★ Перестановкой множества A называется произвольный линейный порядок на A

Пример: пусть $A = \mathbb{N}$

- можно упорядочить по возрастанию ($\leqslant$)
- можно упорядочить по убыванию ($\geqslant$)
- можно упорядочить сначала все нечетные по $\leqslant$, а потом четные по $\geqslant$
- можно по сумме показателей в разложении на простые множители, а при одинаковой сумме — по $\leqslant$

- Если A — конечное, перестановку можно определить как биекцию A на себя:
  - ⋆ $A = \{a_1, \ldots, a_n\} \Rightarrow$ нумерация элементов задает на A линейный порядок
  - перестановка — это линейный порядок $(a_{i_1}, \ldots, a_{i_n})$
  - $\Rightarrow$ определяет биекцию f: $f(a_k) = a_{i_k}$ для всех k
  - обратно, любая биекция $f : A \to A$ задает перестановку $(f(a_1), \ldots, f(a_n))$

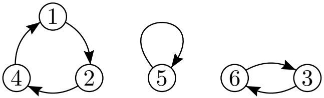
★ Для бесконечных множеств биекции задают не все перестановки!

! 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

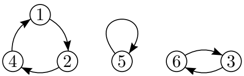
Пример: $A = [1..6]$; $\sigma = (2, 4, 6, 1, 5, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} = (4\,1\,2)(5)(6\,3)$

G_σ :



- ⋆ $\sigma = (4\,1\,2)(5)(6\,3)$ — циклическая запись перестановки
  - перечисляются циклы орграфа как последовательности вершин

Каноническая запись

G_σ: 

- ⋆ далее всюду A — конечно; для удобства полагаем $A = [1..n]$
- ⋆ Множество всех перестановок на A обозначается через S_n

- ⋆ Цикл, в котором находится элемент i, состоит из элементов $i, \sigma(i), \ldots, \sigma^{\ell-1}(i)$, где ℓ — длина цикла
  - здесь $\sigma^2 = \sigma \circ \sigma$, $\sigma^3 = \sigma \circ \sigma \circ \sigma$, ...
  - т.е. $\sigma^2(i) = \sigma(\sigma(i))$, $\sigma^3 = \sigma(\sigma^2(i))$, ...
- Этот цикл называется орбитой элемента i
  - ⋆ орбиты различных элементов либо не пересекаются, либо совпадают
- ⋆ Циклическая запись перестановки неоднозначна:
  - выбор «первого» элемента в каждом цикле
  - перестановка циклов в записи
  - ⋆ часто используется сокращенная запись: выбрасываются циклы длины 1
- ⋆ Каноническая запись перестановки:
  - каждый цикл записывается, начиная с наибольшего элемента
  - циклы выписываются по возрастанию первых элементов
  - ⋆ сокращения не используются

Пример:

- $\sigma = (4\,1\,2)(5)(6\,3)$ — каноническая запись
- $\sigma = (3\,6)(2\,4\,1)$ — пример неканонической записи

- Пусть ψ — функция стирания скобок в канонической записи:
  - $\sigma = (i_1 \cdots i_{\ell_1})(i_{\ell_1+1} \cdots i_{\ell_2}) \cdots (i_{\ell_k+1} \cdots i_n) \Rightarrow \psi(\sigma) = (i_1, \ldots, i_n)$
    Пример: $\sigma = (4\,1\,2)(5)(6\,3) \Rightarrow \psi(\sigma) = (4, 1, 2, 5, 6, 3) = (6\,3\,2\,1\,4\,5)$

Теорема

Функция стирания скобок — биекция S_n на себя.

Доказательство:
- пусть $\pi = (i_1, \ldots, i_n) \in S_n$
- расставим в линейной записи π скобки, чтобы получить каноническую запись (некоторой другой перестановки):
- i_1 принадлежит первому циклу, больше всех элементов в этом цикле и меньше первого элемента следующего цикла

$\Rightarrow$ первый элемент i' второго цикла однозначно определяется как самый левый элемент в линейной записи, больший i_1 (а значит, всех предыдущих элементов)
- аналогично, первый элемент i'' третьего цикла однозначно определяется как самый левый элемент в линейной записи, больший i' (и всех предыдущих)
- ...
- каноническая запись восстанавливается однозначно □
  Пример: $\pi = (4, 1, 2, 5, 6, 3) \Rightarrow \psi^{-1}(\pi) = (4\,1\,2)(5)(6\,3)$

- Элемент, больший всех предыдущих в линейной записи перестановки, называется префикс-максимумом

★ Следствие теоремы: в S_n перестановок с k циклами столько же, сколько перестановок с k префикс-максимумами

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 $\left[{n \atop k}\right]$ и называют (беззнаковым) числом Стирлинга 1 рода
  - мы доказали, что $\left[{n \atop 1}\right] = (n-1)!$; очевидно, $\left[{n \atop n}\right] = 1$; чему равно $\left[{n \atop n-1}\right]$?

Теорема

$\left[{n+1 \atop k}\right] = n \cdot \left[{n \atop k}\right] + \left[{n \atop k-1}\right]$, с начальными условиями $\left[{n \atop n}\right] = 1$ и $\left[{n \atop 0}\right] = 0$ $(n > 0)$.

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

  $\Rightarrow$ таких перестановок $\left[{n \atop k-1}\right]$
  - если элемент $n+1$ входит в неодноэлементный цикл, удалим этот элемент
    - заменив ребра $(i, n+1)$ и $(n+1, j)$ ребром (i, j)

  $\Rightarrow$ получится перестановка из S_n с k циклами
  - в такую перестановку можно вставить $n+1$ в середину любого из n ребер

  $\Rightarrow$ всего получим $n \cdot \left[{n \atop k}\right]$ перестановок
- Поскольку варианты исключают друг друга, получаем $\left[{n+1 \atop k}\right] = n \cdot \left[{n \atop k}\right] + \left[{n \atop k-1}\right]$ □

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

$x^{\bar{n}} = \sum_{k=0}^{n} \left[{n \atop k}\right] x^k$.

★ 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 $\left[{n \atop k}\right]$
- 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 $\left[{n \atop k}\right]$

- $f(n,0) = 0$ при $n > 0$, так как есть множитель x
- $f(n,n) = 1$, так как x^n получается перемножением иксов из всех скобок

$\Rightarrow$ начальные условия тоже выполнены $\Rightarrow f(n,k) = \left[{n \atop k}\right]$ □

Перестановки с двумя циклами. Гармонические числа

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

$$\left[{n \atop 2}\right] = (n-1)\left[{n-1 \atop 2}\right] + \left[{n-1 \atop 1}\right] = (n-1)(n-2)\left[{n-2 \atop 2}\right] + (n-1)\left[{n-2 \atop 1}\right] + \left[{n-1 \atop 1}\right] =$$

$$\ldots = (n-1)\cdot\ldots\cdot 2\left[{2 \atop 2}\right] + (n-1)\cdot\ldots\cdot 3\left[{2 \atop 1}\right] + \cdots + (n-1)\left[{n-2 \atop 1}\right] + \left[{n-1 \atop 1}\right] =$$

$$(n-1)! + \frac{(n-1)!}{2} + \cdots + \frac{(n-1)!}{n-2} + \frac{(n-1)!}{n-1} = \left(1 + \frac{1}{2} + \ldots + \frac{1}{n-1}\right)(n-1)! = H_{n-1}(n-1)!$$

- $H_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$ 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 $\gamma = 0.577\ldots$ — 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 $n \geqslant 3$:
  - $(2,1,3) \circ (3,2,1) = (2,3,1)$, $(3,2,1) \circ (2,1,3) = (3,1,2)$

★ 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: $g(9) = \mathrm{НОК}(4,5) = 20$, $g(10) = \mathrm{НОК}(2,3,5) = 30$

Теорема Кэли

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 $\phi : G \to S_G$ задана правилом $\phi(a) = f_a$
  - $f_a(x) = f_b(x) \Rightarrow xa = xb \Rightarrow a = b$

  $\Rightarrow$ ϕ — 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

- Пусть $\sigma = (i_1, \ldots, i_n)$ — перестановка в линейной записи
- Пара индексов $k < \ell$ называется инверсией (в σ), если $i_k > i_\ell$
  - число инверсий $inv(\sigma)$ — важная характеристика перестановки
  - особенно важна четность $inv(\sigma)$, называемая четностью перестановки
  - ⋆ вспомните формулу определителя: $|A| = \sum\limits_{\sigma \in S_n} (-1)^{inv(\sigma)} a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$
- Перестановка, меняющая местами два элемента, называется транспозицией
  - например, $(1, 2, 5, 4, 3, 6)$
  - 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 $\sigma = (i_1, \ldots, i_n)$ и применим сортировку пузырьком
- шаг сортировки переставляет два элемента (= умножение на транспозицию)
- результатом сортировки является $\Delta = (1, \ldots, n)$
- $\Rightarrow$ $\Delta = \sigma \circ \tau_1 \circ \cdots \circ \tau_k$, 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 $(y_1, \ldots, y_n)$ результат $\sigma(y_1, \ldots, y_n)$ действия перестановки σ есть последовательность $\left(y_{\sigma^{-1}(1)}, \ldots, y_{\sigma^{-1}(n)}\right)$
  - 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 $\theta(w)[i] \leqslant \theta(w)[j]$ 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 $w = \text{ПОДСТРОКА}$

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 (bwt(w))
    - Каждая буква из w является последней ровно для одного циклического сдвига

$\Rightarrow$ bwt(w) является анаграммой w

$\Rightarrow$ bwt как функция является действием некоторой перестановки (зависящей от w)

Пусть $\mathrm{К} < \mathrm{О} < \mathrm{Р}$. Тогда

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

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