

★ **Перестановкой** множества A называется произвольный **линейный порядок** на A

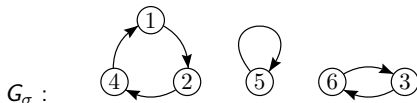
Пример: пусть $A = \mathbb{N}$

- можно упорядочить по возрастанию (\leq)
 - можно упорядочить по убыванию (\geq)
 - можно упорядочить сначала все нечетные по \leq , а потом четные по \geq
 - можно по сумме показателей в разложении на простые множители, а при одинаковой сумме — по \leq
- Если A — **конечное**, перестановку можно определить как **биекцию** A на себя:
- ★ $A = \{a_1, \dots, a_n\} \Rightarrow$ нумерация элементов задает на A линейный порядок
 - перестановка — это линейный порядок $(a_{i_1}, \dots, a_{i_n})$
- \Rightarrow определяет биекцию $f: f(a_k) = a_{i_k}$ для всех k
- обратно, любая биекция $f: A \rightarrow A$ задает перестановку $(f(a_1), \dots, f(a_n))$
- ★ Для бесконечных множеств биекции задают не все перестановки!
- ! какие из приведенных выше перестановок на \mathbb{N} соответствуют биекциям?

★ Перестановке конечного множества можно сопоставить ее граф

- см. фрагмент 1-3 про орграфы функций
- ★ орграф, в котором **все** степени вершин равны 1, называется **линейным**
- ★ **графы перестановок** множества A = **линейные орграфы** с множеством вершин A

Пример: $A = [1..6]$; $\sigma = (2, 4, 6, 1, 5, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} = (4\ 1\ 2)(5)(6\ 3)$



★ $\sigma = (4\ 1\ 2)(5)(6\ 3)$ — **циклическая запись** перестановки

- перечисляются циклы орграфа как последовательности вершин

★ **Перестановкой** множества A называется произвольный **линейный порядок** на A

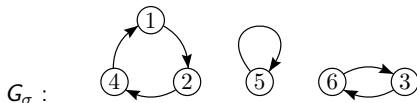
Пример: пусть $A = \mathbb{N}$

- можно упорядочить по возрастанию (\leq)
 - можно упорядочить по убыванию (\geq)
 - можно упорядочить сначала все нечетные по \leq , а потом четные по \geq
 - можно по сумме показателей в разложении на простые множители, а при одинаковой сумме — по \leq
- Если A — **конечное**, перестановку можно определить как **биекцию** A на себя:
- ★ $A = \{a_1, \dots, a_n\} \Rightarrow$ нумерация элементов задает на A линейный порядок
 - перестановка — это линейный порядок $(a_{i_1}, \dots, a_{i_n})$
- \Rightarrow определяет биекцию $f: f(a_k) = a_{i_k}$ для всех k
- обратно, любая биекция $f: A \rightarrow A$ задает перестановку $(f(a_1), \dots, f(a_n))$
- ★ Для бесконечных множеств биекции задают не все перестановки!
- ! какие из приведенных выше перестановок на \mathbb{N} соответствуют биекциям?

★ Перестановке конечного множества можно сопоставить ее граф

- см. фрагмент 1-3 про орграфы функций
- ★ орграф, в котором **все** степени вершин равны 1, называется **линейным**
- ★ **графы перестановок** множества A = **линейные орграфы** с множеством вершин A

Пример: $A = [1..6]$; $\sigma = (2, 4, 6, 1, 5, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} = (4\ 1\ 2)(5)(6\ 3)$



★ $\sigma = (4\ 1\ 2)(5)(6\ 3)$ — **циклическая запись** перестановки

- перечисляются циклы орграфа как последовательности вершин

Числа Стирлинга первого рода

- ★ В S_n имеется $(n-1)!$ перестановок с одним циклом (длины n)
 - каноническая запись такой перестановки: $(n i_1 \dots i_{n-1})$, где (i_1, \dots, i_{n-1}) — линейная запись произвольной перестановки из S_{n-1}
- Сколько в S_n существует перестановок с k циклами?
 - это число обозначают $[n_k]$ и называют (беззнаковым) числом Стирлинга 1 рода
 - мы доказали, что $[n_1] = (n-1)!$; очевидно, $[n_n] = 1$; чему равно $[n_{n-1}]$?

Теорема

$[n+1_k] = n \cdot [n_k] + [n_{k-1}]$, с начальными условиями $[n_n] = 1$ и $[n_0] = 0$ ($n > 0$).

Доказательство:

- Для перестановок из S_{n+1} с k циклами есть 2 варианта:
 - если элемент $n+1$ образует отдельный цикл, то остальные n элементов образуют $k-1$ циклов
 - ⇒ таких перестановок $[n_{k-1}]$
 - если элемент $n+1$ входит в неодноэлементный цикл, удалим этот элемент
 - заменив ребра $(i, n+1)$ и $(n+1, j)$ ребром (i, j)
 - ⇒ получится перестановка из S_n с k циклами
 - в такую перестановку можно вставить $n+1$ в середину любого из n ребер
 - ⇒ всего получим $n \cdot [n_k]$ перестановок
- Поскольку варианты исключают друг друга, получаем $[n+1_k] = n \cdot [n_k] + [n_{k-1}]$ □

Числа Стирлинга первого рода возникают не только при подсчете перестановок:

- **Восходящий факториал** — это функция $x^{\bar{n}} = x(x+1) \cdots (x+n-1)$

Теорема

$$x^{\bar{n}} = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} x^k.$$

★ Формула очень похожа на $(x+1)^n = \sum_{k=0}^n \binom{n}{k} x^k$

Доказательство теоремы:

- пусть коэффициент при x^k в разложении $x^{\bar{n}}$ равен $f(n, k)$
 - докажем, что $f(n, k)$ удовлетворяет рекуррентному соотношению для $\begin{bmatrix} n \\ k \end{bmatrix}$
 - распишем $x^{\overline{n+1}} = x(x+1) \cdots (x+n-1)(x+n) = n \cdot x^{\bar{n}} + x \cdot x^{\bar{n}}$
 - коэффициент при x^k в левой части равен $f(n+1, k)$, а в правой $n \cdot f(n, k) + f(n, k-1)$, и они равны
- $\Rightarrow f(n, k)$ задается тем же рекуррентным соотношением, что и $\begin{bmatrix} n \\ k \end{bmatrix}$
- $f(n, 0) = 0$ при $n > 0$, так как есть множитель x
 - $f(n, n) = 1$, так как x^n получается перемножением n x из всех скобок
- \Rightarrow начальные условия тоже выполнены $\Rightarrow f(n, k) = \begin{bmatrix} n \\ k \end{bmatrix}$ □

Перестановки с двумя циклами. Гармонические числа

Пример: выведем формулу для $\left[\begin{smallmatrix} n \\ 2 \end{smallmatrix} \right]$ — числа перестановок с двумя циклами

$$\begin{aligned} \left[\begin{smallmatrix} n \\ 2 \end{smallmatrix} \right] &= (n-1) \left[\begin{smallmatrix} n-1 \\ 2 \end{smallmatrix} \right] + \left[\begin{smallmatrix} n-1 \\ 1 \end{smallmatrix} \right] = (n-1)(n-2) \left[\begin{smallmatrix} n-2 \\ 2 \end{smallmatrix} \right] + (n-1) \left[\begin{smallmatrix} n-2 \\ 1 \end{smallmatrix} \right] + \left[\begin{smallmatrix} n-1 \\ 1 \end{smallmatrix} \right] = \\ &\dots = (n-1) \dots 2 \left[\begin{smallmatrix} 2 \\ 2 \end{smallmatrix} \right] + (n-1) \dots 3 \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right] + \dots + (n-1) \left[\begin{smallmatrix} n-2 \\ 1 \end{smallmatrix} \right] + \left[\begin{smallmatrix} n-1 \\ 1 \end{smallmatrix} \right] = \\ (n-1)! + \frac{(n-1)!}{2} + \dots + \frac{(n-1)!}{n-2} + \frac{(n-1)!}{n-1} &= \left(1 + \frac{1}{2} + \dots + \frac{1}{n-1} \right) (n-1)! = H_{n-1} (n-1)! \end{aligned}$$

• $H_n = 1 + \frac{1}{2} + \dots + \frac{1}{n}$ называется n -ым гармоническим числом

• $H_n \approx \ln n$, так как $\sum_{x=1}^n \frac{1}{x} \approx \int_1^n \frac{dx}{x}$

! Используя для оценки интегралов метод прямоугольников, докажите, что $\ln(n+1) < H_n < \ln n + 1$

! Попробуйте уточнить оценку, используя метод трапеций

★ Точная оценка: $H_n = \ln n + \gamma + o(1)$, где $\gamma = 0.577 \dots$ — константа Эйлера

★ Перестановок с **двумя циклами** примерно в $\ln n$ раз больше, чем с **одним**

- Множество S_n с операцией композиции образует **группу** — **симметрическую группу n -элементного множества**
 - Композицию (произведение) перестановок удобно вычислять в **линейной записи**: если π и σ заданы массивами длины n , то $(\pi \circ \sigma)(i) = \sigma[\pi[i]]$
- S_n **некоммутативна** при $n \geq 3$:
 - $(2, 1, 3) \circ (3, 2, 1) = (2, 3, 1)$, $(3, 2, 1) \circ (2, 1, 3) = (3, 1, 2)$
- Для любого элемента a конечной группы G существует k такое, что $a^k = 1$
 - найдутся $i < j$ такие, что $a^i = a^j$
 $\Rightarrow a^{-i}$ — обратный к $a^j \Rightarrow a^{j-i} = 1$
- Наименьшее k со свойством $a^k = 1$ называется **порядком** элемента a
- Порядок перестановки $\sigma \in S_n$ равен НОКу длин всех циклов в σ
! проверьте это
- Наибольший порядок перестановки в S_n называется **функцией Ландау** и обозначается $g(n)$
 - Ландау здесь — не советский физик, а немецкий математик начала XX века
- Поскольку длины циклов перестановки $\sigma \in S_n$ образуют разбиение числа n , $g(n)$ альтернативно определяют как максимальный НОК разбиения числа n
- Ландау доказал, что $g(n) \sim e^{\sqrt{n \ln n}}$
Пример: $g(9) = \text{НОК}(4, 5) = 20$, $g(10) = \text{НОК}(2, 3, 5) = 30$

Симметрические группы S_n — это «всеобъемлющие» конечные группы:

Теорема Кэли

Любая n -элементная группа изоморфна некоторой подгруппе группы S_n .

Доказательство:

- Пусть (G, \cdot) — произвольная группа, $|G| = n$
- Заменим S_n на **изоморфную** группу S_G перестановок элементов множества G
- $ba = ca$ в группе влечет $b = c$
 - \Rightarrow функция $f_a: f_a(x) = xa$ является **перестановкой множества G** , т.е. $f_a \in S_G$
- Пусть $\phi: G \rightarrow S_G$ задана правилом $\phi(a) = f_a$
 - $f_a(x) = f_b(x) \Rightarrow xa = xb \Rightarrow a = b$
 - $\Rightarrow \phi$ — инъекция, а значит, биекция G на $\phi(G)$
 - $(f_a \circ f_b)(x) = f_b(xa) = xab = f_{ab}(x)$ для любых $a, b, x \in G$
 - $\Rightarrow \phi(a) \circ \phi(b) = \phi(ab) \Rightarrow \phi$ сохраняет умножение
 - $f_1 = \Delta$ (тождественная перестановка на G) $\Rightarrow \phi$ сохраняет нейтральный элемент
 - $(f_{a^{-1}} \circ f_a)(x) = xa^{-1}a = x = f_1(x)$ для любых $a, x \in G \Rightarrow \phi$ сохраняет обратные элементы
- ★ Итак, ϕ — биекция G на $\phi(G)$, сохраняющая все операции группы; попутно мы выяснили, что $\phi(G)$ замкнуто относительно операций группы S_G , т.е. является подгруппой $\Rightarrow \phi$ — изоморфизм

Инверсии и порождающие множества

- Пусть $\sigma = (i_1, \dots, i_n)$ — перестановка в линейной записи
- Пара индексов $k < \ell$ называется **инверсией** (в σ), если $i_k > i_\ell$
 - **число инверсий** $\text{inv}(\sigma)$ — важная характеристика перестановки
 - особенно важна четность $\text{inv}(\sigma)$, называемая **четностью перестановки**
 - ★ вспомните формулу определителя: $|A| = \sum_{\sigma \in S_n} (-1)^{\text{inv}(\sigma)} a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$
- Перестановка, меняющая местами **два элемента**, называется **транспозицией**
 - например, $(1, 2, \mathbf{5}, 4, \mathbf{3}, 6)$
 - транспозиция имеет один цикл длины 2 и $n - 2$ **неподвижных точки**
 - транспозиция — **нечетная** перестановка (доказывалось в алгебре)
- Группа G **порождается** своим подмножеством X , если любой элемент из G можно получить из элементов множества X применением операций группы
 - если G конечна, достаточно бинарной операции: $x^k = 1 \Rightarrow x^{-1} = x^{k-1}$

Теорема

Группа S_n порождается множеством всех транспозиций.

Доказательство:

- возьмем произвольную $\sigma = (i_1, \dots, i_n)$ и применим **сортировку пузырьком**
 - шаг сортировки переставляет два элемента (= умножение на транспозицию)
 - результатом сортировки является $\Delta = (1, \dots, n)$
- $\Rightarrow \Delta = \sigma \circ \tau_1 \circ \cdots \circ \tau_k$, где все τ — транспозиции
- $\tau_i^2 = \Delta \Rightarrow \tau_i^{-1} = \tau_i \Rightarrow \sigma = \tau_k \circ \cdots \circ \tau_1$

- Перестановкой из S_n можно **подействовать** на любое n -элементное множество A , если элементы A естественным образом **линейно упорядочены**
- Например, можно действовать перестановкой
 - на слово (через номера позиций)
 - на граф (через номера вершин)
 - на матрицу (через номера строк или столбцов)
- Для последовательности объектов (y_1, \dots, y_n) **результат** $\sigma(y_1, \dots, y_n)$ **действия перестановки** σ есть последовательность $(y_{\sigma^{-1}(1)}, \dots, y_{\sigma^{-1}(n)})$
 - определение гласит, что элемент с позиции i перемещается на позицию $\sigma(i)$
 \Rightarrow элемент с позиции $\sigma^{-1}(1)$ перемещается на позицию $\sigma(\sigma^{-1}(1)) = 1$ и т.д.
- **Пример:** если $\sigma = (7, 6, 9, 3, 4, 5, 2, 1, 8)$, то $\sigma(\text{ПОДСТРОКА}) = \text{КОСТРОПАД}$
 - тот же результат получится при $\sigma = (7, 2, 9, 3, 4, 5, 6, 1, 8)$
 - ★ любая перестановка превращает слово в его **анаграмму** (и обратно: любая анаграмма слова получается из него действием некоторой перестановки)
- Перестановка $\theta \in S_n$ называется **сортирующей** для слова w длины n над упорядоченным алфавитом Σ , если $\theta(w)[i] \leq \theta(w)[j]$ для любых $i < j$
 - если $\theta = (6, 4, 2, 8, 9, 7, 5, 3, 1)$, то $\theta(\text{ПОДСТРОКА}) = \text{АДКООПРСТ} \Rightarrow \theta$ — сортирующая
 - ★ если буквы в w повторяются, то сортирующая перестановка не единственна
- $\theta \in S_n$ — **стабильно сортирующая** для w , если θ не меняет порядок **равных букв**
 - для любых $i < j$ таких, что $w[i] = w[j]$, выполнено $\theta(w)[i] < \theta(w)[j]$
 - ★ стабильно сортирующая для w перестановка единственна
 - ★ $\theta = (6, 4, 2, 8, 9, 7, 5, 3, 1)$ — стабильно сортирующая для $w = \text{ПОДСТРОКА}$

Преобразование Бэрроуза–Уилера

Самое известное в современной Computer Science действие перестановки называется **преобразованием Бэрроуза–Уилера (BWT)**

- Взять слово w над упорядоченным алфавитом и выписать все $|w|$ его **циклических сдвигов** в столбик, получив квадратную матрицу
- Отсортировать строки матрицы **лексикографически**, получая матрицу $T(w)$
- Вернуть последний столбец матрицы ($\text{bwt}(w)$)
 - Каждая буква из w является последней ровно для одного циклического сдвига
 - $\Rightarrow \text{bwt}(w)$ является **анаграммой** w
 - $\Rightarrow \text{bwt}$ как функция является **действием некоторой перестановки** (зависящей от w)

Пусть $K < O < P$. Тогда

$$T(\text{ОКОРОК}) = \begin{array}{cccccc} \text{К} & \text{О} & \text{К} & \text{О} & \text{Р} & \text{О} \\ \text{К} & \text{О} & \text{Р} & \text{О} & \text{К} & \text{О} \\ \text{О} & \text{К} & \text{О} & \text{К} & \text{О} & \text{Р} \\ \text{О} & \text{К} & \text{О} & \text{Р} & \text{О} & \text{К} \\ \hline \text{О} & \text{Р} & \text{О} & \text{К} & \text{О} & \text{К} \\ \text{Р} & \text{О} & \text{К} & \text{О} & \text{К} & \text{О} \end{array} \quad \text{bwt}(\text{ОКОРОК}) = \text{ООРККО}$$

- BWT — не биекция, например, $\text{bwt}(\text{ОКОРОК}) = \text{bwt}(\text{РОКОКО})$
- Зная $\text{bwt}(w)$ и номер строки в $T(w)$, можно восстановить эту строку за линейное время, **используя стабильную сортировку для $\text{bwt}(w)$**
- Это обусловило широкое применение BWT для сжатия и индексирования данных