

# Дискретная математика

## Глава 8. Дискретная вероятность и вероятностные методы

А. В. Пастор

02.05.2025

## Дополнительные материалы по теории вероятности

1. А. Н. Ширяев, *Вероятность*. М.: МЦНМО, 2007.
2. П. Эрдёш, Дж. Спенсер, *Вероятностные методы в комбинаторике*. М.: Мир, 1976.
3. S. Jukna, *Extremal Combinatorics: With Applications in Computer Science*. Springer, 2001.

Слайды по дискретной математике будут публиковаться по адресу

<https://logic.pdmi.ras.ru/~pastor/ITMO/2024-25/>

## Дискретное вероятностное пространство

### Определение

- *Дискретным вероятностным пространством* называется упорядоченная пара  $(\Omega, P)$ , где  $\Omega$  — конечное множество и  $P: \Omega \rightarrow [0, 1]$  — такая функция, что  $\sum_{\omega \in \Omega} P(\omega) = 1$ .
- Элементы множества  $\Omega$  называются *элементарными событиями*, а само  $\Omega$  — *пространством элементарных событий* или *пространством исходов*.
- Величина  $P(\omega)$ , где  $\omega \in \Omega$ , называется *вероятностью* элементарного события  $\omega$ . Функция  $P$  называется *распределением вероятностей*.
- *Событием* называется любое подмножество  $A \subset \Omega$ .
- *Вероятностью* события  $A \subset \Omega$  называется величина  $P(A) \stackrel{\text{def}}{=} \sum_{\omega \in A} P(\omega)$ .
- $\emptyset$  — *невозможное событие*. Очевидно, что его вероятность равна нулю. Но могут быть и другие события, имеющие нулевую вероятность.

### Замечание

- Удобно считать, что  $\Omega = \{\omega_1, \dots, \omega_n\}$  и  $P(\omega_i) = p_i$ .
- Тогда  $\forall i (0 \leq p_i \leq 1)$  и  $p_1 + \dots + p_n = 1$ .

## Дискретное вероятностное пространство: примеры

1. Пусть мы  $n$  раз подбросили монетку и после каждого подбрасывания отмечаем, упала ли она орлом или решкой.
  - Если выпал орел, будем писать 1, а если выпала решка — 0.
  - Элементарным событием будем считать совокупность результатов всех  $n$  подбрасываний монетки.
  - То есть  $\Omega = \{(a_1, \dots, a_n) \mid \forall i \ a_i \in \{0, 1\}\} = \{0, 1\}^n$ . Элементы  $\Omega$  соответствуют подмножествам  $[1..n]$  — *случайное подмножество*.
  - Будем считать, что вероятности всех элементарных событий равны. Тогда  $\forall \omega \in \Omega \ (P(\omega) = \frac{1}{2^n})$ .
  - В получившемся вероятностном пространстве можно рассмотреть, например, следующие события.
    - $A$ : “При первом подбрасывании выпал орел”;
    - $B$ : “При втором подбрасывании выпала решка”;
    - $C$ : “Результаты первого и второго подбрасываний одинаковы”.
  - Легко видеть, что  $P(A) = P(B) = P(C) = \frac{1}{2}$ .

### Определение

Распределение вероятностей называется *равномерным*, если вероятности всех элементарных событий равны.

## Дискретное вероятностное пространство: примеры

2. Снова подбросим  $n$  раз монетку. Но распределение вероятностей выберем другое.

- Пусть  $p, q \geq 0$  таковы, что  $p + q = 1$ .
- Обозначим через  $s(\omega)$  число выпавших орлов в элементарном событии  $\omega$ . (Т. е.  $s(a_1, \dots, a_n) = a_1 + \dots + a_n$ ).
- Пусть  $P(\omega) \stackrel{\text{def}}{=} p^{s(\omega)} q^{n-s(\omega)}$ .
- Заметим, что  $\sum_{\omega \in \Omega} P(\omega) = \sum_{k=0}^n C_n^k p^k q^{n-k} = (p + q)^n = 1$ , следовательно,  $(\Omega, P)$  — дискретное вероятностное пространство.
- Рассмотрим следующие события:
  - $S_i \stackrel{\text{def}}{=} \{\omega \in \Omega \mid s(\omega) = i\}$ , где  $i \in [0..n]$ , — “выпало ровно  $i$  орлов”;
  - $T_j \stackrel{\text{def}}{=} \{(a_1, \dots, a_n) \in \Omega \mid a_j = 1\}$ ,  $j \in [1..n]$ , — “на  $j$ -м шаге выпал орёл”.
- Легко видеть, что  $P(S_i) = C_n^i p^i q^{n-i}$ ;
- Далее,  $P(T_j) = \sum_{k=0}^{n-1} C_{n-1}^k p^{k+1} q^{n-1-k} = p(p + q)^{n-1} = p$ .
- Последнее равенство означает, что на  $j$ -м шаге с вероятностью  $p$  выпадет орел и с вероятностью  $q$  — решка.

## Дискретное вероятностное пространство: примеры

3. Заметим, что события  $S_i$  из предыдущего примера образуют разбиение множества  $\Omega$ .
- Тогда  $P(S_0) + P(S_1) + \dots + P(S_n) = 1$ .
  - Это означает, что  $S_i$  можно рассматривать как элементарные события.
  - Более точно, пусть  $\Omega' = \{S_0, S_1, \dots, S_n\}$  и  $P(S_i) = C_n^i p^i q^{n-i}$ .
- Тогда пара  $(\Omega', P)$  является дискретным вероятностным пространством.

### Определение

Распределение вероятностей, задаваемое формулой  $P(S_i) = C_n^i p^i q^{n-i}$ , называется **биномиальным**.

### Замечание

- На самом деле, рассуждения из второго примера хочется проводить в обратную сторону: сказать, что при каждом подбрасывании монетки орел выпадает с вероятностью  $p$ , а решка — с вероятностью  $q$ , и из этого вывести вероятности других событий.
- Для того, чтобы делать это корректно, нам нужно будет ввести понятия условной вероятности и независимых событий.

## Условная вероятность

- Пусть  $(\Omega, P)$  — дискретное вероятностное пространство;  $A, B \subset \Omega$ .
- Будем обозначать через  $AB$  событие, задаваемое множеством  $A \cap B$ . (Т.е.  $AB$  — это событие, означающее то, что одновременно произошли события  $A$  и  $B$ .)

### Определение

Пусть  $P(B) > 0$ . Тогда *условной вероятностью* события  $A$  при условии события  $B$  называется величина  $P(A | B) \stackrel{\text{def}}{=} \frac{P(AB)}{P(B)}$ .

### Замечание

То есть мы предполагаем, что событие  $B$  выполнено: рассматриваем только те исходы, при которых это так. И считаем среди них долю тех исходов, для которых выполнено  $A$ . Эта доля и есть условная вероятность.

### Лемма (Формула Байеса)

$$P(B | A) = \frac{P(B)P(A|B)}{P(A)}.$$

Доказательство.  $P(B | A)P(A) = P(AB) = P(B)P(A | B)$ .



## Формула полной вероятности

Теорема (Формула полной вероятности)

Пусть  $\Omega = B_1 \cup \dots \cup B_m$  — разбиение  $\Omega$  и  $\forall i \ P(B_i) > 0$ .

Тогда  $P(A) = \sum_{i=1}^m P(A | B_i)P(B_i)$ .

Доказательство. Пусть  $A_i \stackrel{\text{def}}{=} AB_i = A \cap B_i$ .

- Тогда  $A = A_1 \cup \dots \cup A_m$  — разбиение  $A$ .

- Следовательно,  $P(A) = \sum_{i=1}^m P(A_i) = \sum_{i=1}^m P(A | B_i)P(B_i)$ . □

Теорема (Байеса)

Пусть  $\Omega = B_1 \cup \dots \cup B_m$  — разбиение  $\Omega$  и  $\forall i \ P(B_i) > 0$ .

Тогда  $P(B_i | A) = \frac{P(A|B_i)P(B_i)}{\sum_{j=1}^m P(A|B_j)P(B_j)}$ .

Доказательство.  $P(A | B_i)P(B_i) = P(AB_i)$ ;  $\sum_{j=1}^m P(A | B_j)P(B_j) = P(A)$ .

- Тогда  $\frac{P(A|B_i)P(B_i)}{\sum_{j=1}^m P(A|B_j)P(B_j)} = \frac{P(AB_i)}{P(A)} = P(B_i | A)$ . □

## Определение

- События  $A$  и  $B$  **независимы**, если  $P(AB) = P(A)P(B)$ .
- События  $A_1, \dots, A_n$  **независимы**, если для любых  $k \in [1..n]$  и  $1 \leq i_1 < i_2 < \dots < i_k \leq n$  выполнено  $P(A_{i_1} \dots A_{i_k}) = P(A_{i_1}) \dots P(A_{i_k})$ .

## Замечание

- Независимость не означает отсутствия пересечения.  
Если  $A \cap B = \emptyset$ , то события  $A$  и  $B$  зависимы!
- Попарная независимость  $n$  событий не означает того, что все  $n$  событий независимы.
  - ▶ Например, события  $A$ ,  $B$  и  $C$  из первого примера попарно независимы.  
Но все вместе они зависимы:  $P(ABC) = 0$ , но  $P(A)P(B)P(C) = \frac{1}{8}$ .
- Во втором примере события  $T_1, \dots, T_n$  независимы  
(напомним, что  $T_j$  — это событие “на  $j$ -м шаге выпал орёл”).

## Независимые события

### Утверждение

Если  $A$  и  $B$  независимы, то  $A$  и  $\overline{B}$  тоже независимы.

Доказательство.

$$\begin{aligned} P(A\overline{B}) &= P(A) - P(AB) = \\ &= P(A) - P(A)P(B) = \\ &= P(A)(1 - P(B)) = P(A)P(\overline{B}). \end{aligned}$$



### Замечание

- Аналогично можно доказать, что если события  $A_1, \dots, A_i, \dots, A_n$  независимы, то и  $A_1, \dots, \overline{A_i}, \dots, A_n$  независимы.
- Тогда независимым будет также и любой набор событий вида  $A'_1, \dots, A'_n$ , где для любого  $j$  событие  $A'_j$  — это либо  $A_j$ , либо  $\overline{A_j}$ .

## Случайные величины

- Пусть  $(\Omega, P)$  — дискретное вероятностное пространство.

### Определение

- *Случайной величиной* называется произвольное отображение  $\xi: \Omega \rightarrow \mathbb{R}$ .

### Примеры

1. Если  $\Omega$  — множество результатов  $n$  подбрасываний монетки, то  $s(\omega)$  (количество выпавших “орлов”) является случайной величиной.
2. Каждому событию  $A \subset \Omega$  соответствует случайная величина, являющаяся характеристической функцией множества  $A$ :

$$\chi_A(\omega) \stackrel{\text{def}}{=} \begin{cases} 0, & \omega \notin A \\ 1, & \omega \in A. \end{cases}$$

- Пусть  $\xi: \Omega \rightarrow \mathbb{R}$  — случайная величина и  $X = \xi(\Omega)$  — множество значений случайной величины  $\xi$ . Тогда мы можем рассматривать события вида  $\xi(\omega) = x$ , где  $x \in X$ , или  $\xi(\omega) \in B$ , где  $B \subset X$ . Тем самым, мы получаем распределение вероятностей на множестве  $X$ .

## Случайные величины: распределение и независимость

- Пусть  $X = \{x_1, \dots, x_m\}$ . Тогда  $P_\xi(x_i) \stackrel{\text{def}}{=} P(\{\omega \in \Omega \mid \xi(\omega) = x_i\})$ .
- Очевидно, что  $P_\xi(x_1) + \dots + P_\xi(x_m) = 1$ .
- Следовательно,  $(X, P_\xi)$  — дискретное вероятностное пространство.
- Функция  $P_\xi$  называется *распределением случайной величины  $\xi$* .
- Для обозначения индуцированной вероятности мы также будем использовать также обозначение  $P\{\xi = x_i\}$ .

### Определение

Случайные величины  $\xi_1, \dots, \xi_r: \Omega \rightarrow X$  называются *независимыми*, если  $\forall t_1, \dots, t_r \in X (P\{\xi_1 = t_1, \dots, \xi_r = t_r\} = P\{\xi_1 = t_1\} \dots P\{\xi_r = t_r\})$ .

### Замечание

Если события  $A_1, \dots, A_r$  независимы если и только если их характеристические функции  $\chi_{A_1}, \dots, \chi_{A_r}$  — независимые случайные величины.

# Случайные величины: математическое ожидание

## Определение

- Пусть  $\xi: \Omega \rightarrow X$  — случайная величина.
- *Математическим ожиданием* случайной величины  $\xi$  называется число

$$E\xi \stackrel{\text{def}}{=} \sum_{\omega \in \Omega} \xi(\omega)P(\omega).$$

## Замечание

- Очевидно, что  $E\xi = \sum_{x \in X} xP\{\xi = x\}$ .
- Если  $\xi$  — случайная величина и  $a \in \mathbb{R}$ , то  $E(a\xi) = aE\xi$ .
- Если  $\xi_1, \dots, \xi_r: \Omega \rightarrow X$  — случайные величины, то  $E(\xi_1 + \dots + \xi_r) = E\xi_1 + \dots + E\xi_r$ .
- Другое обозначение для математического обозначения:  $M\xi$ .

## Теорема

Если случайные величины  $\xi_1, \dots, \xi_r: \Omega \rightarrow X$  независимы, то

$$E(\xi_1 \dots \xi_r) = E\xi_1 \dots E\xi_r.$$

Доказательство. Пусть случайная величина  $\xi_1 \dots \xi_r$  принимает значения из множества  $\mathcal{X}_r$ .

- Заметим, что  $\mathcal{X}_r$  состоит из произведений вида  $x_1 \dots x_r$ , где  $\forall i (x_i \in X)$ .
- Тогда

$$\begin{aligned} E(\xi_1 \dots \xi_r) &= \sum_{x \in \mathcal{X}_r} x P\{\xi_1 \dots \xi_r = x\} = \\ &= \sum_{x_1, \dots, x_r \in X} x_1 \dots x_r P\{\xi_1 = x_1, \dots, \xi_r = x_r\} = \\ &= \sum_{x_1, \dots, x_r \in X} x_1 \dots x_r P\{\xi_1 = x_1\} \dots P\{\xi_r = x_r\} = \\ &= \left( \sum_{x_1 \in X} x_1 P\{\xi_1 = x_1\} \right) \dots \left( \sum_{x_r \in X} x_r P\{\xi_r = x_r\} \right) = E\xi_1 \dots E\xi_r. \quad \square \end{aligned}$$

## Дисперсия случайной величины

### Определение

**Дисперсией** случайной величины  $\xi$  называется число  $D\xi \stackrel{\text{def}}{=} E(\xi - E\xi)^2$ .

### Замечание

- Из определения очевидно, что  $D\xi \geq 0$ .
- Также очевидно, что  $D\xi = 0$ , если и только если  $P\{\xi = E\xi\} = 1$  (т. е. случайная величина  $\xi$  почти всегда постоянна: за исключением, возможно, множества с нулевой вероятностью).
- По сути,  $D\xi$  показывает то, насколько сильно случайная величина  $\xi$  отклоняется от своего среднего.

### Утверждение

1.  $D\xi = E\xi^2 - (E\xi)^2$ .
2. Пусть  $a, b \in \mathbb{R}$ . Тогда  $D(a + b\xi) = b^2 D\xi$ .

### Доказательство.

1.  $D\xi = E(\xi^2 - 2\xi \cdot E\xi + (E\xi)^2) = E\xi^2 - 2E\xi \cdot E\xi + (E\xi)^2 = E\xi^2 - (E\xi)^2$ .
2.  $D(a + b\xi) = E((a + b\xi) - (a + bE\xi))^2 = E(b(\xi - E\xi))^2 = b^2 D\xi$ . □

# Дисперсия и независимость. Ковариация случайных величин

## Теорема

Пусть  $\xi$  и  $\eta$  — независимые случайные величины.

Тогда  $D(\xi + \eta) = D\xi + D\eta$ .

Доказательство.

- Заметим, что случайные величины  $\xi - E\xi$  и  $\eta - E\eta$  также независимы.
- Следовательно,  $E(\xi - E\xi)(\eta - E\eta) = E(\xi - E\xi)E(\eta - E\eta) = 0$ .
- Тогда  $D(\xi + \eta) = E((\xi - E\xi) + (\eta - E\eta))^2 =$   
 $= E(\xi - E\xi)^2 + E(\eta - E\eta)^2 + 2E(\xi - E\xi)(\eta - E\eta) = D\xi + D\eta. \quad \square$

## Определение

Величина  $\text{cov}(\xi, \eta) \stackrel{\text{def}}{=} E(\xi - E\xi)(\eta - E\eta)$  называется **ковариацией** случайных величин  $\xi$  и  $\eta$ .

## Утверждение

$$\text{cov}(\xi, \eta) = E(\xi\eta) - E\xi E\eta.$$

Доказательство.

$$\begin{aligned}\text{cov}(\xi, \eta) &= E(\xi - E\xi)(\eta - E\eta) = \\ &= E(\xi\eta - \xi E\eta - \eta E\xi + E\xi E\eta) = \\ &= E(\xi\eta) - E\xi E\eta - E\xi E\eta + E\xi E\eta = E(\xi\eta) - E\xi E\eta. \quad \square\end{aligned}$$

## Свойства ковариации

### Лемма

Пусть  $\xi, \eta, \theta: \Omega \rightarrow \mathbb{R}$  — случайные величины и  $a, b \in \mathbb{R}$ . Тогда

1.  $\text{cov}(a\xi + b\eta, \theta) = a \text{cov}(\xi, \theta) + b \text{cov}(\eta, \theta)$ ;
2.  $\text{cov}(\xi, \eta) = \text{cov}(\eta, \xi)$ ;
3.  $\text{cov}(\xi, \xi) = D\xi \geq 0$ .

Доказательство.

$$\begin{aligned} 1. \quad \text{cov}(a\xi + b\eta, \theta) &= E((a\xi + b\eta)\theta) - E(a\xi + b\eta)E\theta = \\ &= E(a\xi\theta + b\eta\theta) - (aE\xi + bE\eta)E\theta = \\ &= aE(\xi\theta) + bE(\eta\theta) - aE\xi E\theta - bE\eta E\theta = a \text{cov}(\xi, \theta) + b \text{cov}(\eta, \theta). \end{aligned}$$

2,3. очевидно из определения. □

### Теорема

$$|\text{cov}(\xi, \eta)| \leq \sqrt{D\xi \cdot D\eta}.$$

Доказательство.

- Заметим, что все случайные величины, заданные на вероятностном пространстве  $\Omega$ , образуют линейное пространство над  $\mathbb{R}$ .

## Коэффициент корреляции

- По лемме  $\text{cov}(\xi, \eta)$  — вещественное скалярное произведение на этом пространстве.
- Тогда по неравенству Коши-Буняковского-Шварца имеем  $\text{cov}(\xi, \eta)^2 \leq \text{cov}(\xi, \xi) \text{cov}(\eta, \eta) = D\xi \cdot D\eta$ . □

### Замечание

- На самом деле, условие  $\text{cov}(\xi, \xi) \geq 0$  несколько слабее условия положительности из определения вещественного скалярного произведения. Но для доказательства неравенства Коши-Буняковского-Шварца достаточно этого условия.

### Определение

- Величина  $\rho(\xi, \eta) \stackrel{\text{def}}{=} \frac{\text{cov}(\xi, \eta)}{\sqrt{D\xi \cdot D\eta}}$  называется *коэффициентом корреляции* случайных величин  $\xi$  и  $\eta$ .

### Замечание

- По доказанной выше теореме  $\rho(\xi, \eta) \in [-1, 1]$ .
- Если  $\xi$  и  $\eta$  независимы, то  $\rho(\xi, \eta) = 0$  (но обратное неверно).

## Вероятность в комбинаторике: простейший пример применения

- Основная идея: если нам нужно доказать существование объекта, обладающего нужным нам свойством, выбираем случайный объект и оцениваем вероятность того, что требуемое свойство выполняется. Если эта вероятность больше нуля (или, что эквивалентно, если вероятность того, что свойство не выполняется, меньше единицы), то интересующий нас объект существует.
- В простейшем варианте этот метод эквивалентен уже известному вам из курса теории графов методу оценки числа возможных конфигураций. Но бывают и более сложные случаи.
- В качестве первого примера докажем новым способом нижнюю оценку числа Рамсея. Фактически это будет то же самое доказательство, которое вы уже знаете, только пересказанное на языке теории вероятностей.
- Напомним, что **числа Рамсея**  $r(m, n)$  — это наименьшее из всех таких чисел  $x \in \mathbb{N}$ , что при любой раскраске рёбер полного графа на  $x$  вершинах в два цвета обязательно найдётся клика на  $n$  вершинах с рёбрами цвета 1 или клика на  $m$  вершинах с рёбрами цвета 2.

## Вероятностное доказательство нижней оценки $r(k, k)$

### Теорема (P. Erdős, 1947)

Для любого натурального  $k \geq 2$  выполняется неравенство  $r(k, k) \geq 2^{k/2}$ .

**Доказательство.** Пусть  $k \geq 3$  и  $n < 2^{k/2}$  (случай  $k = 2$  тривиален).

- Рассмотрим полный граф  $G$  на  $n$  вершинах и раскрасим его ребра в два цвета случайным образом.

- То есть мы  $C_n^2$  раз подбрасываем монетку и выбираем цвет очередного ребра в зависимости от результата подбрасывания.

- Все исходы равновероятны. То есть каждое ребро может быть покрашено в цвет 1 или в цвет 2 с вероятностью  $1/2$  и все эти события независимы.

- Для любого подмножества  $S \subset V(G)$ , где  $|S| = k$ , определим событие  $A_S$ : “все ребра подграфа  $G(S)$  одноцветны”. Тогда  $P(A_S) = 2 \cdot 2^{-C_k^2}$ .

- Тогда

$$\begin{aligned} P(\cup_{|S|=k} A_S) &\leq \sum_{|S|=k} P(A_S) = 2 \cdot 2^{-C_k^2} \cdot C_n^k = \frac{2}{2^{k(k-1)/2}} \cdot \frac{n(n-1)\dots(n-k+1)}{k!} < \\ &< \frac{2}{2^{k(k-1)/2}} \cdot \frac{n^k}{k!} < \frac{2}{2^{k(k-1)/2}} \cdot \frac{2^{k^2/2}}{k!} = \frac{2^{(k+2)/2}}{k!} < 1, \text{ при } k \geq 3. \end{aligned}$$

- Следовательно, существует раскраска, при которой нет одноцветной клики размера  $k$ .



## Турнир с наименьшим ациклическим подтурниром

- Обозначим через  $v(n)$  наибольшее целое число, для которого всякий турнир на  $n$  вершинах содержит ациклический подтурнир на  $v(n)$  вершинах.
- Другими словами,  $v(n)$  — это такое наибольшее целое число  $v$ , что в любом турнире  $T$  с множеством вершин  $V(T) = \{u_1, \dots, u_n\}$  можно выбрать такую последовательность вершин  $(u_{i_1}, \dots, u_{i_v})$ , что все стрелки между её вершинами будут направлены слева направо (т. е. при  $1 \leq k < \ell \leq n$  имеем  $u_{i_k} u_{i_\ell} \in A(T)$ ).

Теорема (P. Erdős, L. Moser, 1964)

$$v(n) \leq 1 + \lfloor 2 \log_2 n \rfloor.$$

Доказательство. Пусть  $t = 2 + \lfloor 2 \log_2 n \rfloor$ .

- Нужно доказать, что существует такой турнир на  $n$  вершинах, в котором нет ациклического подтурнира на  $t$  вершинах.
- Построим случайный турнир на  $n$  вершинах.
  - ▶ То есть зафиксируем множество вершин  $V(T) = \{u_1, \dots, u_n\}$  и зададим направления его стрелок при помощи  $C_n^2$  подбрасываний монетки.
  - ▶ Все исходы равновероятны. То есть каждая стрелка может быть направлена в любую из двух сторон с вероятностью  $1/2$  и все эти события независимы.

## Доказательство теоремы Эрдёша-Мозера

- Пусть  $\mathcal{P} = \{(u_{i_1}, \dots, u_{i_t}) \mid i_k \neq i_\ell \text{ при } k \neq \ell\}$  — множество всех последовательностей из  $t$  различных вершин.
- Для каждой последовательности  $S = (u_{i_1}, \dots, u_{i_t}) \in \mathcal{P}$  определим событие  $A_S$ :  $\forall k, \ell \in [1..t] (k < \ell \rightarrow u_{i_k} u_{i_\ell} \in A(T))$ .
  - ▶ Тогда  $P(A_S) = 2^{-C_t^2} = 2^{-\frac{t(t-1)}{2}} = 2^{-\frac{t(1+[2\log_2 n])}{2}} \leq 2^{-t \log_2 n} = n^{-t}$ .
  - ▶ Всего последовательностей  $|\mathcal{P}| = A_n^t = n(n-1) \dots (n-t+1) < n^t$ .
- Тогда  $P(\cup_{S \in \mathcal{P}} A_S) \leq \sum_{S \in \mathcal{P}} P(A_S) < n^t n^{-t} = 1$ .
- Следовательно, найдется турнир в котором нет ациклического подтурнира на  $t$  вершинах.  $\square$

### Замечание

- R. Stearns доказал, что  $v(n) \geq 1 + \lfloor \log_2 n \rfloor$ .
- Тем самым,  $1 + \lfloor \log_2 n \rfloor \leq v(n) \leq 1 + \lfloor 2 \log_2 n \rfloor$ .

## $(n, k)$ -универсальные множества

- Пусть  $a = (a_1, \dots, a_n) \in \{0, 1\}^n$  — 0-1 вектор и  $S = \{i_1, \dots, i_k\}$  — набор координат ( $1 \leq i_1 < \dots < i_k \leq n$ ).
- Тогда  $a|_S \stackrel{\text{def}}{=} (a_{i_1}, \dots, a_{i_k})$  — **проекция** вектора  $a$  на координаты из  $S$ .
- Аналогично, если  $A \subset \{0, 1\}^n$ , то  $A|_S \stackrel{\text{def}}{=} \{(a_{i_1}, \dots, a_{i_k}) \mid (a_1, \dots, a_n) \in A\}$  — **проекция** множества  $A$  на координаты из  $S$ .

### Определение

Множество  $A \subset \{0, 1\}^n$  называется  **$(n, k)$ -универсальным**, если для любого набора координат  $S = \{i_1, \dots, i_k\}$ , где  $1 \leq i_1 < \dots < i_k \leq n$ , проекция  $A|_S$  содержит все  $2^k$  возможных комбинаций нулей и единиц.

### Теорема (D. J. Kleitman, J. Spencer, 1973)

Пусть  $n, k, r \in \mathbb{N}$  таковы, что  $n \geq k$  и  $C_n^k 2^k (1 - 2^{-k})^r < 1$ .

Тогда существует  $(n, k)$ -универсальное множество размера  $r$ .

**Доказательство.** Рассмотрим **случайную матрицу**  $M$  размера  $n \times r$  с коэффициентами из  $\{0, 1\}$ .

## Доказательство теоремы Клейтмана-Спенсера

- То есть мы  $nr$  раз подкидываем монетку и определяем значения всех коэффициентов  $m_{ij}$  этой матрицы. Каждый из коэффициентов будет равен 0 или 1 с вероятностью  $1/2$  и все эти события независимы.
- Обозначим через  $A$  множество строк матрицы  $M$ . Её  $i$ -ю строку будем обозначать  $a_i$ .
- Для фиксированного набора координат  $S = \{j_1, \dots, j_k\}$ , где  $1 \leq j_1 < \dots < j_k \leq n$ , и фиксированного вектора  $v \in \{0, 1\}^k$  посчитаем вероятность того, что проекция  $A$  на координаты из  $S$  не содержит  $v$ .
- $$P(v \notin A|_S) = \prod_{i=1}^r P(v \neq a_i|_S) = \prod_{i=1}^r (1 - 2^{-k}) = (1 - 2^{-k})^r.$$
- Тогда вероятность того, что множество  $A$  не является  $(n, k)$ -универсальным не превосходит  $C_n^k 2^k (1 - 2^{-k})^r < 1$ . □

Для того, чтобы показать, как из этой теоремы следует существование  $(n, k)$ -универсального множества малого размера, нам потребуется следующая лемма.

## $(n, k)$ -универсальные множества малого размера

### Лемма

При всех  $x \in \mathbb{R}$  выполнено неравенство  $e^x \geq x + 1$ , причем равенство достигается только при  $x = 0$ .

**Доказательство.** Рассмотрим функцию  $f(x) = e^x - x - 1$ .

- $f'(x) = e^x - 1$ , следовательно,  $f'(x) < 0$  при  $x < 0$  и  $f'(x) > 0$  при  $x > 0$ .
- Тогда  $f(x)$  убывает на  $(-\infty, 0)$  и возрастает на  $(0, +\infty)$ .
- Таким образом, при  $x \neq 0$  имеем  $f(x) > f(0) = 0$ . □

**Следствие** (А. К. Chandra, L. Kou, G. Markowsky, S. Zaks, 1983)

При любых  $n \geq 2$  и  $k \geq 4$  существует  $(n, k)$ -универсальное множество размера не более  $\lceil k2^k \ln n \rceil$ .

**Доказательство.** Пусть  $r = \lceil k2^k \ln n \rceil$ . Тогда

- $C_n^k 2^k (1 - 2^{-k})^r < \frac{n^k}{k!} \cdot 2^k e^{-r/2^k} \leq \frac{(2n)^k}{k!} \cdot e^{-k \ln n} = \frac{(2n)^k}{k!} \cdot n^{-k} = \frac{2^k}{k!} < 1$ .
- Следовательно, по теореме Клейтмана-Спенсера существует  $(n, k)$ -универсальное множество размера  $r$ . □

## $(n, k)$ -универсальные множества малого размера

### Замечание

На самом деле можно доказать, что  $(n, k)$ -универсальные множества размера не более  $\lceil k 2^k \ln n \rceil$  существуют при любых  $k \in \mathbb{N}$  и  $n \geq 2$ .

- Использование математического ожидания в доказательстве комбинаторных фактов основывается на следующих фактах.

### Утверждение

- Пусть  $(\Omega, P)$  — дискретное вероятностное пространство и  $\xi: \Omega \rightarrow X$  — случайная величина, такая, что  $E(\xi) \geq \lambda$ . Тогда существует элементарное событие  $\omega \in \Omega$ , такое, что  $\xi(\omega) \geq \lambda$ .
- Аналогично, если  $E(\xi) \leq \lambda$ , то существует элементарное событие  $\omega \in \Omega$ , такое, что  $\xi(\omega) \leq \lambda$ .

### Доказательство.

- Докажем первое утверждение (второе доказывается аналогично).
- Предположим противное: пусть  $\forall \omega \in \Omega (\xi(\omega) < \lambda)$ .
- Тогда  $E(\xi) = \sum_{\omega \in \Omega} P(\omega)\xi(\omega) < \lambda \sum_{\omega \in \Omega} P(\omega) = \lambda$ . Противоречие. □

# Неравенства Маркова и Чебышёва

## Теорема (Неравенство Маркова)

Пусть  $(\Omega, P)$  — дискретное вероятностное пространство,  $\xi: \Omega \rightarrow X$  — случайная величина, принимающая неотрицательные значения, и  $\lambda > 0$ .

Тогда  $P\{\xi \geq \lambda\} \leq \frac{E\xi}{\lambda}$ .

Доказательство.

$$\bullet E\xi = \sum_{x \in X} xP\{\xi = x\} \geq \sum_{x \geq \lambda} \lambda P\{\xi = x\} = \lambda P\{\xi \geq \lambda\}.$$

□

## Теорема (Неравенство Чебышёва)

Пусть  $\xi: \Omega \rightarrow X$  — произвольная случайная величина и  $\lambda > 0$ .

Тогда  $P\{|\xi - E\xi| \geq \lambda\} \leq \frac{D\xi}{\lambda^2}$ .

Доказательство.

$$\bullet P\{|\xi - E\xi| \geq \lambda\} = P\{(\xi - E\xi)^2 \geq \lambda^2\} \leq \frac{E(\xi - E\xi)^2}{\lambda^2} = \frac{D\xi}{\lambda^2}.$$

□

## Гамильтоновы пути в турнирах

### Теорема (Т. Szele, 1943)

Для любого  $n \in \mathbb{N}$  существует турнир на  $n$  вершинах,  
в котором есть как минимум  $\frac{n!}{2^{n-1}}$  гамильтоновых путей.

**Доказательство.** Рассмотрим случайный турнир  $T$   
на множестве вершин  $V(T) = \{u_1, \dots, u_n\}$ .

- Как и раньше, ориентация всех стрелок определяется при помощи  $C_n^2$  подбрасываний монетки; каждая стрелка будет ориентированна в любую из сторон с вероятностью  $\frac{1}{2}$  и все эти события независимы.
- Для каждой перестановки  $\sigma \in S_n$  обозначим через  $\xi_\sigma$  характеристическую функцию следующего события:  
“последовательность вершин  $(u_{\sigma(1)}, \dots, u_{\sigma(n)})$  — гамильтонов путь”.
- Тогда  $E\xi_\sigma = \frac{1}{2^{n-1}}$ .
- Пусть  $\xi(T) \stackrel{\text{def}}{=} \sum_{\sigma \in S_n} \xi_\sigma(T)$  — случайная величина, означающая количество гамильтоновых путей в случайном турнире  $T$ .
- Тогда  $E(\xi) = \sum_{\sigma \in S_n} E(\xi_\sigma) = \frac{n!}{2^{n-1}}$ .
- Следовательно, существует турнир  $T$ , для которого  $\xi(T) \geq \frac{n!}{2^{n-1}}$ . □

## Доминирующие множества большого размера

### Определение

В графе  $G$  множество  $S \subset V(G)$  называется *доминирующим*, если  $V(G) = S \cup N_G(S)$  (т. е. если любая вершина графа либо принадлежит  $S$ , либо смежна с вершиной из  $S$ ).

### Теорема (N. Alon, 1990)

Пусть  $v(G) = n$  и  $\delta(G) = d$ . Тогда в графе  $G$  есть доминирующее множество размера не более  $n \frac{1+\ln(d+1)}{d+1}$ .

*Доказательство.* Выделим случайное подмножество  $S \subset V(G)$  следующим образом.

- Каждая вершина будет включаться в  $S$  с вероятностью  $p = \frac{\ln(d+1)}{d+1}$ .

Все эти события независимы.

- Тогда  $|S|$  — случайная величина;  $E(|S|) = np$ .

- Для каждого подмножества  $S \subset V(G)$  определим подмножество  $\bar{S} \stackrel{\text{def}}{=} V(G) \setminus (S \cup N_G(S))$ .

- Очевидно, что тогда  $S \cup \bar{S}$  — доминирующее множество.

- Оценим математическое ожидание случайной величины  $|\bar{S}|$ .
- Для этого для каждой вершины  $v \in V(G)$  рассмотрим случайную величину  $\xi_v$ , являющуюся характеристической функцией события " $v \in \bar{S}$ ".
- Тогда  $E\xi_v = (1 - p)^{d_G(v)+1} \leq (1 - p)^{d+1}$ .
- Следовательно,  $E(|\bar{S}|) = \sum_{v \in V(G)} E\xi_v \leq n(1 - p)^{d+1} \leq ne^{-p(d+1)}$ .
- Таким образом,  $E(|S| + |\bar{S}|) \leq np + ne^{-p(d+1)} = n\frac{1+\ln(d+1)}{d+1}$ , откуда и следует существование доминирующего множества размера не более  $n\frac{1+\ln(d+1)}{d+1}$ .



## О графах с большим обхватом и хроматическим числом

- Ниже мы переведем на вероятностный язык доказательство еще одной известной вам из курса теории графов теоремы.

### Теорема (P. Erdős, 1959)

Пусть  $k, g \in \mathbb{N}$ ,  $k, g \geq 3$ . Тогда существует граф  $G$  с  $g(G) \geq g$  и  $\chi(G) \geq k$ .

Доказательство (Alon-Spencer, 1992).

- Зафиксируем число  $\theta \in (0, \frac{1}{g})$ .
- Выберем достаточно большое  $n$  (насколько большим его нужно взять, мы определим позже) и рассмотрим случайный граф  $G$  на  $n$  вершинах, в котором каждая пара вершин соединяется ребром с вероятностью  $p = n^{\theta-1}$  (как и раньше, все такие события независимы).
- Рассмотрим случайные величины  $\xi_i$  — количество циклов длины  $i$  в графе  $G$ , а также  $\xi = \sum_{i=3}^{g-1} \xi_i$  — количество циклов, длина которых меньше  $g$ .
- Оценим математическое ожидание этих случайных величин.

## О графах с большим обхватом и хроматическим числом

### Утверждение 1

$$P\{\xi \geq \frac{n}{2}\} \xrightarrow{n \rightarrow \infty} 0.$$

Доказательство. В графе  $G$  есть  $n^i = n(n-1)\dots(n-i+1)$  последовательностей вершин длины  $i$ .

- ▶ Каждая из них задает цикл длины  $i$  с вероятностью  $p^i$ .
- ▶ Каждый цикл длины  $i$  задается  $2i$  такими последовательностями.
- Итого,  $E\xi_i = \frac{n^i}{2i} \cdot p^i \leq \frac{(np)^i}{2i} = \frac{n^{\theta i}}{2i}$ .
- Тогда  $E\xi = \sum_{i=3}^{g-1} E\xi_i \leq \sum_{i=3}^{g-1} \frac{n^{\theta i}}{2i} \leq n^{\theta g} \sum_{i=3}^{g-1} \frac{1}{2i}$ .
- По неравенству Маркова получаем, что  $P\{\xi \geq \frac{n}{2}\} \leq \frac{2E\xi}{n} \leq n^{\theta g-1} \sum_{i=3}^{g-1} \frac{1}{i}$ .
- Заметим, что  $\theta g - 1 < 0$ . Следовательно,  $n^{\theta g-1} \sum_{i=3}^{g-1} \frac{1}{i} \xrightarrow{n \rightarrow \infty} 0$ .
- Таким образом,  $P\{\xi \geq \frac{n}{2}\} \xrightarrow{n \rightarrow \infty} 0$ .

□

## О графах с большим обхватом и хроматическим числом

- Пусть  $m = \lceil \frac{5}{p} \ln n \rceil$ . Далее мы оценим вероятность того, что  $\alpha(G) \geq m$ .
  - ▶ Отметим, что  $m \geq 5n^{1-\theta} \ln n \xrightarrow{n \rightarrow \infty} \infty$ . В частности, при достаточно больших  $n$ , число  $m$  будет натуральным.

### Утверждение 2

$$P\{\alpha(G) \geq m\} \xrightarrow{n \rightarrow \infty} 0.$$

**Доказательство.** Для любого подмножества  $S \subset V(G)$ , где  $|S| = m$ , вероятность того, что  $S$  — независимое множество, равна  $(1-p)^{C_m^2}$ .

- Тогда  $P\{\alpha(G) \geq m\} \leq C_n^m \cdot (1-p)^{C_m^2} < n^m \cdot (e^{-p})^{\frac{m(m-1)}{2}} = \left(ne^{-\frac{p(m-1)}{2}}\right)^m$ .
  - ▶ Заметим, что при  $n > 2$  выполнено неравенство  $p(m-1) \geq 5 \ln n - p > 4 \ln n$ .
  - ▶ Следовательно,  $e^{-\frac{p(m-1)}{2}} \leq e^{-2 \ln n} = \frac{1}{n^2}$ .
  - ▶ Тогда  $\left(ne^{-\frac{p(m-1)}{2}}\right)^m \leq \frac{1}{n^m} \xrightarrow{n \rightarrow \infty} 0$ .
- Таким образом,  $P\{\alpha(G) \geq m\} \xrightarrow{n \rightarrow \infty} 0$ . □

## О графах с большим обхватом и хроматическим числом

- Итак, мы доказали, что  $P\{\xi \geq \frac{n}{2}\} \xrightarrow{n \rightarrow \infty} 0$  и  $P\{\alpha(G) \geq m\} \xrightarrow{n \rightarrow \infty} 0$ .
- Следовательно, при достаточно больших  $n$  каждая из вышеприведенных вероятностей будет меньше  $\frac{1}{2}$ .
- Выберем  $n$  настолько большим, чтобы выполнялись оба условия:  
 $P\{\xi \geq \frac{n}{2}\} < \frac{1}{2}$  и  $P\{\alpha(G) \geq m\} < \frac{1}{2}$ .
- Тогда найдется такой граф  $G$ , что  $v(G) = n$ ,  $\alpha(G) < m$  и в  $G$  есть не более  $\frac{n}{2}$  циклов, длина которых меньше  $g$ .
- Удалим из каждого такого цикла по вершине. Получим граф  $G'$ , такой, что  $v(G') \geq \frac{n}{2}$ ,  $g(G') \geq g$  и  $\alpha(G') \leq \alpha(G) \leq m - 1 \leq 5n^{1-\theta} \ln n$ .
- Тогда  $\chi(G') \geq \frac{v(G')}{\alpha(G')} \geq \frac{n/2}{5n^{1-\theta} \ln n} = \frac{n^\theta}{10 \ln n}$ , что больше  $k$  при достаточно большом  $n$ .

