Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ (БИЛЕТЫ К ЭКЗАМЕНУ)

I СЕМЕСТР

Лекторы: *Мусатов Даниил Владимирович*
Райгородский Андрей Михайлович

Авторы:
Николай Спицын
Артемий Клячин
Полина Подзорова
Дмитрий Савичев
Полина Чубенко

Даниил Дрябин
Проект на Github

осень 2020

Содержание

7 Понятия образа и прообраза множества при соответствии. Критерий равенства образа пересечения и пересечения образов. Аналогичные критерии с объединением и разностью.

Соответствие между множествами A и B - произвольное подмножество декартова произведения $F \subset A \times B$. Обозначение: $F : A \to B$; иногда, чтобы подчеркнуть, что одному элементу из A может соответствовать несколько элементов из B, пишут: $F : A \rightrightarrows B$.

Пусть $F : A \to B$ - соответствие, $S \subset A$, $T \subset B$. Тогда **образ** множества S - множество всех элементов B, соответствующих какому-то элементу S. Формально: $F(S) = \bigcup_{s \in S} F(s) \subset B$. **Прообраз** множества T - множество элементов A, которым соответсвует хотя бы один элемент T. Формально: $F^{-1}(T) = \{a : F(a) \cap T \neq \varnothing\}$

Образ пересечения любых двух множеств равняется пересечению образов тех же множеств $\iff$ *соответствие инъективно.*

▲ Пусть соответствие не инъективно. Тогда найдутся такие a_1 и a_2, что $F(a_1)$ и $F(a_2)$ пересекаются. Тогда $F(\{a_1\} \cap \{a_1\}) = F(\varnothing) = \varnothing$, но $F(\{a_1\}) \cap F(\{a_2\}) = F(a_1) \cap F(a_2)$ не пуст по предположению. Значит, образ пересечения множеств $\{a_1\}$ и $\{a_2\}$ не равен пересечению образов.

Теперь пусть соответствие инъективно. Рассмотрим произвольные подмножества S и Q множества A. Докажем, что $F(S \cap Q) = F(S) \cap F(Q)$. Для этого докажем включение в обе стороны. Вначале пусть $y \in F(S \cap Q)$. Это значит, что $y \in F(x)$ для некоторого $x \in S \cap Q$. Тогда $x \in S$ и $x \in Q$. А раз $y \in F(x)$, то $y \in F(S)$ и $y \in F(Q)$. Значит, $y \in F(S) \cap F(Q)$. (Это включение верно для всех соответствий).

Теперь пусть $y \in F(S) \cap F(Q)$. Значит, $y \in F(x_1)$ для некоторого $x_1 \in S$ и $y \in F(x_2)$ для некоторого $x_2 \in Q$. Но при $x_1 \neq x_2$ в силу инъективности множества $F(x_1)$ и $F(x_2)$ не пересекаются. А их пересечение содержит хотя бы y. Значит, $x_1 = x_2 = x$, и $x \in S \cap Q$. А так как $y \in F(x)$, то получаем $y \in F(S \cap Q)$. ■

Образ объединения любых двух множеств равняется объединению образов тех же множеств - выполняется для любых соответствий.

▲ 1) $\left.\begin{array}{l} A \subseteq A \cup B \Rightarrow F(A) \subseteq F(A \cup B) \\ B \subseteq A \cup B \Rightarrow F(B) \subseteq F(A \cup B) \end{array}\right\} \Rightarrow F(A) \cup F(B) \subseteq F(A \cup B)$

2) $y \in F(A \cup B) \Rightarrow \exists x \in A \cup B : y = F(x) \Rightarrow \exists x \in A \cup x \in B : y = F(x) \Rightarrow$
$\Rightarrow y \in F(A) \cup y \in F(B) \Rightarrow y \in F(A) \cup F(B) \Rightarrow F(A \cup B) \subseteq F(A) \cup F(B)$;
Из пунктов 1 и 2 следует, что $F(A \cup B) = F(A) \cup F(B)$ ■

Образ разности любых двух множеств равняется разности образов тех же множеств $\iff$ *соответствие инъективно.*

Доказательство аналогично доказательству для пересечения.

11 Возведение множества в степень. Возведение множества в степень другого множества. Булеан. Свойства возведения множества в степень

Определение: *Декартовой степенью* A^n множества A называется множество кортежей длины n из элементов A.

Определение: Пусть A и B — два множества. Тогда множеством B^A называется множество всех отображений из A в B

Смысл определения: Если множество A состоит из n элементов, а множество B — из k элементов, то существует всего k^n различных отображений из A в B: действительно, есть по k вариантов значения для каждого из n элементов A.

Определение: *Булеаном* множества A называется множество всех подмножеств множества A. Обозначение: $\mathcal{P}(A)$ или 2^A.

Свойства возведения множества в степень:

1. $A^B \times A^C \cong A^{B \cup C}$ (для непересекающихся B и C)

   ▲ Неформально это утверждение означает, что определить функцию на несвязном объединении двух множеств это то же самое, что определить её на каждом из этих множеств по отдельности. Метафорически элемент $A^{B\cup C}$ есть набор контейнеров, помеченных элементами B или C. А $A^B \times A^C$ — это два набора контейнеров, в первом они помечены элементами B, а во втором — элементами C. Таким образом, достаточно один набор разбить на два.

   Формально множество с левой стороны имеет вид $\{(f, g) \mid f : B \to A;\ g : C \to A\}$, а с правой - $\{h \mid h : B \cup C \to A\}$. Рассмотрим такое соответствие между этими множествами: $h \longmapsto (h|_B, h|_C)$. Его инъективность очевидна. Оно также является сюръективным так как $\forall (f, g) \in A^B \times A^C \quad \exists h \in A^{B\cup C}$:
   $h(x) = \begin{cases} f(x), & \text{если } x \in B \\ g(x), & \text{если } x \in C \end{cases}$. Таким образом равномощность доказана. ■

2. $A^C \times B^C \cong (A \times B)^C$

   ▲ Неформально утверждение означает, что пара функций это то же самое, что одна функция, принимающая значение среди пар. Это легко объяснить при помощи метафоры с контейнерами. Пара функций — это два набора контейнеров, индексированных элементами C. В каждом контейнере из первого набора лежит элемент A, а в каждом контейнере из второго набора — элемент B. Если переложить все элементы из контейнеров второго набора в соответствующие контейнеры из первого набора, то получится набор контейнеров с парами элементов A и B.

   Формально пусть $F \in (A \times B)^C$. Это значит, что $F : C \to A \times B$. То есть каждому элементу $c \in C$ сопоставлена некоторая пара $(a, b) \in A \times B$. Вместо этого ему можно сопоставить отдельно элементы $a \in A$ и $b \in B$. Получится два отображения, первое отображает c в a, а второе — c в b, то есть пара отображений $(F_1, F_2) \in A^C \times B^C$. Можно сказать, что $F_i = pr_i \circ F$, где pr_i — проектор на i-ю координату: $pr_i(a_1, a_2) = a_i$. Легко понять, что разные F переводятся в разные пары (F_1, F_2), и каждая пара получается из некоторой функции. Таким образом, эквивалентность установлена. ■

3. $(A^B)^C \cong A^{B\times C}$ (для произвольных A, B, C)

▲ Третья эквивалентность означает, что функция двух аргументов есть то же самое, что отображение первого аргумента в функцию, зависящую от второго аргумента. Метафорически есть набор контейнеров, помеченных элементами C, в каждом из которых лежат контейнеры, помеченные элементами B, а уже в каждом из маленьких контейнеров лежит элемент A. Если убрать внешние контейнеры, но при этом перенести с них метки на внутренние, то получится набор контейнеров, помеченных элементами $B \times C$, что и требовалось.

Формально пусть $F \in (A^B)^C$, $F : C \to A^B$, то есть каждому элементу $c \in C$ сопоставляется некоторая функция $G : B \to A$. Пусть $H \in A^{B\times C}$, $H : B \times C \to A$. Рассмотрим такое соответствие между этими множествами: $(F(x))(y) \longmapsto H(x, y)$. Нетрудно понять, что данное соответствие - это биекция ■

14 Теорема Кантора для множеств

Теорема Кантора: Любое множество A менее мощно, чем его булеан 2^A.

▲ Вначале заметим, что A не более мощно, чем 2^A. Действительно, A равномощно множеству всех одноэлементных подмножеств A. Осталось доказать, что $A \ncong 2^A$.

Предположим противное, т.е. что существует биекция $f : A \to 2^A$. Рассмотрим множество $M = \{x \mid x \notin f(x)\}$. Это множество корректно определено, поскольку $f(x) \in 2^A$, т.е. $f(x) \subset A$, а значит вопрос о том, принадлежит ли x множеству $f(x)$, правомерен. Поскольку f является биекцией, само множество M равно $f(x_0)$ для некоторого x_0. Есть два варианта: $x_0 \in M$ и $x_0 \notin M$. Оба приводят к противоречию.

Действительно, если $x_0 \in M$, то $x \notin f(x)$ для $x = x_0$, т.е. $x_0 \notin f(x_0)$, т.е. $x_0 \notin M$ в силу $f(x_0) = M$, что противоречит предположению. Если же $x_0 \notin M$, то $x \notin f(x)$ неверно для $x = x_0$, т.е. $x_0 \in f(x_0)$, откуда $x_0 \in M$, снова имеем противоречие. Таким образом, противоречие возникает во всех случаях, и теорема доказана. ■

15 Континуальные множества. Доказательство того, что плоскость, пространство, $\mathbb{R}^k$ и $\mathbb{R}^{\mathbb{N}}$ являются континуальными. Формулировка континуум-гипотезы.

Множества, равномощные множеству действительных чисел, называются **континуальными**.

Вспомогательная лемма: Множество бесконечных последовательностей из 0 и 1 континуально

▲ Построим биекцию между этим множеством и отрезком [0,1]. Выберем число. Если оно лежит в левой половине отрезка, то допишем в последовательность 0, иначе - 1. Те же действия повторим с отрезком в который попало число и так далее. Очевидно, что построенное отображение является биекцией.

Отрезок [0,1] равномощен интервалу (0,1), так как они бесконечны и второе множество получено исключением конечного числа точек. А интервал, в свою очередь, равномощен $\mathbb{R}$, биекция: $tg(\pi(x - \frac{1}{2}))$. Получаем $\{0, 1\}^{\mathbb{N}} \cong [0,1] \cong (0,1) \cong \mathbb{R}$ ■

Утверждение: $\mathbb{R} \cong \mathbb{R}^n$, $n \in \mathbb{N}$

▲ Так как $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$, можно доказать данное утрверждение заменив $\mathbb{R}$ на $\{0,1\}^{\mathbb{N}}$. Построим биекцию: набору из n последовательностей сопоставим последовательность $a_1^1 a_1^2 ... a_1^n a_2^1 ...$ (верхний индекс - номер последовательности, нижний - номер элемента). Очевидно, что данное соответствие взаимно-однозначно $\Rightarrow$ эти множества равномощны ■

Утверждение: $\mathbb{R}^{\mathbb{N}} \cong \mathbb{R}$

▲ По свойствам возведения множества в степень другого множества: $\mathbb{R}^{\mathbb{N}} \cong (2^{\mathbb{N}})^{\mathbb{N}} \cong 2^{\mathbb{N}\times\mathbb{N}} \cong 2^{\mathbb{N}} \cong \mathbb{R}$ ■

Континуум-гипотеза: Любое бесконечное подмножество $\mathbb{R}$ либо счётно, либо континуально (иными словами, нет множеств A, удовлетворяющих соотношению $\mathbb{N} \lesssim A \lesssim \mathbb{R}$).

16 Теорема Кантора-Бернштейна

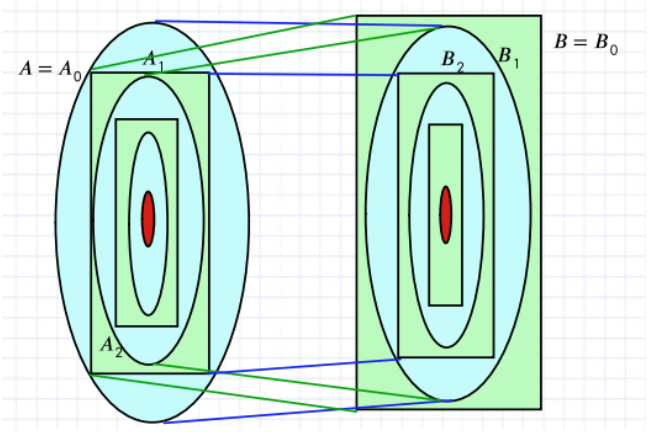
Теорема Кантора Бернштейна: если A не более мощно чем B, и B не более мощно чем A, то $A \cong B$

▲ Если A не более мощно чем B, то $A \cong B_1$ для некоторого $B_1 \subset B$. Обозначим через f соответствующую биекцию из A в B_1. Аналогично $B \cong A_1$ для некоторого $A_1 \subset A$, обозначим через g биекцию из B в A_1. Определим A_2 как $g(B_1)$. Поскольку $B_1 \subset B$, то $A_2 = g(B_1) \subset g(B) = A_1$, при этом $A_2 \cong B_1 \cong A$. Получим утверждение, эквивалентное исходной теореме: если $A_2 \subset A_1 \subset A_0$ и $A_2 \cong A_0$, то $A_1 \cong A_0$. Это утверждение мы и будем доказывать.

Обозначим через h композицию $g \circ f$. Это биекция из A_0 в A_2. Для всех натуральных $k > 2$ определим рекурсивно A_k как $h(A_{k-2})$. Также определим "слои"C_k как $A_k \setminus A_{k+1}$. Поскольку h — биекция, то $h(C_k) = C_{k+2}$ и h задаёт биекцию между C_k и C_{k+2}. Однако не обязательно любой элемент A_0 войдёт в какой-то слой. Будет ещё "ядро"$C = \bigcap_{k=0}^{\infty} A_k$. Тогда $A_0 = C \cup C_0 \cup C_1 \cup C_2 \cup C_3 \cup ...$ и $A_1 = C \cup C_1 \cup C_2 \cup C_3 \cup ....$ Наконец, построим биекцию α между A_0 и A_1:

$$\alpha(x) = \begin{cases} x, x \in C \cup C_1 \cup C_3 \cup C_5 \cup ... \\ h(x),\ x \in C_0 \cup C_2 \cup C_4 \cup ... \end{cases}$$

Это действительно биекция: все элементы слоёв с нечётными номерами, а также элементы ядра, остаются на месте, а все слои с чётными номерами биективно отображаются в слои с номерами, на 2 бОльшими. Поэтому все слои, кроме нулевого, оказываются покрыты. Таким образом, эквивалентное утверждение, а с ним и исходная теорема, доказаны. ■



17 Отношения на множествах. Свойства бинарных отношений. Отношения эквивалентности, теорема о классах эквивалентности

Любое свойство можно отождествить с множеством всех объектов, которые им обладают. Например, свойство чётности соответсвует множеству чётных чисел.

Свойством элементов множества A называется любое подмножество A или, что тоже самое, любая функция из A в $\{0,1\}$.

Бинарным отношением на множестве A называется любое подмножество $A^2 = A \times A$ или, что тоже самое, любая функция из A^2 в $\{0,1\}$. Обозначения: $(x,y) \in R$ или $R(x,y) = 1$ или xRy.

Предикатом валентности k на множестве A называется подмножество A^k или, что тоже самое, функция из A^k в $\{0,1\}$.

Классификация отношений:

1. рефлексивные $\forall x\ xRx$ ($=$ $\leqslant$ $\vdots$ $\subset$ $\cong$)
2. антирефлексивные $\forall x\ \neg(xRx)$ ($<$)
3. симметричные $\forall x,y\ \ xRy \to yRx$ ($=$ $\cong$ mod $\parallel$)
4. антисимметричные $\forall x,y\ \ (xRy \wedge yRx) \to (x = y)$ ($<$ $\leqslant$ $\vdots$ $\subset$)
5. транзитивные $\forall x,y,z\ \ (xRy \wedge yRz) \to xRz$ ($=$ $<$ $\vdots$ $\subset$ $\cong$)
6. антитранзитивные $\forall x,y,z\ \ (xRy \wedge yRz) \to \neg(xRz)$ ($\perp$ на плоскости)
7. евклидово (правое) $\forall x,y,z\ \ (xRy \wedge xRz) \to yRz$ (нетразитивное R = {(1,2),(2,2),(2,3),(3,2),(3,3)

Наборы свойств:

- ▷ отношение эквивалентности: *рефлексив. + симметрич. + транзитив.*
- ▷ отношение нестрогого (частичного) порядка: *рефлексив. + антисимметрич. + транзитив.*
- ▷ отношение строгого (частичного) порядка: *антирефлексив. + антисимметрич. + транзитив.*
- ▷ отношение (нестрогого) предпорядка: *рефлексив. + транзитив.*

Отношения эквивалентности

Примеры: $=$ mod $\sim$ (подобие тругольников) $\parallel$ (паралленльность или совпадение прямых) и тд

Общий пример: задана $F : A \to B$ $\quad x \sim y$, если $f(x) = f(y)$

Тогда:

$\boxed{=}$ $f : A \to A \quad f(x) = x$

$\boxed{\mathrm{mod}k}$ f возвращает остаток при делении на k

$\boxed{\|}$ f возвращает направление (элемент проективной прямой)

$\boxed{\sim}$ f возвращает форму (3 угла, упорядоченных по неубыванию, в сумме дающие 180°)

Пусть на множестве A задано отношение $\sim$, тогда **классом эквивалентности** элемента $x \in A$ называется множество $K_x = \{y \mid y \sim x\}$

Теорема. (Основная теорема об отношениях эквивалентности)
Если на множестве задано отношение эквивалентности, то все множество разбивается на классы эквивалентности (т.е. представляется в виде такого объединения непересекающихся подмножеств, что два элемента эквивалентны тогда и только тогда, когда лежат в одном и том же подмножестве).

Иначе говоря, если на множестве A задано отношение эквивалентности, то $A = \cup_{i \in I} A_i$ таких, что

1. если $x \in A_i$, то $A_i = K_x$
2. если $x \in A_i$ и $y \in A_i$, то $x \sim y$
3. при $i \neq j$ если $x \in A_i$ и $y \in A_j$, то $\neg(x \sim y)$

Искомая функция (отношение эквивалентности) отображает x в K_x и тем самым делит множество на классы эквивалентности.

▶ Так как отношение эквивалентности состоит из рефлексивности, симметричности и транзитивности, то получаем

0. из рефлексивности ($\forall x \; xRx$) следует, что $x \in K_x$, т.е. каждый элемент лежит в своем классе эквивалентности

1. если $y \in K_x$ и $z \in K_x$, то $y \sim z$ получаем следующими рассуждениями. Так как $y \in K_x \to y \sim x$, $z \in K_x \to z \sim x$, т.е. $x \sim z$. Тогда по транзитивности $y \sim z$

2. если $z \in K_x$, $z \in K_y$, то $K_x = K_y$ получем следующими рассуждениями. Так как $z \in K_x \to z \sim x$, т.е. $x \sim z$, $z \in K_y \to z \sim y$. Тогда по транзитивности $x \sim y$.
   Пусть $t \sim K_x$. Тогда $t \sim x$, по транзитивности $t \sim y$. Таким образом, $K_x \subset K_y$ и $K_y \subset K_x$, следовательно $K_x = K_y$. По контрапозиции если $K_x \neq K_y$, то $K_x \cap K_y = \varnothing$.

3. если $K_x \neq K_y$, $z \in K_x$, $t \in K_y$, то $\neg(z \sim t)$ так как, если бы $z \sim t$, то по транзитивности $z \sim y$, откуда $z \in K_x \cap K_y$, что противоречит предыдущему пункту. Следовательно, $\neg(z \sim t)$. ■

Задача: Являются ли следующие отношения отношениями эквивалентности? Если да, то укажите, на какие классы разбиваются соответсвующие множества.

(a) $|x - y| \vdots k, \quad x,y \in \mathbb{Z}, k \in \mathbb{N}, k > 0$

▲ $\forall x \; |x - x| \vdots k$ OK; $\forall x,y \; |x - y| \vdots k \quad |y - x| \vdots k$ OK; $\forall x,y,z \; |x - y| \vdots k \quad |y - z| \vdots k$ имеют одинаковый остаток OK. Следовательно, классы эквивалентности по остаткам. ■

(б) $\{((x_1, y_1), (x_2,y_2)) \mid x_1 - x_2 = y_1 - y_2\}$ на плоскости

▲ Две точки на плоскости, удовлетворяющие заданному отношению, определяют прямую параллельную $y = x$. $\forall (x_1, y_1)\ 0 = 0$ OK; $\forall (x_1, y_1), (x_2,y_2)\ D_1 = D_2$ и $-D_1 = -D_2$ OK; $\forall (x_1, y_1), (x_2,y_2), (x_3,y_3)$
$D_1 = D_2\ D_2 = D_3$ и $D_1 = D_3$ OK. Значит, классы эквивалентности прямых вида $y = x + b$. ■

(в) $|x - y| < 1, \quad x \in \mathbb{R}$

▲ $0\, R\, \frac{2}{3}$ и $\frac{2}{3}\, R\, \frac{4}{3}$, но $0\, R\, \frac{4}{3}$ WA. Следовательно, не является отношением эквивалентности. ■

(г) $\{(AB, CD) \mid ABCD -$ параллелограмм, возможно вырожденный$\}$ на множестве направленных отрезков, возможно вырожденных, на плоскости

▲ Рефлексивность очевидно выполнена OK; симметричность тоже OK; транзитивность для векторов тоже верна, так как возможны вырожденные случаи OK. Следовательно, классы эквивалентности параллелограммов. ■

(д) $x \| y$; $x \| y$ или $x = y$ на множестве всех прямых на плоскости

▲ Если считать, что параллельные прямые - это прямые не имеющие общих точек, то рефлексивность не выполняется WA. Следовательно, первое не является отношением эквивалентности.
Во-втором случае рефлексивность уже выполнена OK; симметричность тоже OK; транзитивность для параллельности с совпадением тоже верна OK. Следовательно, классы эквивалентности направления. ■

(е) x гомотетичен y; x подобен y на множестве всех треугольников на плоскости

▲ Для гомотетии транзитивность неверна. В качестве примера можно рассмотреть треугольники X, Y, Z, где X = Z (со сдвигом в плоскости), а X и Y, Y и Z соответсвенно гомотетичны. Тогда транзитивности нет. WA. Следовательно, первое не является отношением эквивалентности.
Во-втором случае рефлексивность выполнена, так как треугольник подобен сам себе OK; симметричность тоже OK; транзитивность тоже выполнена по равенству углов треугольников (3 признак подобия) OK. Следовательно, классы эквивалентности наборов величин углов треугольника. ■

(ж) из x существует путь в y на множестве всех вершин некоторого графа.

▲ Рефлексивность выполнена, так как существует нулевой путь из вершины в саму себя OK; симметричность тоже выполнена, так как граф не ориентирован OK; транзитивность тоже выполнена, так как можно произвести неформальное сложение путей OK. Следовательно, классы эквивалентности компоненты связности. ■

(з) последовательность $a_n - b_n$ бесконечно мала на множестве всех последовательностей рациональных чисел.

▲ Рефлексивность выполнена, так как $\lim_{x\to\infty}(a_n - a_n) = 0$ OK; симметричность тоже выполнена, так как граф $\lim_{x\to\infty}(a_n - b_n) = \lim_{x\to\infty}(b_n - a_n) = 0$ OK; транзитивность тоже выполнена, так как $\lim_{x\to\infty}(a_n - c_n) = \lim_{x\to\infty}(a_n - b_n + b_n - c_n) = 0$ OK. Следовательно, классы эквивалентности действительных чисел, к которым стремятся последовательности. ■

(з) f и g равны в нуле; f и g равны в некоторой точке на множестве функций из $\mathbb{R}$ в $\mathbb{R}$

▲ В первом случае рефлексивность очевидно выполнена OK; симметричность тоже OK; транзитивность тоже выполнена так как если $f(0) = g(0) = c$ и $g(0) = h(0) = d$, то $c = g(0) = d$ OK. Следовательно, классы эквивалентности по значению в нуле.
Во-втором случае транзитивность не выполнена, так как одна функция может совпадать с другой в точке a, которая совпадает с третьей в точке b, но при этом не факт, что первая и третья функции совпадают в какой-либо точке WA. Следовательно, не является отношением эквивалентности. ■

Задача: Докажите, что ни одно требование в определении отношения эквивалентности не является лишним: например, существует симметричное, транзитивное, но не рефлексивное отношение.

▲ Возьмем социальное отношение «быть знакомым с ...», или в более чёткой форме отношение «когда-либо встретиться с ...». Тогда рефлексивность выполнена, так как всякий человек встречался с собой OK; симметричность тоже выполнена, так как если один человек встретился с другим, то второй встретился с первым OK; но транзитивность не выполнена, так как если один человек встретился с другим, который встретился с третьим, то не факт, что первый и третий встречались WA. Следовательно, существует симметричное, транзитивное, но не рефлексивное отношение. ■

18 Отношения частичного и линейного порядка. Примеры отношений. Любое счётное упорядоченное множество можно доупорядочить линейно

Как было указано ранее, отношение называется **отношением частичного порядка**, если оно рефлексивно, антисимметрично и транзитивно. При этом антисимметричность: $\forall x,y \;\; (xRy \wedge yRx) \to (x = y)$

(Частично) упорядоченным множеством (сокращенно ч.у.м.) называется пара $\langle A, \leqslant_A \rangle$ — множество и частичный порядок (отношение порядка) на нем.

Частичный порядок называется **линейным порядоком**, если любые два различных элемента множества сравнимы. (Диаграмма Хассе вырождается в цепочку, т.е. линию). Если порядок линеен, множество называется **линейно упорядоченным**.

Отношение называется **отношением строгого порядка**, если оно транзитивно и антирефлексивно.

Задача: Проверьте, что следующие множества являются упорядоченными. Какие из них упорядочены линейно?

(а) $\langle A, = \rangle$, $\langle 2^A, \subset \rangle$ где A - произвольное множество.

▲ $A = A$ OK; $x = y$ OK; $\big((x = y) \wedge (y = z)\big) \to (x = z)$ OK; Очевидно, порядок не линеен. WA
Во-втором случае $2^A \subset 2^A$ OK; $\big((x \subset y) \wedge (y \subset x)\big) \to (x = y)$ OK; $x \subset y \subset z \to x \subset z$ OK;
Если $A = \{0,1\}$, то $\{0\}$ и $\{1\}$ не сравнимы, следовательно, порядок не линеен. WA ■

(б) $\langle A, \leqslant\rangle$, $\langle A, \geqslant\rangle$ где A - одно из множеств $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$.

▲ $x \leqslant x$ OK; $\big((x \leqslant y) \wedge (y \leqslant x)\big) \to (x = y)$ OK; $\big((x \leqslant y) \wedge (y \leqslant z)\big) \to (x \leqslant z)$ OK.
Аналогично с $\geqslant$. По очевидным причинам в обоих случаях это линейный порядок. OK ■

(в) $\langle \mathbb{N}, \vdots \rangle$

▲ $x \vdots x$ OK; $\big((x \vdots y) \wedge (y \vdots x)\big) \to (x = y)$ OK; $\big((x \vdots y) \wedge (y \vdots z)\big) \to (x \vdots z)$ OK.
Элементы 2 и 3 не сравнимы, следовательно, порядок не линеен. WA ■

(г) $\langle \mathbb{R}^2, \leqslant_{lex}\rangle$ где $(x_1,y_1) \leqslant_{lex} (x_2,y_2)$, если либо $x_1 < x_2$, либо $x_1 = x_2$ и $y_1 \leqslant y_2$

▲ $(x,y) \leqslant_{lex} (x,y)$ OK; $\Big(\big((x_1,y_1) \leqslant_{lex} (x_2,y_2)\big) \wedge \big((x_2,y_2) \leqslant_{lex} (x_1,y_1)\big)\Big) \to \big((x_1 = x_2) \wedge (y_1 = y_2)\big)$ OK; $\Big(\big((x_1,y_1) \leqslant_{lex} (x_2,y_2)\big) \wedge \big((x_2,y_2) \leqslant_{lex} (x_3,y_3)\big)\Big) \to \big((x_1,y_1) \leqslant_{lex} (x_3,y_3)\big)$ OK.
По очевидным причинам это линейный порядок. OK ■

(д) $\langle \mathbb{R}^2, \leqslant\rangle$ где $(x_1,y_1) \leqslant (x_2,y_2)$, если $x_1 \leqslant x_2$ и $y_1 \leqslant y_2$

▲ $(x,y) \leqslant (x,y)$ OK; $\Big(\big((x_1,y_1) \leqslant (x_2,y_2)\big) \wedge \big((x_2,y_2) \leqslant (x_1,y_1)\big)\Big) \to \big((x_1 = x_2) \wedge (y_1 = y_2)\big)$ OK; $\Big(\big((x_1,y_1) \leqslant (x_2,y_2)\big) \wedge \big((x_2,y_2) \leqslant (x_3,y_3)\big)\Big) \to \big((x_1,y_1) \leqslant (x_3,y_3)\big)$ OK.
Элементы (2,3) и (3,1) не сравнимы, следовательно, порядок не линеен. WA ■

Задача: Докажите, что любое счётное упорядоченное множество можно доупорядочить линейно. (Т.е. для любого отношения порядка R существует отношение линейного порядка S, такое что $R \subset S$.)

▲ Занумеруем все пары, которые еще не упорядочены. Далее, рассмотрим первую пару таких a и b, что $(a,b),(b,a) \notin R$. Построим новое отношение $R' \mid R \subset R'$, в котором положим $cR'd$ для всех таких c и d, что $(c,a),(b,d) \in R$. Проверим, что R' является отношением порядка.
Рефлексивность выполнена, так как R рефлексивно. Рассмотрим антисимметричность $(c,d),(d,c)$:

1. если оба этих отношения из R, тогда $c = d$;
2. если одно из R, а другое из R', тогда имеем cRa, bRd и dRc, откуда по транзитивности R выполнено bRa, т.е. эти элементы сравнимы в R - противоречие;
3. если оба этих соотношения из R', то имеем cRa, bRd, bRc и dRa, и снова по транзитивности aRb и bRa.

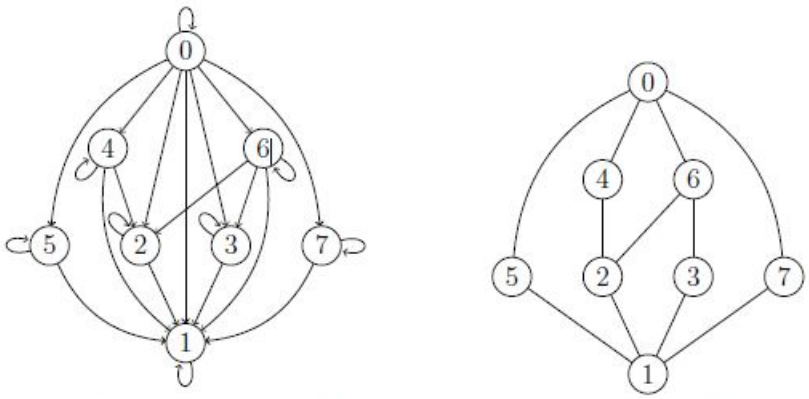
Транзитивность R' проверяется аналогично.

Таким образом, R' - частичный порядок. Тогда выкинем из нашей нумирации все добавленные пары и рассмотрим следующую по номеру пару, которая не упорядочена. Продолжая этот процесс, мы получим линейный порядок S, содержащий данный. ■

19 Частично упорядоченные множества. Диаграмма Хассе. Изоморфизм. Описание попарно неизоморфных ч.у.м. для 3-х и 4-х элементов. Минимальные, максимальные, наибольшие и наименьшие элементы.

Множество A с заданным на нем частичным порядком R называется **частично упорядоченным множеством (ЧУМ)** и обозначается (A; R). **Отношением (нестрого частичного) порядка** называется любое рефлексивное, антисимметричное и транзитивное отношение.

Диаграммой Хассе называется ориентированный граф без циклов, по которому отношение порядка строится так: $a \leqslant b$, если из a в b идёт ориентированный путь. Диаграмму Хассе для отношения можно получить из ориентированного графа, его изображающего, выкидыванием петель и таких рёбер между вершинами a и c, если есть вершина b, такая, что: $a < b < c$. Кроме того, вместо рисования стрелок граф располагают так, чтобы большие элементы находились выше.

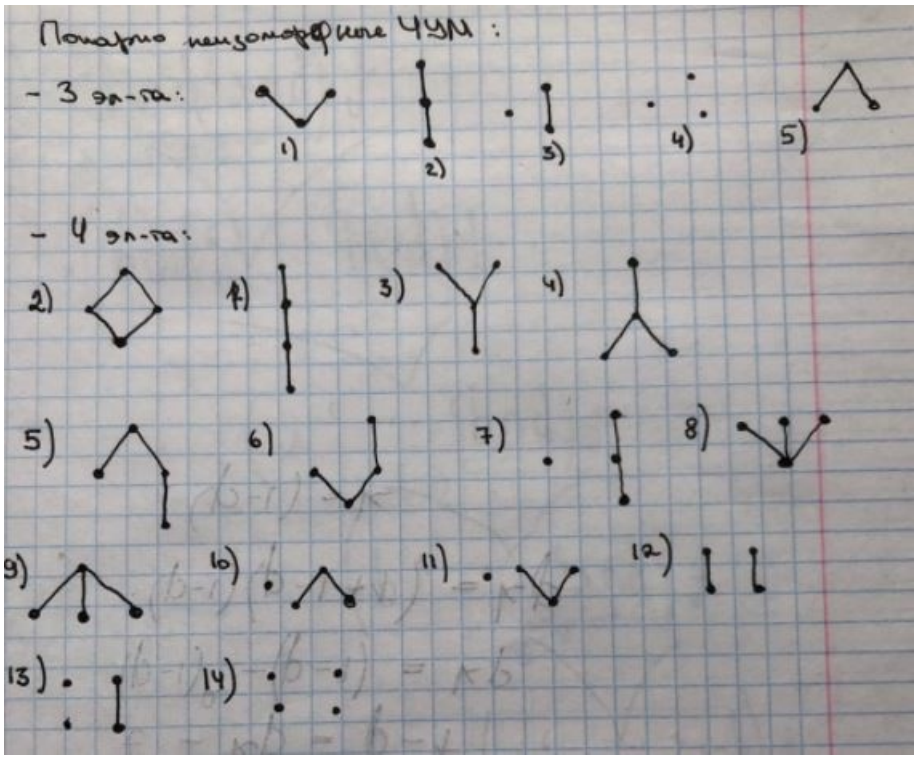


(а) Несокращённый граф (б) Диаграмма Хассе

Рис. 2: Упрощение картины с использованием диаграммы Хассе

Изоморфизмом упорядоченных множеств $(A, \leqslant_A)$ и $(B, \leqslant_B)$ называется биекция $f : A \to B$, для которого выполнено свойство: $x \leqslant_A y \Leftrightarrow f(x) \leqslant_B f(y)$. Обозначение: $A \simeq B$.

Описание попарно неизоморфных ч.у.м. для 3-х и 4-х элементов. Доказательство основывается на попарно неизоморфных графах без петель и кратных рёбер (для n=3 их 4, для n=4 их 11)



Элемент $x \in A$ **наибольший** в упорядоченном множестве $(A, \leqslant_A)$, если $\forall y \in A : y \leqslant_A x$. Элемент $x \in A$ **максимальный** в упорядоченном множестве $(A, \leqslant_A)$, если $\nexists y \in A : x <_A y$. Наименьший и минимальный элементы определяются аналогично.

Свойства максимальных/наибольших/минимальных/наименьших элементов:
1. Наибольший элемент всегда является максимальным, причём единственным;
2. Максимальных элементов может быть несколько;
3. Единственный максимальный элемент не всегда является наибольшим.

▲ 1. Если x наибольший, то $x \leqslant y$ для всех $y \in A$. Поэтому $x \not< y$ для всех y. Поэтому он максимален. Любой другой элемент будет меньше наибольшего и потому не будет максимальным.

2. Например, можно взять натуральные числа от 1 до 10 и отношение делимости. Максимальными будут числа 6, 7, 8, 9, 10: на них никакое число из этого интервала не делится.

3. Например, можно взять множество $\{3\} \cup \{2^n | n \in \mathbb{N}\}$ с отношением делимости. 3 является единственным максимальным элементом, т.к. на любое другое делится ещё какое-то число. Но наибольшего элемента тут нет. ■

20 Диаграмма Хассе. Определение цепи и антицепи. Теорема о длине наибольшей цепи в ч.у.м. (б/д). Доказательство теоремы на примерах задач о людоедах и числах.

Диаграммой Хассе называется ориентированный граф без циклов, по которому отношение порядка строится так: $a \leqslant b$, если из a в b идёт ориентированный путь. (см. билет 19)

Цепь упорядоченного множества $\langle M, \leqslant_M \rangle$ - упорядоченная последовательность элементов $a_1, a_2, \ldots, a_n$, для которой $a_i \leqslant_M a_{i+1}$ для всех $1 \leqslant i \leqslant n-1$. **Антицепь** - набор элементов, никакие два из которых не находятся в отношении $\leqslant_M$.

Теорема. Если d длина наибольшей цепи в упорядоченном множестве, то упорядоченное множество можно разбить на d антицепей.

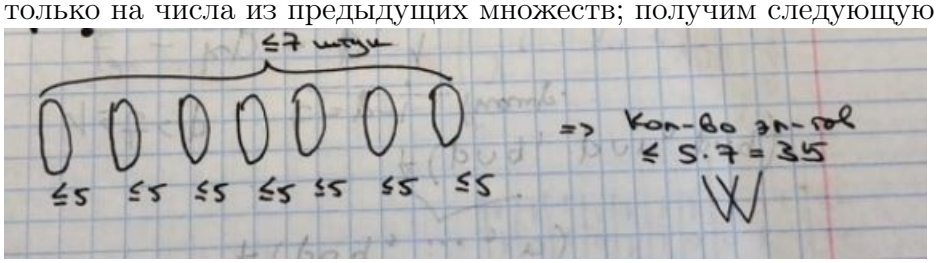
Задача 6.2 про людоедов Некоторые людоеды хотят съесть некоторых других людоедов. Известно, что длина наибольшей цепочки, в которой каждый людоед хочет съесть последующего, равна n (в частности, циклов нет). Докажите, что людоедов можно рассадить в n пещер, в каждой из которых никто никого не хочет съесть. Можно ли гарантированно рассадить их в меньшее число пещер?

▲ Аналогично задаче 6.3, выбираем сначала все минимальные элементы для этого ч.у.м. Каждая следующая пещера: все людоеды, которых хотят съесть только людоеды из предыдущих пещер. Из условия, что максимальная цепь n, мы разбиваем всех великанов на n пещер, в каждой пещере антицепь. При этом гарантированно меньше пещер получить нельзя, рассмотрим пример с n великанами, где каждый великан пронумерован, и хочет съесть всех великанов с номером, большим, чем у него. ■

Теорема. В упорядоченном множестве из mn + 1 элемента есть цепь длины n + 1 или антицепь из $m + 1$ элемента.

Задача 6.3 про числа (а) Докажите, что среди 36 различных натуральных чисел или найдется 6 чисел, среди которых ни одно не делится на другое, или найдется 8 чисел, которые можно выстроить в цепь, где каждое число делится на следующее. (б) Верен ли аналогичный факт для целых чисел?

▲ (а) Пусть не найдётся ни цепь длины 8, ни антицепь длины 6. Тогда возьмём все числа, которые в данном ч.у.м. являются минимальными. Очевидно, что количество таких чисел $\leqslant 5$. Последовательно будем выбирать множества чисел, которые делятся только на числа из предыдущих множеств; получим следующую схему:



Нашли противоречие. Значит, начальное утверждение неверно.
(б) Формально, делимость среди целых чисел не является ч.у.м., т.к. нарушена антисимметричность => теорема не применима с её доказательством. Однако мы можем доопределить целые числа до ч.у.м.: будем считать, что -7 делится на 7, но не наоборот. Тогда делимость на таких целых числах будет ч.у.м. и можно применить теорему (аналогичные рассуждения из пункта а) ■

23 Предпорядки: определение и примеры. Разбиение элементов множества с предпорядком на классы эквивалентности

Предпорядком называется любое рефлексивное транзитивное отношение. Стандартное обозначение: $\precsim$. Если на множестве задан предпорядок, то оно называется предупорядоченным.

Примеры предпорядков: (задача 7.1)

1. любой частичный порядок
2. любое отношение эквивалентности
3. сравнение по мощности на множествах
4. отношение достижимости в ориентированном графе
5. обратное отношение к предпорядку также является предпорядком
6. $x \precsim y$, если $f(x) \leqslant f(y)$, где $f : M \to Q$, а Q - ЧУМ

Разбиение элементов множества с предпорядком на классы эквивалентности:

Пусть на множестве M задан предпорядок $\precsim$. **Отношение безразличия** ($\sim$) - это такое отношение, что $a \sim b$, если $a \precsim b$ и $b \precsim a$.

Отношение безразличия является отношением эквивалентности (задача 7.2), так как выполнены

1. Рефлексивность: $a \sim a$, так как $a \precsim a$
2. Симметричность: $a \sim b \Rightarrow a \precsim b$ и $b \precsim a \Rightarrow b \sim a$
3. Транзитивность: $a \sim b,\ b \sim c \Rightarrow a \precsim b,\ b \precsim c,\ c \precsim b,\ b \precsim a \Rightarrow a \precsim c,\ c \precsim a$ (в силу транзитивности предпорядка) $\Rightarrow a \sim c$

24 Полный предпорядок. Равносильность полноты предпорядка и линейности индуцированного предпорядка.

Предпорядок называется **полным**, если для любых двух элементов x и y выполнено $x \precsim y$ или $y \precsim x$.

Индуцированный порядок:

На множестве классов эквивалентности можно корректно ввести частичный порядок по правилу $K_a \leqslant K_b$, если $\exists a \in K_a,\ b \in K_b$, такие что $a \precsim b$. Докажем, что это действительно отношение порядка (см. задачу 7.3)

1. Рефлексивность: $K \leqslant K$, так как $a \precsim a$
2. Антисимметричность: $K \leqslant L,\ L \leqslant K \Rightarrow \exists l_1, l_2 \in L, k_1, k_2 \in K :\ k_1 \precsim l_1,\ l_2 \precsim k_2 \Rightarrow k_1 \precsim l_1 \precsim l_2,\ l_2 \precsim k_2 \precsim k_1$ (так как они k_1 и k_2, l_1 и l_2 лежат в одном классе эквивалентности) $\Rightarrow k_2 \precsim l_2 \Rightarrow k_2 \sim l_2 \Rightarrow K = L$

3. Транзитивность: $K \leqslant L,\ L \leqslant M \Rightarrow \exists k_1 \in K,\ l_1,\ l_2 \in L,\ m_1 \in M:\ k_1 \precsim l_1,\ l_2 \precsim m_1 \Rightarrow k_1 \precsim l_1 \precsim l_2 \precsim m_1$ (так как l_1 и l_2 лежат в одном классе эквивалентности) $\Rightarrow k_1 \precsim m_1$ (по транзитивности предпорядка) $\Rightarrow K \leqslant M$

Утверждение (задача 7.4): предпорядок полон $\Leftrightarrow$ индуцированный порядок на классах эквивалентности линеен

▲ $\Rightarrow$ Рассмотрим два произвольных класса эквивалентности X и Y. Выберем из них по одному элементу $x \in X$ и $y \in Y$. В силу полноты предпорядка либо $x \precsim y$, либо $y \precsim x \Rightarrow$ либо $X \leqslant Y$, либо $Y \leqslant X \Rightarrow$ индуцированный порядок линеен

$\Leftarrow$ Рассмотрим два произвольных элемента k_1 и l_1, которые принадлежат соответственно классам K и L. Так как индуцированный порядок линеен, то K и L сравнимы (для определенности можем считать, что $K \leqslant L$). Тогда существуют такие элементы $k \in K$ и $l \in L$, что $k \precsim l \Rightarrow k_1 \precsim k \precsim l \precsim l_1$ (так как k и k_1, l и l_1 лежат в одном классе эквивалентности) $\Rightarrow k_1 \precsim l_1$ (по транзитивности) $\Rightarrow$ предпорядок полон ■

25 Квазитранзитивные и ациклические отношения. Свойства и примеры.

Пусть на множестве M задано отношение $\preccurlyeq$. По нему можно построить строгое отношение $\prec$ по правилу: $x \prec y$, если $x \preccurlyeq y$, но $y \not\preccurlyeq x$. Назовём $\preccurlyeq$ **квазитранзитивным**, если из $x \prec y$ и $y \prec z$ следует, что $x \prec z$.

Отношение $\preccurlyeq$ называется **ациклическим**, если в каждом непустом конечном множестве $M_0 \subset M$ найдётся максимальный элемент, т.е. такой x, что $x \prec y$ неверно ни для какого y.

Утверждение (задача 7.5): любой предпорядок квазитранзитивен

▲ Рассморим x, y, z, такие что $x \precsim y,\ y \not\precsim x,\ y \precsim z,\ z \not\precsim y$ (то есть $x \prec y,\ y \prec z$). Тогда по транзитивности предпорядка $x \precsim z$. Пусть $z \precsim x$. Тогда $z \precsim x \precsim y \Rightarrow z \precsim y$ (по транзитивности) - противоречие с выбором $x, y, z \Rightarrow z \not\precsim x \Rightarrow x \prec z \Rightarrow$ предпорядок квазитранзитивен ■

Задача 7.6: Придумайте рефлексивное и квазитранзитивное отношение, не являющееся предпорядком. Может ли такое отношение быть полным?

Решение: Да, такое отношение может быть полным. Пример (петли рисовать не стал):

Утверждение (задача 7.7): квазитранзитивное отношение является ациклическим

▲ Пусть это не так. Тогда существует некоторое конечное множество вершин M_0 являющееся циклом, т.е. $m_0 \prec m_1 \prec ... \prec m_k \prec m_0$. Тогда по транзитивности получаем $m_0 \prec m_k$, но $m_k \prec m_0$ - противоречие определению $\prec \Rightarrow$ отношение ациклическое ■

Задача 7.8: Придумайте ациклическое отношение, не являющееся квазитранзитивным. Может ли такое отношение быть полным?

Решение: Например, $\{(a, b), (b, c)\} \subset \{a, b, c\}^2$ (думаю, комментарии излишни).

Пусть есть полное ациклическое не квазитранзитивное отношение $\preccurlyeq$ над A, тогда $\exists x, y, z \in A$, такие что $x \prec y \wedge y \prec z \wedge \neg(x \prec z)$ (отрицание определения квазитранзитивности). Так как отношение полное, то $z \prec x$, но тогда во множестве $A' = \{x, y, z\}$

$\forall a \in A' \; \exists b \in A' : a \prec b$ - противоречие $\Rightarrow$ такое отношение не может быть полным ■

26 Правило сложения. Правило умножения. Примеры. Принцип Дирихле. Пример на принцип Дирихле.

Предположим, что у нас имеются 2 множества (здесь и далее предполагаем, что рассматриваемые множества конечны, если не оговорено обратного): A = $\{a_1, a_2, \ldots, a_n\}$ и B = $\{b_1, b_2, \ldots, b_m, \}$.

Базовые принципы комбинаторики:

1. **Правило суммы**: Количество способов выбрать один объект из A или B в предположении, что $A \cap B = \varnothing$, равно n + m.
2. **Правило произведения**: Количество способов выбрать один объект из A и к нему в пару один объект из B равно $n * m$.
3. **Принцип Дирихле**: Предположим, имеется n ящиков и $n + 1$ кролик, которые сидят в этих ящиках. Тогда найдется ящик, в котором сидит $\geqslant 2$ кролика.

Обобщённый принцип Дирихле: Если $nk + 1$ элементов разбить на n множеств, то хотя бы в одном множестве содержится $k + 1$ элемент.

Формальная запись: Пусть задано отображение $f : A \to B$ на конечных множествах A и B, причём $|A| > |B|$. Тогда отображение f неинъективно.

Задача: Найти количество шестизначных чисел с различными цифрами.

Решение: Для первой цифры есть 9 возможных вариантов (все, кроме нуля), для второй цифры 9 вариантов (все, кроме первой), для третьей 8 (все, кроме первых двух), и так далее. Тогда по правилу произведения всего количество шестизначных чисел с различными цифрами: $9 * 9 * 8 * 7 * 6 * 5$.

Задача: Пусть есть квадрат со стороной 2, внутри которого выбраны пять точек. Доказать, что внутри него найдутся две точки, такие, что расстояние между ними не превосходит корня из двойки.

▲ Рассмотрим 4 квадратика 1x1. По принципу Дирихле, найдется квадратик, внутри или на границе которого 2 точки. Эти точки — искомые. ■

27 Принцип Дирихле. Оценки мощности множества попарно неортогональных $(-1, 0, 1)$-векторов: верхняя оценка величиной 140 и нижняя оценка величиной 70.

Рассмотрим множество $V = \{\overline{x} = (x_1, \ldots, x_n) : x_i \in \{1; 0; -1\}, x_1^2 + \cdots + x_n^2 = 4\}$. $|V| = C_8^4 * 2^4 = 1120$. Рассмотрим произвольное $W \subset V : \forall \overline{x}, \overline{y} \in W : (x, y) \neq 0$. Max$|W|$ - ?

Нижняя оценка: Пусть $x_1 = 1$, а остальные координаты либо 0, либо 1. Такое множество подходит под условие W. Аналогично построим множество векторов, где $x_1 = -1$, остальные координаты либо 0, либо -1. Это множество тоже подходит под условие W, причём условие сохраняется даже для объединения этих множеств. Тогда нижняя оценка: $\max|W| \geqslant 2 * C_7^3 = 2 * 35 = 70$.

Верхняя оценка: Разобьем множество V на подмножества-ящики, внутри которых любые два вектора гарантированно дают ноль. Первый ящик: (1, 1, 1, 1, 0, 0, 0, 0), (1, -1, -1, 1, 0, 0, 0, 0), (1, -1, 1, -1, 0, 0, 0, 0), (1, 1, -1, -1, 0, 0, 0, 0) и ещё четыре вектора, которые получены из первых четырёх, поменяв местами x_5 и x_1 и.т.д. Второй ящик: (1, -1, -1, -1, 0, 0, 0, 0), (1, -1, 1, 1, 0, 0, 0, 0), (1, 1, -1, 1, 0, 0, 0, 0), (1, 1, 1, -1, 0, 0, 0, 0) и ещё четыре вектора, полученные аналогичным способом. Третий ящик - векторы первого, домноженные на -1, четвёртый - векторы второго, домноженные на -1. Всего способов выбрать четыре нуля - 35, тогда всего таких ящиков $35 * 4 = 140$. Два вектора не могут быть в одном ящике, значит, $\max|W| \leqslant 140$.

28 Теорема о раскраске множества в два цвета.

Теорема. Пусть $R = \{1,2,\ldots,30\}$ $M_1,M_2,\ldots,M_{15} \subset R$ $|M_i| = 5$. Всегда найдется раскраска множества R в два цвета так, что все M_i неодноцветны. mathbb ▲ Заметим, что количество всех раскрасок 2^{30}.
Количество раскрасок, при которых конкретное M_i одноцветное, равно $2^{25} \cdot 2 = 2^{26}$.
Количество раскрасок, при которых хотя бы одно M_i одноцветное, $\leqslant 15 \cdot 2^{26} < 2^4 \cdot 2^{26} = 2^{30}$.

Так как существует "идиотская"раскраска, когда все 30 элементов одного цвета (первого или второго), следовательно, оценку можно улучшить. Количество раскрасок, при которых хотя бы одно M_i одноцветное, $< 15 \cdot 2^{26} < 2^4 \cdot 2^{26} = 2^{30}$. Так как всего раскрасок $= 2^{30}$, а неподходящих по условию $< 2^{30}$, следовательно, найдутся раскраски, при которых все M_i неодноцветны. ■

29 Размещения, перестановки и сочетания. Доказательство формул для чисел размещения и сочетания с повторениями и без повторений.

Пусть $A = \{a_1, \ldots, a_n\}$. Извлекать элементы из A можно по порядку или пригоршнями. Превые называются **размещениями**, вторые - **сочетаниями**.

Размещения с повторениями

$\overline{A}_n^k = n^k$ k - любое порядок важен

Извлекаем с возвращением, а именно, извлекаем один объект из множвества A, вовзращаем его обратно, извлекаем следующий и т.д. k раз. Например, буквы для слова ЖАБА из русского алфавита.

▲ Возьмем n объектов $\{a_1,\ldots,a_n\}$. Мы хотим выбирать объект этого множества и возвращать обратно и так k раз. Это действие можно представить как последовательный выбор объектов по одному из множеств $A_1 = \{a_1,\ldots,a_n\}$, $A_2 = \{a_1,\ldots,a_n\}$, $\ldots$, $A_k = \{a_1,\ldots,a_n\}$. В силу правила умножения мы получим количество способов выбрать k объектов равным n^k. ■

Размещения без повторений

$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$ $0 \leqslant k < n$ порядок важен

Извлекаем объекты последовательно без возвращения, один за другим k раз.

▲ Выберем из $\{a_1, \ldots, a_n\}$ первый объект n способами, назад его не возвращаем, затем извдечем из оставшихся $n-1$ объектов второй объект $n-1$ способом и т.д. вполть до k-го объекта, который мы извлечем $n-k+1$ числом способов. Применим правило умножения и получим требуемое. ■

Перестановки без повторений

$A_n^n = P_n = n! \quad 0 \leqslant k < n$ порядок важен

Частный случай предыдущего.

Сочетания без повторений

$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!} \quad 0 \leqslant k \leqslant n$ порядок не важен

Извлекаем без возвращения, сразу все k объектов, кучей без повторов (неупорядоченно)

▲ Возьмем k объектов и наведем там порядок, следовательно $A_n^k = k! \cdot C_n^k$. ■

Размещения с повторениями

$\overline{C}_n^k = C_{n+k-1}^{k=(n-1)}$ k - любое порядок не важен $\underbrace{\overbrace{11}^{1^{\text{ая}}}\,0\,\overbrace{1}^{2^{\text{ая}}}\,0\overbrace{}^{3^{\text{я}}}0\,\overbrace{111}^{4^{\text{ая}}}}_{k+n-1}$

Извлекаем неупорядоченно k объектов, которые могут повторятся. Например, покупка 5 фруктов в магазине, где есть бесконечное количество лимонов, яблок и груш.

▲ Формула следует из метода шариков и перегородок. ■

Задача: На ютуб-канале есть плейлист из 30 лекций по ОКТЧ. Сколькими способами их можно переставить так, чтобы **(а)** шесть лекций, прочитанных Даниилом Владимировичем, расположились в правильном порядке (не обязательно подряд)? **(б)** те же лекции по-прежнему были в правильном порядке, но никакие две из них не шли подряд?

Решение:

(а) Количество всевозможных перестановок лекций 30!. Так как лекции Мусатова обязательно должны идти в правильном порядке, мы должны из 6! возможных перестановок оставить только 1 корректную.
Ответ: $\frac{30!}{6!}$

(б) Воспользуемся методом шаров и перегородок. Пусть (1) - лекции Мусатова, а (0) - 24 остальные лекции. Тогда расставить остальные лекции можно 24! способами. А для лекций Мусатова у нас 25 мест, на каждое место одна из 6 лекций $\rightarrow$ C_{25}^6 способа.
Ответ: $24! \cdot C_{25}^6$

Задача: Сколькими способами можно нарисовать прямоугольник на клетчатом листке бумаги размером $m \times n$ клеток?

Решение: Первую вершину можно поставить в $(n+1) \cdot (m+1)$ точку сетки. Вершину, которая расположена на диагонале относительно первой, можно поставить в $n \cdot m$ точек сетки. Так как первая вершина выбирается произвольно, то она может совпасть с 2,3 и 4.

Ответ: $\frac{(n+1)\cdot(m+1)\cdot n\cdot m}{4} \sim C_{n+1}^2 \cdot C_{m+1}^2$

Задача: Дано множество $A = \{1,\ldots,n\}$ и числа k, s.**(а)** Сколько можно составить совокупностей из s различных k-элементных подмножеств множества A? **(б)** Сколько из этих совокупностей устроены так, что каждое множество в них имеет непустое пересечение с подмножеством $\{1,\ldots,l\} \subset A$?

Решение:

(а) Количество способов выбрать одно k-элементное подмножество A равно C_n^k. Значит, искомое количество совокупностей - это количество способов выбрать s различных элементов из C_n^k-элементного множества.
Ответ: $C_{C_n^k}^s$

(б) Количество k-элементных подмножеств A, не пересекающихся с множеством $L = \{1,\ldots,l\}$, равно C_{n-l}^k. Поэтому количество k-элементных подмножеств A, пересекающихся с множеством L, равно $C_n^k - C_{n-l}^k$. Аналогично предыдущему пункту получаем количество совокупностей.
Ответ: $C_{C_n^k - C_{n-l}^k}^s$

Задача: Сколькими способами можно выбрать из полной колоды, содержащей 52 карты, 6 карт так, чтобы среди них были все 4 масти?

Решение: Выбираем 4 карты разных мастей 13^4 способами. Осталось выбрать еще 2 карты. Возможно два случая:

- ▷ эти две карты разных мастей, тогда выбор мастей C_4^2 способами и карт 12^2 способами.
- ▷ эти две карты одной масти, тогда выбор масти 4 способами и карт C_{12}^2 способами.

Заметим, что мы разложили карты по мастям двумя способами: 1+1+2+2 и 1+1+1+3. Так как карты, совпавших мастей, можно взять на первои шаге, а можно и на втором, то нужно учесть перестановки.
Ответ: $13^4 \cdot (\frac{12^2 \cdot C_4^2}{2\cdot 2} + \frac{4\cdot C_{12}^2}{3})$

30 Бином Ньютона. Полиномиальный коэффициент и полиномиальная формула

Биномиальные коэффициенты - это коффициенты в разложении $(a+b)^n$ **бинома Ньютона**:

$$(a+b)^n = \underbrace{(a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)}_{n \text{ раз}} =$$

здесь n скобок, после раскрытия которых получается сумма одночленов вида $a^k\, b^{n-k}$ $(k = \overline{0,n})$.
Выясним, сколько раз встречается многочлен $a^k\, b^{n-k}$ при данном k. Он встретится столько раз, сколькими способами можно выбрать k скобок, из которых берется a, т.е. C_n^k. Таким образом, после приведения подобных членов получим формулу

$$\sum_{k=0}^{n} C_n^k\, a^k\, b^{n-k}$$

Полиномиальная формула (обобщение бинома Ньютона)

$$(x_1 + x_2 + \ldots + x_k)^n = \sum_{\substack{\alpha_1 \geqslant 0, \alpha_2 \geqslant 0, \ldots \alpha_k \geqslant 0 \\ \alpha_1 + \alpha_2 + \ldots + \alpha_k = n}} \frac{n!}{\alpha_1! \alpha_2! \ldots \alpha_k!} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}.$$

▲ Выведем полиномиальную формулу. Допустим у нас есть α_1 объект первого типа ... α_k объект k-ого типа. Тогда нас интересует число способов составить "слово" из всех этих объектов. Тогда аналогично биному Ньютона получаем:

$$(x_1 + x_2 + \ldots + x_k)^n = \underbrace{(x_1 + x_2 + \ldots + x_k) \cdot \ldots \cdot (x_1 + x_2 + \ldots + x_k)}_{n \text{ раз}} =$$

Чтобы после раскрытия скобок получился одночлен $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$, нужно выбрать те α_1 скобок, из которых берется x_1, те α_2 скобок, из которых берется x_2 и ... и те α_k скобок, из которых берется α_k. Коэффициент при этом одночлене после приведения подобных членов равен числу способов, которыми можно осуществить такой выбор.
Первый шаг последовательности выборов можно осуществить $C_n^{\alpha_1}$ способами, второй шаг — $C_{n-\alpha_1}^{\alpha_2}$, третий — $C_{n-\alpha_1-\alpha_2}^{\alpha_3}$ и т.д., k-й шаг — $C_{n-\alpha_1-\alpha_2-\ldots-\alpha_{k-1}}$ способами. Искомый полиномиальный коэффициент равен произведению:

$$C_n^{\alpha_1} \cdot C_{n-\alpha_1}^{\alpha_2} \cdot C_{n-\alpha_1-\alpha_2}^{\alpha_3} \cdot \ldots \cdot C_{n-\alpha_1-\alpha_2-\ldots-\alpha_{k-1}} = \frac{n!}{\alpha_1!(n-\alpha_1)!} \cdot \frac{(n-\alpha_1)!}{\alpha_2!(n-\alpha_1-\alpha_2)!} \cdot \ldots \cdot$$

$$\cdot \frac{(n-\alpha_1-\alpha_2-\ldots-\alpha_{k-1})!}{\alpha_k! \underbrace{(n-\alpha_1-\alpha_2-\ldots-\alpha_k)!}_{0!}} = \frac{n!}{\alpha_1! \alpha_2! \ldots \alpha_k!} = P(\alpha_1, \alpha_2, \ldots, \alpha_k) \qquad \blacksquare$$

Задача: Сколько имеется способов раздать 11 разных цветков, трём девушкам: какой-то — 5, а остальным — по 3 цветка?

Решение (1 способ): Тремя способами выбираем девушку, у которой будет больше всех цветов. Цветы для нее можно выбрать C_{11}^5 способами. Одной из двух девушек нужно отдать три цветка из оставшихся шести C_6^3 способами. Оставшиеся 3 цветка идут последней девушке одним способом.
Ответ: $3 \cdot C_{11}^5 \cdot C_6^3$

Решение (2 способ): Воспользуемся полиномиальной формулой для решения это задачи. У нас есть два букета из 3 цветков и один букет из 5 цветков. Тогда остается лишь выбрать двух девушек, которым достанутся маленькие букетики.
Ответ: $C_3^2 \cdot \frac{11!}{(3!)^2 \cdot 5!}$

31 Комбинаторные тождества

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

Замечание: Это свойство симметрии.

$$\textbf{(2)}\ C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

Замечание: Доказательство непосредственно следует из выражения для C_n^k. Однако более интересно другое, раскрывающее его внутреннюю комбинаторную суть, доказательство.

▲ Количество k-сочетаний элементов множества $\{a_1, \ldots, a_n\}$ равно C_n^k. Причем количество таких, которые содержат a_1, равно количеству способов выбрать $k-1$ элементов из $n-1$ оставшихся объектов, то есть C_{n-1}^{k-1}. С другой стороны, количество k-сочетаний, которые не содержат внутри себя a_1, равняется количеству способов выбрать k также из $n-1$ объектов, то есть C_{n-1}^k. Поскольку других возможностей нет: $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$ ■ mathbb

$$\textbf{(3)}\ C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$$

Замечание: Это сумма всех элементов фиксированной строчки треугольника Паскаля.

▲ Формула есть бином Ньютона в случае $a = b = 1$:
$2^n = (1+1)^n = \sum_{k=0}^n C_n^k \, 1^k \, 1^{n-k} = C_n^0 + C_n^1 + \ldots + C_n^n$ ■ mathbb

$$\textbf{(4)}\ (C_n^0)^2 + (C_n^1)^2 + \ldots + (C_n^n)^2 = C_{2n}^n$$

▲ Рассмотрим множество объектов $\{\overbrace{a_1, a_2, \ldots, a_n}\ ;\ \overbrace{a_{n+1}, \ldots, a_{2n}}\}$. Мы выбираем n-сочетаний без повторений из этого множества, при этом k объектов попадает в левую часть, а $n-k$ объектов попадает в правую часть, где $0 \leqslant k \leqslant n$. Тогда получаем, что $C_{2n}^n = \sum_{k=0}^n C_n^k \cdot C_n^{n-k} = \sum_{k=0}^n (C_n^k)^2$ ■ mathbb

$$\textbf{(5)}\ C_n^1 + 2C_n^2 + \ldots + nC_n^n = n \cdot 2^{n-1}$$

▲ Воспользуемся **утверждением**: $kC_n^k = nC_{n-1}^{k-1}$, которое следует из определния числа сочетаний, т.е.
$k \cdot \frac{n!}{k!(n-k)!} = n \cdot \frac{(n-1)!}{(k-1)!(n-k)!}$.
Тогда $0 \cdot C_n^0 + 1C_n^1 + \ldots + nC_n^n = \sum_{k=0}^n k \cdot C_n^k = \sum_{k=0}^n n \cdot C_{n-1}^{k-1} = n \cdot \sum_{k=0}^n C_{n-1}^{k-1} = n \cdot 2^{n-1}$ ■ mathbb

$$\textbf{(6)}\ C_{n+m}^n = C_{n+m-1}^{n-1} + C_{n+m-2}^{n-1} + \ldots + C_{n-1}^{n-1} = \sum_{k=0}^{m} C_{n+m-k-1}^{n-1}$$

▲ Рассмотрим все возможные m-сочетания объектов из множества $\{a_1, \ldots, a_{n+1}\}$ с повторениями. Количество таких m-сочетаний: $\overline{C}_{n+1}^m = C_{n+1+m-1}^m = C_{n+m}^m = C_{n+m}^n$.

Все множество возможных m-сочетаний можно разделить на подмножества, в каждом из которых находятся только такие m-сочетания, где объект a_1 встречается фиксированное количество раз.

Так m-сочетания с повторениями, в которых нет объекта a_1, на самом деле есть m-сочетания из множества $\{a_2, \ldots, a_{n+1}\}$. Их число равно $C_{n+m-1}^m = C_{n+m-1}^{n-1}$. В свою очередь, m-сочетания с повторениями, в которых ровно 1 объект a_1, на самом деле есть $m-1$-сочетания из того же множества. Их число равно $C_{n+m-2}^{m-1} = C_{n+m-2}^{n-1}$. И так далее. ■

32 Сумма степеней натуральных чисел. Знакопеременные тождества

$$\textbf{(1)}\ C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n \cdot C_n^n = \begin{cases} 1 & \text{если } n = 0 \\ 0 & \text{если } n \geqslant 1 \end{cases}$$

▲ Тождество следует из бинома Ньютона в следующем частном случае:
$0 = (1-1)^n = \sum_{k=0}^{n} C_n^k 1^k (-1)^{n-k} = C_n^0 - C_n^1 + C_n^2 - \cdots + (-1)^n C_n^n$ ■
Следствие: $C_n^0 + C_n^2 + C_n^4 + \ldots = C_n^1 + C_n^3 + C_n^5 + \ldots$ mathbb

$$\textbf{(2)}\ \sum_{k=0}^{n} (-1)^k C_n^k (n-k)^m = 0$$

▲ Рассмотрим $A = \{a_1, a_2, \ldots, a_n\},\ m < n$. Положим m-размещения с повторениями, тогда их всего $N = n^m$. Объектами, к которым мы будем применять формулу включений и исключений будут эти N размещений. Размещение обладает свойством α_i, если элемент a_i не принадлежит ему.

Очевидно, $N(\overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_n}) = 0$ это количество объектов не обладающих ни одним из свойств.

Более того: $N(\alpha_i) = (n-1)^m$; $\quad N(\alpha_i, \alpha_j) = (n-2)^m \quad N(\alpha_1, \ldots, \alpha_n) = (n-n)^m = 0$

Тогда, $0 = N(\overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_n}) = \sum_{k=0}^{n} (-1)^k C_n^k (n-k)^m$ ■

Сумма степеней натуральных чисел

Рассмотрим 6 утверждение из комбинаторных тождеств, а именно $C_{n+m}^n = \sum_{k=0}^{m} C_{n+m-k-1}^{n-1}$. Подставим в это тождество $n = 3$ (если в формулу подставить $n = 2$, то получим арифметическую прогрессию).

$$C_{m+3}^3 = \sum_{k=0}^{m} C_{m-k+2}^2 = C_{m+2}^2 + C_{m+1}^2 + \ldots + C_2^2$$

Заменим на эквивалентное левую и правую часть:

$$\frac{(m+1)(m+2)(m+3)}{6} = \frac{(m+1)(m+2)}{2} + \frac{(m+1)m}{2} + \ldots + \frac{2 \cdot 1}{2}$$

На данный момент мы получили пирамиду из апельсинов, но для получения квадратов натуральных чисел проведем дальнейшее преобразование правой части:

$$\frac{(m+1)(m+2)(m+3)}{6} = \frac{(m+1)^2}{2} + \frac{(m+1)}{2} + \frac{m^2}{2} + \frac{m}{2} + \ldots + \frac{1}{2} + \frac{1}{2}$$

Просуммируем те слагаемые, у которых числитель стоит без квадрата (т.е. каждое второе слагаемое) и получим $\frac{(m+1)(m+2)}{4}$ откуда вытекает, что

$$1^2 + 2^2 + \ldots + (m+1)^2 = 2 \cdot \left(\frac{(m+1)(m+2)(m+3)}{6} - \frac{(m+1)(m+2)}{4} \right)$$

Получили желаемое. ■

40 Операция циклического сдвига на линейных последовательностях. Период линейной последовательности. Свойства периода. Общий вид последовательности периода d и длины n.

Пусть дана последовательность символов $a_1a_2...a_n$. Назовём **циклическим сдвигом** операцию, при которой она переходит в последовательность $a_2...a_na_1$.

Периодом линейной последовательности называется минимальное положительное число циклических сдвигов, после применения которых последовательность перейдёт в себя.

Свойства периода:

Лемма 1: Период d слова длины n является делителем n

▲ Пусть $n = d \cdot k + r,\ r > 0$. Очевидно, что после применения n циклических сдвигов последовательность перейдет в себя.

$$\underbrace{a_1...a_n \xrightarrow{d \text{ сдвигов}} a_1...a_n \xrightarrow{d \text{ сдвигов}} ... \xrightarrow{d \text{ сдвигов}} a_1...a_n}_{d \cdot k \text{ сдвигов}} \xrightarrow{r \text{ сдвигов}} a_1...a_n$$

$r < d$, так как остаток всегда меньше делителя, и после r сдвигов последовательность перешла в себя $\Rightarrow$ r является периодом - противоречие $\Rightarrow$ $n = d \cdot k$ ■

Лемма 2: если $a_1...a_n$ - слово периода d, то оно имеет вид $\underbrace{a_1...a_da_1...a_d...a_1...a_d}_{\frac{n}{d} \text{ блоков}}$

▲ Применим d циклических сдвигов. Тогда a_{d+1} окажется на месте a_1 и так далее. Так как d - период, то последовательность перешла в себя, а значит $a_{d+1} = a_1$ и так далее. Дальше по индукции доказываем для остальных блоков. ■

41 Операция циклического сдвига на линейных последовательностях. Период линейной последовательности. Свойства периода (б/д). Явная формула для числа циклических последовательностей для частных случаев ($n = 3, 4, 5, 6$)

1. Пусть в алфавите k букв. Рассмотрим пример для $n = 4$ более подробно так как остальные рассматриваются аналогично. Так как период является делителем n, то $d = 1,2,4$

   (a) $d = 1$: это все последовательности вида $AAAA$. Очевидно, что их k штук

   (b) $d = 2$: это все последовательности вида $ABAB$, где $A \neq B$. Таким образом количество таких последовательностей равно количеству способов выбрать множество $\{A, B\}$, то есть $\frac{k(k-1)}{2}$ способов

   (c) $d = 4$: это все остальные последовательности. Посчитаем количество линейных последовательностей с таким периодом. Количество линейных последовательностей длины 4: k^4; длины 4 периода 2: $k(k-1)$; длины 4 периода 1: k. Таким образом, количество линейных последовательностей длины 4 периода 4: $k^4 - k^2 + k - k = k^4 - k^2$. Так как 4 линейным последовательностям длины 4

периода 4 соответствует только одна циклическая последовательность длины 4 периода 4, то количество таких циклических последовательностей: $\frac{r^4-r^2}{4}$

Всего циклических последовательностей длины 4: $k + \frac{k(k-1)}{2} + \frac{r^4-r^2}{4} = \frac{k^4+k^2+2k}{4}$

2. $n = 3$
   (a) $d = 1$: k штук
   (b) $d = 3$: Всего линейных: k^3; линейных периода 1: k $\Rightarrow$ циклических периода 3: $\frac{k^3-k}{3}$.

   Всего циклических последовательностей длины 3: $k + \frac{k^3-k}{3} = \frac{k^3+2k}{3}$

3. $n = 5$
   (a) $d = 1$: k штук
   (b) $d = 5$: Всего линейных: k^5; линейных периода 1: k $\Rightarrow$ циклических периода 5: $\frac{k^5-k}{5}$.

   Всего циклических последовательностей длины 5: $k + \frac{k^5-k}{5} = \frac{k^5+4k}{5}$

4. $n = 6$
   (a) $d = 1$: k штук
   (b) $d = 2$: $C_k^2 = \frac{k(k-1)}{2}$
   (c) $d = 3$: количество способов составить блок из 3-х букв: k^3, но нам нужно исключить слова периода 1, поэтому получаем $k^3 - k$. Так как нас интересуют циклические слова, то их количество равно $\frac{k^3-k}{3}$
   (d) $d = 6$: это все остальные последовательности. Всего линейных: k^6; линейных периода 1: k; линейных периода 2: $k(k-1)$; линейных периода 3: $k^3 - k$ $\Rightarrow$ циклических периода 6: $\frac{k^6-k^3-k^2+k}{6}$.

   Всего циклических последовательностей длины 6: $k + \frac{k(k-1)}{2} + \frac{k^3-k}{3} + \frac{k^6-k^3-k^2+k}{6} = \frac{k^6+k^3+2k^2+2k}{6}$

42 Применение формулы обращения Мёбиуса для подсчета числа циклических последовательностей.

Пусть V - множество всех линейных последовательностей (не циклических) длины n. $d_1, \ldots, d_s$ - делители числа n, тогда $V = V_1 \cup \cdots \cup V_s$, где V_i - множество линейных последовательностей с периодом d_i. Положим W_i - множество всех линейных последовательностей длины d_i и периода d_i. Очевидно, что $|V_i| = |W_i|$. Пусть U_i - множество циклических последовательностей, которые получаются из последовательностей W_i циклическим сдвигом. Тогда $d_i|U_i| = |W_i|$. Пусть есть функция $M(d_i) = |U_i|$ - число циклич. последовательностей, которые получаются из обычных последовательностей длины d, периода d. Рассмотрим функцию

$$r^n = \sum_{i=1}^{s} |W_i| = \sum_{i=1}^{s} d_i|U_i| = d_1 M(d_1) + \cdots + d_s M(d_s) = \sum_{d|n} dM(d)$$

Тогда возьмём $g(n) = r^n$, $f(n) = nM(n)$. Получается, что $g(n) = \sum_{d|n} f(d)$. Применима ф-ла обращ. Мёбиуса:

$$f(n) = nM(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) = \sum_{d|n} \mu(d) r^{n/d} \Rightarrow M(n) = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d}$$

M(n) - циклические последовательности, отвечающие словам длины n и периода n. Пусть $T_r(n)$ - искомая величина, количество всех циклических слов над алфавитом из r букв, имеющих длину n:

$$\begin{aligned} T_r(n) = \sum_{d\,|\,n} m(d) &= \sum_{d\,|\,n} \frac{1}{d} \Big(\sum_{d'\,|\,d} \mu(d') r^{\frac{d}{d'}} \Big) = \\ &= \sum_{\substack{d\,|\,n \\ d'\,|\,d}} \frac{r^{\frac{d}{d'}}}{\frac{d}{d'}} \frac{\mu(d')}{d'} = [k := \frac{d}{d'}] = \\ &= \sum_{d'k\,|\,n} \frac{r^k}{k} \frac{\mu(d')}{d'} = \sum_{k\,|\,n} \frac{r^k}{k} \sum_{d'\,|\,\frac{n}{k}} \frac{\mu(d')}{d'} = \\ &= \sum_{k\,|\,n} \frac{r^k}{k} \frac{\varphi(\frac{n}{k})}{\frac{n}{k}} = \frac{1}{n} \sum_{k\,|\,n} r^k \varphi(\frac{n}{k}) \end{aligned}$$

где φ — функция Эйлера.

43 Функция Мёбиуса на ч.у.м. Совпадение функции Мёбиуса $\mu(1, n)$ на ч.у.м. $\langle$N, $\vdots$ $\rangle$ и обычной функции Мёбиуса $\mu(n)$ на $\mathbb{N}$ (для всех n). Общая формула обращения Мёбиуса для частично упорядоченных множеств (б/д).

$(P, \preceq)$ - ч.у.м., причём $\forall p \in P\ \exists$ лишь конечное число $p' \in P : p' \preceq p$. Тогда **ф-ия Мёбиуса на ч.у.м.**:

$$x, y \in P : x \preceq y, \mu(x, y) = \begin{cases} 1, x = y \\ -\sum_{x \preceq z \prec y} \mu(x, z), x \neq y \end{cases}$$

"Классическая"функция Мёбиуса $\overline{\mu}(x)$ на $\mathbb{N}$:

$$\overline{\mu}(x) = \begin{cases} 1, x = 1 \\ (-1)^s, x = p_1 \dots p_s \\ 0 \end{cases}$$

Докажем, что на ч.у.м. $\langle$N, $\vdots$ $\rangle$ $\mu(x, y) = \overline{\mu}(y/x)$.

▲ Доказательство мат. индукцией по величине дроби y/x $\mu(x, y) = 1 = \overline{\mu}(x/x) = \overline{\mu}(1)$; Теперь $x \prec y$, т.е. $x|y$, но $x \neq y \Rightarrow y = x * p_1^{a_1} * \dots * p_s^{a_s}$ согласно основной теореме арифметики. Тогда $\mu(x, y) = -\sum_{x \preceq z \prec y} \mu(x, z)$, причём $z = x * p_1^{\beta_1} * \dots * p_s^{\beta_s}$, $0 \leqslant \beta_i \leqslant a_i$,

$z/x < y/x$. Тогда по предположению индукции

$$\mu(x,y) = -\sum_{x\preceq z\prec y}\mu(x,z) = -\sum_{x\preceq z\prec y}\overline{\mu}(z/x) = -\sum_{x\preceq z\prec y}\overline{\mu}(p_1^{\beta_1}*\cdots*p_s^{\beta_s}) = \begin{cases} -\sum_{i=0}^{s-1}(-1)^i C_s^i = (-1)^{s+2} = (- \\ -\sum_{i=0}^{s}(-1)^i C_s^i = \end{cases}$$

■

Обобщённая формула обращения Мёбиуса для ч.у.м.: Пусть $g(y) = \sum_{x\preceq y} f(x)$. Тогда $f(y) = \sum_{x\preceq y}\mu(x,y)g(x)$

44 Формула Мёбиуса на ч.у.м. Вывод формулы $\sum_{a\preceq z\preceq b}\mu(z,b) = \begin{cases} 1, a = b \\ 0, a < b \end{cases}$

▲ 1. $a \prec b$ - между a и b нет элементов ч.у.м. Тогда $\sum_{a\preceq z\preceq b}\mu(z,b) = \mu(a,b) + \mu(b,b) = -\sum_{a\preceq u\prec b}\mu(a,u) + 1 = -\mu(a,a) + 1 = -1 + 1 = 0$ - база индукции. Индукция по длине максимальной цепи между данными элементами ч.у.м. a и b.

$$\sum_{a\preceq z\preceq b}\mu(z,b) = \mu(b,b) + \sum_{a\preceq z\prec b}\mu(z,b) = 1 - \sum_{a\preceq z\prec b}\sum_{z\preceq u\prec b}\mu(z,u) = 1 - \sum_{a\preceq u\prec b}\sum_{a\preceq z\prec u}\mu(z,u) = 1 - 1 - \sum_{a\prec u\prec b}\sum_{a\preceq z\prec u}\mu(z$$

■

45 Формула Мёбиуса на ч.у.м. Обобщёная формула обращения Мёбиуса

Доказательство формулы Мёбиуса на ч.у.м.:

▲ $\sum_{x\preceq y}\mu(x,y)(\sum_{z\preceq x}f(z)) = \sum_{(z,x):z\preceq x\preceq y}\mu(x,y)f(z) = \sum_{z\preceq y}f(z) * (\sum_{z\preceq x\preceq y}\mu(x,y)) = f(y) * 1 + \sum_{z\prec y}f(z) * (\sum_{z\preceq x\preceq y}\mu(x,y)) = f(y) + 0 = f(y)$ ■

46 Передоказательство формулы включений и исключений при помощи формулы обращения Мёбиуса на ч.у.м. Определение множества X, порядка $\preceq$. Вычисление функции Мёбиуса на данном ч.у.м.

Рассмотрим ч.у.м.: $(2^{\{1,\dots,n\}}, \subseteq)$. Вычислим функцию Мёбиуса. Рассмотрим множества $A_1,\dots,A_n, A = A_1\cup\cdots\cup A_n$; $P = \{1,\dots,n\}$.

Разберёмся с формулой Мёбиуса на данном ч.у.м. Рассмотрим $I'\subseteq I\subseteq\{1,\dots,n\}$. Тогда $\mu(I',I) = (-1)^{|I|-|I'|}$

▲ Докажем индукцией по $|I| - |I'|$. База: I = I' (очевидна).
$|I| - |I'| = k > 0$. Тогда $\mu(I',I) = -\sum_{I'\preceq I''\prec I}\mu(I',I'')$. $|I''| - |I'| < k \Rightarrow$ по предположению индукции $\mu(I',I'') = (-1)^{|I''|-|I'|}$. Очевидно, что $|I''| \geqslant |I'|$. Тогда возникает вопрос, если мы зафиксируем $l = |I''|, l = |I'|, |I'|+1,\dots,|I'|+k-1$, сколькими способами можно будет выбрать I'' при фиксированном I'? Очевидно, $C_k^{l-|I'|} = C_k^m$, где $m = l - |I'| = 0,\dots,k-1$.

Тогда

$$\mu(I', I) = -\sum_{I' \preceq I'' \prec I} \mu(I', I'') = -\sum_{m=0}^{k-1} (-1)^m C_k^m = -(-1)^{k+1} = (-1)^k$$

■

47 Передоказательство формулы включений и исключений при помощи формулы обращения Мёбиуса на ч.у.м. Формула для вычисления функции Мёбиуса на данном ч.у.м.(б/д). Вывод формулы включений и исключений.

$f(I \subset P) :=$ количество элементов из A, которые могут не принадлежать $A_i, i \in I$, но обязательно принадлежат всем остальным. Так, $f(P) = |A|$; если же $I \neq P$: $f(I) = |\bigcap_{i \notin I} A_i|$

$g(I \subset P) :=$ количество элементов из A, которые обязаны не принадлежать $A_i, i \in I$, и обязаны принадлежать всем остальным. $f(I) = \sum_{I' \subseteq I} g(I')$; $g(\{1, \dots, n\}) = 0$

Формула обращения Мёбиуса: $f(y) = \sum_{x \preceq y} g(x) \Rightarrow g(y) = \sum_{x \preceq y} \mu(x, y) f(x)$. Применим её: $f(I) = \sum_{I' \subseteq I} g(I') \Rightarrow g(I) = \sum_{I' \subseteq I} \mu(I', I) f(I')$. Рассмотрим $I = \{1, \dots, n\}$. $0 = \sum_{I' \subseteq \{1,\dots,n\}} f(I') = |A| + \sum_{I' \subset \{1,\dots,n\}} \mu(I', \{1, \dots, n\}) |\bigcap_{i \notin I'} A_i|$.

Это значит, что

$$|A| = -\sum_{I' \subset \{1,\dots,n\}} \mu(I', \{1, \dots, n\}) |\bigcap_{i \notin I'} A_i| = -\sum_{I' \subset \{1,\dots,n\}} (-1)^{n-|I'|} |\bigcap_{i \notin I'} A_i| =$$

$$= \sum_{I' \subset \{1,\dots,n\}} (-1)^{n-|I'|+1} |\bigcap_{i \notin I'} A_i| = \sum_{I'' \neq \varnothing} (-1)^{|I''|+1} |\bigcap_{i \in I''} A_i|, I'' = \{1, \dots, n\} \setminus I'$$

54 Формальные степенные ряды, операции над ними. Определение обратного ряда. Критерий обратимости ряда (задача 13.5). Примеры нахождения обратных рядов (задача 13.6).

Формальный степенной ряд (ФСР) — формальное алгебраическое выражение вида: $F = \sum_{i=0}^{\infty} a_i x^i$, где коэффициенты a_i берутся из некоторого кольца R

Операции с ФСР:

1. сложение: $(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$
2. умножение: $(a_0, a_1, ...) * (b_0, b_1, ...) = (..., \sum_{i=0}^{\infty} a_i b_{n-i}, ...)$
3. деление: $\frac{A}{B} = C \Leftrightarrow A = B * C$
4. взятие производной: $(a_0, a_1, ...)' = (a_1, 2a_2, 3a_3, ...)$ (на лекции не было, но рассматривалось на семинаре)

Формальный степенной ряд A называется **обратимым**, если существует ряд B, такой что $A * B = (1, 0, 0, ...)$, а ряд B называется **обратным** к ряду A.

Критерий обратимости ряда: ряд $(a_0, a_1, ...)$ обратим $\Leftrightarrow$ a_0 обратим в кольце R

▲ $\Rightarrow$ Пусть ряд A обратим и B - обратный. Так как $A * B = (1, 0, ...)$, то $b_0 = \frac{1}{a_0} \Rightarrow a_0$ обратим

$\Leftarrow$ Начнем искать коэффициенты обратного ряда

$$b_0 = \frac{1}{a_0}$$

$$b_n = -\frac{1}{a_0} \sum_{i=0}^{n} a_i b_{n-i}, \forall n \geqslant 1$$

Следовательно, так как элемент a_0 обратим, такой ряд существует ■

Примеры нахождения обратных рядов

1. $\frac{1}{1-t}$

   $(1-t)(1-t)^{-1} = (1, 0, ...), (1-t) = (1, -1, 0, ...)$

   $a_0 b_0 = 1 \Rightarrow b_0 = \frac{1}{a_0} = 1$

   $a_0 b_1 + b_0 a_1 = 0 \Rightarrow b_1 = -\frac{a_1 b_0}{a_0} = 1$

   $a_0 b_k + a_1 b_{k-1} = 0 \Rightarrow b_k = -\frac{a_1 b_{k-1}}{a_0} = b_{k-1} = 1$

   Ответ: $\frac{1}{1-t} = (1, 1, 1, ...)$

2. $\frac{1}{(1-t)^2}$

   I способ: $\frac{1}{(1-t)^2} = (\frac{1}{1-t})^2$

   $(1-t)(1-t) = (1, 1, ...)(1, 1, ...) = (1, 2, 3, 4, ...)$

   II способ (через формальную производную): Заметим, что $(\frac{1}{(1-t)})' = \frac{1}{(1-t)^2} = (1, 2, 3, ...)$. В принципе, такое взятие производной согласуется с введенными операциями, так что можно написать и так. Но можем доказать это иначе.

   Продифференциируем выражение $(1-t)\frac{1}{(1-t)} = 1$

   $(1-t)'\frac{1}{(1-t)} + (\frac{1}{1-t})'(1-t) = 0$ (формула производной произведения доказывалась на семинаре просто через равенство коэффициентов)

   $\frac{1}{1-t} = (1-t)(\frac{1}{1-t})'$

   $\frac{1}{(1-t)^2} = (\frac{1}{1-t})'$

   Ответ: $\frac{1}{(1-t)^2} = (1, 2, 3, 4, ...)$

3. $\frac{1}{(1-t)^m}$

   По аналогии с I способом пункта 2:

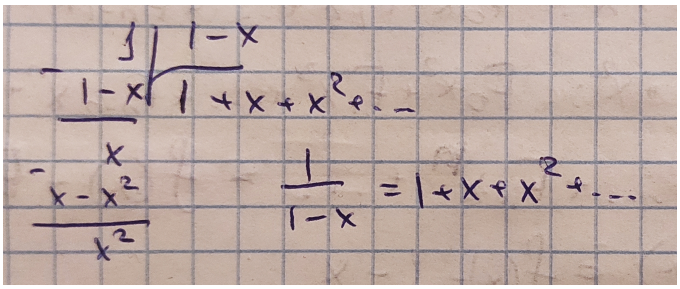
   $$\frac{1}{(1-t)^m} = \underbrace{(1 + t + t^2 + ...)...(1 + t + t^2 + ...)}_{m}$$

   Заметим, что коэффициент при x^i равен количеству неупорядоченных разбиений числа i на ровно m слагаемых. Таким образом i-ый коэффициент ряда имеет вид C^i_{m+i-1}

Ответ: $(..., C^i_{m+i-1}, ...)$

55 Формальные степенные ряды, операции над ними. Определение обратного ряда. Пример деления в столбик. Комбинаторное тождество, получаемое с использованием формального степенного ряда $(\frac{1}{1-x^2})^2$

Пример деления в столбик:



Комбинаторное тождество:

$$\left(\frac{1}{1-x^2}\right)^2 = \left(\frac{1}{1-x}\right)^2 \left(\frac{1}{1+x}\right)^2$$

$$\left(\frac{1}{1-x}\right)^2 = 1 + 2x + 3x^2 + ... + (n+1)x^n + ... \text{ (см. билет 54)}$$

$$\left(\frac{1}{1+x}\right)^2 = 1 - 2x + 3x^2 - ... + (-1)^n(n+1)x^n + ...$$

Коэффициент исходного ряда при x^n, если мы считаем через произведение, равен:

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

Посчитаем формулу исходного ряда через квадрат обратного ряда:

$$\left(\frac{1}{1-x^2}\right)^2 = 1 + 2x^2 + 3x^4 + ... + (n+1)x^{2n}$$

Таким образом, из равенства коэффициентов получаем тождество

$$\sum_{k=0}^{n}(k+1)(n+1-k)(-1)^{n-k} = \begin{cases} 0, \text{ если } n = 2l+1 \\ l+1, \text{ если } n = 2l \end{cases}$$

Строгое формальное определение формального степенного ряда через последовательности. Пример вычисления суммы и произведения рядов

Рассмотрим множество последовательностей $(a_0, a_1, ..., a_n, ...)$ (здесь a_i берутся из множества чисел $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$) и введём на них операции сложения и умножения следующим образом:

$$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...);$$

$$(a_0, a_1, ...)(b_0, b_1, ...) = (c_0, c_1, ...), \text{ где } c_n = \sum_{j=0}^{n} a_j b_{n-j}$$

Выражения $a_0 \cdot 1 + a_1 \cdot t + a_2 \cdot t^2 + ... + a_n \cdot t^n + ...$ (с введёнными операциями сложения и умножения) называют **формальными степенными рядами**. a_0 называют свободным членом ряда.

Пример вычисления суммы и произведения рядов (задача 14.3):

1. $F = 1 + t + t^2 + ..., G = 1 - t + t^2 - t^3 + ...$

$$F + G = (1, 1, ...) + (1, -1, 1, ...) = (2, 0, 2, 0, ...)$$

$$F \cdot G = (1, 1, ...)(1, -1, 1, ...) = (1, 1 - 1, 1 - 1 + 1, ..., \sum_{i=1}^{n} g_i, ...) = (1, 0, 1, 0, ...)$$

2. $F = \sum\limits_{k=0}^{\infty} \frac{1}{k!} t^k,\ G = \sum\limits_{k=0}^{\infty} \frac{(-1)^k}{k!} t^k$

$$F \cdot G:\ c_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!(n-k)!} = \sum_{k=0}^{n} \frac{(-1)^k}{n!} C_n^k = \begin{cases} \frac{1}{n!} = 1, \text{ если } n = 0 \\ 0, \text{ если } n \geqslant 1 \end{cases} \text{ (из знакопеременной суммы см}$$

$$F \cdot G = (1, 0, 0, ...) = 1$$

$$F^2:\ c_n = \sum_{k=0}^{n} \frac{1}{k!(n-k)!} = \frac{1}{n!} \sum_{k=0}^{n} C_n^k = \frac{2^n}{n!} \text{ (из комбинаторного тождества)}$$

$$F^2 = \sum_{k=0}^{\infty} \frac{1}{k!} (2t)^k$$

59 Числа Каталана (определение через пары скобочных последовательностей). Рекуррентное соотношение для чисел Каталана.

T_n - число правильных скобочных последовательностей с 2n скобками (n открывающих и n закрывающих). $T_0 = 1$; $T_n = T_{n-1}T_0 + T_{n-2}T_1 + \cdots + T_0T_{n-1}$. Докажем, что это так. Очевидно, что любая правильная скобочная последовательность начинается с открывающей скобки. Между ней и соответствующей ей закрывающей скобкой можно расположить правильную последовательность из 2k скобок (где $0 \leqslant k < n$). Отсюда и получается это рекуррентное соотношение.

60 Числа Каталана. Производящая функция для чисел Каталана.

Итак, числа Каталана имеют вид:

$$C_n = \begin{cases} 1, n = 0 \\ \sum_{k=0}^{n-1} C_k C_{n-k-1} \end{cases}$$

Ищем производящую функцию в виде: $G(z) = \sum_{n=0}^{\infty} C_n z^n$. В реккурентном соотношении домножаем C_n на z^n: $z^0 C_0 = z^0 = 1$, $z_n C_n = z^n \sum_{k=0}^{n-1} C_k C_{n-k-1}$. Выполним суммирование по всем n: $G(z) = 1 + \sum_{n=1}^{\infty} z^n \sum_{k=0}^{n-1} C_k C_{n-k-1}$. Заметим, что $G^2(z) = T_0 + (T_0T_1 + T_1T_0)z + \dots + (T_0T_n + \dots + T_nT_0)z^n = T + T_2 z + \dots + T_{n+1}z^n + \dots$. Отсюда верно: $G(z) = 1 + z * G^2(z)$. Решая квадратное уравнение и проверяя, подходит ли при z = 0 коэффициент (надо не подставлять z=0, а переходить к пределу), получаем, что нам подходит лишь один корень: $G(z) = \frac{1-\sqrt{1-4z}}{2z}$

61 Числа Каталана. Формула для коэффициентов ряда $\sqrt{1+x}$

$\sqrt{1+x} = (1+x)^{1/2} = 1 + C^1_{1/2}x + C^2_{1/2}x^2 + \dots + C^k_{1/2}x^k + \dots$; $C^k_a = \frac{a!}{k!(a-k)!} = \frac{(a)(a-1)\dots(a-k+1)}{k!}$ $C^n_{\alpha+\beta} = \sum_{j=0}^{n} C^j_\alpha C^{n-j}_\beta$. ▲ Введём понятие убывающего n-ого факториала: $a^{\underline{n}} = (a)(a-1)\dots(a-n+1)$. Тогда наше равенство перепишется в виде: $\frac{(\alpha+\beta)^{\underline{n}}}{n!} = \sum_{j=0}^{n} \frac{\alpha^{\underline{j}}}{j!} \frac{\beta^{\underline{n-j}}}{(n-j)!}$. Домножая обе части равенства на $n!$, получаем: $(\alpha+\beta)^{\underline{n}} = \sum_{j=0}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j}} C^j_n$. Последняя формула доказывается по индукции. Пусть это уже известно, тогда надо доказать, что $(\alpha+\beta)^{\underline{n+1}} = \sum_{j=0}^{n+1} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^j_{n+1}$. $(\alpha+\beta)^{\underline{n+1}} = (\alpha+\beta)^{\underline{n}} * (\alpha+\beta-n)$. Тогда изначальное равенство нам следует лишь домножить на $(\alpha+\beta-n)$: $\sum_{j=0}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j}} C^j_n (\alpha+\beta-n) = \sum_{j=0}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j}} C^j_n (\alpha-j+\beta-n+j) = \sum_{j=0}^{n} \alpha^{\underline{j+1}} \beta^{\underline{n-j}} C^j_n + \sum_{j=0}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^j_n$. Поменяем счётчики и применим тождество: $\sum_{j=-1}^{n-1} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^{j-1}_n + \sum_{j=0}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^j_n = \sum_{j=1}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^j_{n+1} + \alpha^{\underline{0}} \beta^{\underline{n+1}} C^0_n + \alpha^{\underline{n+1}} \beta^{\underline{0}} C^n_n = \sum_{j=1}^{n} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^j_{n+1} + \alpha^{\underline{0}} \beta^{\underline{n+1}} C^0_{n+1} + \alpha^{\underline{n+1}} \beta^{\underline{0}} C^{n+1}_{n+1} = \sum_{j=0}^{n+1} \alpha^{\underline{j}} \beta^{\underline{n-j+1}} C^j_{n+1}$. ■

Коэффициент при x^n по определению равен $C^n_{\frac{1}{2}} = \frac{1}{2} \cdot (-\frac{1}{2}) \cdot (-\frac{3}{2}) \cdot \dots \cdot \frac{3-2n}{2} \cdot \frac{1}{n!} =$
$= \frac{(-1)^{n-1} \cdot 1 \cdot 3 \cdot \dots \cdot (2n-3)}{2^n \cdot n!} = \frac{(-1)^{n-1} \cdot (2n-2)!}{2^{2n-1} \cdot n! \cdot (n-1)!} = \frac{(-1)^{n-1} \cdot (2n-2)! \cdot (2n-1) \cdot (2n)}{2^{2n} \cdot (n!)^2 \cdot (2n-1)} = \frac{(-1)^n \cdot (2n)!}{4^n \cdot (n!)^2 \cdot (1-2n)}$

62 Числа Каталана. Формула для коэффициентов ряда $\sqrt{1+x}$ (б/д). Вывод из неё формулы для чисел Каталана.

$\sqrt{1-4x} = \sqrt{1+(-4x)} = 1 + C^1_{1/2}(-4x) + \dots + C^n_{1/2}(-4x)^n + \dots = 1 + (-4x) + \dots + (1/2) * (-1/2) * (-3/2) * \dots * ((3-2n)/2)(-4x)^n/n! = 1 - 4x + \dots + (-1)^{n-1} * 2^{-n} * 1 * 3 * \dots * (2n-3) * 2 * 4 * \dots * (2n-2)(-4x)^n/(n! * 2 * 4 * \dots * (2n-2)) = 1 - 4x + \dots + (-1)^{n-1} * 2^{-n} * 2^{1-n}(2n-2)!(-4x)^n/(n!(n-1)!)$. Рассмотрим $1 - \sqrt{1-4x} = 4x + \dots - (-1)^n(-1)^{n-1} * 2^{1-2n} * 2^{2n}(2n-2)!x^n/(n!(n-1)!) = 4x + \dots + 2C^{n-1}_{2n-2}x^n/n$; тогда $(1 - \sqrt{1-4x})/2x = 2 + \dots + C^{n-1}_{2n-2}x^{n-1}/n$; но коэффициент при x^{n-1} - T_{n-1} - n-1-ое число Каталана. Отсюда $T_n = C^n_{2n}/(n+1)$

66 Проблема Эрдеша–Гинзбурга–Зива (формулировка для d = 2). Контрпример. История проблемы. Теорема Шевалле (формулировка).

Проблема Эрдеша–Гинзбурга–Зива (d = 2):

$$(a_1, b_1),\ (a_2, b_2), ..., (a_m, b_m) \in \mathbb{Z}^2$$
$$\exists I \subset \{1, 2, ..., m\}, |I| = n : \sum_{i \in I} a_i \equiv 0(m); \sum_{i \in I} b_i \equiv 0(m)$$

Необходимо найти минимальное m, при котором условие выполняется, как функцию от n. Простая оценка:

$$m \geqslant 4n - 3$$

Контрпример для $m = 4n - 4$: (0, 0) $n - 1$ раз, (0, 1) $n - 1$ раз, (1, 0) $n - 1$ раз, (1, 1) $n - 1$ раз

История проблемы:

1. 1983 - Гипотеза Кемница: $m = 4n - 3$
2. 1990 - Алон и Дубинер доказали, что $m \leqslant 6n - 5,\ n \geqslant n_0$
3. 2000 - Роньяи доказал, что $m \leqslant 4n - 2$
4. 2005 - Райер доказал, что $m = 4n - 3$

Теорема Шевалле: если $deg\ F < n$, то число решений уравнения $F(x_1, ..., x_n) \equiv 0(p)$: $N_p \equiv 0(p)$

67 Теорема Шевалле. Сведение к доказательству сравнения суммы.

▲ Заметим, что $N_p \equiv \sum_{x_1=1}^{p} ... \sum_{x_n=1}^{p} (1 - F^{p-1}(x_1, ..., x_n))\ (p)$, так как мы складываем столько единиц, сколько есть наборов, где $F \equiv 0(p)$, а остальные обнуляются по малой теореме Ферма.

Разобьём на 2 суммы. Очевидно, что сумма с 1 делится на p, поэтому нам остается только доказать, что $\sum\limits_{x_1=1}^{p} ... \sum\limits_{x_n=1}^{p} (F^{p-1}(x_1, ..., x_n) \equiv 0(p)$

Многочлен F^{p-1} можно представить как сумму мономов вида $x_1^{\alpha_1}...x_n^{\alpha_n}$, где $\alpha_1 + ... + \alpha_n < n(p-1)$ (так как степень многочлена могла увеличиться не более чем в $p - 1$ раз). Тогда, если мы докажем, что любая сумма вида $\sum\limits_{x_1=1}^{p} ... \sum\limits_{x_n=1}^{p} x_1^{\alpha_1}...x_n^{\alpha_n} \equiv 0(p)$, то всё доказано. ■

68 Теорема Шевалле (формулировка). Доказательство сравнения с суммой. Теорема Варнинга (формулировка).

▲ $\sum\limits_{x_1=1}^{p} ... \sum\limits_{x_n=1}^{p} x_1^{\alpha_1}...x_n^{\alpha_n} = \left(\sum\limits_{x_1=1}^{p} x_1^{\alpha_1}\right)...\left(\sum\limits_{x_n=1}^{p} x_n^{\alpha_n}\right)$ (очевидно). Тогда нам достаточно показать, что хотя бы одна из этих скобок сравнима с 0 по модулю p. Если $\exists i: \ \alpha_i = 0$, то $\sum\limits_{x_i=1}^{p} x_i^{\alpha_i} \equiv 0(p)$. При $p = 2$ такое α_i точно найдется по принципу Дирихле ($\alpha_1 + ... + \alpha_n < n$)

Пусть $p \geqslant 3$ и $\forall i \ \alpha_i \geqslant 1$. Тогда $\exists i: \ 1 \leqslant \alpha_i \leqslant p-2$ (если такого нет, то все $\alpha_i \geqslant p-1$, и $\alpha_1 + ... + \alpha_n \geqslant n(p-1)$ - противоречие).

Утверждение: $\exists a: \ (a,p) = 1$ и $a^{\alpha_i} \not\equiv 1(p)$ $(1 \leqslant \alpha_i \leqslant p-2)$ (будет доказано в весеннем семестре)

Обозначим $S = \sum\limits_{x_i=1}^{p} x_i^{\alpha_i}$. Тогда по утверждению существует такое a, что

$$a^{\alpha_i} S = \sum_{x_i=1}^{p} (ax_i)^{\alpha_i}$$

Так как a и p взаимно просты ax_i это просто какая-то перестановка $\mathbb{Z}_p$. Следовательно

$$a^{\alpha_i} S \equiv S(p)$$

$$(a^{\alpha_i} - 1)S \equiv 0(p)$$

В силу нашего выбора a первая скобка не сравнима с 0 по модулю p. Тогда $S \equiv 0(p)$ ■

Теорема Варнинга: Если $degF < n$ и $F(0,...,0) \equiv 0(p)$, то $\exists (x_1,...,x_n) \neq (0,...,0)$: $F(x_1,...,x_n) \equiv 0(p)$

69 Проблема Эрдеша–Гинзбурга–Зива при d = 2 и n = p: нижняя и верхние оценки (формулировка). Теорема Варнинга (формулировка). Доказательство основной леммы.

Обобщенная теорема Варнинга: Пусть $F_1, ..., F_k$ - многочлены, причём $degF_1 + ... + degF_k < n$. Рассмотрим систему:

$$\begin{cases} F_1(x_1,...,x_n) \equiv 0(p) \\ \qquad ... \\ F_k(x_1,...,x_n) \equiv 0(p) \end{cases}$$

Если ей удовлетворяет набор (0, ..., 0), то существует набор $(x_1,...,x_n) \not\equiv (0,...,0)$, удовлетворяющий системе.

Основная лемма: Пусть $(a_1,b_1),...,(a_{3p},b_{3p})$ - наборы, такие что $\sum\limits_{i=1}^{3p} a_i \equiv \sum\limits_{i=1}^{3p} b_i \equiv 0(p)$. Тогда $\exists I \subset \{1,...,3p\}: \ |I| = p, \ \sum\limits_{i\in I}^{p} a_i \equiv \sum\limits_{i\in I}^{p} b_i \equiv 0(p)$

▲ Рассмотрим некоторый набор переменных $x_1, ..., x_{3p-1}$ и систему

$$\begin{cases} F_1(x_1, ..., x_{3p-1}) = \sum\limits_{i=1}^{3p-1} a_i x_i^{p-1} \equiv 0(p) \\ F_2(x_1, ..., x_{3p-1}) = \sum\limits_{i=1}^{3p-1} a_i x_i^{p-1} \equiv 0(p) \\ F_3(x_1, ..., x_{3p-1}) = \sum\limits_{i=1}^{3p-1} x_i^{p-1} \equiv 0(p) \end{cases}$$

Очевидно, что $degF_1 + degF_2 + degF_3 = 3p - 3 < 3p - 1$, набор (0, ..., 0) удовлетворяет системе $\Rightarrow$ по обобщённой теореме Варнинга существует набор $(x_1, ..., x_{3p-1}) \not\equiv (0, ..., 0)$, удовлетворяющий системе.

Рассмотрим $J \subset \{1, ..., 3p-1\} : \ \forall j \in J \ x_j \not\equiv 0$. Тогда

$$F_1(x_1, ..., x_{3p-1}) = \sum_{i=1}^{3p-1} a_i x_i^{p-1} \equiv \sum_{j \in J} a_j \equiv 0(p) \text{ (по малой теореме Ферма)}$$

$$F_2(x_1, ..., x_{3p-1}) = \sum_{i=1}^{3p-1} b_i x_i^{p-1} \equiv \sum_{j \in J} b_j \equiv 0(p)$$

$$F_3(x_1, ..., x_{3p-1}) = \sum_{i=1}^{3p-1} a_i x_i^{p-1} \equiv \sum_{j \in J} 1 = |J| \equiv 0(p)$$

Из последнего равенства следует, что

1. либо $|J| = p$, тогда всё доказано
2. либо $|J| = 2p$, тогда рассмотрим множество $I = \{1, ..., 3p\} \setminus J$. Получается, что $|I| = p$, $\sum\limits_{i \in I} a_i = \sum\limits_{i=1}^{3p} a_i - \sum\limits_{j \in J} a_j \equiv 0(p)$, так как каждое из слагаемых сравнимо с 0 по модулю p (аналогично для b) ■

70 Проблема Эрдеша–Гинзбурга–Зива при d = 2 и n = p: нижняя и верхние оценки (формулировка). Основная лемма (б/д), вывод из неё теоремы Роньяи.

Теорема Роньяи для n=p: $m \leqslant 4p - 2$

▲ Зафиксируем $m = 4p - 2$. Пусть нельзя выбрать набор, удовлетворяющий проблеме. Тогда $\forall I : \ |I| = p$ либо $\sum\limits_{i \in I} a_i \not\equiv 0(p)$, либо $\sum\limits_{i \in I} b_i \not\equiv 0(p)$. Тогда по основной лемме это же условие выполнено и для $I : \ |I| = 3p$.

Рассмотрим функцию

$$F(x_1, ..., x_m) = \left(\left(\sum_{i=1}^{m} a_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^{m} b_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^{m} x_i \right)^{p-1} - 1 \right) (\sigma_p(x_1, ..., x_m) - 2)$$

где $\sigma_p(x_1, ..., x_m) = \sum\limits_{I \subset \{1..m\}, |I|=p} (\prod\limits_{i \in I} x_i)$ - симметрический многочлен (сумма всех произведений по p множителей)

Подставим вместо $x_1, ..., x_n$ нули и единицы

1. единиц среди аргументов p или $3p$ штук. Тогда в силу предположения о том, что теорема неверна одна из первых двух скобок $\equiv 0(p)$ по малой теореме Ферма

2. число единиц не делится на p, то зануляется 3 скобка по малой теореме Ферма

3. единиц $2p$ штук: $\sigma_p(x_1, ..., x_n) = C_{2p}^p \equiv 2(p)$ (доказано в билете 64) $\Rightarrow$ последняя скобка $\equiv 0(p)$

4. все переменные равны нулю $\Rightarrow F = 2$

Раскроем скобки. Заменим слагаемое $Cx_1^{\alpha_1}...x_n^{\alpha_n}$ на $Cx_1...x_n$ и получим некоторую функцию F'. Тогда значение функции не изменится (так как $0^k = 0$ и $1^k = 1$).

Утверждение: $F'(x_1, ..., x_m) = 2(1 - x_1)...(1 - x_m)$

▲ Докажем, что мономы $x_{i_1}...x_{i_k}$ образуют базис в пространстве функций $\{0, 1\}^m \to \mathbb{Z}_p$. Их линейная независимость очевидна. Также очевидно, что любую функцию можно выразить в базисе характеристических функций:

$$\chi_u(v) = \begin{cases} 1, u = v \\ 0, u \neq v \end{cases} = \prod_{i:u_i=1} v_i \prod_{j:u_j=0} (1 - v_j)$$

Если раскрыть правую часть, то получим линейную комбинацию мономов $\Rightarrow$ любую функцию можно выразить через эти мономы $\Rightarrow$ они образуют базис. Так как разложение по базису единственное, то функция F' представляется именно так ■

$$degF' = m = 4p - 2 \leqslant degF \text{ (т.к. степень не могла увеличиться)}$$

$$degF = (p - 1) + (p - 1) + (p - 1) + p = 4p - 3 \text{ (сложили степени скобок)}$$

Получаем, что $4p - 2 \leqslant 4p - 3$ - противоречие $\Rightarrow$ теорема верна ■