Основы комбинаторики и теории чисел

Сергей Григорян

27 ноября 2024 г.

Содержание

1 Лекция 9 **3**

1.1 Циклические п-ти 4

1.2 Формула обращения Мёбиуса 4

2 Лекция 10 **6**

2.1 Обращение Мёбиуса на чуме (част. уп. мн-во) 8

2.1.1 Ф-ция Мёбиуса 8

3 Лекция 11 **10**

3.1 Линейные рекуррентные соотношения с постоянными коэффициентами 12

1 Лекция 9

7)

$$C_n^0 - C_n^1 + \ldots + (-1)^n C_n^n = \begin{cases} 1, n = 0 \\ 0, n > 0 \end{cases}$$

8) Рассм. $A = \{ a_1, \ldots, a_n \}, m < n, m > 0$. Выберем из A все возм. m-разм. с повтор. Их n^m. $N = n^m, \alpha_1, \ldots \alpha_m$. Размещ. обладает св-вом $\alpha_i \iff \alpha_i \notin$ размещению.

$$N(\alpha_i) = (n-1)^m, N(\alpha_i, \alpha_j) = (n-2)^m$$

$$N(\alpha_1', \ldots, \alpha_n') = 0$$

По формуле вкл.-искл.:

$$N(\alpha_1', \ldots, \alpha_n') = n^m - n(n-1)^m + C_n^2(n-2)^n + \ldots$$

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

Задача 1.1. Задача о беспорядках:

Определение 1.1. Беспорядок - перестановка, при кот. $\sigma_i \neq i, \forall i = \overline{1, n}$

Найдём кол-во беспорядков для $n = 100$: . Пусть α_i - св-во, при кот. $\sigma_i = i$, посчитаем:

$$N = 100!$$

$$N(\alpha_1', \alpha_2', \ldots, \alpha_n') = 100! - 99! * 100 + C_{100}^2 \cdot 98! - \ldots = \sum_{k=0}^{n} C_n^k (n-k)! = !n$$

При раскрытии C-шек, получаем:

$$N(\alpha_1', \ldots, \alpha_n') = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{1}{100!} \approx \frac{1}{e}$$

"Физической интуицией"получаем:

$$\left(1 - \frac{1}{100}\right)^{100} \approx \frac{1}{e}$$

1.1 Циклические n-ти

Алфавит: $X = \{ b_1, \dots, b_r \}$. Из b-шек составляем слова длины n.

$$a_1 a_2 \dots a_n, \forall i, a_i \in X$$

$$a_1 \to a_2 \to a_3 \to \dots \to a_{n-1} \to a_n \to a_1$$

Т. е. $a_1 \dots a_n$ отождествляется с $a_2 \dots a_n a_1$, $a_3 \dots a_n a_1 a_2, \dots$.
Однако r^n - кол-во обычных слов, т. е. n не всегда делит r^n.

Пример.

$$r = 3, X = \{ C, O, H \}, n = 4:$$

Следующие слова нужно поделить на 4:

$$COCH$$

$$OCHC$$

$$CHCO$$

$$HCOC$$

Эти на 2:

$$COCO$$

$$OCOC$$

А это на 1:

$$CCCC$$

Для решение этой задачи, для начала, изучим следующий мощный инструмент:

1.2 Формула обращения Мёбиуса

Теорема 1.1 (ОТА)**.**

$$\forall n \geq 2, \exists! \{ p_1, \dots p_s \}, \{ a_1, \dots a_s \} :$$

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$$

*(Это наз-ся **каноническим разложением** n)*

<u>Определение</u> 1.2. Функция Мёбиуса $\mu(n)$:

$$\mu(n) = \begin{cases} 1, n = 1 \\ (-1)^s, n = p_1 \cdot \ldots \cdot p_s \\ 0, \text{ иначе} \end{cases}$$

<u>Лемма</u> 1.2.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, n = 1 \\ 0, \textit{ иначе} \end{cases}$$

Доказательство. Пусть $n \geq 2 \Rightarrow n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$

$$(d|n) \Rightarrow (d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}, \forall i, 0 \leq \beta_i \leq \alpha_i)$$

$$\sum_{d|n} \mu(d) = \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_k=0}^{\alpha_k} \mu(p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}) = \sum_{\beta_1=0}^{1} \cdots \sum_{\beta_k=0}^{1} \mu(p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k})$$

$$= \mu(1) + C_k^1(-1) + C_k^2(-1)^2 + \ldots + C_k^k(-1)^k = \sum_{i=0}^{k} (-1)^k C_k^i = 0$$

$\square$

<u>Теорема</u> 1.3 (Формула обращения Мёбиуса)**.** *Пусть* $f = f(n)$ *- ф-ция* $n \in \mathbb{N}$. *Пусть* $g(n) = \sum_{d|n} f(d)$. *Тогда:*

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Доказательство.

$$\sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{(d,d')\colon d \cdot d'|n} \mu(d) f(d') = \sum_{d|n} f(d) \sum_{d'|\frac{n}{d}} \mu(d') =$$

$$= f(n) \cdot \sum_{d'|1} \mu(d') + \sum_{d|n, d<n} f(d) \sum_{d'|\frac{n}{d}} \mu(d') = f(n) \cdot 1 + \sum_{d|n, d<n} f(d) \cdot 0 = f(n)$$

$\square$

2 Лекция 10

Вспоминаем задачу:

$$X = \{ b_1, \ldots, b_r \} \text{ - алфавит}$$

$$n, a_1, \ldots, a_n \text{ — линейная последовательность}$$

П-ть r^n:

$$(a_1, \ldots, a_n)$$

Циклический сдвиг $a_1, \ldots, a_n \to a_2, a_3, \ldots, a_n, a_1$

Определение 2.1. Обозначаем как d — **период линейной п-ти**, т. е. min кол-во циклических сдвигов, переводящих её в себя.

Лемма 2.1. $d|n$

Доказательство. Предположим, что $n = kd + r, 1 \leq r < d$. Тогда, сдвинув $a_1, \ldots, a_n$ на d, k раз, получим исходную п-ть. Сдвинув на n 1 раз, тоже получаем исх. п-ть. Отсюда, получаем, что сдвигая $a_1, \ldots, a_n$ на $n - k \cdot d = r$, тоже получ. исх. п-ть. Но $r < d$ — противоречие. □

Лемма 2.2. *$a_1, \ldots, a_n$ - периода d, то она представляется, как $\frac{n}{d}$ одинаковых кусков длины d:*

$$a_1, \ldots, a_n = a_1, \ldots a_d, a_{d+1}, \ldots, a_{2d}, a_{2d+1}, \ldots$$

Доказательство. Очев. □

Пусть V - мн-во всех линейных п-тей сост. из нашего алфавита (т. е. $|V| = r^n$)

$$1 = d_1 < d_2 < d_3 \ldots < d_s = n \text{ - все делители числа } n$$

$$V_i = \{ \{ a_n \} \in V \mid \{ a_n \} \text{ - имеет период } d_i \}$$

$$V = V_1 \sqcup V_2 \sqcup V_3 \sqcup \ldots \sqcup V_s$$

$$\Rightarrow r^n = |V_1| + \ldots + |V_s|$$

Пусть W_i - мн-во лин п-тей длины d_i и периода d_i

$$|W_i| = |V_i|$$

$$\Rightarrow r^n = |W_1| + \ldots + |W_s|$$

Обозначим U_i - мн-во различных цикл. п-тей, кот. отвечают лин. п-тям из W_i. Тогда очевидно, что:

$$\frac{|W_i|}{d_i} = |U_i|$$

Введём обозначение:

$$M(d_i) = |U_i|$$

Получаем:

$$r^n = d_1 M(d_1) + d_2 M(d_2) + \ldots d_s M(d_s)$$

$$r^n = \sum_{d|n} d M(d)$$

Напомним ф-лу обращения Мёбиуса:

$$g(n) = \sum_{d|n} f(d) \Rightarrow$$

$$\Rightarrow f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Получаем:

$$nM(n) = \sum_{d|n} \mu(d) \cdot r^{\frac{n}{d}}$$

$$M(n) = \frac{1}{n} \sum_{d|n} \mu(d) \cdot r^{\frac{n}{d}}$$

Тогда ответ, т. е. кол-во циклических п-тей длины n, представим как теорему:

Теорема 2.3.

$$T_r(n) = \sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \left(\sum_{d'|d} \mu(d') r^{\frac{d}{d'}} \right)$$

2.1 Обращение Мёбиуса на чуме (част. уп. мн-во)

$$\mathscr{P} = (A, \preceq)$$

Локально конечный: $\forall y \in A$

$$|\{\, x \preceq y \,\}| < \infty$$

$$(\mathbb{N}, \leq), (\mathbb{N}, |)$$
$$(2^{\{\,1,2,\ldots,n\,\}}, \subseteq)$$

2.1.1 Ф-ция Мёбиуса

$$x, y \in \mathbb{A}, x \preceq y$$

$$\mu(x, x) = 1$$

$$x \prec y \colon \mu(x, y) = -\sum_{z\colon x \preceq z \prec y} \mu(x, z)$$

Теорема 2.4. *Если $\mu(x, y)$ - это ф-ция Мёбиуса на $(\mathbb{N}, |)$, а $\mu(n)$ - обратная ф-ция Мёбиуса, тогда:*

$$\mu(x, y) = \mu\left(\frac{y}{x}\right)$$

Доказательство.

$$\mu(x, x) = \mu\left(\frac{x}{x}\right) = 1$$

Индукция по величине $\frac{y}{x}$:

$$\mu(x, y) = -\sum_{z\colon x \preceq z \prec y} \mu(x, z) = -\sum_{z\colon x \preceq z \prec y} \mu\left(\frac{z}{x}\right)$$

Распишем $y = x \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Тогда:

$$\frac{z}{x} = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}, \exists i \colon \beta_i < \alpha_i$$

Рассм. несколько случаев:

1) $\alpha_1 = \ldots = \alpha_s = 1$. Тогда:

$$-\sum_{\ldots} \mu\left(\frac{z}{x}\right) = -\sum_{\beta_1=0}^{1} \ldots \sum_{\beta_s=0}^{1} \mu\left(p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\right) + \mu\left(p_1 \cdot \ldots \cdot p_s\right)$$

В рамках док-ва ф-лы обращ. Мёбиуса, страшная сумма слева $= 0$. Получаем:

$$= \mu(p_1 \cdot \ldots \cdot p_s)$$

2) $\exists i\colon \alpha_i > 1$. Тогда всё то же самое, как и в случае 1 (по опр. ф-ции Мёбиуса)

□

Теорема 2.5 (Ф-ла обращения Мёбиуса)**.** *Пусть* $g(y) = \sum_{x \preceq y} f(x)$. *Тогда:*

$$f(y) = \sum_{x \preceq y} \mu(x, y) g(x)$$

Доказательство.

$$\sum_{x \preceq y} \mu(x, y) \cdot g(x) = \sum_{x \preceq y} \mu(x, y) \cdot \sum_{z \preceq x} f(z) = \sum_{(x,z)\colon z \preceq x \preceq y} \mu(x, y) \cdot f(z) =$$

$$= \sum_{z \preceq y} f(z) \left(\sum_{x\colon z \preceq x \preceq y} \mu(x, y) \right) = f(y) + \sum_{z \prec y} f(z) \left(\sum_{x\colon z \preceq x \preceq y} \mu(x, y) \right)$$

Док-во сводится к лемме:

Лемма 2.6.

$$\forall z, y\colon z \prec y$$

$$\sum_{x\colon z \preceq x \preceq y} \mu(x, y) = I_{z=y}$$

□

3 Лекция 11

Лемма 3.1.

$$\sum_{x \preceq z \preceq y} \mu(z, y) = I_{x=y}$$

Доказательство. $x \prec y$
Докажем индукцие по длине самой длинной цепочки вида:

$$x \prec x_1 \prec x_2 \prec \ldots \prec x_k \prec y$$

- База индукции: $x \prec y$, а между ними ничего нет.

$$\sum_{x \preceq z \preceq y} \mu(z, y) = \mu(y, y) + \sum_{x \preceq z \prec y} \mu(z, y) = 1 + \mu(x, y) = 1 - \sum_{x \preceq z \prec y} \mu(x, z) =$$

$$= 1 - \mu(x, x) = 0$$

- Шаг индукции:

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

$$= 1 - \sum_{x \preceq u \prec y} \sum_{x \preceq z \prec u} \mu(z, u) = 1 - \sum_{x \preceq u \prec y} I_{x=u} = 1 - 1 = 0$$

□

Теорема 3.2. ***Формула обращения Мёбиуса:***

$$g(y) = \sum_{x \preceq y} f(x) \Rightarrow f(y) = \sum_{x \preceq y} \mu(x, y) g(x)$$

Пример. *Рассм. чум:*

$$(2^{\{1,2,\ldots,n\}}, \subseteq)$$

Пусть есть ещё некоторые мн-ва $A_1, \ldots, A_n$*. Определим также ф-ции:*

$$I \in 2^{\{1,2,\ldots,n\}}$$

$f(I)$ — кол-во эл-ов мн-в $A_1, \dots, A_n$, к-рые принадлежат всем таким A_i, что $i \notin I$, т. е.:

$$f(I) = \left| \bigcap_{i \notin I} A_i \right|$$

$$f(\{ 1, 2, \dots, n \}) = \left| \bigcup_{i=1}^{n} A_i \right|$$

$g(I)$ — кол-во эл-ов мн-в $A_1, \dots, A_n$, кот-рые принадлежат таким A_i, что $i \notin I$, и не принадлежит всем остальным A_i.

$$f(I) = \sum_{I' \subseteq I} g(I')$$

$$n = 4\colon A_1, \dots, A_4$$

$$I = \{ 1, 2 \}, f(I) = |A_3 \cap A_4|$$

$$(I' \subseteq I) \iff (I' \in \{ \{ 1, 2 \}, \{ 1 \}, \{ 2 \}, \emptyset \})$$

$$g(\{ 1, 2 \}) = |A_3 \cap A_4 \backslash A_1 \backslash A_2|$$

$$g(\{ 1 \}) = |A_2 \cap A_3 \cap A_4 \backslash A_1|$$

$$g(\{ 2 \}) = |A_1 \cap A_3 \cap A_4 \backslash A_2|$$

$$g(\emptyset) = |A_1 \cap A_2 \cap A_3 \cap A_4|$$

$$g(\{ 1, 2, \dots, n \}) = 0$$

Применим ФОМ (ф-лу обращения Мёбиуса):

$$g(I) = \sum_{I' \subseteq I} \mu(I', I) f(I')$$

$$I = \{ 1, 2, \dots, n \} \Rightarrow g(I) = 0 = \sum_{I' \subseteq \{ 1, 2, \dots, n \}} \mu(I', \{ 1, 2, \dots, n \}) \cdot f(I') =$$

<u>Лемма</u> 3.3.

$$\mu(I', \{ 1, 2, \dots, n \}) = (-1)^{|I| - |I'|}$$

Доказательство. Индукция по $|I| - |I'|$:

- Шаг:

$$I' \subset I\colon \mu(I', I) = -\sum_{I' \subseteq I'' \subset I} \mu(I', I'') = -\sum_{I' \subseteq I'' \subset I} (-1)^{|I''| - |I'|}$$

$$|I''| = |I'|\,, |I'| - 1, \ldots, |I| - 1$$

$\Rightarrow$ Кол-во I'' мощности k: $C_{|I|-|I'|}^{k-|I'|}$

$$\Rightarrow -\sum_{I' \subseteq I'' \subset I} (-1)^{|I''|-|I'|} = -\sum_{k=|I'|}^{|I|-1} C_{|I|-|I'|}^{k-|I'|} (-1)^{k-|I'|} = \left[l = |I'|\right] = -\sum_{l=0}^{|I|-|I'|-1} C_{|I|-|I'|}^{l} (-1)^{l} = (0$$

$$= (-1)^{|I|-|I'|}$$

□

$$= \left|\bigcup_{i=1}^{n} A_i\right| + \sum_{I' \subseteq \{\, 1,2,\ldots,n \,\}} (-1)^{n-|I'|} \cdot \left|\bigcap_{i \notin I'} A_i\right|$$

3.1 Линейные рекуррентные соотношения с постоянными коэффициентами

$$F_{n+2} = F_{n+1} + F_n, F_0 = 0, F_1 = 1$$

Последовательность $\{\, y_n \,\}_{n=0}^{\infty}$ удовл. лин. рек. соотношению k-ого порядка с коэф. $a_1, \ldots, a_k \in \mathbb{R}$, если $\forall n$:

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \ldots + a_1 y_{n+1} + a_0 y_n = 0$$

$$k = 1\colon a_1 y_{n+1} + a_0 y_n = 0 \Rightarrow y_n = \left(-\frac{a_0}{a_1}\right) y_0$$

$$k = 2\colon a_2 y_{n+2} + a_1 y_{n+1} + a_0 y_n = 0$$

Алгоритм:

1) Составим ур-е:

$$a_2 x^2 + a_1 x + a_0 = 0$$

$$a_2 (x - \lambda_1)(x - \lambda_2) = 0$$

I) $\lambda_1 \neq \lambda_2$

Теорема 3.4. *1)* $\forall c_1, c_2 \in \mathbb{R}$ *п-ть, задающая ф-лой* $y_n = c_1\lambda_1^n + c_2\lambda_2^n$ *удовл. рекурсии.*

2) *Если* $\{ y_n \}_{n=0}^{\infty}$ *удовл. рек. соотнош., то* $\exists c_1, c_2$:

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n$$

Доказательство. 1)

$$a_2(c_1\lambda_1^{n+2} + c_2\lambda_2^{n+2}) + a_1(c_1\lambda_1^{n+1} + c_2\lambda_2^{n+1}) + a_0(c_1\lambda_1^n + c_2\lambda_2^n) =$$

$$= c_1\lambda_1^n(a_2\lambda_1^2 + a_1\lambda_1 + a_0) + c_2\lambda_2^n(a_2\lambda_2^2 + a_1\lambda_2 + a_0) = 0 + 0 = 0$$

2) Сост. систему:

$$\begin{cases} c_1 + c_2 = y_0 \\ c_1\lambda_1 + c_2\lambda_2 = y_1 \end{cases}$$

$$y_n^* = c_1^*\lambda_1^n + c_2^*\lambda_2^n, c_1^*, c_2^* \text{ - решение системы}$$

По п. 1, это соотнош. удовл. рек. соотнош. $\Rightarrow y_n = y_n^* \Rightarrow$ Победа.

□