ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.07
ДИСКРЕТНАЯ МАТЕМАТИКА

Направление подготовки: 27.03.04 Управление в технических системах

Профиль: Интеллектуальные системы обработки информации и управления

Квалификация: бакалавр

Форма обучения: очная

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция №1 (2 часа).

Тема: «Множества и операции над ними»

1.1.1 Вопросы лекции:

1. Множества и операции над ними. Диаграммы Венна-Эйлера.
2. Элементы алгебры множеств.

1.1-2.2 Краткое содержание вопросов лекции №1.

1. Множества и операции над ними. Диаграммы Венна-Эйлера.
2. Элементы алгебры множеств.
3. Понятие об абстрактной алгебре Буля.
4. Понятие о моделях алгебры Буля.

1. Множества и операции над ними. Диаграммы Венна-Эйлера.

1.Понятия множества, элемента множества, обозначения множества и его элементов, примеры.

2.Способы задания (описания) множеств перечислением элементов и с помощью предикатов.

3.Стандартные множества, их названия и обозначения

$\varnothing$ - пустое множество,

$N = \{1, 2, 3, ...\}$ - множество натуральных чисел(натуральный ряд);

$Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ - множество целых чисел;

$Q = \left\{ \frac{p}{q}, p, q \in Z, q \neq 0 \right\}$ - множество рациональных чисел;

R - множество всех вещественных чисел(всех десятичных дробей);

числовые промежутки $\langle a, b \rangle$.

4. Иллюстрация множеств диаграммами Венна-Эйлера.

5.Отношения и операции с множествами, их иллюстрация диаграммами Венна-Эйлера:

-равенство множеств $A = B$,

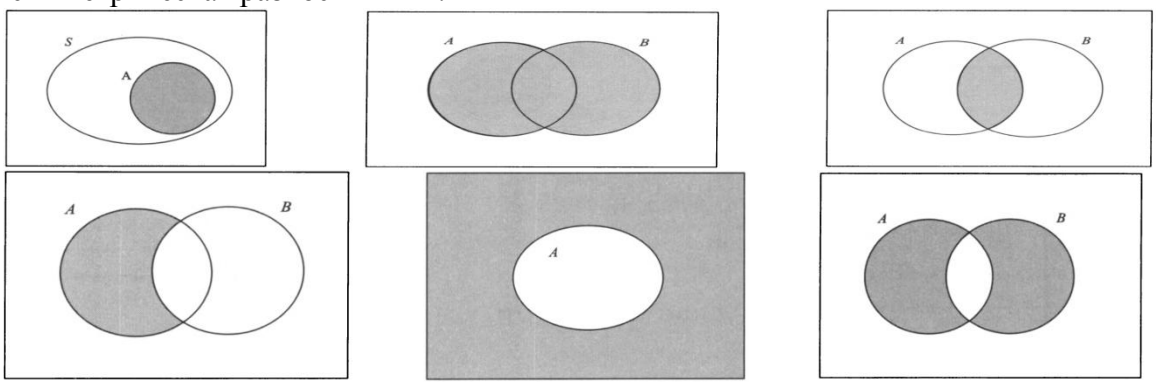
-включение $A \subset B, A \subseteq B$, понятие подмножества,

-объединение множеств $A \cup B$,

-пересечение множеств $A \cap B$,

-разность множеств $A \setminus B$ и дополнение $C_A B$ множества B до множества A, универсальное множество U, дополнение множества A до универсального $\overline{A}$

-симметрическая разность $A \Delta B$.



Дискретная математика представляет собой область математики, в которой изучаются свойства структур конечного характера, а также бесконечных структур, предполагающих скачкообразность происходящих в них процессов или отделимость составляющих их эле-

ментов. В отличие от дискретной математики *классическая* математика занимается изучением свойств структур непрерывного характера. Это деление достаточно условно, поскольку средства дискретной математики используются для изучения непрерывных моделей и наоборот.

Бурное развитие дискретной математики обусловлено прогрессом компьютерной техники, необходимостью создания средств обработки и передачи информации, а также представления различных моделей на компьютерах, которые по своей природе являются структурами конечным

Рассматриваются м*ножества и их спецификация, элементы и множества.* Множество, не содержащее элементов, называется пустым множеством и обозначается символом ∅. Если все рассматриваемые множества (в конкретной задаче) являются подмножествами более широкого множества U, то множество U называется универсальным множеством, или универсумом.

Мощность множества M обозначается как |M| и для конечного множества равняется числу элементов в нем.
Заметим, что |∅| = 0, но |{∅}| = 1.

2. Элементы алгебры множеств.

Теоретико-множественные соотношения(равенства множеств, включения) и методы их вывода и доказательства. Такие соотношения выражают законы алгебры множеств.

Свойства операций над множествами.

Законы ассоциативности

$$A \cup (B \cup C) = (A \cup B) \cup C \qquad A \cap (B \cap C) = (A \cap B) \cap C$$

Законы коммутативности

$$A \cup B = B \cup A \qquad A \cap B = B \cap A$$

Законы тождества

$$A \cup \varnothing = A \qquad A \cap U = A$$
$$A \cup U = U \qquad A \cap \varnothing = \varnothing$$

Законы идемпотентности

$$A \cup A = A \qquad A \cap A = A$$

Законы дистрибутивности

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Законы дополнения

$$A \cup \overline{A} = U \qquad A \cap \overline{A} = \varnothing$$
$$\overline{U} = \varnothing \qquad \overline{\varnothing} = U$$
$$\overline{\overline{A}} = A \qquad \overline{\overline{A}} = A$$

Законы де Моргана

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B} \qquad \overline{(A \cap B)} = \overline{A} \cup \overline{B}$$

Взаимосвязь законов алгебры множеств и алгебры логики, понятие о модели аксиоматической теории и интерпретации, понятие об алгебре Буля.
Булеан множества и его нахождение.

На основании этих свойств можно получить новые свойства и равенства.

Принцип двойственности.

Принцип двойственности состоит в том, что из любого равенства, относящегося к системе подмножеств фиксированного множества *U*, автоматически может быть получено

другое, двойственное, равенство, путем замены всех рассматриваемых множеств их дополнениями, объединений множеств – пересечениями, пересечений множеств – объединениями.

1. 2 Лекция № 2 (2 часа).

Тема: «Бинарные отношения и их свойства. Отношения эквивалентности и частичного порядка»

1.2.1 Вопросы лекции:

1. Понятие бинарного отношения. Способы задания отношений.
2. Свойства отношений, классификация отношений.

1.2.2 Краткое содержание вопросов:

1. Понятие бинарного отношения. Способы задания отношений. Свойства отношений, классификация отношений.

Прямое произведение множеств

Упорядоченная последовательность, содержащая n элементов некоторого множества, называется *n-кой*, или *набором из n элементов*. Обычно n-ка, образованная последовательностью $a_1, a_2, \ldots, a_n$ обозначается $(a_1, a_2, \ldots, a_n)$. При малых n говорят о двойках элементов, тройках и т.д.

Для множества чисел A = {1, 2, 3, 4} можно рассмотреть тройки: (1, 2, 2), (3, 4, 1), (2, 1, 2), причем первая и последняя тройки различны, несмотря на их одинаковый состав.

Прямым (или *декартовым*) *произведением* множеств $A_1, A_2, \ldots, A_n$ называется множество всех упорядоченных наборов $(x_1, x_2, \ldots x_n)$ таких, что $x_i \in A_i$ при $\forall i = 1, 2, \ldots, n$. Декартово произведение обозначается $A_1 \times A_2 \times \ldots \times A_n$. Если одним из сомножителей является пустое множество, то и произведение является пустым множеством.

Степенью множества A называется его прямое произведение само на себя *n* раз; обозначается A^n.

N-местным отношением R или *N-местным предикатом R* на множествах $A_1, \ldots, A_n$ называется любое подмножество прямого произведения $A_1 \times \ldots \times A_n$: $R \subseteq A_1 \times \ldots \times A_n$. Элементы $a_1, a_2, \ldots, a_n \mid a_i \in A_i$ при $\forall i = 1, 2, \ldots, n$ *связаны отношением R* тогда и только тогда, когда упорядоченный набор $(a_1, a_2, \ldots a_n) \in R$. При $N = 1$ отношение R является подмножеством множества A_1 и называется *унарным отношением* или *свойством*.

Наиболее часто встречается двухместное отношение ($N = 2$), которое называется *бинарным отношением R* из множества *A* в множество *B*, или *соответствием*: это подмножество произведения множеств *A* и *B*: $R \subseteq A \times B$. Если элементы *a* и *b* множеств *A* и *B* $(a,b) \in R$, то говорят, что они *находятся в отношении R*, для чего часто используется т.н. инфиксная форма записи: *aRb*. Если $R \subseteq A \times A$ (т.е. *A=B*), то *R* называется *бинарным отношением на множестве A*. Соответственно, отношение $R \subseteq A^n$ называется *N-местным предикатом на множестве A*.

Бинарное отношение можно задать *указанием всех пар*, для которых это отношение выполняется, или *графически*. Способы графического представления также могут быть различными.

Свойства отношений

Теорема: *Для любых бинарных отношений P, Q, R выполняются следующие свойства:*

1. $(P^{-1})^{-1}=P$; 2. $(P\circ Q)^{-1}= Q^{-1}\circ P^{-1}$;
3. $(P\circ Q)\circ R=P\circ(Q\circ R)$ *(ассоциативность композиции).*

Бинарное отношение R на множестве A называется *рефлексивным*, если для любого его элемента a выполняется aRa: $\forall a \in A \quad aRa$.

Бинарное отношение R на множестве A называется *антирефлексивным*, если для любых его элементов $a,b \quad aRb \Rightarrow a \neq b$.

Бинарное отношение R на множестве A называется *симметричным*, если из его выполнения для a, b следует выполнение для b, a: $\forall\, a, b \in A \quad aRb \Rightarrow bRa$.

Бинарное отношение R на множестве A называется *антисимметричным*, если из его выполнения для a, b и b, a следует, что a и b совпадают. $\forall\, a, b \in A \quad aRb$ и $bRa \Rightarrow a = b$.

Бинарное отношение R на множестве A называется *транзитивным*, если из его выполнения для a,b и для b,c следует его выполнение для a,c: $\forall\, a, b, c \in A \quad aRb$ и $bRc \Rightarrow aRc$.

Бинарное отношение R на множестве A называется *полным*, или *линейным*, если для любых двух различных элементов множества A оно выполняется или для a, b, или для b, a: $\forall\, a, b \in A \mid a \neq b \Rightarrow aRb$ или bRa

Рассмотрим отношение R на множестве натуральных чисел следующим образом: $R = \{(x,y) \mid x$ – делитель $y\}$. Это отношение является рефлексивным, т.к. $x/x = 1$ $\forall x \in \mathbf{N}$. Отношение R антисимметрично, т.к. если $x/y \in \mathbf{N}$ и $y/x \in \mathbf{N}$, то $x = y$. Проверим транзитивность R. $y/x \in \mathbf{N}$ и $z/y \in \mathbf{N} \Rightarrow z/x = z/y \cdot y/x \in \mathbf{N}$.

Теорема (о проверке свойств отношения):
Отношение R на множестве A^2*:*
-R рефлексивно $\Leftrightarrow I \subset R$;
-R симметрично $\Leftrightarrow R = R^{-1}$;
-R транзитивно $\Leftrightarrow R\circ R \subset R$;
-R антисимметрично $\Leftrightarrow R \cap R^{-1} \subset I$;
-R полно $\Leftrightarrow R \cup I \cup R^{-1} = U$;

Представление отношений в ЭВМ

Удобным способом представления отношений в ЭВМ является *матричная форма*. Рассмотрим два конечных множества $A=\{a_1,a_2,\ldots,a_m\}$, $B=\{b_1,b_2,\ldots,b_n\}$ и бинарное отношение $P \subseteq A\times B$. Определим матрицу $[P] = (p_{ij})$ бинарного отношения P по следующему правилу: $p_{ij} = \begin{cases} 1, & \text{если } (a_i,b_j) \in P, \\ 0, & \text{если } (a_i,b_j) \notin P. \end{cases}$ Полученная матрица содержит полную информацию о связях между элементами и позволяет представлять эту информацию на компьютере.

Заметим, что любая матрица, состоящая из нулей и единиц, является матрицей некоторого бинарного отношения.

Основные свойства матриц бинарных отношений:

1. Если бинарные отношения $P,Q \subseteq A\times B$, $[P] = (p_{ij})$, $[Q] = (q_{ij})$, то $[P\cup Q] = (p_{ij}+q_{ij})$, $[P\cap Q] = (p_{ij}\cdot q_{ij})$, где умножение осуществляется обычным образом, а сложение – по логическим формулам (т.е. 0+0=0, во всех остальных случаях 1). Итак: **$[P\cup Q] = [P]+[Q]$, $[P\cap Q] = [P]*[Q]$.**

2. Если бинарные отношения $P \subseteq A\times B$, $Q \subseteq B\times C$, то $[P\circ Q] = [P]\cdot[Q]$, где умножение матриц [P] и [Q] осуществляется по обычному правилу, а произведение и сумма элементов из [P] и [Q] – по правилам пункта 1.

3. Матрица обратного отношения P^{-1} равна транспонированной матрице отношения P: $\mathbf{[P^{-1}]=[P]^T}$.

4. Если $P \subseteq Q$, $[P]=(p_{ij})$, $[Q]=(q_{ij})$, то $p_{ij} \le q_{ij}$. $\forall i,j$.

5. Матрица тождественного отношения единична: $[I_A] = (I_{ij})$: $I_{ij} = 1 \Leftrightarrow i=j$.

6. Пусть R – бинарное отношение на A^2. Отношение R называется *рефлексивным*, если $\forall x \in A$ $(x,x) \in R$, т.е. $I_A \in R$ (на главной диагонали R стоят единицы). Отношение R называется *симметричным*, если $\forall x,y \in A$ $(x,y) \in R \Rightarrow (y,x) \in R$, т.е. $R^{-1}=R$, или $[R]=[R]^T$ (матрица симметрична относительно главной диагонали). Отношение R называется *антисимметричным*, если $R \cap R^{-1} \subseteq I_A$, т.е. в матрице $[R \cap R^{-1}]=[R]*[R]^T$ вне главной диагонали все элементы равны 0. Отношение R наз. *транзитивным*, если $(x,y) \in R$, $(y,z) \in R \Rightarrow (x,z) \in R$, т.е. $R \circ R \subseteq R$.

«Отношения эквивалентности»

3 Вопросы лекции:

1. Понятие отношения эквивалентности.
2. Отношения эквивалентности в математических и прикладных концепциях.

Краткое содержание вопросов:

Отношения эквивалентности.

Бинарное отношение *R* на множестве *A* называется *отношением эквивалентности*, если оно является рефлексивным, симметричным и транзитивным. Обычно отношение эквивалентности обозначают через ≡ или ~. Пусть *R* – отношение эквивалентности на множестве *A*. Определим *класс эквивалентности* $[x]$ для $x \in A$: $[x] = \{y \mid xRy\}$, т.е. это множество всех элементов *A*, которые *R*-эквивалентны *x*.

Пусть E – эквивалентность на множестве *M*. Тогда семейство классов эквивалентности множества *M* называется *фактор-множеством* множества *M* по отношению E и обозначается $M/E = \{E(x) \mid x \in M\}$. *Утверждение*: всякое отношение эквивалентности на множестве *M* определяет разбиение множества *M*, причем среди элементов разбиения нет пустых; и обратно, всякое разбиение множества *M*, не содержащее пустых элементов, определяет отношение эквивалентности на множестве *M*: $\equiv \subset M^2 \Leftrightarrow \exists\, \beta = \{B_i \mid B_i \subset M, B_i \neq \varnothing, M = \cup B_i$ и $\forall\, i,j \;\; i \neq j \Rightarrow B_i \cap B_j = \varnothing$

«Отношения частичного порядка»

1.5.1 Вопросы лекции:

1. Отношения порядка.

1.5.2 Краткое содержание вопросов:

Отношение порядка

Бинарное отношение *R* на множестве *A* называется *отношением порядка*, если оно антисимметрично и транзитивно. Отношение порядка может быть рефлексивным, и тогда оно называется отношением *нестрогого порядка* (обычно обозначается ≤). Если отношение порядка антирефлексивно, то оно называется отношением *строгого порядка* и обозначается обычно <. Отношение порядка может быть полным (линейным), и тогда оно называется отношением линейного порядка (если любые два элемента сравнимы между собой), а множество – вполне упорядоченным. Если отношение порядка не обладает свойством полноты, то оно называется отношением *частичного порядка*, а множество с заданным на нем отношением частичного порядка называется *частично упорядоченным множеством*. Обычно отношение порядка в общем случае обозначают <, и вместо aRb или $(a,b) \in R$ пишут $a<b$. Для отношения < обратным является >.

- Отношение < на множестве чисел является отношением строгого полного порядка, отношение ≤ – нестрогого полного порядка. Следовательно, множество чисел

является линейно упорядоченным. Отношение $\subset$ на булеане $P(M)$ является отношением нестрого частичного порядка.

Пусть дано ч.у.м. M с отношением порядка $\leq$: $\breve{U}= \{M,\leq\}$. *Максимальный* и *минимальный* элементы, *наибольший* и *наименьший*. Наибольший (наименьший) элемент обычно называют *единицей*, а наименьший – *нулем* множества. Заметим, что всякий наибольший элемент (если он существует) является максимальным, а всякий наименьший – минимальным. Обратное утверждение неверно. Максимальных (минимальных) элементов может быть несколько; *верхняя грань множества*, *точная верхняя грань* **sup A**, *нижняя грань, точная нижняя грань* **inf A.**

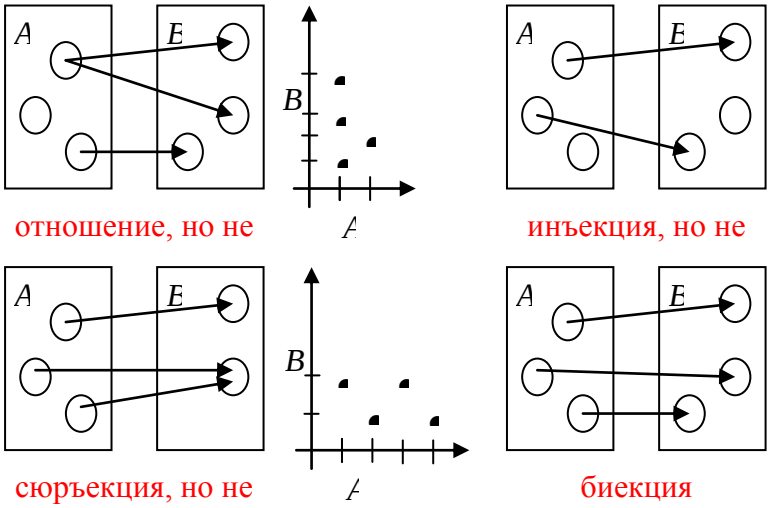


Рис. 1.4 Графическое представле-

Утверждение: Во всяком конечном непустом частично упорядоченном множестве существует минимальный элемент.

Замкнутость множества означает, что многократное повторение допустимых шагов не выводит за пределы этого множества.

Пусть R и R' – отношения на множестве M. Тогда отношение R' называется *замыканием отношения R относительно свойства C*, если:

-R' обладает свойством C: $C(R')$;

-R' является надмножеством R: $R \subset R'$;

-R' является наименьшим: $C(R'')$, $R \subset R'' \Rightarrow R' \subset R''$.

Пусть A – вполне упорядоченное множество с отношением порядка $\leq$. Введем отношение $\leq$ на множестве упорядоченных наборов из A следующим образом:

$(a_1,\ldots,a_m) \leq (b_1,\ldots,b_n) \Leftrightarrow$ $m \leq n$ и $\forall i = 1,..,m$ $a_i = b_i$ или

$\exists\, k \leq \min(n,m) \mid a_k \leq b_k$ и $a_i = b_i$ $\forall i < k$,

т.е. первые элементы совпадают, а k-й меньше.

Такое отношение называется *лексикографическим*, или *алфавитным* порядком.

1. 3 Лекция № 3 (2 часа).

Тема: «Функции. Виды функций»

1.3.1 Вопросы лекции:

1. Функции, классификация функций.
2. Переключательные функции (ПФ).

1.3.2 Краткое содержание вопросов:

1. Функции, классификация функций.

2. Переключательные функции (ПФ).

Функции. Определение функции.

Бинарное отношение R между множествами A и B называется *однозначным*, если из его выполнения для a, b и a, c ($a \in A$, $b,c \in B$) следует, что b и c совпадают. $\forall\, a \in A$, $b,c \in B$ aRb и $aRc \Rightarrow b = c$ (одному элементу множества A не могут соответствовать разные элементы, находящиеся с ним в отношении R).

Однозначное отношение f между множествами A и B, заданное для каждого элемента множества A, называется *отображением* множества A в множество B, или *функцией из A в B*: $f : A \to B$.

Дадим формальное определение. Отношение f между элементами множеств A и B называется *функцией* из A в B и обозначается $f : A \to B$, если оно обладает следующими двумя свойствами:

а) $\forall x \in A \ \exists y \in B \mid (x,y) \in f$; б) если $(x, y) \in f$ и $(x, z) \in f \Rightarrow y = z$.

Для функции f обычно вместо записи $(x,y) \in f$ используется т.н. префиксная форма: $y = f(x)$. При этом x называется *аргументом*, а y *– значением функции* f.

Для $f : A \to B$ *область определения* $Dom(f) \equiv \{x \in A \mid \exists y \in B \mid y = f(x)\}$, *область значений* $Codom(f) \equiv \{y \in B \mid \exists x \in A \mid y = f(x)\}$.

Если $Dom(f) = A$, то функция называется *тотальной*, а если $Dom(f) \neq A$ *– частичной*. *Сужением* функции $f : A \to B$ на множество $M \subset A$ называется функция $f|_M$, определяемая следующим образом: $f|_M \equiv \{(x,y) \mid y = f(x), x \in M\}$.

Для тотальной функции ее сужение на множество $Dom(f)$ совпадает с самой функцией f.

Для $f : A \to B$ и $x \in A$: если $y = f(x)$, то y называется *образом элемента* x, а x *– прообразом элемента* y. Для любого непустого подмножества $C \subset A$ его образом относительно f называется множество $f(C) = \{f(x) \mid x \in C\}$.

Функция $f: A_1 \times A_2 \times \ldots \times A_n \to B$ называется функцией n аргументов, или *n-местной* функцией.

Классификация функций

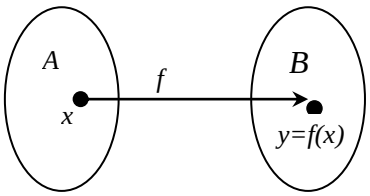
Отображение $f : A \to B$ называется (см. рисунок ниже):

инъективным (инъекцией), если любым различным значениям аргумента соответствуют различные значения функции: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$;

сюръективным, сюръекцией, или *отображением* ***на***, если любому элементу y множества B соответствует элемент x множества A, такой, что $f(x) = y$: $\forall y \in B \ \exists x \in A \mid f(x) = y$;

биективным, биекцией, или *взаимно однозначным соответствием*, если оно является одновременно инъекцией и сюръекцией;

перестановкой множества A, если $A = B$ и функция $f : A \to A$ является взаимно однозначным соответствием.



Если функция $I : A \to A$ определена как $I(a)=a \ \forall a \in A$, то I называется *тождественной функцией* на множестве A.

Обратное отношение f^{-1}, которое определялось ранее, может не быть функцией, даже если f является функцией из A в B. Если обратное отношение f^{-1} является функцией, то ее называют *обращением функции*, или *обратной функцией*.

Теорема (об обратной функции): *Если функция $f : A \to B$ является биекцией, то обратное отношение f^{-1} также является функцией из B в A, причем биекцией. Обратно, если f^{-1} – функция из B в A, то f является биекцией.*

Теорема: *Если функция $f : A \to B$ является биекцией, то: а) $\forall b \in B \ f(f^{-1}(b))=b$,*

б) $\forall a \in A \ f^{-1}(f(a))=a$.

Теорема: *Если функция $f : A \to A$ и I – тождественная функция на A, то $I \circ f = f \circ I = f$. Если для f существует обратная функция, то $f^{-1} \circ f = f \circ f^{-1} = I$.*

Ядро функции обозначается $\ker f = f \circ f^{-1}$.

Утверждение: ядро функции является отношением эквивалентности на области определения функции.

Теорема : *Пусть функции* $g: A \to B$ *и* $f: B \to C$. *Тогда: Если* g *и* f *– сюръекции, то их композиция – сюръекция; Если* g *и* f *– инъекции, то их композиция – инъекция; Если* g *и* f *–биекции, то их композиция – биекция;*

Некоторые специальные функции

1) *Перестановка* множества *A* была определена ранее.
2) *Тождественная* функция была определена ранее.
3) Пусть задано некоторое множество $M \subset U$. *Характеристической функцией* этого множества является функция χ, равная 1 на элементах множества *M*:

$$\chi(x) = \begin{cases} 1, & если \quad x \in M \\ 0, & если \quad x \notin M \end{cases}$$

4) *Бинарной операцией* на множестве *A* называется функция $b: A \times A \to A$. Образ пары (*x*,*y*) при отображении *b* записывается как $b(x,y)$ или как xby. Поскольку область значений бинарной операции на *A* по определению есть подмножество *A*, то множество *A* обладает свойством замкнутости относительно бинарной операции.
5) *Конечной последовательностью* называется функция из $N_0 = \{0, 1, 2, 3, \ldots, n\}$ в некоторое множество *A*. $f: N_0 \to A$ *Бесконечной последовательностью* называется функция из {0, 1, 2, 3, …} в некоторое множество *A*. Элементом последовательности является упорядоченная пара (*n*,*a*), в которой $a = f(n)$. Обычно эта пара обозначается через a_n, а последовательность $f: N_0 \to A$ – через $\{a_n\}$.

Иногда нумерацию членов последовательности начинают с 1, т.е. иногда последовательностью называют функцию, определенную на множестве **N**. Широко известными видами последовательностей являются арифметическая и геометрическая прогрессии.

6) Еще одна известная специальная функция, которая далее потребуется при комбинаторных вычислениях – факториал. На примере этой функции уместно вспомнить о принципе математической индукции.

1. 4 Лекция № 4 (2 часа).

Тема: «Эквивалентные множества. **М**ощность множеств**»**

1.4.1 Вопросы лекции:

1. Эквивалентные множества.
2. Понятие мощности множеств, сравнение мощностей.

1.4.2 Краткое содержание вопросов лекций №4:

1. Эквивалентные множества.
2. Понятие мощности множеств, сравнение мощностей.
3. Счётные множества.
4. Множества мощности континуум.

Отображение $f: A \to B$ называется: *биективным, биекцией*, или *взаимно однозначным соответствием*, если оно является одновременно инъекцией и сюръекцией;

Биекция и эквивалентные множества.

Понятие мощности конечного множества, принцип Дирихле. Свойства эквивалентных множеств.

Мощность множеств, счётные множества. Мощность континуума. Мощность бесконечного множества, счётные множества, множества мощности континуум.

1. 5 Лекция № 5 (2 часа).

Тема: «Бинарные операции. Группы. Подстановки на множестве»

1.5.1 Вопросы лекции:

1. Бинарные операции.
2. Группоид. Полугруппы и группы. Подстановки на множестве.

1.5.2 Краткое содержание вопросов:

1. Бинарные операции.

Определение. На множестве А определена **алгебраическая операция,** если каждым двум элементам этого множества, взятым в определенном порядке, однозначным образом поставлен в соответствие некоторый третий элемент из этого же множества.

Примерами алгебраических операций могут служить такие операции как сложение и вычитание целых чисел, сложение и вычитание векторов, матриц, умножение квадратных матриц, векторное умножение векторов и др.

Отметим, что скалярное произведение векторов не может считаться алгебраической операцией, т.к. результатом скалярного произведения будет число, и числа не относятся к множеству векторов, к которому относятся сомножители

Бинарной операцией на множестве A называется функция $b : A\times A \to A$. Образ пары (x,y) при отображении b записывается как $b(x,y)$ или как xby. Поскольку область значений бинарной операции на A по определению есть подмножество A, то множество A обладает свойством замкнутости относительно бинарной операции.

2. Группоид. Полугруппы и группы. Подстановки на множестве.

Определение. Множество А с определенной на нем алгебраической операцией (например, умножением) называется **группой**, если выполнены следующие условия:

1) для любых трех элементов $a, b, c \in$ А выполняется свойство ассоциативности:

$$a(bc) = (ab)c$$

2) в множестве А существует такой элемент e, что для любого элемента a из этого множества выполняется равенство:

$$ae = ea = a$$

3) для любого элемента a множества существует элемент a' из этого же множества такой, что

$$aa' = a'a = e$$

Различные множества могут являться группой относительно какой- либо операции и не являться группой относительно другой операции.

Число элементов называется **порядком** группы.

Определение. Между элементами множеств M и N установлено **взаимно однозначное соответствие**, если каждому элементу множества M поставлен в соответствие определенный элемент множества N, причем различным элементам одного множества соответствуют различные элементы другого множества.

Определение. Две группы M и N называются **изоморфными**, если между их элементами можно установить взаимно однозначное соответствие, при котором для любых двух элементов $a, b \in M$ и соответствующим им элементам $a', b' \in N$ элементу $c = ab$ будет соответствует элемент $c' = a'b'$.

Определение. Если операция, определенная в группе коммутативна, (т.е. для любых элементов a и b группы верно соотношение $ab=ba$), то такая группа называется **коммутативной** или **абелевой** группой.

Перестановки и подстановки. Симметрическая группа подстановок S_n**.**

Пусть дано множество $M = \{a_1,a_2,\ldots,a_n\}$*. Перестановкой элементов множества M называется любой упорядоченный набор из n различных элементов множества M.*

Перестановки различаются только порядком входящих в них элементов.

Перестановка элементов множества *M* может быть задана посредством *функции подстановки*. Будем определять подстановку как биекцию $\sigma : M \to M$ и задавать ее с помощью матрицы, состоящей из двух строк. Пусть множество M = {1,2,…,n}, а $\sigma(k) = s_k$, $1 \le s_k \le n$, k=1,…,n, $\{s_1,s_2,\ldots,s_n\} = \{1,2,\ldots,n\}$. Тогда матрица подстановки σ будет иметь вид: $[\sigma] \equiv \begin{pmatrix} 1 & 2 & \ldots & n \\ s_1 & s_2 & \ldots & s_n \end{pmatrix}$. Очевидно, что перестановка столбцов в этой матрице не меняет задаваемой ею подстановки.

Если заданы две подстановки σ и τ своими матрицами [σ] и [τ], то их *произведение* $\sigma\cdot\tau$ определяется следующим образом. В матрице [τ] столбцы переставляются так, чтобы ее первая строка совпала со второй строкой матрицы [σ]: $\begin{pmatrix} s_1 & s_2 & \ldots & s_n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}$. В итоге получится:

$$[\sigma]\cdot[\tau] = \begin{pmatrix} 1 & 2 & \ldots & n \\ s_1 & s_2 & \ldots & s_n \end{pmatrix}\begin{pmatrix} s_1 & s_2 & \ldots & s_n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}.$$

Если заданы подстановки $[\sigma] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $[\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, то $[\sigma\cdot\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$.

Тождественная подстановка – это такая подстановка *e*, что $e(x)=x\ \forall x$.

$$[e] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Обратная подстановка – это обратная функция, которая всегда существует (подстановка является биекцией). Для получения таблицы обратной подстановки нужно поменять местами строки таблицы исходной подстановки.

Для подстановки $[\sigma] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ $[\sigma^{-1}] = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

Подстановка σ называется *циклом длины r*, если матрицу [σ] перестановкой столбцов можно привести к виду:

$\begin{pmatrix} s_1 & s_2 & s_3 & \ldots & s_{r-1} & s_r & s_{r+1} & \ldots & s_n \\ s_2 & s_3 & s_4 & \ldots & s_r & s_1 & s_{r+1} & \ldots & s_n \end{pmatrix}$, т.е. первые *r* элементов сменяют друг друга, а остальные неподвижны: $\sigma(s_i) = s_{i+1}$, для $1 \le i \le r-1$ и $\sigma(s_r) = s_1$.

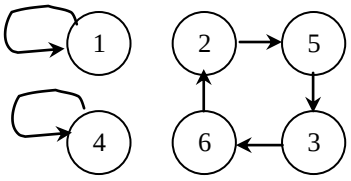
Подстановка σ с матрицей $[\sigma] = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 3 & 6 & 1 & 4 \\ 5 & 3 & 6 & 2 & 1 & 4 \end{pmatrix}$ является циклом (2 5 3 6), а подстановка с матрицей $[\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}$ циклом не является, т.к. из нее можно выделить два цикла (1 4) и (2 5 6 3).

Утверждение : Каждую подстановку можно однозначно (с точностью до порядка сомножителей) представить в виде произведения независимых циклов.

В примере 2.7 [σ] = (2 5 3 6), $[\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}$ = (1 4)·(2 5 6 3).

Двухэлементный цикл (i j) называется *транспозицией*. При транспозиции меняются местами только i-й и j-й элементы, а остальные сохраняют свое положение.

Подстановку удобно изображать *графически*, соединяя стрелками элементы *x* и $\sigma(x)$: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 4 & 3 & 2 \end{pmatrix}$.



Используя только транспозиции, можно выполнить сортировку множества в определенном порядке (например, в лексикографическом). Известный алгоритм сортировки, основанный на этом принципе, на каждом шаге осуществляет перестановку только двух соседних элементов и носит название «пузырьковой сортировки».

Число перестановок объема n принято обозначать как P_n.

Утверждение: Число всех перестановок множества M ($|M| = n$) равно $n!$
Действительно, на первое место в n-ке можно поставить любой из n элементов множества, на второе место – любой из (n–1) оставшихся, и т.д. Для последнего места остается единственный элемент. Поэтому получаем:
$\boldsymbol{P_n = n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot 2\cdot 1 = n!}$

1. 6 Лекция № 6 (2 часа).

Тема: «Кольца и поля. Кольцо классов вычетов целых чисел Z_n»

1.6.1 Вопросы лекции:

1. Кольца и поля.
2. Кольцо классов вычетов целых чисел

1.6.2 Краткое содержание вопросов:

1. Кольца и поля.

Определение. Множество R с двумя определенными в нем алгебраическими операциями, сложением и умножением, называется **кольцом**, если относительно операции сложения оно является абелевой группой, а операция умножения дистрибутивна, т.е. для любых элементов a, b и $c \in$ R справедливы равенства:

$$a(b+c) = ab + ac; \qquad (b+c)a = ba + ca;$$

Если операция умножения, определенная в кольце коммутативна, то такое кольцо называется **коммутативным** кольцом.

Определение. Полем называется коммутативное кольцо, в котором для любого ненулевого элемента $a \neq 0$ и любого элемента b существует единственный элемент x такой, что $ax = b$.

2. Кольцо классов вычетов целых чисел

Кольцо классов вычетов. Множество всех классов вычетов по модулю m обозначается Z_m или Z / mZ. Введем на этом множестве операции сложения классов и умножения классов.

Суммой классов $\bar{a}$ и $\bar{b}$ называется класс $\overline{a+b}$ т.е. класс, содержащий число $a+b$.

Произведением классов $\bar{a}$ и $\bar{b}$ называется класс $\overline{ab}$, т.е. класс, содержащий число ab.

Эти определения корректны, так как сумма любых двух представителей классов $\bar{a}$ и $\bar{b}$ всегда попадает в один и тот же класс, содержащий число $a+b$. Аналогичное утверждение имеет место и для произведения. Действительно, если $a_1 \in \bar{a}$, $b_1 \in \bar{b}$, то

$a_1 \equiv a(\mathrm{mod}\, m)$, $b_1 \equiv b(\mathrm{mod}\, m)$, следовательно, $a_1 + b_1 \equiv a + b(\mathrm{mod}\, m)$ и $a_1 b_1 \equiv ab(\mathrm{mod}\, m)$, т.е. $a_1 + b_1 \in \overline{a+b}$, $a_1 b_1 \in \overline{ab}$. Таким образом, определения суммы и произведения классов не зависят от выбора представителей классов.

1. 7 Лекция №7 (2 часа).

Тема: «Булевы функции. Элементарные булевы функции. Переключательные функции**»**

1.7.1 Вопросы лекции:

1. Булевы функции.
2. Элементарные булевы функции.

1.7.2 Краткое содержание вопросов:

1. Булевы функции.
2. Элементарные булевы функции.

1. Булевы функции. Элементарные булевы функции.

Булевы функции, булевы константы. **Булевыми функциями (или функциями алгебры логики или истинностными функциями) называются функции, значения которых равны 0 или 1 и аргументы которых принимают только два значения 0 и 1.** Булевы функции могут быть заданы специальными таблицами истинности или аналитически в виде специальных высказывательных форм, называемых иногда булевыми формами. Выражения, содержащие одну или несколько переменных (аргументов), соединенных знаками логических операций, называются *логическим формами*. Высказывания, не содержащие ни одной переменной, называются константами. В логике, в отличие от арифметики, только две константы 0 - false и 1- true.

Напомним, что *форма называется числовой,* если при допустимом значении своих аргументов, она обозначает число (является числом). Булева форма является частным случаем числовой формы. Т.о. при помощи суперпозиции, исходя из логических операций над логическими переменными, можно строить сложные составные высказывания и затем вычислять их. Такого рода составные высказывания являются частным случаем так называемых булевых функций, которые являются предметом изучения математической логики. Обобщая все сказанное, можно дать определение булевых функций:

Булевыми функциями, называются предикаты, все аргументы которых определены на множестве {0, 1}, интерпретируемые как {ложь, истина}.

Можно сказать, что понятие булевой функции является частным случаем понятия предиката. Отличие состоит лишь в том, что у булевой функции четко фиксирована как область определения {0, 1}, так и область значений функции {0, 1}, в то время как у предиката четко фиксирована только одна область значений {0, 1}, в то время как область определения задана произвольным множеством.

В свою очередь понятие предиката является частным случаем понятия функции, отличие состоит в том, что у предиката четко фиксирована область значений {0, 1}, а у функции это может быть вся числовая ось.

1. 8 Лекция №8 (2 часа).

Тема: «Представление булевых функций формулами. Понятие о булевой алгебре**»**

1.7.1 Вопросы лекции:

1. Представление булевых функций формулами.
2. Понятие о булевой алгебре.

1.7.2 Краткое содержание вопросов:

1. Представление булевых функций формулами.
2. Понятие о булевой алгебре.

2. Представление булевых функций формулами.

Булевы функции и формулы. *ФАЛ называются также* булевыми *функциями,* двоичными *функциями или* переключательными *функциями. Аргументы булевой функции являются булевыми переменными. Булеву функцию можно задать таблицей истинности.*

Утверждение Для булевой функции от n аргументов существует 2^n различных наборов аргументов.

Булева функция $f(x_1, x_2, \ldots, x_n)$ называется *полностью определенной*, если ее значения определены на всех 2^n наборах переменных. В противном случае функция *частично определенная*.

Функция $f(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n)$ *существенно зависит от переменной* x_i, (или переменная x_i – *существенная*), если $\exists$ такой набор значений $x_1, x_2, \ldots, x_n$ $(\sigma_1,\ldots,\sigma_{i-1},\sigma_i,\sigma_{i+1},\ldots,\sigma_n)$, что

$f(\sigma_1,\ldots,\sigma_{i-1},0,\sigma_{i+1},\ldots,\sigma_n) \neq f(\sigma_1,\ldots,\sigma_{i-1},1,\sigma_{i+1},\ldots,\sigma_n)$. В противном случае переменная x_i – *несущественная (фиктивная)*.

x_1	x_2	f_1	f_2
0	0	0	1
0	1	0	1
1	0	1	0
1	1	1	0

Пусть две булевы функции заданы таблицей истинности. Для них переменная x_1 существенная, а x_2 – несущественна. По определению булевы функции равны, если одна из другой получается введением или удалением несущественных переменных.

Одна и та же функция может иметь множество реализаций формулами над данным базисом (т.е. множеством логических операций). Формулы, реализующие одну и ту же функцию, называются *равносильными* (т.е. на всех наборах переменных их значение истинности совпадает). Отношение равносильности формул является отношением эквивалентности.

Формулы алгебры логики, при образовании которых используются только операции отрицания, конъюнкции и дизъюнкции, называются *булевыми формулами*.

Для любой формулы алгебры логики существует равносильная ей булева формула.

Способы представления булевых функций. Нормальные формы

Табличный способ определения истинности сложного выражения имеет ограниченное применение, т.к. с увеличением числа логических переменных число вариантов становится слишком большим. Тогда может быть использован способ приведения формул к *нормальной форме*.

Аналитическое выражение функции (или формула) находится в *нормальной форме*, если в ней отсутствуют знаки эквивалентности, импликации, двойного отрицания, а знаки отрицания находятся только при переменных.

Элементарной дизъюнкцией (*произведением*) называется дизъюнкция (произведение) переменных или их отрицаний, в котором каждая переменная встречается только один раз.

ДНФ – это дизъюнкция элементарных произведений. *КНФ* – это произведение элементарных дизъюнкций. Как ДНФ, так и КНФ функции не единственна. Обычно предполагают, что входящие в ДНФ (КНФ) элементарные конъюнкции (дизъюнкции) попарно различны.

ДНФ (КНФ) называется *совершенной*, если каждая переменная формулы входит в каждую элементарную конъюнкцию (дизъюнкцию) ровно один раз.
СДНФ (СКНФ) функции единственна.

Элементарные дизъюнкции: $x \vee \bar{y}$, z. Элемент. конъюнкции: $x \cdot \bar{y} \cdot z$, x.
$f(x,y,z) = xyz \vee \bar{x}y$ – ДНФ ; $f(x,y,z) = (x \vee \bar{y}) \cdot z$ – КНФ.

Введем обозначения: $x^{\alpha} = \begin{cases} x, & \alpha = 1 \\ \bar{x}, & \alpha = 0 \end{cases}$

О разложении булевой функции по k переменным (знак $\cup \equiv \vee$**).**

$$f(x_1,\ldots,x_n) = \bigvee_{\alpha_1,\ldots,\alpha_k} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} \cdot f(\alpha_1,\alpha_2,\ldots,\alpha_k,x_{k+1},\ldots,x_n)$$

n=3, k=2.

Доказательство:
Выберем какой-либо набор значений для переменных $x_1, \ldots, x_n$. Пусть это будет $\sigma_1, \ldots, \sigma_n$..
Заметим, что $\sigma_i^{\alpha_i} = \begin{cases} 1, & \sigma_i = \alpha_i \\ 0, & \sigma_i \neq \alpha_i \end{cases}$ ($1^1=1$, $0^0=1$, $1^0=\neg 1=0$, $0^1=0$)
Подставим в правую часть формулировки теоремы вместо $x_1, \ldots, x_n$ набор $\sigma_1, \ldots, \sigma_n$. Получим $\bigvee_{(\alpha_1,\ldots,\alpha_k)} \sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\ldots\sigma_k^{\alpha_k} \cdot f(\alpha_1,\alpha_2,\ldots,\alpha_k,\sigma_{k+1},\ldots,\sigma_n)$. Поскольку коэффициент перед функцией равен 1 только при равных значениях σ_i и α_i, в разложении останется только один член: $\sigma_1^{\alpha_1}\ldots\sigma_k^{\alpha_k} \cdot f(\alpha_1,\ldots,\alpha_k,\sigma_{k+1},\ldots,\sigma_n)$, и $\sigma_i=\alpha_i$, т.е. $f(\sigma_1,\ldots,\sigma_k,\sigma_{k+1},\ldots,\sigma_n)$. Получена левая часть формулы теоремы 4.6. Поскольку набор был выбран произвольно, получаем, что утверждение верно $\forall$ набора $x_1, \ldots, x_n$. ■

Следствие 1: Разложение Шеннона
$$f(x_1,x_2,\ldots,x_n) = \overline{x_1} \cdot f(0,x_2,\ldots,x_n) \vee x_1 \cdot f(1,x_2,\ldots,x_n)$$

Следствие 2: При k=n получаем: $f(x_1,\ldots,x_n) = \bigvee_{f=1} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, т.е. выбираем те слагаемые, на которых функция равна 1. Полученная формула представляет собой *СДНФ*.

Построение совершенных нормальных форм

Построение СДНФ

1. Построение по ТИ.

Найти строки в ТИ, где $f = 1$.
1) $\forall$ найденному набору $\sigma_1, \ldots, \sigma_n$. поставить в соответствие произведение $\tilde{x}_1 \cdot \tilde{x}_2 \cdot \ldots \cdot \tilde{x}_n$, где $\tilde{x}_i = \begin{cases} x_i, & \text{если } \sigma_i = 1 \\ \bar{x}_i, & \text{если } \sigma_i = 0 \end{cases}$
2) Составить дизъюнкцию из произведений п.2.

2. Получение из ДНФ.

Если некоторое произведение ДНФ не содержит какой-либо переменной, то необходимо помножить это произведение на дизъюнкцию этой переменной и ее отрицания и применить дистрибутивный закон.

Построение СКНФ

1. Построение по ТИ.

Найти строки в ТИ, где $f = 0$.

1) $\forall$ найденному набору $\sigma_1, \ldots, \sigma_n$. поставить в соответствие дизъюнкцию $\tilde{x}_1 \vee \tilde{x}_2 \vee \ldots \vee \tilde{x}_n$, где $\tilde{x}_i = \begin{cases} x_i, & \text{если } \sigma_i = 0 \\ \overline{x_i}, & \text{если } \sigma_i = 1 \end{cases}$

2) Составить произведение дизъюнкций из п.2.

2. Получение из КНФ.

Если некоторая элементарная дизъюнкция КНФ не содержит какой-либо переменной, то необходимо дизъюнктивно добавить в нее произведение этой переменной и ее отрицания и применить дистрибутивный закон.

1. 9 Лекция № 9 (2 часа).

Тема: «Правила комбинаторики. Комбинаторные формулы»

1.9.1 Вопросы лекции:

1. Правила комбинаторики.
2. Комбинаторные формулы

1.9.2 Краткое содержание вопросов:

1. Правила комбинаторики.

Комбинаторика – раздел математики, посвященный решению задач выбора и расположения элементов некоторого обычного множества в соответствии с заданными правилами. Каждое такое правило определяет способ построения некоторой конструкции из элементов исходного множества, называемой *комбинаторной конфигурацией*. Простейшими примерами комбинаторных конструкций являются перестановки, размещения, сочетания и разбиения, рассматриваемые ниже. Вычисления на дискретных математических структурах – комбинаторные вычисления – требуют комбинаторного анализа для установления свойств и оценки применимости алгоритмов.

Комбинаторные задачи и основные принципы. Во многих практических задачах возникает необходимость подсчитать количество возможных комбинаций объектов, удовлетворяющих определенным. условиям. Такие задачи называются комбинаторными. Среди всего многообразия таких задач есть ряд наиболее часто встречающихся, для которых известны способы подсчета. Для формулировки и решения комбинаторных задач используются различные модели комбинаторных конфигураций. Рассмотрим две наиболее популярные.

Дано n предметов. Их нужно разместить по m ящикам так, чтобы выполнялись заданные ограничения. Сколькими способами это можно сделать?

1. Дано множество функций $F : X \to Y$, где $|X| = n$, $|Y| = m$, $X = \{1,2,\ldots,n\}$ (предметы – элементы множества X – перенумерованы, т.е. можно считать номер отличительным признаком предмета). Без ограничения общности можно считать, что элементы множества Y также перенумерованы: $Y = \{1,2,\ldots,m\}$, $F = [F(1),\ldots,F(n)]$, $1 \le F(i) \le m$. Сколько существует функций, удовлетворяющих заданным ограничениям?

Наиболее часто соответствие конфигураций 1-го и второго типа очевидно, поэтому анализ проблем и вывод формул можно проводить на любом языке.

Основные комбинаторные принципы

***Утверждение*:** Если множества A и B не пересекаются и содержат по m и n элементов соответственно, то множество $A \cup B$ содержит $m + n$ элементов: для множеств A и B | $A \cap B = \varnothing$: $|A \cup B| = |A| + |B|$.

Теорема(о мощности произведения конечных множеств): Для любых множеств A и B $|A \times B| = |A| \cdot |B|$.

Правило суммы (комбинаторный принцип сложения): Если объект $\alpha \in A$ можно выбрать m способами, а объект $\beta \in B$, отличный от α, n способами, причем α и β нельзя выбрать одновременно, то осуществить выбор «либо α, либо β» можно $m+n$ способами.

Пусть в киоске имеется 5 различных книг по математике и 7 – по физике. Если студент может купить только одну книгу, то у него есть 5 вариантов выбора первой книги и 7 вариантов – второй, т.е. 12 вариантов.

Правило произведения (комбинаторный принцип умножения) Если объект $\alpha \in A$ можно выбрать m способами, а после каждого такого выбора можно выбрать n способами объект $\beta \in B$, отличный от α, то выбор обоих объектов α и β в указанном порядке можно осуществить $m \cdot n$ способами.

Пусть в салоне связи имеется 50 различных моделей сотовых телефонов и по три вида чехлов для каждой модели. Сколькими способами можно выбрать телефон и чехол к нему? Очевидно: имеется 50 вариантов выбора телефона. Выбрав телефон, можно 3 способами выбрать чехол, т.е. всего $50 \times 3 = 150$ вариантов.

Сравнивая утверждение 2.1 и теорему 2.1 с правилами суммы и произведения, можно заметить, что в них речь идет об одних и тех же закономерностях, хотя и используются различные формулировки. Очевидным образом эти правила распространяются на случай большего количества множеств.

2. Комбинаторные формулы»

Комбинаторные конфигурации: перестановки и подстановки

Пусть дано множество $M = \{a_1, a_2, \ldots, a_n\}$. *Перестановкой* элементов множества M называется любой упорядоченный набор из n различных элементов множества M. Перестановки различаются только порядком входящих в них элементов. Перестановка элементов множества M может быть задана посредством *функции подстановки*. Будем определять подстановку как биекцию $\sigma : M \to M$ и задавать ее с помощью матрицы, состоящей из двух строк.

Пусть множество $M = \{1,2,\ldots,n\}$, а $\sigma(k) = s_k$, $1 \le s_k \le n$, $k=1,\ldots,n$, $\{s_1, s_2, \ldots, s_n\} = \{1,2,\ldots,n\}$. Тогда матрица подстановки σ будет иметь вид: $[\sigma] \equiv \begin{pmatrix} 1 & 2 & \ldots & n \\ s_1 & s_2 & \ldots & s_n \end{pmatrix}$.

Число всех перестановок множества M ($|M| = n$) равно $n!$

Сколькими способами можно расставить на полке 6 томов книг? Это можно осуществить $P_6 = 6! = 720$ способами.

Понятие выборки. Пусть дано множество $M = \{a_1, a_2, a_3, \ldots, a_n\}$, $m \le n$. Набор, состоящий из m элементов множества M, называется выборкой объема m из n элементов.

Выборки классифицируются следующим образом:

По критерию повторяемости элементов: С возвращением объема (с повторениями) и без возвращения объема (без повторений).

По критерию упорядоченности: Упорядоченные (размещения) и неупорядоченные (сочетания).

Иллюстрация: ящик с *n* нумерованными шариками.

Размещения из n элементов по m, Сочетания без повторений из n элементов по m, Размещения с повторениями (или *упорядоченными выборками с возвращениями*) *из n элементов по k ,*

В отличие от выборок без повторений, количество выбираемых объектов может быть больше, чем количество типов, т.е. может быть $k \geq n$. Если вернуться к примеру 2.12 (а), то можно рассматривать и 10-разрядные числа.

Теорема*(о мощности множества P(M)): Для конечного множества M* $|2^M| = 2^{|M|}$.

Следствие: м*ожно сгенерировать все подмножества конечного множества M, перечислив некоторым способом все наборы из нулей и единиц длины n.* Можно выполнять такую генерацию различными способами (например, все наборы с одной 1, все с двумя, …). Это можно сделать наиболее эффективно, используя т.н. *бинарный код Грея.* Алгоритм построения бинарного кода Грея позволяет генерировать последовательность всех подмножеств *n*-элементного множества таким образом, что каждое последующее подмножество получается из предыдущего добавлением или удалением единственного элемента.

Определим отношение эквивалентности на множестве размещений с повторениями из *n* элементов по *k*: $(a_1,a_2,\ldots,a_k) \sim (b_1,b_2,\ldots,b_k) \Leftrightarrow \forall c \in M$ число элементов $a_i = c$ совпадает с числом элементов $b_j = c$.

Тогда *сочетанием с повторениями* из *n* элементов по *k* или *неупорядоченной выборкой с возвращениями из n элементов по k* является множество, которое состоит из элементов, выбранных *k* раз из множества *M*, причем один и тот же элемент допускается выбирать повторно.

> В примере с множеством M={1,2,3,4,5} сочетания с повторениями из 5 элементов по 2 будут отличаться от размещений тем, что одинаковые по составу наборы будут независимо от порядка элементов в них считаться эквивалентными: (1,1), (1,2)~(2,1), (2,2), (5,2) и т.п.

При рассмотрении выборок с повторениями число *n* более наглядно трактуется как количество имеющихся в наличии типов объектов, а *k* – количество непосредственно выбираемых объектов. Раз объекты выбираются с повторениями, неважно, каково их реальное количество для каждого из типов. Можно считать их неисчерпаемыми.

Число всех сочетаний с повторениями обозначается $\overline{C}_n^k = \hat{C}(n,k)$ и вычисляется по формуле: $\hat{C}(n,k) = \overline{C}_n^k = C_{n+k-1}^k = \dfrac{(n+k-1)!}{k!(n-1)!}$ **(2.2)**

> Пусть в кондитерской продается 10 различных видов пирожных. (n=10 – число типов). Сколькими способами можно купить 12 пирожных? (k=12). $\hat{C}(10,12)=C(10+12-1,12)=C(21,12)=21!/(12!\ (10-1)!)= 21!/(12!\ 9!)$.

1. 10 Лекция № 10 (2 часа).

Тема: «Биномиальные коэффициенты и их свойства. Метод включений и исключений. Метод рекуррентных соотношений. Производящие функции**»**

1.10.1 Вопросы лекции:

1. Биномиальные коэффициенты и их свойства.
2. Метод включений и исключений. Метод рекуррентных соотношений.
3. Производящие функции.

1.10.2 Краткое содержание вопросов:

1. Биномиальные коэффициенты и их свойства.
2. Метод включений и исключений. Метод рекуррентных соотношений.
3. Производящие функции.

Биномиальные коэффициенты. Число сочетаний *C(n,k)* – число различных *k*-элементных подмножеств *n*-элементного множества – встречается в формулах решения многих комбинаторных задач. Например, для определения числа подмножеств n-элементного множества, удовлетворяющих некоторому условию, задача разбивается на составные части: рассматриваются отдельно 1-элементные подмножества, 2-элементные и т.д., затем результаты складываются. Числа $C_n^k = \frac{n!}{(n-k)!k!}$ называются *биномиальными коэффициентами*.

Свойства биномиальных коэффициентов

Теорема: Число C_n^k обладает следующими свойствами:

1. $C_n^m = C_n^{n-m}$; 2. $C_n^m + C_n^{m+1} = C_{n+1}^{m+1}$; 3. $C_n^k \cdot C_k^m = C_n^m \cdot C_{n-m}^{k-m}$

Доказательство.

1. $C_n^m \equiv \frac{n!}{(n-m)!m!} = \frac{n!}{(n-m)!(n-n+m)!} = \frac{n!}{(n-m)!(n-(n-m))!} \equiv C_n^{n-m}$

2. $C_n^m + C_n^{m+1} = \frac{n!}{(n-m)!m!} + \frac{n!}{(n-(m+1))!(m+1)!} = \frac{n!}{(n-(m+1))!(n-m)m!} + \frac{n!}{(n-(m+1))!m!(m+1)} = \frac{n!(m+1)+n!(n-m)}{(n-(m+1))!(n-m)m!(m+1)} = \frac{n!(m+1+n-m)}{(n-m)!(m+1)!} = = \frac{n!(n+1)}{(n-m)!(m+1)!} = \frac{(n+1)!}{(n+1-(m+1))!(m+1)!} = C_{n+1}^{m+1}.$

3. $C_n^k \cdot C_k^m = \frac{n!}{(n-k)!k!} \cdot \frac{k!}{(k-m)!m!} = \frac{n!}{(n-k)!(k-m)!m!} = \frac{n!(n-m)!}{(n-k)!(k-m)!m!(n-m)!} = \frac{n!}{m!(n-m)!} \cdot \frac{(n-m)!}{(n-k)!(k-m)!} = C_n^m \cdot \frac{(n-m)!}{(n-m-(k-m))!(k-m)!} = C_n^m \cdot C_{n-m}^{k-m}.$

Бином Ньютона: *При любых x, y ∈ R* $(x+y)^n = \sum_{m=0}^{n} C_n^m x^m y^{n-m}$.

Следствие 1. $2^n = \sum_{m=0}^{n} C_n^m$. Действительно, $2^n = (1+1)^n = \sum_{m=0}^{n} C_n^m 1^m 1^{n-m} = \sum_{m=0}^{n} C_n^m$.

Следствие 2. $\sum_{m=0}^{n} (-1)^m C_n^m = 0$. Действительно ,

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

. 1. $\sum_{m=0}^{n} mC_n^m = n2^{n-1}$; 2. $C_{n+m}^k = \sum_{i=0}^{k} C_n^i C_m^{k-i}$ (Тождество Коши).

Треугольник Паскаля. Обобщенные перестановки и разбиения, Перестановки с повторениями, Разбиения и числа Стирлинга.

$R(n; n_1,n_2, \ldots,n_k) = \frac{n!}{n_1!n_2!..n_k!}$.

Теорема: *Число R(n,k) упорядоченных разбиений на k подмножеств вычисляется по формуле* $R(n,k) = \sum_{\substack{n_1+...+n_k=n \\ n_i>0}} R(n; n_1,\ldots,n_k)$.

Числа $R(n; n_1, n_2, \ldots, n_k)$ называются *полиномиальными коэффициентами*, поскольку для $\forall\ a_1, a_2, \ldots, a_k \in \mathbf{R}$ справедливо соотношение

Полиномиальная теорема

$$(a_1+a_2+\ \ldots+a_k)^n = \sum_{\substack{n_1+...+n_k=n \\ n_i\geq 0}} \frac{n!}{n_1!..n_k!} a_1^{n_1} a_2^{n_2}..a_k^{n_k} = \sum_{\substack{n_1+...+n_k=n \\ n_i\geq 0}} R(n; n_1,\ldots,n_k) a_1^{n_1} a_2^{n_2}..a_k^{n_k}$$

Если рассмотренный выше набор $(B_1,\ldots,B_k)$ рассматривать без учета порядка его блоков, то он называется *неупорядоченным разбиением* множества X, или просто *разбиением на k блоков*.

Число разбиений *n*-элементного множества на k блоков называется *числом Стирлинга второго рода* и обозначается *S(n,k)*. Определяются числа Стирлинга 2 рода рекурсивно следующим образом:

S(n,k)=S(n–1,k–1)+ k·S(n–1,k) (0<k<n)

При этом S(n,0)=0 при n>0, S(n,k)=0 при n<k, S(n,n)=1, S(0,0)=1.

Из формулы 2.7 следует удобный способ рекуррентного вычисления значений чисел Стирлинга 2 рода, который можно представить в графической форме (в виде треугольника) следующим образом:

В этом треугольнике каждое k-е в ряду число является суммой левого стоящего над ним числа с правым, умноженным на k. Тогда число Стирлинга *S(n,k)* находится в *n*–м ряду на *k*-м месте, если начинать счет от 0.

					0		1							1
				0		1		1						2
			0		1		3		1					3
		0		1		7		6		1				4
	0		1		15		25		10		1			5

Краткое содержание вопросов лекции №10:

1. Метод включений и исключений.
2. Метод рекуррентных соотношений
3. Производящие функции

Принцип включения и исключения. Рассмотренные ранее формулы и алгоритмы дают способы вычисления комбинаторных чисел для некоторых распространенных комбинаторных конфигураций. Практические задачи не всегда прямо сводятся к известным комбинаторным конфигурациям. В этом случае используются различные методы сведения одних комбинаторных конфигураций к другим. Рассмотрим некоторые наиболее часто

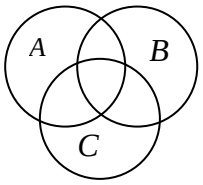
используемые методы. Часто комбинаторная конфигурация является объединением других, число комбинаций в которых вычислить проще. В таком случае требуется уметь вычислять число комбинаций в объединении. В простых случаях формулы для вычисления очевидны:

Теорема (комбинаторный принцип сложения): Пусть множества A и B *могут пересекаться. Тогда количество элементов, которые можно выбрать из A или B, определяется по формуле:*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Очевидно, что рассмотренная теорема будет справедлива для произвольных множеств. Если перейти от двух множеств к большему количеству, в частности, к трем, и проиллюстрировать с помощью диаграмм Венна, то очевидным результатом явится следующая формула:

$|\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}| = |\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}| - |\boldsymbol{A} \cap \boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{C}| - |\boldsymbol{B} \cap \boldsymbol{C}| + |\boldsymbol{A} \cap \boldsymbol{B} \cap \boldsymbol{C}|$, т.е. для вычисления количества элементов объединения трех множеств нужно просуммировать мощности всех этих множеств, вычесть мощности всех попарных пересечений и добавить число элементов, содержащихся в пересечении всех трех множеств.



Более общая формула, известная как принцип включения и исключения, позволяет вычислить мощность объединения произвольного количества множеств, если известны их мощности и мощности всех пересечений.

Теорема (принцип включения и исключения):

$$\left|\bigcup_{i=1}^{m} A_i\right| = \sum_{i=1}^{m} |A_i| - \sum_{1\le i<j\le m} |A_i \cap A_j| + \sum_{1\le i<j<k\le m} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{m-1} |A_i \cap \ldots \cap A_m|$$

Пусть множество A состоит из N элементов и имеется m одноместных отношений (свойств) $P_1, P_2, \ldots, P_m$. Каждый элемент множества может обладать или не обладать любым из этих свойств. Обозначим через $N_{i_1 \ldots i_k}$ число элементов, обладающих свойствами $P_{i_1}, \ldots, P_{i_k}$ и, может быть, некоторыми другими. Тогда число $N(0)$ элементов, не обладающих ни одним из свойств $P_1, \ldots, P_m$, вычисляется по следующей формуле:

$$N(0) = S_0 - S_1 + S_2 - \ldots + (-1)^m S_m, \text{ где } \quad S_0 = N, \quad S_k = \sum_{1\le i_1<\ldots<i_k\le m} N_{i_1 \ldots i_k} \ (k = 1, \ldots, m)$$

Обобщая, получаем формулу, позволяющую вычислить число $N(r)$ элементов, обладающих ровно r свойствами $(1 \le r \le m)$.

$$N(r) = \sum_{k=0}^{m-r} (-1)^k C_{r+k}^{r} S_{r+k}$$

Определим функцию $[x]$ для вещественных чисел как наибольшее целое число, не превосходящее x (*целая часть* числа x). Для положительных чисел a и b значение функции $\left[\frac{b}{a}\right]$ равно количеству чисел из множества $\{1, 2, \ldots, b\}$, которые делятся на a, т.е. кратны a.

2. Метод рекуррентных соотношений

Рекуррентные функции. Понятие последовательности было введено в разделе «специальные функции». Рекуррентным соотношением, рекуррентным уравнением *или* рекуррентной формулой *называется соотношение вида* $a_{n+k} = F(n, a_n, a_{n+1}, \ldots, a_{n+k-1})$,

которое позволяет вычислить все члены последовательности $a_0, a_1, a_2, \ldots$, *если заданы ее первые* k *членов.*

1.Формула $a_{n+1} = a_n + d$ задает *арифметическую прогрессию*.
2. Формула $a_{n+1} = q \cdot a_n$ задает *геометрическую прогрессию*.
3. Формула $a_{n+2} = a_{n+1} + a_n$ задает последовательность *чисел Фибоначчи.*

В случае, когда рекуррентное соотношение линейно и однородно, т.е. для всех n и некоторого k выполняется $a_{n+k} + p_1 a_{n+k-1} + \ldots + p_k a_n = 0,$ где p_i = const, последовательность $a_0, a_1, \ldots$ называется *возвратной*. Соотношение (2.9) называется *возвратным уравнением порядка k.*

Геометрическая прогрессия – это возвратная последовательность первого порядка, так как $a_{n+1} = q \cdot a_n \Rightarrow a_{n+1} - q \cdot a_n = 0$.

Любая последовательность, удовлетворяющая возвратному уравнению, называется его *решением*.

1. 11 Лекция № 11 (2 часа).

Тема: «Основы теории делимости в Z**.** Простые числа**»**

1.11.1 Вопросы лекции:

1. Основы теории делимости.
1. Простые числа.

Если при делении на целое положительное число m два числа a и b дают один и тот же остаток, то они называются *равноостаточными* или *сравнимыми* по модулю m. Записывается это так:

$$a \equiv b (\mathrm{mod}\, m).$$

Свойства сравнений:

1) $a \equiv a (\mathrm{mod}\, m)$ (рефлексивность);
2) если $a \equiv b (\mathrm{mod}\, m)$, то $b \equiv a (\mathrm{mod}\, m)$ (симметричность);
3) если $a \equiv b (\mathrm{mod}\, m)$, $b \equiv c (\mathrm{mod}\, m)$, то $a \equiv c (\mathrm{mod}\, m)$ (транзитивность).

Теорема. $a \equiv b (\mathrm{mod}\, m)$ тогда и только тогда, когда существует целое число t, для которого $a = b + mt$.

Доказательство необходимости. Пусть $a \equiv b (\mathrm{mod}\, m)$, тогда $a = mq_1 + r$, $b = mq_2 + r$; откуда $a - mq_1 = b - mq_2$; $a = b + m(q_1 - q_2)$. Обозначив $q_1 - q_2$ через t и получим представление a в виде $b + mt$.

Доказательство достаточности. Пусть $a = b + mt$ и $b = mq + r$. Тогда $a = m(t + q) + r$, т.е. число a дает тот же остаток при делении на m, что и число b. Теорема доказана.

Теорема. $a \equiv b (\mathrm{mod}\, m)$ тогда и только тогда, когда a-b делится на m.

Доказательство проводится аналогично.

Свойства сравнений, подобные свойствам равенств:

1) Если $a \equiv b (\mathrm{mod}\, m)$, $c \equiv d (\mathrm{mod}\, m)$, то $a + c \equiv b + d (\mathrm{mod}\, m)$, т.е. сравнения можно почленно складывать.

   Доказательство: По условию $a = b + mt_1$, $c = d + mt_2$, тогда $a + c = (b + d) + m(t_1 + t_2)$, а это значит, что $a + c \equiv b + d (\mathrm{mod}\, m)$.

2) Если $a \equiv b (\mathrm{mod}\, m)$, $c \equiv d (\mathrm{mod}\, m)$, то $ac \equiv bd (\mathrm{mod}\, m)$, т.е. сравнения можно почленно перемножать.

Доказательство: $a = b + mt_1$, $c = d + mt_2$, следовательно, $ac = bd + m(t_1t_2 + bt_2 + ct_1)$, т.е. $ac \equiv bd (\mathrm{mod}\, m)$.

3) Если $a \equiv b (\mathrm{mod}\, m)$, то $ak \equiv bk (\mathrm{mod}\, m)$ для любого целого числа *k*.
Доказательство: $a = b + mt$. Отсюда $ak = bk + mkt$.

4) Если $ak \equiv bk (\mathrm{mod}\, m)$, $(k, m) = 1$, то $a \equiv b (\mathrm{mod}\, m)$.
Доказательство: По условию $k(a - b) = ak - bk$ делится на *m*; *k* и *m* взаимно просты. Из теоремы Евклида следует, что *a*-*b* делится на *m*, а это равносильно тому, что $a \equiv b (\mathrm{mod}\, m)$.

Пример: Установить признак делимости на 11.

Решение: Представим число *N* в виде $N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \ldots$, где $0 \le a_i \le 9$. Так как $10 \equiv -1 (\mathrm{mod} 11)$. То $N \equiv a_0 - a_1 + a_2 - a_3 + \ldots (\mathrm{mod} 11)$. Отсюда, *N* делится на 11 тогда и только тогда. Когда на 11 делится $a_0 - a_1 + a_2 - a_3 + \ldots$.

Функция Эйлера

Функция Эйлера $y = \varphi(a)$ определена для всех натуральных *a* и представляет собой количество натуральных чисел, взаимно простых с *a* и не превосходящих *a*, Считаем, что $\varphi(1) = 1$.

Примеры. $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(p) = p - 1$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Теорема. Если каноническое представление натурального числа $n \ne 1$ имеет вид:

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k},$$

то

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$

Доказательство: Применим метод включения и исключения:

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots - \frac{n}{p_k} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \ldots + \frac{n}{p_{k-1}p_k} - \frac{n}{p_1p_2p_3} - \frac{n}{p_1p_2p_4} - \ldots + (-1)^k \frac{n}{p_1p_2\cdots p_k}.$$

Раскрыв скобки в произведении, мы получим эту же сумму. Отсюда следует утверждение теоремы

Теорема Эйлера

Теорема. Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Доказательство: Пусть числа $r_1, r_2, \ldots, r_c$ образуют приведенную систему вычетов по модулю *m*. Тогда числа $ar_1, ar_2, \ldots, ar_c$ все взаимно просты с *m* и попарно не сравнимы по модулю *m*. Число ar_1 попадает в один класс вычетов с каким-то r_{i_1} из чисел $r_1, r_2, \ldots, r_c$. Число ar_2 попадает в один класс с другим числом r_{i_2}, но из этого же множества, т.е. имеем сравнения

$$ar_1 \equiv r_{i_1} (\mathrm{mod}\, m),$$
$$ar_2 \equiv r_{i_2} (\mathrm{mod}\, m),$$
$$\ldots \quad \ldots$$
$$ar_c \equiv r_{i_c} (\mathrm{mod}\, m).$$

Здесь числа $r_{i_1}, r_{i_2}, \ldots, r_{i_c}$ - те же числа $r_1, r_2, \ldots, r_c$, записанные, может быть, в другом порядке. Поэтому после перемножения сравнений можно записать

$$a^c r_1 r_2 \ldots r_c \equiv r_1 r_2 \ldots r_c (\mathrm{mod}\, m).$$

Откуда $a^c \equiv 1(\mathrm{mod}\, m)$. Что и требовалось доказать.

Малая теорема Ферма. Для любых целых чисел a и простого числа p

$$a^p \equiv a(\mathrm{mod}\, p).$$

Доказательство: $\varphi(p) = p - 1$. Поэтому, если a не делится на p, то по теореме Эйлера

$$a^{p-1} \equiv 1(\mathrm{mod}\, p),$$

откуда следует, что $a^p \equiv a(\mathrm{mod}\, p)$. Если a делится на p, то $a \equiv 0(\mathrm{mod}\, p)$, $a^p \equiv 0(\mathrm{mod}\, p)$; откуда и получим сравнение $a^p \equiv a(\mathrm{mod}\, p)$.

1. 12 Лекция № 12 (2 часа).

Тема: «Сравнения. Вычеты. Модульная арифметика. Приложения в криптографии: алгоритм RSA.»

1.12.1 Вопросы лекции:

1. Сравнения. Вычеты. Модульная арифметика.
2. Приложения в криптографии: алгоритм RSA.

1.12.2 Краткое содержание вопросов:

1. Сравнения. Вычеты. Модульная арифметика.
2. Приложения в криптографии: алгоритм RSA.

1. Вычеты. Модульная арифметика.

Из свойств

4) $a \equiv a(\mathrm{mod}\, m)$ (рефлексивность);

5) если $a \equiv b(\mathrm{mod}\, m)$, то $b \equiv a(\mathrm{mod}\, m)$ (симметричность);

6) если $a \equiv b(\mathrm{mod}\, m)$, $b \equiv c(\mathrm{mod}\, m)$, то $a \equiv c(\mathrm{mod}\, m)$ (транзитивность)

сравнений следует, что отношение сравнения в Z является бинарным отношением эквивалентности на Z. Из теории отношений известно, что всякое отношение эквивалентности определяет разбиение множества на классы - классы эквивалентности (классы эквивалентных элементов). Классы эквивалентности при разбиении Z отношением сравнения по модулю называются классами вычетов по этому модулю.

Суммой классов $\bar{a}$ и $\bar{b}$ называется класс $\overline{a+b}$ т.е. класс, содержащий число $a+b$.

Произведением классов $\bar{a}$ и $\bar{b}$ называется класс $\overline{ab}$, т.е. класс, содержащий число ab.

Эти определения корректны, так как сумма любых двух представителей классов $\bar{a}$ и $\bar{b}$ всегда попадает в один и тот же класс, содержащий число $a+b$. Аналогичное утверждение имеет место и для произведения. Действительно, если $a_1 \in \bar{a}$, $b_1 \in \bar{b}$, то $a_1 \equiv a(\mathrm{mod}\, m)$, $b_1 \equiv b(\mathrm{mod}\, m)$, следовательно, $a_1 + b_1 \equiv a + b(\mathrm{mod}\, m)$ и $a_1 b_1 \equiv ab(\mathrm{mod}\, m)$, т.е. $a_1 + b_1 \in \overline{a+b}$, $a_1 b_1 \in \overline{ab}$. Таким образом, определения суммы и произведения классов не зависят от выбора представителей классов.

Пример: Таблица сложения и умножения по модулю 6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2

4	4	5	0	1	2	3
5	5	0	1	2	3	4

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Теорема. Относительно введенных действий сложения и умножения классов множество $Z / m Z$ – ассоциативное, коммутативное кольцо с 1.

Доказательство заключается в проверке аксиом кольца.

Теорема. Кольцо классов вычетов по простому модулю – поле.

Доказательство: Пусть p – простое число, $(a, p) = 1$. Тогда $\bar{a} \neq \bar{0}$ и по теореме Ферма $\bar{a}^{p-1} = \bar{1}$. Отсюда $\bar{a} \cdot \bar{a}^{p-2} = \bar{1}$, т.е. обратным к классу $\bar{a}$ является класс $\bar{a}^{p-2}$. Мы получили, что любой ненулевой класс $\bar{a}$ в $Z / p Z$ имеет обратный, а это означает, что $Z / p Z$ – поле.

Приложения в криптографии: алгоритм RSA

1. ***Выбирают два различных простых числа*** p и q, вычисляют их произведение $n = p \cdot q$.

p и q хранятся в тайне.	n - часть открытого ключа, доступ к нему открыт.

p := 149 q := 157

n := p·q n → 23393

2.Численное представление сообщения.

А	*Б*	*В*	*Г*	*Д*	*Е*	*Ж*	*З*	*И*	*Й*	*К*
10	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*

Л	*М*	*Н*	*О*	*П*	*Р*	*С*	*Т*	*У*	*Ф*	*Х*
21	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*

Ц	*Ч*	*Ш*	*Щ*	*Ъ*	*Ы*	*Ь*	*Э*	*Ю*	*Я*
32	*33*	*34*	*35*	*36*	*37*	*38*	*39*	*40*	*41*

: « … » ⇔ « 231528991415231513»

3.Запись численного сообщения в виде последовательности блоков (каждый блок меньше n):

2315 – 2899 – 1415 – 231 - 513

b1 - b2 - b3 - b4 - b5

4. Открытый кодирующий ключ криптосистемы RSA.

а) Находим $\varphi(n) = (p-1)\cdot(q-1)$; $\varphi(n) = 148 \cdot 156$, $\varphi(n) \to 23088$

б) выбираем натуральное число e *такое, что* $НОД\left(e,\varphi(n)\right)=1\cdot$

Наименьшее простое e*, взаимно простое с* $\varphi(n)\to 23088$*, это число*

$e=5.$

Проверка:

$\gcd(23088,2)\to 2$ $\gcd(23088,3)\to 3$

$\gcd(23088,4)\to 4$ $\gcd(23088,5)\to 1$

в) Пара чисел $(n,e)=(23393,5)$ *называется открытым кодирующим ключом криптосистемы RSA.*

5. Шифрование численного сообщения:

а) Пусть b_i *- блоки численного сообщения,* $0\le b_i\le n-1\cdot$

б) Через $a_i=E(b_i)$ *обозначается блок зашифрованного сообщения, соответствующий* $b_i.$

Он вычисляется по следующей формуле:

$E(b_i)$ *= Вычет* b_i^e *по модулю* $n\Rightarrow E(b_i)=\mathrm{mod}(b_i^e,n)\cdot$

Зашифрованное сообщение будет расположено в виде блоков

$$E(b_1)-E(b_2)-E(b_3)-E(b_4)-E(b_5)\cdot$$

в) Вычисление зашифрованных блоков

$$b_1=2315\ \triangleleft\triangleright\ E(b_1)=\mathrm{mod}(b_1^e,n)=\mathrm{mod}(2315^5,23393)\to 22247$$
$$b_2=2899\triangleleft\triangleright E(b_2)=\mathrm{mod}(b_2^e,n)=\mathrm{mod}(2899^5,23393)\to 19729$$
$$b_3=1415\triangleleft\triangleright E(b_2)=\mathrm{mod}(b_2^e,n)=\mathrm{mod}(1415^5,23393)\to 16674$$
$$b_4=231\triangleleft\triangleright E(b_4)=\mathrm{mod}(b_4^e,n)=\mathrm{mod}(231^5,23393)\to 13212$$
$$b_5=513\triangleleft\triangleright E(b_5)=\mathrm{mod}(b_5^e,n)=\mathrm{mod}(513^5,23393)\to 1135\cdot$$

г) Зашифрованное сообщение

$$\underset{a_1}{22247}-\underset{a_2}{19729}-\underset{a_3}{16674}-\underset{a_4}{13212}-\underset{a_5}{1135}.$$

6. Дешифровка сообщения.

а) Нахождение вычета (класса вычетов) d*, обратного к* e *по модулю* $m=\varphi(n)$*:*

$$[d]\cdot[e]=[1](\mathrm{mod}\,m),\ \textit{где}\ m=\varphi(n),\ \textit{т.е.}$$
$$[d]=[e]^{-1}\ \textit{по}\ \mathrm{mod}\,m.$$

По определению произведения классов по $\mathrm{mod}\,m$

$$[d]\cdot[e]=\{d\cdot e+k\cdot\varphi(n)\},k\in Z. \qquad (1)$$

Так как

$$[d]\cdot[e]=[1](\mathrm{mod}\,m), \qquad (2)$$

а по определению класса $[1]$

$$[1]=\{1+k\cdot\varphi(n)\}, \qquad (3)$$

то

$$[d]\cdot[e]=\left[1+k\cdot\varphi(n)\right],\Rightarrow$$

$$d\cdot e=1+k\cdot\varphi(n),k\in Z \qquad (4)$$

В пункте 4 выбрали $e=5,\ \varphi(n)\to 23088$. *Тогда формула (4) примет вид*

$$d\cdot 5=1+k\cdot 23088,k\in Z \quad (d\cdot 5+(-k)\cdot 23088=1,k\in Z)$$

Преобразуем её к виду

$$d=\frac{1+k\cdot 23088}{5},k\in Z$$

Следовательно, необходимо выбрать целое k *так, чтобы* d *было натуральным. Например,*

$$k=0\_Given\_d\cdot 5=1+k\cdot 23088\_Find(d)\to\frac{1}{5},$$

$$k=1\_Given\_d\cdot 5=1+k\cdot 23088\_Find(d)\to\frac{23089}{5}$$

$$k=2\_Given\_d\cdot 5=1+k\cdot 23088\_Find(d)\to\frac{46177}{5}$$

$$k=3\_Given\_d\cdot 5=1+k\cdot 23088\_Find(d)\to 13853\Rightarrow d=13853$$

б) Пара чисел (n,d) *называется Секретным дешифрующим (декодирующим) ключом системы RSA*

$$D_c=(n,d)=(23393,13853)\cdot$$

в) Дешифрование: если a_i *- блок шифрованного сообщения, то его расшифровка находится по формуле*

$$D(a_i)=\mathrm{mod}(a_i^{\,d},n)\equiv вычет(a_i^{\,d})\ по\ модулю\ n,$$

т.е.

$$D(a_i)\equiv остаток\ от\ деления\ a_i^{\,d}\ на\ модуль\ n\cdot$$

$$D(a_1)=\mathrm{mod}(a_1^{\,d},n)=\mathrm{mod}(22247^{13853},23393)\to 2315=b_1$$

$$D(a_2)=\mathrm{mod}(a_2^{\,d},n)=\mathrm{mod}(19729^{13853},23393)\to 2899=b_2$$

1. 13 Лекция № 13 (2 часа).

Тема: «Определение графов, основные понятия теории графов. Виды графов. Способы задания графов. Матрицы смежности и инцидентности графа. Матрица Кирхгофа. Числовые характеристики графов**»**

1.13.1 Вопросы лекции:

1. Основные понятия теории графов. Виды графов.
2. Операции над графами

1.3.2 Краткое содержание вопросов:

1. Основные понятия теории графов. Виды графов.

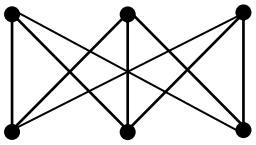
Определение графа. Часто бывает полезно и наглядно изобразить некоторую ситуацию в виде рисунка, состоящего из точек (вершин), представляющих основные элементы ситуации и линий (ребер), отражающих связи между элементами. Такие рисунки называются *графами*.

Между рассмотренным ранее понятием отношения и понятием графа существует тесная связь. Теория графов представляет собой удобный язык для описания программных и других моделей. Граф – это удобный способ изображения различных взаимосвязей (отношений). Граф может изображать сеть улиц в городе (вершины – перекрестки, улицы – ребра), блок-схемы программ, электрические цепи, географические карты и т.д

История теории графов. Теория графов возникла из решения различных прикладных задач. Первые задачи были связаны с решением математических развлекательных задач и головоломок. Рассмотрим эти задачи (пояснить подробнее)

1. *Задача о Кенигсбергских мостах.* Необходимо обойти все 4 части суши, пройдя по каждому мосту один раз, и вернуться в исходную точку. Ее развитие привело к циклу задач об обходах графов (Леонард Эйлер, 1736 г.).

2. *Задача о трех домах и трех колодцах*. Есть три дома и три колодца. Жители домов поссорились. Требуется от каждого дома проложить тропинку к каждому колодцу так, чтобы эти тропинки не пересекались. (Куратовский, 1930)



3.Задача о четырех красках. Любую карту на плоскости раскрасить четырьмя красками так, чтобы никакие две соседние области не были закрашены одинаково. Эта задача была сформулирована в середине XIX века, и попытки ее решить привели к появлению некоторых исследований графов, имеющих теоретическое и прикладное значение.

Многие результаты середины XIX века были получены при решении практических проблем. (Например, Кирхгоф: система уравнений токов и напряжений в электротехнической схеме представлялась графом и решалась с помощью методов теории графов; химия; Задача о перевозках, решение которой привело к созданию эффективных методов решения транспортных задач …). В XX веке задачи, связанные с графами, получили распространение не только в физике, электротехнике, химии, биологии, экономике, но и внутри различных разделов математики (алгебра, теория чисел, теория вероятностей и др.).

В проблематике теории графов можно выделить направления комбинаторного и геометрического характера. К первому относятся задачи о построении графов с заданными свойствами, о подсчете и перечислении таких графов. Геометрический характер носят, например, задачи, связанные с обходами графов. Характерным специфическим направле-

нием теории графов является цикл проблем, связанных с раскрасками, в которых изучаются разбиения множества вершин, обладающие определенными свойствами.

Основные понятия. Граф G *определяется как упорядоченная пара* ⟨V, E⟩*, где* V *– непустое множество* вершин*, отношение* $E \subset V^2$ *– множество* ребер *(набор неупорядоченных или упорядоченных пар вершин). Вершины и ребра графа называются его* элементами.

Граф, содержащий конечное число элементов, называется *конечным*. Число вершин конечного графа называется его *порядком* и обозначается $|V|$, число ребер обозначается как $|E|$: $G(V,E) = \langle V, E\rangle$, $V \neq \varnothing$, $E \subset V\times V$, $E = E^{-1}$.
Граф порядка n, имеющий m ребер, называется *(n,m)-графом*.

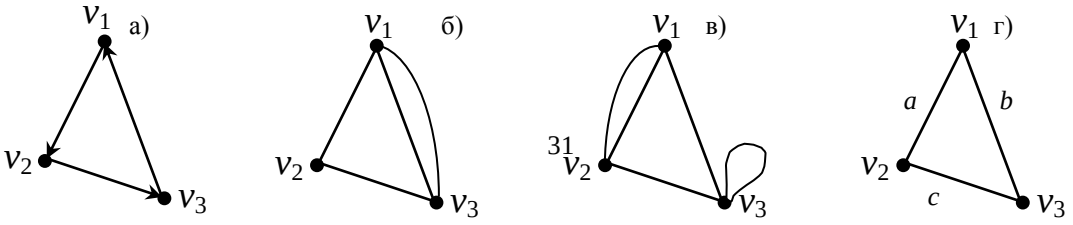
Обычно граф изображают *диаграммой*: вершины – точками или кружками, ребра – линиями (нарисовать). Такой способ задания графа является самым простым и наглядным, хотя и годится только для простейших случаев. Кроме того, затруднительно обрабатывать такой граф с помощью ЭВМ. Поэтому существуют специальные способы представления графа в ЭВМ, которые мы рассмотрим чуть позже.

Пусть v_1 и v_2 – вершины, e – соединяющее их ребро. Тогда ребро e и каждая из этих вершин называются *инцидентными* друг другу, вершины v_1 и v_2 называются *смежными*. Два ребра, имеющие одну общую вершину (инцидентные одной вершине), также называются *смежными*.

Множество вершин, смежных с вершиной v, называется *множеством смежности* (*окружением*) вершины v и обозначается $\Gamma^+(v) = \{u \in V \mid (u,v) \in E\}$, $\Gamma(v) = \Gamma^*(v) = \Gamma^+(v) \cup \{v\}$. Очевидно, что: $u \in \Gamma(v) \Leftrightarrow v \in \Gamma(u)$. Если не оговорено противное, то подразумевается Γ^+ и обозначается просто Г. Если A – множество вершин, то $\Gamma(A)$ – множество вершин, смежных с вершинами из A: $\Gamma(A) = \{u \in V \mid \exists v \in A \ \ u \in \Gamma(v)\} = \cup\Gamma(v) \ \forall v \in A$.
Другие определения графов и бинарные отношения. Часто рассматриваются следующие разновидности графов.

1. В некоторых задачах инцидентные ребру вершины рассматриваются в определенном порядке. Тогда элементами множества $E=\{(u,v) \mid u,v \in V\}$ являются упорядоченные пары, т.е. ребру приписывается направление от одной вершины к другой, и ребра называются *дугами* (говорят, что дуга *выходит* из вершины *u* и *заходит* в вершину *v*). Вершины в таком графе называются *узлами*, а сам граф, все ребра которого являются дугами, называется *ориентированным* графом, или *орграфом* (см. рис. а)). Иногда рассматриваются и *смешанные* графы, имеющие как дуги, так и неориентированные ребра.
2. Различные ребра графа могут быть инцидентны одной и той же паре вершин, в этом случае они называются *кратными* ребрами, а сам граф – *мультиграфом* (см. рис. б)).
3. Если элементом множества E является пара одинаковых элементов V, то такое ребро соединяет вершину саму с собой. Тогда это ребро называется *петлей*, а граф – *псевдографом* (рис. в)). В псевдографе возможно также наличие кратных ребер.
4. В отличие от мультиграфа и псевдографа, граф без петель и кратных ребер называется *простым*.
5. Если задана функция $F : V \to M$ или $F : E \to M$, то множество M называется *множеством пометок*, а сам граф называется *размеченным* (т.е. всем его вершинам или всем ребрам присвоены некоторые метки, в качестве которых обычно используются буквы или целые числа – г)).

Далее, говоря «граф G(V,E)», будем иметь в виду неориентированный непомеченный граф



без петель и кратных ребер.
Фактически, графы и бинарные отношения – это один и тот же класс объектов, описанный разными средствами. Отношения (в частности, функции) являются базовыми средствами для построения большинства математических моделей, используемых при решении практических задач. С другой стороны, графы допускают наглядное представление в виде диаграмм. Это объясняет широкое использование графов при кодировании и проектировании программ.
Любой граф с петлями, но без кратных ребер, задает бинарное отношение E на множестве V, и обратно. Пара элементов принадлежит отношению: $(a,b)\in E\subset V\times V \Leftrightarrow$ в графе есть G ребро (a,b). Неориентированный граф соответствует симметричному отношению. Изменение направления всех дуг соответствует обратному отношению. Мультиграф, все вершины которого имеют петли, задает рефлексивное отношение.

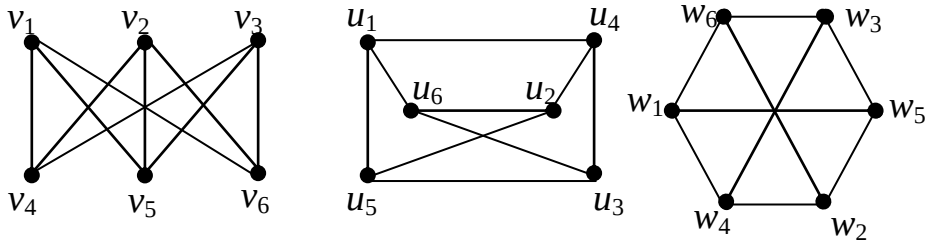
Изоморфизм графов: При изображении графа точки, обозначающие его вершины, берутся совершенно произвольно, поэтому рисунки одного и того же графа могут быть совершенно непохожими. Как же понять, одинаковы ли графы, изображенные разными чертежами? Решение проблемы стандартное – если можно взаимно однозначно отобразить множество вершин одного графа на множество вершин другого так, чтобы сохранилось отношение смежности, то это две копии графа.

Говорят, что два графа $G_1(V_1,E_1)$ и $G_2(V_2,E_2)$ *изоморфны*: $G_1\sim G_2$, если существует биекция (1-1 соответствие) $h: V_1\to V_2$, сохраняющая отношение инцидентности (при которой смежные вершины (ребра) графа G_1 переходят в смежные вершины (ребра) графа G_2): $e_1=(u,v)\in E_1 \Rightarrow e_2=(h(u),h(v))\in E_2$; $e_2=(u,v)\in E_2 \Rightarrow e_1=(h^{-1}(u),h^{-1}(v))\in E_1$;

Графы, отличающиеся только нумерацией вершин, являются *изоморфными*. Изоморфизм графов является отношением эквивалентности. Действительно, изоморфизм обладает всеми необходимыми свойствами: 1) рефлексивность – G~G, где требуемая биекция есть тождественная функция;

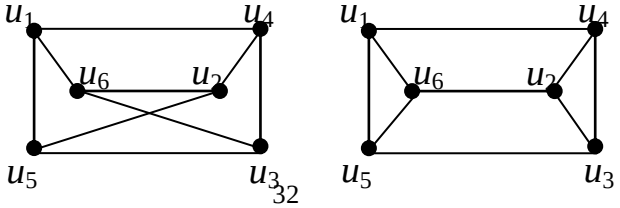
2) симметричность – если $G_1\sim G_2$ с биекцией h, то $G_2\sim G_1$ с биекцией h^{-1};
3) транзитивность – если $G_1\sim G_2$ с биекцией h, а $G_2\sim G_3$ с биекцией g; то $G_1\sim G_3$ с биекцией $g\circ h$.

Графы рассматриваются с точностью до изоморфизма, т.е. рассматриваются классы эквивалентности по отношению изоморфизма.



Три внешне различные диаграммы, приведенные на рисунке, являются диаграммами одного и того же графа.

Числовая характеристика, одинаковая для всех изоморфных графов, называется *инвариантом* графа. В частности, количество вершин и количество ребер – инварианты графа *G*.



Не известно никакого набора инвариантов, определяющих граф с точностью до изоморфизма..

Операции над графами

«Способы задания графов. Матричное представление графов. Числовые характеристики графов»

1. Способы задания графов. Матричное представление графов.
2. Числовые характеристики графов

Краткое содержание вопросов:

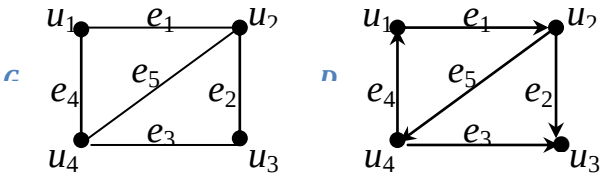
1. Способы задания графов. Матричное представление графов

Представление графов в ЭВМ. Требования к представлению графов. Чтобы задать граф, нужно каким-либо способом описать множество его вершин, множество его ребер, а также указать, какие вершины и ребра инцидентны (или смежные), т.е. задать отношение инцидентности (смежности). Рассмотрим несколько способов представления графа в ЭВМ. Они различаются объемом занимаемой памяти и скоростью выполнения операций над графами. Представление выбирается по потребностям конкретной задачи.

Напомним: число вершин графа обозначаем через *n*, а число ребер – через *m*. Характеристика *M(n,m)*, приведенная для каждого представления, означает требуемый для него объем памяти.

Указанные представления пригодны для графов и орграфов, а после некоторой модификации – для псевдографов, мультиграфов и гиперграфов.

Все представления будем иллюстрировать на конкретных примерах графа *G* и орграфа *D* (см. рисунок.).



Способы представления графа

1) Матрица смежности.

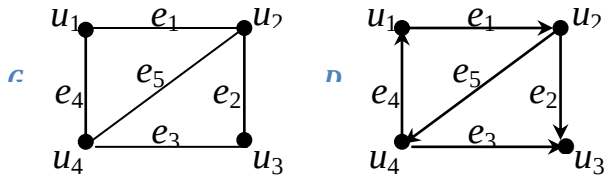
Матрица смежности A(G') графа (орграфа) – это квадратная матрица размера n×n, у которой для любых $i,j \in \{1,2,\ldots,n\}$ элемент в *i*-й строке и *j*-м столбце равен 1, если *i*-я и *j*-я вершины соединены ребром (дугой с началом в вершине *i*), и равен 0 в противном случае.

$$a_{ij} = \begin{cases} 1, & \text{если вершины } v_i \text{ и } v_j - \text{смежные (для орграфа дуга идет из } v_i \text{ в } v_j) \\ 0, & \text{иначе} \end{cases}$$

Память $M(n,m)=O(n^2)$.

Фактически это уже знакомая нам матрица бинарного отношения. Очевидно, что матрица смежности неориентированного графа является симметричной, элементы главной диагонали равны нулю, а количество единиц в каждой строке равно степени вершины, которой соответствует эта строка. По матрице смежности легко построить диаграмму графа.

Матрица смежности орграфа, не являющегося мультиграфом, не может быть симметричной, т.к. при ее составлении вершины орграфа играют различные роли.

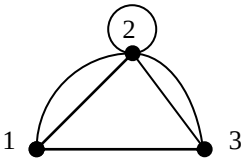


Матрицы смежности для заданных графа *G* и орграфа *D*

$$A(G)=\begin{pmatrix}0&1&0&1\\1&0&1&1\\0&1&0&1\\1&1&1&0\end{pmatrix}\quad A(D)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\0&0&0&0\\1&0&1&0\end{pmatrix}$$

В матрице смежности мультиграфа или псевдографа число, находящееся на пересечении i-й строки и j-го столбца, совпадает с числом ребер, соединяющих вершины i и j, при этом каждая петля считается двумя ребрами.

Псевдограф, изображенный на рисунке, имеет матрицу смежности следующего вида: $A(P)=\begin{pmatrix}0&2&1\\2&2&2\\1&2&0\end{pmatrix}$



2) Матрица инцидентности.

Другой способ задать граф – определить *матрицу инцидентности* (или *инциденций*) *I(G)*, имеющую *n* строк и *m* столбцов, элементы которой задаются следующим образом:

$$i_{kl}=\begin{cases}1, & \text{если вершина } v_k \text{ инцидентна ребру } e_l\\ 0, & \text{иначе}\end{cases}$$

Для ориентированного графа:

$$i_{kl}=\begin{cases}1, \text{если вершина } v_k \text{ инцидентна ребру } e_l \text{ и является его концом}\\ 0, \text{если вершина } v_k \text{ и ребро } e_l \text{ неинцидентны}\\ -1, \text{если вершина } v_k \text{ инцидентна ребру } e_l \text{ и является его началом.}\end{cases}$$

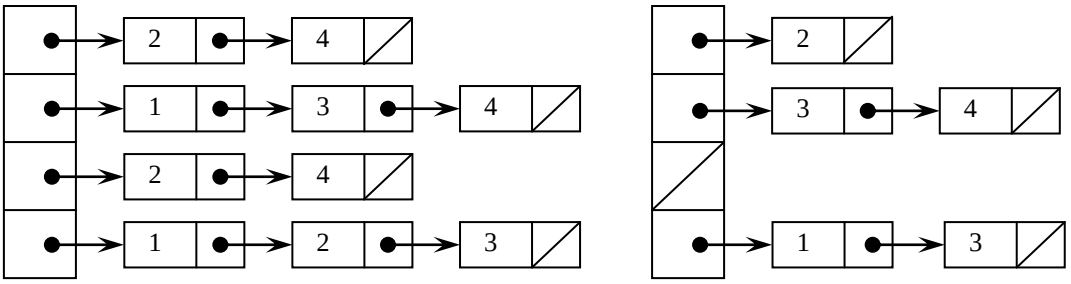
Матрицы инцидентности для заданных графа *G* и орграфа *D*

$$I(G)=\begin{pmatrix}1&0&0&1&0\\1&1&0&0&1\\0&1&1&0&0\\0&0&1&1&1\end{pmatrix}\quad I(D)=\begin{pmatrix}-1&0&0&1&0\\1&-1&0&0&-1\\0&1&1&0&0\\0&0&-1&-1&1\end{pmatrix}$$

Очевидно, что в каждом столбце матрицы инцидентности только два элемента отличны от 0 (или один, если ребро является петлей), т.к. ребро может быть инцидентно не более чем двум вершинам (а столбец соответствует ребру). Поэтому матрица содержит много нулей и такой способ описания неэкономен. *M(n,m)=O(n·m).*

3) Списки смежности.

Граф представляется с помощью списочной структуры (списка смежности), отражающей смежность вершин и состоящей из массива указателей на списки смежных вершин. Элемент списка представлен структурой с двумя полями: номер вершины и указатель. Для неориентированных графов *M(n,m)=O(n+2m),* для орграфов *M(n,m)=O(n+m).*



Списки смежности для заданных графа *G* и орграфа *D:*

	кон	нач	кон
1	2	1	2
1	4	2	3
2	3	2	4
2	4	4	1
3	4	4	3

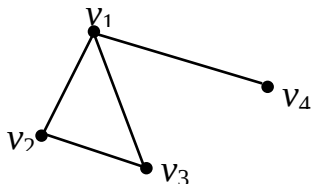
4) Массив ребер (дуг).

Отношение инцидентности можно задать также списком ребер графа. Каждая строка этого списка соответствует ребру, в ней записаны номера вершин, инцидентных ему. *M=O(2m).*

По списку ребер графа легко построить матрицу инцидентности, т.к. каждое ребро этого списка соответствует столбцу матрицы, а номера вершин в каждом элементе списка – это номера строк матрицы инцидентности, элементы в которых равны 1. Для орграфа координата начала – номер строки, где стоит –1, а координата конца – номер строки, где стоит 1.

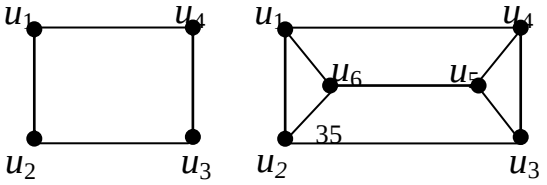
2. Числовые характеристики графов

Степенью (или *валентностью*) *вершины v* называется число инцидентных ей ребер. Степень вершины обозначается *deg(v)*. Очевидно, что для любой вершины $v \in V$ справедливо: $0 \le deg(v) \le |V| - 1$; $deg(v) = |\Gamma(v)|$. Вершина графа, имеющая степень 0, называется *изолированной*, а вершина со степенью 1 – *висячей*, или *концевой*.



В показанном на рисунке графе вершина v_4 является висячей: $deg(v_4) = 1$. Степени остальных вершин: $deg(v_1) = 3$; $deg(v_2) = deg(v_3) = 2$.

Если степени всех вершин графа одинаковы и равны некоторому числу *k*, то такой граф называется *регулярным* графом степени *k*. Степень регулярности является инвариантом графа и обозначается *r(G)*. Для нерегулярных графов *r(G)* не определено. На рисунке показаны регулярные графы соответственно степени 2 и 3. Найдем степенную последовательность для графа *G*. Выпишем степени всех вершин графа в соответствии с их номерами (2,2,3,2,1).



1.14 Лекция № 14 (2 часа).

Тема: «Свойства графов: маршруты, циклы, связность. Свойства регулярных, двудольных и связных графов. Метрические характеристики связных графов»

1.14.1 Вопросы лекции:

1. Маршруты, циклы, связность.
2. Метрические характеристики графов.

1.14.2 Краткое содержание вопросов:

1. Маршруты, циклы, связность.
2. Метрические характеристики графов.

Маршруты, цепи, циклы. Маршрутом *от вершины* u *к вершине* v *или (*u,v*)*-маршрутом *в графе* G *называется всякая последовательность вида* $u = v_0, e_1, v_1, e_2, \ldots, e_n, v_n = v$*, в которой любые два соседних элемента инцидентны, т.е.* e_k *– ребро, соединяющее вершины* v_{k-1} *и* v_k, k = *1,2,…,*n.

Это определение подходит также для псевдо-, мульти- и орграфов. В случае орграфа v_{k-1} *– начало* ребра e_k , а v_k – его *конец*. При этом вершину *u* называют *началом маршрута*, а вершину *v* – его *концом*. В маршруте некоторые вершины и ребра могут совпадать. Если *u* = *v*, то маршрут *замкнут*, а иначе *открыт*. Для «обычного» графа маршрут можно задавать только последовательностью вершин $v_0, v_1, \ldots, v_n$ или ребер $e_1, e_2, \ldots, e_n$.

Маршрут называется *цепью*, если в нем нет совпадающих ребер, и *простой цепью* – если дополнительно нет совпадающих вершин, кроме, может быть, начала и конца цепи. Про цепь $u = v_0, v_1, \ldots, v_n = v$ говорят, что она *соединяет* вершины *u* и *v* и обозначают $\langle u,v \rangle$.

Очевидно, что если есть цепь, соединяющая вершины *u* и *v*, то есть и простая цепь, соединяющая эти вершины.

Замкнутая цепь называется *циклом*; замкнутая простая цепь – *простым циклом*. Число циклов в графе *G* обозначается *z(G)*. Граф без циклов называется *ациклическим*. Для орграфов цепь называется *путем*, а цикл – *контуром*.

Число ребер в маршруте M (возможно, с повторениями) называется его *длиной*, обозначается |M|.

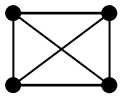
Расстоянием между вершинами u и *v* (обозначается *d*(*u*,*v*)) называется длина кратчайшей цепи $\langle u,v \rangle$, а сама кратчайшая цепь называется *геодезической*. Если не существует цепи, соединяющей вершины *u* и *v*, то по определению *d*(*u*,*v*) = +∞.

Диаметром графа *G* (обозначается *D(G)*) называется длина длиннейшей геодезической.

Максимальным удалением в графе *G от вершины v* называется *r(v) = max* $d(v,v'), \forall\, v' \in V$. Вершина *v* графа *G* является его *центром*, если максимальное удаление от нее до всех вершин принимает наименьшее значение.

Множество вершин, находящихся на одинаковом расстоянии n от вершины v, называется *ярусом* (обозначается $D(v,n)$): $D(v,n) = \{u \in V \mid d(v,u) = n\}$.

Граф, любая из вершин которого является его центром – максимальное удаление до всех вершин от любой =

Связность. *Если две вершины u и v в графе можно соединить*  *цепью, то такие вершины связаны. Граф называется связным, если в нем связаны все вершины.*

Легко видеть, что отношение связности на множестве вершин является отношением эквивалентности. Данное отношение разбивает множество вершин графа на классы, объединяющие вершины, связанные друг с другом. Такие классы называются *компонентами связности*; число компонент связности обозначается $k(G)$.

Граф G является связным тогда и только тогда, когда он имеет одну компоненту связности: $k(G) = 1$. Если $k(G) > 1$, то это *несвязный* граф. Граф, состоящий только из изолированных вершин (в котором k(G)=|V|, r(G)=0), называется *вполне несвязным*.

Вершина графа, удаление которой увеличивает число компонент связности, называется *разделяющей* или *точкой сочленения*.

Ориентированный граф $G(V,E)$ является *слабо связным* (*слабым*), если симметричное замыкание множества E определяет связный граф (иными словами, если после замены всех дуг графа G ребрами полученный граф будет связным). Ориентированный граф является *сильно связным* (*сильным*), если для любой пары вершин $u,v \in V$ существует ориентированный путь из u в v (т.е. из любой вершины графа достижимы все его остальные вершины). Если для любой пары вершин по крайней мере одна достижима из другой, то такой граф является *односторонне связным*, или *односторонним*. Граф, состоящий из одной вершины, по определению считается сильно связным.

Множества вершин связных компонент образуют разбиение множества вершин графа.

1.15 Лекция № 15 (2 часа).
Тема: «Деревья. Свойства деревьев»

1.15.1 Вопросы лекции:
1. Деревья.
2. Свойства деревьев.
3. Задача об остове минимального веса.

1.15.2 Краткое содержание вопросов:

1. Деревья.

Деревья являются простейшим классом графов. Для них выполняются многие свойства, которые не всегда выполняются для обычных графов. Кроме того, деревья широко применяются в программировании при различного рода обработке данных, в частности, в алгоритмах сортировки, кодирования и т.п. Подробно алгоритмы работы с деревьями будут рассматриваться позднее в других курсах, а сейчас только краткое знакомство.

Дерево – это связный граф без циклов. Несколько деревьев (или несвязный граф без циклов) составляют *лес*. Таким образом, дерево является компонентой связности леса.

Пусть $G=(S,U)$ и $|S|=n,\ |U|=m.$ Тогда справедлива эквивалентность следующих утверждений:

1). G - дерево;

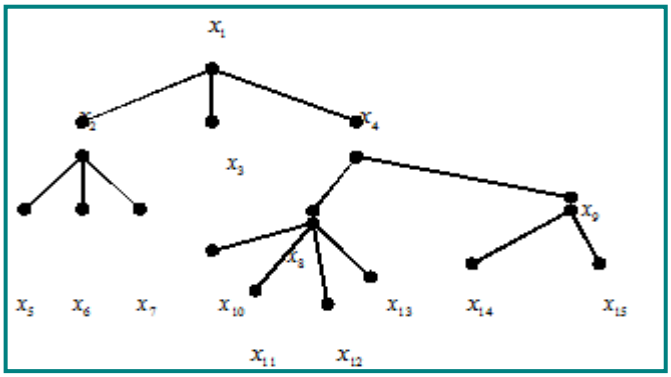
2). G - связный граф и $m=n-1$;

3). G - ациклический граф и $m=n-1$;

4). любые две несовпадающие вершины графа соединяет единственная простая цепь;

5). G - ациклический граф, обладающий тем свойством, что если какую- либо пару его несмежных вершин соединить ребром, то полученный граф будет содержать ровно один цикл.

Ориентированный граф называется ориентированным деревом (ордеревом), если: 1). существует ровно одна вершина $x_1 \in S$, называемая корнем, которая не имеет предшествующих вершин, то есть $P(x_1)=0$;



2). любой вершине $x_j \neq x_1$ в графе G непосредственно предшествует ровно одна вершина, то есть $P(x_j)=1.$

Неориентированное дерево можно превратить в ориентированное, выбрав в качестве корня произвольную вершину. Пусть $G=(S,U)$. Граф $G'=(S',U')$ называется подграфом графа G, если $S' \subset S$ и $U' \subset U.$ Подграф G' графа G называется остовным подграфом, если $S'=S.$ Подграф G' графа графа G называется остовным поддеревом (остовом, каркасом), если $S'=S$ и G - дерево.

2. Свойства деревьев.

Теорема Кэли[*]**.** *Число различных деревьев, которые можно построить на n различных вершинах, равно $t_n=n^{n-2}$.*

В этой формуле подсчитывается число всех деревьев с данными n вершинами. Многие из этих деревьев изоморфны, и возникает вопрос о числе не изоморфных деревьев среди них. Это более трудная задача, она решается для каждого конкретного случая по алгоритму теории Пойа.

Вернемся к произвольным графам. Матрицей Кирхгофа[**] графа G называется матрица $B_{n\times n}$, $n=|S|$, если $b_{ij}=\begin{cases}-1, & x_i \text{ и } x_j \text{ смежны},\\ 0, & x_i \text{ и } x_j \text{ не смежны},\\ P(x_i), & i=j.\end{cases}$ Сумма элементов в каждой строке и каждом столбце этой матрицы равна нулю, то есть $\sum\limits_{i=1}^{n} b_{ij}=0,\ j=\overline{1,n}$, $\sum\limits_{j=1}^{n} b_{ij}=0,\ i=\overline{1,n}$.

Кроме того, из этого следует, что алгебраические дополнения всех элементов матрицы B равны между собой. Матрица Кирхгофа используется для подсчета числа остовов в графе.

[*] Артур Кэли(Кэйли) (1821-1895 г. г.) - английский математик.

[**] Густав Роберт Кирхгоф (1824-1887 г. г.) -немецкий физик

Теорема Кирхгофа. *Число остовных деревьев в связном графе* G *порядка* $n \geq 2$ *равно алгебраическому дополнению любого элемента матрицы Кирхгофа* $B(G)$.

3. Задача об остове минимального веса.

Пусть $G = (S, U)$ - связная сеть. В приложениях часто возникает задача о построении остова графа G, имеющего наименьший вес. Пусть, например, $G = (S, U, \Omega)$ служит моделью железнодорожной сети, соединяющей пункты $x_1, x_2, ..., x_n \in S$, а $\omega(x_i, x_j)$ - расстояние между пунктами x_i и x_j. Требуется проложить сеть телеграфных линий вдоль линий железнодорожной сети так, чтобы все пункты $x_1, x_2, ..., x_n$ были связаны между собой телеграфной сетью и общая протяженность линий телеграфной сети была наименьшей.

Известно несколько алгоритмов построения кратчайшего остовного дерева.

1.16 Лекция № 16 (2 часа).
Тема: «Конечные автоматы»

1.16.1 Вопросы лекции:
1. Конечные автоматы.

1.16.2 Краткое содержание вопросов:

1. Понятие конечного автомата. Историческая справка. Способы задания конечного автомата. Примеры конечных автоматов. Виды автоматов. Общие задачи теории автоматов

1.17 Лекция № 17 (2 часа).
Тема: «Формализации понятия алгоритма. Математические машины. Машина Тьюринга**»**

1.17.1 Вопросы лекции:
1. Формализации понятия алгоритма.
2.Математические машины. Машина Тьюринга.

1.17.2 Краткое содержание вопросов:
Формализация понятия алгоритма. Универсальные модели алгоритмов.

Интуитивное понятие алгоритма обладает целым рядом недостатков. Очевидно, что такие понятия, использованные при описании общих свойств алгоритмов, как элементарность шагов, сами нуждаются в уточнении. Очевидно, что их словесные определения будут содержать новые понятия, которые снова потребуют уточнения и т.д. Начиная с 30-х годов, было предложено несколько уточнений понятия алгоритма. Считается, что все они достаточно полно отражают основные черты интуитивного понятия алгоритма. Действительно, все формальные определения алгоритма в некотором смысле эквивалентны друг другу. Поэтому в теории алгоритмов применяется другой подход: выбирается конечный набор исходных объектов, которые объявляются элементарными и конечный набор способов построения их них новых объектов. Этот метод был уже использован в теории множеств и получил название *конструктивного подхода*.

Алгоритмические модели, которые претендуют на право считаться формализацией понятия «алгоритм», должны быть универсальными, т.е. допускать описание любых алгоритмов.

Можно выделить три основных типа универсальных алгоритмических моделей, различающихся исходными эвристическими соображениями относительно того, что такое алгоритм. Первый тип связывает понятие алгоритма с наиболее традиционными понятиями математики – вычислениями и числовыми функциями. Наиболее развитая и изученная модель этого типа – рекурсивные функции – является исторически первой формализацией понятия алгоритма.

Второй тип модели связан с развитием вычислительной техники и основан на представлении об алгоритме как о некотором детерминированном устройстве, способном выполнять в каждый отдельный дискретный момент времени весьма примитивные операции. Такое представление не оставляет сомнений в однозначности алгоритма и элементарности его шагов. Кроме того, эвристика этой модели близка к ЭВМ и, следовательно, к инженерной интуиции. Основной теоретической моделью этого типа является созданная в 30-х годах концепция машины Тьюринга. Именно машина Тьюринга явилась моделью современной ЭВМ и способствовала развитию современной вычислительной техники.

Наконец, третий тип алгоритмических моделей – это преобразование слов в произвольных алфавитах, в которых элементарными операциями являются подстановки, т.е. замены части слова (подслова) другим словом. Преимущества этого типа моделей заключаются в максимальной абстрактности и возможности применить понятие алгоритма к объектам произвольной, не обязательно числовой природы. Примерами моделей этого типа являются канонические системы Поста и нормальные алгоритмы Маркова. При этом общность формализации в конкретной модели не теряется и доказывается сводимость одних моделей к другим, т.е. показывается, что всякий алгоритм, описанный средствами одной модели, может быть описан средствами другой.

Благодаря взаимной сводимости моделей в общей теории алгоритмов удалось выработать инвариантную по отношению к моделям систему понятий, позволяющую говорить о свойствах алгоритмов независимо от того, какая формализация алгоритма выбрана. Эта система понятий основана на понятии вычислимой функции, т.е. функции, для вычисления которой существует алгоритм.

МАШИНА ТЬЮРИНГА.

Введение. История вопроса.

В 1935 г. возникло такое положение: свойства, обнаруженные у некоторого точно определенного класса вычислимых теоретико-числовых функций, изучавшихся Чёрчем и Клини в 1932—1935 гг. и названных "λ-определимыми функциями", упорно подсказывали мысль, что этот класс, может быть, охватывает все функции, которые в соответствии с нашим интуитивным представлением можно рассматривать как вычислимые. При этих обстоятельствах Чёрч выдвинул тезис (опубликован в 1936 г.), что все функции, которые интуитивно мы можем рассматривать как вычислимые, или, говоря его словами, как «эффективно вычислимые», являются λ-определимыми, или, эквивалентным образом, общерекурсивными.

Несколько позже, но независимо появилась статья Тьюринга (1936), в которой был введен еще один точно определенный класс интуитивно вычислимых функций, которые

мы будем называть «функциями, вычислимыми по Тьюрингу», и относительно этого класса было высказано такое же утверждение; это утверждение мы называем *тезисом Тьюринга.* Вскоре Тьюрингом [1937] было показано, что его вычислимые функции — это то же самое, что λ-определимые функции, и, следовательно, то же самое, что и общерекурсивные функции. Поэтому тезисы Тьюринга и Чёрча эквивалентны. Мы будем обычно ссылаться на оба эти тезиса как на *тезис Чёрча,* а в связи с тем его вариантом, в котором идет речь о «машинах Тьюринга»,— как на *тезис Чёрча — Тьюринга.* В 1936 г. Пост независимо от Тьюринга опубликовал в довольно сжатом изложении формулировку, в основе ту же, что у Тьюринга. В 1943 г., основываясь на своей неопубликованной работе 1920—1922 гг., он опубликовал третий эквивалент аналогичного тезиса. Еще одну эквивалентную формулировку дает теория алгоритмов Маркова [1951г].

Область использования машины Тьюринга

Понятие *машины Тьюринга* возникает в результате прямой попытки разложить интуитивно известные нам вычислительные процедуры на элементарные операции: Тьюринг привел ряд доводов в пользу того, что повторения его элементарных операций было бы достаточно для проведения любого возможного вычисления. Поэтому машина Тьюринга (МТ) используется:

1) если требуется доказать *возможность* алгоритмической реализации вычислительной функции;
2) если требуется *оценить вычислительную сложность* или *трудоемкость* решения задачи по данному алгоритму, т.е. время выполнения алгоритма.

Для этого мы моделируем работу произвольного алгоритма в терминах рассматриваемой задачи. Затем *определяется* класс машин-вычислителей, которые могут решить данную задачу – формально описываются правила работы машины, исходные данные, ограничения и т.д. (поскольку в определении задачи ничего не говорится о программах так таковых в привычном для нас понимании, то алгоритмическая *разрешимость* или *неразрешимость*, сводится к проблеме остановки произвольного алгоритма решения задачи). В качестве машины-вычислителя выберем машину Тьюринга, поскольку ранее было показано, что всякая вычислимая функция реализуема на МТ и сведем решение данной задачи к существующим группам задач, для которых известно, что они решаются на МТ.

Принцип работы машины Тьюринга.

Какая именно команда программы будет выполняться в данный момент, определяется двумя параметрами: читаемым головкой символом и состоянием машины.

Результатами выполнения команды являются: новый символ записанный на ленту в ту ячейку, напротив которой находится в данный момент головка; перемещение головки на одну позицию (ячейку) вправо или влево вдоль ленты; переход машины в новое состояние. В частных случаях новый символ может быть равен старому, перемещение может отсутствовать, состояние может остаться прежним.

Формат команды имеет следующий вид:

$a\ q\ b\ r\ D,$

где a — читаемый символ; q — текущее состояние; b — символ записываемый в обозреваемую ячейку ленты вместо символа a; r — новое состояние; D — направление движения головки машины относительно ленты.

Символы выбираются из конечного алфавита $A = \{a_1, \ldots, a_1\}$.

В дальнейшем будем использовать трехсимвольный алфавит $\{e\ 0, 1\}$, причем e будет

означать «пустой (empty)» символ — отсутствие информации в ячейке, а с помощью нуля и единицы будут кодироваться все данные. Иногда используют двухсимвольный алфавит $A = \{e, 1\}$. В этом случае числа кодируются только единицами: нуль кодируется одной единицей, число один кодируется двумя единицами, а число x кодируется $x + 1$ единицами Это — единичная система счисления. Однако она плоха с точки зрения сложности задач (см. гл. 5).

Множество состояний обозначим $Q = \{ q_1, \ldots, q_k \}$. Направление движения D выбирается из множества {L, *R, S*} где L — движение влево, R — движение вправо, S — отсутствие движения.

Таким образом, команда 1 q_3 0 q_6 L означает: если, находясь в состоянии q_3, машина Тьюринга обозревает ячейку ленты в которой записана 1, то машина должна записать в эту ячейку 0, произвести сдвиг головки относительно ленты влево на одну ячейку и перейти в состояние q_6.

Это описание действия, соответствующего команде говорит о том, что команда может рассматриваться как отображение пар (a, q) в тройки (b, r, D), т. е. отображение

$$AxQ => AxQx \{L, R, S\}.$$

Данное отображение является частичным, так как не для любой пары-аргумента существует тройка-результат. Но для произвольной пары существует не более одной тройки, т. е. отображение не является многозначным.

Все действия производятся в дискретном времени. Иначе говоря, можно рассматривать целочисленные моменты времени t = = 0, 1, 2, 3, . . . Любое изменение происходит мгновенно в момент $t = i$ *и* ничего не меняется между двумя соседними моментами времени.

Работает машина Тьюринга следующим образом. Стартовая конфигурация: на ленте находятся исходные данные — строка символов в алфавите A, состояние внутренней памяти соответствует некоторому оговоренному (всегда одному и тому же) начальному состоянию, например, q_1. При этом головка машины обозревает некоторую ячейку ленты с записанным там символом a. Нормальным считается начальное положение головки напротив самого левого непустого символа, т. е. не совпадающего с e.

Момент старта рассматривается как нулевой момент времени. В момент старта выполняется первая команда, это единственная команда, начинающаяся с пары (a, q_1). В результате выполнения команды машина перейдет в новое состояние, и головка машины прочтет новый символ с ленты. Эта пара (новый символ, новое состояние) станет начальной частью следующей команды и т. д. Машина будет продолжать работать в дискретном времени, шаг за шагом переходя из состояния в состояние, и постепенно изменяя содержимое ленты. Наконец, для некоторой пары (a, q) не окажется команды в программе. Такая ситуация считается завершающей. Машина прекращает функционирование. Оставшаяся запись на ленте считается записью результата.

Таким образом, машина Тьюринга реализует вычисление некоторой функции — отображения исходной строки символов в результирующую строку.

Существует несколько способов представления программы машины Тьюринга (множества команд). Два наиболее употребительных:

1) двумерная таблица (рис. 1.2);

2) диаграмма (нагруженный псевдограф).

В двумерной таблице строки помечаются различными символами алфавита, а столбцы — именами различных состояний машины, т. е. таблица имеет размер Ik. Каждой команде программы

Состояние Символ	q_1	…	q	…	q_k

a_1					
…					
			brD		
…					
a1					

Рис. 1.2. Табличная форма программы машины Тьюринга

соответствует единственная клетка в таблице. Она определяется для команды *a q b r D* следующим образом: в клетку, находящуюся на пересечении строки, помеченной символом я, и столбца помеченного состоянием *q.* вписывается тройка b *r D.*

Для некоторых пар *(a, q)* в программе нет команд, следовательно, соответствующие клетки таблицы остаются пустыми. При достижении в процессе работы пустой клетки машина Тьюринга останавливается.

В качестве простого примера приведем программу вычисления функции S(x) = x + 1, т. е. увеличение аргумента на единицу (рис. 1.3). Используем алфавит A = *{e,* 0, 1}, причем х будем кодировать последовательностью нулей и единиц так. как это принято при двоичном кодировании целых неотрицательных чисел.

предположим также, что в момент старта головка машины Тьюринга находится напротив крайней левой ячейки с символом 1**.**

	q_1	q_2	q_3	q_4
0	$0q_1R$	$1q_3L$	$0q_3L$	
1	$1q_1R$	$0q_2L$	$1q_3L$	
e	eq_2L	$1q_4S$	eq_4R	

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы не предусмотрены рабочим учебным планом

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие №ПЗ-1 (2 часа).

Тема: «Множества и операции над ними».

3.1.1 Задание для работы:

1. Множества и операции над ними. Диаграммы Венна-Эйлера.
2. Элементы алгебры множеств.

3.1.2 Краткое описание проводимого занятия ПЗ-1

1. Множества и операции над ними. Диаграммы Венна-Эйлера.
2. Элементы алгебры множеств.

1. Множества и операции над ними. Диаграммы Венна-Эйлера.

Задание 1.

1.Перечислите элементы следующих множеств:

Задания аудиторные, для самостоятельного выполнения.

а) $A=\{x: x\in Z, 10\le x\le 18\}$ ..... $A=\left\{x: x\in Z, \frac{1}{x^2}\ge\frac{1}{16}\right\}$;

б) $B=\{x: x\in Z, 6x^2+x-1=0\}$ ..... $B=\{x: x\in R, 6x^2+x-1=0\}$.

2.Описать множества с помощью предикатов:

а) $C=\{2,5,8,11,...\}$ ..... $C=\left\{1,\frac{1}{3},\frac{1}{7},\frac{1}{15},...\right\}$.

3. $U=\{1,2,3,4,5,6,7,8\}$-универсальное множество,

$A=\{1,2,3,4\}, B=\{3,5,7\}, C=\{1,4,5,6\}$. Найти элементы множеств:

а) $B\cap C, (A\cup B)\cap(A\cap C)$ ..... $A\cup C$, $A\cap B\cap C$,

б) $B\setminus C, \overline{A\cup B}$ ..... $B\Delta C, \overline{C}$.

4. $A=\{3n: n\in Z, n\ge 4\}, B=\{2n: n\in Z\}, C=\{n: n\in Z, n^2\le 100\}$. С помощью операций на множествах выразить через A, B, C следующие множества:

а) $\{\pm1,\pm3,\pm5,...\}$ ..... $\{6n: n\in Z, n\ge 2\}$

б) $\{-9,-7,-5,-3,-1,0,1,3,5,7,9\}$ ..... $\{-10,-8,-6,-4,-2,0,2,4,6,8,10\}$.

2. Элементы алгебры множеств.

5.Проиллюстрируйте диаграммами Венна тождества:

а) закон дистрибутивности $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$,

б) $A\cap(B\Delta C)=(A\cap B)\Delta(A\cap C)$.

6.Докажите тождества:

а) $(\overline{A\cap\overline{B}})\cup B=\overline{A}\cup B$ ..... $(A\setminus B)\setminus C=A\setminus(B\cup C)$.

7.Найти булеан $P(A)$ множества A:

а) $A=\{a,b,c\}$ ..... $A=\{2,5,8,9\}$.

Задание 2.

1.Пусть A, B, C - произвольные конечные множества. Доказать:

а) $A\times(B\cap C)=(A\times B)\cap(A\times C)$,

б) $(A\cup B)\times C=(A\times C)\cup(B\times C)$.

2. $U=\{1,2,3,4,5\}, A=\{1,3,5\}, B=\{3,4\}$. Найти характеристические векторы подмножеств A, B, по ним найти характеристические векторы множеств а) $A\cup B$, б) $A\cap B$, в) $\overline{B}$ и перечислить элементы этих множеств.

3.1.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили понятия об основных операциях с множествами и алгебре множеств;
- приобрели умения и навыки выполнения операций с множествами, построения бинарных отношений;

3.2 Практические занятия №ПЗ-2 (2 часа),

Тема: «Бинарные отношения и их свойства. Отношения эквивалентности и частичного порядка»

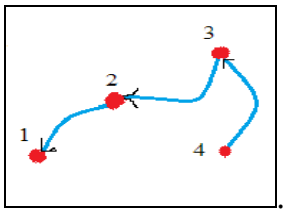
3.2.1 Задание для работы:

1. Бинарные отношения и их свойства.
2. Отношения эквивалентности и частичного порядка

3.2.2 Краткое описание проводимых занятий ПЗ-2:

1. Способы задания отношений.
2. Свойства отношений.
3. Понятие отношения эквивалентности.
4. Отношения эквивалентности в математических и прикладных концепциях.
5.Отношения частичного порядка.
6.Отношения Парето. Принятие решений при многих критериях

1. На множестве $A=\{1,2,3,4\}$ отношение R , данное перечислением пар $R=\{(2,1),(3,2),(4,3)\}$, изобразить графом и задать матрицей.

Решение. 

.

Матрица отношения равна $R=\begin{pmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$.

2. Отношение на паре $A=\{1,2,3\}, B=\{a,b,c,d\}$ множеств задано матрицей $\begin{pmatrix}1&0&1&0\\1&0&1&0\\0&1&1&0\end{pmatrix}$. Описать отношение перечислением пар и изобразить орграфом.

3. Отношения на множестве натуральных чисел N заданы предикатами:

а) $R=\{(x,y):2x+y=9\}$; б) $S=\{(x,y):x+y<7\}$; в) $T=\{(x,y):y=x^2\}$.

Задать эти отношения перечислением пар.

4. На множестве $A=\{1,2,3,4\}$ отношение определено предикатом $R=\{(x,y):x+2y=2n-1, n\in A\}$. Представить R каждым из способов:

а) в виде множества упорядоченных пар;
б) графом;
в) матрицей.

5. Указать, какие из следующих отношений на Z являются рефлексивными, симметричными, транзитивными?

а) $x+y-$нечётное число; б) $x+y-$чётное число; в) $x\cdot y-$ нечётное число;

г) $x+x\cdot y-$ чётное число.

2. Свойства отношений, классификация отношений. Отношения эквивалентности и порядка.

2. Является ли следующее отношение рефлексивным? Симметричным (антисимметричным)? Транзитивным? Отношением эквивалентности или частичного порядка? Линейного порядка? Обосновать.

$$R=\left\{(x,y):x=mq_1+r,y=mq_2+r,q_i\in Z,m\geq 0,m\in Z\right\},m=3$$

Решение. Целые числа x,y находятся в данном отношении тогда и только тогда, когда они имеют одинаковые остатки при делении на модуль m. Отношение

-рефлексивно, т.к. два одинаковых числа имеют одинаковые остатки,

-симметрично,

-транзитивно, т.к. если x,y имеют одинаковые остатки, y,z имеют одинаковые остатки, то у чисел X,Z остатки одинаковые.

Поэтому данное отношение является отношением эквивалентности. Оно разбивает Z на классы эквивалентных элементов, называемых классами вычетов целых чисел по модулю $m=3$. Множество таких классов (здесь 3) называется фактор-множеством А по данному отношению:

$$[0]=\{...,-6,-3,0,3,6,...\},\ [1]=\{...,-5,-2,1,4,7,...\},[2]=\{...,-4,-12,5,8,...\}.$$

6. На множестве Z заданы отношения:

а) $xRy\Leftrightarrow x-y-$чётное; б) $xTy\Leftrightarrow x,y-$при делении на модуль $m=5$ имеют одинаковые остатки.

Выяснить, являются ли R и T отношениями эквивалентности и если являются, то найти разбиения на классы эквивалентных элементов, фактор-множества, индексы разбиения.

3.2.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили понятие отношения, классификацию отношений, свойства отношений;
- приобрели умения и навыки классифицировать отношения.

3.3 Практическое занятие №ПЗ-3 (2 часа).

Тема: «Функции. Виды функций»

3.3.1 Задание для работы:

1. Функции.
2. Классификация функций.

3.3.2 Краткое описание проводимого занятия:

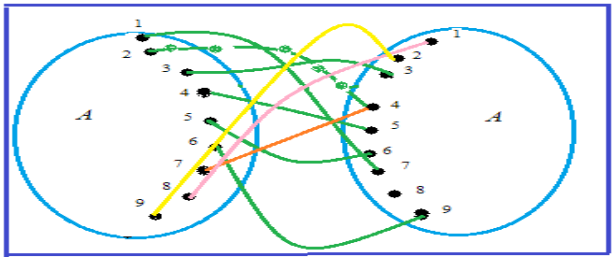
1. Даны пары <x,y>∈ρ, причем x∈{1,...,9}, y∈{1,...,9}

x	3	4	2	9	5	8	7	6	1
y	3	5	4	2	6	1	4	9	7

Является ли отношение ρ функцией? Инъективной функцией? Сюръективной функцией? Биективной функцией? Обосновать.

Решение. В первой задаче удобно изобразить графически данное отношение на

$A^2, A=\{1,2,3,4,5,6,7,8,9\}$:



Отношение ***является функцией*** на множестве А , т.к. каждый элемент множества А находится в отношении только с одним элементом (из каждой точки левого круга выходит только одна стрелка). Отношение ***не является сюръекцией***, т.к. элемент 8 не имеет прообраза и ***не является инъекцией***, т.к. два разных элемента (2, 7) имеют один и тот же образ 4; такая функция ***не является биекцией.***

3.3.3 Результаты и выводы: В результате проведенного занятия студенты:

- освоили понятия функции, свойства и классификацию функций;
- приобрели умения и навыки классификации функций, выявления свойств функций.

3.4 Практическое занятие №ПЗ-4 (2 часа).

Тема: «Эквивалентные множества. Мощность множеств»

3.4.1 Задание для работы:

1.Эквивалентные множества.

2. Понятие мощности множеств, сравнение мощностей.

3.4.2 Краткое описание проводимого занятия:

1.Эквивалентные множества.

2. Понятие мощности множеств, сравнение мощностей.

1. Даны пары $<x,y>\in\rho$, причем $x\in\{1,...,9\}$, $y\in\{1,...,9\}$

x	3	4	2	9	5	8	7	6	1
y	3	5	4	2	6	1	4	9	7

Является ли отношение ρ функцией? Инъективной функцией? Сюръективной функцией? Биективной функцией? Обосновать. Будут ли множества

Решение.

1**.** В первой задаче удобно изобразить графически данное отношение на

$A^2, A=\{1,2,3,4,5,6,7,8,9\}$:

Отношение ***является функцией*** на множестве А , т.к. каждый элемент множества А находится в отношении только с одним элементом (из каждой точки левого круга выходит только одна стрелка). Отношение ***не является сюръекцией***, т.к. элемент 8 не имеет прообраза и ***не является инъекцией***, т.к. два разных элемента (2, 7) имеют один и тот же образ 4; такая функция ***не является биекцией.***

3.4.3 Результаты и выводы: В результате проведенного занятия студенты:

- освоили понятия биекции и эквивалентных множеств;
- приобрели умения и навыки устанавливать эквивалентность числовых множеств.

3.5 Практическое занятие №ПЗ-5 (2 часа).

Тема: «Бинарные операции. Группы. Подстановки на множестве»

3.5.1 Задание для работы:

1. Бинарные операции. Полугруппы и группы.
2. Подстановки на множестве.

3.5.2 Краткое описание проводимого занятия:

1. Бинарные операции. Полугруппы и группы.

На множестве А определена **алгебраическая операция,** если каждым двум элементам этого множества, взятым в определенном порядке, однозначным образом поставлен в соответствие некоторый третий элемент из этого же множества.

Примерами алгебраических операций могут служить такие операции как сложение и вычитание целых чисел, сложение и вычитание векторов, матриц, умножение квадратных матриц, векторное умножение векторов и др.

Множество А с определенной на нем алгебраической операцией (например, умножением) называется **группой**, если выполнены следующие условия:

1) для любых трех элементов $a, b, c \in$ А выполняется свойство ассоциативности:

$$a(bc) = (ab)c$$

2) в множестве А существует такой элемент e, что для любого элемента a из этого множества выполняется равенство:

$$ae = ea = a$$

3) для любого элемента a множества существует элемент a' из этого же множества такой, что

$$aa' = a'a = e$$

Различные множества могут являться группой относительно какой- либо операции и не являться группой относительно другой операции.

Число элементов называется **порядком** группы.

2. Подстановки на множестве.

1. Заданы две подстановки σ и τ своими матрицами [σ] и [τ]. Найти их произведение.

Решение. В матрице [τ] столбцы переставляются так, чтобы ее первая строка совпала со второй строкой матрицы [σ]: $\begin{pmatrix} s_1 & s_2 & \dots & s_n \\ t_1 & t_2 & \dots & t_n \end{pmatrix}$. В итоге получится:

$$[\sigma]\cdot[\tau] = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}\begin{pmatrix} s_1 & s_2 & \dots & s_n \\ t_1 & t_2 & \dots & t_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix}.$$

2. Заданы подстановки $[\sigma] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $[\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. Наити их произведе-ние.

Решение. $[\sigma\cdot\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$.

3. Как называется *подстановка* $[e] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

Решение. *Тождественная подстановка*: такая подстановка e, что $e(x)=x\ \forall x$.

4. Дать понятие *Обратной подстановки.*

Решение. Произведение исходной и обратной подстановок равно тождественной.

5. Назвать правило нахождения *Обратной подстановки* – это обратная функция, которая всегда существует (подстановка является биекцией). Для получения таблицы обратной подстановки нужно поменять местами строки таблицы исходной подстановки.

$$\text{Для подстановки } [\sigma] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad [\sigma^{-1}] = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

6. Дать понятие о цикле.

Решение. Подстановка σ называется *циклом длины r*, если матрицу [σ] перестановкой столбцов можно привести к виду:

$\begin{pmatrix} s_1 & s_2 & s_3 & \dots & s_{r-1} & s_r & s_{r+1} & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_r & s_1 & s_{r+1} & \dots & s_n \end{pmatrix}$, т.е. первые r элементов сменяют друг друга, а остальные неподвижны: $\sigma(s_i) = s_{i+1}$, для $1 \le i \le r-1$ и $\sigma(s_r) = s_1$.

7.Привести пример подстановки являющейся циклом и не являющейся цик-лом.

Решение. Подстановка σ с матрицей $[\sigma] = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 3 & 6 & 1 & 4 \\ 5 & 3 & 6 & 2 & 1 & 4 \end{pmatrix}$ является циклом (2 5 3 6), а подстановка с матрицей $[\tau] = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}$ циклом не является, т.к. из нее можно выделить два цикла (1 4) и (2 5 6 3).

8. Показать, что множество подстановок элементов множества $\{1, 2, ..., n\}$ образуют мультипликативную группу.

3.5.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия бинарной операции, полугруппы, группы;
- приобрели умения и навыки использования свойств групп.

3.6 Практическое занятие №ПЗ-6 (2 часа).

Тема: «Кольца и поля. Кольцо классов вычетов целых чисел Z_n»

3.6.1 Задание для работы:

1. Кольца и поля.
2. Кольцо классов вычетов целых чисел.

3.6.2 Краткое описание проводимого занятия:

1. Кольца и поля.
2. Кольцо классов вычетов целых чисел

1.Указать все классы кольца 1) Z_8, 2), Z_9 3) Z_7, перечислить элементы классов.

2.Найти обратимые элементы колец в задаче 3.

3.Найти делители нуля колец в задаче 3.

4.Найти противоположные элементы в кольцах задачи 1.

5. Составить таблицу умножения в кольце Z_9.

Решение. Таблица умножения в кольце классов вычетов Z_9

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{5}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	8	4
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	6	3
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	4	2
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	2	1

1.а) Найти число не нулевых классов в кольце Z_m вычетов по модулю m. б) Найти число не нулевых классов в кольце вычетов Z_5. в) Число классов вычетов кольце вычетов Z_5 равно?

2. Пусть [0] – класс вычетов из кольца Z_7 . Тогда класс вычетов [0] - это множество

+а) {…, -14, - 7, 0, 7, 14, …}

б) {…, -13, - 6, 1, 8, 15, …}

в) {…, -12, - 5, 2, 9, 16, …}

г) {…, -11, - 4, 3, 10, 17, …}

д) {0, 1, …, 6}

3. Если [1] – класс вычетов из кольца Z_7 , то класс вычетов [1] - это множество

+а) {…, -13, - 6, 1, 8, 15, …}

б) {…, -14, - 7, 0, 7, 14, …}

в) {…, -12, - 5, 2, 9, 16, …}

г) {…, -11, - 4, 3, 10, 17, …}

д) {0, 1, …, 6}.

4.

	.	[3]	[4]	.
.	.	.	.	.
[2]	.	[5]	[6]	.
[3]	.	[6]	[?]	.
.	.	.	.	.

Рисунок - часть таблицы сложения в кольце Z_7 .Пропущенное число равно-...

ОТВЕТ:0

5.

	.	[3]	[4]	.
.	.	.	.	.
[2]	.	[6]	[1]	.
[3]	.	[2]	[?]	.
.	.	.	.	.

Здесь дана часть таблицы умножения в кольце Z_7 .Пропущенное число равно-...

ОТВЕТ:5

9. В формуле умножения [2]·[3] = [ ] классов вычетов в кольце Z_5 пропущенное число равно-...

ОТВЕТ:1

10. При умножении [3]·[3] = [ ] классов вычетов в кольце Z_5 пропущенное число равно-...

ОТВЕТ:4

3.6.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили понятия кольца и поля;
- приобрели умения и навыки использования свойств кольца и поля.

3.7 Практическое занятие №ПЗ-7 (2 часа).

Тема: «Булевы функции. Элементарные булевы функции. Переключательные функции**»**

3.7.1 Задание для работы:

1. Булевы функции.
2. Элементарные булевы функции. Переключательные функции

3.7.2 Краткое описание проводимого занятия:

Булевы функции, булевы константы. **Булевыми функциями (или функциями алгебры логики или истинностными функциями) называются функции, значения которых равны 0 или 1 и аргументы которых принимают только два значения 0 и 1.** Булевы функции могут быть заданы специальными таблицами истинности или аналитически в виде специальных высказывательных форм, называемых иногда булевыми формами. Выражения, содержащие одну или несколько переменных (аргументов), соединенных знаками логических операций, называются *логическим формами*. Высказывания, не содержащие ни одной переменной, называются константами. В логике, в отличие от арифметики, только две константы 0 - false и 1- true.

Напомним, что *форма называется числовой,* если при допустимом значении своих аргументов, она обозначает число (является числом). Булева форма является частным случаем числовой формы. Т.о. при помощи суперпозиции, исходя из логических операций над логическими переменными, можно строить сложные составные высказывания и затем вычислять их. Такого рода составные высказывания являются частным случаем так называемых булевых функций, которые являются предметом изучения математической логики. Обобщая все сказанное, можно дать определение булевых функций:

Булевыми функциями, называются предикаты, все аргументы которых определены на множестве {0, 1}, интерпретируемые как {ложь, истина}.

Можно сказать, что понятие булевой функции является частным случаем понятия предиката. Отличие состоит лишь в том, что у булевой функции четко фиксирована как область определения {0, 1}, так и область значений функции {0, 1}, в то время как у предиката четко фиксирована только одна область значений {0, 1}, в то время как область определения задана произвольным множеством.

В свою очередь понятие предиката является частным случаем понятия функции, отличие состоит в том, что у предиката четко фиксирована область значений {0, 1}, а у функции это может быть вся числовая ось.

3.7.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия булевых функций;
- приобрели умения и навыки использования булевых функций.

3.8 Практическое занятие №ПЗ-8 (2 часа).

Тема: «Представление булевых функций формулами. Понятие о булевой алгебре**»**

3.8.1 Задание для работы:

1. Представление булевых функций формулами.
2.Понятие о булевой алгебре

3.8.2 Краткое описание проводимого занятия:

Представление булевых функций формулами.

Булевы функции и формулы. *ФАЛ называются также* булевыми *функциями,* двоичными *функциями или* переключательными *функциями. Аргументы булевой функции являются булевыми переменными. Булеву функцию можно задать таблицей истинности.*

Утверждение Для булевой функции от n аргументов существует 2^n различных наборов аргументов.

Булева функция $f(x_1, x_2, \ldots, x_n)$ называется *полностью определенной*, если ее значения определены на всех 2^n наборах переменных. В противном случае функция *частично определенная*.

Функция $f(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n)$ *существенно зависит от переменной* x_i, (или переменная x_i – *существенная*), если ∃ такой набор значений $x_1, x_2, \ldots, x_n$ $(\sigma_1,\ldots,\sigma_{i-1},\sigma_i,\sigma_{i+1},\ldots,\sigma_n)$, что

$f(\sigma_1,\ldots,\sigma_{i-1},0,\sigma_{i+1},\ldots,\sigma_n) \neq f(\sigma_1,\ldots,\sigma_{i-1},1,\sigma_{i+1},\ldots,\sigma_n)$. В противном случае переменная x_i – *несущественная (фиктивная)*.

x_1	x_2	f_1	f_2
0	0	0	1
0	1	0	1
1	0	1	0
1	1	1	0

Пусть две булевы функции заданы таблицей истинности. Для них переменная x_1 существенная, а x_2 – несущественна. По определению булевы функции равны, если одна из другой получается введением или удалением несущественных переменных.

Одна и та же функция может иметь множество реализаций формулами над данным базисом (т.е. множеством логических операций). Формулы, реализующие одну и ту же функцию, называются *равносильными* (т.е. на всех наборах переменных их значение истинности совпадает). Отношение равносильности формул является отношением эквивалентности.

Формулы алгебры логики, при образовании которых используются только операции отрицания, конъюнкции и дизъюнкции, называются *булевыми формулами*.

Для любой формулы алгебры логики существует равносильная ей булева формула.

Способы представления булевых функций. Нормальные формы

Табличный способ определения истинности сложного выражения имеет ограниченное применение, т.к. с увеличением числа логических переменных число вариантов становится слишком большим. Тогда может быть использован способ приведения формул к *нормальной форме*.

Аналитическое выражение функции (или формула) находится в *нормальной форме*, если в ней отсутствуют знаки эквивалентности, импликации, двойного отрицания, а знаки отрицания находятся только при переменных.

Элементарной дизъюнкцией (*произведением*) называется дизъюнкция (произведение) переменных или их отрицаний, в котором каждая переменная встречается только один раз.

ДНФ – это дизъюнкция элементарных произведений. *КНФ* – это произведение элементарных дизъюнкций. Как ДНФ, так и КНФ функции не единственна. Обычно предполагают, что входящие в ДНФ (КНФ) элементарные конъюнкции (дизъюнкции) попарно различны.

ДНФ (КНФ) называется *совершенной*, если каждая переменная формулы входит в каждую элементарную конъюнкцию (дизъюнкцию) ровно один раз.
СДНФ (СКНФ) функции единственна.

Элементарные дизъюнкции: $x \vee \bar{y}$, z. Элемент. конъюнкции: $x \cdot \bar{y} \cdot z$, x.
$f(x,y,z) = xyz \vee \bar{x}y$ – ДНФ ; $f(x,y,z) = (x \vee \bar{y}) \cdot z$ – КНФ.

Введем обозначения: $x^{\alpha} = \begin{cases} x, & \alpha = 1 \\ \bar{x}, & \alpha = 0 \end{cases}$

О разложении булевой функции по k переменным (знак $\cup \equiv \vee$**).**

$$f(x_1,\dots,x_n)=\underset{\alpha_1,\dots,\alpha_k}{V} x_1^{\alpha_1}x_2^{\alpha_2}\dots x_k^{\alpha_k}\cdot f(\alpha_1,\alpha_2,\dots,\alpha_k,x_{k+1},\dots,x_n)$$

n=3, k=2.

Доказательство:

Выберем какой-либо набор значений для переменных $x_1, \dots, x_n$. Пусть это будет $\sigma_1, \dots, \sigma_n$..

Заметим, что $\sigma_i^{\alpha_i}=\begin{cases}1, & \sigma_i=\alpha_i\\ 0, & \sigma_i\neq\alpha_i\end{cases}$ ($1^1=1$, $0^0=1$, $1^0=\neg 1=0$, $0^1=0$)

Подставим в правую часть формулировки теоремы вместо $x_1, \dots, x_n$ набор $\sigma_1, \dots, \sigma_n$. Получим $\underset{(\alpha_1,\dots,\alpha_k)}{V}\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\dots\sigma_k^{\alpha_k}\cdot f(\alpha_1,\alpha_2,\dots,\alpha_k,\sigma_{k+1},\dots,\sigma_n)$. Поскольку коэффициент перед функцией равен 1 только при равных значениях σ_i и α_i, в разложении останется только один член: $\sigma_1^{\alpha_1}\dots\sigma_k^{\alpha_k}\cdot f(\alpha_1,\dots,\alpha_k,\sigma_{k+1},\dots,\sigma_n)$, и $\sigma_i=\alpha_i$, т.е. $f(\sigma_1,\dots,\sigma_k,\sigma_{k+1},\dots,\sigma_n)$. Получена левая часть формулы теоремы 4.6. Поскольку набор был выбран произвольно, получаем, что утверждение верно ∀ набора $x_1, \dots, x_n$. ■

Следствие 1: **Разложение Шеннона**

$$f(x_1,x_2,\dots,x_n)=\overline{x_1}\cdot f(0,x_2,\dots,x_n)\vee x_1\cdot f(1,x_2,\dots,x_n)$$

Следствие 2: При k=n получаем: $f(x_1,\dots,x_n)=\underset{f=1}{V}x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$, т.е. выбираем те слагаемые, на которых функция равна 1. Полученная формула представляет собой *СДНФ*.

Построение совершенных нормальных форм

Построение СДНФ

1. Построение по ТИ.

Найти строки в ТИ, где $f = 1$.

3) ∀ найденному набору $\sigma_1, \dots, \sigma_n$. поставить в соответствие произведение $\tilde{x}_1\cdot\tilde{x}_2\cdot\dots\cdot\tilde{x}_n$, где $\tilde{x}_i=\begin{cases}x_i, & \text{если } \sigma_i=1\\ \overline{x_i}, & \text{если } \sigma_i=0\end{cases}$

4) Составить дизъюнкцию из произведений п.2.

2. Получение из ДНФ.

Если некоторое произведение ДНФ не содержит какой-либо переменной, то необходимо помножить это произведение на дизъюнкцию этой переменной и ее отрицания и применить дистрибутивный закон.

Построение СКНФ

1. Построение по ТИ.

Найти строки в ТИ, где $f = 0$.

3) ∀ найденному набору $\sigma_1, \dots, \sigma_n$. поставить в соответствие дизъюнкцию $\tilde{x}_1\vee\tilde{x}_2\vee\dots\vee\tilde{x}_n$, где $\tilde{x}_i=\begin{cases}x_i, & \text{если } \sigma_i=0\\ \overline{x_i}, & \text{если } \sigma_i=1\end{cases}$

4) Составить произведение дизъюнкций из п.2.

2. Получение из КНФ.

Если некоторая элементарная дизъюнкция КНФ не содержит какой-либо переменной, то необходимо дизъюнктивно добавить в нее произведение этой переменной и ее отрицания и применить дистрибутивный закон.

3.8.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили представление булевых функций формулами, понятие о булевой алгебре;
- приобрели умения и навыки использования представления булевых функций формулами.

3.9 Практическое занятие №ПЗ-9 (2 часа).
Тема: «Правила комбинаторики. Комбинаторные формулы»

3.9.1 Задание для работы:
1. Правила комбинаторики.
2. Комбинаторные формулы.

3.9.2 Краткое описание проводимого занятия:

1. Правила комбинаторики.

1. Оценить применимость алгоритма.

Агенство недвижимости, база данных. Запись – пара (предложение, спрос). Найти варианты обмена (т.е. такие пары, где первая компонента одной совпадает со второй компонентой другой). Оценить простейший вариант поиска – «лобовой».

Решение. Трудоемкость $n\times(n-1)/2$. Если на одну проверку нужна 1 миллисекунда, то при n = 100 потребуется около 5 секунд, при n=100 000 – 5×10^6 сек, т.е. около 1389 часов. Алгоритм непригодный.

2. Пусть в киоске имеется 5 различных книг по математике и 7 по физике. Если студент может купить только одну книгу, то сколько у него есть вариантов?

Решение. 5 вариантов выбора первой книги и 7 вариантов – второй, т.е. 12 вариантов.

3. Пусть в салоне связи имеется 50 различных моделей сотовых телефонов и по три вида чехлов для каждой модели. Сколькими способами можно выбрать телефон и чехол к нему?

Решение. Очевидно: имеется 50 вариантов выбора телефона. Выбрав телефон, можно 3 способами выбрать чехол, т.е. всего $50\times3=150$ вариантов.

2. Комбинаторные формулы.

4.На тренировках занимаются 8 баскетболистов. Сколько разных пятерок может быть образовано тренером?

Решение. Т.к. при образовании пятерки важен только ее состав, то достаточно определить $C_8^5 = \frac{8!}{5!(8-5)!} = \frac{8!}{5!3!} = \frac{6\cdot7\cdot8}{1\cdot2\cdot3} = 56$ пятерок.

5. Сколько различных трехзначных чисел можно составить из цифр 1, 2, 3, 4, 5? при условии, что ни одна цифра не повторяется?

Решение. Составить разные числа можно: $\overline{A}_5^3 = 5^3 = 125$ способами (разме-щения с повторениями). Если ни одна цифра не должна повторяться, то таких способов будет $A_5^3 = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 5\cdot4\cdot3 = 60$ (размещения без повторений).

3.9.3 Результаты и выводы: В результате проведенного занятия студенты:
- освоили основные комбинаторные принципы и формулы;
- приобрели умения и навыки решать простейшие комбинаторные задачи.

3.10 Практическое занятие № ПЗ-10 (2 часа).

Тема: «Биномиальные коэффициенты и их свойства. Метод включений и исключений. Метод рекуррентных соотношений. Производящие функции»

3.10.1 Задание для работы:

1. Биномиальные коэффициенты и их свойства.
2. Метод включений и исключений. Метод рекуррентных соотношений.

3.10.2 Краткое описание проводимого занятия:

1. Биномиальные коэффициенты и их свойства.

1. Доказать: $C_n^m = C_n^{n-m}$.

Решение. $C_n^m \equiv \frac{n!}{(n-m)!m!} = \frac{n!}{(n-m)!(n-n+m)!} = \frac{n!}{(n-m)!(n-(n-m))!} \equiv C_n^{n-m}$.

2. Доказать: $C_n^m + C_n^{m+1} = C_{n+1}^{m+1}$.

Решение. $C_n^m + C_n^{m+1} = \frac{n!}{(n-m)!m!} + \frac{n!}{(n-(m+1))!(m+1)!} = \frac{n!}{(n-(m+1))!(n-m)m!} + \frac{n!}{(n-(m+1))!m!(m+1)} = \frac{n!(m+1)+n!(n-m)}{(n-(m+1))!(n-m)m!(m+1)} = \frac{n!(m+1+n-m)}{(n-m)!(m+1)!} = = \frac{n!(n+1)}{(n-m)!(m+1)!} = \frac{(n+1)!}{(n+1-(m+1))!(m+1)!} = C_{n+1}^{m+1}$.

3. Доказать: $\boldsymbol{2^n = \sum_{m=0}^{n} C_n^m}$.

Решение. $2^n = (1+1)^n = \sum_{m=0}^{n} C_n^m 1^m 1^{n-m} = \sum_{m=0}^{n} C_n^m$.

4. $\sum_{m=0}^{n} (-1)^m C_n^m = 0$.

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

5. Сколько разных слов можно образовать при перестановке букв слова «математика»?

Решение. Здесь типы объектов – это различные буквы (число типов k=6), количество неразличимых объектов каждого из типов – это число повторений конкретной буквы. Если бы все буквы были различны, то таких слов = 10!. Количество перестановок, в которых меняются местами только k одинаковых букв, равно k! Очевидно, что такие перестановки не меняют полученного слова $\Rightarrow$ при подсчете нужно разделить 10! на k!, и выполнить это для всех повторяющихся элементов. В слове «математика» буква «м» встречается 2 раза, «а» – 3 раза, «т» – 2 раза, «е» – 1 раз, «и» – 1 раз, «к» – 1 раз. Поэтому число различных слов равно $P(10;2,3,2,1,1,1) = \frac{10!}{2!3!2!1!1!1!} = 151200$.

6. Сколько положительных трехзначных чисел делятся ровно на одно из чисел 3, 5 или 7?

Решение. Обозначим P_3 – свойство делимости на 3, P_5 – на 5, P_7 – на 7. Всего трехзначных чисел 9·10·10=900. Тогда $N_3 = \left[\frac{999}{3}\right] - \left[\frac{99}{3}\right] = 300,$

$$N_5 = \left[\frac{999}{5}\right] - \left[\frac{99}{5}\right] = 180, \quad N_7 = \left[\frac{999}{7}\right] - \left[\frac{99}{7}\right] = 128.$$

Так как $N_{3,5}$ – число чисел, делящихся одновременно на 3 и 5, а наименьшее общее кратное 3 и 5 равно 15, то $N_{3,5} = \left[\frac{999}{15}\right] - \left[\frac{99}{15}\right] = 60$. Аналогично,

$$N_{3,7} = \left[\frac{999}{21}\right] - \left[\frac{99}{21}\right] = 43, \quad N_{5,7} = \left[\frac{999}{35}\right] - \left[\frac{99}{35}\right] = 26, \quad N_{3,5,7} = \left[\frac{999}{105}\right] - \left[\frac{99}{105}\right] = 9.$$

Находим искомое число:

$$N(1) = \sum_{k=0}^{3-1} (-1)^k C_{1+k}^1 S_{1+k} = (-1)^0 C_1^1 S_1 + (-1)^1 C_2^1 S_2 + (-1)^2 C_3^1 S_3 = \left(N_3 + N_5 + N_7\right) -$$

$$- 2\left(N_{3,5} + N_{3,7} + N_{5,7}\right) + 3N_{3,5,7} = (300 + 180 + 128) - 2\left(60 + 43 + 26\right) + 3 \cdot 9 = 608 - 258 + 27 = 377.$$

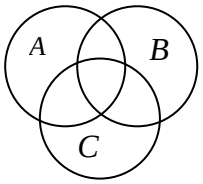
Принцип включения и исключения. Рассмотренные ранее формулы и алгоритмы дают способы вычисления комбинаторных чисел для некоторых распространенных комбинаторных конфигураций. Практические задачи не всегда прямо сводятся к известным комбинаторным конфигурациям. В этом случае используются различные методы сведения одних комбинаторных конфигураций к другим. Рассмотрим некоторые наиболее часто используемые методы. Часто комбинаторная конфигурация является объединением других, число комбинаций в которых вычислить проще. В таком случае требуется уметь вычислять число комбинаций в объединении. В простых случаях формулы для вычисления очевидны:

Теорема (комбинаторный принцип сложения): пусть множества A и B *могут пересекаться. Тогда количество элементов, которые можно выбрать из A или B, определяется по формуле:*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Очевидно, что рассмотренная теорема будет справедлива для произвольных множеств. Если перейти от двух множеств к большему количеству, в частности, к трем, и проиллюстрировать с помощью диаграмм Венна, то очевидным результатом явится следующая формула:

$|\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}| = |\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}| - |\boldsymbol{A} \cap \boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{C}| - |\boldsymbol{B} \cap \boldsymbol{C}| + |\boldsymbol{A} \cap \boldsymbol{B} \cap \boldsymbol{C}|$, т.е. для вычисления количества элементов объединения трех множеств нужно просуммировать мощности всех этих множеств, вычесть мощности всех попарных пересечений и добавить число элементов, содержащихся в пересечении всех трех множеств.



Более общая формула, известная как принцип включения и исключения, позволяет вычислить мощность объединения произвольного количества множеств, если известны их мощности и мощности всех пересечений.

3.10.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили основные свойства биномиальных коэффициентов;
- приобрели умения и навыки применять свойства биномиальных коэффициентов при решении комбинаторных задач.
- освоили понятия о методе включений и исключений, методе рекуррентных соотношений;
- приобрели умения и навыки применять метод включений и исключений, метод рекуррентных соотношений при решении комбинаторных задач.

3.11 Практическое занятие №ПЗ-11 (2 часа).

Тема: «Основы теории делимости в Z. Простые числа»

3.11.1 Задание для работы:

1. Основы теории делимости
2. Простые числа.

3.11.1 Задание для работы:

1. Основы теории делимости
2. Простые числа.

3.12 Практическое занятие №ПЗ-12 (2 часа).

Тема: «Математические основы криптографии: приложения модульной арифметики в алгоритме RSA**»**

3.12.1 Задание для работы:

Математические основы криптографии: приложения модульной арифметики в алгоритме RSA

3.11-12.2 Краткое описание проводимых занятий ПЗ 11, 12:

1. Сравнения.

1. Решить с помощью индексов сравнение первой степени**:** $3x \equiv 8(\mathrm{mod}\,23)$ (1)

Решение. Индексируем обе части сравнения $ind\,3 + indx \equiv ind\,8(\mathrm{mod}\,22)$.

Находим по таблице индексов $ind\,3 = 16$, $ind\,8 = 6$ и подставляем в (1):

$$16 + indx \equiv 6(\mathrm{mod}\,22).$$

$$indx \equiv -10(\mathrm{mod}\,22).$$

Так как $-10 \equiv 12(\mathrm{mod}\,22)$, то

$$indx \equiv 12(\mathrm{mod}\,22).$$

По таблице для нахождения чисел по индексам находим $x \equiv 18(\mathrm{mod}\,23)$.

Решение.

Таблица умножения в кольце классов вычетов Z_9

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{5}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	8	4
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	6	3
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	4	2
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	2	1

2.Вычеты, модульная арифметика. приложения в криптографии: алгоритм RSA.

1. ***Выбирают два различных простых числа*** p и q, вычисляют их произведение $n = p \cdot q$.

p и q хранятся в тайне.	n - часть открытого ключа, доступ к нему открыт.

$p := 149$ $\quad$ $q := 157$

$n := p \cdot q$ $\quad$ $n \to 23393$

2.Численное представление сообщения.

А	*Б*	*В*	*Г*	*Д*	*Е*	*Ж*	*З*	*И*	*Й*	*К*
10	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*

Л	*М*	*Н*	*О*	*П*	*Р*	*С*	*Т*	*У*	*Ф*	*Х*
21	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*

Ц	*Ч*	*Ш*	*Щ*	*Ъ*	*Ы*	*Ь*	*Э*	*Ю*	*Я*
32	*33*	*34*	*35*	*36*	*37*	*38*	*39*	*40*	*41*

: « … » $\Leftrightarrow$ « 231528991415231513»

3.Запись численного сообщения в виде последовательности блоков (каждый блок меньше n):

2315 – 2899 – 1415 – 231 - 513

b1 - b2 - b3 - b4 - b5

4. Открытый кодирующий ключ криптосистемы RSA.

а) Находим $\varphi(n) = (p-1)\cdot(q-1);\ \varphi(n) = 148 \cdot 156,\ \varphi(n) \to 23088$

б) выбираем натуральное число e ***такое, что*** $НОД\left(e, \varphi(n)\right) = 1.$

Наименьшее простое e***, взаимно простое с*** $\varphi(n) \to 23088$***, это число*** $e = 5.$

Проверка:

$\gcd(23088, 2) \to 2$ $\quad$ $\gcd(23088, 3) \to 3$

$\gcd(23088, 4) \to 4$ $\quad$ $\gcd(23088, 5) \to 1$

в) Пара чисел $(n, e) = (23393, 5)$ ***называется открытым кодирующим ключом криптосистемы RSA.***

5. Шифрование численного сообщения:

а) Пусть b_i ***- блоки численного сообщения,*** $0 \le b_i \le n-1.$

б) Через $a_i = E(b_i)$ ***обозначается блок зашифрованного сообщения, соответствующий*** $b_i.$

Он вычисляется по следующей формуле:

$E(b_i)$ = ***Вычет*** b_i^e ***по модулю*** $n \Rightarrow E(b_i) = \mathrm{mod}(b_i^e, n).$

Зашифрованное сообщение будет расположено в виде блоков

$$E(b_1)-E(b_2)-E(b_3)-E(b_4)-E(b_5)\cdot$$

в) Вычисление зашифрованных блоков

$$b_1=2315 \lhd\rhd E(b_1)=\mathrm{mod}(b_1^{\,e},n)=\mathrm{mod}(2315^5,23393)\to 22247$$

$$b_2=2899 \lhd\rhd E(b_2)=\mathrm{mod}(b_2^{\,e},n)=\mathrm{mod}(2899^5,23393)\to 19729$$

$$b_3=1415 \lhd\rhd E(b_2)=\mathrm{mod}(b_2^{\,e},n)=\mathrm{mod}(1415^5,23393)\to 16674$$

$$b_4=231 \lhd\rhd E(b_4)=\mathrm{mod}(b_4^{\,e},n)=\mathrm{mod}(231^5,23393)\to 13212$$

$$b_5=513 \lhd\rhd E(b_5)=\mathrm{mod}(b_5^{\,e},n)=\mathrm{mod}(513^5,23393)\to 1135\cdot$$

г) Зашифрованное сообщение

$$22247-19729-16674-13212-1135.$$
$$a_1---a_2---a_3---a_4---a_5$$

6. Дешифровка сообщения.

а) Нахождение вычета (класса вычетов) d ***, обратного к*** e ***по модулю*** $m=\varphi(n)$***:***

$$[d]\cdot[e]=[1](\mathrm{mod}\,m),\ \textit{где}\ m=\varphi(n),\ \textit{т.е.}$$

$$[d]=[e]^{-1}\ \textit{по}\ \mathrm{mod}\,m.$$

По определению произведения классов по $\mathrm{mod}\,m$

$$[d]\cdot[e]=\{d\cdot e+k\cdot\varphi(n)\},k\in Z\cdot \qquad (1)$$

Так как

$$[d]\cdot[e]=[1](\mathrm{mod}\,m), \qquad (2)$$

а по определению класса $[1]$

$$[1]=\{1+k\cdot\varphi(n)\}, \qquad (3)$$

то

$$[d]\cdot[e]=\left[1+k\cdot\varphi(n)\right],\Rightarrow$$

$$d\cdot e=1+k\cdot\varphi(n),k\in Z \qquad (4)$$

В пункте 4 выбрали $e=5,\ \varphi(n)\to 23088$***. Тогда формула (4) примет вид***

$$d\cdot 5=1+k\cdot 23088,k\in Z \quad (d\cdot 5+(-k)\cdot 23088=1,k\in Z)$$

Преобразуем её к виду

$$d=\frac{1+k\cdot 23088}{5},k\in Z$$

Следовательно, необходимо выбрать целое k ***так, чтобы*** d ***было натуральным. Например,***

$$k=0\_Given\_d\cdot 5=1+k\cdot 23088\_Find(d)\to\frac{1}{5},$$

$$k=1\_Given\_d\cdot 5=1+k\cdot 23088\_Find(d)\to\frac{23089}{5}$$

$$k = 2\_Given\_d \cdot 5 = 1 + k \cdot 23088\_Find(d) \rightarrow \frac{46177}{5}$$

$$k = 3\_Given\_d \cdot 5 = 1 + k \cdot 23088\_Find(d) \rightarrow 13853 \Rightarrow d = 13853$$

б) Пара чисел (n,d) ***называется Секретным дешифрующим (декодирующим) ключом системы RSA***

$$D_C = (n,d) = (23393,13853)\cdot$$

в) Дешифрование: если a_i ***- блок шифрованного сообщения, то его расшифровка находится по формуле***

$$D(a_i) = \mathrm{mod}(a_i^{\,d}, n) \equiv вычет(a_i^{\,d})\ по\ модулю\ n,$$

т.е.

$$D(a_i) \equiv остаток\ от\ деления\ a_i^{\,d}\ на\ модуль\ n\cdot$$

$$D(a_1) = \mathrm{mod}(a_1^{\,d}, n) = \mathrm{mod}(22247^{13853}, 23393) \rightarrow 2315 = b_1$$
$$D(a_2) = \mathrm{mod}(a_2^{\,d}, n) = \mathrm{mod}(19729^{13853}, 23393) \rightarrow 2899 = b_2$$

3.11-12.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия сравнений и вычетов и их свойства, применения модульной арифметики в криптографии (алгоритм RSA);
- приобрели умения и навыки решать основные задачи модульной арифметики и оперировать основными элементами асимметричного алгоритма шифрования RSA.

3.13 Практическое занятие №ПЗ-13 (2 часа).

Тема: «Определение графов, основные понятия теории графов. Виды графов. Способы задания графов. Матрицы смежности и инцидентности графа. Матрица Кирхгофа. Числовые характеристики графов»

3.13.1 Задание для работы:

1. Основные понятия теории графов. Виды графов.
2. Операции над графами
3. Матрицы смежности и инцидентности графа. Матрица Кирхгофа.
4. Числовые характеристики графов

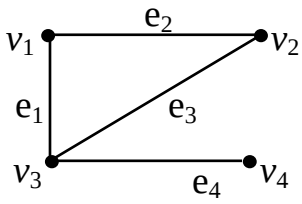
3.13.2 Краткое описание проводимого занятия ПЗ-13:

1. Основные понятия теории графов.
2. Виды графов.
3. Операции над графами.
3. Матрицы смежности и инцидентности графа. Матрица Кирхгофа.
4. Числовые характеристики графов

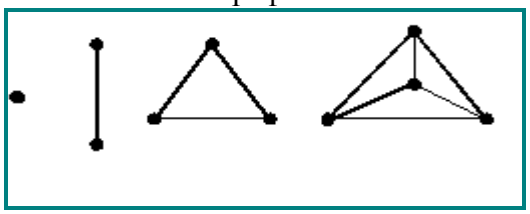
1. Указать смежные вершины, рёбра, инцидентные вершины и рёбра.

Решение. Вершины v_1 и v_2 являются смежными, вершина v_1 инцидентна ребраме$_2$= (v_1,v_2)иe_1= (v_1,v_3).$V = \{v_1, v_2, v_3, v_4\}$, = {$e_1$, e_2, e_3, e_4}. Ребра e_1, e_2, e_3 являются по-

парно смежными, а ребра e_2, e_4 – несмежными, так же как и вершины v_1, v_4 и v_2, v_4.



2. Являются ли графы полными? Указать их порядки.



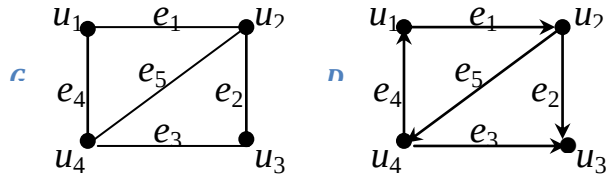
Решение. На рисунке изображены полные графы порядка 1, 2, 3 и 4. Они обозначаются K_n.

Тема(продолжение): «Способы задания графов. Матричное представление графов. Числовые характеристики графов»

1. Способы задания графов. Матричное представление графов.
2. Числовые характеристики графов

1. Способы задания графов. Матричное представление графов.

1. Составить матрицы смежности графов.

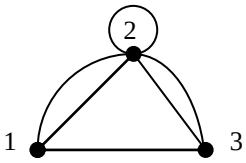


Решение. Матрицы смежности для заданных графа G и орграфа D

$$A(G)=\begin{pmatrix}0&1&0&1\\1&0&1&1\\0&1&0&1\\1&1&1&0\end{pmatrix}\quad A(D)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\0&0&0&0\\1&0&1&0\end{pmatrix}$$

2. Найти матрицу смежности псевдографа.

$$A(P)=\begin{pmatrix}0&2&1\\2&2&2\\1&2&0\end{pmatrix}$$

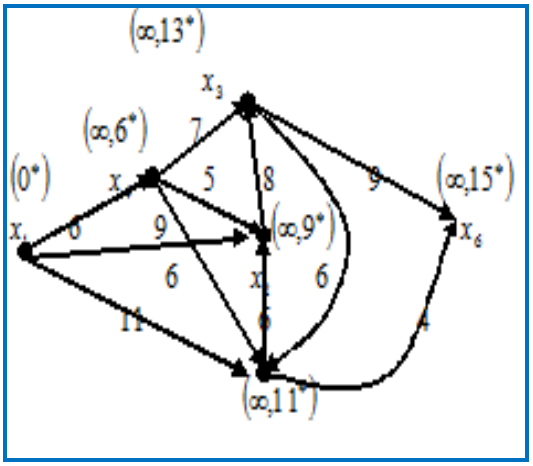


3. Найти матрицы инцидентности для заданных графа G и орграфа D

$$I(G)=\begin{pmatrix}1&0&0&1&0\\1&1&0&0&1\\0&1&1&0&0\\0&0&1&1&1\end{pmatrix}\quad I(D)=\begin{pmatrix}-1&0&0&1&0\\1&-1&0&0&-1\\0&1&1&0&0\\0&0&-1&-1&1\end{pmatrix}$$

4. Задана весовая матрица сети P. Построить по этой матрице сеть,
Изобразим теперь сам граф по данной матрице весов.

$$P = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{array} \begin{array}{c} \begin{array}{cccccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{array} \\ \begin{pmatrix} - & 9 & \infty & 6 & 11 & \infty \\ \infty & - & 8 & \infty & \infty & \infty \\ \infty & \infty & - & \infty & 6 & 9 \\ \infty & 5 & 7 & - & 6 & \infty \\ \infty & 6 & \infty & \infty & - & 4 \\ \infty & \infty & \infty & \infty & \infty & - \end{pmatrix} \end{array}.$$

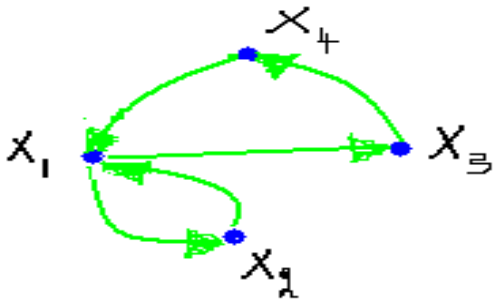


2. Числовые характеристики графов

1. Орграф G задан списком пар начальных и конечных вершин ориентированных рёбер: (x_1, x_2), (x_1, x_3), (x_2, x_1), (x_3, x_4), (x_4, x_1). Для графа G степень входа вершины in deg (x_4) равна-...

ОТВЕТ:1

2.



Степень выхода вершины x_1 равна-...

ОТВЕТ:2

3. В простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), d(G) равно-...

ОТВЕТ:2

3.13.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили основные понятия теории графов, способы задания графов, матричное представление графов;
- приобрели умения и навыки применять основные понятия теории графов, способы задания графов, матричное представление графов при решении задач.

3.14 Практическое занятие № ПЗ-14 (2 часа).

Тема: «Свойства графов: маршруты, циклы, связность. Свойства регулярных, двудольных и связных графов. Метрические характеристики связных графов**»**

3.14.1 Задание для работы:

1. Маршруты, циклы,
2. Связность
3. Понятие о метрических характеристиках графа.
4. Вычисление метрических характеристик графа.

3.14.2 Краткое описание проводимого занятия ПЗ-14:

1. Маршруты, циклы,
2. Связность

3. Понятие о метрических характеристиках графа.
4. Вычисление метрических характеристик графа.

Маршруты, цепи, циклы. Маршрутом *от вершины* u *к вершине* v *или (*u,v*)*-маршрутом *в графе* G *называется всякая последовательность вида* $u = v_0, e_1, v_1, e_2, \ldots, e_n, v_n = v$*, в которой любые два соседних элемента инцидентны, т.е.* e_k *– ребро, соединяющее вершины* v_{k-1} *и* v_k, k = *1,2,…,*n.

Это определение подходит также для псевдо-, мульти- и орграфов. В случае орграфа v_{k-1} *– начало* ребра e_k , а v_k – его *конец*. При этом вершину *u* называют *началом маршрута*, а вершину *v* – его *концом*. В маршруте некоторые вершины и ребра могут совпадать. Если *u* = *v*, то маршрут *замкнут*, а иначе *открыт*. Для «обычного» графа маршрут можно задавать только последовательностью вершин $v_0, v_1, \ldots, v_n$ или ребер $e_1, e_2, \ldots, e_n$.

Маршрут называется *цепью*, если в нем нет совпадающих ребер, и *простой цепью* – если дополнительно нет совпадающих вершин, кроме, может быть, начала и конца цепи. Про цепь $u = v_0, v_1, \ldots, v_n = v$ говорят, что она *соединяет* вершины *u* и *v* и обозначают $\langle u,v \rangle$.

Очевидно, что если есть цепь, соединяющая вершины *u* и *v*, то есть и простая цепь, соединяющая эти вершины.

Замкнутая цепь называется *циклом*; замкнутая простая цепь – *простым циклом*. Число циклов в графе *G* обозначается *z(G)*. Граф без циклов называется *ациклическим*. Для орграфов цепь называется *путем*, а цикл – *контуром*.

Число ребер в маршруте M (возможно, с повторениями) называется его *длиной*, обозначается |M|.

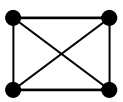
Расстоянием между вершинами u и *v* (обозначается *d*(*u*,*v*)) называется длина кратчайшей цепи $\langle u,v \rangle$, а сама кратчайшая цепь называется *геодезической*. Если не существует цепи, соединяющей вершины *u* и *v*, то по определению *d*(*u*,*v*) = +∞.

Диаметром графа *G* (обозначается *D(G)*) называется длина длиннейшей геодезической.

Максимальным удалением в графе *G от вершины v* называется *r(v) = max d(v,v'),* $\forall\, v' \in V$. Вершина *v* графа *G* является его *центром*, если максимальное удаление от нее до всех вершин принимает наименьшее значение.

Множество вершин, находящихся на одинаковом расстоянии *n* от вершины *v*, называется *ярусом* (обозначается *D(v,n)*): $D(v,n) = \{u \in V \mid d(v,u) = n\}$.

Граф, любая из вершин которого является его центром – максимальное удаление до всех вершин от любой =



Связность. *Если две вершины u и v в графе можно соединить цепью, то такие вершины связаны. Граф называется связным, если в нем связаны все вершины.*

Легко видеть, что отношение связности на множестве вершин является отношением эквивалентности. Данное отношение разбивает множество вершин графа на классы, объединяющие вершины, связанные друг с другом. Такие классы называются *компонентами связности*; число компонент связности обозначается *k(G)*.

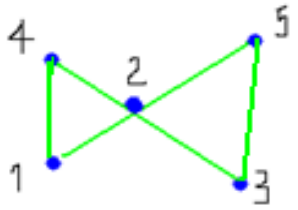
Граф *G* является связным тогда и только тогда, когда он имеет одну компоненту связности: *k(G)* = 1. Если *k(G)* > 1, то это *несвязный* граф. Граф, состоящий только из изолированных вершин (в котором k(G)=|V|, r(G)=0), называется *вполне несвязным*.

Вершина графа, удаление которой увеличивает число компонент связности, называется *разделяющей* или *точкой сочленения*.

Ориентированный граф *G(V,E)* является *слабо связным* (*слабым*), если симметричное замыкание множества *E* определяет связный граф (иными словами, если после замены всех дуг графа *G* ребрами полученный граф будет связным). Ориентированный граф является *сильно связным* (*сильным*), если для любой пары вершин $u,v \in V$ существует ориентированный путь из *u* в *v* (т.е. из любой вершины графа достижимы все его остальные вершины). Если для любой пары вершин по крайней мере одна достижима из другой, то такой граф является *односторонне связным*, или *односторонним*. Граф, состоящий из одной вершины, по определению считается сильно связным.

Множества вершин связных компонент образуют разбиение множества вершин графа.

1.



В графе, представленном на рисунке, e(1) равно-...

ОТВЕТ:2

2.В простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), e(2) равно-...

ОТВЕТ:1

3.В простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), d(G) равно-...

ОТВЕТ:2

4.В простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), r(G) равно-...

ОТВЕТ:1

5.В простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), центром является:

+а) 2

б) 1

в) 3,4

г) 2,3

д) 5

6.В простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), диаметральной цепью является:

+а) 1-2-3

б) 1-4-2-3

в) 1-3

г) 1-4

д) 3-5

7.Количество периферийных вершин в простом графе G , представленном парами смежных вершин G:(1,2), (1, 4), (2,3), (2,4), (2,5), (3,5), равно-…

ОТВЕТ:4

3.14.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили основные понятия маршрута, цепи, цикла, связности, метрических характеристик;
- приобрели умения и навыки применять понятия маршрута, цепи, цикла, связности, метрических характеристик при описании графов.

3.15 Практическое занятие №ПЗ-15 (2 часа).

Тема: «Деревья. Свойства деревьев»

3.15.1 Задание для работы:

1. Деревья.
2. Свойства деревьев.
3. Фундаментальная система циклов графа.
4. Понятие об остове наименьшего веса.
5. Отыскание остова наименьшего веса.

3.15.2 Краткое описание проводимого занятия:

1. Деревья.
2. Свойства деревьев.
3. Фундаментальная система циклов графа.
4. Понятие об остове наименьшего веса.
5. Отыскание остова наименьшего веса.

Для графа, заданного матрицей весов,
а) построить по этой матрице сеть (исходный граф),
б) построить остов наименьшего веса,
в) найти его вес.

$$W = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{array} \begin{array}{c} \begin{array}{cccccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{array} \\ \begin{pmatrix} - & 5 & 10 & 14 & \infty & \infty \\ 5 & - & 5 & 6 & \infty & \infty \\ 10 & 5 & - & 7 & 8 & 9 \\ 14 & 6 & 7 & - & 4 & \infty \\ \infty & \infty & 8 & 4 & - & 12 \\ \infty & \infty & 9 & \infty & 12 & - \end{pmatrix} \end{array}.$$

Шаг1. $S' = \{x_1\},\ S'' = \{x_2, x_3, x_4, x_5, x_6\},\ U' = \varnothing.$

Первая итерация. Шаг 2.

$d(S', S'') = \omega(x_1, x_2) = 5,\ S' = \{x_1, x_2\},\ S'' = \{x_3, x_4, x_5, x_6\},$

$U' = \{(x_1, x_2)\}.$

Шаг 3. $S' \neq S$, переход на начало второго шага.

Вторая итерация. Шаг 2.

$d(S', S'') = \omega(x_2, x_3) = 5,\ S' = \{x_1, x_2, x_3\},\ S'' = \{x_4, x_5, x_6\},$

$U' = \{(x_1, x_2), (x_2, x_3)\}.$

Шаг 3. $S' \neq S$, переход на начало второго шага.

Третья итерация. Шаг 2.

$d(S', S'') = \omega(x_2, x_4) = 6,\ S' = \{x_1, x_2, x_3, x_4\},\ S'' = \{x_5, x_6\},$

$U' = \{(x_1, x_2), (x_2, x_3), (x_2, x_4)\}.$

Шаг 3. $S' \neq S$, переход на начало второго шага.

Четвертая итерация. Шаг 2. $d(S', S'') = \omega(x_4, x_5) = 4,\ S' = \{x_1, x_2, x_3, x_4, x_5\},\ S'' = \{x_6\},$

$U' = \{(x_1, x_2), (x_2, x_3), (x_2, x_4), (x_4, x_5)\}.$

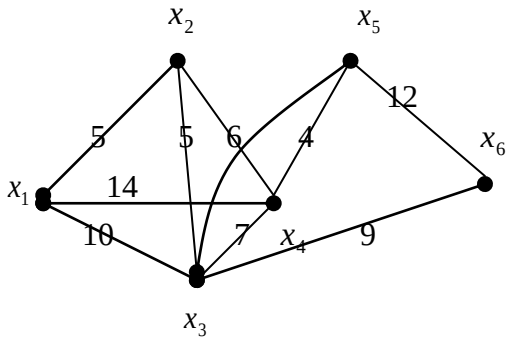
Шаг 3. $S' \neq S$, переход на начало второго шага.

Пятая итерация. Шаг 2. $d(S', S'') = \omega(x_3, x_6) = 9,\ S' = \{x_1, x_2, x_3, x_4, x_5, x_6\},\ S'' = \varnothing,$

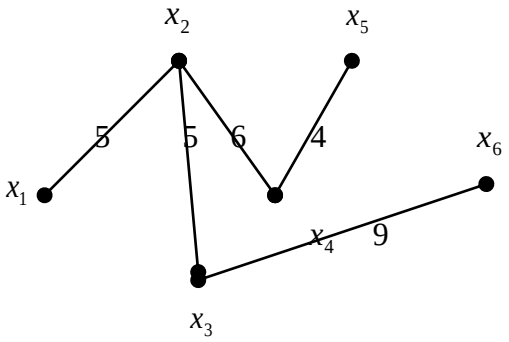
$U' = \{(x_1, x_2), (x_2, x_3), (x_2, x_4), (x_4, x_5), (x_3, x_6)\}.$

Шаг 3. $S' = S$. Итак, получен остовный граф. $G' = (S', U')$ изображен на рисунке справа, его вес $\omega(G') = 5+5+6+4+9 = 29$.

Исходный граф



Остовный граф



3.15.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия дерева, свойства деревьев;
- приобрели умения и навыки применять понятия дерева и его свойства при решении профессиональных задач.

3.16 Практическое занятие № ПЗ-16 (2 часа).

Тема: «Формализации понятия алгоритма. Математические машины. Машина Тьюринга**».**

3.16.1 Задание для работы:

1.Формализации понятия алгоритма.
2. Математические машины. Машина Тьюринга

3.16.2 Краткое описание проводимого занятия:

1. Формализации понятия алгоритма.

2. Математические машины. Машина Тьюринга

1.

	a_0	1
q_1	$1Hq_0$	$1Пq_1$

Из любой начальной конфигурации(УУ обозревает не пустой символ) эта машина Тьюринга переводит слово 11 в слово-...(Отв.: 111)

2. В команде $a_3q_2 \rightarrow a_0Лq_0$ следующее состояние машины Тьюринга

+а) q_0

б) q_2

в) q_1

г) a_0

д) q_2

3. Одной из моделей (формализаций) алгоритма является

+а) машина Тьюринга

б) задача линейного программирования

в) эйлеровы графы

г) алгебра множеств

д) алгебра логики

4.По команде $a_3q_2 \rightarrow a_0Лq_0$ состояние машины меняется

+а) с q_2 на q_0
б) с q_0 на q_2
в) с a_3 на q_2
г) с a_3 на a_0
д) с a_0 на a_3
5.По команде $a_3q_2 \rightarrow a_0Лq_0$ машина меняет в ячейке символ внешнего алфавита
+а) с a_3 на a_0
б) с a_0 на a_3
в) с a_0 на q_2
г) с q_2 на q_1
д) с q_1 на q_2
6.Состояние машины перед исполнением команды $a_3q_2 \rightarrow a_0Лq_0$ это
+а) q_2
б) q_1
в) q_0
г) a_1
д) a_2
7.В конфигурации $\begin{matrix} a_0 & 3 & 1 & 5 & a_0 \\ & & & q_1 & \end{matrix}$ обозревается символ-...

3.16.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили подходы к формализации понятия алгоритма. Рассмотрели математические машины, машину Тьюринга.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ СЕМИНАРСКИХ ЗАНЯТИЙ

Семинарские занятия не предусмотрены рабочим учебным планом.