Полнота и замкнутость.

Студент должен

знать:
-понятие функционально полных систем;
-методику представления булевой функции в виде полинома Жегалкина;
-понятие полнота множества функций;
-понятие замкнутый класс;
-теорему Поста;

уметь:
-представлять булеву функцию в виде полинома Жегалкина;

1. **Функционально-полные системы.**
2. **Алгебра Жегалкина и линейные функции.**
3. **Замкнутые классы. Многотомные функции.**
4. **Две теоремы о функциональной полноте. Лемма 1, Лемма 2.**

1. Функционально-полные системы.

Определение: Система функции Σ называется функционально-полной системой, если любая логическая функция может быть представлена формулой над Σ, то есть является суперпозицией функции из Σ, система $\Sigma_0=\{\&,\vee,-\}$ функционально полна.

Функционально–полной будет любая система Σ, через функции которой можно выразить &,∨,-.

2. Алгебра Жегалкина и линейные функции.

Определение: Алгебра над множеством логических функций с 2-мя бинарными операциями конъюнкция и сложение по модулю называется алгеброй Жегалкина.

В алгебре Жегалкина выполняются следующие соотношения:
$x\oplus y=y\oplus x$
$x(y\oplus z)=xy+xz$
$x\oplus x=0$

$x \oplus 0 = x$

$\bar{x} = x \oplus 1$

$x \vee y = \overline{\bar{x}\bar{y}} = (x \oplus 1)(y \oplus 1) \oplus 1 = xy \oplus x \oplus y$ – полином Жегалкина.

От булевой формулы можно перейти к формуле алгебры Жегалкина, следовательно, можно перейти к полиному Жегалкина:
Если $f_1 f_2 = 0$, то $f_1 \vee f_2 = f_1 \oplus f_2$
Это позволяет перейти к СДНФ, заменить дизъюнкции знаком сложения по модулю 2.

<u>Теорема:</u> Для всякой логической функции существует полином Жегалкина и при том единственный.

Для доказательства единственности покажем, что между множеством всех функций от n переменных и множеством всех полиномов Жегалкина от n переменных существует взаимно однозначное соответствие. Число различных членов (то есть конъюнкций переменных) полиномов от n переменных равно числу всех подмножеств из n элементов, то есть 2^n. Число различных полиномов, которые можно образовать из этих конъюнкций равно числу всех подмножеств множества конъюнкции, то есть 2^2. Таким образом число всех полиномов Жегалкина от n переменных равно числу всех функций от n переменных, так как разным функциям соответствуют разные полиномы, но между множествами функций и полиномов от n переменных установлено взаимно однозначное соответствие, что и доказывает единственность полинома для каждой функции.

<u>Определение</u>: Функция, у которой поленом Жегалкина имеет вид $\Sigma \alpha i\ xi \oplus j$, где αi , j =0 или 1 называется линейной.

Все функции от 1 переменной линейны. Линейными функциями от 2 переменных является эквивалентность и сложение по модулю 2.

3. Замкнутые классы. Многотомные функции.

<u>Определение:</u> Множество М логических функций называется замкнутым классом, если любая суперпозиция функций из множества М снова принадлежит множеству М.

Всякая система Σ логических функций порождает некоторый замкнутый класс, а именно класс, состоящий из всех функций, которые можно

получить суперпозицией из Σ. Такой класс называется замыканием Σ и обозначается $[\Sigma]$.
Если множество M замкнутый класс, то замыканием множества M – это есть само множество M. Если M – это функционально-полная система, то замыкание множества M – это множество логических функций $[M]=P_2$.
Множество всех дизъюнкций, то есть функции вида $x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_n$ является замкнутым классом. Множество всех линейных функций является замкнутым классом, так как подстановка формул вида $\Sigma\alpha i\ xi \oplus j$ в формулу такого же вида снова дает формулу этого же вида.

Важным примером замкнутого класса является класс монотонных функций.

Определение: Функция $f(x_1,\ldots,x_n)$ называется монотонной, если для любых двоичных наборов σ и τ длинны n из того, что $\sigma \leq \tau$ следует, что ъ $\underline{f}(\sigma) \geq f(\tau)$.

Теорема: Множество всех монотонных функций является замкнутым классом. Подстановка формулы без отрицаний в формулу без отрицаний снова дает формулу без отрицаний.

Следствие: Класс множественных функций является замыканием системы функций $\{\&,\vee,0,1\}$. Это утверждение вытекает из этого , что всякая булева формула без отрицаний является суперпозицией дизъюнкции и конъюнкции.

Теорема: Система Σ полна, если дизъюнкция, конъюнкция, отрицание являются суперпозициями функций из Σ, поэтому будем искать свойства функций, позволяющие выразить через них булевы операции.

Лемма 1: (о немонотонных функциях) Если функция $f(x_1,\ldots,x_n)$ не монотонна, то подстановкой констант из нее можно получить отрицание. Точнее: существует такая подстановка n-1- константа что функция оставшейся одной переменной является отрицанием.

Лемма 1: (о нелинейных функциях) Если функция $f(x_1,\ldots,x_n)$ нелинейна, то подстановкой констант и используя отрицание из нее можно получить дизъюнкцию и конъюнкцию.
Точнее: существует представление дизъюнкции и конъюнкции в виде суперпозиции констант отрицаний констант и функции f.

f_i	α,β,j	Вид полинома	Эквивалентная булева формула	Искомая суперпозиция
f_0	0 0 0	x y	x y	xy=f_0(x,y)
f_1	0 0 1	xy⊕1	$\overline{xy}$	xy=nf_0(x,y)
f_2	0 1 0	xy⊕y	$\bar{x}\,y$	xy=f_2(n(x),y)
f_3	0 1 1	xy⊕y⊕1	$\overline{\bar{x}y} = x \vee y$	x∨y=f_3(x,n(y))
f_4	1 0 0	xy⊕x	$x\,\bar{y}$	xy=f_4(x,n(y))
f_5	1 0 1	xy⊕x⊕1	$\overline{x\bar{y}} = \bar{x} \vee y$	x∨y=f_5(n(x),y)
f_6	1 1 0	xy⊕x⊕y	X∨y	x∨y=f_6(x,y)
f_7	1 1 1	xy⊕x⊕y⊕1	$\overline{x \vee y}$	x∨y=nf_7(x,y)

n- отрицание.

Две леммы позволяют получить булевы операции, с помощью немонотонных функций, не- линейных функций и констант. Это еще не функциональная полнота в обычном смысле, так как константы с самого начала предполагались данными, однако такое предположение часто бывает оправданным в различных предложениях и прежде всего в синтезе логических схем, где системе логических функций соответствует набор типовых логических элементов, а полнота системы означает возможность реализовать, с помощью элементов данной схемы любые логические функции. При схемной реализации константы 0 и 1 не имеют специальных элементов.

Введем смысл об ослабленном понятии функций полноты: система функций Σ называется функционально полной в слабом смысле, если любая логическая функция может быть представлена формулой над системой Σ{0,1}, то есть является суперпозицией констант и функций из Σ.

Очевидно, что из обычной полноты системы следует ее слабая полнота.

<u>**Теорема:**</u> (1-я теорема о функциональной полноте): Для того чтобы система функций Σ была функционально полной в слабом смысле, необходимо и достаточно, чтобы она содержала хотя бы одну монотонную и хотя бы одну линейную функцию.

<u>**Необходимость:**</u> классы монотонных и линейных функций замкнуты и содержат 0 и 1. Поэтому, если Σ не содержит немонотонных или не

линейных функций, то их нельзя получить с помощью суперпозиций функций из Σ и констант.

<u>Достаточность:</u> пусть Σсодержит немонотонную и не линейную функции, тогда по лемме 1 подстановкой констант из монотонной функции получаем отрицание, а затем по лемме 2 из линейной функции с помощью отрицаний констант получаем дизъюнкцию и конъюнкцию.

<u>Теорема:</u> (2-я основная теорема о функциональной полноте): Для того чтобы система функций Σ была функционально полной в сильном смысле, необходимо и достаточно, чтобы она содержала: 1) нелинейную функцию; 2) немонотонную функцию; 3) несамодвойственную функцию; 4) функцию не сохраняющую 0; 5) функцию не сохраняющую 1.

Элементы теории и практики шифрования.

Студент должен:

иметь представление*:*
- о задачах теории шифрования и областях ее применения;
- об историческом аспекте развития теории и практики шифрования;

знать:
- понятие шифрования,

уметь:
- применять простейший шифры замены (в частности, шифр Цезаря и шифр Вижинера) для шифрования текста;
- осуществлять дешифровку шифротекста зашифрованного данным шифром замены.

1. **Шифр Цезаря.**
2. **Шифр Вижинера.**

1. Система Цезаря с ключевым словом.

Данная система шифрования является одноалфавитной системой, особенностью является использование слова или фразы что бы создать алфавит подстановки. Слово используется для смещения.

Ключевое слово - DIPLOMAT
K=5

 0 1 2 3 4 5
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V W X Y Z **D I P L O M A T** B C E F G H J K N Q R S U

Этапы шифрования.

Шифруемая фраза (слово) – mony
Зашифрованная - BECD
Используем ключевую фразу: ***Как дым отечества нам сладок и приятен***
0 1 2 3 4
А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Ъ Ь Э Ю **К А Д Ы М О Т Е Ч С В Н Л И П Р Я** Б Г Ж З Й У Ф Х Ц Ш Щ

К=4
Ключевое слово - как дым отечества нам сладок и приятен.
Шифруемая фраза (слово) – ***привет***.
Зашифрованная – НЛМЭАП.

Достоинства системы Цезаря с ключевым словом является, то что количество возможных ключевых слов практически не ограничено. Недостаток является в возможности взлома шифра текста на основе анализа частот появления букв, и в том что шифровальщик должен передать ключ. Шифр Цезаря расшифровать легко.

Известны вероятности букв P_i, I – номер буквы. Подсчитаем частоты букв f_i в зашифрованном сообщении. Если сообщение не очень короткое, то частота f_i букв должна согласовываться с вероятностью P_i. Затем начинаем делать перебор по сдвигам: когда сдвиг не указан общее различие P_i и f_i будет равно $\Delta s=\Sigma| P_i - f_i(s)|$ s – сдвиг. Чем меньше Δs тем больше вероятность того что мы расшифруем шифр Цезаря.

2. Шифр Вижинера

Был изобретен в 1586 году.

П Р И Л Е Т А Ю
А М Б Р О З И Я

П Ъ Й Ы У Щ И Э

Составим каждой букве алфавита - цифру например в английском алфавите буквы нумеруются A=0…Z=25. Ключ задается словом из d букв (цифр). Слово повторно записывается под шифруемым сообщением и в I-м столбце из 2-х букв, буква сообщения $M_{i\text{-я}}$ складывается по модулю |26| со стоящей под ней буквы ключа K_i. $I_i=m_i+k_i \bmod d_i$. Расшифровка осуществляется вычитанием ключа по модулю |26|.

Крупным недостатком данной системы шифрования является то что отправитель должен сообщить ключ который по дороге может быть потерян, продан и т.д. В середине 70-х на базе ЭВМ были построены глобальные системы элементов связи. В 1976 году американец Диффи и Хелман предложили свой способ выработки ключа.

Метод математической индукции, элементы комбинаторики.

Студент должен:
знать:
- принцип метода математической индукции;
- некоторые разновидности (модификации) метода математической индукции;

уметь:
- доказывать утверждения с помощью метода математической индукции.

1. **Индукция и дедукция.**
2. **Метод математической индукции.**
3. **Комбинаторика. Основное правило комбинаторики.**

1. Индукция и дедукция

Утверждения, которые постоянно встречаются в нашем языке, бывают общие и частные.

Общие утверждения:

1. Во всяком ромбе диагонали перпендикулярны.
2. Все числа оканчивающиеся на 0 и 5 делятся на 5.
3. Все люди смертны.
4. Все крокодилы умеют летать.

Частные утверждения:

1. В ромбе АВСД диагонали перпендикулярны.
2. 475:5, 120:5.
3. Джон – смертен.
4. Крокодил Кеша умеет летать.

Определение: Дедуктивный метод рассуждений это рассуждение от общего к частному, то есть рассуждение исходным моментом которого является общий результат, а заключительным моментом – частный.

Определение: Индуктивный метод применяется к рассуждениям, при помощи которого получают общие выводы, опираясь на ряд частных утверждений.
Простым методом рассуждений такого рода является – полная индукция.

Пример:

Требуется установить, что каждое четное, натуральное число n в пределах $n>=4$, $n<=100$ представимо в виде суммы 2-х простых чисел. Для этого переберем такие числа и выпишем соответствующие разложения.
4=2+2, 6=3+3, 8=3+5, 10=5+5,11=6+5,…., 98=91+7, 99=95+4, 100=97+3

эти 49 равенств показывают, что каждое из интересующих нас чисел можно представить в виде суммы 2-х простых чисел. Общее утверждение рассматривается здесь разбором всех частных случаев. Иногда общий результат может быть предугадан после рассмотрения не всех, а достаточно большого числа отдельных случаев (неполная индукция). Однако такой результат не является строгим доказательством так как неполная индукция может привести к ошибке. Провести полную индукцию часто не предоставляется возможным. Выходом из этого положения является обращение к особому методу рассуждений называемым – методом математической индукции.

3. Метод математической индукции

Метод математической индукции основан на следующей аксиоме (принцип математической индукции).

Пусть имеется последовательность утверждений $y_1, y_2, \ldots, y_n, \ldots$ Каждое из этих утверждений справедливо, если:

1. y_1 справедливо (базис индукции).
2. Из справедливости утверждений y_k следует справедливость y_{k+1} (к+1 – индукционный шаг).

Иными словами если имеется утверждение, зависящее от натурального числа n, то

1. Проверяется справедливость его при n=1.
2. Предполагается справедливость этого утверждения для n=k, где k-произвольное число и с учетом этого предположения доказывается его справедливость для n=k+1.

Пример:

Доказать что $1+3+5+\ldots+(2n-1)=n^2$

n=1 формула верна т.к.

$1=1^2$

формула верна при n=k

$1+3+\ldots+(2k-1)=k^2$

Формула верна и для следующего натурального

n=k+1 т.е. докажем что

$1+3+\ldots.+(2k-1)+(2(k+1)-1)=(k+1)^2$

Действительно,

$1+3+\ldots+(2k-1)+(2(k+1)-1)=k^2+(2(k+1)-1)=k^2+(2(k+1)-1)=k^2+2k+1=(k+1)^2$

Следовательно, формула верна при любом натуральном n.

3. Комбинаторика. Основное правило комбинаторики.

Комбинаторика возникла в 16 веке, когда в жизни высших слоев общества прочное место заняли азартные игры. Развитие комбинаторики связано с именами известных ученных: Паскаля, Ферма, Бернули, Эйлера, Лейбенца и многих других.

Основное правило комбинаторики.

Если элемент ***a*** можно выбрать n – способами и для каждого из таких выборов элемента ***a*** другой элемент ***b*** может быть выбран m – способами, то выбор пары элементов (***a,b***), можно найти произведением n*m.

Доказательство: Так как элемент ***a*** может быть выбран n – способами, то получим $\boldsymbol{a_1, a_2, a_3, \ldots, a_n}$, элементы ***b*** m – способами $\boldsymbol{b_1, b_2, b_3, \ldots, b_n}$, тогда выбор пары ***(a,b)***, осуществляется следующим образом:

$(a_1,b_1)(a_1,b_2)\ldots(a_1,b_m)$
$(a_2,b_1)(a_2,b_2)\ldots(a_2,b_m)$
…
$(a_n,b_1)(a_n,b_2)\ldots(a_n,b_m)$

Мы получили матрицу и получим произведение m*n.

Пример:
1). Из города A в город B можно добраться автобусом, самолетом и автобусом из B в C поездом и теплоходом. Сколькими способами можно добраться из A в C?
Из A в C – 6 способов.   3*2=6

2).Сколько различных 3-х значных чисел можно составить из цифр 0,1,2,3,4,5,6,7?

I   II   III
7 * 8   *   8   448 цифр.

3).Сколько различных 3-х значных чисел можно составить из цифр 1,2,3,4,5 если не одна цифра не может повторятся?

$A_3^5=5/(3-5)!=60$

<u>Определение:</u> Размещениями из n элементов по m (m<=n) называются соединения из n элементов по m, отличающихся друг от друга составом элементов или порядком их расположения.
В реальных задачах это выражается в том, что элементы выбираются и расставляются по определенным местам (или должностям).
Пример:
Запишем все размещения из четырех элементов A,B,C,D по два:
AB, BA, AC, CA, AD, DA,BC, CB, BD, DB, CD, DC.
Всего получим 12 размещений из 4 элементов по 2.
Количество размещений из n элементов по m обозначается

$\mathbf{A}^m_n$. Мы нашли , что $A^2_4=12$

$\mathbf{A}^m_n=n!/(n-m)!$

Если m=n, то одно размещение отличается от другого только порядком распределения элементов. Такие размещения называются *перестановками.* Количество перестановок из n элементов обозначается P_n .

$$P_n = n!$$

Принято считать, что 0!=1

Пример 2:

Существует программа, сортирующая списки студентов по убыванию рейтинга. Сколько различных списков может быть получено в группе из 10 человек?

Решение:

Так как один список будет отличатся от другого расположением фамилии, то количество различных списков будет равно числу перестановок из 10 элементов, т.е. $P_{10} = 10! = 3628800$

<u>Определение:</u> Сочетаниями из n элементов по m $(m<=n)$ называются соединения из n элементов по m, отличающиеся составом элементов.

Пример:

Выпишем все сочетания из 4 элементов A, B,C, D по 2:

AB, AC, AD, BC, BD, CD.

Всего получили 6 сочетаний из 4 элементов по 2. Количество сочетаний из n элементов по m обозначается C^m_n . Мы нашли, что $C^2_4=6$. Получим формулу для C^m_n в общем случае.

Выбрать m из n разных элементов можем C_n^m способами, а в каждом из выбранных сочетаний имеется m! Возможностей упорядочения этих элементов. Поэтому по ОПК имеется $m!C^m_n$ способов выбрать и разместится по m разным местам m из имеющихся n элементов, т.е. $\mathbf{A}^m_n=m!C_n^m$

Следовательно $C^m_n=A^m_n/m!=n!/m!(n-m)!$

Пример 3:

В аудитории имеется 10 лампочек. Сколько существует разных способов ее освещения, при которых горит ровно 3 лампочки?

Решение:

Способов освещения столько, сколько существует сочетаний из 10 лампочек по 3, т.е. $C^3_{10}=10!/3!*7!=10*9*8/1*2*3*=120$

Мы рассмотрели 3 вида соединений: размещения, перестановки и сочетания. Следует четко помнить, что:

Перестановки отличаются друг от друга только порядком расположения элементов;
Размещения отличаются либо составом элементов, либо порядком их расположения;
Сочетания отличаются только составом элементов.

Графы.

Студент должен:

знать:

- понятие неориентированный и ориентированный граф, основные определения, связанные с ним;
- теорему о сумме степеней вершин графа;
- формулу количества ребер в полном графе;
- понятие расстояние между вершинами в графе, метрические характеристики графа и методику их нахождения;
- понятие двудольный граф, методику распознавания графа на двудольность;
- понятие изоморфность, методику распознавания изоморфности двух графов;
- понятие эйлеров граф, теорему Эйлера, методику нахождения эйлерова цикла в эйлеровом графе;
- понятие гамильтонов граф, некоторые теоремы о распознавании гамильтоновости (негамильтоновости) графа;
- понятие плоский граф соотношения между количествами вершин, ребер н граней в плоском графе;
- понятие циклический ранг графа, формулу его вычисления;
- понятие дерево, свойства деревьев*;*
- степени вершин графа;
- понятие ориентированное дерево;

уметь:

- записывать матрицу смежности для графов;
- находить количество ребер в графе;
- выделять компоненты связности в графе;
- находить расстояние между двумя вершинами в графе;
- находить радиус и диаметр графа;
- распознавать, является ли данный граф двудольным;

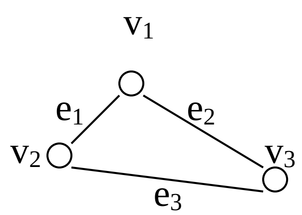
- распознавать, являются ли два данных графа изоморфными (в простейших случаях);
- распознавать, является ли данный граф эйлеровым; находить эйлеров цикл в эйлеровом графе;
- распознавать, является ли данный граф гамильтоновым (в простейших случаях);
- распознавать, является ли данный граф плоским (в простейших случаях);
- вычислить циклический ранг графа;
- выделять в орграфе источники и стоки;

Графы основные понятия и операции.

1) Графы и их вершины, ребра и дуги.
2) Изображение графов.
3) Матрица инцидентности и список ребер.
4) Матрица смежности графов.
5) Идентификация графов заданных своими представлениями.
6) Степени вершин графа.
7) Части графа, суграф и подграф.

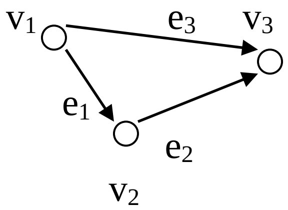
1.Графы и их вершины, ребра и дуги

<u>Определение:</u> Графом называется совокупность двух множеств V(точек), E (линий) между элементами которых определено отношение инцидентности, причем каждый элемент множества E инцидентен равным двум элементам множества V.



<u>Определение:</u> Ребро и любая из его двух вершин называются инцидентными, а вершины соединенные ребром называются смежными

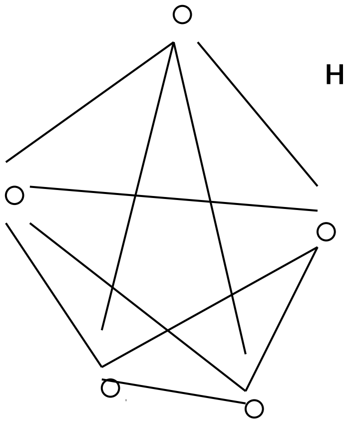
В некоторых задачах вершины не равны, тогда их рассматривать нужно в определенном порядке. Тогда каждому ребру предписывается направление от первой из инцидентных вершин ко второй, направленные ребра называются дугами, ***граф содержащий дуги называется ориентированным.***



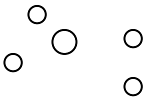
Первая по порядку вершина инцидентная ребру ориентированного графа, называется его началом, вторая - его концом. Следовательно, ребро ориентированного графа выходит из начала и входит в конец.
Понятие графов применяют не только при исследовании геометрических конфигураций. Графы определяются при анализе функционирования систем. С отдельными компонентами этой системы удобно связывать вершины графа, а с парами взаимодействующих компонент - его ребра. Построенный таким образом граф называют ***структурным графом системы***.

2. Изображение графов

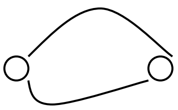
неориентированные графы:



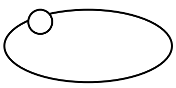
Граф где ребра пересекаются, но точки пересечения не являются вершинами



В данном графе множество E пусто. Граф называется пустым

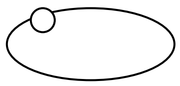


Граф имеющий кратные ребра называется мультиграфом.

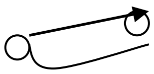


Граф петля

ориентированные графы:

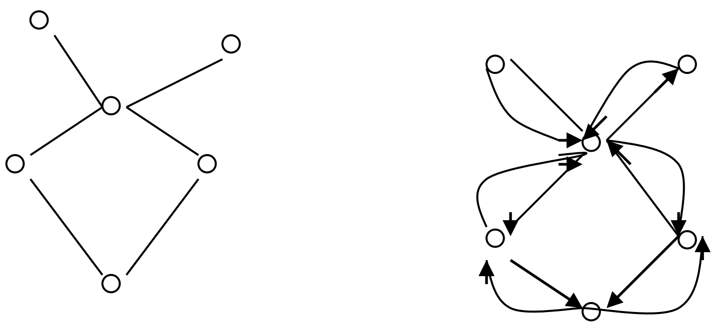


Граф петля



Ориентированный мультиграф

Каждому неориентированному графу можно поставить в соответствии ориентированный граф с тем же множеством вершин в котором каждое ребро заменено двумя ориентированными ребрами, инцидентными тем же вершинам и имеющими противоположенные направления. Такое соответствие будем называть ***каноническим.***



3) Матрица инцидентности и список ребер

Задать граф - значит описать множество его вершин и ребер, а так же рассмотреть отношение инцидентности когда граф конечный для описания его вершин и ребер достаточно их занумеровать.

Матрица смежности для неориентированного графа:

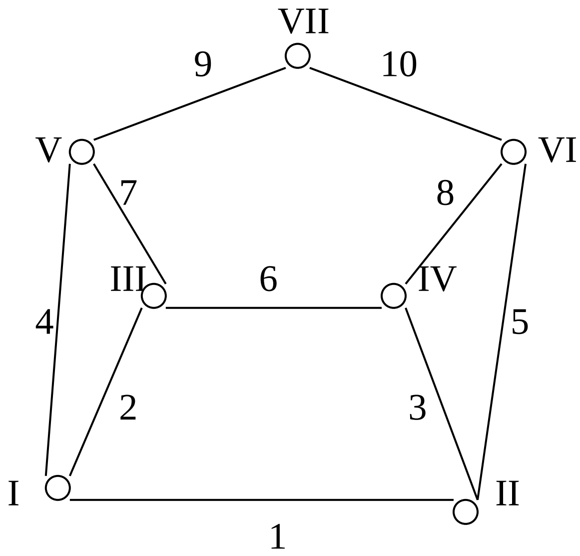


рис. 1

	I	II	III	IV	V	VI	VII
1	1	1	0	0	0	0	0
2	1	0	1	0	0	0	0
3	0	1	0	1	0	0	0
4	1	0	0	0	1	0	0
5	0	1	0	0	0	1	0
6	0	0	1	1	0	0	0
7	0	0	1	0	1	0	0
8	0	0	0	1	0	1	0
9	0	0	0	0	1	0	1
10	0	0	0	0	0	1	1

(к рис.1)

$v_1, v_2 \ldots v_n$ -вершина
$e_1, e_2 \ldots e_m$ - ребра

Отношение инцидентности можно определить матрицей $\left| \varepsilon_{i,j} \right|$, где определяются строки m и столбцы n. Столбцы соответствуют вершинам графа, ребра соответствуют строкам, если ребро e_i инцидентна вершине v_j, то элемент матрицы равен 1 ($\varepsilon_{ij}=1$) в противном случае $\varepsilon_{i,j}=0$.

Матрица инцидентности для ориентированного графа

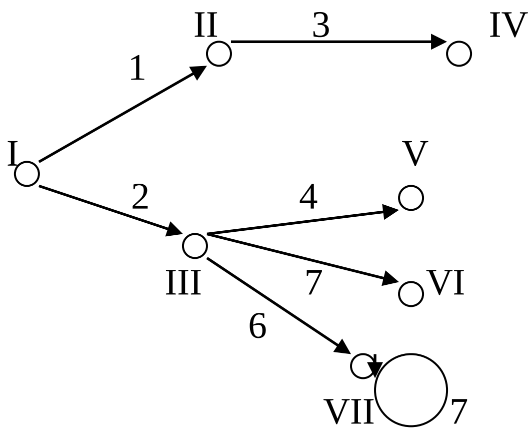


Рис. 2

Если вершина v_j является началом ребра то элемент $\varepsilon_{ij}=-1$, если v_j - конец ребра, то элемент $\varepsilon_{ij}=1$, если инцидентность не прослеживается то $\varepsilon_{ij}=0$, если ребро петля, то $\varepsilon_{ij}=\alpha$ где $\alpha \neq 0,1,-1$.

	I	II	III	IV	V	VI	VII
1	-1	1	0	0	0	0	0
2	-1	0	1	0	0	0	0
3	0	-1	0	1	0	0	0
4	0	0	-1	0	1	0	0
5	0	0	-1	0	0	1	0
6	0	0	-1	0	0	0	1
7	0	0	0	0	0	0	2

(к рис.2)

Матрица инцидентности для задания графа, недостаточно экономична, отношение инцидентности можно задать списком ребер графа. В строке записаны номера вершин инцидентных ребру, для неориентированного графа порядок этих вершин в строке произволен, для ориентированного графа первым стоит номер начала ребра , вторым – его конца.

4.Матрица смежности графов

Матрица смежности - это квадратная матрица $|\delta_{ij}|$ столбцам и строкам которой соответствует вершины графа.

Для неориентированного графа матрица смежности симметрична, для ориентированного не всегда. Если вершины смежные, то δ_{ij} =1, если нет – δ_{ij} =0. .

	I	II	III	IV	V	VI	VII
I	0	1	1	0	1	0	0
II	1	0	0	1	0	1	0
III	1	0	0	1	1	0	0
IV	0	1	1	0	0	1	0
V	1	0	1	0	0	0	1
VI	0	1	0	1	0	0	1
VII	0	0	0	0	1	1	0

(к рис. 1)

	I	II	III	IV	V	VI	VII
I	0	1	1	0	0	0	0
II	0	0	0	1	0	0	0
III	0	0	0	0	1	1	1
IV	0	0	0	0	0	0	0
V	0	0	0	0	0	0	0
VI	0	0	0	0	0	0	0
VII	0	0	0	0	0	0	1

(к рис. 2)

Для ориентированного графа δ_{ij} =1, если этот элемент матрицы смежности равен количеству ребер с началом в i-ой вершине и концом в j-й.

5. Идентификация графов заданных своими представлениями.

Граф может быть представлен различными способами:

1. Изображен на чертеже;
2. Задан матрицей инцидентности;
3. Задан матрицей смежности;
4. Задан списком ребер;

Вид чертежа зависти от формы линий и взаимного расположения вершин. Иногда не легко разобрать одинаковые ли графы, изображенные различными чертежами.

Вид матриц и списка ребер зависит от нумерации вершин и ребер. Граф считается полностью заданным, если нумерация его вершин зафиксирована.

Графы, отличающиеся нумерацией вершин, называется изоморфными.

Пусть дано два графа:

$G=(V,E)$ $G'=(V',E')$

Эти графы будут изоморфны, если существует пара отображений.

$\varphi: V\rightarrow V'$

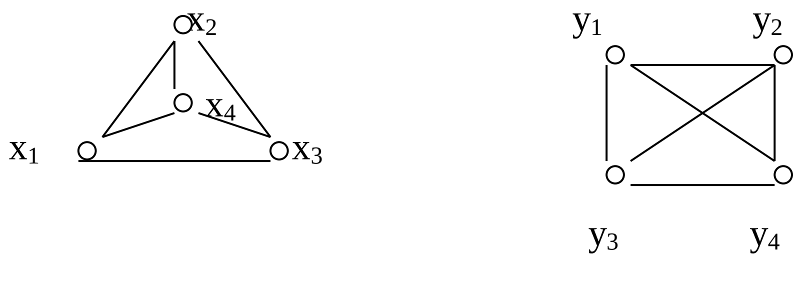
$\Psi: E\rightarrow E'$

таких что для любого ребра $e(v_1,v_2)$, $\Psi(e)=(\varphi(v_1); \varphi(v_2))$.

Иными словами отображение Ψ переводит ребро, соединяющие образы этих вершин при отображении φ.

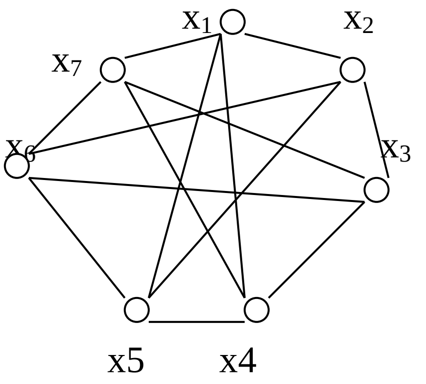
Изоморфные может быть на первый взгляд совсем не похожие графы.

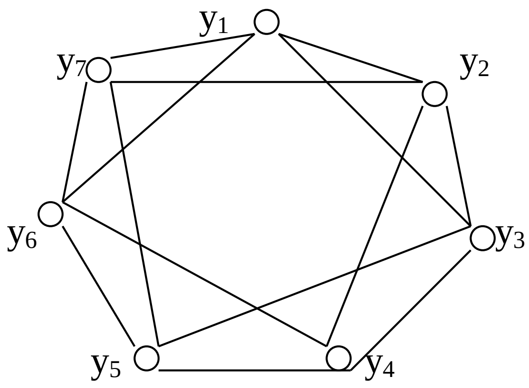
Пример:



Изоморфизм этих графов задается отображением вершин φ: $x_i\rightarrow y_i$,
ребро $(x_i\, x_j)$ переводится отображением $\Psi(y_i\, y_j)$.

Данные графы является полными, т.е. вмести с любыми двумя вершинами содержат единственное соединяющие их ребро. Полные графы с n вершинами обозначаются K_n. Любые два полных графа с одинаковым количеством вершин изоморфны.





Изоморфизм этих двух графов записываются отображением.

$$\varphi: \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ y_1 & y_3 & y_5 & y_7 & y_2 & y_4 & y_6 \end{pmatrix}$$

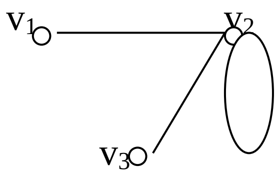
6. Степени вершин графа

Дан неориентированный граф G .

<u>Определение:</u> Количество ребер $\rho(v)$ инцидентных вершине $v \in G$ называется локальной степенью графа или просто степенью.

Если степени всех вершин конечны, рассматриваемый граф называется локально-конечным.
Если в графе есть петля, то она рассматривается двумя способами:

1. Петля, как простое ребро
2. Петля, как петля, т.е. это ребро дает в вершину два входа и вложение в степень этой вершины будет две единицы.



1) $\rho(v_2)=3$
2) $\rho'(v_2)=4$

Когда заданы матрицы смежности или инцидентности графа, степень вершин можно определить по единицам, стоящим на пересечение со строками, которым соответствуют инцидентные этой вершине ребра. Остальные равны 0, следовательно для матрицы инцидентности :

$$\boxed{\rho(v_j)= \sum_{i=1}^{n} \varepsilon_{ij}}$$

Элементы матрицы смежности- это количество ребер инцидентные вершинам v_i и v_j

$$\rho(v_j)=\sum_{i=1}^{n}\delta_{ij}$$

Чтобы учесть петлю, которая дает вклад в степень две единицы, формула для вычисления усложняется.

$$\rho'(v_j)=\sum_{i=1}^{m}\varepsilon_{ij}*(3-\sum_{k=1}^{n}\varepsilon_{ik})$$

$$\rho'(v_j)=\Sigma\delta_{ij}+\delta_{ji}$$

<u>Определение:</u> Граф называется однородным степени K, если степени всех его вершин равны K, тем самым равны между собой. Ели однородный граф имеет n вершин и m ребер, то число ребер считается по следующей формуле:

$$m=1/2\sum_{v\in G}\rho'(v)=kn/2$$

$$n=2m/k$$

7. Части графа, суграф и подграф.

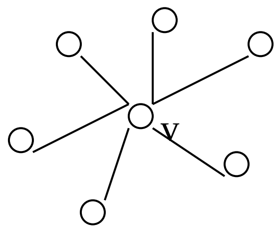
<u>Определение:</u> Граф H называется частью графа G ($H\subset G$), если множество его вершин V(H) содержится в множестве вершинV(G), а множество ребер E(H) в множестве ребер E(G).

Если V(H)=V(G)- часть графа называется ***суграфом***.

Например, имеется нулевой суграф, множество ребер которого пусто. Суграф H покрывает вершины неориентированного графа G, если любая вершина последнего инцидента хотя бы 1 ребру из H. Таким образом, если в графе G есть изолированная вершина v не инцидентная ни одному ребру, покрывающие суграфы этого графа не существуют. Любое множество ребер графа G можно считать множеством ребер некоторой части графа G.

Определение: Подграфом G(U) графа G множеством вершин U С в множество V называется граф, которому (не понял слова) все ребра с обоими концами из множества U.

Определение: Звездный граф для вершины $v \in G$ состоит из всех ребер с началом или концом в вершине v. Множество вершин звездного графа состоит из вершин v и других инцидентных его ребрам вершин.



Рассмотрим операции с частями графа:

Дополнение $\overline{H}$ части графа H определяется множеством всех ребер графа G не принадлежащих H.

Сумма $H_1 \cup H_2$

$V(H_1 \cup H_2)=V(H_1) \cup V(H_2)$

$E(H_1 \cup H_2)=E(H_1) \cup E(H_2)$

Разность $H_1 \cap H_2$

$V(H_1 \cap H_2)=V(H_1) \cap V(H_2)$

$E(H_1 \cap H_2)=E(H_1) \cap E(H_2)$

Вопросы для подготовки к экзаменам:

1.Знать определение алгебры Жегалкина
2.Знать основные соотношения алгебры Жегалкина.
3.Уметь выводить полином Жегалкина.
4.Знать определение замкнутого класса.
5.Знать Леммы.
6.Уметь шифровать информацию с помощью шифров Цезаря и Вижинера.
7.Знать определения индукции и дедукции.
8.Правильно пользоваться формулами комбинаторики.
9.Знать определение графа.
10.Уметь определять вид графа.
11.Уметь строить матрицы.
12.Уметь определять степени вершин графа.
13.Уметь определять виды маршрутов.
14.Уметь определять диаметр, центр, радиус графа.

15.Знать формулы для определения степени графа.

Решить задачи:

Пример1: Записать логические функции формулами алгебры Жегалкина

$$x \vee y = \overline{\overline{x}\,\overline{y}} = \overline{(x \oplus 1)(y \oplus 1)} = (x \oplus 1)(y \oplus 1) \oplus 1 = xy \oplus x \oplus y \oplus 1 \oplus 1 = xy \oplus x \oplus y$$

Это уравнение можно решить, если xy=0 тогда $x \vee y = x \oplus y$

Решить самостоятельно:

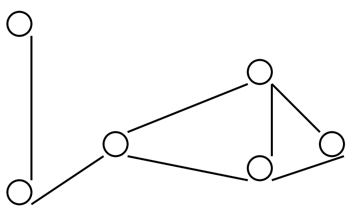
$$x \equiv y = xy \vee \overline{x} \bullet \overline{y}$$

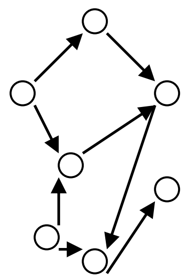
Решить задачи:

1. В группе из 15 студентов нужно выбрать троих для поездки в Аргентину. Сколькими способами можно это сделать ?

2. В группе из 10 юношей и 12 девушек нужно выбрать делегацию из 5 юношей и 5 девушек. Сколькими способами это можно сделать ?

Пример2: Исследовать графы





Построить матрицы смежности и инцидентности, определить степени вершин.