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

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.1.09 Дискретная математика

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: Информационная безопасность автоматизированных систем критически важных объектов

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. 2 Лекция №2 (2 часа).

Тема: «Алгебра Буля»

1.2.1 Вопросы лекции:

1. Понятие об абстрактной алгебре Буля.
2. Понятие о моделях алгебры Буля.

1.1-2.2 Краткое содержание вопросов лекций №1 и №2:

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);

$Z = 0,\pm1,\pm2,\pm3,...$ - 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 $A = B$,

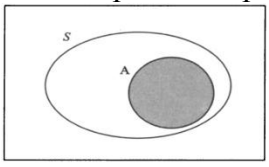
-включение $A \subset B, A \subseteq B$, понятие подмножества,

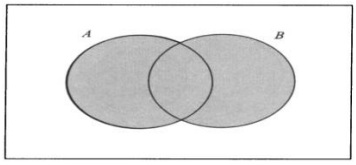
-объединение множеств $A \cup B$,

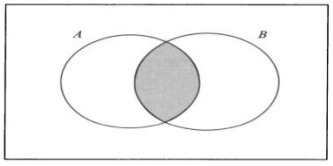
-пересечение множеств $A \cap B$,

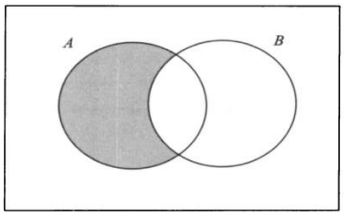
-разность множеств $A \setminus B$ и дополнение $C_A B$ множества B до множества A, универсальное множество U, дополнение множества A до универсального $\overline{A}$

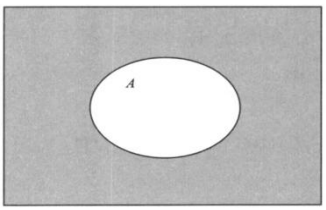
-симметрическая разность $A \Delta B$.

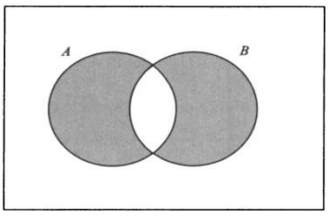












Дискретная математика представляет собой область математики, в которой изучаются свойства структур конечного характера, а также бесконечных структур, предполагающих скачкообразность происходящих в них процессов или отделимость составляющих их элементов. В отличие от дискретной математики *классическая* 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 $\varnothing$. 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 $|\varnothing| = 0$, но $|\{\varnothing\}| = 1$.

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. 3 Лекция №3 (2 часа).

Тема: «Бинарные отношения и их свойства»

1.3.1 Вопросы лекции:

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

1.3.2 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: $p_{ij} = \begin{cases} 1, & если\ (a_i, b_j) \in P, \\ 0, & если\ (a_i, b_j) \notin P. \end{cases}$ 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 логи-

ческим формулам (т.е. 0+0=0, во всех остальных случаях 1). Итак: **[P∪Q] = [P]+[Q], [P∩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: $[P^{-1}]=[P]^T$.

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. $R \circ R \subseteq R$.

1. 4 Лекция №4 (2 часа).

Тема: «Отношения эквивалентности»

1.4.1 Вопросы лекции:

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

1.4.2 Краткое содержание вопросов:

Отношения эквивалентности и порядка.

Отношение 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 $\forall i,j \ i \neq j \Rightarrow B_i \cap B_j = \varnothing$

1. 5 Лекция №5 (2 часа).

Тема: «Отношения частичного порядка. Отношения Парето. Принятие решений при многих критериях»

1.5.1 Вопросы лекции:

1. Отношения порядка.
2. Отношения Парето. Принятие решений при многих критериях.

1.5.2 Краткое содержание вопросов:

1. Отношения порядка.
2. Отношения Парето. Принятие решений при многих критериях.

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 ⊂ на булеане $P(M)$ является отношением нестрого частичного порядка.

Пусть дано ч.у.м. M с отношением порядка ≤: Ũ= $\{M,\leq\}$. М*аксимальный* 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.**

<u>*Утверждение:*</u> 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 ≤. Введем отношение ≤ 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. 6 Лекция №6 (2 часа).

Тема: «Функции. Виды функций»

1.6.1 Вопросы лекции:

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

1.6.2 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).

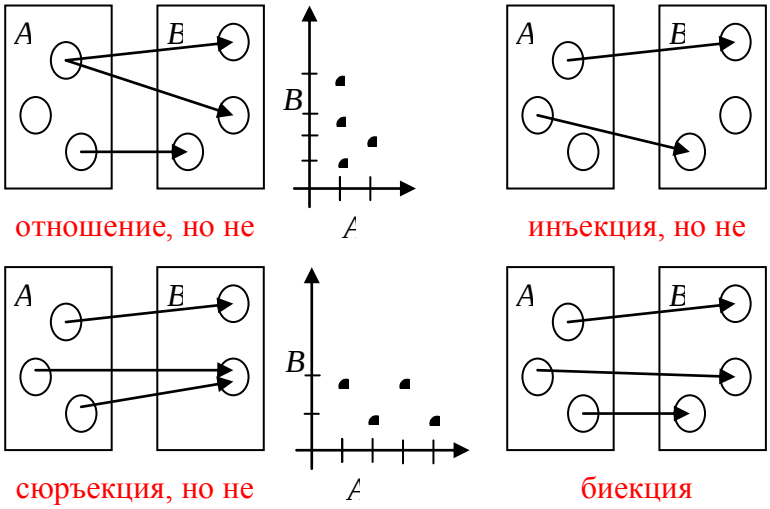


Рис. 1.4 Графическое представле-

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

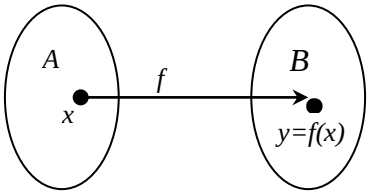
Отображение $f : A \to B$ называется (см. рисунок ниже):

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:

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

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 $\{0, 1, 2, 3, \ldots\}$ 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. 7 Лекция № 7 (2 часа).

Тема: «Эквивалентные множества. Понятие мощности множеств, сравнение мощностей»

1.7.1 Вопросы лекции:

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

1. 8 Лекция №8 (2 часа).

Тема: «Счётные множества. Множества мощности континуум»

1.8.1 Вопросы лекции:

1. Счётные множества.
2. Множества мощности континуум.

1.7-8.2 Краткое содержание вопросов лекций №7 и №8:

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;

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.*

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. 9 Лекция № 9 (2 часа).

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

1.9.1 Вопросы лекции:

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

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

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

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

2) в множестве A 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 $[\sigma]$ и $[\tau]$, то их *произведение* $\sigma\cdot\tau$ определяется следующим образом. В матрице $[\tau]$ столбцы переставляются так, чтобы ее первая строка совпала со второй строкой матрицы $[\sigma]$: $\begin{pmatrix} s_1 & s_2 & \ldots & s_n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}$. 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 $[\sigma]$ 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 $\sigma(s_r) = s_1$.

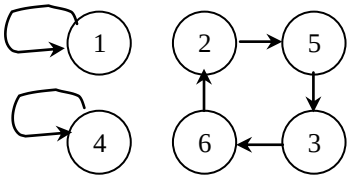
Подстановка σ с матрицей $[\sigma] = \begin{pmatrix}1&2&3&4&5&6\\1&5&6&4&3&2\end{pmatrix} = \begin{pmatrix}2&5&3&6&1&4\\5&3&6&2&1&4\end{pmatrix}$ является циклом (2 5 3 6), а подстановка с матрицей $[\tau] = \begin{pmatrix}1&2&3&4&5&6\\4&5&2&1&6&3\end{pmatrix}$ циклом не является, т.к. из нее можно выделить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

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

В примере 2.7 $[\sigma]$ = (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. 10 Лекция № 10 (2 часа).

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

1.10.1 Вопросы лекции:

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

1.10.2 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* ∈ 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 $Z / m Z$. 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. 11 Лекция № 11 (2 часа).

Тема: «Правила комбинаторики. Комбинаторные формулы»

1.11.1 Вопросы лекции:

1. Правила комбинаторики.
2. Комбинаторные формулы

1.11.2 Краткое содержание вопросов:

1. Правила комбинаторики.

Комбинаторика – раздел математики, посвященный решению задач выбора и расположения элементов некоторого обычного множества в соответствии с заданными пра-

вилами. 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 $M = \{a_1,a_2,...,a_n\}$. *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 $M = \{a_1, a_2, a_3, ..., a_n\}$, $m \le n$. 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 $k \ge n$. 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: $(a_1,a_2,...,a_k) \sim (b_1,b_2,...,b_k) \Leftrightarrow \forall c \in M$ 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. 12 Лекция № 12 (2 часа).

Тема: «Бином Ньютона. Биномиальные коэффициенты и их свойства»

1.12.1 Вопросы лекции:

1. Бином Ньютона.
2. Биномиальные коэффициенты и их свойства.

1.12.2 Краткое содержание вопросов:

1. Бином Ньютона.

2. Биномиальные коэффициенты и их свойства.

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

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. $\sum_{m=0}^{n} m C_n^m = n 2^{n-1}$; 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.

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

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

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

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

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:

$S(n,k)=S(n-1,k-1)+ k\cdot S(n-1,k)$ $(0<k<n)$

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

1. 13 Лекция № 13 (2 часа).

Тема: «Метод включений и исключений. Метод рекуррентных соотношений»

1.13.1 Вопросы лекции:

1. Метод включений и исключений.
2. Метод рекуррентных соотношений

1. 14 Лекция № 14 (2 часа).

Тема: «Производящие функции»

1.14.1 Вопросы лекции:

1. Производящие функции

1.13-14.2 Краткое содержание вопросов лекций № 13 и №14:

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

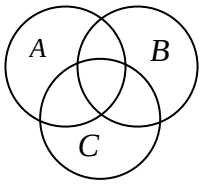
Принцип включения и исключения. Рассмотренные ранее формулы и алгоритмы дают способы вычисления комбинаторных чисел для некоторых распространенных комбинаторных конфигураций. Практические задачи не всегда прямо сводятся к известным комбинаторным конфигурациям. В этом случае используются различные методы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

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$, 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 $(0 \le r \le m)$.

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

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 $p_i = \text{const}$, 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. 15 Лекция № 15 (2 часа).

Тема: «Простые числа»

1.16.1 Вопросы лекции:

1. Простые числа.

1. 16 Лекция № 16 (2 часа).

Тема: «Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным Решение сравнений первой степени»

1.16.1 Вопросы лекции:

1. Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным
2. Решение сравнений первой степени.

1. Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным
2. Решение сравнений первой степени.

1. 17 Лекция №17 (2 часа).

Тема: «Порядок числа и класса вычетов по модулю. Первообразные корни. Индексы по простому модулю и их приложения»

1.17.1 Вопросы лекции:

1. Порядок числа и класса вычетов по модулю. Первообразные корни.
2. Индексы по простому модулю и их приложения.

1.17.2 Краткое содержание вопросов лекций № 11 и № 12:

1. Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным
2. Решение сравнений первой степени.
3. Порядок числа и класса вычетов по модулю. Первообразные корни.
4. Индексы по простому модулю и их приложения.

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, $ac = bd + m(t_1 t_2 + bt_2 + ct_1)$, 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:

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots - \frac{n}{p_k} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \ldots + \frac{n}{p_{k-1} p_k} - \frac{n}{p_1 p_2 p_3} - \frac{n}{p_1 p_2 p_4} - \ldots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k}.$$

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 $r_1, r_2, \ldots, r_c$. Чис-

ло ar_2 попадает в один класс с другим числом r_{i_2}, но из этого же множества, т.е. имеем сравнения

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

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

2. 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.

1.18 Лекция №18 (2 часа).

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

1.18.1 Вопросы лекции:

Математические основы криптографии: приложения модульной арифметики в алгоритме RSA.

1.18.2 Краткое содержание вопросов:

Математические основы криптографии: приложения модульной арифметики в алгоритме RSA.

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.

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

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

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* $НОД \ \ e,\varphi(n) \ =1\cdot$

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

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

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

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

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

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

г) Зашифрованное сообщение

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

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.

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

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

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

1. 19 Лекция № 19 (2 часа).

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

1.19.1 Вопросы лекции:

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

1.9.2 Краткое содержание вопросов:

1. Основные понятия теории графов. Виды графов.

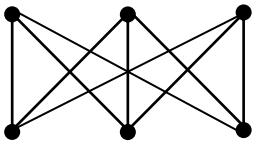
Определение графа. Часто бывает полезно и наглядно изобразить некоторую ситуацию в виде рисунка, состоящего из точек (вершин), представляющих основные элементы ситуации и линий (ребер), отражающих связи между элементами. Такие рисунки называются *графами.*

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* $\langle V, E\rangle$*, 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*.

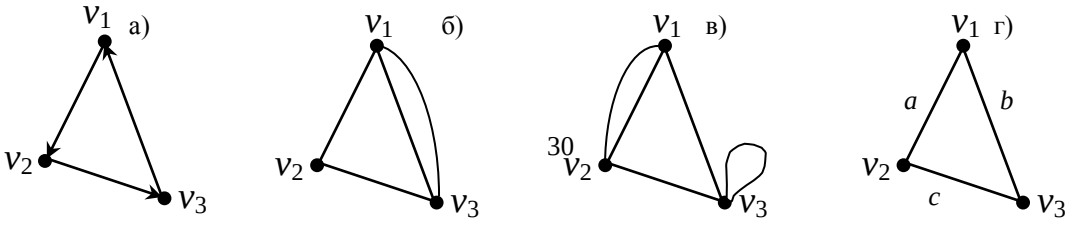
Обычно граф изображают *диаграммой*: вершины – точками или кружками, ребра – линиями (нарисовать). Такой способ задания графа является самым простым и наглядным, хотя и годится только для простейших случаев. Кроме того, затруднительно обрабатывать такой граф с помощью ЭВМ. Поэтому существуют специальные 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 $\Gamma^+(v) = \{u\in V | (u,v)\in E\}$, $\Gamma(v)=\Gamma^*(v) = \Gamma^+(v)\cup\{v\}$. 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 Г(*A*) – множество вершин, смежных с вершинами из *A*: $\Gamma(A) = \{u\in V | \exists v\in A\ \ u\in\Gamma(v)\} = \cup\Gamma(v)\ \forall v\in A$.
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 $E=\{(u,v)|u,v\in V\}$ 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.

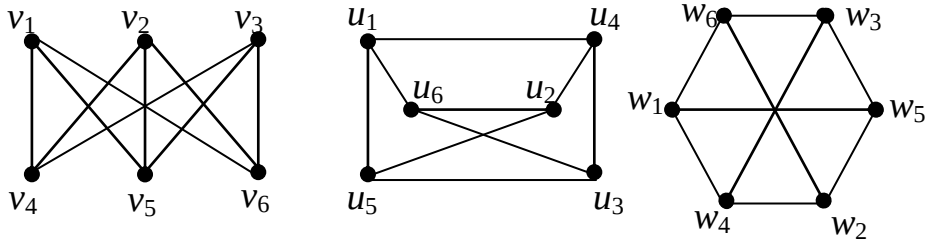
Изоморфизм графов: При изображении графа точки, обозначающие его вершины, берутся совершенно произвольно, поэтому рисунки одного и того же графа могут быть совершенно непохожими. Как же понять, одинаковы ли графы, изображенные разными чертежами? Решение проблемы стандартное – если можно взаимно однозначно 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;

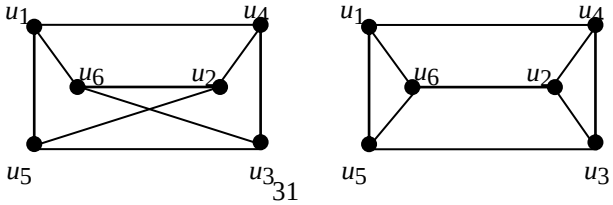
2) симметричность – если $G_1\sim G_2$ с биекцией h, то $G_2\sim G_1$ с биекцией h^{-1};
3) транзитивность – если $G_1\sim G_2$ с биекцией h, а $G_2\sim G_3$ с биекцией g; то $G_1\sim G_3$ с биекцией $g\circ h$.

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.

2. Операции над графами

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

1.19.1 Вопросы лекции:

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

1.19.2 Краткое содержание вопросов:

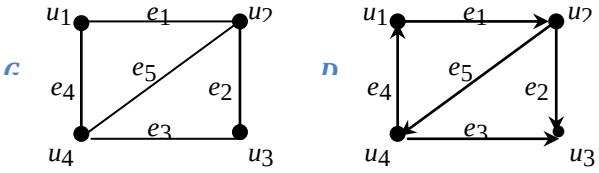
1. Способы задания графов. Матричное представление графов

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.

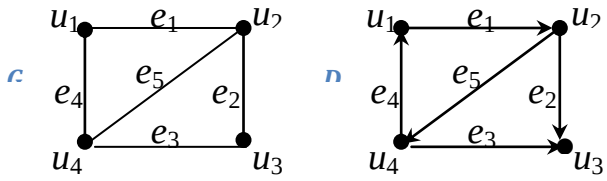
Матрица смежности A(G') графа (орграфа) – это квадратная матрица размера n×n, у которой для любых $i,j \in \{1,2,\ldots,n\}$ элемент в *i*-й строке и *j*-м столбце равен 1, если *i*-я и *j*-я вершины соединены ребром (дугой с началом в вершине *i*), и равен 0 в противном случае.

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

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.

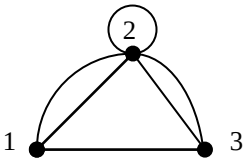


Матрицы смежности для заданных графа *G* и орграфа *D*

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

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:

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

Для ориентированного графа:

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

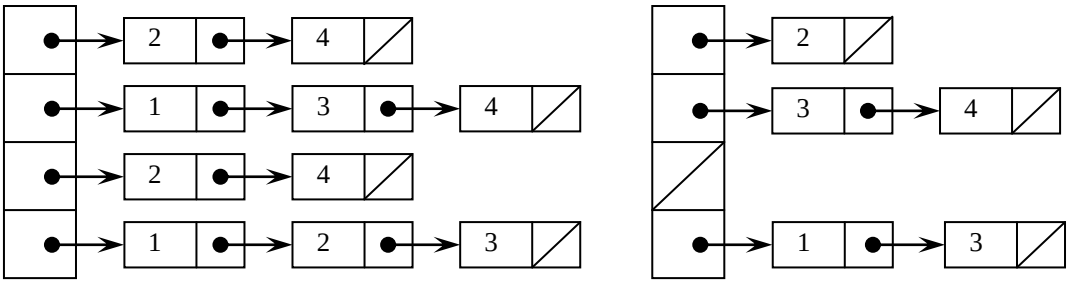
Матрицы инцидентности для заданных графа *G* и орграфа *D*

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

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

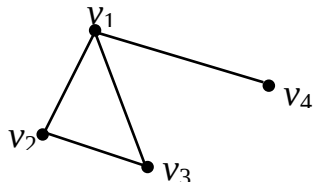
4) Массив ребер (дуг).

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

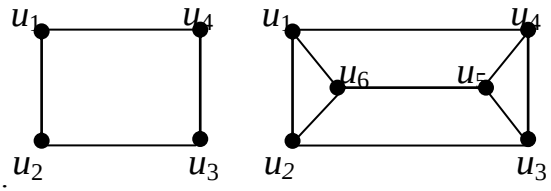
Степенью (или *валентностью*) *вершины v* называется число инцидентных ей ребер. Степень вершины обозначается *deg(v)*. Очевидно, что для любой вершины $v \in V$ справедливо: $0 \le deg(v) \le |V| - 1$; $deg(v) = |\Gamma(v)|$. Вершина графа, имеющая степень 0, называется *изолированной*, а вершина со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

тельность для графа *G*. Выпишем степени всех вершин графа в соответствии с их номера-



ми (2,2,3,2,1).

1.20 Лекция № 20 (2 часа).

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

1.20.1 Вопросы лекции:

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

1.20.2 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 ⟨*u*,*v*⟩.

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 ⟨*u*,*v*⟩, а сама кратчайшая цепь называется *геодезической*. Если не существует цепи, соединяющей вершины *u* и *v*, то по определению *d*(*u*,*v*) = +∞.

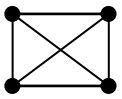
Диаметром графа *G* (обозначается *D(G)*) называется длина длиннейшей геодезической.

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. 23 Лекция №23 (2 часа).

Тема: «Эйлеровы и гамильтоновы циклы в графах. Свойства эйлеровых и гамильтоновых графов (в инт. форме)»

1.23.1 Вопросы лекции:

1. Эйлеровы и гамильтоновы циклы в графах.
2. Свойства эйлеровых и гамильтоновых графов.

1.23.2 Краткое содержание вопросов:

1. Эйлеровы и гамильтоновы циклы в графах.
2. Свойства эйлеровых и гамильтоновых графов.

Обходы графов. *Обход графа – это некоторое систематическое перечисление его вершин (ребер). Среди всех обходов наиболее известны поиск в глубину и в ширину. Алгоритмы такого поиска лежат в основе многих алгоритмов на графах.*

При поиске используется некоторая структура данных T, в которую помещаются вершины графа. Для обозначения пройденных вершин заводят дополнительный массив пометок этих вершин.

Поиск основывается на следующих действиях.

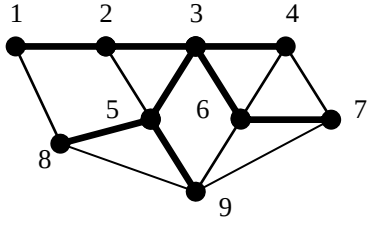
1.Сначала все вершины считаются неотмеченными.

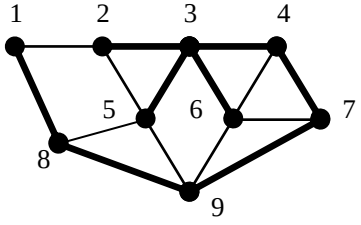
2.Выбирается любая вершина (начало поиска), заносится в структуру данных T и помечается.

3.Следующие действия выполняются в цикле до тех пор, пока структура T не станет пустой: из структуры данных T выбирается вершина *u*; она выдается в качестве очередной пройденной вершины; перебираются все вершины из Γ(u), и все те, которые не помечены, тоже заносятся в структуру T и помечаются.

Если T – это стек (LIFO), то обход называется поиском *в глубину* (т.е. первым делом из структуры T извлекается вершина, попавшая туда последней). Если T – это очередь (FIFO), то обход называется поиском *в ширину*. При поиске в глубину находятся более длинные пути.

Если граф G связен и конечен, то поиск в ширину или поиск в глубину обойдет все вершины графа по одному разу.





Рассмотрим алгоритмы поиска в глубину и в ширину на примере. В качестве стартовой возьмем вершину с номером 3. Тогда поиск <u>в ширину</u> даст последовательность вершин: 3→T. T={3}⇒ **3**: {2,5,6,4}→T; T={2,5,6,4}⇒ **2**: {1}→T; T={5,6,4,1}⇒ **5**: {8,9}→T; T={6,4,1,8,9}⇒ **6**: {7}→T; T={4,1,8,9,7}. Окружения всех этих вершин уже отмечены ⇒ они будут выданы по порядку. Итак, выполнен обход всех вершин графа в следующем порядке: **3,2,5,6,4,1,8,9,7**. При поиске <u>в глубину</u> начало такое же: 3→T. T={3} ⇒ **3**: {2,5,6,4}→T; T={2,5,6,4}⇒ **4**: {7}→T; T={2,5,6,7}⇒ **7**: {9}→T; T={2,5,6,9} ⇒ **9**: {8}→T; T={2,5,6,8}⇒ **8**: {1}→T; T={2,5,6,1}. Оставшиеся вершины выдаются по порядку. В итоге последовательность вершин: **3,4,7,9,8,1,6,5,2.**

Любой из рассмотренных обходов позволяет построить остовное дерево исходного графа с корнем в исходной вершине (связный подграф без циклов).

Эйлеровы и гамильтоновы циклы в графах

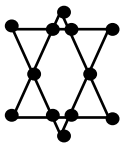
Эйлеровы графы. *Цикл в графе называется* эйлеровым, *если он содержит все ребра графа. Связный граф, в котором существует эйлеров цикл, называется* эйлеровым графом.

Эйлеровой цепью *(или путем) является цепь (путь), которая включает все ребра (дуги) графа по одному разу.* Собственная эйлерова цепь – *это эйлерова цепь, которая не является эйлеровым циклом.*

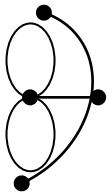
Эйлеров граф можно нарисовать, не отрывая карандаша от бумаги. Известные примеры эйлеровых графов приведены на рисунке. **Теорема Эйлера.** *Связный*

граф является эйлеровым тогда и только тогда, когда степени всех его вершин четны.

сабли Магомета



звезда Давида



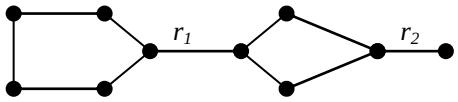
Вспомним задачу о кенигсбергских мостах. Она сводится к вопросу – является ли граф, представляющий эту задачу, эйлеровым? Если вершины будут обозначать участки суши, а ребра – мосты, то получим граф следующего вида:

Очевидно, что этот граф не эйлеров, т.к. все его вершины имеют нечетные степени; поэтому требуемый цикл не существует. Если отменить требование возврата в ту же точку, то вопрос о пути по всем мостам сведется к вопросу о существовании собственной эйлеровой цепи.

Граф имеет собственную эйлерову цепь (путь) ⇔ когда он связный и ровно две его вершины имеют нечетную степень.

Вершины нечетной степени являются началом и концом эйлеровой цепи.
Если снова вернуться к рассмотренному примеру, то увидим, что эйлерова цепь в нем также не существует, т. к. вершин нечетной степени в нем 4.

А теперь разберемся, как найти эйлеров цикл. Сначала еще определение.
Мостом (или *перешейком*) называется такое ребро графа *G*, удаление которого увеличивает число связных компонент. Если ребро *r* принадлежит некоторому циклу *C*, то оно не может быть мостом.



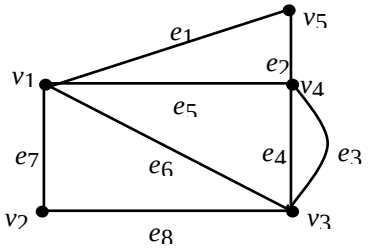
В данном графе ребра r_1 и r_2 являются мостами.

Для нахождения эйлеровой цепи в связном графе, который имеет вершины только четной степени, используют *алгоритм Флери*:

1) Движение начинается из произвольной вершины графа; идем по ребрам, включая эти ребра в эйлерову цепь и удаляя их из графа.

2) В очередной вершине выбираем путь по перешейку только в том случае, если нет пути по циклу.

3) Если в графе остаются ребра, которые нельзя использовать для продолжения имеющегося пути, то следует начать строить простой замкнутый цикл из уже пройденной вершины и инцидентного ей ребра, если последнее ранее не использовалось.



Пусть требуется построить эйлеров цикл для графа, изображенного на рисунке. Начать построение эйлерового цикла можно с любого ребра графа. Начиная с e_1, получим цикл v_1, e_1, v_5, e_2, v_4 ,e_3, v_3 ,e_4 , v_4 ,e_5 ,v_1,e_6 ,v_3, e_8, v_2, e_7 ,v_1. В данном случае сразу получили эйлерову цепь.

Гамильтоновы графы

Гамильтонова цепь (путь) – это простая цепь (путь), которая проходит через каждую вершину (узел) графа ровно по одному разу. Соответственно *гамильтонов цикл* – это простой цикл, который проходит через каждую вершину графа.

Граф, содержащий гамильтонов цикл, называется гамильтоновым графом.

Гиперкуб порядка n при $n \geq 3$ имеет гамильтонов цикл. Этот цикл описывается кодом Грея (каждые два соседних набора отличаются ровно одним разрядом $\Rightarrow$ на графе они соединены ребром). (000, 001, 011, 111, 101, 100, 110, 010, 000).

В отличие от эйлерова графа, не существует четкого критерия для определения, является ли граф гамильтоновым.

В качестве практического применения задачи поиска гамильтонова пути можно назвать т.н. задачу коммивояжера. В ней требуется осуществить обход всех населенных пунктов, посещая каждый по разу, и при этом постараться пройти минимальное расстояние.

1. 21 Лекция № 21 (12 часа).

Тема: «Деревья. Свойства деревьев»

1.21.1 Вопросы лекции:

1. Деревья.
2. Свойства деревьев.
3. Задача об остове минимального веса.

1.21.2 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;

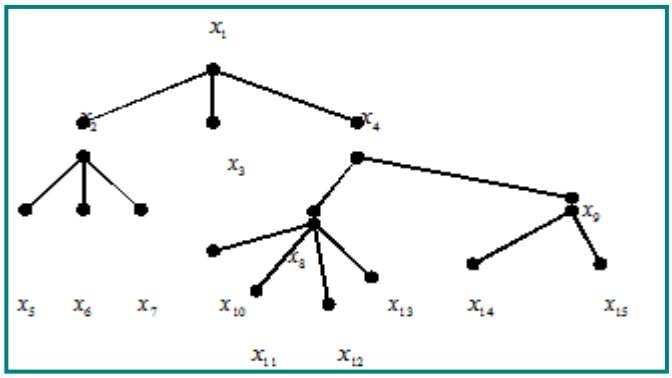
2). G - связный граф и $m = n - 1$;

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 $\sum_{i=1}^{n} b_{ij} = 0,\ j = \overline{1,n}$,

$\sum_{j=1}^{n} b_{ij} = 0,\ i = \overline{1,n}$.

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. 22 Лекция №22 (2 часа).

Тема: «Свойства эйлеровых и гамильтоновых графов»

1.22.1 Вопросы лекции:

Свойства эйлеровых и гамильтоновых графов.

1.22.2 Краткое содержание вопросов:

Свойства эйлеровых и гамильтоновых графов.

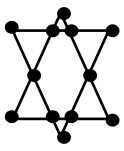
Эйлеровы и гамильтоновы циклы в графах

Эйлеровы графы. *Цикл в графе называется* эйлеровым*, если он содержит все ребра графа. Связный граф, в котором существует эйлеров цикл, называется* эйлеровым графом*.* Эйлеровой цепью *(или путем) является цепь (путь), которая включает все ребра (дуги) графа по одному разу.* Собственная эйлерова цепь – *это эйлерова цепь, которая не является эйлеровым циклом.*

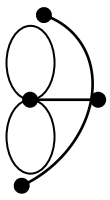
Эйлеров граф можно нарисовать, не отрывая карандаша от бумаги. Известные примеры эйлеровых графов приведены на рисунке. **Теорема Эйлера.** *Связный*

граф является эйлеровым тогда и только тогда, когда степени всех его вершин четны.

сабли Магомета



звезда Давида



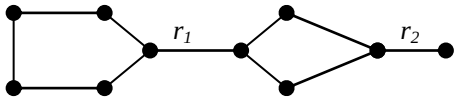
Вспомним задачу о кенигсбергских мостах. Она сводится к вопросу – является ли граф, представляющий эту задачу, эйлеровым? Если вершины будут обозначать участки суши, а ребра – мосты, то получим граф следующего вида:

Очевидно, что этот граф не эйлеров, т.к. все его вершины имеют нечетные степени; поэтому требуемый цикл не существует. Если отменить требование возврата в ту же точку, то вопрос о пути по всем мостам сведется к вопросу о существовании собственной эйлеровой цепи.

Граф имеет собственную эйлерову цепь (путь) ⇔ когда он связный и ровно две его вершины имеют нечетную степень.

Вершины нечетной степени являются началом и концом эйлеровой цепи.
Если снова вернуться к рассмотренному примеру, то увидим, что эйлерова цепь в нем также не существует, т. к. вершин нечетной степени в нем 4.

А теперь разберемся, как найти эйлеров цикл. Сначала еще определение.
Мостом (или *перешейком*) называется такое ребро графа *G*, удаление которого увеличивает число связных компонент. Если ребро *r* принадлежит некоторому циклу *C*, то оно не может быть мостом.



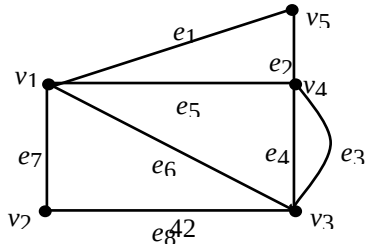
В данном графе ребра r_1 и r_2 являются мостами.

Для нахождения эйлеровой цепи в связном графе, который имеет вершины только четной степени, используют *алгоритм Флери*:

1) Движение начинается из произвольной вершины графа; идем по ребрам, включая эти ребра в эйлерову цепь и удаляя их из графа.

2) В очередной вершине выбираем путь по перешейку только в том случае, если нет пути по циклу.

3) Если в графе остаются ребра, которые нельзя использовать для продолжения имеющегося пути, то следует начать строить простой замкнутый цикл из уже пройденной вершины и инцидентного ей ребра, если последнее ранее не использовалось.



Пусть требуется построить эйлеров цикл для графа, изображенного на рисунке. Начать построение эйлерового цикла можно с любого ребра графа. Начиная с e_1, получим цикл v_1, e_1, v_5, e_2, v_4 ,e_3, v_3 ,e_4 , v_4 ,e_5 ,v_1,e_6 ,v_3, e_8, v_2, e_7 ,v_1. В данном случае сразу получили эйлерову цепь.

Гамильтоновы графы

Гамильтонова цепь (путь) – это простая цепь (путь), которая проходит через каждую вершину (узел) графа ровно по одному разу. Соответственно *гамильтонов цикл* – это простой цикл, который проходит через каждую вершину графа.

Граф, содержащий гамильтонов цикл, называется гамильтоновым графом.

Гиперкуб порядка n при $n \geq 3$ имеет гамильтонов цикл. Этот цикл описывается кодом Грея (каждые два соседних набора отличаются ровно одним разрядом $\Rightarrow$ на графе они соединены ребром). (000, 001, 011, 111, 101, 100, 110, 010, 000).

В отличие от эйлерова графа, не существует четкого критерия для определения, является ли граф гамильтоновым.

В качестве практического применения задачи поиска гамильтонова пути можно назвать т.н. задачу коммивояжера. В ней требуется осуществить обход всех населенных пунктов, посещая каждый по разу, и при этом постараться пройти минимальное расстояние.

1. 23 Лекция №23 (2 часа).

Тема: «Планарность и укладка графов. Раскраска графов. Хроматическое число (в инт. форме)**»**

1.23.1 Вопросы лекции:

1. Планарность и укладка графов.
2. Раскраска графов. Хроматическое число.

1.23.2 Краткое содержание вопросов:

1. Планарность и укладка графов.
2. Раскраска графов. Хроматическое число.

1. 24 Лекция № 24 (2 часа).

Тема: «Орграфы и сети. Прикладные задачи и алгоритмы анализа графов и сетей, задачи оптимизации на графах и сетях. ИТ - технологии анализа графов и сетей.**»**

1.24.1 Вопросы лекции:

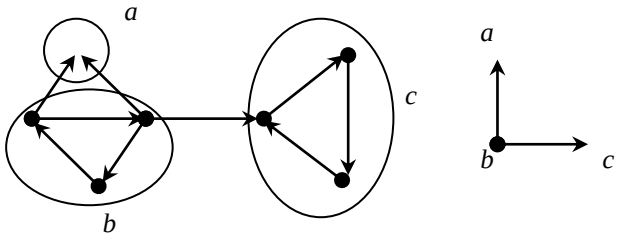
1. Сети.
2. Оптимизационные задачи на графах и сетях, алгоритмы их решения.

1.24.2 Краткое содержание вопросов:

1. Сети.

2. Оптимизационные задачи на графах и сетях, алгоритмы их решения.

1) **Выделение компонент связности в орграфах.** *Компоненты сильной связности (КСС) орграфа* G *– это его максимальные сильно связные подграфы. Каждая вершина орграфа принадлежит только одной КСС. Если вершина не связана с другими, то считается, что она сама образует КСС. Орграф, который получается стягиванием в одну вершину каждой КСС, называется* фактор-графом*, или* конденсацией *орграфа* G.



Слева на рисунке орграф, справа – его фактор-граф. Овальными линиями показаны КСС, стянутые в одну вершину фактор-графа.

Для выделения компонент сильной связности орграфа можно в качестве основы алгоритма использовать метод поиска в глубину.

Теорема. Любой граф представляется в виде объединения непересекающихся связных (сильных) компонент. Разложение графа на связные (сильные) компоненты определяется однозначно.

2) **Кратчайшие пути.** *Задача поиска кратчайшего пути (наиболее дешевого? короткого?) «от пункта А до пункта В» имеет массу практических приложений и различные алгоритмы решения. Математическая постановка задачи имеет следующий вид.*

Рассматривается взвешенный граф (орграф) $G(V,E)$, ребрам (дугам) которого сопоставлены веса, обозначающие длину (или стоимость) пути из одного конца ребра в другой. Если из вершины v_i нет ребра (дуги) в вершину v_j, то вес ребра (v_i,v_j) считается равным ∞. Для ребер, являющихся петлями (диагональ матрицы смежности), их веса считаются равными 0. Все компоненты матрицы – веса ребер, соединяющих соответствующие вершины. Требуется определить кратчайший путь из одной вершины в другую.

Наиболее широко известны два алгоритма поиска кратчайших путей. Алгоритм Дейкстры находит кратчайшее расстояние от одной фиксированной вершины до другой и указывает сам путь, длина которого равна этому расстоянию. Алгоритм Флойда-Уоршалла позволяет найти кратчайшие расстояния между всеми парами вершин графа.

Алгоритм Дейкстры. Находит кратчайшее расстояние от вершины v_1 до вершины v_n

Рассмотрим еще несколько алгоритмов нахождения кратчайшего пути между двумя заданными вершинами в ориентированной сети. Пусть $G = \langle X, U, \Omega \rangle$ - ориентированный граф со взвешенными дугами. Обозначим s - вершину - начало пути и t - вершину – конец пути.

Общий подход к решению задачи о кратчайшем пути был развит американским математиком Ричардом Беллманом**, который предложил название динамическое программирование.

* Едсгер Дейкстра (1930-2002 г.г.) - нидерландский математик.

** Ричард Эрнест Беллман (1920-1984 г.г.) - американский математик.

Задача о кратчайшем пути частный случай следующей задачи: найти в заданном графе пути, соединяющие две заданные вершины и доставляющие минимум или максимум некоторой аддитивной функции, определенной на путях. Чаще всего эта функция трактуется как длина пути и задача называется задачей о кратчайших путях. Алгоритм Дейкстры одна из реализаций этой задачи. Его часто называют алгоритмом расстановки меток. В процессе работы этого алгоритма узлам сети $x_i \in S$ приписываются числа (метки) $d(x_i)$, которые служат оценкой длины (веса) кратчайшего пути от вершины s к вершине x_i. Если вершина x_i получила на некотором шаге метку $d(x_i)$, это означает, что в графе G существует путь из s в x_i, имеющий вес $d(x_i)$. Метки могут находиться в двух

состояниях – быть временными или постоянными. Превращение метки в постоянную означает, что кратчайшее расстояние от вершины s до соответствующей вершины найдено.

Алгоритм Дейкстры состоит из двух этапов. На первом этапе находится длина кратчайшего пути, на втором – строится сам путь от вершины s к вершине t.

Этап 1. Нахождения длины кратчайшего пути.

Шаг 1. Присвоение вершинам начальных меток.

Полагаем $d(s) = 0^*$ и считаем эту метку постоянной (постоянные метки помечаются сверху звездочкой). Для остальных вершин $x_i \in S,\ x_i \neq s$ полагаем $d(x_i) = \infty$ и считаем эти метки временными. Пусть $\tilde{x} = s,\ \tilde{x}$ - обозначение текущей вершины.

Шаг 2. Изменение меток.

Для каждой вершины x_i с временной меткой, непосредственно следующей за вершиной $\tilde{x}$, меняем ее метку в соответствии со следующим правилом:

$$d_{нов.}(x_i) = \min\left[d_{стар.}(x_i), d(\tilde{x}) + \omega(\tilde{x}, x_i)\right] \qquad (4.7.1)$$

Шаг 3. Превращение метки из временной в постоянную.

Из всех вершин с временными метками выбираем вершину x_j^* с наименьшим значением метки

$$d(x_j^*) = \min\left\{ d(x_j) \,/\, x_j \in S,\ d(x_j) - \text{временная} \right\} \qquad (4.7.2)$$

Превращаем эту метку в постоянную и полагаем $\tilde{x} = x_j^*$.

Шаг 4. Проверка на завершение первого этапа.

Если $\tilde{x} = t$, то $d(t)$ - длина кратчайшего пути от s до t. В противном случае происходит возвращение ко второму шагу.

Этап 2. Построение самого кратчайшего пути.

Шаг 5. Последовательный поиск дуг кратчайшего пути.

Среди вершин, непосредственно предшествующих вершине $\tilde{x}$ с постоянными метками, находим вершину x_i, удовлетворяющую соотношению

$$d(\tilde{x}) = d(x_i) + \omega(x_i, \tilde{x}) \qquad (4.7.3)$$

Включаем дугу $(x_i, \tilde{x})$ в искомый путь и полагаем $\tilde{x} = x_i$.

Шаг 6. Проверка на завершение второго этапа.

Если $\tilde{x} = s$, то кратчайший путь найден – его образует последовательность дуг, полученных на пятом шаге и выстроенных в обратном порядке. В противном случае возвращаемся к пятому шагу.

2. Прикладные задачи и алгоритмы анализа графов.

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. Рассмотрим алгоритм Прима[*], представляющий собой итерационную процедуру, состоящую из двух шагов и выполняющуюся $n-1$ раз на графе G с n вершинами.

Пусть $S' \subset S,\ S'' \subset S$ и $S = S' \cup S'',\ S' \cap S'' = \varnothing$, то есть S' и S'' - разбиение множества узлов сети G на два непересекающихся подмножества. Определим пошаговое расстояние между множествами S' и S'' следующим образом:

$$d(S', S'') = \min\left\{ \omega(x_i, x_j) \,/\, x_i \in S',\ x_j \in S'' \right\},$$

где (x_i, x_j) - дуга, соединяющая вершины x_i и x_j.

В алгоритме Прима остовное дерево строится в результате последовательного расширения исходного поддерева. На каждой итерации число вершин и ребер поддерева увеличивается на единицу. Основные шаги алгоритма таковы.

Шаг 1. (Присвоение начальных значений).

Полагают $S' = \{x_1\}$, где x_1 - произвольная вершина, $S'' = S / S'$, $U' = \varnothing$.

Шаг 2. (Обновление данных).

Находится ребро (x_i, x_j) такое, что $x_i \in S'$, $x_j \in S''$ и $\omega(x_i, x_j) = \min\left\{ \omega(x_i, x_j) \,/\, x_i \in S',\ x_j \in S'' \right\}$. Полагают $S' = S' \cup \{x_j\}$, $S'' = S / S'$, $U' = U' \cup (x_i, x_j)$.

Шаг 3. (Проверка на завершение).

Если $S' = S$, то $G' = (S', U')$ - искомый остов. В противном случае переходят ко второму шагу.

Пример. Построить остов с наименьшим весом для сети, заданной матрицей смежности вершин. Построим по этой матрице сеть. Поскольку матрица симметрическая, то граф дан неориентированный. Исходный граф изображен внизу следующей страницы.

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

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

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

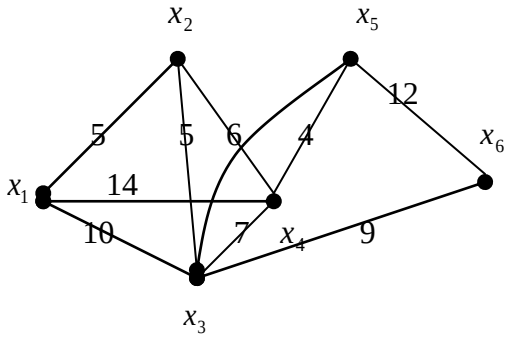
Шаг 3. $S' \neq S$, переход на начало второго шага.

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

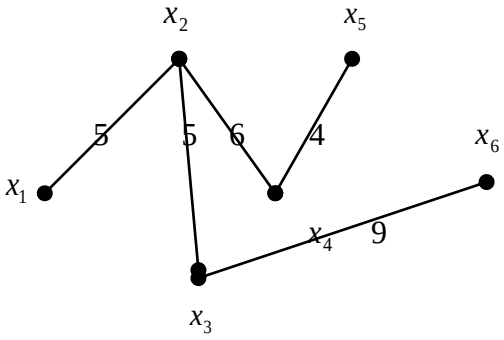
$U' = (x_1, x_2), (x_2, x_3), (x_2, x_4), (x_4, x_5), (x_3, x_6)$.

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



1. Потоки в сетях. Задача о максимальном потоке.

Потоки в сетях. Функциональное назначение большинства физически реализованных сетей состоит в том, что они служат носителями систем потоков, то есть систем, в которых некоторые объекты текут, движутся или транспортируются по системе каналов (дуг сети) ограниченной пропускной способности. Примерами могут служить поток автомобильного транспорта по сети автодорог, поток грузов по участку железнодорожной сети, поток воды в городской сети водоснабжения, поток электрического тока в электросети, поток телефонных или телеграфных сообщений по каналам связи, поток программ в вычислительной сети. Ограниченная пропускная способность означает, что интенсивность перемещения соответствующих предметов по каналу ограничена сверху определенной величиной.

Наиболее часто в сети решается задача о максимальном потоке и минимальном разрезе. При этом граф $G = (S, U)$ должен удовлетворять следующим условиям:

1). G - связный граф без петель;

2). существует ровно одна вершина, не имеющая предшествующих; эта вершина называется источником и обозначается s;

3). существует ровно одна вершина, не имеющая последующих; эта вершина называется стоком и обозначается t;

4). каждой дуге $(x_i, x_j) \in U$ поставлено в соответствие неотрицательное число $c(x_i, x_j)$, называемое пропускной способностью дуги.

Функция $\varphi(x_i, x_j)$, определенная на множестве дуг сети $G = (S, U, \Omega)$, называется потоком, если $0 \le \varphi(x_i, x_j) \le c(x_i, x_j) \; \forall (x_i, x_j) \in U$ и $\sum_{x_j \in S_{np}(x_i)} \varphi(x_i, x_j) = \sum_{x_j \in S_{cl}(x_i)} \varphi(x_i, x_j)$ для любой вершины $x_i \in S$ и $x_i \notin \{s, t\}$.

Последнее условие называется условием сохранения потока, в промежуточных вершинах потоки не создаются и не исчезают.

Величина $\Delta(x_i, x_j) = c(x_i, x_j) - \varphi(x_i, x_j)$ называется остаточной пропускной способностью дуги (x_i, x_j). Если $\varphi(x_i, x_j) = c(x_i, x_j)$, то дуга называется насыщенной.

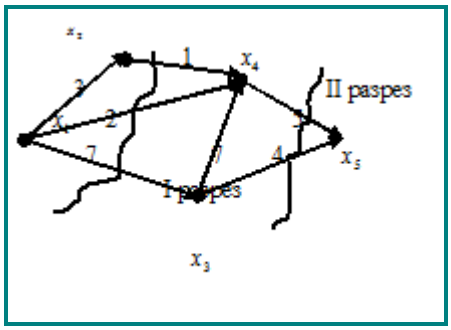
Максимальный поток определяется с помощью одного из основных понятий теории сетей – разреза. Разрез может быть определен как множество дуг, исключение которых из сети отделило бы некоторое множество узлов от остальной сети. Предположим, что множество вершин сети S разбито на два непустых непересекающихся подмножества $S = S' \cup S''$ и $S' \cap S'' = \varnothing$.

Множество дуг, начала которых лежат в S', а концы в S'', называется ориентированным разрезом и обозначается $(S' \to S'')$. Следовательно,

$$(S' \to S'') = \left\{ (x_i, x_j) \;\middle/\; x_i \in S',\ x_j \in S'' \right\}.$$

Пропускной способностью или величиной разреза $(S' \to S'')$ называется сумма пропускных способностей входящих в него дуг, то есть

$$c(S' \to S'') = \sum_{x_i \in S',\, x_j \in S''} c(x_i, x_j).$$



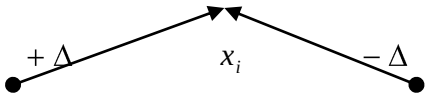
На рисунке слева изображена сеть, на которой около каждого ребра указана его пропускная способность. Произведены два разреза: I и II. При разрезе I вершины оказались разбиты на подмножества $S' = (x_1, x_2)$ и $S'' = (x_3, x_4, x_5)$, а ребрами, образующими разрез стали ребра $(x_1, x_3), (x_1, x_4), (x_2, x_4)$. При разрезе II $S' = (x_1, x_2, x_3, x_4)$, а $S'' = (x_5)$, разрез образуют ребра $(x_3, x_5), (x_4, x_5)$.

Теорема Форда* – Фалкерсона. *Для любой сети с одним источником и одним стоком величина максимального потока в сети от источника к стоку равна величине минимального разреза.*

Алгоритм Форда – Фалкерсона построения максимального потока и минимального разреза основан на следующих обстоятельствах.

1. Предположим, что в сети имеется некоторый поток и путь из s в t, состоящий из ненасыщенных дуг. Тогда очевидно, что поток в сети можно увеличить на величину Δ, равную минимальной из остаточных пропускных способностей дуг, входящих в этот путь. Перебирая все возможные пути из s в t и проводя такую процедуру увеличения потока, пока это возможно, получим в результате полный поток, то есть такой поток, для которого каждый путь из s в t содержит по крайней мере одну насыщенную дугу.

2. Рассмотрим произвольный маршрут (неориентированный путь) из s в t. Дуги, образующие этот маршрут, естественным образом делятся на два типа: прямые (ориентированные от s к t) и обратные (ориентированные от t к s). Пусть существует путь, в котором прямые дуги не насыщены, а потоки на обратных дугах положительны. Пусть Δ_1 - минимальная из остаточных пропускных способностей прямых дуг, а Δ_2 - минимальная из величин потоков обратных дуг. Тогда поток в сети можно увеличить на величину $\Delta = \min(\Delta_1, \Delta_2)$, прибавляя Δ к потокам на прямых дугах и вычитая Δ из потоков на обратных дугах. Очевидно, что при этом условие баланса (условие сохранения потока) $\sum_{x_j \in S_{np}(x_i)} \varphi(x_i, x_j) = \sum_{x_j \in S_{cn}(x_i)} \varphi(x_i, x_j)$ для узлов, входящих в рассматриваемый маршрут, не нарушится.



Ясно, что если множество обратных дуг не пусто, то при такой процедуре увеличения потока в сети фактического перемещения объектов вдоль рассматриваемого маршрута не происходит, так как оно в принципе

невозможно.

Однако эта процедура уменьшает потоки на некоторых дугах, которые, возможно, были перед этим насыщенными, образуя таким образом новые пути из ненасыщенных дуг, вдоль которых и происходит фактическое перемещение потока величины Δ.

Ясно также, что первая процедура является частным случаем второй.

Сетевое планирование. Критический путь и критическое время сетевого графа (Критические пути, работы, резервы.

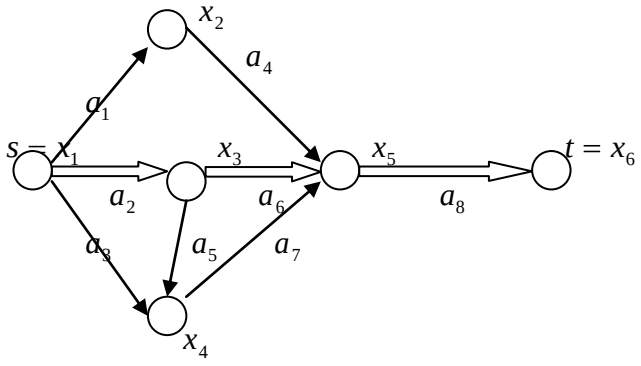
При планировании и управлении сложными комплексами работ используются их графические модели – сетевые графики. С математической точки зрения сетевой график – это связный орграф без петель и контуров. Основными понятиями сетевого планирования являются понятия работы и события.

Работа – это любые действия, сопровождающиеся затратами ресурсов и времени и приводящие к определенным результатам. Событие – это результат завершения одной или нескольких работ. Событие является предпосылкой для выполнения работ, следующих за ним. Любая работа на сети может быть определена двумя событиями, между которыми она находится. Событием может начинаться или заканчиваться несколько работ. Работы на сети изображают дугами, а события – вершинами сети.

Сетевой график обладает рядом особенностей, в частности он имеет только одно исходное событие (исток сети) и только одно завершающее событие – окончание всех работ. Рассмотрим пример построения сети по таблице последовательности работ.

Последовательность работ		
Исходная Работа	Опирается на работу	Продолжительность работ
a_1	-	3
a_2	-	6
a_3	-	4
a_4	a_1	5
a_5	a_2	1
a_6	a_2	9
a_7	a_3, a_5	6
a_8	a_4, a_6, a_7	8

Работы a_1, a_2 и a_3 не имеют предшествующих, поэтому реализация проекта начинается с этих работ, и изобразятся они дугами, выходящими из одной вершины – события x_1. Работе a_4 предшествует работа a_1, поэтому дуга a_4 на сети изображена вслед за дугой a_1.То же самое с дугами a_5 и a_6. Далее надо изобразить дуги a_7 и a_8. Работа a_7 опирается на работы a_3 и a_5. Итоговая работа a_8 опирается на a_4, a_6 и a_7. На рисунках



сети не рекомендуется во избежание путаницы изображать одновременно выполняемые работы параллельными дугами. Однако можно вводить дополнительные события и фиктивные работы (нулевой продолжительности), которые изображаются штриховыми линиями. Если бы, к примеру, работа a_5 опиралась бы еще на a_1, то между событиями x_2 и x_3 пришлось бы ввести штриховую дугу.

Имея сеть работ некоторого проекта можно посчитать время выполнения всего проекта и различных его частей, состоящих из разного набора работ. Для этого введем еще несколько определений. Определим сначала минимальное время, за которое можно выполнить все работы комплекса. Для этого найдем продолжительность $t(\mu_i)$ всех полных путей μ_i. В нашем случае таких путей четыре: $\mu_1: 1-2-5-6$; $\mu_2: 1-3-5-6$; $\mu_3: 1-4-5-6$; $\mu_4: 1-3-4-5-6$. Их продолжительности $t(\mu_1)=16$, $t(\mu_2)=23$, $t(\mu_3)=18$, $t(\mu_4)=21$. Наиболее продолжителен второй путь. Такой путь называют критическим. Этот путь определяет минимальное время выполнения всех работ комплекса. Минимальное время называют критическим сроком и обозначают $t_{кр.}$. Итак, в рассматриваемом примере $t_{кр.}=23$.

Все работы и события, лежащие на критическом пути, называют критическими, все остальные работы и события – некритическими. Задержка любой критической работы вызывает задержку выполнения всего комплекса. Следовательно, чтобы уменьшить время выполнения комплекса работ, надо сократить сроки критических работ. Некритические работы допускают некоторое запаздывание их выполнения без нарушения критического срока. Это запаздывание измеряется резервом времени событий и работ.

Свершением события называется момент, к которому заканчиваются все входящие в него работы и может быть начата любая выходящая работа. Некоторые события можно совершать в разные моменты, то есть варьировать свершение этих событий. Например, событие x_2 может свершиться через три дня (по окончании работы a_1), но может наступить и позже на срок до семи дней, поскольку на пути μ_1, где лежит это событие, есть резерв времени $t_{кр.}-t(\mu_1)=23-16=7$ дней. Поэтому для событий различают ранний и поздний сроки свершения.

Ранним сроком $t_p(x_j)$ свершения события x_j называется самый ранний момент времени, к которому завершатся все работы, предшествующие этому событию. Ранние сроки для всех событий могут быть рассчитаны по формуле

$$t_p(x_j)=\max_{(x_i,x_j)\in U_j^+}\left(t_p(x_i)+t(x_i,x_j)\right),$$

где U_j^+ - множество работ, входящих в x_j событие, $t_p(x_i)$ - ранний срок свершения начального события работы (x_i,x_j), $t(x_i,x_j)$ - продолжительность работы (x_i,x_j).

Поздним сроком $t_n(x_i)$ свершения события x_i называется самый поздний момент времени, после которого остается ровно столько времени, сколько необходимо для завершения всех работ, следующих за этим событием.

В нашем случае $t_n(x_6)=23$. Чтобы не нарушался критический срок, событие x_5 должно произойти в крайнем случае на восемь дней раньше, поэтому $t_n(x_5)=23-8=15$. Аналогично, $t_n(x_2)=15-5=10$. Таким образом, поздние сроки событий рассчитываются по формуле

$$t_n(x_i)=\min_{(x_i,x_j)\in U_i^-}\left(t_n(x_j)-t(x_i,x_j)\right),$$

где U_i^- - множество работ, выходящих из x_i события, $t_n(x_j)$ - поздний срок свершения конечного события работы (x_i,x_j).

Разности между поздним и ранним сроками свершения события x_i составляет *резерв времени* $R(x_i)$ *этого события* $R(x_i) = t_n(x_i) - t_p(x_i)$.

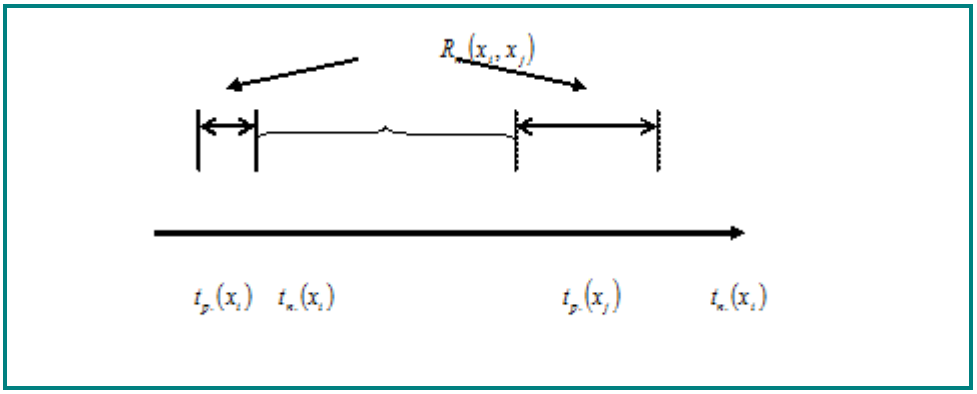
Резерв показывает, на какой предельно допустимый срок может задержаться свершение события x_i без изменения срока наступления итогового события t. У критических событий ранние и поздние сроки совершения совпадают, ибо резерв времени у них равен нулю. Зная сроки свершения событий, можно найти ранние и поздние сроки начала и окончания работы (x_i, x_j). Очевидно, что

$$\begin{cases} t_{p.н.}(x_i, x_j) = t_{p.}(x_i), t_{p.o.}(x_i, x_j) = t_{p.}(x_i) + t(x_i, x_j), \\ t_{n.o.}(x_i, x_j) = t_{n.}(x_j), t_{n.н.}(x_i, x_j) = t_{n.}(x_j) - t(x_i, x_j). \end{cases}$$

Для работ определяются два резерва времени. Полный резерв времени работы – это максимальное количество времени, на которое можно задержать начало работы или увеличить ее продолжительность, не нарушая критический срок

$$R_{n.}(x_i, x_j) = t_{n.}(x_j) - t_{p.}(x_i) - t(x_i, x_j).$$

Формулу (5.1.5) можно проиллюстрировать следующим рисунком.



Отдельные работы, помимо полного резерва, имеют свободный резерв времени, составляющий часть полного резерва, остающуюся после исключения резерва времени $R(x_j)$ конечного события x_j данной работы

$$R_{c.}(x_i, x_j) = t_{p.}(x_j) - t_{p.}(x_i) - t(x_i, x_j).$$

Свободный резерв времени – это запас времени, на который можно отсрочить начало работы или увеличить ее продолжительность при условии, что она начнется в свой ранний срок и при этом ранние сроки начала последующих работ не изменятся. Понятно, что все резервы критических работ равны нулю.

1. 25 Лекция № 25 (2 часа).

Тема: «Нечёткие множества и операции над ними**»**

1.25.1 Вопросы лекции:

1. Нечёткие множества.
2. Операции над нечёткими множествами.

1.25.2 Краткое содержание вопросов:

1. Нечёткие множества.
2. Операции над нечёткими множествами.

Нечеткие множества

Основы моделирования интеллектуальной деятельности человека заложила работа профессора Калифорнийского университета Л.А.Заде «Fuzzy sets», появившаяся в 1965 году.

Заде расширил классическое канторовское понятие множества, допустив, что характеристическая функция (функция принадлежности элемента множеству) может принимать любое значение в промежутке [0,1], а не только 0 или 1. Такие множества были названы им нечеткими. Также он определил ряд операций над нечеткими множествами и предложил обобщение известных методов логического вывода.

В классической математике рассматривается понятие четких множеств.

Например: рассмотрим множество *U* всех чисел от 0 до 10, которое называется универсальным (или универсумом рассуждения). Если определить подмножество *A* множества *U* всех действительных чисел от 5 до 8, то это множество можно описать классической характеристической функцией I_A (рис.1.1). Эта функция ставит в соответствие число 1 или 0 каждому элементу *U*, в зависимости от того, принадлежит данный элемент подмножеству *A* или нет.

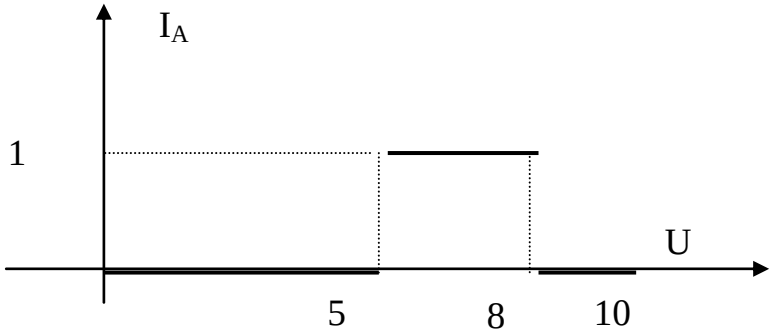


Рис.1.1

Таким образом, элементы, кото ие 1 интерпретируются как элементы находящиеся во множестве А, а элементы, которым поставлен в соответствие 0 – как элементы, не находящиеся во множестве А.

Легко можно обнаружить ситуации, в которых данной концепции будет недоставать гибкости. Рассмотрим ситуацию со степенью принадлежности скорости автомобиля к категории низкой. Если B={низкие скорости автомобиля}, скорости начинаются с 0, то нижний предел этого множества должен быть нулем. Верхний предел определим условно 40 км/ч. Следовательно, получаем B как четко ограниченный интервал B=[0,40]. Возникает вопрос: почему скорость в 40 км/ч низкая, в 40,5 км/ч уже нет? Это структурная проблема и верхнюю границу понятия нижней скорости можно задавать другим числом.

Поэтому более естественный путь получения множества B состоит в ослаблении строгого разделения на низкую и не низкую скорости. Это можно сделать, применив не только четкие суждения: «ДА, эта скорость принадлежит множеству низких скоростей», или «НЕТ, она не принадлежит множеству низких скоростей»; но и более гибкие формулировки: «ДА, она принадлежит к достаточно низким скоростям», или «НЕТ, она не очень низкая», то есть использовав принципы теории нечетких множеств.

В первом примере все элементы универсума рассуждения кодировались с помощью 0 или 1. С точки зрения теории нечетких множеств необходимо ввести значения между 0 и 1. Реально допускается бесконечное число значений между 0 и 1. Тогда интерпретация чисел при соотнесении всех элементов универсума рассуждений становится более сложной. Конечно, число 1 снова ставится в соответствие тому элементу, который принадлежит множеству B, а 0 означает, что элемент точно не принадлежит множеству B, но все

другие значения из интервала [0,1] определяют степень принадлежности элемента множеству B.

Характеристическая функция низких скоростей может выглядеть следующим образом (рис.1.2.):

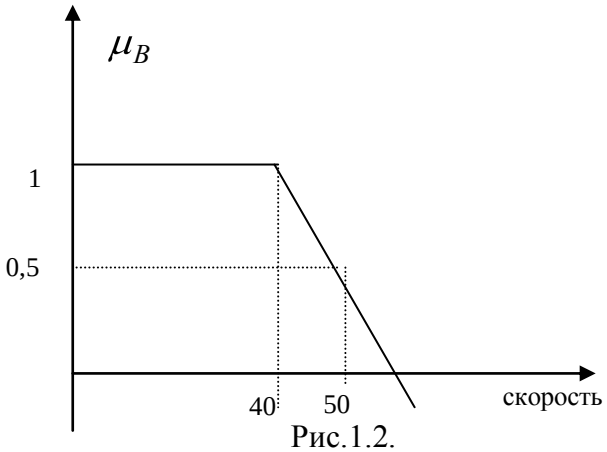


Рис.1.2.

Тогда скорость 50 км/ч все еще можно считать низкой со степенью 0,5.

Понятие нечеткого множества

Дадим строгое определение понятия нечеткого подмножества, введенного Заде. Пусть ***U*** есть множество, счетное или нет, и *x* – элемент ***U***. Тогда *нечетким подмножеством* $\underline{A}$ множества ***U*** называется множество упорядоченных пар

$$\{\mu_{\underline{A}}(x)\}\forall x \in U \qquad (1.1)$$

где $\mu_{\underline{A}}(x)$ – функция принадлежности *x* в $\underline{A}$; $\mu_{\underline{A}}(x) : \mathrm{U} \to [0;1]$, которая ставит в соответствие каждому элементу *x* число $\mu_{\underline{A}}(x)$ из интервала [0;1], характеризующая степень принадлежности элемента *x* подмножеству $\underline{A}$.

Носителем нечеткого множества $\underline{A}$ называется множество таких точек в ***U***, для которых величина $\mu_{\underline{A}}(x)$ положительна.

Высотой нечеткого множества $\underline{A}$ называется величина $\sup_x \mu_{\underline{A}}(x)$.

Точкой перехода нечеткого множества $\underline{A}$ называется такой элемент множества ***U***, степень принадлежности которого множеству $\underline{A}$ равна 0.5.

Нечеткое подмножество $\underline{A}$ универсального множества ***U*** записывается следующим образом

$$\underline{A} = \mu_1/x_1 + \mu_2/x_2 + ... + \mu_n/x_n ,$$

или $\underline{A} = \sum_{i=1}^{n} \mu_i/x_i$,

где μ_{i} – степень принадлежности элемента x_i нечеткому множеству $\underline{A}$, а знак + обозначает объединение, а не арифметическое суммирование.

Если носитель нечеткого множества $\underline{A}$ имеет мощность континуума, то используется следующая запись

$$\underline{A} = \int_E \mu_{\underline{A}}(x)/x,$$

где $\mu_{\underline{A}}(x)$ – степень принадлежности элемента *x* множеству $\underline{A}$, а знак $\int$ обозначает объединение нечетких одноточечных множеств $\mu_{\underline{A}}(x)/x, x \in U$.

Примеры:

1. Универсальное множество ***U*** представляет собой множество чисел [0,…,10]. Его нечеткое подмножество $\underline{A}$, обозначаемое словом «несколько», можно определить следующим образом $\underline{A} = \{0{,}5/4; 0{,}8/5; 1/6; 1/7; 0{,}8/8; 0{,}5/9\}$, а нечеткое подмножество $\underline{B}$, обозначаемое словом «мало» – $\underline{B} = \{1/1; 0{,}8/2; 0{,}5/3; 0{,}3/4; 0{,}1/5\}$

2. Рассмотрим конечное множество $U = \{a, b, c, d, e, f\}$ и конечное упорядоченное множество $M = \{0; 0{,}5; 1\}$. Тогда нечетким подмножеством множества ***U*** может быть $\underline{A} = \{0/a; 1/b; 0{,}5/c; 0/d; 0{,}5/e; 0/f\}$.

Можно записать $a \underset{0}{\in} \underline{A}, b \underset{1}{\in} \underline{A}, c \underset{0{,}5}{\in} \underline{A}, \ldots$

Нечеткое множество $\underline{A}$ *нормально*, если его высота равна единице, т.е. $\sup_x \mu_{\underline{A}}(x) = 1$.

В противном случае нечеткое множество *субнормально*.

Субнормальное нечеткое множество можно нормировать, поделив функцию $\mu_{\underline{A}}(x)$ на величину $\sup_x \mu_{\underline{A}}(x)$.

Простейшие операции над нечеткими подмножествами

Включение

Пусть ***U*** – множество, ***M*** – множество принадлежностей и $\underline{A}$ и $\underline{B}$ – два нечетких подмножества ***U***. $\underline{A}$ *содержится* в $\underline{B}$, если

$$\forall x \in U : \mu_{\underline{A}}(x) \le \mu_{\underline{B}}(x) \tag{3.2}$$

что обозначается $\underline{A} \subset \underline{B}$ или $\underline{A} \subseteq \underline{B}$.

Строгое включение соответствует случаю, когда в (1.2) неравенство строгое и обозначается $\underline{A} \subset\subset \underline{B}$ или $\underline{A} \subseteq\subseteq \underline{B}$.

Примеры:

1. Пусть $U = \{x1, x2, x3, x4\}$, $M = [0,1]$

$\underline{A} = \{(x1|0,4), (x2|0,2), (x3|0), (x4|1)\}$ $\underline{B} = \{(x1|0,3), (x2|0), (x3|0), (x4|0)\}$.

Имеем $\underline{B} \subset \underline{A}$, так как $0,3 < 0,4, 0 < 0,2, 0 = 0,0 < 1$.

Пусть $\forall x \in U : \mu_{\underline{A}}(x) = \mu_{\underline{B}}(x)$, то $\underline{B} \subset \underline{A}$.

Равенство

Пусть **U** – множество, ***M*** – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U.** $\underline{A}$ и $\underline{B}$ *равны* тогда и только тогда, когда

$$\forall x \in U : \mu_{\underline{A}}(x) = \mu_{\underline{B}}(x), \tag{1.3}$$

что обозначается $\underline{A} = \underline{B}$.

Если найдется по крайней мере один такой элемент *x* из **U,** что равенство $\mu_{\underline{A}}(x) = \mu_{\underline{B}}(x)$ не удовлетворяется, то говорят, что $\underline{A}$ и $\underline{B}$ не равны, и обозначают $\underline{A} \neq \underline{B}$.

Дополнение

Пусть **U** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U;** $\underline{A}$ и $\underline{B}$ *дополняют* друг друга, если

$$\forall x \in U : \mu_{\underline{B}}(x) = 1 - \mu_{\underline{A}}(x) \tag{1.4}$$

Это обозначается $\overline{\underline{A}} = \underline{B}$ или $\underline{B} = \overline{\underline{A}}$.

Очевидно, что всегда $\overline{(\overline{\underline{A}})} = \underline{A}$. Здесь дополнение определено для $M = [0,1]$, но его можно распространить на другие упорядоченные множества ***M***.

Пересечение

Пусть **U** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U;** *пересечение* $\underline{A} \cap \underline{B}$ определяют как наибольшее нечеткое подмножество, содержащееся одновременно в $\underline{A}$ и $\underline{B}$:

$$\forall x \in U : \mu_{\underline{A} \cap \underline{B}}(x) = MIN(\mu_{\underline{A}}(x), \mu_{\underline{B}}(x)) \tag{1.5}$$

Пример:

$U = \{x1, x2, x3, x4, x5\}, M = [0,1]$

$\underline{A} = \{(x1|0,2), (x2|0,7), (x3|1), (x4|0), (x5|0,5)\}$

$\underline{B} = \{(x1|0,5), (x2|0,3), (x3|1), (x4|0,1), (x5|0,5)\}$

$\underline{A} \cap \underline{B} = \{(x1|0,2), (x2|0,3), (x3|1), (x4|0), (x5|0,5)\}$.

Кроме того, используя общее определение (1.5), можно записать

$$\forall x \in U : x \underset{\mu_{\underline{A}}}{\in} \underline{A} \text{ и } x \underset{\mu_{\underline{B}}}{\in} \underline{B} \Rightarrow x \underset{\mu_{\underline{A} \cap \underline{B}}}{\in} \underline{A} \cap \underline{B}$$

Объединение

Пусть **U** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U;** определим *объединение* $\underline{A} \cup \underline{B}$ как наименьшее нечеткое подмножество, которое содержит как $\underline{A}$, так и $\underline{B}$:

$$\forall x \in U : \mu_{\underline{A} \cup \underline{B}}(x) = MAX(\mu_{\underline{A}}(x), \mu_{\underline{B}}(x)) \tag{1.6}$$

Пример: Вернувшись к примеру п.1.2.4, получим

$$\underline{A} \cup \underline{B} = \{(x1|0,5), (x27), (x3|1), (x4|0), (x5|0,5)\}$$

Кроме того, в соответствии с общим определением (1.6) можно записать

$$\forall x \in U : x \underset{\mu_{\underline{A}}}{\in} \underline{A} \text{ и } x \underset{\mu_{\underline{B}}}{\in} \underline{B} \Rightarrow x \underset{\mu_{\underline{A} \cup \underline{B}}}{\in} \underline{A} \cup \underline{B}$$

Свойства операций над нечеткими подмножествами

Если $\underline{A}, \underline{B}, \underline{C}$ – нечеткие подмножества универсального множества **U**, то удовлетворяются следующие свойства обычных множеств.

Коммутативность
$$\underline{A} \cap \underline{B} = \underline{B} \cap \underline{A}$$
$$\underline{A} \cup \underline{B} = \underline{B} \cup \underline{A},$$

Ассоциативность
$$(\underline{A} \cap \underline{B}) \cap \underline{C} = \underline{A} \cap (\underline{B} \cap \underline{C})$$
$$(\underline{A} \cup \underline{B}) \cup \underline{C} = \underline{A} \cup (\underline{B} \cup \underline{C}),$$

Идемпотентность $\underline{A} \cap \underline{A} = \underline{A}$, $\underline{A} \cup \underline{A} = \underline{A}$,

Дистрибутивность $\underline{A} \cap (\underline{B} \cup \underline{C}) = (\underline{A} \cap \underline{B}) \cup (\underline{A} \cap \underline{C})$, $\underline{A} \cup (\underline{B} \cap \underline{C}) = (\underline{A} \cup \underline{B}) \cap (\underline{A} \cup \underline{C})$,

Законы констант $\underline{A} \cap \varnothing = \varnothing$ $\quad \underline{A} \cap U = \underline{A}$, $\underline{A} \cup \varnothing = \underline{A}$ $\quad \underline{A} \cup U = U$,

Инволюция $\overline{(\underline{A})} = \underline{A}$

Теоремы Де Моргана $\overline{\underline{A} \cap \underline{B}} = \overline{\underline{A}} \cup \overline{\underline{B}}$, $\overline{\underline{A} \cup \underline{B}} = \overline{\underline{A}} \cap \overline{\underline{B}}$.

Алгебраическое произведение и сумма нечетких подмножеств

Следует иметь в виду, что $\cup (\max)$ *и* $\cap (\min)$ *– не единственные операции, с помощью которых можно определить операции объединения и пересечения.*

Если операция $\cap$ *определяется с помощью операции* min*, то она является «жесткой», в том смысле, что в ней недостаточно учитываются функции принадлежности обоих множеств.*

Пусть ***U*** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества ***U.***

Алгебраическое произведение $\underline{A}$ и $\underline{B}$ обозначается $\underline{A} \cdot \underline{B}$ и определяется следующим образом:

$$\forall x \in U : \mu_{\underline{A} \cdot \underline{B}}(x) = \mu_{\underline{A}}(x) \cdot \mu_{\underline{B}}(x) \qquad (1.8)$$

Алгебраическая сумма этих двух подмножеств обозначается $\underline{A} + \underline{B}$ и определяется следующим образом:

$$\forall x \in U : \mu_{\underline{A} + \underline{B}}(x) = \mu_{\underline{A}}(x) + \mu_{\underline{B}}(x) - \mu_{\underline{A}}(x) \cdot \mu_{\underline{B}}(x) \qquad (1.9)$$

Пример: При $\underline{A} = \{x_1 \mid 0{,}2;\ x_2 \mid 0{,}7;\ x_3 \mid 1;\ x_4 \mid 0;\ x_5 \mid 0{,}5\}$,

и $\underline{B} = \{x_1 \mid 0{,}5;\ x_2 \mid 0{,}3;\ x_3 \mid 1;\ x_4 \mid 0{,}1;\ x_5 \mid 0{,}5\}$.

$\underline{A} \cdot \underline{B} = \{x_1 \mid 0{,}10;\ x_2 \mid 0{,}21;\ x_3 \mid 1;\ x_4 \mid 0;\ x_5 \mid 0{,}25\}$.

$\underline{A} + \underline{B} = \{x_1 \mid 0{,}60\}, \{x_2 \mid 0{,}79\}, \{x_3 \mid 1\}, \{x_4 \mid 0{,}1\}, \{x_5 \mid 0{,}75\}$

Если $M = \{0,1\}$, т. е. в случае обычных подмножеств, имеем

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

Для двух указанных операций $\cdot$ и $+$ на множестве всех нечетких подмножеств справедливы только следующие свойства:

Коммутативность
$$\underline{A} \cdot \underline{B} = \underline{B} \cdot \underline{A}$$
$$\underline{A} + \underline{B} = \underline{B} + \underline{A}$$

Ассоциативность
$$(\underline{A} \cdot \underline{B}) \cdot \underline{C} = \underline{A} \cdot (\underline{B} \cdot \underline{C})$$
$$(\underline{A} + \underline{B}) + \underline{C} = \underline{A} + (\underline{B} + \underline{C})$$

Законы констант
$$\underline{A} \cdot \varnothing = \varnothing \qquad \underline{A} \cdot U = \underline{A}$$
$$\underline{A} + \varnothing = \underline{A} \qquad \underline{A} + U = U,$$

Инволюция
$$\overline{(\underline{A})} = \underline{A},$$

Теоремы Де Моргана
$$\overline{\underline{A} \cdot \underline{B}} = \overline{\underline{A}} + \overline{\underline{B}}$$
$$\overline{\underline{A} + \underline{B}} = \overline{\underline{A}} \cdot \overline{\underline{B}}.$$

Операции $\cup$ и $\cap$ не дистрибутивны относительно $\cdot$ или $+$ однако

$$\underline{A} \cdot (\underline{B} \cup \underline{C}) = (\underline{A} \cdot \underline{B}) \cup (\underline{A} \cdot \underline{C})$$
$$\underline{A} \cdot (\underline{B} \cap \underline{C}) = (\underline{A} \cdot \underline{B}) \cap (\underline{A} \cdot \underline{C}),$$

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

На основании (1.8) любое нечеткое множество $\underline{A}^{\alpha}$, где α – положительное число, можно определить как множество $\forall x \in U : \mu_{\underline{A}^{\alpha}}(x) = \mu_{\underline{A}}^{\alpha}(x)$.

Частными случаями операции возведения в степень являются операция концентрирования $CON(\underline{A}) = \underline{A}^2$ и операция растяжения $DIL(\underline{A}) = \underline{A}^{0,5}$.

Дизъюнктивная сумма

Дизъюнктивная сумма двух нечетких подмножеств определяется в терминах объединений и пересечений следующим образом:

$$\underline{A} \oplus \underline{B} = (\underline{A} \cap \overline{\underline{B}}) \cup (\overline{\underline{A}} \cap \underline{B}) \qquad (1.7)$$

Пример: Рассмотрим пример, который иллюстрировал операции объединения и пересечения для $\underline{A} = \{x1|0,8\}, \{x2|0,3\}, \{x3|0\}, \{x4|1\}, \{x5|0,5\}$ *и*

$\overline{\underline{B}} = \{x1|0,5\}, \{x2|0,7\}, \{x3|0\}, \{x4|0,9\}, \{x5|0,5\}$, *тогда*

$\underline{A} \cap \underline{B} = \{x_1|0,5\}, \{x_2|0,3\}, \{x_3|0\}, \{x_4|0,1\}, \{x_5|0,5\}$, *а*

$\underline{A} \oplus \underline{B} = \{x_1|0,5\}, \{x_2|0,7\}, \{x_3|0\}, \{x_4|0,1\}, \{x_5|0,5\}$.

Разность

Разность определяется соотношением $\underline{A} - \underline{B} = \underline{A} \cap \overline{\underline{B}}$ (1.8)

Конечно, исключая частные случаи, $\underline{A} - \underline{B} \neq \overline{\underline{B}} - \underline{A}$.

1.5.3.10. Декартово произведение

Пусть $\underline{A}_1, \ldots, \underline{A}_n$ – нечеткие подмножества универсальных множеств $U_1, \ldots, U_n$ соответственно. *Декартово произведение* этих подмножеств обозначается

$\underline{A}_1 \times \underline{A}_2 \times \ldots \times \underline{A}_n$ и определяется как нечеткое подмножество множества

$U_1 \times U_2 \times \ldots \times U_n$ с функцией принадлежности

$$\mu_{\underline{A}_1 \times \ldots \times \underline{A}_n}(x_1, \ldots, x_n) = \mu_{\underline{A}_1}(x_1) \wedge \ldots \wedge \mu_{\underline{A}_n}(x_n). \qquad (1.9)$$

Пример:

Для $U_1 = U_2 = \{5,7\}$, $\underline{A}_1 = \{5|0,5\}, \{6|1\}, \{7|0,6\}$, $\underline{A}_2 = \{5|1\}, \{6|0,6\}$

$\underline{A}_1 \times \underline{A}_2 = \{(5,5)|0,5\}, \{(6,5)|1\}, \{(7,5)|0,6\}, \{(5,6)|0,5\}, \{(6,6)|0,6\}, \{(7,6)|0,6\}$.

1.5.4. Наглядное представление простейших операций с нечеткими подмножествами

Для нечетких подмножеств можно построить визуальное представление, родственное представлению обычных подмножеств (диаграмма Вьенна - Эйлера).

Рассмотрим прямоугольную систему координат, на оси ординат которой откладываются значения $\mu_{\underline{A}}(x)$, а на оси абсцисс в произвольном порядке расположены элементы

U. На рис. 1.2 принадлежность каждого элемента изображена его ординатой, заштрихованная часть наглядно изображает нечеткое подмножество $\underline{A} \subset U$.

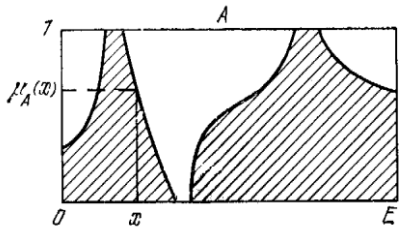


Рис. 1.2

Такое представление позволяет сделать зримыми простые операции на нечетких подмножествах.

1. 19 Лекция № 26 (2 часа).

Тема: «Нечёткие отношения и соответствия. Экспертные системы (в инт. форме)**»**

1.26.1 Вопросы лекции:

1. Нечёткие отношения и соответствия.
2. Экспертные системы.

1.26.2 Краткое содержание вопросов:

1. Нечёткие отношения и соответствия.
2. Экспертные системы.

Нечеткие отношения

Если ***U*** – декартово произведение *n* универсальных множеств $\boldsymbol{U}_1, \ldots, \boldsymbol{U}_n$, то *n*-арное нечеткое отношение *R* в ***U*** определяется как нечеткое подмножество универсального множества ***U***. *R* можно представить в форме объединения составляющих его нечетких одноточечных множеств.

Распространенными примерами (бинарных) нечетких отношений являются *много больше, имеет сходство, близко* и т.д.

Пример: Если *U* = 1+2+3+4, то отношение *много больше чем* можно определить матрицей отношений

R	1	2	3	4
1	0	0.3	0.8	1
2	0	0	0	0.8
3	0	0	0	0.3
4	0	0	0	0

Композиция нечетких отношений

Если *R* – отношение $U \to V$, а *S* – отношение $V \to W$, то *композицией R* и *S* называется нечеткое отношение $U \to W$, обозначаемое $R \circ S$ и определяемое формулой

$$R \circ S = \int_{U \times W} \bigvee_{V} \left(\mu_R (u, v) \wedge \mu_S (v, w) \right) (u, w) \quad (1.10)$$

Если *U, V* и *W* конечные множества, то матрица отношения $R \circ S$ есть максминное произведение матриц отношений и *R* и *S*.

Пример:

$$\begin{bmatrix} 0.3 & 0.8 \\ 0.6 & 0.9 \end{bmatrix}^{R} \circ \circ \begin{bmatrix} 0.5 & 0.9 \\ 0.4 & 1 \end{bmatrix}^{S} = \begin{bmatrix} 0.4 & 0.8 \\ 0.5 & 0.9 \end{bmatrix}^{R \circ S}.$$

1.5.2. Проекции

Если есть *R* *n*–арное нечеткое отношение в $U_1 \times U_2 \times \ldots \times U_n$, то его проекция на $U_{i1} \times \ldots \times U_{ik}$ есть *k*–арное нечеткое отношение R_q в *U*, которое определяется следующим образом

$$R_q = \int_{U_{i1} \times \ldots \times U_{ik}} \left(\bigvee_{u} \mu_R(u_1, \ldots, u_n) \right) / (u_{i1}, \ldots, u_{ik})$$

где q – последовательность индексов ; ; – дополнение; а

где верхняя грань берется по значениям всех тех , которые входят в .

Принцип обобщения

Принцип обобщения для нечетких множеств представляет собой основное равенство, позволяющее расширить область определения отображения ***U*** или отношения, включив в нее произвольные нечеткие подмножества множества ***U***.

Предположим, что *f* – отображение $U \to G$, а $\underline{A}$ – нечеткое подмножество вида $\underline{A} = x_1 \mid \mu_1, \ldots, x_n \mid \mu_n$. Тогда принцип обобщения утверждает, что $f(\underline{A}) = f(x_1) \mid \mu_1, \ldots, f(x_n) \mid \mu_n$. То есть, образ множества $\underline{A}$ при отображении *f* можно получить, зная образы элементов $x_1, \ldots, x_n$ при этом отображении.

Принцип обобщения аналогичен принципу суперпозиции для линейных систем.

Нечеткие переменные и нечеткая логика

Нечеткая переменная

Нечеткая переменная характеризуется тройкой $(X, U, R(X;u))$, где *X*– название переменной, *U* – универсальное множество (конечное или бесконечное), *u* – общее название элементов множества *U*, *R(X;u)* – нечеткое подмножество множества *U*, представляющее собой нечеткое ограничение на значения переменной *u*, обусловленное *X*. Неограниченная обычная (не нечеткая) переменная *u* является для *X базовой переменной*.

Уравнение назначения для *X* имеет вид $x = u : R(X)$ и отражает то, что элементу *x* назначается значение *u* с учетом ограничения $R(X)$.

Та степень, с которой удовлетворяется это равенство называется *совместимостью* значения *u* с $R(X)$ и обозначается $c(u)$.

По определению $c(u) = \mu_{R(X)}(u), u \in U$, где $\mu_{R(X)}(u)$ – степень принадлежности *u* ограничению $R(X)$.

Совместимость значения *u* это не вероятность значения *u*. Совместимость *u* с $R(X)$ – это лишь мера того, насколько значение *u* удовлетворяет ограничению $R(X)$; она не имеет никакого отношения к тому насколько вероятно или невероятно это значение.

Лингвистическая переменная

Лингвистическая переменная отличается от числовой переменной тем, что ее значениями являются не числа, а слова и предложения в естественном или формальном языке. Поскольку слова в общем смысле менее точны, чем числа, понятие лингвистической переменной дает возможность приближенно описывать явления, которые настолько сложны, что не поддаются описанию в общепринятых количественных терминах. В частности, нечеткое множество, представляющее собой ограничение, связанное со значениями лингвистической переменной, можно рассматривать как совокупную характеристику различных подклассов элементов универсального множества.

Лингвистическая переменная является переменной более высокого порядка, чем нечеткая переменная, в том смысле, что значениями лингвистической переменной являются нечеткие переменные.

Лингвистической переменной соответствуют два правила: *синтаксическое* правило, которое может быть задано в форме грамматики, порождающей названия значений переменной; *семантическое* правило, которое определяет алгоритмическую процедуру для вычисления смысла каждого значения. Эти правила составляют существенную часть описания структуры лингвистической переменной.

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.

3.2 Практическое занятие №ПЗ-2 (2 часа).

Тема: «Алгебра Буля»

3.2.1 Задание для работы:

1. Понятие об абстрактной алгебре Буля.
2. Понятие о моделях алгебры Буля.

3.1-2.2 Краткое описание проводимого занятия ПЗ-1 и ПЗ-2:

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.

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) $\pm 1, \pm 3, \pm 5, ...$ ..... $\{6n : n \in Z, n \ge 2\}$

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.

3.1-2.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия об основных операциях с множествами и алгебре множеств;
- приобрели умения и навыки выполнения операций в с множествами, построения бинарных отношений;

- освоили понятия об абстрактной алгебре Буля и о моделях алгебры Буля.

3.3 Практические занятия №ПЗ-3 (2 часа),
Тема: «Бинарные отношения и их свойства, способы задания отношений»

3.3.1 Задание для работы:
1. Способы задания отношений.
2.Свойства отношений.

3.4 Практическое занятие №ПЗ-4 (2 часа).
Тема: «Отношения эквивалентности»

3.4.1 Задание для работы:
1. Понятие отношения эквивалентности.
2. Отношения эквивалентности в математических и прикладных концепциях.

3.5 Практическое занятие №ПЗ-5 (2 часа).
Тема: «Отношения частичного порядка»

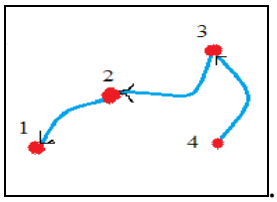
3.5.1 Задание для работы:
1.Отношения частичного порядка.

3.3-5.2 Краткое описание проводимых занятий ПЗ-3, ПЗ-4,ПЗ-5:

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.

$$R=\{\langle x,y\rangle : x=mq_1+r, y=mq_2+r, q_i\in Z, m\geq 0, m\in Z\}, m=3$$

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:

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

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.

3.3-5.3 Результаты и выводы: в результате проведенного занятия студенты:

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

3.6 Практическое занятие №ПЗ-6 (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. Функции

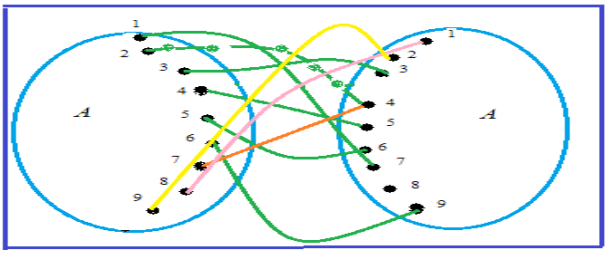
2. Классификация функций.

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 A , т.к. каждый элемент множества A 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.***

3.6.3 Результаты и выводы: В результате проведенного занятия студенты:

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

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

Тема: «Эквивалентные множества. Понятие мощности множеств, сравнение мощностей»

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>∈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. 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.***

3.7.3 Результаты и выводы: В результате проведенного занятия студенты:

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

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

Тема: «Счётные множества. Множества мощности континуум»

3.8.1 Задание для работы:

1. Счётные множества и их свойства.
2. Множества мощности континуум.

3.8.2 Краткое описание проводимого занятия:

1. Счётные множества и их свойства.
2. Множества мощности континуум.

Счётные множества. Мощность континуума.

1. Что можно утверждать относительно приведенных множеств (|*A*|=|*B*|, |*A*|<|*B*| или |*A*|>|*B*|)? Обосновать.

$A = 2,4,6,8,\ldots$, $B = \left\{ b \middle| b = \frac{2}{n}, n \in N \right\}$

Решение. Каждое из множеств А и В эквивалентно множеству натуральных чисел N. Поэтому $|A| = |B| = |N| = a$, т.е. множества A, B счётные и справедливо утверждение $|A| = |B|$.

3.8.3 Результаты и выводы: В результате проведенного занятия студенты:

- освоили понятия счётного множества, множества мощности континуум;
- приобрели умения и навыки идентифицировать счётные множества и множества мощности с.

3.9 Практическое занятие №ПЗ-9 (2 часа).
Тема: «Бинарные операции. Группы. Подстановки на множестве»

3.9.1 Задание для работы:
1. Бинарные операции. Полугруппы и группы.
2. Подстановки на множестве.

3.9.2 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.

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

6. Дать понятие о цикле.

Решение. Подстановка σ называется *циклом длины r*, если матрицу $[\sigma]$ 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 $1, 2, \dots, n$ образуют мультипликативную группу.

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

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

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

3.10.1 Задание для работы:

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

3.10.2 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

3.10.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили понятия кольца и поля;

- приобрели умения и навыки использования свойств кольца и поля.

3.11 Практическое занятие №ПЗ-11 (2 часа).
Тема: «Правила комбинаторики. Комбинаторные формулы»

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

3.11.2 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×(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 50×3=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).

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

3.12 Практическое занятие № ПЗ-12 (2 часа).
Тема: «Бином Ньютона. Биномиальные коэффициенты и их свойства»

3.12.1 Задание для работы:
1. Биномиальные коэффициенты и их свойства.
2. Метод включений и исключений. Метод рекуррентных соотношений.

3.12.2 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:

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

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

3.12.3 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.

3.13-14 Практическое занятие № ПЗ-13-14 (4 часа).
Тема: «Метод включений и исключений. Метод рекуррентных соотношений. Производящие функции»

3.13-14.1 Задание для работы:
1. Метод включений и исключений.
2. Метод рекуррентных соотношений.
3. Производящие функции

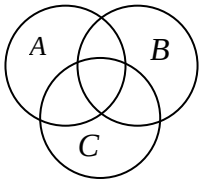
3.16-17.2 Краткое описание проводимых занятий ПЗ 16, ПЗ-17:
1. Метод включений и исключений.
2. Метод рекуррентных соотношений.
3. Производящие функции

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 исключе-

ния, позволяет вычислить мощность объединения произвольного количества множеств, если известны их мощности и мощности всех пересечений.

3.11-14.3 Результаты и выводы: В результате проведенного занятия студенты:
- 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.

3.15 Практическое занятие №ПЗ-15 (2 часа).
Тема: «Простые числа»

3.16-17.1 Задание для работы:
1. Простые числа.

3.16-17 Практическое занятие №ПЗ-16-17 (4 часа).
Тема: «Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным Решение сравнений первой степени**»**

3.16-17.1 Задание для работы:
1. Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным
2. Решение сравнений первой степени.

3.18-19 Практическое занятие №ПЗ-18-19 (4 часа).
Тема: «Порядок числа и класса вычетов по модулю. Первообразные корни. Индексы по простому модулю и их приложения**»**

3.18-19.1 Задание для работы:
1. Порядок числа и класса вычетов по модулю. Первообразные корни.
2. Индексы по простому модулю и их приложения.

3.20-21 Практическое занятие №ПЗ-20-21 (2 часа).
Тема: «Математические основы криптографии: приложения модульной арифметики в алгоритме RSA**»**

3.20-21.1 Задание для работы:
Математические основы криптографии: приложения модульной арифметики в алгоритме RSA

3.15, 16-21.2 Краткое описание проводимых занятий ПЗ 15, 16-213:

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.

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

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

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

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

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.

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

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

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

3.15, 16-21.3 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.

3.22-23 Практическое занятие №ПЗ-22-23 (2 часа).

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

3.22-23.1 Задание для работы:

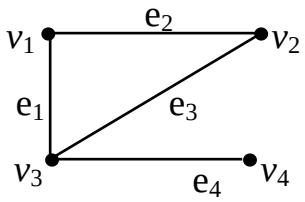
1. Основные понятия теории графов. Виды графов.
2. Операции над графами

3.22-231.2 Краткое описание проводимого занятия ПЗ-22, ПЗ-23:

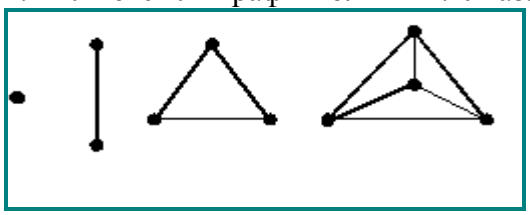
1. Основные понятия теории графов.
2. Виды графов.
3. Операции над графами.

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)ue_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 попарно 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.

3.20-21.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили основные понятия теории графов, виды графов, операции над графами;
- приобрели умения и навыки применять основные понятия теории графов, операции над графами.

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

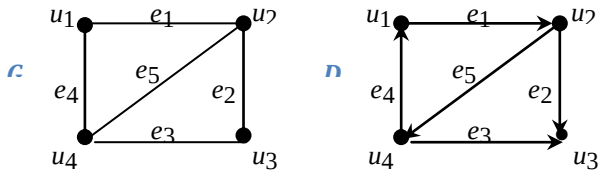
3.22.1 Задание для работы:

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

3.22-23.2 Краткое описание проводимого занятия ПЗ-22, ПЗ-23:

1. Способы задания графов. Матричное представление графов.

1. Составить матрицы смежности графов.

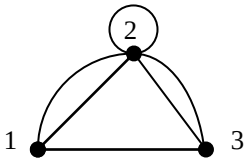


Решение. Матрицы смежности для заданных графа G и орграфа D

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

2. Найти матрицу смежности псевдографа.

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

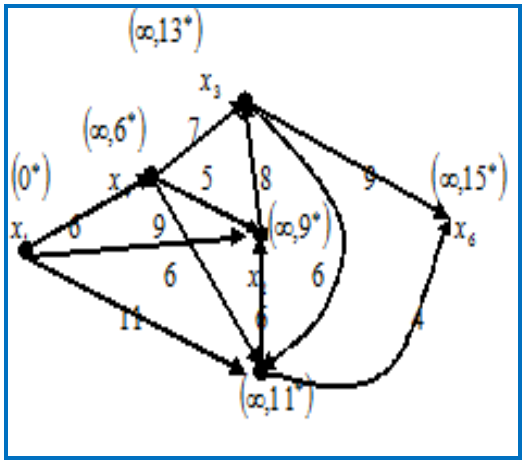


3. Найти матрицы инцидентности для заданных графа G и орграфа D

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

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

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

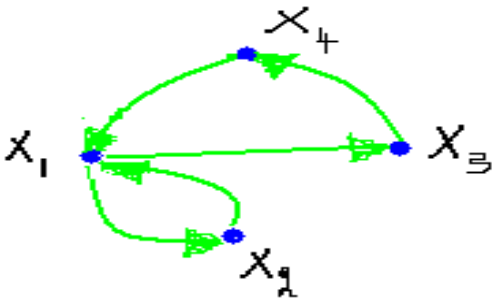


2. Числовые характеристики графов

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

3.22-23.3 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.

3.24 Практическое занятие № ПЗ-24 (2 часа).

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

3.24.1 Задание для работы:

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

3.24.2 Краткое описание проводимого занятия ПЗ-24:

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|.

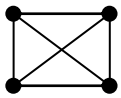
Расстоянием между вершинами u и *v* (обозначается *d*(*u*,*v*)) называется длина кратчайшей цепи $\langle u,v\rangle$, а сама кратчайшая цепь называется *геодезической*. Если не существует цепи, соединяющей вершины *u* и *v*, то по определению $d(u,v) = +\infty$.

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*.

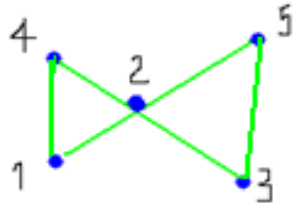
Вершина графа, удаление которой увеличивает число компонент связности, называется *разделяющей* или *точкой сочленения*.

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 та-

кой 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

3.24.3 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.

3.25-26 Практическое занятие №ПЗ-25-26 (4 часа).

Тема: «Деревья. Свойства деревьев»

3.25-26.1 Задание для работы:

1. Деревья.
2. Свойства деревьев.
3. Фундаментальная система циклов графа.

4. Понятие об остове наименьшего веса.
5. Отыскание остова наименьшего веса.

3.25-26.2 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. $d(S', S'') = \omega(x_4, x_5) = 4,\ S' = \{x_1, x_2, x_3, x_4, x_5\}, S'' = \{x_6\},$

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

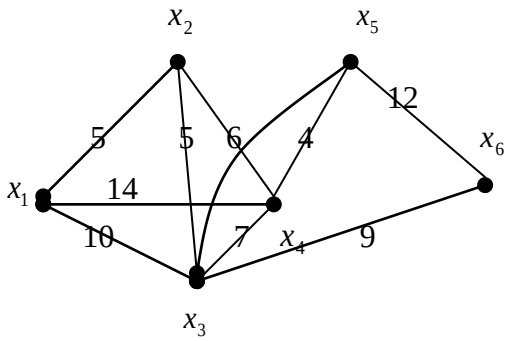
Шаг 3. $S' \neq S$, переход на начало второго шага.

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

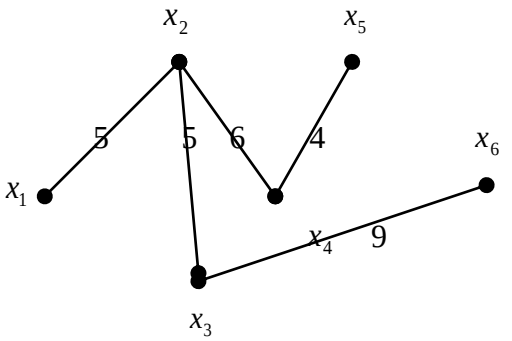
$U' = \{(x_1, x_2), (x_2, x_3), (x_2, x_4), (x_4, x_5), (x_3, x_6)\}$.

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



3.28-29.3 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.

3.27-28 Практическое занятие № ПЗ-27-28 (4 часа).
Тема: «Свойства эйлеровых и гамильтоновых графов».

3.27-28.1 Задание для работы:
1. Эйлеровы циклы в графах.
2. Свойства эйлеровых графов.
3. Понятие гамильтоновых циклов в графах.
4. Нахождение гамильтоновых циклов в графах.

3.27-28.2 Краткое описание проводимого занятия:
1. Эйлеровы циклы в графах.
2. Свойства эйлеровых графов.
3. Понятие гамильтоновых циклов в графах.
4. Нахождение гамильтоновых циклов в графах.

1. Найти Эйлерову цепь в неориентированном графе. Найти Эйлерову цепь в неориентированном графе G, изображенном на рисунке.
Решение. Прежде, чем приступать к нахождению Эйлеровой цепи, необходимо проверить степени вершин графа G − согласно утверждению 2, для существования Эйлеровой цепи, необходимо и достаточно, чтобы в графе G ровно 2 вершины нечетной степени.

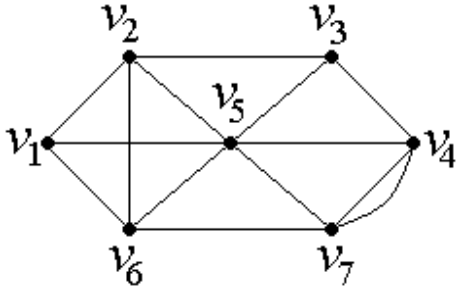


Рис. 1

В рассматриваемом графе нечетные степени имеют вершины v_3 и v_1 (степень этих вершин равна 3). Соединяя эти вершины фиктивным ребром так, как показано на рис. 2, получаем граф G':

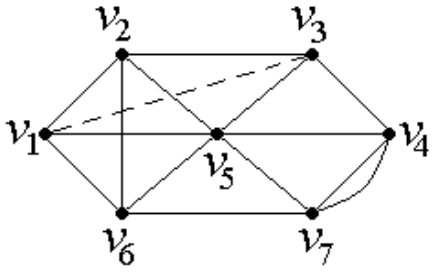


Рис. 2.

Поскольку в конечном итоге будет получена цепь, то очевидно, что началом и концом этой цепи будут вершины с нечетными степенями. Поэтому, следуя описанному выше алгоритму, будем циклы μ_i так, чтобы хотя бы один из них начинался или кончался на вершинах v_3 или v_1.

Пусть цикл μ_1 составят ребра, проходящие через следующие вершины: $v_3\ v_4\ v_7\ v_6\ v_1\ v_2\ v_3$. Согласно алгоритму, удаляем из G' все ребра, задействованные в цикле μ_1. Теперь граф G' будет таким, как показано на рис. 3.

Составляем следующий цикл μ_2: $v_4\ v_5\ v_6\ v_2\ v_5\ v_7\ v_4$. Граф G' после удаления ребер, составляющих цикл μ_2, изображен на рис. 4.

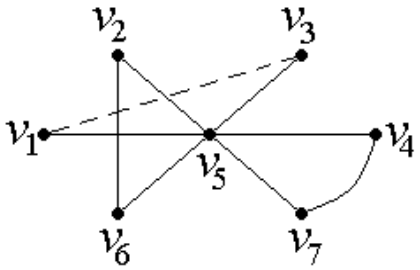


Рис.3

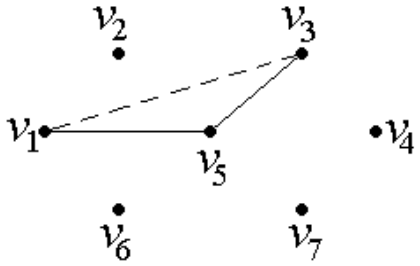


Рис. 4

Очевидно, что последний цикл μ_3 будет состоять из $v_3\ v_5\ v_1|v_3$, где последнее ребро, соединяющее вершины v_1 и v_3 – фиктивно. После удаления ребер, составляющих цикл μ_3, в графе G' не останется ни одного ребра.

Теперь по общим вершинам склеиваем полученные циклы. Поскольку μ_1 и μ_2 имеют общую вершину v_4, то, объединяя их, получим следующий цикл: $v_3\ v_4\ v_5\ v_6\ v_2\ v_5\ v_7\ v_4\ v_7\ v_6\ v_1\ v_2\ v_3$. Теперь склеим получившийся цикл с циклом μ_3: $v_3\ v_4\ v_5\ v_6\ v_2\ v_5\ v_7\ v_4\ v_7\ v_6\ v_1\ v_2\ v_3\ v_5\ v_1|v_3$. Удаляя фиктивное ребро, получаем искомую Эйлерову цепь: $v_3\ v_4\ v_5\ v_6\ v_2\ v_5\ v_7\ v_4\ v_7\ v_6\ v_1\ v_2\ v_3\ v_5\ v_1$.

Алгоритм выделения эйлерова цикла в связном мультиграфе с четными степенями вершин

1) Выделим из G цикл μ_1. (так как степени вершин четны, то висячие вершины отсутствуют). Положим l=1, G'=G.
2) Удаляем из G' ребра, принадлежащие выделенному циклу μ_1. Полученный псевдограф снова обозначаем как G'. Если в G' отсутствуют ребра, то переходим к шагу 4. Если ребра есть, то выделяем из G' цикл μ_{l+1} и переходим к шагу 3.
3) Присваиваем l:=l+1 и переходим к шагу 2.
4) По построению выделенные циклы содержат все ребра по одному разу. Если l:=1, то искомый Эйлеров цикл найден (конец работы алгоритма). В противном случае находим циклы, содержащие хотя бы по одной общей вершине (в силу связности графа это всегда можно сделать). Склеиваем эти циклы. Повторяем эти операции, пока не останется один цикл, который является искомым.

3.26-27.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили понятия маршрута, цикла, связности, обхода графа, эйлерова и гамильтонова цикла в графах;
- приобрели умения и навыки применять понятия маршрута, цикла, связности, обхода графа, эйлерова и гамильтонова цикла в графах, числовых характеристик графов при решении задач.

3.29-30 Практическое занятие №29-30 (2 часа).

Тема: «Планарность и укладка графов. Раскраска графов. Хроматическое число»

3.30.1 Задание для работы:

1. Понятие планарного графа.
2. Проблема укладки графов.
3. Проблема раскраски графов.
4. Хроматическое число.

3.30-31.2 Краткое описание проводимого занятия ПЗ-32. ПЗ-33:

1. Понятие планарного графа.
2. Проблема укладки графов.
3. Проблема раскраски графов.
4. Хроматическое число.

3.30-31.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия понятие планарного графа, проблемы укладки графов, проблемы раскраски графов, хроматического числа.

3.31-32 Практическое занятие № 31-32 (2 часа).

Тема: «Орграфы и сети. Прикладные задачи и алгоритмы анализа графов и сетей, задачи оптимизации на графах и сетях. ИТ - технологии анализа графов и сетей. (в инт. форме)»

3.31-32.1 Задание для работы:

1. Орграфы, Свойства орграфов.
2. Сети.
3. Задача о поиске экстремального пути.
4. Понятие потока в сети.
5. Понятие задачи об экстремальном потоке.

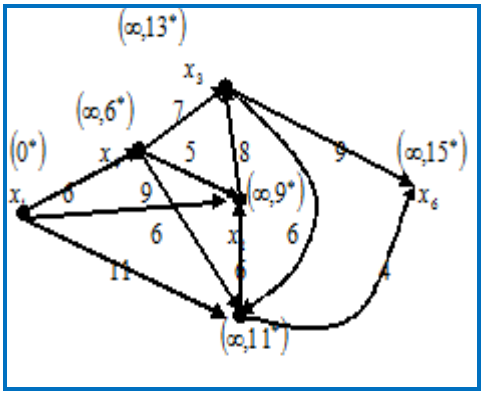
3.32-34.2 Краткое описание проводимого занятия ПЗ-31-32:

1. Сети.
2. Задача о поиске экстремального пути.
3. Понятие потока в сети.
4. Понятие задачи об экстремальном потоке.
5. Орграфы.Свойства орграфов.

Задание. Задана весовая матрица сети G. Найти минимальный путь из вершины x_1 в вершину x_6 по алгоритму Дейкстры.

Решение. Изобразим теперь сам граф по данной матрице весов.

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



Этап1. Шаг1. Полагаем $d(x_1) = 0^*, \tilde{x} = x_1, x_5$ $d(x_2) = d(x_3) = d(x_4) = d(x_5) = d(x_6) = \infty$.

1-я итерация. Шаг 2. Множество вершин, непосредственно следующих за $\tilde{x} = x_1$ с временными метками $\tilde{S} = \{x_2, x_4, x_5\}$. Пересчитываем временные метки этих вершин

$d(x_2) = \min\{\infty, 0^* + 9\} = 9$, $d(x_4) = \min\{\infty, 0^* + 6\} = 6$, $d(x_5) = \min\{\infty, 0^* + 11\} = 11$.

Шаг 3. Одна из временных меток превращается в постоянную $\min\{\infty, 6, 11, \infty\} = 6^* = d(x_4)$, $\tilde{x} = x_4$.

Шаг 4. $\tilde{x} = x_4 \neq t = x_6$, происходит возвращение на второй шаг.

2-я итерация. Шаг 2. $\tilde{S} = \{x_2, x_3, x_5\}$, $d(x_2) = \min\{9, 6^* + 5\} = 9$, $d(x_3) = \min\{\infty, 6^* + 7\} = 13$, $d(x_5) = \min\{11, 6^* + 6\} = 11$.

Шаг 3. $\min\{d(x_2), d(x_3), d(x_5), d(x_6)\} = \min\{9, 13, 11, \infty\} = 9^* = d(x_2)$, $\tilde{x} = x_2$.

Шаг 4. $x_2 \neq x_6$, возвращение на второй шаг.

3-я итерация. Шаг 2. $\tilde{S} = \{x_3\}$, $d(x_3) = \min\{13, 9^* + 8\} = 13$.

Шаг 3. . $\min\{d(x_3), d(x_5), d(x_6)\} = \min\{13, 11, \infty\} = 11^* = d(x_5)$, $\tilde{x} = x_5$.

Шаг 4. $x_5 \neq x_6$, возвращение на второй шаг.

4-я итерация. Шаг 2. $\tilde{S} = \{x_6\}$, $d(x_6) = \min\{\infty, 11^* + 4\} = 15$.

Шаг 3. . $\min\{d(x_3), d(x_6)\} = \min\{13, 15\} = 13^* = d(x_3)$, $\tilde{x} = x_3$.

Шаг 4. $x_3 \neq x_6$, возвращение на второй шаг.

5-я итерация. Шаг 2. $\tilde{S} = \{x_6\}$, $d(x_6) = \min\{15, 13^* + 9\} = 15$.

Шаг 3. $\min\{d(x_6)\} = \min\{15\} = 15^*$, $\tilde{x} = x_6$.

Шаг 4. $x_6 = t = x_6$, конец первого этапа.

Этап 2. Шаг5. Составим множество вершин, непосредственно предшествующих $\tilde{x} = x_6$ с постоянными метками $\tilde{S} = \{x_3, x_5\}$. Проверим для этих двух вершин выполнение равенства (4.7.3).

$d(\tilde{x}) = 15 = 11^* + 4 = d(x_5) + \omega(x_5, x_6)$, $d(\tilde{x}) = 15 \neq 13^* + 9 = d(x_3) + \omega(x_3, x_6)$. Включаем дугу (x_5, x_6) в кратчайший путь. $\tilde{x} = x_5$.

Шаг 6. $\tilde{x} \neq s = x_1$, возвращение на пятый шаг.

2-я итерация. Шаг 5. $\tilde{S} = \{x_1, x_4\}$.

$d(\tilde{x}) = 11 = 0^* + 11 = d(x_1) + \omega(x_1, x_5)$, $d(\tilde{x}) = 11 \neq 6^* + 6 = d(x_4) + \omega(x_4, x_5)$. Включаем дугу (x_1, x_5) в кратчайший путь. $\tilde{x} = x_1$.

Шаг 6. $\tilde{x} = s = x_1$, завершение второго этапа.

Итак, кратчайший путь от вершины x_1 до вершины x_6 построен. Его длина (вес) равна 15, сам путь образует следующая последовательность дуг $\mu = (x_1, x_5), (x_5, x_6)$.

2. Потоки в сетях. Задача о максимальном потоке.
Сетевое планирование. Критический путь и критическое время сетевого графа

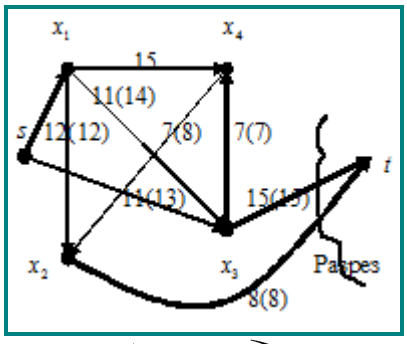
Задание. Пропускные способности дуг заданы следующей матрицей. Построить сеть, найти максимальный поток от s к t и указать минимальный разрез, отделяющий s от t.

Решение.

$$W = \begin{array}{c} \\ s \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ t \end{array} \begin{array}{c} \begin{array}{cccccc} s & x_1 & x_2 & x_3 & x_4 & t \end{array} \\ \begin{pmatrix} - & 12 & - & 13 & - & - \\ - & - & 11 & 14 & 15 & - \\ - & - & - & - & - & 8 \\ - & - & - & - & 7 & 15 \\ - & - & 8 & - & - & - \\ - & - & - & - & - & - \end{pmatrix} \end{array}.$$

Этап 1. Путь $s \xrightarrow{12} x_1 \xrightarrow{14} x_3 \xrightarrow{15} t.$

$\delta = \min(12, 14, 15) = 12.$ Увеличим по этому пути поток до 12 единиц, ребро (s, x_1) становится насыщенным. Поставим величину потока на дугах (x_1, x_3) и (x_3, t).



$\delta = \min(3, 15-12) = 3.$ Поток можно увеличить на три единицы. Дуга (x_3, t) станет насыщенной. Путь $s \xrightarrow{3(3)} x_3 \xrightarrow{7} x_4 \xrightarrow{8} x_2 \xrightarrow{8} t.$ Можно увеличить поток на семь единиц;

Дуга (x_3, x_4) станет насыщенной, потоки примут вид

$$s \xrightarrow{10(3)} x_3 \xrightarrow{7(\ )} x_4 \xrightarrow{7(\ )} x_2 \xrightarrow{7(\ )} t.$$

Больше путей нет. Конец первого этапа.

Этап 2. Рассмотрим теперь маршруты, содержащие противоположные дуги. Маршрут $s \xrightarrow{10(3)} x_3 \xleftarrow{12(4)} x_1 \xrightarrow{11} x_2 \xrightarrow{7(\ )} t.$ Поток можно увеличить на единицу на дуге (x_2, t). Тогда потоки по дугам этого маршрута станут такими $s \xrightarrow{11(3)} x_3 \xleftarrow{11(4)} x_1 \xrightarrow{1(1)} x_2 \xrightarrow{8(\ )} t.$ Дуга (x_2, t) стала насыщенной.

Больше маршрутов нет. Поток максимален. Делаем разрез вокруг t по насыщенным дугам и получаем его величину 15+8=23 единицы.

3.31-32.3 Результаты и выводы: в результате проведенного занятия студенты:

- освоили понятия об оптимизационных задачах на графах и сетях, алгоритмах их решения;
- приобрели умения и навыки решать оптимизационные задачи на графах и сетях.

3.33-34 Практическое занятие №ПЗ-33-34 (4 часа).

Тема: «Нечёткие множества и операции над ними »

3.33-34.1 Задание для работы:

1. Нечёткие множества.
2. Операции над нечёткими множествами.

3.33-34.2 Краткое описание проводимого занятия:

1. Нечёткие множества.
2. Операции над нечёткими множествами.

1. Универсальное множество ***U*** представляет собой множество чисел [0,…,10]. Его нечеткое подмножество $\underline{A}$, обозначаемое словом «несколько», можно определить следующим образом $\underline{A} = \{0{,}5/4, 0{,}8/5, 1/6, 1/7, 0{,}8/8, 0{,}5/9\}$, а нечеткое подмножество $\underline{B}$, обозначаемое словом «мало» – $\underline{B} = \{1/1, 0{,}8/2, 0{,}5/3, 0{,}3/4, 0{,}1/6\}$

2. Рассмотрим конечное множество $U = \{a, b, c, d, e, f\}$ и конечное упорядоченное множество $M = \{0; 0{,}5; 1\}$. Тогда нечетким подмножеством множества ***U*** может быть $\underline{A} = \{0/a, 1/b, 0{,}5/c, 0/d, 0{,}5/e, 0/f\}$.

Можно записать $a \underset{0}{\in} \underline{A}, b \underset{1}{\in} \underline{A}, c \underset{0{,}5}{\in} \underline{A}, \ldots$

Нечеткое множество $\underline{A}$ *нормально*, если его высота равна единице, т.е. $\sup\limits_{x} \mu_{\underline{A}}(x) = 1$.

В противном случае нечеткое множество *субнормально*.

Субнормальное нечеткое множество можно нормировать, поделив функцию $\mu_{\underline{A}}(x)$ на величину $\sup\limits_{x} \mu_{\underline{A}}(x)$.

Простейшие операции над нечеткими подмножествами

Включение

Пусть ***U*** – множество, ***M*** – множество принадлежностей и $\underline{A}$ и $\underline{B}$ – два нечетких подмножества ***U***. $\underline{A}$ *содержится* в $\underline{B}$, если

$$\forall x \in U : \mu_{\underline{A}}(x) \le \mu_{\underline{B}}(x) \tag{3.2}$$

что обозначается $\underline{A} \subset \underline{B}$ или $\underline{A} \subseteq \underline{B}$.

Строгое включение соответствует случаю, когда в (1.2) неравенство строгое и обозначается $\underline{A} \subset\subset \underline{B}$ или $\underline{A} \subseteq\subseteq \underline{B}$.

Примеры:

1. Пусть $U = \{x1, x2, x3, x4\}, M = [0,1]$
   $\underline{A} = \{0{,}4/x1, 0{,}2/x2, 0/x3, 1/x4\}$ $\underline{B} = \{0{,}3/x1, 0/x2, 0/x3, 0/x4\}$.
   Имеем $\underline{B} \subset \underline{A}$, так как $0{,}3 < 0{,}4, 0 < 0{,}2, 0 = 0{,}0 < 1$.

Пусть $\forall x \in U : \mu_{\underline{A}}(x) = \mu_{\underline{B}}(x)$, то $\underline{B} \subset \underline{A}$.

Равенство

Пусть ***U*** – множество, ***M*** – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества ***U***. $\underline{A}$ и $\underline{B}$ *равны* тогда и только тогда, когда

$$\forall x \in U : \mu_{\underline{A}}(x) = \mu_{\underline{B}}(x), \tag{1.3}$$

что обозначается $\underline{A} = \underline{B}$.

Если найдется по крайней мере один такой элемент x из **U,** что равенство $\mu_{\underline{A}}(x) = \mu_{\underline{B}}(x)$ не удовлетворяется, то говорят, что $\underline{A}$ и $\underline{B}$ не равны, и обозначают $\underline{A} \neq \underline{B}$.

Дополнение

Пусть **U** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U;** $\underline{A}$ и $\underline{B}$ *дополняют* друг друга, если

$$\forall x \in U : \mu_{\underline{B}}(x) = 1 - \mu_{\underline{A}}(x) \tag{1.4}$$

Это обозначается $\overline{\underline{A}} = \underline{B}$ или $\underline{B} = \overline{\underline{A}}$.

Очевидно, что всегда $(\overline{\underline{A}}) = \underline{A}$. Здесь дополнение определено для $M = [0,1]$, но его можно распространить на другие упорядоченные множества ***M***.

Пересечение

Пусть **U** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U;** *пересечение* $\underline{A} \cap \underline{B}$ определяют как наибольшее нечеткое подмножество, содержащееся одновременно в $\underline{A}$ и $\underline{B}$:

$$\forall x \in U : \mu_{\underline{A} \cap \underline{B}}(x) = MIN(\mu_{\underline{A}}(x), \mu_{\underline{B}}(x)) \tag{1.5}$$

Пример:

$U = \{x1, x2, x3, x4, x5\}, M = [0,1]$

$\underline{A} = \{(x1|0,2), (x2|0,7), (x3|1), (x4|0), (x5|0,5)\}$

$\underline{B} = \{(x1|0,5), (x2|0,3), (x3|1), (x4|0,1), (x5|0,5)\}$

$\underline{A} \cap \underline{B} = \{(x1|0,2), (x2|0,3), (x3|1), (x4|0), (x5|0,5)\}$.

Кроме того, используя общее определение (1.5), можно записать

$$\forall x \in U : x \underset{\mu_{\underline{A}}}{\in} \underline{A} \text{ и } x \underset{\mu_{\underline{B}}}{\in} \underline{B} \Rightarrow x \underset{\mu_{\underline{A} \cap \underline{B}}}{\in} \underline{A} \cap \underline{B}$$

Объединение

Пусть **U** – множество, $M = [0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U;** определим *объединение* $\underline{A} \cup \underline{B}$ как наименьшее нечеткое подмножество, которое содержит как $\underline{A}$, так и $\underline{B}$:

$$\forall x \in U : \mu_{\underline{A} \cup \underline{B}}(x) = MAX(\mu_{\underline{A}}(x), \mu_{\underline{B}}(x)) \tag{1.6}$$

Пример: Вернувшись к примеру п.1.2.4, получим

$$\underline{A} \cup \underline{B} = \{(x1|0,5), (x27), (x3|1), (x4|0), (x5|0,5)\}$$

Кроме того, в соответствии с общим определением (1.6) можно записать

$$\forall x \in U : x \underset{\mu_{\underline{A}}}{\in} \underline{A} \text{ и } x \underset{\mu_{\underline{B}}}{\in} \underline{B} \Rightarrow x \underset{\mu_{\underline{A} \cup \underline{B}}}{\in} \underline{A} \cup \underline{B}$$

Свойства операций над нечеткими подмножествами

Если $\underline{A},\underline{B},\underline{C}$ – нечеткие подмножества универсального множества **U**, то удовлетворяются следующие свойства обычных множеств.

Коммутативность
$$\underline{A}\cap\underline{B}=\underline{B}\cap\underline{A}$$
$$\underline{A}\cup\underline{B}=\underline{B}\cup\underline{A},$$

Ассоциативность
$$(\underline{A}\cap\underline{B})\cap\underline{C}=\underline{A}\cap(\underline{B}\cap\underline{C})$$
$$(\underline{A}\cup\underline{B})\cup\underline{C}=\underline{A}\cup(\underline{B}\cup\underline{C}),$$

Идемпотентность
$$\underline{A}\cap\underline{A}=\underline{A}$$
$$\underline{A}\cup\underline{A}=\underline{A},$$

Дистрибутивность
$$\underline{A}\cap(\underline{B}\cup\underline{C})=(\underline{A}\cap\underline{B})\cup(\underline{A}\cap\underline{C})$$
$$\underline{A}\cup(\underline{B}\cap\underline{C})=(\underline{A}\cup\underline{B})\cap(\underline{A}\cup\underline{C}),$$

Законы констант
$$\underline{A}\cap\varnothing=\varnothing \qquad \underline{A}\cap U=\underline{A}$$
$$\underline{A}\cup\varnothing=\underline{A} \qquad \underline{A}\cup U=U \quad ,$$

Инволюция
$$\overline{(\overline{\underline{A}})}=\underline{A}$$

Теоремы Де Моргана
$$\overline{\underline{A}\cap\underline{B}}=\overline{\underline{A}}\cup\overline{\underline{B}}$$
$$\overline{\underline{A}\cup\underline{B}}=\overline{\underline{A}}\cap\overline{\underline{B}}.$$

Алгебраическое произведение и сумма нечетких подмножеств

Следует иметь в виду, что $\cup(\max)$ *и* $\cap(\min)$ *– не единственные операции, с помощью которых можно определить операции объединения и пересечения.*

Если операция $\cap$ *определяется с помощью операции* min*, то она является «жесткой», в том смысле, что в ней недостаточно учитываются функции принадлежности обоих множеств.*

Пусть **U** – множество, $M=[0,1]$ – множество принадлежностей, $\underline{A}$ и $\underline{B}$ – два нечетких подмножества **U.**

Алгебраическое произведение $\underline{A}$ и $\underline{B}$ обозначается $\underline{A}\cdot\underline{B}$ и определяется следующим образом:

$$\forall x\in U:\mu_{\underline{A}\hat{\cdot}\underline{B}}(x)=\mu_{\underline{A}}(x)\cdot\mu_{\underline{B}}(x) \qquad (1.8)$$

Алгебраическая сумма этих двух подмножеств обозначается $\underline{A}+\underline{B}$ и определяется следующим образом:

$$\forall x\in U:\mu_{\underline{A}\hat{+}\underline{B}}(x)=\mu_{\underline{A}}(x)+\mu_{\underline{B}}(x)-\mu_{\underline{A}}(x)\cdot\mu_{\underline{B}}(x) \qquad (1.9)$$

Пример: При $\underline{A}=\{x_1\,|\,0{,}2;x_2\,|\,0{,}7;x_3\,|\,1;x_4\,|\,0;x_5\,|\,0{,}5\}$,

и $\underline{B}=\{x_1\,|\,0{,}5;x_2\,|\,0{,}3;x_3\,|\,1;x_4\,|\,0{,}1;x_5\,|\,0{,}5\}$.

$\underline{A}\hat{\cdot}\underline{B}=\{x_1\,|\,0{,}10;x_2\,|\,0{,}21;x_3\,|\,1;x_4\,|\,0;x_5\,|\,0{,}25\}$.

$\underline{A}\hat{+}\underline{B}=\{x_1\,|\,0{,}60;x_2\,|\,0{,}79;x_3\,|\,1;x_4\,|\,0{,}1;x_5\,|\,0{,}75\}$

Если $M = \{0;1\}$, т. е. в случае обычных подмножеств, имеем

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

Для двух указанных операций $\cdot$ и $+$ на множестве всех нечетких подмножеств справедливы только следующие свойства:

Коммутативность
$$\underline{A} \cdot \underline{B} = \underline{B} \cdot \underline{A}$$
$$\underline{A} + \underline{B} = \underline{B} + \underline{A},$$

Ассоциативность
$$(\underline{A} \cdot \underline{B}) \cdot \underline{C} = \underline{A} \cdot (\underline{B} \cdot \underline{C})$$
$$(\underline{A} + \underline{B}) + \underline{C} = \underline{A} + (\underline{B} + \underline{C}),$$

Законы констант
$$\underline{A} \cdot \varnothing = \varnothing \qquad \underline{A} \cdot U = \underline{A}$$
$$\underline{A} + \varnothing = \underline{A} \qquad \underline{A} + U = U,$$

Инволюция
$$\overline{(\underline{A})} = \underline{A},$$

Теоремы Де Моргана
$$\overline{\underline{A} \cdot \underline{B}} = \overline{\underline{A}} + \overline{\underline{B}}$$
$$\overline{\underline{A} + \underline{B}} = \overline{\underline{A}} \cdot \overline{\underline{B}}.$$

Операции $\cup$ и $\cap$ не дистрибутивны относительно $\cdot$ или $+$ однако

$$\underline{A} \cdot (\underline{B} \cup \underline{C}) = (\underline{A} \cdot \underline{B}) \cup (\underline{A} \cdot \underline{C})$$
$$\underline{A} \cdot (\underline{B} \cap \underline{C}) = (\underline{A} \cdot \underline{B}) \cap (\underline{A} \cdot \underline{C}),$$
$$\underline{A} + (\underline{B} \cup \underline{C}) = (\underline{A} + \underline{B}) \cup (\underline{A} + \underline{C})$$
$$\underline{A} + (\underline{B} \cap \underline{C}) = (\underline{A} + \underline{B}) \cap (\underline{A} + \underline{C})$$

На основании (1.8) любое нечеткое множество $\underline{A}^{\alpha}$, где α – положительное число, можно определить как множество $\forall x \in U : \mu_{\underline{A}^{\alpha}}(x) = \mu_{\underline{A}}^{\alpha}(x)$.

Частными случаями операции возведения в степень являются операция концентрирования $CON(\underline{A}) = \underline{A}^2$ и операция растяжения $DIL(\underline{A}) = \underline{A}^{0,5}$.

Дизъюнктивная сумма

Дизъюнктивная сумма двух нечетких подмножеств определяется в терминах объединений и пересечений следующим образом:

$$\underline{A} \oplus \underline{B} = (\underline{A} \cap \overline{\underline{B}}) \cup (\overline{\underline{A}} \cap \underline{B}) \qquad (1.7)$$

Пример: Рассмотрим пример, который иллюстрировал операции объединения и пересечения для $\underline{A} = \{x1|0{,}8, x2|0{,}3, x3|0, x4|1, x5|0{,}5\}$ *и*

$\underline{B} = \{x1|0{,}5, x2|0{,}7, x3|0, x4|0{,}9, x5|0{,}5\}$, *тогда*

$\underline{A} \cap \underline{B} = \{x_1|0{,}5, x_2|0{,}3, x_3|0, x_4|0{,}1, x_5|0{,}5\}$, *а*

$\underline{A} \oplus \underline{B} = \{x_1|0{,}5, x_2|0{,}7, x_3|0, x_4|0{,}1, x_5|0{,}5\}$.

1.5.3.9. Разность

Разность определяется соотношением $\underline{A} - \underline{B} = \underline{A} \cap \overline{\underline{B}}$ (1.8)

Конечно, исключая частные случаи, $\underline{A} - \underline{B} \neq \overline{\underline{B}} - \underline{A}$.

Декартово произведение

Пусть $\underline{A}_1,...,\underline{A}_n$ – нечеткие подмножества универсальных множеств $U_1,...,U_n$ соответственно. *Декартово произведение* этих подмножеств обозначается $\underline{A}_1 \times \underline{A}_2 \times ... \times \underline{A}_n$ и определяется как нечеткое подмножество множества $U_1 \times U_2 \times ... \times U_n$ с функцией принадлежности

$$\mu_{\underline{A}_1 \times ... \times \underline{A}_n}(x_1,...,x_n) = \mu_{\underline{A}_1}(x_1) \wedge ... \wedge \mu_{\underline{A}_n}(x_n). \qquad (1.9)$$

Пример:

Для $U_1 = U_2 = \{5,7\}$, $\underline{A}_1 = \{5|0,5; 6|1; 7|0,6\}$, $\underline{A}_2 = \{5|1; 6|0,6\}$

$\underline{A}_1 \times \underline{A}_2 = \{(5,5)|0,5; (5,6)|1; (5,7)|0,6; (6,5)|0,5; (6,6)|0,6; (7,5)|0,6\}$.

Наглядное представление простейших операций с нечеткими подмножествами

Для нечетких подмножеств можно построить визуальное представление, родственное представлению обычных подмножеств (диаграмма Вьенна - Эйлера).

Рассмотрим прямоугольную систему координат, на оси ординат которой откладываются значения $\mu_{\underline{A}}(x)$, а на оси абсцисс в произвольном порядке расположены элементы ***U***. На рис. 1.2 принадлежность каждого элемента изображена его ординатой, заштрихованная часть наглядно изображает нечеткое подмножество $\underline{A} \subset U$.

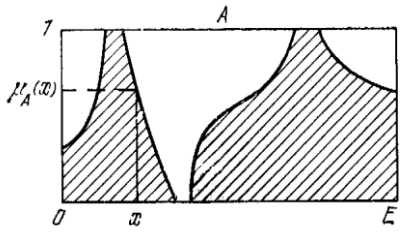
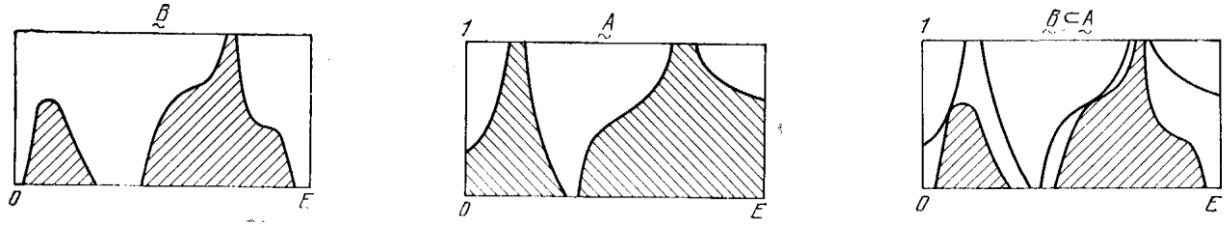


Рис. 1.2

Такое представление позволяет сделать зримыми простые операции на нечетких подмножествах. Ниже показано, как используется это представление.

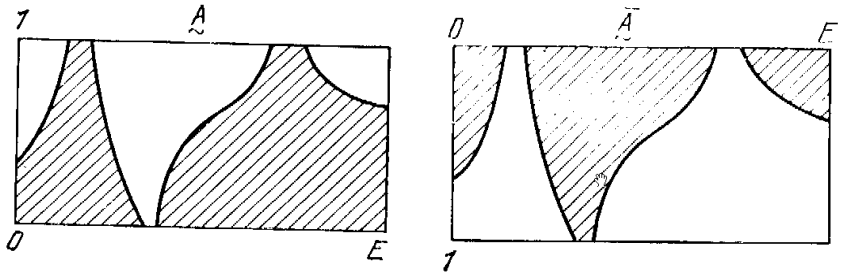
На рис. 1.3, а–в отражено свойство включения.



а б в

Рис.1.3. Диаграмма Вьенна-Эйлера свойства включения нечетких множеств

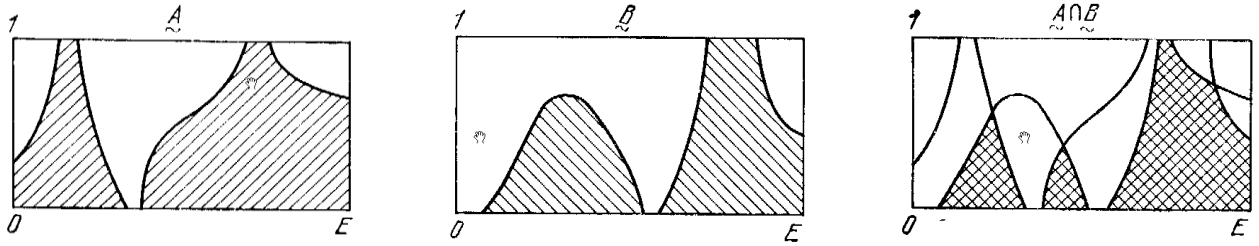
Рис. 1.4, а–б иллюстрируют дополнение.



а б

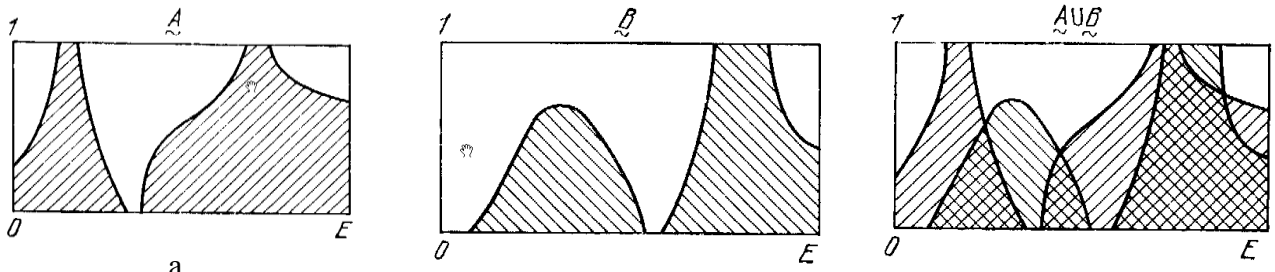
Рис.1.4. Диаграмма Вьенна-Эйлера дополнения нечеткого множества

Свойства пересечения и объединения отражены на рис. 1.5–1.6, а–в .



а б в

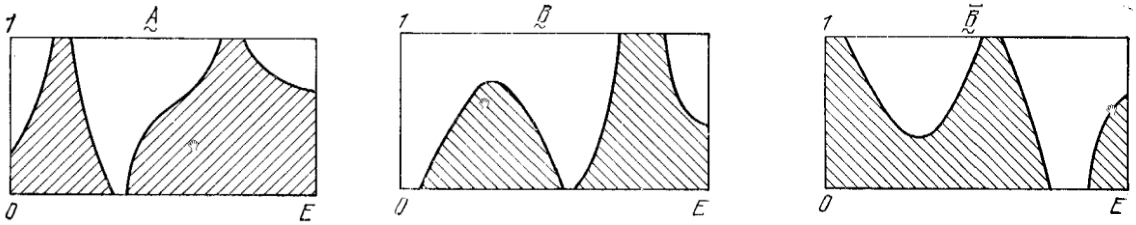
Рис.1.5. Диаграмма Вьенна-Эйлера пересечения нечетких множеств



а б в

Рис.1.6. Диаграмма Вьенна-Эйлера объединения нечетких множеств

На рис. 1.7, а–г представлена разность $\underset{\sim}{A} - \underset{\sim}{B} = \underset{\sim}{A} \bigcap \overline{\underset{\sim}{B}}$.



а б в

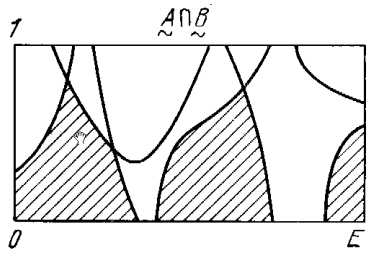


Рис. 1.5. г

Рис.1.7. Диаграмма Вьенна-Эйлера разности нечетких множеств

Рис. 1.8. а–ж иллюстрирует дизъюнктивную сумму $\underset{\sim}{A} \oplus \underset{\sim}{B} = (\underset{\sim}{A} \bigcap \overline{\underset{\sim}{B}}) \bigcup (\overline{\underset{\sim}{A}} \bigcap \underset{\sim}{B})$.

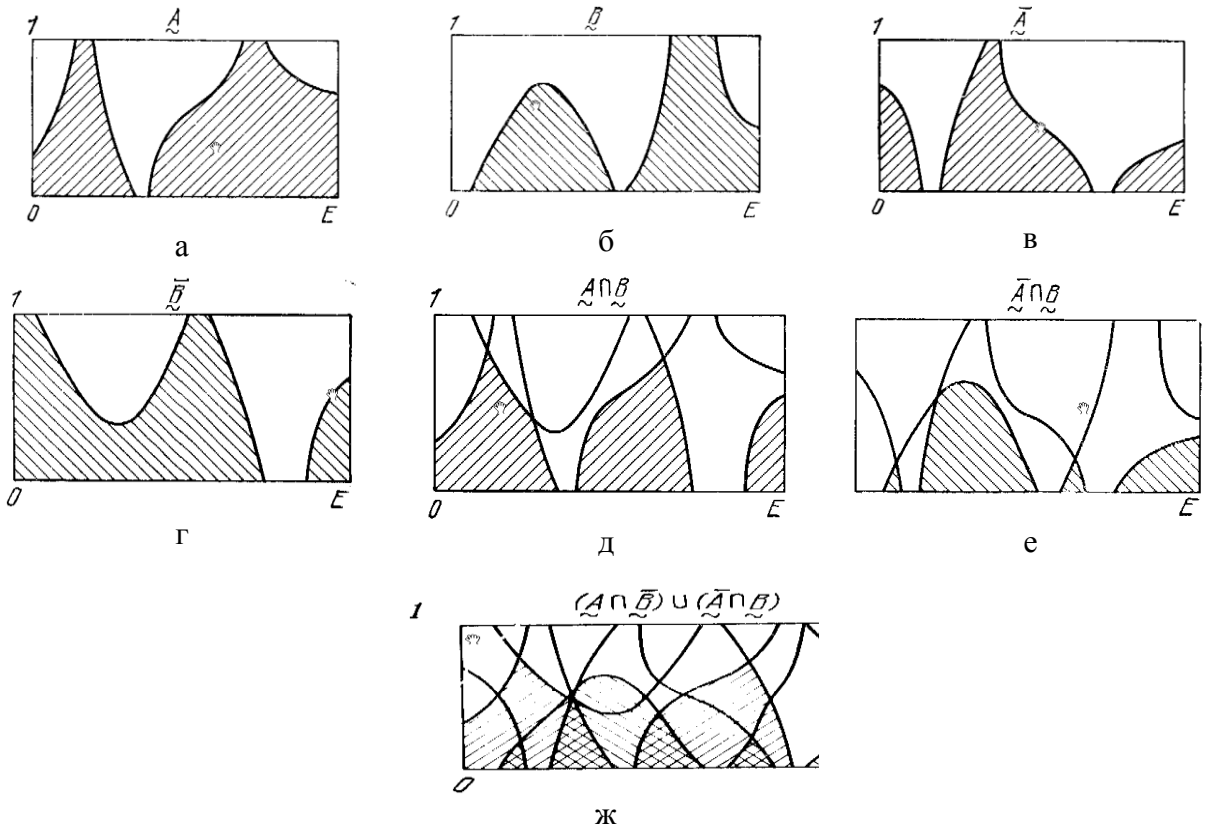


Рис.1.8. Диаграмма Вьенна-Эйлера дизъюнктивной суммы нечетких множеств

Множество нечетких подмножеств для конечных U и M

Рассмотрим случай, когда ***U*** и ***M*** – конечные множества. Напомним определение множества всех подмножеств данного множества на простом примере. Пусть $U = \{x_1, x_2, x_3\}$. Тогда $P(U) = \{\varnothing, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, U\}$.

Это множество состоит из $2^3 = 8$ элементов. В общем случае для множества $U = \{x_1, x_2, x_3, ..., x_n\}$ множество всех подмножеств состоит из 2^n элементов.

Для нечетких подмножеств множество всех подмножеств или «множество нечетких подмножеств» определяется иначе.

Пример: Пусть $U = \{x_1, x_2\}$, $M = \{0;0{,}5;1\}$. *Выпишем множество нечетких подмножеств множества* **U:**

$$P(U) = \left\{ \begin{array}{l} \{x_1 \mid 0\}\{x_2 \mid 0\} \{x_1 \mid 0\}\{x_2 \mid 0{,}5\} \{x_1 \mid 0\}\{x_2 \mid 1\} \\ \{x_1 \mid 0{,}5\}\{x_2 \mid 0\} \{x_1 \mid 0{,}5\}\{x_2 \mid 0{,}5\} \{x_1 \mid 0{,}5\}\{x_2 \mid 1\} \\ \{x_1 \mid 1\}\{x_2 \mid 0\} \{x_1 \mid 1\}\{x_2 \mid 0{,}5\} \{x_1 \mid 1\}\{x_2 \mid 1\} \end{array} \right\}.$$

В общем случае, если $|U| = n$ и $|M| = m$, то $|P(U)| = m^n$.

Известно, что структура множества всех подмножеств $P(U)$ множества ***U*** представляет собой дистрибутивную решетку с дополнениями (булеву решетку). Однако множество нечетких подмножеств $P(U)$ наделено структурой векторной решетки, а точнее – дистрибутивной решетки без дополнения.

На рис. 1.9 – 1.13 изображено несколько простых примеров, где для упрощения обозначений нечеткие подмножества представлены соответствующими им функциями принадлежности.

На рис. 1.9 представлена булева решетка обычных множеств $U = \{x_1, x_2\}$, $M = \{0;1\}$. На рис. 1.10: – векторная решетка нечетких множеств ***U*** и ***M,*** где $U = \{x_1, x_2\}$ и $M = \{0;0{,}5;1\}$.

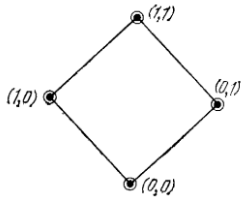


Рис. 1.9. Булева решетка обычного множества $U = \{x_1, x_2\}$, $M = \{0;1\}$

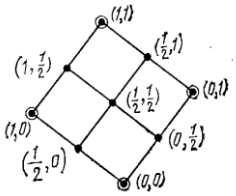


Рис. 1.10. Векторная решетка нечетких множеств $U = \{x_1, x_2\}$ и $M = \{0;0{,}5;1\}$

На рис. 1.11 представлена булева решетка обычных множеств $U = \{x_1, x_2, x_3\}$, $M = \{0;1\}$. На рис. 1.12: – векторная решетка нечетких множеств $U = \{x_1, x_2, x_3\}$ и $M = \{0;0{,}5;1\}$.

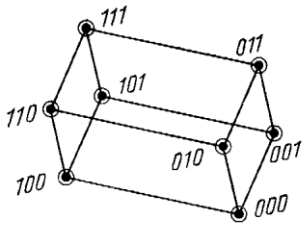


Рис. 1.11. Булева решетка обычных множеств $U = \{x_1, x_2, x_3\}$, $M = \{0;1\}$

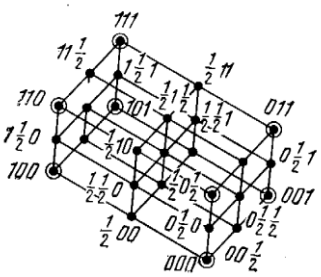


Рис. 1.12. Векторная решетка нечетких множеств $U = \{x_1, x_2, x_3\}$ и $M = \{0;0{,}5;1\}$.

На рис. 1.13: – другое возможное представление векторной решетки рис. 1.12.

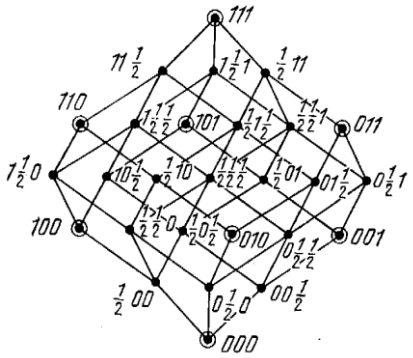


Рис. 1.13. Векторная решетка нечетких множеств $U = \{x_1, x_2, x_3\}$ и $M = \{0;0{,}5;1\}$ (другое представление)

3.33-34.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия о нечётком множестве;
- приобрели умения и навыки выполнения операций с нечёткими множествами.

3.35-36 Практическое занятие №ПЗ-35-36 (4 часа).
Тема: «Нечёткие отношения и соответствия. Экспертные системы**»**

3.35-36.1 Задание для работы:
1. Нечёткие отношения и соответствия.
2. Экспертные системы.

3.35-36.2 Краткое описание проводимого занятия:
1. Нечёткие отношения и соответствия.
2. Экспертные системы.

Нечеткие отношения

Если $\boldsymbol{U}$ – декартово произведение n универсальных множеств $\boldsymbol{U}_1, \ldots, \boldsymbol{U}_n$, то n-арное нечеткое отношение R в $\boldsymbol{U}$ определяется как нечеткое подмножество универсального множества $\boldsymbol{U}$. R можно представить в форме объединения составляющих его нечетких одноточечных множеств.

Распространенными примерами (бинарных) нечетких отношений являются *много больше, имеет сходство, близко* и т.д.

Пример: Если U = 1+2+3+4, то отношение *много больше чем* можно определить матрицей отношений

R	1	2	3	4
1	0	0.3	0.8	1
2	0	0	0	0.8
3	0	0	0	0.3
4	0	0	0	0

Композиция нечетких отношений

Если R – отношение $U \to V$, а S – отношение $V \to W$, то *композицией* R и S называется нечеткое отношение $U \to W$, обозначаемое $R \circ S$ и определяемое формулой

$$R \circ S = \int_{U \times W} \bigvee_{V} \left(\mu_R(u, v) \wedge \mu_S(v, w) \right) / (u, w) \quad (1.10)$$

Если U, V и W конечные множества, то матрица отношения $R \circ S$ есть максминное произведение матриц отношений и R и S.

Пример:

$$\overset{R}{\begin{bmatrix} 0.3 & 0.8 \\ 0.6 & 0.9 \end{bmatrix}} \circ \circ \overset{S}{\begin{bmatrix} 0.5 & 0.9 \\ 0.4 & 1 \end{bmatrix}} = \overset{R \circ S}{\begin{bmatrix} 0.4 & 0.8 \\ 0.5 & 0.9 \end{bmatrix}}.$$

Проекции

Если есть R n–арное нечеткое отношение в $U_1 \times U_2 \times \ldots \times U_n$, то его проекция на $U_{i1} \times \ldots \times U_{ik}$ есть k–арное нечеткое отношение R_q в U, которое определяется следующим образом

$$R_q = \int_{U_{i1} \times \ldots \times U_{ik}} \left(\bigvee_{u} \mu_R(u_1, \ldots, u_n) \right) / (u_{i1}, \ldots, u_{ik})$$

где q – последовательность индексов ; ; – дополнение; а

где верхняя грань берется по значениям всех тех , которые входят в .

Принцип обобщения

Принцип обобщения для нечетких множеств представляет собой основное равенство, позволяющее расширить область определения отображения ***U*** или отношения, включив в нее произвольные нечеткие подмножества множества ***U***.

Предположим, что f – отображение $U \to G$, а $\underline{A}$ – нечеткое подмножество вида $\underline{A} = x_1 / \mu_1, \ldots, x_n / \mu_n$. Тогда принцип обобщения утверждает, что $f(\underline{A}) = f(x_1) / \mu_1, \ldots, f(x_n) / \mu_n$. То есть, образ множества $\underline{A}$ при отображении f можно получить, зная образы элементов $x_1, \ldots, x_n$ при этом отображении.

Принцип обобщения аналогичен принципу суперпозиции для линейных систем.

Нечеткие переменные и нечеткая логика

Нечеткая переменная

Нечеткая переменная характеризуется тройкой $(X, U, R(X;u))$, где X– название переменной, U – универсальное множество (конечное или бесконечное), u – общее название элементов множества U, $R(X;u)$ – нечеткое подмножество множества U, представляющее собой нечеткое ограничение на значения переменной u, обусловленное X. Неограниченная обычная (не нечеткая) переменная u является для X *базовой переменной*.

Уравнение назначения для X имеет вид $x = u : R(X)$ и отражает то, что элементу x назначается значение u с учетом ограничения $R(X)$.

Та степень, с которой удовлетворяется это равенство называется *совместимостью* значения u с $R(X)$ и обозначается $c(u)$.

По определению $c(u) = \mu_{R(X)}(u), u \in U$, где $\mu_{R(X)}(u)$ – степень принадлежности u ограничению $R(X)$.

Совместимость значения u это не вероятность значения u. Совместимость u с $R(X)$ – это лишь мера того, насколько значение u удовлетворяет ограничению $R(X)$; она не имеет никакого отношения к тому насколько вероятно или невероятно это значение.

Лингвистическая переменная

Лингвистическая переменная отличается от числовой переменной тем, что ее значениями являются не числа, а слова и предложения в естественном или формальном языке. Поскольку слова в общем смысле менее точны, чем числа, понятие лингвистической переменной дает возможность приближенно описывать явления, которые настолько

сложны, что не поддаются описанию в общепринятых количественных терминах. В частности, нечеткое множество, представляющее собой ограничение, связанное со значениями лингвистической переменной, можно рассматривать как совокупную характеристику различных подклассов элементов универсального множества.

Лингвистическая переменная является переменной более высокого порядка, чем нечеткая переменная, в том смысле, что значениями лингвистической переменной являются нечеткие переменные.

Лингвистической переменной соответствуют два правила: *синтаксическое* правило, которое может быть задано в форме грамматики, порождающей названия значений переменной; *семантическое* правило, которое определяет алгоритмическую процедуру для вычисления смысла каждого значения. Эти правила составляют существенную часть описания структуры лингвистической переменной.

Нечеткая логика

Часто степень истинности утверждения характеризуется с помощью выражений ***совершенно верно, более или менее верно, абсолютно ложно*** и т.д. В ситуациях, когда истинность или ложность утверждений определены не достаточно хорошо, может оказаться целесообразным трактовать **истинность** как лингвистическую переменную, для которой ***истинно*** и ***ложно*** – лишь два первичных терма, а не пара крайних точек во множестве значений истинности. Такую переменную называют лингвистической переменной истинности, а ее значения – лингвистическими значениями истинности.

Трактовка истинности как лингвистической переменной приводит к нечеткой лингвистической логике (или просто к нечеткой логике), которая отличается от обычной двузначной или даже многозначной логики.

Такая логика является основой того, что можно было бы назвать приближенными рассуждениями, близкими к рассуждениям, которыми пользуются люди в некорректно определенных или не поддающихся количественному описанию ситуациях.

Лингвистические переменные истинности

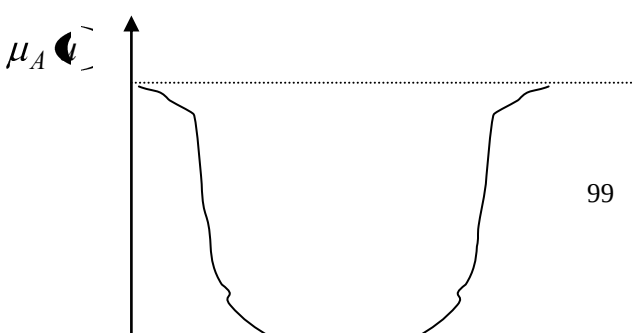
Аналогично алгебре высказываний высказывание «*и есть А*» можно интерпретировать как уравнение назначения, в котором лингвистической переменной, обозначающей какое-либо свойство элемента *и*, назначается в качестве значения нечеткое множество *А*.

Например: X – малый **– Величина(**X**)=малый**.

То есть высказыванию типа «*и есть А*» соответствуют два нечетких подмножества: 1) *M(A)* – смысл *А* и 2) значение истинности утверждения *ν(A)*.

Истинность – название булевой лингвистической переменной, для которой первичным является терм ***истинный***, а терм ***ложный*** определяется как зеркальное отражение относительно точки 0.5 в [0,1]. Такое определение является следствием определения значения ***ложный*** как значение истинности высказывания ***не А*** при предположении, что значением истинности высказывания *А* является ***истинный***.

Предполагается, что смысл первичного терма ***истинный*** является нечетким подмножеством интервала с функцией принадлежности типа приведенной на рис.2.1. Более точно терм ***истинный*** следует рассматривать как название нечеткой переменной, ограничением для которой является нечеткое множество, изображенное на рис.2.1.



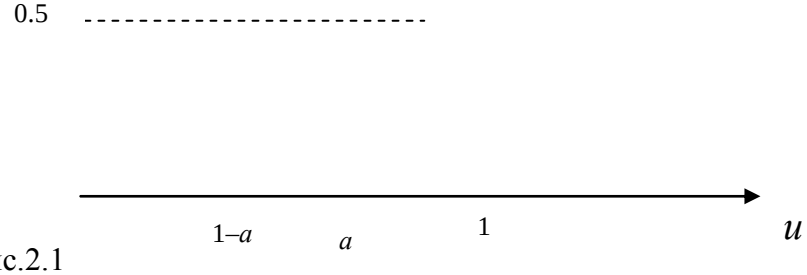


Рис.2.1

В некоторых случаях проще полагать, что терм ***истинный*** является подмножеством конечного универсального множества значений истинности *V={0, 0.1,0.2,0.3…0.9,1},* а не интервала *V*=[0,1].

Логические связки в нечеткой логике

Следует иметь в виду, что если *A* – нечеткое подмножество универсального множества *U* и $u \in U$, то следующие утверждения эквивалентны:

«Степень принадлежности элемента *u* нечеткому множеству *A* есть $\mu_A(u)$» «Значение истинности нечеткого предиката *A* есть $\mu_A(u)$»

Тогда вопрос «что является значением истинности высказывания ***A и B***, если заданы лингвистические значения истинности *A* и *B*» аналогичен вопросу «какова степень принадлежности элемента *u* множеству $A \bigcap B$, если заданы степени принадлежности элемента множествам *A* и *B*».

В частности, если *v(A)* точка в *V*=[0,1], представляющая значение истинности высказывания «*u есть A*», где *u* – элемент универсального множества *U*, то значение истинности высказывания ***не A*** определяется выражением

$$v(неA) = 1 - v(A). \qquad (2.3)$$

Следует, однако, отметить, что если $истинный = \mu_1/v_1 + \mu_2/v_2 + \ldots + \mu_n/v_n$, то

$не\ истинный = (1-\mu_1)/v_1 + (1-\mu_2)/v_2 + \ldots + (1-\mu_n)/v_n$,

а $ложный = v(не\ A) = \mu_1/(1-v_1) + \mu_2/(1-v_2) + \ldots + \mu_n/(1-v_n)$.

То же самое относится к логическим неопределенностям.

Перейдем к бинарным связкам.

Пусть *v(A)* и *v(B)* лингвистические значения истинности высказываний *A* и *B* соответственно, заданные выражениями $v(A) = \alpha_1/v_1 + \alpha_2/v_2 + \ldots + \alpha_n/v_n$ и

$v(B) = \beta_1/w_1 + \beta_2/w_2 + \ldots + \beta_n/w_n$.

Применяя принцип обобщения, получаем

$$v(AuB) = \sum_{i,j} (\alpha_i \wedge \beta_j)/(v_i \wedge w_j) \qquad (2.4)$$

$$v(AилиB) = \sum_{i,j} (\alpha_i \vee \beta_j)/(v_i \vee w_j) \qquad (2.5)$$

$$v(A \to B) = \sum_{i,j} \left(\alpha_i \wedge \beta_j \right) / \left(\neg v_i \vee \left(v_i \wedge w_j \right) \right) \qquad (2.6)$$

Таблицы истинности и лингвистическая аппроксимация

В *n*-значной логике бинарные связки обычно определяются таблицами значения истинности высказываний ***A и B, A или B, A→ B*** в терминах значений истинности высказываний *A* и *B*. В нечеткой логике число значений истинности в общем случае бесконечно и эти операции нельзя определить табулированием.

Можно протабулировать, допустим, операцию для некоторого (представляющего интерес) конечного множества значений истинности.

Например: истинный, не истинный, более или менее истинный, очень истинный и т.п.

Предположим, что каждый элемент *i*–й строки такой таблицы соответствует значению ***не истинный***, а каждый элемент *j*–го столбца – значению ***более или менее истинный***, то

(*i,j*)-й элемент= значение элемента *i*–й строки (***не истинный***) ∧ значение элемента *j*–го столбца (***более или менее истинный***).

При заданном определении первичного терма ***истинный*** и определениях модификаторов ***не*** и ***более или менее*** можно определить ***не истинный∧ более или менее истинный*** используя (2.4).

Трудность состоит в том, что в большинстве случаев результатом вычисления будет нечеткое подмножество универсального множества значений истинности, которое может не соответствовать ни одному из значений истинности в терм-множестве переменной **Истинность**. Поэтому, если придется составлять таблицу лингвистических значений истинности придется довольствоваться приближенным значением элементов таблицы. Такое значение называется лингвистическим приближением.

3.33-36.3 Результаты и выводы: в результате проведенного занятия студенты:
- освоили понятия о нечётких отношениях и соответствиях;

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ СЕМИНАРСКИХ ЗАНЯТИЙ

Семинарские занятия не предусмотрены рабочим учебным планом.