

# Дискретная математика

Вдовец Илья, Войко Андрей и Глебский Никита

17 марта 2023 г.

## Содержание

|  |           |
|--|-----------|
| <b>1 Лекция 13</b>   | <b>6</b>  |
| 1.1 Вероятность . . . . .  | 6         |
| 1.2 Свойства вероятности . . . . .   | 6         |
| 1.3 Оценка объединения . . . . .   | 7         |
| 1.4 Нижняя оценка на числа Рамсея . . . . .  | 7         |
| 1.5 Формула включений-исключений в вероятностном смысле . . . . .  | 7         |
| <b>2 Лекция 14</b>   | <b>8</b>  |
| 2.1 Задача о беспорядках. . . . .  | 8         |
| 2.2 Условная вероятность . . . . .   | 9         |
| 2.3 Формулы Байеса и полной вероятности. . . . .   | 9         |
| 2.4 Независимые события. . . . .   | 11        |
| <b>3 Лекция 15</b>   | <b>11</b> |
| 3.1 Раскраски графов. Хроматическое число графа. . . . .   | 11        |
| 3.2 Конструкция Зыкова-Мыцельского графа без треугольников со сколь угодно большим хроматическим числом. . . . . | 13        |
| 3.3 Хроматический многочлен. . . . .   | 14        |
| <b>4 Лекция 16</b>   | <b>16</b> |
| 4.1 Математическое ожидание . . . . .  | 16        |
| 4.2 Неравенство Маркова . . . . .  | 16        |
| 4.3 Дисперсия . . . . .  | 17        |
| 4.4 Неравенство Чебышева . . . . .   | 17        |
| 4.5 Общий случай вероятностного метода . . . . .   | 18        |
| <b>5 Лекция 17</b>   | <b>18</b> |
| 5.1 Вероятностный метод. Разрезы в графах. . . . .   | 18        |
| 5.2 Независимые случайные величины . . . . .   | 19        |
| 5.3 Оценка биномиальных коэффициентов . . . . .  | 20        |
| 5.4 Неравенство Чернова . . . . .  | 21        |
| <b>6 Лекция 18</b>   | <b>22</b> |
| 6.1 Производящие функции . . . . .   | 22        |
| 6.2 Дифференцирование . . . . .  | 23        |
| 6.3 Пример применения . . . . .  | 24        |
| 6.4 Ещё один пример применения (бонусный) . . . . .  | 24        |

|  |           |
|--|-----------|
| <b>7 Лекция 19</b>   | <b>25</b> |
| 7.1 Неупорядоченные выборки . . . . .  | 25        |
| 7.2 Бином Ньютона . . . . .  | 25        |
| 7.3 Линейные рекуррентные соотношения с постоянными коэффициентами . . . . . | 26        |
| 7.4 Теорема о реккуррентном соотношении . . . . .                            | 26        |
| 7.5 Нахождение общей формулы для $a_n$ . . . . .                             | 27        |
| 7.6 Числа Каталана . . . . .   | 27        |
| <b>8 Лекция 20</b>   | <b>29</b> |
| 8.1 Комбинаторные игры(определения и примеры) . . . . .                      | 29        |
| 8.2 Теорема о цене игры . . . . .  | 30        |
| <b>9 Лекция 21</b>   | <b>31</b> |
| 9.1 N и P позиции (выигрышные и проигрышные) . . . . .                       | 31        |
| 9.2 Игра Ним . . . . .   | 32        |
| 9.3 Задача об угадывании числа . . . . .                                     | 33        |
| 9.4 Разрешающие деревья . . . . .  | 33        |
| 9.5 Примеры задач . . . . .  | 34        |
| 9.5.1 Задача о взвешивании . . . . .   | 34        |
| 9.5.2 Задача о связности графа . . . . .                                     | 35        |
| <b>10 Лекция 22</b>  | <b>36</b> |
| 10.1 Булевы схемы . . . . .  | 36        |
| 10.2 Сложение двоичных чисел . . . . .                                       | 37        |
| 10.3 Вычисление произвольной функции . . . . .                               | 38        |
| <b>11 Лекция 23</b>  | <b>39</b> |
| 11.1 Функция $XOR_n$ . . . . .   | 39        |
| 11.2 Глубина схемы . . . . .   | 42        |
| 11.3 Формулы . . . . .   | 44        |
| 11.4 Задачи выполнимости . . . . .   | 45        |
| <b>12 Лекция 24</b>  | <b>46</b> |
| 12.1 Задача выполнимости . . . . .   | 46        |
| 12.2 Теорема о балансировке булевых функций . . . . .                        | 47        |
| <b>13 Семинар 16</b>   | <b>48</b> |
| 13.1 Задача 1 . . . . .  | 48        |
| 13.2 Задача 2 . . . . .  | 48        |
| 13.3 Задача 3 . . . . .  | 48        |
| 13.4 Задача 4 . . . . .  | 49        |
| 13.5 Задача 5 . . . . .  | 49        |
| 13.6 Задача 6 . . . . .  | 49        |
| 13.7 Задача 7 . . . . .  | 50        |
| 13.8 Задача 8 . . . . .  | 50        |
| 13.9 Задача 9 . . . . .  | 50        |
| 13.10 Задача 10 . . . . .  | 50        |

|   |           |
|---|-----------|
| <b>14 Семинар 17</b>                      | <b>51</b> |
| 14.1 Задача 1                             | 51        |
| 14.2 Задача 2 (дублирует 8 с семинара 16) | 51        |
| 14.3 Задача 3                             | 51        |
| 14.4 Задача 4                             | 52        |
| 14.5 Задача 5                             | 52        |
| 14.6 Задача 6                             | 52        |
| 14.7 Задача 7                             | 52        |
| <b>15 Семинар 18</b>                      | <b>53</b> |
| 15.1 Задача 1                             | 53        |
| 15.2 Задача 2                             | 53        |
| 15.3 Задача 3                             | 53        |
| 15.4 Задача 4                             | 54        |
| 15.5 Задача 5                             | 54        |
| 15.6 Задача 6                             | 54        |
| 15.7 Задача 7                             | 54        |
| 15.8 Задача 8                             | 55        |
| 15.9 Задача 9                             | 55        |
| <b>16 Семинар 19</b>                      | <b>56</b> |
| 16.1 Задача 1                             | 57        |
| 16.2 Задача 2                             | 57        |
| 16.3 Задача 3                             | 57        |
| 16.4 Задача 4                             | 58        |
| 16.5 Задача 5                             | 58        |
| 16.6 Задача 6                             | 58        |
| 16.7 Задача 7                             | 58        |
| 16.8 Задача 8                             | 58        |
| 16.9 Задача 9                             | 58        |
| 16.10 Задача 10                           | 59        |
| <b>17 Домашнее задание 13</b>             | <b>59</b> |
| 17.1 Задача 1                             | 59        |
| 17.2 Задача 3                             | 59        |
| 17.3 Задача 2                             | 59        |
| 17.4 Задача 4                             | 59        |
| 17.5 Задача 6                             | 60        |
| 17.6 Задача 5                             | 60        |
| 17.7 Задача 7                             | 60        |
| 17.8 Задача 8                             | 61        |
| <b>18 Домашнее задание 14</b>             | <b>61</b> |
| 18.1 Задача 3                             | 61        |
| 18.2 Задача 2                             | 61        |
| 18.3 Задача 1                             | 62        |

|                               |           |
|-------------------------------|-----------|
| 18.4 Задача 4                 | 62        |
| 18.5 Задача 5                 | 62        |
| 18.6 Задача 6                 | 63        |
| 18.7 Задача 7                 | 63        |
| 18.8 Задача 8                 | 64        |
| <b>19 Домашнее задание 16</b> | <b>64</b> |
| 19.1 Задача 1                 | 64        |
| 19.2 Задача 2                 | 65        |
| 19.3 Задача 3                 | 65        |
| 19.4 Задача 4                 | 66        |
| 19.5 Задача 5                 | 66        |
| 19.6 Задача 6                 | 67        |
| <b>20 Домашнее задание 17</b> | <b>68</b> |
| 20.1 Задача 1                 | 68        |
| 20.2 Задача 2                 | 68        |
| 20.3 Задача 3                 | 69        |
| 20.4 Задача 4                 | 69        |
| 20.5 Задача 5                 | 69        |
| <b>21 Домашнее задание 18</b> | <b>70</b> |
| 21.1 Задача 1                 | 70        |
| 21.2 Задача 2                 | 70        |
| 21.3 Задача 3                 | 70        |
| 21.4 Задача 4                 | 71        |
| 21.5 Задача 5                 | 71        |
| 21.6 Задача 6                 | 71        |
| <b>22 Домашнее задание 19</b> | <b>72</b> |
| 22.1 Задача 1                 | 72        |
| 22.2 Задача 2                 | 73        |
| 22.3 Задача 3                 | 73        |
| 22.4 Задача 4                 | 74        |
| 22.5 Задача 5                 | 75        |
| <b>23 Домашнее задание 20</b> | <b>76</b> |
| 23.1 Задача 1                 | 77        |
| 23.2 Задача 2                 | 77        |
| 23.3 Задача 4                 | 78        |
| 23.4 Задача 5                 | 78        |
| <b>24 Домашнее задание 21</b> | <b>79</b> |
| 24.1 Задача 1                 | 79        |
| 24.2 Задача 2                 | 79        |
| 24.3 Задача 3                 | 80        |
| 24.4 Задача 4                 | 80        |

|                               |           |
|-------------------------------|-----------|
| 24.5 Задача 5 . . . . .       | 80        |
| <b>25 Домашнее задание 22</b> | <b>81</b> |
| 25.1 Задача 1 . . . . .       | 81        |
| 25.2 Задача 2 . . . . .       | 81        |
| 25.3 Задание 3 . . . . .      | 82        |
| 25.4 Задача 4 . . . . .       | 82        |
| 25.5 Задача 5 . . . . .       | 83        |
| 25.6 Задача 6 . . . . .       | 83        |
| 25.7 Задача 7 . . . . .       | 84        |
| 25.8 Задача 8 . . . . .       | 84        |
| 25.9 Задача 9 . . . . .       | 85        |

# 1 Лекция 13

(Андрей)

## 1.1 Вероятность

$\Omega = \{\omega_0, \omega_1, \dots, \omega_n\}$  - пространство элементарных исходов. Будем считать, что это множество конечно.

Зададим следующее отображение  $P : \Omega \rightarrow [0,1]$ , причем  $\sum_{i=1}^n P(\omega_i) = 1$ . Такое отображение называется вероятностным распределением. Число  $P(\omega_i)$  называют вероятностью исхода  $\omega_i \in \Omega$ .

Событие - это подмножество  $A$  пространства элементарных исходов  $\Omega$ . Вероятность события  $A$ :  $P(A) = \sum_{x \in A} P(x)$ .

Равновероятная модель:  $P(w) = \frac{1}{n}$ ,  $P(A) = \frac{|A|}{n}$ .

Примеры (в равновероятной модели):

- Найдем вероятность выпадения орла при подбрасывании монеты. Обозначим орла за 1, решку - за 0. Тогда  $\Omega = \{0, 1\}$ , а  $P(1) = P(0) = \frac{1}{2}$ .
- Теперь кидаем кубик. Тогда  $\Omega = \{0, 1, 2, 3, 4, 5, 6\}$ . Найдем вероятность выпадения четного числа. Тогда  $A = \{2, 4, 6\}$ , и  $P(A) = \frac{3}{6}$ .
- Теперь подбросили монетку 6 раз. Тогда  $\Omega = \{0, 1\}^6$ . Пусть событие  $A$  - "выпало 3 орла". Тогда  $P(A) = \frac{|A|}{|\Omega|} = \frac{C_6^3}{2^6}$ .
- Теперь подбросили монету  $n$  раз. Тогда  $\Omega = \{0, 1\}^n$ . Рассмотрим следующее событие  $A$  - "в  $i$ -ом подбрасывании выпал орел". Честно покажем, почему вероятность этого события равна  $\frac{1}{2}$ . Так как  $A = \{(a_1, \dots, 1, \dots, a_n) : a_i \in [0,1]\}$ , то  $P(A) = \frac{2^{n-1}}{2^n} = \frac{1}{2}$ .
- Случайная перестановка.** Рассмотрим перестановки на трех элементах, то есть  $\Omega = S_3$ . Мы хотим случайным образом выбрать какую-то перестановку, и так как перестановок всего 6, то каждую перестановку можно задать с вероятностью  $\frac{1}{6}$ . Но мы поступим по-другому: 1-е число перестановки выберем равновероятно из  $\{1, 2, 3\}$ , 2-е число выберем равновероятно из оставшихся двух чисел, а 3-е число определится автоматически. Эту светлую мысль хочется записать строго, поэтому давайте изобразим нашу ситуацию в виде дерева.



Здесь на ребрах указана вероятность выбора каждой из цифр. В нашем случае  $\Omega$  - это листья, а итоговая вероятность выбрать одну перестановку будет равна произведению чисел на ребрах в пути от корня до  $\Omega$ . В данном случае вероятность каждого исхода равна  $\frac{1}{6}$ .

## 1.2 Свойства вероятности

- $P(\emptyset) = 0, P(\Omega) = 1$
- Пусть  $A, B \subseteq \Omega, A \cap B = \emptyset$ , тогда  $P(A \sqcup B) = P(A) + P(B)$
- $P(\bar{A}) = 1 - P(A)$
- Если  $A \subseteq B$ , то  $P(A) \leq P(B)$

### 1.3 Оценка объединения

Пусть  $A_1, A_2, \dots, A_s \subseteq \Omega$ . Тогда  $P(A_1 \cup A_2 \cup \dots \cup A_s) \leq P(A_1) + P(A_2) + \dots + P(A_s)$ .

#### Доказательство

По определению  $P(\bigcup_{i=1}^n A_i) = \sum_{x \in A_1 \cup \dots \cup A_s} P(x) = [\sum_{x \in A_1} P(x_1)] + [\sum_{x \in A_2 \setminus A_1} P(x_2)] + [\sum_{x \in A_3 \setminus (A_1 \cup A_2)} P(x_3)] + \dots + [\sum_{x \in A_s \setminus (A_1 \cup \dots \cup A_{s-1})} P(x_s)] \leq P(A_1) + P(A_2) + \dots + P(A_s)$ .

### 1.4 Нижняя оценка на числа Рамсея

Докажем следующую теорему:  $R(k, k) > 2^{\frac{k-1}{2}}$ .

#### Доказательство

Рассмотрим  $n \leq 2^{\frac{k-1}{2}}$ ,  $n \in \mathbb{N}$ . Построим граф на  $n$  вершинах так, чтобы не было клик и независимых множеств размера  $k$ . Возьмем случайный граф. Что это значит? Это значит, что мы рассматриваем следующее вероятностное пространство  $\Omega = \{\text{все графы на множестве вершин } 1, 2, \dots, n\}$ . Тогда  $|\Omega| = 2^{C_n^2}$  (всего ребер в граfe на  $n$  вершинах  $C_n^2$ , а различных подмножеств этих ребер как раз  $2^{C_n^2}$ ). Рассмотрим вероятность события  $A$  - "в граfe есть клика размера  $k$  или независимое множество размера  $k$ ".

Рассмотрим произвольное подмножество  $w$  множества вершин:  $w \subset \{1, 2, \dots, n\}$ ,  $|w| = k$ . Тогда рассмотрим следующее событие  $A_w$  - "в граfe именно данное фиксированное  $w$  является кликой или независимым множеством". Тогда  $P(A) = P(\bigcup_{w \subset \{1, \dots, n\}} A_w)$ , причем для таких  $w$  выполняется, что  $|w| = k$ . Воспользуемся оценкой объединения (см. пункт 1.3)

и получим:  $P(\bigcup_{w \subset \{1, \dots, n\}} A_w) \leq \sum_{w \subset \{1, \dots, n\}} P(A_w)$ , причем  $P(A_w) = 2 \cdot \frac{2^{C_n^2 - C_k^2}}{2^{C_n^2}} = 2^{1 - C_k^2}$  ( $C_n^2 - C_k^2$  - количество ребер в исходном

графе без ребер в  $w$ ; умножаем на 2, потому что  $w$  может быть как кликой, так и независимым множеством). Тогда  $\sum_{w \subset \{1, \dots, n\}} P(A_w) = C_n^k \cdot 2^{1 - C_k^2} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k!} \cdot 2^{1 - C_k^2} \leq \frac{n^k}{k!} \cdot 2^{1 - C_k^2} \leq \frac{2^{\frac{k \cdot (k-1)}{2}} \cdot 2^{1 - C_k^2}}{k!} = \frac{2}{k!} \leq \frac{1}{3}$ . Эта оценка показывает,

что вероятность того, что в граfe нет ни клики размера  $k$ , ни независимого множества размера  $k$  хотя бы  $\frac{2}{3}$ . Но это как раз означает, что существует граf на  $n$  вершинах, в котором нет ни клики размера  $k$ , ни независимого множества размера  $k$ , поэтому  $R(k, k) > 2^{\frac{k-1}{2}}$ , что и требовалось доказать. (скорее всего, Вы офигели с этого доказательства, поэтому попробуйте это перечитать под запись от лектора).

### 1.5 Формула включений-исключений в вероятностном смысле

**Теорема:**  $P(A_1 \cup A_2 \cup \dots \cup A_n) = P(A_1) + P(A_2) + \dots + P(A_n) - P(A_1 \cap A_2) - \dots - P(A_{n-1} \cap A_n) + \dots (-1)^{n-1} \cdot P(A_1 \cap A_2 \cap \dots \cap A_n)$ .

#### Доказательство

Для начала введем характеристическую функцию  $\chi_A : \Omega \rightarrow \{0, 1\}$ . Тогда для множества  $A$  такого, что  $A \subseteq \Omega$ , определим:

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Отметим следующие свойства этой функции:

$$\chi_{\bar{A}}(x) = 1 - \chi_A(x)$$

$$\chi_{A \cap B}(x) = \chi_A(x) \chi_B(x)$$

Положим для начала  $A = A_1 \cup A_2 \cup \dots \cup A_n$ . Применим сначала те же рассуждения, которые мы применяли при доказательстве этой формулы ранее для мощностей множеств.

$$\begin{aligned} \chi_{A_1 \cup A_2 \cup \dots \cup A_n} &= \chi_{\overline{\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}}} = 1 - \chi_{\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}} = \\ &= 1 - \chi_{\overline{A_1}} \chi_{\overline{A_2}} \dots \chi_{\overline{A_n}} = 1 - (1 - \chi_{A_1})(1 - \chi_{A_2}) \dots (1 - \chi_{A_n}) = \sum_{k=1}^n \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} (-1)^{k+1} \chi_{A_{i_1}} \chi_{A_{i_2}} \dots \chi_{A_{i_k}} \end{aligned}$$

Далее, перейдя к вероятности, имеем:  $P(A) = \sum_{x \in A} P(x) = \sum_{x \in \Omega} P(x) \cdot \chi_A(x)$ . Теперь, подставляя вместо  $A$  объединение множеств  $A_1 \cup A_2 \cup \dots \cup A_n$  и вместо  $\chi_A(x)$  выражение  $1 - (1 - \chi_{A_1})(1 - \chi_{A_2}) \dots (1 - \chi_{A_n})$ , раскроем скобки и получим

следующую красоту:

$$P(A_1 \cup A_2 \cup \dots \cup A_n) = \sum_{k=1}^n \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} (-1)^{k+1} P(A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k})$$

## 2 Лекция 14

(Илья)

### 2.1 Задача о беспорядках.

**Беспорядок** - это перестановка  $\sigma = (\begin{smallmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{smallmatrix}) \forall i \sigma_i \neq i$

Обозначим за  $\Omega_n = S_n$  - множество всех перестановок на числах  $1, 2, \dots, n$

В равновероятной модели вероятность выбрать случайную перестановку  $P(\sigma) = \frac{1}{n!}$ , воспользуемся этим, чтобы решить задачу о беспорядках (то есть будем полагать, что все перестановки равновероятны).

$A_n \subseteq \Omega_n$  - это множество беспорядков на  $n$  элементах.

Так вот, сама формулировка задачи:

**Посчитать вероятность того, что случайно выбранная перестановка окажется беспорядком.**

1. Будем считать её через вероятность дополнения.  $P(A_n) = 1 - P(\overline{A_n})$

То есть  $P(\overline{A_n})$  - это вероятность того, что случайно выбранная перестановка оставила на месте **хотя бы** один элемент от 1 до  $n$

Вероятность "**хотя бы**" очень удобно считать по формуле включений и исключений, введём пару обозначений и так и сделаем.

Обозначим за  $B_i \subseteq \Omega_n$  перестановку, которая оставляет элемент  $i$  на своём месте.

2.  $\overline{A_n} = B_1 \cup B_2 \cup \dots \cup B_n$ . Тогда

$$P(\overline{A_n}) = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} P(B_{i_1} \cap B_{i_2} \cap \dots \cap B_{i_k})$$

Чему равна вероятность  $P(B_{i_1} \cap B_{i_2} \cap \dots \cap B_{i_k})$ ? То есть это вероятность того, что на  $i_1, i_2, \dots, i_k$  местах ничего не переставилось, а на остальных переставилось или нет, мы не знаем. Легко понять, что это  $\frac{(n-k)!}{n!}$

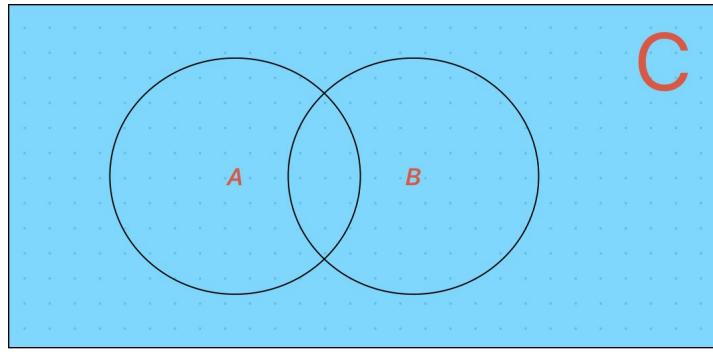
3. Как теперь зная это можно посчитать искомую вероятность дополнения? Очень просто! Надо понять, что второе суммирование производится по всем неподвижным точкам, коих  $k$  штук. То есть тогда можно записать так:

$$P(\overline{A_n}) = \sum_{k=1}^n (-1)^{k+1} \cdot \frac{(n-k)!}{n!} \cdot \binom{n}{k} = \sum_{k=1}^n (-1)^{k+1} \cdot \frac{(n-k)!}{n!} \cdot \frac{n!}{k!(n-k)!} = \sum_{k=1}^n (-1)^{k+1} \cdot \frac{1}{k!}$$

Окончательно получаем, что  $P(A_n) = 1 - \sum_{k=1}^n (-1)^{k+1} \cdot \frac{1}{k!}$

Вам этот ряд ничего не напоминает? Конечно же это похоже на  $e^{-1}$  (А если не похоже, то напомню факт  $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ ). Тогда  $\lim_{n \rightarrow \infty} P(A_n) = \frac{1}{e}$

## 2.2 Условная вероятность



$C$  - это вероятностное пространство.

Пусть  $A \subseteq C$  - это событие, которое произошло ( $P(A) > 0$ ),  $B \subseteq C$  - это событие, которое мы хотим посчитать, при условии того, что событие  $A$  уже произошло.

Формула условной вероятности:

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

Пример:

*Задача:* У нас имеется 9 коробочек(они лежат на столе пронумерованные). Разрешается делать пару вещей:

1. Выбрать равновероятно одну коробку.
2. Равновероятно положить или не положить в неё монетку.

Известно после открытия, что в первых 8 коробках монетки нет. **Какова вероятность того, что в 9-ой коробке лежит монетка?**

*Решение:*

1. Пусть  $A$  - событие 'монет нет в первых 8 коробках', а  $B$  - событие 'монета в 9-ой коробке', тогда мы хотим найти  $P(B|A) = \frac{P(A \cap B)}{P(A)}$
2. В любой задаче на вероятность надо сначала выбрать вероятностное пространство. Пусть  $C = \{(i,j) | 1 \leq i \leq 9, j = 0,1\}$ , где  $i$  - номер коробки,  $j$  - есть монета или нет.  
Тогда понятно, что  $P((i,j)) = \frac{1}{18}$  (это можно легко осознать, нарисовав дерево вероятностное)
3. Теперь мы имеем, что  $A = \{(i,0) | i = 1, 2, \dots, 8\} \cup \{(9,1)\}$ ,  $B = \{(9,1)\}$ . Значит  $|A| = 10$  и  $|B| = 1$ . Ну тогда искомая вероятность  $P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{1}{10}$

Перепишем формулу немного по-другому:  $P(B|A) \cdot P(A) = P(A \cap B)$ . Эту формулу можно обобщить на произвольное количество событий.

**Теорема умножения.**

Пусть имеется  $A_1, A_2, \dots, A_n \subseteq C$  - события положительной вероятности. Тогда  $P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_n) \cdot P(A_{n-1}|A_n) \cdot P(A_{n-2}|A_{n-1} \cap A_n) \cdot \dots \cdot P(A_1| \bigcap_{i=2}^n A_i)$  Более строго это утверждение можно доказать по индукции, но оставим это в качестве упражнения.

## 2.3 Формулы Байеса и полной вероятности.

**Формула Байеса.** Пусть  $A, B \subseteq C$  - события положительной вероятности, тогда  $P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$

Доказательство этого факта очевидно.

**Пример про болезни.**

Предположим есть болезнь и мы хотим знать болен ли человек или нет. Существует 2 теста: дешёвый (менее точный) и дорогой (более точный). Мы можем отправить человека сначала на дешёвое тестирование. Если тест показал положительный результат, то отправляем его на дорогое тестирование, которое почти гарантированно может дать точный результат, иначе отправляем его сразу домой. **Хотим понять с какой вероятностью мы отпустим больного человека домой.**

*Решение:*

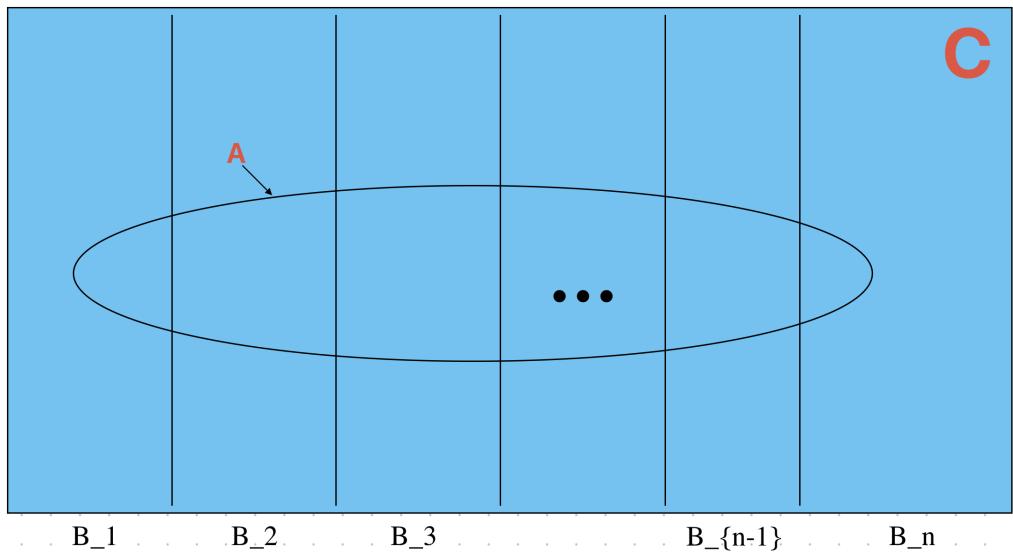
1. Пусть  $B$  - событие 'человек болен',  $A$  - событие 'дешёвый тест показал "не болен"', тогда нужно посчитать  $P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$ . Давайте посчитаем искомую вероятность через две другие:  $P(\bar{A}|B)$  и  $P(B|\bar{A})$ .
2. Заметим, что  $P(B|\bar{A})$  мы знаем, потому что это в точности то, что нам выдаёт дорогой тест, но как же посчитать  $P(\bar{A}|B)$ ? По формуле Байеса!
- Окей. Осталось понять, как считать искомую вероятность, зная  $P(\bar{A}|B)$ .
- Заметим, что  $P(A|B) + P(\bar{A}|B) = \frac{P(\bar{A} \cap B) + P(A \cap B)}{P(B)} = 1$ . Это легко увидеть, так как сумма вероятностей несовместных событий есть вероятность объединения этих событий. Получаем в числителе  $P(B)$ .
- Ну и всё, зная  $P(A|B)$ , находим искомую вероятность по той же формуле Байеса.

**Формула полной вероятности.** Пусть  $B_1, B_2, \dots, B_n \subseteq C$  - это события с положительной вероятностью и  $B_1 \sqcup B_2 \sqcup \dots \sqcup B_n = C$  ( $B_i \cap B_j = \emptyset, i \neq j$ )

Тогда вероятность произвольного события  $A \subseteq C$  равна  $\sum_{i=1}^n P(A|B_i) \cdot P(B_i)$ .

**Доказательство:**

1. Сделаем наглядный рисунок, демонстрирующий разбиение вероятностного пространства  $C$  на не пересекающиеся множества.



2. Тогда  $A = (A \cap B_1) \sqcup (A \cap B_2) \sqcup \dots \sqcup (A \cap B_n)$ , откуда  $P(A) = \sum_{i=1}^n (A \cap B_i) = \sum_{i=1}^n P(A|B_i) \cdot P(B_i)$ .

**Ч.Т.Д.**

**Пример о распределении на рёбрах графа.** Предположим у нас есть граф  $G = (V, E)$ ,  $|V| = n$ ,  $\forall v \in V, \deg(v) = d$  ( $G$  - регулярный граф, потому что степень каждой вершины константа.)

**Мы хотим случайно выбрать ребро этого графа.** Есть несколько способов это сделать:

1. Равновероятно выбрать из множества рёбер.
2. Сначала равновероятно выбрать вершину этого графа, а потом равновероятно выбрать ребро, смежное этой вершине.

Формально это разные конструкции, но с точки зрения распределения на рёбрах это эквивалентные построения, давайте покажем это.

В случае 1:

$P(e) = \frac{1}{\frac{n \cdot d}{2}} = \frac{2}{nd}$  (по лемме о рукопожатиях, так как сумма степеней вершин есть удвоенное число рёбер)

В случае 2:

Пусть  $B_i$  - событие 'была выбрана  $i$ -ая вершина', тогда  $P(e) = \sum_{i=1}^n P(e|B_i) \cdot P(B_i) = \sum_{i=1}^n P(e|B_i) \cdot \frac{1}{n}$

Тут надо подумать, когда  $P(e|B_i)$  не ноль. Ну она не ноль только при двух конкретных  $i$ . Поэтому  $P(e) = \frac{1}{d} \cdot \frac{1}{n} + \frac{1}{d} \cdot \frac{1}{n} = \frac{2}{dn}$

Далее идёт ещё один пример с болезнью, но он идентичен первому, просто с числами, не вижу смысла вставлять его ещё раз.

## 2.4 Независимые события.

Сначала дадим парочку определений, которые нужно отличать.

**Несовместные события**  $A$  и  $B \subseteq C$  называются таковыми, если  $P(A \cap B) = 0$ .

**Независимые события**  $A$  и  $B \subseteq C$  называются таковыми, если  $P(A \cap B) = P(A) \cdot P(B)$ .

**Замечание:** Если  $P(B) > 0$ , то независимость  $A$  и  $B$  равносильна  $P(A|B) = \frac{P(A \cap B)}{P(B)} = P(A)$ .

Далее шёл пример с подбрасыванием монетки, но он очень простой.

Что если я хочу определить независимость большего числа событий? Пусть  $A_1, A_2, \dots, A_n \subseteq C$  называются независимыми в совокупности, если  $\forall i_1 < i_2 < \dots < i_k P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_{i_1}) \cdot P(A_{i_2}) \cdot \dots \cdot P(A_{i_k})$

Далее опять пример с монеткой, но он опять же довольно очевидный.

## 3 Лекция 15

(Никита)

### 3.1 Раскраски графов. Хроматическое число графа.

Для начала введём несколько обозначений, которые будут использоваться на протяжении всей лекции:

- $G = (V, E)$  - неориентированный граф без петель и кратных рёбер.
- $n$  - количество рёбер в графе  $G$ ,  $|V|$ .
- $\deg v$  - степень вершины  $v$  в  $G$ .
- $\Delta(G)$  - максимальная степень в  $G$ .
- $\omega(G)$  - размер максимальной клики в  $G$  (кликовое число).
- $\alpha(G)$  - число независимости в  $G$ , размер максимального независимого множества в  $G$ .

Дадим определение раскраски:

**Раскраска (правильная) графа  $G$  в  $k$  цветов** - это

$$f : V \rightarrow \{1, 2, \dots, k\} : \forall v_1, v_2 \in V : \{v_1, v_2\} \in E \Rightarrow f(v_1) \neq f(v_2)$$

**Хроматическое число**  $G$  - это минимальное число цветов, в которые можно раскрасить  $G$ .

Обозначение:  $\chi(G)$ .

**Замечание.**  $\chi(G) = \min\{k \in \mathbb{N} \mid V = V_1 \sqcup V_2 \sqcup \dots \sqcup V_k, \forall V_i \text{ - независимое множество}\}$ .

Если мы разбили граф на независимые множества - красим каждое независимое множество в свой цвет, и наоборот - если смогли раскрасить граф в  $k$  цветов, то все вершины одного цвета обязаны образовывать независимое множество. Тогда понятно, что хроматическое число - это и есть минимальное кол-во множеств в разбиении вершин на независимые множества.

**Свойства хроматического числа:**

1.  $\chi(G) \geq \omega(G)$ . На клику требуется  $\omega(G)$  цветов, т.к. каждые две вершины в ней соединены ребром.
2.  $\chi(G) \geq \frac{n}{\alpha(G)}$ .

**Доказательство:**

$\chi(G) = k$  и  $V = V_1 \sqcup V_2 \sqcup \dots \sqcup V_k$ , где  $V_i$  - независимое множество.

$$|V_i| \leq \alpha(G) \Rightarrow n \leq k \cdot \alpha(G) \Rightarrow k \geq \frac{n}{\alpha(G)} \blacksquare$$

3.  $\chi(G) \leq n - \alpha(G) + 1$ .

**Доказательство:**

$\chi(G) = k$  и  $V = V_1 \sqcup V_2 \sqcup \dots \sqcup V_k$ , где  $V_i$  - независимое множество.

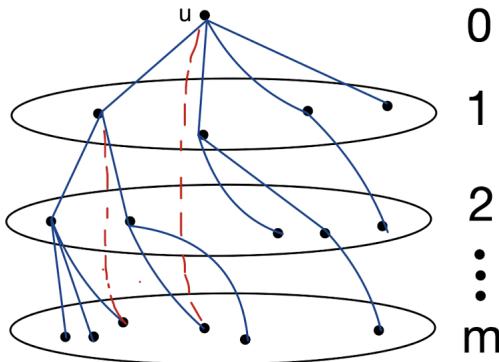
Красим максимальное независимое множество в какой-то цвет, а каждую из оставшихся  $n - \alpha(G)$  вершин в свой уникальный цвет. Тогда  $\chi(G) \leq n - \alpha(G) + 1$  ■

4.  $\chi(G) \leq \Delta(G) + 1$

**Доказательство:**

Не умоляя общности,  $G$  - связен (иначе можно провести описанное ниже рассуждение для каждой компоненты связности и выбрать в качестве хроматического числа максимальное из хроматических чисел компонент).

Тогда выделим в  $G$  остовное дерево (напомним, что это всегда можно сделать для связного графа). Подвесим его за произвольную вершину  $u$  (значит выберем её в качестве корня).



Теперь будем действовать по такому алгоритму: начиная с последнего слоя будем красить вершины в цвета  $\{1, 2, \dots, \Delta(G)\}$ . Для каждой вершины  $x$  будем смотреть, с какими уже покрашенными она соединена (учитывая и рёбра вне дерева - обозначены красным на картинке). Если  $x$  - не корень, то есть хотя бы одно ребро в верхний слой, то есть рёбер в слоях с уже покрашенными вершинами строго меньше, чем  $\Delta(G)$ . Значит вершину  $x$  можем покрасить в какой-то из оставшихся цветов (один точно найдётся).

Теперь рассмотрим ситуацию с корнем. Может получиться так, что корень соединён с  $\Delta(G)$  вершинами из нижнего покрашенного слоя (ему ведь не нужно быть соединённым ребром с кем-то выше), так что в нашей оценке мы добавляем 1, чтобы в таком случае корень можно было покрасить в  $(\Delta(G) + 1)$ -й цвет ■

*Следствие:*

Если  $G$  связен и  $\exists w \in V : \deg w < \Delta(G)$ , то  $\chi(G) \leq \Delta(G)$ .

**Доказательство:**

Повторим описанное выше рассуждение, только подвесим остовное дерево именно за  $w$ . Тогда в любом случае получится так, что на последнем шаге раскраски рёбер в покрашенные вершины строго меньше чем  $\Delta(G)$  (просто по условию). Аналогично второму абзацу предыдущего доказательства может понадобиться ещё один цвет. То есть  $\chi(G) \leq \Delta(G)$  ■

**Примеры:**

(a)  $G = K_n$  (полный граф). Тогда  $\chi(G) = n$ ,  $\Delta(G) = n - 1$ .

(b)  $G = C_{2s+1}$  (нечётный цикл). Тогда  $\chi(G) = 3$ ,  $\Delta(G) = 2$ .

**Теорема Брукса (без доказательства)**

Если  $G$  - связен и  $\chi(G) = \Delta(G) + 1$ , то  $G$  "изоморфен"  $K_n$  или  $C_{2s+1}$ .

**Определение изоморфизма графов**

Графы  $G = (V_1, E_1)$  и  $G = (V_2, E_2)$  изоморфны (обозначается как  $G_1 \cong G_2$ ), если  $\exists f : V_1 \rightarrow V_2$  такая, что:

- $f$  - биекция
- $\forall u, v \in V_1 : \{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$

### 3.2 Конструкция Зыкова-Мыцельского графа без треугольников со сколь угодно большим хроматическим числом.

**Теорема Зыкова-Мыцельского**

Пусть  $k \in \mathbb{N}$ . Тогда существует граф  $G$ :  $\omega(G) = 2$ ,  $\chi(G) = k$ .

**Доказательство:**

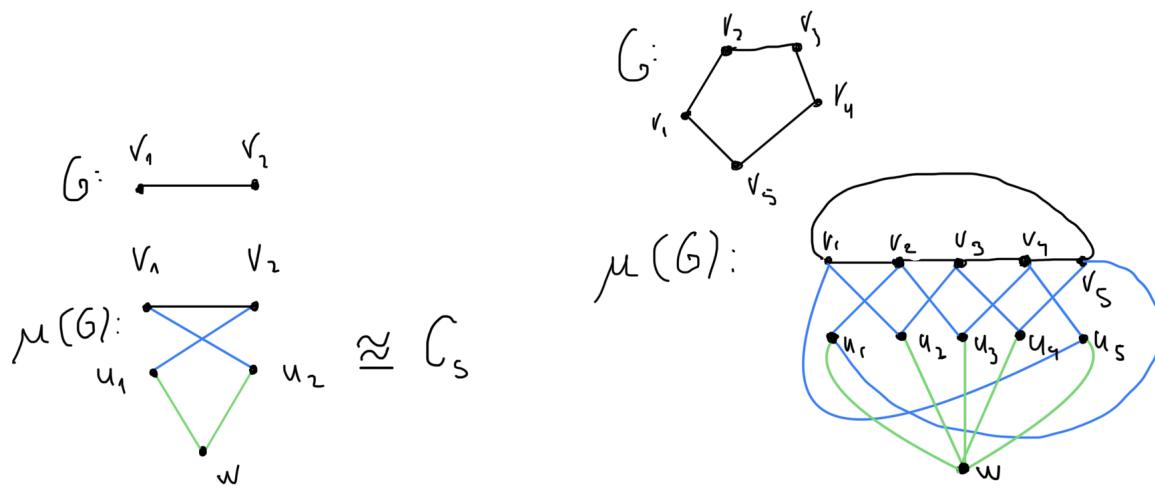
**Мыцельскийан**

Граф  $G \rightarrow \mu(G)$ , где  $G = (\{v_1, v_2, \dots, v_n\}, E)$

Вершины в  $\mu(G)$ :  $v_1, v_2, \dots, v_n, u_1, u_2, \dots, u_n, w$  - всего  $2n + 1$  штук.

Рёбра в  $\mu(G)$ : если  $\{v_i, v_j\} \in E(G)$ , то  $\{v_i, v_j\}, \{u_i, v_j\}, \{v_i, u_j\} \in E(\mu(G))$ . А также  $\{w, u_i\} \in E(\mu(G)) \forall i$ .

**Примеры:**



Утверждается, что рассматривая последовательность графов  $G_1 = K_2$ ,  $G_2 = \mu(G_1)$ ,  $G_3 = \mu(G_2) = \mu(\mu(G_1))$ , ...,  $G_s = \mu(G_{s-1})$ , ..., получим, что  $G_s$  не содержит треугольников и  $\chi(G_s) = s + 1$ .

1. Докажем, что  $G_s$  не содержит треугольников:

Пусть  $s$  - минимальное такое число ( $\geq 3$ ), что в  $G_s = \mu(G_{s-1})$  есть треугольник. По построению могут образовываться лишь вершины  $v_i, v_j, u_l$  (именно такой набор, потому что две вершины  $u$  не могут быть в треугольнике, так как не соединены ребром;  $w$  также не может - иначе две вершины  $u$  должны быть соединены ребром) причём  $l \neq i, j$  по построению.

Раз в  $G_s = \mu(G_{s-1})$  есть ребро  $\{u_l, v_i\}$ , то в исходном графе  $G_{s-1}$  было ребро  $\{v_i, v_l\}$ . Аналогично, если в  $G_s = \mu(G_{s-1})$  есть ребро  $\{u_l, v_j\}$ , то в исходном графе  $G_{s-1}$  было ребро  $\{v_j, v_l\}$ . Но в  $G_{s-1}$  есть и ребро  $\{v_i, v_j\}$ , значит рёбра  $\{v_i, v_l\}$ ,  $\{v_j, v_l\}$ ,  $\{v_i, v_j\}$  образуют треугольник в графе  $G_{s-1}$ . Противоречие, потому что  $s$  оказалось не минимальным таким числом.

2. Докажем, что  $\chi(G_s) = s + 1$  индукцией по  $s$ :

*База* проверена выше.

*Переход*  $s - 1 \rightarrow s$ .

Известно, что  $\chi(G_{s-1}) = s$ , нужно доказать, что  $\chi(G_s) = \chi(\mu(G_{s-1})) = s + 1$

Можно считать, что  $s \geq 3$ . Тогда покрасим  $u_i$  в  $(s + 1)$ -й цвет,  $w$  в 1-й цвет, а  $v_i$  уже покрашены в  $s$  первых цветов. Покажем что меньшим числом мы не обойдёмся.

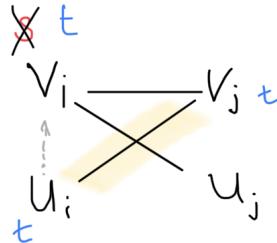
Нам известно, что  $\chi(\mu(G_{s-1})) \geq s$ , т.к.  $G_{s-1}$  содержится в  $\mu(G_{s-1})$  как подграф. Покажем, что ровно  $s$  цветами мы не обойдёмся.

От противного: пусть  $\chi(\mu(G_{s-1})) = s$ . Будем считать, что  $w$  покрашена в  $s$ -ый цвет. Тогда среди  $u_i$  нет цвета  $s$  (потому что  $w$  соединена со всеми  $u_i$  ребром). Но по предположению индукции цвет  $s$  должен найтись среди вершин  $v_j$  (их нельзя было покрасить меньшим чем  $s$  кол-вом цветов). Тогда есть некоторое количество вершин  $v_j$  цвета  $s$ . Перекрасим их в цвета по такому правилу:  $v_j$  красится в цвет, который имеет вершина  $u_j$  (для наглядности можно смотреть на пример 2 выше). Утверждается, что у нас получилась правильная раскраска вершин подграфа  $G_{s-1}(v_1, \dots, v_n)$  в  $s - 1$  цвет.

*Замечание.* Несмотря на популярное заблуждение, раскраска в  $k$  цветов всё ещё будет называться таковой, даже если мы не использовали все цвета. То есть раскраской в 4 цвета может называться и двухцветная раскраска (два цвета могут просто не использоваться).

Продолжим. Докажем, что получилась именно правильная раскраска вершин подграфа  $G_{s-1}(v_1, \dots, v_n)$  в  $s-1$  цвет.

От противного: пусть после этого перекрашивания пусть соединены ребром какие-то одноцветные  $v_i$  и  $v_j$  (пусть их цвета -  $t$ ). То есть до перекрашивания ровно одна из них была цвета  $s$  (понятно, что не обе, т.к. это была бы неправильная раскраска всего графа). Ну  $v_i$  была цвета  $s$ , а  $v_j$  была покрашена в какой-то цвет  $t$ . Мы не знаем, какого цвета в Мыцельскиане была  $u_j$ , но точно знаем, что  $u_i$  была цвета  $t$ , потому что мы в него перекрасили  $v_i$  по нашему правилу. Противоречие, т.к. в Мыцельскиане есть одноцветное ребро  $\{u_i, v_j\}$ . То есть  $\chi(G_s) > s \Rightarrow \chi(G_s) \geq s+1$ , а как раскрасить в  $s+1$  цвет мы показали выше. Переход доказан, значит  $\chi(\mu(G_{s-1})) = s+1$  ■



Чем интересен граф Зыкова-Мыцельского? Смотрите: если мы знаем, что у графа бесконечно большое кликовое число, то можем сказать, что и хроматическое число графа бесконечно большое (оно как минимум равно кликовому). Однако обратное неверно. Мы построили граф, в котором при бесконечно большом хроматическом числе кликовое число равно 2.

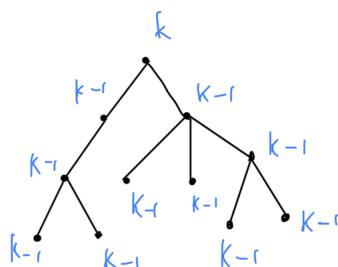
### 3.3 Хроматический многочлен.

**Хроматический многочлен.** Функция от числа цветов, возвращающая количество способов раскрасить (естественно правильно) фиксированный граф  $G$  в  $k$  цветов.

Обозначение:  $\chi_G(k)$ .

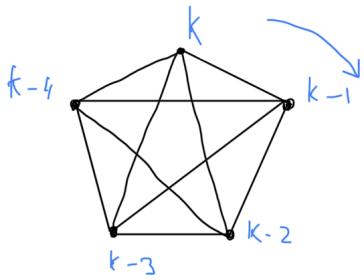
**Примеры:**

- $G$  - дерево.  $\chi_G(k) = k \cdot (k-1)^{n-1}$



Для корня цвет выбираем  $k$  способами, а для любой другой вершины есть запрет одного цвета от вершины из над-слоя. То есть  $k-1$  способов для такой вершины. Отсюда такой вид многочлена.

- $G$  - полный граф.  $\chi_G(k) = k \cdot (k-1) \cdot (k-2) \cdot \dots \cdot (k-n+1)$



Выбираем для какой-то вершины цвет  $k$  способами, потому выбираем любую другую. Для неё уже  $k - 1$  способ выбрать цвет, т.к. она соединена с покрашенной (в полном графе любые две соединены). И так далее.

- $G$  - независимое множество.  $\chi_G(k) = k^n$ . Очевидно, т.к. никакие две вершины не соединены ребром.

Определим две операции:

- удалить  $\{u, v\}$ . Обозначение:  $G - uv$ .
- склеить  $u$  и  $v$ . Обозначение:  $G \cdot uv$ . Что это значит: мы объединяем вершины  $u$  и  $v$  в одну, и все ребра, которые вели в  $u$  и  $v$  теперь будут вести в эту новую вершину (если получилось кратное ребро - заменим его на одно).

**Утверждение.**  $\chi_{G-uv}(k) = \chi_G(k) + \chi_{G\cdot uv}(k)$ , если  $\{u, v\} \in E(G)$ .

**Доказательство:**

Удалим  $\{u, v\}$ . Теперь посчитаем кол-во способ раскрасить  $G - uv$ :

1.  $u$  и  $v$  раскрашены в разные цвета. Тогда нам ничего не мешает вернуть ребро  $\{u, v\}$  и раскраска останется правильной. Тогда очевидна биекция: таких раскрасок ровно столько же, сколько у графа  $G$ .
2.  $u$  и  $v$  раскрашены в один цвет. Тогда рассмотрим граф со склеенными вершинами  $u$  и  $v$  в одну. Тогда любая его раскраска соответствует правильной раскраске исходного графа, где  $u$  и  $v$  раскрашены в один цвет (точнее почти правильной, "неправильным" будет только ребро  $\{u, v\}$ ). И наоборот. Вспоминаем, что ребра  $\{u, v\}$  уже нет, тогда устанавливаем биекцию: таких раскрасок ровно столько же, сколько у графа  $G \cdot uv$ .

Итого:  $\chi_{G-uv}(k) = \chi_G(k) + \chi_{G\cdot uv}(k)$  ■

**Теорема Уитни о хроматическом многочлене и его свойствах**

$\chi_G(k)$  - многочлен вида  $k^n - a_1 k^{n-1} + a_2 k^{n-2} - \dots + (-1)^{n-r} a_{n-r} k^r$ , где  $a_i \in \mathbb{N}$ ,  $a_1 = |E(G)|$ ,  $r$  - количество компонент связности.

**Доказательство:**

Полная индукция по числу ребер в графе.

**База** очевидна: если 0 ребер, то граф - независимое множество,  $\chi_G(k) = k^n$  (см. пример выше).

**Переход.**

$\chi_G(k) = \chi_{G-uv}(k) - \chi_{G\cdot uv}(k)$ , если  $\{u, v\} \in E(G)$  по доказанному выше утверждению. Кол-во ребер в графах  $G - uv$  и  $G \cdot uv$  меньше чем в  $G$ , поэтому по индукционному предположению для их хроматических многочленов верны все свойства.

Будем считать, что в  $|E(G)| = m$

В графе  $G - uv$  при удалении одного ребра количество компонент связности может или не измениться, или увеличиться на 1.

В графе  $G \cdot uv$  при склеивании двух вершин количество компонент связности не меняется.

$\chi_{G-uv}(k)$  выглядит как  $k^n - (m-1)k^{n-1} + \dots + (-1)^{n-r-1} b_{n-r-1} k^{r+1} + (-1)^{n-r} b_{n-r} k^r$ . При этом имеем в виду, что  $b_{n-r}$ -й коэффициент может быть равен 0 в случае увеличения количества компонент на 1. Будем считать 0 как положительным, так и отрицательным.

$\chi_{G\cdot uv}(k)$  выглядит как  $k^{n-1} - c_1 k^{n-2} + \dots + (-1)^{n-r-1} c_{n-r-1} k^r$

При вычитании многочлена с натуральными  $a_i$  из многочлена с натуральными  $b_i$  очевидно, что получится также многочлен с натуральными  $c_i$ . Старший коэф-т при  $k^n$  действительно будет 1. Коэф-т при  $k^{n-1}$  будет равен  $m-1+1 = m$ . Теперь проверим, что будет знакочередование: в многочлене  $\chi_{G-uv}(k)$  коэф-ты знакочередуются и можно заметить, что в вычитаемом многочлене  $\chi_{G\cdot uv}(k)$  при симметричных степенях знаки противоположны. Поэтому при вычитании из отрицательного коэф-та положительного он будет оставаться отрицательным, а при вычитании из положительного коэф-та отрицательного он будет оставаться положительным ■

Как с помощью хроматического многочлена найти хроматическое число? Нужно просто подставлять вместо  $k$  натуральные числа. Получим:

$\chi_G(1) = \chi_G(2) = \dots = \chi_G(\chi(G) - 1) = 0$  - то есть до какого-то натурального будет получаться значение 0, а первое натуральное  $m$  при котором многочлен равен ненулевому числу  $\chi_G(m)$  и будет  $\chi(G)$ .

*Упражнение.* Если  $G$  - связен, то  $\chi_G(0) = 0$ , причём кратность нуля = 1.

## 4 Лекция 16

(Андрей)

### 4.1 Математическое ожидание

Пусть имеем  $\Omega = \{\omega_1, \dots, \omega_k\}$  - вероятностное пространство с вероятностным распределением  $p_1, \dots, p_k$  соответственно, причем понятно, что  $\sum_{i=1}^k p_i = 1$ . Далее, назовем *случайной величиной* функцию  $f : \Omega \rightarrow \mathbb{R}$  и на  $\omega_1, \omega_2, \dots, \omega_k$   $f$  принимает значения  $\{a_1, a_2, \dots, a_k\}$ .

Предположим, что выбор случайного элемента из  $\Omega$  повторяется  $n$  раз. Если  $n$  достаточно большое, то случайная величина  $f$  примет значение  $a_1$  примерно  $p_1 \cdot n$  раз, значение  $a_2$  — примерно  $p_2 \cdot n$  раз, и так далее, значение  $a_k$  — примерно  $p_k \cdot n$  раз. Подсчитаем теперь примерное среднее арифметическое значений случайной величины  $f$  в этих экспериментах:

$$\frac{a_1 p_1 n + a_2 p_2 n + \dots + a_k p_k n}{n} = a_1 p_1 + a_2 p_2 + \dots + a_k p_k$$

Такую сумму  $\sum_{i=1}^k f(\omega_i)p_i$  называют *математическим ожиданием* случайной величины  $f$  и обозначают  $E[f]$ .

**Пример:**

Давайте покидаем кубик что ли. Имеем  $\Omega = \{1, 2, 3, 4, 5, 6\}$  (все исходы равновероятны). Положим  $f$  - число очков, которое выпадает при одном броске кубика. Тогда  $E[f] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = \frac{21}{6} = 3,5$ .

Докажем лемму о линейности мат. ожидания.

**Лемма:**  $E[f + g] = E[f] + E[g]$  ( $f, g$  - случайные величины).

**Доказательство:**  $E[f + g] = \sum_{i=1}^k (f + g)(\omega_i)p_i = \sum_{i=1}^k f(\omega_i)p_i + \sum_{i=1}^k g(\omega_i)p_i = E[f] + E[g]$ .

**Пример:** задача о днях рождения.

*Дано:*  $n = 28$  - количество людей, случайная величина  $f$  - число пар людей, у которых день рождения в один и тот же день.

*Утверждается:*  $E[f] > 1$ .

**Доказательство:**

Для начала поймем, что  $\Omega = \{1, 2, \dots, 365\}^n$  (распределение равновероятно). Теперь делаем финт ушами и вводим следующую функцию:

$$g_{ij} = \begin{cases} 1, & \text{если } i\text{-й человек и } j\text{-й человек родились в один день} \\ 0, & \text{иначе} \end{cases}$$

Тогда  $f = \sum_{1 \leq i < j \leq 28} g_{ij}$ . Тогда  $E[f] = \sum_{1 \leq i < j \leq 28} E[g_{ij}]$ . Заметим, что  $E[g_{ij}] = 1 \cdot P$ , где  $P$  - вероятность того, что два человека с номерами  $i$  и  $j$ , родились в один день. Она равна  $\frac{365^{n-1}}{365^n} = \frac{1}{365}$ . И, наконец,  $E[f] = \frac{n(n-1)}{2} \cdot \frac{1}{365}$  (для тех, кто не понял, откуда взялся множитель с  $n$ , то кол-во пар равно  $\frac{n(n-1)}{2}$ ). Так как  $n = 28$ , то  $E[f] = \frac{378}{365} > 1$ .

### 4.2 Неравенство Маркова

**Теорема (неравенство Маркова):** Пусть  $f : \Omega \rightarrow \mathbb{R}_{\geq 0}$  - неотрицательная случайная величина и пусть некоторое число  $\alpha > 0$ . Тогда  $P(f \geq \alpha) \leq \frac{E[f]}{\alpha}$ .

**Доказательство:**

Жестко идем по определению:  $E[f] = p_1 f(\omega_1) + p_2 f(\omega_2) + \dots + p_k f(\omega_k)$ . Дальше хотим сделать следующее:

$$f(\omega_i) = \begin{cases} 0, & \text{если } f(\omega_i) < \alpha \\ \alpha, & \text{если } f(\omega_i) \geq \alpha \end{cases}$$

При такой замене для исходного выражения выполнится следующее неравенство:

$$E[f] = p_1 f(\omega_1) + p_2 f(\omega_2) + \dots + p_k f(\omega_k) \geq \alpha(p_{i1} + p_{i2} + \dots + p_{ij}) = \alpha P(f \geq \alpha)$$

**Ч.Т.Д.**

**Пример:** вероятностный алгоритм.

Пусть имеем некоторый алгоритм  $A_1$ , который обладает следующими свойствами:

- Он всегда корректно работает.
- Работает **в среднем** за время  $T = O(n^2)$ .
- Иногда сильно тормозит.

Хотим: Модифицировать его так, чтобы новый алгоритм  $A_2$  работал следующим образом:

- Он может ошибиться в 0,01% случаев.
- Работает всегда за  $O(n^2)$ .

Тогда сделаем следующие действия:

- Запустим  $A_1$  на время  $10000 \cdot T$ .
- Если получили ответ, то выведем его
- Иначе выведем 0.

Пусть случайная величина  $f$  - реальное время работы нашего алгоритма.

Тогда имеем  $E[f] = T$  (так как  $T$  - среднее время работы). Но в таком случае  $P(f \geq 10000T) \leq \frac{E[f]}{10000T} = \frac{T}{10000T} = \frac{1}{10000} = 0,01\%$  случаев. Получили требуемый алгоритм.

### 4.3 Дисперсия

Дисперсия случайной величины  $f : \Omega \rightarrow \mathbb{R}$  - это  $D[f] = E([f - E\{f\}]^2)$

**Утверждение:**  $D[f] = E[f^2] - (E[f])^2$

**Доказательство:**

$$D[f] = E([f - E\{f\}]^2) = E(f^2 - 2fE[f] + (E[f])^2) = E[f^2] + E(-2fE[f]) + E\{(E[f])^2\} = E[f^2] - 2E[f]E[f] + (E[f])^2 = E[f^2] - (E[f])^2$$

**Ч.Т.Д.**

### 4.4 Неравенство Чебышева

Пусть  $f$  - произвольная случайная величина, число  $\alpha > 0$ . Тогда  $P(|f - E[f]| \geq \alpha) \leq \frac{D[f]}{\alpha^2}$

**Доказательство:**

Рассмотрим случайную величину  $g = (f - E[f])^2$ . По неравенству Маркова:

$$P(g \geq \alpha^2) \leq \frac{E[g]}{\alpha^2}$$

Так как  $P(g \geq \alpha^2) = P(|f - E[f]| \geq \alpha)$  и  $E[g] = D[f]$  (из определения дисперсии), то:

$$P(|f - E[f]| \geq \alpha) \leq \frac{D[f]}{\alpha^2}$$

**Ч.Т.Д.**

## 4.5 Общий случай вероятностного метода

**Лемма:** Пусть  $E[f] = c$ , при этом имеем  $\Omega$  и  $f : \Omega \rightarrow \mathbb{R}$ . Тогда:

- $\exists \omega_{min} \in \Omega : f(\omega_{min}) \leq c$
- $\exists \omega_{max} \in \Omega : f(\omega_{max}) \geq c$

**Доказательство:**

По определению  $E[f] = p_1 f(\omega_1) + p_2 f(\omega_2) + \dots + p_k f(\omega_k)$ .

Пойдем от противного. Пусть  $f(\omega_i) \geq c \forall i$ , то  $E[f] > c(p_1 + p_2 + \dots + p_k) = c$ . Получили противоречие с условием леммы, следовательно,  $\exists \omega_{min} \in \Omega : f(\omega_{min}) \leq c$ . Для второго случая доказательство аналогично.

**Ч.Т.Д.**

**Пример:** Разрезы в графах

Рассмотрим простой неориентированный граф  $G = (V, E)$ . *Разрезом* графа называется разбиение множества его вершин на два непересекающихся подмножества:  $V = V_1 \sqcup V_2$ . Мы говорим, что ребро попадает в разрез, если один его конец лежит в  $V_1$ , а другой в  $V_2$ . Размером разреза называется число рёбер, попадающих в разрез.



**Утверждение:** В любом графе есть разрез размера  $\frac{|E|}{2}$ .

**Доказательство:**

Пусть  $S$  - случайное подмножество  $V$ . Имеем случайный разрез графа  $(S, V \setminus S)$ . Введем случайную величину  $g_e = \begin{cases} 1, & \text{если ребро } e \text{ лежит в разрезе} \\ 0, & \text{иначе} \end{cases}$

Далее определим случайную величину  $f$  как  $f = \sum_{e \in E} g_e$ . Тогда  $E[f] = \sum_{e \in E} E[g_e] = \sum_{e \in E} \frac{1}{2} = \frac{|E|}{2}$  ( $E[g_e] = \frac{1}{2}$ , из определения мат. ожидания).

**Ч.Т.Д.**

## 5 Лекция 17

(Илья)

### 5.1 Вероятностный метод. Разрезы в графах.

Пусть нам дан неориентированный граф  $G = (V, E)$  без кратных рёбер и петель и разрез  $S \subseteq V$  величиной  $|E(S, V \setminus S)|$  (более подробно о том, что такое разрез в графе и его величина можно прочитать в конце 16 лекции)

**Теорема:** В  $G$  существует разрез величиной не меньше, чем  $\frac{|E|}{2}$ .

Данная теорема была доказана на прошлой лекции, поэтому опять отсылаю вас прочитать её.

Так вот, к чему это я веду, оказывается, что можно немного усилить предыдущую теорему.

**Теорема:** Пусть  $|V| = 2n$  - чётное число вершин графа (аналогично можно доказать и для нечётного числа вершин). Тогда в  $G$  существует разрез не меньше, чем  $\frac{|E|n}{2n-1}$ .

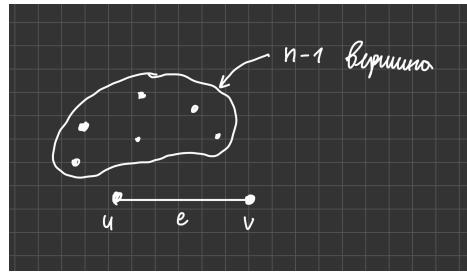
**Доказательство:**

1. Пусть  $\Omega = \{S \subseteq V | |S| = n\}$  - наше вероятностное пространство и все события равновероятны, тогда понятно, что  $|\Omega| = \binom{2n}{n}$ .

Пусть  $f$  - случайная величина и  $f : \Omega \rightarrow \mathbb{R}$  и  $f(S) = |E(S, V \setminus S)|$ . То есть она разрезу ставит в соответствие его величину. Тогда давайте воспользуемся вероятностным методом, как мы доказывали предыдущую теорему, и просто посчитаем  $E[f]$ .

2. Давайте зададим индикаторную функцию  $g_e = \begin{cases} 1, & \text{если ребро } e \in E(S, V/S) \\ 0, & \text{если ребро не лежит в разрезе} \end{cases}$

Тогда  $f = \sum_{e \in E} g_e$ , а значит, что  $E[f] = \sum_{e \in E} P(g_e = 1)$ . Посчитаем, чему равна вероятность того, что ребро входит в разрез графа. Чтобы осознать это давайте сделаем поясняющий рисунок.



Вероятность того, что ребро  $e$  попадёт в разрез, означает, что мы сможем разделить множество вершин из  $2n$  вершин на 2 непересекающихся подмножества вершин по  $n$  вершин в каждом, причём вершины соединённые ребром  $e$  лежат в разных подмножествах. Давайте посмотрим, сколькими способами мы можем это сделать. Понятно, что я могу посчитать количество способов выбрать одно такое подмножество на  $n$  вершинах, тогда второе задаётся однозначно.

Вот пусть у меня есть вершины  $u$  и  $v$  и они соединены ребром  $e$ , тогда зафиксировав вершину  $u$  мы получим, что количество способов дополнить её до множества размером  $n$ , причём, чтобы  $v$  не лежало в нём, равно  $\binom{2n-2}{n-1}$  (если до сих пор не понятно, то прочитайте вдумчиво, что я тут написал). Но данное количество способов надо домножить на 2, потому что в самом начале я мог зафиксировать не вершину  $u$ , а вершину  $v$ . Итого количество подходящих разбиений множества для того, чтобы ребро  $e$  попало в разрез равно  $2\binom{2n-2}{n-1}$ .

Понятно, что всего разбиений множества из  $2n$  вершин на 2 подмножества из  $n$  вершин это  $\binom{2n}{n}$ .

$$\text{Итого, } P(g_e = 1) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{2 \cdot (2n-2)! \cdot n! \cdot n!}{(n-1)! \cdot (n-1)! \cdot (2n)!} = \frac{2 \cdot n^2}{2n(2n-1)} = \frac{n}{2n-1}$$

3. Значит,  $E[f] = \sum_{e \in E} P(g_e = 1) = \frac{|E|n}{2n-1}$ . Тогда по лемме о вероятностном методе (прочтите прошлую лекцию, если не понятно, о чём я) получаем, что существует разрез в графе величиной  $\frac{|E|n}{2n-1}$

## Ч.Т.Д.

**Упражнение:** Если  $V = 2n + 1$ , то существует разрез в графе величиной не меньше, чем  $\frac{|E|(n+1)}{2n+1}$

## 5.2 Независимые случайные величины

Пусть  $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$  - вероятностное пространство.

**Определение:** Случайные величины  $X, Y : \Omega \rightarrow \mathbb{R}$  называются независимыми, если  $\forall x, y \in \mathbb{R}$  события  $\{\omega \in \Omega | X(\omega) = x\}$  и  $\{\omega \in \Omega | Y(\omega) = y\}$  независимы. (напомню, что события  $A, B$  называются независимыми, если  $P(A \cap B) = P(A) \cdot P(B)$ ).

**Замечание:**  $X_1, X_2, \dots, X_n$  независимы, если  $\forall x_{i_1}, x_{i_2}, \dots, x_{i_s} \in \mathbb{R} P((X_{i_1} = x_{i_1}) \cap (X_{i_2} = x_{i_2}) \cap \dots \cap (X_{i_s} = x_{i_s})) = P(X_{i_1} = x_{i_1}) \cdot P((X_{i_2} = x_{i_2}) \cdot \dots \cdot P((X_{i_s} = x_{i_s}))$

**Теорема:** Если случайные величины  $X, Y$  независимы, то  $E[X \cdot Y] = E[X] \cdot E[Y]$

**Доказательство:**

1. По определению  $E[X] = \sum_{x \in X(\Omega)} x \cdot P(X = x), E[Y] = \sum_{y \in Y(\Omega)} y \cdot P(Y = y)$ .

2. Тогда  $E[X] \cdot E[Y] = (\sum_{x \in X(\Omega)} x \cdot P(X = x)) \cdot (\sum_{y \in Y(\Omega)} y \cdot P(Y = y)) = \sum_{(x,y) \in X(\Omega) \times Y(\Omega)} xyP(X = x)P(Y = y) = \sum_{(x,y) \in X(\Omega) \times Y(\Omega)} xyP((X = x) \cap (Y = y))$ .

Положим  $xy = z$ , тогда это равно  $\sum_{z \in (XY)(\Omega)} z \cdot P(X \cdot Y = z) = E[X \cdot Y]$

## Ч.Т.Д.

**Следствие:** Если случайные величины  $X, Y$  независимы, то  $D[X + Y] = D[X] + D[Y]$ .

### Доказательство:

По определению  $D[X] = E[X^2] - (E[X])^2$ , тогда  $D[X+Y] = E[(X+Y)^2] - (E[X+Y])^2 = E[X^2 + 2XY + Y^2] - (E[X])^2 - 2E[X]E[Y] - (E[Y])^2 = E[X^2] + 2E[XY] + E[Y^2] - (E[X])^2 - 2E[XY] - (E[Y])^2 = E[X^2] + E[Y^2] - (E[X])^2 - (E[Y])^2 = D[X] + D[Y]$

(пользовались тем фактом, что  $E[X+Y] = E[X] + E[Y]$ )

**Ч.Т.Д.**

**Упражнение:** Если  $X_1, X_2, \dots, X_n$  - случайные независимые величины, то

- $E[X_1 \cdot X_2 \cdot \dots \cdot X_n] = E[X_1] \cdot \dots \cdot E[X_n]$
- $D[X_1 + X_2 + \dots + X_n] = D[X_1] + D[X_2] + \dots + D[X_n]$

## 5.3 Оценка биномиальных коэффициентов

(добро пожаловать в матан)

Вот представим себе, что мы подбрасываем монетку  $n$  раз. Посчитаем  $P(\text{выпало } \frac{n}{2} \text{ орлов})$ , что очевидно равно  $\binom{\frac{n}{2}}{2^n}$ . Вот мы хотим что-то понять про эту вероятность, но для этого нам очень надо уметь оценивать биномиальный коэффициент из числителя.

Давайте выпишем пару очевидных оценок:  $\frac{2^n}{n+1} \leq \binom{\frac{n}{2}}{2^n} \leq \sum_{i=0}^n \binom{n}{i} = 2^n$ .

Левая оценка верна просто потому что это сумма положительных чисел и туда входит наш биномиальный коэффициент, поэтому очевидно, а правая оценка получена путём рассмотрения строки в треугольнике Паскаля и замечанием того, что наш рассматриваемый биномиальный коэффициент стоит ровно посередине нашей строки Паскаля, поэтому он среди всех в этой строке самый большой. Всего элементов в строке  $n+1$ , ну и сумма их равна  $2^n$ , поэтому это не что иное, как неравенство о среднем арифметическом и максимумом из всех чисел.

Давайте взглянем теперь на наш биномиальный коэффициент по-другому.  $\binom{\frac{n}{2}}{2^n} = \frac{n!}{(\frac{n}{2})! \cdot (\frac{n}{2})!}$ . Именно поэтому мы хотим оценить факториалы.

**Лемма (Формула Стирлинга):**  $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$

Вернёмся обратно к нашей вероятности и попробуем посмотреть, что с ней творится на  $+\infty$ .

1. Вспомним fun fact с матана.  $f(n) \sim g(n) \Leftrightarrow \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$ .

2. Тогда требуется доказать, что  $\lim_{n \rightarrow \infty} \frac{n!}{(\frac{n}{2})! \cdot (\frac{n}{2})! \cdot 2^n} = \lim_{n \rightarrow \infty} \frac{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n}{2^n \cdot \sqrt{\pi n} \cdot \sqrt{\pi n} \cdot \left(\frac{n}{2e}\right)^{\frac{n}{2}} \cdot \left(\frac{n}{2e}\right)^{\frac{n}{2}}} = \lim_{n \rightarrow \infty} \frac{1}{\sqrt{\frac{\pi n}{2}}} = 0$ .

Получаем, что наша вероятность при достаточно больших  $n$  стремится к 0.

Теперь сформулируем ещё парочку лемм.

**Лемма:** a)  $\binom{n}{k}^k \leq \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$ , б)  $\sum_{i=0}^k \binom{n}{i} \leq \left(\frac{en}{k}\right)^k$

**Доказательство:**

1. Докажем сначала пункт а) и его правую оценку.

**Мини лемма:**  $\frac{a}{b} \leq \frac{a-1}{b-1}$  при  $a \geq b \geq 1$ .

**Доказательство:** Перемножим крест на крест и получим, что  $a(b-1) \leq b(a-1) \implies a \geq b$ , что верно. **Ч.Т.Д.**

Тогда так как  $\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots(k-k+1)}$ , то в силу мини леммы получаем, что  $\binom{n}{k} \geq \left(\frac{n}{k}\right)^k$

2. Теперь докажем в левую оценку пункта а), однако для этого понадобится сначала доказать пункт б).

**Доказательство:**

Заметим, что  $\sum_{i=0}^k \binom{n}{i} \leq \sum_{i=0}^n \binom{n}{i} \cdot \frac{t^i}{t^k}$ , где  $t \in (0,1]$ . Тогда можно вынести  $\frac{1}{t^k}$  за сумму и получим  $\frac{1}{t^k} \cdot (1+t)^n$

Пусть теперь  $t = \frac{k}{n}$ , тогда  $\frac{(1+t)^n}{t^k} = \frac{n^k}{k^k} \cdot (1 + \frac{k}{n})^n$ . Ну и теперь ещё один fun fact с матана, что  $e^k \geq (1 + \frac{k}{n})^n$ , поэтому в итоге  $\sum_{i=0}^k \binom{n}{i} \leq \frac{n^k}{k^k} \cdot e^k = \left(\frac{en}{k}\right)^k$

## Ч.Т.Д.

3. Ну и для полного завершения доказательства осталось заметить, что  $\binom{n}{k} \leq \sum_{i=0}^k \binom{n}{i} \leq (\frac{en}{k})^k$ , тем самым мы доказали и левую оценку пункта а).

## Ч.Т.Д.

### 5.4 Неравенство Чернова

(сначала может показаться, что матан отступил, но не тут-то было)

Пусть у нас есть монетка, в которой выпадает орёл с вероятностью  $p$  и есть случайные независимые величины  $X_1, X_2, \dots, X_n$  и  $P(X_i = 0) = 1 - p$ , а  $P(X_i = 1) = p$ . Тогда случайная величина  $X = \sum_{i=1}^n X_i$  - число выпадения орлов.

Пусть также наше вероятностное пространство - это  $\Omega = \{0,1\}^n$ , то есть 0 - это решка и 1 - это орёл. Тогда обозначим за  $a_1, a_2, \dots, a_n$  результаты подбрасывания монетки  $n$  раз, то есть  $a_i \in \Omega$  - это результат в  $i$ -ом броске.

$$\text{Тогда } P(a_1 \cap a_2 \cap \dots \cap a_n) = p \left( \sum_{i=1}^n a_i \right) \left( 1 - p \right)^{(n - \sum_{i=1}^n a_i)}$$

Перед формулировкой и доказательством самого неравенства Чернова нужен..., угадайте кто... правильно -fun fact с матана.

**Лемма:**  $e^x \geq 1 + x$  (не думаю, что на колке попросят доказывать, но тут просто надо перенести всё в одну сторону и исследовать функцию на монотонность и точки экстремума, взяв производную, и всё получится)

**Теорема (Неравенство Чернова):**

$$\forall \varepsilon \in (0,1) \quad P(X \geq (1 + \varepsilon)pn) \leq e^{-\frac{\varepsilon^2 np}{3}}$$

Неравенство Чернова утверждает, что вероятность того, что число выпавших орлов отклонится от математического ожидания числа орлов не менее, чем в эпсилон раз, не более  $e^{-\frac{\varepsilon^2 np}{3}}$

**Доказательство:**

1. Рассмотрим случайную величину  $Y = e^{tX}$ , где  $t > 0$ . Тогда перепишем неравенство Чернова в терминах случайной величины  $Y$  и запишем неравенство Маркова (если хз, что оно, то прочитайте бля уже лекцию) для левой части неравенства.

$$P(Y \geq e^{t(1+\varepsilon)pn}) \leq \frac{E[e^{tX}]}{e^{t(1+\varepsilon)pn}}$$

2. Посчитаем мат. ожидание по определению для каждой возможной последовательности орлов и решек:  $E[e^{tX}] = \sum_{k=0}^n \binom{n}{k} \cdot p^k (1-p)^{n-k} \cdot e^{tk} = (e^t p + (1-p))^n$ . Свернём по битону Ньютона.

$$3. \text{ Значит, } \frac{E[e^{tX}]}{e^{t(1+\varepsilon)pn}} = \frac{(e^t p + (1-p))^n}{e^{t(1+\varepsilon)pn}}$$

Оценим числитель:  $(e^t p + (1-p))^n = (1 + \frac{pn(e^t - 1)}{n})^n \leq e^{pn(e^t - 1)}$

$$\text{Итого, } E[e^{tX}] \leq \frac{e^{pn(e^t - 1)}}{e^{t(1+\varepsilon)pn}} = e^{np(e^t - 1 - t(1+\varepsilon))}$$

4. Мы хотим сделать оценку как можно более точную, поэтому надо подобрать такой  $t$ , чтобы  $e^{np(e^t - 1 - t(1+\varepsilon))}$  был минимален.

Давайте рассмотрим функцию  $g(t) = e^t - 1 - t(1+\varepsilon) \implies g'(t) = e^t - (1+\varepsilon) \implies t = \ln(1+\varepsilon)$ . Можно убедиться, что полученная точка - это точка минимума. Подставим вместо  $t$  её и получим, что  $e^{np(\varepsilon - \ln(1+\varepsilon)(1+\varepsilon))}$ .

$$\text{Так как } \ln(1+\varepsilon) = \varepsilon - \frac{\varepsilon^2}{2} + \frac{\varepsilon^3}{3} - \dots = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{\varepsilon^k}{k}$$

$$\text{Тогда } (1+\varepsilon)\ln(1+\varepsilon) = (1+\varepsilon)(\varepsilon - \frac{\varepsilon^2}{2} + \frac{\varepsilon^3}{3} - \dots) = \varepsilon + \frac{\varepsilon^2}{2} - \frac{\varepsilon^3}{6} + \frac{\varepsilon^4}{12} - \frac{\varepsilon^5}{20} + \dots = \varepsilon + \sum_{k=2}^{\infty} (-1)^k \frac{\varepsilon^k}{k(k-1)} \geq \varepsilon + \frac{\varepsilon^2}{2} - \frac{\varepsilon^3}{6} \geq \varepsilon + \frac{\varepsilon^2}{2} - \frac{\varepsilon^2}{6} \geq \varepsilon + \frac{\varepsilon^2}{3}$$

5. Окончательно получаем, что  $\frac{E[e^{tX}]}{e^{t(1+\varepsilon)p^n}} \leq e^{np(\varepsilon - \ln(1+\varepsilon)(1+\varepsilon))} \leq e^{np(\varepsilon - (\varepsilon + \frac{\varepsilon^2}{3}))} = e^{-\frac{\varepsilon^2 np}{3}}$

**Ч.Т.Д.**

## 6 Лекция 18

([Никита](#))

### 6.1 Производящие функции

На данной лекции начнём с весьма формального взгляда на производящие функции.

$F = (f_1, f_2, f_3, \dots)$ ,  $f_i \in \mathbb{C}$  - некоторая бесконечная последовательность комплексных чисел.

Тогда мы ей можем сопоставить "функцию" (строго говоря, по определению это функцией являться не будет):

$$F(x) = f_0 + f_1x + f_2x^2 + f_3x^3 + \dots = \sum_{k=0}^{+\infty} f_k x^k.$$

Стоит воспринимать эту запись как некоторый формальный (степенной) ряд, то есть мы не собираемся ничего туда подставлять (по крайней мере на данный момент). Можно воспринимать  $x, x^2, x^3, \dots$  просто как "картинки".

Тогда  $F(x) = \sum_{k=0}^{+\infty} f_k x^k$  называют производящей функцией для последовательности  $F$ .

Теперь мы хотим определить некоторые арифметические операции для производящих функций:

- Сложение,  $+$ :  $F(x) = \sum_{k=0}^{+\infty} f_k x^k$ ,  $G(x) = \sum_{k=0}^{+\infty} g_k x^k \rightarrow (F+G)(x) = \sum_{k=0}^{+\infty} (f_k + g_k) x^k$
- Умножение на скаляр:  $F(x), c \in \mathbb{C} \rightarrow (cF)(x) = \sum_{k=0}^{+\infty} (cf_k) x^k$

Вместе с операциями сложения и умножения множество производящих функций (обозначается как  $\mathbb{C}[[x]]$ ) образует векторное пространство над  $\mathbb{C}$ . Проверка аксиом векторного пространства предоставляется читателю в качестве упражнения.

Также покажем как происходит умножение производящих функций:

Интуитивно (это важно) умножение можно выполнить таким образом:

$(F \cdot G)(x) = (f_0 + f_1x + f_2x^2 + \dots)(g_0 + g_1x + g_2x^2 + \dots) = f_0g_0 + (f_1g_0 + f_0g_1)x + (f_2g_0 + f_1g_1 + f_0g_2)x^2 + \dots + (\sum_{k=0}^n f_k g_{n-k})x^n + \dots$ . Однако это лишь некоторый способ понять суть умножения, а так оно формально задаётся определением:

$$(F \cdot G)(x) = F(x) \cdot G(x) = H(x), \text{ где } h_n = \sum_{k=0}^n f_k g_{n-k}$$

Теперь мы можем показать, что выполняются некоторые привычные свойства умножения.

**Утверждение.**  $A(x) \cdot (B(x) \cdot C(x)) = (A(x) \cdot B(x)) \cdot C(x)$ .

*Примечание.*  $F(x) = G(x) \Leftrightarrow f_i = g_i \forall i \in \mathbb{N} \cup \{0\}$

**Доказательство:**

$$A(x) \cdot B(x) = D(x). \text{ Посмотрим на коэффициент при } x^k : \sum_{l=0}^k a_l b_{k-l} = \sum_{\substack{i+j=0 \\ i,j \geq 0}} a_i b_j.$$

$$D(x) \cdot C(x). \text{ Посмотрим на коэффициент при } x^n : \sum_{k=0}^n d_k c_{n-k} = \sum_{k=0}^n \sum_{\substack{i+j=0 \\ i,j \geq 0}} a_i b_j c_{n-k} = \sum_{\substack{i+j+t=n \\ i,j,t \geq 0}} a_i b_j c_t.$$

Последний переход следует из того, что сумма всех коэффициентов равна  $n$ , то есть мы просто рассматриваем произведение всех коэффициентов таких, чтобы их сумма давала  $n$ . Проделав такие же действия для левой части равенства, также получим инвариантное относительно  $n$  (по сумме индексов) выражение. Значит, ассоциативность умножения верна ■

*Примечание.* Мы не отметили это ранее, но умножение производящих функций коммутативно ровно потому, что коммутативно умножение комплексных чисел (см. определение умножения).

Давайте выпишем свойства умножения:

1.  $A(x) \cdot B(x) = B(x) \cdot A(x)$  - коммутативность.
2.  $A(x) \cdot (B(x) \cdot C(x)) = (A(x) \cdot B(x)) \cdot C(x)$  - ассоциативность.

3.  $A(x) \cdot (B(x) + C(x)) = A(x) \cdot B(x) + A(x) \cdot C(x)$  - дистрибутивность.

**Доказательство:**

Посмотрим на коэффициент при  $x^n$  у выражения слева:  $\sum_{k=0}^n a_k(b_{n-k} + c_{n-k}) = \sum_{k=0}^n a_k b_{n-k} + \sum_{k=0}^n a_k c_{n-k} = A(x)C(x) + B(x)C(x)$ .

4.  $\exists 1 = (1, 0, 0, \dots) = 1 + 0x + 0x^2 + \dots$

$$1 \cdot A(x) = A(x)$$

**Утверждение.** Введём определение константы:  $c = (c, 0, 0, \dots)$ ,  $c(x) = c + 0x + 0x^2 + \dots$  Тогда  $c(x) \cdot A(x) = (cA)(x)$

**Доказательство:**

Посмотрим на коэффициент при  $x^n$  у выражения слева:  $\sum_{k=0}^n c_k a_{n-k} = ca_n$ , т.к. все  $c_k$  кроме  $c_0$  равны 0.

5. Обратный элемент не всегда существует.

**Определение.** Пусть  $A(x)$  - производящая функция. Тогда  $B(x)$  - обратная к  $A(x)$ , если  $A(x) \cdot B(x) = 1$  ( $B(x) = A(x)^{-1}$ )

**Примеры:**

$A(x) = 1 + x + x^2 + x^3 + \dots$  - обратима. Для неё существует обратный:  $1 - x$ .  $A(x)(1 - x) = 1 + 0x + 0x^2 + \dots = 1$   
 $B(x) = x$  - необратима, т.к.  $xC(x) = 0 + c_0x + c_1x^2 + \dots \neq 1$

Будем обозначать обратный таким образом:  $A(x)^{-1} = \frac{1}{A(x)}$ .

Запишем несколько свойств, которые позже будут доказаны на семинарах:

$$1. \frac{1}{A(x)} \cdot \frac{1}{B(x)} = \frac{1}{A(x)B(x)}$$

$$2. \frac{A(x)}{B(x)} + \frac{C(x)}{D(x)} = \frac{A(x)D(x) + B(x)C(x)}{B(x)D(x)}$$

Поясним, что по определению  $\frac{A(x)}{B(x)}$  значит  $A(x) \cdot B(x)^{-1}$ .

## 6.2 Дифференцирование

По **определению** производная к производящей функции  $F = f_0 + f_1x + f_2x^2 + \dots$  это:

$$F'(x) = f_1 + 2f_2x^2 + 3f_3x^3 + \dots = \sum_{k=1}^{+\infty} kf_k x^{k-1}$$

Свойства производных:

$$1. (F(x) + G(x))' = F'(x) + G'(x)$$

**Доказательство:**

Посмотрим на коэффициент при  $x^{k-1}$  у выражения слева:  $k(f_k + g_k) = kf_k + kg_k$ .

$$2. (cF(x))' = cF'(x) = (cF'(x))(x)$$

**Доказательство:**

Посмотрим на коэффициент при  $x^{k-1}$  у выражения слева:  $k \cdot cf_k = ckf_k$ .

$$3. \text{Правило Лейбница: } (F(x)G(x))' = F'(x)G(x) + F(x)G'(x).$$

**Доказательство:**

Посмотрим на коэффициент при  $x^{n-1}$  у выражения  $(F(x)G(x))'$ : при  $x^n$  в  $F(x)G(x)$  коэффициент равен  $\sum_{k=0}^n f_k g_{n-k}$ , значит при  $x^{n-1}$  у  $(F(x)G(x))'$  он равен  $n(f_0g_n + f_1g_{n-1} + \dots + f_ng_0)$ .

Теперь посмотрим на коэффициент при  $x^{n-1}$  у выражения  $F'(x)G(x)$ :  $\sum_{k=0}^{n-1} (k+1)f_{k+1}g_{n-1-k} = f_1g_{n-1} + 2f_2g_{n-2} + 3f_3g_{n-3} + \dots + nf_ng_0$ .

И на коэффициент при  $x^{n-1}$  у выражения  $F(x)G'(x)$  (он почти такой же как у предыдущего выражения):  $g_1f_{n-1} + 2g_2f_{n-2} + 3g_3f_{n-3} + \dots + ng_nf_0$ .

Тогда рассмотрим сумму коэффициентов при  $x^{n-1}$  у выражений  $F'(x)G(x)$  и  $F(x)G'(x)$ : любой  $f_i g_{n-i}$  входит в сумму два раза с коэф-ми  $i$  и  $n - i$ , которые в сумме дадут  $n$ . Тогда коэффициент у данной суммы как раз и будет  $nf_0g_n + nf_1g_{n-1} + \dots + nf_ng_0 = n(f_0g_n + f_1g_{n-1} + \dots + f_ng_0)$

$$4. \left(\frac{1}{F(x)}\right)' = -\frac{F'(x)}{F^2(x)} - \text{будет обговорено на семинаре}$$

$$5. \left(\frac{A(x)}{B(x)}\right)' = \frac{A'(x)B(x) - A(x)B'(x)}{B^2(x)}$$

Сводится к (3) и (4), т.к.  $\left(\frac{A(x)}{B(x)}\right)' = (A(x) \cdot \frac{1}{B(x)})'$

### 6.3 Пример применения

Задача будет заключаться в вычислении  $\sum_{i=0}^n i^2$  с помощью производящих функций. Т.е. по факту мы хотим найти производящую функцию для последовательности  $(0^2, 0^2 + 1^2, 0^2 + 1^2 + 2^2, \dots)$ .

Возьмём  $F(x) : (1, 1, 1, \dots) \rightarrow 1 + x^2 + x^3 + \dots$ ;  $F(x) = \frac{1}{1-x}$

$F'(x) : (1, 2, 3, \dots); F'(x) = (\frac{1}{1-x})' = \frac{1}{(1-x)^2}$

Давайте получим это же но с 0, домножив на  $x$ :

$xF'(x) : (0, 1, 2, 3, \dots); xF'(x) = \frac{x}{(1-x)^2}$

$(xF'(x))' : (1^2, 2^2, 3^2, \dots); (xF'(x))' = (\frac{x}{(1-x)^2})' = \frac{1+x}{(1-x)^3}$

Давайте снова получим это же но с 0, домножив на  $x$ :

$x(xF'(x))' : (0^2, 1^2, 2^2, 3^2, \dots); x(xF'(x))' = \frac{x(1+x)}{(1-x)^3}$

**Утверждение.** Пусть  $A(x) \rightarrow (a_0, a_1, a_2, a_3, \dots)$

$S = (a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots, \sum_{k=0}^n a_k, \dots)$ . Тогда  $S(x) = \frac{A(x)}{1-x}$ .

**Доказательство:**

Просто по определению  $\frac{A(x)}{1-x} = A(x)(1 + x + x^2 + \dots) = S(x)$

Поэтому производящая функция для  $(0^2, 0^2 + 1^2, 0^2 + 1^2 + 2^2, \dots) \rightarrow \frac{x(xF'(x))'}{(1-x)} = \frac{x(1+x)}{(1-x)^4}$

$G(x) = \frac{x(1+x)}{(1-x)^4}, g_n = \sum_{i=0}^n i^2$

Теперь наша задача понять, как "вытащить" из производящей функции её коэффициент. Хотя мы договорились пока ничего не подставлять в нашу производящую функцию, давайте определим подстановку 0:

$A(x) = a_0 + a_1 x + a_2 x^2 + \dots$ , тогда  $A(0) = a_0$ .

Запишем несколько очевидных свойств:

$$1. (A + B)(0) = A(0) + B(0)$$

$$2. (A \cdot B)(0) = A(0) \cdot B(0)$$

$$3. (cA)(0) = cA(0)$$

**Утверждение.**  $A \rightarrow (a_0, a_1, a_2, \dots)$ . Тогда  $a_n = \left. \frac{A^{(n)}(x)}{n!} \right|_{x=0}$  Несложно проверить, взяв производную  $n$  раз.

Разложим  $G(x)$  на сумму двух дробей  $\frac{x(1+x)}{(1-x)^4} = \frac{x^2}{(1-x)^4} + \frac{x}{(1-x)^4}$ . Но искать  $n$ -ые производные данных дробей тоже не просто, поэтому можем ввести вспомогательную производящую функцию  $H(x) = \frac{1}{(1-x)^4}$ . Понятно, что умножение на  $x^2$  и  $x$  делает сдвиг коэффициентов  $H(x)$  на 2 и на 1 вправо соответственно, поэтому коэффициенты  $h_{n-2}$  и  $h_{n-1}$  будут  $n$ -ми коэффициентами данных дробей соответственно. Тогда посчитаем производную в общем виде для  $\frac{1}{(1-x)^4}$ :

$H'(x) = \frac{5}{(1-x)^5}, H''(x) = \frac{4 \cdot 5}{(1-x)^6}, H'''(x) = \frac{4 \cdot 5 \cdot 6}{(1-x)^7}, \dots$  по индукции несложно проверяется, что  $H^{(n)}(x) = \frac{4 \cdot 5 \cdot 6 \cdots (n+3)}{(1-x)^{n+4}} = \frac{(n+3)!}{6(1-x)^{n+4}}$ .

Тогда  $h_n = \left. \frac{(n+3)!}{n! \cdot 6(1-x)^4} \right|_{x=0} = \frac{(n+1)(n+2)(n+3)}{6}$

Ответом будет  $g_n = \sum_{i=0}^n i^2 = h_{n-2} + h_{n-1} = \frac{(n-1)n(n+1)}{6} + \frac{n(n+1)(n+2)}{6} = \frac{n(n+1)(2n+1)}{6}$

### 6.4 Ещё один пример применения (бонусный)

Пусть  $A(x)$  - производящая функция для неупорядоченных выборок из  $S$  (то есть  $a_n$  = количество способов выбрать  $n$  элементов из  $S$  без учёта порядка). Аналогично  $B(x)$  - такая же функция, но для множества  $T$ . Будем также считать, что  $S \cap T = \emptyset$

**Неформальное утверждение.** Производящей функцией для количества выборок из  $S \cup T$  является функция  $A(x) \cdot B(x)$ .

**Пример про салат (всё-таки прикладная математика)**

Сразу отметим, что все овощи идентичны. Мы хотим сделать салат из огурцов (можно добавлять сколько угодно), помидоров (можно добавить или 0 шт., или 2 шт.) и авокадо (можно добавить не более 3 шт.). Тогда производящая функция для неупорядоченных выборок огурцов  $C(x) = 1 + x + x^2 + x^3 + \dots$ , помидоров  $T(x) = 1 + x^2$ , авокадо  $A(x) = 1 + x + x^2 + x^3$ .

Тогда производящая функция для объединения это  $C(x)T(x)A(x) = (1 + x + x^2 + x^3 + \dots)(1 + x^2)(1 + x + x^2 + x^3) = \frac{(1+x^2)(1+x+x^2+x^3)}{1-x} = \frac{(1+x^2)(1-x^4)}{(1-x)^2}$

## 7 Лекция 19

(Андрей)

### 7.1 Неупорядоченные выборки

Пусть имеем  $n$  различных объектов, из которых мы неупорядоченно хотим выбрать  $k$  штук. Конечно, мы могли бы это сделать, пользуясь обычной комбинаторикой, но иногда жизнь несправедлива, поэтому применим соображения из производящих функций.

Рассмотрим  $n$ -элементный набор  $S = \{a_1, a_2, \dots, a_n\}$  который представим в виде объединения  $n$  одноэлементных множеств, то есть  $S = \{a_1\} \cup \{a_2\} \cup \dots \cup \{a_n\}$ .

Рассмотрим произвольный элемент  $a_i$ . Понятно, что для него производящая функция в смысле нашей задачи будет иметь вид:  $1 + x$ . Далее, из прошлой лекции мы знаем, что производящая функция для объединения  $n$  объектов будет равна произведению производящих функций каждого из этих объектов. Поэтому искомая функция будем иметь вид:

$$(1+x)(1+x)\dots(1+x) = (1+x)^n = \sum_{i=0}^n C_n^i \cdot x^i$$

Таким образом, мы получили функцию вида:  $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$ , где коэффициент  $f_i$  обозначает количество способов выбрать неупорядоченно  $k$  элементов из  $n$ .

### 7.2 Бином Ньютона

Давайте обобщим формулу бинома Ньютона для целых коэффициентов и получим:

$$(1+x)^{-n} = \sum_{i=0}^{\infty} \binom{-n}{i} \cdot x^i$$

Давайте поясним, чему равен коэффициент  $\binom{-n}{k}$ .

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

Отсюда предыдущая формула переписывается в виде:

$$(1+x)^{-n} = \sum_{i=0}^{\infty} \binom{-n}{i} \cdot x^i = \sum_{i=0}^{\infty} \binom{n+i-1}{i} \cdot x^i$$

На самом деле, можно пойти дальше и определить биномиальный коэффициент  $\binom{\alpha}{k}$ , где  $\alpha \in \mathbb{R}, k \in \mathbb{N}$ .

$$\binom{\alpha}{k} = \frac{\alpha(\alpha+1)\dots(\alpha-k+1)}{k!}$$

Отдельно стоит отметить, что  $\binom{\alpha}{0} = 1$ .

**Пример:**

Рассмотрим равенство  $(1+x)^k \cdot (1+x)^l = (1+x)^{k+l}$ ,  $k, l \in \mathbb{N}$ . Оно очевидно, если мы рассматриваем его как равенство многочленов, но давайте взглянем на него на как на равенство производящих функций. Перепишем наше равенство:

$$\sum_{i=0}^{\infty} \binom{k}{i} x^i \cdot \sum_{j=0}^{\infty} \binom{l}{j} x^j = \sum_{n=0}^{\infty} \binom{k+l}{n} x^n.$$

При  $x^n$  стоит коэффициент:

$$\sum_{\substack{i+j=n \\ i,j \geq 0}} \binom{k}{i} \binom{l}{j} = \binom{k+l}{n}$$

Справа и слева мы получили многочлены от  $k$  и  $l$ , при этом  $n$  фиксировано. Заметим, что эти многочлены равны в бесконечном количестве точек. Далее, зафиксируем  $l \in \mathbb{N} \Rightarrow$  левая часть равна правой части  $\forall k \in \mathbb{R}$ . Затем зафиксируем  $k \in \mathbb{R}$  и получим, что левая часть равна правой части  $\forall l \in \mathbb{R} \Rightarrow$  эти многочлены равны  $\forall k, l \in \mathbb{R}$ .

### 7.3 Линейные рекуррентные соотношения с постоянными коэффициентами

Найдем явную формулу для  $n$ -го числа Фибоначчи, используя производящие функции.

Числа Фибоначчи задаются следующим рекуррентным соотношением:

$$F_{n+2} = F_{n+1} + F_n$$

причем  $F_0 = F_1 = 1$ .

Рассмотрим производящую функцию для последовательности Фибоначчи:

$$F(x) = F_0 + F_1 \cdot x + F_2 \cdot x^2 + \dots + F_n \cdot x^n + \dots$$

Умножим  $F(x)$  на  $x$ , а потом на  $x^2$ . Получаем:

$$xF(x) = F_0 \cdot x + F_1 \cdot x^2 + F_2 \cdot x^3 + F_3 \cdot x^4 + \dots + F_n \cdot x^{n+1} + \dots$$

$$x^2F(x) = F_0 \cdot x^2 + F_1 \cdot x^3 + F_2 \cdot x^4 + F_3 \cdot x^5 + \dots + F_n \cdot x^{n+2} + \dots$$

Сложим получившиеся две функции:

$$(x + x^2) \cdot F(x) = F_0 \cdot x + (F_0 + F_1) \cdot x^2 + (F_1 + F_2) \cdot x^3 + \dots + (F_{n-1} + F_n) \cdot x^{n+1} + \dots$$

Заметим, что каждый коэффициент этой функции тоже является числом Фибоначчи, поэтому перепишем эту функцию в таком виде:

$$(x + x^2) \cdot F(x) = F_1 \cdot x + (F_2) \cdot x^2 + (F_3) \cdot x^3 + \dots + (F_{n+1}) \cdot x^{n+1} + \dots = F(x) - F_0 = F(x) - 1$$

Теперь можем получить явный вид  $F(x)$ :

$$F(x) = \frac{1}{1 - x - x^2} = \frac{-1}{(x - x_1)(x - x_2)}$$

$$x_1 = \frac{-1 + \sqrt{5}}{2}, \quad x_2 = \frac{-1 - \sqrt{5}}{2}$$

Преобразуем наше выражение:

$$\begin{aligned} \frac{-1}{(x - x_1)(x - x_2)} &= \left( \frac{1}{x - x_1} - \frac{1}{x - x_2} \right) \cdot \frac{1}{x_2 - x_1} = \frac{-1}{\sqrt{5}} \cdot \left( \frac{1}{x - x_1} - \frac{1}{x - x_2} \right) = \frac{1}{\sqrt{5}} \cdot \left( \frac{1}{x - x_2} - \frac{1}{x - x_1} \right) = \\ &= \frac{1}{\sqrt{5}} \cdot \left( \frac{1}{-x_2 \cdot (1 - \frac{x}{x_2})} - \frac{1}{-x_1 \cdot (1 - \frac{x}{x_1})} \right) = \frac{1}{x_1 \cdot \sqrt{5}} \cdot (1 - \frac{x}{x_1})^{-1} - \frac{1}{x_2 \cdot \sqrt{5}} \cdot (1 - \frac{x}{x_2})^{-1} = \\ &= \frac{1}{x_1 \cdot \sqrt{5}} \cdot (1 + \frac{x}{x_1} + \frac{x^2}{x_1^2} + \dots) - \frac{1}{x_2 \cdot \sqrt{5}} \cdot (1 + \frac{x}{x_2} + \frac{x^2}{x_2^2} + \dots) = \dots + x^n \cdot \left( \frac{1}{x_1^{n+1} \cdot \sqrt{5}} - \frac{1}{x_2^{n+1} \cdot \sqrt{5}} \right) \end{aligned}$$

Итого:  $F_n = \frac{(-1)^{n+1}}{\sqrt{5}} \cdot (x_2^{n+1} - x_1^{n+1}) = \frac{1}{\sqrt{5}} \cdot \left( \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \right)$ . Победа, получили формулу Бине!

### 7.4 Теорема о рекуррентном соотношении

Пусть имеем некоторую рекуррентную последовательность  $\{a_i\}_{i=0}^{\infty}$  и пусть для некоторого  $k \in \mathbb{N}$  выполняется, что  $a_j$  член выражается через  $k$  предыдущих с постоянными коэффициентами. То есть:

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \dots + c_k a_n$$

Тогда если рассмотрим производящую функцию  $A(x) = a_0 + a_1 x + a_2 x^2 + \dots$

То  $A(x) = \frac{P(x)}{Q(x)}$ , где  $P(x), Q(x) \in \mathbb{C}(x)$  и  $\deg Q = k$ ,  $\deg P \leq k - 1$ .

**Доказательство:**

Рассмотрим произведение  $A(x) \cdot (c_1x + c_2x^2 + \dots + c_kx^k)$ :

$$c_1x \cdot A(x) = c_1a_0x + c_1a_2x^2 + \dots + c_1a_{n+k-1}x^{n+k} + \dots$$

$$c_1x^2 \cdot A(x) = c_1a_0x^2 + c_1a_2x^3 + \dots + c_1a_{n+k-2}x^{n+k} + \dots$$

Делаем так  $k$  раз и получаем:

$$c_kx^k \cdot A(x) = c_ka_0x^k + \dots + c_ka_nx^{n+k} + \dots$$

Просуммируем все эти выражения и получим:

$$A(x)(c_1x + c_2x^2 + \dots + c_kx^k) = (\text{какой-то многочлен } R(x)) + a_kx^k + a_{k+1}x^{k+1} + \dots = A(x) + P(x)$$

$P(x)$  - тоже некоторый многочлен, причем  $\deg P(x) \leq k - 1$ .

Теперь вспомним, что рассматривали произведение  $A(x) \cdot (c_1x + c_2x^2 + \dots + c_kx^k)$ . Мы получили, что оно равно  $A(x) + P(x)$ , откуда  $P(x) = A(x) \cdot (-1 + c_1x + c_2x^2 + \dots + c_kx^k)$ . Обозначим  $(-1 + c_1x + c_2x^2 + \dots + c_kx^k)$  за  $Q(x)$  и получим, что  $A(x) = \frac{P(x)}{Q(x)}$ .

**Ч.Т.Д.**

## 7.5 Нахождение общей формулы для $a_n$

Теперь мы получили, что  $A(x) = \frac{P(x)}{Q(x)} = \frac{P(x)}{(1-q_1x)^{r_1} \dots (1-q_nx)^{r_s}} = \dots + \frac{A}{(1-q_i \cdot x)^m} + \dots$  (разложение в сумму простых дробей ( $A$  - это какой-то коэффициент)). Заметим, что слагаемое вида:

$$\frac{A}{(1-q_i \cdot x)^m}$$

в точности равно:

$$A \cdot \sum_{k=0}^{\infty} \binom{-m}{k} \cdot (-q_i \cdot x)^k$$

Тогда чтобы получить коэффициент при  $x^n$  у производящей функции, мы пройдемся по всем элементарным дробям и соберем в сумму все коэффициенты при  $x^n$ . Причем итоговый коэффициент будем иметь вид:

$$a_n = q_1^n \cdot p_1(n) + \dots + q_t^n \cdot p_t(n)$$

$(p_i(n)$  - какой-то многочлен от  $n$ , который возникает из-за биномиального коэффициента при  $q_i^n$ )

Выражение вида  $p_i(n) \cdot q_i^n$  называют квазимногочленом.

## 7.6 Числа Каталана

### Задача о правильной скобочной последовательности

Я буду обозначать правильную скобочную последовательность как **ПСП**.

ПСП - это такая последовательность, которая получается за конечное число шагов по следующим правилам:

1. () - ПСП.
2. Если  $P$  - ПСП, то  $(P)$  - тоже ПСП.
3. Если  $P_1$  и  $P_2$  - ПСП, то  $P_1 + P_2$  - ПСП (под + подразумевается конкатенация).

Обозначим за  $C_n$  - число правильных скобочных последовательностей длины  $2n$ . Найдем это число, выразив число  $C_{n+1}$  через предыдущие.

Для этого рассмотрим первый момент, когда число левых скобок равно числу правых скобок (см. картинку)

Получили, что длина  $P_1$  равна  $2k$ , а длина  $P_2$  равна  $2(n+1) - 2k$ . Тогда получаем, что число  $C_{n+1}$  выражается следующим образом:

$$C_{n+1} = C_0 \cdot C_n + C_1 \cdot C_{n-1} + C_2 \cdot C_{n-2} + \dots + C_n \cdot C_0 = \sum_{k=0}^n C_k \cdot C_{n-k}$$

При этом  $C_0$  мы полагаем равным 1. Рассмотрим производящую функцию для нашего рекуррентного соотношения:

$$C(x) = C_0 + C_1x + C_2x^2 + \dots$$

Рассмотрим произведение  $C(x) \cdot C(x)$ :

$$C(x) \cdot C(x) \Rightarrow \text{при } x^n \text{ стоит коэффициент } \sum_{k=0}^n C_k \cdot C_{n-k} = C_{n+1}$$

Тогда умножим  $C(x) \cdot C(x)$  на  $x$  и при члене  $x^{n+1}$  получим коэффициент:  $\sum_{k=0}^n C_k \cdot C_{n-k} = C_{n+1}$  (что мы и хотели). Но тогда:

$$x \cdot C(x) \cdot C(x) = C_1x + C_2x^2 + \dots = C(x) - C_0$$

Таким образом, получили соотношение:

$$x \cdot C(x)^2 - C(x) + 1 = 0$$

Решая относительно  $C(x)$ , получим, что:

$$C(x) = \frac{1 \pm \sqrt{1 - 4x}}{2x} = \frac{1 \pm (1 - 4x)^{1/2}}{2x}$$

Далее, возьмем знак минус и раскроем  $(1 - 4x)^{1/2}$  по биному и тогда получим явную формулу для  $C(x)$ :

$$C(x) = \frac{1 \pm \sqrt{1 - 4x}}{2x} = \frac{1 - (1 - 4x)^{1/2}}{2x}$$

Рассмотрим  $1 - (1 - 4x)^{1/2}$ :

$$1 - (1 - 4x)^{1/2} = 1 - \sum_{k=1}^{\infty} \binom{\frac{1}{2}}{k} (-4x)^k = - \sum_{k=1}^{\infty} \frac{\frac{1}{2}(\frac{1}{2}-1)\dots(\frac{1}{2}-k+1)}{k!} (-4x)^k = - \sum_{k=1}^{\infty} \frac{1(-1)(-3)\dots(-(2k-3))}{2^k \cdot k!} \cdot (-4x)^k =$$

$$= \sum_{k=1}^{\infty} \frac{1(1)(3)\dots(2k-3)}{2^k \cdot k!} 4^k \cdot x^k = \sum_{k=1}^{\infty} \frac{1 \cdot 1 \cdot 3 \cdot \dots \cdot (2k-3) \cdot 2 \cdot 4 \cdot 6 \cdot \dots \cdot (2k-2)}{2^{k-1} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (k-1) \cdot 2^k \cdot k!} 4^k \cdot x^k = \sum_{k=1}^{\infty} \frac{(2k-2)!}{(k-1)! \cdot (k-1)!} \cdot \frac{2}{k} \cdot x^k$$

$$\text{Значит, } \frac{1-(1-4x)^{1/2}}{2x} = \sum_{k=1}^{\infty} \frac{(2k-2)!}{(k-1)!(k-1)!} \cdot \frac{1}{k} \cdot x^{k-1} = \sum_{k=1}^{\infty} \binom{2n}{n} \cdot \frac{1}{n+1} \cdot x^n$$

На данный момент мы, можно сказать, угадали ответ - теперь можно строго доказать эту формулу по индукции.

**Утверждение:**  $C_n = \binom{2n}{n} \cdot \frac{1}{n+1}$ ,  $C_0 = 1$ ,  $C_1 = 1$ .

**Доказательство:**

Введем числа  $\tilde{C}_n = \binom{2n}{n} \cdot \frac{1}{n+1}$  (знак тильды просто означает, что мы хотим отличать числа Каталана, полученные из производящих функций и полученные из комбинаторных рассуждений). Докажем, что для них выполняется рекуррентное соотношение:

$$\tilde{C}_n = \sum_{\substack{k+l=n-1 \\ k, l \geq 0}} \tilde{C}_k \tilde{C}_l$$

Пока что непонятно, как это можно хорошо доказать. Чтобы сделать нашу жизнь лучше, рассмотрим следующее равенство (просто воспользуемся тем, как мы определили биномиальный коэффициент с дробным показателем):

$$\binom{\frac{1}{2}}{n} = \frac{(-1)^n}{2^{2n-1}} \tilde{C}_{n-1}$$

Правда, при  $n = 0$  правая часть не имеет смысла, и чтобы придать ей смысл, надо положить  $\tilde{C}_{-1} = -1/2$ . Теперь мы можем вспомнить тождество, которое верно  $\forall k, l \in \mathbb{R}$ :

$$\sum_{\substack{i+j=n \\ i,j \geq 0}} \binom{k}{i} \binom{l}{j} = \binom{k+l}{n}$$

После этого запишем его для  $k = 1 = \frac{1}{2}$ , правая часть обратится в нуль, и получится тождество:

$$0 = \tilde{C}_{-1} \cdot \tilde{C}_{n-1} + \tilde{C}_0 \cdot \tilde{C}_{n-2} + \tilde{C}_1 \cdot \tilde{C}_{n-3} + \dots + \tilde{C}_{n-1} \cdot \tilde{C}_{-1}$$

Вспоминая о соглашении  $C_{-1} = -\frac{1}{2}$ , мы получаем искомое рекуррентное соотношение (только для меньшего на единицу значения  $n$ ).

**Ч.Т.Д.**

## 8 Лекция 20

(Илья)

### 8.1 Комбинаторные игры(определения и примеры)



Начнём с небольшого примера.

#### Пример(игра в монетницу)

Игроки Первый и Второй по очереди достают монеты из монетницы, в которой изначально лежат 20 монет, 2 или 3 монеты. За один ход соответственно можно взять 2 или 3 монеты. Проигрывает тот, кто не может сделать ход.

Нужно сказать, есть ли у какого-то игрока выигрышная стратегия, если оба игрока будут играть *оптимальным способом*. (пока не очень понятно, как это с формальной точки зрения, но потом станет понятно)

**Ответ:** Выигрывает Второй.

**Решение:**

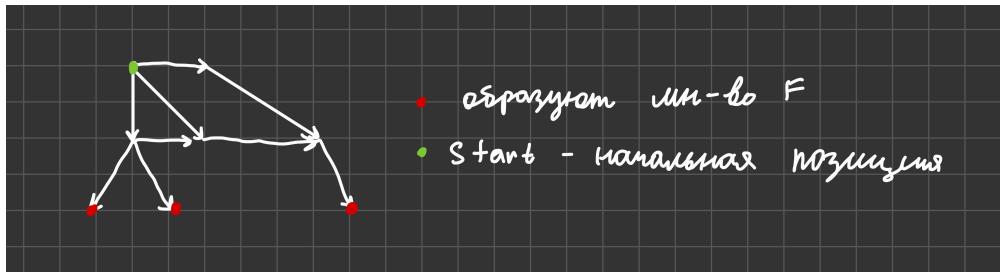
1. Приведём некую стратегию для второго игрока. Заметим, что 20 - это 4 раза по 5 монет.
2. Если Первый берёт 2 монеты, то Второй должен взять 3 и наоборот. То есть Второй своим ходом дополняет ход Первого до 5. Тогда проделав так 4 раза, Второй заберёт последние монеты и тем самым победит.

Мы хотим формально ввести понятие игры, введя всё, что нам нужно для этого.

**Задание комбинаторной игры с 2 игроками**(будем называть их Макс и Мин, позже поймёте почему), с полной информацией:

1. Множество позиций  $S$ , с указанием, кто ходит в конкретной позиции.
2. Начальная позиция:  $start$  и множество позиций  $F$ , в которых игра заканчивается.
3. Ходы:  $\forall s \in S \rightarrow N(s)$  - множество позиций, куда можно попасть из  $s$ . Причём, если  $s \notin F$ , то  $N(S) \neq \emptyset$
4. Выигрыш - некая функция  $f : F \rightarrow R$

Заметим, что игра - это по сути ориентированный граф (см. картинку), причём мы договоримся, что граф ацикличен, чтобы игра не могла длиться вечно. Понятно, что есть игры, в которых может так получиться, что в игре могут быть циклы, но такие моменты обычно оговорены правилами (например, игра в шахматах про ничью в случае повтора хода 3 раза подряд). Это некий технический момент, который понадобится нам.



### Пример описания игры в шахматы:

Заметим, что нам недостаточно знать расстановку фигур и чей ход для описания позиций, потому что в шахматах есть куча нюансов по типу взятия на проходе, рокировки и тд, и нам важно знать, были ли они или нет, чтобы понять кто ходит при той или иной расстановке фигур, поэтому нам необходимо вести за собой по-хорошему всю историю игры.

### Пример описания игры в крестики и нолики:

Тут уже всё попроще, поэтому тут под позицией действительно можно понимать просто расстановку какую-то крестиков и ноликов, которая реально могла встретиться в игре (модуль разности крестиков и ноликов равен 1 или 0)

Поговорим про то, как устроена функция выигрыша: (покажу на примерах, и сразу станет понятно)

- В игре в монетницу функция выигрыша может принимать значения 1 и -1, потому что тут можно или выиграть, или проиграть.
- В шахматах и крестиках-ноликах функция выигрыша может принимать значения -1, 0 и 1, потому что может быть ещё и ничья.

Теперь понятно, почему игроков назвали Макс и Мин, потому что Макс стремится максимизировать выигрыши в игре, а Мин минимизировать, поэтому если значение функции равно 1, то победил Макс, а если -1, то Мин.

Дадим ещё пару определений.

**Партия**- это набор  $v_0, v_1, \dots, v_k$  - таких, что  $v_i \in S$  и  $(v_i, v_{i+1}) \in E$  (ребра графа) и  $v_0$  - начальная позиция и  $v_k \in F$

**Стратегия (для Макса)** - это функция  $g : \text{множество позиций} \rightarrow \text{множество позиций}$ , где ходит Макс  $\rightarrow$  множество позиций, в которую можно сходить ( $s \rightarrow v \in N(s)$ )

Стратегия для Мина строится полностью аналогично.

**Замечание:** В нашем курсе мы будем рассматривать только позиционные стратегии, где стратегия зависит только от текущей позиции, то есть нам не важна история всех позиций до этого, а только с конкретной позиции (заметим, что формально это ничего не нарушает, так как у нас само понятие конкретной позиции может включать в себя уже некую историю игры (см. пример с шахматами выше)).

Мы будем говорить, что стратегия  $g$  для игрока Макс (для Мин аналогично) гарантирует выигрыш  $c \in R$ , если для любой партии  $v_0, v_1, \dots, v_k$ , согласованной с этой стратегией  $g$ , Макс получит выигрыш не меньше  $c$ , то есть  $f(v_k) \geq c$

Для Мина будет аналогично, но только  $f(v_k) \leq c$

Ещё одно определение...

Число  $C$  называется **ценой игры**, если у Макса и у Мина есть стратегии, гарантирующие выигрыш  $C$ .

## 8.2 Теорема о цене игры

**Теорема о цене игры:** У любой описанной выше игры существует единственная цена.

**Доказательство:**

1. Сначала докажем единственность, потому что она очевидна, ведь если у игры была не одна цена, а , например  $c_1$  и  $c_2$  и не умоляя обности  $c_1 < c_2$ , то давайте возьмём стратегию Макса, которая гарантирует выигрыш  $c_2$ , то есть  $f(v_k) \geq c_2$ , и стратегию Мина, которая гарантирует выигрыш  $c_1$ , то есть  $f(v_k) \leq c_1$ , откуда  $c_1 \geq c_2$  - противоречие!

2. Теперь покажем существование. Давайте введём вспомогательное определение:

Назовём позицию **хорошой**, если игра, начинающаяся с этой позиции, имеет цену. Для каждой хорошей позиции мы выберем в этой позиции тот ход, который согласован со стратегией, гарантирующей эту цену.

**Лемма:** Если все позиции, в которые можно попасть из данной (быть может, за несколько ходов), хороши (следовательно, в каждой из них выбран ход стратегий), то и данная позиция хороша (следовательно, в ней также выбран ход стратегий).

Что говорит эта лемма про заключительные позиции? По правилам логики хороши все позиции, в которые можно попасть из заключительной (таких позиций просто нет, так как из заключительной позиции попасть никуда нельзя). Но и утверждение леммы тривиально: в заключительных позициях результат уже известен, так что оба игрока его уже обеспечили.

#### Доказательство:

- Для доказательства леммы осталось рассмотреть случай незаключительной позиции. В ней ходит либо Макс, либо Мин. Рассуждения в обоих случаях аналогичны, разберём подробно только случай, когда в позиции  $x$ , принятой за начальную, ходит Макс.
- Пусть  $y_1, \dots, y_k$  — все позиции, в которые Макс может попасть по правилам игры. По предположению все эти позиции хороши и потому имеют некоторые цены  $c_1, \dots, c_k$ . Более того, мы предполагаем, что в каждой из этих позиций, как и во всех позициях, в которые можно попасть из них, выбран ход стратегий. Что должен делать Макс «при правильной игре»?
- Понятное дело — он должен выбрать позицию с наибольшим  $c_i$  (одну из таких, если максимум достигается в нескольких) и пойти туда. И дальше следовать той стратегии для позиции  $y_i$ , которая гарантирует ему  $c_i$  и которая всегда выбирает ход стратегий (по условию такая существует). Так он обеспечит себе результат не меньше  $c_i$ . С другой стороны, в какую бы позицию  $y_j$  он ни пошёл, у Мина есть такая стратегия, которая обеспечивает ему результат не больше  $c_j$  и всегда выбирает ход стратегий. Заметим, что  $c_j \leq c_i$ , поскольку  $c_i$  было максимальным.
- Повторим это рассуждение более формально. Не ограничивая общности, будем считать, что в начальной позиции  $x$  ходит Макс. Докажем, что цена игры с началом в  $x$  равна  $c = \max(c_1, \dots, c_k)$ , где  $c_i$  — цена игры с началом в  $y_i$ , существующая по предположению индукции. Ходом стратегий в позиции  $x$  объявим ход в позицию  $y_i$  с наименьшим индексом  $i$ , для которой достигается максимум, то есть  $c_i = c$ .
- По предположению позиция  $y_i$  хороша, то есть у Макса есть стратегия, которая выбирает ходы стратегий и гарантирует цену не ниже  $c = c_i$ . Значит, стратегия Макса, которая выбирает ход стратегий в каждой позиции, начиная с  $x$ , гарантирует ему результат не меньше  $c$ .
- С другой стороны, стратегия Мина, которая выбирает ходы стратегий в позициях, которые возникают в партии, начинающейся с позиции  $x$ , гарантирует ему результат не больше  $c_i$ . Действительно, пусть Макс пошёл в  $y_j$ . Тогда по предположению у Мина есть стратегия, которая гарантирует Мину результат не больше  $c_j \leq c$  ( $c$  — максимум) в игре с началом в  $y_j$  и всегда выбирает ходы стратегий.
- Здесь существенен выбор ходов стратегий в каждой из позиций, благодаря чему стратегия Мина при игре из начальной позиции  $x$  корректно определена.

Теперь можно доказать очень просто и существование.

Пусть есть плохая позиция. Тогда по лемме есть позиция, в которую можно из неё перейти, которая тоже будет плохой (в частности, наша позиция не заключительная). Из этой новой плохой позиции по тем же причинам можно перейти в какую-то плохую позицию, и так далее. Рано или поздно (граф ведь конечный) получится цикл, которого быть не может — противоречие.

#### Ч.Т.Д.

## 9 Лекция 21

(Никита)

### 9.1 N и P позиции (выигрышные и проигрышные)

**Беспрестрастная игра** — это такая игра, в которой два игрока ходят по очереди и проигрывает тот, кто не может сделать ход (иногда рассматривается, что выигрывает тот, кто не может сделать ход). При этом допустимые ходы зависят только от позиции, а не от того, кто из игроков ходит сейчас. Соответственно есть позиции двух типов:  $\{1, -1\}$ .

Тогда **N-позиции (выигрышные)** — позиции, в которых выигрывает тот, кто ходит следующим (от слова Next).

*P*-позиции (проигрышные) - позиции, в которых выигрывает тот, кто ходил предыдущим (от слова Previous).

Понятно, что текущая позиция:

- N-позиция, если есть ход в *P*-позицию.
- P-позиция, если все ходы ведут в *N*-позиции.

Исследовать вершины нужно в соответствии с топологической сортировкой. Данная процедура когда мы идём из проанализированных позиций в ещё не проанализированные называется *Анализом с конца*.

**Пример:**

Приведём пример несложной игры, в которой мы можем применить анализ с конца.

*Правила:* за свой ход можно подвинуть ладью на сколько угодно клеток вправо или вверх. Проигрывает тот игрок, который не может сдвинуть ладью. Изначально ладья стоит в левой нижней клетке.

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| N | N | N | N | N | N | N | N | P |
| N | N | N | N | N | N | P | N | N |
| N | N | N | N | N | P | N | N | N |
| N | N | N | N | P | N | N | N | N |
| N | N | N | P | N | N | N | N | N |
| N | N | P | N | N | N | N | N | N |
| N | P | N | N | N | N | N | N | N |
| P | N | N | N | N | N | N | N | N |

Проанализировав позиции, видим, что при правильной игре второго игрока первый всегда проигрывает. Несложно восстанавливается и сам стратегия: после каждого хода первого игрока, второй своим следующим ходом возвращает его на главную диагональ.

## 9.2 Игра Ним

Есть  $n$  кучек камней:  $x_1, x_2, \dots, x_n (x_i > 0)$

Разрешается в свой ход взять любое количество камней, но только из одной кучки (в том числе все камни из кучки). Проигрывает тот, кто не может сделать ход.

$N = 1 : x_1$  - выигрывает *I* игрок (берёт всю кучку).

$N = 2 : x_1, x_2$  - можно посмотреть на эту ситуацию как на игру с ладьей, только можно ходить влево и вниз из верхнего правого угла (то есть за ход можно уменьшать одну координату,  $x_1$  или  $x_2$ . И тогда если  $x_1 = x_2$  - выигрывает *II* игрок ровно так, как мы описывали выше, а если  $x_1 \neq x_2$  - выигрывает *I*, первым ходом выравниваю количество камней в кучках и сводя задачу к предыдущей.

$N = 3$  : позиция  $(n, n, m)$ , например, - *N*-позиция, т.к. она сводится к  $(n, n, 0)$ , *P*-позиции. Но в общем случае довольно сложно проанализировать позицию. Однако это возможно сделать с помощью двоичной СС.

**Теорема:** Каждую из  $n$  кучек записываем в двоичной системе счисления:

$$x_1 = x_1^{(r)} \dots x_1^{(1)} x_1^{(0)}$$

$$x_2 = x_2^{(r)} \dots x_2^{(1)} x_2^{(0)}$$

$$\dots$$

$$x_n = x_n^{(r)} \dots x_n^{(1)} x_n^{(0)}$$

Далее вычислим побитовый *XOR*, т.е. суммируем по модулю 2 биты у всех кучек в одном разряде. Получившуюся строку результатов будем называть *res*.

Наконец, теорема гласит, что  $(x_1, x_2, \dots, x_n)$  - *P*-позиция  $\Leftrightarrow res = 00\dots0$

**Пример:**

Проанализируем позицию  $(1, 2, 3)$ :

$$1 = 01$$

$$2 = 10$$

$$3 = 11$$

$$res = 00 \Rightarrow \text{это } P\text{-позиция.}$$

Проанализируем позицию (2, 3, 4):

$$2 = 010$$

$$3 = 011$$

$$4 = 100$$

$res = 101 \Rightarrow$  это  $N$ -позиция.

#### Доказательство:

Докажем два факта (с их помощью можно будет применить анализ с конца, т.к. в заключительной позиции  $res = 0$ ):

1. если  $res \neq 0$ , то можно сделать ход в позицию, где  $res = 0$ .
2. если  $res = 0$ , то любой ход ведёт в позицию, где  $res \neq 0$ .

1) Возьмём первую 1 слева в  $res$ . Пусть она соответствует некоторому  $k$ -му биту. Тогда должна найтись кучка  $x_i$ , у которой в  $k$ -м бите стоит 1. Заменяем эту единицу на 0. Далее идём вправо по двоичной записи  $x_i$  и инвертируем биты в тех столбцах, у которых в соответствующих позициях  $res$  стоит 1. Понятно, что получилось меньшее число  $x_i$ . То есть просто убираем из  $x_i$ -й кучи  $x_i - x'_i$  камней и действительно получаем  $res' = 0$ . Этот факт доказан.

2) Этот факт совсем очевиден. Если мы уменьшаем кучку, мы точно поменяли какой-то его бит. Тогда понятно, что  $XOR$  по этой строке станет противоположным тому, что был, то есть 1. Значит  $res \neq 0$ . Теорема доказана.

### 9.3 Задача об угадывании числа

Есть числа  $1, 2, \dots, N$ . Есть два игрока: Алиса и Боб. Алиса загадывает число, а Боб может задавать вопросы, на которые можно ответить да или нет. Боб задаёт  $k$  вопросов. Его цель: точно определить загаданное число.

Одна из стратегий Боба заключается в том, что он может каждый раз выбирать среднее число, и спрашивать, находится ли загаданное число в первой половине (включая среднее). Если да, то он рассматривает первую половину (или примерно половину в случае нечётного). Иначе - вторую. Тогда понятно, что  $k \leq \lceil \log_2 N \rceil$ . Чтобы не было этой неудобной ситуации с тем, что нечетное число чисел не делится на две равные половины, можем предположить, что чисел изначально было, не  $N$ , а  $2^s (2^s \geq N)$ , где  $2^s$  - наименьшая степень  $2 \geq N$ . Теперь Боб всегда может угадать число точно за  $s$  вопросов:  $k \leq s = \lceil \log_2 N \rceil$ .

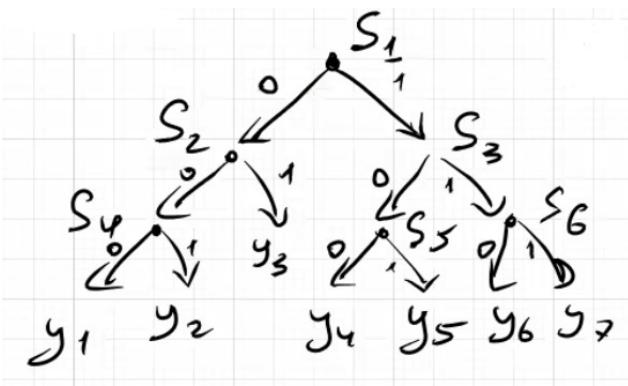
Поясним, почему не получится гарантированно угадать число за меньшее число вопросов  $k$ . Пусть хватило  $k$  вопросов: получили последовательность ответов  $a_1 a_2 \dots a_k$  из да/нет, по которой мы восстанавливаем число. Понятно, что каждая последовательность однозначно задаёт своё число. Действительно, если для двух различных чисел  $x$  и  $y$  Алиса даёт Бобу на его вопросы полностью одинаковые ответы, то для Боба эти случаи неразличимы: его диалоги с Алисой для  $x$  и для  $y$  выглядят одинаково. При этом Боб после диалога выдаёт какой-то ответ, который определяется только состоявшимся диалогом. Значит в одном из случаев ответ будет неправильным. Далее, заметим, что не может быть так, что для двух различных  $x$  и  $y$ , загаданных Алисой, цепочка ответов для  $x$  является началом цепочки ответов для  $y$ . Действительно, иначе диалог Боба с Алисой выглядит одинаково для  $x$  и  $y$  до того момента, когда будут заданы все вопросы из цепочки ответов для  $x$ . Значит, к этому моменту Боб не может отличить  $x$  от  $y$  и должен делать для них одно и то же, тогда как он в одном случае задаёт следующий вопрос, а в другом - нет.

Таким образом, мы получили, что каждому числу от 1 до  $N$  соответствует последовательность из не более чем  $k$  нулей и единиц, все эти последовательности различны, и ни одна не является началом другой. Заметим, что семейство этих последовательностей содержит не более  $2^k$  элементов. Действительно, если какая-то из них имеет длину меньше  $k$ , то продолжим её, например, нулями. Тогда для различных  $x$  и  $y$  полученные последовательности длины  $k$  различны: иначе они либо совпадают, либо одна (более короткая) является началом другой. Таким образом, каждому числу от 1 до  $N$  соответствует последовательность длины  $k$  из нулей и единиц, и все эти последовательности различны. Всего последовательностей длины  $k$  из нулей и единиц  $2^k$ . По принципу Дирихле, чисел от 1 до  $N$  должно быть не больше  $2^k$  (иначе двум разным числам соответствуют одинаковые последовательности). Значит нужно, чтобы  $2^k \geq N \Rightarrow k \geq \lceil \log_2 N \rceil$  ■

### 9.4 Разрешающие деревья

Даны  $X, Y$  - конечные множества и  $f : X \rightarrow Y$ . Требуется вычислить  $f(x)$  при некотором неизвестном входе  $x$ . Разрешается задавать вопросы типа  $x \in S$  для подмножеств  $S$  множества  $X$ . Тогда разрешающим деревом будем называть двоичное дерево, каждая промежуточная вершина которого (не лист) помечена некоторым подмножеством  $S \subseteq X$ . Каждый лист помечен элементом  $b \in Y$ . Из каждой промежуточной вершин выходит три ребра: одно к корню и два к листьям. Для каждой промежуточной вершины одно из рёбер, ведущих к листьям, помечено единицей, а другое - нулюм.

Некоторый конкретный пример разрешающего дерева:



Мы строим путь от корня на каждом шаге переходя по ребру с 1, если ответ положительный, и 0, если ответ отрицательный. Вычисления завершается тогда, когда мы попадаем в лист. Мы говорим, что протокол (по-другому разрешающее дерево) вычисляет функцию  $f$ , если для всякого  $x \in X$  протокол выдаёт  $f(x)$ .

**Сложностью** адаптивного протокола (адаптивным протоколом - такой протокол, вопрос в котором может зависеть от предыдущих ответов) называется глубина дерева (несложно убедиться, что она равна количеству вопросов, которое потребуется задать в худшем случае).

Рассмотрим неадаптивную постановку задачи. Предположим, что Боб отправляет сразу  $k$  вопросов по почте. Тогда можем задавать такие независимые вопросы: верно ли, что в  $i$ -м бите числа стоит 1?  $\forall i$ . Битов в числе не более чем  $\lceil \log_2 N \rceil$ , значит  $k \geq \lceil \log_2 N \rceil$ . Понятно, что меньше вопросов, чем в адаптивном точно не получится, поскольку неадаптивный протокол не опирается на историю ответов, что несколько усложняет вычисление (ведь если Боб в неадаптивном протоколе справляется с задачей за  $k$  вопросов, то он точно справится за  $k$  и в адаптивном - достаточно задать те же вопросы).

Давайте покажем на изображённом выше примере (к задаче об угадывании числа), как переписать адаптивный протокол в неадаптивный. Приведём вопросы, которые мы будем задавать:

- 1) Верно ли, что  $x \in S_1$ ?
- 2) Верно ли, что если  $x \in S_1$ , то  $x \in S_3$ , а если же  $x \notin S_1$ , то  $x \in S_2$ ?
- 3) ...

Вопросы будут получаться большими и громоздкими, однако данное рассуждение работает для любой задачи такого типа и любого адаптивного алгоритма.

## 9.5 Примеры задач

### 9.5.1 Задача о взвешивании

Есть  $n$  монет различной массы, ход заключается в сравнении весов двух монет. Наша цель: найти самую тяжёлую монету за как можно меньшее число вопросов  $k$ .

**Решение:**

**Лемма.** Для адаптивной модели необходимо и достаточно  $n - 1$  взвешивание.

**Доказательство:**

**Достаточность:** можно взять любую монету и сравнивать её с какой-нибудь другой. Если она оказалась тяжелее, то выкидываем ту, с которой сравнивали и продолжаем сравнение с оставшимися. Если же она оказалась легче, то выкидываем её и берём ту, которой она "проиграла" и уже с ней продолжим сравнение с оставшимися. Таким образом за  $n - 1$  сравнение мы вычислим максимум.

**Необходимость:** пусть мы нашли максимум за  $n - 2$  взвешивания. Тогда построим граф, где вершинами будут монеты, а ребрами будут соединены те монеты, которые мы попарно сравнивали. Если в графе на  $n$  вершинах  $n - 2$  ребра, то он несвязен. Тогда рассмотрим его компоненту связности  $V_1$ , в которой находится максимум, и  $V_2$  - все остальные объекты. Увеличим веса всех монет в  $V_2$  на одно и то же число так, чтобы они были тяжелее максимума в  $V_1$ . Причём результаты взвешиваний не изменятся, потому что они были или в пределах  $V_1$ , или в пределах  $V_2$ , а самая тяжёлая монета станет другой (теперь она в  $V_2$ ). Таким образом результат взвешивания даст один и тот же результат при разных максимумах, значит алгоритм работает неправильно. Противоречие, значит  $n - 1$  взвешиваний необходимо.

Теперь посмотрим на неадаптивную модель для данной задачи. Как мы видели ранее в общей модели разрешающих деревьев, отличий между адаптивным и неадаптивным протоколом нет, их сложности одинаковые. Но это достигается за счёт весьма нетривиальных запросов в неадаптивной модели. Если же мы ставим ограничения на тип запросов, то логично ожидать, что разница между моделями появится.

**Лемма.** Докажем, что для неадаптивной модели необходимо и достаточно  $\binom{n}{2} = \frac{n(n-1)}{2}$  взвешивания.

**Доказательство:**

**Достаточность:** очевидна, т.к. можем просто сравнить попарно все объекты и найти максимум. Как раз будет  $\binom{n}{2}$  сравнения.

**Необходимость:** пусть мы нашли максимум меньше чем за  $\binom{n}{2}$  взвешивания. Значит есть два объекта  $x$  и  $y$ , которые не сравнивались. Тогда подадим на вход те же объекты, но увеличим массу у  $x$ . А затем еще один вход с теми же объектами, но увеличим массу у  $y$ . Мы получим одинаковые ответы при разных входах, а значит алгоритм выдаст на них один и тот же результат. Поскольку самые тяжёлые объекты в этих двух входах разные, алгоритм работает неправильно. Противоречие, значит  $\binom{n}{2}$  сравнения необходимо.

### 9.5.2 Задача о связности графа

Для начала определим, что такая сложность протокола для вычисления булевой функции: нам дана  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , причём сам набор  $x_1, \dots, x_n$  не дан. Мы можем задавать вопросы вида: верно ли, что  $x_i = 0$ . Однако есть функции, для которых можно задать меньше вопросов, чтобы вычислить её значение. Тогда сложность протокола - минимальное число вопросов указанного вида, которое нужно задать, чтобы вычислить  $f(x_1, \dots, x_n)$ .

В доказательствах нижних оценок используется метод противника. Будем играть в модели разрешающих деревьев. Противник задаёт какой-нибудь вход в алгоритм, в процессе возможно видоизменяя его, но так, чтобы его ответы согласовывались с предыдущими его ответами и не противоречили реальности. Тогда алгоритм пытается выдать ответ за как можно меньшее число вопросов, а противник (за него будем играть мы) наоборот пытается увеличить это число вопросов. То есть алгоритм играет за MIN, а мы играем за MAX. У такой игры есть цена  $k$ , то есть такое число вопросов, что алгоритм всегда может выдать правильный ответ за  $\leq k$  вопросов, а противник задать такой вход, чтобы алгоритму нужно было задать  $\geq k$  вопросов. Тогда число  $k$  - это будет необходимое число вопросов.

Решим такую задачу: нужно проверить связность графа. Введём булеву функцию  $CONN : \{0, 1\}^{\binom{n}{2}} \rightarrow \{0, 1\}$  от  $\binom{n}{2}$  переменных, где  $x_{ij}$  - есть ребро ли ребро (1), или нет (0). То есть функция  $CONN$  принимает граф (множество его рёбер) и выдаёт 1, если он связан, 0 - в противоположном случае.

Нужно узнать сложность булевой функции в модели, указанной выше.

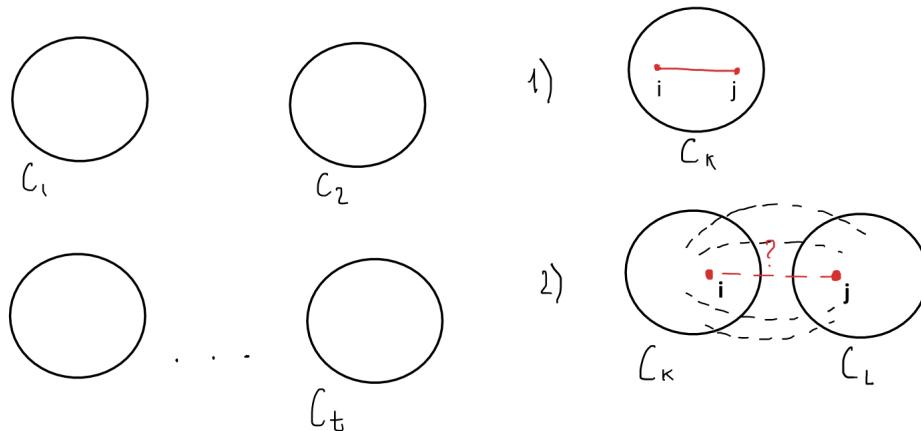
**Утверждение:** Сложность функции  $CONN$  в модели булевых функций =  $\binom{n}{2}$

**Доказательство:**

**Достаточность:** Достаточность очевидна, можно просто задать вопрос про каждое ребро (которых  $\binom{n}{2}$  штук) и в получившемся графе проверить связность.

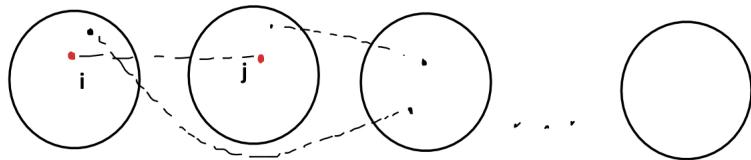
**Необходимость:** Играем за противника. В данной игре на самом деле даже не важна согласованность действий противника, поскольку рёбра не зависят друг от друга (хотя, конечно, если вопрос повторяется дважды - каждый раз нужно отвечать одно и то же). Так что требуется описать только стратегию противнику.

На конкретном ходе у нас есть какие-то компоненты связности (изначально точки). Есть несколько ситуаций, в зависимости от того, про какие рёбра был задан вопрос:



1. Вопрос задан про ребро между вершинами  $i$  и  $j$  внутри одной компоненты связности. В таком случае  $x_{ij} = 1$  (если эта переменная не спрашивалась ранее).
2. Вопрос задан про ребро между вершинами  $i$  и  $j$  из разных компонент связности. В таком, случае, если про все рёбра из  $C_k$  в  $C_l$  были даны ответы "нет"(0), то  $x_{ij} = 1$ , иначе  $x_{ij} = 0$ .

Предположим, что алгоритм не спрашивал про некоторое ребро  $x_{ij}$  и при этом выдал ответ. Чтобы прийти к противоречию, нужно найти два входа и со связным и не связным графом, в зависимости от того, какое ребро находится на месте  $x_{ij}$ .



Посмотрим на то, есть ли путь между вершинами  $i$  и  $j$  (это и нужно для связности). Во-первых, заметим, что при расширении компоненты связности (когда мы соединяем две), все ребра внутри компоненты связности нам известны (показывается индуктивно). Поэтому  $i$  и  $j$  не могли быть связаны путём (иначе они лежат в одной компоненте связности, но все рёбра внутри компоненты связности должны быть известны, а про  $x_{ij}$  информации нет). Значит  $i$  и  $j$  лежат в разных компонентах связности. Могут быть и другие компоненты, не содержащие  $i$  и  $j$ , но при этом не по построению не бывает, что между двумя компонентами рёбер нет совсем (тоже сохраняется индуктивно). Значит алгоритм просто не спросил про нужное ребро между этими компонентами. Поэтому если всех этих неспрошенных рёбер нет, то граф несвязен. А если они все есть - то он связан. Поэтому нельзя не спросить про какое-то ребро, иначе мы точно не можем определить, связан график или нет. Значит  $\binom{n}{2}$  вопросов необходимо. Понятно, что и в неадаптивном протоколе меньшее число вопросов нельзя было задать (неадаптивный только сложнее).

## 10 Лекция 22

(Андрей)

### 10.1 Булевы схемы

Вначале введем понятие булевых функций (отображений).

Булевые функции - это такие функции  $f$ , что они определены на множестве  $\{0, 1\}^n$  и принимают значения в множестве  $\{0, 1\}^k$ . То есть из  $n$  переменных мы получаем  $k$ -элементный вектор из 0 или 1.

Булева схема - последовательность булевых функций  $g_1, g_2, \dots, g_s : \{0, 1\}^n \rightarrow \{0, 1\}$ , где:

$$g_i = \begin{cases} h_j \cup h_k \\ h_j \cap h_k \\ \neg h_j \end{cases}$$

В свою очередь,  $h_j = \begin{cases} x_r, r = \{1, \dots, n\} \\ g_m, m < i \end{cases}$

Случай  $h_j = g_m, m < i$  означает, что мы можем пользоваться тем, что мы сконструировали ранее.

Размер схемы - количество функций  $g_i$ .

Сложность схемы - наименьший размер схемы, вычисляющей данную функцию.

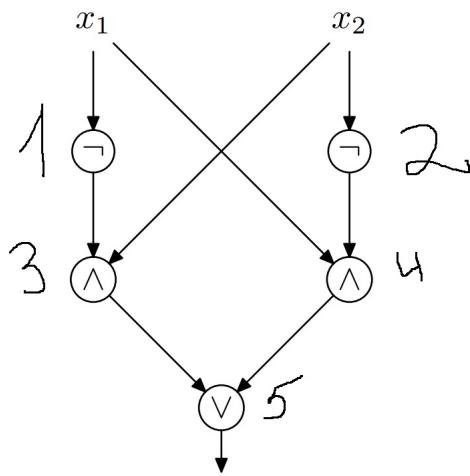
Говорят, что схема вычисляет функцию  $f$ , если  $\forall x \in \{0, 1\}^n f(x) = (g_{s-k+1}(x), g_{s-k+2}(x), \dots, g_s(x))$ . Обратим внимание, что т.к. исходная функция выдает ровно  $k$  чисел, то и на выходе мы получили именно  $k$  элементов нашей схемы, причем это будут последние  $k$  элементов. (ни один филолог не пострадал при прочтении этого предложения).

Также эти функции  $(g_{s-k+1}(x), g_{s-k+2}(x), \dots, g_s(x))$  называют выходами функции.

**Пример:**  $x_1, x_2$

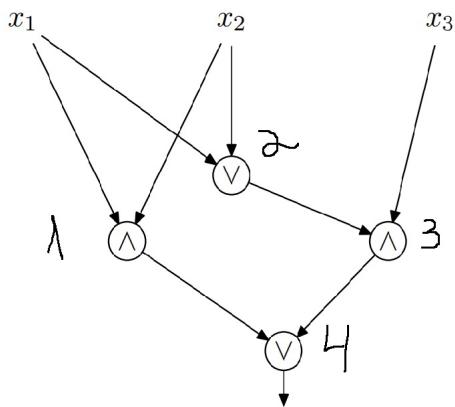
Проделаем следующие операции:  $\neg x_1, \neg x_2, \neg x_1 \wedge x_2, \neg x_2 \wedge x_1, (\neg x_1 \wedge x_2) \vee (\neg x_2 \wedge x_1)$ . Такая схема с одним выходом вычисляет  $x_1 \oplus x_2$ .

Иногда бывает полезно визуализировать булевые схемы в виде ориентированного графа:



Причем стоит отметить, что такой граф всегда будет ациклическим в силу топологической сортировки.

Приведем такую же визуализацию для функции  $MAJ_3$ :



## 10.2 Сложение двоичных чисел

Пусть нам даны две  $n$ -битовых двоичных записи чисел  $x$  и  $y$  и мы хотим вычислить двоичную запись их суммы  $z = x + y$ . Для удобства обозначим  $x = x_{n-1} \dots x_1 x_0$ , где  $x_0$  младший разряд двоичной записи. Аналогично,  $y = y_{n-1} \dots y_1 y_0$ . Во-первых, заметим, что в двоичной записи  $z$  будет не более  $n + 1$  разрядов. Так что мы хотим построить схему с  $2n$  входами и  $n + 1$  выходом.

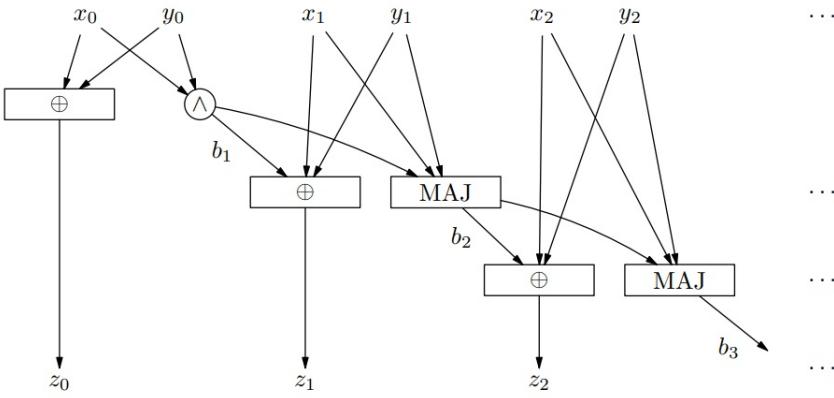
Идея конструкции схемы будет та же, что и в обычном школьном сложении в столбик. Мы будем складывать числа  $x$  и  $y$  поразрядно, попутно вычисляя биты переноса в следующий разряд.

Для удобства будем обозначать через  $b_i$  бит, который переносится в  $i$ -ый разряд из предыдущих.

Заметим, что мы уже готовы вычислить первый разряд ответа  $z_0 = x_0 \oplus y_0$ . Конечно, мы не можем сразу применить операцию  $\oplus$ , но выше мы показали, как её можно вычислить небольшой схемой. Добавим эту маленькую схему в нашу как подсхему. Далее, заметим, что  $b_1 = x_0 \wedge y_0$ , добавим соответствующий элемент в схему. Переидём к следующему разряду. Здесь  $z_1 = x_1 \oplus y_1 \oplus b_1$  и  $b_2 = MAJ_3(x_1, y_1, b_1)$ .

Для вычисления первого выражения добавим сначала подсхему, вычисляющую промежуточную величину  $c_1 = x_1 \oplus y_1$ , а затем подсхему, вычисляющую  $z_1 = c_1 \oplus b_1$ . Для вычисления  $b_2$  просто добавим подсхему, вычисляющую функцию  $MAJ_3$ . Такая схема также приведена выше. Дальше, случай произвольных  $z_i$  и  $b_i$  полностью аналогичен случаю  $z_1$  и  $b_1$  и мы можем последовательно вычислить все эти значения.

Приведем пример визуализации для сложения чисел:



Оценим теперь размер описанной схемы. Для каждого разряда ответа нам нужно не больше двух раз применить подсхему для вычисления функции  $\oplus$  и не более одного раза подсхему для вычисления  $MAJ_3$ . Все эти схемы имеют фиксированный размер, так что для вычисления каждого разряда  $z$  мы используем фиксированное число элементов, не зависящее от числа входных переменных. Поэтому всего в схеме  $O(n)$  элементов.

### 10.3 Вычисление произвольной функции

**Теорема:** Пусть имеется функция  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . Тогда такая функция может быть вычислена схемой размера  $O(n \cdot 2^n)$ .

**Доказательство:**

Мы знаем, что любая булева функция представляется в виде СДНФ:

$$f(x_1, x_2, \dots, x_n) = \bigvee_{\substack{\alpha_1, \alpha_2, \dots, \alpha_n \\ f(\alpha)=1}} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

Напомним:  $x^\alpha = \begin{cases} x, & \alpha = 1 \\ \neg x, & \alpha = 0 \end{cases}$

Понятно, что число дизъюнкций не превышает  $2^n$ , а число элементов в каждом из конъюнктов не превышает  $n$ . Таким образом, при вычислении функции на все дизъюнкции мы потратим не более  $2^n$  операций, а внутри каждого конъюнкта мы используем не более  $n + n - 1$  операции (может быть  $n$  отрицаний, и еще надо добавить  $n - 1$  конъюнкцию). Итого получили, что общее число операций не превысит  $2^n + 2^n(2n - 1) = 2n \cdot 2^n = O(n \cdot 2^n)$  операций.

**Теорема:** Для всякого  $n > 10$  существует функция  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , которую нельзя вычислить схемой размера меньше  $\frac{2^n}{10n}$ .

**Доказательство:**

Для доказательства применим мощностной метод: докажем, что функций больше, чем схем нужного размера. Тогда схем не хватит, чтобы вычислить все функции.

Понятно, что булевых функций от  $n$  переменных  $2^{2^n}$ .

Оценим количество схем размера  $S$  (в нашем случае  $S = \frac{2^n}{10n}$ ). Причем стоит отметить, что если мы вычислили функцию схемой размера меньше  $S$ , то мы можем добавить некоторое количество фиктивных переменных так, чтобы размер схемы стал равен  $S$ .

Посчитаем количество бит, необходимых для задания схемы. Теперь сделаем для себя некоторое удобство, чтобы было легче описать нашу схему, — а именно, выпишем все элементы схемы, включая переменные:

$$x_1, x_2, \dots, x_n, g_1, g_2, \dots, g_s$$

Теперь надо понять, как мы можем закодировать нашу последовательность. Для каждого элемента нам нужно сделать две вещи:

1. Указать два предыдущих элемента (в смысле из каких двух элементов был составлен данный).
2. Указать, какая операция была использована, чтобы получить данный элемент (конъюнкция, дизъюнкция или отрицание).

Для первого случая нам потребуется не более  $2 \cdot \log_2(n + S)$  бит (для каждого из двух предыдущих элементов потребуется не более  $\log_2(n + S)$  бит).

Далее, для второго случая нам достаточно 2 бит, чтобы указать какой тип операции был использован.

Итого для каждого из  $S$  элементов в схеме потребуется  $2(1 + \log_2(n + S))$  бит. Тогда для всей схемы получаем итоговый размер  $2S(1 + \log_2(n + S))$  бит. Сделаем оценку на полученное число:

$$2S(1 + \log_2(n + S)) \leq 2S \cdot (2 + \log_2 S) \leq 4S \cdot \log_2 S$$

При  $S = \frac{2^n}{10n}$  получаем:

$$4 \cdot \frac{2^n}{10n} \cdot (n - \log_2(10n)) \leq 2 \cdot \frac{2^n}{5}$$

Поэтому количество схем размера  $S$  не больше, чем количество таких строк, то есть не больше  $2^{2 \cdot \frac{2^n}{5}}$ , что меньше, чем кол-во всех булевых функций ( $2^{2^n}$ ), следовательно, не всякую функцию можно вычислить схемой размера  $S$ .

**Ч.Т.Д**

## 11 Лекция 23

(Илья)

### 11.1 Функция $XOR_n$

Мы знаем, что  $XOR_n = x_1 \oplus x_2 \oplus \dots \oplus x_n$

**Определение:** Схемная сложность функции - минимальное количество элементов в схеме, вычисляющей данную функцию.

Тогда давайте сформулируем теорему:

**Теорема:** Схемная сложность  $XOR_n \geq 2n - 1$

**Доказательство:**

- Доказательство будем вести по индукцией по  $n$ , однако хитрой индукцией. Сразу для функции  $XOR_n$  и её отрицания -  $\neg XOR_n$

Мы раньше говорили, что в схеме будем допускать только элементы  $\vee, \wedge, \neg$ , однако в этом доказательстве будем допускать схемы более общего характера, поэтому будем допускать, что элементами схемы могут быть:  $(h_i^a \wedge h_j^b)^c$

Тут имеется в виду, что  $x^a = \begin{cases} x, & \text{если } a = 1 \\ \neg x, & \text{если } a = 0 \end{cases}$

Что такое  $h_i$  и  $h_j$ ?

Ну вот раньше у нас были функции  $g_1, g_2, \dots, g_s$ , такие что  $g_k = \begin{bmatrix} \neg h_i \\ h_i \wedge h_j \\ h_i \vee h_i \end{bmatrix}$ , где  $h_p$  - это или предыдущий элемент или переменная, которая встречалась раньше.

Теперь же мы просто рассматриваем более общие элементы.

**Примеры:**

- $a = b = c = 1$ , тогда получаем  $h_i \wedge h_j$
- $a = b = c = 0$ , тогда получаем  $h_i \vee h_j$
- $i = j$  и  $a = b = 1$ , тогда получим или  $h_i$ , или  $\neg h_i$  в зависимости от того, чему равно  $c$
- $i = j$  и  $a = 0, b = 1$ , тогда мы получаем или 0, или 1

Отсюда видно, что размер новой схемы будет точно не меньше размера новой схемы, потому что элементы старой схемы включены в элементы новой схемы, что мы и показали в примерах, однако в новой схеме мы можем получать и другие элементы другими комбинациями  $a, b, c$ .

- Теперь запускаем индукцию.

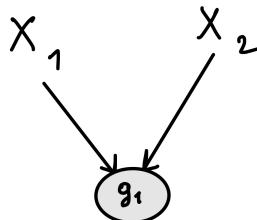
**База:**  $n = 1$  и получим, что нам будет необходимо для  $XOR_1 = x_1$  минимум 1 элемента в схеме. Ну это правда, потому что нам нужен какой-то выход в схеме (тут, конечно, вопрос с обозначениями, но мы выход из схемы в данном случае считаем за элемент).

**Переход:**  $n - 1 \rightarrow n$

Рассмотрим "новую" схему минимального размера, которая имеет строго меньше, чем  $2n - 1$  элемента, которая вычисляет  $XOR_n$  или  $\neg XOR_n$ .

У нас есть  $n$  переменных  $x_1, x_2, \dots, x_n$  и вот в этой схеме наши элементы как-то устроены, пусть это  $g_1, g_2, \dots, g_s = (XOR_n)^\alpha$

Берём первый элемент  $g_1$ , понятно, что в первый элемент мы подставляли две переменные или одну переменную. Не умоляя общности давайте обозначим эти переменные за  $x_1$  и  $x_2$ , тогда имеем, что



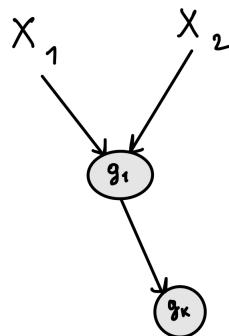
**Замечание:**  $(x_i^a \wedge x_j^b)^c \neq x_i \oplus x_j$  ни при каких  $a, b, c$ , потому что  $\oplus$  принимает две единицы и два нуля, а та конъюнкция истинна только на одном наборе  $(x_i, x_j)$

Это замечание просто к тому, чтобы было понятно, что мы не сможем на первом шаге вычислить  $XOR_2$ , то есть  $g_1 \neq XOR_2$ .

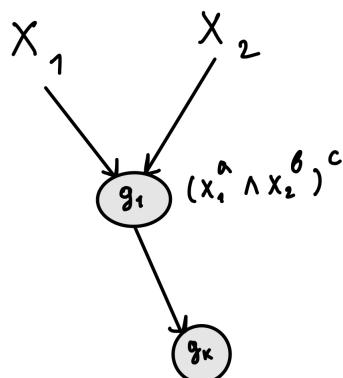
Значит, элемент  $g_1$  участвовал в дальнейшей реализации нашей схемы, то есть он поступал в какой-то элемент  $g_k$ . (может быть в несколько поступал, но вот мы конкретное место выберем и посмотрим туда)

Почему? Ну если это не так, то он не помогал вычислять  $XOR_n$ , а значит бы не нужный этой схеме, поэтому мы бы его выкинули и получили бы схему меньшего размера, но по условию схема была минимального размера.

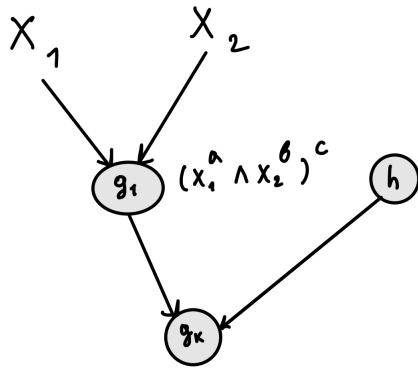
Значит, имеем вот, что



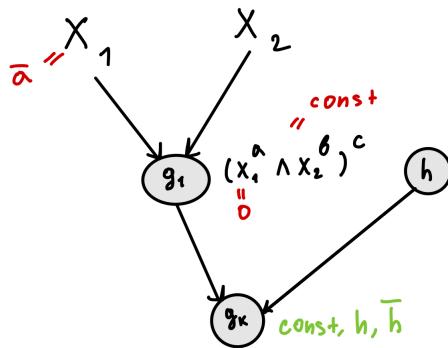
Давайте подпишем, что такое  $g_1$ .



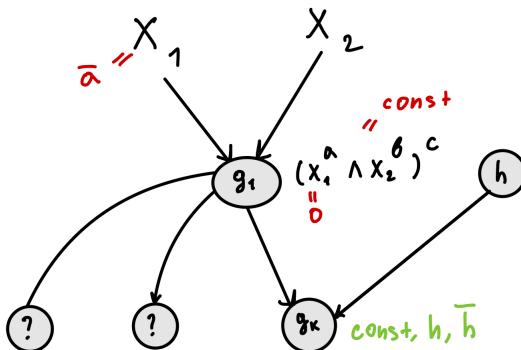
А  $g_k$  - это тоже элемент которому на вход что-то приходило, одна из частей входа - это  $g_1$ , а вторая пусть будет  $h$ .



Давайте теперь поменяем вход и подставим вместо  $x_1 - \neg a$  и получим, что  $g_1 = ((\neg a)^a \wedge x_2^b)^c = (0 \wedge x_2^b)^c = 0^c$ . То есть мы получили, что  $g_1$  стал константой. Тогда что можно сказать про  $g_k$ ? Ну на самом деле так как там стоит  $(g_1^a \wedge h^b)^c$ , а  $g_1$  - это или 0 или 1, то получаем, что в  $g_k$  может стоять или константа, или  $\neg h$ , или  $h$



Ну от  $g_1$  вероятно мог подаваться не только на  $g_k$ , но и в какие-то другие элементы, изобразим их.



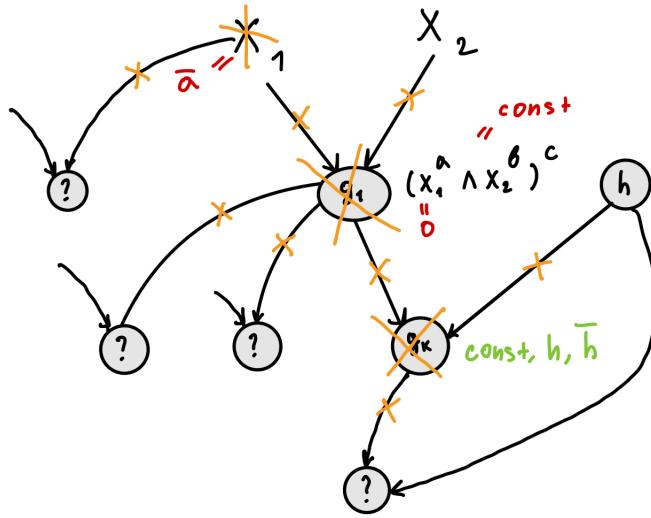
Теперь мы делаем следующее. Мы удаляем из схемы  $g_1, g_k, x_1$ .

Что произошло с функцией после всех предыдущих манипуляций? Ну после подстановки в  $XOR_n$  вместо одной из переменных константы мы получаем или  $XOR_{n-1}$  или  $\neg XOR_{n-1}$ . Почему? Ну просто из-за того, что  $1 \oplus x_1 \oplus x_2 = \neg(x_1 \oplus x_2)$  и  $0 \oplus x_1 \oplus x_2 = x_1 \oplus x_2$

Однако теперь схема может стать не совсем корректной, поэтому нам надо поправить график, который получился, чтобы он стал настоящей схемой

Какая у нас есть проблема? У нас  $g_k, g_1, x_1$  кому-то могли подаваться на вход.

Но на самом деле проблемы нет, потому что мы можем просто заметить, что так как  $x_1$  и  $g_1$  стали константами, то мы можем, если они поступали куда-то, просто оставить второй вход, который шёл к этим элементам. А что касается  $g_k$ , то так как он что-то из  $const, h, \neg h$ , то можем направить, если он куда-то поступал, в его входной элемент просто  $h$ , потому что за счёт второго входа мы сможем использовать как раз  $const, h, \neg h$ .



Ну тут есть ещё небольшой нюансик с тем, что, кто нам сказал, что  $h$  - это функция, ведь это может быть переменной. Но на самом деле это не проблема, а вот что если у нас  $h$  был равен  $g_1$  или  $x_1$ , например? Ну тогда раз это у нас константы, то по-прежнему всё хорошо, а если он был равен  $g_k$ , то у же было сказано, что делать - надо заменять просто на  $h$ .

Итого, мы получили корректную схему, вычисляющую  $XOR_{n-1}$  или  $\neg XOR_{n-1}$  размера  $< 2n-3$ , но по предположению индукции у нас схема была размера  $\geq 2n-3$  - противоречие!

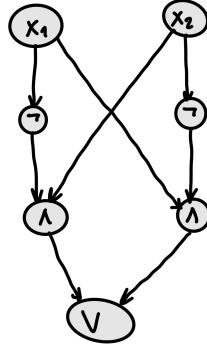
Значит схемная сложность  $XOR_n \geq 2n-1$

### Ч.Т.Д.

То, что мы сейчас доказали - это доказали нижнюю оценку.

Однако очень просто можно показать верхнюю оценку.

Заметим, что для выражения  $XOR_2$  нам понадобится 5 операций



А для  $XOR_3$  нам понадобится ещё 5 операций, ну и тд, поэтому понятно, что верхняя оценка на сложность схемы  $XOR_n$  - это  $5(n-1)$

## 11.2 Глубина схемы

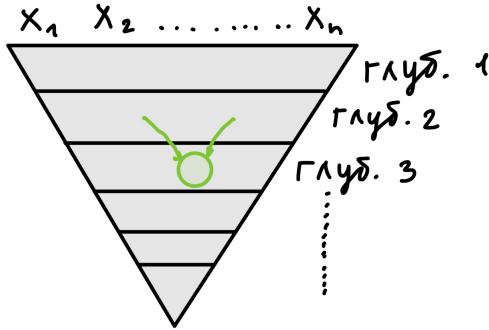
**Определение:** Глубина элемента  $g_i$  в нашей схеме - это длина наибольшего пути от переменной к  $g_i$ .

Глубина всей схемы - это максимальная из глубин элементов.

Например, глубина схемы для  $XOR_2$ , приведённой чуть выше равна 3.

Теперь представьте себе, что у вас есть булева схема и вы можете разбить элементы по глубине, как бы по уровням.

Ну и в элемент, скажем, глубины 3 могут вести стрелки только из элементов меньшей глубины. Ну иначе у него глубина была бы больше, чем 3.



**Пример:**

- Давайте вычислим глубину дизъюнкции.  $x_1 \vee x_2 \vee \dots \vee x_n$

Это можно сделать последовательно и получить глубину  $O(n)$

А можно сделать не так и разбить их на пары и получить меньшую длину, то если как бы по двоичному дереву. Получим глубину  $O(\log_2(n))$

- Давайте посчитаем пример, связанный с функцией  $CONN : \{0,1\}^{\binom{n}{2}} \rightarrow \{0,1\}$

Хочется, понять, как можно просто построить схему, которая её вычисляет и при этом может быть сэкономить на глубине и понять какой тут размер в теории возможен.

Мы вводим, так называемую модифицированную матрицу смежности:

Мы берём граф  $G$  и рассматриваем матрицу  $A(G)$  - это матрица  $n$  на  $n$ , состоит из элементов

$$a_{ij} = \begin{cases} 1, & \text{если вершины } v_i \text{ и } v_j \text{ соединены ребром и } i \neq j \\ 0, & \text{если вершины } v_i \text{ и } v_j \text{ не соединены ребром и } i \neq j \\ 1, & \text{если } i = j \end{cases}$$

У матрицы смежности по диагонали обычно стоят нули, но мы поставим единицы, потому что единицы будут соответствовать петлям. И мы понимаем, чтобы проверить, связан ли граф, надо просто понять, есть ли путь просто вершины  $u$  в  $v$  какой-то длины и длину эту можно ограничить числом вершин, то есть длина должна быть не больше, чем  $n - 1$ . Но за счёт того, что у нас есть петли мы сможем найти путь длины ровно  $n - 1$ . И вот эта информация как раз и хранится в степенях матрицы  $A(G)$

**Утверждение:** Матрица  $A^k$  на позиции  $a_{ij}$  содержит количество путей длины  $k$  из  $v_i$  в  $v_j$ .

**Доказательство:**

1. Будем вести индукцию по  $k$ .

**База:**  $k = 1$  - очевидно.

**Переход:**  $k - 1 \rightarrow k$ .

$$A^k = A^{k-1} \cdot A, \text{ а } a_{ij}^{(k)} = \sum_{t=1}^n a_{it}^{(k-1)} \cdot a_{tj}$$

Однако посмотрим на то, что написано с комбинаторной точки зрения. Вот у нас есть вершины  $v_i, v_t, v_j$  и мы хотим посчитать количество путей длины  $k$  из  $v_i$  в  $v_j$ . Для этого мы проведём одно ребро, если оно есть из  $v_j$  в  $v_t$  и будем считать количество путей длины  $k - 1$  из  $v_i$  в  $v_t$ . Как раз тогда  $a_{tj}$  будет отвечать за наличие ребра между  $v_t$  и  $v_j$  и тогда мы просто суммируем по всем таким вершинам  $v_t$ , а это ровно то, что у нас и написано.

### Ч.Т.Д.

Ну и при построении схемы возникает потребность в подсчёте  $A^{n-1}$ . Чтобы это сделать, давайте будем возводить матрицу в степень  $n - 1$  в булевом смысле, то есть сложение заменим на  $\vee$ , а умножение на  $\wedge$ .

Тогда конкретно формула матричного произведения принимает вид:  $(A \cdot B)_{(ij)} = \bigvee_{t=1}^n A_{(i,t)} \wedge B_{(t,j)}$

Однако теперь,

$$A_{(i,k)}^k = \begin{cases} 1, & \text{если } \exists \text{ путь длины } k \text{ из } v_i \text{ в } v_j \\ \text{иначе} & \end{cases}$$

Поэтому теперь нам достаточно возвести матрицу в  $n - 1$  степень и проверить, что она состоит из всех единиц.

Ну на самом деле удобно вычислять степень не  $n - 1$ , а  $2^m (2^m \geq n) \Rightarrow m = \lceil \log_2(n) \rceil$ )

какую-то, для быстрого возвведения в степень.

Ну и тогда получаем, что на каждом шаге мы будем возводить матрицу в квадрат. Это занимает порядка  $n^3$  действий, ну и таких шагов будет  $m$  штук, поэтому схема будет размера порядка  $O(n^3 \log_2(n))$  Ну там ещё надо будет взять конъюнкцию по всем  $n^2$  элементам матрицы, чтобы проверить, что там все единички, ну это ещё  $n^2$  действий, но сложность это не поменяет.

А вот , что касается глубины, то мы делаем  $m$  операций и каждую матрицу мы вычисляем дизьюнкцией и глубина там  $\log_2(n)$ (было обсуждено в первом примере), поэтому глубина здесь  $O(\log_2^2(n))$ , ну на самом деле там ещё нужно из-за конъюнкции  $\log_2(n^2)$ , итого выйдет  $O(\log_2^2(n) + \log_2(n^2)) = O(\log_2^2(n))$ .

Здесь можно немножечко сэкономить в размере и посчитать не за  $n^3 \log_2(n)$ , а за  $n^3$ , потому что на самом деле нам не нужна информация про всю матрицу, а нужна информация только про её первый столбец, потому что если из первой вершины достижимы все другие, то это уже означает, что граф связан.

То есть должно быть выполнено вот такое:

$$A^{n(\geq n-1)} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

•

Умножение здесь подразумевается булево.

Теперь мы можем вычислять с конца:

$$\left( A \dots \left( A \left( A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right) \right) \dots \right)$$

Теперь умножение матрицы на столбец занимает  $n^2$  операций, ну и делаем так  $n$  раз и получим порядка  $n^3$  операций. То есть размер - это  $O(n^3)$

А глубиной мы теперь пожертвовали и теперь она равна  $O(n \log_2(n))$

### 11.3 Формулы

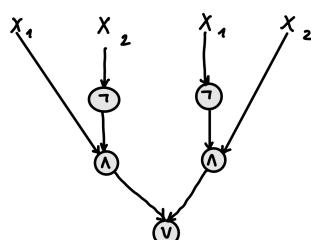
- $x_i$  - это формула
- $\Phi$  - формула, то и  $\neg\Phi$  тоже
- $\Phi_1, \Phi_2$  - формулы, то и  $\Phi_1 \wedge \Phi_2$  и  $\Phi_1 \vee \Phi_2$  тоже формулы

Ну и теперь за конечное число шагов можно получить любую формулу.

**Пример:**

Формула для  $XOR_2 = \neg x_1 \wedge x_2 \vee \neg x_2 \wedge x_1$

Формулу тоже можно рисовать как график, тогда получим, что



Чем этот граф отличается от булевой схемы?

Ну на самом деле исходящие степени всех вершин равны 1, ведь в булевой схеме это может быть не так, даже на примере  $XOR_2$  (чуть выше была картинка).

Поэтому формула - это частный случай булевой схемы, она тоже имеет глубину и размер. Между ними имеется связь и оказывается, что любую схему можно переделать в формулу.

**Утверждение:** Для любой схемы  $C$  от переменных  $x_1, x_2, \dots, x_n$  размера  $s$  и глубины  $d$  существует эквивалентная ей формула размера не больше, чем  $2^s - 1$  и глубины не больше, чем  $d$ .

**Доказательство:**

1. Доказательство можно вести индукцией по  $d$  и по  $s$  одновременно, можно и по их сумме, но возьмём на примере  $s$ .

Итого, индукция по  $s$ .

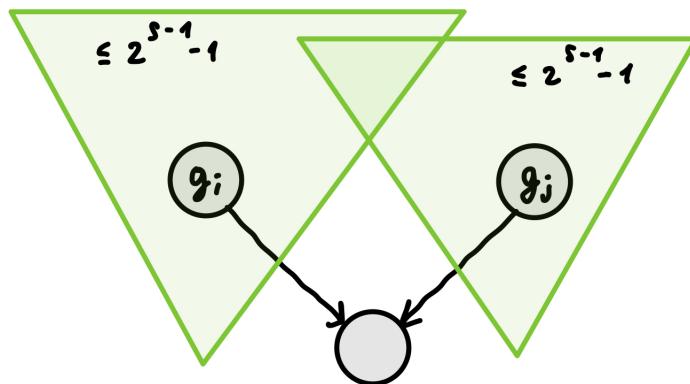
**База:**  $s = 1$  - очевидно.

**Переход:**  $s - 1 \rightarrow s$ .

Рассмотрим теперь промежуточный случай, когда два элемента подаются на вход другому элементу.

То есть пусть на вход подаются два элемента -  $g_i$  и  $g_j$ .

Ну и рассмотрим схемы, которые были ранее.



Ну и тогда суммарный размер формулы не превосходит  $(2^{s-1} - 1) \cdot 2 + 1 = 2^s - 1$

Аналогично, с глубиной, она не превышала у  $g_i$  и  $g_j$   $d-1$ , тогда суммарная глубина не превышала  $d - 1 + 1 = d$ .

**Ч.Т.Д.**

**Следствие:** Схема глубины  $d$  допускает эквивалентную реализацию тоже глубины  $d$  и размера не больше, чем  $2^d$ .

**Доказательство:**

1. Переделываем её в формулу и получаем дерево, не обязательно полным двоичным деревом. Поэтому глубина у нашего дерева  $d$ , а листьев(то есть операций) у этого дерева не больше, чем  $2^d$ .

**Ч.Т.Д.**

## 11.4 Задачи выполнимости

Их бывает несколько вариаций:

1. Для схем.

Нам даётся схема  $C$  на вход и спрашивают, существует ли  $x$ , такой, что  $C(x) = 1$ ,  $x = (x_1, x_2, \dots, x_n)$

2. КНФ - конъюнкция элементарных дизъюнктов.

Есть некая КНФ  $K$  и спрашивают, существует ли такой  $x$ , что  $K(x) = 1$ .

3. 3-КНФ - частный случай КНФ, где каждый дизъюнкт имеет не более трёх переменных.

Например,  $(x_1 \vee x_2 \vee \neg x_3) \wedge (x_1 \vee x_2) \wedge (\neg x_5)$

Почему эти задачи так важны? Ну на самом деле, если мы умеем отвечать на вопрос про КНФ-3, то тогда мы сможем эффективно свести к задаче КНФ. Эффективно значит свести полиномиально. Аналогично с вопросами про схему.

## 12 Лекция 24

(Никита)

### 12.1 Задача выполнимости

Давайте напомним, какие типы задач выполнимости мы рассматриваем:

- Схема  $C(x)$

$$\exists x \in \{0, 1\}^n : C(x) = 1?$$

- КНФ  $K(x)$

$\exists x \in \{0, 1\}^n : K(x) = 1?$  Напомним, что  $K(x) = D_1 \wedge D_2 \wedge \dots \wedge D_r$ , где  $D = x_1^{\alpha_1} \vee x_2^{\alpha_2} \vee \dots \vee x_s^{\alpha_s}$ . Факт для расширения развития терминологии:  $x, \neg x$  называют *литералами*.

- 3-КНФ: КНФ, в которой каждый  $D_j$  содержит  $\leq 3$  литералов.

$$\exists x \in \{0, 1\}^n : K(x) = 1?$$

Отметим, что каждая функция имеет КНФ (подумайте, это напрямую следует из существования СДНФ и закона Де Моргана).

Мы хотим подавать некоторой программе (solver для 3-КНФ) некоторый вход и хотим получить ответ на задачу выполнимости. На вход подаём нашу задачу и хотим, чтобы за полиномиальное время (например, от размера схемы, которая подаётся) наша задача сводилась к 3-КНФ.

*Упражнение.* Не любая схема обладает 3-КНФ (подумайте, почему!). Один из таких примеров:  $XOR$  некоторого большого числа переменных.

Что же тогда делать для таких функций? Для них мы построим некоторую другую функцию (например, добавляя переменные) так, чтобы она была выполнима тогда и только тогда, когда выполнима исходная.

Свести КНФ к схеме несложно - просто пошагово построить схему. 3-КНФ вообще к КНФ сводить не нужно - это её частный случай. Трудность вызывает лишь сведение схемы к задаче выполнимости 3-КНФ. Сведение за полиномиальное время называют *эффективным*.

**Теорема.** Задача выполнимости для схемы эффективно сводится к задаче выполнимости 3-КНФ.

**Доказательство:**

Введём переменные  $x_1, x_2, \dots, x_n$ , а еще добавим к ним  $g_1, g_2, \dots, g_s$  (которые у нас соответствуют элементам схемы). Тогда:

$$"g_i = \neg h_j" \Leftrightarrow (g_i \vee h_j) \wedge (\neg g_i \vee \neg h_j)$$

$$"g_i = h_k \vee h_l" \Leftrightarrow (h_k \vee h_l \vee \neg g_i) \wedge (\neg h_k \vee g_i) \wedge (\neg h_l \vee g_i)$$

$$"g_i = h_k \wedge h_l" \Leftrightarrow (\neg h_k \vee \neg h_l \vee g_i) \wedge (h_k \vee \neg g_i) \wedge (h_l \vee \neg g_i)$$

Для каждого  $g_i$  выписываем эквивалентную формулу и тогда 3-КНФ получается конъюнкцией всех этих выражений для  $g_1, \dots, g_s + \wedge(g_s)$

Тогда  $\exists \vec{x} : C(\vec{x}) \Leftrightarrow \exists \vec{x}, \vec{g} : K(\vec{x}, \vec{g}) = 1$ .

Теперь осталось показать, почему собственно эти задачи будут действительно эквивалентны:

$\Rightarrow$  В эту сторону почти очевидно. Если схема выполнима, существует набор переменных, при котором  $g_s = 1$ . Тогда просто вычислим  $g_1, \dots, g_s$ , подставив переменные из данного набора и из построения 3-КНФ видно, что итоговая конъюнкция будет равна 1.

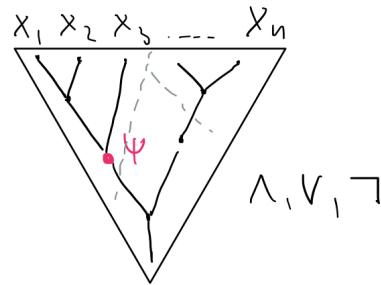
$\Leftarrow$  В эту сторону тоже почти очевидно, но формально тут индукция по номеру элемента схемы. Отметим, что набор  $\vec{x}$  фиксирован. Нужно показать, что набор  $\vec{g}$  в КНФ соответствует значениям  $g_i$  в схеме. КНФ выполнима, т.е. каждый её конъюнкт равен 1. Посмотрим, например, на переменную  $g_1$ : из того, как мы кодировали выражение для соответствующего ей элемента схемы, следует, что конъюнкт равен 1, если  $g_1$  принимает верное значение равное значению операции над теми иксами, на которые ссылается. Это в точности и значит, что  $g_1$  равно значению в схеме. Индуктивно показываем для всех остальные переменных  $g_i$ . Тогда при условии, что  $g_s = 1$  получаем, что схема выполнима (прочувствуйте это).

Каждый элемент даёт константное число дизъюнктов (а в каждом не более 5 операций), поэтому сведение осуществляется за линейное время  $\leq 15s$ , где  $s$  - размер схемы, это  $O(n)$ .

## 12.2 Теорема о балансировке булевых функций

**Теорема (о балансировке).** Для формулы размера  $s$  существует формула глубины, не превышающей глубины  $\leq 1 + 4 \log_2 s$

**Доказательство:**

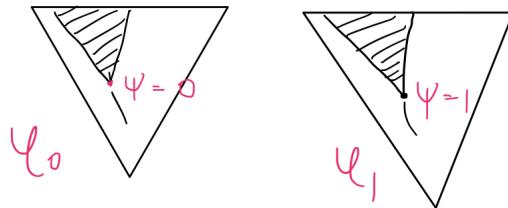


Формула представима в виде дерева (см. рисунок). Можно рассматривать подформулы (которые соответственно являются поддеревьями).

**Лемма.**  $\exists \psi$ : подформула с корнем  $\psi$  имеет размер  $\geq \frac{s}{2}$ , а в свою очередь любая её подформула имеет размер  $< \frac{s}{2}$ .

**Доказательство леммы:**

Доказательство этого утверждения совсем простое. Достаточно начать из выходного элемента и спускаться по ребрам формулы в подформулы так, чтобы каждый раз оставаться в подформуле размера  $\leq \frac{s}{2}$ . В выходном элементе размер подформулы равен  $s$ , а в переменных размер подформулы равен 0, так что в какой-то момент мы не сможем спуститься из очередной вершины в подформулу. Это как раз и будет означать, что у текущей подформулы размер не меньше  $\frac{s}{2}$ , а во всех ее подформулах уже меньше ■

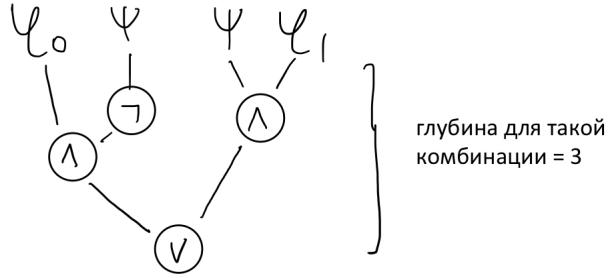


Вернёмся к док-ву самой теоремы. Воспользуемся индукцией по  $s$ . База очевидна верна для малых значений  $s$ . Будем действовать полной индукцией: для любой формулы размера меньше чем  $s$  утверждение верно. Находим  $\psi$  с соответствующим свойством по лемме. Важно, что каждый элемент в формуле используется один раз. Тогда сотрём все элементы в формуле кроме самой  $\psi$ . Создадим две новые формулы. В одной формуле зададим  $\psi$  константой 0, это будет  $\varphi_0$ . Аналогично в  $\varphi_1$  зададим  $\psi$  константой 1.

Описанная конструкция не соответствует нашим определениям: мы не разрешали использовать константы вместо переменных. Однако отрицание константы - константа, конъюнкция с 0 - то 0, с 1 - это второй аргумент конъюнкции. Аналогично дизъюнкция с 1 - это 1, с 0 - это второй аргумент дизъюнкции.

Пользуясь этими соображениями, в схеме с константами можно удалить лишние элементы. Ни размер схемы, ни глубина при таком удалении не увеличиваются. Тогда таким образом избавляясь от констант, какие-то константы могут спускаться ниже и в итоге получится формула без констант (или собственно константа, но это мы потом решим).

Рассмотрим тогда новую формулу  $\alpha = (\varphi_0 \wedge \neg\psi) \vee (\varphi_1 \wedge \psi)$ . Размер  $\psi \geq \frac{s}{2}$ , размер  $\varphi_0$  и  $\varphi_1 < \frac{s}{2}$ , поэтому, применяя к ним предположение индукции, получаем, что для каждого из  $\varphi_0$  и  $\varphi_1$  существует формула глубиной  $\leq 4 \log_2 \frac{s}{2} + 1 = 4(\log_2 s - 1) + 1 = 4 \log_2 s - 3$ . Для того чтобы получить  $\psi$  нужно получить две подформулы  $\psi$  (потратив на это 1 глубины), причём для каждой подформулы  $\psi$  тоже верно предположение индукции. На этом шаге глубина уже  $\leq 4 \log_2 s - 3 + 1 = 4 \log_2 s - 2$ . И у общей формулы  $\alpha$  глубина  $\leq 4 \log_2 s - 2 + 3 = 4 \log_2 s + 1$  ■



## 13 Семинар 16

(Никита)

### 13.1 Задача 1

Для начала зафиксируем утверждение из Лекции 15:

**Утверждение.**  $\chi_{G-uv}(x) = \chi_G(x) + \chi_{G\cdot uv}(x)$ , если  $\{u, v\} \in E(G)$ .

По условию  $G = C_n$ . Отсюда легко выражается, что  $\chi_{C_n}(x) = \chi_{C_n-uv}(x) - \chi_{C_n\cdot uv}(x)$ , где  $\chi_{C_n\cdot uv}$  на самом деле хроматический многочлен для простого цикла на  $n-1$ -й вершине, а  $\chi_{C_n-uv}(x)$  - хроматический многочлен для дерева, который мы научились считать в Лекции 15 (см. примеры оттуда). Поэтому можно просто доказать по индукции следующую формулу, полученную методом пристального взгляда:

$$\chi_{C_n}(x) = (x-1)^n + (-1)^n(x-1)$$

**Доказательство:**

**База.** Легко можно убедиться руками, что  $C_3 = x(x-1)(x-2)$ . По предположению  $C_3 = (x-1)^3 + (-1)^3(x-1) = (x-1)^3 - (x-1) = (x-1)(x^2 - 2x + 1 - 1) = x(x-1)(x-2)$ . База верна.

**Переход.** Мы знаем, что  $\chi_{C_n}(x) = (x-1)^n + (-1)^n(x-1)$ , нужно показать, что  $\chi_{C_{n+1}}(x) = (x-1)^{n+1} + (-1)^{n+1}(x-1)$ .

По утверждению выше  $\chi_{C_{n+1}}(x) = \chi_{C_{n+1}-uv}(x) - \chi_{C_{n+1}\cdot uv}(x) = x(x-1)^n - \chi_{C_n}(x) = x(x-1)^n - (x-1)^n - (-1)^n(x-1) = (x-1)^n(x-1) + (-1)^{n+1}(x-1) = (x-1)^{n+1} + (-1)^{n+1}(x-1)$  ■

**Ответ:**  $\chi_{C_n}(x) = (x-1)^n + (-1)^n(x-1)$

### 13.2 Задача 2

$\chi_G(x) = x(x-1)^{n-1}$ . Можем заметить, что после раскрытия скобок коэффициент при  $x^{n-1}$  будет равен  $-1 \cdot \binom{n-1}{1} = -(n-1)$ , т.е.  $|E(G)| = n-1$ , а младшая степень равна 1, значит в графе 1 компонента связности ( $G$  - связан). В сумме эти два замечания дают одно из эквивалентных определений дерева.

**Ответ:** Да, всегда

### 13.3 Задача 3

Введем вспомогательную случайную величину (индикаторную функцию)  $I_k = \begin{cases} 1, & \text{если } k\text{-ый элемент лежит в } S_p \\ 0, & \text{иначе} \end{cases}$

Теперь определим случайную величину так:  $I = \sum_{k=1}^n I_k$ .

$$\text{Тогда } E[I] = \sum_{k=1}^n E[I_k] = \sum_{k=1}^n 1 \cdot p = np.$$

**Ответ:**  $np$

### 13.4 Задача 4

а) Обозначим суммарное количество единиц подмножества  $S$ . Для каждой двоичной строки  $w$  обозначим через  $S_w$  случайную величину, которая равна  $|w|$ , т.е. количеству 1 в строке  $w$ , если эта строка попала в случайное множество, и 0 в противном случае. Тогда  $S = \sum_w S_w$ . Поскольку все подмножества равновероятны, вероятность для каждого попасть в случайное множество равна  $\frac{1}{2}$  (одинаково количество тех подмножеств, которые содержат  $w$ , и тех, которые не содержат). Поэтому математическое ожидание  $S_w$  равно  $E[S_w] = \frac{1}{2} \cdot |w| + \frac{1}{2} \cdot 0 = \frac{|w|}{2}$

Значит,  $E[S]$  равно общему количеству единиц в двоичных строках длины  $n$ , делённому на 2. В каждом разряде во всех строках вместе ровно  $2^{n-1}$  единиц (нулей и единиц в каждом разряде поровну). Поэтому общее количество единиц равно  $n2^{n-1}$ , откуда получаем  $E[S] = n2^{n-2}$ .

**Ответ:**  $n2^{n-2}$

б) Рассматриваем аналогичные случайные величины  $S$  и  $S_w$  как в п. (а). Но теперь у нас пространство состоит из подмножеств мощности  $k$ . Какова вероятность события «строка  $w$  попала в случайное  $k$ -элементное подмножество строк  $X$ »? Всего  $k$ -элементных подмножеств строк  $\binom{2^n}{k}$ . Из них  $\binom{2^n-1}{k-1}$  содержат данную строку  $w$ . Вероятность равна отношению этих двух чисел.

$$\text{Получаем } E[S_w] = |w| \frac{\binom{2^n-1}{k-1}}{\binom{2^n}{k}} = \frac{|w|k}{2^n}.$$

Отсюда, пользуясь вычислениями из п. (а), находим ответ:

$$E[S] = \sum_w E[S_w] = \frac{k}{2^n} \sum_w |w| = \frac{k}{2^n} \cdot n2^{n-1} = \frac{kn}{2}.$$

**Ответ:**  $\frac{kn}{2}$

### 13.5 Задача 5

По определению математического ожидания:  $E[X] = \sum_{i=1}^n x_i \cdot P(x_i)$ . Давайте разобьём эту сумму на 3 суммы по разным значениям  $x_i$ .

$$\text{Итак, } E[X] = \sum_{i:x_i < 3}^n x_i \cdot P(x_i) + \sum_{i:x_i \geq 3 \& x_i < 6}^n x_i \cdot P(x_i) + \sum_{i:x_i \geq 6}^n x_i \cdot P(x_i).$$

Давайте посчитаем каждую из вероятностей в этих трёх суммах. По условию,  $P(x_i) = \frac{1}{3}|x_i| < 3$ ,  $P(x_i) = \frac{1}{6}|x_i| \geq 6$ , а значит  $P(x_i) = 1 - \frac{1}{3} - \frac{1}{6} = \frac{1}{2}|3 \leq x_i < 6|$ .

Теперь давайте с учётом этого оценим снизу каждую из этих сумм.  $\sum_{i:x_i < 3}^n x_i \cdot P(x_i) \geq 0$ , так как по условию  $x_i \geq 0$ ,  $\sum_{i:x_i \geq 3 \& x_i < 6}^n x_i \cdot P(x_i) \geq 3 \cdot \frac{1}{2} = 1.5$  и  $\sum_{i:x_i \geq 6}^n x_i \cdot P(x_i) \geq 6 \cdot \frac{1}{6} = 1$ . Тогда  $E[X] \geq 1 + 1.5 + 0 = 2.5$ . Получена нижняя оценка.

Давайте покажем, что она достигается. Пусть наша величина принимает значение 0 с вероятностью  $\frac{1}{3}$ , значение 6 с вероятностью  $\frac{1}{6}$  и 3 с вероятностью  $\frac{1}{2}$ , тогда как раз-таки и получится 2.5.

Для получения оценки сверху давайте положим, что наша случайная величина принимает значение  $m \geq 6$  при  $x_i \geq 6$  и всё остальное так же, как и в предыдущем примере, тогда наше мат. ожидание можно записать вот так  $E[X] = 1.5 + \frac{m}{6}$ . Понятно, что я могу подобрать любое, сколь угодно большое число  $m$ , поэтому верхняя оценка на наше мат. ожидание - это  $+\infty$ .

**Ответ:**  $[2.5, +\infty)$

### 13.6 Задача 6

Пусть  $p$  - доля работ студента, оценка за которые меньше 4. Максимальная оценка, которую он мог получить за все работы гарантированно не меньше средней (здесь используется идея похожая на ту, что была в доказательстве леммы для общего случая вероятностного метода, см. лекцию 16). Запишем неравенство:

$$3p + 10(1-p) \geq 6$$

$$3p + 10 - 10p \geq 6$$

$$4 \geq 7p$$

$$p \leq \frac{4}{7} \blacksquare$$

### 13.7 Задача 7

Для удобства будем обозначать  $E[X]$  как  $EX$ .

Воспользуемся неравенством Чебышева:  $P(|x - EX| \geq \alpha) \leq \frac{DX}{\alpha^2}$ .

Случайная величина  $X = \sum_{i=1}^n I_i$ , где  $I_i = \begin{cases} 1, & \text{если } i\text{-ый элемент строки - единица} \\ 0, & \text{иначе} \end{cases}$

$$EX = \frac{n}{2}, DX = EX^2 - (EX)^2$$

$$EX^2 = E\left(\sum_{i=1}^n I_i\right)^2 = E\left(\sum_{i=1}^n I_i^2 + \sum_{i \neq j} I_i I_j\right) = \frac{n}{2} + \frac{n(n-1)}{4}.$$

Выше мы использовали, то что  $I^2$  на самом деле равно  $I$ , поэтому  $E\left(\sum_{i=1}^n I_i^2\right) = E\left(\sum_{i=1}^n I_i\right) = EX = \frac{n}{2}$ , а так же то, что выражение  $I_i I_j$  равно 1 ровно в том, случае, когда обе индикаторных функции равны 1, вероятность чего равна  $\frac{1}{4}$ .

Следовательно,  $E\left(\sum_{i \neq j} I_i I_j\right) = n(n-1) \cdot \frac{1}{4} = \frac{n(n-1)}{4}$  (Отметим, что  $n(n-1)$  - количество мономов  $I_i I_j$ , где  $i \neq j$ ).

Тогда  $DX = EX^2 - (EX)^2 = \frac{n}{2} + \frac{n(n-1)}{4} - \left(\frac{n}{2}\right)^2 = \frac{n}{4}$ , и тогда  $P(\dots) \leq \frac{n}{4(\sqrt{n})^2} = \frac{1}{4}$  ■

### 13.8 Задача 8

Будем рассматривать случайно выбранную перестановку из множества всех перестановок вершин графа.

Введём случайную величину  $X$  равную количеству соседних пар вершин в перестановке, которые являются рёбрами в графе (или что эквивалентно числу рёбер в графе, которые встречаются в виде соседних пар вершин в перестановке).

Введем индикаторную функцию  $I_e = \begin{cases} 1, & \text{если ребро является парой в перестановке} \\ 0, & \text{иначе} \end{cases}$

$$\text{Тогда } X = \sum_{e \in E} I_e. \text{ Следовательно } EX = E\left(\sum_{e \in E} I_e\right) = \sum_{e \in E} EI_e.$$

Осталось найти вероятность того, что ребро является парой в перестановке. Пусть есть некоторое случайное ребро  $\{v, w\}$ . Подходящих перестановок с этим ребром  $2 \cdot n \cdot (n-2)!$  штук (выбираем  $n$  способами место для вершины  $v$ , потом 2-мя способами, справа или слева с учётом зацикливания по концам, место для вершины  $w$ , и просто расставляем как угодно  $n-2$  оставшиеся вершины). Всего перестановок  $n!$ , поэтому вероятность того, что ребро подходящее:  $\frac{2 \cdot n \cdot (n-2)!}{n!} = \frac{2}{n-1}$ .

В графе по условию  $\frac{nd}{2}$  рёбер, поэтому  $EX = \sum_{e \in E} EI_e = \frac{nd}{2} \cdot \frac{2}{n-1} = \frac{nd}{n-1} > \frac{nd}{n} = d$ . Тогда по вероятностному методу найдётся такая перестановка, что более  $d$  пар в ней будут являться рёбрами графа ■

### 13.9 Задача 9

Случайная величина  $X = \sum_{i=1}^{15} I_i$ , где  $I_i = \begin{cases} 1, & \text{если } i\text{-ая девочка стоит левее всех мальчиков} \\ 0, & \text{иначе} \end{cases}$

Теперь для подсчёта мат. ожидания осталось узнать вероятность того, что выбранная девочка стоит левее всех мальчиков. Это можно сделать с помощью идеи близкой к методу шаров и перегородок: давайте выстроим подряд 15 мальчиков, образовалось (с учётом мест перед 1-м и после 15-го) 16 промежутков, куда мы можем поставить девочек. Чтобы девочка была левее всех мальчиков, нужно просто, чтобы она стояла в первом промежутке. Вероятность этого  $= \frac{1}{16}$ .

$$\text{Тогда } EX = E\left(\sum_{i=1}^{15} I_i\right) = 15 \cdot \frac{1}{16} = \frac{15}{16}.$$

**Ответ:**  $\frac{15}{16}$

### 13.10 Задача 10

Не решали на семинаре (возможно, появится после факультатива).

# 14 Семинар 17

(Никита)

## 14.1 Задача 1

**Условие:** Докажите, что вершины полного графа  $K_n$  можно раскрасить в два цвета так, что в полученном графе есть не более

$$\binom{n}{t} 2^{1-t}$$

одноцветных подграфов  $K_t$

**Решение:**

Введём случайную величину  $X$  равную количеству одноцветных подграфов на  $t$  вершинах.

Введем индикаторную функцию  $I_{K_t} = \begin{cases} 1, & \text{если подграф одноцветен} \\ 0, & \text{иначе} \end{cases}$

Тогда  $X = \sum_{K_t \in G} I_{K_t}$ . Следовательно  $EX = E\left(\sum_{K_t \in G} I_{K_t}\right) = \sum_{K_t \in G} EI_{K_t}$ .

Осталось найти вероятность того, что выбранный подграф  $K_t$  будет одноцветным. У нас есть всего 2 цвета (НУО чёрный и белый), каждая вершина независимо красится или в чёрный, или в белый с вероятностью  $\frac{1}{2}$ , поэтому, чтобы подграф был одноцветным, все вершины должны быть полностью чёрными или полностью белыми. Вероятность этого:  $2 \cdot \left(\frac{1}{2}\right)^t = \left(\frac{1}{2}\right)^{t-1} = 2^{1-t}$ . Всего в полном графе есть  $\binom{n}{t}$  полных подграфов на  $t$  вершинах, следовательно  $EX = \sum_{K_t \in G} EI_{K_t} = \binom{n}{t} 2^{1-t}$ , а тогда по вероятностному методу найдётся раскраска вершин, при которой количество одноцветных подграфов будет  $\leq \binom{n}{t} 2^{1-t}$  ■

## 14.2 Задача 2 (дублирует 8 с семинара 16)

**Условие:** В неориентированном графе (без петель и кратных ребер)  $n$  вершин и  $\frac{nd}{2}$  ребер (то есть средняя степень вершины равна  $d$ ),  $d \geq 1$ . Докажите, что существует такое упорядочение вершин графа  $(v_1, v_2, \dots, v_n)$ , в котором каждая вершина встречается ровно один раз и более  $d$  из  $n$  пар  $\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_{n-1}, v_n\}, \{v_n, v_1\}$  являются ребрами графа.

**Решение:**

Будем рассматривать случайно выбранную перестановку из множества всех перестановок вершин графа.

Введём случайную величину  $X$  равную количеству соседних пар вершин в перестановке, которые являются рёбрами в графе (или что эквивалентно числу рёбер в графе, которые встречаются в виде соседних пар вершин в перестановке).

Введем индикаторную функцию  $I_e = \begin{cases} 1, & \text{если ребро является парой в перестановке} \\ 0, & \text{иначе} \end{cases}$

Тогда  $X = \sum_{e \in E} I_e$ . Следовательно  $EX = E\left(\sum_{e \in E} I_e\right) = \sum_{e \in E} EI_e$ .

Осталось найти вероятность того, что ребро является парой в перестановке. Пусть есть некоторое случайное ребро  $\{v, w\}$ . Подходящих перестановок с этим ребром  $2 \cdot n \cdot (n-2)!$  штук (выбираем  $n$  способами место для вершины  $v$ , потом 2-мя способами, справа или слева с учётом зацикливания по концам, место для вершины  $w$ , и просто расставляем как угодно  $n-2$  оставшиеся вершины). Всего перестановок  $n!$ , поэтому вероятность того, что ребро подходящее:  $\frac{2 \cdot n \cdot (n-2)!}{n!} = \frac{2}{n-1}$ .

В графе по условию  $\frac{nd}{2}$  рёбер, поэтому  $EX = \sum_{e \in E} EI_e = \frac{nd}{2} \cdot \frac{2}{n-1} = \frac{nd}{n-1} > \frac{nd}{n} = d$ . Тогда по вероятностному методу найдётся такая перестановка, что более  $d$  пар в ней будут являться рёбрами графа ■

## 14.3 Задача 3

**Условие:** Для одного и того же вероятностного пространства приведите пример двух зависимых случайных величин, а также двух независимых случайных величин.

**Решение:**

Определим вероятностное пространство, как множество всех двоичных слов длины 2 (их всего 4: 00, 01, 10, 11).

а) Зависимые случайные величины.

Введём случайные величины  $X$  - кол-во нулей в слове,  $Y$  - количество единиц в слове. Если данные величины независимы, то для них верно следующее:

Случайные величины  $X, Y : \Omega \rightarrow \mathbb{R}$  называются независимыми, если  $\forall x, y \in \mathbb{R}$  события  $\{\omega \in \Omega | X(\omega) = x\}$  и  $\{\omega \in \Omega | Y(\omega) = y\}$  независимы. (напомню, что события  $A, B$  называются независимыми, если  $P(A \cap B) = P(A) \cdot P(B)$ ).

Приведём такие  $x, y$ , при которых утверждение выше неверно:  $x = 2, y = 2$ . Можем видеть, что  $P(X = 2) = \frac{1}{4}$ ,  $P(Y = 2) = \frac{1}{4}$ , однако вероятность того  $P(X = 2, Y = 2) = 0$ , т.к. нет чисел с двумя нулями и единицами одновременно. Значит  $P(X = 2) \cdot P(Y = 2) \neq P(X = 2, Y = 2)$ , следовательно  $X$  и  $Y$  зависимы.

6) Независимые случайные величины.

Введём случайные величины  $X$  - значение в первом разряде (0 или 1),  $Y$  - значение во втором разряде (0 или 1). Независимость величин тривиальна и предоставляется на проверку читателю.

#### 14.4 Задача 4

**Условие:** Что можно сказать про случайную величину  $X$ , если известно, что  $E[X^2] = (E[X])^2$ ?

**Решение:**

Давайте для начала докажем лемму:

Если  $f \geq 0$  и  $Ef = 0$ , то  $f = 0$ . Доказать этот факт можно разными способами, мы воспользуемся неравенством Маркова:

$P(f \geq \alpha) \leq \frac{E[f]}{\alpha}$  при подстановке туда  $Ef = 0$  превращается в  $P(f \geq \alpha) \leq 0 \forall \alpha > 0$ . Вероятность по определению неотрицательна, поэтому  $P(f \geq \alpha) = 0 \forall \alpha > 0$ . Но раз вероятность того, что  $f$  принимает положительное значение равна 0 и  $f \geq 0$ , то  $f$  это константный 0 ■

Теперь перейдём к основной части. По условию  $EX^2 = (EX)^2$ , значит  $DX = E(X - EX)^2 = EX^2 - (EX)^2 = 0$ . По лемме из того, что  $E(X - EX)^2 = 0$ , следует, что  $(X - EX)^2 = 0$ , значит  $X = EX$ .

**Ответ:** про такую случайную величину мы можем сказать, что она равна своему мат. ожиданию.

#### 14.5 Задача 5

**Условие:** Про независимые случайные величины  $X_1, X_2, X_3, X_4$  известно, что  $E[X_i] = -1, D[X_i] = 1$ . Найдите  $D[X_1 X_2 X_3 X_4]$ .

**Решение:**

$$EX_i = -1, DX_i = 1. DX_i = EX_i^2 - (EX_i)^2 \Rightarrow EX_i^2 = DX_i + (EX_i)^2 = 1 + (-1)^2 = 2.$$

Отметим, что для независимых величин  $X_1, X_2, \dots, X_n$  верно, что  $EX_1 X_2 \dots X_N = EX_1 \cdot EX_2 \dots EX_n$  (доказывалось на лекции). Помимо того, далее мы воспользуемся фактом, что  $f(X), g(Y)$  независимы, если  $X, Y$  независимы (это доказывается чуть более сложно, заинтересованный читатель может доказать данный факт в качестве упражнения или же привлечь дополнительную литературу - по крайне мере строгое обоснование на семинаре не приводилось).

$$\text{Тогда } DX_1 X_2 X_3 X_4 = E(X_1 X_2 X_3 X_4)^2 - (EX_1 X_2 X_3 X_4)^2 = EX_1^2 X_2^2 X_3^2 X_4^2 - (EX_1)^2 (EX_2)^2 (EX_3)^2 (EX_4)^2 = EX_1^2 EX_2^2 EX_3^2 EX_4^2 - (EX_1)^2 (EX_2)^2 (EX_3)^2 (EX_4)^2 = 2^4 - (-1)^2 \cdot 4 = 16 - 1 = 15.$$

**Ответ:** 15.

#### 14.6 Задача 6

**Условие:** Пусть  $X_i \in \{0, 1\}, i = 1, 2, \dots, n$  - независимые случайные величины, принимающие значения 0 и 1 с вероятностью  $\frac{1}{2}$ . Рассмотрим  $X = X_1 + X_2 + \dots + X_n$ . Докажите, что существует некоторое  $\gamma = O(\sqrt{n})$ , для которого

$$P[X \geq \frac{n}{2} + \gamma] \leq \frac{1}{100}$$

**Решение:**

Уточняется.

#### 14.7 Задача 7

**Условие:** Пусть  $f : \{0, 1\} \rightarrow \{0, 1\}$  - булева функция и пусть  $A$  - вероятностный алгоритм, вычисляющий  $f$ , работающий за время  $O(n^2)$  и ошибающийся с вероятностью  $\frac{1}{3}$ . Постройте вероятностный алгоритм  $B$ , вычисляющий  $f$ , работающий за время  $O(n^2)$  и ошибающийся с вероятностью не более  $\frac{1}{1000}$ .

**Решение:**

Построим алгоритм  $B$  так: запустим 1000 раз алгоритм  $A$  и выберем то число, которое выдавалось чаще (при равенстве пусть выдаёт заведомо ошибочное число - например 2). Раз алгоритм  $A$  работал за  $O(n^2)$ , то и  $B$  будет работать за  $O(n^2)$ . Осталось проверить, что вероятность ошибки  $\leq \frac{1}{1000}$ :

Введем индикаторную функцию  $I_i = \begin{cases} 1, & \text{если на } i\text{-м запуске алгоритма } A \text{ внутри } B, \text{ алгоритм } A \text{ ошибся} \\ 0, & \text{иначе} \end{cases}$

Тогда  $X = \sum_{i=1}^{1000} I_i$  - количество ошибок в запусках алгоритма  $A$  внутри  $B$ . Чтобы алгоритм  $B$  в итоге выдал ошибочный ответ, нужно чтобы  $X \geq 500$ . Воспользуемся неравенством Чернова:

$$\forall \varepsilon \in (0,1) \quad P(X \geq (1 + \varepsilon)pn) \leq e^{-\frac{\varepsilon^2 np}{3}}.$$

$$P(X \geq 500) = P(X \geq (1 + \frac{1}{2})\frac{1000}{3}) \leq e^{-\frac{(\frac{1}{2})^2 \frac{1000}{3}}{3}} = e^{-\frac{1000}{36}}. \text{ Последним шагом осталось показать что } e^{-\frac{1000}{36}} \leq \frac{1}{1000}.$$

Сработает любая грубая оценка:

$$e^{-\frac{1000}{36}} < e^{-20} < 2^{-20} = \frac{1}{1024^2} < \frac{1}{1000} \blacksquare$$

## 15 Семинар 18

([Никита](#))

### 15.1 Задача 1

*Условие:* Найдите обратную к производящей функции:

a)  $1 - x + x^2 - x^3 + x^4 - \dots$

б)  $1 + x^2 + x^4 + x^6 + \dots$

*Решение:*

Эти задачи скорее решаются методом пристального взгляда и некоторой интуицией. Просто заметим, что для а) обратной будет  $1 + x$ . Это можно показать по определению: коэффициент при  $x^n$  будет равен  $1 \cdot 1 + 1 \cdot (-1) = 0$ , а  $a_0$  в действительности 1.

Аналогично для б) проверяется, что обратная это  $1 - x^2$ .

**Ответ:** а)  $1 + x$ ; б)  $1 - x^2$ .

### 15.2 Задача 2

*Условие:* Найдите произведение следующих производящих функций:

$$(1 + x + x^2 + x^3 + \dots)(1 - x + x^2 - x^3 + \dots)$$

*Решение:*

Здесь мы воспользуемся фактом из задачи 3 (который мы докажем чуть ниже):

$$(FG)^{-1} = G^{-1}F^{-1}$$

Заметим, что  $1 - x + x^2 - x^3 + x^4 - \dots = \frac{1}{1+x}$ , а  $1 + x + x^2 + x^3 + \dots = \frac{1}{1-x}$  (было показано на лекции). Тогда  $(1 + x + x^2 + x^3 + \dots)(1 - x + x^2 - x^3 + \dots) = \frac{1}{1+x} \cdot \frac{1}{1-x} = \frac{1}{(1-x)(1+x)} = \frac{1}{1-x^2} = 1 + x^2 + x^4 + x^6 + \dots$  (см 1(б)).

**Ответ:**  $1 + x^2 + x^4 + x^6 + \dots$

### 15.3 Задача 3

*Условие:* Пусть  $F$  и  $G$  — обратимые производящие функции. Докажите, что  $(FG)^{-1} = G^{-1}F^{-1}$ .

*Решение:*

Достаточно проверить, что  $FG \cdot G^{-1}F^{-1} = 1$ . Пользуемся ассоциативностью умножения производящих функций:  $FG \cdot G^{-1}F^{-1} = F(GG^{-1})F^{-1} = FF^{-1} = 1 \blacksquare$

## 15.4 Задача 4

*Условие:* Пусть  $A, B, C, D$  - обратимые функции. Докажите равенство:

$$\frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD}$$

*Решение:*

Покажем следующий несложный факт, равенства  $X = Y$  и  $XZ = YZ$  эквивалентны, если  $Z$  - обратима. Следование справа налево очевидно, а слева направа импликация верна потому, что можно домножить на существующий обратный к  $Z$  и получить исходное равенство. Тогда домножим данное в задаче равенство на обратимую  $BD$  (обратима по задаче 3). Получится:

$AD + BC = AD + BC$ , что верно. Значит и исходное было верно ■

## 15.5 Задача 5

*Условие:* Докажите равенство:

$$(F^{-1})' = -\frac{F'}{F^2}$$

*Решение:*

Воспользуемся доказанной на лекции формулой Лейбница для взятия производной  $FF^{-1} = 1$ :

$$(FF^{-1})' = F'F^{-1} + F(F^{-1})'$$

$$(1)' = F'F^{-1} + F(F^{-1})'$$

$$0 = F'F^{-1} + F(F^{-1})', \text{ откуда } (F^{-1})' = -\frac{F'}{F^2} \blacksquare$$

## 15.6 Задача 6

*Условие:* Какие производящие функции обратимы, то есть для каких производящих функций  $g$  существует производящая функция  $f$ , такая что  $f \cdot g = 1$ ?

*Решение:*

Пусть  $g = g_0 + g_1x + g_2x^2 + g_3x^3 + \dots$ , а  $f = f_0 + f_1x + f_2x^2 + f_3x^3 + \dots$ . Тогда  $f \cdot g = f_0g_0 + (f_0g_1 + f_1g_0)x + (f_0g_2 + f_1g_1 + f_2g_0)x^2 + \dots$ . Коэффициенты функции  $f$  мы знаем, а функцию  $g$  будем строить пошагово. Свободный член  $f \cdot g$  равен 1, а коэффициент при  $x^n \forall n$  равен 0.

Запишем:

$f_0g_0 = 1$ , значит  $f_0 = \frac{1}{g_0}$ , что верно при  $g_0 \neq 1$ . Рассмотрим следующее равенство  $f_0g_1 + f_1g_0 = 0$ . Это линейное уравнение с одной неизвестной  $g_1$  и нулевым коэффициентом при ней, т.е. такое уравнение всегда имеет решение. Аналогично можем находить и следующие коэффициенты, так как в уравнении коэффициент при  $x^k$  всегда будет участвовать ровно одна неизвестная  $g_k$  умноженная на что-то ненулевое (совсем строго это всё показывается по индукции). Вывод: единственное условие на то, чтобы функция была обратима, это наличие ненулевого свободного члена.

**Ответ:**  $g_0 \neq 0$

## 15.7 Задача 7

*Условие:* Пусть  $a_n$  — число решений уравнения  $x_1 + \dots + x_k = n$  в целых неотрицательных числах. Пусть  $F(x)$  — производящая функция для последовательности  $a_n$ . Докажите, что  $F(x) = (1-x)^{-k}$ .

*Решение:*

$$F(x) = (1-x)^{-k} = (1+x+x^2+\dots)(1+x+x^2+\dots)\dots(1+x+x^2+\dots) \text{ (к раз).}$$

Тогда посмотрим чему равен коэффициент при  $x^n$  по определению:  $\sum_{x_1+\dots+x_k} 1 \dots 1 = a_n$  (иначе говоря, мы должны выбрать из каждой скобки свой член ряда, так чтобы сумма всех степеней при их  $x$  давала  $n$ , и перемножить числовые коэффициенты при всех выбранных членах рядов. А поскольку  $1 \dots 1 = 1$  мы для каждого решения уравнения  $x_1 + \dots + x_k = n$  прибавим единицу, то есть в точности посчитаем число решений  $a_n$ . Значит  $(1-x)^{-k}$  — действительно производящая функция для последовательности  $a_n$  ■

## 15.8 Задача 8

*Условие:* Докажите, что для всех неотрицательных  $n$  верно:

$$\begin{aligned} \text{a)} \quad & \binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \\ \text{б)} \quad & (1+x)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} x^k \end{aligned}$$

## 15.9 Задача 9

Спасибо за решение и .tex задачи [Любови Николаевне](#)

*Условие:* С помощью производящих функций найдите сумму  $\sum_{i=0}^n i^3$ .

*Решение:*

Рассмотрим сначала последовательность 1,1,1,1,1, ... и ее производящую функцию

$$F(x) = 1 + x + x^2 + x^3 + \dots = \frac{1}{1-x}.$$

Построим используя  $F(x)$  производящую функцию последовательности 1,2,3,4,5, ...

$$F'(x) = 1 + 2x + 3x^2 + 4x^3 + \dots = \left( \frac{1}{1-x} \right)' = \frac{1}{(1-x)^2}.$$

Домножим  $F'(x)$  на  $x$  и возьмем еще одну производную, чтобы получить производящую функцию последовательности 1<sup>2</sup>, 2<sup>2</sup>, 3<sup>2</sup>, 4<sup>2</sup>, ...

$$(x \cdot F'(x))' = 1 + 2^2 x + 3^2 x^2 + 4^2 x^3 + \dots = \left( \frac{x}{(1-x)^2} \right)' = \frac{(1-x)^2 + x \cdot 2(1-x)}{(1-x)^4} = \frac{1+x}{(1-x)^3}.$$

Снова домножим получившуюся функцию на  $x$  и возьмем еще одну производную, чтобы получить производящую функцию последовательности 1<sup>3</sup>, 2<sup>3</sup>, 3<sup>3</sup>, 4<sup>3</sup>, ...

$$(x \cdot (x \cdot F'(x))')' = 1 + 2^3 x + 3^3 x^2 + 4^3 x^3 + \dots = \left( \frac{x+x^2}{(1-x)^3} \right)' = \frac{(1+2x)(1-x) + 3(x+x^2)}{(1-x)^4} = \frac{1+4x+x^2}{(1-x)^4}.$$

Заметим, что если домножить некий формальный ряд

$$G(x) = g_0 + g_1 x + g_2 x^2 + \dots$$

на ряд

$$\frac{1}{1-x} = 1 + x + x^2 + \dots,$$

то получится ряд

$$\frac{1}{1-x} \cdot G(x) = \sum_{k=0}^{\infty} (g_0 + g_1 + \dots + g_k) x^k.$$

Поэтому для получения производящей функции последовательности  $a_n = 1^3 + 2^3 + \dots + n^3$  нужно производящую функцию последовательности  $b_n = n^3$  домножить на  $\frac{1}{1-x}$ :

$$\frac{1}{1-x} \cdot \frac{1+4x+x^2}{(1-x)^4} = 1^3 + (1^3 + 2^3)x + (1^3 + 2^3 + 3^3)x^2 + \dots$$

Нас интересует коэффициент данного ряда при  $x^{n-1}$ . Для того, чтобы было проще считать, разобьем дробь на сумму дробей:

$$\frac{1+4x+x^2}{(1-x)^5} = \frac{1}{(1-x)^5} + \frac{4x}{(1-x)^5} + \frac{x^2}{(1-x)^5}.$$

Вспомним, что (см. задачу 7 с семинара)

$$\frac{1}{(1-x)^5} = (1 + x + x^2 + x^3 + \dots)^5 = \sum_{k=0}^{\infty} C_{k+4}^4 x^k,$$

$$\frac{4x}{(1-x)^5} = 4x(1 + x + x^2 + x^3 + \dots)^5 = \sum_{k=0}^{\infty} 4 \cdot C_{k+4}^4 x^{k+1} = \sum_{k=1}^{\infty} 4 \cdot C_{k+3}^4 x^k,$$

$$\frac{x^2}{(1-x)^5} = x^2(1+x+x^2+x^3+\dots)^5 = \sum_{k=0}^{\infty} C_{k+4}^4 x^{k+2} = \sum_{k=2}^{\infty} C_{k+2}^4 x^k.$$

Откуда

$$\begin{aligned} \frac{1+4x+x^2}{(1-x)^5} &= \sum_{k=0}^{\infty} (C_{k+4}^4 + 4 \cdot C_{k+3}^4 + C_{k+2}^4) x^k = \\ &= \sum_{k=0}^{\infty} \left( \frac{(k+4)(k+3)(k+2)(k+1)}{4!} + \frac{4(k+3)(k+2)(k+1)k}{4!} + \frac{(k+2)(k+1)k(k-1)}{4!} \right) x^k = \\ &= \sum_{k=0}^{\infty} \frac{((k+4)(k+3) + 4(k+3)k + k(k-1))(k+2)(k+1)}{4!} x^k = \\ \sum_{k=0}^{\infty} \frac{(k^2+7k+12+4k^2+12k+k^2-k)(k+2)(k+1)}{4!} x^k &= \sum_{k=0}^{\infty} \frac{(6k^2+18k+12)(k+2)(k+1)}{4!} x^k = \\ \sum_{k=0}^{\infty} \frac{(k^2+3k+2)(k+2)(k+1)}{4} x^k &= \sum_{k=0}^{\infty} \frac{(k+2)^2(k+1)^2}{4} x^k. \end{aligned}$$

Ответ:  $\left(\frac{(n+1)n}{2}\right)^2$ .

**Второй способ.** Очень похоже на первый способ, но рассматривается конечный ряд.

Сразу ограничимся конечной суммой. То есть рассмотрим

$$F(x) = \frac{1-x^{n+1}}{1-x} = 1+x+x^2+\dots+x^n.$$

С этой конечной суммой произведем те же операции (взятия производной и умножения на  $x$ )

$$\begin{aligned} 1+2^3x+3^3x^2+4^3x^3+\dots+n^3x^{n-1} &= (x \cdot (x \cdot F'(x))')' = \left( x \cdot \left( x \cdot \left( \frac{1-x^{n+1}}{1-x} \right)' \right)' \right)' = \\ \left( x \cdot \left( \frac{-(n+1)x^{n+1}+nx^{n+2}+x}{(1-x)^2} \right)' \right)' &= \left( x \cdot \frac{-n^2x^{n+2}+(2n^2+2n-1)x^{n+1}-(n+1)^2x^n+x+1}{(1-x)^3} \right)' = \\ \frac{n^3x^{n+3}+(-3n^3-3n^2+3n-1)x^{n+2}+(3n^3+6n^2-4)x^{n+1}-(n+1)^3x^n+x^2+4x+1}{(1-x)^4}. \end{aligned}$$

Посчитать нам нужно значение этой функции при  $x=1$ . Просто подставить не получится, т.к. знаменатель обратится в ноль. Можно посчитать предел, например, через правило Лопитала (опять куча производных, но уже отдельно для числителя и знаменателя). Через правило Лопитала: вычисляем четвертые производные числителя и знаменателя и подставляем  $x=1$ :

$$\begin{aligned} &\frac{n^3(n+3)(n+2)(n+1)n+(-3n^3-3n^2+3n-1)(n+2)(n+1)n(n-1)+}{(1-x)^4} \\ &+ \frac{(3n^3+6n^2-4)(n+1)n(n-1)(n-2)-(n+1)^3n(n-1)(n-2)(n-3)}{4!} = \\ &= \frac{n(n+1)}{4!} \cdot (n^3(n+3)(n+2)+(-3n^3-3n^2+3n-1)(n+2)(n+1)+ \\ &+(3n^3+6n^2-4)(n-1)(n-2)-(n+1)^2(n-1)(n-2)(n-3)) = // \text{оно упрощается, записывать не хочу} \\ &= \frac{n(n+1)}{4!} \cdot (6n^2+6n) = \left( \frac{n(n+1)}{2} \right)^2. \end{aligned}$$

Ответ:  $\left(\frac{(n+1)n}{2}\right)^2$ .

## 16 Семинар 19

(Илья)

## 16.1 Задача 1

*Условие:* Найдите производящие функции и явные выражения для элементов последовательностей, заданных рекуррентными формулами:

- a)  $a_{n+3} = -3a_{n+2} - 3a_{n+1} - a_n, a_0 = 1, a_1 = a_2 = 0$
- б)  $a_{n+2} = a_{n+1} + 2a_n, a_0 = 2, a_1 = 0$

**Решение:**

а) Пусть  $C(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots$  - производящая функция для последовательности  $a_n$ .

Давайте домножим уравнение на  $x^{n+3}$  и получим, что  $x^{n+3}a_{n+3} = -3x \cdot x^{n+2}a_{n+2} - 3x^2 \cdot x^{n+1}a_{n+1} - x^3 \cdot x^n a_n$

Просуммируем уравнение по всем  $n \geq 0$  и получим, что  $C(x) - a_0 - a_1x - a_2x^2 = -3x(C(x) - a_0 - a_1x) - 3x^2(C(x) - a_0) - x^3C(x)$

Отсюда,  $C(x) - 1 = -3x(C(x) - 1) - 3x^2(C(x) - 1) - x^3C(x)$ , значит  $C(x) = \frac{3x+3x^2+1}{1+3x+3x^2+x^3} = \frac{1+3x+3x^2}{(x+1)^3}$

Мы хотим найти  $a_n = \frac{C^{(n)}(0)}{n!}$ . Но давайте заметим, что  $C(x) = \frac{1}{(x+1)^3} + 3\frac{x}{(x+1)^3} + 3\frac{x^2}{(x+1)^3}$  и каждое слагаемое отличается от  $\frac{1}{(x+1)^3}$  только сдвигом коэффициентов на 1 и 2 соответственно.

Пусть  $f(x) = \frac{1}{(x+1)^3}$

Так что давайте найдём  $b_n = \frac{f(x)^{(n)}(0)}{n!}$

Узнаём  $f(x)^{(n)} = \frac{(-1)^n(n+2)!}{2!(x+1)^{n+3}}$ , тогда  $b_n = \frac{(-1)^n(n+1)(n+2)}{2}$

Тогда  $a_n = b_n + 3b_{n-2} + 3b_{n-1} = \frac{(-1)(n-2)}{2}$

б) Пусть  $C(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots$  - производящая функция для последовательности  $a_n$ .

Давайте домножим уравнение на  $x^{n+2}$  и получим, что  $x^{n+2}a_{n+2} = x \cdot x^{n+1}a_{n+1} + 2x^2 \cdot x^n a_n$

Просуммируем уравнение по всем  $n \geq 0$  и получим, что  $C(x) - a_0 - a_1x = x(C(x) - a_0) + 2x^2C(x)$

Отсюда,  $C(x) - 2 = x(C(x) - 2) + 2x^2C(x)$ , значит  $C(x) = \frac{2(x-1)}{2x^2+x-1} = \frac{2(x-1)}{(x+1)(2x-1)} = \frac{4}{3(x+1)} - \frac{2}{3(2x-1)}$

Мы хотим найти  $a_n = \frac{C^{(n)}(0)}{n!}$ . Тогда  $C^{(n)}(x) = \frac{4}{3} \cdot \frac{(-1)^n n!}{(x+1)^{n+1}} - \frac{2}{3} \cdot \frac{(-1)^n n! \cdot 2^n}{(2x-1)^{n+1}}$

Тогда  $a_n = \frac{4(-1)^n + 2^{n+1}}{3}$

**Ответ:**  $\begin{cases} \text{а) } C(x) = \frac{1+3x+3x^2}{(x+1)^3}, a_n = \frac{(-1)(n-2)}{2} \\ \text{б) } C(x) = \frac{2(x-1)}{(x+1)(2x-1)}, a_n = \frac{4(-1)^n + 2^{n+1}}{3} \end{cases}$

## 16.2 Задача 2

*Условие:* Используя производящую функцию для чисел Фибоначчи  $F_n$  докажите тождество:

$$F_0 + F_1 + \dots + F_n = F_{n+2} - 1$$

**Решение:**

1.

## 16.3 Задача 3

*Условие:* Имеется неограниченное количество монет 1 рубль и 5 рублей. Обозначим через  $a_n$  число способов разменять  $n$  рублей этими монетами. Используя производящие функции, выпишите рекуррентное соотношение на  $a_n$

**Решение:**

1. Запишем производящую  $(1 + x + x^2 + x^3 + x^4 + \dots)(1 + x^5 + x^{10} + x^{15} + \dots) = C(x)$ . Причём коэффициент при  $t^n$  будет в точности равен  $a_n$ .
2. Немного преобразуем  $C(x) = \frac{1}{(1-x)(1-x^5)}$

## 16.4 Задача 4

*Условие:* Используя производящие функции, покажите, что любое натуральное число однозначно представляется в виде суммы различных степеней двоек с целым неотрицательным показателем (т. е. однозначно записывается в двоичной системе счисления). Докажите аналогичный результат для десятичной системы счисления.

**Решение:**

1.

## 16.5 Задача 5

*Условие:* Найдите число монотонных функций  $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ .

**Решение:**

1.

## 16.6 Задача 6

**Определение:** Производящую функцию назовем рациональной, если она представляется в виде отношения двух многочленов.

*Условие:* Существует ли последовательность, производящая функция которой не рациональна?

**Решение:**

1.

## 16.7 Задача 7

*Условие:* Докажите, что производящие функции следующих последовательностей рациональны: а)  $a_n = \binom{n+m}{m}$ ; б)  $a_n = \binom{n}{m}$ .

**Решение:**

1.

## 16.8 Задача 8

Пусть  $A(x) = \sum_{ik=0}^{\infty} a_k x^k$ ,  $B(x) = \sum_{ik=0}^{\infty} b_k x^k$ . Произведением Адамара назовем

$$A(x) \circ B(x) = \sum_{k=0}^{\infty} a_k b_k x^k$$

*Условие:* Пусть  $A(x)$  и  $B(x)$  — рациональные производящие функции. Докажите, что  $A(x) \circ B(x)$  рациональна.

**Решение:**

1.

## 16.9 Задача 9

*Условие:* Используя производящие функции, докажите, что число разбиений натурального числа  $n$  на различные (положительные) слагаемые равно числу его разбиений на нечетные слагаемые.

**Решение:**

1.

## 16.10 Задача 10

*Условие:* Найдите число «перестановок»  $\sigma \in S_n$ , т.е. таких, что  $\sigma(1) < \sigma(2), \sigma(2) > \sigma(3), \sigma(3) < \sigma(4)$  и т.д.

*Решение:*

1.

## 17 Домашнее задание 13

([Никита](#))

### 17.1 Задача 1

*Условие:* При бросании двух кубиков какова вероятность получить два одинаковых числа?

*Решение:*

Зафиксируем какое-нибудь из чисел от 1 до 6. Вероятность, что на одном кубике выпало это число и оно же на другом равна  $\frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$ . Всего чисел 6, поэтому общая вероятность  $6 \cdot \frac{1}{36} = \frac{1}{6}$

**Ответ:**  $\frac{1}{6}$

### 17.2 Задача 3

*Условие:* Бросаем кубик четыре раза. Какова вероятность того, что выпадающие числа строго возрастают? Укажите числовой ответ с абсолютной погрешностью 0.1.

*Решение:*

Возьмём возрастающую последовательность 1,2,3,4,5,6.

Все подходящие под условие подпоследовательности получаются вычёркиванием из неё двух символов. Тогда посчитаем, сколько существует четырёхэлементных подмножеств (будем брать элементы с сохранением порядка в исходной последовательности, следовательно получим строго возрастающую подпоследовательность): их  $\binom{6}{4} = \frac{6!}{4!2!} = \frac{6 \cdot 5}{2} = 15$ . Значит  $P = \frac{15}{6^4} = \frac{15}{1296} \approx 0,011574$

**Ответ:** 0,011574

### 17.3 Задача 2

*Условие:* Случайно и равновероятно выбрано целое число от 1 до 100. Найдите вероятность того, что сумма цифр этого числа равна 8.

*Решение:*

Выпишем все числа с суммой цифр 8: 8, 17, 26, 35, 44, 53, 62, 71, 80. Их 9, следовательно,  $P = \frac{9}{100} = 0,09$

**Ответ:** 0,09

### 17.4 Задача 4

*Условие:* На лотерейном билете требуется отметить 8 клеточек из 64. Какова вероятность того, что после розыгрыша, в котором также будет выбрано 8 каких-то клеток из 64 (все такие возможности равновероятны), окажется, что угаданы ровно 4 клеток?

*Решение:*

Зафиксируем выбранные игроками 8 чисел. Подходящими билетами будут те, в которых есть 4 элемента из выбранных 8 + 4 из оставшихся 56. Тогда  $P = \frac{\binom{8}{4} \cdot \binom{56}{4}}{\binom{64}{8}} = \frac{8!56!8!56!}{4!4!4!52!64!} = \frac{714175}{122948038}$

**Ответ:**  $\frac{714175}{122948038}$

## 17.5 Задача 6

*Условие:* Вася и Петя бросают монету: Вася бросил ее 10 раз, а Петя — 11 раз. Чему равна вероятность того, что у Пети монета упала орлом большее число раз, чем у Васи?

*Решение:*

Заметим, что события "у Пети больше орлов, чем у Васи" и "у Васи больше решек, чем у Пети" равновероятны, так как они симметричны. Покажем, что они дополняют друг друга до 1. Действительно, так как Петя бросал ровно на 1 раз больше, то либо у Пети орлов больше либо у Васи больше решек, но не одновременно. Значит вероятность каждого события по  $\frac{1}{2}$ .

**Ответ:**  $\frac{1}{2}$

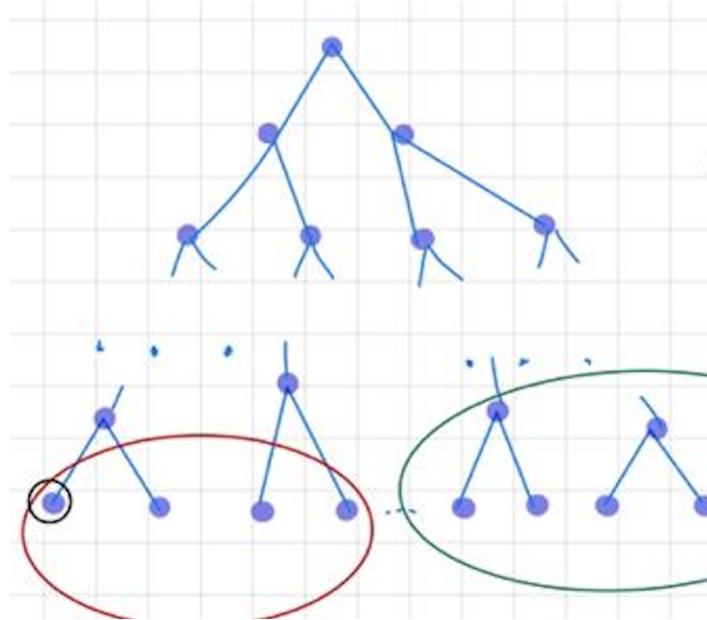
## 17.6 Задача 5

*Условие:* Шестьдесят четыре команды участвуют в турнире по олимпийской системе (команды случайно и равновероятно разбиваются на пары, парные команды играют между собой, победители проходят в следующий раунд, где процедура повторяется). Все команды упорядочены по силе, и более сильная всегда выигрывает у более слабой. Какова вероятность того, что в финале встретятся две самые сильные команды?

*Решение:*

Олимпийский турнир можно изобразить в виде дерева (вершина-пара соревнующихся, а ребро соединяет вершину из одного раунда с вершиной следующего раунда, если в них есть один и тот же участник)

Две сильнейшие команды могут не сыграть вместе в финале только если сыграли вместе до этого. Значит, чтобы было как в условии, то надо, чтобы у этих игроков были разные поддеревья.



Листьев у дерева 32 (так как вершина — это пара человек). Зафиксируем для самого сильного один элемент из поддерева. Значит осталось 63 места для второго игрока. Ему подходит другая половина, то есть 32 места. Итого  $P = \frac{32}{63}$ .

**Ответ:**  $\frac{32}{63}$

## 17.7 Задача 7

*Условие:* Докажите, что случайный граф на вершинах связен. Точная формулировка: исходы — все неориентированные графы без кратных ребер с одним и тем же множеством вершин, в котором  $n$  элементов. Все исходы равновозможны. Нужно доказать, что вероятность события «граф несвязный» стремится к нулю при  $n \rightarrow \infty$ .

*Решение:*

Уточняется.

## 17.8 Задача 8

*Условие:* Докажите, что найдется такой турнир, в котором любые 10 команд проиграли какой-то одной команде (победители разных десяток могут различаться).

*Решение:*

Рассмотрим какой-нибудь турнир при  $n \rightarrow \infty$  (будем доказывать аналогично предыдущей).

Зафиксируем тогда какие-нибудь 10 команд. Выберем из оставшихся ( $n-10$ ) команду, которой все эти 10 команд проиграли. Это происходит с вероятностью  $(\frac{1}{2})^{10}$ . Отрицание этого события с вероятностью  $\frac{1023}{1024}$ . Тогда для конкретной команды вероятность того, что такое событие не произойдет равна  $(\frac{1023}{1024})^{n-10} \rightarrow 0$ ,  $n \rightarrow \infty$ . Однако всего наборов из 10 команд  $\binom{n}{10}$ . Поэтому вероятность того, что вообще не найдется ни одной команды такой, что условие выполняется  $\leq (\binom{n}{10}) \cdot (\frac{1023}{1024})^{n-10}$  (по теореме о сумме и пересечении вероятностей). Аналогично задаче 7, эта вероятность стремится к 0 при  $n \rightarrow \infty$ . Значит, найдется команда из условия.

**Ч.Т.Д.**

## 18 Домашнее задание 14

(Илья)

### 18.1 Задача 3

*Условие:* Равновероятно выбирается случайная перестановка на множестве  $\{1, 2, \dots, n\}$ . Независимы ли события «число 1 остается на месте» и «число 2 остается на месте»?

*Решение:*

1. Пусть  $A$  - событие «число 1 остается на месте», а  $B$  - событие «число 2 остается на месте». Тогда посчитаем 3 вероятности:  $P(A \cap B)$ ,  $P(A)$ ,  $P(B)$ .
2. Сначала найдём  $P(A)$  и  $P(B)$ . Так как мы выбираем перестановку равновероятно, то вероятность того, что случайная перестановка оставляет число  $i$  на месте равна  $\frac{(n-1)!}{n!} = \frac{1}{n}$  и понятно, что тогда  $P(A) = P(B) = \frac{1}{n}$
3. Теперь посчитаем вероятность  $P(A \cap B)$ . Событие  $A \cap B$  - перестановка оставляет и 1, и 2 на месте. Вероятность такого события  $\frac{(n-2)!}{n!} = \frac{1}{n(n-1)}$
4. По определению независимости двух событий, события независимы, если  $P(A \cap B) = P(A) \cdot P(B)$ . Проверка:  $\frac{1}{n(n-1)} \neq \frac{1}{n} \cdot \frac{1}{n}$   
Значит события  $A, B$  зависимы.

**Ответ:** Нет, зависимы.

### 18.2 Задача 2

*Условие:* Заранее известно, что пациент болен тяжелой болезнью с вероятностью  $10^{-5}$ . Ему сделали тест на эту болезнь, который дает правильный результат с вероятностью 99% (независимо от того, здоров пациент или нет). Найдите отношение вероятностей событий «пациент болен этой болезнью» и «пациент не болен этой болезнью» при условии, что результат теста положительный.

*Решение:*

1. Пусть  $A$  - событие «пациент болен этой болезнью» и  $B$  - событие «пациент не болен этой болезнью»,  $C$  - событие «результат теста положительный». Тогда требуется найти  $\frac{P(A|C)}{P(B|C)} = \frac{P(A \cap C)}{P(B \cap C)}$  (по формуле условной вероятности)
2. Вероятность события  $A \cap C$ , то есть того, что пациент болен этой болезнью и тест его положительный, равна  $10^{-5} \cdot 0.99$ . Вероятность события  $B \cap C$ , то есть того, что пациент не болен этой болезнью и результат теста положительный, равна  $(1 - 10^{-5}) \cdot (1 - 0.99)$

$$\text{Значит } \frac{P(A \cap C)}{P(B \cap C)} = \frac{10^{-5} \cdot 0.99}{(1 - 10^{-5}) \cdot (1 - 0.99)} = \frac{10^{-5} \cdot 0.99}{10^{-2} \cdot 0.9999} = 10^{-3} \cdot \frac{11000}{11111} = \frac{11}{11111}$$

**Ответ:**  $\frac{11}{11111}$

### 18.3 Задача 1

*Условие:* Во сколько раз доля блондинов среди голубоглазых больше доли голубоглазых среди блондинов, если всего голубоглазых вдвое больше, чем блондинов?

*Решение:*

1. Пусть  $A$  - событие "случайный человек голубоглазый" и  $B$  - событие "случайный человек блондин". Тогда ответом на задачу будет отношение условных вероятностей  $\frac{P(B|A)}{P(A|B)} = \frac{P(B)}{P(A)}$  (по формуле Байеса).
2. Так как  $|A| = 2 \cdot |B|$ , то  $\frac{P(B)}{P(A)} = \frac{1}{2}$

**Ответ:**  $\frac{1}{2}$

### 18.4 Задача 4

*Условие:* Жюри из трех человек нужно принять одно из двух возможных решений, одно из которых правильное. Два члена жюри независимо друг от друга принимают правильное решение с вероятностью  $p$ , а третий случайно выбирает одно из двух возможных решений с равными вероятностями. Окончательное решение жюри выносится большинством голосов. Какова вероятность, что жюри примет правильное решение? (Сравните ее с вероятностью  $p$  правильного решения, принимаемого одним добросовестным членом жюри.)

*Решение:*

1. Есть 3 случая, когда жюри примет правильное решение: первые двое приняли верное решение (тут учитывается вариант, когда все 3 приняли верное решение), первый принял верное решение, второй принял неверное решение, а третий принял верное решение, первый принял неверное решение, второй и третий верное решение.  
Посчитаем их.
2. Начнём с первого случая. Вероятность такого события равна  $p \cdot p = p^2$
3. Посчитаем второй и третий случаи, так как они симметричны. Вероятность второго случая равна  $p \cdot (1-p) \cdot \frac{1}{2}$  и вероятность третьего случая равна  $(1-p) \cdot p \cdot \frac{1}{2}$
4. Итого получаем, что вероятность того, что жюри приняло верное решение равна  $p \cdot (1-p) \cdot \frac{1}{2} + p \cdot (1-p) \cdot \frac{1}{2} + p^2 = p(1-p) + p^2 = p$ . Получается, что эта вероятность совпадает с вероятностью  $p$  правильного решения, принимаемого одним добросовестным членом жюри.

**Ответ:** Вероятность совпадает.

### 18.5 Задача 5

*Условие:* Король предлагает узнику разложить десять белых и десять чёрных шаров по двум одинаковым коробкам (надо использовать все шары; в каждой коробке должен быть хотя бы один шар). После этого сначала король выбирает случайно одну из коробок, каждую с вероятностью  $1/2$ , а затем из выбранной коробки выбирает случайный шар, все с равными вероятностями. Если шар чёрный, то узника казнят, если белый — отпускают. Как нужно разложить шары, чтобы вероятность выжить была максимальной?

*Решение:*

1. Пусть в первой коробке после разложения оказалось  $w$  белых шаров и  $b$  чёрных шаров, тогда во второй коробке их  $10-w$  и  $10-b$  соответственно. Тогда вероятность выживания состоит из двух случаев: если король выбрал первую коробку и из неё выбрал белый шарик или король выбрал вторую коробку и из неё выбрал белый шарик.  
Посчитаем эти вероятности.
2. Итак, вероятность первого случая есть  $\frac{1}{2} \cdot \frac{w}{w+b}$ , так как сначала король выбирает первую коробку с вероятностью  $\frac{1}{2}$ , а потом достаёт один из  $w$  белых шаров из  $w+b$  шаров.  
Второй случай аналогичен, там выходит  $\frac{1}{2} \cdot \frac{10-w}{20-(w+b)}$
3. Итого получаем, что вероятность выжить равна  $\frac{1}{2} \cdot \frac{10-w}{20-(w+b)} + \frac{1}{2} \cdot \frac{w}{w+b}$ . Получили функцию от двух переменных, надо найти её максимум, учитывая, что  $w, b$  натуральные числа, не превышающие 9.

Зафиксируем  $w+b = k$ . Тогда вероятность имеет вид  $\frac{1}{2} \cdot \frac{10-w}{20-(w+b)} + \frac{1}{2} \cdot \frac{w}{w+b} = \frac{1}{2} \cdot \left( \frac{10-w}{20-k} + \frac{w}{k} \right) = \frac{1}{2} \cdot \left( \frac{(10-w)k+w(20-k)}{k(20-k)} \right) = \frac{1}{2} \cdot \left( \frac{10k-2wk+20w}{k(20-k)} \right)$ . Так как знаменатель фиксирован, то выражение максимально, когда числитель максимальен, поэтому нужно найти максимум числителя. Опять же таки, так как  $k$  фиксировано, то достаточно найти максимум выражения  $20w - 2wk = 2w(10 - k)$ . Можем считать, что  $k \leq 10$ , так как иначе просто переименуем коробки. Так как  $w \leq k$ , то понятно, что максимум такого выражения будет при  $w = k$ , но тогда  $b = 0$ . То есть в первой коробке будут лежать только белые шары.

Пользуясь этим знанием найдём  $w$ .

4. Так как  $b = 0$ , то исходная вероятность имеет вид  $\frac{1}{2} \cdot \frac{10-w}{20-(w+b)} + \frac{1}{2} \cdot \frac{w}{w+b} = \frac{1}{2} \cdot \left( \frac{10-w}{20-w} + 1 \right)$ . Найдём максимум выражения  $\frac{10-w}{20-w}$ . Он достигается при минимуме обратного. То есть ищем минимум выржания  $\frac{20-w}{10-w} = 1 + \frac{10}{10-w}$ . Минимум будет, когда знаменатель максимальный, следовательно, когда  $w$  минимально. Так как  $w \geq 1$ , то положим  $w = 1$ .

**Ответ:** В одну коробку положить 1 белый шар, а во вторую положить все остальные.

## 18.6 Задача 6

**Условие:** Двое играют в бой яиц. Перед ними стоит корзина с яйцами. Они наугад берут по яйцу и ударяют их носами. Разбитое яйцо выбрасывается и побеждённый берёт новое, а победитель раунда сохраняет своё яйцо для следующего раунда (предполагается, что победившее яйцо сохранило свою прочность и что исход каждого раунда зависит только от относительного качества яиц). Какова вероятность победы в  $(n+1)$ -м раунде после победы в предыдущих?

**Решение:**

1. Для начала поймём, что раз прошёл  $n+1$  раунд, то успело поучавствовать  $n+2$  яйца. (в первом раунде появилось 2 новых яйца, а в остальных  $n$  раундах добавлялось по 1 яйцу за раунд)
2. Так, теперь надо как-то подумать о том, как вообще считать данную вероятность. Давайте введём два события. Пусть событие  $A$  - "яйцо победило в  $n+1$  раунде" и событие  $B$  - "яйцо победило в предыдущих  $n$  раундах". Ну теперь хотя понятно, что надо искать  $P(A|B)$ .
3. По формуле условной вероятности,  $P(A|B) = \frac{P(A \cap B)}{P(B)}$ . Давайте поймём, что победа определяется только относительной прочностью яйца, поэтому выпишем в ряд все числа от 1 до  $n+2$ , где каждое из чисел - это номер яйца и определим на этом множестве такой порядок - одно из чисел стоит левее другого, если оно прочнее его. Тогда понятно, чему равносильна  $P(A \cap B)$  (вероятность того, что яйцо выиграет все  $n+1$  раунды) - тому, что первое яйцо будет левее (прочнее), чем все остальные, то есть яйцо с номером 1 стоит самым первым. Такая вероятность равна  $\frac{(n+1)!}{(n+2)!}$  (номер 1 стоит на первом месте, а остальные как-то перемешаны).
- Аналогично понятно, чему равна  $P(B)$ . Тут 2 варианта, либо  $n+2$  яйцо оказалось прочнее, чем первое яйцо, но все остальные проиграли (таких  $n!$  вариантов, так как 2 элемента из  $n+2$  фиксированы, а остальные как-то перемешаны), или первое яйцо оказалось самым сильным и это уже в точности посчитано( $(n+1)!$ ). Итого  $P(B) = \frac{n!+(n+1)!}{(n+2)!}$ .
4. Значит искомая вероятность равна  $P(A|B) = \frac{(n+1)!}{n!+(n+1)!} = \frac{n+1}{n+2}$

**Ответ:**  $\frac{n+1}{n+2}$

## 18.7 Задача 7

**Условие:** Приведите пример вероятностного пространства и  $n$  зависимых его событий, любые  $n-1$  из которых независимы в совокупности.

**Решение:**

1. Пусть у нас есть нечестная монетка (то есть вероятность выпадения орла равна  $p \neq \frac{1}{2}$  и решки  $= 1 - p$ ) и мы бросаем её из  $n-1$  раз. Наше вероятностное пространство состоит из  $n$  событий (и их вероятностей): "в  $i$ -ом броске выпал орёл", коих  $n-1$  штука и события "всего выпала 1 решка".
2. Заметим, что все  $n$  событий вместе невозможны, поэтому они не могут быть независимыми, значит они зависимы. Ещё можно заметить, что если рассматривать  $n-1$  событие вида "в  $i$ -ом броске выпал орёл", то понятно, что они все независимы при любом  $p$ . Осталось подобрать такое  $p$ , при котором событие "в  $i$ -ом броске выпал орёл", где  $1 \leq i \leq n-2$ , и "всего выпала 1 решка" будут независимы, тогда любые  $n-1$  события будут независимы.

3. Вероятность события "в  $i$ -ом броске выпал орёл" равна  $p$ , а вероятность  $n - 2$  таких событий равна  $p^{n-2}$ . Без ограничения общности можно положить, например, что в  $n - 1$ -ом броске не выпал орёл.
- Тогда вероятность события "в  $i$ -ом броске выпал орёл" ( $n - 2$  раза) и "всего выпала 1 решка" равна  $p^{n-2} \cdot (1-p)$ .
- Посчитаем теперь вероятность того, что "всего выпала 1 решка". Это значит, что в каких-то  $n - 2$  бросках выпал орёл и в оставшемся броске выпала решка. Вероятность этого равна  $\binom{n-1}{1} \cdot p^{n-2} \cdot (1-p) = (n-1) \cdot p^{n-2} \cdot (1-p)$ .
- Чтобы события "в  $i$ -ом броске выпал орёл" ( $n - 2$  раза) и "всего выпала 1 решка" были независимы в совокупности необходимо, чтобы было выполнено равенство:  $p^{n-2} \cdot (n-1) \cdot (1-p) \cdot p^{n-2} = p^{n-2} \cdot (1-p)$

Отсюда,  $p = \sqrt[n-2]{\frac{1}{n-1}}$  (договоримся, что  $n \geq 2$ , так как при  $n = 1$  у нас ровно одно событие и понятно, что там всё выполняется.)

Значит, мы смогли подобрать такое  $p$ . Тогда условие выполняется и мы построили пример с  $n$  зависимыми событиями, где любые  $n - 1$  событие независимы в совокупности.

## 18.8 Задача 8

**Условие:** Прямоугольная таблица заполнена нулями и единицами. В таблице  $3n$  столбцов, в каждой строке ровно  $n$  единиц, все строки различны. Известно, что для любых двух строк найдется такой столбец, в котором в данных строках стоят единицы.

- a) Докажите, что вероятность того, что случайно выбранная строка из  $n$  единиц и  $2n$  нулей входит в такую таблицу, не больше  $\frac{1}{3}$ .
- б) Докажите, что количество строк в такой таблице не больше  $\binom{3n-1}{n-1}$ .

**Решение:**

Давайте сначала переформулируем условие задачи. Сопоставим каждой строке  $n$  подмножество  $3n$  элементного множества - номера столбцов, где стоят единицы. Условие означает, что пересечение любых двух множеств непусто. Требуется доказать, что всего множеств (для простоты будем называть их особыми), обладающих таким свойством, не более трети от всего  $3n$  элементного множества.

Начнём с пункта а):

1. Заметим, что если разбить всё  $3n$  элементное множество на  $3n$  - непересекающихся подмножеств, то в каждой тройке будет не более одного особого множества, иначе есть 2 у которых пересечение пусто и тогда они не особые. Всего способов сделать это  $N = \binom{3n}{n} \cdot \binom{2n}{n} \cdot \frac{1}{3!}$
2. Теперь пусть у нас есть уже какое-то фиксированное  $n$  элементное множество, тогда способов выбрать 2 оставшихся  $n$  - элементных множества равно  $M = \binom{2n}{n} \cdot \frac{1}{2!}$ . Представим теперь список всевозможных разбиений на тройки нашего множества, в каждом пункте списка есть не более одного особого множества и причём каждое такое множество встретиться в списке не более  $M$  раз. Отсюда, всего особых множеств не более, чем  $\frac{N}{M} = \binom{3n}{n} \cdot \frac{1}{3}$ . Что и завершает доказательство пункта а).

Пункт б):

1. Так как мы поняли, что особое множество задаётся строкой в таблице и особых множеств не более трети от всех всех троек, на которые можно разбить  $3n$  элементное множество, то давайте приведём пример, когда достигается ровно треть. Такой пример как раз таки можно построить если выбрать все  $n$  элементные множества, куда входит один фиксированный элемент. Тогда этих множеств будет  $\binom{3n-1}{n-1} = \frac{1}{3} \cdot \binom{3n}{n}$ . То есть всего строк в таблице не более, чем  $\binom{3n-1}{n-1}$

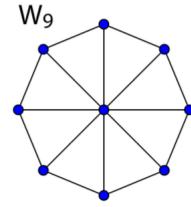
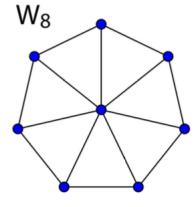
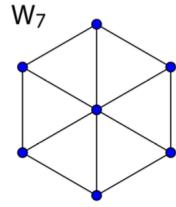
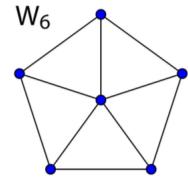
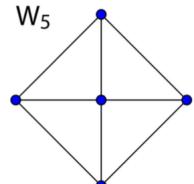
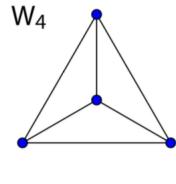
**Ч.Т.Д.**

## 19 Домашнее задание 16

(Илья)

### 19.1 Задача 1

**Условие:** Граф-колесо  $W_n$  ( $n > 3$ ) получается из простого цикла  $C_{n-1}$  добавлением  $n$ -ой вершины, смежной со всеми остальными. Примеры таких графов можно видеть на рисунке ниже.



Вычислите хроматический многочлен  $\chi_{w_n}(x)$ .

*Решение:*

1. Вершину, смежную со всеми другими вершинами, можно покрасить в один из  $x$  цветов, тогда останется покрасить цикл длиной  $n-1(C_{n-1})$ , причём использовать можно уже  $x-1$  цвет. Способов сделать это  $\chi_{C_{n-1}} = (x-2)^{n-1} + (-1)^{n-1}(x-2)$  (по задаче 1 из семинара)

Тогда ответом будет:  $x((x-2)^{n-1} + (-1)^{n-1}(x-2))$

**Ответ:**  $\chi_{w_n}(x) = x((x-2)^{n-1} + (-1)^{n-1}(x-2))$ .

## 19.2 Задача 2

*Условие:* Выбирается случайно и равновозможно 10 различных чисел из множества целых чисел от 0 до 29. Найдите математическое ожидание суммы этих чисел.

*Решение:*

1. Пусть  $\Omega = \{(a_1, a_2, \dots, a_{10}) | a_i \in \{0, 1, \dots, 29\}\}$  - вероятностное пространство, где  $a_i$  - это какое-то из 10 выбранных чисел и  $X$  - это случайная величина (по условию задачи - это сумма 10 выбранных чисел).

2. Давайте введём индикаторную функцию  $I_i = \begin{cases} 1, & \text{if } i \in \{a_1, a_2, \dots, a_{10}\} \\ 0, & \text{if } i \notin \{a_1, a_2, \dots, a_{10}\} \end{cases}$  Тогда  $X_s = 0 \cdot I_0 + 1 \cdot I_1 + \dots + 29 \cdot I_{29} = \sum_{k=0}^{29} k \cdot I_k$ .

3. Посчитаем наконец математическое ожидание  $E[X] = E[\sum_{k=0}^{29} k \cdot I_k] = \sum_{k=0}^{29} k \cdot P(I_k = 1)$ .

Посчитаем, чему равна вероятность того, что число  $k$  вошло в нашу десятку, это означает, что оно входит в какую-то из  $\binom{29}{9}$  десяток из  $\binom{30}{10}$  десяток. Значит,  $P(I_k = 1) = \frac{\binom{29}{9}}{\binom{30}{10}}$ , отсюда  $E[X] = \frac{\binom{29}{9}}{\binom{30}{10}}(0 + 1 + \dots + 29) = \frac{1}{3} \cdot \frac{0+29}{2} \cdot 30 = 29 \cdot 5 = 145$

**Ответ:** 145.

## 19.3 Задача 3

*Условие:* 3. Честную монету подбросили 100 раз. Докажите, что вероятность события «орлов выпало не менее 60 или не более 40» не превосходит  $1/4$ .

*Решение:*

1. Воспользуемся задачей номер 7 из семинара, только переобозначим орла за 1 и решку за 0. Тогда подкидывание 100 раз монетки порождает двоичную строку длиной 100.

Теперь положим  $n = 100$  в 7-ой задаче и получим, что вероятность события "количество единиц в строке отличается от 50 не меньше, чем на 10" не превосходит  $1/4$ . С учётом введённых обозначений это то же самое, что нам и нужно доказать(причём доказано и про 60 орлов, и про 40, потому что отличаться от 50 на 10 можно в обе стороны), поэтому **Ч.Т.Д.**

## 19.4 Задача 4

*Условие:* Каждое из чисел  $a_1, a_2, \dots, a_n$  выбирается случайно, равномерно и независимо среди чисел  $1, 2, \dots, n$ . Найдите математическое ожидание количества различных чисел среди  $a_1, a_2, \dots, a_n$ .

*Решение:*

- Пусть  $X$  - это случайная величина(в нашем случае количество различных чисел в наборе  $a_1, a_2, \dots, a_n$ )

Давайте введём индикаторную функцию  $I_k = \begin{cases} 1, & \text{если число } k \text{ новое} \\ 0, & \text{если число } k \text{ уже было} \end{cases}$

Тогда понятно, что  $X = \sum_{k=1}^n I_k$

- По линейности получаем, что  $E[X] = E\left[\sum_{k=1}^n I_k\right] = \sum_{k=1}^n P(I_k = 1)$

Давайте посчитаем  $P(I_k = 1)$ . То есть это вероятность того, что  $a_k$  - это новое число, а все  $a_1, a_2, \dots, a_{k-1}$  числа не равны  $a_k$ . Это событие состоит из многих независимых событий вида " $a_i (i \in [1, k-1])$  не равно  $a_k$ ". Тогда понятно, что вероятность одного такого события равна  $\frac{n-1}{n}$ , тогда из независимости следует, что вероятность  $k-1$  таких событий равна  $(\frac{n-1}{n})^{k-1} = (1 - \frac{1}{n})^{k-1} = P(I_k = 1)$ .

Тогда осталось посчитать  $\sum_{k=1}^n (1 - \frac{1}{n})^{k-1}$ . Ну а это просто сумма геометрической прогрессии, которая равна  $\frac{1 \cdot ((1 - \frac{1}{n})^n - 1)}{(1 - \frac{1}{n}) - 1} = n(1 - (1 - \frac{1}{n})^n)$

**Ответ:**  $n(1 - (1 - \frac{1}{n})^n)$ .

## 19.5 Задача 5

*Условие:* Дан неориентированный граф  $G$ (без петель и кратных ребер). Известно, что в  $G$  есть вершина степени не более 2022 и что при удалении произвольного собственного подмножества вершин  $G$  (и смежных им ребер) в полученном графе обязательно найдется вершина степени не более 2022. Докажите, что  $\chi(G) \leq 2023$ .

*Решение:*

- Буду доказывать индукцией по количеству вершин.

Предположение индукции: Я смогу покрасить граф, на котором выполняется условие, в 2023 цвета.

- База:  $n = 1$ . Понятно, что там предположение выполняется.(это подходит под условие, потому что лектор сказал, что можно удалять пустое подмножество, поэтому термин собственное подмножество в этой задаче немного некорректен)

- Шаг индукции:  $n \rightarrow n+1$ . Рассмотрим граф  $G$  на  $n+1$  вершине, на котором выполняется условие задачи. Значит в нём есть вершина степени не выше 2022. Пусть это вершина  $v$ .

Заметим, что такую вершину всегда можно правильно покрасить в 2023 цвета, потому что она имеет степень не выше 2022, то есть максимум у неё соседей 2022, а у нас 2023 цвета в запасе.

Давайте забудем про вершину  $v$  вместе со всеми рёбрами, идущими из неё.(потом вспомним о ней, по сути я её удаляю, но потом верну.) Получили граф  $G/v$ .

Рассмотрим непустое подмножество вершин  $X$  и посмотрим на граф  $(G/v)/X$  этот граф получается из  $G$  путём удаления собственного подмножества  $X \cup v$ . Тогда по условию в графе  $(G/v)/X$  выполняется условие.

И в графе  $G/v$  есть вершина степени не выше 2022, потому что этот граф получен удалением собственного подмножества -  $\{v\}$  из графа  $G$ . Значит граф  $G/v$  красится в 2023 цвета по предположению индукции. Теперь просто возвращаем вершину  $v$  на место и тоже красим её в один из 2023 цветов(это можно сделать всегда, было доказано ранее) и получаем граф  $G$  на  $n+1$  вершине, покрашенный правильно в 2023 цвета.

**Ч.Т.Д.**

## 19.6 Задача 6

*Условие:* В неориентированном графе (без петель и кратных ребер)  $n$  вершин и  $\frac{n}{2d}$  рёбер (то есть средняя степень вершины равна  $d$ ),  $d \geq 1$ . Докажите, что в графе есть независимое множество размера не меньше  $\frac{n}{2d}$ .

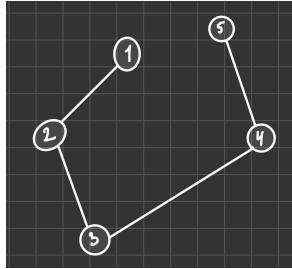
*Решение:*

- Давайте занумеруем все вершины графа числами от 1 до  $n$ . Будем рассматривать произвольную перестановку этих вершин и будем формировать независимое множество жадно.

Подробное описание жадного алгоритма(обходим перестановку слева направо):

- Включаем первую вершину из перестановки в множество.
- Каждую следующую вершину проверяем на смежность с уже добавленными. Если не соединена, то добавляем в множество, а если соединена, то не добавляем.

Приведём пример работы данного алгоритма.



Рассматриваем перестановку  $(1\ 2\ 3\ 4\ 5)$ , тогда по алгоритму мы сначала берём вершину 1 в наше множество. Теперь смотрим на вершину 2. Она соединена с вершиной 1, поэтому не берём. Теперь смотрим вершину 3. Она не соединена с вершиной 1, поэтому берём в наше множество. Смотрим вершину 4. Она соединена с вершиной 3, поэтому не берём. Смотрим вершину 5. Она не соединена ни с вершиной 3, ни с вершиной 1, поэтому включаем её в наше множество.

Итого получаем множество  $\{1, 3, 5\}$

Теперь посмотрим на другую перестановку, например  $(2\ 3\ 1\ 4\ 5)$ . Вершину 2 включаем в множество. Смотрим на вершину 3, она соединена с вершиной 2, поэтому не берём её. Смотрим на вершину 1, она соединена с вершиной 2, поэтому тоже не берём её в множество. Смотрим на вершину 4, она не соединена с вершиной 2, поэтому берём её в наше множество. Теперь смотрим на вершину 5, она соединена с вершиной 4, поэтому не берём её.

Итого получаем множество  $\{2, 4\}$

- Главная идея решения заключается в том, что мы смотрим на всевозможные перестановки и хотим понять, какой размер в среднем будет у нашего независимого множества, которое мы жадно сформируем. Если оно вдруг окажется больше нужного результата, то тогда мы можем воспользоваться леммой вероятностного метода, которая гласит, что если среднее значение равно  $m$ , то существует исход  $c \geq m$ .

Так вот, давайте посчитаем математическое ожидание размера независимого множества.

- Пусть  $X$  - случайная величина, размер независимого множества, построенного по перестановке. Так же введём индикаторную функцию  $I_k = \begin{cases} 1, & \text{если вершина } k \text{ вошла в множество} \\ 0, & \text{если не вошла} \end{cases}$

$$\text{Тогда } X = \sum_{k=1}^n I_k. \text{ По линейности } E[X] = E\left[\sum_{k=1}^n I_k\right] = \sum_{k=1}^n P(I_k = 1).$$

Осталось только посчитать вероятность  $P(I_k = 1)$ . Давайте сделаем это.

- Искомая вероятность - это вероятность того, что вершина  $k$  войдёт в наше независимое множество.

Пусть вершина  $k$  имеет степень  $\deg(k)$ , то есть она соединена с  $\deg(k)$  вершинами, которые имеют номера  $k_1, k_2, \dots, k_{\deg(k)}$ , тогда если вдруг в перестановке вершина  $k$  стоит первой среди  $k, k_1, k_2, \dots, k_{\deg(k)}$ , то по описанному выше алгоритму вершина  $k$  точно попадёт в наше независимое множество. Вероятность того, что вершина  $k$  окажется на первом месте среди своих смежных вершин равна  $\frac{\deg(k)!}{(\deg(k)+1)!} = \frac{1}{\deg(k)+1}$ . Отсюда,  $P(I_k = 1) \geq \frac{1}{\deg(k)+1}$

$$\text{Значит, } E[X] \geq \sum_{k=1}^n \frac{1}{\deg(k)+1}$$

- Пусть  $f(x) = \frac{1}{x+1}$ , тогда заметим, что рассматриваемая функция выпукла вниз при  $x \geq 0$ , так как её вторая производная  $f''(x) = \frac{2}{(x+1)^3} \geq 0$ .

Тогда для такой функции выполнено неравенство Йенсена:

$$\frac{f(x_1) + f(x_2) + \dots + f(x_n)}{n} \geq f\left(\frac{x_1 + x_2 + \dots + x_n}{n}\right)$$

Положим  $x_k = \deg(k)$ , тогда в левой части стоит  $\frac{E[X]}{n}$ , а справа стоит  $f(d) = \frac{1}{d+1}$ , так как средняя степень всех вершин это как раз-таки  $d$ .

Окончательно получим, что  $E[X] \geq \frac{n}{d+1} \geq \frac{n}{2d}$ . Значит, по лемме из лекции о вероятностном методе мы получаем, что существует такое независимое множество размером не менее  $\frac{n}{2d}$ .

**Ч.Т.Д.**

## 20 Домашнее задание 17

(Илья)

### 20.1 Задача 1

*Условие:* Докажите, что ребра полного графа на  $2^n$  вершинах можно раскрасить в два цвета так, чтобы не нашлось полного одноцветного подграфа на  $2n$  вершинах.

**Решение:**

1. Пусть  $X$  - случайная величина количества одноцветных подграфов на  $2n$  вершинах.

Введём индикаторную функцию  $I_k = \begin{cases} 1, & \text{если полный подграф на } 2n \text{ вершинах одноцветный} \\ 0, & \text{иначе} \end{cases}$

Тогда  $X = \sum_{k \in [K_{2n}]} I_k$ , тогда  $E[X] = \sum_{k \in [K_{2n}]} P(I_k = 1)$ . Так как мы красим рёбра и у нас есть 2 цвета, то вероятность

того, что граф покрасился в один цвет равна  $2 \cdot \left(\frac{1}{2}\right)^{\binom{2n}{2}} = \left(\frac{1}{2}\right)^{2n^2-n-1}$  (так как цвета у нас 2 и каждое ребро с вероятностью  $\frac{1}{2}$  может быть покрашено + у нас рёбер  $\binom{2n}{2}$ ).

2. Тогда  $E[X] = \binom{2^n}{2} \cdot \left(\frac{1}{2}\right)^{2n^2-n-1} = \frac{2^n(2^n-1)\dots(2^n-2n+1)}{2n(2n-1)\dots2\cdot1\cdot2^{2n^2-n-1}} \leq \frac{(2^n)^{2n}}{2^{2n-1}\cdot2^{2n^2-n-1}} = 2^{2-n}$

По словам лектора, мы считаем в этой задаче, что  $n > 1$ , поэтому при  $n \geq 2$  имеем, что  $E[X] < 1$ , а значит по лемме о вероятностном методе найдётся такая раскраска при которой все полные подграфы на  $2n$  вершинах будут разноцветны.

**Ч.Т.Д.**

### 20.2 Задача 2

*Условие:* Пусть  $f$  — случайная функция из  $n$ -элементного множества в  $100n$ -элементное (функция выбирается равномерно). Докажите, что

$$P[f \text{ инъективная}] \rightarrow 0 \text{ при } n \rightarrow \infty$$

**Решение:**

1. Посчитаем вероятность влоб. Всего функций из  $n$ -элементного множества в  $100n$ -элементное множество  $(100n)^n$ .

Можем посчитать, сколько из них инъективных. Так как мы считаем, что функция всюду определена (так как  $f: n \rightarrow 100n$  и на курсе мы договорились, что стрелочка означает, что функция всюду определена), то есть из каждого элемента в множестве из  $n$  элементов исходит стрелочка куда-то в  $100n$ -элементное множество, то всего таких функций будет  $\binom{100n}{n} \cdot n!$  (так как мы однозначно зафиксируем инъективную функцию выбрав какие-то  $n$  элементов из  $100n$ , но выбранные  $n$  элементов можно перетасовать и будут разные функции, поэтому надо домножить на перестановки из  $n$  элементов)

2. Итого, искомая вероятность имеет вид  $\frac{\binom{100n}{n} \cdot n!}{(100n)^n} = \frac{\frac{(100n)!}{99n!}}{(100n)^n} = \frac{(100n)!}{(99n)!(100n)^n}$

3. Да начнётся матан!!!! Посчитаем предел  $\lim_{n \rightarrow \infty} \frac{(100n)!}{(99n)!(100n)^n}$ . Воспользуемся формулой Стирлинга для оценки факториала (была на лекции).

Напомню:  $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$  при  $n \rightarrow \infty$

$$\text{Тогда } \lim_{n \rightarrow \infty} \frac{(100n)!}{(99n)!(100n)^n} = \lim_{n \rightarrow \infty} \frac{\sqrt{200\pi n} \left(\frac{100n}{e}\right)^{100n}}{\sqrt{2\cdot 99\pi n} \left(\frac{99n}{e}\right)^{99n} (100n)^n} = \sqrt{\frac{200}{198}} \lim_{n \rightarrow \infty} \left(\frac{\frac{100}{99}}{e}\right)^{99n} = \sqrt{\frac{200}{198}} \lim_{n \rightarrow \infty} \left(\frac{\left(1 + \frac{1}{99}\right)^{99}}{e}\right)^n.$$

Теперь последний fun fact с матана, что  $e > \left(1 + \frac{1}{n}\right)^n$  при любых натуральных  $n$ , а значит и при  $n = 99$  тоже, поэтому  $\frac{\left(1 + \frac{1}{99}\right)^{99}}{e} < 1$ . Значит искомый предел при  $n \rightarrow \infty$  равен 0

Ч.Т.Д.

### 20.3 Задача 3

*Условие:* Пусть  $X$  — случайная величина, для которой  $E[X^2] = E[X^3] = E[X^4]$ . Докажите, что если  $X$  принимает значение  $r \in \mathbf{R}$  с ненулевой вероятностью, то  $r = 0$  или  $r = 1$ .

**Решение:**

1. Рассмотрим вот такое выражение  $E[X^4] - E[X^3] + E[X^2] - E[X^3]$ . По условию оно равно 0. Распишем по линейности математического ожидания и получим, что  $E[X^4 - 2X^3 + X^2] = E[X^2(X^2 - 2X + 1)] = E[X^2(X - 1)^2] = 0$ .

2. **Лемма:** Если  $Y \geq 0$  и  $E[Y] = 0$ , то  $Y = 0$ .

**Доказательство:**

- Воспользуемся неравенством Маркова:  $P(Y \geq \alpha) \leq \frac{E[Y]}{\alpha} = 0 (\alpha > 0)$ . Значит,  $P(Y \geq \alpha) = 0$ .
- Получается, что вероятность того, что случайная величина положительная равна 0, но по условию  $Y \geq 0 \rightarrow Y = 0$ .

Ч.Т.Д.

3. Так как  $X^2(X - 1)^2 \geq 0$  и  $E[X^2(X - 1)^2] = 0$ , то по лемме из пункта 2 получим, что  $X^2(X - 1)^2 = 0$ . Значит,  $\begin{cases} X = 1 \\ X = 0 \end{cases}$ . То есть случайная величина принимает значение или 0, или 1.

Тогда вероятность того, что она примет какое-то значение, кроме 0 и 1, равна 0, а вероятность того, что она примет значение 1 ненулевая и вероятность того, что она примет значение 0 тоже ненулевая.

Отсюда и следует то, что требовалось доказать.

Ч.Т.Д.

### 20.4 Задача 4

*Условие:* Пусть  $X_i \in \{0, 1\}, i = 1, 2, \dots, n$  — независимые случайные величины, принимающие значения 0 и 1 с вероятностью  $\frac{1}{2}$ . Рассмотрим  $X = X_1 + X_2 + \dots + X_n$ . Докажите, что для любого  $C > 0$  существует некоторое  $\gamma = O(\sqrt{n \cdot \log n})$  такое, что

$$P[X \geq \frac{n}{2} + \gamma] \leq \frac{1}{n^C}$$

**Решение:**

Уточняется.

### 20.5 Задача 5

*Условие:* Пусть  $V = \{1, 2, \dots, n\}$ . Гиперребром на  $V$  называется любое непустое подмножество  $S \subseteq V$ . Гиперграфом  $H$  с множеством вершин  $V$  называется произвольное семейство гиперребер  $S_1, S_2, \dots, S_m$  на  $V$ . Мы хотим раскрасить вершины гиперграфа в два цвета: 0 и 1, — чтобы каждое гиперребро было раскрашено как можно «равномернее». Для данной раскраски назовем пестротой  $disc(S_i)$  гиперребра  $S_i$  модуль разности числа вершин цвета 0 и числа вершин цвета 1 в  $S_i$ . Пестротой гиперграфа  $H$  назовем  $disc(H) = \max_{i=1,2,\dots,m} disc(S_i)$ . Докажите, что для всякого гиперграфа  $H$  с множеством вершин  $V$  существует такая раскраска, что  $disc(H) = O(\sqrt{n \cdot \log m})$ .

**Решение:**

Уточняется.

## 21 Домашнее задание 18

(Илья)

### 21.1 Задача 1

Условие: Пусть  $F$  и  $G$  — производящие функции. Докажите равенство  $\left(\frac{F}{G}\right)' = \frac{F'G - FG'}{G^2}$

Доказательство:

1.  $\left(\frac{F}{G}\right)' = (F \cdot \frac{1}{G})'$  Это можно расписать по правилу Лейбница(на лекции доказали, что для производящих функций оно тоже верно). Поэтому  $(F \cdot \frac{1}{G})' = F' \cdot \frac{1}{G} + F \cdot (\frac{1}{G})'$
2. По задаче 5 с семинара имеем, что  $(\frac{1}{G})' = -\frac{G'}{G^2} \implies F' \cdot \frac{1}{G} + F \cdot (\frac{1}{G})' = \frac{F'}{G} - \frac{FG'}{G^2}$
3. По задаче 4 с семинара<sup>1</sup> имеем, что  $\frac{F'}{G} - \frac{FG'}{G^2} = \frac{F'G - FG'}{G^2}$

Ч.Т.Д.

### 21.2 Задача 2

Условие: Рассмотрим класс производящих функций, у которых коэффициент при  $x^0$  равен нулю. Для каких производящих функций  $F(x) = f_1x + f_2x^2 + \dots$  из этого класса существует производящая функция  $G(x)$  из этого класса, такая что  $F(G(x)) = x$ ?

Решение:

1. Пусть  $G(x) = g_1x + g_2x^2 + \dots$ . Тогда композиция  $F(G(x))$  определяется как  $f_1(g_1x + g_2x^2 + \dots) + f_2(g_1x + g_2x^2 + \dots)^2 + \dots$
2. Посчитаем коэффициент при  $x^1$ : По условию он должен быть равен 1, поэтому  $f_1g_1 = 1 \implies g_1 = \frac{1}{f_1} (f_1 \neq 0)$   
Посчитаем коэффициент при  $x^2$ : По условию все коэффициенты при более высоких степенях должны быть равны 0, поэтому  $f_1g_2 + f_2g_1 = 0 = f_1g_2 + \frac{f_2}{f_1} \implies g_2 = -\frac{f_2}{f_1}$   
Посчитаем коэффициент при  $x^k$ , но уже понятно, что зная все  $f_i$  и  $g_i (i \leq k-1)$  я смогу приравнивая найти коэффициент  $g_k$ . (это можно более строго показать при помощи индукции, но надеюсь, что и так понятно)
3. Тогда при условии, что  $f_1 \neq 0$  мы сможем посторить такой  $G(x)$ , что  $F(G(x)) = x$ .

Ответ:  $F(x) = f_1x + f_2x^2 + \dots (f_1 \neq 0)$

### 21.3 Задача 3

Условие: С помощью производящих функций вычислите сумму  $1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2} + 3 \cdot \binom{n}{3} + \dots + n \cdot \binom{n}{n}$

Решение:

1. Рассмотрим функцию  $(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \dots + \binom{n}{n}x^n$   
Тогда  $((1+x)^n)' = n(1+x)^{n-1} = 1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2}x + \dots + n \cdot \binom{n}{n}x^{n-1}$   
Так как при  $n=1$  должно выйти  $1 \cdot \binom{1}{1}$ , то надо домножить функцию на  $x$ :  $nx(1+x)^{n-1} = 1 \cdot \binom{n}{1}x + 2 \cdot \binom{n}{2}x^2 + \dots + n \cdot \binom{n}{n}x^n$

Тогда по утверждению с лекции<sup>2</sup>: Поделим на  $1-x$ , чтобы перейти к сумме и получим  $\frac{nx(1+x)^{n-1}}{1-x}$

2. Посчитаем  $a_n = \frac{(nx(1+x)^{n-1})^{(n)}}{n!}$ . Пусть  $x+1=y$ , тогда  $x=y-1 \implies \frac{nx(1+x)^{n-1}}{1-x} = \frac{n(y-1)y^{n-1}}{2-y} = \frac{ny^n}{2-y} - \frac{ny^{n-1}}{2-y} = n\left(\frac{(y+1)^n}{1-x} - \frac{(y+1)^{n-1}}{1-x}\right) = n\left(\frac{1}{1-x} + \frac{\binom{n}{1}x}{1-x} + \frac{\binom{n}{2}x^2}{1-x} + \dots + \frac{\binom{n}{n}x^n}{1-x} - \left(\frac{1}{1-x} + \frac{\binom{n-1}{1}x}{1-x} + \frac{\binom{n-1}{2}x^2}{1-x} + \dots + \frac{\binom{n-1}{n-1}x^{n-1}}{1-x}\right)\right)$   
Давайте рассмотрим функцию  $\frac{1}{1-x} = 1 + x^2 + x^3 + \dots$  и понятно, что  $a_n$  здесь это 1, потому что  $\frac{(\frac{1}{1-x})^{(n)}}{n!} = 1$ (легко проверяется руками). Заметим, что домножение функции  $\frac{1}{1-x}$  на  $x^k$  всего лишь делает  $b_{n-k}$  коэффициент функции  $\frac{1}{1-x}$   $b_n$  коэффициентом функции  $\frac{x^k}{1-x}$

<sup>1</sup>Там написано, что А и С должны быть обратимыми, но это необязательное условие: уточнял у лектора и семинариста

<sup>2</sup>Пусть  $A(x) \rightarrow (a_0, a_1, a_2, a_3, \dots)$

$S = (a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots, \sum_{k=0}^n a_k, \dots)$ . Тогда  $S(x) = \frac{A(x)}{1-x}$ .

Поэтому  $a_n = n(b_n + \binom{n}{1}b_{n-1} + \binom{n}{2}b_{n-2} + \dots + \binom{n}{n}b_0 - (b_n + \binom{n-1}{1}b_{n-1} + \dots + \binom{n-1}{n-1}b_0)) = n(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} - (\binom{n-1}{0} + \binom{n-1}{1} + \dots + \binom{n-1}{n-1})) = n(2^n - 2^{n-1}) = 2^{n-1}n$

**Ответ:**  $2^{n-1}n$

## 21.4 Задача 4

*Условие:* С помощью производящих функций найдите и докажите формулу для суммы

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + (n-1) \cdot n$$

**Решение:**

1. Рассмотрим функцию  $F(x) = x^2 + x^3 + x^4 + \dots = \frac{x^2}{1-x}$ . Тогда  $(F(x))'' = 1 \cdot 2 + 2 \cdot 3x + 3 \cdot 4x^2 + \dots = \frac{2x^2}{(1-x)^3}$

Так как при  $n = 2$  значение  $1 \cdot 2$ , то надо домножить на  $x^2$  и получим  $\frac{2x^2}{(1-x)^3}$

Чтобы перейти к сумме надо поделить на  $1-x$  и получим:  $\frac{2x^2}{(1-x)^4}$

2. Давайте рассмотрим функцию  $H(x) = \frac{2}{(1-x)^4}$ . Мы искали  $h_n$  на лекции - это  $\frac{(n+1)(n+2)(n+3)}{3}$

Как я говорил в задаче 3, функция  $\frac{2x^2}{(1-x)^4}$  имеет  $n$ -ый коэффициент, равный  $h_{n-2} = \frac{n(n-1)(n+1)}{3}$

**Ответ:**  $\frac{n(n-1)(n+1)}{3}$

## 21.5 Задача 5

*Условие:* Пусть у нас есть неограниченное количество монет по 2 и 5 рублей, а также 4 монеты по 1 рублю. Обозначим через  $a_n$  число способов набрать  $n$  рублей с помощью имеющихся монет (монеты одинакового достоинства считаются одинаковыми). Выразите производящую функцию для последовательности  $a_n$  в виде отношения многочленов.

**Решение:**

1. Пусть Производящая функция для выдачи монет номиналом 2 рубля - это  $G(x) = 1 + x^2 + x^4 + x^8 + \dots$ , 5 рублей - это  $H(x) = 1 + x^5 + x^{10} + x^{15} + x^{20} + \dots$ , 1 рубль - это  $L(x) = 1 + x + x^2 + x^3 + x^4$ . Тогда  $a_n = H(x)L(x)G(x) = \frac{x^5-1}{(1-x^2)(1-x^5)(x-1)} = \frac{1}{(x^2-1)(x-1)} = \frac{1}{(x-1)^2(x+1)}$

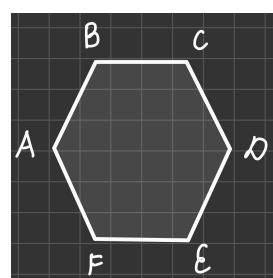
**Ответ:**  $\frac{1}{(x-1)^2(x+1)}$

## 21.6 Задача 6

*Условие:* Лягушка прыгает по вершинам правильного шестиугольника  $ABCDEF$  начиная из вершины  $A$ . На каждом прыжке лягушка прыгает в одну из соседних вершин. Найдите производящую функцию для последовательности  $a_n$ , где  $a_n$  равно числу способов оказаться в вершине  $C$  через  $n$  шагов.

**Решение:**

1. Давайте сделаем рисунок.



Пусть  $a_n, c_n, e_n, b_n, f_n, d_n$  - количество способов попасть из вершины A в A,C,E,B,F и D соответственно (то есть я ищу  $c_n$ ). Понятно, что  $c_n = e_n$  в силу симметрии.

Сделаем пару наблюдений.

$$\begin{cases} c_n = b_{n-1} + d_{n-1} \\ a_n = b_{n-1} + f_{n-1} \\ d_n = c_{n-1} + e_{n-1} = 2c_{n-1} \\ f_n = a_{n-1} + e_{n-1} = a_{n-1} + c_{n-1} \\ b_n = a_{n-1} + c_{n-1} \end{cases}$$

Отсюда,  $a_n = b_{n-1} + f_{n-1} = 2a_{n-2} + 2c_{n-2} \Rightarrow c_n = b_{n-1} + d_{n-1} = 3c_{n-2} + a_{n-2} \Rightarrow c_{n+2} = 3c_n + 2a_{n-2} + 2c_{n-2} \Rightarrow c_{n+4} = 3c_{n+2} + 2c_n + 2a_n = 3c_{n+2} + 2c_n + 2(c_{n+2} - 3c_n) = 5c_{n+2} - 4c_n$

Итого,  $c_{n+4} = 5c_{n+2} - 4c_n$ . Выпишем первые очевидные значения рекурренты:  $c_0 = 0, c_1 = 0, c_2 = 1, c_3 = 0$

Отсюда можно сделать вывод, что для любых нечётных  $n$   $c_n = 0$ .

2. Пусть  $C(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \dots + c_nx^n + \dots$  - производящая функция последовательности  $c_n$ .

Домножим наше рекуррентное уравнение на  $x^{n+4}$  и получим, что  $c_{n+4}x^{n+4} = 5x^2c_{n+2}x^{n+2} - 4x^4c_nx^n$

Просуммируем по всем  $n \geq 0$  и получим, что  $(c_4x^4 + c_5x^5 + \dots + c_nx^n + \dots) = 5x^2(c_2x^2 + c_3x^3 + \dots + c_nx^n + \dots) - 4x^4(c_0 + c_1x + c_2x^2 + \dots + c_nx^n + \dots)$

Итого,  $C(x) - c_3x^3 - c_2x^2 - c_1x - c_0 = 5x^2(C(x) - c_1x - c_0) - 4x^4C(x)$

С учётом того, что  $c_0 = 0, c_1 = 0, c_2 = 1, c_3 = 0$  имеем, что  $C(x) - x^2 = 5x^2C(x) - 4x^4C(x) \Rightarrow C(x) = \frac{x^2}{4x^4 - 5x^2 + 1}$

**Ответ:**  $\frac{x^2}{4x^4 - 5x^2 + 1}$

## 22 Домашнее задание 19

(Илья)

### 22.1 Задача 1

**Условие:** Найдите производящие функции и явные выражения для элементов последовательностей, заданных рекуррентными формулами  $n \geq 0$ :

a)  $2a_{n+3} = -9a_{n+2} - 12a_{n+1} - 5a_n; a_0 = 5, a_1 = -12, a_2 = 28;$

b)  $a_{n+2} = -2a_{n+1} + 8a_n + 2^n; a_0 = 1, a_1 = 0;$

**Решение:**

1. Пункт а). Пусть  $C(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots$  - производящая функция последовательности  $a_n$ .

Домножим обе части уравнения на  $x^{n+3}$  и получим, что  $2a_{n+3}x^{n+3} = -9xa_{n+2}x^{n+2} - 12x^2a_{n+1}x^{n+1} - 5x^3a_nx^n$

Просуммируем по всем  $n \geq 0$  и получим, что  $2(C(x) - a_0x^0 - a_1x^1 - a_2x^2) = -9x(C(x) - a_0x^0 - a_1x^1) - 12x^2(C(x) - a_0x^0) - 5x^3C(x)$

Отсюда,  $C(x)(2 + 9x + 12x^2 + 5x^3) = 45x - 108x^2 + 60x^2 + 10 - 24x + 56x^2$

Значит,  $C(x) = \frac{8x^2 + 21x + 10}{5x^3 + 12x^2 + 9x + 2}$

Заметим, что  $C(x) = \frac{1}{(x+1)^2} + \frac{8}{5x+2}$

Теперь надо посчитать  $a_n = \frac{C^{(n)}(0)}{n!}$

Пусть  $A(x) = \frac{1}{(x+1)^2}$  и  $B(x) = \frac{8}{5x+2}$

Найдём  $A^{(n)}(x)$ :

- Заметим, что  $A'(x) = -2(x+1)^{-3}$

- $A''(x) = 6(x+1)^{-4}$

- $A'''(x) = -24(x+1)^{-5}$

Понятно, что  $A^{(n)}(x) = (-1)^n(n+1)!(x+1)^{-(n+2)}$

Теперь найдём  $B^{(n)}(x)$ :

- $B'(x) = 8(-1(5x+2)^{-2}5^1)$

- $B''(x) = 8(-1)(-2)(5x+2)^{-3}5^2$

Понятно, что  $B^{(n)}(x) = 8(-1)^n n!(5x+2)^{-(n+1)}5^n$

Тогда  $C^{(n)}(x) = 8(-1)^n n!(5x+2)^{-(n+1)}5^n + (-1)^n(n+1)!(x+1)^{-(n+1)}$

$$\text{Значит, } a_n = \frac{8(-1)^n n!(2)^{-(n+1)}5^n + (-1)^n(n+1)!(1)^{-(n+2)}}{n!} = 2^{-n}(4(-5)^n + (-2)^n(n+1))$$

2. Пусть  $C(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots$  - производящая функция последовательности  $a_n$ .

Домножим обе части уравнения на  $x^{n+2}$  и получим, что  $a_{n+2}x^{n+2} = -2xa_{n+1}x^{n+1} + 8x^2a_nx^n + x^22^n x^n$

Просуммируем по всем  $n \geq 0$  и подставим  $a_0, a_1$  и получим, что  $C(x) - 1 = -2x(C(x) - 1) + 8x^2C(x) + x^2(1 + 2x + 2^2x^2 + 2^3x^3 + \dots)$

Вспомним, что  $1 + 2x + 2^2x^2 + 2^3x^3 + \dots = \frac{1}{1-2x}$

Получим, что  $C(x)(1 + 2x - 8x^2) = 1 + 2x + \frac{x^2}{1-2x}$

$$C(x) = \frac{1-3x^2}{(1-2x)(1+2x-8x^2)}$$

$$\text{Заметим, что } C(x) = \frac{1}{12(2x-1)^2} - \frac{5}{9(2x-1)} + \frac{13}{36(4x+1)}$$

$$\text{Пусть } A(x) = \frac{1}{12(2x-1)^2}$$

Тогда, посчитав первые пару её производных, понимаем, что  $A^{(n)}(x) = \frac{1}{12}(-1)^n(n+1)!(2x-1)^{-(n+2)}2^n$

Пусть  $B(x) = \frac{5}{9(2x-1)}$ , тогда  $B^{(n)}(x) = \frac{5}{9}2^n(-1)^n n!(2x-1)^{-(n+1)}$

Пусть  $D(x) = \frac{13}{36(4x+1)}$ , тогда  $D^{(n)}(x) = \frac{13}{36}(-1)^n 4^n(4x+1)^{-(n+1)}n!$

Тогда  $a_n = \frac{C^{(n)}(0)}{n!} = \frac{13}{36}(-1)^n 4^n(1)^{-(n+1)} + \frac{5}{9}2^n(-1)^n(-1)^{-(n+1)} + \frac{1}{12}(-1)^n(n+1)(-1)^{-(n+2)}2^n = \frac{1}{36}2^n(13(-2)^n + 3n + 23)$

**Ответ:**  $\begin{cases} a) C(x) = \frac{8x^2+21x+10}{5x^3+12x^2+9x+2}, a_n = 2^{-n}(4(-5)^n + (-2)^n(n+1)) \\ b) C(x) = \frac{1-3x^2}{(1-2x)(1+2x-8x^2)}, a_n = \frac{1}{36}2^n(13(-2)^n + 3n + 23) \end{cases}$

## 22.2 Задача 2

*Условие:* Используя производящую функцию для чисел Фибоначчи, докажите тождество ( $n \geq 1$ ):

$$F_1 + F_3 + F_5 + \dots + F_{2n-1} = F_{2n} - 1$$

**Решение:**

1. По задаче номер 2, доказанной на семинаре имеем, что  $F_0 + F_1 + F_2 + \dots + F_n = F_{n+2} - 1$

Заметим, что  $F_1 + F_3 + F_5 + F_7 + \dots + F_{2n-1} = F_1 + F_1 + F_2 + F_3 + F_4 + F_5 + \dots + F_{2n-3} + F_{2n-2} = F_0 + F_1 + F_2 + F_3 + F_4 + \dots + F_{2n-2}$

Заметим, что мы получили сумму чисел фибоначчи от 0 до  $2n-2$ , тогда подставим вместо  $n$  в задаче семинара число  $2n-2$  и получим, что  $F_0 + F_1 + F_2 + F_3 + F_4 + \dots + F_{2n-2} = F_{2n-2+2} - 1 = F_{2n} - 1$

На семинаре задача 2 решалась через производящую функцию.

**Ч.Т.Д.**

## 22.3 Задача 3

*Условие:* Пусть  $A(x)$  — производящая функция последовательности  $(0, 1, 2, \dots)$ . Известно, что  $A(x) = \frac{P(x)}{Q(x)}$  где  $P(x), Q(x)$  — ненулевые многочлены с комплексными коэффициентами, не имеющие общих корней. Пусть  $\deg Q = k$ . Докажите, что, начиная с некоторого номера  $n$ , выполняется линейное рекуррентное соотношение:

$$a_{n+k} = c_1a_{n+k-1} + c_2a_{n+k-2} + \dots + c_ka_n.$$

**Решение:**

1. Пусть  $A(x) = \frac{P(x)}{Q(x)}$  и  $Q(x) = 1 - c_1x^1 - c_2x^2 - \dots - c_kx^k$ ,  $\deg P < k$ .

Выразим  $P(x) = A(x) \cdot Q(x)$  и так как  $\deg(P) < k$ , то  $p_n = 0 \forall n \geq k$ . Распишем  $p_n$  по определению и получим, что  $p_n = \sum_{i=0}^n a_{n-i}q_i = 0$ ;

Разобьём теперь полученную сумму на две:  $p_n = \sum_{i=0}^k a_{n-i}q_i + \sum_{i=k+1}^n a_{n-i}q_i = 0$  Так как  $Q(x)$  задан, то я могу понять, чему равны эти суммы. Для первой выполняется, что:  $q_0 = 1, q_i = -c_i \quad \forall i \neq 0$  Так же понятно, что вторая сумма равна 0, так как  $\deg(Q) = k$

Отсюда,  $p_n = a_n + \sum_{i=1}^k a_{n-i} \cdot (-c_i) = a_n - \sum_{i=1}^k a_{n-i}c_i = 0$

2. Распакуем наше выражение для  $p_n$  и получим, что

$$a_n - \sum_{i=1}^k a_{n-i}c_i = a_n - a_{n-1}c_1 - a_{n-2}c_2 - \dots - a_nc_k = 0$$

Отсюда и получаем результат, что  $a_n = a_{n-1} \cdot c_1 + a_{n-2} \cdot c_2 + \dots + a_{n-k} \cdot c_k$

**Ч.Т.Д.**

## 22.4 Задача 4

*Условие:* Рациональна ли производящая функция последовательности последовательности  $(a_0, a_1, a_2, \dots)$ , где

a)  $a_k = k^{2023}$

b)  $a_k = \frac{1}{(k+1)^2}$

**Решение:**

1. Давайте возьмём производящую функцию вот такой последовательности  $(1, 1, 1, \dots) = \frac{1}{1-x}$  Это рациональная функция. Теперь будем проводить одну и ту же операцию до тех пор, пока не получим последовательность из условия -  $(0^{2023}, 1^{2023}, \dots)$ . Будем брать производную и умножать на результат на  $x$ . Взятие производной от рациональной функции не меняет рациональной и домножение на  $x$  тоже.

Тогда после первых итераций получим:

$$(1, 1, 1, \dots) = \frac{1}{1-x}$$

$$(0, 1, 1, 1, \dots) = \frac{x}{1-x}$$

$$(0, 1, 2, \dots) = x \left( \frac{x}{1-x} \right)'$$

$$(1^2, 2^2, 3^2, 4^2, \dots) = (x \left( \frac{x}{1-x} \right)')'$$

$$(0^2, 1^2, 2^2, 3^2, \dots) = x(x \left( \frac{x}{1-x} \right)')'$$

Понятно, что тогда мы дойдём до 2023 степени и получим рациональную производящую функцию.

2. Из матана мы знаем, что ряд Тейлора функции  $\ln(\frac{1}{1-x})$  характеризует последовательность  $(0, \frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \dots)$

На семинаре так же говорилось, что в производящие функции наследуют некоторые свойства аналитических функций, в том числе и нерациональность. Так как  $\ln(\frac{1}{1-x})$  нерационален, то и формальный степенной ряд  $0x^0 + \frac{1}{1}x^1 + \frac{1}{2}x^2 + \dots$  тоже.

Теперь посмотрим на задачу 8 с семинара и предположим, что наша функция из условия рациональна, то есть  $\frac{1}{1^2}x^0 + \frac{1}{2^2}x^1 + \dots$  рациональная, тогда и  $0 + \frac{1}{1^2}x + \frac{1}{2^2}x^2 + \dots$  тоже рациональна. Тогда рассмотрим её Адамарово произведение с функцией  $0 + 1x^1 + 2x^2 + \dots = \frac{x}{(1-x)^2}$  Получаем ряд  $0 \cdot 0 + 1 \cdot \frac{1}{1^2} + 2 \cdot \frac{1}{2^2} + \dots$  и получаем, гармонический ряд из первого замечания, который, как мы выяснили, не рациональный. Противоречие с задачей номер 8.

Значит, изначальное предположение было неверным, то есть функция  $\frac{1}{1^2}x^0 + \frac{1}{2^2}x^1 + \dots$  нерациональна.

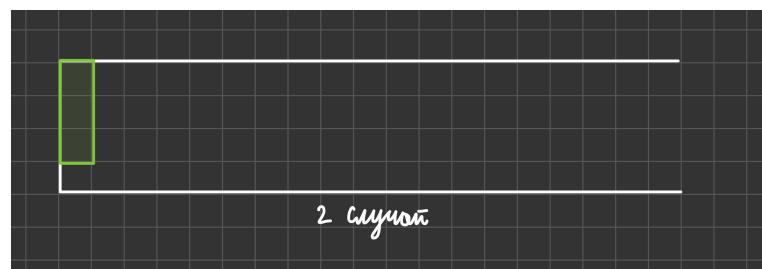
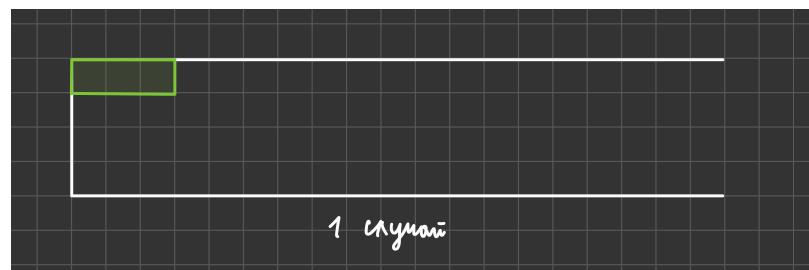
**Ответ:**  $\begin{cases} \text{а) да} \\ \text{б) нет} \end{cases}$

## 22.5 Задача 5

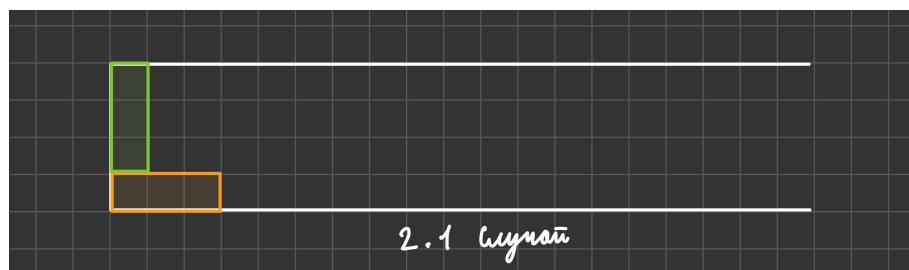
*Условие:* Обозначим через количество способов разрезать прямоугольник  $4 \times n$  на прямоугольники  $1 \times 3$  (как горизонтальные, так и вертикальные). Будем считать, что  $d_0 = 1$ . Найдите производящую функцию последовательности  $(d_0, d_1, d_2, \dots)$ . Представьте её в виде отношения многочленов.

**Решение:**

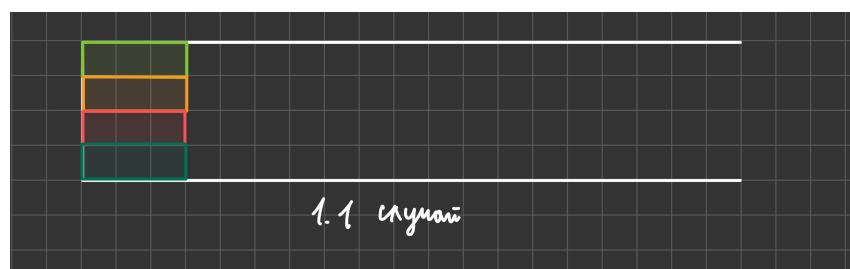
Первую дощечку можно поставить 2 способами.



Теперь следующую дощечку в 2 случае можно поставить однозначно.

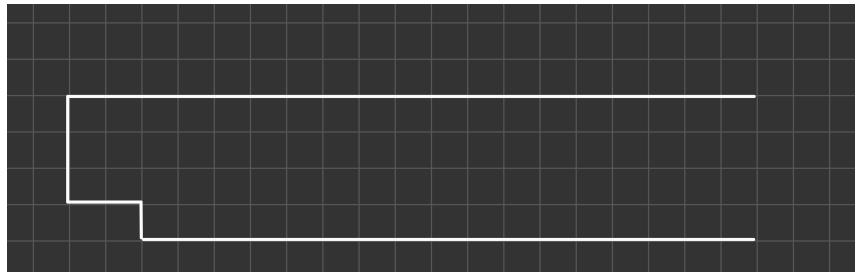


Следующую дощечку в 1 случае можно поставить вертикально и получить симметричный случай с 2.1, а можно поставить дощечку горизонтально и получить затем однозначное замощение.

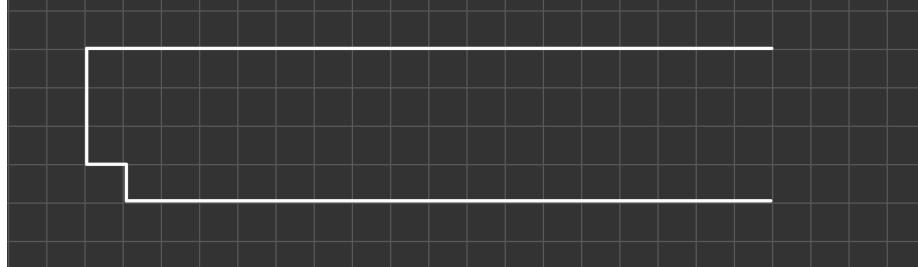


Итого, получаем, что мы свели в случае 1.1 к замощению прямоугольника размером  $4$  на  $n-3$ , количество способов сделать это  $d_{n-3}$ .

Обозначим за  $c_n$  - количество способов замостить вот такую фигуру



Обозначим за  $b_n$  -количество способов замостить вот такую фигуру:



Судя по рисункам, можно понять, что в  $d_n = d_{n-3} + 2c_{n-1}$

Ещё мы можем понять, что  $c_n = b_{n-1} + c_{n-3}$  и  $b_n = d_{n-1} + b_{n-3}$

Итого имеем, что  $\begin{cases} d_n = d_{n-3} + 2c_{n-1} \\ c_n = b_{n-1} + c_{n-3} \\ b_n = d_{n-1} + b_{n-3} \end{cases}$

Пусть  $B(x), C(x), D(x)$  - производящие функции  $b_n, c_n, d_n$  соответственно. Перепишем систему уравнений в эквивалентном виде:

$$\begin{cases} d_{n+3} = d_n + 2c_{n+2} \\ c_{n+3} = b_{n+2} + c_n \\ b_{n+3} = d_{n+2} + b_n \end{cases}$$

Домножим все уравнения на  $x^{n+k}$ , где  $k$  - порядок рекурренты и просуммируем по всем  $n \geq 0$  и получим, что

$$\begin{cases} D(x) - d_0x^0 - d_1x^1 - d_2x^2 = x^3D(x) + 2x(C(x) - c_0x^0 - c_1x^1) \\ C(x) - c_0x^0 - c_1x^1 - c_2x^2 = x(B(x) - b_0x^0 - b_1x^1) + x^3C(x) \\ B(x) - b_0x^0 - b_1x^1 - b_2x^2 = x(D(x) - d_0x^0 - d_1x^1) + x^3B(x) \end{cases}$$

Легко посчитать руками, что  $c_0 = 0, c_1 = 0, c_2 = 1, d_0 = 1, d_1 = 0, d_2 = 0, b_0 = 0, b_1 = 1, b_2 = 0$

Тогда имеем систему:

$$\begin{cases} D(x) - 1 = x^3D(x) + 2xC(x) \\ C(x) - x^2 = x(B(x) - x) + x^3C(x) \\ B(x) - x = x(D(x) - 1) + x^3B(x) \end{cases}$$

Из первого уравнения  $C(x) = \frac{D(x)(1-x^3)-1}{2x}$

Подставим во второе уравнение и получим, что  $B(x) = \frac{D(x)(1-x^3)^2-1+x^3}{2x^2}$

Подставим теперь в последнее уравнение и получим, что

$$D(x) = \frac{-(1-x^3)^2}{2x^3-(1-x^3)^3}$$

**Ответ:**  $D(x) = \frac{-(1-x^3)^2}{2x^3-(1-x^3)^3}$

## 23 Домашнее задание 20

(Илья)

## 23.1 Задача 1

**Условие:** Два игрока по очереди последовательно пишут 10 (не обязательно различных) цифр слева направо. Первый игрок выигрывает, если полученное число (после отбрасывания ведущих нулей) не делится на 7. В противном случае выигрывает второй игрок. У кого из игроков есть выигрышная стратегия?

**Решение:**

1. Давайте вспомним признак делимости на 7: число делится на 7 тогда и только тогда, когда разность числа, полученного убиением разряда единиц и удвоенного числа единиц делится на 7.

Отсюда высвечивается стратегия второго игорока, потому что 10 - чётное число, поэтому последний ход делает второй игрок.

2. Достаточно проверить, что последняя цифра, умноженная на 2, может давать всевозможные остатки по модулю 7.

$$0 \rightarrow 0 \equiv 0$$

$$1 \rightarrow 2 \equiv 2$$

$$2 \rightarrow 4 \equiv 4$$

$$3 \rightarrow 6 \equiv 6$$

$$4 \rightarrow 8 \equiv 1$$

$$5 \rightarrow 10 \equiv 3$$

$$6 \rightarrow 12 \equiv 5$$

Получили всевозможные остатки, которые может давать число из 9 цифр при делении на 7, значит второй просто ставит такую цифру, чтобы в итоге выражение из признака делимости на 7 было сравнимо с 0 по модулю 7.

**Ответ:** У второго игрока.

## 23.2 Задача 2

**Условие:** На доске написано число 60. За один ход разрешается уменьшить число на любой из его целых положительных делителей (в том числе на единицу или на само это число). Если при этом получается нуль, игрок проиграл. У кого из игроков есть выигрышная стратегия?

**Решение:**

1. Давайте покажем по индукции такой факт. Если начинать игру с нечётной позиции (то есть с нечётного числа), то выигрывает второй игрок, иначе - первый.

Пусть мы стартуем с позиции  $n > 0$ . Будем идти индукцией с конца.

**База:** ну если  $n = 1$ , то понятно, что первому нужно сделать ход и он обязан вычесть 1 и получить 0, то есть проиграть.

Если же  $n = 2$ , то первый может просто вычесть 1 и привести второго к 1, откуда он обязан пойти в 0 и проиграть.

**Переход:**  $k(k \leq n - 1) \rightarrow n$ . (полная индукция)

Предположим, что мы сейчас находимся в позиции  $n$  и у нас 2 варианта:

если  $n$  - чётное, то первый игрок может сделать из этой позиции нечётное, сделав вычитание 1, и по предположению индукции тогда второй игрок проиграет.

Если же  $n$  - нечётное, то у этого числа только нечётный делители, поэтому, вычитая любой из них, он получит чётное число и по предположению индукции второй игрок тогда там выиграет.

**Ч.Т.Д.**

Так как 60 - чётное число, то выигрывает первый игрок.

**Ответ:** У первого игрока.

## Задача 3

**Условие:** Есть две коробки с  $m$  и  $n$  монетами,  $m, n > 0$ . Обозначим эту позицию через  $(m, n)$ . Два игрока играют в игру, делая ходы по очереди. На каждом ходу разрешается убрать все монеты из одной из коробок, а монеты из второй коробки распределить между двумя этими коробками так, чтобы в каждой было хотя бы по одной монете. Проигрывает тот, кто не может сделать ход, т. е. оказывается в позиции  $(1, 1)$ . Опишите все  $P$ -позиции данной игры.

**Решение:**

1. Докажем по индукции такой факт, что если мы начинаем игру с позиции, где есть хотя бы одна чётная куча(то есть куча с чётным числом монет в ней), то тогда выигрывает первый игрок, а если начинать с двух куч с нечётным числом монет в них, то выигрывает второй.

Будем вести полную индукцию с конца по сумме монет в кучах.

**База:** Если кучи (1,2), то тогда первый оставляет двойку и расскладывает её на (1,1) и выигрывает, а если мы начинаем с (1,1), то тогда проигрывает первый игрок сразу.

**Переход:**  $k(k \leq n - 1) \rightarrow n$ (полная индукция)

Рассмотрим ситуацию, когда у нас есть две кучи монет суммой  $n$  и хотя бы одна из них чётная, тогда первый игрок может взять чётное число и разложить его на два нечётных, при этом сумма камней уменьшится хотя бы на 1, поэтому можем воспользоваться предположением индукции и получим, что проиграет второй.

Если же мы начинаем с позиции с обеими нечётными кучами, то тогда первый может оставить любую нечётную кучу(если она не 1, конечно, но этот случай проверен в базе) и разложить на чётную и нечётную кучи. Мы опять уменьшили сумму минимум на 1 и можем воспользоваться предположением индукции, получив, что проиграет второй, то есть выиграет первый.

Тогда получаем, что  $P$ -позиции - это те, где обе кучи нечётные.

**Ответ:** Позиции, где в обоих кучах нечётное число камней.

### 23.3 Задача 4

**Условие:** Игроки по очереди красят ребра полного графа на  $n \geq 2$  вершинах в красный (первый игрок) и синий (второй игрок) цвета. Красить ребро, которое уже покрашено в другой цвет, запрещено. Игрок выигрывает, если ребра его цвета задают на вершинах связный граф. При каких  $n$  у первого игрока есть выигрышная стратегия?

**Решение:**

1. Будем доказывать, что первый игрок всегда сможет выиграть.

Делать это буду по индукции. Покажем, что первый всегда сможет добавить одну вершину к своему уже построенному связному графу-цепочке. Таким образом он дойдёт до  $n$  вершин.

То есть предположение такое: на  $k-1$ -ом ходу первого игрока у него  $k$ -связный граф.

**База:**  $k = 2$  - очевидно

**Переход:**  $k \rightarrow k + 1$

То есть мы знаем, что сейчас был  $k-1$  ход первого, второй сейчас походил и он всего поставил  $k-1$  ребро, а сейчас  $k$ -ый ход первого, надо показать, что найдётся хотя бы одно ребро непокрашенное, чтобы мы могли дополнить цепочку красного.

Если всего у первого цепочка на  $k$ -вершинах и тогда остальных вершин  $(n-k) \rightarrow$  рёбер соединяет эти вершины в полном графе  $(n-k)k$  штук, из которых по-максимуму могут быть заняты  $k-1$  ребро вторым игроком, то есть надо показать, что  $(n-k)k - k + 1 \geq 1 \rightarrow n \geq k + 1$ , что верно, так как  $k \leq n - 1$ , ведь на  $n-1$  ходу игра закончится.

**Ответ:** Первый имеет выигрышную стратегию при всех  $n$ .

### 23.4 Задача 5

**Условие:** Шоколадка представляет собой прямоугольник  $m \times n$ , поделенный углублением на единичные квадратики. Два игрока играют в следующую игру, делая ходы по очереди. На каждом ходу разрешается забрать один еще не взятый квадратик шоколадки, а также все еще не взятые квадратики, лежащие правее и выше (в т. ч. квадратики, лежащие выше в том же столбце и правее в той же строке). Проигрывает тот, кто забирает последний квадратик. Для всех натуральных  $m$  и  $n$  укажите, у кого из игроков есть выигрышная стратегия.

**Решение:**

1. Решим аналогично 5-ой задачи семинара. Ничья по условию быть не может.

Надо доказать, что у второго нет выигрышной стратегии.

**Док-во:**

Предположим, что у второго игрока есть такая стратегия, то есть он из каждой позиции точно знает, куда сходить, чтобы победить.

Пусть тогда первым ходом первый игрок закрасил правую верхнюю клетку.

Второй же любыми своими выхрышными ходами захватывает блок из плиток шоколада, содержащий в том числе и ту (уже пустую) плитку, что взял первый своим первым ходом.

Тогда первый думает, что раз из такой позиции Y можно гарантированно выиграть, потому что второй знает как это сделать, то он просто своим первым ходом сделает ход второго и прийдёт в Y, уже в выигрышную позицию, из которой первый сможет выиграть.

Противоречие! Значит, у второго нет выигрышной стратегии, а раз у него нет и нет ничей, то у первого должна быть выигрышная стратегия (следует из теоремы о цене игры данного типа).

Исключением является случай, когда m и n равны 1, потому что там прям явно можно указать стратегию для второго игрока.

**Ответ:** При m = 1 и n = 1 выигрывает второй, а при остальных первый.

## 24 Домашнее задание 21

(Илья)

### 24.1 Задача 1

**Условие:** Опишите P-позиции и стратегию для аналога игры Ним, в которой тот, кто не может сделать ход, не проигрывает, а выигрывает.

**Решение:**

На самом деле игра почти полностью аналогична Ним. Пусть у нас есть n кучек с  $a_i$  камней в i-ой кучке.

Покажем, что все P-позиции - это

- $a_1 \oplus a_2 \oplus \dots \oplus a_n = 0, \exists a_i \geq 2$  (отсюда следует, что существует хотя бы ещё одна кучка с  $a_j \geq 2$  камней, иначе 0 не получить)
- $a_1 \oplus a_2 \oplus \dots \oplus a_n = 1, \forall a_i \leq 1$

1. Рассмотрим второй случай, когда  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 1, \forall a_i \leq 1$ , тогда каждым своим ходом игроки увеличивают количество нулевых куч на 1

Тогда раз уж  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 1$ , то сейчас непустых куч нечётно, поэтому это P-позиция

Тогда по аналогии понятно, что  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 0$  - N-позиция, так как имеется чётное количество непустых кучек.

2. Теперь посмотрим на первый случай, когда  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 0, \exists a_i \geq 2$ .

Давайте покажем, что  $\begin{cases} a_1 \oplus a_2 \oplus \dots \oplus a_n = 0 & \text{P-позиция} \\ a_1 \oplus a_2 \oplus \dots \oplus a_n \neq 0 & \text{N-позиция} \end{cases}$

Заметим, что из позиции, когда  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 0$  можно попасть только в позицию, когда  $a_1 \oplus a_2 \oplus \dots \oplus a_n \neq 0$  (известно с семинара и лекции)

Почему же тогда  $a_1 \oplus a_2 \oplus \dots \oplus a_n \neq 0$  - N-позиция?

Посмотрим, что сможет сделать игрок, оказавшийся в этой позиции.

- Если среди  $a_i$  есть хотя бы 2 кучи  $\geq 2$ , то с лекции и семинара мы знаем, что существует такой ход, который приведёт его в ситуацию, когда  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 0$ , так как это всё произошло за 1 ход, то среди новых позиций есть та кучка, у которой  $a_i \geq 2$ , но по замечанию в самом начале, у нас есть ещё одна  $a_j \geq 2$ , тогда после хода второго игрока, который уже оказался в своей P-позиции, он сможет привести в позицию, когда у первого игрока будет  $a_1 \oplus a_2 \oplus \dots \oplus a_n \neq 0$  - N-позиция
- Если же среди  $a_i$  ровно одна куча с  $\geq 2$  камнями, то сделаем её 1 или 0 и тогда получим P-позицию первого типа, а из неё второй игрок просто сделает для нас N-позицию первого типа, когда  $a_1 \oplus a_2 \oplus \dots \oplus a_n = 0, \forall a_i \leq 1$

### 24.2 Задача 2

**Условие:** Найдите сложность вычисления дизъюнкции  $\vee_{i=1}^n x_i$  в модели разрешающих деревьев.

**Решение:**

1. Если у нас все переменные равны 0, то нам нужно задать  $n$  вопросов про все переменные, иначе мы не можем однозначно сказать про результат.

**Ответ:**  $n$

### 24.3 Задача 3

**Условие:** Есть монет, среди которых одна фальшивая. Настоящие монеты все имеют одинаковый вес, а фальшивая легче. За одно взвешивание можно сравнить по весу любые две монеты.

- a) Докажите, что фальшивую монету можно найти за  $\lfloor \frac{n}{2} \rfloor$  взвешиваний.  
 б) Докажите, что для нахождения фальшивой монеты необходимо  $\lfloor \frac{n}{2} \rfloor$  взвешиваний.

**Решение:**

- a) Если  $n$  - чётное, то мы можем просто разделить на пары все  $n$  монет и за  $\frac{n}{2}$  сравнений понять, кто фальшивка. Если же  $n$  нечётное, то можно просто отложить одну монету и дальше за  $\frac{n-1}{2}$  понять, кто есть кто из оставшихся. А если среди них нет фальшивой, то мы точно знаем, что это отложенная монета.

Чтобы объединить чётный и нечётный результат можем просто записать, что нам достаточно  $\lfloor \frac{n}{2} \rfloor$  сравнений.

- б) Теперь чтобы показать необходимость, давайте заметим, что после каждого сравнения двух монет мы узнаём информацию про 2 монеты. Давайте посмотрим в принципе, сколько необходимо сравнений для того, чтобы узнать информацию про все монеты (понятно, что если мы не знаем про это информацию, то ничего гарантировать мы не можем). То есть если  $n = 2k$ , то нам необходимо  $\frac{2k}{2} = k$  сравнений, а если  $n = 2k + 1$ , то нам тоже будет необходима  $k$  сравнений, потому что тогда мы будем знать информацию о  $2k$  монетах, чего нам хватит, чтобы однозначно сказать, про все монеты.

к сравнений это как раз  $\lfloor \frac{n}{2} \rfloor$  для чётного и нечётных случаев.

### 24.4 Задача 4

**Условие:** Имеется  $n$  монет, среди которых одна фальшивая, и чашечные весы. Настоящие монеты все имеют одинаковый вес, а фальшивая легче. На каждую чашку весов можно класть произвольное количество монет.

- a) Докажите, что фальшивую монету можно найти за  $\log_3 n + O(1)$  взвешиваний.  
 б) Докажите, что существует константа  $C \in \mathbf{Z}$ , что для нахождения фальшивой монеты необходимо по крайней мере  $\log_3 n + C$  взвешиваний для любого натурального  $n$ .

**Решение:**

- a) Итеративный алгоритм:(на каждой итерации будет происходить вот это)

- Делим  $n$  монет на 3 кучи: если  $n \equiv 1 \pmod{3}$ , то добавим в одну из куч оставшуюся монету, а если  $n \equiv 2 \pmod{3}$ , то добавим 2 монеты в любую кучу.
- Ставим любые две кучи на чашки весов и сравниваем. Если они равны по весу, то мы знаем, где фальшивая по весу, а если нет, то мы тоже знаем, в какой из них фальшивая монета.
- Потом берём кучу, в которой есть фальшивая монета и проделываем то же самое с первого пункта.

Этот алгоритм сведёт нас к куче размера  $\lceil \frac{n}{3} \rceil$ . Таким образом за  $\log_3 n + O(1)$  сравнений мы сможем найти фальшивую монету.

- б) Давайте заметим, что одно сравнение может иметь 3 исхода: монета в 1 куче, монета во 2 куче и монета в 3 куче. Поскольку для нахождения фальшивой монеты нам необходимо не менее  $n$  исходов(так как иначе будут 2 монеты, о которых ничего нельзя сказать), то тогда раз если сделано  $k$  сравнений, то мы имеем  $3^k$  исходов, то тогда имеем неравенство  $3^k \geq n \implies k \geq \log_3 n + C$  ( $C = 0$ )

### 24.5 Задача 5

**Условие:** Есть  $n$  монет разного веса. За одно взвешивание можно сравнить по весу любые две монеты. Найдите среди монет самую тяжелую и вторую по тяжести монету за  $n + \log_2 n + O(1)$  взвешиваний.

**Решение:**

Давайте сделаем турнирную систему. Поделим все монеты на пары(если их чётное количество) или отложим одну монету(она сразу проходит во второй тур) и оставшиеся поделим на пары(если всего монет было нечётное количество).

Тогда в след тур будут выходить более тяжёлые монеты и так далее. Понятно, что для поиска самой тяжёлой монеты нам необходимо  $n - 1$  сравнение, а что касается предтяжёлой, то тут стоит заметить, что у нас получилось дерево турнира и поэтому мы имеем  $\log_2 n$  раундов и понятно, что предтяжёлая монета могла проиграть только самой тяжёлой и нам понадобится сделать не более, чем  $\log_2 n$  сравнений для поиска предтяжёлой (возможно +1).

Итого, нам понадобится  $n + \log_2 n + O(1)$  взвешиваний.

## 25 Домашнее задание 22

(Tim Zhamoidin)

### 25.1 Задача 1

*Условие:* Треугольником в графе называется тройка вершин, попарно соединенных между собой. Рассмотрим вход функции  $T: \{0, 1\}^{\binom{n}{2}} \rightarrow \{0, 1\}$  как неориентированный граф на вершинах и положим  $T(G) = 1$  тогда и только тогда, когда в  $G$  нет треугольников. Постройте схему полиномиального размера, которая вычисляет функцию  $T$ .

**Решение:**

Пусть переменная  $x_{ij}, i < j$  обозначает, существует ли ребро между вершинами  $v_i, v_j$ .

Тогда функция  $T$  будет выглядеть как

Пусть  $A = \{y \in 2^{\{x_{12}, \dots, x_{n-1,n}\}} : |y| = 3\}$

$$T(x_1 2, \dots, x_{n-1,n}) = \neg \bigvee_{\{a,b,c\} \in A} x_{ab} \wedge x_{ac} \wedge x_{cb}$$

Конъюнкцию трех переменных можно вычислять следующей схемой  $g_1 = x_1 \wedge x_2, g_2 = g_1 \wedge x_3$

Дизъюнкцию  $m$  переменных можно вычислять по следующей схеме  $g_1 = x_1 \vee x_2, g_2 = g_1 \vee x_3, \dots, g_m = g_{m-1} \vee x_m + 1$

Тогда размер схемы будет равен  $2 \cdot \binom{n}{3} + 1 = O(n^3)$

### 25.2 Задача 2

*Условие:* Булева функция равенства  $EQ(x_1, \dots, x_n; y_1, \dots, y_n)$  равна 1 тогда и только тогда, когда

$$(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n)$$

Постройте схему размера  $O(n)$ , которая вычисляет  $EQ(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_n)$ .

**Решение:**

Переменные равны тогда только тогда когда их  $XOR$  равен 0.

Тогда функцию  $EQ$  можно представить как

$$EQ(x_1, \dots, x_n; y_1, \dots, y_n) = \neg \bigvee_{i=1}^n x_i \oplus y_i = \neg \bigvee_{i=1}^n (\neg x_i \wedge y_i) \vee (x_i \wedge \neg y_i)$$

Схема:

$$\begin{aligned} g_1 &= x_1 \oplus y_1 \\ &\dots \\ g_n &= x_n \oplus y_n \\ g_{n+1} &= g_1 \wedge g_2 \\ g_{n+2} &= g_{n+1} \wedge g_3 \\ &\dots \\ g_{2n-1} &= g_{2n-2} \wedge g_n \end{aligned}$$

Размер схемы:  $5n + 1 = O(n)$

### 25.3 Задание 3

*Условие:* Постройте схему полиномиального размера, вычисляющую функцию голосования  $MAJ(x_1, \dots, x_n)$  и не использующую отрицаний. В схеме разрешается использовать константы 0 и 1 (Напомним:  $MAJ(x_1, x_2, \dots, x_n) = 1$  тогда и только тогда, когда  $\sum_i x_i > \frac{n}{2}$ .)

**Решение:**

Мы уже умеем за полиномиальное время считать сумму двух чисел в двоичной системе счисления длины. Научимся считать функцию  $GREATER(x_1, \dots, x_n; y_1, \dots, y_n)$ , которая будет говорить больше ли число  $x$  числа  $y$ . Зададим схему рекуррентно

$$\begin{aligned} GREATER(x_1; y_1) &= (g_1 = \neg y_1, g_2 = x_1 \wedge g_1) \\ GREATER(x_1, \dots, x_n; y_1, \dots, y_n) : g_1 &= GREATER(x_1, \dots, x_{n-1}; y_1, \dots, y_{n-1}) \\ g_2 &= EQ(x_1, \dots, x_{n-1}; y_1, \dots, y_{n-1}) \\ g_3 &= GREATER(x_n; y_n) \\ g_4 &= g_2 \wedge g_3 \\ g_5 &= g_1 \vee 4 \end{aligned}$$

Размер схемы  $GREATER - O(n^2)$

Посчитаем тогда количество всех единиц и количество всех нулей среди переменных и сравним их

$$\begin{aligned} 0 &= x_1 \wedge \neg x_1 \\ &\vdots 1 = \neg 0 \\ (g_1, \dots, g_n) &= SUM(0, \dots, 0, 0, \dots, 0, x_1) \\ (g_{n+1}, \dots, g_{2n}) &= SUM(g_1, \dots, g_n, 0, \dots, 0, x_2) \\ &\dots \\ (g_{n^2-n+1}, \dots, g_{n^2}) &= SUM(g_{n^2-2n+1}, \dots, g_{n^2-n+1}, 0, \dots, 0, x_n) \\ (k_1, \dots, k_n) &= SUM(0, \dots, 0, 0, \dots, 0, x_1) \\ (k_{n+1}, \dots, k_{2n}) &= SUM(k_1, \dots, k_n, 0, \dots, 0, x_2) \\ &\dots \\ (k_{n^2-n+1}, \dots, k_{n^2}) &= SUM(k_{n^2-2n+1}, \dots, k_{n^2-n+1}, 0, \dots, 0, x_n) \end{aligned}$$

Теперь нужно определить схему сравнения двух числе размера  $n$   $GREATER(x_1, \dots, x_n; y_1, \dots, y_n)$  Размер итоговой схемы  $O(n^2)$

### 25.4 Задача 4

*Условие:* Постройте схему полиномиального размера для функции  $f: \{0, 1\}^{\binom{n}{2}} \rightarrow \{0, 1\}$ , равной единице, тогда и только тогда, когда данный на вход график связен и содержит эйлеров цикл.

**Решение:**

Критерий существования эйлерова цикла это то, что график связен и степени всех вершин четные.

Схема, для проверки графа на связность у нас есть с лекции. Остается только узнать являются ли все степени четными. На этот вопрос сможет ответить следующая функция:  $f(x_1, \dots, x_m) = \bigvee_{i=1}^n \bigoplus_{j=1}^n x_{ij}$ , где  $x_{ij}$  это переменная, обозначающая есть ли ребро между вершинами  $i, j$  (если  $i = j$  считаем, что  $x_{ii} = 0$ )

Чтобы посчитать  $XOR$  от  $n$  элементов мы можем  $n - 1$  последовательным ксомом двух, размер такой схемы будет равен  $5n - 5$ . А дизъюнкцию  $n$  элементов мы можем посчитать известной нам схемой размера  $n - 1$ . Тогда итоговый размер схемы для вычисления  $f$  будет равен  $(5n - 5)(n - 1) = O(n^2)$ .

Тогда схема для поиска эйлерова пути будет выглядеть так:

$$\begin{aligned}
g_1 &= \text{CONN}(x_1, \dots, x_m) \\
g_2 &= f(x_1, \dots, x_m) \\
g_3 &= \neg g_2 \\
g_4 &= g_1 \wedge g_3
\end{aligned}$$

## 25.5 Задача 5

**Условие:** Постройте схему полиномиального размера и глубины  $O(\log_2 n)$ , которая вычисляет сумму  $n$ -битовых двоичных чисел.

**Решение:**

Для вычисления суммы  $n$ -битовых двоичных чисел можно использовать бинарный дерево, где каждый узел соответствует одному биту суммы. Каждый узел может иметь два дочерних узла, которые соответствуют двум битам, складываемым на этом шаге. Корень дерева соответствует старшему биту суммы.

Для вычисления каждого бита суммы необходимо сложить два бита и возможный перенос из предыдущего разряда. Перенос из предыдущего разряда может быть либо 0, либо 1. Поэтому каждый узел дерева должен принимать на вход три бита: бит первого слагаемого, бит второго слагаемого и перенос из предыдущего разряда. Он должен производить два выхода: бит результата и перенос в следующий разряд.

Для вычисления бита результата используется XOR-гейт. Для вычисления переноса в следующий разряд используется AND-гейт. Перенос из предыдущего разряда передается на вход AND-гейта, а его выход передается на вход следующего узла дерева.

Схема вычисления суммы  $n$ -битовых двоичных чисел будет иметь глубину  $O(\log n)$ , так как количество уровней бинарного дерева равно  $\log n$ , где  $n$  - количество битов в числах. Количество узлов в дереве равно  $2 \log n$ , так как на каждом уровне дерева удваивается количество узлов.

Таким образом, схема вычисления суммы  $n$ -битовых двоичных чисел имеет полиномиальный размер и глубину  $O(\log n)$ .

## 25.6 Задача 6

**Условие:** Постройте эффективное сведение задачи о существовании в двудольном неориентированном графе совершенного паросочетания (паросочетания, размер которого равен мощности каждой из долей) к задаче выполнимости КНФ.

**Решение:**

Для сведения задачи о существовании совершенного паросочетания в двудольном неориентированном графе к задаче выполнимости КНФ, мы можем использовать следующую конструкцию.

Пусть дан двудольный граф  $G = (X, Y, E)$ , где  $X$  и  $Y$  - это две доли графа, а  $E$  - множество ребер. Мы создадим КНФ формулу  $F$  следующим образом:

Для каждого вершины  $x$  в  $X$  создадим переменную  $px$ .

Для каждого вершины  $y$  в  $Y$  создадим переменную  $qy$ .

Для каждого ребра  $(x, y)$  в  $E$  создадим дизъюнкцию двух литералов:  $px \vee qy$ .

Для каждой вершины  $x$  в  $X$  создадим дизъюнкцию всех соответствующих ребрам, связанным с  $x$ :  $(px \vee qy_1) \wedge (px \vee qy_2) \wedge \dots \wedge (px \vee qy_m)$ , где  $y_1, y_2, \dots, y_m$  - вершины, смежные с  $x$ .

Для каждой вершины  $y$  в  $Y$  создадим дизъюнкцию всех соответствующих ребрам, связанным с  $y$ :  $(px_1 \vee qy) \wedge (px_2 \vee qy) \wedge \dots \wedge (px_n \vee qy)$ , где  $x_1, x_2, \dots, x_n$  - вершины, смежные с  $y$ .

Теперь мы покажем, что существование совершенного паросочетания в  $G$  равносильно выполнению  $F$ .

Для начала предположим, что существует совершенное паросочетание  $M$  в  $G$ . Пусть  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$  - это ребра в  $M$ . Тогда мы можем установить переменные в  $F$  следующим образом:  $px_1 = qy_1 = 1, px_2 = qy_2 = 1, \dots, px_n = qy_n = 1$ . Тогда каждое ребро в  $M$  будет удовлетворено, потому что в каждой дизъюнкции  $(px \vee qy)$  будет хотя бы одна истина.

Обратно, предположим, что  $F$  выполнена. Это означает, что каждая дизъюнкция в  $F$  содержит хотя бы одну истину. Рассмотрим подмножество ребер  $M$  в  $G$ , состоящее из ребер, для которых  $px = qy = 1$ . Тогда каждая вершина в  $X$  и  $Y$  имеет ровно одно инцидентное ребро в  $M$ , потому что для каждой вершины  $x$  в  $X$ , дизъюнкция  $(px \vee qy)$  содержит хотя бы один литерал с истинной переменной, а для каждой вершины  $y$  в  $Y$ , дизъюнкция  $(px \vee qy)$  содержит хотя бы один литерал с истинной переменной. Таким образом,  $M$  - это паросочетание в  $G$ .

Кроме того, так как каждая вершина в  $X$  и  $Y$  имеет ровно одно инцидентное ребро в  $M$ , то  $M$  - совершенное паросочетание в  $G$ .

Таким образом, мы показали, что существование совершенного паросочетания в  $G$  равносильно выполнению  $F$ , что доказывает эффективное сведение задачи о существовании совершенного паросочетания в двудольном неориентированном графе к задаче выполнимости КНФ.

## 25.7 Задача 7

**Условие:** Пусть в 3-КНФ в каждый дизъюнкт входит ровно три различных переменных. Какое минимальное число дизъюнктов должно быть в такой 3-КНФ, чтобы она была невыполнима?

**Решение:**

Зафиксируем количество переменных равным  $n$

Заметим, что если существует функция  $f$  из  $m$  дизъюнктов которая выполнима на наборе переменных  $\{1\}^n$ , то для любого набора из  $\{0,1\}^n$  такая функция тоже существует. Ее можно получить из функции  $f$ , заменив в ней все  $x_i$ , значение которой в входных данных равно нулю на  $\neg x_i$ , а  $\neg x_i$  заменить на  $x_i$ . Тогда нам достаточно найти такое  $m$ , что не существует функции  $g$  из  $m$  дизъюнктов, такой, что  $g(1, \dots, 1) = 1$ , но существует функция из  $m-1$  дизъюнкта.

Заметим, что чтобы каждый дизъюнкт выполнялся нужно, чтобы в нем была хотя бы одна переменная без отрицания.

Найдем количество таких дизъюнктов. Количество дизъюнктов содержащих 1 переменную без отрицания:  $n \cdot \binom{n-1}{2}$   
Количество дизъюнктов содержащих 2 переменных без отрицания:  $n \cdot \binom{n-1}{2}$  Количество дизъюнктов содержащих 3 переменных без отрицания:  $\binom{n}{3}$

Тогда общее количество таких дизъюнктов:  $2 \cdot n \cdot \binom{n-1}{2} + \binom{n}{3} = 7/6(n-2)(n-1)n$

Тогда мы можем построить функции из  $7/6(n-2)(n-1)n$  дизъюнктов, которая выполнима, но функция из  $7/6(n-2)(n-1)n+1 = 7\binom{n}{3}$  дизъюнктов будет содержать хотя бы один дизъюнкт, который не выполнится при всех единицах в переменных, что вместе с первым замечанием ведет к тому, что искомое число это  $7\binom{n}{3}n+1$

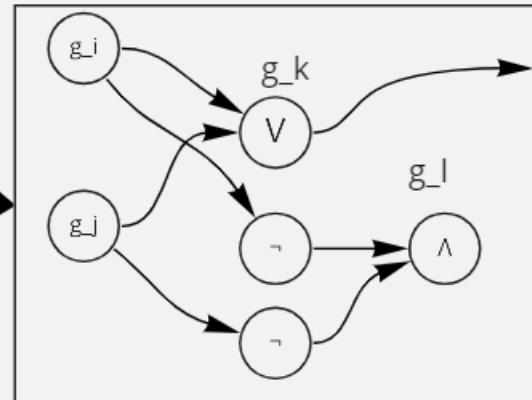
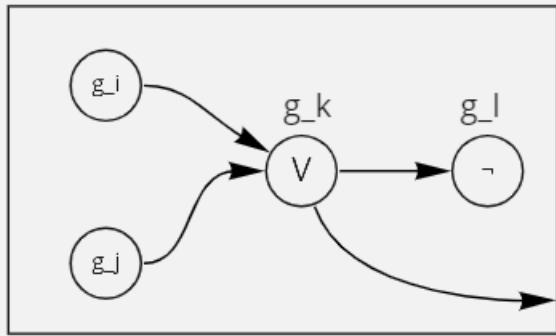
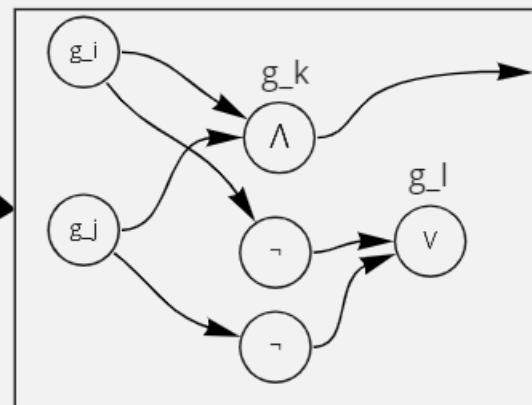
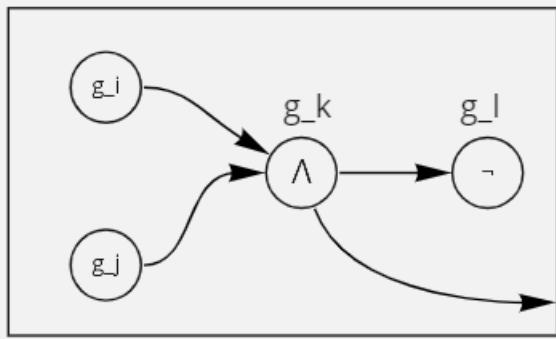
**Ответ:**  $7\binom{n}{3} + 1$

## 25.8 Задача 8

**Условие:** Докажите, что всякую булеву схему размера  $s$  с  $n$  переменными можно переделать в булеву схему, в которой все отрицания применяются только к переменным, и при этом размер новой схемы не превышает  $p(s,n)$ , где  $p$  - некоторый фиксированный полином.

**Решение:**

Будем проделывать следующие преобразования в порядке от наиболее глубоких элементов схемы к наименее глубоким



Благодаря порядку ты сделал не более  $s$  преобразований, при каждом преобразовании размер схемы увеличивается на 2, тогда после всех преобразований размер схемы будет не более чем  $3s$

### 25.9 Задача 9

*Условие:* Будем говорить, что булева переменная входит в два дизъюнкта в КНФ с разными знаками, если в один она входит с отрицанием, а в другой — без отрицания. Пусть в КНФ у любой пары дизъюнктов либо нет переменных, входящих в них с разными знаками, либо таких переменных не меньше двух. Докажите, что такая КНФ выполнима.

**Решение:**