

Дискретная математика

Харитонцев-Беглов Сергей

5 октября 2021 г.

Содержание

1. Теория множеств	1
1.1 Базовые понятия	1
1.2 Операции с множествами	1
2. Комбинаторика	4
2.1 Сетки	4
2.2 Биномиальные коэффициенты	5
2.3 Мультимножество	5
2.4 k -перестановки	5
2.5 Комбинаторика в схемах и мемах	6
3. Дискретная вероятность	8

1. Теория множеств

1.1. Базовые понятия

Есть официальный конспект, который будет Здесь.

Определение 1.1. Множество — набор различных между собой по какому-то признаку предметов.

Определение 1.2. Предметы входящие в это множество называются его элементами.

Если мы хотим описать множество, то нужно просто описать предметы этого множества. Например, чтобы задать множество студентов необходимо задать просто студентов.

Есть конечные, счетные, несчетные и целый зоопарк множеств разных мощностей. Самое простое множество — \emptyset , множество ничего не содержащее — пустое.

Определение 1.3. X подмножество (\subseteq) $Y \Leftrightarrow \forall y \in Y : y \in X$.

\emptyset и X — тривиальные, остальные — нетривиальные. все подмножества, кроме X — собственные.

1.2. Операции с множествами

Символ	Определение	Словами
\cap	$A \cap B = \dots$	Пересечение множества
\cup	$A \cup B = \dots$	Объединение множеств
\setminus	$A \setminus B = \dots$	Разность множеств
Δ	$A \Delta B = \dots$	Симметрическая разность множеств

Определение 1.4. Алгебраическая структура — множество, на котором ввели какую-то операцию.

Пример. Пусть заданы несколько множеств:

1. $\exists e : a \cdot e = a \ \forall a \in G$
2. $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$
3. $\forall a, b, c : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
4. $\forall a, b \in G a \cdot b = b \cdot a$

То это абелева группа и это к алгебре.

А дискретная математика не имеет аксиом, то есть мало чего можно использовать из алгебры / матана.

Если задать какое-то надмножество X над A , то появится операция дополнения: $A' = X \setminus A$.
Законы Де Моргана:

Теорема 1.1. $(A \cup B)' = A' \cap B'$

Теорема 1.2. $(A \cap B)' = A' \cup B'$

Доказательство смотри в конспекте Омеля, тут мне лень это делать.

Определение 1.5. Система иномножеств — множество, элементами которого являются множества.

Определение 1.6. Семейство множеств — упорядоченный набор неких множеств (X_1, X_2, \dots, X_k) . Причем множества в наборе могут повторяться.

Определение 1.7. Некоторое покрытие множества X системой множеств — система множеств, объединение элементов которого равняется X .

Определение 1.8. Разбиение множества X на блоки — система (X_1, X_2, \dots, X_k) , удовлетворяющая неким условиям:

1. $X = \bigcup_{i=1}^k X_i$
2. $\forall i: X_i \neq \emptyset$
3. $\forall i, j = 1..k: X_i \cap X_j = \emptyset$

Определение 1.9. Пара элементов (x, y) — упорядоченный набор из двух элементов. То есть для $x \neq y: (x, y) \neq (y, x)$

Определение 1.10 (Декартово произведение). $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$

можно ввести понятие « n ки» — упорядоченный набор из n элементов. Поэтому можно ввести $A \times B \times C \times \dots$ и A^2, A^n

Определение 1.11. Отношение между множествами — некое подмножество декартова произведения этих множеств

Пусть ω — отношение между X и Y . Тогда их записывают $X\omega Y$, а отсутствие — $X \not\omega Y$.

Определение 1.12. Отношение эквивалентности (X, \sim) :

1. $x \sim x \forall x \in X$
2. $x \sim y \Rightarrow y \sim x \forall x, y \in X$
3. $x \sim y, y \sim z \Rightarrow x \sim z \forall x, y, z \in X$

Пусть $\tilde{x} = \{y \in X \mid y \sim x\}$.

Свойство. пусть $y \in \tilde{x} \Rightarrow \tilde{y} = \tilde{x}$

Теорема 1.3. Разбиение на блоки задает классы эквивалентности.

- $X = \bigcup_{x \in X} \tilde{x}$
- $\tilde{x} \neq \emptyset$, т.к. хотя бы $x \in \tilde{x}$.
- Рассмотрим \tilde{x}, \tilde{y} . Пусть $\exists z: z \in \tilde{x} \cap \tilde{y}$. Тогда $\left. \begin{matrix} \tilde{z} = \tilde{x} \\ \tilde{z} = \tilde{y} \end{matrix} \right\} \Rightarrow \tilde{x} = \tilde{y}$

Определение 1.13. Мультимножество — $(x; \varphi): \varphi \rightarrow \mathbb{Z}_+$

Есть еще несколько базовых понятий: k -перестановки/сочетания из n элементов с/без повторений.

$|A \cup B| = |A| + |B|$, если $A \cap B = \emptyset$. Поэтому, если есть разбиение на блоки, то $X = X_1 \cup \dots \cup X_k \Rightarrow |X| = |X_1| + \dots + |X_k|$

$X = X_1 \times \dots \times X_k$, тогда $|X| = |X_1| \cdot \dots \cdot |X_k|$

$$|A' \cap B'| = |(A \cup B)'| = |X| - |A \cup B| = |X| - |A| - |B| + |A \cap B|$$

2. Комбинаторика

2.1. Сшки

Есть два способа записи цэшек: $C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$. Обычно формулы в комбинаторике используются не для подсчетов, а для определения асимптотики/верней оценки и так далее. Например если взять $n = 100$, то уже проблема: $100!$ — довольно большое число. Но там еще и деление!!! Короче, может получится небольшое число при больших числах в подсчетах.

Давайте забудем эту дурацкую формулу и будем использовать рекурренты: легко считать, пишется в миг. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, $\binom{0}{0} = 1$.

Доказательство. Пусть есть множество из n элементов. Разобьем все k -элементные подмножества на блоки: в одном все без последнего элемента, в другом все с последним. Тогда в первом блоке тогда есть $\binom{n-1}{k}$ элементов. В другом $\binom{n-1}{k-1}$ элементов. А значит $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ \square

Есть пара граничных случаев: $\binom{n}{0} = 1$, $\binom{n}{k} (n < k) = 0$. После этого можно сделать треугольник Паскаля:

$$\begin{array}{cccccccc}
 & & & & & & & 1 \\
 & & & & & & 1 & 1 \\
 & & & & & 1 & 2 & 1 \\
 & & & 1 & 3 & 3 & 1 \\
 & & 1 & 4 & 6 & 4 & 1 \\
 & 1 & 5 & 10 & 10 & 5 & 1 \\
 1 & 6 & 15 & 20 & 15 & 6 & 1
 \end{array}$$

Рассмотрим решетчатую плоскость (если вы это читаете это и здесь нет картиночки напишите @doktorkrab, чтобы я добавил картиночку). Какое здесь количество путей? Ну $A_n^k = A_{n-1}^k + A_{n-1}^{k-1}$. А это Сшки.

Теперь посмотрим на сумму на диагонали. Получаем гипотезу: $\sum m = 0^n \binom{m}{k} = \binom{k}{k} + \binom{k+1}{k} + \dots + \binom{n-1}{k} + \binom{n}{k} = \binom{n+1}{k+1}$.

Доказательство. По основному комбинаторному тождеству: $\binom{m+1}{k+1} = \binom{m}{k+1} \binom{m}{k} \Rightarrow \binom{m}{k} = \binom{m+1}{k+1} - \binom{m}{k+1}$. Тогда:

$$\sum_{m=k}^n \binom{m}{k} = \underbrace{\sum_{m=k}^n \binom{m+1}{k+1}}_{\binom{n+1}{k+1} + \sum_{m=k}^{n-1} \binom{m+1}{k+1}} - \underbrace{\sum_{m=k}^n \binom{m}{k+1}}_{\sum_{m=k+1}^n \binom{m}{k+1}}.$$

Дальше, если, расписать сумму все получится.

Пусть хочу набрать $k+1$ -элементное подмножество из $n+1$ -элементного множества. Пусть мы выбрали последний элемент, тогда у нас есть $\binom{n}{k}$ способов, а если не выбрали, то $\binom{n}{k+1}$ способов. А по индукции $\binom{n}{k+1} = \binom{n-1}{k+1} + \binom{n-1}{k}$. И так далее. \square

Рассмотрим $\binom{n+m}{k} = \sum_{i=0}^k \binom{n}{i} \cdot \binom{m}{k-i}$

Доказательство. Рассмотрим два множества: одно n -элементное ("мальчики"), другое m -элементное ("девушки"). Тогда пусть мы выбрали i мальчиков, тогда нам нужно выбрать $k-i$ девушек. \square

Мы здесь применили принцип **double counting**: если мы посчитали что-то двумя способами, то результаты равны.

2.2. Биномиальные коэффициенты

Подробности на втором курсе.

Рассмотрим бином Ньютона: $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k \cdot y^{n-k}$

Доказательство. Раскроем скобки в левой части: $(x+y)(x+y)(x+y) \dots$ Когда у нас x^k ? Когда мы ровно в k скобках выбрали x . Сколько способов? Очевидно $\binom{n}{k}$. \square

Частные случаи:

- $x = y = 1$. Тогда $2^n = \sum_{k=0}^n \binom{n}{k}$

Рассмотрим множество $\{x_1, x_2, \dots, x_n\}$. Каждому числу можно сопоставить 0/1 — берем/не берем. Тогда количество подмножеств — количество бинарных строчек длины n . Такой метод называется биективным: когда мы доказываем, что один объект является биекцией другого, то их количества равны.

- $x = 1, y = -1$. Тогда $0 = \sum_{k=0}^n (-1)^k \binom{n}{k}$ — количества способов выбрать подмножество четных длин и нечетных длин равны.

2.3. Мультимножество

Хотим посчитать $\left(\!\!\binom{n}{k}\!\!\right)$ — количество k -элементных подмультимножеств.

Пусть $X = [n]$. По принципу биекции найдем сначала $\left(\!\!\binom{n}{k}\!\!\right)$ для X , а потом найти для произвольного множества.

Пусть есть множество A , заменим его на множество $\{i + A_i\}$. $\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k}$

2.4. k -перестановки

Определение 2.1. Упорядоченные набор из k элементов, где все элементы принадлежат множеству X .

Если мы считаем, что с повторениями, то ответ n^k , а если без то $n \cdot (n-1) \cdot \dots \cdot (n-k+1) = (n)_k$. Перестановку можно записать как: $\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \end{pmatrix}$. То есть i перешло в a_i . После

этого можно композировать перестановки: $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Заметим, что:

1. Существует нейтральный элемент — тождественная перестановка $e = \{1, 2, \dots, n-1, n\}$
2. Существует обратный элемент: $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$
3. Ассоциативность: $\sigma \cdot (\tau \cdot \pi) = (\sigma \cdot \tau) \cdot \pi$

Значит перестановки с операцией композиции — группа. Носит название S_n . Есть теорема о том, что любая конечная группа представима как подгруппа S_n .

Рассмотрим $(n)_k = n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \binom{n}{k} \cdot k!$. Тогда $\binom{n}{k} = \frac{(n)_k}{k!}$. Тогда можно заменить n на $q, q \in \mathbb{C}$. Тогда

$$\binom{q}{k} = \begin{cases} \frac{(q)_k}{k!} & k > 0 \\ 1 & k = 0 \\ 0 & k < 0 \end{cases}$$

Пусть $(n)^k = n \cdot (n+1) \cdot \dots \cdot (n+k-1)$. Тогда $\binom{n}{k} = \frac{(n)^k}{k!}$

2.5. Комбинаторика в схемах и мемах

Пусть есть n различных предметов. Нужно выбрать k предметов с различными ограничениями: с повторениями/без, упорядоченные/неупорядоченные.

	с повторениями	без повторений
упорядоченные	n^k	$(n)_k$
неупорядоченные	$\binom{n}{k}$	$\binom{n}{k}$

Схема ящиков.

	\forall	≤ 1	1	≥ 1
ящики+предметы различимы	n^k	$(n)_k$	$1/n!$	$\widehat{S}(n, k)$
ящики различимы, а предметы — нет	$\binom{n}{k}$	$\binom{n}{k}$	$1/0$	$\binom{n}{k-n}$
ящики не различимы, а предметы различимы				$S(n, k)$
ящики+предметы неразличимы				

Последнюю строчку мы не сможем заполнить на первом курсе, нужны производящие функции. Эта строчка решает множество задач, например, разложение числа на слагаемые.

Отображение $f : X \rightarrow Y$ — такое правило, что $\forall x \in X \exists! y \in Y : y = f(x)$. Количество k^n ($|X| = n, |Y| = k$)

Определение 2.2. Отображение — тройка из $(x, y, \Gamma \subseteq X \times Y)$, причем каждый x_i встречается в Γ ровно один раз.

Определение 2.3. Отображение называется инъективным, если $\forall x_1, x_2 \in X \ f(x_1) \neq f(x_2) \Rightarrow x_1 = x_2$. Их количество — $(k)_n$

Определение 2.4. Отображение называется биективным, если $\forall y \in Y \exists! x \in X : y = f(x)$. Количество — $n!$.

Определение 2.5. Отображение называется сюръективным, если $\forall y \in Y \exists x \in X : y = f(x)$.

Посчитаем количество сюръективных отображений. Пусть $\text{Im}(f) = \{y \in Y \mid \exists x \in X : y = f(x)\}$. Тогда для любого отношения $f : X \rightarrow \text{Im}(f)$ — сюръективно.

Пусть $|\text{Im}(f)| = i$, а количество сюръективных отображений — $\widehat{S}(n, i)$. Тогда $\widehat{S}(n, i) \cdot \binom{k}{i}$ — количество сюръективных подмножеств мощности k .

$$\text{Тогда } k^n = \sum_{i=0}^k \binom{k}{i} \widehat{S}(n, i)$$

Пусть есть две числовые последовательности $f_0, f_1, \dots, f_k, \dots$ и $g_0, g_1, \dots, g_k, \dots$. Причем $g_k = \sum_{i=0}^k \binom{k}{i} f_i$, тогда $f_k = \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} g_i$. Значит $\widehat{S}(n, k) = \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} \cdot i^n$

Рассмотрим отображение $\{\{x_1, x_2\}, \{x_3\}, \emptyset\}$. Получение разбиение на блоки. Предположим, что отображение сюръективно, значит получили разбиение k предметов n ящиков.

Предположим, что в первый ящик нужно положить a_1 предмет, во второй — a_2 , и так далее. Тогда количество вариантов: $\sum \binom{n}{a_1} \binom{n-a_1}{a_2} \dots$. Если взять $\sum_{a_i \geq 0, a_1 + \dots + a_k = n} \binom{n}{a_1} \binom{n-a_1}{a_2} = k^n = \frac{n!}{a_1! a_2! \dots a_k!}$. А если $\sum_{a_i > 0, a_1 + \dots + a_k = n} \binom{n}{a_1} \binom{n-a_1}{a_2} = \widehat{S}(n, k)$

Хотим разбить на блоки вида a_1 предметов + a_2 предметов + a_3 предметов... Тогда заметим, что это $\sum_{a_i \geq 0, \sum a_i = n} \binom{n}{a_1} \binom{n-a_1}{a_2} \dots \binom{n-a_1-a_2-\dots-a_{k-1}}{a_k}$. Заметим, что суммарно это k^n , а если строго больше нуля, то $\widehat{S}(n, k)$. Также можно раскрыть скобки и получить. $\frac{n!}{a_1! a_2! \dots a_k!}$

Рассмотрим $\binom{n}{k} = \frac{n!}{k!(n-k)!} = P(n; k; n-k)$. Комбинаторно они равны через битовые строки.

Теперь посмотрим на $\left\langle \binom{n}{k} \right\rangle = \frac{(n-1+k)!}{(n-1)!k!}$, через шары и перегородки.

Вернемся к k^n — все отображения, $\widehat{S}(n, k)$ — все сюръективные отображение, $S(n, k)$ — количество разбиений n -множества на k -подмножества. (Числа Стирлинга второго рода).

Заметим, что $S(n, k) \cdot k! = \widehat{S}(n, k)$, так как в S с крышечкой это про неупорядоченные. $S(n, k) = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} i^n$. $S(0, 0) = 1$. $\forall S(n, 0) = 0$. $S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k)$. Доказываем так: либо удаляем x_n , либо пишем x_n куда-то.

$$k^n = \sum_{i=0}^n \binom{k}{i} \widehat{S}(n, i) = \sum_{i=0}^n \frac{k!}{i!(k-i)!} S(n, i).$$

Откуда:

$$x^n = \sum_{i=0}^n (x)_i \cdot S(n, i) \iff (x)_n = \sum_{i=0}^n x^i s(n, i)..$$

Где $s(n, i)$ — числа Стирлинга первого рода.

Решим задачу, где мы хотим разбить n различных предметов в k различных ящиков $B(n, k) = \sum_{i=0}^k S(n, i)$. Причем $B(n, n) = B_n$ — числа Белла. Количество способов разбить n -множество на блоки.

3. Дискретная вероятность

Вероятностное событие — событие в какой-то вероятностной математической модели. (Результат трудно предсказать)

Множество исходов $\Omega = \{\omega_1, \dots, \omega_n\}$ — состоит из элементарных исходов. В дискретной вероятности Ω конечно или счетно.

Событие A — подмножество Ω .

Рассмотрим какой-то набор событий, добавим туда \emptyset, Ω . Получим алгебру. Тогда вероятность это отображение $P : \Omega \mapsto [0, 1]$, такое что $\sum_{\omega \in \Omega} P(\omega) = 1$. Тогда $P(A) = \sum_{\omega \in A} P(\omega)$.

$$1. P(\emptyset) = 0, P(\Omega) = 1$$

$$2. P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Определение 3.1. Назовем события A и B несовместными, если $A \cap B = \emptyset$.

Некоторым очень хочется дать определение вида $P_r(A) = \frac{|A|}{|\Omega|}$. Это не работает, если события не равновероятны.

Пусть есть два события на кубике: A — число > 3 , B — четное число. $P_r(A) = \frac{1}{2}, P_r(B) = \frac{1}{2}$.

Теперь пусть есть инсайд: событие A произошло. Тогда $P_r(B | A) = \frac{2}{3}$. Тогда посмотрим на картинку и получим $P_r(B | A = \frac{|A \cap B|}{|A|})$. Но не забудем, про то, что мы смотрели на равновероятные события, тогда поделим на $|\Omega|$. Получим $P_r(B|A) \stackrel{\text{def}}{=} \frac{P_r(A \cap B)}{P_r(A)}$.

Посмотрим на крайние случаи: $P_r(A|A) = 1$, $P_r(A|\Omega) = P_r(A)$, $P_r(B|A) = 1$, если $A \subseteq B$.

Тогда пусть $B_1 \cap B_2 = \emptyset$. Тогда $P_r((B_1 \cup B_2) \cap A) = P_r((B_1 \cap A) \cup (B_2 \cap A)) = P_r(B_1 \cap A) + P_r(B_2 \cap A)$. А $P_r(B_1 \cup B_2 | A) = P_r(B_1 | A) + P_r(B_2 | A)$.

Посмотрим на $P_r(B|\bar{A}) = \frac{1}{3}$. Докажем, что $P_r(B | A) \cdot P_r(A) + P_r(B | \bar{A}) \cdot P_r(\bar{A}) = 1$. Докажем формулу полной вероятности.

Доказательство. Пусть Ω разбита на блоки $\{A_1, \dots, A_k\}$. Заметим, что $P_r(B) = P_r(B \cap \Omega) = P_r(B \cap (A_1 \cup \dots \cup A_k)) = P_r((B \cap A_1) \cup (B \cap A_2) \cup \dots \cup (B \cap A_k))$. Дальше заметим, что $\forall i, j : A_i \cap A_j = \emptyset$. Тогда получаем $P_r(B \cap A_1) + P_r(B \cap A_2) + \dots + P_r(B \cap A_k)$. Применив формулу условной вероятности, получим формулу полной вероятности:

$$P_r(B) = P_r(B | A_1) \cdot P_r(A_1) + P_r(B | A_2) \cdot P_r(A_2) + \dots + P_r(B | A_k) \cdot P_r(A_k).$$

□

Заметим, что $P_r(A \cap B) = P_r(B | A) \cdot P_r(A)$ и $P_r(B \cap A) = P_r(A | B) \cdot P_r(B) \Rightarrow P_r(A | B) = \frac{P_r(B|A)P_r(A)}{P_r(B)}$. Тогда, вспомнив формулу полной вероятности, получаем:

$$P_r(A_i | B) = \frac{P_r(B | A_i) \cdot P_r(A_i)}{\sum_{j=1}^k P_r(B | A_j) \cdot P_r(A_j)}.$$

Пусть у вас есть событие $P_r(B)$, причем $P_r(B) = P_r(B | A) = \frac{P_r(A \cap B)}{P_r(A)} P_r(A) \Rightarrow P_r(A \cap B) = P_r(A) \cdot P_r(B)$

Определение 3.2. Два события называются независимыми, если вероятность их пересечения равна произведению вероятностей этих событий.

Схема Бернулли: есть n независимых испытаний, где есть два исхода: $p > 0$ и $q > 0$, $p+q = 1$. Все элементарных исходов можно записать в виде бинарной строки длины n . Тогда для какого-то ω $P_r(\omega) = p^k \cdot q^{n-k}$, $k = \sum_{i=1}^n a_i$. Заметим, что $\sum_{k=0}^n \binom{n}{k} p^k q^{n-k} = (p+q)^n = 1^n = 1$.

Определение 3.3. Независимые в совокупности события — события A_1, \dots, A_k , такие что $P_r(A_1 \cap A_2 \cap \dots \cap A_k) = P_r(A_1) \cdot P_r(A_2) \cdot \dots \cdot P_r(A_k)$,

$\Omega_1 = \{\text{успех, неудача}\}$, $P_{r_1}(\omega) = \begin{cases} p & \text{успех} \\ q & \text{неуспех} \end{cases}$, $A_1 = \{\emptyset, \text{успех, неудача}, \Omega\}$. Тогда $\Omega = \Omega_1 \times \dots \times \Omega_n$,

$A = A_1 \times \dots \times A_n$.

Тогда рассмотрим (Ω_1, A_1, P_{r_1}) , (Ω_2, A_2, P_{r_2}) . Тогда $\Omega = \Omega_1 \times \Omega_2$, $A = A_1 \times A_2$. Тогда события $A_1 \times \Omega_2$, $\Omega_1 \times A_2$.