

# Летний экзамен по алгебре

hse-ami-open-exams

## Содержание

<b>1</b>	<b>Дискретное вероятностное пространство. Задача о разделе ставки. Вероятностный алгоритм проверки на простоту. Универсальная хеш-функция.</b>	<b>2</b>
1.1	Дискретное вероятностное пространство. . . . .	2
1.2	Задача о разделе ставки. . . . .	2
1.3	Вероятностный алгоритм проверки на простоту. . . . .	2
1.4	Универсальная хеш-функция. . . . .	3
<b>2</b>	<b>Свойства вероятностной меры. Формула включений и исключений. Парадокс распределения подарков. Задача про конференцию.</b>	<b>4</b>
2.1	Свойства вероятностной меры. . . . .	4
2.2	Формула включений и исключений. . . . .	4
2.3	Парадокс распределения подарков. . . . .	4
2.4	Задача про конференцию. . . . .	4
<b>3</b>	<b>Условная вероятность. Независимые события. Отличие попарной независимости и независимости в совокупности.</b>	<b>5</b>
3.1	Условная вероятность. . . . .	5
3.2	Независимые события. . . . .	5
3.3	Отличие попарной независимости и независимости в совокупности. . . . .	5
<b>4</b>	<b>Формула полной вероятности. Формула Байеса. Задача о сумасшедшей старушке. Парадокс Байеса.</b>	<b>6</b>
4.1	Формула полной вероятности. . . . .	6
4.2	Формула Байеса. . . . .	6
4.3	Задача о сумасшедшей старушке. . . . .	6
4.4	Парадокс Байеса. . . . .	6
<b>5</b>	<b>Схема Бернулли. Моделирование бросания правильной монеты. Теорема Муавра-Лапласа. Закон больших чисел для схемы Бернулли.</b>	<b>7</b>
5.1	Схема Бернулли. . . . .	7
5.2	Моделирование бросания правильной монеты. . . . .	7
5.3	Теорема Муавра-Лапласа. . . . .	7
5.4	Закон больших чисел для схемы Бернулли. . . . .	7
<b>6</b>	<b>Случайное блуждание: принцип отражения, задача о баллотировке и задача о возвращении в начало координат. Броуновское движение.</b>	<b>8</b>
6.1	Случайное блуждание: принцип отражения, задача о баллотировке и задача о возвращении в начало координат. . . . .	8
6.2	Броуновское движение. . . . .	8
<b>7</b>	<b>Теорема Пуассона. Распределение Пуассона. Задача про изюм. Пуассоновский процесс.</b>	<b>9</b>
7.1	Теорема Пуассона. . . . .	9
7.2	Распределение Пуассона. . . . .	9
7.3	Задача про изюм. . . . .	9
7.4	Пуассоновский процесс. . . . .	9
<b>8</b>	<b>Марковские цепи. Существование стационарного распределения и сходимость к стационарному распределению.</b>	<b>10</b>
8.1	Марковские цепи. . . . .	10
8.2	Существование стационарного распределения и сходимость к стационарному распределению. . .	10

# 1 Дискретное вероятностное пространство. Задача о разделе ставки. Вероятностный алгоритм проверки на простоту. Универсальная хеш-функция.

## 1.1 Дискретное вероятностное пространство.

Пусть  $\Omega$  – непустое конечное множество элементарных исходов.

**Определение 1.** Всякое подмножество  $A \subseteq \Omega$  называют *событием*.

**Определение 2.** Функцию  $P : 2^\Omega \rightarrow [0, 1]$ , удовлетворяющую следующим свойствам:

- $P(\Omega) = 1$
- $A \cap B = \emptyset \Rightarrow P(A \cup B) = P(A) + P(B)$

называют *вероятностной мерой*, а значение  $P(A)$  *вероятностью события*  $A$ . Вероятностная мера полностью определяется значениями  $P(\{\omega\}) = p_\omega$ , т.е.

$$P(A) = \sum_{\omega \in A} p_\omega$$

Если все элементарные исходы равновозможны, то полагаем  $p_{\omega_1} = \dots = p_{\omega_n} = 1/n$ .

## 1.2 Задача о разделе ставки.

Два человека играют в некоторую игру, причем у обоих шансы победить одинаковые. Они договорились, что тот, кто первым выиграет 6 партий, получит весь приз. Однако игра остановилась раньше, когда первый выиграл пять партий, а второй выиграл три партии. Как справедливо разделить приз?

Предлагается разделить приз в отношении, в котором относятся вероятности выиграть для каждого из игроков в случае продолжения игры. Ясно, что еще надо сыграть не более трех партий. Пространство исходов этих трех партий состоит из восьми элементов, причем только один из этих исходов означает выигрыш второго игрока. Значит приз надо разделить в отношении 7 к 1.

## 1.3 Вероятностный алгоритм проверки на простоту.

Пусть дано некоторое натуральное число  $N > 1$ . Если  $N$  простое число, то по малой теореме Ферма для всякого натурального числа, такого, что  $(b, N) = 1$ , число  $b^{N-1} - 1$  делится на  $N$ . Следовательно, если для некоторого  $b$ , удовлетворяющего условию  $(b, N) = 1$ , число  $b^{N-1} - 1$  не делится на  $N$ , то  $N$  не является простым. Это наблюдение используют для построения простейшего теста на простоту. Если  $b^{N-1} - 1$  не делится на  $N$ , то говорим, что  $N$  не проходит тест для основания  $b$ .

Пусть основание мы выбираем случайно из множества  $\mathbb{Z}_N^*$ . Предположим, что существует такое основание, для которого  $N$  не проходит тест. Какова вероятность выбрать такое основание?

Предположим, что для  $a \in \mathbb{Z}_N^*$  число  $N$  не проходит тест. Если  $N$  проходит тест для основания  $b$ , то для основания  $ab$  число  $N$  уже тест не проходит. В противном случае  $(ab)^{N-1} \equiv_N 1$  и  $(b^{-1})^{N-1} \equiv_N 1$ . Следовательно,  $a^{N-1} \equiv (b^{-1})^{N-1}(ab)^{N-1} \equiv 1$ , что противоречит предположению. Таким образом, каждому основанию  $b$ , для которого  $N$  проходит тест, можно сопоставить основания  $ab$ , для которого результат теста отрицательный. Значит, оснований, для которых  $N$  не проходит тест, не больше оснований, для которых  $N$  проходит тест на простоту. Искомая вероятность не меньше  $1/2$ . Если независимым образом повторять набор основания  $k$  раз, то вероятность выбрать основание, для которого данное число не проходит тест, меньше  $1/2^k$ .

## 1.4 Универсальная хеш-функция.

Пусть  $K = \{0, 1, 2, \dots, n-1\}$  – множество «ключей». Отображение

$$h : K \rightarrow \{0, 1, 2, \dots, m-1\}$$

называется хеш-функцией. Предполагается, что  $m < n$ . Одним из важнейших свойств функции  $h$  является равномерность, когда доля ключей  $k$  с фиксированным значением  $h(k)$  должно быть примерно  $n/m$ . Это означает, что вероятность коллизии  $h(k_1) = h(k_2)$  при  $k_1 \neq k_2$  не больше  $1/m$ . Ясно, что не всегда можно предполагать, что ключи равномерно распределены по таблице. Предположим, что  $h(k) = k \bmod m$  и на вход сначала подаются ключи вида  $m, 2m, 3m, \dots$ . Ясно, что всем таким ключам присваивается хеш-код 0 и реально никакого равномерного распределения значений не происходит. Оказывается, с этой проблемой можно справиться, если перед началом хеширования случайным образом выбрать функцию  $h$  из некоторого набора таких функций. Зафиксируем простое число  $p > n$ . Пусть  $a \in \{1, 2, \dots, p-1\}$  и  $b \in \{0, 1, 2, \dots, p-1\}$ . Положим

$$h_{a,b} = ak + b \bmod p \bmod m.$$

Пара параметров  $(a, b)$  выбирается случайным образом из множества

$$\{1, 2, \dots, p-1\} \times \{0, 1, 2, \dots, p-1\},$$

причем все элементы этого множества считаем равновероятными. Докажем, что для любых  $k_1, k_2 \in \{0, 1, 2, \dots, n-1\}$ ,  $k_1 \neq k_2$ , вероятность коллизии  $h_{a,b}(k_1) = h_{a,b}(k_2)$  не превосходит  $1/m$ .

Заметим, что  $ak_1 + b = ak_2 + b \bmod p$  тогда и только тогда, когда  $k_1 = k_2$ . Кроме того, для различных  $k_1$  и  $k_2$  по значениям  $ak_1 + b \bmod p$  и  $ak_2 + b \bmod p$  однозначно находятся числа  $a$  и  $b$ . Пусть  $k_1 \neq k_2$ . Отображение

$$(a, b) \rightarrow (ak_1 + b \bmod p, ak_2 + b \bmod p)$$

является биекцией множества

$$\{1, 2, \dots, p-1\} \times \{0, 1, 2, \dots, p-1\}$$

на множество

$$(\{0, 1, 2, \dots, p-1\} \times \{0, 1, 2, \dots, p-1\}) \setminus \{(i, i) \mid 0 \leq i \leq p-1\}.$$

Остается отметить, что для всякого  $t \in \{0, 1, 2, \dots, p-1\}$  количество чисел  $s \in \{0, 1, 2, \dots, p-1\}$  таких, что  $s \neq t$  и  $s = t \bmod m$ , не превосходит  $(p-1)/m$ , т.е. вероятность выбора такой пары  $(t, s)$  или, что эквивалентно, выбора пары  $(a, b)$ , у которой  $h_{a,b}(k_1) = h_{a,b}(k_2)$ , не превосходит  $1/m$ .

## 2 Свойства вероятностной меры. Формула включений и исключений. Парадокс распределения подарков. Задача про конференцию.

2.1 Свойства вероятностной меры.

2.2 Формула включений и исключений.

2.3 Парадокс распределения подарков.

2.4 Задача про конференцию.

### **3 Условная вероятность. Независимые события. Отличие попарной независимости и независимости в совокупности.**

**3.1 Условная вероятность.**

**3.2 Независимые события.**

**3.3 Отличие попарной независимости и независимости в совокупности.**

## 4    Формула полной вероятности. Формула Байеса. Задача о сумасшедшей старушке. Парадокс Байеса.

4.1    Формула полной вероятности.

4.2    Формула Байеса.

4.3    Задача о сумасшедшей старушке.

4.4    Парадокс Байеса.

## 5 Схема Бернулли. Моделирования бросания правильной монеты. Теорема Муавра-Лапласа. Закон больших чисел для схемы Бернулли.

### 5.1 Схема Бернулли.

### 5.2 Моделирования бросания правильной монеты.

### 5.3 Теорема Муавра-Лапласа.

### 5.4 Закон больших чисел для схемы Бернулли.

- 6   Случайное блуждание: принцип отражения, задача о баллотировке и задача о возвращении в начало координат. Броуновское движение.
- 6.1   Случайное блуждание: принцип отражения, задача о баллотировке и задача о возвращении в начало координат.
- 6.2   Броуновское движение.



## 7 Теорема Пуассона. Распределение Пуассона. Задача про изюм. Пуассоновский процесс.

7.1 Теорема Пуассона.

7.2 Распределение Пуассона.

7.3 Задача про изюм.

7.4 Пуассоновский процесс.

## 8 Марковские цепи. Существование стационарного распределения и сходимость к стационарному распределению.

### 8.1 Марковские цепи.

### 8.2 Существование стационарного распределения и сходимость к стационарному распределению.