Содержание (пиши в лс че если чет добавить хочешь)

Модуль 1.

Модуль 1. Множества, отношения, алгебры.

1. Множества, подмножества. Способы определения множеств. Равенство множеств. Операции над множествами (объединение, пересечение, разность, симметрическая разность, дополнение). Методы доказательства теоретико-множественных тождеств.

Множество – свойства, которые объединяют что-то. Явной формулировки нет.

Способы определения:

A = {x: P(x)} предикат.

A = {x: x – студент МГТУ спец. ИУ7}

A = {x: x – четное число} – множество четных чисел.

a – элемент множества A. Тогда можно записать $a \in A, A \ni a$

Конечное множество: A ={a_1, …, a_n}

Два **множества** A и B считаются **равными**, если $x \in A \Leftrightarrow x \in B$ (они состоят из одних и тех же элементов)

- Порядок не важен
- Количество повторов не важно

Подмножество: $A \subseteq B \Leftrightarrow \forall x: (x \in A \Rightarrow x \in B)$ но не наоборот.

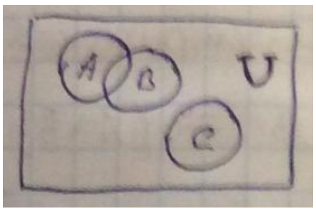
$$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

$A \subset B = (A \subseteq B) \wedge (A \neq B)$ – Строгое включение.

Пустое множество:

$\emptyset = \{x: F(x)\}\ (\forall x)(F(x) = \text{ложь})$

Для любого A: $\emptyset \subseteq A$.



Универсальное множество U:

Для любого A: $A \subseteq U$

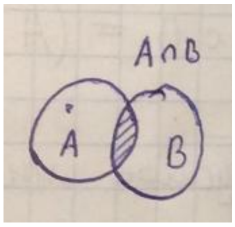
Операции над множествами:

1) Объединение:

$$A \cup B \rightleftharpoons \{x: x \in A \wedge x \in B\}$$

2) Пересечение:

$A \cap B \rightleftharpoons \{x: x \in A \vee x \in B\}$



Если $A \cap B = \emptyset$, то A и B называются непересекающимися множествами.

3) Разность:

$A \backslash B \rightleftharpoons \{x \in A \& x \notin B\}$ // без рисунка обойдетесь

4) Симетрическая разность:
$A\Delta B \rightleftharpoons (A\backslash B)\cup(B\backslash A) = \{x: (x \in A \& x \notin B) \vee (x \in B \& x \notin A)\}$
$A\Delta B = (A\cup B)(A\cap B)$
5) Дополнение: $\bar{A} \rightleftharpoons \{x: x \notin A\} = U\backslash A$
Теоретико-множественными тождествами называют равенства

$$\mathrm{A}\cup\mathrm{B} = \mathrm{B}\cup\mathrm{A}$$

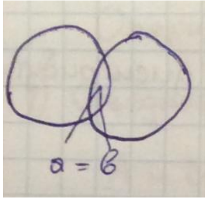
$$\mathrm{A}\cap(\mathrm{B}\cup C) = (\mathrm{A}\cap\mathrm{B})\cup(\mathrm{A}\cap\mathrm{C})$$

и т.п., верные для любых входящих в них множеств. Доказать эти равенства можно

- методом двух включений (доказать что если х принадлежит левой части, то он принадлежит и правой, и наоборот)
- методом характеристических функций (основывается на свойствах характеристических функций вида $\Phi_{\mathrm{A}}(x) = \begin{cases} 1, x \in A \\ 0, \text{иначе} \end{cases}$)
- методом эквивалентных преобразований (основывается на использовании ранее доказанных тождеств).

2. Неупорядоченная пара, упорядоченная пара, кортеж. Декартово произведение множеств.

$A, B \neq \emptyset, a \in A, b \in B$ => {a,b} – <u>неупорядоченная</u> пара на множествах А и В.



Если a = b, то {a, b} = {a, a} = {a}

{a, b} = {a', b'} ⇔(a = a') & (b = b') V (a = b') & (b = a')

{1, 2} = {2, 1}

<u>Упорядоченная пара:</u>

(a, b) = (a', b') ⇔(a = a') & (b=b')

(a, b) ≠ (b, a)

(1, 2) ≠ (2, 1)

<u>Кортеж</u>

$A_1, \ldots, A_n \neq \emptyset$ n≥2

$(a_1, \ldots, a_n)$, где $(\forall i = \overline{1,n})(a_i \in A_i)$

$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \Leftrightarrow \left(\forall i = \overline{1,n}\right)(a_i = b_i)$ Два кортежа равны, если они покомпонентно совпадают.

<u>Декартово произведение:</u>

$A_1 \text{x} \ldots \text{x} A_n \rightleftharpoons \{(a_1, \ldots, a_n): (\forall i = \overline{1,n})(a_i \in A_i)\}$ n≥0

n = 1: A

n = 0: $A^o = \{\lambda\}$ пустой кортеж

$A_1 = \ldots = A_n = A$: $A_1 \text{x} \ldots \text{x} A_n = A^n$ - n-ая декартова степень.

$A \text{x} \emptyset \rightleftharpoons \{(x, y): x \in A, y \in \emptyset\} = \emptyset$ Аналогично $\emptyset \text{x} A = \emptyset$

3. Отображения: область определения, область значений. Инъективное, сюръективное и биективное отображения. Частичное отображение.

Отображение f из множества A в множество B считается заданным, если каждому элементу $x \in A$ сопоставлен единственный элемент $y \in B$; $f: A \to B$. Элемент y называют образом элемента x при отображении f, элемент x – прообразом.

$D(f) \rightleftharpoons \{x: (x, y) \in f\}$ – область определения.

$R(f) \rightleftharpoons \{y: (x, y) \in f\}$ – область значений.

Отображение называется **частичным**, если образ определен не для каждого элемента множества A, а для некоторых элементов этого множества. f: $A \dot{-}> B$

$(x, y) \in f => y = f(x)$

Инъекция - отображение, каждый элемент из области значений которого имеет единственный прообраз, т.е. из равенства $f(x1) = f(x2)$ следует равенство x_1=x_2.

Сюрьекция: область значений отображения совпадает со всем множеством B (сюръективное отображением ИЗ A в B называют также отображением A НА B).

$(\forall y \in B)(\exists x \in A)\big(y = f(x)\big)$ // B – область значений.

2. Если отображение инъективно и сюрьективно, то называется **биекция.** т.е. каждому элементу множества A отвечает единственный элемент множества B и наоборот.

биекция = инъекция & сюрьекция.

4. Соответствия. График и граф соответствия, область определения, область значения. Сечение соответствия. Сечение соответствия по множеству. Функциональность соответствия по компоненте. Бинарные и n-арные отношения. Связь между отношениями, соответствиями и отображениями.

n-арным отношением на множествах $A_1, \dots, A_n$ называют произвольное подмножество ρ декартова произведения $A_1 \times \dots \times A_n$: $\rho \subseteq A_1 \text{x} \dots \text{x} A_n$

при n = 2 – бинарное отношение.

Если $A_1 = \dots = A_n = A$, то $\rho \subseteq A^n$ - n-арное отношение на A.

n≥1 A,B $\rho \subseteq A\text{x}B$ - соответствие из A в B.

Если каждому элементу $x \in A$ сопоставлен не один, а несколько образов $y \in B$, то говорят, что задано **соответствие** из множества A в множество B.

$D(\rho) \rightleftharpoons \{x: (x, y) \in \rho\}$ – область определения.

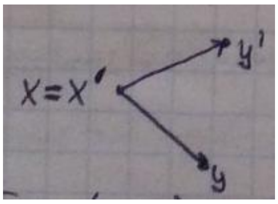
$R(\rho) \rightleftharpoons \{y: (x, y) \in \rho\}$ – область значений.

Сечение: $\rho(x_0)$ это $\{y: (x_0, y) \in \rho\}$

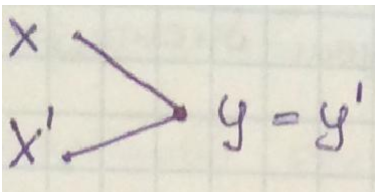
Сечение на множестве C: $C \subseteq A, \rho(C) \rightleftharpoons \{y: (x, y) \in \rho, x \in C\}$

Функциональность:

По первой компоненте: для любых (x, y) и (x’, y’) из x=x’ следует y=y’.

Не может быть 

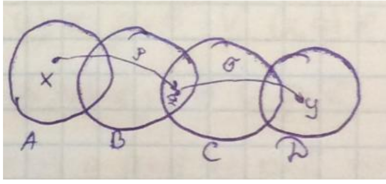
По второй компоненте: для любых (x, y) и (x’, y’) из y=y’ следует x=x’

Не может быть 

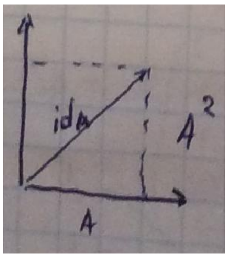
Отображением называется всюду определенное и функциональное по второй компонетне **соответствие.**

5. Композиция соответствий, обратное соответствие и их свойства (с доказательством).

Композицией соответствий $\rho \subseteq A \times B$ и $\sigma \subseteq C \times D$ называют соответствие $\rho \circ \sigma = \{ (\exists z \in B)\left((x,z) \in \rho\right) \wedge \left((z,y) \in \sigma\right) \}$.



Соответствие, **обратное** соответствию $\rho \subseteq A \times B$, есть соответствие из B в A, обозначаемое $\rho^{-1} = \{(y,x): (x,y) \in \rho\}$.



Если рассматривается бинарное отношение на A, то введем соответствие $id_A \rightleftharpoons \{(x,x): x \in A\}$ $(\forall x)(id_A(x) = x)$

<u>Основные свойства:</u>

- $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$ *ассоциативность*
- $\forall \rho$: $\rho \circ \emptyset = \emptyset \circ \rho = \emptyset$ *аннулирующее свойство*
- $\rho \circ (\sigma \cup \tau) = (\rho \circ \sigma) \cup (\rho \circ \tau)$ *дистрибутивность по объединению*
- $\forall \rho \in A^2$: $\rho \circ id_A = id_A \circ \rho = \rho$ *нейтральный элемент*
- $(\rho^{-1})^{-1} = \rho$
- $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$.

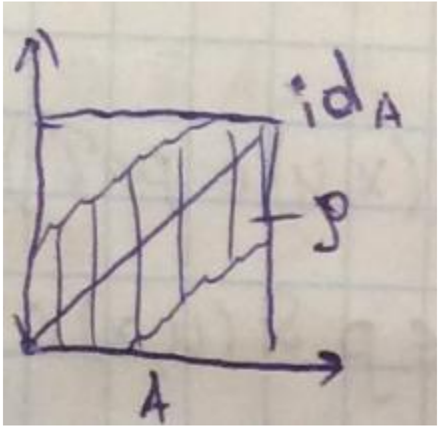
Все доказательства проводятся методом двух включений. На примере свойства 3: пусть $(x,y) \in \rho \circ (\sigma \cup \tau)$. Тогда $\exists z$: $(x,z) \in \rho$, $(z,y) \in (\sigma \cup \tau)$. Последнее означает, что $(z,y) \in \sigma$ или $(z,y) \in \tau$; следовательно для элемента z: $[(x,z) \in \rho,\ (z,y) \in \sigma]$ или $[(x,z) \in \rho,\ (z,y) \in \tau]$. Первое возможно при $(x,y) \in (\rho \circ \tau)$, второе при $(x,y) \in (\rho \circ \tau)$, $\Rightarrow$ $(x,y) \in (\rho \circ \sigma) \cup (\rho \circ \tau)$ - включение доказано. *//в обратную сторону аналогично, и аналогично же для всего остального*

6. Специальные свойства бинарных отношений на множестве (рефлексивность, иррефлексивность, симметричность, антисимметричность, транзитивность).

$\rho \subseteq A^2$ Вместо $(x, y) \in \rho$ пишем $x \; \rho \; y$

Бинарное отношение ρ на множестве А называют:

- **Рефлексивным**, если $(\forall x)(x \; \rho \; y) \Leftrightarrow id_A \subseteq \rho$

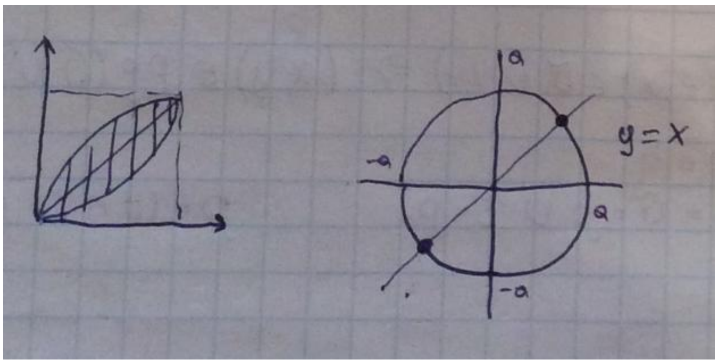


- **Иррефлексивным**, если $\forall x \in A \; (x, x) \notin \rho$

$id_A \cap \rho = \emptyset$

- **Симметричным**, если для любых$(\forall x, y)(x \; \rho \; y \;\; \Leftrightarrow y \; \rho \; x)$

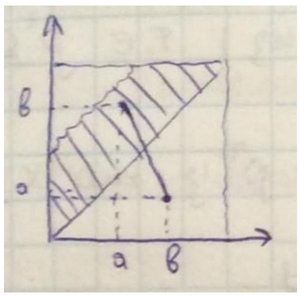
  $\rho^{-1} = \rho$



- **Антисимметричным**, если $(\forall x, y)(x\rho y \; \& \; y\rho x \;\; \Rightarrow x = y)$

  $\rho^{-1} \cap \rho \subseteq id_A$

  $(a, b) \in \rho$ при



- **Транзитивным**, если $(\forall x, y, z)(x\rho y \; \& \; y\rho z \Rightarrow x\rho z)$

7. **Классификация бинарных отношений на множестве: эквивалентность, толерантность, порядок, предпорядок, строгий порядок.**

Классификация отношений: (Тип бинарного отношения определяется набором свойств бинарных отношений)

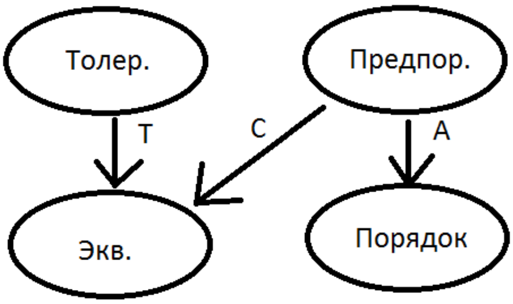
1)Эквивалентность: **р**ефлексивность, **с**имметричность, **т**ранзитивность

2) Порядок: **р**, **т**, **а**нтисимметричность

3) Толерантность: **р, с**

4) Предпорядок: **р, т**

5) Строгий порядок: иррефлексивность, **а, т** **//** в лекциях этого года не было



8. Отношение эквивалентности. Класс эквивалентности. Фактор-множество.

Бинарное отношение на некотором множестве называют эквивалентностью, если оно рефлексивно, симметрично и транзитивно.

Пусть ρ − эквивалентность на множестве А, и $x \in A$. Классом эквивалентности по отношению ρ называется множество элементов $\{y\colon y \in A,\ y\ \rho\ x\}$ (эквивалентных х); класс эквивалентности обозначается $[x]_\rho$.

Теорема: классы эквивалентности попарно не пересекаются.

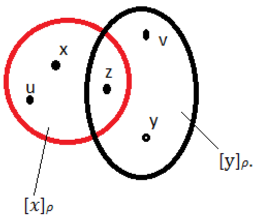
Доказательство:

$[x]_\rho \neq [y]_\rho$, но $[x]_\rho \cap [y]_\rho \neq \emptyset$.

$(\exists u)(u \rho x \ \&\ \rceil(u \rho y)) \vee (\exists u)\ (v \rho y \ \&\ \rceil(v \rho x))$

$(\exists z)(z \rho x \ \&\ z \rho y)$

$u \rho x,\ z \rho x,\ z \rho y \Rightarrow u \rho x,\ x \rho z,\ z \rho y \Rightarrow u \rho y$ - противоречие



Фактор-множеством множества А по отношению ρ (обозначается A/ρ) называют множество всех классов эквивалентности по данному отношению на данном множестве. $A/\rho \Leftrightarrow \{[x]_\rho\colon x \in A\}$

9. Отношения предпорядка и порядка. Наибольший, максимальные, наименьший и минимальные элементы. Точная нижняя и верхняя грани множества.

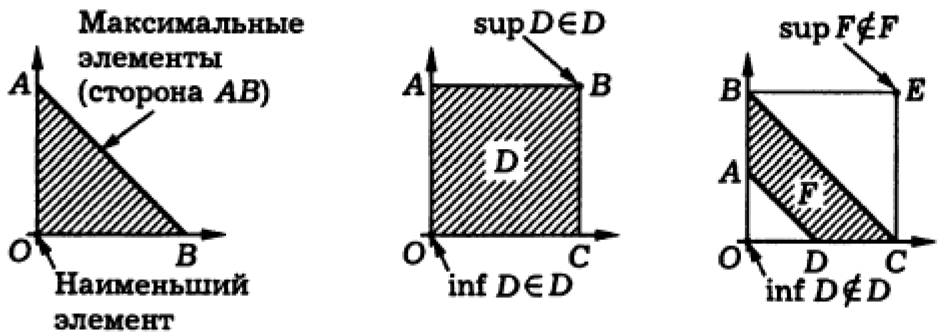
• Бинарное отношение на некотором множестве называют **порядком**, если оно рефлексивно, антисимметрично и транзитивно; **предпорядком**,
если оно только рефлексивно и транзитивно.

• Упорядоченным множеством называют множество М вместе с заданным на нем отношением порядка ≤; элементы x и y упорядоченного множества $(M, \le)$ называют сравнимыми, если $x \le y$ или $y \le x$, и несравнимыми в противном случае.

Пусть $(A, \le)$ − упорядоченное множество. Элемент $a \in A$ называют:

1) **наибольшим** элементом множества A, если $\forall x \in A\ x \le a$;
2) **максимальным** элементом множества A, если $\forall x \in A\ x \le a$ или x и a не сравнимы
3) **наименьшим**, если $\forall x \in A\ a \le x$;
4) **минимальным**, если $\forall x \in A\ a \le x$ или a и x не сравнимы.

• Пусть также $B \subseteq A$. Элемент $a \in A$ называется верхней (нижней) гранью множества B, если для всех элементов $x \in B$
$x \le a$ (или соответственно $(a \le x)$). **Точной верхней** (**точной нижней**) гранью B называют наименьший элемент множества всех верхних граней (соответственно наибольший элемент множества всех нижних граней); обозначается sup B (inf B)



Примечание: в отличие от наибольшего и наименьшего элементов множества B элементы sup(B) и inf(B) не обязательно должны принадлежать множеству B.(См. пример выше)

10. Точная верхняя грань последовательности. Индуктивное упорядоченное множество. Теорема о неподвижной точке (с доказательством). Пример вычисления неподвижной точки.

Последовательность $\{x_{\text{i}}\}_{i\in N}$ элементов упорядоченного множества $\mathcal{A} = (A, \leq)$ называют <u>неубывающей</u>, если $\forall i \in \mathbb{N}\ x_i \leq x_i$+1. Элемент a упорядоченного множества $\mathcal{A}$ называют **точной верхней гранью** последовательности $\{xi\}i\in N$, если он есть
точная верхняя грань множества всех членов этой последовательности(sup).
Упорядоченное множество $\mathcal{A}$ называется **индуктивно упорядоченным**, если в нем есть наименьший элемент, а любая неубывающая последовательность элементов $\{a_n\}_{n\geq 0}$ имеет точную верхнюю грань.
Пусть $(A, \leq)$, $(B, \preccurlyeq)$ − индуктивные упорядоченные множества. Отображение $f\colon A \to B$ называется <u>непрерывным</u>, если справедливо равенство $f(\sup a_n) = \sup f(a_n)$. Элемент $a \in A$ называют **неподвижной точкой** отображения $f\colon A \to A$,
если $f(a) = a$. Элемент a называют <u>наименьшей</u> неподвижной точкой отображения, если он является наименьшим элементом множества всех неподвижных точек отображения.
Теорема: любое непрерывное отображение f индуктивно упорядоченного множества $(M, \leq)$ $f\colon M \to M$ имеет наименьшую неподвижную точку.
Доказательство: Пусть $\mathbb{O}$ – наименьший элемент **И**ндуктивно **У**порядоченного **М**ножества *M*. Построим последовательность $\{\mathbb{O}, f(\mathbb{O}), f(f(\mathbb{O})), \dots f^n(\mathbb{O}), \dots\}$,
где $f^n(x) = f(f^{n-1}(x))$.
Т.к. $\mathbb{O}$ − наименьший элемент, то $\mathbb{O} \leq f(\mathbb{O})$, т.е.
при n=0 $f^n(\mathbb{O}) \leq f^{n+1}(\mathbb{O})$.
Пусть $f^n(\mathbb{O}) \leq f^{n+1}(\mathbb{O})\ \forall n \leq k$.
$f^{k+1}(\mathbb{O}) = f(f^k(\mathbb{O})) \leq f(f^{k+1}(\mathbb{O}))$, следовательно,
$f^{k+1} \leq f^{k+2}(\mathbb{O})$, т.е. последовательность не убывает.
Обозначим $a = \sup f^n(\mathbb{O})$, $n \geq 0$.
Тогда $f(a) = f(\sup f^n(\mathbb{O})) = \sup(f^{n+1}(\mathbb{O}))\ (n \geq 0) = \sup f^n(\mathbb{O})\ (n \geq 1) = a$.
Таким образом, f(a)=a, т.е. a –неподвижная точка.
Пусть теперь f(b)=b.

$\mathbb{O} \le b, \Longrightarrow f(\mathbb{O}) \le f(b) = b$, $f(f(\mathbb{O})) \le f(f(b)) = b$, … . $(\forall n \ge 0)$ $(f^n(\mathbb{O}) \le b)$ – значит b является верхней гранью последовательности $\{f^n (\mathbb{O})\}n$≥0. Однако a – <u>ТОЧНАЯ</u> верхняя грань этой последовательности, поэтому $a \le b$.

<u>Пример</u>: рассмотрим уравнение $f(x)$ =1/2x +1/4 на ИУМ A = [0; 1] с естественным числовым порядком. Для данного множества наименьшим элементом является 0. Последовательно вычисляя f^0 (0) = 0, f(0) =1/4, $f(f(0))$ =1/2∗1/4+1/4=3/8, f^3(0) =7/16, …, получаем последовательность приближений к наименьшей неподвижной точке.

f^n (0) =$(2^{n-1})/(2^{n+1})$, $\lim_{n\to+\infty} f^n$ (0) =1/2.

Следовательно, наименьшая неподвижная точка отображения f, определяемого правой частью уравнения, равна ½.

11. **Операции на множестве. Понятие алгебраической структуры. Свойства операций (ассоциативность, коммутативность, идемпотентность). Нуль и нейтральный элемент (единица) относительно операции. Примеры. Универсальная алгебра, носитель, сигнатура. Примеры. Однотипные алгебры.**

// Понятия алгебраической структуры в учебнике и в лекциях нет явно сформулированного.

• n-арной операцией на множестве A называется любое отображение ω: $A^n \to A$; n-арная операция ω каждому кортежу (a_1,…,a_n)∈A^n

однозначно сопоставляет элемент $b \in A$. Рассмотрим бинарную операцию (n=2) на множестве A, обозначив её *. Эту операцию называют:
1) ассоциативной, если $(x * y) * z = x * (y * z)$;
2) коммутативной, если $x * y = y * x$;
3) идемпотентной, если $x * x = x$,
$\forall x, y, z \in A$.
• Элемент 0 множества A называют **левым** (**правым**) **нулем** относительно операции •, если 0 • x=0 (x • 0=0) $\forall x \in A$. Если левый и правый нуль существуют, то они совпадают; в этом случае говорят просто о нуле относительно операции.
Элемент 1 множества A называют **левым** (**правым**) **нейтральным** элементом относительно •, если 1 • x=x (x • 1=x). Если существуют левый и правый нейтральный элемент, то они также совпадают; элемент 1 называют просто нейтральным элементом.
Примеры: На множестве целых чисел нулем является число 0, а нейтральным элементом – число 1; на множестве квадратных матриц – нулевая и единичная матрица соответственно.
• **Универсальная алгебра** считается заданной, если задано некоторое множество A (носитель алгебры) и некоторое множество операций Ω на A (сигнатура алгебры). Если носитель алгебры – конечное множество, то алгебру называют конечной. Две алгебры ($A1$, Ω1) и ($A2$, Ω2) называются **однотипными**, если существует

такая биекция Ω1 на Ω2, при которой n-арная операция из Ω1 для любого n переходит в n-арную из Ω2.

• <u>Примеры</u>: $(2M, \{\cup, \cap, \setminus, \Delta, \bar{\ }, \emptyset, M\})$: носитель – множество всех подмножеств произвольно фиксированного множествм M, сигнатура состоит из объединения, пересечения, разности, симметрической разности и дополнения; пустое множество и множество M определяют нульарные операции.

Алгебры $\mathcal{A}1 = (2M, \cup, \cap, \emptyset, M)$ и $\mathcal{A}2 = (\mathbb{R}, +, \bullet, 0, 1)$ являются однотипными; биекцию между их сигнатурами, сохраняющую арность операций, можно определить как

$\cup \rightarrow +$, $\cap \rightarrow *$, $\emptyset \rightarrow 0$, $M \rightarrow 1$.

12. Группоиды, полугруппы, моноиды. Единственность нейтрального элемента. Обратный элемент. Группа. Единственность обратного элемента в группе.

Группоид – это алгебра с одной бинарной операцией $\boldsymbol{\sigma} = (\boldsymbol{G}, *)$
Примеры: $(\mathbb{N}, +), (2^M, \Delta), (2^M, \backslash), (\mathbb{V}, x)$
$(a * b) * c = a * (b * c)$ – ассоциативность. Если операция группоида ассоциативна, то он называется **полугруппой.**
$\mathcal{E}$ - называется **нейтральным элементом**, если
$\mathcal{E} \in G \;\; (\forall a \in G)(a * \mathcal{E} = \mathcal{E} * a = a)$

Теорема. (О единстве нейтрального элемента):

Если группоид имеет нейтральный элемент, то он единственный.

Доказательство:

Пусть есть группоид у которого 2 нейтральных элемента: $\mathcal{E}, \mathcal{E}'$ тогда:
$\mathcal{E} * \mathcal{E}' = \mathcal{E}'$ т.к. $\mathcal{E}$ - нейтральный элемент.
$\mathcal{E} * \mathcal{E}' = \mathcal{E}$ т.к. $\mathcal{E}'$ - нейтральный элемент, следовательно $\mathcal{E} = \mathcal{E}'$.

Моноид – полугруппа с нейтральным элементом
$\mathcal{M} = (M, *, \mathcal{E})$
Примеры: $(\mathbb{N}_0, +, 0), (\mathbb{N}_0, \cdot, 0), (2^M, \cup, \emptyset), (2^M, \cap, M), (2^{M\times N}, 0, id_M)$
Элемент a называется **обратным** если a' - обратный к a.
$a \in M$ называется обратным, если $(\exists a' \in M)(a * a' = a' * a = \mathcal{E})$

Теорема. (О единстве обратного элемента):

Если элемент моноида обратим, то обратный к нему – единственный.

Доказательство:

a, a', a'' – обратный к a

$$a'' = a'' * \mathcal{E} = a'' * (a * a') \xLongleftrightarrow{\text{ассоциативность}} \underbrace{(a'' * a)}_{\mathcal{E}} * a' = \mathcal{E} * a' = a'$$

Моноид, каждый элемент которого обратим называется **группой**.
Например множество невырожденных матриц.

13. Циклическая полугруппа (группа). Образующий элемент. Примеры конечных и бесконечных циклических полугрупп и групп. Порядок конечной группы. Порядок элемента. Теорема о равенстве порядка образующего элемента конечной циклической группы порядку группы.

Группоид $(\boldsymbol{G},*)$ называют **группой** если операция ассоциативна, существует нейтральный элемент - ε относительно умножения, для каждого $x \in G$ существует обратный элемент x', что $x * x' = x' * x = \varepsilon$.

Группа: $\mathcal{G} = (G,\cdot, \ ^{-1}, 1)$

Полугруппу $(\mathrm{A},\cdot)$ называют **циклической**, если существует такой элемент a, что любой элемент x полугруппы является некоторой (целой) степенью элемента a. Элемент a называют **образующим элементом полугруппы(группы).**

Пример: $(\mathbb{Z}, +, 0)$-циклическая. Образующие элементы: -1 и 1.

Тогда $0 \cdot 1 = 0$, $n \cdot 1 = \underbrace{1 + \ldots + 1}_{n \text{ раз}} = n$ $(n > 0)$ и $(-1) \cdot 1 = -1$,

$$(-n) \cdot 1 = n \cdot (-1) = \underbrace{(-1) + \ldots + (-1)}_{n \text{ раз}} = -n \ (n > 0).$$

Конечная алгебра (группа) – это алгебра, носитель которой – конечное множество.

Порядок конечной группы – количество элементов в этой группе.

Порядок элемента a циклической группы – это наименьшее положительное n, такое, что $a^n = 1$.

Теорема. (О равенстве порядка образующего элемента конечной циклической группы порядку группы)

> Порядок образующего элемента конечной циклической группы равен порядку самой группы.

Доказательство:

Пусть $\mathcal{G} = (G,\cdot, 1)$ – конечная циклическая группа с образующим элементом a и $n > 0$ – порядок этого элемента.

Тогда все степени $a^0 = 1, a^1 = a, \ldots, a^{n-1}$ попарно различны.

Действительно, если $a^k = a^l, 0 < l < k < n$, то $a^{k-l} = a^{k+(-l)} = a^k a^{-l} = a^l a^{-l} = a^{l-l} = 1$. Поскольку $k - l < n$, получено противоречие с выбором n как порядка элемента a (ибо найдена степень, меньшая n, при возведении в которую элемента a получается единица).

Осталось доказать, что любая степень элемента a принадлежит множеству $\{1, a, \dots, a^{n-1}\}$. Для любого целого m существуют также целые n, k, такие, что $m = kn + q$, где q – целое и $0 \le q < n$. Тогда $a^m = a^{kn+q} = a^{kn} \cdot a^q = (a^n)^k \cdot \cdot a^q = 1 \cdot a^q = a^q \in \{1, a, \dots, a^{n-1}\}$. Поскольку каждый элемент группы $\mathcal{G}$ есть некоторая степень элемента a, то $G = \{1, a, \dots, a^{n-1}\}$ и порядок группы равен n.

Из доказанной теоремы следует, что в бесконечной циклической группе не существует такого n>0, что для образующего элемента a группы выполняется равенство $a^n = 1$.

14. Кольца. Аддитивная группа и мультипликативный моноид кольца. Коммутативное кольцо. Кольца вычетов. Теорема о тождествах кольца (аннулирующем свойстве нуля, свойстве обратного по сложению при умножении, дистрибутивности вычитания относительно умножения).

Кольцом называют алгебру вида (R, +,$*$,0,1), сигнатура которой состоит из двух бинарных (сложение кольца и умножение кольца) и двух нульарных операций, причем для любых a, b, $c \in R$ выполняются равенства, называемые аксиомами кольца:

1) $a + (b + c) = (a + b) + c$
2) $a + b = b + a$
3) $a + 0 = a$
4) $\forall a \in R\ \exists(-a)$: $a + (-a) = 0$
5) $a * (b * c) = (a * b) * c$
6) $a * 1 = 1 * a = 1$
7) $a * (b + c) = a * b + a * c$; $(b + c) * a = b * a + c * a$

• Аксиомы 1-4 означают, что алгебра (R,+,0) является абелевой (коммутативной) группой, называемой **аддитивной группой** кольца. Аксиомы
5 и 6 показывают, что алгебра (R,*,1) является моноидом, называемым **мультипликативным моноидом** кольца.

• Кольцо называется **коммутативным**, если его операция умножения коммутативна.

• **Кольцо** (коммутативное) **вычетов** по модулю k – алгебра вида Zk = ({0,1,…, k − 1},$\oplus k$,$\odot k$, 0, 1) с операциями сложения по модулю к и умножения по модулю к.

Теорема. (О тождествах кольца)

В любом кольце выполняются следующие тождества:

1) $0 * a = a * 0 = 0$
2) $(-a) * b = -(a * b) = a * (-b)$
3) $(a - b) * c = a * c - b * c$; $c * (a - b) = c * a - c * b$

Доказательство:

- Для $0 * a = a * 0 = 0$

$$a + 0 * a = 1 * a + 0 * a = (1 + 0) * a = 1 * a = a$$

- Для $(-a) * b = -(a * b) = a * (-b)$ с учетом доказанного выше
  $$a * (-b) + a * b = a * \left((-b) + b\right) = a * 0$$
  $$= 0 \text{ откуда } a * (-b) = -(a * b)$$
- Для $(a - b) * c = a * c - b * c$ с учетом доказанного выше
  $$a * (b - a) = a * \left(b + (-c)\right) = a * b + a * (-c)$$
  $$= a * b - a * c$$

15. Тела и поля. Примеры полей. Область целостности. Теорема о конечной области целостности (с доказательством). Поля вычетов. Решение систем линейных уравнений в поле вычетов.

Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**; коммутативное тело – **полем**. В поле, помимо аксиом кольца, выполняются еще два тождества:

1) $\forall a \neq 0 \in R$, $\exists a{-}1$: $a * a{-}1 = 1$;
2) $a * b = b * a$.

Примеры: поля рациональных чисел ($\mathbb{Q}$, +,$*$,0,1), действительных чисел ($\mathbb{R}$, +,$*$,0,1).

Ненулевые элементы a,b кольца R называют **делителями нуля**, если $a * b = 0$ или $b * a = 0$. **Областью целостности** называется коммутативное кольцо без делителей нуля (к примеру, кольцо целых чисел).

Теорема. (О конечной области целостности)

Конечная область целостности является полем.

Доказательство:

Поле – кольцо, умножение которого коммутативно, а каждый ненулевой элемент имеет обратный элемент относительно умножения. Так как по определению область целости является коммутативным кольцом, то достаточно доказать, что для конечной области целостности любой ненулевой элемент обратим, т.е. для всякого $a \neq 0$ существует единственный x, такой, что $a \cdot x = 1$

Фиксируем произвольный $a \neq 0$ и определим отображение f_a множества всех ненулевых элементов в себя:$f_a = a \cdot x$. Это отображение будет инъекцией – из равенства $a * x = a * y$ следует $a * (x - y) = 0$; ввиду отсутствия делителей нуля получаем что $x - y = 0$; $x = y$. Так как носитель по условию теоремы конечен, то f_a будет также и биекцией. Поэтому для любого y существует единственный элемент x, такой, что $y = a * x$. При $y = 1$ равенство $a * x = 1$ выполняется для некоторого однозначно определенного $x = a^{-1}$.

Кольцо вычетов по модулю p $\mathbb{Z}p$ является полем тогда и только тогда, когда p – простое число.
Рассмотрим пример решения СЛАУ в поле $\mathbb{Z}5$; при записи уравнений будем опускать знак $\odot 5$ умножения, если это не приводит к путанице.

$$\begin{cases} x_1 \oplus_5 2x_2 \oplus_5 3x_3 = 1, \\ 2x_1 \oplus_5 2x_2 \oplus_5 4x_3 = 3, \\ 4x_1 \oplus_5 3x_2 \oplus_5 \ \ x_3 = 0, \end{cases}$$

Домножим первую строку на 3, прибавим ее к 2 строке:

$$(3 \oplus_5 2)x_1 \oplus_5 (3 \odot_5 2 \oplus_5 2)x_2 \oplus_5 (3 \odot_5 3 \oplus_5 4)x_3 = 3 \oplus_5 3.$$

В итоге имеем.

$$0 \odot_5 x_1 \oplus_5 3x_2 \oplus_5 3x_3 = 1.$$

Прибавив к третьей строке первую, получим

$$(1 \oplus_5 4)x_1 \oplus_5 (2 \oplus_5 3)x_2 \oplus_5 (3 \oplus_5 1)x_3 = 1,$$

откуда **4x3 = 1.**
Система привелась к виду

$$\begin{cases} x_1 \oplus_5 2x_2 \oplus_5 3x_3 = 1, \\ \qquad\quad 3x_2 \oplus_5 3x_3 = 1, \\ \qquad\qquad\qquad 4x_3 = 1. \end{cases}$$

Из последнего уравнения находим
x3 =4−1 ∗ 1 = 4 ∗ 1 = 4.
Подставив **x3 = 4** во второе уравнение будем иметь

$$3x_2 \oplus_5 3 \odot_5 4 = 1,$$

т.е. **3x2 = 1 + (−2) = −1 = 4.**
Отсюда **x2 = 3−1 ∗ 4 = 2 ∗ 4 = 3**.
Из первого и второго уравнения после подстановки найденных значений переменных получим
x1 + 2 ∗ 3 + 3 ∗ 4 = 1,
x1 + 1 + 2 = 1,
x1 = −2 = 3.

16. Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы. Подкольца и подполя.

Пусть $\mathcal{G} = (G,*)$ - произвольный группоид, $H \subseteq G$ – некоторое подмножество G. Множество H замкнуто относительно относительно операции *, если $\forall x, y \in H\ (x * y \in H)$. Подмножество H с операцией * будет группоидом $\mathcal{H} = (H,*)$, называемым ***подгруппоидом*** группоида $\mathcal{G}$. Если группоид $\mathcal{G}$ является полугруппой, то всякий его подгруппоид также является полугруппой, называемой ***подполугруппой*** полугруппы $\mathcal{G}$.

Пусть $\mathcal{M} = (M,*\ ,1)$ − моноид. Если подмножество $P \subseteq M$ замкнуто относительно операции * и содержит единицу этого моноида, то $\mathcal{P} = (P,*\ ,1)$ также является моноидом – ***подмоноидом*** моноида $\mathcal{M}$.

Пусть $\mathcal{G} = (G,*,-1\ ,\ 1)$ − группа, $H \subseteq G$ подмножество замкнуто относительно операции *, содержит единицу этой группы и вместе с каждым элементом $x \in H$ содержит x^{-1} обратный к x. Тогда $\mathcal{H} = (H,*,-1\ ,\ 1)$ также есть группа – ***подгруппа*** группы $\mathcal{G}$.

Пример: Рассмотрим аддитивную полугруппу натуральных чисел вместе с нулем (ℕ0, +). Подмножество всех положительных четных чисел замкнуто относительно сложения, поэтому на нем может быть определена подполугруппа *полугруппы* (ℕ0, +). В то же время аддитивная полугруппа натуральных чисел с нулем также является моноидом с нейтральным элементов 0. Тогда построенная выше подполугруппа всех положительных не будет подмножеством *моноида* (ℕ0, +, 0), поскольку ее носитель не содержит нуля, являющегося единицей моноида.

Подгруппу группы $\mathcal{G}$, заданную на множестве всех степеней фиксированного элемента a, называют **циклической подгруппой**, порождённой элементом a.

Рассмотрим кольцо $\mathcal{R} = (R, +,*\ ,0,1)$. Если множество $Q \subseteq R$ замкнуто относительно сложения и умножения кольца, содержит нуль и единицу кольца и вместе с каждым $x \in Q$ содержит противоположный к нему (по сложению) элемент –x, то $\mathcal{Q} = (Q, +,*\ ,0,1)$ также является кольцом – **подкольцом** кольца $\mathcal{G}$.

Аналогично дается определение **подполя** какого-либо поля (добавляется условие содержания в Q обратного элемента по умножению)

17. Смежные классы подгруппы по элементу. Теорема Лагранжа.

Пусть $\mathcal{G} = (G, *, 1)$ − группа, $\mathcal{H} = (H, *, 1)$ − ее подгруппа. Левым смежным классом подгруппы $\mathcal{H}$ по элементу $a \in G$ называют множество $aH = \{y\colon\ y = a * h, h \in H\}$.; правым смежным классом – множество $Ha = \{y\colon\ y = h * a, h \in H\}$.

Теорема Лагранжа: порядок конечной группы делится на порядок любой ее подгруппы.

// я блять не знаю че тут вставить

18. Полукольцо. Идемпотентное полукольцо. Естественный порядок идемпотентного полукольца.

Полукольцом называется алгебра с двумя бинарными и двумя нульарными операциями, $(S, +, * , 0, 1)$, два призвольные элементы a,b,c которой обладают следующими свойствами:

1) $a + (b + c) = (a + b) + c$
2) $a + b = b + a$;
3) $a + 0 = a$
4) $(a * b) * c = a * (b * c)$
5) $a * 1 = 1 * a = a$
6) $a(b + c) = ab + ac$ и $(b + c)a = ba + ca$
7) $a * 0 = 0 * a = 0$.

Данные равенства называют аксиомами или основными тождествами полукольца. *//в отличие от кольца: нет свойства про –a по сложению, есть 0 по умножению*

Полукольцо называется идемпотентным, если его операция сложения идемпотентна, т.е. a+a=a.

На носителе *идемпотентного* полукольца может быть введено отношение порядка; для произвольных $x, y \in S$ положим $x \leq y$ тогда и только тогда, когда $x + y = y$. Отношение $\leq$ есть отношение порядка (рефлексивно, антисимметрично, транзитивно), называемое естественным порядком полукольца.

19. Замкнутое полукольцо. Итерация элемента. Примеры вычисления итерации в различных замкнутых полукольцах.

Полукольцо$(S, +,* ,0,1)$ называется замкнутым, если:

1) оно идемпотентно
2) любая последовательность X элементов множества S имеет точную верхнюю грань относительно естественного порядка этого полукольца
3) операция умножения полукольца сохраняет точные верхние грани последовательностей;
$\forall a \in S, \forall X = \{x_n \in S\}_{n\in\mathbb{N}} \quad a \sup X = \sup aX, \quad (\sup X)a = \sup(Xa)$.

• Итерация x^* элемента x определяется как точная верхняя грань последовательности всех степеней элемента, т.е. $x^* = \sum_{n=0}^{\infty} x^n$, где $x^0 = 1, \quad x^n = x^{n-1}x, \ n = 1,2, \dots$.

Пример: $\mathcal{B} = (\{0,1\}, +,* ,0,1)$ – идемпотентное полукольцо. $\operatorname{Sup} \mathcal{B} = 1$, если хотя бы один ее член равен 1, и =0 в противном случае. Итерация любого элемента полукольца $\mathcal{B}$ равна 1. Для 1* это очевидно, для 0* имеем $0^* = 0^0 + 0^1 + \dots + 0^K + \dots = 1 + 0 + \dots + 0 + \dots = 1$.

20. Непрерывность операции сложения в замкнутом полукольце. Теорема о наименьшем решении линейного уравнения в замкнутом полукольце.

Для любой последовательности $\{x_n\}_{n\in\mathbb{N}}$ элементов замкнутого полукольца и любого элемента a этого полукольца выполняется равенство $a + \sum x_n = \sum(a + x_n)$ – операция сложения в замкнутом полукольце непрерывна.

Теорема: Наименьшими решениями уравнений $x = ax + b$ и $x = xa + b$ в замкнутых полукольцах являются соответственно $x = a^*b$ и $x = ba^*$; a* - итерация элемента a.

21. Квадратные матрицы порядка n над идемпотентным полукольцом. Теорема о полукольце квадратных матриц. Замкнутость полукольца квадратных матриц над замкнутым полукольцом. Решение систем линейных уравнений в замкнутых полукольцах.

Рассмотрим систему линейных уравнений вида

$(*)\ \begin{cases} x_1 = a_{11}x_1 + \cdots + a_{1n}x_n + b_1 \\ \qquad\qquad \cdots \\ x_n = a_{n1}x_1 + \cdots + a_{nn}x_n + b_n \end{cases}$, где все элементы a_{ij} и b_i – элементы некоторого замкнутого полукольца. Введем в рассмотрение множество $M_{m\times n}(\mathcal{S})$ прямоугольных матриц с элементами из произвольного идемпотентного полукольца $\mathcal{S} = (S, +, \bullet, 0, 1)$. Обозначим как $\mathbb{M}_n(\mathcal{S})$ множество всех квадратных матриц порядка n, элементы которых принадлежат этому полукольцу.

- **<u>Теорема:</u>** Алгебра $M_n(S) = (\mathbb{M}_n(\mathcal{S}), +, \bullet, O, E)$ есть идемпотентное полукольцо. Если замкнуто полукольцо $\mathcal{S}$, то полукольцо $M_n(S)$ также замкнуто.

- Пусть $\mathcal{S}$ – замкнутое полукольцо, $\{A_m\}_{m\in\mathbb{N}}$ - произвольная последовательность квадратных матриц $A_m = (a_{ij}^m)$ порядка n. Рассмотрим матрицу $B = \left(\sum_{m\in N} a_{ij}^m\right)$. Каждый элемент $b_{ij} = \sum_{m\in N} a_{ij}^m$ является точной верхней гранью последовательности элементов a_{ij}^m (эти точные верхние грани существуют, поскольку a_{ij}^m – элементы замкнутого полукольца $\mathcal{S}$). Так как сложение матриц и отношение порядка в полукольце матриц определяется поэлементно, то матрица B и будет точной верхней гранью последовательности матриц A_m. Следовательно полукольцо $M_n(\mathcal{S})$ – замкнуто над полукольцом $\mathcal{S}$.

- Рассмотрим процедуру решения системы уравнений (*).

Запишем первое уравнение системы так:

$x_1 = a_{11}x_1 + (a_{12}x_2 + \cdots + a_{1n}x_n + b_1)$. Из первого уравнения системы выразим x_1 через остальные неизвестные:

$x_1 = a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1)$. Подставляя это выражение вместо x1 в остальные уравнения, получаем систему из n-1 уравнений, не содержащую x1:

$$\begin{cases} x_2 = a_{21}a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1) + a_{22}x_2 + \cdots + a_{2n}x_n + b_2 \\ x_3 = a_{31}a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1) + a_{32}x_2 + \cdots + a_{3n}x_n + b_3 \\ \ldots \\ x_n = a_{n1}a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1) + a_{n2}x_2 + \cdots + a_{nn}x_n + b_n \end{cases}.$$

Приводя подобные члены и повторяя процедуру, получаем (**) $x_i = a_i^*\gamma_i$, где выражение a_i^* не содержит неизвестных, а γ_i может содержать только неизвестные, начиная с (i+1)-го. При i=n имеем $x_n = a_n^*\gamma_n$, где оба выражения не содержат неизвестных.

Таким образом, исходная система преобразована к «треугольному» виду: правая часть уравнения не содержит неизвестных, уравнение (**) при i=n-1 в правой части содержит только неизвестное. Каждое следующее уравнение при просмотре «снизу вверх» содержит на одно неизвестное больше чем предыдущее. После этого мы последовательно вычисляем значения всех неизвестных $x_1, \ldots, x_{n-1}$, начиная с последнего.

МОДУЛЬ 2: Элементы теории графов

1. Основные понятия теории графов: неориентированные и ориентированные графы, цепи, пути, циклы, контуры. Подграфы.

Неориентированные графы:

G = (V, E), где

V – конечное множество, элементы которого называются вершинами или узлами.

E – множество неупорядоченных пар на V, т.е. подмножество множества двухэлементных подмножеств V, элементы которого называются ребрами.

Цепь: в неориентированном графе G это последовательность вершин $V_0, V_1, \ldots, V_n, \ldots$ такая, что $(V_i - V_{i+1})(\forall i)(\exists V_{i+1})$. Под конечной последовательностью понимают кортеж вершин.

Простая цепь – это цепь, все вершины которой, возможно кроме первой и последней, попарно различны и все ребра попарно различны.

Цикл – простая цепь ненулевой длины с совпадающими концами.

Ребро **e** называют инцидентным вершине V, если она является одним из его концов.

Ориентированный граф:

G = (V, E), где

V – конечное множество, элементы которого называются вершинами или узлами.

E – множество упорядоченных пар на V, т.е. подмножество множества VxV, элементы которого называются дугами.

Дугу (U, V) называют заходящей в вершину V и исходящей из вершины U.

Дугу называют инцидентной вершине V, если она заходит в V или исходит из V.

Путь в ориентированном графе G – последовательность вершин V_0, V_1, …, V_n, … такая, что(V_i – V_{i+1})($\forall$ i)($\exists$ V_{i+1})

Простой путь – путь, все вершины которого, кроме возможно первой и последней, попарно различны.

Контур – простой путь ненулевой длины, начало и конец которого совпадают.

Маршрутом в графе называется чередующаяся последовательность вершин и ребер, в которой любые два соседних элемента инцидентны: V_0, e_1, V_1, …, e_k, V_k

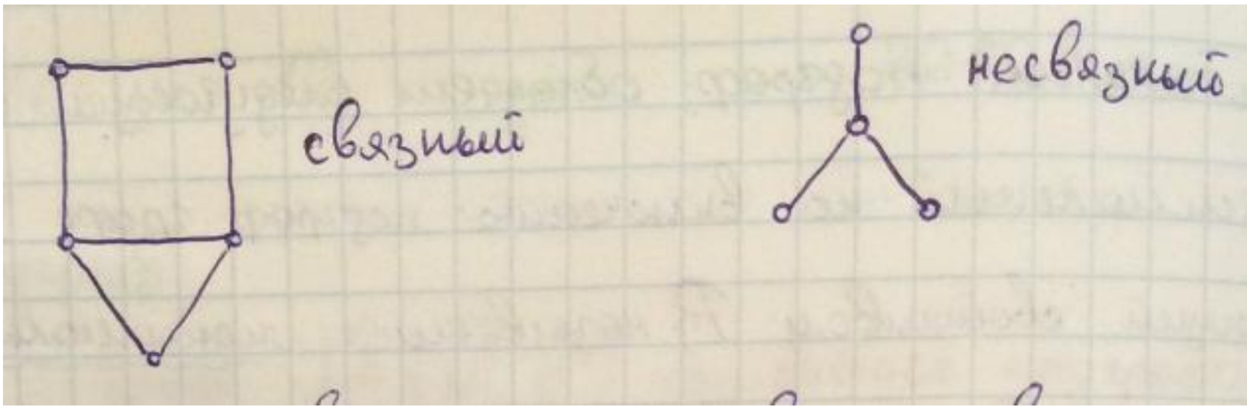
Если $V_0 = V_k$, то маршрут замкнут, иначе – открыт.

Неориентированный (ориентированный) граф $G_1 = (V_1, E_1)$ называют подграфом неориентированного (ориентированного) графа $G = (V, E)$, если $V_1 \subseteq V$, $E_1 \subseteq E$.

2. Связность неориентированного графа. Компоненты связности.

Неориентированный граф называют <u>связанным</u>, если любые две его вершины U и V соединены цепью.

<u>**Компонента связности неориентированного графа**</u> – его максимальный связанный подграф.



3. Связность, сильная и слабая связность орграфа. Компоненты связности (сильной, слабой).

Ориентированный граф называют **связанным**, если для любых двух его вершин U, V вершина V достижима из вершины U или наоборот.

$$(\forall U, V)\big((U \Rightarrow* V) \vee (V \Rightarrow* U)\big)$$

Компонента связности (сильной, слабой) ориентированного графа – его максимально связанный (сильно, слабо) подграф.

Бикомпонента ориентированного графа – это его максимально сильно связанный подграф.

Сильно связанный ориентированный граф – для любых двух вершин U и V вершина V достижима из вершины U и наоборот.

$$(\forall u, v)(u \Rightarrow* v \ \& \ v \Rightarrow* u)$$

Слабо связанный ориентированный граф – если ассоциированный с ним неориентированный граф связен.

Критерий связанности орграфа:

Орграф связан тогда и только тогда, когда в нем существует путь, проходящий через все вершины.

Теорема: если в ор. графе из u достижима v, то существует простой путь из u в v.

Следствия:

1: Если в ор. графе вершина лежит на простом замкнутом пути, то она лежит на контуре.

2: Если в неор. Графе 2 вершины соединены цепью, то существует простая цепь, соединяющая их.

3: Если в неор.графе вершина лежит на замкнутом пути, то она лежит на цикле.

4. Деревья и их классификация. Теорема о числе листьев в полном *p*-дереве.

<u>Сеть</u> – произвольный бесконтурный ориентированный граф.

<u>Вход (источник) сети</u> – вершина, имеющая 0 полустепень захода.

<u>Выход (сток) сети</u> – вершина, имеющая 0 полустепень исхода.

<u>Ориентированное дерево</u> – сеть с одним входом, в котором каждая вершина, не являющаяся входом, имеет полустепель захода 1.

<u>Вход дерева</u> – корень.

<u>Выходы дерева</u> – листья.

<u>Поддерево</u> – подграф графа исходного дерева.

Из корня в лист получаем <u>компоненту связанности</u>.

<u>Высота узла</u> h(V) – максимальная длина пути, ведущая из данного узла в лист.

<u>Высота дерева</u> h_T – высота корня.

<u>Глубина узла</u> d(V) – длина пути из корня в данную вершину.

<u>Уровень вершины</u> – $b(V) = h_T – d(V)$

<u>Дерево сбалансировано,</u> если уровни всех листьев одинаковы.

Вершина V <u>потомок</u> (подлинный потомок) вершины U если $\exists$путь из U в V (путь ненулевой длины из U в V). Тогда U – <u>предок</u> (подлинный предок) вершины V.

Если длина пути из U в V равна 1, то V – <u>сын</u>, а U – <u>отец</u>.

<u>Лист</u> – вершина, не имеющая потомков.

<u>Корень</u> – предок всех вершин.

<u>Куст</u> – дерево из корня и его сыновей.

<u>Неориентированное дерево</u> – любой связный ациклический граф.

<u>Ориентированный лес</u> – граф в котором каждая слабая компонента дерево.

<u>Неориентированный лес</u> – произвольный ациклический неор. граф.

<u>p-дерево</u> – если полустепень исхода любой вершины не превышает p.

p = 2 – бинарное дерево.

<u>Полное p-дерево</u> – если полустепень исхода любой вершины, не являющейся листом, равняется p, и уровни всех листьев одинаковы.

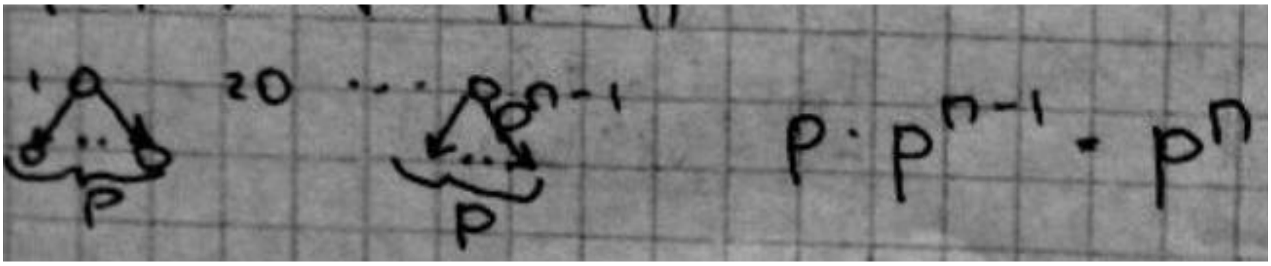
<u>Теорема</u>: *В полном p-дереве высоты h, число листьев = p^h*

<u>Док-во:</u>

$h = 0 \Rightarrow p^0=1$ – лист

$\forall h \leqslant n-1$ утверждение справедливо.

Положим h = n

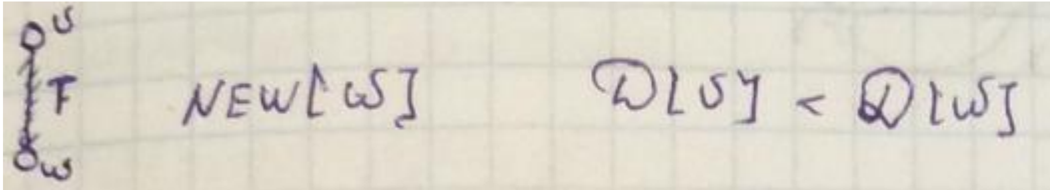


5. Поиск в глубину в неориентированном графе. Древесные и обратные ребра. Поиск фундаментальных циклов на основе поиска в глубину.

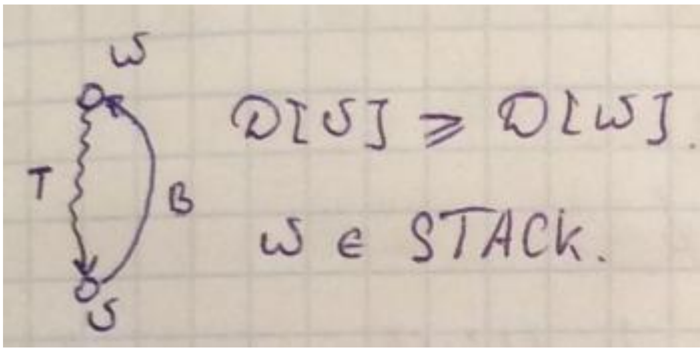
```
begin
        T, B, FC := ∅; stack := ∅;
        count := 1;
        for all  V ∈V
                NEW[V] := 1;
        for all  V ∈V
                while (∃V)(NEW[V]= 1) do
                        search_D(V);
end;
proc search_D(V)
        NEW[V] := 0;
        D[V] := count; count++;
        V -> stack;
        for all (ω ∈L[V]) do
                if (NEW[ω]) then begin
                        {V,ω}-> T;
                        search_D(ω);
                end;
                else if({V,ω} ∉ T) then
                        if ({V, ω}∉ B) then begin
                                {V, ω} -> B
                                Read(V..ω) -> FC;
                        end;
           stack -> V;
        end;
```

Лес, который строится методом поиска в глубину называется **глубинный остовной лес.**

Древесные дуги (T) – идет от отца к сыну через глубинный остовный лес.

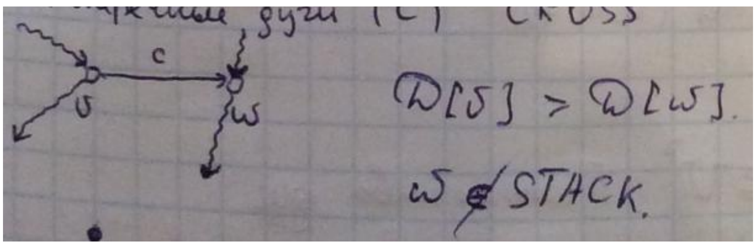


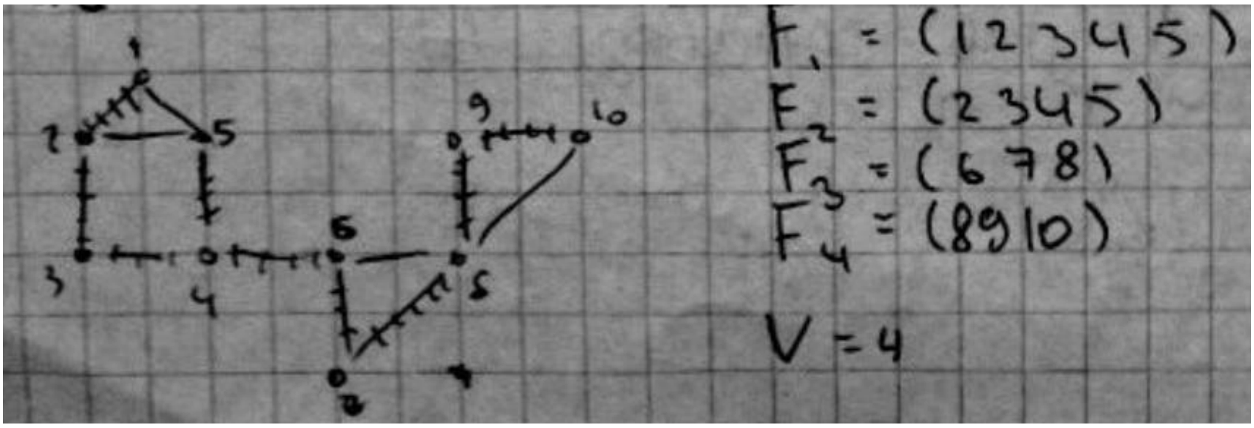
Обратные дуги (B) – ведет от потомка к предку в глубинном остовном лесу (в частности мб петля.



Прямые дуги (F) – ведет от подлинного предка к подлинному потомку, но не от отца к сыну в глубинном остовном лесу.

Поперечные дуги (C):





Пусть в неориентированном графе G = (V,E) произвольно фиксирован ***максимальный*** *остовный* ***лес****. Для связного графа это будет максимальное остовное дерево. Множество его ребер обозначим Т. Все ребра из Т назовем* ***древесными****, а рёбра исходного графа G, не принадлежащие Т –* ***обратными.***

Любой цикл графа G, содержащий только одно обратное ребро, назовем фундаментальным.

6. Поиск в глубину в орграфе. Классификация дуг. Критерий бесконтурности.

```
begin
        for all v ∈V do
        NEW[v] := 1;
        T, B, F, C := ∅;  stack := ∅;
        const := 1;
        for all v ∈V do
        while (∃v)(NEW[v] = 1) do
                search_DOR(v);
end;

proc search_DOR(v)
        NEW[v]  := 0;
        D[v] := const;  const++;
        v -> stack;
        for all ω ∈L[v] do
                if NEW[ω] then begin
                        (v,ω) -> T;
                        search_DOR(ω);
                end
                else begin
                                if (D(v) >= D(ω))&(ω∈stack) then
                                (v, ω) ->B;
                                if (D(v) < D(ω)) then
```

```
                    (v, ω) -> F;
                    if (D(v) > D(ω))&(ω∉ stack) then
                    (v, ω) ->C;
          end;
end;
```

Классификация дуг:

1) **Древесные дуги** – каждая такая дуга ведет от отца к сыну в глубинном остовном лесу.
2) **Прямые дуги** – каждая такая дуга ведет от подлинного предка к подлинному потомку (но не от отца к сыну) в глубинном остовном лесу.
3) **Обратные дуги** – от потомков к предкам (включая все петли).
4) **Поперечные дуги** – все дуги, не являющиеся ни древесными, ни прямыми, ни обратными.

Критерий бесконтурности: ориентированный граф является бесконтурным тогда и только тогда, когда при поиске в глубину от некоторой начальной вершины множество обратных дуг оказывается пустым.

7. Поиск в ширину в орграфе и поиск (на основе поиска в ширину) кратчайших расстояний от фиксированной вершины: алгоритм волнового фронта и поиск в ширину в орграфе с числовыми метками дуг.

Поиск в ширину

Охватываем весь список смежностей используется очередь. Расставляем метки на вершинах графа.

```
begin
    for all (v ∈ V) do
        M[v] := +∞;
    Q := ∅;
    M[v0] := 0;
    V0 -> Q;
    for all (v ∈ Q)
        while (Q != ∅) do
            for all (w ∈ L[v]) do
                if M[w] = +∞ then begin
                    M[w] := M[v] + 1;
                    w -> Q;
                end;
    Q -> V;
end
```

Алгоритм волнового фронта

G = (V,E) – орграф, φ = E->R^+ (функция разметки)

```
begin
    for all (v ∈ V) do
```

```
        M[v] := +∞;
    Q := Ø;
    M[v0] := 0;
    V0 -> Q;
    for all (v ∈ Q)
        while (Q != Ø) do
            for all (w ∈ L[v]) do begin
                d := M[v] + φ(v,w);
                if(d < M[w]) then begin
                    M[w] := d;
                    if(w ∉ Q) then
                        (w -> Q)
                end;
                Q -> v;
            end;
end;
```

8. Алгоритм Дейкстры.

```
begin
    for all (v ∈ V \ {v0}) do
        M[v] := +∞;
    M[v0] := 0;
    S := ∅;
    while (S != V) & (∃v ∈ V \ S) (M[v] != +∞) do begin
        S <- w (v ∈ S) & (M[w] = min);
        for all (v ∈ L[w] ∩ (V\S) do
            M[v] := min(M[v], M[w + φ(w,v))
    end;
end;
```

9. Изоморфизм графов. Группа автоморфизмов графа и ее вычисление.

$G_1 = (V_1,\rho_1)$; $G_2 = (V_2,\rho_2)$; $G_1 \equiv G_2$ = существует биекция

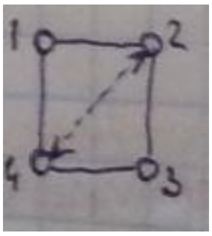
$h: V_1 \to V_2$ $(\forall\, u,v \in V_1)(u\rho_1 v \Leftrightarrow h(u)\, \rho_2 h(v))$

Неор. граф: $u\text{-}v \Leftrightarrow h(u)\text{-}h(v)$

$(\forall v)\ dg\,(h(v)) = dg(v)$

$G_1 \equiv G_2 \Leftrightarrow G_1 \equiv G_2$

Изоморфизм графа на себя – автоморфизм



Если переставив 2 и 4, то не изменится => автоморфизм

- Если g и h - автоморфизм, то $g \bullet h$ – автоморфизм
- Если h – автоморфизм, то h^{-1} – автоморфизм
- Тождественная подстановка – автоморфизм

$G = (V,E)$ $h: V \to V$ (биекция)

$(\forall\, u,v)(u\text{-}v \Leftrightarrow h(u)\text{-}h(v))$

$Aut(G)$ – подгруппа S_n

$v \in V$ $G_v = \{\sigma: \sigma(v) = v\}$ – стабилизатор

$|Aut(G)| = |G_v| \cdot |orb(v)|$

//какашки

10. Задача о путях в ориентированном графе, размеченном над полукольцом и ее решение с помощью алгоритма Флойда — Уоршелла — Клини. Задача о достижимости и поиске кратчайших расстояний между двумя узлами графа.

Размеченным ориентированным графом называют пару $W = (G, \phi)$, где $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$ – обычный ориентированный граф,

$\boldsymbol{\phi}: \boldsymbol{E} \to \boldsymbol{R}$ – функция разметки со значениями в некотором идемпотентном полукольце $\mathcal{S} = (S, +, *, \mathbb{O}, \mathbf{1})$, $(\forall e \in E)(\phi(e) \neq 1)$.

Если задать орграф с помощью матрицы смежности

$A = (a_{ij}),\ a_{ij} = \begin{cases} 1, & (v_i, v_j) \in E \\ 0, \text{иначе} \end{cases}$, то задача о достижимости

сводится к вычислению матрицы достижимости графа:

$$C = (c_{ij}),\ c_{ij} = \begin{cases} 1, & v_i \to^* v_j \\ 0, \text{иначе} \end{cases}.$$

Если задать орграф с помощью матрицы меток дуг

$A = (a_{ij}),\ a_{ij} = \begin{cases} \phi(v_i, v_j), \text{если } (v_i, v_j) \in E \\ 0, \text{иначе} \end{cases}$, то задача о поиске

кратчайших расстояний между двумя узлами графа сводится к вычислению матрицы кратчайших расстояний:

$$C = (c_{ij}), c_{ij} = \begin{cases} \text{длине кратчайшего пути из } v_i \text{в } v_j, \text{если } v_i \Longrightarrow^* v_j \\ +\infty, \text{иначе} \end{cases}.$$

Обе задачи можно решить с помощью алгоритма Флойда – Уоршелла – Клини.

В случае задачи о достижимости, в качестве полукольца $\mathcal{S}$, выбирают полукольцо $\mathbb{B} = (\{0,1\}, max, min, 0,1)$.

В случае задачи о поиске кратчайших расстояний, выбирают полукольцо $\mathcal{R}^+ = ([0, +\infty], min, +, +\infty, 0)$.

После этого матрица C путем решения системы уравнений

$$c_{ij}^{(k)} = c_{ij}^{(k-1)} + c_{ik}^{(k-1)} c_{kj}^{(k-1)}, \text{ где}$$

$$c_{ij}^{(0)} = \begin{cases} a_{ij}, & i \neq j \\ 1 + a_{ij}, & i = j \end{cases}$$

k – максимальный номер вершины, в которую разрешено заходить по пути из v_i в v_j.

Модуль 2. Регулярные языки и конечные автоматы.

1. Алфавит, слово, язык. Операции над языками, полукольцо всех языков в заданном алфавите и его замкнутость.

$\mathbf{V} = \{a_1, \dots, a_n\} \neq \varnothing$ - **Алфавит**.

Слово – $x \in V^k, k \geq 0$;

Пустое слово – $\{\lambda\} = V^0$

Длина слова: $|x| = k \rightleftharpoons x \in V^k, k \geq 0; |\lambda| = 0$

Равенство слов ⇔ равенство картежей

$x = x(1)x(2) \dots x(k), k \geq 0$

$x = y \rightleftharpoons (|x| = |y|) \& \left(\forall i = \overline{1, |x|}\right) \left(x(i) = y(i)\right)$

Итерация: $V^* \rightleftharpoons \bigcup_{k=0}^{\infty} V^k$ - множество всех слов в алфавите

Положительная итерация: $V^+ \rightleftharpoons V^* \setminus \{\lambda\}$ - множество всех не пустых слов в алфавите

Конкатенация слов:

$x = x(1)x(2) \dots x(k); y = y(1)y(2) \dots y(m), k, m \geq 0$

$xy = x(1)x(2) \dots x(k)y(1)y(2) \dots y(m) \in V^{k+m}$

$|xy| = |x| + |y|$

Свойства:

1)$(xy)z = x(yz)$

2) $xy \neq yx$

3) $(\forall \lambda)(\lambda x = x\lambda = x)$

Язык в алфавите V: $L \subseteq V^*$

Операции над языками:

а) **Теоретико-множественные операции**: $\cup \cap \setminus \Delta$; $\overline{L} = V^* \setminus L$

б) **Соединение языков:**

$$L_1 * L_2 \rightleftharpoons \{x * y : x \in L_1, y \in L_2\}$$

$L_1 L_2 \neq L_2 L_1$

$K(LM) = (KL)M$

$\{\lambda\}$ - язык из одного пустого слова

$L\{\lambda\} = \{\lambda\}L = L$

$2^{V^*} = \{L: L \subseteq V^*\}$

$\mathcal{L}_V = (2^{V^*}, V, *, \varnothing, \{\lambda\})$

Теорема: *Алгебра $\mathcal{L}_V$ - является замкнутым полукольцом.*

Док-во:

Используя аксиомы полукольца:

1) $K \cup (L \cup M) = (K \cup L) \cup M$

2) $K \cup L = L \cup K$

3) $K \cup \varnothing = K$

4) $K \cup K = K$

5) $K(LM) = (KL)M$

6) $L\{\lambda\} = \{\lambda\}L = L$

7) $K(L \cup M) = KL \cup KM$

Седьмое докажем:

$x \in K(L \cup M) => x = yz, y \in K, z \in L \cup M =>$

$=> (y \in K, z \in L) \vee (y \in K, z \in M) => yz \in KL \vee yz \in KM =>$

$=> yz = x \in KL \cup KM$

8) $L\varnothing = \varnothing L = \varnothing$

$K \subseteq L \Leftrightarrow K \cup L = L \Leftrightarrow K \leq L$

$\sup L_n = \bigcup_{n=1}^{\infty} L_n = \{x : (\exists n)(x \in L_n)\}$

$K \cdot \bigcup^{\infty} L_n = \bigcup_{n=1}^{\infty} K L_n$

$(\bigcup_{n=1}^{\infty} L_n) K = \bigcup_{n=1}^{\infty} (L_n K)$

$x \in K \cdot \bigcup_{n=1}^{\infty} L_n \Rightarrow x = yz$, где $y \in K$, $z \in \bigcup_{n=1}^{\infty} L_n \Rightarrow$

$\Rightarrow y \in K, (\exists n)(z \in L_n) \Rightarrow (\exists n)(yz = x \in K L_n) \Rightarrow x \in \bigcup_{n=1}^{\infty} K L_n$

2. Регулярные языки и регулярные выражения. Полукольцо регулярных языков как полукольцо с итерацией (не являющееся замкнутым).

Множество регулярных языков в V

1) $\varnothing, \{\lambda\}, \{a\}_{a\in V}$ - регулярные языки

2)Если K и L – регулярные языки, то K⋃L и KL тоже регулярные

3)Если L – регулярный, L^* - регулярный

$$L^n \rightleftharpoons L\cdot L^{n-1} = L^{n-1}\cdot L, \quad L^0 = \{\lambda\}$$

4)Никаких других регулярных языков в алфавите нет

$\mathcal{R}_V = (R_V, \cup, *, \varnothing, \{\lambda\})$ - полукольцо регулярных языков в V.

$L^* = \bigcup_{n=0}^{\infty} L^n$ - итерация языка

$L^+ = \bigcup_{n=1}^{\infty} L^n$ - позитивная итерация языка

<u>Регулярное выражение</u> – формула, обозначающая какой-то регулярный язык (α -> L)

1) $\varnothing \to \varnothing, \lambda \to \{\lambda\}, a \to \{a\}, a \in V$

2)Если $\alpha \to K, \beta \to L \Rightarrow (\alpha + \beta) \to K \cup L, (\alpha * \beta) \to K * L$

3)Если $\alpha \to L \Rightarrow \alpha^* = L^*, \alpha^+ = L^+$

4)Никаких других регулярных выражений не существует

Базовые регулярные тождества:

1) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

2) $\alpha + \beta = \beta + \alpha$

3) $\alpha + \varnothing = \alpha$

4) $\alpha + \alpha = \alpha$

5) $\alpha\lambda = \lambda\alpha = \alpha$

6) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$

7) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma; (\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha$

8) $\alpha\varnothing = \varnothing\alpha = \varnothing$

9) $(\alpha^*)^* = (\alpha^+)^* = (\alpha^*)^+ = \alpha^*$

10) $\alpha\alpha^* = \alpha^*\alpha = \alpha^+$

11) $\alpha^* + \lambda = \alpha^+$
12) $\alpha^+ + \lambda = \alpha^+$
13) $(\alpha + \beta)^* = (\alpha^* \beta^*)^*$
14) $\emptyset^* = \lambda$

3. Понятие конечного автомата (КА) и языка, допускаемого КА. Анализ и синтез КА.

Определение КА

Пусть V – некоторый алфавит. Конечным автоматом называется орграф (Q,E), размеченный над полукольцом R(V), при этом:

1) на функцию разметки φ:E->R(V) наложены ограничения:
   - $\varphi(e) \neq \emptyset$
   - $\varphi(e) = \{\lambda\}$ или $\varphi(e) \subseteq V$
2) Задана вершина $q_0 \in Q$, называемая входной
3) Задано множество вершин F, называемых заключительными

Таким образом, КА может быть задан как пятерка:

$$M = (Q,E,\varphi,q_0,F), \text{ где}$$

Q – множество состояний автомата

E – множество дуг

φ – функция разметки(весовая функция)

q_0 – входная вершина

F$\subseteq$ Q – подмножество заключительных состояний

КА допускает цепочку x, если она читается на некотором пути, ведущем из начальной вершины в одну из заключительных.

Язык, допускаемый КА – множество всех допускаемых им цепочек.

Задача синтеза КА – задача построение КА по регулярному языку

Задача анализа КА – вычисление языка КА

Теорема: *Для любого регулярного языка может быть построен КА, допускающий этот язык*

4. Теорема Клини о совпадении класса языков, допускаемых КА и класса регулярных языков: теорема о регулярности языка любого КА и теорема о построении КА по произвольному регулярному выражению.

Теорема: *язык регулярен тогда и только тогда, когда он допускается КА.*

Док-во:

1) *Докажем, что решение системы линейных уравнений с регулярными коэффициентами – регулярно, т.е. является вектором, каждая компонента которого – регулярный язык.*

Индукция по порядку n системы ЛУ:

Базис n = 1 $x = \lambda x+\beta$ (λ,β – рег. выраж.)

$x = \lambda^*\beta$ – рег. язык

Предположим: пусть для любого порядка ≤ n-1 утверждение верно (n ≤ 2)

Рассмотрим систему n-го порядка:

$$\begin{cases} x_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1 \\ x_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n + b_2 \\ \ldots \\ X_n = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n + b_n \end{cases}$$

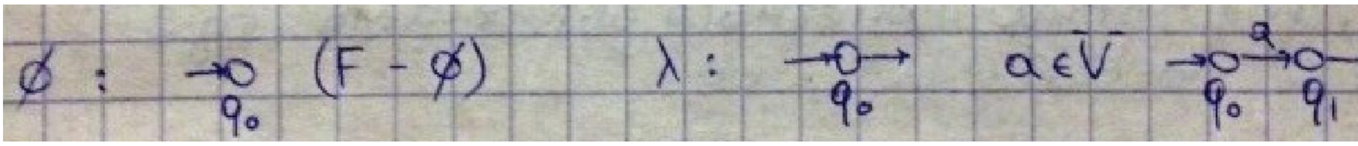
Эта система имеет решение:

$x_1 = a_{11}{}^*(a_{12}x_2 + \ldots + a_{1n}x_n + b_1)$

Подставим полученное выражение x_1 в остальные выражения системы и, приводя подобные члены в правых частях, получим систему с рег. коэффициентами порядка n-1, решение которой регулярно по предположению.

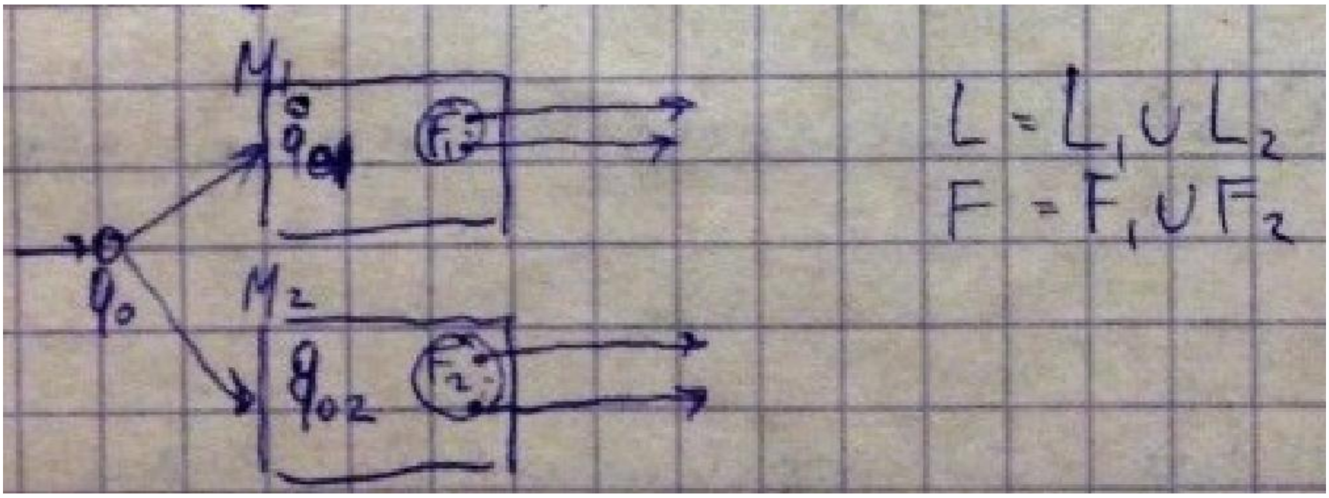
$x_2 \ldots x_n$ – регулярные языки. Тогда x_1 – тоже регулярно.

2) Построим КА по данному регулярному выражению

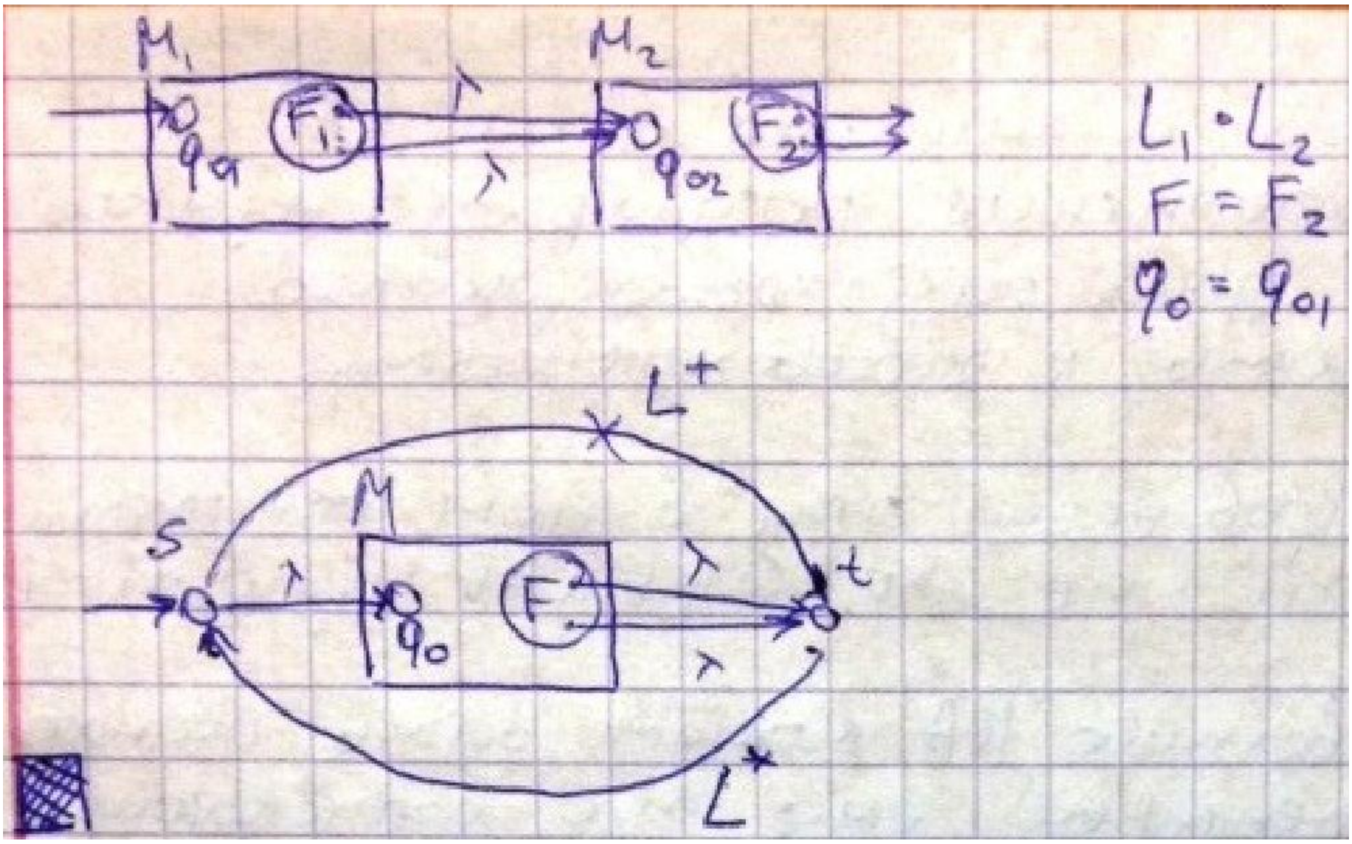


∅ :
q_0
(F - ∅)
λ :
q_0
a ∈ V
q_0
q_1

$L(M_1) = L_1, L(M_2) = L_2$



M_1
q_{01}
F_1
q_0
M_2
q_{02}
F_2
$L = L_1 \cup L_2$
$F = F_1 \cup F_2$



M_1
q_{01}
F_1
λ
M_2
q_{02}
F_2
$L_1 \cdot L_2$
$F = F_2$
$q_0 = q_{01}$
L^+
M
s
λ
q_0
F
t
L^*

5. Детерминизация и минимизация КА. Регулярность дополнения регулярного языка и пересечения двух регулярных языков. Проблемы пустоты и эквивалентности.

КА называют детерминированным, если в нем отсутствуют λ-переходы, а также $(\forall q \in Q)(\forall a \in V)(|\delta(q,a)| = 1)$

Теорема: для любого КА может быть построен эквивалентный ему, т.е. допускающий тот же самый детерминированный КА.

$$M_1 \approx M_2 <-> L(M_1) = L(M_2)$$

1) Удаление лямбда переходов

Исходный $M = (Q, E, q_0, F, \delta)$.

Строим $M' = (Q', E', q'_0, F', \delta')$.

По правилу :

В M: $q \xrightarrow{\lambda} r \xrightarrow{a} p$

В M’: $q \xrightarrow{a} p$

2) Детерминизация

Исходный КА $M = (Q, E, q_0, F, \delta)$ – без λ-переходов

Строим КА $M' = (Q', E', q'_0, F', \delta')$.

$Q' = 2^Q$; $q_0' = \{q_0\}$; $F' = \{T\colon T \cap F \neq \emptyset\}$

$\delta'(S,a) = \bigcup_{(q \in S)} \delta(q,a)$

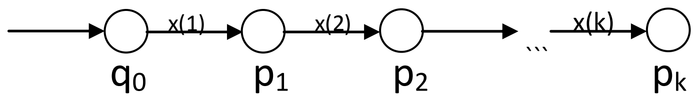
Теорема: если $L \subseteq V^*$ регулярный, то его дополнение $\overline{L} = V^* \setminus L$ – регулярный язык

Док-во:

Т.к. L – регулярный, то $L = L(M)$,где $M = (Q, E, q_0, F, \delta)$ – детерминированный КА.

Пусть x=

$= x(1)\ldots x(k) \in V^*$, $k \geq 0$



$x \in L \Leftrightarrow p_k \in F$ $(p_0 = q_0)$

$x \notin L \Leftrightarrow p_k \notin F$

Следствие:

Если L_1 и L_2 – регулярные языки, то $L_1 \setminus L_2$; $L_1 \cap L_2$; $L_1 \Delta L_2$ – регулярные

$L_1 \cap L_2 = \overline{\overline{L1} \cup \overline{L2}}$ – рег. $L_1 \setminus L_2 = L_1 \cap \overline{L2}$ – рег. $L_1 \Delta L_2 = (L_1 \setminus L_2) \cup (L_2 \setminus L_1)$

Проблема пустоты:

Выяснить, не является ли язык, допускаемый автоматом пустым?

Проблема эквивалентности:

Для любых двух заданных КА выяснить, не допускают ли они один и тот же язык?

6. Лемма о разрастании для регулярных языков.

Теорема: *Для ∀ регулярного языка L в алфавите V определена константа k_L такая, что для $(\forall x \in L)(|x| \geq K_L \Rightarrow x = uvw)$, где $0 < |v| \leq K_L$ и $(\forall n \geq 0)(uv^n w \in L)$*

Рассмотрим язык: $L = \{a^n b^n : n \geq 0\}$

Предположим, что этот язык регулярен, тогда $n \geq K_L$

a..a	b..b

X =

1) $v = a^M$, $M \leq n$
2) $v = b^M$, $M \leq n$
3) $v = a^M b^L$, $M,L > 0$; $M,L \leq n$

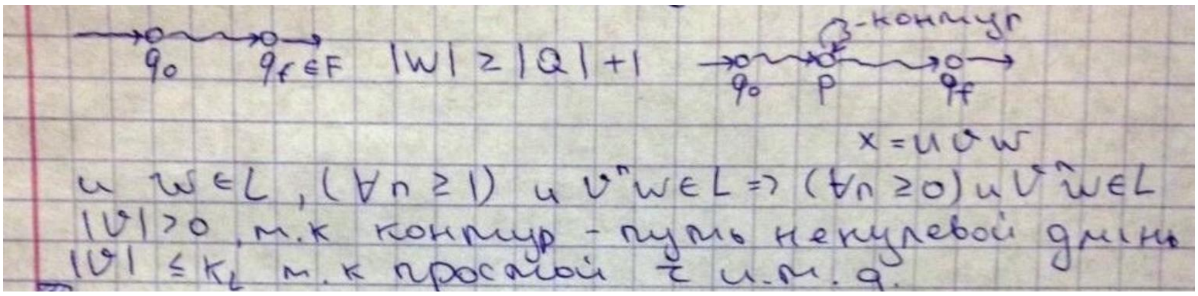
$v^2 = a^M \underline{b^L a^M} b^L$ (подчеркнутое не допускается)

Док-во:

$L \subseteq V^*$ регулярен $\Rightarrow L = L(M)$, где

$M = (Q, E, q_0, F, \delta)$ – детерминированный КА

Положим $K_L = |Q|$ и пусть $x \in L$ и $|x| \geq |Q| = K_L$



Следствие:

Во всяком регулярном языке найдется последовательность цепочек, длины которых образуют возрастающую арифметическую прогрессию.

$X_n = uv^n w$, $d = |x_{n+1}| - |x_n|$

Модуль 3.

1. Формулы включения и исключения (с выводом).

Формула для числа элементов объединения множеств.

$A_1, A_2, \ldots, A_n \neq \emptyset$

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{p=1}^{n} (-1)^{p+1} \sum_{i_1 < i_2 < \ldots < i_p} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_p}|$$ - <u>первая формула</u>

Заметим, что внутренняя сумма для заданного p содержит C_n^p слагаемых.

В частности:

$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$;

$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| -$

$-(|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|$

Знак при внутренней сумме «минус» для четного p и «плюс» для нечетного.

<u>Доказательство:</u>

Достаточно доказать, что каждый элемент рассматриваемого объединения учтен в правой части равенства ровно один раз.

Пусть элемент a принадлежит в точности k множествам из n.

Тогда в сумме $\sum_{i_1 < i_2 < \ldots < i_p} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_p}|$ этот элемент фигурирует C_k^p раз (выбраны какие-то p подмножеств из k, содержащих a).

Следовательно, во всей правой части этот элемент фигурирует $\sum_{p=1}^{k} (-1)^{p+1} C_k^p$ раз.

Но

$0 = (1-1)^k = \sum_{p=0}^{k} (-1)^p C_k^p = 1 - \sum_{p=1}^{k} (-1)^{p+1} C_k^p$, откуда $\sum_{p=1}^{k} (-1)^{p+1} C_k^p = 1$,

итд.

Формула для пересечения дополнений множеств.

Подсчет числа элементов в объединении множеств позволяет находить число элементов, обладающих хотя одним из n свойств. Следующая формула позволяет находить число элементов, не обладающих ни одним из n свойств. Если обозначить через A_i

множество всех тех элементов, которые обладают свойством P_i (при $i = 1,\dots,n$), то множество всех тех элементов, которые не обладают ни одним из указанных свойств, есть пересечение дополнений $\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_n$.

Тогда

$$|\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_n| = |\overline{A_1 \cup A_2 \cup \dots \cup A_n}| =$$

$$= |U| - |A_1 \cup A_2 \cup \dots \cup A_n| =$$

$$= |U| - \sum_{p=1}^{n} (-1)^{p+1} \sum_{i_1 < i_2 < \dots < i_p} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_p}| =$$

$$= |U| + \sum_{p=1}^{n} (-1)^{p} \sum_{i_1 < i_2 < \dots < i_p} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_p}|.$$

// на доказательство не очень похоже, но на лекциях Белоусов даже короче давал

(Здесь U - универсальное множество, т.е. «высший род» в заданном классе элементов.)

2. Задача о числе сюръекций одного конечного множества на другое.

Формулы включения-исключения можно применить для подсчета числа сюръективных отображений одного конечного множества на другое.

<u>Задача:</u> найти число S(m,n) всех сюръекций из A на B, где |A| = m, |B| = n. (m >=n)

Пусть $A=\{a_1,...a_m\}, B=\{b_1,...,b_n\}$; пусть $W_i=\{f : f\in B^A, b_i \notin R(f)\}$ - множество всех таких отображений A в B, в область значений которых не попадает элемент b_i. Тогда для фиксированных $i_1,...,i_k$ имеем $|W_{i_1}\cap ...\cap W_{i_k}|=(n-k)^m$, а

$$\sum_{i_1<...<i_k}|W_{i_1}\cap ...\cap W_{i_k}|=C_n^k(n-k)^m.$$

Тогда число $S(m,n)$ всех сюръекций A на B составит

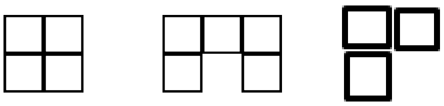
$$S(m,n)=n^m-\sum_{k=1}^{n}(-1)^{k+1}C_n^k(n-k)^m=\sum_{k=0}^{n}(-1)^k C_n^k(n-k)^m.$$

//Несколько примеров на всякий случай:

1) $S(4,3) = 3^4-3*2^4+3*1^4 = 81 - 48 + 3 = 36$;
2) $S(3,2)=2^3-2\cdot 1=6$

3. Ладейные полиномы и методы их вычисления (с доказательством основных теорем).

Доске C с m клетками, которая является частью квадратной доски $n \times n$, сопоставляется полином $R(x,C)=\sum_{k=0}^{m} r_k(C)x^k$,коэффициент $r_k(C)$ которого равен числу способов, которым на доске C можно разместить k ладей в не атакующих позициях.



C1 C2 C3

Для изображенных выше досок имеем:

$R(x,C_1)=1+4x+2x^2$,

$R(x,C_2)=1+5x+4x^2$

$R(x, C_3) = 1 + 3x + x^2$;

Коэффициент при нулевой степени x означает, что существует 1 способ оставить доску пустой, т.е. разместить 0 ладей.

Теорема 1. Если доски C_1 и C_2 дизъюнктны (не имеют общих строк и столбцов), то $R(x,C_1 \cup C_2)=R(x,C_1)R(x,C_2)$.

Доказательство. Рассмотрим коэффициент $r_k(C_1 \cup C_2)$. Если на доске $C=C_1 \cup C_2$ размещено k ладей[1], то можно выбрать l ладей на доске C_1 и $k-l$ ладей на доске C_2. Тем самым при заданном l существует $r_l(C_1)r_{k-l}(C_2)$ способов разместить k ладей на объединенной доске (заметим, что если бы доски не были дизъюнктны, то это было бы неверно). Рассматривая все возможные значения l от нуля до k, получим

$$r_k(C)=\sum_{l=0}^{k} r_l(C_1)r_{k-l}(C_2),$$

что и является коэффициентом при x^k в произведении $R(x,C_1)R(x,C_2)$.

Рассмотрим теперь более сложную комбинацию досок.

[1] Везде в дальнейшем, говоря о размещении ладей, мы, естественно, имеем в виду размещение в не атакующих позициях.

Теорема 2. Пусть C - доска с m клетками, а s - клетка этой доски; пусть C_s - доска, полученная из доски C удалением клетки s, и пусть $C_s^{\#}$, полученная из доски C удалением строки и столбца, содержащих клетку s.
Тогда $R(x,C) = xR(x,C_s^{\#}) + R(x,C_s)$.
Доказательство. Определим число способов, которыми можно разместить k ладей на доске C.
Возможны два случая: 1) в клетке s есть ладья и 2) в клетке s ладьи нет.
В первом случае остальные $k-1$ ладей можно разместить на доске $C_s^{\#}$ $r_{k-1}(C_s^{\#})$ способами, а во втором размещение всех k ладей производится на доске C_s, и число способов составит $r_k(C_s)$.
Следовательно, всего существует $r_{k-1}(C_s^{\#}) + r_k(C_s)$ способов разместить k ладей, т.е. $r_k(C) = r_{k-1}(C_s^{\#}) + r_k(C_s)$.
Теперь преобразуем ладейный полином для всей доски:

$$R(x,C) = \sum_{k=1}^{m} r_{k-1}(C_s^{\#})x^k + \sum_{k=0}^{m} r_k(C_s)x^k =$$

$$= \sum_{k=0}^{m-1} r_k(C_s^{\#})x^{k+1} + \sum_{k=0}^{m} r_k(C_s)x^k =$$

$$= x\sum_{k=0}^{m} r_k(C_s^{\#})x^k + \sum_{k=0}^{m} r_k(C_s)x^k,$$

так как $r_m(C_s^{\#}) = 0$ (на этой доске меньше m клеток).
Для доски C_2 на рисунке выше, выбирая в качестве клетки s среднюю, получим:

$$R(x,C_{2,s}^{\#}) = 1 + 2x, R(x,C_{2,s}) = 1 + 4x + 2x^2,$$

$$R(x,C_2) = 1 + 5x + 4x^2.$$

4. Вывод формулы для числа подстановок с запрещенными позициями.

// В начале приведены несколько определений(лекции Белоусова), не знаю нужны ли они для вывода формулы.

Рассмотрим снова группу подстановок S_n множества $M = \{1, 2, ..., n\}$.

Пусть для каждого $i = \overline{1, n}$ определено множество F_i ***запрещенных значений***, т.е. из группы S_n исключаются все такие подстановки σ, для которых $\sigma(i) \in F_i$. Упорядоченная пара $(i, \sigma(i))$ при $\sigma(i) \in F_i$ называется ***запрещенной парой***. Множество

$$F = \bigcup_{i=1}^{n} \{(i, \sigma(i)) : \sigma(i) \in F_i\}$$

называется ***запрещенной областью***.

На доске, соответствующей матрице подстановок, клетки запрещенной области закрашиваются.

Заметим, что для беспорядков запрещенной областью является главная диагональ.

Чтобы определить число подстановок, которые не принимают значений в запрещенной области, введем для фиксированного $i \in \{1, ..., n\}$ множество A_i как множество всех таких подстановок σ, для которых $\sigma(i) \in F_i$.

Тогда число всех подстановок, значения которых не являются запрещенными, равно

$$|\bar{A}_1 \cap \bar{A}_2 \cap ... \cap \bar{A}_n| = |U| - \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1 < i_2 < ... < i_k} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_p}| =$$

$$= |U| + \sum_{k=1}^{n} (-1)^{k} \sum_{i_1 < i_2 < ... < i_k} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}|.$$

Определим значение $|A_i|$ при фиксированном i. Это будет число всех подстановок, у которых все элементы, кроме i-го переставляются как угодно, а i-й обязан попасть в одну из закрашенных клеток, т.е. значение подстановки на этом элементе должно принадлежать множеству F_i. Очевидно, существует

$n_i = |F_i|$ способов это сделать. Таким образом, $|A_i| = n_i(n-1)!$, а

$$\sum_{i=1}^{n} |A_i| = (\sum_{i=1}^{n} n_i)(n-1)! = r_1(F)(n-1)!.$$

Далее, при фиксированных i и j число $|A_i \cap A_j|$ равно числу всех перестановок из $n-2$ элементов, помноженному на число всех способов, которыми можно значения i-го и j-го элементов задать так, чтобы они попали в множества F_i и F_j соответственно. Это число способов равно, как нетрудно видеть, числу способов, которыми можно разместить две ладьи в той части запрещенной области, которая соответствует множествам F_i и F_j. Обозначим это последнее через n_{ij}. Суммируя по i и по j, получим

$$\sum_{i<j} |A_i \cap A_j| = (\sum_{i<j} n_{ij})(n-2)! = r_2(F)(n-2)!.$$

Рассуждая аналогично, можно показать, что

$$\sum_{i_1<i_2<\ldots<i_k} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = r_k(F)(n-k)!.$$

Итак, число допустимых подстановок составит

$$L_n = n! - (R(x,F)-1)|_{x^k=(-1)^{k+1}(n-k)!} = n! - \sum_{k=1}^{n} (-1)^{k+1} r_k(F)(n-k)!,$$ т.е. из

числа всех подстановок надо вычесть значение ладейного полинома запрещенной области (без единицы) при подстановке вместо k-ой степени переменной числа $(-1)^{k+1}(n-k)!$.

Формула может быть, очевидно, переписана и в таком виде:

$$L_n = \sum_{k=0}^{n} (-1)^k r_k(F)(n-k)!$$

В частности, для беспорядков $r_k(F) = C_n^k$ - число способов размещения k ладей на главной диагонали.

5. Однородные линейные рекуррентные соотношения (ОЛРС) с постоянными коэффициентами. Понятие решения, фундаментальной системы решений (ФСР). Теорема о связи между решениями и начальными условиями.

Пусть дана числовая последовательность $\{x_n\}_{n\in\mathbb{N}_0}$, причем она не определена явно как функция натуральной переменной, но всякий ее член выражается через k предыдущих (для фиксированного k) в виде:

$$x_n = \varphi(x_{n-1},\dots,x_{n-k}) + f(n) \qquad (1)$$

В этом случае соотношение (1) называют ***рекуррентным соотношением*** k***-го порядка***. При $f(n)=0$ соотношение называют ***однородным***.

Если функция φ в (1) линейна по своим аргументам, то такое соотношение называют ***линейным***. Будем, как правило, записывать линейное рекуррентное соотношение в виде:

$$x_n + a_1(n)x_{n-1} + \dots + a_k(n)x_{n-k} = f(n) \qquad (3)$$

В соотношении (3) последовательности $a_i(n), i=1,\dots,k$ называют ***коэффициентами***, а последовательность $f(n)$ - ***правой частью***. В случае нулевой правой части получаем ***однородное линейное рекуррентное соотношение***.

Здесь мы ограничимся рассмотрением только линейных соотношений ***с постоянными коэффициентами***, полагая, что все последовательности $a_i(n), i=1,\dots,k$ суть числа (как правило, вещественные).

Общий вид соотношения (k-го порядка):

$$x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = 0 \qquad (4)$$

$x_0=\alpha_0,\dots,x_{k-1}=\alpha_{k-1}$ (2) - начальные условия

Произвольная линейно независимая система $(y_n^{(1)},\dots,y_n^{(k)})$ решений соотношения (4) называется ***фундаментальной системой решений*** (ФСР), а ее компоненты – ***фундаментальными решениями***.

Теорем о связи между решениями и начальными условиями.
Заданные начальные условия (2) однозначно определяют частное решение соотношения (4). Наоборот, фиксированное частное решение соотношения (4) однозначно определяет начальные условия, которым оно удовлетворяет.
Доказательство. Пусть выполняются начальные условия вида (2):
$y_0 = \alpha_0, ..., y_{k-1} = \alpha_{k-1}$ (6)
Тогда, в силу (4) $y_k = -a_1 y_{k-1} - ... - a_k y_0$, и далее для любого $s > 0$ $y_{k+s} = -a_1 y_{k+s-1} - ... - a_k y_s$, и член y_n определен однозначно для любого $n \geq 0$.
Пусть теперь y_n - какое-то частное решение соотношения (4).
Покажем, что числа
$\alpha_0, ..., \alpha_{k-1}$ можно подобрать так, чтобы выполнялось (6).
Имеем:

$$
\begin{aligned}
& y_k + a_1 \alpha_{k-1} + ... + a_k \alpha_0 = 0, \\
& y_{k+1} + a_1 y_k + a_2 \alpha_{k-1} ... + a_k \alpha_1 = 0 \\
& .... \\
& y_{2k-1} + a_1 y_{2k-2} + a_2 y_{2k-3} + ... + a_{k-1} y_k + a_k \alpha_{k-1} = 0.
\end{aligned}
\qquad (7)
$$

Система (7) есть система относительно неизвестных $\alpha_0, ..., \alpha_{k-1}$, заданная в треугольной форме. Из последнего уравнения однозначно определяется α_{k-1}, и далее («обратным ходом» метода Гаусса) все остальные неизвестные до α_0 включительно (при условии, что $a_k \neq 0$, но это в соотношении (4) и предполагается, так как иначе порядок соотношения будет меньше k).

6. Теорема об общем решении ОЛРС как линейной комбинации фундаментальных решений.

Теорема 3. Любое решение соотношения $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4) является линейной комбинацией фундаментальных решений.

Доказательство. Докажем, что каковы бы ни были начальные условия вида $x_0 = \alpha_0, \ldots, x_{k-1} = \alpha_{k-1}$ (2), которым должна удовлетворять линейная комбинация $\sum_{i=1}^{k} C_i y_n^{(i)}$, ее коэффициенты однозначно определяются этими начальными условиями. Этого достаточно в силу того, что каждое решение однозначно определено начальными условиями и обратно.

Имеем такую систему для определения этих коэффициентов:

$$\begin{cases} \sum_{i=1}^{k} C_i y_0^{(i)} = \alpha_0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = \alpha_{k-1} \end{cases}$$

(8) главный определитель этой системы

$$\Delta = \begin{vmatrix} y_0^{(1)} \ldots y_0^{(k)} \\ \ldots\ldots\ldots\ldots \\ y_{k-1}^{(1)} \ldots y_{k-1}^{(k)} \end{vmatrix}$$

(9) отличен от нуля.

Действительно, если бы он был равен нулю, то *однородная* система, соответствующая системе (8), имела бы ненулевое решение, т.е. нашлись бы коэффициенты $C_i, i = 1, \ldots, k$, не все равные нулю, для которых бы выполнялось

$$\begin{cases} \sum_{i=1}^{k} C_i y_0^{(i)} = 0, \\ \dots\dots\dots\dots\dots\dots\dots \\ \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = 0, \end{cases}$$

т.е. решение, являющееся нетривиальной линейной комбинацией фундаментальных решений, удовлетворяет нулевым начальным условиям и, следовательно, в силу **теоремы 2**, само является нулевым. Но это невозможно в силу линейной независимости фундаментальных решений.

//**Теорема 2**. Существует единственное частное решение соотношения (4), удовлетворяющее начальным условиям $x_0 = \alpha_0, \dots, x_{k-1} = \alpha_{k-1}$ (2).

Итак, $\Delta \neq 0$, система (8) имеет единственное решение, и коэффициенты линейной комбинации фундаментальных решений однозначно определяются начальными условиями, которым она должна удовлетворять.

Форма $\varphi_n = \sum_{i=1}^{k} C_i y_n^{(i)}$ называется ***общим решением*** соотношения (2). Это значит, что любое частное решение (4) может быть получено при определенных значениях коэффициентов (произвольных констант) $C_i, i = 1, \dots, k$ (при заданной ФСР).

7. Характеристический полином и характеристическое уравнение ОЛРС. Структура общего решения в случае вещественных и комплексных корней характеристического полинома.

//Теорема 1. Пусть $y_n^{(1)}$ и $y_n^{(2)}$ - решения соотношения $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4). Тогда произвольная линейная комбинация их также является решением соотношения $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4).

Доказательство. Пусть $\varphi_n = C_1 y_n^{(1)} + C_2 y_n^{(2)}$. Подставляя φ_n в $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4), будем иметь:

$$C_1 y_n^{(1)} + C_2 y_n^{(2)} + a_1(C_1 y_{n-1}^{(1)} + C_2 y_{n-1}^{(2)}) + \ldots + a_k(C_1 y_{n-k}^{(1)} + C_2 y_{n-k}^{(2)}) =$$
$$= C_1(y_n^{(1)} + a_1 y_{n-1}^{(1)} + \ldots + a_k y_{n-k}^{(1)}) + C_2(y_n^{(2)} + a_1 y_{n-1}^{(2)} + \ldots + a_k y_{n-k}^{(2)}) \equiv 0,$$

что и требовалось.

Следствие. Множество решений соотношения $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4) образует подпространство в пространстве всех последовательностей (над полем комплексных чисел).

Очевидно, что соотношение $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4) всегда имеет тривиальное нулевое решение. Докажем, что существуют (в общем случае) и ненулевые решения.

Будем искать решение (4) в виде $y_n = \lambda^n$ для какого-то (в общем случае, комплексного) числа λ.

Имеем:

$\lambda^n + a_1 \lambda^{n-1} + \ldots + a_k \lambda^{n-k} = 0$, или

$\lambda^{n-k}(\lambda^k + a_1 \lambda^{k-1} + \ldots + a_{k-1}\lambda + a_k) = 0$.Так как нулевое решение уже учтено, то получаем: $\lambda^k + a_1 \lambda^{k-1} + \ldots + a_{k-1}\lambda + a_k = 0$. (5) Уравнение (5) называется ***характеристическим уравнением*** соотношения (4), а его правая часть – ***характеристическим многочленом*** соотношения (4).

Предположим, что найдены все r корней этого уравнения, включая комплексные (при этом каждый корень учитывается столько раз, какова его кратность). Для построения базиса в пространстве решений можно использовать следующие правила.

1. Если $\lambda = \alpha$ – вещественный корень кратности s уравнения (2.7), то ему отвечают s линейно независимых частных решений:

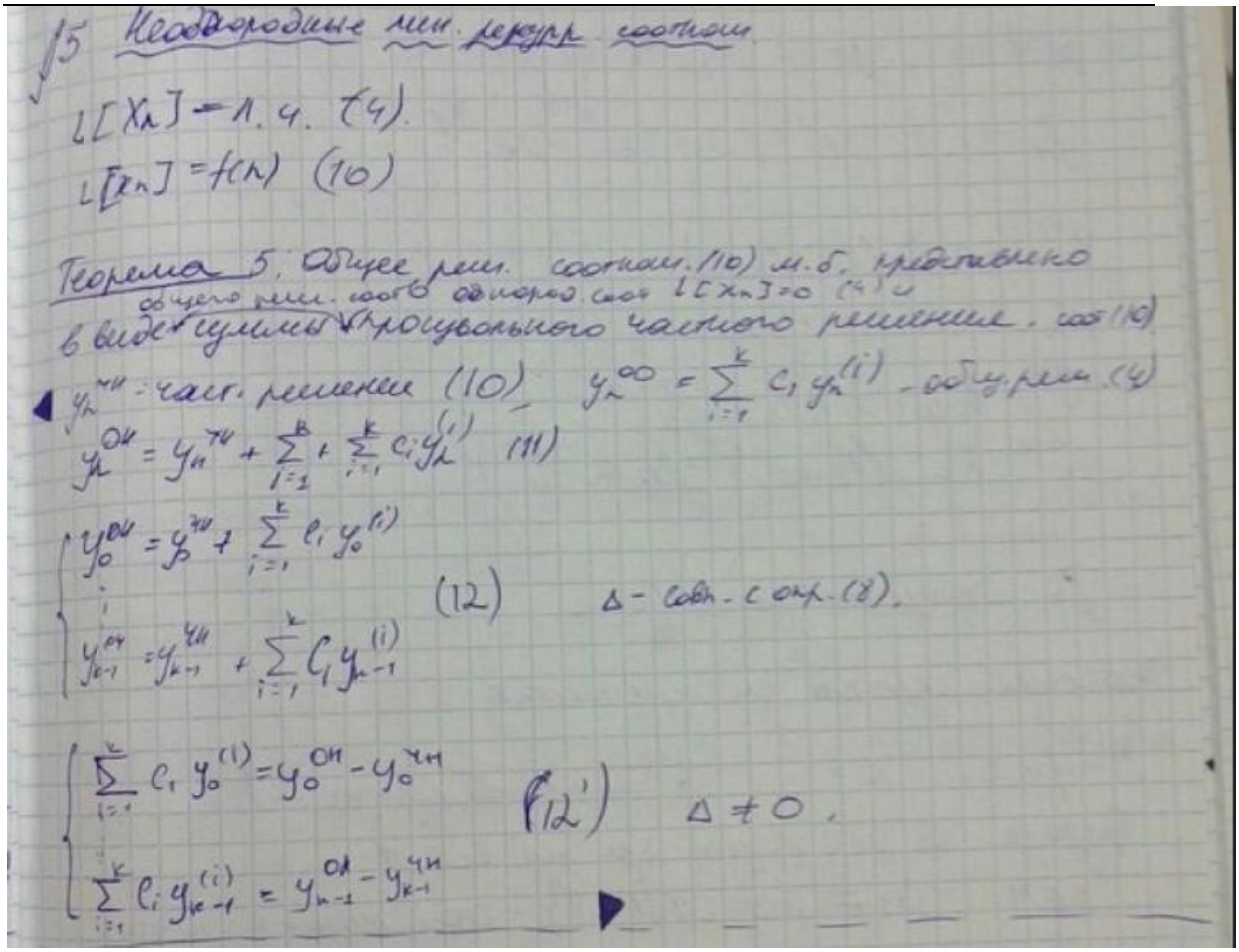
$$\varphi_n^{(1)} = \alpha^n, \quad \varphi_n^{(2)} = n\alpha^n, \quad \ldots, \quad \varphi_n^{(s)} = n^{s-1}\alpha^n.$$

2. Если $\lambda = \alpha \pm i\beta$ – пара комплексно сопряженных корней уравнения (2.7) кратности s каждый, то им отвечают $2s$ линейно независимых частных решений

$$\varphi_n^{(1)} = \rho^n \cos(n\theta),\ \varphi_n^{(3)} = n\rho^n \cos(n\theta),\ \ldots,\ \varphi_n^{(2s-1)} = n^{s-1}\rho^n \cos(n\theta),$$
$$\varphi_n^{(2)} = \rho^n \sin(n\theta),\ \varphi_n^{(4)} = n\rho^n \sin(n\theta),\ \ldots,\ \varphi_n^{(2s)} = n^{s-1}\rho^n \sin(n\theta),$$

где $\rho = |\alpha + i\beta|$, $\theta = \arg(\alpha + i\beta)$.

8. Неоднородные линейные рекуррентные соотношения с постоянными коэффициентами. Теорема о структуре общего решения. Поиск частного решения методом подбора. Принцип суперпозиции (без доказательства).



№5 Неоднородные лин. рекурр. соотнош.

$L[x_n] = $ л. ч. (4)

$L[x_n] = f(n)$ (10)

Теорема 5. Общее реш. соотнош. (10) м.б. представлено в виде суммы общего реш. соотв. однород. соот. $L[x_n]=0$ (4) и произвольного частного решения. соот (10)

$y_n^{чн}$ - част. решение (10), $y_n^{oo} = \sum_{i=1}^{k} c_i y_n^{(i)}$ - общ. реш. (4)

$$y_n^{он} = y_n^{чн} + \sum_{i=1}^{k} c_i y_n^{(i)} \quad (11)$$

$$\begin{cases} y_0^{он} = y_0^{чн} + \sum_{i=1}^{k} c_i y_0^{(i)} \\ \vdots \\ y_{k-1}^{он} = y_{k-1}^{чн} + \sum_{i=1}^{k} c_i y_{k-1}^{(i)} \end{cases} \quad (12)$$

Δ - совп. с опр. (8).

$$\begin{cases} \sum_{i=1}^{k} c_i y_0^{(i)} = y_0^{он} - y_0^{чн} \\ \vdots \\ \sum_{i=1}^{k} c_i y_{k-1}^{(i)} = y_{k-1}^{он} - y_{k-1}^{чн} \end{cases} \quad (12')$$

$\Delta \neq 0$.

// Это хуйня какая то тут

Не надо шутить с войной. Здесь другие ребята. Это не Германия, это не Афганистан. Джордж, твоих солдат здесь порвут на части. 250 тысяч отборных солдат Ирака! Они все разнесут. Они всю пустыню пройдут на один час! Они взорвут все твои эсминцы, всех твоих журналистов, дипломатов. Джордж, ты ковбой. Ты остановись, б..., ты кончай, ты патроны спрячь подальше на склад и забудь про своего папу. У нас был один *удак, отомстил за брата, б..., и рухнула Великая Российская империя. И другой чудак был, за своего дедушку отомстил, и рухнул Советский Союз. И ты повторишь ту же ошибку. Ты папу забудь, папа отработал свое. Ты подумай о будущем Америки. Она гибнет! Твоя молодежь бежит из твоей страны. Там никто не хочет жить в Америке, никто! Эта барахолка, б.... Доллар, доллар, доллар, ... Эта грязная зеленая бумажка! Ни души, музыки нету, б..., нет писателей у тебя. Весь мир слушает Чайковского, Достоевского, б.... Фестивали, спорт только в России… И здесь, в Ираке. Здесь любят президента, а тебя презирают, презирают

При решении задач для нахождения частного решения удобно использовать следующие правила.

1. Если $b_n = \alpha^n P_k(n)$, где $P_k(n)$ – многочлен степени k, то частное решение соотношения (2.3) следует искать в виде

$$x_n = n^s \alpha^n \tilde{P}_k(n),$$

где $\tilde{P}_k(n)$ – многочлен степени k с неопределенными коэффициентами; s – кратность корня $\lambda = \alpha$ характеристического уравнения для соответствующего однородного соотношения ($s = 0$, если оно не имеет корня $\lambda = \alpha$).

2. Если $b_n = \rho^n \left(P_k(n)\cos(n\theta) + Q_l(n)\sin(n\theta)\right)$, где $P_k(n)$, $Q_l(n)$ – многочлены степени k и l соответственно, то частное решение соотношения (2.3) следует искать в виде

$$x_n = n^s \rho^n \left(\tilde{P}_N(n)\cos(n\theta) + \tilde{Q}_N(n)\sin(n\theta)\right),$$

где $\tilde{P}_N(n), \tilde{Q}_N(n)$ – многочлены степени N с неопределенными коэффициентами, $N = \max\{k, l\}$; s – кратность каждого из корней $\lambda = \rho(\cos\theta \pm i\sin\theta)$ характеристического уравнения для соответствующего однородного соотношения ($s = 0$, если оно не имеет корней $\lambda = \rho(\cos\theta \pm i\sin\theta)$).

Утверждение теоремы 8 называют ***принципом суперпозиции***.

Теорема 8. Пусть правая часть неоднородного соотношения $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = f(n)$ (12) является суммой некоторых последовательностей: $f(n) = \sum_{i=1}^{p} g_i(n)$, и пусть последовательность $\varphi_n^{(i)}$ есть решение неоднородного соотношения с правой частью $g_i(n), i = 1, \ldots, p$.

Тогда сумма $\theta_n = \sum_{i=1}^{p} \varphi_n^{(i)}$ является решением соотношения $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = f(n)$ (12).

// **Доказательство**. Имеем:

$$\theta_n + a_1\theta_{n-1} + \ldots + a_k\theta_{n-k} =$$

$$= \sum_{i=1}^{p} \varphi_n^{(i)} + a_1 \sum_{i=1}^{p} \varphi_{n-1}^{(i)} + \ldots + a_k \sum_{i=1}^{p} \varphi_{n-k}^{(i)} =$$

$$= \sum_{i=1}^{p} (\varphi_n^{(i)} + a_1 \varphi_{n-1}^{(i)} + \ldots + a_k \varphi_{n-k}^{(i)}) = \sum_{i=1}^{p} g_i(n) = f(n),$$

что и требовалось.

9. Понятие действия группы на множестве. Стабилизаторы и орбиты. Лемма Бернсайда (с доказательством).

// из wiki

Группа G **действует** на X, если любых $g \in G$ и $x \in X$ определено **действие элемента** g **на элемент** x (обозначаемое gx), обладающее следующими свойствами:

1. $gx \in X$,
2. Для любых $g_1, g_2 \in G, x \in X$ выполнено $(g_1 g_2)x = g_1(g_2 x)$,
3. Для любого $x \in X$ выполнено $ex = x$.

Орбита $Orb(x)$ элемента $x \in X$ — это множество $\{gx \mid g \in G\}$.

Стабилизатор $St(x)$ элемента $x \in X$ — это множество $\{g \in G \mid gx = x\}$.

// Дальше что писать, решай сам

Лемма Бернсайда вычисляет количество орбит действия группы на множестве с помощью суммы по всем элементам группы. Она применяется в том случае, когда порядок множества X намного больше, чем порядок группы G.

Теорема 2.1 (Лемма Бернсайда). *Количество орбит действия группы G на множестве X равно*

$$\frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Доказательство. Обозначим число орбит через N. Каждый элемент $x \in X$ лежит в орбите Gx. Сопоставим ему число $\frac{1}{|Gx|}$. Сумма этих чисел по всем x из данной орбиты $\mathcal{O}$ очевидно равна 1 (мы просто $|\mathcal{O}|$ раз складываем число $\frac{1}{|\mathcal{O}|}$ с самим собой). Поэтому количество орбит можно вычислить по формуле $N = \sum_{x\in X}\frac{1}{|Gx|}$. Подставляя сюда формулу для длины орбиты из леммы 1.7 получим $N = \sum_{x\in X}\frac{|\mathrm{St}(x)|}{|G|} = \frac{1}{|G|}\sum_{x\in X}|\mathrm{St}(x)|$. Используя формулу из замечания 1.6 получим $N = \frac{1}{|G|}\sum_{g\in G}|X^g|$, что и требовалось доказать. $\square$

// Доказательство взято не из лекций Белоуса, однако замечания 1.6 и лемма 1.7 у него, в принципе, приведены как утверждения. (далее ниже)

Лемма 1.7. *Длина орбиты элемента x равна индексу стабилизатора этого элемента. Поэтому, если группа G конечна, то $|Gx| \cdot |\operatorname{St}(x)| = |G|$.*

Доказательство. Напомним, что индекс подгруппы – это количество (левых) смежных классов по этой подгруппе. Пусть $G/\operatorname{St}(x)$ обозначает множество левых смежных классов. Зададим функцию $f : G/\operatorname{St}(x) \to Gx$ формулой $f\big(g\operatorname{St}(x)\big) = gx$ (очевидно, что правая часть не зависит от выбора представителя смежного класса) и докажем, что f биективна. Сюръективность сразу следует из определения орбиты. Предположим, что $f\big(g\operatorname{St}(x)\big) = f\big(h\operatorname{St}(x)\big)$, т. е. $gx = hx$. Но тогда $h^{-1}gx = x$, откуда $h^{-1}g \in \operatorname{St}(x)$, а из этого сразу следует, что $g\operatorname{St}(x) = h\operatorname{St}(x)$. Таким образом f биективно отображает $G/\operatorname{St}(x)$ на Gx, а это возможно только если $|G/\operatorname{St}(x)| = |Gx|$. □

Замечание 1.6. Обратите внимание на то, что количество пар $(g, x) \in G \times X$, для которых $gx = x$ можно вычислить двумя способами, которые указаны в разных частях следующего равенства:

$$\sum_{x\in X} |\operatorname{St}(x)| = \sum_{g\in G} |X^g|.$$

Последнее равенство несмотря на свою очевидность играет важную роль при доказательстве леммы Бернсайда. Второе ключевое соображение приведено в следующей лемме.

Определение 1.4. Неподвижными точками элемента $g \in G$ называются те $x \in X$, для которых $gx = x$. *Множество неподвижных точек* элемента g обозначается через X^g.

10. Функции разметки. Понятие эквивалентных функций разметки. Структурный перечень функций разметки.

Функции разметки

Пусть на множестве S задана функция $C:S \to R$, отображающая S в множество ***меток*** (***красок***, ***цветов***) R. Такая функция называется ***функцией разметки***, или ***функцией раскраски*** (или просто ***раскраской***). Действие группы G на множестве S стандартным образом распространяется на множество R^S всех раскрасок: $\sigma(C)(s) = C(\sigma(s))$ (для каждого $s \in S$). Эквивалентность раскрасок C, C' означает тем самым, что для некоторой подстановки σ имеет место равенство $C' = \sigma(C)$, т.е. для каждого $s \in S$ выполняется $C'(s) = C(\sigma^{-1}(s)) = \sigma^{-1} \cdot C(s)$. Число классов эквивалентности на множестве раскрасок определяется по лемме Бернсайда.

Две раскраски C и D назовем ***эквивалентными***, если одна из них переходит в другую под действием некоторого автоморфизма графа G, т. е.

$$C \sim D \Leftrightarrow (\exists h \in \operatorname{Aut} G)\Big(\big(C(v_1), \dots, C(v_n)\big) = \\ = \big(D(h(v_1)), \dots, D(h(v_n))\big)\Big).$$

Весом раскраски $C = \big(C(1), \dots, C(n)\big)$ назовем произведение

$$w(C) = w(C(1)) \cdot \ldots \cdot w(C(n))$$

весов ее значений. ***Перечнем раскрасок***[4] будем называть сумму весов всех возможных раскрасок:

$$\operatorname{Invt}\left(R^S\right) = \sum_{C \in R^S} w(C).$$

11. Циклический (цикловой) индекс группы. Теорема Пойа (с выводом числа классов эквивалентности, без доказательства утверждения о структурном перечне классов эквивалентности).

Циклический индекс группы: //Это по Белоусову

$$\sigma \in G, \sigma = x_1, x_2 \dots x_{k(\sigma)}$$

$$t_\sigma \leftrightarrow \ x_1^{q_1}, x_2^{q_2} \dots x_n^{q_n}, \qquad \text{где } x_1, x_2 \dots x_n - \text{рациональные переменные}$$

$$q_j - \text{число циклов длины } j \text{ в подстоновке } \sigma$$

$$(\forall j = \overline{1,n})(0 \le \ q_j \le n),\ q_1 + q_2 + \dots + q_n = k(\sigma)$$

$$1q_1 + 2q_2 + \dots + nq_n = n = |M|$$

$$P(x_1 x_2 \dots x_n) \leftrightarrow \frac{1}{|G|} \sum_{\sigma \in G} t_\sigma$$

//А это из wiki

Цикловой индекс подгруппы A симметрической группы S_n определяется как многочлен от n переменных $t_1, t_2, \dots, t_n$

$$Z_A(t_1, t_2, \dots, t_n) = \frac{1}{|A|} \sum_{a \in A} t_1^{j_1(a)} \cdot t_2^{j_2(a)} \cdot \dots \cdot t_n^{j_n(a)},$$

где $j_k(a)$ — число циклов длины k в перестановке a.

... поле

Структурный перечень классов экв. ф-ций разметки $Inv(C^M/\tilde{G}) \rightleftarrows \sum_{w} \alpha_w w$

α_w означает число попарно неэкв. ф-ций разметки веса w.

Теорема: $Inv(C^M/\tilde{G}) = P_G(\underbrace{w_1 + \dots w_m}_{x_1}, \underbrace{w_1^2 + \dots + w_m^2}_{x_2}, \dots, w_1^n + \dots + w_m^n)$;

$N = |C^M/\tilde{G}| = P_G(m, m, \dots m)$, где $m = |C|$, $n = |M|$

◀ $P_G(x_1, \dots, x_n) = \frac{1}{|G|} \sum_{\sigma \in G} t_\sigma$;

1) $P_G(m, \dots, m) = \frac{1}{|G|} \sum_{\sigma \in G} t_\sigma \Big|_{x_i = m} = \frac{1}{|G|} \sum_{\sigma \in G} m^{\nu(\sigma)} = \frac{1}{|G|} \sum_{\sigma \in G} \psi(\sigma) =$

$= N$ (по лемме Бернсайда)

2) $P_G(w_1 + w_m, w_1^2 + w_2^2 + \dots + w_m^2, \dots, w_1^n + w_2^n + \dots + w_m^n) =$

$= \frac{1}{|G|} \sum_{\sigma \in G} \hat{t}_\sigma = \frac{1}{|G|} \sum_{\sigma \in G} \sum_{w} \psi_w(\sigma) w =$

$= \sum_{w} \left(\frac{1}{|G|} \sum_{\sigma \in G} \psi_w(\sigma) \right) w$. Докажем, что $\alpha_w =$

$= \frac{1}{|G|} \sum_{\sigma \in G} \psi_w(\sigma)$

Это следует из того факта, что группа, действующая на мн-ве ф-ций разметки, не выводит за пределы мн-ва ф-ций любого фиксир. веса, т.к., как было доказано выше, все эквив. ф-ции разметки имеют один и тот же вес. ▶

12. **Приложение для рекуррентных соотношений.**

Более точно, алгебраическое уравнение

$$\lambda^r + c_1\lambda^{r-1} + \ldots + c_{r-1}\lambda + c_r = 0 \tag{2.7}$$

называется ***характеристическим уравнением*** соотношения (2.6). Предположим, что найдены все r корней этого уравнения, включая комплексные (при этом каждый корень учитывается столько раз, какова его кратность). Для построения базиса в пространстве решений можно использовать следующие правила.

1. Если $\lambda = \alpha$ – вещественный корень кратности s уравнения (2.7), то ему отвечают s линейно независимых частных решений:

$$\varphi_n^{(1)} = \alpha^n, \quad \varphi_n^{(2)} = n\alpha^n, \quad \ldots, \quad \varphi_n^{(s)} = n^{s-1}\alpha^n.$$

2. Если $\lambda = \alpha \pm i\beta$ – пара комплексно сопряженных корней уравнения (2.7) кратности s каждый, то им отвечают $2s$ линейно независимых частных решений

$$\varphi_n^{(1)} = \rho^n\cos(n\theta),\ \varphi_n^{(3)} = n\rho^n\cos(n\theta),\ \ldots,\ \varphi_n^{(2s-1)} = n^{s-1}\rho^n\cos(n\theta),$$
$$\varphi_n^{(2)} = \rho^n\sin(n\theta),\ \varphi_n^{(4)} = n\rho^n\sin(n\theta),\ \ldots,\ \varphi_n^{(2s)} = n^{s-1}\rho^n\sin(n\theta),$$

где $\rho = |\alpha + i\beta|$, $\theta = \arg(\alpha + i\beta)$.

При решении задач для нахождения частного решения удобно использовать следующие правила.

1. Если $b_n = \alpha^n P_k(n)$, где $P_k(n)$ – многочлен степени k, то частное решение соотношения (2.3) следует искать в виде

$$x_n = n^s \alpha^n \tilde{P}_k(n),$$

где $\tilde{P}_k(n)$ – многочлен степени k с неопределенными коэффициентами; s – кратность корня $\lambda = \alpha$ характеристического уравнения для соответствующего однородного соотношения ($s = 0$, если оно не имеет корня $\lambda = \alpha$).

2. Если $b_n = \rho^n \big(P_k(n)\cos(n\theta) + Q_l(n)\sin(n\theta)\big)$, где $P_k(n)$, $Q_l(n)$ – многочлены степени k и l соответственно, то частное решение соотношения (2.3) следует искать в виде

$$x_n = n^s \rho^n \left(\tilde{P}_N(n)\cos(n\theta) + \tilde{Q}_N(n)\sin(n\theta)\right),$$

где $\tilde{P}_N(n), \tilde{Q}_N(n)$ – многочлены степени N с неопределенными коэффициентами, $N = \max\{k, l\}$; s – кратность каждого из корней $\lambda = \rho\,(\cos\theta \pm i\sin\theta)$ характеристического уравнения для соответствующего однородного соотношения ($s = 0$, если оно не имеет корней $\lambda = \rho\,(\cos\theta \pm i\sin\theta)$).