Основы математической логики и дискретной математики
Семестр 1

Лектор: Ицыксон Дмитрий Михайлович

Автор конспекта: Ольга Черникова

Собрано 25 декабря 2014 г. в 16:30

Содержание

1 Пропозициональные формулы

1.1 Пропозициальные формулы

(Формулы вычисления высказывания)

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

Определение пропозициональная формула:

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

Ф — пропозициальная формула от n перменных.

1.3 Булева функция

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

Пропозициальная формула $\leftrightarrow$ булева функция.

1.4 Представление булевой функции в ДНФ и КНФ

Литерал - это пременная 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 - противоричива, если она ложна, при всех значениях переменной.

Ф — выполнимая формула, если она не является противоричивой. $\exists$ значение переменных, что значение формулы истино.

2.2 Выполнимость КНФ

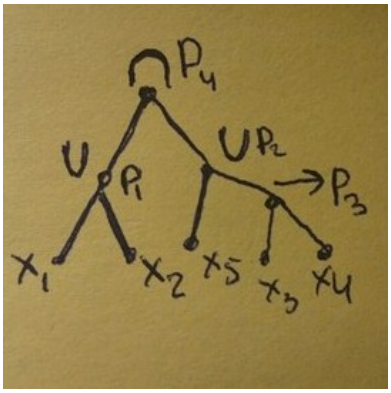
Задача SAT —- выаолнима ли формула в КНФ.

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 любой зачений 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 Ф.

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 $\blacksquare$.

Переход $n \rightarrow n+1$

x — переменная.

разобъем 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 противоричие, либо $\dfrac{x \_ \neg x}{\blacksquare}$

Замечание Если в d_1 и d_2 входит le 2 литералов, то и в резальвенту входит ≤ 2 литералов.

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

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

4 Алгоритм проверяющий выполнимость формулы 2-КНФ

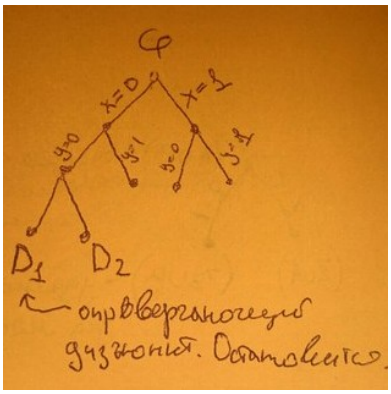
1. пока можем вывести новую резальвенту — выводим.
2. остановка:
   (a) вывели ■
   (b) больше ничего не можем вывести.

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

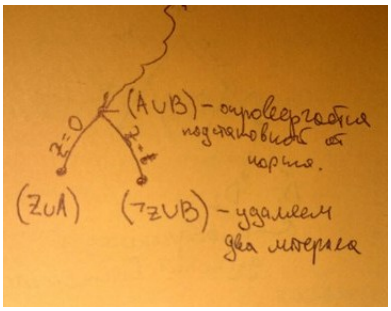
Построим дерево расщиплений.



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 — множемтво 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 — внутрение(gates).

Каждая внутренння 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 B называется полным, если для любой булевой функции существует схема над B 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 $\exists C > 0 : \forall n, k \forall f : \{0,1\}^n \to \{0,1\}^k size_{B_1}(f) \leq Csize_{B_2}(f)$

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 $g_i^{k_i}$

Получем 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 длинв $\mathcal{O}(S \log S) = 2^{CS \log S}$

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

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

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

$S = \frac{2^n}{Dn}$ 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.ы

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. Множетсво термов наименьшее множество строк, удовлетворяющие 1, 2.

Определение: Атомарная формула.

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

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

Определение: Предикатная формула.

1. атомарная формула —- предикатная формула.
2. Φ — предикатная формула, то $\neg\Phi$ — 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 M $\neq 0$

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

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

Оценка для множества пременных $\Gamma \to M$

Значение формулы в данной интерпретации при данной оценке.

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

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.

   $\Phi, \Psi, (\Phi \cup \Psi), (\Phi \cap \Psi), (\Phi \to \Psi)$

   $\forall x\Phi$, $\exists x\Phi$ — k-1 предикат

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

Предикат $P = M^k \to \{0, 1\}$ 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"$\forall y((xmody == 0) \to (y = 1) \cup (y = x)) \cap \neg(x = 1)$
7. "x - степень 2"$\forall y((xmody == 0) \cap (y -) \to y = 2)$
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. $X = \{x_1, x_2, \ldots, x_n\}$
   $a : \tilde{a}$ длинне 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

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

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

Число подмножеств [n] $= 2^n$

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

$A_n^1 = n$

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

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

$C_n^k = \binom{n}{k} = |s \subset [n]||s| = k|$ 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

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

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

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

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

13 Характеристическая функция

$\chi A \subset X$

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

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

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

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

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

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

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

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 которго $a_1 + a_2 + a_3 = a_4 + a_5 + a_6$.

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

$|\{$количество счастливых билетов$\}| = |\{$билеты с суммай 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 слогаемых у которого $a_1 \geq 10$

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

...

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 последовательностий 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 множест

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 множест —- счетно.

2. $\mathbb{N}^k$ — счетно.

   Индукция по k.

   База $\mathbb{N}^2$ объединиение 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. алгеброических 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] $\times$ [0, 1] равномощен [0, 1].

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

$\alpha \leftrightarrow a_1 a_2 a_3 \ldots$

$\beta \leftrightarrow b_1 b_2 b_3 \ldots$

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

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.

$f(A_1) = A_3 \subset A_2$

$f(A_2) = A_4 \subset A_3$

...

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

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

$c_0 = A_0/A_1$

$c_1 = A_1/A_2$

$c_2 = A_2/A_3$

...

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

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

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

Биекция:

$c_0 = c_2$

$c_1 = c_1$

$c_2 = c_4$

$c_3 = c_3$

...

$f : A \to B_1 B_1 \subset B, f$ — 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.

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

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

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

$\ldots$

$\neg x_{11}, \neg x_{22}, \neg x_{33}, \ldots$ - 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 равноможно [0, 1]

Пример: Существует неалгеброическое вещественное число.

Пример: Существует характеристическая функция не вычисляемая программой.

Количество программ счетно, количество множеств континум.

19 Введение в графы

Орентированный 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 эквиволентности.

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

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

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

Фактор граф на отношение эквиволентности — 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 эквиволентности.

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. Выкиним 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 свзяность теряется.

Доказательство: 1) $\rightarrow$ 2) доказали

2) $\rightarrow$ 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) $\rightarrow$ 1)

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

1) $\rightarrow$ 4)

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

4) $\rightarrow$ 1)

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

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

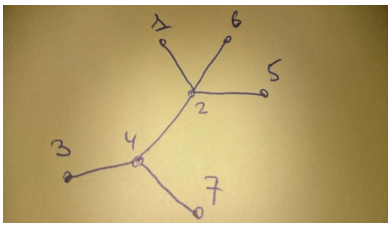
Доказательство: Если G — дерево, то |E| = |V| - 1

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 прекрепляется.

Повторяем, пока число вершин $\geq$ 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 рово одно дерево.

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

21 Эйлеров путь, цикл. Расскраски 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. Выкиним из G все ребра цикла C получлся 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 прохоящий 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, соеденим ребром.

21.3 Расскраска графов

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

Правильная расскраска 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 расскрасим отдельно.

Теперь G - связный граф $u \in V$

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

Если расскраска не одназначна, то существует цикл нечетной длины.

Пусть h неправильная расскарска, 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, нечетнй цикл не самый короткий.

22 Конечная теория вероятностей

Конечное вероятностоное 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. Вормула 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.

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

$P(\exists$ 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 $S = \{0, 1, \ldots, n-1\}$

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

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

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

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:

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

...

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

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

КОНЕЦ