

Основы математической логики и дискретной математики

Семестр 1

Лектор: Ицыксон Дмитрий Михайлович

Автор конспекта: Ольга Черникова

Собрано 25 декабря 2014 г. в 16:54

Содержание

1	Пропозициональные формулы	3
1.1	Пропозициональные формулы	3
1.2	Интерпретации	3
1.3	Булева функция	3
1.4	Представление булевой функции в ДНФ и КНФ	4
1.5	Эквивалентные формулы	4
2	Выполнимость формулы	5
2.1	Тавтологии, противоречия, выполнимые формулы	5
2.2	Выполнимость КНФ	5
3	Резолюционное исчисление	6
4	Алгоритм проверяющий выполнимость формулы 2-КНФ	8
5	Построение резолюционного доказательства по дереву расщепления	8
6	Схемы из функциональных элементов	9
6.1	Ориентированный граф без циклов и топологическая сортировка.	9
6.2	Схемы	9
6.3	Эквивалентность различных базисов	10
7	Схема умножения	10
7.1	Схема для сложения	10
7.2	Схема умножения	11
8	Существование булевой функции, которая не вычисляется схемой размера $\frac{2^n}{Cn}$	11
9	Предикатные формулы	12
9.1	Арифметика	13
10	Кодирование конечных множеств в арифметике	14

11 Доказательство непрерывности методом автоморфизмов	15
12 Конечные множества	16
13 Характеристическая функция	16
13.1 Формула включений-исключений	17
14 Количество счастливых билетов	17
15 Равномощные множества	17
15.1 счетные множества	17
16 Бесконечное множество	18
16.1 Примеры счетных множеств	18
16.2 Объединение бесконечного и счетного множества	19
16.3 Равномощность $[0, 1]$ и множество бесконечных последовательностей из 0 и 1	19
16.4 Равномощность квадрата и отрезка	19
17 Теорема Кантора-Бернштейна	20
18 Теорема Кантора	20
18.1 Континум	21
19 Введение в графы	21
19.1 Компоненты связности, пути и циклы	22
19.2 Деревья	23
20 Теорема Келли	24
21 Эйлеров путь, цикл. Раскраски графов	25
21.1 Эйлеров цикл	25
21.2 Эйлеров путь	25
21.3 Раскраска графов	25
22 Конечная теория вероятностей	26
22.1 Задача о галстуках	27
23 Теорема Эрдеша-Ко-Радо	27

1 Пропозициональные формулы

1.1 Пропозициональные формулы

(Формулы вычисления высказывания)

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

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

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

1.2 Интерпретации

0 - False

1 - True

	x	y		$x \cup y$
	0	0		0
Дизъюнкция:	0	1		1
	1	0		1
	1	1		1

	x	y		$x \cap y$
	0	0		0
Конъюнкция:	0	1		0
	1	0		0
	1	1		1

	x	y		$x \rightarrow y$
	0	0		1
Импликация:	0	1		1
	1	0		0
	1	1		1

Φ — пропозициональная формула от n переменных.

1.3 Булева функция

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

Пропозициональная 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) $l_1 \wedge l_2 \wedge \dots \wedge l_n$

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

Дизъюнкт(сlouse(кюз)): $l_1 \vee l_2 \vee \dots \vee l_n$, где l_i - литерал.

Формула в конъюктивной нормальной форме(КНФ): $d_1 \wedge d_2 \wedge \dots \wedge d_k$, где d_i - дизъюнкт.

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

Доказательство: ДНФ

$x_1 \dots x_n$	
$0 \dots 0$	
\dots	1
\vdots	
\dots	1
$1 \dots 1$	

Для каждой строчки, где стоит 1 запишем соответствующий конъюнкт. $(\neg x_1 \wedge x_2 \wedge \dots \wedge x_n) \vee \dots$

$\neg x_i$ - 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

$$\neg(x \vee y) \sim \neg x \wedge \neg y$$

$$\neg(x \wedge y) \sim \neg x \vee \neg y$$

$$\neg(c_1 \vee c_2 \vee \dots \vee c_n) \sim \neg c_1 \wedge \neg c_2 \wedge \dots \wedge \neg c_n$$

$$c_1 = l_1 \wedge l_2 \wedge \dots \wedge l_k$$

$$\neg c_1 = \neg l_1 \vee \neg l_2 \vee \dots \vee \neg l_k$$

$$x \wedge (y \vee z) \sim x \wedge y \vee x \wedge z$$

$$x \rightarrow y \sim \neg x \vee y$$

Алгоритм приведение в ДНФ:

1. избавиться \rightarrow

2. перенести отрицание к переменным
3. раскрыть скобки пользуясь дистрибутивностью.

2 Выполнимость формулы

2.1 Тавтологии, противоречия, выполнимые формулы

Определение Формула - тавтология, если она истинна, 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

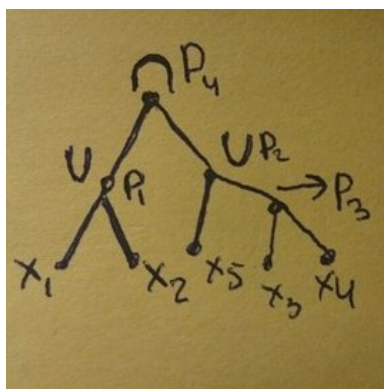
Задача SAT — выполнима ли формула в КНФ.

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

Доказательство.

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

Для формулы построим дерево разбора.



Для промежуточных вершин, заведем переменные P_1, P_2, \dots, P_k .

Формула выполняется, если выполняется система.

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

Каждое уравнение можно представить как несколько дизъюнктов.

Следствие из доказательства: В полученной формуле в КНФ в каждой дизъюнкте 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: $d_1 \cap d_2 \cap \dots \cap d_k$

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

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

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

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

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

■

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

\Leftrightarrow **Корректность** c_1, c_2, \dots, c_m — резолюционное опровержение Φ .

Пусть набор значений σ выполняет Φ .

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

c_i — дизъюнкт Φ очевидно.

$\frac{c_k _ c_l}{c_i} k, l < i$ по индукционному предположению σ выполняет c_k и $c_l \Rightarrow \sigma$ выполняет

$c_i \Rightarrow c_m = \blacksquare$ выполняет σ , противоречие.

⇒ **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 ⇒ 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 $\frac{x \quad \neg x}{\quad}$ ■

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

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

$$\frac{\frac{\frac{\frac{\frac{\frac{\neg x \cup y}{\quad} \quad (x \cup z)}{\quad} \quad (\neg y \cup z)}{\quad} \quad (\neg z \cup y)}{\quad} \quad (x \cup z)}{\quad} \quad (\neg x \cup \neg z)}{\quad} \quad z \quad (\neg z \cup y)}{\quad} \quad y \quad (\neg y \cup x)}{\quad} \quad x \quad (\neg x \cup \neg z)}{\quad} \quad \neg z \quad z$$

■

4 Алгоритм проверяющий выполнимость формулы 2-КНФ

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

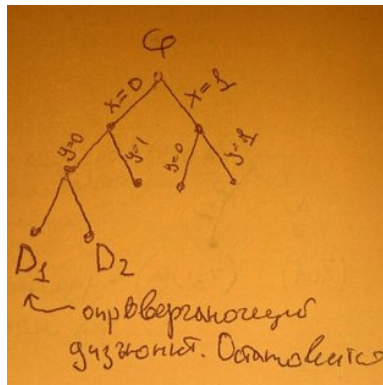
Время работы — $O(n^2)$

Количество дизъюнктов:

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

5 Построение резолюционного доказательства по дереву расщепления

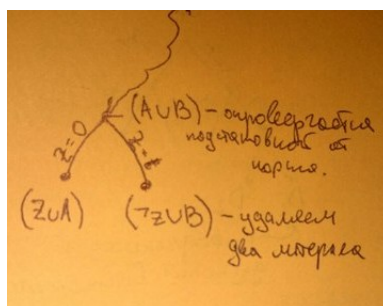
Построим дерево расщепление.



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

Заполняем все дерево. Если в каком-то листе ничего не написано, значит формула выполняется.

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 $\exists h : V \rightarrow \{1, 2, \dots, |V|\}$

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 сортировку для G' .

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

6.2 Схемы

$$B = \{f_1^{(k_1)}, f_2^{(k_2)}, \dots, f_l^{(k_l)}\}$$
$$f_i^{(k_i)} : \{0, 1\}^{k_i} \rightarrow \{0, 1\}$$

Схема под базисом B :

DAG

Вершины, в которые ничего не входит, называются входами x_1, x_2, \dots, 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 $\{0, 1\}^n \rightarrow \{0, 1\}^m$

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.

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

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

6.3 Эквивалентность различных базисов

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

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

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

$g_i^{k_i}$ 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

$$P_n, \dots, P_1$$

$$\dots, x_{n-1}, x_{n-2}, \dots, x_0$$

$$\dots, y_{n-1}, y_{n-2}, \dots, y_0$$

$$P_1 = x_0 \cap y_0$$

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

...

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.

$$x = a * 2^{\frac{n}{2}} + b$$

$$y = c * 2^{\frac{n}{2}} + d$$

$$xy = ac2^n + (ad + bc)2^{\frac{n}{2}} + bd$$

$$S(n) = 4S(\frac{n}{2}) + cn$$

$$S(n) = \mathcal{O}(n^2)$$

$$(a + b)(c + d) = ac + ad + bc + bd$$

$$S(n) = 3S(\frac{n}{2}) + cn$$

$$S(n) = n^{\frac{2}{3}}$$

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

Теорема: $f : \{0, 1\}^n \rightarrow \{0, 1\}$

B - полный базис.

Тогда $size_B(f) = \mathcal{O}(2^n)$

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

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

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

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 $D \forall n$

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

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

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

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

9 Предикатные формулы

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

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

k -ичная функция $f : M^k \rightarrow M$

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

$f_i^{(k_i)}$ — k -местная функция.

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

Пример: $\mathcal{P} = \{=(2)\}$

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

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

Определение: Терм

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

Определение: Атомарная формула.

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

атомарная формула — $p^{(k)}(t_1, t_2, \dots, t_k)$

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 $(\Phi \cup \Psi), (\Phi \cap \Psi), (\Phi \rightarrow \Psi)$
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 $M \neq \emptyset$

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

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

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. $f^{(k)}(t_1, \dots, t_k)$ — 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 M .

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

$$\mathcal{P} = \{=\}$$

$$\mathcal{F} = \{+, *\}$$

$$N\{0, 1, 2, \dots\}$$

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. " $x = 179$ " $\exists y(x = y + y + \dots + y \cap y = 1)$

5. " $x \bmod y = 0$ " $\exists z(zy = x)$

6. "x - простое" $\forall y((x \text{ mod } y == 0) \rightarrow (y = 1) \cup (y = x)) \cap \neg(x = 1)$

7. "x - степень 2" $\forall y((x \text{ mod } y == 0) \cap (y -) \rightarrow y = 2)$

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

\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 $\forall c ((c - \text{ степень } 2) \rightarrow (x + 1 \leq c) \leftrightarrow (y + 1 \leq c))$

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

$\exists t ((t - \text{ c } \text{ s } \text{ n } \text{ j } \text{ b } \text{ n } \text{ b } \text{ p } \text{ y } \text{ e } \text{ k } \text{ t } \text{ q}) \cap (|\tilde{t}| = |\tilde{y}|) \cap z = (x + 1)(t + 1) + (y - t) - 1)$

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

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. $\forall \tilde{x} \in \mathbb{N} \tilde{x} - \exists a, b \in \mathbb{N} \tilde{x} = S_{a,b}$

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

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

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

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

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

x - степень 6

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

$x = 6^n$

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

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

$x = 6^n$

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

11 Доказательство непрерывности методом автоморфизмов

$\mathbb{Z}, =, +$ невыразимо $x < y$.

$P(x, y)$

↓

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

Определение I - интерпретация с носителем M.

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

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

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

Доказательство 1. Термы задают устойчивые относительно α функции.

2. Атомарные формулы задают устойчивые предикаты.

3. $\neg\Phi$

$\Phi_1 \cup \Phi_2$

$\Phi_1 \cap \Phi_2$

$\Phi_1 \rightarrow \Phi_2$

4. $\forall x\Phi(x)$

$\exists x\Phi(x)$

$P(x, y_1, y_2, \dots)$

$P(\alpha(x), y_1, \dots)$ — 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

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

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

$$\text{Число подмножеств } [n] = 2^n$$

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

$$A_n^1 = n$$

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

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

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

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

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

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

Треугольник Паскаля

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

Бином Ньютона

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

$$\text{База } a+b = aC_1^0 + bC_1^1$$

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

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

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

13 Характеристическая функция

$$\chi_A \subset X$$

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

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

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

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

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

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

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

13.1 Формула включений-исключений

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

14 Количество счастливых билетов

Счастливым билетом, у которого $a_1 + a_2 + a_3 = a_4 + a_5 + a_6$.

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

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

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

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 $a_2 \geq 10$

...

15 Равномощные множества

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

1. равномощность двух отрезков.

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

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

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

$$S \subset \mathbb{N}$$

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

15.1 счетные множества

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

$$\mathbb{N} \xrightarrow{f} S = \{f(1), f(2), f(3), \dots\}$$

Свойства счетных множеств: 1. Любое подмножество счетного множества конечно, либо счетно.

A - счетно.

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

$g(k)$ = первый элемент в последовательности A после $g(k-1)$

2. Объединение конечного или счетного числа конечных множеств конечно или счетно.

$$A_1 f_1(1) f_1(2) f_1(3) f_1(4) \dots$$

$$A_2 f_2(1) f_2(2) f_2(3) f_2(4) \dots$$

$$A_3 f_3(1) f_3(2) f_3(3) f_3(4) \dots$$

$$A_4 f_4(1) f_4(2) f_4(3) f_4(4) \dots$$

...

$$f_1(1) f_1(2) f_2(1) f_1(3) f_2(2) f_3(1) \dots$$

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

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

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

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

...

Объединение счетного числа счетных множеств — счетно.

2. \mathbb{N}^k — счетно.

Индукция по k .

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

Переход $k \rightarrow k + 1$

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

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

$$x \in \mathbb{N}$$

Оба множества счетны. Можем занумеровать 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.

⇒ 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

$$B' \cap A = \emptyset$$

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

A — бесконечное ⇒ 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: $(\alpha, \beta) \in [0, 1] \times [0, 1]$

$$\alpha \leftrightarrow a_1 a_2 a_3 \dots$$

$$\beta \leftrightarrow b_1 b_2 b_3 \dots$$

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

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: $f : A_0 \rightarrow A_2$ — биекция.

$$f(A_1) = A_3 \subset A_2$$

$$f(A_2) = A_4 \subset A_3$$

...

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

$$A_0 \supset A_1 \supset A_2 \supset A_3 \dots$$

$$c_0 = A_0/A_1$$

$$c_1 = A_1/A_2$$

$$c_2 = A_2/A_3$$

...

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

$$A_1 = c_1 \cup c_2 \cup \dots$$

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

Биекция:

$$c_0 = c_2$$

$$c_1 = c_3$$

$$c_2 = c_4$$

$$c_3 = c_5$$

...

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

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

$$g(B_1) = A_2 \subset A_1$$

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 пронумеровали.

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

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

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

...

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

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

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

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

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

$$D \subset X$$

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

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

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

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

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

19.1 Компоненты связности, пути и циклы

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

Простой путь: — путь в котором все вершины различны.

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

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

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

Доказательство: самый короткий путь — простой.

$$u, \dots, w, \dots, w, \dots, v \rightarrow u, \dots, v$$

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 $v_1, \dots, v_n : v_n = v_1$

Длина цикла — $n - 1$

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

$(v_1, v_2), \dots, (v_{n-1}, v_n)$ — 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, \dots, u_k — простой путь максимальной длины. 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 удалении любого ребра связность 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 связан 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) \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 компонентами.

1) \rightarrow 5)

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

5) \rightarrow 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.

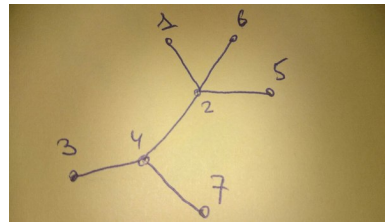
Лемма: Если G — неориентированный связный граф, то $|E| \geq |V| - 1$

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 $E' \neq 0$

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

Если раскраска не однозначна, то существует цикл нечетной длины.

Пусть h неправильная раскраска, то существует цикл нечетной длины.

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

Доказательство: Рассмотрим самый короткий нечетный цикл.

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

В центре 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)

$p : 2^\Omega \rightarrow [0, 1]$

Вероятностная мера:

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

Элементы множества Ω — элементарные события.

$A \subset \Omega$ A — событие.

$P(A)$ — вероятность события.

Свойства конечного вероятностного пространства.

1. $P(\emptyset) = 0$ $P(\Omega) + P(\emptyset) = P(\Omega)$
2. $A \subset B$, то $P(A) \leq P(B)$ $P(B) = P(A) + P(B/A) \geq 0$
3. $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$
 $P_1 = P(\{\omega_1\})$
 $P_2 = P(\{\omega_2\})$
...
 $P_n = P(\{\omega_n\})$
 $P(A) = \sum_{\omega_i \in A} P_i$
4. $P(A_1 \cup A_2 \dots A_n) \leq \sum_{i=1}^n P(A_i)$
5. Формула включений/исключений.
 $P(A_1 \cup A_2 \dots \cup A_n) = \sum_{i=1}^n P(A_i) - \sum_{i < j} P(A_i \cap A_j) + \dots$

22.1 Задача о галстуках

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

Утверждение Можно выдать галстуки так, что бы в каждой 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.

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

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

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

23 Теорема Эрдеша-Ко-Радо

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

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

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

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

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

Доказательство: $A_s = \{s, s+1, \dots, s+k-1\} \bmod n$

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.

↓

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

↓

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

КОНЕЦ