доказательство: пусть в дереве n вершин \Rightarrow в нём $n-1$ ребро

$$d_1, d_2, \dots, d_n \text{ — степени вершин} \Rightarrow d_1 + \dots + d_n = 2(n-1) \Rightarrow (d_1-2) + (d_2-2) + \dots + (d_n-2) = -2$$

$$d_i > 0 \Rightarrow (d_i-2) \geq -1 \Rightarrow \text{наибольшая из } 2 \text{ слагаемых} = -1;$$

$$d_i-2 = 1-2 = -1 \Rightarrow \text{это и есть висячие вершины.}$$

Определение Подграф графа — подмножество вершин и ребер с копиями в этих вершинах.

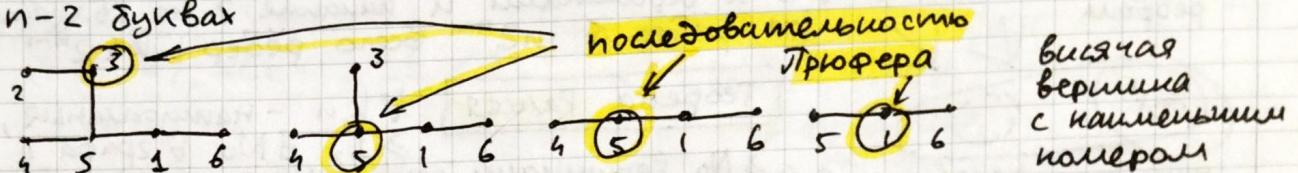
Индуктированный граф — выбираются все ребра с копиями в выбранных вершинах.

Подграф называется основным, если его множество вершин совпадает с множеством вершин самого графа.

Теорема В любом связном графе есть основное дерево.



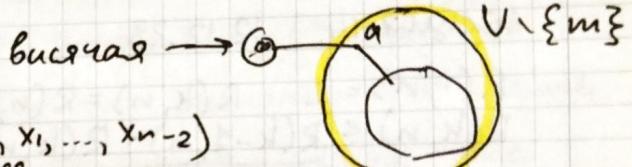
Теорема (Кэли) Деревьев на n замкнутых вершинах n^{n-2} — число последовательностей длины $n-1$ на $n-2$ буквах



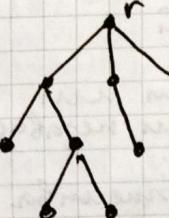
Существует биекция между деревьями на вершинах из конечного $V \subseteq \mathbb{N}$ и последовательностями длины $|V|-2$ элементов V

База
 $|V|=2$ \rightarrow биекция пусто

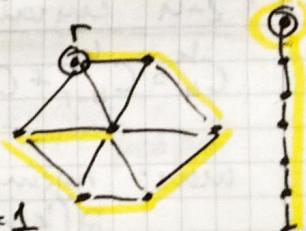
шаг
 $|V|=n+1$ последовательность (a, x_1, \dots, x_{n-2})
 $a \in V \setminus \{x_1, \dots, x_{n-2}\}$, a — наименьшее
последовательность (x_1, \dots, x_{n-2}) — дерево с вершинами $V \setminus \{a\}$



Определение Корневое дерево! $r \in V$ — корень
и выше r , $v \notin V$ и лежит на
простом пути из r в v



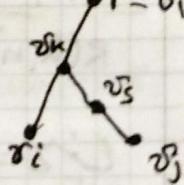
Определение Монотонное основное дерево:
выделен корень и k ребра
 $\{v_i, v_j\}$ из графа G одна из вершин лежит
выше другой.



Теорема В любом связном графе существует монотонное основное дерево.

Док-бо: r — любая вершина, v_1 — связь и
шаг +1 в., +1 ребро, v_1 — вершины = ребер +1
связность сохраняется и в 'новом'
дерево. Пусть построено (v_1, \dots, v_i) дерево
 $v_i \in V \setminus \{v_1, \dots, v_{i-1}\}$ — надо выбрать
ребро (v_i, v_j) , где j — максимальное. $1 \leq j \leq i$ добавляем вершину
и получим монотонное? пусть не так. \Rightarrow
если ребра в графе (v_i, v_j) — ни одна из них не выше другой: $i < j$
Выберем v_k , выше v_i, v_j , к максимально, $k > i, k < j$

Рассмотрим момент, когда добавим вершину v_k .
Почему добавили её, а не ребро (v_i, v_j) ?



Определение Клика — индуцированный подграф,
в котором любые 2 вершины
соединенны ребрами

Определение

Независимое множество — подграф, в котором любые 2 вершины не соединены ребром.

$w(G)$ — max размер независимого множества, число независимости

$$w(G) = \alpha(\bar{G}), \quad \alpha(G) = w(\bar{G})$$

K_n — полный граф
 $w(K_n) = n$ $\alpha(K_n) = 1$

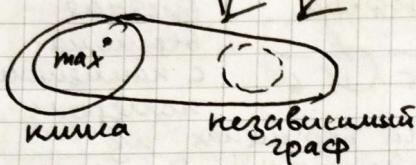


Q_n — бүлэг нүд

$w(Q_n) = 2$, если $n \geq 1$

$\alpha(Q_n) = 2^{n-1}$ пример последовательности с числом единиц одинаковой чётности

Лусий подграф с k вершинами и никакие 2 не связаны ребром
количество рёбер $\leq n2^{n-1}$ всего рёбер $k \leq 2^{n-1}$



Теорема Райса

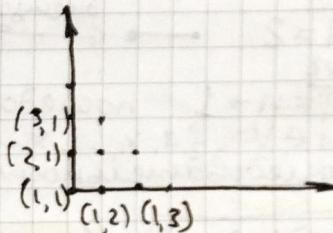
$\forall k, n \in \text{натуральные},$
 $\geq 1, \exists N$ \forall графа с
 $\geq N$ вершинами есть исхода размера k
или независимое множество размера n
 $R(k, n)$ — число Райса, мин N

ЛЕКУЧИЙ-14. 12.12.23.

$$R(1, n) = 1 \quad R(k, n) = R(n, k)$$

$$R(k, n) \leq R(k-1, n) + R(k, n-1)$$

L вершин



$R(k-1, n)$ вершины или хотят быть $R(k-1, n)$ соседей
или хотят быть $R(k, n-1)$ не-соседей

Случай 1

$R(k-1, n)$ соседей. В нём или
имеет размера $k-1$, или независи-

мое множество размера n .

2-й случай, аналогично для независимого множества

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

Верхняя оценка

$$R(k, n) \leq C_{k+n-2}^{k-1} = C_{k+n-2}^{n-1}$$

шаг; пусть верно для некоторого $k+1$

$$\begin{aligned} R(k, n) &\leq R(k-1, n) + R(k, n-1) \leq C_{k-1+n-2}^{k-1-1} + C_{k+n-1-2}^{k-1} = C_{k+n-2}^{k-1} \\ k > 1 & \\ n > 1 & \\ S+1 & \text{ предположение} \end{aligned}$$

$$R(3, 3) = 6 \quad C_{3+3-2}^{3-1} = 6 \quad R(2, n) = n \quad C_{2+n-2}^{3-1} = n$$

$$R(3, n) - ? \quad R(6, 6) \leq C_{6+6-2}^{6-1} = C_{10}^5$$

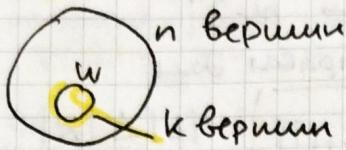
$$R(k, n) \leq R(k-1, n) + R(k, n-1) - 1, \text{ если } R(k-1, n) \text{ чётные}$$

$L/2 \Rightarrow$ есть вершина чётной степени — это v

v • $L-1$ вершины чётные у v или $R(k-1, n)$ соседей, хотят быть или $R(k, n-1)$ несоседей, хотят быть иначе $R(k-1, n)-2 + R(k, n-1)-2$ число вершин

Нижняя оценка $R(k, k) \geq k$, $R(k, k) > (k-1)^2$

Теорема $R(k, k) > \lfloor 2^{\frac{k-1}{2}} \rfloor \cdot 2^{C_n^2}$ для $k \geq 3$



$2 \cdot 2^{C_n^2 - C_k^2}$ - графы, в которых w или клик, или независимое множество, A_w есть клик или независимое множество.

$$|A| = |\bigcup_w A_w| \leq \sum_w |A_w| = C_n^k \cdot 2^{C_n^2 - C_k^2 + 1} < 2^{C_n^2}$$

$$C_n^k \cdot 2^{C_n^2 - C_k^2 + 1} < 1 \Rightarrow n(n-1) \cdots (n-k+1) \cdot 2^{-C_k^2 + 1} < \frac{n^k}{k!} 2^{-C_k^2 + 1} \leq$$

$$\leq \frac{(2^{\frac{k-1}{2}})^k}{k!} 2^{-C_k^2 + 1} = \frac{2^k}{k!} < 1$$

$$C_{2k-2}^{k-1} \geq R(k, k) > 2^{\lfloor \frac{k-1}{2} \rfloor}$$

$$\frac{2^{2k}}{\sqrt{k}} \cdot \Theta(1) \quad \begin{matrix} \text{ограничена,} \\ \text{не } \delta/\epsilon \end{matrix}$$

РАСКРАСКА ГРАФОВ

Определение Раскраска - минимальная функция $V \rightarrow \{1, \dots, k\}$ номера красок

Правильная раскраска: $\{x, y\} \in E \Rightarrow C(x) \neq C(y)$
k-раскрашиваемый граф: Э правильная раскраска в k цветов.

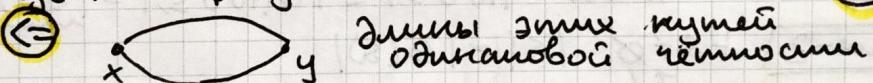
Определение $\chi(G)$ - хроматическое число графа - мин k, что

$$\chi(G) = 1 - \text{кем рёбер}$$

$$\chi(G) = 2 - ?$$

Теорема G - 2-раскрашиваемый, если там все циклы чётной длины.

Доп-бы: цвета чередуются \Rightarrow это очевидно \Rightarrow



если путь из y в x чётной длины, то краски x в цвет-1, а y в цвет-2.

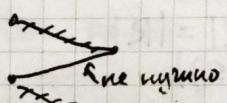
$$\{x, y\} - \text{ребро}$$

$$xy \dots x$$

$$y \dots xy$$

ЛЕКЦИЯ-15 09.01.24

Определение Двудольный граф \leftrightarrow бинарное отношение на L и R. Множество вершин раздelenо на две доли: L - левую и R - правую. Любое ребро имеет вид (v, u) , $v \in L$, $u \in R$



дели фундами

Определение Паросочетание - граф, степень каждой вершины равна 1.

Определение Размер паросочетания - количество рёбер.

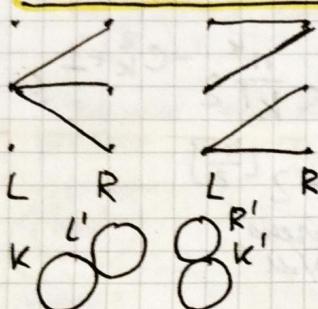
Определение С совершенное паросочетание в графе G - каждая вершина G попала в паросочетание.

K_{2n} сколько в нём совершенных паросочетаний? P_{2n}

$\{x_1, x_2, \dots, x_{2n}\} \xrightarrow{\text{перестановка } 2n!} \{\{x_1, x_2\}, \{x_3, x_4\}, \dots, \{x_{2n-1}, x_{2n}\}\}$
паросочетаний $n! \cdot 2^n$

$(2n)! = n! \cdot 2^n \cdot P_{2n}$ L-левая доля, R-правая доля

$$P_{2n} = \frac{(2n)!}{n! \cdot 2^n} = \frac{2n!}{2 \cdot 4 \cdot 6 \cdot \dots \cdot 2n} = 1 \cdot 3 \cdot \dots \cdot (2n-1) = (2n-1)!! \quad |L| \leq |R|$$

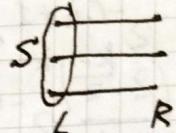


Необходимое условие: $\forall S \subseteq L \quad G(S)$ - множество соседей всех вершин из S

$$|G(S)| \geq |S|$$

$$|G(k)| = k-1 \in |k|$$

$$S \subseteq k \quad G(S) = k' \quad S \cap L' \neq \emptyset \quad G(S) = R$$



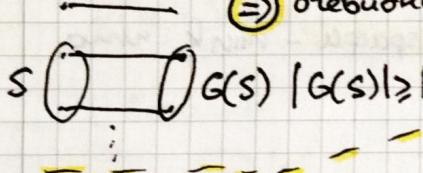
$$|k| = k \quad |k'| = k-1$$

$$L = L' \cup k \quad R = R' \cup k'$$

$$|L'| = n \quad |R'| = n+1$$

Теорема Хами $G = (L, R, E)$ - двудольный
граф. В G есть паросочетание размера $|L| \Leftrightarrow \forall S \subseteq L \quad |G(S)| \geq |S|$.

Док-бо: \Leftarrow индукция по размеру $|L|$
база $|L|=1$



\Rightarrow очевидно

\Leftarrow индукция по размеру $|L|$

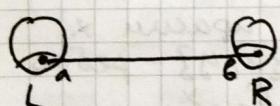
база $|L|=1$

переход $|L| < n$ - для таких все ок

Следствие-1 $\exists S \neq \emptyset \quad S \neq L \quad |S| = |G(S)|$

$$\begin{aligned} S &\not\subseteq G(S) \quad T \subseteq S \quad G(T) \text{ в новом графе такое же,} \\ X &\not\subseteq G(Y) \quad |G(T)| \geq |T| \text{ для старого графа} \\ &N \subseteq X \quad |N \setminus S| \leq |G(N \setminus S)| = |G(S)| + |G'(N)| \end{aligned}$$

Следствие-2 $\forall S \neq \emptyset \quad |S| < |G(S)|$



$S \subseteq L \setminus \{a\}$ $G(S)$ можно поменять разве что в
было: $|S| < |G(S)|$
стало: $|S| \leq |G(S)|$

Определение Регулярный граф - граф, у которого степени всех вершин равны.

Следствие В регулярном графе (степени вершин > 0) есть совершенные паросочетания.

Док-бо: d - степень вершины $|L|d = |R|d \Rightarrow |L| = |R|$
 $S \subseteq L \quad |S| \cdot d \leq |G(S)|d \Rightarrow |S| \leq |G(S)|$

Следствие Регулярный двудольный граф степени каждой вершины d . Его рёбра можно разбить на d паросочетаний.

Док-бо: 1 паросочетание есть, вынимем его \Rightarrow
степень каждой вершины $= d-1$.

Вершинное покрытие графа - множество вершин S графа G , чтобы были один из концов любого ребра лежали в S .
 $\tau(G)$ - мин. размер вершинного покрытия

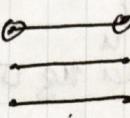
[Определение]

$$K_3 \triangleq \tau(K_3) = 2$$

Лемма S -вершинное покрытие $\Leftrightarrow V \setminus S$ - независимое множество. $\tau(G) + \alpha(G) = |V|$

$\mu(G)$ - размер max паросочетания (кн-во рёбер) [Определение]

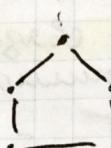
Теорема $\tau(G) \geq \mu(G) \quad \forall G$



паросочетание
одна из них
должна быть в вершинном покрытии

Теорема Кёнига G -эзубильный
 $\Rightarrow \tau(G) = \mu(G)$

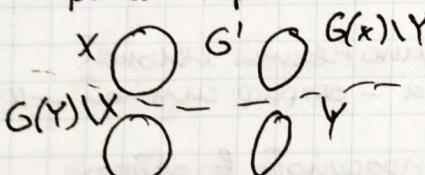
Док-бо: $\tau(G) \geq \mu(G)$
уче дополнено



$$\tau(G) = 3$$

$$\mu(G) = 2$$

хочу: $\tau(G) \leq \mu(G)$
рассмотрим min вершинное покрытие $X \cup Y, X \subseteq L, Y \subseteq R$



$S \subseteq X$
 $|S| \leq |G'(S)|$
 $(X \setminus S) \cup G'(S) \cup Y$ - тоже вершинное покрытие, а оно множеством $|X| + |Y|$

если вдруг

$|S| > |G'(S)|$

ЛЕКУЧИЯ-16. 16.01.24

[Определение] Простой ориентированный граф - множество вершин и рёбер E . E состоит из упорядоченных пар множества V .

$$E \subseteq V \times V$$

$$u \xrightarrow{v} (u, v) \in E$$

матрица смежности:

$$(u, v), (v, u) \in E$$

$$u_i \begin{pmatrix} & \\ & 1 \end{pmatrix}$$

$$a_{ij} = 1 \Leftrightarrow (u_i, u_j) \in E$$

$$\bigcirc (u, u) \in E$$

[Определение] Входящая степень - количество входящих в вершины рёбер.

[Определение] Исходящая степень - количество выходящих из вершин рёбер.

Теорема Сумма всех входящих степеней равна сумме всех исходящих степеней и равна количеству всех рёбер в графе.

[Определение] Путь в орграфе - последовательность вершин $v_0, v_1, \dots, v_t, (v_i, v_{i+1}) \in E \quad \forall i = 0, \dots, t-1$

[Определение] Простой путь - кем одинарных вершин.

[Определение] Цикл - путь, т. ч. $v_1 = v_t$

Определение

Простой цикл: $v_0 = v_t$, остальные разные.

Определение

Простой в рёбрах путь — все рёбра разные.

Определение

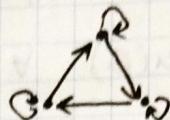
и достижима из вершины v существует путь v, \dots, u

Теорема

Отношение достижимости в орграфе рефлексивно и транзитивно.

$v \rightarrow u$

v достижима из u и не достижима из u



Определение

u, v сильно связаны, если и достижима из u и u достижима из v .

Теорема

Отношение сильной связности рефлексивно, симметрично, транзитивно.

Определение

Классы эквивалентности — компоненты сильной связности, 1 компонента — орграф сильной \Rightarrow .

Определение

Эйлеров граф — существует простой в рёбрах цикл, проходящий через все рёбра.

Теорема

Орграф Эйлеров \Leftrightarrow степень входа = степень выхода без изолированных вершин

Док-во:

$\Rightarrow v, v$ — эйлеров цикл,
 $v \in V$ $v \rightarrow v \rightarrow v \rightarrow v$

сильно связан; в цикле есть все вершины

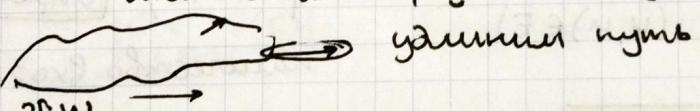
$\Leftarrow v_0, \dots, v_t$ — самый длинный простой в рёбрах путь цикл путь $v_0 \neq v_t$ v_0, v_t, v_t, v_0

3 раза входил, 2 раза выходит \Rightarrow можно выйти, удалив путь

содержит все рёбра!

путь нет рёбра

$(v_i, w) \quad v_{i+1}, v_{i+2}, \dots, v_l w$



Теорема

Несквозимоустроенный граф без изолированных вершин эйлеров \Leftrightarrow степени чётны и граф связен

Определение

Ациклический орграф — нет циклов длины больше 0.
(нет петель)

Теорема

орграфы без петель ① равносильны: 1 компонента сильной связности состоит из 1 вершины

② граф является ациклическим

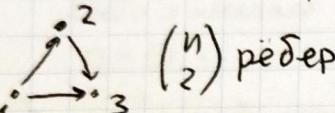
③ вершины можно перенумеровать, рёбра менять \rightarrow большие

Лемма

В ациклическом графе существует вершина входящей степени 0 и исходящей степени 0.

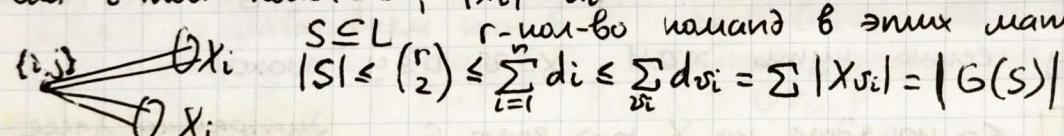
Док-во: выбирайт ^{простой} из v_1 ничего не идёт, $v_2 \dots v_k$ из v_2 ничего не идёт, никак можно удалишь или это будем знать

Док-во: $\textcircled{1} \Rightarrow \textcircled{2}$, $\neg \textcircled{2} \Rightarrow \neg \textcircled{1}$
 пусть существует цепь $v_1 \dots v_k$
 Все эти вершины в одной компоненте сильно связности \Rightarrow противоречие. $\textcircled{2} \Rightarrow \textcircled{1}$, $\neg \textcircled{1} \Rightarrow \neg \textcircled{2}$
 пусть существует компонента связности с > 1 вершиной и v_1 в $\textcircled{1}$ компоненте \Rightarrow пусть $v_1 \dots v_k$ и $\textcircled{3} \Rightarrow \textcircled{2}$ номера вершин вдоль пути возрастают
 $\textcircled{3} \Rightarrow \textcircled{2}$ Эта вершина находящей степени 0 у неё номер и вынимем её, присвоим $n-1$ новой вершине
 по индукции всё доказывается.

Определение Турнир - орграф без петель, $\forall i \neq j$ $(i, j) \in E$ xor $(j, i) \in E$ исключая все или 1...n команды, $E = f(i, j) : i < j$ ациклический, транзитивный
 $\binom{n}{2}$ ребер v_1, \dots, v_n d_{i_1}, \dots, d_{i_n} - исходящие степени d_{i_1}, \dots, d_{i_n} к командам $n-1-d_{i_1}, \dots, n-d_{i_n}-1$ - входящие степени $d_{i_1}, \dots, d_{i_n} \geq \binom{k}{2}$
 $0 \leq d_i \leq n-1$ $d_1 + \dots + d_n = \binom{n}{2}$
 $d_1 \leq d_2 \leq \dots \leq d_n$ по неубыванию.

Лайдж

Теорема орграф-турнир \Leftrightarrow для его степенной последовательности (d_1, \dots, d_n) , $d_1 \leq \dots \leq d_n$ для $\forall k = 1 \dots n$
 $d_1 + \dots + d_k \geq \binom{k}{2}$ $d_1 + \dots + d_n = \binom{n}{2}$

Док-во: \Rightarrow ясно \Leftarrow ясно $L = \{(i, j) : 1 \leq i, j \leq n, i \neq j\}$ - множество матчей
 $R = X_1 \cup \dots \cup X_n$, где X_i - медали для i -ной команды, $|X_i| = d_i$

 $S \subseteq L$ r -мат-во команд в этих матчах
 $|S| \leq \binom{r}{2} \leq \sum_{i=1}^n d_i \leq \sum_{j=1}^n d_{v_j} = \sum |X_{v_j}| = |G(S)|$

ЛЕКУНИЯ-17 23.01.24.

Бинарное отношение R на множестве X строгий частичный порядок если оно асимметрически и транзитивно.

$\forall x, y \in X$ $xRy \wedge yRx \rightarrow x = y$

Определение

Определение R строгий линейный порядок, если это строгий частичный порядок и $\forall a, b \in X$ aRb или bRa
 X - множество $(P(X), \subset)$ $\{a\} \not\subset \{b\}$

Асимметрическость: $xRy \rightarrow \neg yRx$
 Аntисимметрическость: $xRy \wedge yRx \rightarrow x = y$
 асимм. \Rightarrow антирефл.
 асимм. \Rightarrow антисимм.

R -антисимметрическо \Rightarrow
 $R \setminus id_X$ - асимметрическо
 Отношение строгое частичного порядка
 ассимметрическо

нестрогоий частичный порядок R на множестве X :

(1) рефлексивный (2) $R \setminus id_X$ - строгий частичный порядок

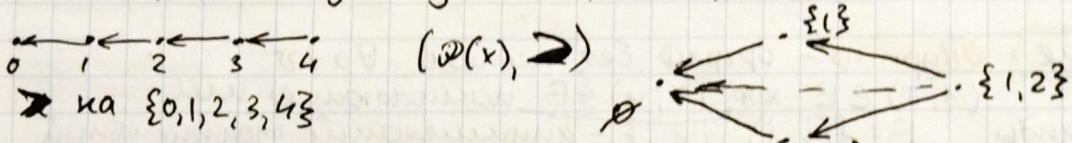
Утверждение: Отношение R на множестве X - нестрогий частичный порядок $\Leftrightarrow R$ рефл., транзитивно, антисимметрично.

Доказ-во: $xRy, yRz \quad x \neq y, y \neq z \Rightarrow xRz$ по транзитивности
 $R \setminus id_X \quad x=y$ или $y=z$ - то очевидно xRz

Пусть xRy и yRx , $x \neq y$

$S = R \setminus id_X \quad xSy, ySz$ - можно

(2) $S=R \setminus id_X$ антисимметрично / транзитивно $xSy, ySz \Rightarrow$
 $xRy, yRz \Rightarrow xRz$ по транзитивности $R \Rightarrow xSz$
если $x=z$ xRy и yRx - противоречие с антисимметричностью R



Утверждение: Г-антический график $\Rightarrow \leq_G$ - нестрогий частичный порядок

Доказ-во: рефл., транз. очевидны
антисимметричность $a \leq_G b \quad b \leq_G a \quad a \neq b$ $\xrightarrow{\text{если } a \neq b}$ $b \leq_G a$

Определение: $(x, <)$ \times предшествует элементу y ,
если $x < y$ и $\forall z. x < z, z < y$

Утверждение: \leq - порядок на X , \times предшествует y , Г-график
с множеством вершин X и $\leq = \leq_G \Rightarrow (x, y)$ - ребро G .

$x \leq y \quad x \leq_G y$ если есть путь $x \xrightarrow{*} y \quad x \leq v, v \leq y$ можно

Определение: $<$ - порядок на X \mapsto график G **диаграмма Хассе** H_C
вершины: X ребра: (x, y) , \times предшествует y

Утверждение: H_C - всегда антический график

пусть есть цепь $a_1 \dots a_n$ + нет путь $\xleftarrow{*}$
 $a_1 < a_2 < \dots < a_n < a_1 \Rightarrow$ что неверно по антисимметричности

Утверждение: Любой частичный порядок на конечном множестве задается своей диаграммой Хассе.

$\leftarrow \rightarrow H_C \Rightarrow \leq = \leq_{H_C}$ предшествует

Доказ-во: $x < y$ есть max длина $x < y_2 < y_3 < \dots < y_n < y$

пусть $x <_{H_C} y$ существует путь $x_{n+1} y$

$\leq_{H_C} \subset \leq$ выполнено всегда $x <_{H_C} y \Rightarrow x < y$ по транзитивности
 \supset - асим

Определение Понординационное умножение:
 $\mathbb{R}^n \quad x = (x_1, \dots, x_n) \leq (y_1, \dots, y_n) = y \quad x_i \leq y_i \quad \forall i$
 линейный $(1, 2)$ и $(2, 1)$
 P, Q - 2 частичных порядка $P \times Q$
 $(p_1, q_1) \leq (p_2, q_2) : p_1 \leq_p p_2 \text{ и } q_1 \leq_Q q_2$

P, Q - линейно упорядочены $\Rightarrow P \times Q$ линейно упорядочены

Определение Лексикографическое умножение $P \times_{lex} Q$
 $(p_1, q_1) \leq_{lex} (p_2, q_2) : p_1 <_P p_2 \text{ или } (p_1 = p_2 \text{ и } q_1 <_Q q_2)$

Утверждение P, Q - частичные порядки $\Rightarrow P \times_{lex} Q$ тоже
 линейно упорядочены \Rightarrow

Док-во: антимонотонность отвивда
 транзитивность $(p_1, q_1) \leq_{lex} (p_2, q_2) \leq_{lex} (p_3, q_3)$

A-алфавит с порядком $x < y$ x, y - конечные
 либо x -начало y , либо слова в
 $x_1 = y_1, \dots, x_n = y_n \quad x_{n+1} < y_{n+1}$ алфавите A

$$\begin{array}{l} p_1 \leq p_2 \leq p_3 \\ p_1 = p_2 \leq p_3 \end{array}$$

$$\begin{array}{l} p_1 < p_2 = p_3 \\ p_1 = p_2 = p_3 = \\ \Rightarrow q_1 < q_2 \leq q_3 \end{array}$$

Определение Порядки P и Q - изоморфные ($P \cong Q$), если \exists единичная
 $f: P \rightarrow Q$ т.ч. $x <_P y \Leftrightarrow f(x) \leq_Q f(y)$

$[n] = \{0, 1, \dots, n-1\} \quad (P([n]), \leq) \quad \{0, 1\} \times \dots \times \{0, 1\}$
 нонординационный порядок
 $A \subset [n] \rightarrow$ хар. функция $001\dots\underset{i \in A}{1}$ линии $i \in A$

Определение Сложение порядков: $P + Q$
 $P' \cong P, Q' \cong Q, P' \cap Q' = \emptyset$

$$\begin{array}{c} P \\ \cdot \\ Q \\ \cdot \end{array}$$

$a, b \in P' \cup Q'$
 $a, b \in P' \Rightarrow$ сравниваем как в P' $a \in P', b \in Q': a < b$

$P + Q$ - это порядок, если P, Q - линейные порядки, то $P + Q$ линейное
 не всегда $P + Q \cong Q + P \quad P \times_{lex} Q \cong Q \times_{lex} P$

Примеры $\begin{array}{c} Q \\ \hline \mathbb{N} \end{array} \dots \begin{array}{c} \dots \\ \mathbb{Z} \\ \dots \end{array} \dots \begin{array}{c} \dots \\ \mathbb{Z} \\ \dots \end{array} \dots \begin{array}{c} \dots \\ \mathbb{N} \\ \dots \end{array} \Rightarrow \mathbb{N} + \mathbb{Z} \neq \mathbb{Z} + \mathbb{N}$
 есть элементы, меньшие всех $\mathbb{N} \times_{lex} \mathbb{Z} \neq \mathbb{Z} \times_{lex} \mathbb{N}$

$\begin{array}{c} \dots \\ \mathbb{Z} \\ \dots \end{array} \begin{array}{c} \dots \\ \mathbb{Z} \\ \dots \end{array} \dots \begin{array}{c} \dots \\ \mathbb{N} \\ \dots \end{array} \dots \begin{array}{c} \dots \\ \mathbb{N} \\ \dots \end{array} \dots \begin{array}{c} \dots \\ \mathbb{Z} \\ \dots \end{array}$ раз

ЛЕКЦИЯ-18 30.01.24

Определение Наименьший элемент a : $\forall x \quad a \leq x$

Максимальный элемент a : не существует $x < a$.

Отрезок $[x, y]$: $\{z: x \leq z \leq y\}$

Предельный элемент: кем предшественника

Утверждение

- $\varphi: P \rightarrow Q$ - изоморфизм \Rightarrow
- (1) минимальный элемент \rightarrow минимальный элемент
 - (2) наименьший элемент \rightarrow наименьший элемент
 - (3) $[x, y] \rightarrow [\varphi(x), \varphi(y)]$ той же мощности
 - (4) предельный \rightarrow предельный (непредельный \rightarrow непредельный)

Док-бо: (1) $x \in P$ - минимальный
если $y < \varphi(x)$, то $\varphi^{-1}(y) < x$ не минимальный
(2) $x \in P$ - наименьший $\forall y \in P \quad x \leq P \quad \forall y \in P \quad \varphi(x) \leq \varphi(y)$
 $\Rightarrow \varphi(x)$ наименьший
продолжаем все Q

(3) $[x, y] \in P \quad x \leq z \leq y \quad \varphi(x) \leq \varphi(z) \leq \varphi(y)$
 $\varphi(z) \in [\varphi(x), \varphi(y)] \quad \varphi([x, y]) \subset [\varphi(x), \varphi(y)] \Rightarrow [x, y] \subset \varphi([x, y])$

(4) $\varphi(x) \leq u \leq \varphi(y) \Rightarrow \varphi^{-1}(\varphi(x)) \leq \varphi^{-1}(u) \leq \varphi^{-1}(\varphi(y)) \Rightarrow x \leq \varphi^{-1}(u) \leq y$
 $\varphi(x) \leq u \leq \varphi(y) \Rightarrow \varphi^{-1}(\varphi(x)) \leq \varphi^{-1}(u) \leq \varphi^{-1}(\varphi(y)) \Rightarrow x \leq \varphi^{-1}(u) \leq y$
 $x \in P$ - предельный $y < \varphi(x)$ - пусть он непредельный \Rightarrow
 $\varphi^{-1}(y) < x \Rightarrow \exists \varphi^{-1}(y) < z < x$, т.е. y - предшественник

Теорема Пусть $|X|=|Y|$ конечные, (X, \leq_X) , (Y, \leq_Y) - линейные
порядки \Rightarrow они изоморфны.

Док-бо: $|X|=|Y|=1$ очевидно

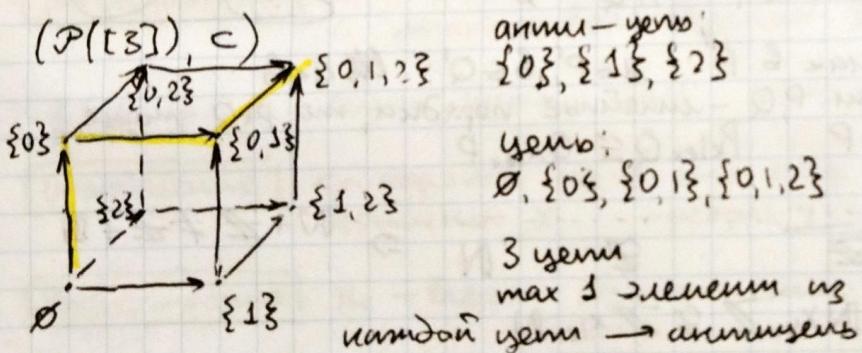
Маж, $|X|=|Y|=n+1$
в X и Y есть наименьший элементы a, b (алгебраический граф -
- есть вершина со входящей степенью $= 0$)
 $a \rightarrow b \quad X \setminus \{a\} \quad Y \setminus \{b\}$ - n элементов

(P, \leq_P)

Определение

Чепь - подмножество, что любые 2 элемента
сравнимы.

Антисимметрическое - подмножество, что любые 2 элемента не сравнимы.



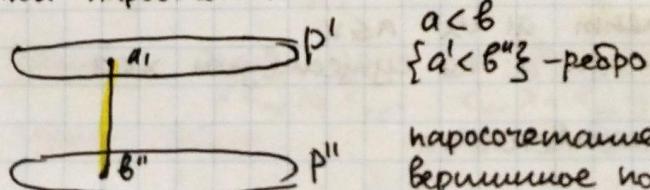
(P, \leq_P) разбивается на
 n античепей \Rightarrow
размер античепи
в P не больше n

Теорема Димитрова

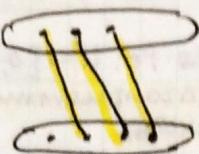
(P, \leq_P) - конечный
порядок \Rightarrow макс размер
антисимметрическое = мин кол-во
чепей в разбиении P .

Док-бо: \leq очевидно

\geq приведем пример античепи какого-то размера N и
разбиение P на N чепей
т.к. если; в 2-замощенном графике мин. вершинное покрытие \geq
макс покрытие



нарочетование и
вершинное покрытие $c >$ одиночного
размера

$A = \{x \in P : x' \in C, x'' \notin C''\}$ $|A| \geq n-m$
 A -антицепт если $a, b \in A$ и $a \neq b$
 $\{a', b''\}$ ребро не попало в вершинное покрытие $a' \notin C$
 $b'' \notin C$

 $M \cup \{\{x_1, x''\} : x \in P\}$ - без цепей длины $> 2 \Rightarrow$ это не
 рёбра + цепи. сб. - вершины = 0
 $n+m$ $n-m$ $2n$
 Каждая компонента связности задаёт цепь
 Разбиение на $n-m$ цепей

Теорема В любом бесконечном порядке есть либо бесконечная цепь, либо бесконечный антицепт.

Док-во: А-будущая антицепт С-будущая цепь
 x_i сравним с бесконечным множеством элементов
 $W_k \mapsto x_i \in C$, otherwise $x_i \in A$
 A, C, W_k
 \uparrow Все сравнимы друг с другом и с W_k
 Все несравнимы друг с другом и с W_k
 $x_{k+1} \in W_k \quad W_{k+1} \subseteq W_k \leftarrow$ либо x_{k+1} сравним
 бесконечное с ними всеми, либо нет



Примеры: $(\mathbb{Z}^2, <)$ координатный
 бесконечная цепь: $(0,0), (1,1), (2,2)$
 бесконечная антицепт: $(0,0), (1,-1), (2,-2)$
 $(\mathbb{N}^d, <)$ координатный порядок \leftarrow есть угодно большое конечное антицепт
 $d \geq 1 \quad \{x_1, \dots, x_d\} : \sum_{i=1}^d x_i = a\}$ $C^a \rightarrow \infty$ при $a \rightarrow \infty$
 \Rightarrow невозможно разбить на конечное число цепей
 разбивается на сколько число цепей, $|\mathbb{N}^d|$ сколько

Утверждение В \mathbb{N}^d нет сколько антицепей

Док-во: $d=1$ очевидно
 пусть $a_1, a_2, \dots \in \mathbb{N}^d$ - антицепт
 (z_1, z_2, \dots, z_d)

\downarrow
 (z_1, \dots, z_{d-1}) - проекция каждой a_i, \dots на первые $d-1$
 $\in \mathbb{N}^{d-1}$ - нет сколько антицепей по одномерам

\Rightarrow есть бесконечная цепь $(z_1, \dots, z_{d-1}) < (y_1, \dots, y_{d-1}) < (x_1, \dots, x_{d-1}) < \dots$

$\Rightarrow z_d > y_d > x_d > \dots$

$z_d \quad y_d \quad x_d$

ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ВЕРОЯТНОСТЕЙ

Определение Вероятностное пространство - конечное множество $x \in \Omega$ - возможные исходы

Определение Вероятностное распределение - функция $\Pr: \Omega \rightarrow [0, 1]$

$$\sum_{x \in \Omega} \Pr(x) = \Pr(\Omega)$$

$$\sum_{x \in \Omega} \Pr(x) = 1$$

Событие: $A \subseteq \Omega$, $x \in A$ - благоприятные исходы.

Вероятностная модель - вероятностное пространство + распределение.

Определение

Равновозможные исходы:

$$\Pr(x) = \frac{1}{|\Omega|}, \Pr(A) = \frac{|A|}{|\Omega|}$$

Примеры: $\Omega = \{\text{орёл, решка}\}$ $\Omega = \{0, 1\}$, $\Pr(0) = \Pr(1) = \frac{1}{2}$

Подбрасывание монеты 6 раз

Ω - последовательности из 6 0 и 1

$$\Pr(x) = \frac{1}{2^6}$$

$$\Pr(\text{выпало ровно } 3 \text{ орла}) = \frac{C_6^3}{2^6} = \frac{5 \cdot 4}{64} = \frac{5}{16}$$

Подбрасываем 6 монет

$$\Pr(\text{на } i\text{-том месте - орёл}) = \frac{2^{n-1}}{2^n} = \frac{1}{2}$$

Вычисляем в раз с возвращением из лотоматона, к вариантов всего

$$\Pr(\text{послед-ть возрастает}) - ?$$

$$= \frac{C_{10}^3}{10 \cdot 9 \cdot 8} = \frac{1}{6}$$

$$\begin{array}{ccccccc} & & 0 & 1 & 2 & 3 & 4 \\ \dots & \dots & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 3 & 5 & 7 & 11 \end{array} \dots$$



авс - благоприятный исход асв, сав ... 5 неблагоприятных
подбрасываем 3 шубика $P(X_1 + X_2 + X_3 \text{ делится на 3}) = \frac{1}{3}$
 $(X_1, X_2, 1), (X_1, X_2, 2), \dots, (X_1, X_2, 6)$ - 2 благоприятных

10 студентов 10 билетов

Вся выгодна 1 билет первым $\frac{1}{10}$ (аналогично с любым n)

Вероятностное пространство: перестановки чисел от 1 до 10

$$(X_1, \dots, X_{10}) \mapsto (X_{10}, \dots, X_1)$$

100 пассажиров 1-й - случайное место

100 мест следующий: если свободно его место - сядем на него
если занято - сядем на случайное место

$P(\text{следующий сядет на своё место}) - ?$

$$1 \ 2 \ \dots \ a_{i-1} \ a_i \ a_{i+1} \ \dots \ a_{2-1} \ a_2 \quad 100$$

$$a_1 \ 2 \ \dots \ a_{i-1} \ a_2 \ a_{i+1} \ \dots \ a_{2-1} \text{ и т.д.} \quad 100 \text{ или } 1$$

1 и 100 поменялись билетами \Rightarrow ничего не меняется $\Rightarrow P = \frac{1}{2}$

π - перестановка чисел 1..100

$\pi(i)$ - билет для этого пассажира $\Omega = \text{перестановки чисел}$

$P(\text{места}) = \text{перемножение вероятностей на пути к месту}$

100! распределений π - последний сел на своё место $\frac{1}{100}$

Второй последний сел на место π

$\Pr_{\pi}(G_{\pi}) + \Pr_{\pi}(B_{\pi}) = 1$

$$\Pr_{\pi}(G_{\pi}) = \Pr_{\pi}(G_0) \quad x \in G_{\pi} \Leftrightarrow x \in B_{\pi}$$

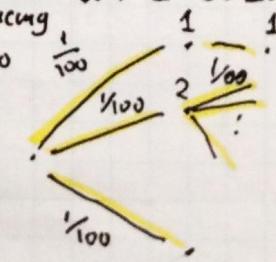
$$\Pr_{\pi}(B_{\pi}) = \Pr_{\pi}(B_0)$$

$$\Pr_{\pi}(x) = \Pr_G(x) \quad x \in \Omega - \text{небольшой исход} \Rightarrow \Pr_{\pi}(G_{\pi}) = \Pr_G(G_{\pi})$$

$$\Omega = \{1, 2, \dots, 99, 100\}$$

$$\sigma = \{100, 2, \dots, 99, 1\}$$

$$\Pr_{\pi}(x) = \Pr_G(x) \quad x \in \Omega - \text{небольшой исход} \Rightarrow \Pr_{\pi}(G_{\pi}) = \Pr_G(G_{\pi})$$



Определение $\bar{A} = \cup A_i$ $\Pr(\bar{A}) = 1 - \Pr(A)$
 A, B - несовместные: $\Pr(A \cap B) = 0$

Факт A_1, \dots, A_n попарно несовместны $\Rightarrow \Pr(\bigcup_{i=1}^n A_i) = \sum_{i=1}^n \Pr(A_i)$

Док-во: $\Pr(\bigcup_{i=1}^n A_i) = \sum_{\substack{x \in \bigcup A_i \\ i=1}} \Pr(x) = \sum_{i=1}^n \sum_{x \in A_i} \Pr(x)$

Факт $\Pr(\bigcup_{i=1}^n A_i) \leq \sum_{i=1}^n \Pr(A_i)$

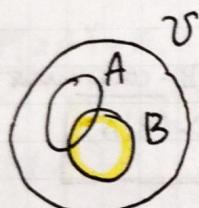
Формула включений-исключений

$$\Pr(\bigcup_{i=1}^n A_i) = \sum_{i=1}^n \Pr(A_i) - \sum_{1 \leq j \leq j \leq n} \Pr(A_i \cap A_j) + \dots = \sum_{\emptyset \neq S \subseteq \{1, \dots, n\}} (-1)^{|S|+1} \Pr(\bigcap_{i \in S} A_i)$$

Док-во: $\chi_A(x) = 1 - (1 - \chi_{A_1}(x)) \cdots (1 - \chi_{A_n}(x))$

$$\begin{aligned} \Pr(A) &= \sum_{x \in A} \Pr(x) = \sum_{x \in U} \Pr(x) \chi_A(x) = \sum_{x \in U} \Pr(x) (1 - (1 - \chi_{A_1}(x)) \cdots (1 - \chi_{A_n}(x))) = \\ &= \sum_{\emptyset \neq S \subseteq \{1, \dots, n\}} (-1)^{|S|+1} \sum_{x \in S} \Pr(x) \cdot \frac{\chi_A(x)}{\prod_{j \in S} \chi_{A_j}(x)} \Pr(\bigcap_{j \in S} A_j) \end{aligned}$$

ЛЕКУЧИЯ-20 13.02.24



знаем, что B - случайность \Rightarrow

$$\sum_{x \in U} \Pr(x) = 1 \quad \sum_{x \in B} \Pr(x) \neq 0$$

Определение

условная вероятность события A при событии B :

$$\Pr(B|A) \neq \Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)} \quad \Pr(B) \neq 0 \quad \text{масштабирование}$$

$$\sum_{x \in A \cap B} \frac{\Pr(x)}{\Pr(B)} \quad \text{Пример } (33) \quad (CC) \quad (3C) \quad \begin{array}{l} * \text{ Выбираем мешочек} \\ * \text{ Выбираем ложку} \end{array}$$

$\Pr(\text{выбрал мешочек с 2 золотыми ложками} \mid \text{выбрал золотую}) = \frac{1/3}{1/2} = \frac{2}{3}$

10 коробок, 1 шарик
★ случайно выбирают коробку $\Pr(\text{шарик есть} \mid \text{первые 10 - пусты}) = \frac{1}{11}$
★ с $\frac{1}{2}$ кладут шарик в неё —

Определение Событие A не зависит от события B , если $\Pr(A|B) = \Pr(A)$, $\Pr(B) \neq 0$

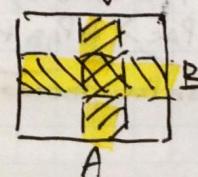
$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)} \quad \Pr(A \cap B) = \Pr(B) \Pr(A) \quad \Pr(B) = \frac{\Pr(A \cap B)}{\Pr(A)} = \Pr(B|A)$$

U, V - конечные множества, $U \times V$ с равномерным распределением
 $A = U \times A_1 \quad B = B_1 \times V$

A, B - независимые

$$\frac{|A \cap B|}{|U \times V|} = \frac{|A_1| \cdot |B_1|}{|U \times V|} = \frac{|A_1| \cdot |B_1|}{|U \times V|} = \frac{|A_1| / |U|}{|V \times V|} \cdot \frac{|B_1| / |V|}{|U \times V|}$$

$$\Pr(A \cap B) = \Pr(A) \Pr(B)$$



2000 раз подбрасываем монетку
 "первые 1000 раз $O > P"$
 "последние 1000 раз $O > P"$ \rightarrow независимые

36 карт

$A = \text{"выпало чётное"} \frac{18}{36}$

$B = \text{"выпало чётную 8 карту"} \frac{9}{36}$

$$P(A \wedge B) = \frac{1}{36}$$

37 карт: $36 + 3$ монета

$$P(A) = \frac{18}{37}$$

$$P(B) = \frac{9}{37}$$

$$P(A \wedge B) = \frac{1}{37} \neq P(A)P(B)$$

36 бочонков 1, ..., 36

выпало 2 случайно без возвращения
 Все (A, B) - вероятностные пространства

$A = \text{"в первый раз выпало чётное число"}$
 $B = \text{"во второй раз --- // ---"}$

$$Pr(B) > Pr(B|A) \quad Pr(A) = \frac{1}{2} = Pr(B)$$

$$Pr(A \wedge B) = \frac{1}{2} \cdot \frac{17}{35} \neq Pr(A)Pr(B)$$

$$Pr(A) \quad Pr(B|A)$$

	1	2	3	-	34	35	36
1	0						
2		0	1				
3			0	1			
:				1	.	1	
34				1	0		
35				1	0		
36				1	0	0	

Формула полной вероятности

$B_1, B_2, \dots, B_k = \Sigma, \Pr(B_i) \neq 0, A - \text{событие} \Rightarrow$

$$\Pr(A) = \sum_{i=1}^k \Pr(A|B_i) \Pr(B_i) \quad A = (A \wedge B_1) \cup \dots \cup (A \wedge B_k) \quad \Pr(A) = \sum_{i=1}^k \Pr(A \wedge B_i)$$

не пересекаются

Σ - вероятностное пространство
 B_1, \dots, B_k - события, т.ч. $B_i \wedge B_j = \emptyset (i \neq j)$

Формула Байеса

$\Pr(A \wedge B) = \Pr(A) \Pr(B|A) = \Pr(B) \Pr(A|B)$

$$\Pr(A|B) = \frac{\Pr(A)}{\Pr(B)}$$

Болезнь К в городе и болеют 1% людей

Лесен 99% с вероятностью 99% и для больных, и для здоровых
 дадим верный ответ

Тест: "Вы больны"

Вопрос: "С какой вероятностью я болен?"

$A = \text{"я болен"}$

$B = \text{"положительный тест"}$

$$\Pr(A) = \Pr(B|A) \cdot \Pr(A) + \Pr(B|\bar{A}) \cdot \Pr(\bar{A}) = 0,99 \cdot 0,01 + 0,001 \cdot 0,99 = 0,0198$$

$$\Pr(A|B) = \frac{0,01 \cdot 0,99}{2 \cdot 0,01 \cdot 0,99} = \frac{1}{2}$$

$$\Pr(A|B \wedge C) = \Pr(B|B \wedge C) \Pr(A|B) + \Pr(C|B \wedge C) \Pr(A|C)$$

$$\Pr(A|B \wedge (\bar{B} \wedge C))$$

B, C не пересекаются

\bar{B}, \bar{C} не пересекаются

$$\Pr(A|\bar{B} \wedge \bar{C}) = \Pr(\bar{B}|\bar{B} \wedge \bar{C}) \Pr(A|\bar{B}) + \Pr(\bar{C}|\bar{B} \wedge \bar{C}) \Pr(A|\bar{C})$$

Парadox Симпсона

$$\Pr(A|B) < \Pr(A|\bar{B}) \Rightarrow \Pr(A|B \wedge C) > \Pr(A|\bar{B} \wedge \bar{C})$$

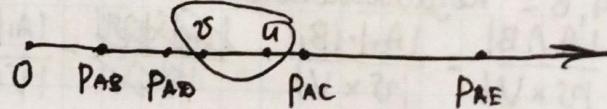
$$\Pr(A|C) < \Pr(A|\bar{C}) \Rightarrow \Pr(A|\bar{B} \wedge C) < \Pr(A|\bar{B} \wedge \bar{C})$$

$$\Pr_{AB} < \Pr_{\bar{B}\bar{C}} \quad \alpha = \Pr(B|B \wedge C)$$

$$\Pr_{AC} < \Pr_{\bar{B}\bar{C}} \quad \beta = \Pr(\bar{B}|\bar{B} \wedge \bar{C}) \Rightarrow \Pr(A|B \wedge C) = \alpha \Pr_{AB} + (1-\alpha) \Pr_{AC}$$

$$\Pr_{\bar{B}\bar{C}} = \beta \Pr_{AB} + (1-\beta) \Pr_{AC}$$

точка между \Pr_{AB}, \Pr_{AC} точка между $\Pr_{\bar{B}\bar{C}}, \Pr_{AB}$



Пример Г-простой неорграф с n вершинами степени d .
Всего $nd/2$ рёбер.

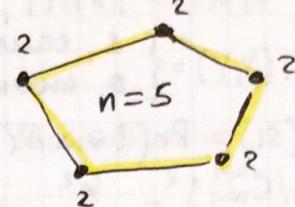
\nexists 2 распределения на рёбрах

- * равномерное каждое из $nd/2$ рёбер выбирается с одинаковой вероятностью $2/nd$
- * сначала выбираем ~~ребро~~ вершину, а затем инцидентное ребро

(v, e) . Выбрали $\nexists e$ и $\nexists \Pr(e) \neq \forall e$, получим различие

$$\Pr[e] = \sum_{v \in V} \Pr[e|B_v] \cdot \Pr[B_v] \quad \Pr[B_v] = \frac{1}{n} \text{ и } \forall$$

$\Pr[e|B_v] = 0$, если вершина v не является концом e , иначе $\frac{1}{d} \Rightarrow \Pr[e|B_v] = \frac{1}{d}$, если v инцидентна e . У ребра два конца $\Rightarrow \frac{1}{dn} \Rightarrow$ и всего $\frac{2}{dn}$



Пример n -элементное множество, 2 k -элементных подмножества
 $\binom{C_n^k}^2$ - исходов

Равномерное распределение $\Pr(X \wedge Y = \emptyset)$ - ?

$$\Pr(X \wedge Y = \emptyset | X=A) = \Pr(X \wedge Y = \emptyset | X=B) \text{ т.к. исходов поровну} \stackrel{1}{=} \\ \Pr(X \wedge Y = \emptyset) = \sum_{c=k}^{n-k} \Pr(X \wedge Y = \emptyset | X=C) \Pr(X=C) = \Pr(X \wedge Y = \emptyset | X=A) \sum_{c=k}^{n-k} \Pr(X=C) = \\ = \Pr(X \wedge Y = \emptyset | X=A) = \frac{\binom{n-k}{k}}{\binom{n}{k}} = \frac{(n-k)(n-k-1)\dots(n-2k+1)}{k!} \cdot \frac{k!}{n(n-1)\dots(n-k-1)} =$$

$$\Pr(X \wedge Y = \emptyset, X=A) = \Pr(X=A) \left(1 - \frac{k}{n}\right) \left(1 - \frac{k}{n-1}\right) \dots \left(1 - \frac{k}{n-k+1}\right) \leq \left(1 - \frac{k}{n}\right)^k \quad k \approx \ln n$$

$$\left(1 - \frac{C\sqrt{n}}{n}\right)^{\sqrt{n}} = \left(\left(1 - \frac{C}{\sqrt{n}}\right)^{\frac{\sqrt{n}}{C}}\right)^{C^2} \rightarrow \left(\frac{1}{e}\right)^{C^2} = e^{-C^2}$$

Определение

Случайная величина - Входу определенная функция
 V -вероятностное пространство $\rightarrow \mathbb{R}$

Определение

Матожидание f : $E(f) = \sum_{x \in V} f(x) \Pr(x) \quad \int_V f(x) dx$

$$f=1 \Rightarrow E(f)=1 \\ V = \{1, 2, 3, 4, 5, 6\} \Rightarrow E(f) = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + \dots + 6 \cdot \frac{1}{6} = 3,5 \\ \text{равномерное } f(x)=x$$

Определение

Линейность мат ожидания f, g - 2 случайные величины на одном и том же вероятностном пространстве (одинаковое распределение) $\Rightarrow E(f+g) = E(f) + E(g)$

$$E(f+g) = \sum_{x \in V} (f+g)(x) \Pr(x) = \sum_{x \in V} (f(x)+g(x)) \Pr(x) =$$

$$= \sum_{x \in V} f(x) \Pr(x) + \sum_{x \in V} g(x) \Pr(x) = E(f) + E(g) \quad E(f \cdot g) \neq E(f) \cdot E(g)$$

X, Y -пара k -элементных подмножеств n -элементного множества
 $f(X, Y) = |X \cap Y|$, $E(f)$?

$$S_i(X, Y) = \begin{cases} 1, & \text{если } i \in X \cap Y \\ 0, & \text{иначе} \end{cases} \quad f(X, Y) = \sum_{i=1}^n S_i(X, Y)$$

$$E(S_i) = \Pr(i \in X \cap Y) = \Pr(i \in X, i \in Y) = \Pr(i \in X) \Pr(i \in Y) = \\ = \left(\frac{\binom{k-1}{n-1}}{\binom{k}{n}}\right)^2 = \frac{k^2}{n^2} \Rightarrow E(f) = n \frac{k^2}{n^2} = \frac{k^2}{n} \quad k = c\sqrt{n} \Rightarrow E(f) = c^2$$

Парadox дней рождения в модей, у сильных пар совпадают?

365 вероятность рождения в каждый день $\frac{1}{365}$

$$S_{ij} = \begin{cases} 1, & \text{если } i \text{ и } j \text{ др. события} \\ 0, & \text{иначе} \end{cases}$$

$$f = \sum_{i,j} S_{ij} \quad E(S_{ij}) = \frac{1}{365}$$

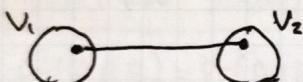
$$C_n^2 \cdot \frac{1}{365} = \frac{n(n-1)}{2 \cdot 365} > 1 \quad \text{при } n \geq 28$$

Лемма f -случайная величина $E(f) = C \Rightarrow$
 \exists исход x , т.ч. $f(x) \geq C$

Доказ. от противного:
 $f(x) < C \quad \forall x$

$$E(f) = \sum_{x \in S} f(x) \Pr(x) < \sum_{x \in S} C \Pr(x) = C \Rightarrow E(f) < C - \text{противоречие}$$

$G = (V, E)$ **Определение** Разрез графа - разбиение его вершин на 2 множества, $V_1 \cup V_2 = \emptyset$, $V_1 \cap V_2 = V$



Определение Размер разреза - кол-во рёбер, что один конец в V_1 , другой в V_2 .

Утверждение В графе существует разрез размера $\geq \frac{|E|}{2}$

Вероятностное пространство: все разрезы $(S, V \setminus S)$, равномерное, $\geq |V|$ исходов, $f(S, V \setminus S)$ - размер этого разреза

$$g_e(S, V \setminus S) = \begin{cases} 1, & e \in \text{разрезе} \\ 0, & \text{иначе} \end{cases} \quad - \text{их } |E| \text{ штук}$$

$$E(g_e) = \Pr(e \in \text{разрезе}) = \frac{1}{2} \quad E(f) = \sum_{e \in E} E(g_e) = \frac{|E|}{2} \Rightarrow$$

$$\Pr(u \in S) = \frac{2^{|V|-1}}{2^{|V|}} = \frac{1}{2} \quad \text{З конкретный разрез размера } \geq \frac{|E|}{2}$$

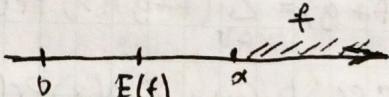
Лемма $E(f) = C \Rightarrow \exists x \quad f(x) \geq C$

Неравенство Маркова f -случайная величина, $f \geq 0 \quad \forall x, \alpha > 0 \Rightarrow$
 $P(f \geq \alpha) \leq \frac{E(f)}{\alpha}$

$0 < \alpha \leq E(f)$ очевидно

$E(f) \geq \alpha P(f \geq \alpha)$

$$E(f) = \sum_{x \in S} f(x) \Pr(x) = \sum_{x: f(x) \geq \alpha} f(x) \Pr(x) + \sum_{x: f(x) < \alpha} f(x) \Pr(x) \geq \alpha \sum_{x: f(x) > \alpha} \Pr(x) = \alpha P(f \geq \alpha)$$



Билет - 100р, 40% ^{на} выигрыши $P(\text{выигрыш} \geq 5000) < 1\%$

$$E(f) = 40$$

$$P(f \geq 5000) \leq \frac{E(f)}{5000} = \frac{40}{5000} < 0.01$$

q-sort в среднем $O(n \log n)$ в 0.01% случаев неправильно

$O(n \log n) \cdot 10000$ шагов $\xrightarrow{\text{OK}}$ случайное

$$P(\text{работаем} \geq O(n \log n) \cdot 10^4) \leq \frac{O(n \log n)}{O(n \log n) \cdot 10^4} = 0.01\%$$

ЛЕКУНИЯ-22 27.02.24

$$\begin{aligned} E(C \cdot f) &= C \cdot E(f) \\ \sum_{x \in \Omega} C \cdot f(x) \Pr(x) &= C \sum_{x \in \Omega} f(x) \Pr(x) \end{aligned}$$

Лемма $D(f) = E(f^2) - (E(f))^2$
дисперсия

$$\begin{aligned} D(f) &= E(f^2 - 2fE(f) + E(f)^2) = \\ &= E(f^2) - E(2fE(f)) + E(E(f)^2) = \\ &= E(f^2) - (E(f))^2 \end{aligned}$$

Неравенство Чебышева $\Pr(|f - E(f)| \geq \alpha) \leq \frac{D(f)}{\alpha^2}$

$$\Pr(|f - E(f)| \geq \alpha) = \Pr((f - E(f))^2 \geq \alpha^2) \leq \frac{E(f - E(f))^2}{\alpha^2} = \frac{D(f)}{\alpha^2}$$

$$E(f+g) = E(f) + E(g)$$

$$E(f \cdot g) \neq E(f) \cdot E(g)$$

$$D(f) = 0 \iff E(f \cdot f) = E(f) \cdot E(f)$$

независимые случайные величины f и g : для любых x, y события $f=x$ и $g=y$ независимы: $\Pr(f=x) \Pr(g=y) = \Pr(f=x \text{ и } g=y)$

$\Omega = A \times B$ f зависит только от первых координат,
 g — только от второй; f, g — независимы

$$f^{-1}(x) = A_1 \times B$$

$$\Pr(f=x) = \Pr(A_1) \quad g^{-1}(y) = A \times B_1$$

$$\Pr(f=x, g=y) = \Pr(A_1 \times B_1) = \Pr(A_1) \Pr(B_1)$$

Лемма f, g — независимы $\Rightarrow E(f \cdot g) = E(f) \cdot E(g)$

$$E(f) \cdot E(g) = \left(\sum_{x \in \Omega} f(x) \Pr(x) \right) \cdot \left(\sum_{y \in \Omega} g(y) \Pr(y) \right) =$$

$$= \left(\sum_{a \in f(\Omega)} a \Pr(f=a) \right) \left(\sum_{b \in g(\Omega)} b \Pr(g=b) \right) = \sum_{\substack{a \in f(\Omega) \\ b \in g(\Omega)}} ab \Pr(f=a, g=b) = E(f \cdot g)$$

1-орен, архимеда $\Pr(k \text{ раз из } n \text{ выпал орёл}) = \frac{C_n^k}{2^n}$

$$\frac{C_n^{n/2}}{2^n} \rightarrow 0$$

X_n — кол-во выпавших орлов

$$\xi_n = \frac{X_n}{n} — доля орлов$$

$$X_n = X_1 + \dots + X_n$$

$$x_i = 0 \text{ или } x_i = 1 \text{ с } \Pr(x_i) = 0.5$$

max

Неравенство Хофдинга-Чернова

$$\Pr(|X_n - \frac{n}{2}| > \varepsilon n) = \Pr(|\xi_n - \frac{1}{2}| > \varepsilon) < 2e^{-2\varepsilon^2 n}$$

$$Y_n = 2X_n - n \quad Y_n = y_1 + \dots + y_n \quad Y_i = 2X_i - 1 \text{ или } -1 \text{ с } \Pr(\cdot) = 0.5$$

$$Z_n = e^{Y_n} = e^{2(y_1 + \dots + y_n)} = e^{2y_1} \cdots e^{2y_n} = z_1 \cdots z_n \quad \xrightarrow{\text{выберем помимо}} \text{независимые}$$

$$\Pr(X_n - n/2 > \varepsilon_n) = \Pr(Y_n > 2\varepsilon_n) =$$

$$= \Pr(Z_n > e^{2\varepsilon_n}) \leq \frac{E(Z_n)}{e^{2\varepsilon_n}} \leftarrow \begin{array}{l} \text{неравенство,} \\ \text{маршба} \end{array} \quad E(Z_n) = \prod_{i=1}^n E(z_i) =$$

$$= \prod_{i=1}^n \left(\frac{e^2 + e^{-2}}{2} \right) = (ch 2)^n \quad ch x < e^{x^2/2} \text{ строгое если } x \neq 0$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!} (-1)^n \quad e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots$$

$$ch x = \sum_{n=0}^{\infty} \frac{x^{2n}}{(2n)!} \quad e^{\frac{x^2}{2}} = \sum_{n=0}^{\infty} \frac{x^{2n}}{2^n n!} \quad \frac{x^{2n}}{(2n)!} < \frac{x^{2n}}{2^n n!} \quad \text{строгое при } n \geq 2$$

$$\lambda = 2\varepsilon: \quad \frac{E(Z_n)}{e^{2\varepsilon_n}} = \frac{(ch 2)^n}{e^{2\varepsilon_n}} = \frac{(ch(2\varepsilon))^n}{e^{4\varepsilon_n}} < \frac{(e^{2\varepsilon^2/2})^n}{e^{4\varepsilon_n}} = e^{-2\varepsilon^2 n}$$

a, b - целые числа $\in \mathbb{Z}$

[Определение]

a делится на b : $\exists k \in \mathbb{Z}$, что $a = b \cdot k$ a/b

[Определение]

$a, b \in \mathbb{Z}, b > 0$ деление с остатком:
 $q, r \in \mathbb{Z}: a = bq + r, 0 \leq r < b$

Значит, что деление с остатком ① всегда возможно
 и ② единственно.

$$\textcircled{2} \quad a = bq_1 + r_1 = bq_2 + r_2 \quad bq_1 - bq_2 = r_2 - r_1 \quad b(q_1 - q_2) = r_2 - r_1 \Rightarrow r_2 \geq r_1$$

$$\Rightarrow r_1 = r_2 \Rightarrow b(q_1 - q_2) = 0 \Rightarrow q_1 = q_2$$

$$\textcircled{1} \quad \text{индукция по } a \geq 0 \quad a=0: 0=b \cdot 0 + 0 \quad a \mapsto a+1;$$

$$a=bq+r \quad a+1=bq+r+1$$

$$\text{a) } r+1=b \Rightarrow a+1=b(q+1) \quad \delta) r+1 < b \text{ так и остаток}$$

$$\text{индукция по } a < 0: \quad a=bq+r, \quad -a=bq-r$$

$$\text{a) } r=0 \quad \delta) r>0: -a=-b(q+1)+b(b-r)$$

$$\text{Пример. } \begin{matrix} 100^{10001} \% 7 - ? \\ 10001 \% 3 = 2 \end{matrix} \Rightarrow 100\% 7 = 2, 4, 1 \quad \text{ответ}$$

ЛЕКУНИЯ-23. 05.03.24.

[Определение]

a и b сравнимы по модулю N : $a \equiv b \pmod{N}$
 они дают одинаковые остатки $a \equiv b \pmod{N}$
 при делении на $N \Leftrightarrow a-b$ делится на N $\xrightarrow{\text{вычел}}$

Означение "быть сравнимым по модулю N " - означение
 эквивалентности N классов эквивалентности - вычел

[Лемма]

класс суммы, разности и произведения корректичен
 определён (не зависит от конкретного элемента
 вычелов)

$$\text{на 1: } 10^k \equiv (-1)^k$$

$$a_k \cdot 10^k + \dots + a_0 \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \dots + a_2 - a_1 + a_0$$

$$\begin{array}{lll} a + (b+c) & 0 \cdot a = 0 & 0 + a = a \\ ab \neq ba & 1 \cdot a = a & \end{array}$$

Вычтем a по модулю N обратимый, если \exists решение $ax \equiv 1$

$N=12$

$$a=1 \text{ - обратимый: } 1 \cdot x \equiv_{12} 1 \Rightarrow x=1$$

$$a=5 \text{ - обратимый: } 5 \cdot x \equiv_{12} 1 \Rightarrow x=17$$

$$a=8 \text{ - необратимый: } 8 \cdot x \equiv_{12} 1 \Rightarrow 8x = 1 + 12k$$

$$a \pm b \equiv (a+Nk) \pm (b+Nm)$$

$$(a+Nk)(b+Nm) = ab + N(k+m+Nkm) \equiv ab$$

$$a = \overline{a_k a_{k-1} \dots a_0} = a_k 10^k + \dots + a_0$$

$$\text{на 2: } a_0 : 2 \quad a = a' \cdot 10 + a_0 \equiv_{2} a_0$$

$$\text{на 5: } a_0 = 0 \text{ или } 5$$

$$\text{на 4: } \overline{a_1 a_0} : 4 \quad 10^k \equiv_{3} 1 \quad 10^k \equiv_{8} 1$$

$$\text{на 3: } a_k + a_{k-1} + \dots + a_0 : 3$$

$$\text{на 9: } a_k + a_{k-1} + \dots + a_0 : 9 \quad a_k 10^k + \dots + a_0 \equiv_{3} a_k + \dots + a_0$$

решение

Утверждение a обратим по модулю $N \Rightarrow \exists! ax \equiv 1 \pmod{N}$

Док-бо: $\exists a \in \mathbb{Z} \quad a \not\equiv 0 \pmod{N} \quad a(yb) \equiv b \pmod{N}$

единственность: пусть $ax \equiv 1 \pmod{N}$, $ay \equiv 1 \pmod{N}$ a^{-1}
 $x \equiv (ya)x \equiv y(ax) \equiv y \pmod{N}$ $ax \equiv b \pmod{N} \quad a^{-1}a \cdot x \equiv a^{-1}b \pmod{N}$

Определение a и b взаимно просты — у них нет общего
натурального делителя, кроме 1
 a и N взаимно просты $\Rightarrow a+kN$ и N взаимно просты
вычтем a взаимно простой с N

Теорема вычтем a обратим мод $N \Leftrightarrow a$ и N взаимно
просты

Док-бо: \Rightarrow пусть a и N не взаимно просты $a = da_1, N = dN_1, d > 1$
 $ax \equiv 1 \pmod{N}$ $ax = 1 + Nk$

$$da_1 x = 1 + dN_1 k \quad d(a_1 x - N_1 k) = 1$$

$$d \mid a_1 x \quad d \mid N_1 k$$

$$d \mid a_1 \quad d \mid N_1$$

$$d \mid \text{min}$$

$$d \mid a_1, N_1$$

$$d \mid a, N$$

$d = \text{НОД}(a, N)$ d -общий делитель a и N

Лемма пусть d' -общий делитель a и $N \Rightarrow d' | d$

$$\begin{array}{c} d = ak \cdot N \\ ; d' \quad ; d' \end{array}$$

Лемма $\text{НОД}(a, b) = \text{НОД}(a, b - a \cdot q)$
 d -общий делитель $a, b \Leftrightarrow d$ -общий делитель $a, b - aq$
 $a, d | b, d \quad d | \dots$

Расширенный алгоритм Евклида $\text{НОД}(a, b) = ax + by$
 $(a_i, x_i, y_i) \quad a_i = x_i a + y_i b$

$$\text{НОД}(a_{i-1}, a_{i-2}) = \text{НОД}(a_{i-1}, a_i) = \text{НОД}\left(\frac{a}{a}, \frac{a}{a}\right)$$

$$\text{База: } \begin{array}{l} a = 1 \cdot a + 0 \cdot b \\ a_0 \quad x_0 \quad y_0 \end{array} \quad \begin{array}{l} b = 0 \cdot a + 1 \cdot b \\ a_1 \quad x_1 \quad y_1 \end{array}$$

делит a_{i-1} на a_{i-2} с остатком, этот остаток обозначим a_i

$$a_{i-1} = a_{i-2} q_{i-2} + a_i$$

$$a_i = a_{i-1} - a_{i-2} q_{i-2}$$

$$x_i = x_{i-1} - x_{i-2} q_{i-2}$$

$$y_i = y_{i-1} - y_{i-2} q_{i-2}$$

$$\begin{aligned} x_i a + y_i b &= (x_{i-1} - x_{i-2} q_{i-2}) a + \\ &\quad + (y_{i-1} - y_{i-2} q_{i-2}) b = \\ &= a_{i-1} - a_{i-2} q_{i-2} = a_i \end{aligned}$$

Линейные диофантовы уравнения $ax + by = c$

$c | \text{НОД}(a, b) \Rightarrow$ нет решений

$c : \text{НОД}(a, b)$ — спарим на него

без ограничения общности считаем, что a и b взаимно простые

Лемма Пусть (x_0, y_0) — какое-то 1 конкретное решение уравнения $ax + by = c \Rightarrow$ все решения уравнения $ax + by = c$ имеют вид $(x_0 + x, y_0 + y)$, где (x, y) — решения уравнения $ax + by = 0$
 $a(x_0 + x) + b(y_0 + y) = c \Leftrightarrow ax + by = 0 \quad ax_0 + by_0 = c$

Найдем частное решение уравнения:

мы умеем находить k и l , что $ak + bl = 1$ $5x + 3y = 0$
 $\underbrace{akc}_{x_0} + \underbrace{blc}_{y_0} = c \quad y = 5k \quad x = -3k$

Лемма Все решения уравнения $ax + by = 0$ имеют вид $x = -blk$, $y = ak$, $k \in \mathbb{Z}$

Доказ.: $ak + bl = 1$ (для некоторого k и l)

$$ax + by = 0 \Leftrightarrow akx + blky = 0$$

$$x(1 - bl) + blky = 0$$

$$x = xbl - blky = b(xl - ky)$$

$$x; b$$

$$x = bt \quad a \cdot bt + by = 0 \Rightarrow y = -at$$

$3y:5$, $\text{НОД}(3, 5 = 1) \Rightarrow y:5$ основная теорема арифметики
Одночлене 1 на целых положительных числах — одночлене частичного порядка (транзитивность, антисимметричность, 1-минимальный 1! н, но нет $k \mid 1/k$, $k \mid 1$ рефлексивность)
простое число

Утверждение Для любого $n \in \mathbb{N}$ Э н подряд идущих составных чисел

Док-во: $(n+1)! + 2 \equiv 2$
 $(n+1)! + 3 \equiv 3$ $\pmod n$ чисел
 \vdots
 $(n+1)! + (n+1) \equiv (n+1)$

теорема простых чисел бесконечно много.

Док-во: у любого составного числа есть простой делитель. Допустим, что простых чисел и штуки: p_1, \dots, p_k и $p_1 \cdots p_k + 1 > 1$ простое или составное не делится на p_i

Основная теорема арифметики любое натуральное число > 1 раскладывается на простые множители, причём единственным способом.
Сущность разложения: $n > 1$ непростое: разложи его на 2 множителя

Лемма p -простое, $p|x,y \Rightarrow p|x$ или $p|y$

Док-во: $\text{НОД}(p,x) = \begin{cases} p & \Rightarrow p|x \\ 1 & \Rightarrow x - \text{однозначный } \pmod p \\ & \exists z \text{ т.ч. } xz \equiv 1 \pmod p \end{cases}$
 $xy \equiv 0 \pmod p \quad xyz \equiv 0 \pmod p \Rightarrow y \equiv 0 \pmod p$

Док-во-2: $\exists a,b \quad p \cdot a + x \cdot b = 1 \mid y \quad \frac{p}{p} \cdot \frac{a}{p} + \frac{x}{p} \cdot \frac{b}{p} = \frac{y}{p}$

пусть не единственные \Rightarrow скрещенные одинарные простые
 $p_1 \cdots p_k = q_1 \cdots q_k \quad q_i | p_i \cdots p_k \stackrel{\text{по лемме}}{\Rightarrow} q_i | p_i \quad \forall i \Rightarrow q_i = p_i$ — противв.

$2 = p_1 < p_2 < p_3 < \dots$

каноническое разложение: $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots$
 $\alpha_i \geq 0, \alpha_i = 0$ с нашим же момента

$n \mapsto (\alpha_1, \alpha_2, \dots)$ — последовательность

$\geq 1 \geq 0$ равных 0 с нашим же момента

$1 \mapsto (0, 0, \dots)$

Утверждение $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots, m = p_1^{\beta_1} p_2^{\beta_2} \cdots$

$n|m \Leftrightarrow \alpha_i \leq \beta_i \forall i$

изоморфизм

1 — отношение порядка на $\mathbb{N} \setminus \{0\}$

Порядок на финитных последовательностях: полоординатно

Док-во: Пусть $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ Сколько делителей?

$(\alpha_1 + 1) \cdots (\alpha_k + 1)$ возможностей

$0 \leq \beta_i \leq \alpha_i \quad \alpha_i + 1$ возможностей

$$n \mapsto (\alpha_i) \quad m \mapsto (\beta_i) \quad \leq \alpha_i, \beta_i \\ \text{НОД}(n, m) \mapsto (\min(\alpha_i, \beta_i)) \quad \text{НОК}(n, m) \mapsto (\max(\alpha_i, \beta_i))$$

Следствие $n \cdot m = \text{НОД}(n, m) \cdot \text{НОК}(n, m)$

$$\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)$$

[Малая теорема Ферма] p -простое, $a \neq p \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Доказательство: $1, 2, \dots, p-1$ $\text{НОД}(a, p) = 1 \Rightarrow a - \text{обратимый} \Rightarrow$
на него можно делить
 $a, 2a, \dots, (p-1)a$ — тут есть все вычеты $1, \dots, p-1$
 $(p-1)! \equiv a^{p-1} (p-1)! \pmod{p}$ $(p-1)!$ взаимно просто с $p \Rightarrow$
можно поделить на него

[Функция Эйлера] $\varphi(n)$ — число вычетов, взаимно простых с n

[Теорема Эйлера] n — любое > 1 , a взаимно просто с $n \Rightarrow$
 $a^{\varphi(n)} \equiv 1 \pmod{n}$ $\varphi(p) = p-1$

вычеты, взаимно простые с n : $b_1, b_2, \dots, b_{\varphi(n)}$
 $a b_1, a b_2, \dots, a b_{\varphi(n)}$ — тут есть все
 $\text{НОД}(b_i, n) = 1, \text{НОД}(a, n) = 1 \Rightarrow \text{НОД}(a b_i, n) = 1$
поскольку $a b_i \equiv a b_j \pmod{n}$ на a можно делить \Rightarrow
 $b_i \equiv b_j \pmod{n}$ $a b_1, a b_2, \dots, a b_{\varphi(n)} \equiv a^{\varphi(n)} b_1, \dots, a^{\varphi(n)} b_{\varphi(n)} \pmod{n}$
поделим на все b_i

[Китайская теорема об остатках] Пусть u, v взаимно
простые, $a, b \in \mathbb{Z} \Rightarrow$

$$\exists! x \text{ от } 0 \text{ до } uv-1 \text{ т. ч. } \begin{cases} x \equiv a \pmod{u} \\ x \equiv b \pmod{v} \end{cases}$$

Примеры $x \equiv 1 \pmod{27} \quad x \equiv 26 \pmod{27}$

$$x \equiv 1 \pmod{31} \quad x \equiv 30 \pmod{31}$$

$$x = 1 \quad x = -1 + 27 \cdot 31$$

$$x \equiv 1 \pmod{27} \Rightarrow x = 27k+1$$

$$x \equiv 30 \pmod{31} \quad 27k+1 \equiv -1 \pmod{31}$$

$$27k = -2$$

$$x = 27 \cdot 16 + 1$$

$$-4k \equiv -2$$

$$4k \equiv 2 \cdot 8$$

$$32k \equiv 16$$

$$k \equiv 16$$

Доказательство:

Существование: $\text{НОД}(u, v) = 1 \Rightarrow \exists \tilde{u} \text{ т. ч. } u\tilde{u} \equiv 1 \pmod{v}$

$$x = a + u\tilde{u}(b-a) + k \cdot uv$$

$$x \equiv a \pmod{u}; \quad x \equiv a + (b-a) \equiv b \pmod{v}$$

Единственность: пусть x, y — 2 таких числа

$x-y$ делится на u , на v

$$\text{НОД}(u, v) = 1 \Rightarrow x-y \mid uv$$

$$|x-y| < uv \Rightarrow x=y$$

$$\begin{cases} x \equiv a_1 \pmod{u_1} \\ x \equiv a_2 \pmod{u_2} \\ \vdots \\ x \equiv a_n \pmod{u_n} \end{cases}$$

[Обобщение КТО]

Пусть u_1, \dots, u_n — любые 2 взаимно простые,
 a_1, \dots, a_n — любые $\Rightarrow \exists! x$ от 0 до $u_1 \cdots u_{n-1}$, т. ч.

Мультипликативность $\varphi(n)$

если u, v взаимно простые,
то $\varphi(uv) = \varphi(u)\varphi(v)$
но кТО существует доказательство $\varphi(a) \cdot \varphi(b)$

$$(a, b) \rightsquigarrow c \quad \begin{array}{l} \text{вычет} \\ \text{mod } u \\ \text{вычет mod } v \end{array} \quad \begin{array}{l} \text{вычет} \\ \text{mod } u \\ -uv \end{array}$$

$$\text{НОД}(a, u) = 1, \text{НОД}(b, v) = 1 \Leftrightarrow \text{НОД}(c, uv) = 1$$

$$\Rightarrow \left. \begin{array}{l} c \equiv a \pmod{u} \Rightarrow \text{НОД}(c, u) = 1 \\ c \equiv b \pmod{v} \Rightarrow \text{НОД}(c, v) = 1 \end{array} \right\} \Rightarrow \text{НОД}(c, uv)$$

$$\Leftarrow \left. \begin{array}{l} \varphi(p) = p-1 \\ 1, \dots, p^2 \text{ не взаимно просты с } p^2 \end{array} \right\} \begin{array}{l} \varphi(p^2) = p^2 - p \neq \varphi(p) \cdot \varphi(p) \\ p, 2p, \dots, p^2 \end{array}$$

p - простое

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

p - простое

$$1, \dots, p^\alpha \text{ не взаимно просты с } p^\alpha: 1p, 2p, 3p, \dots, p^\alpha = p^{\alpha-1} p$$

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$$

$$= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = n \cdot \prod_{i:p_i|n} \left(1 - \frac{1}{p_i}\right)$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2^1)(5^2 - 5^1) = 40$$

$$\begin{array}{r} 2 \\ 5 \\ 10 \end{array} \quad \begin{array}{r} 50 \\ 20 \\ 10 \end{array} \quad \text{не взаимно просты со } 100:$$

$$50 + 20 - 10 = 60$$