

1. Теория множеств

Определение 1. Множество — неопределяемое понятие. В некотором приближении множество — некоторый набор объектов.

Пример 1. $1, 2, 5$ — множество.

Способы задания множеств:

- Перечисление $A = \{1, 2, 5\}$
- Задание свойством или *Set builder notation* $\{n \in \mathbb{N} | 2|n\}$

Замечание. Будем считать, что $0 \in \mathbb{N}$

$\{n \in \mathbb{N} | x > 10, 2|x, n \text{ простое}\} = \text{Множество крокодилов в этой комнате} = \emptyset$

$\{\{\{\emptyset\}, \emptyset\}, \{\emptyset\}, \emptyset\}$

$x \in A$ — x является элементом A .

$B \subset A$, если любой элемент B , лежит в A .

$A = B \Leftrightarrow (B \subset A) \wedge (A \subset B)$

Утверждение.

- $\emptyset \subset A$
- $A \subset A$
- $A \subset B, B \subset C \Rightarrow A \subset C$

Парадокс Рассела

Рассмотрим множество $M = A | A \notin A$. Определим, лежит ли элемент M в множестве M . С одной стороны, если $M \in M$, то $M \notin M$ по построению. Если же $M \notin M$, то по построению $M \in M$. Получили противоречие.

Законы де Моргана

- $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$
- $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

Определение 2. Пара — множество из двух объектов $\{a_1, a_2\}$

Определение 3. Упорядоченная пара — $\{\{a_1, a_2\}, a_i\}$

Определение 4. Декартово произведение множества A на множество B — множество всех упорядоченных пар с первым элементом из A и вторым из B . $A \times B = \{(a, b) | a \in A, b \in B\}$ $A^n = \{(a_1, \dots, a_n) | \forall a_i \in A\}$

Свойство 1. Декартово произведение ассоциативно.

Определение 5. Соответствие между A и B — произвольное подмножество $A \times B$

Определение 6. *Отображение* или *функция* — однозначное соответствие. $\forall a \in A \exists! b \in B (a, b) \in A \times B$

Определение 7. *Инъекция* — несклеивающее отображение $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

Определение 8. *Сюръекция* — накрывающее отображение. $\forall b \in B \exists a \in A f(a) = b$

Определение 9. *Биекция* — взаимно-однозначное соответствие. Иначе говоря, это отображение, являющееся инъекцией и сюръекцией.

Определение 10. *Образ множества* $P \subset A$ при соответствии $F \subset A \times B$ — это $\{b \in B | \exists a \in P (a, b) \in F\}$

Определение 11. *Прообраз множества* $Q \subset B$ при соответствии $F \subset A \times B$ — это $\{a \in A | \exists b \in Q (a, b) \in F\}$

F — инъекция $\Rightarrow P = F^{-1}(F(P))$

$$1) \ P \subset F^{-1}(F(P))$$
$$a \in P \Rightarrow a \in F^{-1}(F(a))$$

$$2) \ F^{-1}(F(P)) \subset P$$
$$a' \in F^{-1}(F(P)), a' \notin P.$$
$$a' \in F^{-1}(F(P)) \Rightarrow F(a') \in F(P) \Rightarrow \exists a \in P F(a') = F(a). \text{ Имеем:}$$
$$a' \neq a, F(a) = F(a') \text{ — противоречие с инъекцией.}$$

Теорема 1. $\forall P P = F^{-1}(F(P)) \Leftrightarrow \forall x \in A F(x) \neq \emptyset, \forall x_1, x_2 \in A x_1 \neq x_2 \Rightarrow F(x_1) \cap F(x_2) = \emptyset$

Определение 12. Пусть $F \subset A \times B$ — соответствие. Тогда *обратное соответствие* — это $F^{-1} \subset B \times A : (b, a) \in F^{-1} \Leftrightarrow (a, b) \in F$

Композиция отображений и соответствий $F : A \rightarrow B, G : B \rightarrow C, H = G \circ F : A \rightarrow C, H(a) = G(F(a))$

Тождественное преобразование (identity) $\text{id}_A : A \rightarrow A$.

Утверждение. Если $F : A \rightarrow B$, то $F \circ \text{id}_A = \text{id}_B \circ F = F$

Утверждение. $F : A \rightarrow B, G : B \rightarrow C, H : C \rightarrow D \Rightarrow H \circ (G \circ F) = (H \circ G) \circ F$

Утверждение. $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$

Упражнение 1. Доказать вышеприведенные утверждения.
Когда $F \circ F^{-1} = \text{id}_B$?

Определение 13. $|A|$ — количество элементов в множестве A .

Упражнение 2. • \exists инъекция из A и $B \Leftrightarrow |A| \leq |B|$

• \exists сюръекция из A и $B \Leftrightarrow |A| \geq |B|$

• \exists биекция из A и $B \Leftrightarrow |A| = |B|$

Определение 14. A и B равномощны ($A \cong B$), если существует биекция из A и B .

Примеры:

• $\mathbb{N} \cong \{x \in \mathbb{N} | x — \text{четное}\}$

• $[0, 1] \cong [0, 2]$

• $(0, 1) \cong \mathbb{R}$

Свойства:

1) $A \cong A$ (рефлексивность)

2) $A \cong B \Leftarrow B \cong A$ (симметричность)

3) $A \cong B, B \cong C \Leftarrow A \cong C$ (транзитивность)

Определение 15. A не более мощно чем B , если существует $B_1 \subset B$, такое что $A \cong B_1$. Обозначение: $A \leq B$.

Примеры:

$$\bullet \mathbb{N} \leq [0, 1]. \quad X = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots \cong \mathbb{N}$$

Свойства:

- 1) $A \leq A$ (рефлексивность)
- 2) $A \leq B \Leftarrow B \cong A$
- 3) $\emptyset \leq A$
- 4) $A \leq B, B \leq C \Leftarrow A \leq C$ (транзитивность)

Теорема 2. Теорема Кантора-Бернштейна Если $A \leq B$ и $B \leq A$, то $A \cong B$

Доказательство. $A \cong B_1 \subset B$. $f: A \mapsto B_1$ — биекция

$B \cong A_1 \subset A$. $g: B \mapsto A_1$ — биекция

$A_2 = g(B_1)$, $A_2 \subset A_1$. $A_1 \cong B_1 \cong A \Rightarrow A_2 \cong A$

Надо: $A \cong B$

Достаточно оказать: $A \cong A_1$

Переформулируем:

Дано: $A_2 \subset A_1 \subset A$, $A_0 \cong A_2$; доказать: $A_0 \cong A_1$

$h: A \mapsto B$ — биекция. Пусть $A_i = h(A_{i-2})$. Тогда $A_{i+1} \subset A_i$

Пусть $C_i = A_i$

$A_{i+1} \subset C = \bigcap_{i=0}^{\infty} A_i$. $A_j = \bigcup_{i=j} C_i \cup C$. Заметим, что $A_i \cup C_j = \emptyset$, $C \cup C_i = \emptyset$.

$h(C_i) = h(A_i)$

$A_{i+1} = h(A_i)$

$h(A_{i+1}) = A_{i+2}/A_{i+3} = C_{i+2}$. Получили $h(C_i) = C_{i+2}$

$A_0 = \bigcup_{i=0} C_i \cup C$.

$A_1 = \bigcup_{i=1} C_i \cup C$.

Сделаем такую биекцию: Все нечетные слои оставляем на месте, все четные "сдвигаем" на один шаг.

$k(x) = h(x)$, если $x \in (C_0 \cup C_2 \cup C_4 \cup \dots)$; x если $x \in (C_1 \cup C_3 \cup \dots) \cup C$

□

Определение 16. A счетно, если A равномощно множеству натуральных чисел.

Утверждение. Если A счетно, то $A \cup a_i$ — счетно

Утверждение. Если A и B счетно, то $A \cup B$ — счетно

Следствие 1. \mathbb{Z} — счетно.

Утверждение. Если A и B счетны, то $A \times B$ счетно.

Теорема 3. Объединение счетного числа счетных множеств счетно.

Доказательство. • Множества A_0, A_1, A_2, \dots попарно не пересекаются. Доказательство аналогично

- Общий случай: $A_0 \subset A_0 \cup A_1 \cup \dots \subset B_0 \cup B_1 \cup B_2$, где $B_i = A_i \times i$; $B_i \cong A_i$, $B_i \cap B_j = \emptyset$. Используй теорему Кантора-Бернштейна, Люк!

□

Теорема 4. Теорема Кантора Множество всех бесконечных последовательностей 0 и 1 несчетно.

Доказательство. Пусть оно счетно. f_0, f_1, \dots — все последовательности. Рассмотрим d , такое что $d[n] = f_n[n]$. Рассмотрим \bar{d} , такое что $\bar{d}[n] = 1 - d[n]$. С одной стороны, она должна быть в f по предположению. Пусть $\bar{d} = f_k$. Тогда $f_k(k) = \bar{d}[k] = 1 - f(k)[k]$. Противоречие. Значит d не лежит в f . Значит предположение и неверно это множество несчетно. □

Обозначение. $2^A = B | B \subset A$

Обозначение. $X < Y$, если $X \leq Y$ и $X \not\cong Y$

Теорема 5. Теорема Кантора в общем виде $A < 2^A$

Доказательство. $A \leq 2^A$, т.к. $A \cong B = \{\{x\} | x \in A\}$. Пусть A равномощно 2^A . Тогда есть биекция из A в 2^A . Можно рассмотреть вопрос о том, правда ли, что $x \in f(x)$. Рассмотрим $D = \{x \in A | x \notin f(x)\} \subset A$. Поскольку это биекция, то $D = f(d)$. Вопрос в том, правда ли, что $d \in f(d)$. Пусть $d \in f(d) \Rightarrow d \in D \Rightarrow d \notin f(d)$. Пусть $d \notin f(d)$. Тогда $d \in D$ по определению D . Но значит $d \in f(d)$. □

1. Предикаты

Определение 17. Пусть есть множество α . Предикатом валентности k на множестве α называется любое подмножество A^k (или любая функция из A^k в $\{0, 1\}$).

Если $k = 1$, то предикат называют свойством.

Если $k = 2$, то предикат называют отношением.

Есть всего два

Обозначение. Произвольное отношение обозначают R . Вместо $(x, y) \in R$ пишут xRy

Определение 18. Свойства отношений

- Рефлексивность: $\forall x : xRx$
- Антирефлексивность: $\forall x : \neg xRx$
- Симметричность: $\forall x, y : xRy \Rightarrow yRx$
- Антисимметричность: $\forall x, y : xRy, yRx \Rightarrow x = y$
- Транзитивность: $\forall x, y, z : xRy, yRz \Rightarrow xRz$
- Полнота: $\forall x, y : xRy \vee yRx$

Определение 19. Отношение R называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Теорема 6. Основная теорема отношения эквивалентности

Если \sim — отношение эквивалентности на множестве A , то A представляется в виде непересекающихся классов эквивалентности.

Доказательство. 1) $K_x = \{y \mid y \sim x\}$ — класс эквивалентности одного элемента.

2) $x \in K_x$ (из рефлексивности)

3) Если есть $x \in K_y \Rightarrow y \in K_x$ (из симметричности)

4) $\forall y, z : y, z \in K_x \Leftrightarrow y \sim z$ (из транзитивности)

5) либо $K_x = K_y$, либо $K_x \cap K_y = \emptyset$

□

Определение 20. Отношение R называется отношением (частичного) порядка, если оно рефлексивно, антисимметрично и транзитивно.

Определение 21. Порядок называется линейным, если любые два элемента сравнимы.

Определение 22. Упорядоченное множество — пара множество и отношение порядка на нем

Определение 23. (A, \leq_A) — упорядоченное множество.

$x \in A$ — наибольший элемент, если $\forall y : \leq_a x$

$x \in A$ — максимальный элемент, если $\forall y \in A : x \leq_a y \Rightarrow x = y$

2. Комбинаторика

Определение 24. Правило сложения

Если есть два набора объектов, причем в первом N объектов a_1, \dots, a_n , во втором M объектов b_1, \dots, b_m . Тогда есть $N + M$ способов выбрать объект либо из первого множества, либо из второго.

Определение 25. Правило умножения

Если есть два набора объектов, причем в первом N объектов a_1, \dots, a_n , во втором M объектов b_1, \dots, b_m . Тогда есть NM способов выбрать объект сначала из первого множества, затем из второго.

Определение 26. Принцип Дирихле

Если есть N ящиков и $N + 1$ кролик, то для любой рассадки кроликов по ящикам найдется ящик, в котором находится не менее двух кроликов.

Пример 2. Возьмем квадрат на плоскости со стороной 2 и случайно кинем в него 5 точек. Тогда среди этих 5 точек есть такие две, расстояние между которыми не превосходит $\sqrt{2}$. Рассмотрим разбиение этого квадрата на четыре непересекающихся квадрата со стороной 1. Тогда согласно принципу Дирихле, в одном маленьком квадрате есть две точки. Очевидно, что расстояние между ними не превосходит диагонали маленьком

Пример 3. Пусть есть множество \mathcal{R} , состоящее из 20 натуральных чисел от 1 до 20. Выберем 15 различных подмножеств \mathcal{R} мощности 5: M_1, M_2, \dots . Рассмотрим множество этим множеств $\mathcal{M} = M_1, M_2, \dots, M_{15}$. Верно ли, что для любого \mathcal{M} найдется такая раскраска элементов множества \mathcal{R} в два цвета так, что каждое множество $M_i \in \mathcal{M}$ не одноцветно, то есть содержит оба цвета?

Теорема 7. *Теорема о раскраски гиперграфа*

Ответ на поставленный вопрос положителен, то есть для любой $\mathcal{M} = \{M_1, \dots, M_{15}\}$, $|M_i| = 5$, $M_i \in \mathcal{R}$

Доказательство. Зафиксируем $\mathcal{M} = \{M_1, \dots, M_{15}\}$. По правилу умножения всего двуцветных раскрасок \mathcal{R} есть 2^{20} . Раскрасок, в которой множество M_1 одноцветно — 2^{16} , так как есть 15 элементов вне множества M_1 , которые мы можем покрасить как угодно, и само множество M_1 мы можем покрасить двумя способами. Посчитаем количество раскрасок, в котором одноцветно хотя бы одно из M_i . Очевидно, что количество таких раскрасок не превосходит $15 \cdot 2^{16} < 16 \cdot 2^{16} = 2^{20}$. Так как плохих раскрасок меньше чем количество всего раскрасок, то надется хотя бы одна хорошая раскраска. \square

Числа размещений, сочетаний, перестановок и прочее

Пусть $A = \{a_1, \dots, a_n\}$. Можно составлять упорядоченные последовательности элементов A . А можно извлекать объекты "кучами" то есть без учета порядка. Если мы рассматриваем A как упорядоченную последовательность, то говорят о *размещении* объектов. Если же мы извлекаем объекты без учета порядка, то говорят о *сочетании* объектов. Бывают размещения с повторениями и без повторений. Аналогично, сочетания бывают с повторениями и без повторений.

Будем говорить о k -сочетании и k -размещении, если в сочетании(размещении) ровно k объектов.

Пусть дано множество объектов $\{a_1, \dots, a_n\}$. Обозначим через \overline{A}_n^k число всех k -размещений с повторениями и A_n^k число всех k -размещений без повторения. Аналогично обозначим \overline{C}_n^k и C_n^k число k -размещений с повторениями и без повторений соответственно.

Теорема 8. $\overline{A}_n^k = n^k$

Доказательство. На первую позицию нашего размещения можно поставить любой из n объектов. Как, впрочем, и на все остальные. Тогда по правилу умножения получаем n^k \square

Теорема 9. $A_n^k = \frac{n!}{(n-k)!}$

Доказательство. На первую позицию нашего размещения можно поставить любой из n объектов. На вторую — все, кроме того, который мы

поставили на первую позицию, то есть любой из $n - 1$ объектов. Иначе говоря, на i -тую позицию можно поставить объект $n - i$ способами. То есть $A_n^k = n(n - 1)(n - 2) \dots (n - k + 1) = \prod_{i=0}^{k-1} n - i = \frac{n!}{(n-k)!}$ \square

Теорема 10. $C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$

Доказательство. Каждому k -сочетанию без повторений соответствует $k!$ различных размещений без повторения. То есть $k!C_n^k = A_n^k$, откуда следует, что $C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$ \square

Теорема 11. $\overline{C}_n^k = C_{n+k-1}^k$

Доказательство. Рассмотрим исходное множество объектов a_1, \dots, a_n . Каждому k -сочетанию с повторениями поставим в соответствие некоторую последовательность из нулей и единиц. Ставить в соответствие последовательность из нулей и единиц мы будем по следующему алгоритму: пусть дано k -сочетание с повторениями. Рисуем в нашу последовательность столько единиц, сколько раз нам встретился элемент a_i , после этого рисуем ноль, если это не был последний, n -ый объект, и так делаем последовательно n раз для каждого i от 1 до n . Всего у нас в нашей последовательности k единиц, так как каждому элементу, входящему в наше сочетание с повторениями соответствует ровно одна единица и $n - 1$ единиц. Утверждается, что между такими 0, 1 векторами длины $n - k + 1$ с k единицами и сочетаниями с повторениями установилась биекция. Но количество таких последовательностей из нулей и единиц это число способов зафиксировать ровно k позиций среди $n - k + 1$, а как известно, это количество равно C_n^k \square

Упражнение 3. Есть n символов из которых n_i раз встречается символ a_i . Сколько существует различных последовательностей символов?

Определение 27. $P(n_1, \dots, n_k)$ — число различных последовательностей, которые можно составить из наших символов, если задействовать их все.

Теорема 12. $P(n_1, \dots, n_k) = \frac{n!}{n_1!n_2!\dots n_k!}$

Доказательство. У нас есть всего n позиций. Для a_1 нужно n_1 позиций и есть $C_n^{n_1}$ способов зафиксировать нужные позиции. Для символа a_2 нужно n_2 позиций и остальность $n - n_1$ свободных позиций, То есть $P(n_1, \dots, n_k) = C_n^{n_1} C_{n-n_1}^{n_2} C_{n-n_1-n_2}^{n_3} \dots = \frac{n!}{n_1!(n-n_1)!} + \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} + \dots = \frac{n!}{n_1!n_2!\dots n_k!}$ \square

Теорема 13. *Бином Ньютона* $(x + y)^n = \sum_{k=0}^n C_n^k x^k y^{n-k}$

Доказательство. $(x + y)^n = (x + y)(x + y) \dots (x + y)$. Из каждой скобки надо взять либо x , либо y . Пусть из k скобок мы взяли x , то есть из остальных $n - k$ скобок мы взяли y . Но мы выбрать k скобок можем выбрать C_n^k способами, то есть $x^k y^{n-k}$ встречается C_n^k раз, то есть $(x + y)^n = \sum_k C_n^k x^k y^{n-k}$ \square

Замечание. C_n^k также называются биномиальными коэффициентами и в западной традиции пишут $\binom{n}{k}$

Теорема 14. *Полиномиальная формула*

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{(n_1, n_2, \dots, n_k): n_i \in \mathbb{N}, \sum n_i = n} P(n_1, n_2, \dots, n_k) x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$$

Доказательство. Возьмем n_1 скобок из которых извлекается x_1 , n_2 из которых извлекается x_2 , \dots , n_k скобок, из которых извлекается x_k . Очевидно, что $x_i \in \mathbb{N}$, $\sum n_i = n$. Тогда в произведении получится $x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$. Этот моном встретится в $P(n_1, n_2, \dots, n_k)$ раз в качестве слагаемого, т.к. число способов выбрать скобки для x_1 равно $C_n^{n_1}$, для x_2 остается $n - n_1$ свободных скобок, то есть количество способов выбрать x_2 равно $C_{n-n_1}^{n_2}$, и так далее. А как известно, произведение таких биномиальных коэффициентов равно $P(n_1, n_2, \dots, n_k)$. \square

Замечание. Числа $P(n_1, n_2, \dots, n_k)$ называются *полиномиальными* коэффициентами

Комбинаторные тождества:

- $C_n^k = C_n^{n-k}$
- $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$
- $\sum_{i=0}^n C_n^i = 2^n$

Доказательство. $\sum_{i=0}^n C_n^i = (1 + 1)^n = 2^n$ \square

- $\sum_{(n_1, n_2, \dots, n_k): n_i \in \mathbb{N}, \sum n_i = n} P(n_1, n_2, \dots, n_k) = k^n$

- $\sum_{i=0}^n (C_n^i)^2 = C_{2n}^n$

Доказательство. $A = \{a_1, \dots, a_{2n}\}$. V — множество всех n -сочетаний из A . $|V| = C_{2n}^n$. $V = \bigsqcup_{i=0}^n V_i$, где V_k — множество тех n -сочетаний, которые содержат ровно k из первых n элементов, то есть C_n^k способов выбрать k элементов из первых n элементов и C_{n-k}^{n-k} способов выбрать оставшиеся $n-k$ элементов из последних n элементов. То есть $|V_k| = C_n^k C_{n-k}^{n-k} = (C_n^k)^2$. $|V| = \sum |V_i| \Leftrightarrow C_{2n}^n = \sum_{i=0}^n (C_n^i)^2$ \square

- $\forall n, m : C_{n+m}^n = \sum_{i=n-1}^{n+m-1} C_i^{m-1}$

Доказательство. Рассмотрим $A = \{a_1, \dots, a_n, a_{n+1}\}$. V — множество всех m -сочетаний с повторениями из A . $|V| = C_{n+1+m-1}^m = C_{n+m}^m$. Пусть V_k это те сочетания из V , в которые объект a_1 входит ровно k раз. Осталось оценить $|V_k|$. В любое сочетание из V_k k раз встречается элемент a_1 и в этом сочетании еще есть $m-k+1$ "свободных" мест, на котором стоят остальные n элементов. То есть количество элементов в V_k равно количеству $sm-k+1$ -сочетаний с повторениями их n элементов. То есть $|V_k| = C$ \square

Следствие 2. Если мы возьмем $n = 1$ и подставим в тождество, то мы получим $C_{m+1}^1 = C_m^0 + C_{m-1}^0 + \dots + C_0^0$

Следствие 3. Если $n = 2$, то $C_{m+2}^2 = C_{m+1}^1 + C_m^1 + \dots + C_1^1 \Leftrightarrow \frac{(m+2)(m+1)}{2} = (m+1) + m + (m-1) \dots 1$

Следствие 4. Если $n = 3$, то $C_{m+3}^3 = C_{m+2}^2 + C_{m+1}^2 + \dots + C_2^2 \Leftrightarrow \frac{(m+1)(m+2)(m+3)}{6} = \frac{9(m+1)(m+2)}{2} + \frac{m(m+1)}{2} + \dots + \frac{1 \cdot 2}{2} = \frac{1}{2}(1^2 + 2^2 + \dots + (m+1)^2) + \frac{1}{2}(1 + 2 + \dots + (m+1)) \Rightarrow \frac{1}{2}(1^2 + 2^2 + \dots + (m+1)^2) = \frac{(m+1)(m+2)(m+3)}{6} - \frac{1}{4}(m+1)(m+2) = \frac{1}{12}(m+1)(m+2)(2m+3)$

1. Формула включения-исключения

Рассмотрим произвольное N объектов a_1, a_2, \dots, a_N . Выделим некоторые свойства $\alpha_1, \alpha_2, \dots, \alpha_N$, которые могут быть присущи некоторым объектам.

Обозначение. Пусть $N(\alpha_i)$ — количество объектов, обладающих свойством α_i , $N(\alpha_i, \alpha_j)$ — количество объектов, обладающих свойствами α_i и α_j одновременно.

Обозначение. α'_i — отрицание свойства α_i

Теорема 15. $N(\alpha'_1, \alpha'_2, \dots, \alpha'_n) = N - N(\alpha_1) - N(\alpha_2) - \dots - N(\alpha_n) + N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + \dots + N(\alpha_{n-1}, \alpha_n) - N(\alpha_1, \alpha_2, \alpha_3) + \dots + (-1)^n N(\alpha_1, \alpha_2, \dots, \alpha_n)$

Доказательство. Докажем индукцией по n

База индукции: $\forall N \forall a_1, \dots, a_N \forall \alpha_i N(\alpha'_i) = N - N(\alpha_i)$

Предположение: $\forall N \forall a_1, \dots, a_N \forall \alpha_1, \dots, \alpha_n$ выполняется утверждение теоремы.

Шаг индукции: $\forall N \forall a_1, \dots, a_N \forall \alpha_1, \dots, \alpha_{n+1}$ выполнено утверждение теоремы.

Зафиксируем произвольные $N, a_1, \dots, a_N, \alpha_1, \dots, \alpha_n$. Рассмотрим все из наших объектов, которые обладают свойством α_{n+1} . Обозначим их $\{b_1, b_2, \dots, b_M\} \subset \{a_1, \dots, a_N\}$, где $M = N(\alpha_{n+1})$. Применим предположение индукции к объектам $\{b_1, \dots, b_M\}$ и свойствам $\{\alpha_1, \dots, \alpha_n\}$. $M(\alpha'_1, \dots, \alpha'_n) = M - M(\alpha_1) - \dots - M(\alpha_n) + M(\alpha_1, \alpha_2) + \dots + (-1)^n M(\alpha_1, \dots, \alpha_n)$.
 $N(\alpha'_1, \alpha'_2, \dots, \alpha'_n, \alpha_{n+1}) = N(\alpha_{n+1}) - \dots - N(\alpha_1, \alpha_{n+1}) - \dots - N(\alpha_n, \alpha_{n+1}) + \dots + (-1)^n N(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$. Применим предположение индукции к множеству $\{a_1, \dots, a_N\}$ и свойствам $\{\alpha_1, \dots, \alpha_n\}$ $N(\alpha'_1, \dots, \alpha'_n) = N - N(\alpha_1) - \dots - N(\alpha_n) + N(\alpha_1, \alpha_2) + \dots + (-1)^n N(\alpha_1, \dots, \alpha_n)$.

Вычтем полученные утверждения: $N(\alpha'_1, \dots, \alpha'_n) - N(\alpha'_1, \dots, \alpha'_n, \alpha_{n+1}) = N(\alpha'_1, \dots, \alpha'_n, \alpha_{n+1}) - N(\alpha'_1, \dots, \alpha'_n, \alpha_{n+1}) + N(\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1})$
 $N(\alpha'_1, \dots, \alpha'_n, \alpha_{n+1}) = N - N(\alpha_1) - \dots - N(\alpha_n) - N(\alpha_{n+1}) + \dots + (-1)^{n+1} N(\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1})$
□

Еще один вариант формулы включения-исключения. Рассмотрим множества S_1, \dots, S_n . Тогда $|S_1 \cup \dots \cup S_n| = |S_1| + |S_2| + \dots + (-1)^{n+1} |S_1 \cap S_2 \cap \dots \cap S_n|$

Пара занкопеременных тождеств

- $C_n^0 - C_n^1 + \dots + (-1)^n C_n^n = 0$ для всех $n \geq 1$, и равно 0 при $n = 0$
- Рассмотрим множество $\{a_1, \dots, a_n\}$, $m < n$. Пусть V - множество всех m -размещений с повторениями из A . $|V| = n^m$. Скормим множество V со m свойствами "не содержать i -й символ. $N(\alpha'_1, \dots, \alpha'_n) = 0$, так как $m < n$. $N(\alpha_i) = (n-1)^m$, $N(\alpha_i, \alpha_j) = (n-2)^m$. В итоге получаем тождество: $0 = C_n^0 n^m - C_n^1 (n-1)^m + C_n^2 (n-2)^m + \dots + (-1)^n C_n^n (n-n)^m$

Циклические последовательности и формула обращения Мебиуса

Есть алфавит $X = \{b_1, \dots, b_n\}$ — алфавит. Назовем обычное слово a_1, a_2, \dots, a_n составленным из символов алфавита линейным и будем обозначать его $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_n$. Циклическое слово (a_1, a_2, \dots, a_n) — это циклическое слово. Все повороты циклического слова превращают его в себя. Спрашивается, сколько есть различных циклических слов. Обозначим его $T(n)$ — число различных циклических комбинаций.

Определение 28. Число p называется простым, если $p \neq 1$ и у него нет делителей, кроме 1 и p .

Теорема 16. Основная теорема арифметики

Пусть $n \geq 2$. Тогда существует единственное разложение числа n на простые. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ (p_i — попарно различные простые).

Определение 29. Функция Мёбиуса $\mu(n)$

Обозначение. $d|n \Leftrightarrow d$ делит n

Лемма 1. $\sum_{d|n} \mu(d) = 1, n = 1, 2, n \geq 2$

Доказательство.

- Если $n = 1$, то $\sum_{d|n} \mu(d) = 1$
- $n \geq 2 \Rightarrow n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$
 $d|n \Leftrightarrow d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}, \forall i: \beta_i \leq \alpha_i$
 $\sum_{d|n} = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \dots \sum_{\beta_s=0}^{\alpha_s} \mu p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s} = \sum_{\beta_1=0}^1 \sum_{\beta_2=0}^1 \dots \sum_{\beta_s=0}^1 \mu p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s} =$
 $\sum_{\beta_1=0}^1 \sum_{\beta_2=0}^1 \dots \sum_{\beta_s=0}^1 (-1)^{\sum \beta_i} = \sum_{(\beta_1, \beta_2, \dots, \beta_n), \forall i \beta_i \in \{0,1\}} (-1)^{\sum \beta_i} = C_n^0 -$
 $C_n^1 + \dots = 0$

□

Теорема 17. Формула обращения Мебиуса

Пусть $\forall n \in \mathbb{N}: f(n) = \sum_{d|n} g(d)$. Тогда $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$.

Доказательство. $g(n) = \sum_{d|n} \mu(d) (\sum_{d'|\frac{n}{d}} g(d')) = \sum_{d|n} g(d) \cdot (\sum_{d'|\frac{n}{d}} \mu(d')) = g(n) \cdot$

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

□

Обозначение. $T_r(n)$ — количество циклических последовательностей длины n над алфавитом из r символов.

Теорема 18. $T_r(n) = \sum_{d|n} \frac{1}{d} \left(\sum_{d'|\frac{n}{d}} \mu(d') r^{\frac{d}{d'}} \right)$

Определение 30. Назовем циклическим сдвигом линейного слова $a_1 a_2 \dots a_n$ назовем $a_2 a_3 \dots a_n a_1$.

Замечание. Если применить циклический сдвиг к данному линейному слову n раз, то получится то же самое линейное слово.

Определение 31. Период линейного слова — это минимальное число $d > 1$: после d циклических сдвигов слово переходит в себя.

Лемма 2. Период любой линейной последовательности длины n является делителем n .

Лемма 3. Любая линейная последовательность длины n и периода d имеет вид $a_1 a_2 a_3 \dots a_d a_1 a_2 \dots a_d \dots a_1 a_2 \dots a_d$. ($\frac{n}{d}$ одинаковых блоков по d символов)

Замечание. Каждый из $\frac{n}{d}$ блоков — это множество слов длины d и периодом d .

Замечание. Между множеством всех слов длины n и периода d и множеством всех слов длины d и периода d есть биекция.

Пусть V — множество всех линейных слов длины n над алфавитом X . $|V| = r^n$. Пусть d_1, d_2, \dots, d_m — все делители n . Тогда $V = V(d_1) \sqcup V(d_2) \sqcup \dots \sqcup V(d_m)$. Тогда $|V| = |V(d_1)| + |V(d_2)| + \dots + |V(d_m)|$.

Пусть $W(d_i)$ — множество всех линейных слов длины d_i и периода d_i . $r^n = |W(d_1)| + |W(d_2)| + \dots + |W(d_m)|$

$U(d_i)$ — множество всех различных циклических слов, которые получаются из линейных слов $W(d_i)$. $|U(d_i)| = \frac{|W(d_i)|}{d_i}$. Тогда $r^n = d_1 |U(d_1)| + d_2 |U(d_2)| + \dots + d_m |U(d_m)|$. $r^n = \sum_{d|n} d |U(d)|$. Обозначим $f(n) = r^n$, $g(n) =$

$$n |U(n)|. \text{ Тогда } f(n) = \sum_{d|n} g(d) \Rightarrow g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \Leftrightarrow n |U(n)| = \sum_{d|n} \mu(d) r^{\frac{n}{d}} \Leftrightarrow |U(n)| = \frac{1}{n} \sum_{d|n} \mu(d) r^{\frac{n}{d}}.$$

Но $|U(n)|$ — это число циклических слов, полученных из линейных с периодом n . Следовательно $T_r(n) = \sum_{d|n} |U(d)| = \sum_{d|n} \frac{1}{d} \left(\sum_{d'|\frac{n}{d}} \mu(d') r^{\frac{d}{d'}} \right)$

2. Общая теория обращения Мёбиуса

Рассмотрим частично упорядоченное множество $\mathcal{P} = p_1, p_2, \dots$, с отношением порядка \preceq , такое что $\forall i |\{x, x \preceq p_i \mid |\} < \infty$

Пример 4.

- 1) $\mathcal{P} = (\mathbb{N}, " \preceq - " \leq)$
- 2) $\mathcal{P} = (\mathbb{N}, "x \preceq y - "x|y")$
- 3) $\mathcal{P} = (2^{1,2,\dots,n}, " \preceq - " \subseteq)$

Определение 32. *Общая функция Мёбиуса:*

- 1) $\forall x \in \mathcal{P} : \mu(x, x) = 1$
- 2) $\forall x, y \in \mathcal{P}, x \prec y : \mu(x, y) = - \sum_{z: x \preceq z \prec y} \mu(x, z)$

Рассмотрим $\mu(1, n)$ при $\mathcal{P} = (\mathbb{N}, "x \preceq y - "x|y")$

- $\mu(1, 1) = 1 = \mu(1)$
- p — простое. Тогда $\mu(1, p) = - \sum_{z: 1 \preceq z \prec p} \mu(1, z) = - \sum_{d: d|n} \mu(1, d) = -1.$
- $\mu(1, p_1 p_2 \dots p_s) = - \sum_{d: d|n} \mu(1, d) = - \sum_{d: d|p_1 \dots p_s, d \neq p_1 \dots p_s} \mu(1, d) = 1 - C_s^1 + C_s^2 \dots + (-1)^{s-1} C_s^{s-1} = (-1)^s C_s^s = (-1)^{s+1}$
- $\mu(1, p^2) = -(\mu(1, 1) + \mu(1, p)) = 0$
- $\mu(1, p^k) =$

Теорема 19. *Формула обращения Мёбиуса* Пусть \mathcal{P} — частично упорядоченное множество, пусть $g : \mathcal{P} \mapsto \mathcal{X}$, и $f(y) = \sum_{x \prec y} g(x)$. Тогда

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

Рассмотрим S_1, \dots, S_n . Тогда чум $\mathcal{P} = \left\{ \bigcap_{i \in I, I \subseteq \{1, 2, \dots, n\}} S_i \right\}$. Пусть $P_i = \bigcap_{i \in I_1} S_i$, $P_2 = \bigcap_{i \in I_2} S_i$ $P_i \preceq P_j \Leftrightarrow I_1 \supseteq I_2$.

$$g(P) := |P|$$

Определим $f(P)$ как количество элементов множества P , которые не принадлежат ни одному P' , такому что $P' \prec P$.

$$g(p) = \sum_{P' \preceq P} f(P')$$

Применим формулу обращения Мёбиуса $f(p) = \sum_{P' \preceq P} \mu(p', p) |p'|$.

В качестве P возьмем $S_1 \cup \dots \cup S_n$. $f(S_1, \dots, S_n) = 0$

$$P' \preceq P \Leftrightarrow P' = \cap_{i \in I} S_i; I \in \{1, 2, 3, \dots, n\}$$

$$\mu(S_i, P) = - \sum_{S_i \preceq P' \prec P} \mu(S_i, P') = -\mu(S_i, S_i) = -1$$

$|I| = 2$. Тогда $\mu(S_i \cap S_j, P) = -(\mu(S_i \cap S_j, S_i) + \mu(S_i \cap S_j, S_j) + \mu(S_i \cap S_j, S_i \cap S_j)) = -(-1 + (-1) + 1) = 1$.

Аналогично можно доказать по индукции $\mu(\bigcap_{i \in I} S_i, P) = (-1)^{|I|}$

Формула включения-исключения!!!1111

3. Разбиения чисел на слагаемые

Определение 33. $f(N; n_1, n_2, \dots, n_k)$ — количество попарных разбиений числа на слагаемые, т.е. таких которые учитывают порядок слагаемых.

Определение 34. $F(N; n_1, n_2, \dots, n_k)$ — количество попарных разбиений числа на слагаемые, которые не учитывают порядок слагаемых.

Теорема 20. $f(N; n_1, \dots, n_k) = \sum_i f(N - n_i; n_1, \dots, n_k)$

Определение 35. Количество разбиений числа N на слагаемые обозначается $\varphi(N)$ и равно $f(N, 1; 2, 3, \dots, N)$

Теорема 21. $\varphi(N) = 2^{N-1}$

Доказательство. Доказательство по индукции: $\varphi(0) = 1$, $\varphi(N+1) = f(N+1, 1, \dots, N+1) = f(N; 1, \dots, N+1) + \dots + f(1; 1, \dots, N+1) + f(0; 1, \dots, N+1) + f(0; 1, \dots, N+1) = \varphi(N) + \dots + \varphi(1) + \varphi(0) = 2^{N-1} + \dots + 2^1 + 2^0 + 1 = 2^N$ \square

Теорема 22. $F(N; n_1, \dots, n_k) = F(N - n_1; n_1, \dots, n_k) + F(N, n_2, \dots, n_k)$

Определение 36. $p(N) = F(N; 1, \dots, N)$

Теорема 23. Теорема Харди и Рамануджана $p(N) \cong \frac{1}{4N\sqrt{3}} e^{\pi\sqrt{\frac{2}{3}N}}$

Определение 37. Диаграммы Юнга

$N = n_1 + n_2 + \dots + n_k$. Можно считать, что $n_1 \geq n_2 \geq \dots \geq n_k$

Теорема 24. Количество разбиений N на не более чем k слагаемых равно количеству разбиений $N + k$ на ровно k слагаемых

Теорема 25. Количество разбиений N на не более чем k слагаемых равно количеству разбиений $N + \frac{k(k-1)}{2}$ на ровно k различных слагаемых

Доказательство. Сольем каждую диаграмму с диаграммой $1 + 2 + 3 + \dots + k$. В новой диаграмме k строк и $N + \frac{k(k-1)}{2}$ точек. \square

$$(1-x)(1-x^2)(1-x^3)\dots(1-x^n)\dots = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \dots$$

Теорема 26. Если $N = \frac{3k^2 \pm k}{2}, k \in \mathbb{N}$, то коэффициент при x равен $(-1)^k$. Если $N \neq \frac{3k^2 \pm k}{2}$, то коэффициент при x^N равен нулю.

Теорема 27. Пусть $N_{\text{чет}}$ — число помидорных разбиений на четное число различных слагаемых. $N_{\text{нечет}}$ определяется аналогично. Если $N = \frac{3k^2 \pm 1}{2}$, то ;;

4. Формальные степенные ряды

Определение 38. Назовем $A = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + \dots$ формальным степенным рядом с коэффициентами $\{a_i\} \in \mathbb{R}$.

Определение 39. Пусть A и B два формальных степенных ряда. Назовем их суммой формальный степенной ряд C с коэффициентами $c_i = a_i + b_i$.

Определение 40. Пусть A и B два формальных степенных ряда. Назовем их произведением формальный степенной ряд C с коэффициентами $c_i = \sum_{j=0}^i a_j \cdot b_{i-j}$.

Определение 41. Пусть A и B два формальных степенных ряда. Назовем их отношением формальный степенной ряд C , если $A = BC$.

$$\begin{aligned} b_0 c_0 = a_0 &\Rightarrow c_0 = \frac{a_0}{b_0} \\ b_1 c_0 + b_0 c_1 = a_1 &\Rightarrow c_1 = \frac{a_1 - b_1 c_0}{b_0} \\ \dots \end{aligned}$$

5. Производящая функция

Определение 42. Пусть есть последовательность чисел a_0, a_1, a_2, \dots . Её производящая функция — ряд $a_0 + a_1x + a_2x^2 + \dots$. Хочется научиться понимать какой смысл принимает это выражение

Обозначение. $A(x) = \sum_{n=0}^{\infty} a_n x^n$

Определение 43. Ряд $A(x)$ имеет значение A в точке $x \in \mathbb{R}$, если $\lim_{k \rightarrow \infty} \sum_{n=0}^k a_n x^n = A$.

Вопрос — при каких условиях на $x \in \mathbb{R}$ такой предел существует.

Теорема 28. Положим $\rho = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{a_n}}$. Тогда ряд $\sum_{n=0}^{\infty} a_n x^n$ сходится при всех $x : |x| < \rho$.

Теорема 29. Пусть $A(x) = \frac{b_0 + b_1x + b_2x^2 + \dots}{c_0 + c_1x + c_2x^2 + \dots}$, $c_0 \neq 0, b_0 \neq 0$, и выполнены два следующих условия: все корни знаменателя лежат в \mathbb{R} (то есть нет комплексных корней) и множество корней числителя и корней знаменателя не пересекается. Тогда ряд $A(x)$ сходится для всех x , таких что $|x|$ меньше наименьшего значения модуля корня знаменателя.

Теорема 30. Если $|x| < \rho$. $A'(x) = \sum_{n=1}^{\infty} a_n n x^{n-1}$

Пример 5. Найти $\sum_{k=0}^n k^2 C_n^k (\frac{1}{3})^k$

Возьмем $\{C_n^k (\frac{1}{3})^k\}$ и составим её производящую функцию.

$$f(x) = \sum_{k=0}^n C_n^k (\frac{1}{3})^k = (1 + \frac{x}{3})^n$$

$$f'(x) = \sum_{k=1}^n k C_n^k (\frac{1}{3})^k x^{k-1}$$

$$x f'(x) = \sum_{k=1}^n k C_n^k (\frac{1}{3})^k x^k$$

$$(x f'(x))' = \sum_{k=1}^n k^2 C_n^k (\frac{1}{3})^k x^{k-1}$$

$$x(x f'(x))' = \sum_{k=1}^n k^2 C_n^k (\frac{1}{3})^k x^k$$

$$x(x f'(x))' = x(x^{\frac{n}{3}} (1 + \frac{x}{3})^{n-1})'$$

Пример 6. $F_0 = 1, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ Найдем $\sum_{n=0}^{\infty} F_n (\frac{1}{2})^n$.

$$xf(x) = F_0x + F_1x^2 + F_2x^3 + \dots$$

$$x^2f(x) = F_0x^2 + F_1x^3 + F_2x^4 + \dots$$

$$xf(x) + x^2f(x) = F_1x + (F_0 + F_1)x^2 + \dots + (F_{n-2} + F_{n-1})x^n + \dots = F_1x + F_2x^2 + \dots = f(x) - F_0$$

$$xf(x) + x^2f(x) = f(x) - 1 \Rightarrow f(x) = \frac{1}{1-x-x^2} \text{ Корни знаменателя: } \frac{\sqrt{5}+1}{2}, \frac{\sqrt{5}-1}{2}.$$

По теореме о сходимости $|x| < \frac{\sqrt{5}-1}{2}$

Линейные рекуррентные зависимости

Линейная зависимость порядка k : $x_n = a_{n-1}x_{n-1} + \dots + a_{n-k}x_{n-k}$.

Для $k = 2$ $a_2y_{n+2} + a_1y_{n+1} + a_0y_n = 0$

Определение 44. Характеристическое уравнение для линейной зависимости порядка 2 есть $a_2\lambda^2 + a_1\lambda + a_0 = 0$

Теорема 31. Пусть y характеристического уравнения есть решение $\lambda_1 \neq \lambda_2$. Тогда

- любая последовательность $y_n = c_1\lambda_1^n + c_2\lambda_2^n$, $c_1, c_2 \in \mathbb{C}$ являются решениями зависимости.
- если y_n — решение. Тогда $\exists c_1, c_2 \in \mathbb{C} : y_n = c_1\lambda_1^n + c_2\lambda_2^n$

Доказательство.

- Подставим и получим равносильность утверждения и характеристического уравнения.
- Пусть $y_0, y_1, \dots, y_n, \dots$. Рассмотрим уравнения $c_1 + c_2 = y_0$, $c_1\lambda_1 + c_2\lambda_2 = y_1$ с неизвестными c_1, c_2 . Так как $\lambda_1 \neq \lambda_2$, то у этой системы есть решения. Пусть c_1^*, c_2^* — решения этой системы. Рассмотрим последовательность $y_n^* = c_1^*\lambda_1^n + c_2^*\lambda_2^n$.

□

Теорема 32. Пусть y характеристического уравнения $\lambda_1 = \lambda_2 = \lambda$. Тогда для любое решение представимо в виде $y_n = (c_1n + c_2)\lambda^n$, и для любых c_1, c_2 $y_n = (c_1n + c_2)\lambda^n$ есть решение

Доказательство. Доказательство аналогично.

□

Общий случай $a_k \lambda^k + a_{k-1} \lambda^{k-1} + \dots + a_0 = 0$ — характеристическое уравнение

$\lambda_1, \dots, \lambda_k \in \mathbb{C}$ (основная теорема алгебры).

Обозначим все различные корни через μ_1, \dots, μ_l . Пусть

Теорема 33. Пусть $P_1(n), \dots, P_l(n)$, таких что $P_i(n)$ — многочлен с произвольными коэффициентами из \mathbb{C} , имеющий степень $n_i - 1$. Тогда любое $y_n = P_1(n)\mu_1^n + \dots + P_l(n)\mu_l^n$ — решение и любое решение представимо в таком виде.