Дискретная математика

Sokolnikov Alex

2025 — 2026

Содержание

1. Математическая индукция

1.1. Что это такое?

Пример 1.1

Докажите, что если на плоскости проведены n прямых, то можно раскрасить полученные области в два цвета так, что никакие две соседних не покрашены в один цвет.

Выкинем прямую, покрасим для $n-1$, потом добавим прямую обратно и инвертируем полуплоскость.

Что необходимо для индукции?

1. База: $A(1)$ — истинно
2. Переход: $\forall n(A(n) \Rightarrow A(n+1))$

По принципу математической индукции $\forall n\ A(n)$ — истинно

Пример 1.2

$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

База:

$$1 = \frac{1 \cdot 2}{2}$$

Переход:

$$\frac{n(n+1)}{2} + (n+1) = (n+1)(\frac{n}{2} + 1) = \frac{(n+1)(n+2)}{2}$$

Пример 1.3

$1 + \frac{1}{2^2} + \ldots + \frac{1}{100^2} < 2$

$A(n) = 1 + \frac{1}{2^2} + \ldots \frac{1}{n^2} \leq 2 - \frac{1}{n}$

База:

$$1 \leq 1$$

Переход:

$$1 + \frac{1}{2^2} + \ldots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \leq$$
$$\leq 2 - \frac{1}{n} + \frac{1}{n(n+1)} = 2 - \frac{1}{n+1}$$

Что нужно делать аккуратно:

- Не забыть проверить базу
- Убедиться, что переход работает для всех n (не забыть всякие крайние случаи $1 \to 2$ и т.п.)
- Не надо добавлять объект к конструкции на n элементах, надо выкинуть один из $n+1$

1.2. Полная индукция

Есть $A(1), A(2), \ldots, A(n), \ldots$
Главное отличие в переходе: $(\forall k < n\ A(k)) \Rightarrow A(n)$

Пример 1.4

Докажите, что выпуклый многоугольник можно триангулировать, причем всего будет $n-2$ треугольника.

1.3. Эквивалентность различных принципов индукции

1. Принцип математической индукции:

$$\left.\begin{array}{l} A(1) \\ \forall n\ A(n) \Rightarrow A(n+1) \end{array}\right\} \Rightarrow \forall n\ A(n)$$

2. Полная индукция:

$$((\forall k < n\ A(k)) \Rightarrow A(n)) \Rightarrow \forall n\ A(n)$$

3. Принцип наименьшего числа $\forall S \subseteq \mathbb{N}, S \neq \varnothing$ Тогда в S. есть наименьший элемент: $\exists s \in S : \forall t \in S\ s \leq t$

Теорема 1.5

Три вышеуказанных принципа индукции эквивалентны.

- $3 \to 1$

  Имеем $A(1), A(2), \ldots, A(n), \ldots$ и $A(n) \Rightarrow A(n+1)$

  $S = \{n \in N \mid A(n) - \text{ложно}\}$

  Либо S пустое, либо в нем есть минимальный элемент s. Но тогда либо $s = 1$ и неверна база, либо неверен переход $A(s-1) \Rightarrow A(s)$. Значит S пустое и все $A(n)$ верны.

- $2 \to 3$

  Есть $S \neq \varnothing$. Пусть S не имеет наименьшего элемента.

  $A(n) = n \notin S$

  $\forall k < n \; A(k) \Rightarrow A(n)$

  $\forall k < n \; k \notin S \Rightarrow n \notin S$ — иначе в S есть минимальный элемент.

  Тогда $\forall n \; n \notin S \Rightarrow S = \varnothing$

- $1 \to 2$

  $B(n) = A(1) \wedge A(2) \wedge \ldots \wedge A(n)$

  $$\left.\begin{array}{l} B(1) = A(1) \\ B(n) \Rightarrow A(n) \Rightarrow A(n+1) \Rightarrow B(n+1) \end{array}\right\} \Rightarrow \forall n \; B(n)$$

2. Множества

$$X = \{a, b, c\}$$

Принятно, что множества упорядочены, а их элементы не повторяются, то есть

$$\{a, b, c\} = \{a, b, a, c, c, b\} = \{b, c, a\}$$

- $a \in X$ — a принадлежит X
  $a \notin X$ — a не принадлежит X
- $X \subseteq Y$ — X является подмножеством Y
  $\forall x\ (x \in X \Rightarrow x \in Y)$
- $X = Y \Leftrightarrow (X \subseteq Y \wedge Y \subseteq X)$

Пример 2.1

Примеры множеств:

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$
- $\{1, 2, 3, 5, 7\}$
- $\varnothing$ — пустое множество

Пример 2.2

Определение натуральных чисел через множества:

$$0 = \varnothing$$
$$n + 1 = n \cup \{n\}$$

2.1. Операции с множествами

1. Выделение условием
   X — множество
   $Y = \{x \in X \mid \phi(x)\}$
2. Объединение
   A, B — множества
   $A \cup B = \{x \mid x \in A \vee x \in B\}$

3. Пересечение

   A, B — множества

   $A \cap B = \{x \mid x \in A \wedge x \in B\}$

4. Разность множеств

   A, B — множества

   $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

5. Симметрическая разность

   A, B — множества

   $A \oplus B = \{x \mid x$ лежит в ровно одном из $A, B\}$

6. Взятие всех подмножеств X

   $2^X = \{Y \mid Y \subseteq X\}$

7. Дополнение

   $\overline{A} = U \setminus A$

2.2. Парадокс Рассела

$R = \{x \mid x \notin x\}$
Лежит ли R в R

- $R \in R \Rightarrow R \notin R$
- $R \notin R \Rightarrow R \in R$

Получили парадокс.

Мы использовали выделение условием, но мы можем выделять только из другого множества. Но на самом деле “множество” всех множеств не является множеством.

Чтобы такого не происходило, существует аксиоматика Цермело-Френкеля — ZF или ZFC (с аксиомой выбора)

2.3. Базовые тождества

1. $A \cup B = B \cup A$
2. $(A \cup B) \cup C = A \cup (B \cup C)$
3. $A \cap \varnothing = \varnothing$
4. $A \cup \varnothing = A$

5. $A \cap B = B \cap A$
6. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$

3. Функции

Определение 3.1: Упорядоченная пара

$(a, b) = \{\{a\}, \{a, b\}\}$

Определение 3.2: Декартово произведение

Декартово произведение множеств A и B обозначается $A \times B$ и является множеством всех упорядоченных пар (a, b), где $a \in A, b \in B$.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Определение 3.3: Функция

Подмножество f декартова произведения $X \times Y$ называется функцией из X в Y $(f : X \to Y)$, если $\forall x \in X \; \exists! \; (x, y) \in f$

$y = f(x)$.
x — прообраз y, y — образ x.
X — область определения, Y — область значений.

Когда пишут $f : X \to Y$ обычно считают, что X — полная область определения, то есть f определена на всем X. Тогда f — тотальная функция.

Определение 3.4: Инъекция

f — инъекция (вложение) множества X на множество Y, если

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Определение 3.5: Сюръекция

f — сюръекция (накрытие) множества X на множество Y, если

$$\forall y \in Y \; \exists x \in X : f(x) = y$$

Определение 3.6: Биекция

f — биекция множества X на множество Y, если она является и сюръекцией, и инъекцией.

3.1. Композиция функций

Определение 3.7: Композиция

Пусть есть тотальные $f : A \to B, g : B \to C$
Определим функцию $g \circ f : A \to C$
$(g \circ f)(a) = g(f(a))$

Теорема 3.8: Ассоциативность композиции

Пусть есть тотальные $f : A \to B, g : B \to C, h : C \to D$
$h \circ (g \circ f) = (h \circ g) \circ f$

Доказательство:

$$h \circ (g \circ f) : A \to D$$
$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$$
$$(h \circ g) \circ f : A \to D$$
$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$

3.2. Критерий биективности

Определение 3.9: Тождественная на X функция

Определим на множестве X функцию $id_X : X \to X$

$$\forall x \in X \; id_X(x) = x$$

Замечание 3.10

$f \circ id_A = f$
$id_B \circ f = f$

Теорема 3.11: Критерий биективности функций

Пусть $f : A \to B$.
Тогда f — биекция $\Leftrightarrow \exists g : B \to A : f \circ g = id_B, g \circ f = id_A$

Доказательство:

- $\Rightarrow$

  Построим $g : B \to A$

  $g(b) \in f^{-1}(b)$

  Тогда $f(g(b)) = b \Rightarrow f \circ g = id_B$.

$g(f(a)) \in f^{-1}(f(a)) = fa \Rightarrow g(f(a)) = a \Rightarrow g \circ f = id_A$

- $\Leftarrow$

  $\exists g : B \to A : f \circ g = id_A, g \circ f = id_B$

  1. Покажем, что f — инъекция
     $f(a_1) = f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow id_A(a_1) = id_A(a_2) \Rightarrow a_1 = a_2$
  2. Покажем, что f — сюръекция
     Рассмотрим $b \in B$. Найдем $a \in A : f(a) = b$.

$$(f \circ g)(b) = b$$
$$f(g(b)) = b$$
$$a = g(b) \in A - \text{подходит}$$

f — сюръекция и инъекция, а значит f — биекция.

Определение 3.12: Обратная функция

Пусть $f : A \to B$ — биекция
Тогда $g : B \to A$, для которой $f \circ g = id_B$ и $g \circ f = id_A$, называют обратной к f и обозначают f^{-1}

Упражнение 3.13

Если f — биекция, то f^{-1} единственна

Лемма 3.14

Пусть $f : A \to B, g : B \to C$ — биекции
Тогда

- $g \circ f$ биективна
- $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Доказательство:
Просто проверим критерий биективности, используя две эти функции.

Упражнение 3.15

$f : A \to B, g : B \to C$

1. если f, g — инъекции, то $g \circ f$ — инъекция
2. если f, g — сюръекции, то $g \circ f$ — сюръекция

4. Булевы функции

4.1. Определение

Определение 4.1: Булева функция

$\mathbb{B} = \{0, 1\}$
Булева функция — это $f : \mathbb{B}^n \to \mathbb{B}$

Пример 4.2

x	y	$x \vee y$	$x \wedge y$	$\neg x$	$x \oplus y$	$x \to y$	$x \equiv y$
0	0	0	0	1	0	1	1
0	1	1	0	1	1	1	0
1	0	1	0	0	1	0	0
1	1	1	1	0	0	1	1

Количество булевых функций от n переменных равно 2^{2^n}

4.2. Свойства

Упражнение 4.3

- $x \wedge (y \wedge z) = (x \wedge y) \wedge z,\ x \wedge y = y \wedge x,\ x \wedge 0 = 0,\ x \wedge 1 = x$
- $x \vee (y \vee z) = (x \vee y) \vee z,\ x \vee y = y \vee x,\ x \vee 0 = x,\ x \vee 1 = 1$
- $x \oplus (y \oplus z) = (x \oplus y) \oplus z,\ x \oplus y = y \oplus x,\ x \oplus 0 = x,\ x \oplus 1 = \neg x$
- $x \wedge (y \oplus z) = (x \wedge y) \oplus (x \wedge z)$
- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),\ x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
- $\neg(\neg x) = x$ — закон двойного отрицания
- $x \to y = \neg y \to \neg x$ — контрапозиция
- $\neg(x \wedge y) = \neg x \vee \neg y,\ \neg(x \vee y) = \neg x \wedge \neg y$ — законы де Моргана

4.3. Дизъюнктивная нормальная форма

$\neg x = \overline{x}$

Для $\alpha \in \{0,1\}$ $x^\alpha = \begin{cases} x, \text{при } \alpha = 1 \\ \overline{x}, \text{при } \alpha = 0 \end{cases}$ — литерал

Определение 4.4: Конъюнкт

$$x_{i_1}^{\alpha_1} \wedge x_{i_2}^{\alpha_2} \wedge \ldots \wedge x_{i_k}^{\alpha_k} = K$$

Определение 4.5: Дизъюнктивная нормальная форма

ДНФ — дизъюнкция конъюнктов

$$K_1 \vee K_2 \vee \ldots \vee K_n$$

Теорема 4.6

Каждая булева функция $f : \mathbb{B}^n \to \mathbb{B}$ может быть представлена в виде ДНФ

Доказательство:

Пусть $f(x_1, x_2, \ldots, x_n) \not\equiv 0$

Если $f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 1$, возьмем конъюнкт $K = x_1^{\sigma_1} \wedge x_2^{\sigma_2} \wedge \ldots \wedge x_n^{\sigma_n}$. Очевидно, он принимает значение 1 только на наборе своих степеней.

Возьмем произведение этих конъюнктов по всем наборам f, где она равна 1

Это представление называется совершенное ДНФ (СДНФ).

Определение 4.7: Дизъюнкт

$$x_{i_1}^{\alpha_1} \vee x_{i_2}^{\alpha_2} \vee \ldots \vee x_{i_k}^{\alpha_k} = K$$

Определение 4.8: Конъюктивная нормальная форма

КНФ — конъюнкция дизъюнктов

$$D_1 \vee D_2 \vee \ldots \vee D_n$$

Упражнение 4.9

Любая булева функция имеет КНФ

4.4. Многочлен Жегалкина

Определение 4.10: Многочлен Жегалкина

$$\bigoplus_{I=\{i_1,i_2,\ldots,i_k\}\subseteq\{1,2,\ldots,n\}} a_i \wedge x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_k}$$
$$a_i \in \{0,1\}$$

По сути каждый возможный моном либо входит в сумму, либо нет.

Пример 4.11

$$x \vee y = x \oplus y \oplus (x \wedge y) = x + y + xy$$

Теорема 4.12

Каждая булева функция $f : \mathbb{B}^n \to B$ имеет представление в виде многочлена Жегалкина (от n переменных), и притом единственное с точностью до перестановки мономов

Доказательство:

$$f(x_1, x_2, \ldots, x_n) = (x_n \wedge f(x_1, \ldots, x_{n-1}, 1)) \oplus ((x_n \oplus 1) \wedge f(x_1, \ldots, x_{n-1}, 0)$$

Теперь докажем по индукции, что всякая функция представима в виде многочлена Жегалкина:

База $n = 1$: очевидно

Переход $n \to n + 1$:

$$f_0(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0),\ \ f_1(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 1)$$

По формуле выше:

$$f(x_1, \ldots, x_n) = (x_n \wedge f_1(x_1, \ldots, x_{n-1})) \oplus ((x_n \oplus 1) \wedge f_0(x_1, \ldots, x_{n-1}))$$

По индукции f_0, f_1 представимы в виде многочлена Жегалкина, остается просто раскрыть скобки.

Покажем единственность:

Всего 2^{2^n} различных булевых функций. Также всего различных 2^{2^n} различных многочленов Жегалкина. Значит каждой функции сопоставлен уникальный многочлен Жегалкина.

4.5. Замыкание системы связок

Определение 4.13

P_2 — множество всех булевых функций
$P_2(n)$ — множество всех булевых функций от $x_1, \ldots, x_n$
$\mathcal{F} \subseteq P_2$ — систему связок

Пример 4.14

- $\{\vee, \wedge, \neg\}$
- $\{\vee, \oplus, 1\}$

Определение 4.15

Замыкание $\mathcal{F}$ — это $[\mathcal{F}]$, равное следующему:

$$\mathcal{F}_0 = \mathcal{F} \cup \{x_1, x_2, \ldots\}$$

$$\mathcal{F}_k \to \mathcal{F}_{k+1} : \begin{cases} F_k \subseteq F_{k+1} \\ g = h(f_1(y_1^{(1)}, \ldots y_{l_1}^{(1)}), \ldots, f_s(y_1^{(s)}, \ldots y_{l_s}^{(s)})) \in F_{k+1} \end{cases}$$

$$[\mathcal{F}] = \bigcup_{k=0}^{\infty} \mathcal{F}_k$$

Пример 4.16

- $[\{\wedge, \vee, \neg\}] = P_2$ (ДНФ)
- $[\{\wedge, \oplus, 1\}] = P_2$ (многочлены Жегалкина)

Определение 4.17

$\mathcal{F} \subseteq P_2$ — полная система связок, если $[\mathcal{F}] = P_2$

Упражнение 4.18

- $\mathcal{F} \subseteq [\mathcal{F}]$
- $A \subseteq B \Rightarrow [A] \subseteq [B]$
- $[[\mathcal{F}]] = [\mathcal{F}]$

Лемма 4.19: Достаточное условие полноты системы

Пусть $A \subseteq P_2$ — полная система и $\forall f \in A$ верно, что $f \in [B]$
Тогда B — полная система.

Доказательство:

$$A \subseteq [B] \Rightarrow [A] \subseteq [[B]] = B \Rightarrow P_2 \subseteq [B] \Rightarrow [B] = P_2$$

Следствие 4.20

$\{\wedge, \neg\}, \{\vee, \neg\}$ — полные системы

Доказательство:
$B = \{\wedge, \neg\}$
$A = \{\wedge, \vee, \neg\},\ [A] = P_2$
$x \vee y = \neg(\neg x \wedge \neg y) \in [B]$
Для второй системы аналогично

4.6. Замкнутые классы

Определение 4.21

Пусть $F \subseteq P_2$. F называется замкнутым классом, если $[F] = F$

Пример 4.22

- $F = P_2$
- $F = [A],\ A \in P_2, A \neq \varnothing$
- $F = L$

4.6.1. Класс L

Определение 4.23: Класс L

$f(x_1, \ldots, x_n)$ — линейная, если

$$f(x_1, \ldots, x_n) = a_0 \oplus (a_1 \oplus x_1) \oplus \ldots \oplus (a_n \oplus x_n)$$

Определение 4.24

L — все линейные функций.

Замечание 4.25

$[L] = L$

Лемма 4.26: Лемма о нелинейной функции

Из любой нелинейной функции $f(x_1, \dots x_n), n > 1$ подстановкой вместо переменных $0, x, y$ можно получить $g(x, y) \notin L$

Доказательство:

Рассмотрим полином Жегалкина для f и выберем моном наименьшей длины, большей 1.

Не умаляя общности, это моном $x_1 x_2 \dots x_r, r > 1$.

Рассмотрим $g(x, y, \dots, y, 0, \dots 0$ (последние $n-r$ — нули). Нетрудно убедиться, что получим $xy + linear \Rightarrow$ получили нелинейную функцию g.

Следствие 4.27

Пусть $f \notin L$, тогда $x \wedge y \in [\{0, \neg, f\}]$

Доказательство:

По лемме построим $g(x, y)$. Понятно, что $g(x, y) \in [\{f, 0\}]$.

$$g(x, y) = xy + ax + by + c,\ a, b, c \in \{0, 1\}$$
$$g(x + b, y + a) = (x + b)(y + a) + a(x + b) + b(y + a) + c =$$
$$= xy + by + xa + ba + ax + ab + by + ab + c = xy + ab + c$$
$$g(x + b, y + a) = \begin{bmatrix} x \wedge y \\ \neg(x \wedge y) \end{bmatrix} \in [\{f, 0, \neg x\}]$$
$$\Downarrow$$
$$x \wedge y \in [\{f, 0, \neg x\}]$$

4.6.2. Класс S

Определение 4.28

Пусть $f(x_1, \dots, x_n) \in P_2$

Тогда двойственная булевая функция к f — это $f^* = \neg f(\neg x_1, \dots, \neg x_n)$

Пример 4.29

- $x^* = \neg\neg x = x$
- $(x \wedge y)^* = \neg(\neg x \wedge \neg y) = x \vee y$
- $(f^*)^* = f$

Лемма 4.30: Принцип двойственности

$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$
Тогда
$f(x_1, \ldots, x_n) = f_0^*(f_1^*(x_1, \ldots, x_n), \ldots, f_n^*(x_1, \ldots, x_n))$

Определение 4.31: Класс S

$S = \{f \in P_2 : f = f^*\}$ — самодвойственные функции.

Пример 4.32

- $x = x^*$
- $MAJ(x, y, z) = MAJ^*(x, y, z)$
- $(x \oplus y)^* = \neg(\neg x \oplus \neg y) = x \oplus y \oplus 1 = x \equiv y$

Лемма 4.33

$$[S] = S$$

Доказательство:

$$h(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) =$$
$$= f_0^*(f_1^*(x_1, \ldots, x_n), \ldots, f_n^*(x_1, \ldots, x_n)) = h^*(x_1, \ldots, x_n)$$

Лемма 4.34: Лемма о самодвойственной функции

Пусть $f(x_1, \ldots, x_n) \notin S$
Тогда подстановкой вместо переменных $x, \neg x$ можно получить константу.

Доказательство:

$$\exists(\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n : f(\alpha_1, \ldots, \alpha_n) = f(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) \ (f \notin S)$$
$$x_i \to \begin{cases} x, \alpha_i = 0 \\ \neg x, \alpha_i = 1 \end{cases}$$
$$g(0) = f(\alpha_1, \ldots, \alpha_n) = f(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) = g(1)$$

4.6.3. Классы T_0, T_1

Определение 4.35: T_0, T_1

$$T_0 = \{f \in P_2 : f(0, \dots, 0) = 0\}$$
$$T_1 = \{f \in P_2 : f(1, \dots, 1) = 1\}$$

Пример 4.36

- $x \wedge y, x \vee y \in T_0, T_1$
- $1 \in T_1, 0 \in T_0$
- $x \oplus y \in T_0 \setminus T_1$

Лемма 4.37: Лемма о функции, не сохраняющей константу

1. $f \notin T_0 \Rightarrow f(x, \dots, x) \in \{1, \neg x\}$
2. $f \notin T_1 \Rightarrow f(x, \dots, x) \in \{0, \neg x\}$

4.6.4. Класс M

Определение 4.38

$$0 < 1$$
$$(\alpha_1, \dots, \alpha_n) \leq (\beta_1, \dots, \beta_2)$$
$$\Updownarrow$$
$$\forall i \ \alpha_i \leq \beta_i$$

Определение 4.39: Монотонная функция

$f(x_1, \dots, x_n)$ — монотонная, если $\forall \tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n : (\tilde{\alpha} < \tilde{\beta} \Rightarrow f(\tilde{\alpha}) \leq f(\tilde{\beta}))$

Определение 4.40: Класс M

$$M = \{f \in P_2 : f - \text{ монотонная}\}$$

Пример 4.41

- $1, 0 \in M$
- $MAJ \in M$
- $x \oplus y \notin M$

Упражнение 4.42

$$[M] = M$$

Лемма 4.43: Лемма о немонотонной функции

Пусть $f \notin M$.
Тогда подставляя в f вместо переменных $0, 1, x$ можно получить $\neg x$.

Доказательство:

$$f \notin M \Rightarrow \exists \tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n : \tilde{\alpha} \leq \tilde{\beta}, f(\tilde{\alpha}) = 1, f(\tilde{\beta}) = 0$$
$$\tilde{\alpha} = (0, \dots, 0, 1, \dots 1, 0, \dots 0)$$
$$\tilde{\beta} = (0, \dots, 0, 1, \dots 1, 1, \dots 1)$$

различающиеся позиции есть, так как значения функции на наборах различны

$$g(x) = (0, \dots, 0, 1, \dots 1, x, \dots x)$$
$$g(0) = f(\tilde{\alpha}) = 1$$
$$g(1) = f(\tilde{\beta}) = 0$$

Теорема 4.44: Критерий Поста

F — полная $\Leftrightarrow F \not\subseteq L, F \not\subseteq S, F \not\subseteq T_0, F \not\subseteq T_1, F \not\subseteq M$

Доказательство:

- $\Rightarrow$

  Тривиально

- $\Leftarrow$

  Покажем, что $x \wedge y, \neg x \in [F]$

  Дано: $\exists f_M \in F \setminus M, f_L \in F \setminus L, f_{T_0} \in F \setminus T_0, f_{T_1} \in F \setminus T_1, f_S \in F \setminus S$

По лемме о функции, не сохраняющей константу:

$$f_{T_0}(x, \dots x) = \begin{bmatrix} 1 \in [F] \\ \neg x \in [F] \end{bmatrix}$$
$$f_{T_1}(x, \dots x) = \begin{bmatrix} 0 \in [F] \\ \neg x \in [F] \end{bmatrix}$$

Рассмотрим два случая:

1. $0, 1 \in [F]$
   По лемме о немонотонной функции: $f_M, 0, 1, x \to \neg x \in [F]$
2. $\neg x \in [F]$
   Лемма о несамодвойстенной функции: $f_S, x, \neg x \to const \Rightarrow 0, 1 \in [F]$

Значит $0, 1, \neg x \in [F]$.

По лемме о нелинейной функции и следствию из нее:

$x \wedge y \in [\{0, f_L, \neg x\}] \subseteq [F]$

Получили, что $\neg x, x \wedge y \in [F] \Rightarrow [F] = [[F]] = P_2$

4.7. Предполные классы

Определение 4.45: Предполный класс

$F \subseteq P_2$ — предполный класс (в P_2), если

- $[F] = F$
- $F \neq P_2$
- $\forall g \in P_2 \setminus F \; [F \cup \{g\}] = P_2$

Теорема 4.46

В P_2 существует лишь 5 предполных классов: L, S, M, T_0, T_1

Доказательство:
Пусть $F \neq L, S, M, T_0, T_1$ — предполный.
Тогда $[F] = F \neq P_2$.
По критерию Поста $F \subseteq L$ или S или M или T_0 или T_1. Не умаляя общности, $F \subseteq L$. Тогда $\exists g_L \in L \setminus F \Rightarrow P_2 = [F \cup \{g_L\}] \subseteq L$ — противоречие.
Почему эти пять классов подходят?

	T_0	T_1	M	S	L
T_0		0	$x \oplus y$	0	$x \wedge y$
T_1	1		$x \equiv y$	1	$x \wedge y$
M	1	0		1	$x \wedge y$
S	$\neg x$	$\neg x$	$\neg x$		$MAJ(x, y, z)$
L	1	0	$x \oplus y$	1	

5. Формула включений-исключений

Теорема 5.1: Формула включений-исключений

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{k=1}^{n} \sum_{1 \le i_1 < \ldots < i_k \le n} |A_{i_1} \cap \ldots \cap A_{i_k}|$$

Доказательство (через характеристические функции):

6. Опять множества

Определение 6.1: Равномощные множества

Множества A и B равномощны, если существует биекция $f : A \to B$
Обозначается $A \sim B, |A| = |B|$

Пример 6.2

- $\mathbb{N} \sim \mathbb{N} \cup \{0\}$ $n \mapsto n - 1$
- $[0, 1] \sim [0, 2]$ $x \mapsto 2x$
- $(0, 1) \sim (1, +\infty)$ $x \mapsto \frac{1}{x}$

Упражнение 6.3

$[a, b] \sim [c, d],\ a, b, c, d \in \mathbb{R}$

Свойства:

1. $\forall A\ A \sim A$ (рефлексивность)
2. $\forall A, B\ A \sim B \Rightarrow B \sim A$ (симметричность)
3. $\forall A, B, C\ A \sim B, B \sim C \Rightarrow A \sim C$ (транзитивность)

Определение 6.4: Счетные множества

Множество A счетно, если $A \sim \mathbb{N}$

Пример 6.5

- $\mathbb{Z} \sim \mathbb{N}$
- $\mathbb{Q} \sim \mathbb{N}$

Лемма 6.6

- A, B — счетны $\Rightarrow A \cup B$ — счетно
- A — конечно, B — счетно $\Rightarrow A \cup B$ — счетно

Лемма 6.7

A — счетно, $B \subseteq A$.
Тогда B не более чем счетно.

Лемма 6.8

A — бесконечно, тогда существует счетное $B \subseteq A$

Доказательство:
Будем строить итеративно: берем любой $a_{n+1} \in A \setminus \{a_1, a_2, \ldots, a_n\}$.

$$B_n = \{a_1, \ldots, a_n\}, B = \bigcup_{n=1}^{\infty} B_n$$

Лемма 6.9

$A_1, A_2, \ldots, A_n, \ldots$ — счетны
Тогда $\bigcup_{n=1}^{\infty} \Rightarrow A_n$ — счетно

Лемма 6.10

A, B — счетны
Тогда $A \times B$ — тоже счетно

Доказательство:

$$A \times B = \bigcup_{n=1}^{\infty} A \times \{B_n\}$$

Теорема 6.11

Пусть A — бесконечно, а B — счетно.
Тогда $A \cup B \sim A$

Доказательство:

$$A \cup B = A \cup (B \setminus A)$$
$$A \cup B = A \cup B', A \cap B' = \varnothing$$

Рассмотрим счетное C
$C \sim C \cup B'$
$\exists f : C \to C \cup B'$ — биекция
Построим биекцию $g : A \to A \cup B'$

$$g = \begin{cases} x, x \notin C \\ f(x), x \in C \end{cases}$$

6.1. Несчетные множества

Счетные ($\sim A$): $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{N}^k, \bigcup\limits_{k=1}^{n} \mathbb{N}^k$

Определение 6.12

$$\mathbb{B}^\infty = \{(b_1, b_2, \ldots) \mid b_i \in \{0, 1\}\}$$

Теорема 6.13

$$\mathbb{B}^\infty \not\sim \mathbb{N}$$

Лемма 6.14

$$\mathbb{B}^\infty \sim [0, 1) \sim [0, 1] \sim (0, 1) \sim \mathbb{R} \sim 2^{\mathbb{N}}$$

Доказательство:
$\mathbb{B}^\infty \sim [0, 1)$, так как можно сопоставить последовательности число в двоичной записи.
Все кроме последнего тривиально.
$2^{\mathbb{N}} \sim \mathbb{B}^\infty$, так как по сути выбираем что взяли в набор, а что нет.

Определение 6.15

Множество A имеет мощность континуум, если $A \sim \mathbb{R}$

Теорема 6.16

$$[0, 1] \sim [0, 1]^2$$

Будем доказывать $\mathbb{B}^\infty = (\mathbb{B}^\infty)^2$
$(x_1, x_2, \ldots) \leftrightarrow (x_1, x_3, \ldots)(x_2, x_4, \ldots)$

Следствие 6.17

$$\mathbb{R}^k \sim \mathbb{R}$$

Определение 6.18

$|A| \leq |B|$, если существует инъекция $f : A \to B$
$|A| < |B|$, если $|A| \leq |B|$ и $|A| \neq |B|$

Свойства:

- $|A| \leq |B| \Leftrightarrow \exists A' \subseteq B : A' \sim A$
- $|A| \leq |A|$
- $|A| \leq |B|, |B| \leq |C| \Rightarrow |A| \leq |C|$
- $|A| \leq |B|, |B| \leq |A| \Rightarrow |A| \sim |B|$ (теорема Кантора-Бернштейна)
- $\forall A, B \ |A| \leq |B| \vee |B| \leq |A|$

Теорема 6.19

$$|X| < |2^X|$$

Доказательство:

1. $|X| \leq |2^X|$
   $\exists f : X \to 2^X$, $f(x) = x$ — инъекция
2. $|X| \neq |2^X|$
   Докажем от противного. Пусть существует $f : X \to 2^X$.
   Определим $Y = \{x \in X \mid x \notin f(x)\} \subseteq X$.
   Поскольку $Y \in 2^X, \exists y \in X : f(y) = Y$
   - $y \in Y \Rightarrow y \notin f(y) = Y$ — противоречие
   - $y \notin Y \Rightarrow y \in f(y) = Y$ — противоречие

Следствие 6.20

Существует бесконечно много мощностей.

$$\mathbb{N} < 2^{\mathbb{N}} < 2^{2^{\mathbb{N}}} < \dots$$

Теорема 6.21: Теорема Кантора Бернштейна

$$|A| \leq |B|, |B| \leq |A| \Rightarrow |A| = |B|$$

Доказательство:
Пусть $f : A \to B, g : B \to A$ — инъекции.
Определим $C_0 = A \setminus g(B)$. $A \supseteq C_{n+1} = g(f(C_n)), n \geq 0$
$C = \bigcup\limits_{n \geq 0} C_n$

Возьмем $h = \begin{cases} f(x), x \in C \\ g^{-1}(x), x \notin C \end{cases}$, $(x \notin C \Rightarrow x \notin C_0 \Rightarrow x \in g(B))$

Покажем, что мы построили биекцию.

1. h — инъекция

   $h(x_1) = h(x_2)$

   - $x_1, x_2 \in C \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
   - $x_1, x_2 \notin C \Rightarrow g^{-1}(x_1) = g^{-1}(x_2) \Rightarrow x_1 = x_2$
   - $x_1 \in C, x_2 \notin C \Rightarrow f(x_1) = g^{-1}(x_2)$. Но тогда $g(f(x_1)) = x_2$. $x_1 \in C_n \Rightarrow x_2 \in C_{n+1}$ — противоречие.

2. h — сюръекция

   Хотим найти такой x, что $h(x) = y$

   - $y \in f(C) \Rightarrow y = f(x) = h(x)$
   - $y \notin f(C)$.
     Рассмотрим $g(y)$
     Если $g(y) \notin C$, то $h(g(y)) = y$.
     В противном случае $g(y) \in C_n, n > 0$.
     В таком случае $g(y) = g(f(x')), x \in C_{n-1} \Rightarrow y = f(x') = h(x')$, так как $x' \in C$.

7. Отношения

Определение 7.1: Отношение

Отношение на множествах $A,\ B$ — это $R \subseteq A \times B$
$a\ R\ b \Leftrightarrow (a, b) \in R$

Пример 7.2

Функция — частный пример отношения

Определение 7.3

Пусть $R \subseteq A \times B,\ S \subseteq B \times C$ — отношения.
Тогда $S \circ R$ — это отношение на $A,\ C$.
$a\ (S \circ R)\ b \Leftrightarrow \exists b \in B : a\ R\ b \wedge b\ S\ c$

Пример 7.4

$A = B = C$ — множество людей.
$x\ R\ y$ — x сын y
$x\ S\ y$ — x брат y
Тогда:

1. $a\ (S \circ R)\ c \Rightarrow c$ дядя a

   (причем работает в обе стороны)

2. $a\ (R \circ S)\ c \Rightarrow c$ отец a

   (работает только в одну сторону)

3. $a\ (R \circ R)\ c \Rightarrow c$ дедушка a

Теорема 7.5

Пусть $R \subseteq A \times B,\ S \subseteq B \times C,\ T \subseteq C \times D$ — отношения.
Тогда $(T \circ S) \circ R = T \circ (S \circ R)$

Доказательство:
Левая и правая части — отношения на A, D
Левая часть:

$$a\ ((T \circ S) \circ R)\ d$$
$$\exists b \in B : a\ R\ b \wedge b\ (T \circ S)\ d$$
$$\exists b \in B,\ c \in C : a\ R\ b \wedge b\ S\ c \wedge c\ T\ d$$

Правая часть:

$$a\ (T \circ (S \circ R))\ d$$
$$\exists c \in C : a\ (S \circ R)\ c \wedge c\ T\ d$$
$$\exists b \in B,\ c \in C : a\ R\ b \wedge b\ S\ c \wedge c\ T\ d$$

Определение 7.6: Отношение эквивалентности

$R \subseteq A \times A$
Отношение R на множестве A — отношение эквивалентности, если оно удовлетворяет следующим условиям:

1. Рефлексивность

   $\forall a \in A\ (a\ R\ a)$

2. Симметричность

   $\forall a, b \in A\ (a\ R\ b \Rightarrow b\ R\ a)$

3. Транзитивность

   $\forall a, b, c \in A\ (a\ R\ b \wedge b\ R\ c \Rightarrow a\ R\ c)$

Пример 7.7

- A — множество людей, $x\ R\ y \Leftrightarrow x$ и y имеют одинаковые имена
- $A = \mathbb{Z},\ x\ R\ y \Leftrightarrow x \equiv_n y$
- $A = \mathbb{N}^2,\ (x, y)\ R\ (p, q) \Leftrightarrow xq = yp$

Пример 7.8

$A = \bigsqcup_{i \in I} A_i$.
Есть R на A.
$x\ R\ y \Leftrightarrow \exists i \in I : x, y \in A_i$.
Тогда R — отношение эквивалентности.

Теорема 7.9

Пусть $A \neq \varnothing$ и R — отношение эквивалентности.
Тогда существует разбиение $A = \bigsqcup_{i \in I} A_i$ такое, что

$$\forall x, y \in A \; x \; R \; y \Leftrightarrow \exists i \in I : x, y \in A_i$$

A_i называют классами эквивалентностями.

Доказательство:
$a \in A$, определим $[a] = \{x \in A \mid a \; R \; x\}$
Тогда

1. $\forall a \in A \; a \in [a] \Rightarrow A = \bigcup_{a \in A} [a]$
2. $\forall a, b \in A \; [a] \cap [b] = \begin{cases} \varnothing \\ [a] = [b] \end{cases}$

   Докажем это.

   Пусть $x \in [a] \cap [b]$

   $a \; R \; x \wedge x \; R \; b \Rightarrow a \; R \; b \Rightarrow b \in [a]$.

   Но тогда $\forall y \in [b] \; a \; R \; b \wedge b \; R \; y \Rightarrow a \; R \; y \Rightarrow y \in [a]$

   Значит $[b] \subseteq [a]$.

   Аналогично $[a] \subseteq [b]$, поэтому $[a] = [b]$
3. Если выкинем повторы, то получим $A = \bigcup_{i \in I} [a_i]$
4. Покажем, что $x \; R \; y \Leftrightarrow \exists i \in I : x, y \in [a_i]$

   - $\Rightarrow$
     $x \; R \; y \Rightarrow x \in [x], \; y \in [x]$
   - $\Leftarrow$
     $x, y \in [a_i] \Rightarrow x \; R \; a_i \wedge a_i \; R \; y \Rightarrow x \; R \; y$

Замечание 7.10

$\{A_i \mid i \in I\} = A/R$ — фактор множество A по R

8. Графы

8.1. Определения

Определение 8.1: Ориентированный граф

$G = (V, E)$, где V — конечное множество (вершины), а $E \subseteq V \times V$ — ребра.

Определение 8.2

Пусть в ориентированном графе — это последовательность $a_0, a_1, \ldots, a_k \in V$, причем $\forall\ 0 \leq i \leq k-1$ выполнено $(a_i, a_{i+1}) \in E$.
$k \geq 0$ — длина пути.
Пусть называется простым, если $a_0, a_1, \ldots, a_k$ различны.

Упражнение 8.3

Если в ориентированном графе G существует путь из x в y, то существует простой путь из x в y.

Определение 8.4

$x, y \in V$ сильно связаны в G, если есть путь как из x в y, так и из y в x

Лемма 8.5

Сильная связность на G — отношение эквивалентности на V

Следствие 8.6

$V = \bigsqcup_{i=1}^{t} V_i$, где V_i — класс сильно связных вершин.

Определение 8.7

V_i — компонента сильной связности.

Определение 8.8

G — сильно связный, если $t = 1$.

Определение 8.9: Степень вершины

Исходящая степень: $d_+(v) = |\{x \in V \mid (v, x) \in E\}|$
Входящая степень: $d_-(v) = |\{x \in V \mid (x, v) \in E\}|$

Теорема 8.10: Лемма о рукопожатиях

$$\sum_{v \in V} d_+(v) = \sum_{v \in V} d_-(v) = |E|$$

Определение 8.11

Цикл в ориентированном графе G — путь длины $k \geq 1$, в котором $a_0 = a_k$.

Определение 8.12: Ацикличность

Граф G называют ациклическим, если в G нет циклов.

Теорема 8.13

Пусть G — ориентированный граф без петель.
Тогда следующие утверждения эквивалентны:

1. G — ациклический.
2. Все компоненты сильной связности в G одноэлементны.
3. Можно пронумеровать вершины G в от 1 до n так, что $(i, j) \in E \Rightarrow i < j$ (топологическая сортировка)

Доказательство:

- $1 \to 2$

  Если размер какой-то компоненты сильной связности хотя бы 2, то в графе, очевидно, есть цикл (по определению компоненты сильной связности).

- $3 \to 1$

  Перенумеруем граф. Пусть есть цикл $a_0, a_1, \ldots, a_k$.

  Тогда $a_0 < a_1 < \ldots < a_k = a_0$ — противоречие.

- $2 \to 3$

  Докажем по индукции по количеству вершин:

  1. $n = 1$:
     Верно
  2. $n \to n + 1$:
     Покажем, что есть какая-то вершина, из которой не выходит ребра.
     Если это не так, то давайте сделаем граф конденсации. В нем нет циклов. Мы знаем, что из каждой компоненты сильной связности выходит

хотя бы одно ребро в другую компоненту (так как $|V_i| = 1$). Давайте пойдем по этим ребрам. Когда-нибудь мы посетим какую-нибудь вершину дважды. Поскольку в графе нет петель, мы нашли цикл, а такого в графе конденсации быть не может.

Противоречие $\Rightarrow$ есть вершина без исходящего ребра.

Теперь давайте выкинем эту вершину, пронумеруем оставшиеся (по индукции), после чего присвоим выкинутой вершине номер $n + 1$.

Научились получать топологическую сортировку.

8.2. Эйлеровы графы

Определение 8.14

Граф G — эйлеров, если в нем существует цикл, содержащий все ребра G по одному разу.

Теорема 8.15: Критерий Эйлеровости

1. Пусть G — неориентированный граф без изолированных вершин.

   Тогда G эйлеров $\Leftrightarrow$ G связен и $\forall v \in V$ $\deg(v)$ — четное.

2. Пусть G — ориентированный граф без изолированных вершин ($d_-(v) = d_+(v) = 0$).

   Тогда G эйлеров $\Leftrightarrow$ G сильносвязен и $\forall v \in V$ $d_-(v) = d_+(v)$.

Докажем второе:

- $\Rightarrow$

  Очевидно

- $\Leftarrow$

  Рассмотрим самый длинный путь, в котором все ребра различны.

  $v_0 \to v_1 \to \ldots \to v_k$

  Покажем, что $v_k = v_0$.

  Пусть это не так, тогда у нас просто путь.

  Пусть v_k встречается в цикле $d + 1$ раз. Все ребра из v_k есть в цикле (иначе можем продлить). Поэтому $d_+(v_k) = d$. Но $d_-(v_k) \geq d + 1$ — противоречие с критерием.

  Значит это цикл. Покажем, что это эйлеров цикл.

  Пусть это не так, значит существует ребро $(x, y) \notin$ цикл.

Существует путь $v_0 \to x \to y$. Тогда найдется такая вершина цикла v_i, что из нее ведет ребро (v_i, u) не из цикла. Но тогда мы можем удлинить наш путь, сделав $v_i, v_{i+1}, \ldots, v_i, u$.

Определение 8.16

$G = (V, E)$ — двудольный, если $\exists X, Y : V = X \sqcup Y$, причем

$$\forall e = \{a, b\} \in E \Rightarrow \begin{bmatrix} a \in X, b \in Y \\ a \in Y, b \in X \end{bmatrix}$$

Теорема 8.17: Критерий двудольности

G двудолен $\Leftrightarrow$ в G нет циклов нечетной длины.

Доказательство:

- $\Rightarrow$

  Пусть есть нечетный цикл $v_0, v_1, \ldots, v_k$

  Не умаляя общности $v_0 \in X \Rightarrow v_1 \in Y \Rightarrow v_2 \in X \Rightarrow \ldots$.

  В силу нечетности цикла получим, что $v_0 = v_k \in Y$ — противоречие.

- $\Leftarrow$

  Если G не связен, то проверим критерий отдельно для каждой компоненты связности. Теперь можно считать G связным.

  Зафиксируем какую-нибудь $v_0 \in V$.

8.3. Хроматическое число графа

8.3.1. Раскраски графа

Определение 8.18

$G = (V, E)$ правильно раскрашиваем в k цветов, если $\exists f : V \to \{1, \ldots, k\} : \forall \{x, y\} \in E \ f(x) \neq f(y)$

Определение 8.19: Хроматическое число

Хроматическое число G:
$\mathcal{X}(G) = \min\{k \in \mathbb{N} \mid G$ правильно раскрашиваем в k цветов$\}$

Определение 8.20: Кликовое число

Клика в G — это $W \subseteq V : \forall a \neq b \in W \ \{a, b\} \in E$
Кликовое число G:
$\omega(G) = \max\{m \in \mathbb{N} \mid \exists \text{ клика } W \subseteq V, |W| = m\}$

Определение 8.21: Число независимости

Независимое множество в G — это $U \subseteq V : \forall a \neq b \in U \ \{a, b\} \notin E$
Число независимости G:
$\alpha(G) = \max\{m \in \mathbb{N} \mid \exists \text{ независимое множество } W \subseteq V, |W| = m\}$

Свойства $\mathcal{X}(G)$

1. $1 \leq \mathcal{X}(G) \leq n$
2. $\mathcal{X}(G) \geq \omega(G)$
3. $G = \bigsqcup_{i=1}^{s} G_i$ — разбиение на компоненты связности $\Rightarrow \mathcal{X}(G) = \max\limits_{i=1,\ldots,s} \mathcal{X}(G_i)$
4. $\mathcal{X}(G) \leq n - \alpha(G) + 1$
5. $\mathcal{X}(G) \cdot \alpha(G) \geq n$

   Доказательство:

   Пусть $\mathcal{X}(G) = k$.

   Рассмотрим все вершины покрашенный в цвет i: V_i.

   V_i — независимое множество $\Rightarrow |V_i| \leq \alpha(G)$

   $n = |V_1| + \ldots + |V_k| \leq \alpha(G) \cdot k$
6. $\Delta(G) = \max\limits_{v \in V} \deg v$

   $\mathcal{X}(G) \leq \Delta(G) + 1$.

   Работает жадная покраска: в любой момент времени у вершины покрашено не больше $\Delta(G)$ соседей, поэтому точно найдется отличный от них цвет.

Лемма 8.22

Пусть G связен и $\exists v \in V : \deg v < \Delta(G) \Rightarrow \mathcal{X}(G) \leq \Delta(G)$

Доказательство:

Пусть эта вершина v_0. Сделаем остовное дерево и подвесим его за v_0.

Будем красить дерево сверху вниз. Тогда для всех вершин кроме корня $< \Delta(G)$ детей, так как $\deg u \leq \Delta(G)$, значит сможем покрасить. А у корня детей тоже $< \Delta(G)$, так как $\deg v_0 < \Delta(G)$.

Теорема 8.23: Теорема Брукса (без доказательства)

Пусть G — связный граф и $G \neq K_n$ (полный граф), C_{2n+1} (простой цикл нечетной длины)
Тогда $\mathcal{X}(G) \leq \Delta(G)$

8.3.2. Хроматический многочлен

Определение 8.24: Хроматический многочлен

G — граф, $\mathcal{X}_G(k)$ — количество правильных раскрасок G в k цветов.

Пример 8.25

- Пустой граф на n вершинах: $\mathcal{X}_G(k) = k^n$
- Полный граф на n вершинах: $\mathcal{X}_G(k) = \frac{k!}{(k-n)!}$
- Дерево на n вершинах: $\mathcal{X}_G(k) = k \cdot (k-1)^{n-1}$

Теорема 8.26: Теорема Уитни

Пусть G — граф на n вершинах и m ребрах с s компонентами связности.
Тогда $\mathcal{X}_G(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \ldots + (-1)^{n-s} a_{n-s} x^s$, где $a_1, \ldots, a_{n-s} \in \mathbb{N}$, причем $a_1 = m$.

Лемма 8.27

Пусть G — граф, $\{u, v\} \in E$.
$G - uv$ — удаление ребра $\{u, v\}$
$G \cdot uv$ — стягивание ребра $\{u, v\}$
Тогда $\mathcal{X}_{G-uv}(k) = \mathcal{X}_G(k) + \mathcal{X}_{G \cdot uv}(k)$

Раскраски бывают двух разных цветов:

- u и v разных цветов

  Такая раскраска неотличима от раскраски G

- u и v одинаковых цветов

  Такая раскраска неотличима от раскраски $G \cdot uv$

Теперь докажем теорему Уитни полной индукцией по m.
База $m = 0$: проверили выше
Переход $< m \to m$:
Рассмотрим ребро $\{u, v\} \in E$.

По лемме $\mathcal{X}_G(x) = \mathcal{X}_{G-uv}(x) - \mathcal{X}_{G\cdot uv}(x)$
В G: n вершин, m ребер, s компонент связности.
В $G - uv$: n вершин, $m-1$ ребер, s или $s+1$ компонента связности.
В $G \cdot uv$: $n-1$ вершин, $< m$ ребер, s компонент связности.

$$\mathcal{X}_G(x) = (x^n - (m-1)x^{n-1} + a_2x^{n-2} - \ldots + (-1)^{n-s}a_{n-s}x^s) -$$
$$-(x^{n-1} - b_1x^{n-1} + b_2x^{n-2} - \ldots + (-1)^{n-1-s}b_{n-1-s}x^s) =$$
$$= x^n - mx^{n-1} + (a_2+b_1)x^{n-2} - (a_3+b_2)x^{n-3} + \ldots + (-1)^{n-s}(a_{n-s}+b_{n-1-s})x^s$$

Поскольку $a_1, a_2, \ldots, a_{n-1-s}, b_1, b_2, \ldots, b_{n-1-s} > 0$ и $a_{n-s} \geq 0$, теорема доказана.

8.3.3. Графы с большим хроматическим числом

Существует ли граф с "большим" хроматическим числом, не содержащий треугольников?

$$G : \mathcal{X}(G) > k, \omega(G) = 2$$

Пример Зыкова (1949) - Мыцельского (1955)

Определение 8.28

Пусть $G = (V, E)$ — граф.
Мыцельскиан G — это граф $\mu(G) = (V', E')$:

$$V' = \{v_1, v_2, \ldots, v_n, u_1, u_2, \ldots, u_n, \omega\}$$
$$E' = E \cup \{(v_i, u_j) \mid \forall i, j : (v_i, v_j) \in E\} \cup \{(\omega, u_i) \mid i = 1, \ldots, n\}$$

Теорема 8.29

Пусть $G_2 = K_2, G_3 = \mu(G_2), \ldots, G_t = \mu(G_{t-1}), t \geq 3$.
Тогда G_t — граф без треугольников, причем $\mathcal{X}(G_t) = t$.

Докажем индукцией по t.

- База:

  $t = 2$ — очевидно.

  $t = 3$ — $G_3 = C_5$ — очевидно.

- Переход $< t \to t$.

  Покажем, что в G_t нет треугольников.

  Поскольку u_i не соединено с u_j, возможен только треугольник вида v_i, v_j, u_k.

  $i, j \neq k$, так как иначе в G_{t-1} были бы петли.

  С другой стороны, если в G_t есть такой треугольник, в G_{t-1} был бы треугольник v_i, v_j, v_k — противоречие.

Теперь докажем, что $\mathcal{X}(G_t) \leq t$.

Знаем, что $\mathcal{X}(G_{t-1}) = t-1$, поэтому давайте покрасим v_i, а после сделаем у u_i такой же цвет как и у v_i.

ω покрасим в новый цвет.

Теперь сделаем оценку в другую сторону: $\mathcal{X}(G_t) \geq t$.

От противного: $\mathcal{X}(G_t) = t-1$ (так как $\mathcal{X}(G_{t-1}) = t-1$).

Допустим, раскрасили G_t в $t-1$ цвет, причем ω покрашена в $t-1$.

Тогда u_i покрашены в цвета $1, \ldots, t-2$.

Давайте научимся красить G_{t-1} в $t-2$ цвета:

$$c'(v_i) = \begin{cases} c(v_i) \text{ если } c(v_i) \neq t-1 \\ c(u_i), \text{ если } c(v_i) = t-1 \end{cases}$$

Покажем, что эта раскраска корректна. Когда раскраска могла сломаться? Если у каких-то вершин совпали цвета, то значит, мы перекрасили одну из них.

$c'(v_i) = c(u_i), c'(v_j) = c(v_j)$.

Но в G_t есть ребро (u_i, v_j) — противоречие.

По предположению индукции G_{t-1} нельзя корректно покрасить в $t-2$ цвета — снова противоречие.

Значит $\mathcal{X}(G_t) = t$

8.4. Паросочетания и вершинные покрытия

Определение 8.30: Паросочетание

Пусть G — граф, паросочетание в G — это $M \subseteq E : \forall m_1 \neq m_2 \in M \; m_1 \cap m_2 = \varnothing$

Определение 8.31: Вершинное покрытие

Пусть G — граф, вершинное покрытие в G — это $U \subseteq V : \forall \{a, b\} \in \quad a \in U \vee b \in U$

Предложение 8.32

Пусть G — граф, M — паросочетание в G, U — вершинное покрытие в G. Тогда $|M| \leq |U|$

Среди концов каждого ребра паросочетания должна быть хотя бы одна вершина из вершинного покрытия — доказали.

Следствие 8.33

$\max |M| \leq \min |U|$.

Теорема 8.34: Теорема Кенига

Если G — двудольный граф, то $\max |M| = \min |U|$

$G = (L \cup R, E)$

Определение 8.35: Чередующийся путь

Чередующийся путь относительно M — это простой по ребрам путь длины хотя бы один, стартующий в $a \in L$, не покрытой M, ребра в котором чередуются: $\notin M, \in M, \notin M, \ldots$

Определение 8.36: Увеличивающий путь

Увеличивающий путь относительно M — чередующийся путь, завершающийся в $b \in R$, не покрытой M

Упражнение 8.37

Если существует увеличивающий путь относительно M, то M не максимально.

Упражнение 8.38

M — максимальное паросочетание $\Leftrightarrow$ не существует увеличивающего пути относительно M

Докажем теорему Кенига:
Рассмотрим паросочетание M максимального размера.
Строим $U \subseteq V$:

$$\forall \{x, y\} \in M$$

$$\begin{cases} y \in U, \ \exists \text{ чередующийся путь относительно } M, \text{ оканчивающийся в } y \\ x \in U, \ \text{иначе} \end{cases}$$

Рассмотрим ребро $\{a, b\} \in E$.
Для $\{a, b\} \in M$ очевидно, дальше считаем, что $\{a, b\} \notin M$

1. a не покрыта M

   (a) b не покрыта M
   Тогда $\{a, b\}$ в M — увеличивающий путь $\Rightarrow$ противоречие.

   (b) b покрыта M
   Тогда $b \in U$, так как $\{a, b\}$ — чередующийся путь относительно M, заканчивающийся в b

2. a покрыта M

   В таком случае $\exists\{a, b'\} \in M$. Если $b' = b$, то $\{a, b\}$ лежит в $M \Rightarrow$ точно покрыто U. Значит можно считать $b' \neq b$.

   Если $a \in U$, то точно верно, поэтому дальше считаем, что $b' \in U$. Это значит, что существует чередующийся путь из a' в b'. Возьмем такой кратчайший путь. По очевидной причине в нем нет ребра $\{b', a\}$. Если ребра $\{a, b\}$ нет в нашем пути, то добавим его и получим чередующийся путь из a' в b, а если есть, то, получается, некоторый префикс пути является чередующимся из a' в b.

   В любом случае найдем чередующийся путь из a' в b

   (a) b не покрыта M
   Тогда чередующийся путь из a в b — увеличивающий $\Rightarrow$ противоречие.

   (b) b покрыта M
   $\{a'', b\} \in M$.
   Но тогда $b \in U$, так как существует чередующийся путь из a' в b.

Разобрали все случаи $\Rightarrow$ доказали теорему.

Теорема 8.39: Лемма Холла

Пусть $G = (L \cup R, E)$
$S \subseteq L$, пусть $N(S) = \{y \in R \mid \exists x \in S : \{x, y\} \in E$
Существует паросочетание мощности $|L|$ тогда и только тогда, когда $\forall S \subseteq L$ верно $|S| \leq |N(S)|$.

Доказательство:

- $\Rightarrow$

  Тривиально.

- $\Leftarrow$

  Если вершина R является изолированной, выкинем ее. Теперь из каждой вершины R выходит какое-нибудь ребро в L.

  Используем теорему Кенига: $\max |M| = \min |U|$.

  Рассмотрим какое-то U.

  Теперь пусть $L = L_1 \sqcup L_2$, $R = R_1 \sqcup R_2$, причем $U = L_1 \cup R_2$.

  Тогда нетрудно понять, что между L_2 и R_1 нет ребер, но при этом есть между L_2 и R_2; L_1 и R_2; L_1 и R_1.

  $|L_2| \leq |N(L_2)| \leq |R_2|$. Тогда $|U| = |L_1| + |R_2| \geq |L_1| + |L_2| = |L|$.

  Но L, очевидно, является вершинным покрытием, поэтому $\min |U| = |L|$. Значит и $\max |M| = |L|$, что и требовалось доказать.

8.5. Числа Рамсея

Упражнение 8.40

Из 6 человек можно выбрать трех попарно знакомых или попарно незнакомых людей (знакомство взаимно).

Определение 8.41

Пусть $n, k \geq 1$
Тогда $R(n, k)$ — минимальное число $N \in \mathbb{N} : \forall G$ на $\geq N$ вершинах в G найдется клика размера n или независимое множество размера k.

Свойства:

1. $R(n, k) = R(k, n)$
2. $R(1, k) = 1$
3. $R(2, k) = k$

Теорема 8.42

$R(n,k) \le R(n-1,k) + R(n,k-1)$

Докажем индукцией по сумме:
База $n = 2, 3$: косвенно описана выше в свойствах
Рассматриваем $n + k$:
Пусть $R(n-1,k) + R(n,k-1) = N$.
Рассмотрим граф с $\ge N$ вершинами.
Посмотрим на какую-нибудь вершину v.
Пусть X — множество вершин, с которым v соединено, Y — остальные.
Тогда $|X| \ge R(n-1,k)$ или $|Y| \ge R(n,k-1)$.
В обоих случаях найдем либо клику размера n, либо независимое множество размера k.

Следствие 8.43

$$R(n,k) \le C(n+k-2, n-1) = C(n+k-2, k-1)$$

Доказательство: очевидно по индукции.

9. Частично упорядоченные множества

9.1. Отношения частичного порядка

Определение 9.1: Отношение строгого частичного порядка

Отношение R на A называется отношением строгого порядка, если:

1. $\neg\ a\ R\ a$ (иррефлексивность)
2. $a\ R\ b\ \wedge\ b\ R\ c \Rightarrow a\ R\ c$ (транзитивность)

$R\ = <$

Определение 9.2: Отношение нестрогого частичного порядка

Отношение R на A называется отношением нестрогого порядка, если:

1. $a\ R\ a$ (рефлексивность)
2. $a\ R\ b\ \wedge b\ R\ a \Rightarrow a = b$ (антисимметричность)
3. $a\ R\ b\ \wedge\ b\ R\ c \Rightarrow a\ R\ c$ (транзитивность)

$R\ = \leq$

Лемма 9.3: О связи строгого и нестрогого порядков

- $\leq$ — нестрогий порядок на $A \Rightarrow < = \leq\ \setminus\{(a,a) \mid a \in A\}$ - отношение строгого порядка на A
- $<$ — строгий порядок на $A \Rightarrow \leq = <\ \cap\{(a,a) \mid a \in A\}$ - отношение строгого порядка на A

Доказательство:

- 1. $\neg\ a\ R\ a$ — очевидно.
  2. $a\ R\ b\ \wedge b\ R\ c \Rightarrow a \neq b, b \neq c, a \leq b, b \leq c \Rightarrow a \leq c$
     Если $a = c$, то $a \leq b, b \leq a \Rightarrow a = b$ — противоречие.
- 1. $a\ R\ a$ — очевидно.
  2. Пусть $a \leq b \wedge b \leq a$
     Допустим, что $a \neq b$. Тогда $a < b \wedge b < a$, получили противоречие иррефлексивности.
  3. $a \leq b \wedge b \leq c$

Если $a = b$ или $b = c$, то очевидно.
Иначе $a < b \wedge b < c \Rightarrow a < c \Rightarrow a \leq c$

9.2. Частично упорядоченные множества

Определение 9.4: Частично упорядоченное множество

Множество $A \neq \varnothing$ с заданным на нем отношением частичного порядка называется частично упорядоченным множеством.
$(A, <), (A, \leq)$

Пример 9.5

1. $(\mathbb{N}, \leq)$
2. $(\mathbb{N}, |)$ (отношение делимости)
3. $(\mathbb{Z} \setminus \{0\}, |)$ — не ЧУМ $((-1)|1, 1|(-1)$, но $-1 \neq 1)$
4. $(2^A, \subseteq)$
5. $(\mathbb{B}^n, \leq)$

9.3. Операции над порядками

1. Покоординатный порядок $(P \times Q, \leq)$:
$$(p_1, q_1) \leq (p_2, q_) \Leftrightarrow \begin{cases} p_1 \leq_P p_2 \\ q_1 \leq_Q q_2 \end{cases}$$
2. Лексикографический порядок $(P \times Q, \leq)$:
$(p_1, q_1) \leq (p_2, q_2) \Leftrightarrow p_1 < p_2 \vee (p_1 = p_2 \wedge q_1 \leq q_2)$
3. Считаем, что $P \cap Q = \varnothing$
$P + Q = (P \sqcup Q, \leq)$:
$$x \leq y \Leftrightarrow \begin{cases} x \leq_P y \\ x \leq_Q y \\ x \in P, y \in Q \end{cases}$$

Определение 9.6: Изоморфизм

Пусть $(P, \leq_P), (Q, \leq_Q)$.
Тогда говорят, что они изоморфны, если существует биекция $\varphi : P \to Q$

такая, что $\forall x, y \in P\ x \leq_P y \Leftrightarrow \varphi(x) \leq_Q \varphi(y)$.
Обозначается $(P, \leq_P) \cong (Q, \leq_Q)$

Пример 9.7

1. $(\mathbb{N}, \leq) \cong (\mathbb{N} \cup \{0\})\ \varphi(n) = n - 1$
2. $(\mathbb{Q}, \leq) \ncong (\mathbb{R}, \leq)$, так как нет биекции.
3. $([0, 1], \leq) \ncong ((0, 1), \leq)$, так как нет наименьшего и наибольшего элементов.

Определение 9.8

$a \in P$ — минимальный, если $\nexists b \in P : b < a$
$a \in P$ — наименьший, если $\forall b \in P\ a \leq b$
$a \in P$ — максимальный, если $\nexists b \in P : b > a$
$a \in P$ — наибольший, если $\forall b \in P\ a \geq b$

Пример 9.9

$(Z, \leq) \ncong (Q, \leq)$

Определение 9.10: Плотный порядок

$\forall a < b\ \exists c : a < c \wedge c < b$

$(Q, \leq)$ — плотный порядок, а $(Z, \leq)$ — нет.

Определение 9.11: Отрезок

Для $a \leq b$ $[a, b] = \{c \in P \mid a \leq c \wedge c \leq b\}$

Если $\varphi : P \to Q$ — изоморфизм порядков, то $\phi([a, b]) = [\phi(a), \phi(b)]$. Доказательство тривиально.

9.4. Фундированные подмножества

Определение 9.12: Фундированное множество

ЧУМ $(P, \leq)$ называется фундированным, если $\forall X \subseteq P, x \neq \varnothing$ имеет минимальный элемент.

Пример 9.13

- $(N, \leq)$ — фундированное
- $(Z, \leq)$ — не фундированное, возьмем $X = \mathbb{Z}$

Теорема 9.14

Для ЧУМ-а $(P, \leq)$ эквивалентны следующие условия:

1. $\forall X \subseteq P, x \neq \varnothing \Rightarrow X$ имеет минимальный элемент.
2. $\nexists$ бесконечно убывающей цепи $p_1 > p_2 > p_3 > \dots$
3. Для P справедлив принцип индукции:
   $\forall p \in P\ ((\forall q < p\ A(q) - \text{ист}) \Rightarrow A(p) - \text{ист}) \Rightarrow \forall p \in P\ A(p) - \text{ист}$

Доказательство:

1. $1 \Rightarrow 2$

   Докажем от противного: есть бесконечная цепь $\Rightarrow$ нет минимального

2. $2 \Rightarrow 1$

   Вновь докажем от противного. Построим бесконечную цепь: в $X \subseteq P$ нет минимального, значит всегда можем найти новый элемент для цепи.

3. $1 \Rightarrow 3$

   Пусть $X = \{p \in P \mid A(p) - \text{ложно}\} \neq \varnothing$.

   Рассмотрим p' — минимальный элемент в X.

   Но тогда $\forall q < p'\ A(q)$ — ист. Значит $A(p')$ — ист $\Rightarrow$ противоречие $\Rightarrow X = \varnothing$.

4. $3 \Rightarrow 1$

   Пусть $X \subseteq P, X \neq \varnothing$, и $A(p) = p \notin X$

   Допустим, что X не имеет минимальных элементов.

   $\forall p \in P\ ((\forall q < p\ q \notin X) \Rightarrow p \notin X)$ — верно, так как иначе p — минимальный элемент.

Но тогда $\forall p\ p \notin X \Rightarrow X = \varnothing$ — противоречие.

Значит у $\forall X \subseteq P$ есть минимальный элемент.

9.5. Что-то про изоморфизмы

Теорема 9.15

Пусть $(P, \leq_P)$, $(Q, \leq_Q)$ — счетные плотные линейные порядки без наименьшего и наибольшего элементов.
Тогда $(P, \leq_P) \cong (Q, \leq_Q)$

Доказательство:

$$P = \{p_1, p_2, p_3, \ldots\}$$
$$Q = \{q_1, q_2, q_3, \ldots\}$$

Строим изоморфизм $\varphi : P \to Q$

Возьмем наименьший (по номеру) невзятый элемент из P, пусть это p.

Пусть отсортированные уже взятые p_i — $a_1, \ldots, a_k$, а q_i — $b_1, \ldots, b_k$.

Он расположен между какими-то двумя уже взятыми $a_i \leq q \leq a_{i+1}$ (или перед a_0 / после a_{k-1})

Но за счет плотности и отсутствия наибольшего (и наименьшего элемента) у нас найдется элемент из Q, который находится между b_i и b_{i+1}.

Давайте продолжать выбирать так пары элементов, поочередно беря то минимальный по номеру невзятый p_i, то q_i.

9.6. Цепи и антицепи

Пусть $(P, \leq)$ — ЧУМ

Определение 9.16

Цепь в P — это $\varnothing \neq C \subseteq P : \forall x, y \in C\ x \leq y \vee y \leq x$
Антицепь в P — это $\varnothing \neq A \subseteq P : \forall x \neq y \in A\ x, y$ не сравнимы

Упражнение 9.17

Если C — цепь в P, а A — антицепь в P, то $|A \cap C| \leq 1$

Упражнение 9.18

Пусть P — конечный ЧУМ
Пусть множество разбивается на k цепей.
Тогда $\max |A| \leq k$

Пусть множество разбивается на l антицепей.
Тогда $\max |C| \leq l$

Теорема 9.19: Теорема Мирского

Пусть P — конечный ЧУМ
Пусть P можно разбить на l антицепей и нельзя разбить на меньшее число.
Тогда $\max |C| = l$

Учитывая упражнения выше, достаточно показать, что можно разбить множество на $\max |C| = l$ антицепей.

$\min X = \{x \in X \mid x - \text{минимальный в } X\}$

$$P_1 = \min P$$
$$P_2 = \min(P \setminus P_1)$$
$$P_3 = \min(P \setminus (P_1 \cup P_2))$$
$$\vdots$$
$$P_k = \min(P \setminus (P_1 \cup \ldots \cup P_{k-1}))$$
$$\vdots$$

$P_1, \ldots, P_m$ — антицепи, причем не пересекаются.
$p_m \in P_m \Rightarrow \exists p_{m-1} \in P_{m-1} : p_m > p_{m-1}$.
Значит можем так достать цепь $p_m > p_{m-1} > \ldots > p_1$.
Отсюда $m \leq \max |C| = l \leq m \Rightarrow l = m$, что и требовалось доказать.

Теорема 9.20: Теорема Дилуорса

Пусть P — конечный ЧУМ
Пусть P можно разбить на k цепей и нельзя разбить на меньшее число.
Тогда $\max |A| = k$

Нужно доказать только $\max |A| \geq k$, неравенство в обратную сторону было раньше в упражнении.

Докажем по индукции по размеру множества:
База: $s = 1$ — очевидно.
Переход: $< s \to s$
Рассмотрим минимальный элемент $m \in P$.
Удалим его: $P \setminus \{m\} = P'$. Рассмотрим в полученном множестве $\max\limits_{A \in P'} |A| = l$.
Очевидно, что в изначальном множестве $\max\limits_{A \in P} |A| = l$ или $l + 1$.

- Случай $\max\limits_{A \in P} |A| = l+1$ очевиден, так как в новой антицепи точно содержится m, а значит его можно покрыть отдельной цепью из одного элемента.
- Теперь разберем случай $\max\limits_{A \in P} |A| = l$.

  Рассмотрим разбиение P' на цепи $C_1, C_2, \ldots, C_l$. p_i — наименьший возможный элемент в C_i, входящий в антицепь размера l в P'.

  Покажем, что $\{p_1, \ldots, p_l\}$ — антицепь.

  Предположим противное, путь $p_i < p_j$.

  Рассмотрим антицепь A размера l, в которой находится p_i.

  $A \cap C_j = \{y\}$

  $p_j \leq y$, так как p_j — наименьший возможный в такой антицепи.

  Но тогда $p_i < p_j \leq y$ — противоречие, так как p_i и y находятся в A.

  Размер антицепи не меняется при добавлении $m \Rightarrow \exists j : p_j$ сравним с m.

  m — минимальный, поэтому $m < p_j$.

  Давайте обрежем начало цепи C_j перед p_j, заменим на m, получим $C = m \to p_j \to \ldots$.

  Давайте выкинем эту цепь, получим новое множество. Понятно, что в этом новом множестве размер антицепи не превышает l, так как есть разбиение на l цепей.

  Но размер не может быть l, так как тогда бы в остатке (начале) цепи был элемент из антицепи, меньший p_j. Значит антицепи не превышает $l-1$, значит есть разбиение $P \setminus C$ на $l-1$ цепь. Вернем C, получим разбиение P на l цепей.

  Значит $\max |A| \geq l$, что и требовалось доказать.

9.7. Цепи и антицепи в булевом кубе

$\mathbb{B}^n = \{0,1\}$, $\leq$ — покоординатно, то есть $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n) \Leftrightarrow \forall i\ a_i \leq b_i$

Определение 9.21

Вес набора $\tilde{a} = (a_1, \ldots, a_n) \in \mathbb{B}^n$ — количество единиц в нем.
Обозначается $|\tilde{a}|$

Определение 9.22

Уровни $\mathbb{B}^n$: $B_0, B_1, \ldots, B_n$
$B_k = \{$все наборы веса $k\}$
Не трудно заметить, что $|B_k| = C_n^k$

Упражнение 9.23

Максимальная цепь в $\mathbb{B}^n$ имеет длину $n+1$

Теорема 9.24: Теорема Шпернера

Максимальный размер антицепи в $\mathbb{B}^n$ — $C_n^{\lfloor \frac{n}{2} \rfloor}$

Лемма 9.25: LYM-неравенство

Lubell (1966), Yamamoto (1954), Meshalkin (1963)
Пусть A — антицепь в $\mathbb{B}^n$. Обозначим $a_k = |A \cap B_k|$
Тогда $\sum\limits_{k=0}^{n} \frac{a_k}{C_n^k} \leq 1$

Зададимся вопросами:

1. Сколько всего цепей размера $n+1$ в $\mathbb{B}^n$?

   Ответ: $n!$

2. Сколько есть цепей размера $n+1$ в $\mathbb{B}^n$ проходят через $\tilde{a}$ на уровне k?

   Ответ: $k!(n-k)!$

$$n! \geq \sum_{a \in A} |a|! \cdot (n - |a|)! = \sum_{k=0}^{n} k!(n-k)! a_k$$
$$\Downarrow$$
$$\sum_{k=0}^{n} \frac{a_k}{C_n^k} \leq 1$$

Вернемся к доказательству теоремы Шпернера:

$$\sum_{k=0}^{n} \frac{a_k}{C_n^{\lfloor \frac{n}{2} \rfloor}} \leq \sum_{k=0}^{n} \frac{a_k}{C_n^k} \leq 1$$
$$\Downarrow$$
$$|A| = \sum_{k=0}^{n} a_k \leq C_n^{\lfloor \frac{n}{2} \rfloor}$$

9.8. Графы сравнимости

Определение 9.26

Пусть $(P, \leq)$ — конечный ЧУМ. Его графом сравнимости называется граф G_P: $V = P$, $\{x, y\} \in E \Leftrightarrow x < y \vee y < x$

Определение 9.27

G — совершенный, если $\forall$ индуцированного подграфа $H \subseteq G$ $\mathcal{X}(H) = \omega(H)$

Определение 9.28

Для $\forall$ конечного ЧУМ-а P его граф сравнимости G_P и $\overline{G_P}$ — совершенные графы.

Теорема 9.29: Strong Perfect Graph Theorem

Граф G является совершенным, если и только если среди его индуцированных подграфов нет ни C_m, ни $\overline{C_m}$ для нечётного $m > 3$.

10. Дискретная теория вероятностей

10.1. Вероятность

Определение 10.1: Вероятностное пространство

Вероятностное пространство — (Ω, P), где $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$ — множество элементарных исходов, а P — функция $\Omega \to \mathbb{R}$, обладающая свойствами:

- $0 \leq P(\omega_i) \leq 1$
- $\sum\limits_{i=1}^{n} P(\omega_i) = 1$

Пример 10.2

1. Подбрасывание монетки: $\Omega = \{\text{O}, \text{P}\}$, вероятности — $\frac{1}{2}$
2. Подбрасывание кубика: $\Omega = \{1, 2, 3, 4, 5, 6\}$, вероятности — $\frac{1}{6}$

Определение 10.3: Событие

Событие A — подмножество Ω
Вероятность события $P(A) = \sum\limits_{\omega_i \in A} P(\omega_i)$

Пример 10.4

3. Подбрасывание нечестной монетки t раз

   Решка падает с вероятностью p, орел с $1 - p$

   Тогда $\Omega = \{0, 1\}^t$

   $P(\{a_1, \ldots, a_t\}) = p^{|a|} \cdot (1 - p)^{t - |a|}$

4. Равновероятный случай

   $P(\omega_i) = \frac{1}{n}$

   Тогда $P(A) = \frac{|A|}{n}$

10.2. Дерево событий

Не повезло, мне лень это рисовать в tikz.

Условно, если хотим как-то описать все события вида “случайная перестановка из символов $(1, 2, 3)$” можно просто сделать бор, написав на ребрах вероятности.

10.3. Свойства вероятности

1. $P(\varnothing) = 0, P(\Omega) = 1$
2. $P(A \sqcup B) = P(A) + P(B)$
3. $P(\overline{A}) = 1 - P(A)$
4. $A \subseteq B \Rightarrow P(A) \leq P(B)$
5. Формула включений-исключений

Теорема 10.5

Пусть (Ω, P) — вероятностное пространство, $A_1, \ldots, A_n$ — события. Тогда выполнено

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

Введем индикаторную функцию $I_A : \Omega \to R$, $I_A(x) = (x \in A)$.

Отсюда следует несколько очевидных свойств:

- $I_{A \cap B} = I_A \cdot I_B$
- $I_{\overline{A}} = 1 - I_A$
- $I_{A \cup B} = I_A + I_B - I_{A \cap B}$

$$I_{\overline{A_1 \cup \ldots \cup A_n}} = I_{\overline{A_1} \cap \ldots \cap \overline{A_n}} = I_{\overline{A_1}} \cdot \ldots \cdot I_{\overline{A_n}} = (1 - I_{A_1}) \ldots (1 - I_{A_n})$$
$$\Downarrow$$
$$I_{A_1 \cup \ldots \cup A_n} = 1 - (1 - I_{A_1}) \ldots (1 - I_{A_n})$$

Раскрыв скобочки в последнем равенстве получим искомое.

Пример 10.6: Задача о беспорядках

$\Omega = S_n$, перестановки равновероятны.
$\sigma \in S_n$ — беспорядок, если $\forall i \ \sigma(i) \neq i$
Необходимо посчитать $P(\sigma$ — беспорядок$)$

$Y_i = \{\sigma \in S_n \,|\, \sigma(i) = i\}$
$P(\sigma$ — не беспорядок$) = P(Y_1 \cup \ldots \cup Y_n)$

$$P(Y_{i_1} \cap \ldots \cap Y_{i_k}) = \frac{(n-k)!}{n!}$$

$$\Downarrow$$

$$P(Y_1 \cup \ldots \cup Y_n) = \sum_{k=1}^{n} (-1)^{k+1} C_n^k \frac{(n-k)!}{n!} = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}$$

$$\Downarrow$$

$$P(\sigma \text{ — беспорядок}) = 1 - \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

При большом n такая штука стремится к $\frac{1}{e}$

10.4. Условная вероятность

$P(A|B)$ — вероятность события A при условии B

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

Пример 10.7

Есть коробки, пронумерованные от 1 до 4, и один шарик.
Сначала равновероятно выбирается коробка, а потом подбрасывается монетка, и с вероятностью $\frac{1}{2}$ шарик кладется в выбранную коробку.
Ведущий показал, что в первых трех коробках нет шара, какова вероятность, что он в четвертой?

A — шарик в четвертой коробке, B — шарик не в первых трех коробках.
$P(B) = \frac{5}{8}$ и $P(A \cap B) = \frac{1}{8}$
Получаем, что ответ равен $\frac{1}{5}$

10.5. Формулы полной вероятности и Байеса

Теорема 10.8: Формула полной вероятности

Пусть (Ω, P) — вероятностное пространство и $\Omega = \bigsqcup_{i=1}^{m} A_i$, причем $P(A_i) > 0$

Тогда $P(B) = \sum_{i=1}^{n} P(B|A_i) \cdot P(A_i)$

$$\sum_{i=1}^{n} P(B|A_i) \cdot P(A_i) = \sum_{i=1}^{n} P(A_i \cap B) = P(B \cap (A_1 \cup \ldots \cup A_n)) = P(B)$$

Теорема 10.9: Формула Байеса

Пусть (Ω, P) — вероятностное пространство.
Есть события A, B ненулевой вероятности.
Тогда $P(B|A) = \dfrac{P(A|B) \cdot P(B)}{P(A)}$

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

Пример 10.10

Болеет 1% населения.
Тест на болезнь ошибается в 1% случаев.

Посчитаем P(человек болен (A) | тест положительный (B))

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)} = \frac{99\% \cdot 1\%}{P(B|A) \cdot P(A) + P(B|\overline{A}) \cdot P(\overline{A})} =$$
$$= \frac{99\% \cdot 1\%}{99\% \cdot 1\% + 1\% \cdot 99\%} = 0.5$$

10.6. Независимые события

Пусть (Ω, P) — вероятностное пространство.

Определение 10.11

- A и B — независимые события, если $P(A \cap B) = P(A) \cdot P(B)$
- $A_1, \ldots, A_m$ — независимые в совокупности, если для любого подмножества $A_{i_1}, \ldots, A_{i_k}$ выполнено

$$P(A_{i_1} \cap \ldots \cap A_{i_k}) = P(A_{i_1}) \cdot \ldots \cdot P(A_{i_k})$$

Приведем пример, показывающий недостаточность попарной независимости для независимости в совокупности:

Пример 10.12

Подбросим монетку дважды.
A_1 — в первом броске выпал орел
A_2 — во втором броске выпал орел
B — выпал ровно один орел
Нетрудно убедиться, что события попарно независимы, но при этом

$$P(A_1 \cap A_2 \cap B) = 0 \neq \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}$$

Упражнение 10.13

Докажите, что при подбрасывании монетке события вида A_i = (в i-м броске выпал орел) независимы в совокупности.

10.7. Математическое ожидание

(Ω, P) — вероятностное пространство.

Определение 10.14

Случайная величина — это $f : \Omega \to \mathbb{R}$

Определение 10.15

Математическое ожидание f — это $E(f) = p_1 f(\omega_1) + \ldots + p_n f(\omega_n) = \sum\limits_{i=1}^{n} p_i f(\omega_i)$

Пример 10.16

Математическое ожидание выпавшего на игральном кубике числа:

$$\frac{1}{6} \cdot (1 + 2 + 3 + 4 + 5 + 6) = \frac{21}{6} = 3.5$$

Свойства математического ожидания:

- $f = const = c$ — константная случайная величина
  $E(f) = c$

- $A \subseteq \Omega$ — событие, $I_A(\omega) = \begin{cases} 1, \ \omega \in A \\ 0, \ \omega \notin A \end{cases}$

  $E(I_A) = P(A)$
- $E(f) = \sum\limits_{x \in range(f)} x \cdot P(f = x)$

Лемма 10.17: Линейность математического ожидания

Пусть (Ω, P) — вероятность пространство, f, g — случайные величины.
Тогда:

- $E(f + g) = E(f) + E(g)$
- $E(c \cdot f) = c \cdot E(f)$

Доказательство тривиально (прямая проверка по формуле)

Пример 10.18: Задача о днях рождения

Есть $n = 28$ людей, посчитать математическое ожидание числа пар людей, у которых даты совпали.

Считаем, что $\Omega = \{1, 2, \ldots, 365\}^n$, все варианты равновероятны.
Пусть f — количество пар людей, родившихся в один день года.

Упражнение 10.19

Если Ω не равновероятна, то $E(f)$ может лишь увеличиться.

$f = \sum\limits_{i<j} g_{ij}$, где $g_{ij}(\omega) = \begin{cases} 1, i, j \text{ родились в один день} \\ 0, \text{иначе} \end{cases}$
Понятно, что $E(g_{ij}) = \frac{1}{365}$
Тогда математическое ожидание f:

$$E(f) = E\left(\sum_{i<j} g_{ij}\right) = \sum_{i<j} E(g_{ij}) = \frac{n \cdot (n-1)}{2} \cdot \frac{1}{365} = \frac{28 \cdot 27}{2 \cdot 365} = \frac{378}{365} > 1$$

Теорема 10.20

Пусть $f : \Omega \to \mathbb{R}_{\geq 0}$ — неотрицательная случайная величина, $\alpha > 0$.
Тогда $P(f \geq \alpha) \leq \frac{E(f)}{\alpha}$

Пусть $f(\omega_i) = a_i$

$$E(f) = p_1 a_1 + p_2 a_2 + \ldots + p_n a_n$$

Заменим все числа $\geq \alpha$ на α, а все меньшие — на 0. Тогда мы только уменьшим сумму, но в то же время получим оценку:

$$E(f) \geq P(f \geq \alpha) \cdot \alpha$$

А именно это мы и хотели доказать.

Упражнение 10.21

Приведите контрпример в случае произвольной (то есть, не неотрицательной) случайной величины.

Пример 10.22

Имеется вероятностный алгоритм I

- Всегда работает правильно
- Иногда работает долго
- Среднее время работы $T = O(n^2)$

Хотим: алгоритм II

- Всегда работает за $O(n^2)$
- Иногда работает неправильно ($\leq 0.01\%$ случаев)

План: запустим алгоритм I $10000 \cdot T$ шагов, после чего обрываем алгоритм. Если мы успели получить ответ, то будем считать его результатом работы II, иначе выдадим какой-нибудь мусор.

Рассмотрим f — время работы I:

$$P(f \geq 10000T) \leq \frac{E(f)}{10000T} = \frac{T}{10000T} = \frac{1}{10000}$$

10.8. Дисперсия

Определение 10.23

Дисперсия случайной величины $f : \Omega \to \mathbb{R}$ — это $D(f) = E\left((f - E(f))^2\right)$

Теорема 10.24

$$D(f) = E(f^2) - E(f)^2$$

$$D(f) = E\left((f - E(f))^2\right) = E(f^2 - 2f \cdot E(f) + (E(f))^2) =$$
$$= E(f^2) - 2E(f \cdot E(f)) + E(E(f)^2) =$$
$$= E(f^2) - 2E(f)^2 + E(f)^2 = E(f^2) - E(f)^2$$

Теорема 10.25: Неравенство Чебышева

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

Пусть $g = (f - E(f))^2 \geq 0$

Тогда $P(|f - E(f)| \geq \alpha) = P(g \geq \alpha^2) \leq \dfrac{E(g)}{\alpha^2} = \dfrac{D(f)}{\alpha^2}$

10.9. Независимые случайные величины

Определение 10.26

Случайные величины f, g называются независимыми, если $\forall x, y \in \mathbb{R}$ выполнено $P(f = x \cap g = y) = P(f = x) \cdot P(g = y)$
Случайные величины $f_1, \ldots, f_k$ независимы в совокупности, если $\forall x_1, \ldots, x_k \in \mathbb{R}$ события "$f_1 = x_1$", $\ldots$, "$f_k = x_k$" — независимые в совокупности.

Теорема 10.27

Пусть f, g — независимые случайные величины, тогда $E(fg) = E(f)E(g)$

$$E(f) = \sum_{x \in \mathbb{R}} x \cdot P(f = x), E(g) = \sum_{y \in \mathbb{R}} y \cdot P(g = y)$$
$$E(f)E(g) = \left(\sum_{x \in \mathbb{R}} x \cdot P(f = x)\right)\left(\sum_{y \in \mathbb{R}} yP(g = y)\right) =$$
$$= \sum_{x,y \in \mathbb{R}} xy \cdot P(f = x) \cdot P(g = y) = \sum_{x,y \in \mathbb{R}} xy \cdot P(f = x,\ g = y) = E(fg)$$

Теорема 10.28

Пусть f, g — независимые случайные величины, тогда $D(f+g) = D(f)+D(g)$

$$D(f+g) = E(f+g)^2 - (E(f+g))^2 = E(f^2+2fg+g^2) - (E(f)+E(g))^2 =$$
$$= E(f^2) + 2E(fg) + E(g^2) - (E(f))^2 - 2E(f)E(g) - (E(g))^2 =$$
$$= (E(f^2) - (E(f))^2) + (E(g^2) - (E(g))^2) = D(f) + D(g)$$

Упражнение 10.29

Докажите эти факты для n независимых в совокупности величин

10.10. Оценки биномиальных коэффициентов

Подбросим монету n раз ($n \vdots 2$), посчитаем вероятность того, что выпала ровно половина орлов:

$$P\left(\text{выпало } \frac{n}{2}\right) = \frac{C_n^{n/2}}{2^n}$$

Теорема 10.30: Формула Стирлинга

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

$$\frac{C_n^{n/2}}{2^n} = \frac{n!}{(n/2)!\cdot(n/2)!\cdot 2^n} \sim \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{2^n\cdot\pi n\cdot\left(\frac{n}{2e}\right)^n} = \frac{\sqrt{2\pi n}}{\pi n} = \frac{\sqrt{2}}{\sqrt{\pi n}}$$

Теорема 10.31: Оценка биномиальных коэффициентов

$$\left(\frac{n}{k}\right)^k \le C_n^k \le \left(\frac{ne}{k}\right)^k$$

$$C_n^k = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k\cdot(k-1)\cdot\ldots\cdot 1} \ge \left(\frac{n}{k}\right)^k$$

Вспомним факт $\forall x \in \mathbb{R} \quad e^x \ge 1+x$.

Для оценки сверху покажем, что $\sum\limits_{i=0}^{k} C_n^i \le \left(\frac{ne}{k}\right)^k$

Рассмотрим $t \in (0,1)$:

$$\sum_{i=0}^{k} C_n^i \le \sum_{i=0}^{k} C_n^i \cdot \frac{t^i}{t^k} = \frac{1}{t^k}\sum_{i=0}^{k} C_n^i \cdot t^i \le \frac{1}{t^k}(1+t)^n$$

Возьмем $t = \frac{k}{n}$:

$$\sum_{i=0}^{k} C_n^i \le \frac{n^k}{k^k} \cdot \left(1 + \frac{k}{n}\right)^n = \left(\frac{n}{k}\right)^k \cdot \left(1 + \frac{k}{n}\right)^{\frac{n}{k} \cdot k} \le \left(\frac{n}{k}\right)^k \cdot e^k = \left(\frac{ne}{k}\right)^k$$

10.11. Вероятностные методы

Лемма 10.32: Вероятностный метод

Пусть $f : \Omega \to \mathbb{R}$ — случайная величина, $E(f) = c$.
Тогда:

1. $\exists \omega_{\min} \in \Omega : f(\omega_{\min}) \le c$
2. $\exists \omega_{\max} \in \Omega : f(\omega_{\max}) \ge c$

Доказательство: тривиально

Определение 10.33

$G = (V, E)$ — простой неориентированный граф.
Разрез в G — это $S \subseteq V$.
Величина разреза — это $|E(S, V \setminus S)|$

Теорема 10.34

Пусть $G = (V, E)$ — простой неориентированный граф, тогда существует разрез величины хотя бы $\frac{|E|}{2}$.

$\Omega = 2^V, \quad |\Omega| = 2^n$, каждый разрез равновероятен.
За случайную величину примем величину разреза.
Очевидно, что $E(X) = \frac{|E|}{2}$ (доказывается через индикаторы).

Теорема 10.35

Пусть в графе $G = (V, E)$ $2n$ вершин, тогда сушествует разрез величины хотя бы $\frac{|E| \cdot n}{2n-1}$.

Давайте выбирать все разрезы размера n равновероятно.

$$E(I_e) = \frac{2 \cdot C_{2n-2}^{n-1}}{C_{2n}^n} = \frac{2 \cdot (2n-2)! \cdot n! \cdot n!}{(2n)! \cdot (n-1)! \cdot (n-1)!} = \frac{2 \cdot n \cdot n}{2n \cdot (2n-1)} = \frac{n}{2n-1}$$

Упражнение 10.36

Проделайте то же самое для нечетного числа вершин:
Если в графе $2n+1$ вершина, то есть разрез величины $\frac{|E|(n+1)}{2n+1}$

10.12. Нижняя оценка числа Рамсея

Лемма 10.37

Пусть $A_1, \ldots, A_n$ — события.
Тогда $P(A_1 \cup \ldots \cup A_n) \leq \sum P(A_i)$

Замечание 10.38

$$R(n,k) \leq \binom{n+k-2}{n-1}$$

Следствие 10.39

$$R(k,k) \leq \binom{2k-2}{k-1} < 2^{2k-2}$$

Теорема 10.40

$$R(k,k) > \left[\frac{k \cdot 2^{k/2}}{2e}\right], \quad k \geq 3$$

Хотим построить граф на $n = \left[\frac{k \cdot 2^{k/2}}{2e}\right]$ вершинах без клик и независимых множеств размера k.

Ω — все графы на n вершинах равновероятно, $|\Omega| = 2^{\binom{n}{2}}$
Для $W \subseteq \{1, 2, \ldots, n\}$ посчитаем вероятности событий:

1. $A_W = W$ — клика
2. $B_W = W$ — независимое множество

$$P(A_W) = P(B_W) = \frac{2^{\binom{n}{2}-\binom{k}{2}}}{2^{\binom{n}{2}}}$$

$$P(\text{в } G \text{ есть клика или независимое множество размера } k) = P\left(\bigcup_W (A_W + B_W)\right) \leq$$

$$\leq \sum_W (P(A_W) + P(B_W)) = \binom{n}{k} \cdot 2^{1-\binom{k}{2}} \leq \left(\frac{ne}{k}\right)^k \cdot 2^{1-\binom{k}{2}} \leq$$

$$\left(\frac{k \cdot 2^{k/2} \cdot e}{2e \cdot k}\right)^k \cdot 2^{1-\binom{k}{2}} = \left(\frac{2^{k/2}}{2}\right)^k \cdot 2^{1-\binom{k}{2}} = 2^{\frac{k^2}{2}-k+1-\frac{k(k-1)}{2}} = 2^{1-\frac{k}{2}}$$

Что меньше единицы при $k \geq 3$

Значит с какой-то ненулевой вероятностью нам может попасть граф, для которого число Рамсея удовлетворяет оценке из теоремы, что и требовалось доказать.

10.13. Теорема Эрдеша

Теорема 10.41

$\forall k \in \mathbb{N}$ существует граф G такой, что:

1. $S(G) > k$ (нет циклов длины k и меньше)
2. $\mathcal{X}(G) > k$

Модель Эрдеша-Реньи: каждое ребро проводится с вероятностью p.

Положим $p = \frac{\ln n}{n}$.

Давайте докажем, что $P\left(\alpha(G) \geq \frac{n}{2k}\right)$ стремится к нулю.

Положим $r = \lceil \frac{n}{2k} \rceil$.

$$P\left(\alpha(G) \geq \frac{n}{2k}\right) = P\left(\bigcup_{\substack{X \subseteq V \\ |X|=r}} (X - \text{антиклика})\right) \leq$$

$$\leq \sum_{\substack{X \subseteq V \\ |X|=r}} P\left(X - \text{антиклика}\right) = \binom{n}{r}(1-p)^{\binom{r}{2}}$$

Воспользуемся тем, что $\binom{n}{r} \leq \left(\frac{ne}{r}\right)^r$ и $e^{-p} \geq 1 - p$:

$$\binom{n}{r}(1-p)^{\binom{r}{2}} \leq \left(\frac{ne}{r}\right)^r \cdot e^{-p \cdot \frac{r(r-1)}{2}} = \left(\frac{ne}{r} \cdot e^{-p \cdot \frac{r-1}{2}}\right)^r$$

Поскольку $r \to \infty$ при $n \to \infty$, достаточно показать, что выражение внутри скобок стремится к нулю:

$$\frac{ne}{r} \cdot e^{-p \cdot \frac{r-1}{2}} \leq 2ke \cdot n^{-\frac{r-1}{2n}} \leq 2ke \cdot n^{-\frac{n}{2k \cdot 2n}} \leq 2ke \cdot n^{-\frac{1}{4k}}$$

Очевидно, что последнее выражение стремится к нулю.

Теперь покажем, что вероятность того, что у нас графе более $\frac{n}{2}$ циклов длины $\leq k$ тоже стремится к нулю.

По неравенству Маркова: $P\left(\#\text{ плохих циклов} \geq \frac{n}{2}\right) \leq \frac{2 \cdot E(\#\text{ число плохих циклов})}{n}$

Давайте оценим нужное нам математическое ожидание.

Сколько существует циклов на $i \geq 3$ вершинах?

Ответ: $\frac{i!}{2i}$

Используя это, оценим математическое ожидание:

$$E(\#\text{ число плохих циклов}) \leq \sum_{i=3}^{k} \binom{n}{i} \cdot \frac{i!}{2i} \cdot p^i \leq$$

$$\leq \sum_{i=3}^{k} n \cdot (n-1) \cdot \ldots \cdot (n-i+1) \cdot p^i \leq \sum_{i=3}^{k} (np)^i \leq$$

$$\leq \frac{(np)^{k+1} - 1}{np - 1} = \frac{(\ln n)^{k+1} - 1}{\ln n - 1} < (\ln n)^{k+1}$$

Подставим в неравенство Маркова выше:

$$P\left(\#\text{ плохих циклов} \geq \frac{n}{2}\right) \leq \frac{2(\ln n)^{k+1}}{n}$$

Выражение справа стремится к нулю — доказали.

Выберем n такое, что:

$$\begin{cases} P\left(\alpha(G) \geq \frac{n}{2k}\right) < \frac{1}{2} \\ P(\#\text{ плохих циклов} \geq \frac{n}{2}) < \frac{1}{2} \end{cases}$$

Тогда найдется граф такой, что $\alpha(G) < \frac{n}{2k}$, и в G не более $\frac{n}{2}$ циклов длины не больше k. Давайте выкинем из каждого такого цикла по вершине. Тогда в $\tilde{G}$ не менее $\frac{n}{2}$ вершин, в нем нет циклов длины меньше k, а также $\alpha(\tilde{G}) < \frac{n}{2k}$.

Но тогда $\mathcal{X}(\tilde{G}) \geq \frac{n}{2\alpha(\tilde{G})} > \frac{n}{2 \cdot \frac{n}{2k}} = k$.

То есть граф $\tilde{G}$ является искомым для заданного k — доказали.

11. Производящие функции

11.1. Определение и операции

Определение 11.1: Производящая функция

Есть последовательность чисел $(a_0, a_1, \ldots, a_n, \ldots)$

Тогда $A(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots = \sum\limits_{n=0}^{\infty} a_n x^n$ называется ее ПФ.

Операции с ПФ:

- Взятие свободного члена:

  $a_0 = A(0)$

- Сложение:

  $[A + B]_n = a_n + b_n$

- Умножение:

  $[AB]_n = \sum\limits_{k=0}^{n} a_k b_{n-k}$

- Деление:

  Лемма 11.2

  Если $a_0 \neq 0$, то существует единственная $B(x)$ такая, что $A(x)B(x) = 1$

  Доказательство: поделите в столбик или по индукции найдите все коэффициенты $B(x)$

  Пример 11.3

  $$1 + x + \ldots + x^n + \ldots = \frac{1}{1 - x}$$

Свойства операций:

- коммунитативность
- ассоциативность
- дистрибутивность
- константная ПФ (умножение на константу эквивалентно умножению на $1 + 0x + 0x^2 + \ldots$)

- $A(x)B(x) = 0 \Rightarrow A(x) = 0 \vee B(x) = 0$

Доказательство: для сложения очевидно, для умножения при вычислении a_n обрежем все следующие члены и получим равенство для многочленов.

Определение 11.4: Формальная производная ПФ

Формальная производная ПФ $A(x) = \sum\limits_{n=0}^{\infty} a_n x^n$:

$$A'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}$$

Свойства производной:

1. $(A(x) \pm B(x))' = A'(x) \pm B'(x)$
2. $(cA(x))' = cA'(x)$
3. (Правило Лейбница)

$$(A(x)B(x))' = A'(x)B(x) + A(x)B'(x)$$

Доказательство правила Лейбница:
Левая часть при $[x^n]$:

$$(n+1)\sum_{k=0}^{n+1} a_k b_{n+1-k}$$

Правая часть при $[x^n]$:

$$\sum_{t=0}^{n} a_{t+1} b_{n-t} + \sum_{s=0}^{n} a_{n-s} b_{s+1}$$

Замена $s = n - t$

$$\begin{aligned}(n+1)a_{n+1}b_0 + na_n b_1 + (n-1)a_{n-1}b_2 + \ldots + \\ +(n+1)a_0 b_{n+1} + na_1 b_n + (n-1)a_2 b_{n-1} + \ldots\end{aligned}$$

А это равно левой части.

Пример 11.5

$$A(x) = 1 + x + x^2 + \ldots$$
$$(1 + x + x^2 + \ldots)(1 - x) = 1 \Rightarrow A(x) = \frac{1}{1-x} = (1-x)^{-1}$$

Замечание 11.6

Явная формула для a_n:

$$a_n = \left.\frac{A^{(n)}(x)}{n!}\right|_{x=0}$$

Пример 11.7: Сумма первых n натуральных чисел

$$(1, 1, 1, \ldots) \longrightarrow \frac{1}{1-x}$$
$$(1, 2, 3, \ldots) \longrightarrow \left(\frac{1}{1-x}\right)' = \frac{1}{(1-x)^2}$$
$$(1, 1+2, 1+2+3, \ldots) \longrightarrow \left(\frac{1}{(1-x)^2}\right)' = \frac{1}{(1-x)^3}$$
$$(0, 0+1, 0+1+2, \ldots) \longrightarrow \frac{x}{(1-x)^3}$$
$$a_n = 0 + 1 + \ldots + n$$
$$A(x) = \frac{x}{(1-x)^3}$$
$$a_n = \left.\frac{A^{(n)}(x)}{n!}\right|_{x=0}$$
$$B(x) = (1-x)^{-3}$$
$$B^{(n)}(x) = 3 \cdot 4 \cdot \ldots \cdot (n+2) \cdot (1-x)^{-n-3}$$

$\frac{B^{(n)}(0)}{n!} = \frac{3 \cdot 4 \cdot \ldots \cdot (n+2)}{n!} = \frac{(n+2)(n+1)}{2} = b_n \Rightarrow a_n = \frac{(n+1)n}{2}$

11.2. Связь ПФ с неупорядоченными выборками

S, T — множества, $S \cap T \neq \varnothing$
$A(x)$ — ПФ неупорядоченных выборок из S
$B(x)$ — ПФ неупорядоченных выборок из T
Тогда $A(x)B(x)$ — ПФ неупорядоченных выборок из $S \cup T$

Пример 11.8

- Бином Ньютона

  $\{a_1, \ldots, a_n\}$: $\binom{n}{k}$ способов выбрать k элементов

  $C(x) = \sum \binom{n}{k} x^k = (1+x)^n$

  Поскольку изначальный набор представлялся в виде объединения $\{a_i\}$ этот же результат можно было получить, сразу возведя $(1+x)$ в степень n.

- Количество салатов

  перец: 0 или 1

  редиска: $0, 2, 4, \ldots$

  помидор: любое

  баклажан: ≤ 3

  Какое есть число салатов из n овощей при данных ограничениях?

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

Определение 11.9

Пусть $\alpha \in \mathbb{C}$, $k \in \mathbb{N}_0$
Тогда $\binom{\alpha}{k} = \frac{\alpha \cdot (\alpha-1) \cdot \ldots \cdot (\alpha-k+1)}{k!}$

Замечание 11.10

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

Теорема 11.11

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k \quad \forall n \in \mathbb{Z}$$

Рассмотрим $(1-x)^{-n}$, $n \in \mathbb{N}$.
$(1-x)^{-n} = (1+x+x^2+\ldots)^n$.

Тогда коэффициент при k степени — число разбиений числа k на неотрицательные целые слагаемые, то есть $\binom{n+k-1}{k}$.

Поменяв x на $-x$ получим:

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

Что и требовалось доказать.

11.3. Степень

Определение 11.12

$$(1+x)^\alpha = \sum_{k=0}^{\infty}\binom{\alpha}{k}x^k$$

Лемма 11.13

$$(1+x)^\alpha \cdot (1+x)^\beta = (1+x)^{\alpha+\beta}$$

$$\left[(1+x)^\alpha \cdot (1+x)^\beta\right]_n = \sum_{\substack{s+t=n\\ s,t\geq 0}}\binom{\alpha}{t}\binom{\beta}{s}$$

$$\left[(1+x)^{\alpha+\beta}\right]_n = \binom{\alpha+\beta}{n}$$

Мы знаем, что при всех натуральных α, β равенство верно.

Зафиксируем $\tilde{\alpha} \in \mathbb{N}$. Тогда ЛЧ$(\tilde{\alpha}, \beta)$ и ПЧ$(\tilde{\alpha}, \beta)$ — многочлены от β. Они равны во всех натуральных точках, а значит совпадают во всех комплексных β. Аналогично можем зафиксировать $\tilde{\beta} \in \mathbb{C}$ и повторить идею. Во всех натуральных точках части снова будут совпадать, а значит доказали.

Определение 11.14

Последовательность $(a_0, \ldots, a_n)$ — линейное рекуррентное соотношение порядка k с постоянными коэффициентами, если

$$\exists c_1, \ldots, c_k \in \mathbb{C} : c_k \neq 0,\ \forall n \geq 0\ a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \ldots + c_k a_n$$

Теорема 11.15

Пусть $A(x)$ — ПФ линейного рекуррентного соотношения с постоянными коэффициентами порядка k.

Тогда существуют $P(x), Q(x) \in \mathbb{C}[x] : \deg P < k, \deg Q = k, Q(0) \neq 0$ и $A(x) = \frac{P(x)}{Q(x)}$

Рассмотрим $A(x)(c_1x + c_2x^2 + \ldots + c_kx^k)$

Раскрытием скобочек получим, что $A(x) = A(x)(c_1x+c_2x^2+\ldots+c_kx^k)+P(x)$.

Мы добавляем $P(x)$, чтобы подправить первые k коэффициентов (отсюда $\deg P < k$), которые могли неправильно посчитаться.

Тогда $A(x) = \frac{P(x)}{1-c_1x-\ldots-c_kx^k}$

11.4. Явная формула для линейных рекуррент

$$A(x) = \frac{P(x)}{Q(x)} = \frac{P(x)}{(x-a_1)^{t_1} \cdot \ldots \cdot (x-a_s)^{t_s}} = \\ = \sum_{j=1}^{s} \sum_{l=1}^{t_j} \frac{C_{jl}}{(x-a_j)^l}$$

А явные значения коэффициента у степени n у таких дробей мы умеем считать через бином Ньютона.

11.5. Правильные скобочные последовательности

Последовательность из левых и правых скобок (,) называется правильной скобочной последовательностью (ПСП), если она может быть получена за конечное число шагов по данным правилам:

- $\varnothing$ — ПСП
- A — ПСП $\Rightarrow$ (A) — тоже ПСП
- A, B — ПСП $\Rightarrow$ AB — тоже ПСП

Число скобочных последовательностей длины $2n$ обозначается C_n — числа Каталана

Теорема 11.16

Скобочная последовательность является ПСП, тогда и только тогда, когда в ней равное число левых и правых скобок, а так же на любом префиксе число левых скобок больше или равно числа правых скобок.

- $\Rightarrow$

  Следует из определения ПСП

- $\Leftarrow$

  Докажем достаточность по индукции

  База понятна.

  Переход:

  Рассмотрим наименьший префикс, на котором баланс равен 0. Очевидно, что это закрывающая скобка. Тогда наша ПСП равна (A)B. Нетрудно убедиться, что у A и B выполнены те же условия на баланс, а значит все хорошо.

Следствие 11.17

Каждая непустая ПСП представляется в виде (A)B, где A, B — ПСП, и притом единственным образом.

Существование следует из доказательства выше. Единственность.
Пусть есть $(A)B$ и $(A')B'$.

Тогда заметим, что если "внутри" A' или A есть нулевой баланс в изначальной ПСП, то кто-то из них не ПСП. Но это значит, что обе A и A' кончаются перед первым нулевым балансом (так как сами являются ПСП). То есть разбиения совпадают.

Следствие 11.18

$$C_n = \sum_{k=0}^{n-1} C_k \cdot C_{n-1-k}$$

Заметим, что если мы введем производящую, то получим уравнение вида:

$$C(x) = xC^2(x) + c_0 = xC^2(x) + 1$$

Решив такое квадратное уравнение получим $C_{1,2}(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$.

Теорема 11.19

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

Немного (нестрогой) магии:

$$xC^2(x) - C(x) + 1 = x\left(C(x) - \frac{1}{2x}\right)^2 - \frac{1}{4x} + 1$$

$$x\left(C(x) - \frac{1}{2x}\right)^2 = \frac{1-4x}{4x}$$

$$4x^2\left(C(x) - \frac{1}{2x}\right)^2 = 1 - 4x$$

Заметим, что полученное выражение равносильно изначальному:

$$4x^2C^2(x) - 4xC(x) + 1 = 1 - 4x$$
$$x^2C(x) - xC(x) + x = 0$$
$$x(xC^2(x) - C(x) + 1) = 0$$

Заметим, что $Y^2(x) = 1 - 4x$ имеет ровно два решения, так как изначально $y_0^2 = 1$, после чего все коэффициенты определяются однозначно. По очевидной причине это $\pm(1-4x)^{\frac{1}{2}}$.

Из штуки выше получается, что $Y(x) = 2xC(x) - 1$.

Подставим $x = 0$ получим, что $Y(0) = -1$, а значит $Y(x) = -\sqrt{1-4x}$

Следствие 11.20

$$C_n = \frac{1}{n+1}C_{2n}^n.$$

$\sqrt{1-4x}$ раскладывается по Тейлору:

$$1 - \sqrt{1-4x} = 1 - \sum_{n=0}^{\infty}\binom{1/2}{n}(-4x)^n =$$
$$= -\sum_{n=1}^{\infty}\frac{\frac{1}{2}\cdot\left(\frac{1}{2}-n+1\right)\cdot\ldots\cdot\left(\frac{1}{2}-1\right)}{n!}(-4x)^n =$$
$$= -\sum_{n=1}^{\infty}\frac{1(-1)(-3)\ldots(-2n+3)}{2^n\cdot k!}(-4x)^n =$$
$$= \sum_{n=1}^{\infty}\frac{1\cdot 2\cdot 3\cdot\ldots\cdot(2n-3)}{2^n\cdot n!}4^nx^n = \sum_{n=1}^{\infty}\frac{(2n-2)!\cdot 2^n}{n!\cdot 2\cdot 4\cdot\ldots\cdot(2n-2)}x^n =$$
$$= \sum_{n=1}^{\infty}\frac{(2n-2)!\cdot 2}{n!\cdot(n-1)!}x^n$$
$$C(x) = \frac{1-\sqrt{1-4x}}{2x} = \sum_{n=1}^{\infty}\frac{(2n-2)!}{n!\cdot(n-1)!}x^{n-1} = \sum_{n=0}^{\infty}\frac{(2n)!}{(n+1)\cdot(n!)^2}x^n$$

12. Комбинаторные игры

12.1. Определения

Определение 12.1

$G = (V, E)$ — ориентированный граф (считаем его конечным и ациклическим, для удобства)
MIN, MAX — игроки
V — "позиции" игры, в каждой позиции определено, кто ходит: MIN или MAX
E — ходы в игре
$s \in V$ — стартовая вершина
$T \subseteq V$ — терминальный позиции (игра в них кончается).
Понятно, что $T = \{v \in V \mid \deg_+(v) = 0\}$.
$f : T \to \mathbb{R}$ — функция выигрыша для MAX: если игра заканчивается в $t \in T$, то он выигрывает $f(t)$, а MIN получает $-f(t)$.

Определение 12.2

Партия — путь в графе игры G, стартующий в s и завершающийся в $t \in T$.
Результат партии — $f(t)$

Определение 12.3

Стратегия — это функция $g : V \setminus T \to V$

Определение 12.4

MAX может гарантировать себе выигрыш $\geq c$, если $\exists g_{MAX} \forall g_{MIN}$ результат партии $\geq c$.

Определение 12.5

Говорят, что цена игры $= c$, если MAX может гарантировать себе выигрыш $\geq c$, а MIN может гарантировать себе выигрыш $\leq c$.

Теорема 12.6

Для любой комбинаторной игры существует цена c, причем c единственная.

Сначала покажем единственность.
Пусть у игры есть две цены $c_1 > c_2$.
Тогда $\exists g_{MAX}$ с результатом $\geq c_1$ и $\exists g_{MIN}$ с результатом $\leq c_2$.
Если сыграть g_{MAX} против g_{MIN}, то результат будет $\geq c_1 > c_2$, что противо-

речит тому, что g_{MIN} гарантирует результат $\leq c_2$.

Теперь докажем существование.

Возьмем топологическую сортировку вершин графа игры $v_1, v_2, \ldots, v_n$, причем $v_1 = s$, а все вершины из T идут в конце.

Будем доказывать индукцией по суффиксу вершин, что цена игры определена и реализуется на согласованных стратегиях:

- База:

  Для всех вершин из T цена игры — это $f(t)$.

- Переход:

  Пусть v_i — вершина, в которой ходит MAX.

  Тогда $c_i = \max\limits_{(v_i,v_j)\in E} c_j$, продолжаем стратегию через максимум.

  Пусть v_i — вершина, в которой ходит MIN.

  Тогда $c_i = \min\limits_{(v_i,v_j)\in E} c_j$, продолжаем стратегию через минимум.

12.2. Беспристрастная игра Ним

Определение 12.7

Беспристрастная игра — игроки ходят по очереди, проигрывает тот, кто не может сделать ход.
$c = \pm 1$

Определение 12.8

Ним — это беспристрастная игра, в которой есть k кучек, в каждой кучке a_i камней.
Во время хода может взять > 0 камней из одной кучки.

Теорема 12.9

$c = -1$ тогда и только тогда, когда $a_1 \oplus a_2 \oplus \cdots \oplus a_k = 0$.

- $a_1 \oplus a_2 \oplus \cdots \oplus a_k = 0$

  Очевидно, что после любого хода XOR перестанет быть нулем.

- $a_1 \oplus a_2 \oplus \cdots \oplus a_k \neq 0$.

  Пусть a_i — кучка, в которой стоит старшая единица в XOR. Тогда можно сделать ход в a_i, чтобы XOR стал нулем: уберем эту старшую единицу, а все более младшие биты в a_i сделаем такими же, как в XOR (можем так

сделать, потому что после удаления “старшей единицы” на более младших позициях можно получить любую комбинацию битов)

Поскольку k пустых кучек — терминальная позиция, то $c = -1$ тогда и только тогда, когда $a_1 \oplus a_2 \oplus \cdots \oplus a_k = 0$.

12.3. Решающие деревья

12.3.1. Примеры и определения

Пример 12.10: Задача об угадывании числа

- Алиса загадывает число от 1 до N
- Боб хочет угадать число, задавая вопросы вида “верно ли, что $x \in S$?”

По индукции показывается, что нам хватит $k = \lceil \log_2 N \rceil$ вопросов.

Определение 12.11

Алгоритм (протокол) — дерево.

- Узлы — $S_i \subseteq A$ (соответствующие вопросы)
- Листья — ответы ($f(x)$)
- Вопросы вила “$x \in S$?” ($S \subseteq A$)
- Цель: найти $f(x)$
- Сложность протокола — глубина дерева

Есть два вида протоколов:

- Адаптивный — вопросы задаются последовательно.
- Неадаптивный — все вопросы задаются сразу.

Теорема 12.12

Адаптивная сложность задачи об угадывании числа $x \in [1, N]$ равна $\lceil \log_2 N \rceil$.

Пусть есть протокол, решающий задачу, глубины k. Значит в нем $r \leq 2^k$ листьев. $N \leq r \leq 2^k$, а значит $k \geq \lceil \log_2 N \rceil$. А само число, например, можно найти бинарным поиском.

Замечание 12.13

На самом деле, неадаптивная сложность тоже равна $\lceil \log_2 N \rceil$.
Если считать, что $0 < x < N \leq 2^k$ (сдвинем отрезок $[1, N]$ на 1), то можно за k вопросов узнать каждый бит числа.

Теорема 12.14

Для каждого адаптивного протокола сложности t существует неадаптивный протокол сложности t, решающий ту же задачу.

1. $x \in S_1$
2. Если $x \in S_1$, то верно ли, что $x \in S_3$?

   Иначе верно ли, что $x \in S_2$?

   На самом деле это вопрос вида $x \in (S_1 \cap S_3) \cup (\overline{S_1} \cap S_2)$
3. Продолжать в том же духе

12.3.2. Задача о сортировке

Есть неизвестная нам перестановка $\sigma \in S_n$.
Можем спрашивать вопросы вида "$\sigma_i < \sigma_j$?"
Нужно найти σ.

Теорема 12.15

$$\lceil \log_2 n! \rceil \leq SORT(n) \leq \sum_{k=1}^{n} \lceil \log_2 k \rceil$$

Упражнение 12.16

Выведите из этого, что $SORT(n) = \Theta(n \log n)$

Нижняя оценка доказывается так, как и в задаче об угадывании числа, в нашем случае $|S_n| = n!$

Вторую оценку докажем по индукции:

Пусть $SORT(n) \leq \sum_{k=1}^{n} \lceil \log_2 k \rceil$.

Сделаем переход $n \to n + 1$

Временно отложим первый элемент и найдем относительный порядок оставшихся n за $SORT(n)$. Теперь нужно понять, в каком из $n+1$ промежутков находится первый элемент. Сделаем это с помощью бинарного поиска за $\lceil \log_2(n+1) \rceil$.

Получили, что:

$$SORT(n+1) \le SORT(n) + \lceil \log_2(n+1) \rceil \le \sum_{k=1}^{n} \lceil \log_2 k \rceil + \lceil \log_2(n+1) \rceil \le \sum_{k=1}^{n+1} \lceil \log_2 k \rceil$$

12.3.3. Задача о поиске максимума

Есть неизвестная нам перестановка $\sigma \in S_n$.
Можем спрашивать вопросы вида "$\sigma_i < \sigma_j$?"
Нужно найти позицию максимального элемента в σ.

Теорема 12.17

$$MAX(n) = n - 1$$

Сначала приведем алгоритм: пройдемся слева направо по перестановке, каждый раз сравнивая текущего кандидата на максимума с рассматриваемым элементом.

Осталось показать, что за меньшее число вопросов не получится найти ответ. Пусть существует протокол сложности $k < n - 1$, решающий данную задачу. Посмтроим граф: $V = \{1, \dots, n\}$. Ребрами же соединим те элементы, которые мы сравнили в процессе алгоритма между собой. Поскольку $k < n - 1$, в нашем графе точно меньше $n-1$ ребра, а значит он несвязен. Пусть нам выдало какой-то ответ. Давайте в какой-нибудь другой компоненте прибавим n (и подкорректируем порядок в перестановке), тогда ответы на вопросы не изменятся, но наш ответ будет неправильным.

Теорема 12.18

Неадаптивная сложность задачи о поиске максимума из n объектов равна $\binom{n}{2}$

Найти максимум за такое число вопросов несложно — нужно просто спросить про все пары.

Теперь предположим, что мы задали $k < \binom{n}{2}$ вопросов. В таком случае мы не спросили про какую-то пару объектов a, b. Давайте сделаем их двумя максимальными. В таком случае, если поменять их местами, то ответы на вопросы не изменятся, но при этом максимальный элемент поменяется. А значит k вопросов не хватит.

12.3.4. Сложность булевой функции

Определение 12.19

Сложность булевой функции $f : \{0,1\}^b \to \{0,1\}$ в модели решающих деревьев ($D(f)$) — это сложность адаптивного протокола для вычисления f (мы знаем функцию, но не знаем набор входных параметров) при вопросах вида:

$$S_i = \{(a_1, \ldots, a_n) \in \{0,1\}^n \mid a_i = 1\}$$

Упражнение 12.20

Существует функция, у которой сложность меньше числа существенных переменных в ней.

Определение 12.21

$CONN : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$

- Переменные функции — наличие соответствующих ребер в графе на n вершинах.
- Результат — связен ли граф на данных ребрах.

Теорема 12.22

$$D(CONN(n)) = \binom{n}{2}$$

Очевидно, что оценка реализуется.

Пусть существует алгоритм, который раскрывает $k < \binom{n}{2}$ ребер. Снова будем играть за противника:

- Ребро внутри компоненты.

  Ответим как хотим.

- Ребро между разными компонентами.

  Если про все остальные ребра между этими компонентами уже спросили, то ответим “Да”, иначе — “Нет”.

Если раскрыты не все ребра, то “неспрошенные” ребра связывают разные компоненты связности. Это можно доказать индукцией по числу спрошенных ребер.