

q-комбинаторика

Тимофей Равнушкин

Август 2025

orz Geoffrey Critzer

Содержание

1 Немного пререквезитов из линейной алгебры	1
2 Линейно независимые наборы в $\mathbb{F}_q^n$	3
3 Количество подпространств в $\mathbb{F}_q^n$	5
4 Считаем матрицы	5
4.1 Предчувствие рангов	6
4.2 Цветные гомоморфизмы	7
4.3 Количество матриц заданного ранга	8
5 Рекурренты и прямоугольники	9
5.1 Рекуррента	9
5.2 Прямоугольники	10
6 Применения	11
6.1 Codeforces Round #752 (Div. 1) F (link)	11
6.2 Atcoder Regular Contest 146 C (link)	12
7 Количество диагонализуемых матриц	12
8 q-производящие функции	14

1 Немного пререквезитов из линейной алгебры

Поле – алгебраический объект, абстрагирующий "интуитивные" свойства вещественных чисел.

Определение 1.1

Множество S с операциями $\cdot : S \times S \rightarrow S$ и $+: S \times S \rightarrow S$ называется **полем**, если выполняются следующие аксиомы:

1. Ассоциативность сложения: $(a + b) + c = a + (b + c)$
2. Существование нуля: $\exists 0 \in S : a + 0 = 0 + a = a$
3. Коммутативность сложения: $a + b = b + a$
4. Обратимость сложения: $\forall a \in S \exists (-a) \in S$ т.ч. $a + (-a) = 0$
5. Ассоциативность умножения: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

6. Существование единицы: $\exists 1 \in S$ т.ч. $a \cdot 1 = 1 \cdot a = a$
7. Коммутативность умножения: $a \cdot b = b \cdot a$
8. Частичная обратимость умножения: $\forall a \in S \setminus \{0\} \exists a^{-1} \in S$ т.ч. $a \cdot a^{-1} = 1$
9. $0 \neq 1$
10. Дистрибутивность: $a \cdot (b + c) = ab + ac$

Примеры полей:

- $\mathbb{R}, \mathbb{Q}$
- $\mathbb{Z}/p\mathbb{Z}$, где p – простое число — поле остатков по простому модулю
- $\mathbb{F}_q$, где $q = p^n$, где p – простое и $n \geq 1$ – натуральное — поле из q элементов (в существование таких полей для $n \neq 1$ предлагается просто поверить; в практических применениях в спортивном программировании чаще всего встречается $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$)

Определение 1.2

Векторным пространством над полем F называется множество S с операциями $+$: $S \times S \rightarrow S$ и $(- \cdot -) : F \times S \rightarrow S$, для которых выполняются следующие аксиомы:

1. Ассоциативность сложения: $(a + b) + c = a + (b + c)$
2. Существование нуля: $\exists 0 \in S$ т. ч. $a + 0 = 0 + a = a$
3. Коммутативность сложения: $a + b = b + a$
4. Обратимость сложения: $\forall a \in S \exists (-a) \in S$ т.ч. $a + (-a) = 0$
5. $a(b(v)) = (ab)v$ для любых $a, b \in F, v \in S$
6. $1 \cdot v = v$ для любого $v \in S$
7. $a(u + v) = au + av$
8. $(a + b)v = av + bv$

Будем называть элементы S **векторами**, а F – **скалярами**.

Примеры векторных пространств:

- F над F — поле является векторным пространством над собой
- $\mathbb{R}^n$ над $\mathbb{R}$ — пространство столбцов из n вещественных чисел (матриц $n \times 1$) с поэлементным сложением и умножением на скаляры
- $\mathbb{F}_q^n$ над $\mathbb{F}_q$ — пространство столбцов из n элементов $\mathbb{F}_q$ с поэлементным сложением и умножением на скаляры
- $\mathbb{R}[x]$ над $\mathbb{R}$ — пространство многочленов с коэффициентами из $\mathbb{R}$

Определение 1.3

Набор векторов $v_1, \dots, v_n$ из V над F называется **линейно зависимым**, если существует такой набор скаляров $a_1, \dots, a_n$ из F , не все из которых равны нулю, что $a_1 v_1 + \dots + a_n v_n = 0$. Набор векторов $v_1, \dots, v_n$ называется **базисом** V над F , если он линейно **независим** и добавление любого другого вектора сделает его линейно зависимым.

Пространство называется **конечномерным**, если в нем есть конечный базис (все рассматриваемые в дальнейшем пространства будут конечномерными).

В таком случае **размерностью** пространства V называется количество элементов в его базисе (обозначение: $\dim V$).

Упражнение. Докажите, что определение размерности корректно, то есть что все базисы конечномерного пространства имеют одинаковый размер.

Например, одним из базисов $\mathbb{R}^n$ является множество столбцов чисел таких, что в них в одной позиции стоит 1, а в остальных 0 (такой базис называется стандартным).

Определение 1.4

Линейной комбинацией векторов $v_1, \dots, v_n$ с коэффициентами $a_1, \dots, a_n$ называется сумма $a_1 v_1 + \dots + a_n v_n$.

Линейной оболочкой набора векторов $v_1, \dots, v_n$ будем называть множество всех возможных линейных комбинаций из этих векторов.

Будем обозначать линейную оболочку $\text{span}(v_1, \dots, v_n)$.

Упражнение. Докажите, что если $e_1, \dots, e_n$ - базис в векторном пространстве V , то любой вектор $v \in V$ единственным образом раскладывается в линейную комбинацию $a_1 e_1 + \dots + a_n e_n$. В таком случае $a_1, \dots, a_n$ называются **координатами** v в базисе $e_1, \dots, e_n$.

Определение 1.5

Непустое подмножество $U \subset V$ называется **подпространством**, если $\text{span}(U) = U$.

Подпространство $U \subset V$ называется **собственным**, если $U \neq V$ и $U \neq \{0\}$.

2 Линейно независимые наборы в $\mathbb{F}_q^n$

Для начала заметим, что мы можем отождествить любое векторное пространство V над $\mathbb{F}_q$ с $\mathbb{F}_q^{\dim V}$, если выберем в нём базис – отождествим вектор из V со столбцом его координат в этом базисе.

Предложение 2.1

Общее количество векторов в $\mathbb{F}_q^n$ равно q^n .

Определение 2.2

Количество линейно независимых упорядоченных наборов из k векторов из $\mathbb{F}_q^n$ называется **нисходящим q -факториалом** из n по k и обозначается $((n)_k)_q$.

Теорема 2.3

$$((n)_k)_q = \prod_{i=0}^{k-1} (q^n - q^i)$$

Доказательство. Для начала заметим, что в качестве первого вектора в наборе мы можем выбрать любой ненулевой вектор, т. е. у нас $q^n - 1$ вариант. Заметим, что единственное условие, которое нам нужно соблюсти, выбирая i -й вектор для сохранения линейной независимости, это $v_i \notin \text{span}(v_1, \dots, v_{i-1})$. В $\text{span}(v_1, \dots, v_{i-1})$ всего q^{i-1} вектор (т. к. $v_1, \dots, v_{i-1}$ линейно независимы, они порождают $(i-1)$ -мерное подпространство), т. е. мы можем выбрать i -й вектор $q^n - q^{i-1}$ способами. Итого, каждый из k векторов выбирается $q^n - q^{i-1}$ способами, т. е. весь набор выбирается $\prod_{i=0}^{k-1} (q^n - q^i)$ способами. $\square$

О нисходящих q -факториалах можно думать, как об аналоге нисходящих факториалов $((n)_k = \frac{n!}{(n-k)!})$ для векторных пространств. Обычный нисходящий факториал считает количество способов выбрать упорядоченный набор из k элементов из n -элементного множества, т. е. количество инъективных функций из k -элементного множества в n -элементное. Нисходящий q -факториал, соответственно, считает количество инъективных **линейных отображений** из k -мерного пространства в n -мерное.

Замечание. Иногда полезно выражать $((n)_k)_q = q^{\binom{k}{2}} \prod_{i=0}^{k-1} (q^{n-i} - 1)$, вынеся q в максимально возможной степени из каждой скобки.

Определение 2.4

q -аналогом натурального числа n будем называть

$$[n]_q := 1 + q + \dots + q^{n-1} = \frac{1 - q^n}{1 - q}$$

Будем считать $[0]_q := 1$.

q -факториалом натурального числа n будем называть

$$[n]_q! := [n]_q [n-1]_q \dots [1]_q = \prod_{i=1}^n \frac{1 - q^i}{1 - q}$$

Аналогично, положим $[0]_q! := 1$

Предложение 2.5

$$\begin{aligned} ((n)_k)_q &= q^{\binom{k}{2}} \prod_{i=0}^{k-1} (q^{n-i} - 1) \\ ((n)_k)_q &= (q-1)^k q^{\binom{k}{2}} \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q - 1} \\ \boxed{((n)_k)_q} &= \frac{(q-1)^k q^{\binom{k}{2}} [n]_q!}{[n-k]_q!} \end{aligned}$$

Теорема 2.6

Обозначим количество инверсий в перестановке σ за $\text{inv}(\sigma)$. Тогда $\sum_{\sigma \in S_n} q^{\text{inv}(\sigma)} = \prod_{i=1}^n [i]_q$, то есть $[n]_q!$ - обыкновенная производящая функция количеств n -элементных перестановок с заданным количеством инверсий (многочлен, в котором коэффициент при q^m равен количеству перестановок из n элементов с m инверсиями).

Доказательство. Индукция по n .

База: Для $n = 1$ обе стороны равны 1.

Шаг индукции: Пусть предположение верно для $n = k - 1$. Перестановку из k элементов можно получить из перестановки из $(k - 1)$ элемента добавлением числа k в любую из k позиций (в начало, между элементами или в конец), при этом добавление в j -ю позицию увеличивает количество инверсий на $(k - j)$. Получается, что в итоговом многочлене i -й коэффициент должен быть равен сумме первых i коэффициентов $[k - 1]_q!$. Такого эффекта на многочленах можно добиться умножением на $1 + q + \dots + q^{k-1} = [k]_q$, то есть итоговый многочлен $[k]_q [k - 1]_q! = [k]_q!$. $\square$

3 Количество подпространств в $\mathbb{F}_q^n$

Определение 3.1

$\gamma_n := ((n)_n)_q = (q-1)^n q^{\binom{n}{2}} [n]_q!$ - количество базисов в $\mathbb{F}_q^n$

Для $n \geq k$ введём $\binom{n}{k}_q$ - количество k -мерных подпространств в $\mathbb{F}_q^n$, q -биномиальный коэффициент из n по k , Гауссов биномиальный коэффициент.

Теорема 3.2

$$\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q! [k]_q!}$$

Доказательство. Количество k -мерных подпространств можно выразить, как отношение количества упорядоченных наборов из k векторов к количеству таких наборов, порождающих одно и то же подпространство, т. е. как $\frac{((n)_k)_q}{\gamma_k}$:

$$\begin{aligned} \binom{n}{k}_q &= \frac{((n)_k)_q}{\gamma_k} \\ &= \frac{(q-1)^k q^{\binom{k}{2}} [k]_q!}{(q-1)^k q^{\binom{k}{2}} [k]_q!} \\ &= \frac{[n]_q!}{[n-k]_q! [k]_q!} \end{aligned}$$

□

Замечание. $\binom{n}{k}_q = \binom{n}{n-k}_q$

Глобальная идея q -аналогов состоит в том, чтобы перейти от утверждений про конечные множества (и, соответственно, вычислений для множеств) к утверждениям про конечномерные векторные пространства над F_q . Например, как уже было упомянуто, нисходящие факториалы считают инъективные функции между конечными множествами, тогда как их q -аналоги - инъективные линейные отображения между векторными пространствами соответствующих размерностей. Также и биномиальные коэффициенты - их "обычная" версия считает количество подмножеств заданного размера, в то время как q -биномиальные коэффициенты считают подпространства.

Что же произойдёт, если мы рассмотрим пределы при $q \rightarrow 1$? Непосредственные определения всех наших q -понятий не будут иметь смысла, так как поля из одного элемента не существует (т. к. мы потребовали $0 \neq 1$ в полях). Однако, если рассматривать исключительно формульные выражения наших q -аналогов, можно заметить, что при $q \rightarrow 1$ они превращаются в свои "обычные" версии! Так, например, $\lim_{q \rightarrow 1} [n]_q = n$ так же, как $\lim_{q \rightarrow 1} \binom{n}{k}_q = \binom{n}{k}$ и т. д.

4 Считаем матрицы

Мы получили достаточно много инструментов, с помощью которых можно изучать векторные пространства над конечными полями. О векторах *иногда* можно думать, как о столбцах из чисел. А что будет, если составить несколько столбцов вместе? Матрица! Однако, для того, чтобы эффективнее изучать матрицы с помощью наших инструментов и понятий, удобно сначала понять, как можно смотреть на матрицы с другой стороны (не как на таблицы чисел).

4.1 Предчувствие рангов

Определение 4.1

Линейным отображением (также гомоморфизмом векторных пространств) между векторными пространствами U и V над одним и тем же полем F называется такое отображение $f : U \rightarrow V$ как множество, что:

1. $f(u + v) = f(u) + f(v)$
2. $f(av) = af(v)$

Линейное отображение называется **изоморфизмом**, если оно биективно. Два пространства называются **изоморфными**, если между ними существует изоморфизм.

Упражнение. Докажите, что линейное отображение задаётся своими значениями на базисных векторах.

Лемма 4.2

Матрицы размера $n \times m$ с коэффициентами из $\mathbb{F}_q$ находятся в биекции с линейными отображениями $\mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$.

Доказательство. Сначала научимся задавать отображение по матрице.

Пусть у нас есть матрица $A \in \text{Mat}_{n \times m}(\mathbb{F}_q)$. $\mathbb{F}_q^m$ состоит из столбцов размера m , поэтому можно определить отображение $\varphi_A : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$, действующее на элементах $\mathbb{F}_q^m$ умножением справа на матрицу: $\varphi_A(v) = Av$. Очевидно, что это отображение линейно.

Пусть теперь у нас есть линейное отображение $\xi : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$. Обозначим стандартный базис в $\mathbb{F}_q^m$ (столбцы, где ровно в 1 клетке стоит 1, а в остальных 0) за $e_1, \dots, e_m$. Определим матрицу $B_\xi \in \text{Mat}_{n \times m}(\mathbb{F}_q)$, в i -м столбце которой будут записаны координаты $\xi(e_i)$ в стандартном базисе $\mathbb{F}_q^n$.

Рассмотрим произвольную матрицу C . Соответствующее ей линейное отображение φ_C переводит e_i в её i -й столбец, поэтому построенная по нему матрица B_{φ_C} будет совпадать с исходной.

Теперь возьмём какое-то линейное отображение ψ . Оно переводит вектор $a_1 e_1 + \dots + a_m e_m$ в $a_1 \psi(e_1) + \dots + a_m \psi(e_m)$. При этом линейное отображение φ_{B_ψ} , соответствующее его матрице B_ψ , переводит такой вектор в линейную комбинацию столбцов этой матрицы с коэффициентами $a_1, \dots, a_m$, но в столбцах записаны в точности $\psi(e_i)$, следовательно, эти отображения совпадают. $\square$

Замечание. В дальнейшем будем обозначать линейные отображения и соответствующие им матрицы одними и теми же буквами.

Определение 4.3

Ядром линейного отображения f называется подмножество U , которое отображается в 0, т. е. $\text{Ker } f := \{u \in U \mid f(u) = 0\}$.

Образом линейного отображения f называется подмножество V , в которое отображается U , т. е. $\text{Im } f := \{f(u) \mid u \in U\}$.

Предложение 4.4

Для линейного отображения $U \xrightarrow{\varphi} V$:

1. $\text{Ker } \varphi$ – подпространство в U
2. $\text{Im } \varphi$ – подпространство в V
3. φ инъективно $\iff \text{Ker } \varphi = 0$

4. φ сюръективно $\iff \text{Im } \varphi = V$

Определение 4.5

Рангом матрицы называется размерность образа соответствующего линейного отображения $\dim \text{Im } A$, или, эквивалентно, размер максимального линейно независимого подмножества её столбцов.

Главной задачей всей этой главы будет подсчёт матриц заданного ранга (в частности, нам пригодится взгляд на матрицы, как на отображения, потому что ядро и образ - подпространства, а про них мы что-то знаем из предыдущих глав).

4.2 Цветные гомоморфизмы

Пусть мы зафиксировали какое-то подпространство $W \subset V$. Тогда на V можно ввести отношение эквивалентности $u \sim v \iff (u - v) \in W$. На множестве классов эквивалентности этого отношения (обозначим класс элемента u за $u + W$) есть естественная структура векторного пространства:

- $(u + W) + (v + W) = (u + v) + W$
- $a(u + W) = (au) + W$

Определение 4.6

Множество классов эквивалентности этого отношения с определёнными выше операциями называется **факторпространством** V по W и обозначается V/W .

Замечание. Размерность факторпространства равна разности размерностей пространства и подпространства, т. е. $\dim V/U = \dim V - \dim U$.

Важно отметить, что из пространства есть естественное линейное отображение в его фактор, отправляющее вектор в его класс эквивалентности. Будем называть такое отображение **факторным**.

Упражнение. Докажите, что ядром факторного отображения $\pi : V \rightarrow V/U$ является U .

В качестве примера рассмотрим факторпространство $\mathbb{R}^3$ (обозначим его стандартный базис e_x, e_y, e_z) по подпространству $\text{span}(e_z)$. Элементами этого факторпространства будут прямые, параллельные O_z (оно же $\text{span}(e_z)$), и оно, на самом деле, будет изоморфно $\text{span}(e_x, e_y)$. Об операции взятия факторпространства можно думать, как о "схлопывании" подпространства в 0; например, в данном случае мы схлопнули все " z -составляющие" всех векторов.

Теорема 4.7: Теорема о гомоморфизме

Зафиксируем линейное отображение $\varphi : U \rightarrow V$. Тогда факторпространство U по ядру φ изоморфно образу φ .

Доказательство. Обозначим $\text{Ker } \varphi$ за W .

Определим $\psi : U/W \rightarrow \text{Im } \varphi$, как $\psi(v + W) = \varphi(v)$.

Проверим корректность определения ψ , т. е. что оно переводит представителей одного класса эквивалентности в один и тот же вектор ($u \sim v \implies \psi(u + W) = \psi(v + W)$). Пусть $u \sim v$, тогда $\psi(u + W) - \psi(v + W) = \varphi(u) - \varphi(v) = \varphi(u - v)$. Но $(u - v) \in W$, т. е. $\psi(u + W) - \psi(v + W) = 0$, что и требовалось.

Очевидно, что определённое таким образом отображение линейно, значит, нам осталось проверить, что оно является изоморфизмом. Для этого докажем, что оно инъективно и сюръективно:

- $v \in \text{Im } \varphi \implies \exists u \in U \text{ т. ч. } \varphi(u) = v \implies \psi(u + W) = v$

- $\text{Ker } \psi = \{(u + W) \in U/W \mid \psi(u + W) = 0\} = \{(u + W) \in U/W \mid \varphi(u) = 0\}$. Но мы знаем, что $\varphi(u) = 0 \implies (u - 0) \in W \implies (u + W) = (0 + W)$, то есть $\text{Ker } \psi = 0$, что и требовалось. $\square$

Следствие 4.8

Всякое линейное отображение $\varphi : U \rightarrow V$ раскладывается в композицию $\iota\psi\pi$, где π - факторное, ψ - изоморфизм, ι - вложение подпространства.

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & V \\ & \searrow \pi & \nearrow \iota \\ & U/\text{Ker } \varphi & \xrightarrow{\sim_{\psi}} \text{Im } \varphi \end{array}$$

4.3 Количество матриц заданного ранга

Теорема 4.9

Количество матриц размера $m \times n$ с коэффициентами из $\mathbb{F}_q$, имеющих ранг k , равно $((n)_k)_q \cdot \binom{m}{k}_q$.

Доказательство. Пользуясь следствием 4.8, любое отображение ранга k раскладывается в композицию $\iota\psi\pi$.

Заметим, что отображение π зависит только от того, какое подпространство $\mathbb{F}_q^n$ является ядром φ , следовательно, возможных π всего $\binom{n}{k}_q$ (в силу теоремы о гомоморфизме из того, что образ имеет размерность k , следует, что ядро – подпространство размерности $n - k$, при этом $\binom{n}{n-k}_q = \binom{n}{k}_q$). Аналогично, отображение ι зависит только от того, каким подпространством $\mathbb{F}_q^m$ является образ φ , следовательно, таких ι всего $\binom{m}{k}_q$. Осталось научиться считать возможные ψ .

Из-за того, что ранг φ равен k , $\dim \mathbb{F}_q^n / \text{Ker } \varphi = \dim \text{Im } \varphi = k$, то есть ψ – изоморфизм пространств размерности k .

Лемма 4.10

Пусть U, V – векторные пространства над F_q размерности k . Тогда между ними существует ровно γ_k различных изоморфизмов.

Доказательство. Выберем произвольный базис в U . Заметим, что при изоморфизме он переходит в какой-то базис V , при этом изоморфизм полностью задаётся своими значениями на каком-либо базисе U , следовательно, в таких условиях изоморфизмы находятся в биекции с базисами V , следовательно, их γ_k . $\square$

Таким образом у нас $\binom{n}{k}_q$ способов выбрать π , $\binom{m}{k}_q$ вариантов ι и γ_k вариантов ψ . Получается, что возможных ϕ всего $\binom{n}{k}_q \cdot \gamma_k \cdot \binom{m}{k}_q$:

$$\begin{aligned} \binom{n}{k}_q \cdot \gamma_k \cdot \binom{m}{k}_q &= \left(\frac{[n]_q!}{[n-k]_q! [k]_q!} \cdot (q-1)^k q^{\binom{k}{2}} [k]_q! \right) \cdot \binom{m}{k}_q \\ &= \left(\frac{(q-1)^k q^{\binom{k}{2}} [n]_q!}{[n-k]_q!} \right) \cdot \binom{m}{k}_q \\ &= ((n)_k)_q \cdot \binom{m}{k}_q \end{aligned}$$

$\square$

5 Рекурренты и прямоугольники

Можно считать q -биномиальные коэффициенты по определению, считая произведения q -аналогов натуральных чисел. Однако, в следующем разделе мы научимся считать их рекуррентно.

5.1 Рекуррента

Теорема 5.1

$$\binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q$$

Доказательство. Фиксируем какой-то вектор $v \in \mathbb{F}_q^n$. Тогда первое слагаемое в правой части равенства равно количеству k -мерных подпространств $\mathbb{F}_q^n$, не содержащих v , так как такие подпространства можно посчитать аналогично 2.3 с дополнительным условием, что вектора мы все время выбираем не из $\text{span}(v)$. Получается, нам нужно доказать, что второе слагаемое считает k -мерные подпространства, содержащие v .

Лемма 5.2

Пусть V – конечномерное векторное пространство, а U – его подпространство. Тогда подпространства V/U находятся в биекции с подпространствами V , содержащими U .

Доказательство. Обозначим факторное отображение $V \rightarrow U$ за π .

Для доказательства:

1. построим отображение f из множества подпространств V , содержащих U , в множество подпространств V/U и покажем, что оно корректно определено
 2. построим отображение g из множества подпространств V/U , в множество подпространств V , содержащих U , и покажем, что оно корректно определено
 3. проверим, что они обратны друг другу.
1. Итак, начнём с построения f . Пусть W – подпространство V , содержащее U , тогда $f(W) := \pi(W) := \{\pi(w) \mid w \in W\}$. Для проверки, что $f(W)$ действительно является подпространством, достаточно проверить $\pi(w_1) + \pi(w_2) = \pi(w_1 + w_2)$ и $a\pi(w) = \pi(aw)$ для любых $w_1, w_2 \in W$. Это следует из линейности факторного отображения.
2. Пусть теперь $\hat{Y}$ – подпространство V/U (оно состоит из некоторых классов эквивалентности вида $v + U$). Определим $g(\hat{Y}) := \pi^{-1}(\hat{Y}) := \{v \in V \mid \pi(v) \in \hat{Y}\}$. Проверим, что g корректно определено, т. е. прообразы элементов из $\hat{Y}$ не зависят от выбора их представителей, то есть $a + U = b + U \implies \pi^{-1}(a + U) = \pi^{-1}(b + U)$:

$$\begin{aligned} \pi^{-1}(a + U) &= \{v \in V \mid (v - a) \in U\} \\ &= \{v \in V \mid v + U = a + U\} \\ &= \{v \in V \mid v + U = b + U\} \\ &= \{v \in V \mid (v - b) \in U\} \\ &= \pi^{-1}(b + U) \end{aligned}$$

То, что $g(\hat{Y})$ является подпространством V , проверяется по определению:

- (а) $v \in \pi^{-1}(\hat{Y}) \implies (v - a) \in U$ для некоторого $a \in V$ такого, что $a + U \in \hat{Y}$. При этом для любого скаляра γ , $\gamma a + U \in \hat{Y}$ и $(\gamma v - \gamma a) \in U$, значит, $\gamma v \in \pi^{-1}(\hat{Y})$.
- (б) Аналогично п. 1, $u, v \in \pi^{-1}(\hat{Y}) \implies (u - a) \in U, (v - b) \in U$. При этом $a + U \in \hat{Y}$ и $b + U \in \hat{Y}$, следовательно, $(a + b) + U \in \hat{Y}$. Но $((u + v) - (a + b)) \in U$, получается, что $(u + v) \in \pi^{-1}(\hat{Y})$.

То, что $g(\hat{Y})$ содержит U , следует из того, что $0 + U \in \hat{Y}$, ведь $\pi^{-1}(0 + U) = U$.

3. Осталось показать, что f и g обратны друг другу.

Сначала покажем, что $f \circ g(\hat{Y}) = \hat{Y}$. Пусть $a + U$ - произвольный элемент $\hat{Y}$, тогда если $v \in \pi^{-1}(\hat{Y})$, то $(v - a) \in U$, следовательно, $\pi(v) = v + U = a + U$. То есть f переводит подмножество $\{v \in V \mid v - a \in U\}$ в $a + U$, поэтому $f \circ g(\hat{Y}) \subset \hat{Y}$. Для обратного включения заметим, что для $a + U \in \hat{Y}$ существует $a \in \pi^{-1}(\hat{Y})$ и $\pi(a) = a + U$.

При этом $g \circ f(W) = \pi^{-1}(\pi(W))$. Пусть теперь v - любой элемент $\pi^{-1}(\pi(W))$, то есть любой вектор $v \in V$ такой, что $\pi(v) \in \pi(W)$. То есть для какого-то $w \in W$ верно $\pi(v) = \pi(w)$, то есть $\pi(v - w) = \pi(v) - \pi(w) = 0$, но ядром π является в точности U , т. е. $v - w \in U$. При этом W таково, что $U \subset W$, получается, что $v - w \in W$, то есть $v \in W$. Получили, что $g \circ f(W) \subset W$. Для обратного включения заметим, что $v \in \pi^{-1}(\pi(v))$.

□

Получается, что k -мерному подпространству $U \subset V$, содержащему v , по нашей биекции соответствует единственное $(k - 1)$ -мерное подпространство $\pi(U) \subset V/\text{span}(v)$, при этом мы знаем, что $\dim V/\text{span}(v) = \dim V - \dim \text{span}(v) = n - 1$, то есть возможных $\pi(U)$ всего $\binom{n-1}{k-1}_q$, следовательно, возможных U столько же: $\binom{n-1}{k-1}_q$. □

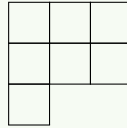
Упражнение. С помощью индукции покажите, что $\binom{n}{k}_q$ - многочлен степени $k(n - k)$.

5.2 Прямоугольники

В этом разделе мы, пользуясь результатом из предыдущего, поймём, как можно думать о q -биномиальных коэффициентах немного с другой стороны.

Определение 5.3

Диаграммой Юнга длины n называется любая невозрастающая последовательность из n неотрицательных чисел. (О диаграммах Юнга можно думать, как о наборах столбиков из кубиков, высоты которых невозрастают.)



Визуализация диаграммы $(3, 3, 1)$.

Диаграмма Юнга λ называется **вписанной в прямоугольник** $n \times t$, если её длина n и каждое из чисел в ней $\leq t$. Будем обозначать множество диаграмм Юнга, вписанных в данный прямоугольник $n \times t$, за $\mathbb{Y}(n \times t)$.

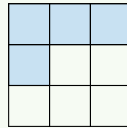


Диаграмма $(3, 1, 0)$ вписана в прямоугольник 3×3 .

Весом диаграммы Юнга λ называется сумма её элементов. (Обозначение $|\lambda|$, пример: $|(3, 2, 1)| = 6$.)

Для $n \geq k$ обозначим за $f(n, k)$ многочлен $\sum_{\lambda \in \mathbb{Y}(k \times (n-k))} q^{|\lambda|}$, где q - некоторая формальная переменная. (То есть коэффициент при x^i в $f(n, k)$ - количество диаграмм веса i , вписанных в $k \times (n - k)$.)

Теорема 5.4

$f(n, k)$ и $\binom{n}{k}_q$ равны, как многочлены от q .

Доказательство. Доказательство будет опираться на рекурренту из предыдущего раздела (Теорема 5.1).

Нетрудно показать, что для $k \leq n \leq 1$ верно, что $f(n, k) = \binom{n}{k}_q$. Остаётся доказать, что для $f(n, k)$ выполняется такая же рекуррента.

Лемма 5.5

$$f(n, k) = q^k f(n-1, k) + f(n-1, k-1)$$

Доказательство. Разобьём $\mathbb{Y}(k \times (n-k))$ на два множества - в одном (обозначим его $\mathbb{A}_1$) будут лежать диаграммы, каждое число в которых ≥ 1 , а в другом ($\mathbb{A}_0$) - остальные (очевидно, что это те диаграммы, последнее число в которых равно 0).

Заметим, что диаграммы из $\mathbb{A}_0$ в точности совпадают с диаграммами из $\mathbb{Y}((k-1) \times (n-k))$, так как последнее число в каждой из них равно 0. Получается, что часть $f(n, k)$, соответствующая таким диаграммам, равна $f(n-1, k-1)$.

Теперь посмотрим на диаграммы из $\mathbb{A}_1$. Заметим, что каждая такая диаграмма получается из какой-то диаграммы из $\mathbb{Y}(k \times (n-k-1))$ добавлением 1 к каждому числу в последней. При этом по любой диаграмме из $\mathbb{Y}(k \times (n-k-1))$ можно построить диаграмму из $\mathbb{A}_1$, поэтому между $\mathbb{A}_1$ и $\mathbb{Y}(k \times (n-k-1))$ существует биекция. Получается, часть $f(n, k)$, соответствующая $\mathbb{A}_1$, равна $f(n-1, k)$? Нет, потому что при переходе от $\lambda \in \mathbb{A}_1$ к $\gamma \in \mathbb{Y}(k \times (n-k-1))$ вычитанием 1 из каждого числа в λ мы уменьшили вес λ в точности на k (так как в ней k строк). Получается, что соответствующая часть равна $q^k f(n-1, k)$.

При этом $\mathbb{Y}(k \times (n-k)) = \mathbb{A}_1 \sqcup \mathbb{A}_0$, следовательно, $f(n, k) = q^k f(n-1, k) + f(n-1, k-1)$. $\square$

$\square$

Пользуясь этой рекуррентой, мы можем считать количество диаграмм заданного веса w , вписанных в прямоугольник $n \times m$, за $O((n+m)n)$. Однако, если мы хотим вычислить такую величину для всех весов от 0 до W , мы можем посчитать первые W коэффициентов $\binom{n+m}{n}_q$, что можно сделать за $O(W \log W)$ за счёт логарифмирования и взятия экспоненты.

6 Применения

6.1 Codeforces Round #752 (Div. 1) F ([link](#))

Задача: для данных n, k, x посчитать количество упорядоченных наборов из n чисел, каждое из которых лежит в диапазоне $[0, 2^k - 1]$ таких, что хог никакого непустого подмножества не равен x .

Решение: о двоичных числах длины k с операцией хог можно думать, как о векторах из $\mathbb{F}_2^k$. Если $x = 0$, то нам необходимо считать линейно независимые наборы длины n , что мы умеем делать (Определение 2.2). Если $x \neq 0$, то для набора $a_1, \dots, a_n$ условие, которое должно выполняться, в точности $x \notin \text{span}(a_1, \dots, a_n)$. Как считать такие наборы?

Классифицируем такие наборы по тому, подпространства какой размерности они порождают. Построим по нашему набору $a_1, \dots, a_n$ матрицу A размера $k \times n$, выписав их координаты в столбцах матрицы. Тогда $\dim \text{span}(a_1, \dots, a_n) = \text{rk} A$ по определению ранга матрицы (потому что линейная оболочка столбцов матрицы это в точности образ соответствующего ей линейного отображения). При этом матрицы ранга d мы научились считать в Теореме 4.9. Сколько из d -мерных подпространств нам подходят? Как мы выяснили в Теореме 5.1, ответ на этот вопрос - $2^d \binom{k-1}{d}_2$. Заметим, что у всех подпространств размерности d одинаковое число порождающих их наборов из n векторов, при этом всего таких подпространств $\binom{k}{d}_2$, а следовательно, доля

подходящих нам - $\frac{2^d \binom{k-1}{d}_2}{\binom{k}{d}_2}$. Получается, что подходящих наборов, порождающих подпространство размерности d , не содержащее x , в точности $((n)_d)_2 \cdot \binom{k}{d}_2 \cdot \frac{2^d \binom{k-1}{d}_2}{\binom{k}{d}_2}$. Итого ответ на задачу:

$$\sum_{d=1}^k ((n)_d)_2 \cdot \binom{k}{d}_2 \cdot \frac{2^d \binom{k-1}{d}_2}{\binom{k}{d}_2} = \sum_{d=1}^{k-1} ((n)_d)_2 \cdot 2^d \cdot \binom{k-1}{d}_2$$

6.2 Atcoder Regular Contest 146 C ([link](#))

Задача: сколько множеств неотрицательных чисел от 0 до $2^N - 1$ (включительно) таковы, что в каждом из них нет непустого подмножества чётного размера с хог-суммой, равной 0.

Решение: эта задача не непосредственно на применение q -биномов, однако, использует технику подсчёта, похожую на вычисление $((n)_k)_q$.

Пусть у нас уже есть некоторое множество S размера n , удовлетворяющее условию задачи. Заметим, что из этого следует, что у всех подмножеств S нечётного размера различные хог-суммы. Какой вектор можно добавить в S так, что для нового множества условие также будет выполняться? Любой, неравный хог-сумме ни одного из подмножеств S нечётного размера! Всего таких подмножеств 2^{n-1} , при этом у всех из них различные хог-суммы, получается, что мы можем добавить любой из $2^N - 2^{n-1}$ векторов.

Пользуясь "постепенным добавлением векторов" из предыдущего абзаца, получаем, что подходящих подмножеств размера $k \geq 2$ всего $\frac{2^N \cdot \prod_{i=0}^{k-2} (2^N - 2^i)}{k!}$ (деление на факториал появляется из неупорядоченности множеств). Подходящих множеств размера 1 всего 2^N (мы можем взять любой вектор), а размера 0 - всего одно. Ответ на задачу равен сумме таких значений по всем размерам подмножеств до $N + 1$ (очевидно, что не существует множеств размера $N + 2$ или более, удовлетворяющих условию).

Также через q -аналоги можно решить Atcoder Regular Contest 139 F ([link](#)) и Atcoder Beginner Contest 278 H ([link](#)).

7 Количество диагонализуемых матриц

Определение 7.1

Матрица называется **диагонализуемой**, если существует базис, в котором соответствующий ей линейный оператор записывается диагональной матрицей.

Определение 7.2

Для линейного оператора $A : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ вектор $v \in \mathbb{F}_q^n$ называется **собственным**, если $Av = \lambda v$ для какого-то $\lambda \in \mathbb{F}_q$. В таком случае λ называется **собственным значением** A . Собственные вектора A с одним и тем же собственным значением λ образуют подпространство V . Будем называть это подпространство **собственным подпространством** $E(\lambda, A) = \text{Ker}(A - \lambda I)$.

Определение 7.3

Суммой подпространств $U_1, U_2 \subset V$ называется подпространство $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$. Сумма подпространств называется **прямой**, если $U_1 \cap U_2 = \{0\}$. Прямая сумма обозначается $U_1 \oplus U_2$.

Замечание. Любой вектор $u \in U_1 \oplus U_2$ единственным образом раскладывается в сумму вектора из U_1 и вектора из U_2 .

Предложение 7.4

$A : V \rightarrow V$ диагоналізуем $\iff$ существует базис V из собственных векторов $A \iff V$ раскладывается в прямую сумму собственных подпространств A .

Определим **слабое разложение** векторного пространства V , как последовательность подпространств V , прямая сумма ненулевых членов которой даёт V . Другими словами, слабое разложение - последовательность $U_1, \dots, U_k \subset V$, в которой некоторые U_i могут быть равны 0 и $U_1 \oplus U_2 \oplus \dots \oplus U_k = V$.

Теорема 7.5

Диагоналізуемые операторы на V над $\mathbb{F}_q$ находятся в биекции со слабыми разложениями V на q подпространств.

Доказательство. Пусть A - диагоналізуемый оператор на $V = \mathbb{F}_q^n$. Пронумеруем элементы $\mathbb{F}_q$ как $0, 1, \dots, q-1$. Рассмотрим последовательность подпространств $E(0, A), E(1, A), \dots, E(q-1, A)$. Так как A - диагоналізуемый, V раскладывается в прямую сумму ненулевых собственных подпространств A . $E(\lambda, A) = 0$, если λ - не собственное значение A . Получается, что $E(0, A) \oplus \dots \oplus E(q-1, A) = V$, и $E(i, A)$ - слабое разложение A .

Обратно: пусть у нас есть слабое разложение $U_0, \dots, U_{q-1}$. Пусть $U_{i_1}, \dots, U_{i_m}$ - ненулевые члены этого разложения. Тогда $V = U_{i_1} \oplus \dots \oplus U_{i_m}$, и мы можем определить оператор A , который будет действовать на элементах U_{i_j} умножением на i_j , и линейно продолжается до всего V . $\square$

Как посчитать слабые разложения $\mathbb{F}_q^n$?

Пусть $n_1, \dots, n_q$ - неотрицательные целые числа, такие, что $n_1 + \dots + n_q = n$. Научимся считать слабые разбиения $U_1, \dots, U_q$ такие, что $\dim U_i = n_i$.

Предложение 7.6

Слабых разбиений $U_1, \dots, U_q$ таких, что $\dim U_i = n_i$ ровно $\frac{\gamma_n}{\gamma_{n_1} \gamma_{n_2} \dots \gamma_{n_q}}$.

Доказательство. Существует $\binom{n}{n_1}_q = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n_1-1})}{\gamma_{n_1}}$ подпространств $\mathbb{F}_q^n$ размерности n_1 . Количество подпространств размерности n_2 , избегающих выбранного подпространства размерности n_1 , равно $\frac{(q^n-q^{n_1})(q^n-q^{n_1+1})\dots(q^n-q^{n_1+n_2-1})}{\gamma_{n_2}}$. Продолжая, получим:

$$\begin{aligned} & \frac{(q^n-1)\dots(q^n-q^{n_1-1})}{\gamma_{n_1}} \cdot \frac{(q^n-q^{n_1})\dots(q^n-q^{n_1+n_2-1})}{\gamma_{n_2}} \dots \frac{(q^n-q^{n_1+\dots+n_{q-1}})\dots(q^n-q^{n-1})}{\gamma_{n_q}} = \\ & = \frac{\gamma_n}{\gamma_{n_1} \gamma_{n_2} \dots \gamma_{n_q}} \quad \square \end{aligned}$$

Получается, что количество диагоналізуемых операторов на $\mathbb{F}_q^n$ равно $\gamma_n \sum_{n_1+\dots+n_q=n} \frac{1}{\gamma_{n_1} \dots \gamma_{n_q}}$. Как такое вычислять?

Вспомним, как выглядит формула произведения двух формальных степенных рядов:

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n$$

Получается, что если $F(x) = \sum_{i=0}^{\infty} a_i x^i$, то $F^k(x) = \sum_{n=0}^{\infty} \left(\sum_{n_1+\dots+n_k=n} a_{n_1} a_{n_2} \dots a_{n_k} \right) x^n$. Это подводит нас к удобному комбинаторному трюку, которым можно пользоваться, если выписать формульное решение для количества каких-то объектов не получается:

Определение 7.7

Обыкновенной производящей функцией для последовательности $a_0, a_1, \dots$ называется формальный степенной ряд $F(x) = \sum_{i=0}^{\infty} a_i x^i$.

Рассмотрим $\gamma(x) = \sum_{i=0}^{\infty} \frac{1}{\gamma_i} x^i$. Пользуясь формулой для q -й степени ФСР, получаем, что

$$\gamma^q(x) = \sum_{n=0}^{\infty} \left(\sum_{n_1+n_2+\dots+n_q=n} \frac{1}{\gamma_{n_1} \dots \gamma_{n_q}} \right) x^n$$

Для того, чтобы сделать из $\gamma^q(x)$ полноценную производящую функцию для количества диагонализуемых операторов над $\mathbb{F}_q^n$, нам достаточно домножить каждый его коэффициент при x^n на γ_n . Это даёт способ считать количество операторов, потому что узнать первые n коэффициентов q -й степени можно за $O(n \log n)$, как первые n коэффициентов $\exp(q \ln \gamma(x))$.

Также из нашей формулы легко получить, например, количество обратимых диагонализуемых операторов. Оператор обратим тогда и только тогда, когда 0 - не его собственное значение. Получается, что $E(0, A)$ должно быть равно, следовательно, производящая функция для этой величины это $\gamma^{q-1}(x)$.

Также можно рассматривать производящие функции двух аргументов, тогда, например, коэффициент при $x^n y^m$ в $\gamma(x) \gamma^{q-1}(xy)$ - количество диагонализуемых операторов A на $\mathbb{F}_q^n$ таких, что $\dim \text{Im } A = m$ (только делённое на γ_n).

8 q -производящие функции

Теперь, когда мы узнали про какие-то обыкновенные производящие функции, можно посмотреть на чуть другое их семейство - q -экспоненциальные производящие функции (сокращённо q -e.g.f от q -exponential generating function). Это, на самом деле, тоже ряды, но в них мы будем писать перед членами нужных степеней не просто члены нашей последовательности, но их, делённые на q -факториал.

Определение 8.1

q -экспоненциальной производящей функцией для последовательности $a_1, a_2, \dots$ называется ряд $F(x) = \sum_{n=0}^{\infty} \frac{a_n}{[n]_q!} x^n$

q -экспонентой называется q -e.g.f. для последовательности из единиц, т. е. ряд $e_q(x) = \sum_{n=0}^{\infty} \frac{x^n}{[n]_q!}$

Пусть $(f_{n,k})$ - двумерный массив чисел (возможно, бесконечный). Тогда q -e.g.f. от двух переменных называется ряд $G(x, y) = \sum_{n,k} f_{n,k} y^k \frac{x^n}{[n]_q!}$

Учитывая, что $\binom{n}{k}_q = \frac{[n]_q!}{[k]_q! [n-k]_q!}$, получим формулу для произведения q -e.g.f:

$$\begin{aligned} \left(\sum_{i=0}^{\infty} \frac{a_i}{[i]_q!} x^i \right) \left(\sum_{j=0}^{\infty} \frac{b_j}{[j]_q!} x^j \right) &= \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{a_k b_{n-k} x^n}{[k]_q! [n-k]_q!} \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^n \binom{n}{k}_q a_k b_{n-k} \right) \frac{x^n}{[n]_q!} \end{aligned}$$

Получается, что произведение q -e.g.f. для последовательностей a_i и b_i является q -e.g.f. для последовательности $(\sum_{k=0}^n \binom{n}{k}_q a_k b_{n-k})$ (буквально то же самое, что с экспоненциальными производящими, но вместо факториалов q -аналоги).

Заметим, что из этого следует, что $e_q(x)^2$ — q -e.g.f. для последовательности $(\sum_{k=0}^n \binom{n}{k}_q)$, т. е. для общего количества подпространств в пространстве размера n . А, например, $\frac{x^k}{[k]_q!} e_q(x)$ — это q -e.g.f. для $\binom{n}{k}_q$, т. е. количества k -мерных подпространств. Также можно посмотреть на $e_q(xy)e_q(x)$, как на q -e.g.f. двух переменных; тогда член массива при $y_k x^n$ — ровно $\binom{n}{k}_q$.

Обозначим $ch_q(x) = \sum_{n=0}^{\infty} \frac{x^{2n}}{[2n]_q!}$ и $sh_q(x) = \sum_{n=0}^{\infty} \frac{x^{2n+1}}{[2n+1]_q!}$. Тогда $ch_q(x)e_q(x)$ считает количество подпространств чётной размерности, а $sh_q(x)e_q(x)$ — нечётной.

Пусть мы теперь хотим считать количество способов выбрать последовательность $W \subset U \subset V$. Если $\dim V = n, \dim U = k, \dim W = m$, то это число равно $\binom{n}{k}_q \binom{k}{m}_q$. Если мы хотим просуммировать это по всем m, k , то достаточно взять $e_q(x)^3$. Также можно добавить в один из множителей ещё одну формальную переменную, и получить q -e.g.f., считающую количество таких цепочек, в которых $\dim W = m$ (т. е. коэффициент при $x^n y^m$ в $e_q(xy)e_q(x)^2$ равен $\sum_{k=m}^n \binom{n}{k}_q \binom{k}{m}_q$).

Определение 8.2

Флагом длины m в конечномерном векторном пространстве V называется последовательность подпространств $V = V_0 \supset V_1 \supset V_2 \supset \dots \supset V_{m-1} \supset V_m = 0$, где каждое включение строгое.

Из предыдущего абзаца мы поняли, что $(e_q(x) - 1)^k$ считает количество флагов длины k (-1 появился из-за того, что все включения во флагах строгие). Получается, что общее число флагов должна считать функция $1 + (e_q(x) - 1) + (e_q(x) - 1)^2 + \dots = \frac{1}{1 - (e_q(x) - 1)}$. При этом добавление ещё одной переменной опять-таки позволяет классифицировать флаги по длине — $\frac{1}{1 - y(e_q(x) - 1)}$ считает флаги длины k в n -мерных пространствах.

Теперь давайте ослабим условие на флаг, перестав требовать $V_0 = V$ и $V_m = 0$. Будем называть наши новые объекты **цепями** (это пути в графе частичного порядка подпространств V по включению). Из цепи, не являющейся флагом, можно сделать флаг, добавив в начало и конец V и 0 , соответственно. Получается, что количество цепей считает $\frac{e_q(x)^2}{1 - (e_q(x) - 1)}$.

Вспоминая теорему 7.6, несложно понять, как считать количество разложений V в прямую сумму подпространств. От использованных там слабых разложений они отличаются недопустимостью нулевых подпространств в сумме (все разбиения n на m слагаемых должны не содержать 0) и, в данном случае, неупорядоченностью. То есть количество разбиений на ровно m слагаемых равно $\frac{1}{m!} \sum_{n_1+n_2+\dots+n_m=n, n_i \geq 1} \frac{\gamma_n}{\gamma_{n_1} \gamma_{n_2} \dots \gamma_{n_m}}$. Как такое считать? Заметим, что $(\gamma(x) - 1)^m$ считает такую сумму, только без деления на $m!$ (-1 появился, опять-таки, из-за недопустимости нулевых подпространств). Однако, можно вспомнить, что существует прекрасный ряд $\exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}$, подстановка $(\gamma(x) - 1)$ в который даст нам нужную производящую! Сумма по всем степеням посчитает разбиения на всевозможные количества слагаемых, а деление на факториал сделает так, что они будут неупорядоченными. Итого, производящая функция разбиений на подпространства это $\exp(\gamma(x) - 1)$. Другими словами, $\gamma_n[x^n] \exp(\gamma(x) - 1)$ — это количество разбиений $\mathbb{F}_q^n$. (Опытный читатель заметит, что это очень похоже на экспоненциальную производящую для чисел Белла $\exp(\exp(x) - 1)$, которая считает количество неупорядоченных разбиений именованного множества). Как и раньше, добавление ещё одной переменной позволяет считать разбиения на ровно k слагаемых, как коэффициенты $\exp(y(\gamma(x) - 1))$.