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

~~~ ~~~

• Множество – совокупность объектов, заданных перечислением ($A = \{4,8,15,16,23,42\}$), или указанием какого-либо их общего свойства, называемым коллективизирующим ($B = \{x \in \mathbb{R}, x \geq 0\}$). Множество называется пустым, если оно не содержит элементов

• Пусть A и B множества. Тогда A является подмножеством B, если любой элемент из A является элементом B. A равно B, если любой элемент из A является элементом B и наоборот.

• Пусть $A, B \subseteq U$ (универсум). По определению,

- пересечение $A \cap B = \{x \in U: \ x \in A, x \in B\}$;
- объединение $A \cup B = \{x \in U: \ x \in A \ \vee \ x \in B\}$; *//логическое или, дизъюнкция*
- разность $A/B = \{x \in U: \ x \in A, x \notin B\}$
- симметрическая разность $A\Delta B = \{(A/B) \cup (B/A)\}$
- дополнение $\bar{A} = U/A$

• Теоретико-множественными тождествами называют равенства $A \cup B = B \cup A, \ A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ и т.п., верные для любых входящих в них множеств. Доказать эти равенства можно

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

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

~~~ ~~~

• Пусть A и B – произвольные множества.

Неупорядоченной парой на множествах A и B называется любое множество $\{a, b\}$, где $a \in A, \ b \in B$ или $a \in B, b \in A$. Если A=B, то говорят о неупорядоченной паре на множестве A.

Упорядоченная пара (a,b) на множествах A и B определяется не только самимим элементами $a \in A, \ b \in B,$ но и порядком, в котором они записаны.

Кортеж (упорядоченный n-набор) $(a_1, \dots, a_n)$ на множествах $A_1, \dots, A_n$ характеризуется не только входящими в него элементами $a_1 \in A_1, \dots a_n \in A_n$, но и порядком, в котором они перечисляются; кортеж является обобщением понятия упорядоченной пары.

• Множество всех кортежей длины n на множествах $(A_1, \dots, A_n)$ называют декартовым произведением этих множеств и обозначают как $A_1 \times \dots \times A_n$. Если все множества $A_i, \ i = \overline{1,n}$ равны между собой, то декартово произведение называют n-й декартовой степенью множества A.

I.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.

Множество всех $y \in B$ таких, что найдётся $x \in A$, для которого $y = f(x)$ называют областью значений отображения f, R(f).

• Отображение $f: A \to B$ называют:

- инъективным, если каждый элемент из области его значений имеет единственный прообраз, т.е. из равенства $f(x1) = f(x2)$ следует равенство x1=x2.
- сюръективным, если его область значений совпадает со всем множеством B (сюръективное отображением ИЗ A в B называют также отображением A НА B).
- биективным, если оно одновременно инъективно и сюръективно – т.е. каждому элементу множества A отвечает единственный элемент множества B и наоборот.

• Отображение называется частичным, если образ определен не для каждого элемента множества A, а для некоторых элементов этого множества.

I.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.*

~~~ ~~~

• 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.

• График соответствия p из множества A в множество B можно определить как множество C_p упорядоченных пар (x,y) таких, что $x \in A, y \in B$ и элементы x,y связаны соответствием p, т.е. $y \in p(x)$.

Область определения соответствия $\rho \subseteq A \times B$ из множества A в B – это множество всех первых компонент упорядоченных пар из ρ, $D(\rho) = \{x: (\exists y \in B)(x, y) \in \rho\}$. Область значения соответствия – множество всех вторых компонент упорядоченных пар, $R(\rho) = \{y: (\exists x \in A)(x, y) \in \rho\}$.

• Сечением соответствия p для фиксированного элемента $x \in A$ называется множество $\rho(x) = \{y: (x, y) \in \rho\}$; сечение соответствия p(x) есть множество всех образов элемента x при данном соответствии. Сечением соответствия по множеству $C \subseteq A$ называется множество $\rho(C) = \{y: (x, y) \in \rho, x \in C\}$.

• Соответствие $\rho \subseteq A \times B$ называется функциональным по первой компоненте, если для любых двух упорядоченных пар $(x, y) \in \rho$, $(x', y') \in \rho$ из равенства y=y' следует равенство x=x'; функциональным по второй компоненте, если из x=x' следует y=y'. *(//1 – два x не могут вести в один y, 2 – один x не может вести в два y).*

• n-арным отношением на множествах $A_1, \dots, A_n$ называют произвольное подмножество ρ декартова произведения $A_1 \times \dots \times A_n$; в случае n=2 говорят о бинарном отношении на множествах A1 и A2 – соответствии из A1 в A2, где эти множества в общем случае различны.

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

~~~ ~~~

Композицией соответствий $\rho \subseteq A \times B$ и $\sigma \subseteq B \times C$ называют соответствие $\rho \circ \sigma = \{ (\exists z \in B)\big((x,z) \in \rho\big) \wedge \big((z,y) \in \sigma\big) \}$. Соответствие, обратное соответствию $\rho \subseteq A \times B$, есть соответствие из B в A, обозначаемое $\rho^{-1} = \{(y,x) : (x,y) \in \rho\}$.

Основные свойства:

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

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 $(x,y) \in (\rho \circ \tau)$, $\Longrightarrow$
$(x,y) \in (\rho \circ \sigma) \cup (\rho \circ \tau)$ - включение доказано. *//в обратную сторону аналогично, и аналогично же для всего остального, ну вы пони*

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

~~~ ~~~

Бинарное отношение ρ на множестве A называют:

1) Рефлексивным, если $\forall x \in A\ (x,x) \in \rho$ $id_A \subseteq \rho$
2) Иррефлексивным, если $\forall x \in A\ (x,x) \notin \rho$ $id_A \cap \rho = \emptyset$
3) Симметричным, если для любых $x, y \in A$ из $x\ \rho\ y$ следует $y\ \rho\ x$ $\rho^{-1} = \rho$
4) Антисимметричным, если для любых $x, y \in A$ из $x\ \rho\ y$ и $y\ \rho\ x$ следует, что $x = y$ $\rho^{-1} \cap \rho \subseteq id_A$
5) Транзитивным, если для любых $x, y, z \in A$ из $x\ \rho\ y$ и $y\ \rho\ z$, следует $x\ \rho\ z$ $\rho \circ \rho \subseteq \rho$

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

~~~ ~~~

Бинарное отношение на *некотором* множестве называют:

1) Эквивалентностью, если оно рефлексивно, симметрично и транзитивно; (P _ C _ T)
2) Толерантностью, если оно рефлексивно и симметрично; (P _ C _ _)
3) Порядком, если оно рефлексивно, антисимметрично и транзитивно; (P _ _ A T)
4) Предпорядком, если оно рефлексивно и транзитивно; (P _ _ _ T)
5) Строгим порядком, если оно иррефлексивно, антисимметрично и транзитивно. (_ И _ A T)

I.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 A, и $x \in A$. Классом эквивалентности по отношению ρ называется множество элементов $\{y : y \in A,\ y\ \rho\ x\}$ (эквивалентных x); класс эквивалентности обозначается $[x]_\rho$.

• Фактор-множеством множества A по отношению ρ (обозначается A/ρ) называют множество всех классов эквивалентности по данному отношению на данном множестве.

I.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 M вместе с заданным на нем отношением порядка $\leq$; элементы x и y упорядоченного множества $(M, \leq)$ называют сравнимыми, если $x \leq y$ или $y \leq x$, и несравнимыми в противном случае.

Пусть $(A, \leq)$ – упорядоченное множество. Элемент $a \in A$ называют:

1) наибольшим элементом множества A, если $\forall x \in A\ \ x \leq a$;
2) максимальным элементом множества A, если $\forall x \in A\ \ x \leq a$ или x и a не сравнимы
3) наименьшим, если $\forall x \in A\ \ a \leq x$;
4) минимальным, если $\forall x \in A\ \ a \leq x$ 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 $x \in B$ $x \leq a$ (или соответственно $(a \leq x)$). 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) *//sup, /b/*

I.10
~~~

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

~~~ ~~~

• n-арной операцией на множестве A называется любое отображение $\omega: A^n \to A$; n-арная операция ω каждому кортежу $(a_1, \dots, a_n) \in A^n$ 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 (A_1, Ω_1) и (A_2, Ω_2) называются однотипными, если существует такая биекция Ω_1 на Ω_2, при которой n-арная операция из Ω_1для любого n переходит в n-арную из Ω_2.

• Примеры: $\left(2^M, \{\cup, \cap, /, \Delta, \bar{}, \emptyset, M\}\right)$: 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 $\mathcal{A}_1 = (2^M, \cup, \cap, \emptyset, M)$ и $\mathcal{A}_2 = (\mathbb{R}, +, \bullet, 0, 1)$ являются однотипными; биекцию между их сигнатурами, сохраняющую арность операций, можно определить как $\cup \to +,\ \cap \to *,\ \emptyset \to 0,\ M \to 1$.

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

~~~ ~~~

• *Группоидом* называют произвольную алгебру $\mathcal{G} = (G, \bullet)$ сигнатура которой состоит из одной бинарной операции (ограничений на операцию нет). Группоид $\mathcal{G}$ называют *полугруппой*, если его операция ассоциативна $(\forall a, b, c \in G\ \ a \bullet (b \bullet c) = (a \bullet b) \bullet c)$. Группоид называют *моноидом*, если его операция ассоциативна и относительно неё существует нейтральный элемент (единица моноида). Группоид называют *группой*, если его операция ассоциативна, относительно нее существует нейтральный элемент, и $(\forall x \in G)$ существует обратный элемент по данной операции.

• Для левого и правого нейтральных элементов 1' и 1", если они существуют, выполннены равенства $1' = 1' * 1'' = 1''$ - т.е. они совпадают; единица моноида определена однозначно. Элемент $x' \in G$ называют обратным к элементу $x \in G$ по операции •, если $x \bullet x' = x' \bullet x = 1$.

• Пусть в группе $(G, *)$ с единицей 1 для некоторого a существуют элементы a', a", обратные ему. Тогда $a' = a' * 1$, и т.к. $1 = a * a''$, то $a' = a' * (a * a'') = (a' * a) * a'' = a''$. Обратный элемент определен однозначно.

I.13 I.14 I.15

I.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 вмете 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 $(\mathbb{N}_0, +)$. Подмножество всех положительных четных чисел замкнуто относительно сложения, поэтому на нем может быть определена подполугруппа *полугруппы* $(\mathbb{N}_0, +)$. 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* $(\mathbb{N}_0, +, 0)$, 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 $\mathcal{R}$. Аналогично дается определение подполя какого-либо поля (добавляется условие содержания в Q обратного элемента по умножению)

I.17
~~~

I.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.

I.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;

$\forall a \in S, \forall X = \{x_n \in S\}_{n\in\mathbb{N}}$ $a \sup X = \sup aX$, $(\sup X)a = \sup(Xa)$.

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

Пример: $\mathcal{B} = (\{0,1\}, +, *, 0, 1)$ – идемпотентное полукольцо. $\sup \mathcal{B} = 1$, 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 $0^* = 0^0 + 0^1 + \cdots + 0^K + \cdots = 1 + 0 + \cdots + 0 + \cdots = 1$.

I.20 I.21

\- \- \- \- \- \- \- \- \- \- \- \- \- \-

II.1 *Основные понятия теории графов: неориентированные и ориентированные графы(276), цепи, пути, циклы, контуры, маршруты. Подграфы.(286).*

~~~ ~~~

• - Неориентированный граф G задается двумя множествами $G = (V, E)$, где V – конечное множество вершин (узлов), E – множество *неупорядоченных* пар на V, элементы которого называют ребрами.

- Ориентированный граф G задается двмя множествами $G = (V, E)$, где V – конечное множество вершин (узлов), E – множество *упорядоченных* пар на V, элементами которого называют дугами.

- Цепь в *неориентированном* графе – последовательность вершин $v_0, v_1, \ldots, v_n, \ldots$ такая, что $v_i - v_{i+1}$ (вершины соединены ребром) для любого i, если v_{i+1} существует. *//на деле тут не –, а |–|, такое тире с короткими палочками на концах*

- Путь в *ориентированном* графе – последовательность вершин $v_0, v_1, \ldots, v_n, \ldots$ такая, что $v_i \to v_{i+1}$ (из вершины в вершину ведет дуга) для любого i, если v_{i+1} существует.

Простая – цепь, все вершины которой, кроме быть может первой и последней, попарно различны и все ребра попарно различны. Простой – путь, все вершины которого, кроме быть может первой и последней, попарно различны.

- Цикл (контур) – простая цепь (путь) ненулевой длины с совпадающими концами (началом и концом).

- Маршрутом в графе (ориентированном) $G = (V, E)$ называется последовательность вершин и рёбер (дуг) вида $v_0, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v_n$, где $v_i \in V, i \in [0, n]$, $e_i \in E$, где ребра (дуги) e_i связывают вершины v_{i-1} и v_i. *//определение взято наполовину из вики, наполовину из здравого смысла, я вообще не уверен что Белоусов это давал…*

• Граф $G_1 = (V_1, E_1)$ называют подграфом графа $G = (V, E)$, если $V_1 \subseteq V$, $E_1 \subseteq E$.

II.2 *Связность неориентированного графа. Компоненты связности.*

~~~ ~~~

• Неориентированный граф называют связным, если любые две его вершины соединены цепью.

• Граф $G_1 = (V_1, E_1)$ называют подграфом графа $G = (V, E)$, если $V_1 \subseteq V$, $E_1 \subseteq E$; если хотя бы одно из включений строгое, то G_1 называют **собственным** подграфом G. Подграф $G_1 \subseteq G$ называют максимальным подграфом по свойству P, если он не является собственным подграфом никакого другого подграфа графа G, обладающего свойством P. Компонента связности графа – его максимальный *связный* подграф.

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

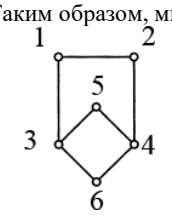
~~~ ~~~

• Ориентированный граф называют связным, если для любых двух его вершин u,v вершина v достижима из u ИЛИ u достижима из v. Ориентированный граф называют сильно связным, если для любых двух его вершин u и v вершина v достижима из u И u достижима из v.

• Граф $G_1 = (V_1, E_1)$ называют подграфом графа $G = (V, E)$, если $V_1 \subseteq V$, $E_1 \subseteq E$; если хотя бы одно из включений строгое, то G_1 называют **собственным** подграфом G. Подграф $G_1 \subseteq G$ называют максимальным подграфом по свойству P, если он не является собственным подграфом никакого другого подграфа графа G, обладающего свойством P. Компонента связности графа (любого) – его максимальный *связный* подграф. Бикомпонента ориентированного графа – его максимальный сильно связный подграф.

II.4 II.5 II.6 II.7 II.8
~~~

II.9 *Изоморфизм графов. (342) Группа автоморфизмов графа и ее вычисление.*

~~~ ~~~

• Пусть даны графы $G_1 = (V_1, E_1),\ G_2 = (V_2, E_2)$. Отображение $h: V_1 \to V_2$ называют изоморфизмом, если оно биективно и сохраняет отношение смежности, $(\forall\, u, v \in V)\big(u\ \rho_1\ v \iff h(u)\ \rho_2\ h(v)\big)$. Изоморфизм графа на себя называют автоморфизмом.

• Композиция любых двух автоморфизмов графа есть автоморфизм; подстановка, обратная к автоморфизму также является автоморфизмом. Таким образом, множество всех автоморфизмов графа образует группу по операции композиции, называемую группой автоморфизмов графа.



Для графа, изображенного на рисунке, группу автоморфизмов образуют подстановки e, (3 4)(1 2), (5 6) и их композиция (3 4)(1 2)(5 6).

II.10

II.11 *Алфавит, слово, язык. (462) Операции над языками(469), полукольцо всех языков в заданном алфавите и его замкнутость.*

~~~ ~~~

• - Алфавит – произвольное непустое конечное множество $V = \{a_1, \dots, a_n\}$, элементы которого называют буквами или символами.

- Словом или цепочкой в алфавите V называют произвольный кортеж из множества V^k для различных k; при k=0 получаем пустой кортеж, называемый пустым словом λ.

- Языком в алфавите V называется произвольное подмножество множества всех слов V^* в алфавите V.

• - Над языками допустимы все теоретико-множественные операции: объединение, пересечение, разность, симметрическая разность, дополнение ($\overline{L} = V^*/L$).

- Соединением языков L1, L2 называют язык L1L2, состоящий из всех возможных соединений слов xy, в которых слово x принадлежит первому, а слово y второму языку; $L_1L_2 = \{xy : x \in L_1, y \in L_2\}$

- Итерацией языка L называют объединение всех его степеней, $L^* = \{\lambda\} + L + L^2 + L^3 + \cdots$.

• Алгебра $\mathbb{L}(V) = \big(2^{V^*}, \cup, *, \emptyset, \{\lambda\}\big)$ является замкнутым полукольцом. Аксиомы полукольца проверяются непосредственно; замкнутость полукольца следует из существования объединения любого семейства множеств, служащего точной верхней гранью этого семейства (относительно операции включения), а также из тождеств $L(\bigcup_{i\in I} P_i) = (\bigcup_{i\in I} LP_i),\ \ (\bigcup_{i\in I} P_i)L = \bigcup_{i\in I} P_iL$.

II.12 *Регулярные языки и регулярные выражения. (490) Полукольцо регулярных языков как полукольцо с итерацией (не являющееся замкнутым).*

~~~ ~~~

• Среди всех языков в алфавите V выделяют множество регулярных языков. База: языки $\emptyset, \{\lambda\}, \{a\}$ – регулярные. Если L_1, L_2 – регулярные языки в алфавите V, то регулярны также будут их объединение, соединение и итерация. Других регулярных языков в алфавите V нет.

Регулярное выражение – слово, обозначающее регулярный язык. Регулярные выражения $\emptyset, \lambda, a$ обозначают соответственно языки $\emptyset, \{\lambda\}, \{a\}$. Если $\alpha \longmapsto K, \beta \longmapsto L,$ то $(\alpha \cup \beta) \longmapsto K \cup L;\ \ (\alpha\beta) \longmapsto K * L;\ \ \alpha^* \longmapsto K^*,\ \ \alpha^+ \longmapsto K^+$.

• Множество регулярных языков R_V в алфавите Vобразует полукольцо $\mathcal{R} = (R_V, \cup, *, \emptyset, \{\lambda\})$ – незамкнутое полукольцо с итерацией (являющееся подполукольцом замкнутого полукольца, и вместе с каждым своим элементом содержащее его итерацию).

II.13 *Понятие конечного автомата (КА) и языка, допускаемого КА(502,8). Анализ и синтез КА. (518)*

~~~ ~~~

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

1) на функцию разметки ϕ: $E \to R(V)$ наложены ограничения: $\phi(e) \neq \emptyset;\ \ \phi(e) = \{\lambda\}$ или $\phi(e) \subseteq V$
2) задана вершина $q_0 \in Q$, называемая входной
3) задано множество вершин F, называемых заключительными

КА допускает цепочку x, если она читается на некотором пути, ведущем из начальной вершины в одну из заключительных. Язык, допускаемый КА – множество всех допустимых им цепочек.

• Для КА существует две задачи – анализа (для данного КА найти допускаемый им язык) и синтеза (для данного регулярного языка построить допускающий его КА).

II.14

II.15 *Детерминизация и минимизация КА(521,31). Регулярность дополнения регулярного языка и пересечения двух регулярных языков(526). Проблемы пустоты и эквивалентности. (531)*

~~~ ~~~

• КА называют детерминированным, если: в нем нет λ -переходов, и из каждого состояния по любому символу возможен переход только в одно состояние. КА M1 и M2 называют эквивалентными, если они допускают один и тот же язык.

Для любого конечного автомата может быть построен эквивалентный ему детерминированный КА. Детерминизация происходит в два этапа – на первом происходит удаление из автомата лямбда-переходов, на втором непосредственно детерминизация (например с помощью метода вытягивания).

Если дан КА $M = (V, Q, q_0, F, \delta)$без λ -переходов, то детерминированный $M' = (V, Q', q_0', F', \delta')$, где $Q' = 2^Q, q_0' = \{q_0\},\ \ F' = \{T : T \cap F = \emptyset\}$, $\delta'(S, a) = \bigcup_{q\in S} \delta(q, a)$.

В свою очередь, для любого детерминированного КА может быть построен эквивалентный ему детерминированный КА с минимальным числом состояний. Минимизация происходит за счет «группировки» состояний в классы эквивалентности.

• Пусть даны два регулярных языка L1 и L2. Тогда регулярными языками также будут их дополнения ($\overline{L} = V^*/L$), пересечение $\big(L1 \cap L2 = \overline{\overline{L1} \cup \overline{L2}}\big)$, разность $(L1/L2 = L1 \cap \overline{L2})$ и симметрическая разность $\big(L1\Delta L2 = (L1/L2) \cup (L2/L1)\big)$

• Проблема пустоты: дан КА, необходимо выяснить, не является ли пустым язык, который он допускает. Проблема эквивалентности: для двух заданных КА M1 и M2 необходимо проверить, являются ли они эквивалентными, т.е. совпадают ли допускемые ими языки.

II.16

- - - - - - - - - - - - - -
~~~

III.1 *Формулы включения и исключения (с выводом). (10)*

~~~ ~~~

Даны конечные множества $A_1 \dots A_n \subseteq U, n \geq 1$.

• Докажем, что $|A_1 \cup \dots \cup A_n| = \sum_{k=1}^{n}[(-1)^{k+1} \sum_{i1<\dots<ik}|A_{i1} \cap \dots \cap A_{ik}|]$ (формула включения). Пусть а принадлежит ровно p множествам из n. Тогда во внутренней сумме при фиксированном числе k, а встречается C_p^k раз (//размещение из p по к), а во всей правой части равенства - $\sum_{k=1}^{p}\left[(-1)^{k+1}C_p^k\right]$. Можно представить $0 = (1-1)^p$, по биному Ньютона получаем что $0 = \sum_{k=0}^{p}\left[(-1)^k C_p^k\right] = 1 + \sum_{k=1}^{p}(-1)^k C_p^k = 1 - \sum_{k=1}^{p}(-1)^{k+1}C_p^k$. Следовательно, $\sum_{k=1}^{p}\left[(-1)^{k+1}C_p^k\right] = 1$. Следовательно, ЛЮБОЙ элемент $a \in A_1 \cup \dots \cup A_n$ встречается в правой части равенства ровно один раз – формула верна.

• $|\overline{A_1 \cup \dots \cup A_n}| = |U| - \sum_{k=1}^{n}[(-1)^k \sum_{i1<\dots<ik}|A_{i1} \cap \dots \cap A_{ik}|]$ (формула исключения).

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

~~~ ~~~

• Пусть даны два множества $A = \{a_1 \dots a_m\}, B = \{b_1 \dots b_n\}$. Найдем число сюръекций из A на B ($m \geq n$).

Обозначим $W_i = \{f: f \in B^A,\ b_i \notin R(f)\},\ |W_i| = (n-1)^m$. При фиксированном k $|W_{i1} \cap \dots \cap W_{ik}| = (n-k)^m$ (при фиксированных индексах ij). $|W_1 \cup \dots \cup W_n| = \sum_{k=1}^{n}[(-1)^{k+1} \sum_{i1<\dots<ik} |W_{i1} \cap \dots \cap W_{ik}|] = \sum_{k=1}^{n}[(-1)^{k+1}C_n^k(n-k)^m]$ – число отображений, не являющихся сюръективными. Следовательно Число сюръекций будет равно $N = n^m - \sum_{k=1}^{n}[(-1)^{k+1}C_n^k(n-k)^m] = n^m + \sum_{k=1}^{n}[(-1)^k C_n^k(n-k)^m] = \sum_{k=0}^{n}[(-1)^k C_n^k(n-k)^m]$.

III.3 III.4 III.5 III.6

III.7 *Характеристический полином и характеристическое уравнение ОЛРС. Структура общего решения в случае вещественных и комплексных корней характеристического полинома. (22)*

~~~ ~~~

• Характеристическим уравнением однородной ЛРС (**1**) $x_n + a_1 x_{n-1} + \dots + a_k x_{n-k} = 0$ называют уравнение вида (**2**) $\lambda^k + a_1\lambda^{k-1} + \dots + a_{k-1}\lambda + a_k = 0$. Характеристическим полиномом называют левую часть этого уравнения.

• Пусть все корни λ характеристического уравнения (2) действительны, среди них есть корни кратности s. Тогда каждому корню λ_0 кратности S соответствуют S ЛНЗ последовательностей $\phi_n^{(1)} = \lambda_0^n,\ \phi_n^{(2)} = n\lambda_0^n, \dots\ ,\ \phi_n^{(s)} = n^{s-1}\lambda_0^n$; общее решение $x_n^{\text{общ}} = \sum_{i=1}^{k} C_i \phi_n^{(i)}$.

Пусть среди корней λ есть комплексно-сопряженные корни $\lambda_{1,2} = \rho e^{\pm i\phi}$ кратности S. Тогда каждой паре корней $\lambda_{1,2}$ соответствует 2S ЛНЗ последовательностей $\phi_n^{(1)} = \rho^n \cos n\phi, \dots, \phi_n^{(s)} = n^{s-1}\rho^n \cos n\phi, \phi_n^{(s+1)} = \rho^n \sin n\phi, \dots,$
$\phi_n^{(2s)} = n^{s-1}\rho^n \sin n\phi$.

//примеры:

$x_n - 4x_{n-1} + 4x_{n-2} = 0, \quad \lambda^2 - 4\lambda + 4 = 0, \quad \lambda_{1,2} = 2,$
$x_n^{\text{общ}} = C_1 2^n + C_2 n 2^n$

$x_n + 8x_{n-4} + 16x_{n-8} = 0, \quad \lambda^8 + 8\lambda^4 + 16 = 0, \quad \lambda_{1..8} = \sqrt[4]{-4} = \sqrt[2]{2}e^{\frac{i(\pi+2\pi k)}{4}}, \quad \lambda_{1,2} = \sqrt{2}e^{\pm i\frac{\pi}{4}}, s = 2, \quad \lambda_{3,4} = \sqrt{2}e^{\pm i\frac{3\pi}{4}}, s = 2,$
$x_n^{\text{общ}} = \left(\sqrt{2}\right)^n C_1 \cos\frac{n\pi}{4} + \left(\sqrt{2}\right)^n C_2 n \cos\frac{n\pi}{4} + \left(\sqrt{2}\right)^n C_3 \sin\frac{n\pi}{4} + \left(\sqrt{2}\right)^n C_4 n \sin\frac{n\pi}{4} + \left(\sqrt{2}\right)^n C_5 \cos\frac{3n\pi}{4} + \left(\sqrt{2}\right)^n C_6 \cos\frac{3n\pi}{4} + \left(\sqrt{2}\right)^n C_7 \sin\frac{3n\pi}{4} + \left(\sqrt{2}\right)^n C_8 n \sin\frac{3n\pi}{4}$.

III.8 III.9

III.10 *Функции разметки. (41) Понятие эквивалентных функций разметки. (41) Структурный перечень функций разметки. (42)*

~~~ ~~~

• Пусть задано некоторое конечное множество S (например множество вершин графа), подгруппа $H \subseteq \mathcal{S}_S$ симметрической группы множества S, и некое множество цветов $R = \{r_1, \dots r_m\}$. Функцией разметки (раскраской графа) называется отображение вида $C: S \to R$, сопоставляющее каждой вершине графа цвет из множества R. Если элементы S пронумерованы, то функцию разметки можно задать кортежем $C = (C(1), \dots, C(n))$.

• Две функции разметки C и D называют эквивалентными, если одна из них переводится в другую некоторой подстановкой $h \in H$.

• Пусть каждому цвету $r \in R$ поставлена в соответствие переменная $w(r)$, называемая весом цвета r. Весом раскраски $C = \big(C(1), \dots, C(n)\big)$ называют произведение $w(C) = w\big(C(1)\big) * \dots * w\big(C(n)\big)$.

Перечнем цветов будем называть сумму весов всех цветов: $Invt(R) = \sum_{r \in R} w(r)$, перечнем раскрасок – сумму весов всех возможных раскрасок $Invt(R^S) = \sum_{C \in R^S} w(C)$

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

~~~ ~~~

• Последовательность $\{x_i\}_{i\in N}$ элементов упорядоченного множества $\mathcal{A} = (A, \leq)$ называют неубывающей, если $\forall i \in \mathbb{N}\ x_i \leq x_{i+1}$. Элемент a упорядоченного множества $\mathcal{A}$ называют точной верхней гранью последовательности $\{x_i\}_{i\in N}$, если он есть точная верхняя грань множества всех членов этой последовательности.

• 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 $f: A \to B$ называется непрерывным, если справедливо равенство $f(\sup a_n) = \sup f(a_n)$. Элемент $a \in A$ называют неподвижной точкой отображения $f: A \to A$, если $f(a) = a$. Элемент a называют наименьшей неподвижной точкой отображения, если он является наименьшим элементом множества всех неподвижных точек отображения.

Теорема: любое непрерывное отображение f индуктивно упорядоченного множества $(M, \leq)$ $f: M \to M$ имеет наименьшую неподвижную точку.

Доказательство: Пусть $\mathbb{O}$ – наименьший элемент ИндуктивноУпорядоченногоМножества *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 $f^n(\mathbb{O}) \leq f^{n+1}(\mathbb{O})\ \forall n \leq k$. $f^{k+1}(\mathbb{O}) = f\left(f^k(\mathbb{O})\right) \leq f\left(f^{k+1}(\mathbb{O})\right)$, 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 $f(a) = f(\sup f^n(\mathbb{O})) = \underset{n\geq 0}{\sup}\left(f^{n+1}(\mathbb{O})\right) = \underset{n\geq 1}{\sup} f^n(\mathbb{O}) = a$. Таким образом, f(a)=a, т.е. a – неподвижная точка.

Пусть теперь f(b)=b. $\mathbb{O} \leq b, \Longrightarrow f(\mathbb{O}) \leq f(b) = b,\ f(f(\mathbb{O})) \leq f(f(b)) = b, \dots .\ (\forall n \geq 0)\ (f^n(\mathbb{O}) \leq b)$ – значит b является верхней гранью последовательности $\{f^n(\mathbb{O})\}_{n\geq 0}$. Однако a – ТОЧНАЯ верхняя грань этой последовательности, поэтому $a \leq b$.

• Пример: рассмотрим уравнение $f(x) = \frac{1}{2}x + \frac{1}{4}$ на ИУМ $A = [0; 1]$ с естественным числовым порядком. Для данного множества наименьшим элементом является 0. Последовательно вычисляя $f^0(0) = 0, f(0) = \frac{1}{4}, f(f(0) = \frac{1}{2} * \frac{1}{4} + \frac{1}{4} = \frac{3}{8}, f^3(0) = \frac{7}{16}, \dots$, получаем последовательность приближений к наименьшей неподвижной точке. $f^n(0) = \frac{2^n-1}{2^{n+1}}$, и предел $\lim\limits_{n\to+\infty} f^n(0) = \frac{1}{2}$. Следовательно, наименьшая неподвижная точка отображения f, определяемого правой частью уравнения, равна ½.

I.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.*

~~~ ~~~

• Полугруппу (в частности – группу) $(A, *)$ называют циклической, если существует такой элемент a, что любой элемент x полугруппы является некоторой целой степенью элемента a, который называют образующим элементом полугруппы (группы).

• Пример: полугруппа $(\mathbb{N}, +)$ является циклической, образующий элемент: 1 (также бесконечная - $\forall n\ \ 1^n$ попарно различны). Возведение элемента a в положительную степень n есть сумма n этих элементов, что можно записать как n*a. Группа вычетов по модулю 3 $(\mathbb{Z}_3, +, 0)$ также циклическая; любой ее ненулевой элемент является образующим.

• Группа называется конечной, если ее носитель – конечное множество; порядком конечной группы называют количество элементов в ней. Порядок элемента a циклической группы – наименьшее положительное число n такое, что $a^n = 1$.

• **Теорема:** Порядок образующего элемента конечной циклической группы равен порядку самой этой группы

Доказательство: Пусть $(G, *, 1)$ – конечная циклическая группа с образующим элементом a, n>0 – порядок этого элемента. Тогда все степени $a^0 = 1, a^1 = a, \dots a^{n-1}$ – попарно различны. Если бы $a^k = a^l, o < l < k < n$, то $a^{k-l} = a^{k+(-l)} = a^k a^{-l} = a^l a^{-l} = 1$ – существовала бы степень, меньшая n, при возведении в которую элемента a получится единица..

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

I.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) $\forall a \in R\ \exists(-a)\colon\ a + (-a) = 0$
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 $Z_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$ с операциями сложения по модулю к и умножения по модулю к.

• **Теорема:** 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: 1) для произвольного a, $a + 0a = 1a + 0a = (1 + 0)a = 1a = a$. $a + 0a = a$ можно рассматривать как уравнение относительно неизвестного 0a: $0a = a - a = 0$. Тождество a0=0 доказывается аналогично.

2) Докажем $-(ab) = a(-b)$: $a(-b) + ab = a\big((-b) + b\big) = a0 = 0$. Отсюда $a(-b) = -(ab)$. Аналогично доказывается $(-a)b = -(ab)$.

3) Рассмотрим $(a - b)c = ac - bc$. С учетом доказанного выше, $a(b - c) = a\big(b + (-c)\big) = ab + a(-c) = ab - ac$. Второе тождество доказывается аналогично.
~~~

I.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: $\forall a \neq 0 \in R,\ \exists a^{-1}\colon\ a * a^{-1} = 1;\quad a * b = b * a.$

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: 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.

Фиксируем произвольный $a \neq 0$ и определим отображение f_a множества всех ненулевых элементов в себя: $f_a(x) = a * x$. Это отображение будет инъекцией – из равенства $a * x = a * y$ следует $a * (x - y) = 0$; ввиду отсутствия делителей нуля получаем что $x - y = 0;\quad x = y$. 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. *//а я так вообще не буду писать кружки и индексы – думай сам, тут всё просто!*

$\begin{cases} x_1 \oplus_5 2x_2 \oplus_5 3x_3 = 1 \\ 2x_1 \oplus_5 2x_2 \oplus_5 4x_3 = 3 \\ 4x_1 \oplus_5 3x_2 \oplus_5 x_3 = 0 \end{cases}$ Домножим первую строку на 3, прибавим ее к 2 строке:

$(3+2)x_1 + (3*2+2)x_2 + (3*3+4)x_3 = 3+3$. В итоге имеем $0 * x_1 + 3x_2 + 3x_3 = 1$. Прибавив к третьей строке первую, получим $(1+4)x_1 + (2+3)x_2 + (3+1)x_3 = 1$, откуда $4x_3 = 1$. Система привелась к виду $\begin{cases} x_1 + 2x_2 + 3x_3 = 1 \\ 3x_2 + 3x_3 = 1 \\ 4x_3 = 1. \end{cases}$. Из последнего уравнения находим $x_3 = 4^{-1} * 1 = 4 * 1 = 4$. Подставив $x_3 = 4$ во второе уравнение будем иметь

$3x_2 + 3 * 4 = 1$, т.е. $3x_2 = 1 + (-2) = -1 = 4$. Отсюда $x_2 = 3^{-1} * 4 = 2 * 4 = 3$. Из первого и второго уравнения после подстановки найденных значений переменных получим $x_1 + 2 * 3 + 3 * 4 = 1,\ \ x_1 + 1 + 2 = 1,\ \ x_1 = -2 = 3$.

I.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.

I.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.

Доказательство: Для случая x=ax+b, $x = \sum_{n\geq 0}^{\infty} f^n(0)$, где 0 – нуль полукольца, f(x)=ax+b. $f^0(0) = 0, f^1(0) = b, f^2(0) = (a+1)b, \dots, f^n(0) = (a^{n-1} + \dots + a + 1)b$. Получаем, что $\sum_{n=0}^{\infty} f^n(0) = \sum_{n=1}^{\infty}[(a^{n-1} + \dots + a + 1)b] = [\sum_{n=1}^{\infty}(a^{n-1} + \dots + a + 1)] * b$. $\sum_{n=1}^{\infty}(a^{n-1} + \dots + a + 1) = \sum_{n=1}^{\infty} a^n = a^*$, т.е. в итоге получаем что $x = \sum_{n=1}^{\infty} f^n = a^*b$.

I.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 **(*)** $\begin{cases} x_1 = a_{11}x_1 + \dots + a_{1n}x_n + b_1 \\ \dots \\ x_n = a_{n1}x_1 + \dots + a_{nn}x_n + b_n \end{cases}$, 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.

• **Теорема:** 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.

Доказательство: Пусть $\mathcal{S}$ – замкнутое полукольцо, $\{A_m\}_{m\in\mathbb{N}}$ - произвольная последовательность квадратных матриц $A_m = \left(a_{ij}^m\right)$ 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:

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

$x_1 = a_{11}^*(a_{12}x_2 + \dots + a_{1n}x_n + b_1)$. Подставляя это выражение вместо x1 в остальные уравнения, получаем систему из n-1 уравнений, не содержащую x1: $\begin{cases} x_2 = a_{21}a_{11}^*(a_{12}x_2 + \dots + a_{1n}x_n + b_1) + a_{22}x_2 + \dots + a_{2n}x_n + b_2 \\ x_3 = a_{31}a_{11}^*(a_{12}x_2 + \dots + a_{1n}x_n + b_1) + a_{32}x_2 + \dots + a_{3n}x_n + b_3 \\ \dots \\ x_n = a_{n1}a_{11}^*(a_{12}x_2 + \dots + a_{1n}x_n + b_1) + a_{n2}x_2 + \dots + a_{nn}x_n + b_n \end{cases}$.

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 последовательно вычисляем значения всех неизвестных $x_1, \dots, x_{n-1}$, начиная с последнего.

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

• *Ориентированное* дерево – бесконтурный ориентированный граф с *одним входом* (вершиной с нулевой полустепенью захода), в котором для любой вершины, кроме входа, полустепень захода равна 1; вершины с полустепенью исхода равной 0 называются *листьями* дерева.

Неориентированное дерево – любой связный неориентированный граф, в котором нет циклов.

• Высота *вершины* h(v) – максимальная длина пути из этой вершины в лист;

высота *дерева* h(r)– высота его корня;

глубина вершины d(v) – длина пути из корня дерева в эту вершину;

уровень вершины $l(v) = (h(r) - d(v))$

Ориентированное дерево называют p-деревом, если полустепень *исхода* для каждой его вершины *не больше* p. P-дерево называют полным, если полустепень исхода всех его вершин кроме листьев *равна* p, и уровни его листьев одинаковы.

Теорема: В полном p-дереве высоты H число листьев равно p^H.

Доказательство: проведем по методу индукции. Если H=0, то число листьев $p^0 = 1$. Пусть утверждение верно $\forall H \leq n-1$, число листьев в полном p-дереве высоты n-1 равно p^{n-1}. Тогда, при H=n, из каждого листа «вырастает» ещё p листов, таким образом, число листов $= p * p^{n-1} = p^n$. Слеовательно, при произвольной высоте H число листьев равно p^H

II.5 *Поиск в глубину в неорграфе. Древесные рёбра. Поиск фундаментальных циклов на основе поиска в глубину.* (319)

• Поиск в глубину. На вход подается граф $G = (V, E)$, заданный списками смежности, и начальная вершина v0. На выходе имеем множества древесных и обратных ребер (T и B), множество F_c фундаментальных циклов, массив D, содержащий номера вершин.

Вначале все вершины графа помечаются как «новые».

При достижении некоторой вершины v (при запуске алгоритма v=v0), с неё снимается метка «новая», ей присваивается D-номер, вершина v заносится в стек и просматриваются вершины из её списка смежности $L[v]$.

Если вершина w из этого списка «новая», то ребро $\{v, w\}$ помечается как древесное, после чего переходим к вершине w. Далее процесс повторяется – просматривается список смежности, выбирается первая «новая» вершина, анализ же остальных вершин из списка «откладывается на потом».

Если же вершина w пройденная, и ребро $\{v, w\}$ не является древесным, то $\{v, w\}$ помечается как обратное, а из вершин, находящихся в стеке (с верхушины стека до w) формируется фундаментальный цикл (подграф, являющийся циклом, и содержащий *только одно* обратное ребро).

После анализа всех вершин из списка смежности L[w], возвращаемся в вершину v и продолжаем анализировать список смежности L[v].

«Путешествие» прекратится, когда мы вернемся в исходную вершину v0 и окажется что либо все вершины перестали быть «новыми», либо остались «новые» вершины, но из v0 больше никуда перейти нельзя.

```
    begin                                   //вглубь
1.  T,B,FC,Stack:=0; Count := 1
2.  For all v ∈ V do New[v] := 1 end
3.  For all v ∈ V while (∃v)(New[v] = 1) do
4.    Search_D(v) end
    End

    Proc Search_D(v)
5.  New[v] := 0
6.  D[v] := Count;  Count := Count + 1
7.  v → Stack
8.  For all (w ∈ L[v]) do
9.  . If New[w] then begin
10. .   {v,w} → T
11. .   Search_D(w)
12. . End if
13. . Else
    .   if {v,w} ∉ T then begin
    .     {v,w} → B
    .     Read(v..w)→ F_c
    .   end if
14. End for
15. Stack → v
    End Search_D
```

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

• В случае ориентированного графа, в результате поиска в глубину получают также множество прямых дуг $F = \{(u, v): D[u] < D[v],\ v \notin Stack\}$, ведущих от подлинного предка к подлинному потомку в глубинном остовном лесу; обратных дуг $B = \{(u, v): D[u] \geq D[v],\ v \in Stack\}$, ведущих от потомков к предкам (в том числе петли); поперечных дуг $C = \{(u, v):\ D[u] > D[v],\ v \notin Stack\}$, не являющихся ни древесными, ни прямыми, ни обратными.

• Орграф бесконтурен тогда и только тогда, когда при поиске в глубину (независимо от выбора начальной вершины) множество обратных дуг пусто.

II.7 *Поиск кратчайших расстояний от фиксированной вершины: алгоритм волнового фронта и поиск в ширину в орграфе с числовыми метками дуг. (324)*

~~~ ~~~

• Алгоритм волнового фронта. На вход подается граф $G = (V, E)$, заданный списками смежности; v0 – начальная вершина. На выходе имеем массив M меток вершин.

Вначале всем вершинам графа присваиваются метки бесконечности, начальной вершине v0 M[v0] = 0. Достигнув некоторой вершины v (при запуске поиска, v=v0, и v0 сразу же заносится в очередь), просматриваем все вершины w из её списка смежности L[v]. Если метка M[w] равна бесконечности, то присваиваем вершине w метку M[w] := M[v]+1, и заносим вершину w в очередь. Просмотрев весь список L[v], выгружаем вершину v из очереди, и повторяем процес для следующей вершины в очереди. Алгоритм завершится, когда очередь опустеет.

В случае ориентированного графа $M[w] := M[v] + \phi(v, w)$, если $M[w] > M[v] + \phi(v, w)$; на выходе получают длины кратчайших путей из v0 в остальные вершины ($+\infty$, если пути не существует).

```
1.  For all v ∈ V do M[v] := +∞ end
2.  Q := 0
3.  v0 → Q;  M[v0] = 0
4.  For all v ∈ V while Q ≠ 0 do
5.    For all w ∈ L[v] do
6.      If M[w] = +∞ then begin
7.        M[w] := M[v]+1
8.        w → Q
        End if
      End for
9.    Q → v
10. End for
```

II.8 *Алгоритм Дейкстры.*

~~~ ~~~

• На вход подается орграф $G = (V, E)$, функция разметки $\phi: E \to R_0^+$ и начальная вершина $v_0 \in V$. На выходе имеем длины кратчайших путей из v0 в остальные вершины.

При запуске алгоритма начальной вершине присваивается метка 0, остальным вершинам – метки бесконечности. Метки делятся на постоянные и временные.

На очередном шаге из всех вершин с не-бесконечными метками выбирают вершину v, которая имеет наименьшую временную метку среди вершин с временными метками, и меняют её метку с временной на постоянную. Далее для всех вершин $w \in L[v]$, если $M[w] > M[v] + \phi(v, w)$, то $M[w] \coloneqq M[v] + \phi(v, w)$. Алгоритм завершается, когда не остается временных меток, не равных бесконечности.

```
Begin
1.  M[v0] := 0
2.  For all (v ∈ V/{v0}) do M[v] ≔ +∞ end
3.  S := ∅
4.  While (v ≠ S) & (∃v ∈ V/S)(M[v] ≠ +∞) do
5.    w|min M[w] → S
6.    For all v ∈ L[w] ∩ (V/S) do
7.      M[v] := min(M[v], M[w]+ϕ(v,w))
End
```

II.10 *Задача о путях в ориентированном графе, размеченном над полукольцом (326)и ее решение с помощью алгоритма Флойда — Уоршелла — Клини(339). Задача о достижимости и поиске кратчайших расстояний между двумя узлами графа. (327)*

~~~ ~~~

• Размеченным ориентированным графом называют пару $W = (G, \phi)$, где $G = (V, E)$ – обычный ориентированный граф, $\phi: E \to S/\{0\}$ – функция разметки со значениями в некотором идемпотентном полукольце $\mathcal{S} = (S, +, *, \mathbb{0}, \mathbf{1})$, $(\forall e \in E)(\phi(e) \neq \mathbb{0})$.

Если задать орграф с помощью матрицы смежности $A = \left(a_{ij} = \begin{cases} 1, & (v_i, v_j) \in E \\ \mathbb{0}, & \text{иначе} \end{cases}\right)$, то задача о достижимости сводится к вычислению матрицы достижимости графа $C = \left(c_{ij} = \begin{cases} 1, & v_i \to^* v_j \\ \mathbb{0}, & \text{иначе} \end{cases}\right)$.

Если задать орграф с помощью матрицы меток дуг $A = \left(a_{ij} = \begin{cases} \phi(v_i, v_j), & (v_i, v_j) \in E \\ \mathbb{0}, & \text{иначе} \end{cases}\right)$, то задача о поиске кратчайших расстояний между двумя узлами графа сводится к вычислению матрицы кратчайших расстояний $C = \left(c_{ij} = \begin{cases} \text{длине кратчайшего пути из } v_i \text{ в } v_j, \text{если } v_i \Rightarrow^* v_j \\ +\infty, \text{иначе} \end{cases}\right)$.

• Обе задачи можно решить с помощью алгоритма Флойда – Уоршелла – Клини. В случае задачи о достижимости, в качестве полукольца $\mathcal{S}$ выбирают полукольцо $\mathbb{B} = (\{0,1\}, max, min, 0, 1)$, а в случае задачи о поиске кратчайших расстояний: $\mathcal{R}^+ = ([0, +\infty], min, +, +\infty, 0)$. После этого матрица $C = A^*$ находится путем ерешения системы уравнений $\xi = A\xi + \varepsilon_j$, где $\varepsilon_j \in \mathcal{R}^n$ – j-й вектор единичной матрицы в полукольце B или R+. Наименьшее решение имеет вид $\xi = A^*\varepsilon_j$, тогда столбцы ξ есть j-е столбцы матрицы C.
~~~

II.14 *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.. (514)*

~~~ ~~~

• **Теорема:** Пусть $V = \{a_1, \dots, a_n\}$ – произвольный алфавит. Язык $L \subseteq V^*$ является элементом полукольца R(V) (то есть является регулярным языком) тогда и только тогда, когда он допускается некоторым конечным автоматом.

Доказательство: Докажем, что если язык допускается КА, то он регулярен. Достаточно доказать, что решение системы линейных уравнений с регулярными коэффициентами регулярно, т.е. является вектором, каждая компонента которого – регулярный язык. По индукции, для n=1 $x = ax + b \Rightarrow x = a^*b$. Предположим, что утверждение доказано для любого числа уравнений $\leq n-1$. Тогда имеем систему с регулярными коэффициентами $\begin{matrix} x_1 = a_{11}x_1 + \dots + a_{1n}x_n + b_1 \\ \dots \\ x_n = a_{n1}x_1 + \dots + a_{nn}x_n + b\_n \end{matrix}$. $x_1 = a_{11}^*(a_{12}x_2 + \dots + a_{1n}x_n + b_1) \Rightarrow$

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

$\dots$

$x_n = a_{n1}a_{11}^*(a_{12}x_2 + \dots + a_{1n}x_n + b_1) + \dots + a_{nn}x_n + b\_n$

. Возникает система из $n-1$ линейных уравнений с n-1 неизвестными и регулярными коэффициентами. По предположению индукции её решение регулярно (x2..xн – РЯ), значит x1 – также регулярно.

Докажем, что если язык регулярен, то его допускает КА. Рассмотрим КА для простейших языков: $\emptyset: \to q_0$, $\lambda: \to q_0 \to$, $a: \to q_0 \to_a q_1 \to$. Предположим, что есть автомат M1, L(M1)=L1, M2, L(M2)=L2. Рассмотрим КА их объединения, соединения и итерации. Так как любой РЯ может быть представлен в виде ^ операций над более простыми РЯ, то КА можно построить для любого РЯ.

II.16 *Лемма о разрастании для регулярных языков. (538)*

~~~ ~~~

• **Теорема:** Если L – регулярный язык, то существует натуральная константа K_L, зависящая от L, такая, что для любой цепочки $x \in L$, длина которой не меньше K_L, x допускает представление в виде $x = uvw$, где $v \neq \lambda$ и $|v| \leq K_L$. При этом для любого $n \geq 0$ существует цепочка $x_n = uv^n w \in L$.

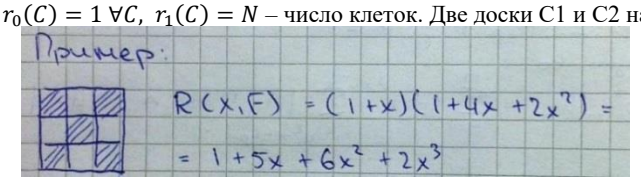
Доказательство: Т.к. L – РЯ, его допускает некий детерминированный КА $M = (V, Q, q_0, F, \delta)$. Пусть $K_l = |Q|, x \in L, |x| \geq K_l$. Значит, цепочка читается на единственном пути длины $m = |x| \geq |Q|$. Значит, число вершин в пути больше числа дуг, а следовательно, путь можно разбить на три части: $\to q_0 \rightsquigarrow_u p \circlearrowleft_v, p \rightsquigarrow_w p_m \to$. Тогда $(\forall n \geq 0)(uv^n w \in L)$; т.к. контур – простой путь длины$\neq 0$, то $0 < |v| \leq K_l$.

\- \- \- \- \- \- \- \- \- \- \- \- \- \-

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

~~~ ~~~

• Ладейным называют полином $R(x, C) = \sum_{k=0}^{N} r_k(C)x^k$, где r_k – число способов размещения k ладей в небоевых позициях на доске C. $r_0(C) = 1 \; \forall C$, $r_1(C) = N$ – число клеток. Две доски C1 и C2 называют дизъюнктными, если они не имеют общих строк и столбцов.



Теоерма (о декомпозиции досок): Если доски C1 и C2 дизъюнктны, то ладейный полином объединения $C1 \cup C2$ $R(x, C1 \cup C2) = R(x, C1) * R(x, C2)$.

Доказательство: Пусть даны дизъюнктные доски C1 и C2, на C1 можно разместить не более l ладей, на C2 – не более k-l, $0 \leq l \leq k$. Рассмотрим число способов размещения k ладей на обеих досках.

Число способов размещения l ладей на C1 равно $r_l(C1)$, на C2 - $r_{k-l}(C2)$. При фиксированном l число способов размещения k ладей $N_l = r_l(C1) * r_{k-l}(C2)$. При изменении l получаем $N = \sum_{l=0}^{k} r_l(C1) * r_{k-l}(C2) = r_k(C1 \cup C2)$. Следовательно, $R(x, C1 \cup C2) = R(x, C1)R(x, C2)$.

Теорема: Пусть дана доска C, S – её произвольная фиксированная клетка. Обозначим C_S – доску, полученную из C удалением клетки S, а $C_S^{\#}$ – доску, полученную удалением строки и столбца, содержащих S. Тогда ладейный полином доски C $R(x, C) = R(x, C_S) + xR(x, C_S^{\#})$.

Доказательство: Коэффициент при x^k в $R(x, C)$ равен $r_k(C_S) + r_{k-1}(C_S^{\#})$. Следовательно, $R(x, C) = \sum_{k=0}^{N} r_k(C_S)x^k + \sum_{k=1}^{N} r_{k-1}(C_S^{\#})x^k = \sum_{k=0}^{N} r_k(C_S)x^k + \sum_{k=0}^{N} r_k(C_S^{\#})x^{k+1} = \sum_{k=0}^{N} r_k(C_S)x^k + x\sum_{k=0}^{N} r_k(C_S^{\#})x^k$, где N – число клеток в доске C.

III.4 *Вывод формулы для числа подстановок с запрещенными позициями.*

~~~ ~~~

• Пусть Sn – группа подстановок, $\sigma \in S_n$. Обозначим $F_i \subseteq \{1, \dots, n\}$ – множество запрещенных подстановок на элементе i. Тогда $\{\sigma: \sigma(i) \notin F_i\}$ есть множество допустимых подстановок. (К примеру, на 4элементном множестве при $F_4 = \{3,4\}$ запрещена подстановка (1234 -> 1344), т.к. в 4й «линии» доски запрещены клетки 3 и 4).

Обозначим $A_i = \{\sigma(i) \in F_i\}$, F – заданная запрещенная область; Ln – число подстановок, значения которых не попадают в область F. Тогда $L_n = n! - |A_1 \cup \dots \cup A_n|$,

$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^{n}[(-1)^{k+1} \sum_{i1<\dots<ik} |A_{i1} \cap \dots \cap A_{in}|]$ Фиксируем i. Число подстановок $|A_i| = (n-1)! * |F_i|$. Тогда $\sum_{i=1}^{n} |A_i| = (n-1)! * r_1(F)$. Фиксируя $i_1 \dots i_k$: $|A_{i1} \cap \dots \cap A_{in}| = (n-k)! * N_{i1\dots ik}$, где N – число способов разместить k ладей в строках с фиксированными номерами, принадлежащими запрещенной зоне.

$$\sum_{i1<\dots ik} |A_{i1} \cap \dots \cap A_{ik}| = (n-k)! * r_k(F) \Rightarrow$$

$$|A_{i1} \cup \dots \cup A_{in}| = \sum_{k=1}^{n} [(-1)^{k+1} r_k(F)(n-k)!] \Rightarrow$$

$$L_n = n! - \sum_{k=1}^{n} [(-1)^{k+1} r_k(F)(n-k)!] = n! + \sum_{k=1}^{n} [(-1)^k r_k(F)(n-k)!] = \sum_{k=0}^{n} [(-1)^k r_k(F)(n-k)!] = R(x, F)|_{x^k = (-1)^k (n-k)!}$$

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

~~~ ~~~

• Рекуррентным соотношением k-го порядка называется последовательность $(\mathbf{0})\ x_n = \phi(x_{n-1}, x_{n-2}, \dots, x_{n-k}) + f(n)$. Порядок указывает, от скольких предыдущих членов зависит n-й член последовательности. При $f(n) \equiv 0$ рекуррент называется однородным. Если ф – линейна по аргументам, т.е. $(\mathbf{1})\ x_n = a_1(n)x_{n-1} + \dots + a_k(n)x_{n-k}$, то соотношение называется линейным. Если $a_i = const$, то ЛРС $(\mathbf{2})\ x_n = a_1x_{n-1} + \dots + a_kx_{n-k}$ называется ЛРС с постоянными коэффициентами.

• Решить РС в общем случае – найти такую последовательность {yn} (частное решение), что будучи подставленной в (1) yn обращает его в тождество. Решение ЛРС (2) должно быть дополнено начальными условиями $(\mathbf{3})\ x_i = \alpha_i,\ i = \overline{0, k-1}$. **k** линейно независимых решений ЛРС **k**-го порядка образуют фундаментальную систему решений этого ЛРС.

• **Теорема**: Начальные условия вида (3) однозначно определяют частное решение соотношения (2). Наоборот, произвольно заданное ЧР однозначно определяет НУ вида (3).

Доказательство: Пусть даны начальные условия. Положим, что $y_i = \alpha_i\ \ \forall i = 0..k-1$. В силу соотношения (2),

$$y_k = a_1y_{k-1} + a_2y_{k-2} + \dots + a_ky_0 = a_1\alpha_{k-1} + \dots + a_k\alpha_0$$
$$y_{k+1} = a_1y_k + a_2\alpha_{k-1} + \dots + a_k\alpha_1$$
$$y_{k+j} = a_1y_{k+j-1} + \dots + a_ky_j, \qquad j \geq 0$$

Следовательно, если заданы НУ в виде (3), то решение $\{y_n\}$ задано единственным образом.

Пусть теперь дана последовательность $\{y_n\}$. Тогда,

$$\begin{cases} y_k + a_1\alpha_{k-1} + \dots + a_k\alpha_0 = 0 \\ y_{k+1} + a_1y_k + \dots + a_k\alpha_1 = 0 \\ \dots \\ y_{2k-2} + a_1y_{2k-3} + \dots + a_{k-1}\alpha_{k-1} + a_k\alpha_{k-2} = 0 \\ y_{2k-1} + a_1y_{2k-2} + \dots + a_{k-1}y_k + a_k\alpha_{k-1} = 0 \end{cases}$$

Данную систему можно рассматривать как систему линейных уравнений, представленную в треугольной форме. Из последнего уравнения можно определить α_{k-1}, из предпоследнего: к-2 и так далее. Таким образом, заданное частное решение однозначно определяет начальные условия.

III.6 *Теорема об общем решении ОЛРС как линейной комбинации фундаментальных решений. (21)*

~~~ ~~~

• **Теорема**: Пусть $\left\{y_n^{(1)}\right\} \dots \left\{y_n^{(k)}\right\}$ – ЛНЗ решения соотношения $x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = 0$. Тогда любое его решение можно представить в виде их линейной комбинации для некоторых констант С.

Доказательство: Задав некоторые начальные условия, покажем что константы С задаются однозначно. Запишем начальные условия для линейной комбинации $(\mathbf{1})\begin{cases} \sum_{i=1}^k C_iy_0^{(i)} = \alpha_0 \\ \sum_{i=1}^k C_iy_1^{(i)} = \alpha_1 \\ \dots \\ \sum_{i=1}^k C_iy_{k-1}^{(i)} = \alpha_{k-1} \end{cases}$. Для системы (1) $\Delta = \begin{bmatrix} y_0^{(1)} & \dots & y_0^{(k)} \\ \vdots & \ddots & \vdots \\ y_{k-1}^{(1)} & \dots & y_{k-1}^{(k)} \end{bmatrix}$. Предположим, что $\Delta = 0$ – тогда однородная система $(\mathbf{2})\ \sum_{i=1}^k C_iy_j^{(i)} = 0$ соответствующая системе (1) имеет тривиальное решение. В этом случае из (2) можно найти (не все равные нулю) константы С. Однако (2) также определяет решение, соответствующее *нулевым начальным условиям*, следовательно, $\sum_{i=1}^k C_iy_n^{(i)} \equiv 0$. Возникает противоречие, следовательно $\Delta \neq 0$, а (1) имеет единственное решение. Таким образом, начальные условия задают однозначный набор С, т.е. любое решение (1) можно определить в виде ЛК фундаментальных

III.8 *Неоднородные линейные рекуррентные соотношения с постоянными коэффициентами. (17) Теорема о структуре общего решения. (24) Поиск частного решения методом подбора. (27) Принцип суперпозиции (без доказательства). (28)*

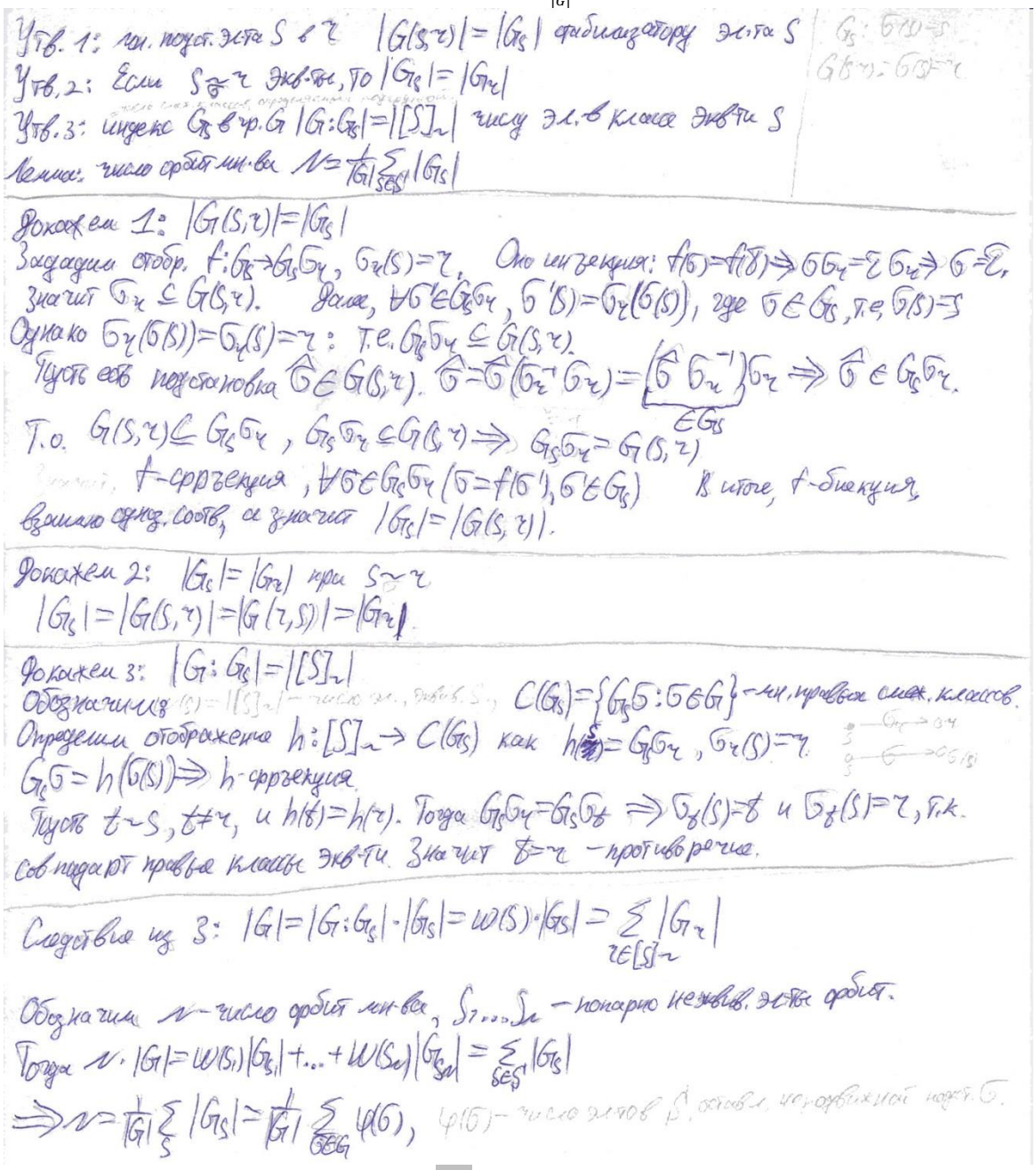
~~~ ~~~

• Неоднородным ЛРС с постоянными коэффициентами называют ЛРС вида $(\mathbf{1})\ x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = f(n)$, a=const.

• **Теорема**: Общее решение соотношения (1) есть сумма общего решения соответствующего ему однородного ЛРС $x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = 0$ и частного решения неоднородного ЛРС (1).

Доказательство: пусть Y_n – какое-то частное решение (1). Тогда $(\mathbf{2})\ x_n^{\text{он}} = Y_n + \sum_{i=1}^k C_iy_n^{(i)}$, где $\{y_n^{(1)} \dots\ y_n^{(k)}\}$ – ФСР соответствующего ОЛРС. Зададим произвольные начальные условия, $y_o = \alpha_0, \dots y_{k-1} = \alpha_{k-1}$, которым соответствует решение $y_n, \Rightarrow$

$$(\mathbf{3})\begin{cases} Y_0 + \sum_{i=1}^k C_iy_0^{(i)} = \alpha_0 \\ Y_1 + \sum_{i=1}^k C_iy_1^{(i)} = \alpha_1 \\ \dots \\ Y_{k-1} + \sum_{i=1}^k C_iy_{k-1}^{(i)} = \alpha_{k-1} \end{cases} \Rightarrow (\mathbf{4})\begin{cases} \sum_{i=1}^k C_iy_0^{(i)} = \alpha_0 - Y_0 \\ \sum_{i=1}^k C_iy_1^{(i)} = \alpha_1 - Y_1 \\ \dots \\ \sum_{i=1}^k C_iy_{k-1}^{(i)} = \alpha_{k-1} - Y_{k-1} \end{cases}$$

. Для системы (4) $\Delta = \begin{bmatrix} y_0^{(1)} & \dots & y_0^{(k)} \\ \vdots & \ddots & \vdots \\ y_{k-1}^{(1)} & \dots & y_{k-1}^{(k)} \end{bmatrix}$. Предположим, что $\Delta = 0$ – тогда однородная система $(\mathbf{5})\begin{cases} \sum_{i=1}^k C_iy_0^{(i)} = 0 \\ \sum_{i=1}^k C_iy_1^{(i)} = 0 \\ \dots \\ \sum_{i=1}^k C_iy_{k-1}^{(i)} = 0 \end{cases}$ соответствующая системе (4) имеет тривиальное решение. В этом случае из (5) можно найти (не все равные нулю) константы С. Однако (5) также определяет решение, соответствующее *нулевым начальным условиям*, следовательно, $\sum_{i=1}^k C_iy_n^{(i)} \equiv 0$. Возникает противоречие, следовательно $\Delta \neq 0$, а (4) имеет единственное решение. Таким образом, начальные условия задают однозначный набор С, т.е. любое регение (1) можно определить в виде (2).

• Частное решение неоднородного ЛРС находится методами подбора.

Если $f(n) = a^nP^{(m)}(n)$, то $x_n^{\text{чн}} = n^sa^nQ^{(m)}(n)$, где Q – полином с неопределенными коэффициентами, которые могут быть определены путем подстановки в соотношение, s – кратность корня a характеристического уравнения (если a не является корнем, то s=0).

Если $f(n) = a^n\left[P^{(m)}(n)\cos n\phi + Q^{(l)}(n)\sin n\phi\right]$, то $x_n^{\text{чн}} = n^sa^n\left[P^{(p)}(n)\cos n\phi + Q^{(p)}(n)\sin n\phi\right]$, где s – кратность корня $ae^{i\phi}$ характеристического уравнения, $p = \max m, l$.

• **Принцип суперпозиции**: Пусть в неоднородном ЛРС (1) $f(n) = \sum_{i=1}^l g_i(n)$ – сумма последовательностей, и пусть $x_n^{\text{чн}_i}$ есть решение соотношения (1) при $f(n) = g_i(n)$. Тогда частное решение $x_n^{\text{чр}} = \sum_{i=1}^l x_n^{\text{чн}_i}$.
~~~

III.9 *Понятие действия группы на множестве. Стабилизаторы и орбиты. (37) Лемма Бернсайда (с доказательством).*

• Говорят, что группа G действует слева на множестве M, если задан гомоморфизм $\phi: G \to S(M)$ из группы G в симметрическую группу S(M) множества M, т.е. на симметрической группе множества задано множество подстановок.

• Пусть $A = \{a_1 \dots a_n\}$ – множество, $G \subseteq S_n$ – подгруппа циклической группы этого множества. Элементы $a, b \in A$ называют эквивалентными $a \sim b$, если $b = \sigma(a), \sigma \in G$. Орбитой элемента a называют его класс эквивалентности $[a]_\sim$ по подстановке σ. Стабилизатором элемента $s \in A$ называют множество $G_s = \{\sigma: \sigma(s) = s\}$.

Лемма Бернсайда: Число N орбит множества S равно $N = \frac{1}{|G|}\sum_{s \in S}|G_s|$.



III.11 *Циклический (цикловой) индекс группы. (38) Теорема Пойа (с выводом числа классов эквивалентности, без доказательства утверждения о структурном перечне классов эквивалентности). (41)*

• Пусть H – некая конечная группа, являющаяся подгруппой группы подстановок Sn. Произвольную подстановку $h \in H$ можно представить в виде произведения независимых циклов $h = c_1 \circ \dots \circ c_m,\ m \le n$. Цикловым индексом группы H называется многочлен $p_H(x_1, \dots, x_n) = \frac{1}{|H|}\sum_{h \in H} t_\sigma$, где $t_\sigma = x_1^{l_1} \dots x_k^{l_k}$ – мультипликативный терм, li – число циклов длины I в разложении элемента на независимые циклы.

• **Теорема Пойа:** пусть $S = \{1..n\}$ – множество, на котором действует группа G, $R = \{r_1, \dots, r_m\}$ – множество цветов, $p_{G(x_1,\dots,x_n)}$ – цикловой индекс группы G. Тогда:

1) перечень классов эквивалентности можно представить в виде $Invt(R^S/\sim) = p_G(\sum_{r \in R} w(r), \dots, \sum_{r \in R} w^n(r))$

2) число неэквивалентных раскрасок из {R} множества $N = P_G(|R|, \dots, |R|)$.

Доказательство второго утверждения: по лемме Бернсайда, $N = \frac{1}{|G|}\sum_{s \in S}|G_s| = \frac{1}{|G|}\sum_{\sigma \in G}\psi(\sigma)$, где $\psi(\sigma)$ – число всех элементов s, остающихся неподвижными в результате действия подстановки σ. Подстановка $\sigma = c_1 c_2 \dots c_{l=K(\sigma)}$ представлена в виде m независимых циклов. Чтобы циклы сохраняли разметку, элементы должны быть покрашены одинаково. Вычислим терм $\hat{t}_\sigma = (w_1 + \dots + w_m)^{l1}(w_1^2 + \dots + w_m^2)^{l2} \dots (w_1^n + \dots + w_m^n)^{ln}$. Циклический индекс группы G $P_G(x_1 \dots x_n) = \frac{1}{|G|}\sum_{h \in H} t_\sigma = \frac{1}{|G|}\sum_{h \in H} x_1^{l_1} \dots x_k^{l_k}$. Тогда, $\hat{t}_\sigma = t_\sigma|_{x_k = (w_1^k + \dots + w_m^k)}$.

$\psi(\sigma) = |R|^{K(\sigma)};\ \ l_1 + \dots + l_n = K(\sigma) \ \ \Rightarrow$

$\psi(\sigma) = \hat{t_\sigma}|_{\forall w_i\, w_i = 1} = \hat{t_\sigma}|_{\forall i\, x_i = m}$. Поэтому само число классов эквивалентности $N = \frac{1}{|G|}\sum_{\sigma \in G} t_\sigma|_{x_i = m} = P_G(x_1 \dots x_m)|_{x_i = m} = P_G(m \dots m)$.