Дискретная математика

Козырнов Александр Дмитриевич, ИУ7-32Б

8 января 2024 г.

Оглавление

Множества, отношения, алгебры

1.1 Опр. множества и операций над ним

1.1.1 Условие

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

1.1.2 Множество

Определение. Множество - это свойства, которые объединяют что-то. Явного определения нет.

Способы определения. Можно задать как предикат: $A = \{x : P(x)\}$.

Если a - элемент множества A, то можно записать $a \in A$.

Множество называется конечным, если он состоит из конечного количества элементов: $A = \{a_1, a_2, \ldots, a_n\}$

1.1.3 Подмножество

Определение. Можно задать в виде формулы: $A \subseteq B \leftrightharpoons (\forall x)(x \in A \implies x$
$inB)$

1.1.4 Операции над множествами

- объединение $A \cup B \leftrightharpoons \{x : x \in A \vee x \in B\}$
- пересечение $A \cap B \leftrightharpoons \{x : x \in A \ \& \ x \in B\}$
- разность $A \setminus B \leftrightharpoons \{x : x \in A \ \& \ x \notin B\}$
- симметрическая разность $A \triangle B \leftrightharpoons (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
- дополнение $\overline{A} \leftrightharpoons \{x : x \notin A\} = U \setminus A$

1.1.5 Методы доказательства теоретико-множественных тождеств

- Метод двух включений (На примере декартового умножения)
  $A \times (B \cap C) = (A \times B) \cap (A \times C)$
  Доказательство
  $(x, y) \in A \times (B \cap C) \Leftrightarrow (x \in A) \ \& \ (y \in (B \cap C)) \Leftrightarrow (x \in A) \ \& \ (y \in B) \ \& \ (y \in C) \Leftrightarrow ((x, y) \in A \times B) \ \& \ ((x, y) \in A \times C) \Leftrightarrow (x, y) \in (A \times B) \cap (A \times C)$

- Методом Характеристических функций ($\chi_{A\times B\cap C}$)
- Методом эквивалетных преобазований ($\cap, \cup$, $\&$, $\setminus$, ..., а также ранее доказанными тождествами)

1.2 Неупорядоченная и упорядоченная пары, кортеж, Декартово произведение.

1.2.1 Условие

Неупорядоченная пара, упорядоченная пара, кортеж. Декартово произведение множеств

1.2.2 Виды вар

Неупорядоченная пара

$A, B \neq 0, a \in A, b \in B$
Тогда $\{a, b\}$ - неупорядоченная пара на множествах A и B

$$\begin{cases} \{a, b\} = \{a\}, |\{a\}| = 1, \text{ если } a = b \\ |\{a, b\}| = 2, \text{ если } a \neq b \end{cases}$$

$\{a, b\} = \{c, d\} \leftrightharpoons ((a = c)\ \&\ (b = d)) \vee ((a = d)\ \&\ (b = c))$
То есть $\{1, 2\} = \{2, 1\}$

Упорядоченная пара

$A, B \neq 0, a \in A, b \in B$
Тогда (a, b) - упорядоченная пара на множествах A и B
$(a, b) = (c, d) \leftrightharpoons (a = c)\ \&\ (b = d)$
То есть $(a, b) \neq (b, a)$
Ее можно свести к множеству: $(a, b) \leftrightharpoons \{\{a\}, \{a, b\}\}$

1.2.3 Кортеж

$A_1, A_2, \ldots, A_n, n \geq 1$
Тогда $(a_1, a_2, \ldots, a_n)$, где $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$ - кортеж
Кортеж может быть задан так: $B = A_1 \times A_2 \times \ldots \times A_n$

- Равенство кортежей:
  $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \leftrightharpoons (\forall i = \overline{1, n})(a_i = b_i)$
- Определение:
  $A_1 \times A_2 \times \ldots \times A_n \leftrightharpoons \{(x_1, x_2, \ldots, x_n) : (\forall i = \overline{1, n})(x_i \in A_i)\}$
  По определению если $(\exists i = \overline{1, n})(A_i = \varnothing)$, то $A_1 \times A_1 \times \ldots \times A_n = \varnothing$
- Степень кортежа:
  Если $A_1 = A_2 = \ldots = A_n, n \geq 1$, то $A_1 \times A_2 \ldots \times A_n = A^n$
  $A^0 \leftrightharpoons \{\lambda\}$, где λ - пустой кортеж, $A \neq \varnothing$

Некоторые свойства декартового умножения:

- $\overline{A \times B} = (\overline{A} \times \overline{B}) \cup (\overline{A} \times B) \cup (A \times \overline{B})$
- $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$
- $A \times B \neq B \times A$

1.3 Отображение, частичное отображение

1.3.1 Условие

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

1.3.2 Отображение

Определение. Отображение - это соответствие, которое всюду определено и функционально по второй компоненте

Пусть $\rho \subseteq A \times B$, тогда

- Область определения: $D(\rho) \leftharpoons \{x : x \in A, (x, y) \in \rho\}$
- Область значений: $R(\rho) \leftharpoons \{y : y \in B, (x, y) \in \rho\}$

$f : A \overset{\bullet}{\to} B$ - частичное отображение, или отображение, где $D(\rho) \neq A$
$f : A \to B$ - просто отображение
Виды отображений:

- Инъективное отображение:
  Если отображение функционально и по первой компоненте, то она называется инъекцией. то есть $f(x_1) = f(x_2) \implies x_1 = x_2$
  $(\forall x \in A)(\exists! y = f(x))$ & $(\forall y \in R(f))(\exists! x \in A)(y = f(x))$
- Сюръективное отображение:
  Это такое отображение, где $R(f) = B$, то есть
  $(\forall y \in B)(\exists x \in A)(y = f(x))$
- Биективное отображение:
  Это такое отображение, которое инъективно и сюръективно.
  $(\forall x \in A)(\exists! y = f(x))$ & $(\forall y \in B)(\exists! x)(y = f(x))$

1.4 Соответствие

Условие

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.

1.4.1 Соответствие

$\rho \subseteq A \times B$ - соответствие из A в множество B, причем $A, B \neq \varnothing$

- Область определения: $D(\rho) \leftrightharpoons \{x : x \in A, (x, y) \in \rho\}$
- Область значений: $R(\rho) \leftrightharpoons \{y : y \in B, (x, y) \in \rho\}$
- Сечение по $a \in A : \rho(a) \leftrightharpoons \{y : (a, y) \in \rho\}$
- Сечение по множеству $C \subseteq D(\rho) : \rho(C) \leftrightharpoons \{(x, y) : x \in C, (x, y) \in \rho\}$

Соответствие $\rho = A \times B$ называют функциональным по второй компоненте, если $\forall(x, y)$ и $(x', y') : x = x' \Rightarrow y = y'$

Соответствие $\rho = A \times B$ называют функциональным по первой компоненте, если $\forall(x, y)$ и $(x', y') : y = y' \Rightarrow x = x'$

1.4.2 График и граф соответствия

СДЕЛАТЬ

1.4.3 Бинарные и н-арные (н-местные) отношения

Н-местное (н-арное) отношение на множествах $A_1, A_2, \ldots, A_n, n \geq 1$: $\rho \subseteq A_1 \times A_2 \times \ldots \times A_n$

Бинарное отношение: $\rho = A^2, A \neq \varnothing$, иногда записывается как $x\rho y$

Свойства

- Рефлексивность
  $(\forall x \in A)(x\rho x)$, то есть диагональ $id_A \subseteq \rho$
- Иррефлексивность
  $id_A \cap \rho = \varnothing$
- Симметричность
  $\forall(x, y) \in A, x\rho y \Rightarrow y\rho x$, то есть $\rho = \rho^{-1}$
- Антисимметричность
  $\forall(x, y) \in A, x\rho y \ \& \ y\rho x \Rightarrow x = y$, например $x \leq y \ \& \ y \leq x \Rightarrow x = y$
- Транзитивность
  $(\forall x, y, z \in A)(x\rho z \ \& \ z\rho y \Rightarrow x\rho y)$, например $x = z, z = y \Rightarrow x = y$

1.4.4 Связь отношения, соответствия, отображения

Соответствие - это бинарное отношения вида $\rho = A \times B$ или $\rho = A \times A$. Отображение - это соответствие, которое всюду определено и функционально по второй компоненте.

1.5 Композиция соответсвий, их свойства

1.5.1 Условие

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

1.5.2 Композиция соответсвий

$\rho \subseteq A \times B, \sigma \subseteq C \times D$

Тогда композиция:

- $\rho \circ \sigma \rightleftharpoons \{(x,y) : (x,z) \in \rho \ \& \ (z,y) \in \sigma\}$
- $\rho = A \times B, \sigma = B \times C, \rho \circ \sigma = A \times C$
- $f : A \to B, g : B \to C, f \circ g : A \to C$

причем $R(\rho) \cap D(\sigma) \neq \varnothing$

Покажем, что $f \circ g(x) = g(f(x))$

$f \circ g = \{(x,y) : (\exists z)((x,z) \in f) \ \& \ ((z,y) \in g)\} = \{(x,y) : (\exists z)(z = f(x), y = g(z))\} = \{(x,y) : y = g(f(x))\}$

1.5.3 Обратное соответствие

$\rho^{-1} \rightleftharpoons \{(x,y) : (y,x) \in \rho\}$ - обратное соответствие
Если $\rho = A \times B$, то $\rho^{-1} = B \times A$

1.5.4 Свойства и их доказательства

- $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$
  Рассмотрим $(\rho \circ (\sigma \circ \tau))(x)$: $(\rho \circ (\sigma \circ \tau))(x) = \rho((\sigma \circ \tau)(x)) = \rho(\sigma(\tau(x)))$
  Рассмотрим $((\rho \circ \sigma) \circ \tau)(x)$: $((\rho \circ \sigma) \circ \tau)(x) = ((\rho \circ \sigma)(f(x)) = \rho(\sigma(\tau(x)))$
  Как можем заметить, результат получен одинаковый

- $\rho \circ \sigma \neq \sigma \circ \rho$
  Пусть $\rho = A \times B, f : A \to B$ и $\sigma = B \times C, g : B \to C$
  Тогда $\rho \circ \sigma : A \to C$
  Получаем $\sigma \circ \rho : B \to B$ при условии, что $B \cap A \neq \varnothing$, иначе $\sigma \circ \rho = \varnothing$
  В обоих случаях $R(\rho \circ \sigma) \neq R(\sigma \circ \rho), D(\rho \circ \sigma) \neq D(\sigma \circ \rho) \Rightarrow \rho \circ \sigma \neq \sigma \circ \rho$
  в общем случае

- $\rho \circ (\sigma \cup \tau) = (\rho \circ \sigma) \cup (\rho \circ \tau)$
  $(x,y) \in \rho \circ (\sigma \circ \tau) \Rightarrow (\exists z)(((x,z) \in \rho) \wedge ((z,y) \in \sigma \cup \tau)) \Rightarrow (\exists z)((((x,z) \in \rho) \wedge ((z,y) \in \sigma) \vee ((z,y) \in \tau))) \Rightarrow (\exists u)(((x,u) \in \rho) \wedge ((u,y) \in \sigma) \vee (\exists v)((x,v) \in \rho \wedge (v,y) \in \tau)) \Rightarrow (\rho \circ \sigma) \cup \rho \circ \tau$

- $\rho \circ (\sigma \cap \tau) \subseteq (\rho \circ \sigma) \cap (\rho \circ \tau)$
  Доказательство Аналогично прошлому доказательству

- $(\rho^{-1})^{-1} = \rho$
  $\rho^{-1} \rightleftharpoons \{(y,x) : (x,y) \in \rho\}$
  Тогда $(\rho^{-1})^{-1} \rightleftharpoons \{(x,y) : (y,x) \in \rho^{-1}\} \rightleftharpoons \{(x,y) : (x,y) \in \rho\} \rightleftharpoons \rho$

- $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$
  Пусть $\rho : A \to B, \sigma : B \to C$, тогда $\rho \circ \sigma : A \to C$
  Тогда $(\rho \circ \sigma)^{-1} : C \to A$
  $\rho^{-1} : B \to A, \ \sigma^{-1} : C \to B$
  Из этого следует $\sigma^{-1} \circ \rho^{-1} : C \to A$, что равно $(\rho \circ \sigma)^{-1} : C \to A$

- $\rho \subseteq A^2$

1.6 Специальные свойства бинарных отношений

Условие

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

1.6.1 Свойства

- Рефлексивность
  $(\forall x \in A)(x\rho x)$, то есть диагональ $id_A \subseteq \rho$
- Иррефлексивность
  $id_A \cap \rho = \varnothing$
- Симметричность
  $\forall (x, y) \in A, x\rho y \Rightarrow y\rho x$, то есть $\rho = \rho^{-1}$
- Антисимметричность
  $\forall (x, y) \in A, x\rho y \ \& \ y\rho x \Rightarrow x = y$, например $x \leq y \ \& \ y \leq x \Rightarrow x = y$
- Транзитивность
  $(\forall x, y, z \in A)(x\rho z \ \& \ z\rho y \Rightarrow x\rho y)$, например $x = z, z = y \Rightarrow x = y$

1.7 Классификация бинарных отношений на множестве

Условие

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

1.7.1 Классификация

- Отношение эквивалентности
  - Рефлексивность
  - Симметричность
  - Транзитивность
- Отношение Толерантности
  - Рефлексивность
  - Симметричность
- Отношение Порядка
  - Рефлексивность
  - Антисимметричность
  - Транзитивность
- Отношение Предпорядка
  - Рефлексивность
  - Транзитивность

1.8 Отношение эквивалентности, класс эквивалентности, фактор-множество

1.8.1 Условие

Отношение эквивалентности. Класс эквивалентности. Фактор-множество.

1.8.2 Отношение эквивалентности

Отношение эквивалентности можно охарактеризовать так:

- Рефлексивность
- Симметричность
- Транзитивность

1.8.3 Класс эквивалентности

$[x]_\rho \rightleftharpoons \{y : y\rho x\}$ - класс эквивалентности элемента x по отношению ρ. Причем $(\forall x \in A)(x \in [x]_\rho)$

Пример: $[(x_0, y_0)]_\rho = \{(x, y) : x^2 + y^2 = x_0^2 + y_0^2\}$, где x_0, y_0 не изменяются (константы). График такого класса эквивалентности представляет собой окружность радиуса $x_0^2 + y_0^2$

Теорема Класс эквивалентности для любого произвольного отношения эквивалентности попарно не пересекаются

Это означает, что два класса эквивалентности не имеют общих элементов, или $[x]_\rho \cap [z]_\rho = \varnothing$.

Говорят, что некоторое семейство подмножеств создает разбиение множества A, если: 1) все подмножества не пусты, 2)каждый элемент из A (множества) принадлежит хотя бы одному из классов эквивалентности, 3) Классы попарно не пересекаются (что было сказано выше).

1.8.4 Фактор-множество

$A\backslash\rho$ - это фактор-множество

$A\backslash\rho \rightleftharpoons \{[x]_\rho : x \in A\}$, где $[x]_\rho$ - это элемент класс эквивалентности

То есть простыми словами фактор-множество - это все классы эквивалентности: $A\backslash\rho = \{[x_1]_\rho, [x_2]_\rho, \ldots, [x_n]_\rho\}$ - то есть множество множеств. Также по определению это является разбиением множества (см. выше)

1.9 Отношение порядка и предпорядка. Грани множества

1.9.1 Условие

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

1.9.2 Отношение предпорядка и порядка

Отношение Порядка

- Рефлексивность
- Антисимметричность
- Транзитивность

Отношение Предпорядка

- Рефлексивность
- Транзитивность

Если отношение порядка таково, что несравнимых элементов нет, то отношение является линейным порядком

Знаки сравнимости:

- Знаки нестрогого порядка: $\leq, \geq$
- Знаки строгого порядка: $<, >$
  $a < b \rightleftharpoons a \leq b \ \& \ a \neq b$
- Отношение несравнимости $a \asymp b \leftrightharpoons a \not\leq b \ \& \ a \not\geq b$

1.9.3 Наименьший, наибольший, минимальный, максимальный элементы

Элемент $a \in A$ называется наименьшим, если $(\forall x \in A)(x \leq a)$

Элемент $a \in A$ называется наибольшим, если $(\forall x \in A)(x \geq a)$

Элемент $a \in A$ называется минимальным, если $(\forall x \in A)(a \leq x \vee a \asymp x)$

Элемент $a \in A$ называется максимальным, если $(\forall x \in A)(a \geq x \vee a \asymp x)$

Теорема. Если наименьший (наибольший) элемент существует, то он единственный

Прошу заметить, что минимальных и максимальных элементов может быть бесконечность!

1.9.4 Верхняя и нижняя грани

$\mathcal{A} = (A, \leq)$ - отношение порядка.

$B \subseteq A$ - отношение порядка на подмножестве B (индуцированный порядок)

Верхняя грань $B^{\triangledown}$ - верхний конус B. $B^{\triangledown} \rightleftharpoons \{x : (\forall b \in B)(b \leq x)\}$, где x - это **верхняя грань**

Нижняя грань $B^{\triangle}$ - нижний конус B. $B^{\triangle} \rightleftharpoons \{x : (\forall b \in B)(b \geq x\})$, где x - это **нижняя грань**

Если из всех верхних граней есть наименьшая, то она называется точная верхняя грань или супремум. Если из всех нижних граней есть наибольшая, то она называется точная нижняя грань или инфинум.

1.10 Точная верхняя грань последовательности. Индуктивно упорядоченное множество

1.10.1 Условие

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

1.10.2 Индуктивно упорядоченное множество

Определение. Упорядоченное множество $\mathcal{A} = (A, \leq)$ называют индуктивно упорядоченным, если

1) Оно имеет наименьший элемент
2) Любая неубывающая последовательность элементов A имеет супремум (sup)

1.10.3 Точная верхняя грань последовательности

Определение. $\lim\limits_{x \to \infty} a_n = sup(a_n)$ - точная верхняя грань последовательности

1.10.4 Теорема о неподвижной точке

Теорема. f называется непрерывным, если для любой неубывающей последовательности $a_0 \leq a_1 \leq \ldots \leq a_n \leq \ldots$ и $f(supa_n) = supf(a_n)$

Теорема (о монотонности). Всякое непрерывное отображение одного ИУМ в другое монотонно

Теорема (о неподвижной точке). Всякое непрерывное отображение ИУМ в себя имеет наименьшую неподвижную точку

Доказательство. Пусть A - ИУМ, $f : A \to A$ - непрерывно. Обозначим Θ наименьшим элементом A.

Построим последовательность:
$\Theta, f(\Theta), f(f(\Theta)), \ldots, f^n(\Theta), n \geq 0$, где $f^n\Theta = f(f^{n-1}(\Theta))$

Докажем, что наша последовательность не убывает
$\Theta \leq f(\Theta)$, так как Θ - наименьший элемент

Тогда $f^{n-1}(\Theta) \leq f^n(\Theta)$, тогда в силу монотонности f верно $f(f^{n-1}(\Theta)) \leq f(f^n(\Theta)) \Rightarrow f^n(\Theta) \leq f^{n-1}(\Theta)$.

Положим $a = \sup\limits_{n \geq 0} f^n(\Theta)$

Вычислим $f(a)$

$$f(a) = f(supf^n(\Theta)) = supf(f^n(\Theta)) =$$
$$= supf^{n+1}(\Theta) = sup\{f(\Theta), f(f(\Theta)), \ldots\} =$$
$$supf^n(\Theta) = a$$

Из этого следует, что a - неподвижная точка, то есть $f(a) = a$

Пусть $(\exists b \in A)(f(b) = b)$
Тогда $\Theta \leq b, f(\Theta) \leq f(b), \ldots$
То есть $(\forall n \geq 0)(f^n(\Theta) \leq b)$. Отсюда b - верхняя грань $\{f^n(\Theta)\}$. Так как $a = supf^n(\Theta)$, то $a \leq b$

Ч.Т.Д

Пример вычисления (из лекции):
На отрезке $[0, 1]$ рассмотрим уравнение $x = \frac{1}{2}x + \frac{1}{4}$
В данном случае $\Theta = 0$, так как 0 - наименьшее число.
Строим последовательность: $0, f(0), f^2(0), \ldots = 0, \frac{1}{4}, \frac{3}{8}, \frac{7}{16}, \ldots$

Получаем формулу: $f^n(0) = \frac{2^n-1}{2^{n+1}}$
Найдем супремум: $supf^n(0) = \lim_{n\to\infty} f^n(0) = \frac{1}{2}$

1.11 Алгебры, операции на множестве, свойства операций

1.11.1 Условие

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.

1.11.2 Операции на множестве

Определение. n-арная операция на множестве $A \neq \varnothing$, тогда
$\omega : A^k \to A, k \geq 0$

Простыми словами: A^k - это количество операторов (k операторов), а ω - это функция, которая из k элементов делает результат в виде 1-го элемента. Причем как и k операторов, так и результат находится в множестве A

Нулярная операция ($k = 0$) - это фиксированное значение $\omega(\lambda)$

Свойства операций:

1) Результат всегда существует

2) Результат принадлежит тому же множеству

Пусть $*$ - операция алгебры, Тогда:

- Ассоциативность
  $a * (b * c) = (a * b) * c$
- Коммутативность
  $a * b = b * a$
- Идемпотентность
  $a * a = a^n = a$

Относительно операции есть особые элементы. Пусть $*, +$ - операции алгебры, Тогда:

- Нуль (ноль, нулевой элемент)
  $a * 0 = 0$ и $a + 0 = a$
- Нейтральный элемент по отношению к операции $*$
  $a * \epsilon = a$

1.11.3 Алгебры

Определение. $\mathcal{A} = (A, \Omega)$ - это (Универсальная) алгебра, где A - это носитель, Ω - это сигнатура
$\Omega = \Omega^{(0)} \cup \Omega^{(1)} \cup \ldots \cup \Omega^{(n)} \cup \ldots$ - это все i-арные операции, где $i = \overline{0, \infty}$.

Носитель A - это всевозможные значения, которые можно получить с помощью операций, а также значения, которые могут принимать операторы.

Определение (Из интернета). Универсальной алгеброй называется совокупность непустого множества A и произвольного набора Ω заданных на A алгебраических операций. Записывается в таком виде: $\mathcal{A} = (A, \Omega)$

Примеры алгебр:

1) Числовые алгебры $(R, +, *, 0, 1)$

2.1) Векторные алгебры $\mathcal{L} = (L, +, \alpha, \theta)$

2.2) Векторные алгебры $\mathcal{V} = (V^3, +, \times, \overline{0})$

3) Матричные алгебры $\mathcal{M} = (\mathbb{M}, +, *, 0, E)$

Определение. Тип алгебры - это кортеж, составленный из арностей сигнатуры алгебры, то есть: $(\alpha_1, \alpha_2, \ldots, \alpha_n)$

Алгебры, имеющий один и тот же тип алгебры, называются однотипными.

1.12 Группоид, полугруппа, моноид, группа. Единственность нейтрального, обратного элементов

1.12.1 Условие

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

1.12.2 Группоид - группа

$\mathcal{A} = (G, *)$, где $*$ - бинарная операция.

Определение. Если операция $\mathcal{A}$ 'замкнута' (то есть результат есть в носителе A), то $\mathcal{A}$ - **группоид**.

Пример алгебры, который не имеет свойств группоида - это скалярное умножение векторов.

Определение. Если операция группоида ассоциативная, то этот группоид - **полугруппа**

Пусть ϵ - нейтральный элемент в полугруппе, тогда по отношению к его операции верно: $\epsilon * a = a * \epsilon = a$

Определение. Если в полугруппе есть нейтральный элемент, то он является **моноидом**.

Теорема (о единственности нейтрального элемента) Если полугруппа имеет нейтральный элемент, то он единственный

Доказательство ϵ', ϵ'' - нейтральные элементы.
$\epsilon' * \epsilon'' = \epsilon''$, так как ϵ' - нейтральный
$\epsilon'' * \epsilon' = \epsilon'$, так как ϵ'' - нейтральный
Тогда $\epsilon' = \epsilon''$

Пусть существует обратный элемент к a такой, что $a * a' = a' * a = \epsilon$

Определение. Если каждый элемент моноида обратим, то это **группа**

Теорема (о единственности обратного элемента) Если элемент моноида обратим, то обратный к нему единственный

Доказательство a', a'' - обратные элементы к a
$a'' = a'' * \epsilon = a'' * (a * a') = (a'' * a) * a' = \epsilon * a' = a'$

1.13 Циклическая полугруппа (группа)

Условие

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.

1.13.1 Циклическая группа и полугруппа

Определение. Группа $\mathcal{J} = (G, *, 1)$ называется циклической, если $(\exists a \in G)(\exists n \in \mathbb{Z})(\forall g \in G)(g = a^n)$, где a - образующий элемент.

$\mathcal{J} = [a] = [a^{-1}]$, где a - образующий элемент.

Образующий элемент не может существовать без обратного элемента. Если есть a, то есть a^{-1}

Примеры циклических групп:

- Бесконечная
  $(\mathbb{Z}, +, 0), \underline{n > 0} : n = 1 + 1 + 1 + \ldots + 1 = n * 1$
- Конечная
  $\mathbb{Z}_3^* = (\{1, 2\}, *_3, 1)$ - мультипликативная группа вычетов по модулю 3

Определение. Полугруппа $\mathcal{J} = (G, *, 1)$ называется циклической, если $(\exists a \in G)(\exists n \in \mathbb{Z})(\forall g \in G)(g = a^n)$, где a - образующий элемент.

В отличие от циклической группы Циклическая полугруппа не имеет обратных элементов, отчего образующие элементы не имеют обратных к себе, то есть неверно $\exists a \Rightarrow \exists a^{-1}$

Примеры циклических полугрупп:

- Бесконечная
  $(\mathbb{N}_0, +, 0), \underline{n > 0} : n = 1 + 1 + 1 + \ldots + 1 = n * 1$, где $\mathbb{N}_\nvDash$ - множество натуральных чисел начиная с нуля.
- Конечная
  Полугруппа $\mathcal{P}$ по операции сложения положительных натуральных чисел

Порядок конечной группы - это количество ее элементов, или $|G|$.

Порядком элемента конечной группы элемента a называется наименьшее $n > 0$, при котором $a^n = \epsilon$

Теорема (о равенстве порядка...). Порядок образующего элемента конечной циклической группы равен порядку группы

Доказательство. Пусть есть $[a]$ - конечная циклическая группа с образующим элементом a. Рассмотрим $\{1, a, a^2, \ldots, a^{n-1}\}$

Пусть найдутся 2 такие степени, что $a^p = a^q$, $0 < p < q < n$, где n - порядок элемента a

Тогда

$$a^p = a^q$$
$$a^p * a^{-q} = a^p * a^{-p}$$
$$a^{p-q} = 1, \text{ но p - q} < \text{n}$$

По определению n - наименьшая степень, при которой $a^n = 1 \Rightarrow$ противоречие.

1.14 Кольца

1.14.1 Условие

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).

1.14.2 Кольца, группа и моноид кольца

$\mathcal{R} = (R, +.*, 0, 1)$ - так выглядит кольцо

Аксиомы кольца:

1) $a + (b + c) = (a + b) + c$ - ассоциативность сложения
2) $a + b = b + a$ - коммутативность сложения
3) $a + 0 = a$ - 0 нейтральный элемент для сложения
4) $(\forall a \in R)(\exists a^{-1} \in R) : a + a' = 0$ - для любого числа по сложению есть обратный к нему
5) $a * (b * c) = (a * b) * c$ - ассоциативность умножения
6) $a * 1 = a$ - 1 нейтральный элемент умножения
7) $a*(b+c) = a*b+a*c$ - коммутативность умножения по сложению

Как можем заметить из аксиом кольца, операция сложения на носителе R создает группу, а операция умножения - моноид. Поэтому аддитивной группой кольца называется такая алгебра $\mathcal{G} = (R, +, 0)$, являющаяся группой, а мультипликативным моноидом такая - $\mathcal{M} = (R, *, 1)$, являющаяся моноидом. (Буквы алгебр неважны, поэтому можно не указывать)

Колько называется коммутативным, если его операция $*$ является коммутативной, то есть верно $a * b = b * a$

Кольца вычетов - это такие кольца, где все значения носителя меньше числа, по модулю которого идет вычет. Например кольцо вычетов по модулю 3 выглядит так: $\mathcal{Z}_3 = (\{0, 1, 2\}, +, *, 1, 0)$. В нем никогда не будет числа 3 и больше. $2 * 2 = 4\%3 = 1$

1.14.3 Теорема о тождествах кольца

1) $a * 0 = 0$

   Доказательство. Пусть Θ - неизвестная, значение которой нужно найти.
   $a + a * \Theta = a * 1 + a * \Theta = a(1 + \Theta) = a * 1 = a.$
   Найдем значение $\Theta : a + a * \Theta = a \Rightarrow a * \Theta = a - 1 \Rightarrow \Theta = 0$, где 0 - ноль кольца

2) $(-a) * b = (-ab)$

Доказательство. $(-a)b + ab = ((-a) + a)b = 0 * b = 0 \Rightarrow (-a)b$ - обратное к $ab \Rightarrow (-a)b = -(ab)$

3) $a * (b - c) = ab - ab$

Доказательство. $a*(b-c) = a*(b+(-c)) = ab+b(-c) = ab-bc$

1.15 Тела и поля

1.15.1 Условие

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

1.15.2 Тело и поле

Определение. Кольцо, в котором все ненулевые элементы обратимы по умножению, называется **телом**.

Определение. Тело с коммутативным умножением называется **полем**.

Пример поля - это обычная числовая прямая вещественных чисел.

1.15.3 Область целостности. (+делители нуля)

Определение. Областью целостности, или целостным кольцом, называют коммутативное кольцо без делителей нуля.

Определение. Делители нуля на примере: $a \neq 0, b \neq 0$, $a * b = 0 \vee b * a = 0$

Почему они называются делителями нуля? А потому, что обычное число состоит из простых и они являются его делителями. Вот с нулем в поле может случиться такая же ситуация - он состоит из делителей.

Теорема. Конечная область целостности является полем

Доказательство. $\mathcal{R} = (R, +, *, 0, 1)$ - конечная область целостности.

По определению примем, что $f_a(x) = ax, a \neq 0$ и $f_a : R\backslash\{0\} \to R\backslash\{0\}$

Докажем, что f_a - инъекция:
Пусть $ax = ay$, тогда $f_a(x) = f_a(y)$
Тогда $ax - ay = a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$, то есть $f_a(x) = f_a(y) \Rightarrow x = y$ - инъекция.

Посколько носитель - это конечное множество, то его инъекция считается биекцией: $(\forall y \neq 0)(\exists! x)(y = ax)$

В частности при $y = 1 : (\exists! x)(ax = 1)$, то есть $x = a^{-1}$. Из этого следует, что оно обратимо по умножению, значит, это поле.

1.15.4 Поля вычетов. Решение систем ЛУ в полях вычета

Поля вычетов - это такие поля, где все значения носителя меньше числа, по модулю которого идет вычет. Например поле вычетов по модулю 3 выглядит так: $\mathcal{Z}_3 = (\{0, 1, 2\}, +, *, 1, 0)$. В нем никогда не будет числа 3 и больше. $2 * 2 = 4\%3 = 1$

Пример решения в поле вычетов:

$$\mathbb{Z}_{19} : \begin{cases} 11x - 5y + z = 1 \\ 21x + 4y - z = 2 \\ 5x - 6z = 5 \end{cases}$$

Решаем методом Лагранжа с помощью матрицы коэффициентов:

$$\left(\begin{array}{ccc|c} 1 & -5 & 1 & 1 \\ -2 & 4 & -1 & 2 \\ 5 & 0 & 6 & 5 \end{array}\right)$$

Ответ: $(x, y, z) = \begin{pmatrix} 2 \\ 18 \\ 20 \end{pmatrix}$

Алгоритм:

1) Списываем коэффициенты перед x,y,z в матрицу, а также свободный член

2) Решаем ее методом Лагранжа, учитывая, что все операции по модулю поля вычета

2.1) Если число отрицательное (пусть -2 при кольце вычетов 19), то оно равно $(19 + (-2)) = 17$

1.16 Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы.

Условие

Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы.

1.16.1 Под[группа, моноид, полугруппа]

$\mathcal{J} = (G, *, 1)$ - группа.

$H \subseteq G$ замкнуто, если:

1) $1 \in H$

2) $(\forall x \in H)(x^{-1} \in H)$

3) $(\forall x, y \in H)(x * y \in H)$

Тогда $\mathcal{H} = (H, *, 1)$ - подгруппа группы $\mathcal{J}$

Более понятным языком. Есть подмножество носителя $H \subseteq G$. Если в подмножестве H есть единица группы, для всех x из множества H есть x^{-1} в H, а также для любой пары из H результат операции из группы $\mathcal{J}$ есть в множестве H, то $\mathcal{H}$ - подгруппа группы $\mathcal{J}$.

Вкратце про остальные два. Пусть есть группа $\mathcal{J} = (G, *, 1)$ и пусть есть $H \subseteq G$

Подмоноид:

1) Если $1 \in H$

2) Если $(\forall x, y \in H)(x * y \in H)$

То есть тоже самое, что и подгруппа, но без обратного элемента.

Подполугруппа:

1) Если $(\forall x, y \in H)(x * y \in H)$

Тоже самое, что и подмоноид, но только без требования к $1 \in H$.

Если все подытожить, то подгруппа обладает нейтральным элементом группы, для каждого числа есть к нему обратное в подгруппе, операция замкнута на носителе подгруппы. Подмоноид - это полугруппа без обратного элемента в носителе подгруппы. Подполугруппа не обладает к тому же еще и нейтральным элементом.

Пример. $(\mathbb{Z}, +, 0)$ - группа сложения целых чисел.

Тогда подгруппа этой группы: $\mathcal{H} = \{2n : n \in \mathbb{Z}\}$ - подгруппа всех четных чисел

Пример. $(\mathbb{N}, +, 0)$ - группа сложения натуральных чисел.

Тогда подмоноид этой группы: $\mathcal{H} = \{2n : n \in \mathbb{N}\}$ - подмоноид всех четных положительных чисел. Это является моноидом потому, что все числа натуральные, значит, в этом множестве нет обратных к любому числу по сложению (в натуральном множестве нет отрицательных). Однако число 0, являющееся нейтральным, присутствует в моноиде $\Rightarrow$ подмоноид.

Пример. $(\mathbb{N}, +, 0)$ - группа сложения натуральных чисел.

Тогда подполугруппа этой группы: $\mathcal{H} = \{n : n \in \mathbb{N} \,\&\, n \geq 1\}$ - подполугруппа всех натуральных чисел начиная с 1. Тут нет нейтральных элементов и нет обратных к любому элементу множества. Единственное, что выполняется здесь, это замкнутость операции.

1.16.2 Циклические подгруппы

$\mathcal{J} = (G, *, 1)$ - группа.

$a \in G$

$\mathcal{H} = \{a^n : n \in \mathbb{Z}\}$ - замкнута, так как:

- $1 = a^0 \in H$
- $a^p * a^q = a^{p+q} \in H$
- $(a^p)^{-1} = a^{-p} \in H$

a - образующий элеметь циклической группы. Тогда
$[a]$ - циклическая подгруппа группы $\mathcal{J}$

1.17 Смежные классы подгруппы. Теорема Лагранжа

1.17.1 Условие

Смежные классы подгруппы по элементу. Теорема Лагранжа.

1.17.2 Смежные классы

Пусть $\mathcal{H}$ - подгруппа группы $\mathcal{J} = (G, *, \epsilon)$. Пусть $a \in G$.

Тогда правый смежный класс: $a\mathcal{H}$

Тогда левый смежный класс: $\mathcal{H}a$

В общем случае $a\mathcal{H} \neq \mathcal{H}a$. Если они равны, то это нормальная подгруппа.

Теорема. Порядок любой конечной группы делится на порядок любой ее подгруппы

Доказательство Докажем 4 леммы:

1) Лемма 1
   $(\forall h \in H)(hH = H)$

   Доказательство:

   Пусть $x \in hH; x = hh_1, h_1 \in H, hh_1 \in H$.

   Пусть $x \in H \Rightarrow x = hh^{-1}x = h(h^{-1}x) \in hH$

2) Лемма 2
   $abH = a(bH)$

   Доказательство:

   Является прямым следствием ассоциативности операции группы.

3) Лемма 3
   Левые смежные классы образуют разбиение группы (носителя группы)

   Доказательство:

   $(\forall a \in G)(a \in aH)$, так как $1 \in H$

   Пусть $aH \cap bh \neq 0 \Rightarrow (\exists c)(c \in aH \cap bH)$. Тогда $c = ah_1 = bh_2$, где $h_1, h_2 \in H$.

   $b = abh_1h_2^{-1} \Rightarrow bH = (ah_1h_2^{-1})H = (ah_1)(h_2^{-1}H) = (ah_1)H = aH$.

4) Лемма 4
   Все левые смежные классы находятся в однозначном соответствии (то есть два таких класса образуют биекцию)

   Доказательство:

   $\varphi : H \to aH$

   $\varphi(h) \rightleftharpoons ah$

   φ - сюръекция, так как $(\forall x \in H)(x = ah = \varphi(h))$

   Пусть $\varphi(h_1) = \varphi(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2 \Rightarrow \varphi$ - инъекция

   Отсюда φ - биекция.

1.18 Полукольцо. Идемпотентное полукольцо

1.18.1 Условие

Полукольцо. Идемпотентное полукольцо. Естественный порядок идемпотентного полукольца

1.18.2 Полукольца

Определение (сжатое). Полукольцо - это кольцо, в котором по операции сложения нет обратного элемента

$\mathcal{S} = (S, +, *, 0, 1)$ - полукольцо.

Аксиомы полукольца:

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) $a * (b + c) = a * b + a * c$
7) $a * 0 = 0 * a = 0$

Определение. Полукольцо называется идемпотентным, если $a + a = a$

Естественный порядок кольца: $a \leq b \rightleftharpoons a+b = b$. Является отношением порядка, то есть Р+А+Т.

Из этого следует, что $a^n = a$

1.19 Замкнутое полукольцо. Итерация элемента

1.19.1 Условие

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

1.19.2 Замкнутое полукольцо

Определение. Идемпотентное полукольцо называется замкнутым, если:

1) Любая последовательность имеет точную верхнюю грань по естественному порядку

2) Для любых a и последовательности $\{X_n\}_{n\geq 0}$:
$a * supX_n = sup(a * X_n)$
$(supX_n) * a = sup(X_n a)$

Любое полукольцо, которое конечно, замкнуто.

1.19.3 Итерация элемента

Определение. Итерация - это точная верхняя грань последовательности всех ее степеней

В общем случае итерация - это бесконечное применение операции к одному и тому же элементу в какой-то степени.

Например, в полукольце бинарных операций по операции "или": $(Z_2, \vee, \wedge)$

$1^* = 1^0 \vee 1^1 \vee 1^2 \vee \ldots = \sum\limits_{i=0}^{\infty} 1^i$

В нашем случае $1^* = 1 \vee 1 \vee 1 \vee \cdots = 1$

Если в замкнутом полукольце 0 - наибольшее по естественному порядку, то итерация любого элемента равна: $a^* = 1$

1.20 Непрерывность сложения в замкнутом полукольце. Теорема о наименьшем решении ЛУ

1.20.1 Условие

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

1.20.2 Непрерывность сложения

Чтобы ее определить, нужна Теорема.

Теорема (о свойствах бесконечной суммы).

1) $\Sigma(a_n + b_n) = \Sigma a_n + \Sigma b_n$
2) Для любых a и последовательности $\{b_n\}$ верно:
   $a + \Sigma b_n = \Sigma(a + b_n)$
3) Если $S_n = \sum\limits_{i=0}^{n} a_i$, то $\Sigma S_n = \Sigma a_n$, где a_i - частичная сумма последовательности $\{a_n\}$

Доказательство.

1) $(a_n + b_n) + \Sigma a_n + \Sigma b_n = (a_n + \Sigma a_n) + (b_n + \Sigma b_n) = \Sigma a_n + \Sigma b_n$.
   $\Sigma a_n + \Sigma b_n$ - верхняя грань $\{a_n + b_n\}$
   Пусть $(\exists C)(\forall n)(a_n + b_n <= C)$. Тогда $a_n \leq a_n + b_n \leq C$ и $b_n \leq a_n + b_n \leq C$, то есть C - верхняя грань $\{a_n\}$ и $\{b_n\}$.
   $C + \Sigma a_n + \Sigma b_n = C + \Sigma b_n = C$
   Итак, мы доказали, что $\Sigma a_n + \Sigma b_n \leq C$, то есть $\Sigma a_n + \Sigma b_n = \Sigma(a_n + b_n)$
2) Является прямым следствием первого, когда одна из последовательностей постоянная

Отсюда можно доказать непрерывность сложения. В следствие второго пункта сложение непрерывно: $f(x) = a + x$
$f(\Sigma X_n) = a + \Sigma X_n = \Sigma(a + X_n) = \Sigma f(X_n)$

1.20.3 Теорема о наименьшем решении

Теорема. Наименьшим решением $x = ax + b$ и $x = xa + b$ в замкнутых полукольцах будет соответственно $x = a^*b$ и $x = ba^*$

Доказательство. Используем формулу для вычисления наименьшей неподвижной точки и, записывая в случае замкнутого полукольца как бесконечную сумму, получим для уравнения решение в виде $x = a^*b$
$x = \sum\limits_{n=0}^{\infty} f^n(\Theta)$ - где Θ - нуль полукольца и $f(x) = ax + b$
Учитывая, что $f^0(\Theta) = b, f^1(\Theta) = ab + b, \ldots$ получаем $\sum\limits_{n=0}^{\infty} f^n(\Theta) = \sum\limits_{n=1}^{\infty}(1 + a + \ldots + a^n)b$

Используя непрерывность умножения вынесем b:
$\left(\sum\limits_{n=1}^{\infty}(1+a+\ldots+a^n)\right)b$

Так как $1+a\ldots+a^n$ - частичная сумма $\{a^n\}_{n\geq 0}$. Тогда
$\sum\limits_{n=0}^{\infty}(1+a\ldots a^n)=\sum\limits_{n=0}^{\infty}a^n=a^* \implies a^*b=f^n(\Theta)$

Из этого следует, что мы нашли точную верхнюю грань частичной суммы, значит мы нашли мы нашли точную верхнюю грань последовательности. Тогда окончательно получаем $x=a^*b$ в замкнутом полукольце

1.21 Квадратные матрицы размером n над идемпотентным полукольцом. Решение СЛУ в замкнутых полукольцах

1.21.1 Условие

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

1.21.2 Ответ

Ответ будет получен по ходу рассуждения. Будет описано решение СЛУ, а также почему и как определяется полукольцо квадратных матриц над полукольцом СЛУ.

Существует 2 вида ЛУ:
$x = ax + b$ (1) - праволинейное уравнение
$x = xa + b$ (2) - леволинейное уравнение

$x = f(x)$
$f(x) = ax + b$ - непрерывна по теореме (о свойствах бесконечных сумм)

В силу теоремы о наименьшей неподвижной точки:
$x = supf^{(n)}(0), n \geq 0$ - n-кратное применение 0

$supf^{(n)}(0) = \{0, b, ab + b = (a + 1)b, a(ab + b) + b, \ldots, (1 + a + \ldots + a^n)b, \ldots\} = \sum\limits_{n=1}^{\infty}(1 + a + \ldots + a^{n-1})b = \sum\limits_{n=0}^{\infty}(1 + a + \ldots + a^n)b = (\sum\limits_{n=0}^{\infty}a_n)b$
$\sum\limits_{n=0}^{\infty}a_n \rightleftharpoons a^*$ - итерация (замыкание) a

То есть решение $x = a^*b$ или $x = ba^*$

Решение СЛУ в замкнутом полукольце СЛУ в полукольцах: (3)

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

Составим матрицу $A = (a_{ij})_{m\times n}$, где m, n - размер матрицы.

$\mathcal{S} = (S, +, *, 0, 1)$ - Идемпотентное полукольцо.
Рассмотрим такую алгебру матриц: $\mathcal{M}(\mathcal{S}) = (M_n(S), +, *, 0, E)$

Операция сложения: $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n} \Rightarrow C = A + B = (a_{ij} + b_{ij})_{m\times n}$
Операция умножения: $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n} \Rightarrow C = A + B = (\sum\limits_{k=1}^{n}a_{ik}b_{kj})_{m\times p}$

Так как $m = n$ (матрицы квадратные), то все операции замкнуты. Множество $M_n(S)$ - это множество квадратных матриц размером n и со значениями элементов из носителя полукольца $\mathcal{S}$.

Теорема. Алгебра $\mathcal{M}(\mathcal{S})$ есть идемпотентное полукольцо. Если кольцо $\mathcal{S}$ замкнуто, то и полукольцо $\mathcal{M}(\mathcal{S})$ тоже замкнуто

Из этой теоремы следует, что мы можем решить такие уравнения:
$X = AX + B$ и $X = XA + B$ (4)
То есть в $\mathcal{M}(\mathcal{S}) \implies X = A^*B$ (5)

Система (3) в матричной форме (ε - столбец β - столбец):
$\varepsilon = A\varepsilon + \beta$, где $\varepsilon = (x_1, x_2, \ldots, x_n)^T$, $\beta = (b_1, b_2, \ldots, b_n)^T$ (6)

Матричное уравнение может быть расписано по столбцам:
$\varepsilon_j = A\varepsilon_j + \beta_j$, $1 \leq j \leq n$ (7)
Тогда в матрицах это выглядит так:
$X = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j, \varepsilon_n]$
$B = [\beta_1, \beta_2, \ldots, \beta_n]$

Матрица (4) разрешима в виде (5). (4) может быть расписано как (7). (7) разрешимо, так как вся матрица разрешима. И решение для каждого столбца $\varepsilon_j = A^*B, 1 \leq j \leq n$. То есть $\varepsilon = A^*B$

Элементы теории графов

2.1 Основные понятия теории графов

2.1.1 Условие

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

2.1.2 Неориентированный граф

Определение. $\mathcal{G} = (V, E)$ - неориентированный граф, где
V - конечное мнодество вершин графа.
E - Множество смежностей, или множество неупорядоченных пар на V, то есть подмножество множества двуъэлементных подмножеств V, элементы которого называются ребрами

Определение. Цепь в неорграфе - это последовательность вершин G $v_0, v_1, \ldots, v_n, \ldots$ такая, что $(v_i - v_{i+1})(\forall i)(\exists v_{i+1})$, если v_{i+1} определен в последовательности. Под конечной последовательностью понимается кортеж вершин

Определение. Цепь называется простой, если все ее вершины (кроме, может быть, первой и последней) попарно различны.

Определение. Цикл - простая цепь ненулевой длины с совпадающими концами.

Определение. Ребро e называется инцидентным вершине v, если она является одним из его концов.

2.1.3 Ориентированный граф

Определение. $\mathcal{G} = (V, E)$ - ориентированный граф, где
V - конечное множество вершин графа.
E - Множество смежностей, или множество упорядоченных пар на V, то есть подмножество множества $V \times V$, элементы которого называются дугами.

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

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

Определение. Путь в орграфе: последовательность вершин $u_0, u_1, u_2, \ldots, u_n, \ldots$, где $(\forall i \geq 0)(u_i \to u_{i+1})$, если u_{i+1} определен в последовательности.

Определение. Простой путь - это такой путь, если все его вершины (кроме, может быть, первой и последней) попарно различны.

Определение. Контур - это простой ненулевой длины путь, в котором совпадают начало и конец.

2.1.4 Подграф

Определение. Неориентированный (ориентированный) граф $\mathcal{G}_1 = (V_1, E_1)$ называют подграфом неориентированного (ориентированного) графа $\mathcal{G} = (V, E)$, если $V_1 \subseteq V, E_1 \subseteq E$.

2.2 Связность неорграфа, компонента связности неорграфа

2.2.1 Условие

Связность неориентированного графа. Компоненты связности.

2.2.2 Ответ

Определение. Неориентированный граф называют связным, если любые две его вершины U и V соединены цепью.

Определение. Компонента связности неографа - это максимальный связный подграф текущего графа.

2.3 Связность орграфа (слабая сильная). Компонента связности (слабая, сильная)

2.3.1 Условие

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

2.3.2 Связность орграфа

Определение. Ориентированный граф называют связным, если для любых двух его вершин U, V вершина V достижима из U или наоборот.
$(\forall U, V)((U \Rightarrow^* V) \vee (V \Rightarrow^* U))$

Определение. Граф является слабо связанным, если ассоциированный с ним неорграф является связным

Определение. Граф является сильно связанным, если для любых двух его вершин U, V вершина U достижима из V и наоборот
$(\forall U, V)(U \Rightarrow^* V \ \& \ V \Rightarrow^* U)$

Определение. Компонента связности (сильная, слабая) ориентированного графа - это максимальный связный (слабо, сильно) подграф.

Теорема. Если в орграфе из u достижима v, то существует простой путь из u в v

Следствия из теоремы. Если в орграфе вершина лежит на простом замкнутом пути, то она лежит на контуре. Если в неорграфе 2 вершины соединены цепью, то существует простая цепь, соединяющая их. Если в неорграфе вершина лежит на замкнутой цепи, то она лежит на цикле.

2.4 Поиск в глубину. Древесные и обратные ребра

2.4.1 Условие

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

2.4.2 Алгоритм

T - древесные ребра, FC - фундаментальные циклы

```
begin
        T, B, FC := 0; stack := 0;
        count := 1;
        for all v in V
                NEW[V] := 0;
        for all v in V
                while (exists V)(NEW[V] = 1) do
                        search_D(V);
end;

proc search_D(v)
        NEW[V] := 0;
        D[V] := count; count := count + 1;
        v -> stack;

        for all (w in L[V]) do
                if (NEW[w]) then begin
                        {V,w} -> T;
                        search_D(w);
                end;
                else if ({V,w} not in T) then
                        if ({V,w} not in B) then begin
                                {V,w} -> B;
                                read(V..w) -> FC;
                        end;
        stack -> V;
end;
```

2.4.3 Типы дуг

Определение. Лес, который строится методом поиска в глубину, называется глубинный остовный лес

Определение. Древесные дуги (T) - это те дуги, которые ведут от отца к сыну в глубинном остовном лесе.
$D[v] < D[\omega]$
$NEW[w] = 1$

Определение. Обратные дуги (B) - это те дуги, которые ведут от потомка к предку в глубинном остовном лесу.
$D[v] \geq D[\omega]$
$NEW[\omega] = 0$

$\omega \in stack$

Определение. Прямые дуги (F) - это те дуги, которые ведут от подлинного предка к подлинному потомку, НО не от отца к сыну в глубинном остовном лесу.

$D[v] < D[\omega]$

Определение. Поперечные дуги (C) - это все остальные дуги в глубинном остовном дереве.

$D[v] > D[\omega]$

$\omega \notin stack$

2.5 Поиск в глубину в орграфе. Классификация дуг в орграфе.

2.5.1 Условие

Поиск в глубину в орграфе. Классификация дуг. Критерий бесконтурности

2.5.2 Алгоритм

```
begin
        T,B,C,F,C := 0; stack := 0;
        for all v in V do
                NEW[v] := 1;
        const := 1;

        for all v in V do
                while (exists v)(NEW[v] = 1) do
                        search_DOR(v);
end;

proc search_DOR(v)
        NEW[v] := 0;
        D[v] := const; const := const + 1;

        v -> stack;
        for all w in L[v] do
                if NEW[w] then begin
                        (v,w) -> T;
                        search_DOR(w);
                end;
                else begin
                        if (D(v) >= D(w)) & (w in stack) then
                                (v,w) -> B;
                        if (D(v) < D(w)) then
                                (v,w) -> F;
                        if (D(v) > D(w)) & (w not in stack) then
                                (v,w) -> C;
                end;
end;
```

2.5.3 Классификация дуг

Определение. Лес, который строится методом поиска в глубину, называется глубинный остовный лес

Определение. Древесные дуги (T) - это те дуги, которые ведут от отца к сыну в глубинном остовном лесе.
$D[v] < D[\omega]$
$NEW[w] = 1$

Определение. Обратные дуги (B) - это те дуги, которые ведут от потомка к предку в глубинном остовном лесу.
$D[v] \geq D[\omega]$

$NEW[\omega] = 0$
$\omega \in stack$

Определение. Прямые дуги (F) - это те дуги, которые ведут от подлинного предка к подлинному потомку, НО не от отца к сыну в глубинном остовном лесу.
$D[v] < D[\omega]$

Определение. Поперечные дуги (C) - это все остальные дуги в глубинном остовном дереве.
$D[v] > D[\omega]$
$\omega \notin stack$

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

2.6 Поиск в ширину в орграфе

2.6.1 Условие

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.

2.6.2 Алгоритм.

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

```
begin
        for all v in V do
                M[v] = infinity;
        Q := 0;
        M[v0] := 0;
        v0 -> Q;

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

Алгоритм волнового фронта.
$\mathcal{G} = (V, E)$ - орграф, $\varphi = E \to R^+$ - функция разметки

```
begin
        for all (v in V) do
                M[v] := infinity;
        Q := 0;
        M[v0] := 0
        v0 -> Q;

        for all (v in Q)
                while (Q != 0) do
                        for all (w in L[v]) do begin
                                d := M[v] + phi(v,w);
                                if (d < M[w]) then begin
                                        M[w] := d;
                                        if (w not in Q) then
                                                w -> Q;
                                end;
                                Q -> v;
                        end;
end;
```

2.7 Изоморфизм графов. Автоморфизмы

2.7.1 Условие

Изоморфизм графов. Группа автоморфизмов графа и ее вычисление

2.7.2 Изоморфизм графов

Пусть даны графы: $\mathcal{J}_1 = (V_1, \rho_1), \mathcal{J}_2 = (V_2, \rho_2)$

Определение. Биекция $h : V_1 \to V_2$ называется изоморфизмом графа $\mathcal{J}_1$ на граф $\mathcal{J}_2$, если верно $(\forall(u, v) \in V_1)(h(u)\rho_2 h(v))$

Выражение вида $(\forall(u, v) \in V_1)(h(u)\rho_2 h(v))$ можно записать в виде $u\rho v$ (что говорит о том, что две вершины смежны). Автоморфизм кратко записывается в виде $\mathcal{J}_1 \simeq \mathcal{J}_2$

В неорграфе $\mathcal{J}_1 \simeq \mathcal{J}_2 \leftrightharpoons (\forall u, v \in V_1)(h(u) - h(v) \iff u - v)$, где знак '-' - это ребро между вершинами графа.

Для орграфа (неорграфа) верно: если $\mathcal{J}_1 \simeq \mathcal{J}_2$, то $(\forall u \in V_1)(dg(u) = dg(h(u)))$, то есть степень вершины не меняется.

2.7.3 Автоморфизм графа

Определение. Изоморфизм графа самого на себя называют автоморфизмом графа.

Некоторые свойства автоморфизмов:

- Если g, h - автоморфизм, то $g \circ h$ - тоже автоморфизм
- Если h - автоморфизм, то h^{-1} - тоже автоморфизм
- Тождественная подстановка (ε) тоже автоморфизм

Группу автоморфизмов графа записывают так: $Aut(\mathcal{J})$

Способы вычисления группы автоморфизмов. Пусть дан граф $\mathcal{J}$.

Первый способ - это найти орбиту $orb(S)$ и стабилизатор G_S какой-то одной вершины.

Определение. Орбита - это подмножество вершин графа, в которые может перейти текущая вершина в результате действия автоморфизмов. Записывается так: $S \subseteq M : orb(S) \leftrightharpoons \{t : (\exists\delta \in G)(t = \delta(S))\}$, где S - вершина, а δ - перестановка всех вершин и $\delta(S)$ - вершина, стоящая вместо вершины S в автоморфизме.

Пример: пусть дан граф в виде квадрата. Тогда любая вершина может стоять на месте любой другой вершины. То есть в орбите будет 4 вершины: $\mid orb(S) \mid = 4$, и если задать номера вершинам квадрата (1, 2, 3, 4), то $orb(S) = \{1, 2, 3, 4\}$

Определение. Стабилизатор вершины - это такое подмножество вершин графа, в которым не меняется место текущей вершины в результате действий автоморфизма. Записывается так: $G_S \leftrightharpoons \{\delta : \delta(S) = S\}$

Второй способ - комбинаторный. Нужно найти всевозможные комбинации поворотов, отражений и т.п.

2.8 Задача о путях в орграфе. Алгоритм Флойда-Уоршелла-Клини

2.8.1 Условие

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.

2.8.2 Ответ

Определение. Размеченным ориентированным графом называют пару $W = (\mathcal{G}, \phi)$, где $\mathcal{G} = (V, E)$ - обычный орграф, $\phi : E \to R$ - функция разметки в некотором идемпотентном полукольце $\mathcal{S} = (S, +, *, \mathbb{O}, 1)$ и $(\forall e \in E)(\phi(e) \neq 1)$

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 сводится к вычислению матрицы достижимости:

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

Если задать орграф с помощью матрицы метод 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 сводится к поиску кратчайшего расстояния между узлами графа, то есть к расчету матрицы кратчайших расстояний:

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

В обоих случаях нужно найти матрицу C, которая называется в матрицей стоимостей (cost)

Теорема. $C = A^*$ (матрица стоимостей равна итерации матрицы A)

В общем случае придется решить такую систему уравнений:

$$\begin{cases} x_1 = a_{11}x_1 + \ldots + a_{1j}x_j + \ldots + a_{1n}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_j = a_{j_1}x_1 + \ldots + a_{ij}x_j + \ldots + a_{jn}x_n + \Theta \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = a_{n_1}x_{11} + \ldots + a_{nj}x_j + \ldots + a_{nn}x_n \end{cases}$$

Где x_j - выбранная вершина, а Θ - нейтральный элемент по умножению. При решении мы получаем j-ый столбец матрицы C. То есть решение для x_1 - это первый столбец матрицы C.

В зависимости от того, как задана матрица, мы выбираем разные полукольца. В случае задачи на достижимость выбирается $\mathbb{B} = (\{0, 1\}, max, min, 0, 1)$ В случае задачи на кратчайший путь выбирается $\mathcal{R}^+ = ([0, +\infty], min, +, +\infty, 0)$

Регулярные языки и конечные автоматы

3.1 Алфавит, слово, язык

3.1.1 Условие

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

3.1.2 Алфавит, слово, язык

Определение. Алфавит - это множество всех букв (буквами может быть что угодно). $V = \{a_1, \ldots, a_n\} \neq \varnothing$

Определение. Слово - это цепочка в алфавите (кортеж): $a_{i_1}, a_{i_2}, \ldots, a_{ik} = x$ или $x = x(1)x(2)\ldots x(k)$ или $x \in V^k, k \geq 0$

Определение. Пустое слово $\{\lambda\} = V^0$

Определение. Длина слова $= \mid x \mid = k \leftrightharpoons x \in V^k, k \geq 0, \mid \lambda \mid = 0$

Определение. Язык - это итерация алфавита. $\mathcal{L} \subseteq V^*$.

Различают несколько видов итераций.

Определение. Итерация: $V^* \leftrightharpoons \bigcup_{k=0}^{\infty} V^k$

Определение. Положительная итерация: $V^+ \leftrightharpoons V^* \backslash \{\lambda\}$

3.1.3 Операции над языками

Зададим операции над словами:
Сложение: $x = x(1)x(2)\ldots x(k), y = y(1)y(2)\ldots y(m), k, m \geq 0$
$xy = x(1)x(2)\ldots x(k)y(1)y(2)\ldots y(m)$
$\mid xy \mid = \mid x \mid + \mid y \mid$
Свойства этой операции:

- $(xy)z = x(yz)$
- $xy \neq yx$
- $(\forall\lambda)(\lambda x = x\lambda = x)$

Операции над языками:

- Теоретико-множественные операции $(\cap, \cup, \ \backslash \ , \triangle, \ldots)$
- Соединение языков: $L_1 * L_2 \leftrightharpoons \{xy : x \in L_1, y \in L_2\}$

Можем сделать полукольцо языков:
$\mathcal{L}_V = (2^{V^*}, \cup, *, \varnothing, \{\lambda\})$ - замкнутое полукольцо

Теорема. Алгебра $\mathcal{L}_{V_1}$ - является замкнутым полукольцом.

Доказательство. Используя аксиомы полукольца:
1)$K \cup (L \cup M) = (K \cup L) \cup M$
2)$K \cup L = L \cup K$
3)$L \cup \varnothing = L$
4)$L \cup L = L$
5)$K * (L * M) = (K * L) * M$
6)$L\{\lambda\} = L$
7)$K * (L \cup M) = K * L \cup K * M$
8)$L * \varnothing = \varnothing * L = \varnothing$
Докажем 7-ю аксиому.
$x \in K * (L \cup M) \leftrightharpoons x = yz, y \in K, z \in L \cup M \leftrightharpoons y \in K, z \in L \vee z \in M \leftrightharpoons yz \in K * L \vee yz \in KM \leftrightharpoons yz = x \in KL \cup KM$

Определение. $L^* = \bigcup_{n=0}^{\infty} L^n$ - итерация языка $(L^0 \cup L \cup L^1 \cup \ldots)$

Определение. $L^+ = \bigcup_{n=1}^{\infty} L^n$ - положительная итерация языка (без $\{\lambda\}$)

3.2 Регулярные языки и регулярные выражения

3.2.1 Условие

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

3.2.2 Регулярные языки

Определение. 1) $\varnothing, \{\lambda\}, \{a\}$ - регулярные языки в алфавите V
2) L_1, L_2 - регулярные $\implies L_1 \cup L_2, L_1 * L_2$ - тоже регулярные
3) L - регулярный язык $\implies L^*$ - регулярный язык
4) Других регулярных языков не существует

3.2.3 Полукольцо регулярных языков, регулярные выражения

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

Определение. Полукольцо с итерацией - это полукольцо, которое содержится в некотором замкнутом полукольце и вместе с каждым своим элементом содержит его итерацию по определению.

Определение. Регулярное выражение - это формула, обозначающая какой-то регулярный язык ($a \mapsto \mathcal{L}$)

Рассмотрим некоторые формулы регулярных выражений:

- $\varnothing \mapsto \varnothing$
- $\lambda \mapsto \{\lambda\}$
- $a \mapsto \{a\}_V$
- $\alpha \mapsto K, \beta \mapsto L \implies (\alpha + \beta) \mapsto K \cup L, (\alpha * \beta) \mapsto K * L$
- $\alpha \mapsto L \implies \alpha^* \mapsto L^*, \alpha^+ \mapsto L^+$
- Других регулярных выражений нет.

3.3 Конечный автомат и регулярный язык, допускаемый КА

3.3.1 Условие

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

3.3.2 Конечный автомат и язык, допускаемый им

Определение. Пусть V - некоторый алфавит, тогда конечный автомат с входным алфавитом V по определению орграф $\mathcal{J}$, размеченный над $Reg(V)$, при этом по определению $(\forall e \in E)(\varphi(e) = \{\lambda\} \vee \varphi(e) \subseteq V)$

При этом $\varphi(e) \neq \varnothing$, задана начальная вершина $q_0 \in Q$ и задано множество вершин F, называемых заключительными.

Тогда конечный автомат может быть задан так:
$M = (Q, E, \varphi, q_0, F)$, где
Q - множество состояний КА
E - множество дуг КА
φ - функция разметки КА
q_0 - входная вершина
$F \subseteq Q$ - подмножество заключительных состояний

Определение. КА допускает цепочку x, если она читается на некотором пути из входной вершины в одну из заключительных вершин.

Определение. Язык, допускаемый КА, - множество всех допускаемых цепочек КА

Определение. Задача синтеза КА - задача построения КА по регулярному языку

Определение. Задача анализа КА - задача вычисления регулярного языка по КА

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

3.4 Теорема Клини

3.4.1 Условие

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

3.4.2 Ответ

Теорема. Язык регулярен тогда и только тогда, когда он допускается конечным автоматом.

Доказательство. 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. выражения

$x = \lambda^* \beta$ - регулярный язык

Предположим: пусть для любого порядка $\leq n-1$ утверждение верно ($n \leq 2$)

Рассмотрим систему n-го порядка:

$$\begin{cases} x_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1 \\ x_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n + b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = a_{n_1}x_1 + a_{n_2}x_2 + \ldots + a_{nn}x_n + b_b \end{cases}$$

$A = (a_{ij})_{n \times n}$ - регулярные выражения

Тогда выразим x_1:

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

Подставим его во все остальные:

$$\begin{cases} x_2 = a_{21} * a_{11}^*(a_{12}x_2 + \ldots + a_{1n}x_n + b_1) + a_{22}x_2 + \ldots + a_{2n}x_n + b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = a_{n_1} * a_{11}^*(a_{12}x_2 + \ldots + a_{1n}x_n + b_1) + a_{n_2}x_2 + \ldots + a_{nn}x_n + b_n \end{cases}$$

После приведения подобных членов в правых частях, получим систему с регулярными коэффициентами порядка $n-1$, решение которой регулярно по предположению

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

Теорема. Для каждого регулярного языка может быть построен КА, допускающий этот язык

Доказательство. Сделать рисунки синтеза КА (НЕ СДЕЛАНО, НО БУДЕТ)

3.5 Детерминизация КА

3.5.1 Условие

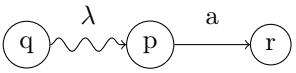
Детерминизация КА. Регулярность дополнения регулярного языка и пересечения двух регулярных языков. Проблемы пустоты и эквивалентности

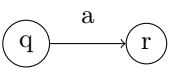
3.5.2 Детерминизация КА

Определение. КА называют детерминизированным, если в нем отсутствуют λ-переходы, а также $(\forall q \in Q)(\forall a \in V)(\mid \delta(q,a) \mid = 1)$, где $q \in Q$ - состояние, $a \in V$ - дуга, то есть выражение $\mid \delta(q,a) \mid = 1$ говорит о том, что переход в детерминизированном КА производится ровно в 1 состояние.

Теорема. Для любого КА может быть построен эквивалентный ему детерминизированный КА.

Алгоритм детерминизации:
Дано: КА $M = (V, Q, q_0, F, \delta)$
Строим: КА $M' = (V, Q', q_0', F, \delta')$
1) Удаление λ-переходов

Уберем λ-переход: 

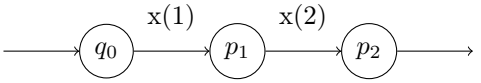
Получаем в детерминированном: 

$Q' = \{q_0\} \cup \{q : (\exists r \in Q)(\exists a \in V)(r \mapsto_a q)\}$
$qo' = q_0$
$F' = (F \cap Q') \cup (f : (\exists q \in Q)(q \Rightarrow^* q_f, q_f \in F))$
$\delta'(q,a) = \delta(q,a) \vee \{r : (\exists p \in Q)(q \Rightarrow_\lambda^* p \mapsto_a r)\}$

Теорема. Дополнение регулярного языка регулярно.

Доказательство. Пусть $\mathcal{L}$ - регулярный язык. Тогда язык $\mathcal{L} = L(M)$ (язык, допускаемый КА), где $M = (V, E, q_0, F, \delta)$ - детерминированный КА.

Пусть $x \subseteq V^* : x = x(1)x(2)\dots x(k), k \geq 0$



Тогда
$x \in L \iff p_k \in F$
$\begin{cases} x \notin L \iff p_k \notin F \\ x \in \overline{L} \end{cases}$

$\overline{M} = (V, Q, q_0, Q \setminus F, \delta)$
$L(\overline{M}) = \overline{L}$

Следствие. Если L_1, L_2 - регулярные языки, то $L_1 \setminus L_2, L_1 \cap L_2, \dots$ - регулярные языки.

3.5.3 Проблемы

Проблема пустоты. Выяснить, не является ли язык, допускаемый КА, пустым?

Решается поиском в ширину, фронтом. Пуст, если из начала недостижима ни одна вершина F.

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

Решается, скорее всего, синтезом регулярных языков двух КА. Если языки равны, то равны и КА.

3.6 Лемма о разрастании для регулярных языков

3.6.1 Условие

Лемма о разрастании для регулярных языков

3.6.2 Ответ

Теорема. Для любого регулярного языка $\mathcal{L} \subseteq V^*$ существует числовая константа k_L такая, что $(\forall x \in L)(|\ x\ | \geq k_L \implies x = uvw)$, где $0 <| v |\leq k_L$ и $(\forall n \geq 0)(x_n = uv^n w \in \mathcal{L})$

Доказательство. Пусть $\mathcal{L} \subseteq V^*$ - регулярный язык. Тогда $\mathcal{L} = L(M)$, $M = (V, E, q_0, F, \delta)$ - детерминированный КА.

Положим $k_L = |Q|$ и пусть $x = x(1)x(2)\dots x(l)$, где $l \geq k_L = |Q|, x \in L$

$l \geq |Q| \implies$ число вершин пути $\geq |Q| + 1$, то существует вершина, которая повторится и будет на контуре.

$x = uvw$

$x_0 = uw \in L$, так как v на контуре, а в контур можно не заходить.

$(\forall n \geq 1)(x_n = uv^n w \in L)$, где n - сколько раз проходим по контуру. Причем контур ненулевой длины: $0 < |v| \leq k_L = |q|$

Следствие. Из любого бесконечного регулярного языка найдется последовательность цепочек, которые формируют арифметическую прогрессию, то есть $|x_{n+1}| = |x_n| + |v|$

Элементы Комбинаторики

4.1 Формулы включения и исключения. Формула для числа сюръекций

4.1.1 Условие

Формулы включения и исключения (без вывода). Формула для числа сюръекций (с выводом)

4.1.2 Формула включения и исключения

Формула включения:

$$|A_1 \cap A_2 \cap \ldots \cap A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1 < i_2 < \ldots < i_k} |A_{i1} \cap A_{i2} \cap \ldots \cap A_{ik}|.$$

Формула исключений:

$$|\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_n}| = |U| - \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1 < i_2 < \ldots < i_k} |A_{i1} \cap A_{i2} \cap \ldots \cap A_{ik}|.$$

4.1.3 Формула для числа сюръекций

Сразу выведем формулу для числа сюръекций.

Пусть есть $|A| = m, |B| = n, m \geq n$
$W_i = \{f : f \in B^A, b_i \notin R(f)\}$, $R(f)$ - область значений f
$|W_i| = (n-1)^m$

$W_{i1} \cap W_{i2} \cap \ldots W_{ik} = \{f : i_1, i_2, \ldots, i_k \notin R(f)\}$
$|W_{i1} \cap W_{i2} \cap \ldots W_{ik}| = (n-k)^m$
$C_n^k (n-k)^m = \sum_{i_1 < i_2 < \ldots < i_k} |W_{i1} \cap W_{i2} \cap \ldots W_{ik}|$

Число отображений, не являющихся сюръекцией:
$\sum_{k=1}^{n} (-1)^{k+1} C_n^k (n-k)^m$
Тогда число сюръекций:
$S(m,n) = n^m - \sum_{k=1}^{n} (-1)^{k+1} C_n^k (n-k)^m = \sum_{k=0}^{n} (-1)^k C_n^k (n-k)^m$

4.2 Однородные линейные рекуррентные соотношен

4.2.1 Условие

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

4.2.2 Ответ

Определение. Пусть дана числовая последовательность вида $\{x_n\}_{n\geq 0}$, причем она не определена явно как функция натуральной переменной, но всякий ее член выражается через k предыдущих (для фиксированного k) в виде:

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

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

Если функция φ линейна по своим аргументам, то такое соотношение называется линейным. Будем, как правило, записывать линейное рекуррентное соотношение в виде:

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

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

В рассмотрении таких соотношений мы полагаем, что коэффициенты числа. То есть рассматриваются рекуррентные соотношения с постоянными коэффициентами.

Общий вид k-го порядка:

$x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$ (4)

Пусть есть начальные условия: $x_0 = a_0, x_1 = a_1, \ldots, x_{k-1} = a_{k-1}$

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

Теорема о связи между решениями и начальными условиями. Заданные начальные условия (2) однозначно определяют частное решение соотношения (4) Наоборот, фиксированное частное решение соотношения однозначно определяет начальные условия, которым она удовлетворяет.

Доказательство. Пусть выполняются начальные условия вида (2):

$y_0 = \alpha_0, \ldots y_{k-1} = \alpha_{k-1}$ (6)

Тогда в силу (4): $y_k = -a_1 y_{k-1} - \ldots - \alpha_k y_0$, и далее для любого $s > 0$ верно $y_{k+s} = -\alpha_1 y_{k+s-1} - \ldots - \alpha_k y_s$ и член y_n определен однозначно для любого $n \geq 0$

Пусть теперь y_n - какое-то частное решение соотношения (4).

Покажем, что числа $\alpha_0, \ldots, \alpha_{k-1}$ можно подобрать так, чтобы выполнялось (6).

Имеем: (7)

$$\begin{cases} y_k + a_1\alpha_{k-1} + \ldots + a_k\alpha_0 = 0 \\ y_{k+1} + a_1\alpha_k + \ldots + a_k\alpha_1 = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_{2k-1} + a_1\alpha_{2k-2} + \ldots + a_{k-i}\alpha_k + a_k\alpha_{k-1} = 0 \end{cases}$$

Система (7) есть система относительно неизвестных $\alpha_0, \ldots, \alpha_{k-1}$, заданная в треугольной форме. Из последнего уравнения однозначно определяется α_{k-1}, и далее (обратным ходом метода Гаусса) все остальные члены 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).

4.3 Теорема об общем решении ОЛРС

4.3.1 Условие

Теорема об общем решении ОЛРС как линейной комбинации фундаментальных решений

4.4 Ответ

Теорема 3. Любое решение соотношения $x_n+a_1x_{n-1}+\ldots+a_kx_{n-k}=0$ (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 решениями и обратно.

Имеем такую систему для определения этих коэффициентов: (8)

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

Причем: (9)

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

где $\triangle$ 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 $C_i, i = \overline{1,k}$ не все равные нулю, для которых бы выполнялось:

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

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 $x_0 = \alpha_0, \ldots, x_{k-1} = \alpha_{k-1}$

Итак, 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)

4.5 Характеристический полином

4.5.1 Условие

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

4.5.2 Характеристический полином и хар-ое ур-ие

Ответ на все вопросы будет получен в ходе рассуждения

Теорема 1. Пусть $y_n^{(1)}$ и $y_n^{(2)}$ - решения рекуррентного соотношения. Тогда их произвольная линейная комбинация тоже является решением соотношения.

Доказательство. Пусть $\varphi_n = C_1 y_n^{(1)} + C_2 y_n^{(2)}$. Подставим φ_n в соотношение $x_n + a_1 x_{n-1} + \ldots + a_{k-1} x_{n-k} = 0$.

Будем иметь:

$$
\begin{aligned}
&C_1 y_n^{(1)} + C_2 y_n^{(2)} + a_1 (C_1 y_{n-1}^{(1)} + C_2 y_{n-1}^{(2)}) + \ldots + \\
&a_k (C_1 y_{n-k}^{(1)} + C_2 y_{n-k}^{(2)}) = \\
&C_1 (y_n^{(1)} + a_1 y_{n-1}^{(1)} + \ldots + a_k y_{n-k}^{(1)}) + \\
&C_2 (y_n^{(2)} + a_1 y_{n-1}^{(2)} + \ldots + a_k y_{n-k}^{(2)}) = 0
\end{aligned}
$$

Ч.Т.Д

Следствие. Множество решений рекуррентного соотношения 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) имеет тривиальное нулевое решение. Докажем, что существуют в общем случае 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 учтено ($\lambda^{n-k} = 0$), то получаем:

$$\lambda^k + a_1 \lambda^{k-1} + \ldots + a_{k-1}\lambda + a_k = 0$$

(5)

Определение. Уравнение (5) называется характеристическим уравнением соотношения (4), а его правая часть - характеристическим многочленом.

4.5.3 Виды корней

Предположим, что найдены все r корней этого уравнения, включая комплексные (при этом корень учитывается столько раз, какова его кратность). Для построения базиса используют следующие правила:

- Если $\lambda = \alpha$ - вещественный корень кратности s, то ему отвечают s линейно независимых решений:
  $\varphi_n^{(1)} = \alpha^n, \ldots, \varphi_n^{(s)} = n^{s-1}\alpha^n$
- Если $\lambda = \alpha \pm i\beta$ - пара комплексно сопряженных корней уравнения кратности s каждый, то им отвечает в общей сумме $2s$ лин. независимых решений:
  $\varphi_n^{(1)} = \rho^n \cos(n\theta), \varphi_n^{(3)} = n\rho^n \cos(n\theta), \ldots, \varphi_n^{(2s-1)} = n^{2s-1}\rho^n \cos(n\theta)$
  $\varphi_n^{(2)} = \rho^n \sin(n\theta), \varphi_n^{(4)} = n\rho^n \sin(n\theta), \ldots, \varphi_n^{(2s)} = n^{2s}\rho^n \sin(n\theta)$
  где $\rho = \sqrt{\alpha^2 + \beta^2}, \theta = tg(\frac{\alpha}{\beta})$

4.6 Неоднородные линейные рекуррентные соотношения

4.6.1 Условие

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

4.6.2 НЛРС

Определение. $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = f(n), f(n) \neq 0$ (11) - неоднородное линейное рекуррентное соотношение

Теорема. Общее решение НЛРС есть сумма частных и общего решения соответствующей ОЛРС.

$y_n^{\text{общ.н}} = y_n^{\text{ч.н}} + \sum_{i=1}^{n} C_i y_n^{(i)}$ (12)

Доказательство. Подставим (12) в (11):

$(y_n^{\text{ч.н}} + y_n^{\text{о.о}}) + a_1(y_{n-1}^{\text{ч.н}} + y_{n-1}^{\text{о.о}}) + \ldots + a_k(y_{n-k}^{\text{ч.н}} + y_{n-k}^{\text{о.о}}) = f(n) + 0$

Для доказательства того, что (11) может быть представлена в виде (12), нужно доказать, что для произвольно заданных начальных условий однозначно определяются константы $C_i, \ldots, C_k$

Выпишем первые k решений: (13)

$$\begin{cases} y_0^{\text{ч.н}} + \sum_{i=1}^{k} C_i y_0^{(i)} = \alpha_0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_{k-1}^{\text{ч.н}} + \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = \alpha_{k-1} \end{cases}$$

Немного изменим решение (13) в (13′) :

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

Определитель всей системы при этом не изменился.

Тогда:

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

Ч.Т.Д

4.6.3 Метод подбора, принцип суперпозиции

Смотрим на функцию $f(n)$

Если $f(n) = a^n p^{(m)}$ - многочлен $p^{(m)}$ степени m, $a \in \mathbb{R}$, тогда частное решение ищется так:

$y_n^{\text{ч.н}} = n^s a^n R^{(m)}$ - корень a кратности s

Если $f(n) = r^n(P^c(n)\cos n\varphi + Q^p(n)\sin n\varphi)$ - квазиполином, P, Q - полиномы степени c и p соответственно.

Пусть $\lambda = re^{\pm\varphi}$ - корень кратности $s \geq 0$

$y_n^{\text{ч.н}} = n^s r^n(\overline{P}^q(n)\cos n\varphi + \overline{Q}^q(n)\sin n\varphi)$, где $q = max(c, p)$

4.7 Действия группы на множество. Лемма Бернсайда

4.7.1 Условие

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

4.7.2 Действие группы на множестве, орбита, стабилизатор

Определение. Группа $\mathcal{G}$ действует на множество X, если для любых $g \in \mathcal{G}$ и $x \in X$ определено действие элемента g на элемент x (обозначаемое gx), обладающими свойствами:

1) $gx \in X$

2) $\forall g_1, g_1 \in \mathcal{G}, x \in X$ верно $(g_1 g_2)x = g_1(g_2 x)$

3) $\forall x \in X : ex = x$

Определение. Орбита элемента $orb(x), x \in X$ - это множество $\{gx | g \in \mathcal{G}\}$

Определение. Стабилизатор элемента S(x) $x \in X$ - это множество $\{g \in \mathcal{G} | gx = x\}$

4.7.3 Лемма Бернсайда

Некоторые вещи. $S = \{s_1, \ldots, s_n\}, G \subseteq S_n$, где S_n - перестановки

Группа G действует на множество S:

$S \underset{G}{\sim} r \leftrightharpoons (\exists \delta \in G)(r = \delta(S))$

$G(S, r) \leftrightharpoons \{\delta : r = \delta(s)\}$

Доказательство. Утверждение 1: $G(S, r) = G_S \delta_r$, где $\delta_r(S) = r$, а G_s - правый смежный класс.

Доказательство утверждения 1:

$\delta \in G(S, r); \delta = \delta(\delta_r^{-1}\delta_r) = (\delta\delta_r^{-1})\delta_r$, но $\delta\delta^{-1}(S) = \delta_r^{-1}(\delta(S)) = \delta_r^{-1}(r) = S$

То есть $\delta\delta_r^{-1}$ - элемент стабилизатора G_S,

$\delta = (\delta\delta_r^{-1})\delta_r \in G_S\delta_r$

Ч.Т.Д

Утверждение 2. $|G : G_S| = w(S)$, где $|G : G_S|$ - индекс (число левых/правых подклассов), $w(S)$ - орбита вершины S

Доказательство утверждения 2:

$h : [S]_{\tilde{G}} \to \{G_S\delta : \delta \in G\}$

По определению $h(r) = G_S\delta \leftrightharpoons r = \delta(S)$

$h(\delta(S)) = G_S\delta$ - из-за этого h - сюръекция

Докажем, что h - инъективно

$r \neq t \in [S]_{\tilde{G}}$. Пусть при этом $h(r) = h(r)$

$h(r) = h(\delta_r(S))$, где $r = \delta_r(S)$

$h(t) = h(\delta_t(S))$, где $t = \delta_t(S)$

Значит $h(r) = h(r) \implies G_S\delta_r = G_s\delta_t$, где G_S - смежные классы.

Однако такое невозможно из-за неоднозначности отображения $\Longrightarrow$ h - биективно.

$h : [S]_{\tilde{G}} \underset{G}{\sim} |G : G_S| = w(S)$

Ч.Т.Д

Вернемся к самой лемме Бернсайда.

По теореме Лагранжа:

$|G| = |G : G_S| * |G_S| = w(S) * |G_S|$ - количество автоморфизмов равно орбита * стабилизатор.

N - число орбит, где в каждой орбите произвольно выбираем элементы $S_1, S_2, \ldots, S_n$

Получаем: $w(S_1) * |G_{S_1}| + w(S_2) * |G_{S_2}| * \ldots + w(S_n) * |G_{S_n}| = N * |G|$

Лемма Бернсайда. Тогда сама Лемма Бернсайда может быть сформулирована так:

$$N = \frac{1}{|G|} \sum_{s \in S} |G_S| = \frac{1}{|G|} \sum_{s \in m} \psi(\sigma)$$

где $\psi(\sigma)$ - число элементов множества S, которое оставляет подстановка σ неподвижной

4.8 Функция разметки

4.8.1 Условие

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

4.8.2 Ответ

Определение. Пусть на множестве S задана функция $F : C \to R$, отображающая S в множество меток (красок, цветов) R. Такая функция называется функцией разметки, или функцией раскраски (или просто краской).

Действие группы G на множестве S стандартным образом распространяется на множество R^S всех красок : $\sigma(f)(S) = f(\sigma(s)), \forall s \in S$. Таким образом эквивалентность раскрасок f, g означает, что для некоторой подстановки σ имеет равенство $f = \sigma(g)$, то есть для каждого $s \in S$ выполняется $g(S) = f(\sigma^{-1}(S)) = \sigma^{-1} * f(S)$. Число классов эквивалентности определяется по лемме Бернсайда.

Определение. Две раскраски C, D называются эквивалентными, если одна из них переходит в другую под действием некоторого автоморфизма графа G, то есть:

$$C \sim D \iff (\exists h \in Aut(G))((C(v_1), \ldots, C(v_n))) = (D(h(v_1)), \ldots, D(h(v_n))).$$

Определение. Весом раскраски $C = (C(1), \ldots, C(n))$ назовем произведение весов ее значений: $w(C) = w(C(1)) * \ldots * w(C(n))$

Определение. Перечнем раскрасок будем называть сумму весов всех возможных раскрасок:
$Invt(R^S) = \sum_{C \in R^S} w(C)$

4.9 Ступенчатые функции разметки

4.9.1 Условие

Ступенчатые функции разметки. Структурный перечень функций, сохраняемых произвольной подстановкой, разложенной на независимые циклы

4.9.2 Ответ

Внимание. В ответе на данный вопрос не уверен (нет нормальной лекции на тему)

Определение. $S = \bigcup_{j=1}^{p} T_j$, где $T_k \cap T_l \varnothing$ при $k \neq l$ и все множества непустые.

$f \in D : w(f) = w_{i1}^{|T_1|} w_{i2}^{k_2=|T_2|} \dots w_{ip}^{k_p}$

$k_1 + k_2 + \ldots + k_p = n = |S|$

Структурный перечень множества ступенчатой функции:

$Invt(D) = (w_1^{k_1} + w_2^{k_1} + \ldots + w_m^{k_1}) * (w_1^{k_2} + w_2^{k_2} + \ldots + w_m^{k_2}) * \ldots * (w_1^{k_p} + w_2^{k_p} + \ldots + w_m^{k_p}) = \prod_{j=1}^{p} (w_1^{k_j} + w_2^{k_j} + \ldots + w_m^{k_j})$

4.10 Теорема Пойа

4.10.1 Условие

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

4.10.2 Ответ

Внимание! В ответе на данный вопрос не уверен (нет нормальной лекции на тему)

Теорема.

1) $N = P_a(x_1, x_2, \ldots, x_n) \mid_{(\forall i=\overline{1,n})(x_j:=m)}$

2) $Invt(R^S|_{\tilde{G}}) = P_G(w_1 + \ldots + w_m, w_1^2 + \ldots + w_m^2, \ldots, w_1^n + \ldots + w_m^n)$

$x_l = \sum_{i=1}^n w_i^l$

Доказательство. Докажем каждый из пунктов.
1) $P_G(x_1, \ldots, x_n)|_{(\forall i=\overline{1,n})(x_i:=m)} =$
$\frac{1}{|G|} \sum_{\sigma \in G} t_\sigma|_{(\forall i=\overline{1,n})(x_i:=m)} =$
$\frac{1}{|G|} \sum_{\sigma \in G} m^{k(\sigma)} =$
$\frac{1}{|G|} \sum_{\sigma \in G} \psi(\sigma)$ - по Лемме Бернсайде это и есть число классов эквивалентности

2) $P_G(x_1, x_2, \ldots, x_n)|_{x_l:=\sum_{i=1}^m w_i^l} = \frac{1}{|G|} \sum_{\sigma \in G} \hat{t}_\sigma = \frac{1}{|G|} \sum_{\sigma \in G} \sum_\omega \psi_w(\sigma)\omega =$
$\sum_\omega (\frac{1}{|G|} \sum_{\sigma \in G} \psi_w(\sigma))\omega = \sum_\omega d_\omega \omega$

Смысл второго доказательства: поскольку все это действует на множестве функций разметки, не выводит(?выходит?) за пределы множества функций функционального(????) веса, так как было доказано выше, что все функции раскраски(?) имеют один и тот же вес.