Основы математической логики и дискретной математики
Семестр 1

Лектор: Ицыксон Дмитрий Михайлович

Автор конспекта: Ольга Черникова

Собрано 27 декабря 2014 г. в 20:58

Содержание

1 Пропозициональные формулы

1.1 Пропозициальные формулы

(Формулы вычисления высказывания)

Γ - множество пропозициональных переменных $(x_1, x_2, x_3, \ldots)$

Определение пропозициональная формула:

1. Пропозициональная переменная - это формула
2. A - формула $\Rightarrow \neg A$ - формула
3. A, B - формулы $\Rightarrow (A \cup B), (A \cap B), (A \rightarrow B)$ - формулы

Пропозициальные формулы - минимальное множество строк, которые удовлетворяют 1, 2, 3 условиям.

1.2 Интерпретации

0 - False

1 - True

Дизъюнкция:

x	y	x ∪ y
0	0	0
0	1	1
1	0	1
1	1	1

Конъюнкция:

x	y	x ∩ y
0	0	0
0	1	0
1	0	0
1	1	1

Импликация:

x	y	x → y
0	0	1
0	1	1
1	0	0
1	1	1

Φ — пропозициальная формула от n переменных.

1.3 Булева функция

$\{0,1\}^n \rightarrow \{0,1\}$ — булева функция.

Пропозициальная формула $\leftrightarrow$ булева функция.

1.4 Представление булевой функции в ДНФ и КНФ

Литерал - это переменная или отрицание переменной $x, \neg x, y, \neg y$

Конъюнкт(терм) $l_1 \cap l_2 \cap \ldots \cap l_n$

Формула в дизъюнктивной нормальной форме(ДНФ): $c_1 \cup c_2 \cup \ldots \cup c_k$, где c_i - конъюнкт.

Дизъюнкт(clouse(клоз)): $l_1 \cup l_2 \cup \ldots \cup l_n$, где l_i — литерал.

Формула в конъюктивной нормальной форме(КНФ): $d_1 \cap d_2 \cap \ldots \cap d_k$, где d_i — дизъюнкт.

Теорема: любая булевая функция представляется в виде КНФ и ДНФ.

Доказательство: ДНФ

$x_1 \ldots x_n$	
$0 \ldots 0$	
$\ldots$	1
$\vdots$	
$\ldots$	1
$1 \ldots 1$	

Для каждой строчки, где стоит 1 запишем соответствующий конъюнкт. $(\neg x_1 \cap x_2 \cap \ldots \cap x_n) \cup \ldots$

$\neg x_i$ — если $x_i = 0$

x_i — если $x_i = 1$

КНФ

Рассмотрим строчки, где записаны 0. Они все не должны выполняться.

1.5 Эквивалентные формулы

Определение две формулы эквивалентные, если они задают одну и ту же булеву функцию.

Формулы де Морга

$\neg(x \cup y) \sim \neg x \cap \neg y$

$\neg(x \cap y) \sim \neg x \cup \neg y$

$\neg(c_1 \cup c_2 \cup \ldots \cup c_n) \sim \neg c_1 \cap \neg c_2 \ldots \cap \neg c_n$
$c_1 = l_1 \cap l_2 \cap \ldots \cap l_k$
$\neg c_1 = \neg l_1 \cap \neg l_2 \cap \ldots \cap \neg l_k$
$x \cap (y \cup z) \sim x \cap y \cup x \cap z$
$x \to y \sim \neg x \cup y$
Алгоритм приведение в ДНФ:

1. избавится $\to$

2. перенести отрицание к переменным

3. раскрыть скобки пользуясь дистрибутивностью.

2 Выполнимость формулы

2.1 Тавтологии, противоречия, выполнимые формулы

Определение Формула - тавтология, если она истена, при всех значениях переменной.

Определение Формула - противоречива, если она ложна, при всех значениях переменной.

Φ — выполнимая формула, если она не является противоречивой. $\exists$ значение переменных, что значение формулы истина.

2.2 Выполнимость КНФ

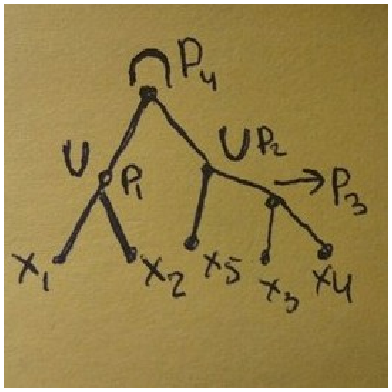
Задача SAT —- выполнима ли формула в КНФ.

Теорема. По любой формуле можно за быстро построить формулу в КНФ, выполнимость которой эквивалентна выполнимости исходной.

Доказательство.

$(x_1 \cup x_2) \cap ((x_3 \to x_4) \cup x_5)$

Для формулы построим дерево разбора.



Для промежуточных вершин, заведем переменные $P_1, P_2, \ldots, P_k$.

Формула выполняется, если выполняется система.

$$\begin{cases} P_4 = P_1 \cap P_2 \\ P_1 = x_1 \cup x_2 \\ P_2 = x_5 \cup P_3 \\ P_3 = x_3 \to x_4 \end{cases}$$

Каждое уравнение можно представить как несколько дизъюнктов.

Следствие из доказательства: В полученной формуле в КНФ в каждой дизъюнкт входит ≤ 3 литерала. 3-КНФ.

3 Резолюционное исчисление

Φ — тавтология $\Leftrightarrow \neg\Phi$ —невыполнима.

$\neg\Phi \sim \Psi$ в КНФ.

$\neg\Phi$ невыполнимо $\Leftrightarrow \Psi$ невыполнима.

КНФ: $d_1 \cap d_2 \cap \ldots \cap d_k$

$d_i = (l_1 \cup l_2 \cup \ldots \cup l_m)$

$S = \{d_1, d_2, \ldots, d_k\}$

Правило резолюции $\dfrac{(x \cup A)\_(\neg x \cup B)}{A \cup B(\text{резольвента})}$

Утверждение Если C — резольвента дизъюнктов D и E, то любое значение переменных, который выполняет D и E, выполняет и C.

$\dfrac{x\_\neg x}{\blacksquare}$

Определение Φ — формула в КНФ. Резолюционным опровержением формулы Φ называется последовательность дизъюнктов $c_1, c_2, \ldots, c_m$.

1. c_m — пустой дизъюнкт.
2. $\forall i$ от 1 до m c_i — либо дизъюнкт формулы Φ, либо c_i — резольвента c_k и c_l, где $k, l < i$

Теорема Φ — формула в КНФ. Φ невыполнима $\Leftrightarrow \exists$ резолюционное опровержение формулы Φ

$\Leftarrow$ **Корректность** $c_1, c_2, \ldots, c_m$ — резалюционное опровержение Φ.

Пусть набор значений σ выполняет Φ.

По индукции можно доказать σ выполняется $c_i \forall i$

c_i — дизъюнкт Φ очевидно.

$\dfrac{c_k\_c_l}{c_i} k, l < i$ по индукционному предположению σ выполняет c_k и $c_l \Rightarrow \sigma$ выполняет $c_i \Rightarrow c_m = \blacksquare$ выполняет σ, противоречие.

$\Rightarrow$ **Полнота**

Индукция по числу n переменных в Φ.

База n = 1.

$(x \cup \neg x) \rightarrow$ заменим на 1

$x \cup x \cup x \rightarrow$ заменим на x

дизъюнкты на будут повторяться.

$x \cap \neg x$ — единственный не выполнимый вариант $\Rightarrow$ получим ■.

Переход $n \rightarrow n + 1$

x — переменная.

разобьем формулы на 3 группы.

1. S_1 =A
2. $S_2 = x \cup A$
3. $S_3 = \neg x \cup A$

$\Phi|_{x=0}$(подставим x = 0) $S_1 \cap S_2'$

S_2' = дизъюнкт из S_2 без x.

$\Phi|_{x=1}$ $S_1 \cap S_3'$

$\Phi_{x=0}$ — невыполнима, на одну переменную меньше. По индукционному предположению существует опровержение.

Вернем в опровержение x. Тогда получим или пустой дизъюнкт, или x.

Аналогично, для $\Phi_{x=1}$. Получим $\neg x$ или опровержение.

Или получили противоречие, либо $\dfrac{x\_\neg x}{\blacksquare}$

Замечание Если в d_1 и d_2 входит le 2 литералов, то и в резальвенту входит $\leq$ 2 литералов.

Пример $(\neg x \cup y) \cap (\neg y \cup x) \cap (\neg y \cup z) \cap (\neg z \cup y) \cap (x \cup z) \cap (\neg x \cup \neg z)$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{(\neg x \cup y)\_(x \cup z)}{(y \cup z)\_(\neg y \cup z)}}{z\_(\neg z \cup y)}}{y\_(\neg y \cup x)}}{x\_(\neg x \cup \neg z)}}{\neg z\_z}}{\blacksquare}$$

4 Алгоритм проверяющий выполнимость формулы 2-КНФ

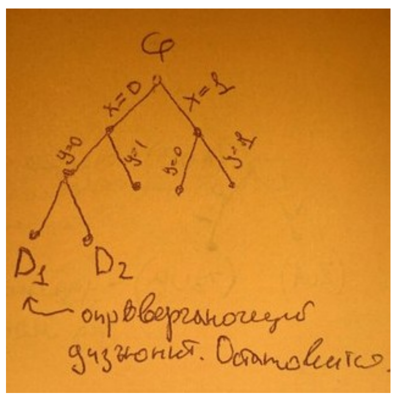
1. пока можем вывести новую резальвенту — выводим.
2. остановка:
   (a) вывели ■
   (b) больше ничего не можем вывести.

Время работы — $\mathcal{O}(n^2)$
Количество дизъюнктов:

1. дизъюнктов из 1 литерала —- 2n
2. из 2 — $\frac{2n(2n-1)}{2}$

5 Построение резолюционного доказательства по дереву расщепления

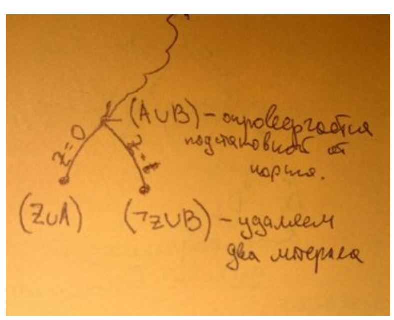
Построим дерево расщепление.



В каждом листе написан дизъюнкт, который опровергается подстановкой от листа до корня.

Заполняем все дерево. Если в каком-то листе ничего не написано, значит вормула выполнима.

Построим резолюционное опровержение по дереву.



Пока есть что заменять, будем выводить резольвенту из двух братьев и записывать в их предка.

В каждой вершине окажется дизъюнкт, который опровергается подстановкой переменных от вершины до корня.

В корне должен оказаться пустой дизъюнкт.

6 Схемы из функциональных элементов

6.1 Ориентированный граф без циклов и топологическая сортировка.

Ориентированный граф без циклов(DAG)

Утверждение G — DAG, тогда $\exists$ вершина без исходящих ребер, $\exists$ вершина без входящих ребер.

Лемма(о топологической сортировке)

G - DAG, V — множество вершин, тогда $\exists h : V \to \{1, 2, \ldots .|V|$

1. биекция
2. (u, v) — ребро $\Rightarrow h(u) < h(v)$

Доказательство

Индукция по числу вершин.

База одна вершина

Переход пусть v — вершина без исходящих ребер.

h(v) = |V|

Выкидываем вершину v из G и получаем G'. По предположению индукции можем построить топологическую мортировку для G'.

Определим h на $V/\{v\}$ совпадающей с h'.

6.2 Схемы

$B = \{f_1^{(k_1)}, f_2^{(k_2)}, \ldots, f_l^{(k_l)}\}$

$f_i^{(k_i)} : \{0, 1\}^{k_i} \to \{0, 1\}$

Схема под базисом B:

DAG

Вершины, в которые ничего не входит, называются входами $x_1, x_2, \ldots, x_n$

Вершин, из которых ничего не выходит — выходы.

Вершины кроме входов — внутренние(gates).

Каждая внутренняя вершина помечена $f_i^{(k_i)} \in B$ и имеет вход степени k_i. Входящие ребра пронумерованы.

Выполнение схемы:

1. топологически сортируем
2. задаем начальные значения
3. считаем значения в порядке топологической сортировки.

Если у схемы n входов и m выходов, то она задает функцию $\{0,1\}^n \to \{0,1\}^m$

Определение Базис В называется полным, если для любой булевой функции существует схема над В выражающая ее.

Размер схемы —- число вершин в графе.

Глубина схемы —- длина максимального пути от входа до выхода.

$f : \{0,1\}^n \to \{0,1,\}^k$

$size_B(f)$ — min размер схемы в базисе B, которые вычисляют f.

6.3 Эквивалентность различных базисов

Лемма B_1, B_2 — полные базисы. Тогда $\exists C > 0 : \forall n, k \forall f : \{0,1\}^n \to \{0,1\}^k size_{B_1}(f) \leq C size_{B_2}(f)$

Доказательство $B_1 = \{h_1, h_2, \ldots, h_t\}$

$B_2 = \{g_1, g_2, \ldots, g_m\}$

$g_i^{k_i}$ задается схемой в базисе B_1

f в базисе B_2 заменяем $g_i^{k_i}$ на схему в базисе B_1, которая вычисляет $g_i^{k_i}$

Получим схему для f в B_1

C — размер максимального представления g_i в виде B_1 схемы.

7 Схема умножения

7.1 Схема для сложения

$P_n, \ldots, p_1$

$...., x_{n-1}, x_{n-2}, \ldots, x_0$

$...., y_{n-1}, y_{n-2}, \ldots, y_0$

$P_1 = x_0 \cap y_0$

$P_2 = (x_1 \cap y_1) \cup (y_1 \cap P_1) \cup (x_1 \cap P_1)$

...
Размер $\mathcal{O}(n)$
Глубина $\mathcal{O}(n)$

7.2 Схема умножения

Размер $\mathcal{O}(n^2)$
Глубина $\mathcal{O}(n \log n)$ $T(n) = cn + T(\frac{n}{2})$
$n = 2^k$
n — длина числа.
$x = a * 2^{\frac{n}{2}} + b$
$y = c * 2^{\frac{n}{2}} + d$
$xy = ac2^n + (ad + bc)2^{\frac{n}{2}} + bd$
$S(n) = 4S(\frac{n}{2}) + cn$
$S(n) = \mathcal{O}(n^2)$
$(a + b)(c + d) - ac - bd$
$S(n) = 3S(\frac{n}{2}) + cn$
$S(n) = n^{\frac{2}{3}}$

8 Существование булевой функции, которая не вычисляется схемой размера $\frac{2^n}{Cn}$

Теорема: $f : \{0,1\}^n \to \{0,1\}$

B - полный базис.

Тогда $size_B(f) = \mathcal{O}(2^n n)$

Доказательство: рассмотрим $B_1 = \{\neg, \cap, \cup\}$

ДНФ для f $\mathcal{O}(\frac{2^n}{n})$

Количество функций $\{0,1\}^n \to \{0,1\} = 2^{2^n}$

Количество схем размер $\leq S$

Пусть все формулы имеют арность $\leq 2(\{\cup, \cap, \neg\})$

Для каждой вершины указываем номер вершины из которой в нее ведут ребра. Что бы это указать, достаточно $\mathcal{O}(\log S)$ битов.

Значит для шифрования схемы достаточно $\mathcal{O}(S \log S)$.

Количество схем размера $\leq S$ не больше, чем число битовых строк длины $\mathcal{O}(S \log S) = 2^{CS \log S}$

Следствие: $\exists$ константа $D \forall n$

$\exists f : \{0,1\}^n \to \{0,1\}$

$size(f) \geq \frac{2^n}{Dn}$

$S = \frac{2^n}{Dn}$ Число схем размера $\leq s \leq 2^{C\frac{2^n}{Dn}n} = 2^{n\frac{C}{D}}$

Если D > C, то число схем размера $\leq \frac{2^n}{Dn}$ меньше общего числа функций.

9 Предикатные формулы

Определение: $M \neq 0$ k-местным предикатом на M называется $P : M^k \to \{0, 1\}$

$k \in \{0, 1, 2 \ldots\}$

k-ичная функция $f : M^k \to M$

Сигнатура: $\mathcal{F} = \{f_1^{(k_1)}, f_2^{(k_2)}, \ldots\}$

$f_i^{(k_i)}$ — к-местная функция.

$\mathcal{P} = \{p_1^{(l_1)}, p_2^{(l_2)}, \ldots\}$

Пример: $\mathcal{P} = \{=^{(2)}\}$

$\mathcal{F} = \{+^{(2)}, *^{(2)}\}$

$\Gamma = \{x_1, x_2, \ldots\}$ — множество предметных переменных.

Определение: Терм

1. x — предметная переменная, то x — терм.
2. $f^{(k)} \in, t_1, t_2, \ldots, t_k$ — термы, тогда $f^{(k)}(t_1, t_2, \ldots, t_k)$ — терм.
3. Множество термов наименьшее множество строк, удовлетворяющие 1, 2.

Определение: Атомарная формула.

Если $p^{(k)} \in \mathcal{P}, t_1, t_2, \ldots, t_k$ –

атомарная формула — $p^(k)(t_1, t_2, \ldots, t_k)$

Определение: Предикатная формула.

1. атомарная формула —- предикатная формула.
2. Φ — предикатная формула, то ¬Φ — тоже предикатная формула.
3. Если Φ и Ψ предикатные формулы, то $(\Phi \cup \Psi), (\Phi \cap \Psi), (\Phi \to \Psi)$
4. Φ — формула, x — предметная переменная $\forall x(\Phi), \exists x(\Phi)$
5. множество формул минимальное множество, удовлетворяющие 1-4.

Область действия квантора.

Связанное вхождение переменной находится в области действия квантора на этой переменной.

Свободная переменная — не связанная.

Формулы без свободных вхождений переменных — замкнутая.

Интерпретация: для сигнатуры$(\mathcal{P}, \mathcal{F})$ носитель М $\neq 0$

$p^{(k)} \in \mathcal{P} \leftrightarrow M^k \rightarrow 0, 1$

$f^{(k)} \in \mathcal{F} \leftrightarrow M^k \rightarrow M$

Оценка для множества переменных $\Gamma \rightarrow M$

Значение формулы в данной интерпретации при данной оценке.

Терм с k связанными переменными задает отображение из $M^k \rightarrow M$

1. x — переменная, то это тождественное отображение.
2. $f^{(k)}(t_1, \ldots, t_k)$ — композиция функций.
   Атомарная формула с k переменными задает предикат.
   Φ — предикат.
   $\neg\Phi$ — отрицание предиката.
   $\Phi, \Psi, (\Phi \cup \Psi), (\Phi \cap \Psi), (\Phi \rightarrow \Psi)$
   $\forall x\Phi$, $\exists x\Phi$ — k-1 предикат

Определение I - интерпретация сигнатуры $(\mathcal{F}, \mathcal{P})$ с носителем М.

Предикат $P = M^k \rightarrow \{0, 1\}$ называется выразимым в I, если его можно задать формулой с k свободными переменными.

Замкнутая формула называется тавтологией, если она истина при всех интерпретациях.

9.1 Арифметика

$\mathcal{P} = \{=\}$
$\mathcal{F} = \{+, *\}$
$N\{0, 1, 2, \ldots\}$

1. "x = 0"x + x = x
2. "x = 1"$(x * x = x) \cap \neg(x + x = x)$
3. "x $\geq$ y"$\exists z(z + y = x)$
4. "x = 179"$\exists y(x = y + y + \ldots + y \cap y = 1)$
5. "x mod y == 0"$\exists z(zy = x)$

6. "x - простое"$\forall y((x mod y == 0) \to (y = 1) \cup (y = x)) \cap \neg(x = 1)$

7. "x - степень 2"$\forall y((x mod y == 0) \cap (y -) \to y = 2)$

8. "x - степень 4"$\exists y(y * y = xx -)$

   $\tilde{k} =$ переводим k + 1 в двоичную систему и удаляем первую цифру.

9. $\tilde{x}$ из нулей (x + 1) - степень двойки.

10. Строки $\tilde{x}$ и $\tilde{y}$ имеют одинаковую длину $\forall$ c ((c - степень 2) $\to (x + 1 \leq c) \leftrightarrow (y + 1 \leq c))$

11. $\tilde{z} = \tilde{x}\tilde{y}$

    $\exists t$ ((t - cjcnjbn bp yektq) $\cap(|\tilde{t}| = |\tilde{y}|) \cap z = (x + 1)(t + 1) + (y - t) - 1)$

12. $\tilde{x}$ - начало строки $\tilde{y}$ $\exists t : \tilde{y} = \tilde{x}\tilde{t}$

13. $\tilde{x}$ - конец $\tilde{y}$

14. $\tilde{x}$ - подслово $\tilde{y}$ $\exists t((\tilde{x}$ конец $\tilde{t}) \cap (\tilde{t}$ начало $\tilde{y}))$

15. $\tilde{x}$ короче $\tilde{Y}$ $\exists zt(t = \tilde{z}\tilde{x}) \cap (z \neq 0) \cap |\tilde{t}| = |\tilde{y}|$

10 Кодирование конечных множеств в арифметике

Теорема: Существует 3-местный выразимый предикат S(x, a, b):

1. $\forall a, b \in \mathbb{N} S_{a,b} = \{x | S(x, a, b) = 1\}$ конечно.
2. $\forall \tilde{x} \in \mathbb{N} x - \exists a, b \in \mathbb{N} x = S_{a,b}$

S(x, a, b) $=$ $\tilde{x}\tilde{x}$ короче $\tilde{a}$ и $\tilde{a}\tilde{x}\tilde{a}$ подстрока $\tilde{b}$

Доказательство: 1. $S_{a,b}$ - конечно.

2. $X = \{x_1, x_2, \ldots, x_n\}$

   $a : \tilde{a}$ длиннее всех $\tilde{x}_i \tilde{a} = 10 \ldots 01$

   $b : \tilde{b} = \tilde{a}\tilde{x}_1\tilde{a}\tilde{x}_2 \ldots \tilde{x}_n\tilde{a}$

x - степень 6

$\exists a, b(S(x, a, b) \cap \forall y(S(y, a, b) \to ((y = 1) \cup \exists t((6 * t = y) \cap S(t, a, b))))$

$x = 6^n$

$[x, y] = (x + y)^2 + x$

$first(x, p) \forall z((z^2 \leq p) \cap \forall t((t > z) \to (t^2 > p))) \to (x + z = p))$

$x = 6^n$

$\exists a, b(S([x, n], a, b) \cap \forall y(S(y, a, b) \to \exists z, my = [z, m] \cap (z = 1 \cap m = 0) \cup \exists kz = 6k \cap S([k, m - 1], a, b)$

11 Доказательство непрерывности методом автоморфизмов

$\mathbb{Z}, =, +$ невыразимо x < y.

P(x, y)

$\downarrow$

P(-x, -y) поведение не должно было изменится.

Определение I - интерпретация с носителем M.

$\alpha : M \to M$ называется автоморфизмом I.

1. α — биекция
2. $\forall p^{(k)} \in {}^{(k)}$ устойчиво по α $p^{(k)}(\alpha(x_1), \ldots, \alpha(x_n)) = p^{(k)}(x_1, x_2, \ldots, x_n)$
3. $\forall f^{(k)} \in \mathcal{F}$
   $f^{(k)}$ устойчиво относительно α
   $f^{(n)}(\alpha(x_1), \ldots, \alpha(x_n)) = \alpha(f^{(k)}(x_1, \ldots, x_n))$

Теорема Если $P : M^k \to \{0, 1\}$ выразим в I, α — автоморфизм I $\Rightarrow$ P устойчиво относительно автоморфизмов.

Доказательство

1. Термы задают устойчивые относительно α функции.
2. Атамарные формулы задают устойчивые предикаты.
3. $\neg\Phi$
   $\Phi_1 \cup \Phi_2$
   $\Phi_1 \cap \Phi_2$
   $\Phi_1 \to \Phi_2$
4. $\forall x \Phi(x)$
   $\exists x \Phi(x)$
   $P(x, y_1, y_2, \ldots)$
   $P(\alpha(x), y_1, \ldots)$ — так как биекция $\alpha(x)$ пробегает все значения $M \Rightarrow$ истина.

Примеры

1. $(\mathbb{Z}, =, <) x = 0$
   $\alpha(x) = x - 1$
2. $(\mathbb{Q}, =, <, +) x = 1$
   $\alpha(x) = 2x$
3. $(\mathbb{R}, =, <, 0, 1) x = \frac{1}{2}$
   $\alpha(x) = x * |x|$

12 Конечные множества

$\mathbb{N} = \{1, 2, \dots\}$

$[n] = \{1, 2, \dots, n\}$

Число подмножеств [n] $= 2^n$

$A_n^k = |\{(s_1, \dots, s_k) \subset [n] * \dots * [n]\} s_i \neq s_j$ при всех $i, j|$

$A_n^1 = n$

$A_n^k = nA_{n-1}^{k-1}$

$A_n^k = n(n-1)\dots(n-k+1) = \dfrac{n!}{(n-k)!}$

$C_n^k = \binom{n}{k} = |s \subset [n]||s| = k|$ число сочетаний из n по k.

$A_n^k = C_n^k * k!$

$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$ (число подмножеств, содержащих 1 + число подмножеств не содержащих 1)

$C_n^k = C_n^{n-k} = \dfrac{n!}{k!(n-k)!}$

Треугольник Паскаля

$$
\begin{array}{ccccccc}
 & & & C_1^0 & & & \\
 & & C_1^0 & & C_1^1 & & \\
 & C_2^0 & & C_2^1 & & C_2^2 & \\
C_3^0 & & C_3^1 & & C_3^2 & & C_3^3
\end{array}
$$

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
1 & & 3 & & 3 & & 1
\end{array}
$$

Бином Ньютона

$(a+b)^n = \sum_k C_n^k a^k b^{n-k}$

База a + b = a$C_1^0 + bC_1^1$

Переход $(a+b)^{n+1} = (a+b)^n(a+b) = (\sum_{k=0}^n C_n^k a^k b^{n-k})(a+b) = \sum_{k=0}^{n+1} C_{n+1}^k a^k b^{n-k+1}$

$(1+1)^n = C_n^0 + C_n^1 + \dots$

$(1-1)^n = C_n^0 - C_n^1 + \dots$

13 Характеристическая функция

$\chi A \subset X$

Характеристическая функция: $\chi_A : x \to \{0, 1\}$

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

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

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

$\chi_{A \cup B}(x) = X_{\overline{\overline{A} \cap \overline{B}}} = 1 - (1 - \chi_A)(1 - \chi_B) = \chi_A + \chi_B - \chi_A\chi_B$

$\chi_{A_1 \cup A_2 \cup \dots \cup A_n} = 1 - (1 - \chi_{A_1})(1 - \chi_{A_2})\dots(1 - \chi_{A_n})$

$|A| = \sum_x \chi_A(x)$

13.1 Формула включений-исключений

$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_x \chi_{A_1 \cup \ldots \cup A_n}(x) = \sum_{i=1}^n |A_i| - \sum_{i \neq j} |A_i \cap A_j| + \sum_{i \neq j \neq k} |A_i \cap A_j \cap A_k| - \ldots$

14 Количество счастливых билетов

Счастливый билет, у которого $a_1 + a_2 + a_3 = a_4 + a_5 + a_6$.

$\overline{a_1 a_2 a_3 a_4 a_5 a_6} \leftrightarrow \overline{a_1 a_2 a_3 (9-a_1)(9-a_2)(9-a_3)}$

$|\{$количество счастливых билетов$\}| = |\{$билеты с суммой цифр 27$\}|$

Из метода шаров и перегородок количество разбиений $C_{32}^5 - |c_1 \cup c_2 \cup \ldots \cup c_6|$

c_1 — множество разбиений числа 27 на 6 неотрицательных слагаемых у которого $a_1 \geq 10$

c_2 — множество разбиений числа 27 на 6 неотрицательных слагаемых у которого $a_2 \geq 10$

$\ldots$

15 Равномощные множества

Определение: множества A и B равномощны, если $\exists$ биекция $f : A \to B$

1. равномощность двух отрезков.

   $[a, b] \to [c, d]$

   $x \to (x - a)(d - c)/(b - a) + c$

2. равномощность множества последовательностей из 0 и 1 и множества натуральных чисел.

   $S \subset N$

   $x_n = \begin{cases} 1, & \text{если } n \in S \\ 0, & \text{если } n \notin S \end{cases}$

15.1 счетные множества

Определение: множество называется счетным, если оно равномощно $\mathbb{N}$

$\mathbb{N} \to^f S = \{f(1), f(2), f(3), \ldots\}$

Свойства счетных множеств:

1. Любое подмножество счетного множества конечно, либо счетно.

   A - счетно.

   $A = \{f(1)(g(1)), f(2), f(3), f(4)(g(2)), \ldots\}$

   $g(k) =$ первый элемент в последовательностиAпосле$g(k-1)$

2. Объединение конечного или счетного числа конечных множеств конечно или счетно.
   $A_1 f_1(1) f_1(2) f_1(3) f_1(4) \dots$
   $A_2 f_2(1) f_2(2) f_2(3) f_2(4) \dots$
   $A_3 f_3(1) f_3(2) f_3(3) f_3(4) \dots$
   $A_4 f_4(1) f_4(2) f_4(3) f_4(4) \dots$
   $\dots$
   $f_1(1) f_1(2) f_2(1) f_1(3) f_2(2) f_3(1) \dots$
3. Любое бесконечное множество содержит счетное подмножество.
   $x_1, x_2, x_3, \dots$ если не можем выбрать $\Rightarrow$ множество конечно.

16 Бесконечное множество

16.1 Примеры счетных множеств

1. $\mathbb{Q} = \frac{p}{q}$

   $\frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \frac{4}{1}, \dots$
   $-\frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \frac{4}{1}, \dots$
   $\frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \frac{4}{2}, \dots$
   $\dots$

   Объединение счетного числа счетных множество —- счетно.

2. $\mathbb{N}^k$ — счетно.

   Индукция по k.

   База $\mathbb{N}^2$ объединение счетного числа счетных множеств.

   Переход $k \to k+1$

   $\mathbb{N}^{k+1}(a, x)$

   $a \in \mathbb{N}^k$

   $x \in \mathbb{N}$

   Оба множества счетны. Можем занумировать их декартово произведение.

3. множество конечных последовательностей натуральных

   Количество последовательностей длины 1 — $\mathbb{N}$

   Количество последовательностей длины 2 — $\mathbb{N}^2$

...

Объединение счетно.

4. алгебраических чисел — счетно.

   Количество уравнений — счетно

   Корней у каждого уравнения конечно.

   $\Rightarrow$ их объединение счетно.

16.2 Объединение бесконечного и счетного множества

Теорема: A — бесконечное, B —- счетное или конечное, то $A \cup B$ равномощно A.

Доказательство: B' = B/A

B' = счетное или конечное

$B' \cap A = 0$

$A \cup B' = A \cup B$

A — бесконечное $\Rightarrow$ в A есть счетное подмножество Q.

$A = Q \cup (A/Q)$

$A \cup B' = (Q \cup B') \cup (A/Q)$

Q равномощно B'

16.3 Равномощность [0, 1] и множество бесконечных последовательностей из 0 и 1

Теорема: [0, 1] равномощен множеству бесконечных последовательностей из 0 и 1.

Доказательство: $\alpha \in [0, 1]$

Если $\alpha < \frac{1}{2}$ на первое место последовательности ставим 0, иначе 1. Переходим к отрезку, где лежит α

Это биекция.

16.4 Равномощность квадрата и отрезка

Теорема: [0, 1] × [0, 1] равномощен [0, 1].

Доказательство: $(\alpha, \beta) \in [0, 1] \times [0, 1]$

$\alpha \leftrightarrow a_1 a_2 a_3 \dots$

$\beta \leftrightarrow b_1 b_2 b_3 \dots$

$(\alpha, \beta) \leftrightarrow a_1 b_1 a_2 b_2 a_3 b_3 \dots$

17 Теорема Кантора-Бернштейна

Теорема: Если A равномощно подмножеству B, B равномощно подмножеству A, то A и B равномощны.

Доказательство: **Лемма:** $A_0 \supset A_1 \supset A_2$

A_0 равномощно A_2, тогда A_0 равномощно A_1.

Доказательство: $f : A_0 \to A_2$ — биекция.

$f(A_1) = A_3 \subset A_2$

$f(A_2) = A_4 \subset A_3$

$\ldots$

$A_{n+2} = f(A_n)$

$A_0 \supset A_1 \supset A_2 \supset A_3 \ldots$

$c_0 = A_0/A_1$

$c_1 = A_1/A_2$

$c_2 = A_2/A_3$

$\ldots$

$A_0 = c_0 \cup c_1 \cup c_2 \cup \ldots$

$A_1 = c_1 \cup c_2 \cup \ldots$

$f(c_i) = f(A_i/A_{i+1}) = f(A_i)/f(A_{i+1}) = A_{i+2}/A_{i+3} = c_{i+2}$

Биекция:

$c_0 = c_2$

$c_1 = c_1$

$c_2 = c_4$

$c_3 = c_3$

$\ldots$

$f : A \to B_1 B_1 \subset B, f$ — биекция.

$g : B \to A_1 A_1 \subset A, g$ — биекция.

$g(B1) = A_2 \subset A_1$

B_1 — равномощно A_2

A —- равномощно B_1

$\Rightarrow$ A равномощно A_2

$A \supset A_1 \supset A_2 \Rightarrow A_1$ равномощно $A \Rightarrow A$ равномощно B.

18 Теорема Кантора

Теорема Кантора: [0, 1] несчетно.

Доказательство: Пусть пронумировали.

$1 : x_{11}, x_{12}, x_{13}, \dots$

$2 : x_{21}, x_{22}, x_{23}, \dots$

$3 : x_{31}, x_{32}, x_{33}, \dots$

$\dots$

$\neg x_{11}, \neg x_{22}, \neg x_{33}, \dots$ - не пронумировали.

Следствие: множество $2^{\mathbb{N}}$ — несчетно.

Обобщенная теорема Кантора: X не равномощно множеству своих подмножеств 2^x

Доказательство: Пусть f — биекция $x \to 2^x$.

$D = \{a \in X | a \notin f(a)\}$

$D \subset X$

Пусть $f(d) = D$

1. $d \in D \Rightarrow d \notin f(d)$ — противоречие
2. $d \notin D \Rightarrow d \in f(d)$ —- противоречие

18.1 Континум

Определение: Множество имеет мощность континум если оно равномощно [0, 1]

Пример: Существует неалгебраическое вещественное число.

Пример: Существует характеристическая функция не вычисляемая программой.

Количество программ счетно, количество множеств континум.

19 Введение в графы

Ориентированный граф: (V, E), V — множество

$E \subset V \times V$

Петля: $(u, u) \in E$

Входящая степень: $d_{in}(u) = |\{(v, u) \in E | v \in V\}|$

Исходящая степень: $d_{out}(u) = |\{(u, v) \in E | v \in V\}|$

Неориентированный граф: (V, E), $E \subset \{\{v, u\} | v \in V, u \in V\}$

Степень вершины: $deg(v) = |\{e \in E | v \in e\}|$

Простой граф: — неориентированный граф без петель и кратных ребер.

19.1 Компоненты связности, пути и циклы

Путь в ориентированном/неориентированном графе: $V_1, V_2, V_3, \ldots, V_n \in V : \forall i \in [n-1](V_i, V_{i+1}) \in E$

Простой путь: —- путь в котором все вершины различны.

Длина пути: — $u_1, \ldots, u_n = n - 1$

Определение: вершины u и v связаны путем, если существует путь $w_1 = u, w_2, \ldots, w_k = v$

Замечание: Если u и v связаны путем, то они связаны простым путем.

Доказательство: самый короткий путь — простой.

$u, \ldots, w, \ldots, w, \ldots v \to u, \ldots, v$

Утверждение: Отношение быть связным путем в неориентированном графе —- отношение эквивалентности.

В ориентированных графах $u \sim v$ из u в v есть путь и из v в u есть путь.

Определение: Разбиение на классы эквивалентности в неориентированном графе — компоненты связности

Определение: Разбиение на классы эквивалентности в ориентированном графе — компоненты сильной связности

Фактор граф на отношение эквивалентности — компоненты сильной связности C. Есть ребро между c_i и c_j если $\exists u \in C_i, v \in c_j (u, v) \in E$

Утверждение: Фактор граф - DAG(граф без циклов)

В фактор графе нет петель, по определению. Путь есть цикл и в цикле лежит C_i и C_j. Рассмотрим вершины u из C_i и v из C_j, тогда существует путь из u в v и из v в u, значит они должны лежать в одном классе эквивалентности.

Цикл — это путь $v_1, \ldots, v_n : v_n = v_1$

Длина цикла — n - 1

Простой цикл $v_1, \ldots, v_{n-1}$ — различны.

$(v_1, v_2), \ldots (v_{n-1}, v_n)$ — различные ребра.

19.2 Деревья

Неориентированный граф.

Определение: Граф связный, если в нем одна компонента связности.

Определение: Дерево — это связный граф без простых циклов.

Утверждение: Если в дереве ≥ 2 вершины, то в нем ≥ 2 вершины степени 1(висячие вершины).

Доказательство: Пусть $u_1, u_2, \ldots, u_k$ — простой путь максимальной длинны. u_1 и u_k имеют степень 1.

Утверждение: Если в дереве n вершин, то в нем $n - 1$ ребро.

Доказательство: Индукция по числу вершин.

База: n = 1

Переход: Пусть u вершина степени 1. Выкинем ребро. (G/u) — дерево, по предположению индукции в нем n - 2 ребра $\Rightarrow$ в G n - 1 ребро.

Теорема: Следующий утверждения эквивалентны.

1. G — дерево
2. связны граф n - 1 ребро.
3. G — граф без циклов, в котором n - 1 ребро.
4. G — граф без циклов, но при добавление любого ребра появляется цикл.
5. G — связный граф, при удаление любого ребра связность теряется.

Доказательство: 1) $\to$ 2) доказали

2) $\to$ 3)

Пусть в G есть цикл. Будем удалять по ребру из цикла, пока циклы не закончатся.

Получилось дерево $\Rightarrow$ количество ребер n - 1 $\Rightarrow$ ничего не удалили.

3) $\to$ 1)

Если граф не связен можем добавить ребро между компонентами связности и циклов не появится. Добавляем пока не станет деревом, а в дереве n - 1 ребро, значит, мы ничего не добавили.

1) $\to$ 4)

Между любыми двумя вершинами есть простой путь, добавим ребро и получим цикл.

4) $\to$ 1)

Если бы граф не был связан смогли бы добавить ребро между компонентами.

1) $\to$ 5)

Пусть не теряется, тогда когда вернем ребро, получим цикл.

5) $\to$ 1)

Если бы в графе был цикл, то могли бы удалить ребро.

Остовное дерево: Из любого связного графа можно выкинуть несколько ребер так, что бы он стал деревом.

Дерево, которое получилось — остовное дерево.

Доказательство: Пока есть цикл, удаляем в цикле ребро.

Лес — граф, каждая компонента связности которого — дерево.

Лемма: Если G — неориентрованный связный граф, то |E| $\geq$ |V| - 1

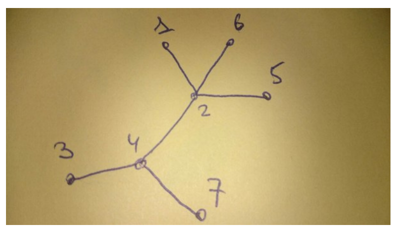
Доказательство: Если G — дерево, то |E| = |V| - 1

Рассмотрим остовное дерево G', в нем |V| - 1 ребро, в исходном графе ребер больше.

20 Теорема Келли

Теорема Келли: число деревьев с V = [n] равняется n^{n-2}

Доказательство(код Прюффера)



Находи лист с минимальным номером, выкидываем, записываем, к чему прикрепляется.

Повторяем, пока число вершин ≥ 2

2, 3, 2, 2, 4

Получилось n - 2 числа от 1 до n.

Это биекция.

Индукцией по n показываем, что каждому элементу из n^{n-2} соответствует ровно одно дерево.

База: n = 2 **Переход** Восстанавливаем первый лист и удаляем из последовательности первый элемент. По предположению индукции дерево восстанавливается однозначно.

21 Эйлеров путь, цикл. Раскраски графов

21.1 Эйлеров цикл

Эйлеров цикл — цикл, который проходит по всем ребрам ровно один раз.

Теорема: Пусть G — связный граф. В G есть эйлеров цикл $\Leftrightarrow$ степени всех вершин четны.

Доказательство: $\Rightarrow$ У каждой вершины на каждое входящее ребро, есть исходящее.

$\Leftarrow$

Рассмотрим самый длинный цикл, в котором не повторяются ребра C. Выкинем из G все ребра цикла C получился граф G'. В G' тоже все степени четные.

Цикл обязательно закончится в начальной вершин. Пойдем по ребру, найдем еще один цикл.

Если E' = 0, то все доказано.

Пусть E' != 0

1. Из связности G следует, что хотя бы из одной вершины C выходит ребро в E'.
2. Начинаем путь в G' по этому ребру, получаем цикл C'.
3. Склеиваем C и C' в большой цикл.

Противоречие с максимальностью C.

21.2 Эйлеров путь

Эйлеров путь — это путь проходящий по всем ребрам один раз.

Теорема: G — связный граф. В G есть эйлеров путь $\Leftrightarrow$ в G либо 0, либо 2 вершины нечетной степени.

Доказательство: $\Rightarrow$ все понятно

$\Leftarrow$ Если 0, то есть Эйлеров цикл, если 2, соединим ребром.

21.3 Раскраска графов

Правильная раскраска графов: G(V, E) неориентированный граф.

Правильная раскраска в k цветов.

Двудольный (2-дольный)

Теорема: Граф двудольный $\Leftrightarrow$

Доказательство: $\Rightarrow$ очевидно, так как вершины цикла обязаны менять цвет.

$\Leftarrow$ Пусть нет нечетных циклов.

В каждой компоненте раскрасим отдельно.

Теперь G - связный граф $u \in V$

Определим раскрасим $h(v) = \begin{cases} 1, & \text{если путь из u в v имеет нечетную длину} \\ 2, & \text{если четно} \end{cases}$

Если раскраска не однозначна, то существует цикл нечетной длины.

Пусть h неправильная раскраска, то существует цикл нечетной длинны.

Лемма: Если в G нет простых нечетных циклов, тот там нет нечетных циклов.

Доказательство: Рассмотрим самый короткий нечетный цикл.

Пусть он не простой. $u, \ldots, v, \ldots, v, \ldots, u$

В центе нечетный цикл, или если выкинуть получится нечетный. Значит, нечетный цикл не самый короткий.

22 Конечная теория вероятностей

Конечное вероятностное пространство.

Ω — конечное множество(пространство элементарных событий)

$p : 2^{\Omega} \to [0, 1]$

Вероятностная мера:

1. $P(\Omega) = 1$
2. $A, B \subset \Omega A \cap B = 0 P(A \cup B) = P(A) + P(B)$

Элементы множества Ω — элементарные события.

$A \subset \Omega$ A — событие.

$P(A)$ — вероятность события.

Свойства конечного вероятностного пространства.

1. P(0) = 0 $P(\Omega) + P(0) = P(\Omega)$
2. $A \subset B$, то $P(A) \subset P(B) P(B) = P(A) + P(B/A) \geq 0$
3. $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$
   $P_1 = P(\{\omega_1\})$
   $P_1 = P(\{\omega_2\})$
   $\ldots$
   $P_1 = P(\{\omega_n\})$
   $P(A) = \sum_{\omega_i \in A} P_i$
4. $P(A_1 \cup A_2 \ldots A_n) \leq \sum_{i=1}^{n} P(A_i)$
5. Формула включений/исключений.
   $P(A_1 \cup A_2 \ldots \cup A_n) = \sum_{i=1}^{n} P(A_i) - \sum_{i!=j}^{n} P(A_i \cap A_j) + \ldots$

22.1 Задача о галстуках

В каждом кружке d человек. Всего кружков $\leq 2^{d-1}$

Утверждение Можно выдать галстуки так, что бы в каждом кружке были как с галстуком, так и без.

Доказательство Рассмотрим случайный способ раздачи галстуков, что бы все способы были равновероятны.

A_i — в i-ом кружке либо все дети с галстуком, либо без.

$P(A_i) = (2^{n-d} + 2^{n-d})\dfrac{1}{2^n} = 2^{1-d}$

$P(\exists$ кружок, в котором либо все в галстуке, либо все без$) = P(A_1 \cup A_2 \cup \ldots \cup A_k) \leq 2^{d-1} * 2^{1-d} = 1$

$P(A_i \cap A_j) > 0 \Rightarrow P < 1$

23 Теорема Эрдеша-Ко-Радо

Теорема Эрдеша-Ко-Радо $S = \{0, 1, \ldots, n-1\}$

$\mathcal{F} \subset 2^s$

$\forall A \in \mathcal{F} |A| = kk \leq \dfrac{n}{2}$

$\forall A, B \in \mathcal{F} A \cap B \neq 0$

Тогда $|\mathcal{F}| \leq C_{n-1}^{k-1}$

Доказательство: $A_s = \{s, s+1, \ldots, s+k-1\}$ mod n

Лемма: $\mathcal{F}$ содержит $\leq k$ элементов A_s

Доказательство: $A_s \in \mathcal{F}$

Рассмотрим элементы, которые пересекаются с A_s их 2k - 2

Разбиваем на пары:

$A_{s-k+1} - A_{s+1}$

$\ldots$

$A_{s-1} - A_{s+k-1}$

Из каждой пары можем взять не более одного элемента.

$\Downarrow$

Кроме A_s может быть $\leq k-1$ элемента.

$\Downarrow$

$\mathcal{F}$ содержит $\leq k$ элементов A_s

$\sigma : [n] \to [n]$ — биекция.

$i \in [n]$

$A_{\sigma,i} = \{\sigma(i), \sigma(i+1), \ldots, \sigma(i+k-1)\}$

$\Omega = \{(\sigma, i) | \sigma \in S_n, i \in n\}$

$|\Omega| = nn!$

$P(\{\sigma, i\}) = \dfrac{1}{nn!}$

$X \subset \Omega$

$X = \{(\sigma, i) | A_{\sigma,i} \in \mathcal{F}\}$

$P(x) \leq \dfrac{kn!}{nn!}$

$P(x) \leq \dfrac{k}{n}$

$P(x) = \dfrac{|\mathcal{F}|}{C_n^k}$

$|\mathcal{F}| \leq \dfrac{k}{n} C_n^k = C_{n-1}^{k-1}$

24 Математическое ожидание

24.1 Случайная величина

Случайная величина: $\xi : \Omega \to \mathbb{R}$

Примеры:
1. $\Omega = \{0, 1\}^3$
   $\xi(\omega) =$ число единиц в ω
2. $\Omega = \{1, 2, 3, 4, 5, 6\}$
   $\xi(\omega) = \omega$
3. $\Omega = \{$ множество простых графов на n вершинах$\}$
   $|\Omega| = 2^{C_n^2}$
   $P(\omega) = \dfrac{1}{2^{C_n^2}}$
   $\xi(\omega)$ — число ребер в ω

24.2 Математическая ожидание

Математическое ожидание: $E[\xi] = \sum_{\omega \in \Omega} P(\{\omega\}) \xi \omega$

Лемма: $\alpha, \beta \in \mathbb{R}$

Тогда $E[\alpha\xi + \beta\eta] = \alpha E[\xi] + \beta E[\eta]$

Доказательство: $E[\alpha\xi + \beta\eta] = \sum_{\omega \in \Omega} P(\omega)(\alpha\xi(\omega) + \beta\eta(\omega)) = \alpha \sum_\omega P(\omega)\xi(\omega) + \beta \sum_\omega P(\omega)\eta(\omega) = \alpha E[\xi] + \beta E[\eta]$

Пример: $\xi(\omega)$ — число ребер в графе ω

$$\xi(\omega_e) = \begin{cases} 1, & \text{ребро e есть в} \omega \\ 0, & \text{иначе} \end{cases}$$

$\xi = \sum_e \xi_e$

$E[\xi_e] = \sum_{\omega, e\text{ ---ребро}} P(\{\omega\}) = \dfrac{1}{2}$

$E[\xi] = \sum_e E[\xi_e] = C_n^2 \dfrac{1}{2}$

Линейность: ξ принимает значения $a_1, a_2, \ldots, a_n$

$P[\xi \in A] = P(\xi_\omega | \xi(\omega) \in A)$

$A \subset \mathbb{R}$

$q_i = P[\xi = a_i]$

$E[\xi] = a_1 q_1 + a_2 q_2 + \ldots + a_n q_n$

Лемма(принцип усреднения): $\xi : \Omega \to \mathbb{R} E[\xi] = \mu$

Тогда $\exists \omega \in \Omega$, что $\xi(\omega) \geq \mu$ и $\exists \omega' \in \Omega \xi(\omega') \leq \mu$

Доказательство: Пусть все $\xi(\omega) < \mu$

Тогда $E[\xi] = \sum_{\omega \in \Omega} \xi(\omega) P(\{\omega\}) < \mu (\sum_\omega P(\{\omega\}) = 1)$

24.3 Турнир с большим числом гамильтоновых путей

Турнир — ориентированный граф на n вершин между любыми 2-мя вершинами ровно одно ребро.

Гамильтонов путь — простой путь, который проходит по каждой вершине ровно один раз.

Утверждение: $\exists$ турнир на n вершинах, в которых $\geq \dfrac{n!}{2^{n-1}}$ гамильтонов путь.

Доказательство: $\Omega = \{$ множество турниров на n вершинах$\}$

$|\Omega| = 2^{C_n^2}$

$P(\omega) = \dfrac{1}{2^{C_n^2}}$

$X : \Omega \to \mathbb{R}$

$X(\omega)$ $-$ $--$ число гамильтоновых путей в ω

Пусть $\sigma \in S_n$

$X_\sigma(\omega) = \begin{cases} 1, & \text{если } \sigma(1), \sigma(2), \ldots \text{ гамильтонов путь} \\ 0, & \text{иначе} \end{cases}$

$X = \sum_\sigma X_\sigma$

$E[X_\sigma] = P(\{\omega | \sigma(1), \sigma(2), \ldots \text{ — гамильтонов путь}\})$

$E[X_\sigma] = \dfrac{2^{C_n^2 - (n-1)}}{2^{c_n^2}} = \dfrac{1}{2^{n-1}}$

$E[x] = \dfrac{n!}{2^{n-1}}$

25 Набор выполняющий $\frac{7}{8}$ дизъюнктов 3-КНФ. Неравенство Маркова

25.1 Набор выполняющий $\frac{7}{8}$ дизъюнктов 3-КНФ

Пример: 3-КНФ

e — формула в 3-КНФ, в каждый дизъюнкт входит 3 различных переменных .

$(x \cup y \cup \neg z) \cap (x \cup z \cup \neg y) \cap \dots$

m — число дизъюнктов.

$\exists$ набор значений переменных, который выполнит $\geq \dfrac{7}{8}m$

Доказательство: $\Omega = \{$множество наборов значений переменных$\}$

$X(\omega) =$ число выполненных дизъюнктов.

C — дизъюнкт

$X_c(\omega) = \begin{cases} 1, & \text{если c выполняет } \omega \\ 0, & \text{иначе} \end{cases}$

$E[X_c] = \dfrac{7}{8}$

$E[X] = \sum_c E[X_c] = \dfrac{7}{8}m \Rightarrow$ есть такое значение, которое выполняет $\dfrac{7}{8}m$ дизъюнктов.

25.2 Неравенство Маркова

Теорема(Неравенство Маркова): $X : \Omega \to \mathbb{R}, X \geq 0, E[x] > 0$

Тогда $\forall c > 0$

$P[x \geq cE[x]] = P(\{\omega | X(\omega) \geq cE[x]]\}) \leq \dfrac{1}{c}$

Доказательство: Пусть $P[x \geq cE[c]] > \frac{1}{c}$

$E[x] = \sum_\omega X(\omega)P(\{\omega\}) \geq \sum_{\omega : X(\omega) \geq cE[x]} X(\omega)P(\{\omega\}) \geq cE[c] \sum_{\omega X(\omega) \in cE[x]} P(\{\omega\}) > E[x]$

25.3 Алгоритм, который находит набор.

Φm

y — число не выполненных дизъюнктов.

$E[y] = \dfrac{1}{8}m$

$P[y > \dfrac{1}{8}m] = P[8y > m] = P[8y \geq m + 1] = P[y \geq (\dfrac{1}{8}m)\dfrac{m+1}{m}] \leq \dfrac{m}{m+1} = 1 - \dfrac{1}{m+1}$

Алгоритм Повторить t раз.

Взять случайный набор и проверить подходит ли он.

P[Алгоритм не нашел набор, выполняющий $\geq \frac{7}{8}m] \leq (1-\frac{1}{m+1})^t = ((1-\frac{1}{m+1})^{m+1})^N < \frac{1}{e^N}$

$t = N(m+1)$

26 Независимые событие

26.1 Независимые события

Определение: Ω, p

$A_1, A_2, \ldots, A_n \subset \Omega$

События $A_1, A_2, \ldots, A_n$ независимы, если $P(A_1 \cap A_2 \cap \ldots A_n) = P(A_1) * P(A_2) * \ldots P(A_n)$

26.2 независимые случайные величины

Определение: $X_1, X_2, \ldots, X_n : \Omega \to \mathbb{R}$ независимые, если

$\forall a_1, a_2, \ldots, a_n \in \mathbb{R}$

$P[x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n] = P[x_1 = a_1]P[x_2 = a_2]\ldots P[x_n = a_n]$ — независимые события.

Свойства:

1. $x_1, x_2, \ldots, x_n$ — — — независимые.
   $A_1, A_2, \ldots, A_n \in \mathbb{R}$
   Тогда $P[x_1 \in A, x_2 \in A_2, \ldots x_n \in A_n] = \prod_{i=1}^n P(x_i \in A_i)$
2. $x_1, x_2, \ldots, x_n$ — — — независимые
   $f_1, f_2, \ldots, f_n : \mathbb{R} \to \mathbb{R}$
   Тогда $f_1(x_1), f_2(x_2), \ldots, f_n(x_n)$ — — — независимые.

26.3 Распределение Бернули:

Распределение Бернули: $X : \Omega \to \mathbb{R}$

$p[x = 1] = p$

$p[x = 0] = 1 - p$

Биномиальное распределение: $x_1, x_2, \ldots, x_n$ — независимые

$p[x_i = 1] = p, p[x_i = 0] = 1 - p$

$x = x_1 + x_2 + \ldots + x_n$

$p[x=k]=C_n^k p^k(1-p)^{n-k}$
$E[x_i]=p$
$E[x]=\sum_1^n E[x_i]=pn$

26.4 Закон больших чисел для распределения Бернули

Теорема(Закон больших чисел для распределения Бернули) $\forall p,\epsilon \exists c<1$
$x_1,\ldots,x_n$ — независимые
$E[x_i]=p$
$p[|\dfrac{x_1+\ldots+x_n}{n}-p|\geq\epsilon]\leq 2c^n$

Доказательство: $A=X_1\circ X_2\circ\ldots\circ X_n$
$A:\Omega\to\{0,1\}^n$
$Y_1,Y_2,\ldots,Y_n$ —независимые.
$P[Y_i=1]=p+\epsilon$
$P[Y_i=0]=1-p-\epsilon$
$\mathrm{B}=Y_1\circ Y_2\circ\ldots\circ Y_n$
$S\in\{0,1\}^n$
$\omega(s)$ — число единиц в S.
$P[A=S]=p^{\omega(s)}(1-p)^{n-\omega(s)}$
$P[B=S]=(p+\epsilon)^{\omega(s)}(1-p-\epsilon)^{n-\omega(s)}$
Пусть $\omega(s)\geq(p+\epsilon)n$
$P[A=S]\leq P[B=S]$
$P[A=S]=P[B=S](\dfrac{p}{p+\epsilon})^{\omega(s)}(\dfrac{1-p}{1-p-\epsilon})^{n-\omega(s)}\leq P[B=S](\dfrac{p}{p+\epsilon})^{(p+\epsilon)n}(\dfrac{1-p}{1-p-\epsilon})^{1-p-\epsilon}n=$
$P[B=S]c^n$, где $=(\dfrac{p}{p+\epsilon})^{p+\epsilon}(\dfrac{1-p}{1-p-\epsilon})^{1-p-\epsilon}$
Позже покажем, что $\mathrm{c}<1$
$P[\dfrac{\sum x_i}{n}\geq p+\epsilon]=\sum_{s,w(s)\geq(p+\epsilon)n}P[A=S]\leq\sum_{s,w(s)\geq(p+\epsilon)n}P[B=S]c^n\leq c^n$
Аналогично $p[\dfrac{\sum x_i}{n}\leq p-\epsilon]\leq c'^n$
$P[|\dfrac{\sum x_i}{n}-p|\geq\epsilon]\leq c'^n+c^n\leq 2max(c',c)^n$
$\ln(x)\leq x-1$
$\ln(c)=(p+\epsilon)\ln\dfrac{p}{p+\epsilon}+(1-p-\epsilon)\ln(\dfrac{1-p}{1-p-\epsilon})\leq(p+\epsilon)(\dfrac{p}{p+\epsilon}-1)+(1-p-\epsilon)(\dfrac{1-p}{1-p-\epsilon}-1)=p-(p+\epsilon)+((1-p)-(1-p-\epsilon))=0$

27 Дисперсия

27.1 Математическое ожидание произведения независимых случайных величин

Лемма X, Y — независимы, тогда $E[xy] = E[x]E[y]$

Доказательство $E[xy] = \sum_{a \in \mathbb{R} \text{конечная сумма}} = \sum_{a_1(\text{значение x}, a_2(\text{значение y}))} a_1 a_2 P[x = a_1, y = a_2] = \sum a_1 a_2 P[x = a_1] P[y = a_2] = (\sum a_1 P[x = a_1])(\sum a_2 P[y = a_2]) = E[x]E[y]$

27.2 Дисперсия

Определение: $D[x] = E[(x - E[x])^2]$ — дисперсия случайной величины X.

$D[x] = E[x^2 + (E[x])^2 - 2xE[x]] = E[x^2] + (E[x])^2 - 2E[x]E[x] = E[x^2] - (E[x])^2 \geq 0$

Примеры: $p[x = 1] = p$

$p[x = 0] = 1 - p$

$D[x] = E[x^2] - (E[x])^2 = p - p^2 = p(1 - p)$

Свойства дисперсии:

1. $D[\alpha x] = \alpha^2 D[x]$
   $E[(\alpha x)^2] = (E[\alpha x])^2 = \alpha^2 (E[x^2] - (E[x])^2)$
2. $x_1, x_2, \ldots, x_n$ — случайные величины.
   $\forall i \neq j, x_i$ и x_j — независимы(попарно независимы)
   Тогда $D[x_1 + \ldots + x_n] = \sum_{i=1}^n D[x_i]$
   Доказательство $D[x_1 + \ldots + x_n] = E[(x_1 + \ldots + x_n)^2] - (E[x_1 + \ldots + x_n])^2 = \sum E[x_i^2] + \sum_{i \neq j} E[x_i x_j] - \sum (E[x_i])^2 - \sum_{i \neq j} E[x_i]E[x_j] = \sum_{i=1}^n E[x_i^2] - (E[x_i])^2 = \sum_{i=1}^n D[x_i]$

28 Неравенство Чебышева

28.1 Неравенство Чебышева

Теорема. Неравенство Чебышева $p[|x - E[x]| \geq \epsilon] \leq \dfrac{D[x]}{\epsilon^2}$

Доказательство: $P[|x - E[x]| \geq \epsilon] = P[(x - E[x])^2 \geq \epsilon^2] = P[(x - E[x])^2 \geq \dfrac{\epsilon^2 D[x]}{D[x]}] \leq \dfrac{D[x]}{\epsilon^2}$

28.2 Закон больших чисел для попарно независимых случайных величин

Теорема. $x_1, x_2, \ldots, x_n$ — попарно независимые.

$p[x_i = 1] = p, p[x_i = 0] = 1 - p$

Тогда $P[|\dfrac{\sum x_i}{n} - p| \geq \epsilon]$

Доказательство: $y = \dfrac{\sum x_i}{n}$

$E[y] = p$

$D[y] = \dfrac{D[\sum x_i]}{n^2} = \dfrac{np(1-p)}{n^2} = \dfrac{p(1-p)}{n}$

$P[|y - p| \geq \epsilon] \leq \dfrac{p(1-p)}{\epsilon^2 n} \leq \dfrac{1}{4\epsilon^2 n}$

$\sqrt{p(1-p)} \leq \dfrac{p + (1-p)}{2}$

29 Условная вероятность

29.1 Условная вероятность

Условная вероятность: $\Omega, pA \subset \Omega P(A) > 0$

$B \subset \Omega$

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

1. A, B — независимые. $P(B|A) = P(B)$
2. (Формула Байеса) $P(B \cap A) = P(B|A)P(A)$
3. (Формула полной вероятности) $A_1 \cup A_2 \ldots A_n = \Omega$
   $A_i \cap A_j = 0 \forall i, j$
   Тогда $P(B) = \sum_{i=1}^{n} P(B|A_i)P(A_i)$

30 Лемма Фаркаша

Имеет ли система решение?

$$\begin{cases} a_{11}x_1 + a_{12} + \ldots + a_{1n}x_n \leq b_1 \\ \ldots \\ a_{m1}x_1 + a_{m2} + \ldots + a_{mn}x_n \leq b_n \end{cases}$$

Можно сложить с коэффициентами и получить противоречие.

Лемма Фаркаша Если система линейных неравенств несовместима $\Leftrightarrow \exists \alpha_1, \alpha_2, \dots, \alpha_m \geq 0:$

$\alpha_1(a_{11}x_1 + a_{12}x_2 + \dots) + \alpha_2() + \dots = 0$

$\alpha_1 b_1 + \dots + \alpha_m b_m = -1$

Доказательство: $\Leftarrow$ очевидно.

$\Rightarrow$

Индукция по n.

База n $=$ 1

$x_1 \leq c_1$

$\dots$

$x_1 \leq c_k$

$x_1 \geq d_1$

$\dots$

$x_1 \geq d_l$

$\exists i, j : c_i < d_j$

$0 \leq c_i - d_j$

Переход

неравенство без x_1 (**)

$x1 \leq f_1(x_2 \dots x_n)$

$x1 \leq f_2(x_2 \dots x_n)$

$\dots$

$x1 \leq f_k(x_2 \dots x_n)$

$x1 \geq g_1(x_2 \dots x_n)$

$x1 \geq g_2(x_2 \dots x_n)$

$\dots$

$x1 \geq g_t(x_2 \dots x_n)$

$$\begin{cases} (**) \\ g_i(x_2, \dots, x_n) \leq f_j(x_2, \dots, x_n) \\ i \in [l], j \in [k] \end{cases}$$

Эта система не содержит x_i

Новые неравенства — это линейная комбинация старых с неотрицательными коэффициентами. $x_1 \leq f_j(x_2, \dots, x_n)$

$-x_1 \leq -g_i(x_2, \dots, x_n)$

31 Задача линейного программирования. Двойственная задача.

31.1 Задача линейного программирования.

$c_1x_1 + c_2x_2 + \ldots + c_nx_n \to \max$

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n \le b_1 \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \le b_n \end{cases}$$

Множество решений системы (*) — множество допустимых решений.

$c_1x_1 + \ldots + c_nx_n$ — целевая функция.

Факт Если целевая функция ограничена на множестве допустимых решения, то задача линейного программирования имеет оптимальное решение.

31.2 Двойственная задача

$y_1b_1 + y_2b_2 + \ldots + y_mb_m \to \min$

$$\begin{cases} a_{11}y_1 + \ldots + a_{m1}y_m \le c_1 \\ \ldots \\ a_{1n}y_1 + \ldots + a_{mn}y_m \le c_m \\ y_1, \ldots, y_m \ge 0 \end{cases}$$

Теорема 1. $x_1, \ldots, x_n$ $---$ допустимое решение.
$y_1, \ldots, y_m$ $---$ допустимое решение.
то $c_1x_1 + c_2x_2 + \ldots + c_nx_n \le y_1b_1 + \ldots + y_mb_m$

2. Если множество допустимых решений (1) и (2) не пусто, то $\exists$ оптимальное решение $x_1^*, \ldots, x_n^*(1)$
$y_1^*, \ldots, y_n^*(2)$
$c_1x_1^* + \ldots + c_nx_n^* = b_1y_1^* + \ldots + b_my_m^*$

3. Если $x_1^*, \ldots, x_n^*, y_1^*, \ldots, y_m^*$ оптимальное решение и $a_{i1}x_1^* + \ldots + a_{in}x_n^* < b_i \Rightarrow y_i^* = 0$

Доказательство: 1. $y_1b_1 + y_2b_2 + \ldots + y_mb_m \ge \sum_{i=1}^m y_i \sum_{j-1}^n a_{ij}x_j = \sum_{j=1}^n x_j \sum_{i=1}^m y_ia_{ij} = \sum_{j=1}^n x_jc_j$

2. $c_1x_1 + \ldots + c_nx_n \le y_1b_1 + \ldots + y_mb_m$
$c_1x_1 + \ldots + c_nx_n \le inf_{y\text{ — допустимые решения (2)}}(y_1b_1 + \ldots + y_mb_m) = d_2$
Докажем, что $\exists x_1^*, \ldots, x_n^*$ — допустимые решение(1)
$c_1x_1^* + c_2x_2^* + \ldots + c_nx_n^* = d_2$
От противного, пусть такого решения нет.

$$\begin{cases} (*) \\ -c_1x_1 - c_2x_2 - \ldots - c_nx_n \leq -d_2 \end{cases}$$
несовместимая система.
$\exists y_1, \ldots, y_m :$
$\sum y_i a_i 1 = c_1$
$\ldots$
$\sum y_i a_i n = c_n$
$(\sum_{i=1}^m y_i b_i) - d_2 < 0$
y_i $- --$ допустимое решение (2)
$y_1 b_1 + \ldots + y_m b_m < d_2 = inf$ противоречие.
Аналогично $\exists y_1^*, \ldots, y_m^*$
$\sum b_i y_i^* = d1 = sup()$

3. Если стоит строгое равенство в решение и существует $\sum_j a_{ij} x_j < b_j$, то $y_j = 0$

32 Поток в графе

32.1 Поток

G — ориентированный граф $G(V, E)$

$s, t \in V$

s — исток.

t — сток.

$c : v \times v \to \mathbb{R}_+$ — пропускная способность

Если $(u, v) \notin E$, то C(u, v) = 0

Пусть $\mathcal{P}$ — множество простых путей из s в t.

Поток $\{f_p\}_{p \in \mathbb{R}}$

$f_p \geq 0$

$\forall e \in E \sum_{p \in \mathcal{P}} f_p \leq c(e)$

Размер потока $\sum_{p \in \mathcal{P}} f_p$

$\sum_{p \in \mathcal{P}} f_p \to max$

$$\begin{cases} f_p \geq 0 \\ \sum_e f_p \leq c(e) \end{cases}$$

32.2 Двойственная задача

$\sum_e l_e c(e) \to min$

$$\begin{cases} \sum_{l \in p} l_e - \gamma_p = 1 \\ l_e \geq 0 \\ \gamma_p \geq 0 \end{cases}$$

32.3 разрез

$S, T \subset V S \cap T = 0, s \in S, t \in T, S \cup T = V$

(S, T) — разрез

Пусть (S, T) разрез определим $l_e = \begin{cases} 1, & \text{если e ведет из S в T} \\ 0, & \text{иначе} \end{cases}$

$\sum f_p \leq \sum l_e c(e)$ — суммарный поток меньше любого разреза.

32.4 Теорема Форда-Фолкерсона

Теорема Форда-Фолкерсона Размер максимального потока равен минимальной пропускной стоимости разреза.

Доказательство Пусть f_p^* — оптимальное решение прямой задачи, l_e^*, γ_p^* — оптимальное решение двойственной задачи.

1. $\sum_{p \in P} f_p^* = \sum_e l_e^* c(e)$
2. $f_p^* > 0$, то $\gamma_p^* = 0 \sum_e l_e^* = 1$
3. $\sum f_p < c(e)$, то $l_e^* = 0$

Строим разрез по l_e^*

S — множество всех вершин, в которое можно дойти из S по ребрам $e : l_e^* = 0$

T — все остальные. $T = V - S$

Пусть e ведет из S в T.

$c(e) = \sum f_p^*$, так как $l_e^* > 0$

$\sum_{l \text{из S в T}} c(e) \leq \sum_p f_p^*$, если было бы верно, что $\forall p : f_p^* > 0$ пересекает S, T ровно 1 раз.

Пусть $f_p^* > 0$ и p пересекает S, T несколько раз $f_p^* > 0$, то $\sum_{l \in p} l_e^* = 1$

33 Целочисленный поток

Теорема: Если $\forall e c(e) \in \mathbb{Z}_+$

Тогда $\exists$ целочисленный максимальный поток.

Доказательство: Размножим ребра, теперь у всех ребер пропускная способность = 1.

Найдем путь из S в T пустим поток и удалим ребро.

Проблема, решение может быть не оптимально. Можем пройти через разрез несколько раз.

Правильный алгоритм:

1. Ищем путь из S в T
2. Пускаем по нему поток.
3. удаляем ребро.
4. добавляем обратное ребро.

Нет пути ⇒ поток совпадает с разрезом ⇒ он максимальный.

34 Паросочетания

34.1 Паросочетания

Определение: Неориентированный граф.

$G(V, E)$

$E' \subset E$ E' — паросочетание, если ребра из E' не имеет общих концов.

34.2 Теорема Кенинга

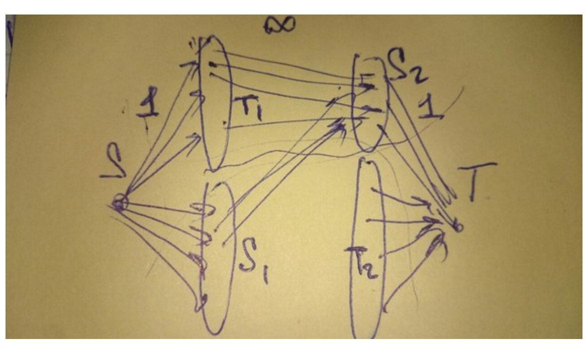
G — двудольный граф.

Из каждый вершины исходит хотя бы одно ребро.

Теорема Кенинга Размер максимального паросочетания в G = размер минимального покрывающего множества.

$S \subset V$ покрывающие множество $\forall e \in E$ имеет конец в S.

Доказательство: Размер любого паросочетания $\leq$ размера любого покрывающего множества(любое ребро паросочетания нужно покрыть)



Добавим вершины S и T, ребра из S в первую долю с пропускными способностями 1, из ребер второй доли в T с пропускными способностями 1 и между долями пропускные способности +inf.

Рассмотрим минимальный разрез. Пусть он равен $T_1 + S_2$, тогда из S_1 в T_2 нет ребер.

Паросочетание — ребра, по которым течет поток.

T_1 и S_2 — покрытие, поскольку нет ребер из S_1 в T_2;

Размер паросочетания = размеру потока = $|T_1| + |S_2|$ = размеру покрытия.

34.3 Теорема Холла

Теорема Холла G — двудольный граф, тогда в G есть паросочетание размера |M| $\Leftrightarrow \forall S \subset M |\Gamma(S)| \geq |S|$

$\Gamma(S) = \{v \subset N : \exists u \in S (u, v) \in E\}$

Доказательство: $\Rightarrow$ очевидно.

$\Leftarrow$ От противного. Пусть есть покрывающее множество размера < |M|

$\forall v \in M/S_1$ соединяется только с вершинами из S_2

$\Gamma(M/S_1) \subset S_2$

$\Leftarrow |S_2| \geq |M/S_1|$

$\Leftarrow |S_1 + S_2| \geq |S_1| + |M/S_1| = |M|$

35 Частично упорядоченные множества

35.1 Частично упорядоченные множества

Определение: M — множество.

$\leq$ бинарное отношение.

$\leq$ частичный порядок, если

1. транзитивно:
   $a \leq b, b \leq c \Rightarrow a \leq c$
2. антисимметрично
   $a \leq b, b \leq a \Rightarrow a = b$
3. рефлексивность
   $a \leq a$

35.2 Цепь

$(M, \leq)$

Определение: Цепь — такое $S \subset M$

$\forall x, y \in S(x \leq y$ или $y \leq x)$

$(M, \leq)$

Покрытие цепями $M = S_1 \cup S_2 \cup \ldots \cup S_k$

$S_i \cap S_j = 0 \forall S_i$ — цепь.

k — размер покрытия.

35.3 Антицепь

Определение: Антицепь — $S \subset M, S$ — антицепь , если $\forall x, y \in S$

$$x \neq y \Rightarrow \begin{cases} \neg(x \leq y) \\ \neg(y \leq x) \end{cases}$$

35.4 Теорема Дилвортса

Теорема Дилвортса: $(M, \leq)$

Размер максимальной антицепи равен минимальному размеру покрытия М цепями.

Доказательство: Размер $\forall$ покрытия цепями $\geq$ размер $\forall$ антицепями. (Так как цепь не может содержать 2 элемента антицепи)

Создадим копию каждого элемента множества М, М'.

Проведем ребро между x_i и x'_j, если $x_i < x_j$

Рассмотрим максимальное паросочетание в двудольном графе. Пусть его размер К.

Нарисуем ребра, которые вошли в паросочетание в исходном графе.

Получилось: из каждой вершины выходит ≤ 1 ребра и ≤ 1 ребра входит.

По транзитивности циклов нет.

Получили покрытие n - k цепями. (при добавление ребра каждые две цепи объединяются)

В двудольном графе есть минимальное покрывающее множества размера k(по теореме Кенга)

$S \subset M : \forall x \in Sx, x'$ не входит в покрывающее множество.

$\forall x, y \in S$ нет ребра между (x, y') и (y, x') $\Rightarrow S$ антицепь размера $S \geq n - k$

36 Теорема Менгера

Реберная теорема Менгера $G(V, E)$ — простой неориентированный граф.

$s, t \in V$

μ — максимальное количество не пересекающихся по ребрам путей из s в t.

ν — минимальное количество ребер, которое нужно удалить, чтобы s и t оказались в разных компонентах связности.

$\mu = \nu$

Доказательство: $\mu < \nu$, так как из каждого пути нужно удалить хотя бы одно ребро.

Из s все ребра исходящие.

В t все ребра входящие. Все остальные ребра ориентированные и туда и туда.

Все пропускные способности равны 1.

Утверждение: Пропускная способность минимального размера $= \nu$

Разрез достаточно удалить, что бы вершины оказались в разных компонентах.

По теорема Форда-Фолкинсона $\exists$ поток, размер которого равен ν

Поскольку все пропускные способности целочисленные, то поток состоит из путей по которым течет 1.

37 Код Хемминга

37.1 Игра с угадыванием числа

Задача: $k = \lceil \log_2 n \rceil$ — необходимое количество вопросов, что бы угадать число.

Алгоритм: бинарный поиск.

Доказательство оптимальности ответа: Построим дерево ответов. Листья — возможные ответы.

m — вопросов.

2^m — листьев.

$2^m \geq log_2 n$

$m \geq \lceil log_2 n \rceil$

37.2 Игра с одной ошибкой

n один ответ может быть не верный.

m вопросов. Каждое число должно быть записано m + 1 раз.

$2^m \geq (m+1)n$

$m \geq log_2(m+1) + log_2(n)$

37.3 Код Хемминга

Определение: Расстояние по Хеммингу

$x, y \in \{0,1\}^n$

$\delta(x, y) = \{i | x_i \neq y_i\}$

Определение: $C : \{0,1\}^k \to \{0,1\}^m$ называется кодом исправляющем ошибку с расстоянием d, если

$\forall x, y \in \{0,1\}^k$

$\delta(C(x), C(y)) \geq d$

$x \neq y$

Если $2r + 1 \leq d$, то говорят, что код исправляет r ошибок.

Утверждение: Пусть код $C : \{0,1\}^k \to \{0,1\}^m$ исправляет 1 ошибку(расстояние 3).

Тогда в предыдущей игре можно угадать число за m вопросов ($n \leq 2^k$)

$[n] \to \{0,1\}^k$

находим кодовое слово C(y) которое max на расстояние 1 от $z_1 z_2 \ldots z_m$. Ответ y.

Теорема $C : \{0,1\}^k \to \{0,1\}^m$ — код, исправляющий 1 ошибку(код на расстояние 3), то $2^m \geq (m+1)2^k$

Код Хемминга Пусть $2^m \geq (m+1)2^k$. Тогда существует код $C : \{0,1\}^k \to \{0,1\}^m$, исправляющий 1 ошибку.

$2m \geq 2^{m-k} \geq m + 1$

$2^{m-k} - 1 \geq m$

Выпишем все не нулевые числа.

				m			
	1	0	1	0	1	1	
m-k	0	1	1	0	0	1	
	0	0	0	1	1	1	
	0	0	0	0	0	0	

$y \in \{0,1\}^m$ — кодовое слово, если скалярное произведение по mod 2 на каждую строку таблицы равно 0.

Столбцы, в которых одна 1 — дополнительные, остальные информационные.

38 Теорема Рамсея

$R(M, N)$ — это минимальное такое число K, что $\forall$ полного графа на k вершинах, ребра которого раскрашены в два цветы, найдутся либо m вершин, все ребра покрашены в 1 цвет, либо n вершин, все ребра между ними покрашены во 2 цвет.

$R(n, n) \leq C_{2n-2}^{n-1} \leq 2^{2n-2}$

38.1 Верхняя оценка

$R(2, n) = n$

$m, n \geq 3$

R(m, n) = R(n, m)

$R(m, n) \leq R(m-1, n) + R(m, n-1)$

Пусть в графе k = $R(m-1, n) + R(m, n-1)$ вершин.

Выбираем 1 вершину у нее $R(m-1, n) + R(m, n-1)$ - 1 сосед. $\Rightarrow$

1. У этой вершины $\geq R(m-1, n)$ соседей первого цвета.
2. $\geq R(m, n-1)$ соседей 2 цвета.

$\Rightarrow$ R(m, n) — конечно(по индукции)

$R(m, n) \leq C_{m+n-2}^{m-1}$

Доказательство: индукция по m+n

База n = 2 R(m, 2) = m

Переход $R(m, n) \leq R(m-1, n) + R(m, n-1) \leq C_{m+n-3}^{m-2} + C_{m+n-3}^{m-1} = C_{m+n-2}^{m-1}$

39 Обобщение чисел Рамсея

R(s, m, n) — это наименьшее такое число k, что при любой раскраске всех s — элементных подмножеств [k] в 2 цвета найдется, либо m элементное множество, все s-элементные подмножества покрашены в 1 цвет, либо n элементное подмножество, все s-элементы которого покрашены во второй цвет.

$R(1, m, n) = m + n - 1$

$R(2, m, n) = R(m, n)$

$R(2, m, n) \leq R(2, m-1, n) + R(2, m, n-1) - 1 + 1$

$R(s, m, n) \leq R(s-1, R(s, m-1, n), R(s, m, n-1)) + 1$

Пусть k = R(s - 1; R(s, m - 1, n), R(s, m, n - 1)) + 1

Выберем $u \in [k]$

Все (s - 1) — элементные подмножества $[k]/\{u\}$

$A \subset [k]/\{u\}|A| = s - 1$ красим A в цвет $A \cup \{u\}$

Среди $[k]/\{u\}$ есть либо

1. R(S; m - 1, n) элементов: $\forall (s-1)$ подмножество покрашенное в цвет 1
2. $R(S; m, n-1)$ элементов: $\forall (s-1)$ элементов подмножества покрашенные в цвет 2.

39.1 Для раскраски во много цветов

$R_r(S, n_1, n_2, \ldots, n_r)$
$R_r(S, n_1, \ldots, n_r) \leq R_r(s-1, R_r(s, n_1-1, \ldots), R_r(s, n_1, n_2-1, \ldots), \ldots, R_r(s, n_1, \ldots, n_r-1)) + 1$

40 Нижняя оценка на R(k, k). Бесконечный вариант теоремы Рамсея

40.1 Нижняя оценка на R(k, k)

Предложение: $R(n, n) \geq 2^{\overline{\frac{n}{2}}}$ при $n \geq 3$

Доказательство: Возьмем полный граф на k вершинах и покрасим его ребра в 2 цвета случайным образом.

ρ — подмножество из n вершин.

p[все ребра множества S покрашены в 1 цвет] $= 22^{-C_n^2}$

p[$\exists$ n вершин множества, что все ребра покрашены в 1 цвет] $\leq \sum_{\rho\text{ — n вершин множества}}$P[все ребра в S покрашены в 1 цвет] $\leq C_k^n 2^{1-C_n^2} < 1()$

Пусть k = $\lfloor 2^{\overline{\frac{n}{2}}} \rfloor$

$$C_n^k 2^{1-C_n^2} < \frac{k^n}{n!} \frac{2^{\overline{\frac{n}{2}}+1}}{2^{\overline{\frac{n^2}{2}}}} \leq \frac{2^{\overline{\frac{n}{2}}+1}}{n!} < 1 n \geq 3$$

$$1 - C_n^2 = 1 - \frac{n(n-1)}{2}$$

40.2 Бесконечный вариант теоремы Рамсея

Теорема: Если ребра бесконечного графа покрашены в r цветов, то $\exists$ бесконечное число вершин, что все ребра между ними покрашены в 1 цвет.

Доказательство: Достаточно доказать для двух цветов(в противном случае склеиваем цвета)

Рассмотрим два случая.

1. Рассмотрим только вершины,у которых соседей первого цвета конечно. Если таких бесконечное количество.
   Выбираем вершину, выкидываем всех соседей первого цвета. Оставшихся вершин бесконечно. Повторим операцию.

2. Если таких вершин конечно.
   Выбираем вершину, у которой бесконечное количество соседей первого цвета и оставляем только ее соседей. Если можем повторять операцию бесконечное количество раз, все ок. Иначе в какой-то момент получим первый случай.

41 Примеры использования теоремы Рамсея

41.1 Теорема Эрдеша-Секереша

Теорема: $\exists k$, что из k точек на плоскости, ни какие 3 не лежат на одной прямой, можно найти выпуклый n-угольник.

Доказательство: $k = R_2(3, n, n)$

$$\chi(A, B, C) = \begin{cases} 1, & \text{если в треугольнике ABC лежит нечетное число точек} \\ 0, & \text{иначе} \end{cases}$$

$\chi(A, B, C) = \chi(B, D, C) + \chi(A, D, C) + \chi(A, B, D) + 1$

Значит можем выбрать n точек, что в любом треугольник не лежат точки из подмножества.

41.2 Раскраска натуральных чисел

Раскраска натуральных чисел: $\forall r \exists k$: $\forall$ раскраски [k] в r цветов $\exists a, b, c$: покрашенные в один цвет и a + b = c

Доказательство: $C : [k] \to [r]$ — раскраска.

$\chi(a, b) = C(|a - b|)$

$K = R_r(2; 3, 3, 3, \ldots, 3)$

$a \leq b \leq dc(b - a) = c(d - b) = c(d - a)$

d - a = d - b + b - a

КОНЕЦ