Билет1.

I.Опр.<u>**Мн-во**</u> – простейшее матем. понятие, оно не определяется, это совокупность каких-то объектов. Мн-ва могут быть конечными или бесконечными.

<u>**Способы задания мн-в**</u>: 1)Перечислением, 2)Указание св-ва элементов мн-ва, 3) с помощью проверяющих процедур(уравнение) 4) С помощью порождающей процедуры

<u>**Опр:**</u>1)$A=B \Leftrightarrow \{\forall x: x\in A \Leftrightarrow x\in B\}$; 2) *включение:* $A\subseteq B \Leftrightarrow \{x\in A \Rightarrow x\in B\}$ A подмн-во B; 3)*собств. включение:* $A\subset B \Leftrightarrow \{A\subseteq B$ и $A\neq B\}$ A собственное подмн-во мн-ва B.

<u>**Св-ва включения:**</u> 1)$A\subseteq B$, $B\subseteq A \Rightarrow A=B$ 2)$A\subseteq B, B\subseteq C \Rightarrow A\subseteq C$(транзетивность)

<u>**Операции над мн-ми:**</u> 1)Объединение 2)Пересечение 3)Разность 4)Дополнение 5)Симметрическая разность *Диаграмма Венна(круги Эйлера);*

Опр: <u>Универсальное мн-во</u> - мн-во, содержащие все элементы, находящиеся в рассмотрении

<u>**Св-ва операций на мн-вах:**</u>

1)Законы нуля и единицы: $A\cup\varnothing=A$; $A\cap\varnothing=\varnothing$; $A\cup U=U$; $A\cap U=A$;

2) $A\cup A\hat{}=U$; $A\cap A\hat{}=\varnothing$;

3)Идемпотентность: $A\cup A=A$; $A\cap A=A$;

4)Знак двойного дополнения:$A\hat{}\hat{}=A$(инволютивность)

5)Коммутативность:$A\cup B=B\cup A$; $A\cap B=B\cap A$

6)Ассоциативность:$(A\cup B)\cup C=A\cup(B\cup C)=A\cup B\cup C$; $(A\cap B)\cap C=A\cap(B\cap C)=A\cap B\cap C$

7)Дистрибутивность:$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$; $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

8)Законы де Моргана: $(A\cup B)\hat{}=A\hat{}\cap B\hat{}$;$(A\cap B)\hat{}=A\hat{}\cup B\hat{}$

9*)Закон поглощения: $A\cup(A\cap B)=A$; $A\cap(A\cup B)=A$-двойственность поглощения

II.<u>**Прямое произведение**</u>

Опр: <u>*Упорядоченный набор*</u> длины n, есть упорядоченная последовательность длины n $(a_1,a_2,...,a_n)$, в которой могут быть повторения. Набор из 2-х элементов называется <u>*пара*</u>.

Опр: <u>*Декартовым(прямым) произведением*</u> мн-в $A_1,A_2,...,A_n$ называется мн-во $\{(x_1,...,x_n) \mid x_1\in A_1,...,x_n\in A_n\}=A_1\times...\times A_n=\Pi A_i$

Если $A_1=...=A_n$, то ΠA_i называется *n-й декартовой степенью* мн-ва A: A^n . $A^0=\{\varnothing\}$, $A^1=A$, A^2 - декартов квадрат.

III.Число подмн-в конечного мн-ва.

2^A - мн-во всех подмн-в мн-ва A(булеон). $|2^A|=2^{|A|}$.

Пр.: $A=\{a,b\}$; $2^A=\{\varnothing,\{a\},\{b\},\{a,b\}\}$; $|2^A|=2^2=4$;

<u>Билет 2.</u>

<u>**Опр.**</u> n-местным отношением R на мн-ве $A_1,...,A_т$ называется любое подмн-во прямого произведения ΠA_i , т.е. элементы $x_1\in A_1,...,x_n\in A_n$ связаны соотношением $R(R(x_1,...,x_n))$ тогда и только тогда, когда $(x_1,...,x_n)\in R$. <u>Если n=1</u> то R называется **унарным**. <u>Если n=2</u> то R называется **бинарным**. Если $x,y\in A$, то $R\subseteq A^2$ и $(x,y)\in R$. !Есди мн-во A конечно, то и R конечно. Напр.: $A=\{1,2,3,4\}$, x|y, y делится на x без остатка. Тогда R - делимость, $R=\{(1,1),(1,2)(1,3)(1,4)(2,2),(3,3),(4,4),(2,4)\}$. *Нарисовать граф!*

<u>**Св-ва отношений R на A:**</u>

1)Рефликсивность: $\forall x\in A$: xRx(=,‖,≤,..)

2*)Антирефликсивность: $\forall x\in A:(x,x)\notin R$

3)Симметричность: $\forall(xRy)\Rightarrow yRx$(=,‖,..)

4)Антисимметричность: $\forall(xRy)$ и $\forall(yRx)$:x=y(≤,<..)

5)Транзитивность: $\forall x,y,z$: xRy yRz $\Rightarrow$xRz(=,‖,<..)

<u>**Опр.**</u>*Отношение эквивалентно,* если оно: 1)Рефликсивно 2)Симметрично 3)Транзитивно

Опр.X-любое мн-во, представленное в виде семейства q непустых непересекающихся подмн-в $P_1,...,P_n=X$ таких, что $P_1\cup...\cup P_n$. Такое семейство $q=\{P_1,...,P_n\}$ называется **разбиением** мн-ва X.

Теорема о факторизации: Для $\forall$ отношения эквивалентности R на A,$\exists$ такое разбиение q мн-ва A, что при отношении xRy $\Leftrightarrow$ x и y принадлежат одной части этого разбиения.

Опр.Подмн-ва(мн-ва) семейства q - разбиение мн-ва A отношения экв-ти R-называется **классами экв-ти(A/R**). Это семейство называется **фактор-мн-ом** A по отношению к R. Поскольку классы не пересекаются, то каждый из них может быть определен одним элементом - **представитель класса**(x/R), а другие элементы могут быть полученны с посощью св-в эквивалентности этих элементов по отношению к нему.

<u>Билет 3.</u>

Опр. Бинарное отношение R, построенное на мн-ве A, называется **отношением порядка**, если оно: 1)Транзитивно 2)Антисиммметрично $\forall a,b\in R$:aRb,bRa$\Rightarrow$a=b;3)Рефликсивно

<u>**Опр.**</u> Мн-во A с определенным на нем отношением порядка R называется **упорядоченным мн-ом**: (A,R).(Z, ≤)

Опр. Два элемента $a,b\in A$ называются сравнимыми элементами упорядоченного множества A, если либо aRb, либо bRa.
Опр. Отношение порядка на множестве A называется отношением **линейного порядка**, а множество A называется **линейно упорядоченным множеством**, если на нем нет несравнимых элементов: (A, L). Если не выполняется, то **частичной упорядоченностью(2^X, $\subseteq$).**
Опр*. Отношение порядка R называется отношением **строгого порядка** на мн-ве A, если R антирефлексивно: $\forall a,b\in A$, $aRb\Rightarrow a\neq b$.
Опр: (A,R) – упорядоченное мн-во. Элемент $a\in A$ называют **наиб. (наим.)** элементом мн-ва A, если $\forall x\in A$: xRa (aRx) или $b=\max A\Leftrightarrow\forall x\in A$, $bRx\Rightarrow b=x$ ($b=\max A\Leftrightarrow\forall x\in A$, $xRb\Rightarrow b=x$)
Опр: (A,R) – упорядоченное мн-во. Элемент $b\in A$ называют **макс. (мин.**) элементом мн-ва A, если $\forall$ $x\in A$ имеет место одно из двух: или $x\leq b$ или x и b несравнимы.
Зам.:Макс.элемент - больше которого нет, наиб.элемент - больше всех. **Пр.**$A=\{1,...,6\}$,x|y, (A,|) - ч.у.м.,1-min; 4,5,6-max;1-наим, наиб.нет
Опр. (A,R) – упорядоченное мн-во, $a,b\in(A,R)$. Говорят, что a **непосредственно предшествует** b (b R^(c ^) a), если выполнены следующие условия: 1)$a\neq b$ 2)bRa 3)$\forall c\in A$ (bRc) и (cRa) $\Rightarrow$ (b=c) или (c=a)
Опр. (A, R) – упорядоченное множество. Последовательность $\{x_i\}$ (i=0…n), $x_i\in A$, называется **цепью непоср. предшеств**. элементов длины n, соединяющей x c y, если выполнены следующие условия: 1)$x=x_o$,$y=x_n$ 2)$x_{i-1}R$^x_i(i=1...n)
Теорема: (A,R)-конечное упор.мн-во, тогда у этого мн-ва 1)$\exists$ наиб.(наим) элемент, и притом единств.2) $\exists$ и единств. максимальный элемент этого мн-ва, совпадающий с его наиб.(наим) элементом.3)$x,y\in A$,$x\neq y$,xRy, тогда $\exists$ цепь непоср.предшеств. элементов, соединяющая x с y.
Док-во:1)Возьмем произвольный элемент $x_o\in A$. Если x_o есть наибольший элемент, то $\exists$ доказано. Если нет, тогда $\exists$ $x_1\in A$: x_oRx_1. Если x_1 - наибольший, то $\exists$ доказано. Иначе $\exists$ $x_2\in A$: x_1Rx_2 и т.д. Допустим, что уже выбрано n+1 элементов. В силу свойства транзитивности: x_oRx_n. В силу конечности мн-ва A процесс должен прерваться за конечное число шагов. Элемент x_n , выбранный на последнем шаге, по определению будет являться наибольшим: $\forall x\in A$: xR x_n . (!) Пусть a, a' – наибольшие элементы A по отношению порядка R, тогда $\forall x\in A$: xRa, xRa'. В частности: aRa', a'Ra. Из антисимметричности отношения порядка следует: a=a'.
2) Пусть a есть наибольший элемент множества A, согласно п.1 такой элемент существует и единственен. Покажем, что a=max A. Пусть max A=a'$\neq$a, a'$\in$A, тогда $\forall x\in A$, a'Rx$\Rightarrow$a'=x. Пусть x=a: a'Ra $\Rightarrow$ a'=a. В данном случае a'Ra допустимо, т.к. по условию a есть наибольший элемент в A. То, что maxA=a, следует прямо из определения наибольшего элемента.
3) Для $\forall$ пары (x,y) такой, что $x\neq y$, xRy, в конечном уп-ом мн-ве (A,R) введем характеристику $\theta(x,y)$ – число элементов, лежащих между x и y. Говорят, что z лежит между x и y, если xRz и zRy и $z\neq x$ и $z\neq y$. Проведем индукцию по $\theta(x,y)$. Базис индукции: $\theta(x,y)=0\Rightarrow$ xR^y, $z_1=x$, $z_2=y$ - цепь построена.] $\forall$ v, $w\in A$, $\theta(v,w)\leq n_o$ - теорема справедлива $\Rightarrow$ док-ем для $\forall$ x, $y\in A$, $\theta(x,y)=n_o+1$.] z лежит между x и y, тогда: $\theta(x,z)\leq n_o$, $\theta(z,y)\leq n_o$. По предпо-ию индукции: $\exists$ $\{x_i^{(1)}\}$ (i=0…n_{xz}), $\{x_i^{(2)}\}$(i=0…n_{zy}). Рассмотрим $\{x_i\}$(i=0...$n_{xz}+n_{zy}$): $x_i=\{1)x_i^{(1)}$,если $0\leq i\leq n_{xz}$;2)$x_{i-nxz}^{(2)}$, если $n_{xz}<i\leq n_{xz}+n_{zy}\}$. Ясно, что $\{x_i\}$-искомая цепь.

Покоординатный порядок(частичный).
Лексикографический порядок(линейный элемент): $a(a_1,...,a_n)$,$b(b_1,...,b_n)$; $a<b\Leftrightarrow\exists k$, $a_i=b_i$,i=1,...,k-1$\Rightarrow a_k<b_k$

Билет 4.
1)Правило суммы: Если A, B – конечные множества, $A\cap B=\varnothing$, то $|A\cup B|=|A|+|B|$. Обобщение правила суммы:$A_1,...,A_n$, $A_i\cap A_j=\varnothing$ ...
2) Правило произведения:Если A, B – конечные множества, $|A\times B|=|A|*|B|$. Обобщение правила произведения:$|A_1|*...*|A_n|$. Если $A_1=...=A_n$, $|A^n|=|A|^n$
3)Правило равенства: Если $\exists$ f: $A\leftrightarrow B$, то |A|=|B|
Опр. Характерестическим вектором мн-ва X называется двоичный набор ($h_1...h_n$), такой что, если $A=\{a_1,...,a_n\}$, $X=\{x_1,...,x_k\}$, то $h_i=\{1$,если $a_i\in X$; 0,если $a_i\notin X\}$,$a_i\in A$, i=1..n
Теорема: $\forall$ конечного мн-ва A: $|2^A|=2^{|A|}$. Док-во:] $A=\{a_1...a_n\}$. Каждому подмн-ву $X\subseteq A$ поставим в соответствие хар-ий вектор: h:$2^A\leftrightarrow E^n$, тогда по правилу равенства $|2^A|=|E^n|=|E|^n=2^n=2^{|A|}$ ($E=\{0,1\}$)
Опр. $A=\{a_1,...,a_n\}$-кон-ое мн-во. Набор элементов ($a_{i1}...a_{ik}$) из A называется (n,k)-**выборкой**. *Выборка может быть упорядоченной и неупорядоченной.*
1.Перестановки с повторениями (ПП) - упорядоченная выборка с повторениями
2. Перестановки без повторений (ПбП) - упорядоченная выборка без повторений
3.Сочетания с повторениями(СП)-неупорядоченная выборка с повторениями
4. Сочетания без повторений(СбП)-неупорядоченная выборка без повторений
Теорема:Число (n,k) ПП равно n^k.Док-во: Будем делать выбор из мн-ва $I_n=\{1...n\}$.(n,k)-ПП, есть элементы мн-ва I_n^k. Согласно обобщенному правилу произведения, $|I_n^k|=|I_n|^k=n^k$

Теорема: Число (n,k) ПбП равно $P_n^k=n!/(n-k)!$ Док-во: Первый элемент перестановки может быть любой из I_n. Поскольку повторения недопустимы, второй элемент можно выбрать (n-1) способами, третий (n-2) и ..., k-ый - (n-(k-1)) способами. В итоге: $P_n^k=n(n-1)(n-2)...(n-(n-k+1))=n!/(n-k)!$

Правило последовательного выбора: Упорядоченный набор $(x_1...x_n)$ формируется в результате последовательного выбора элементов $x_1...x_n$, причем $\forall i\in\{1...n\}$ элемент x_i можно выбрать k_i способами. Тогда весь набор можно выбрать $k_1...k_n$ способами. Док-во: 1) Для n=2 док-но; 2) $(x_1,...,x_{n-1})$ - ист, док-ем для $(x_1,...,x_{n-1},x_n)$. $(x_1,...,x_{n-1})$ - можно выбрать $k_1...k_{n-1}$ способами, а x_n-k_n. След-но $(x_1,...,x_{n-1},x_n)$- $k_1...k_n$ способами.

Теорема. Число (n,k)-СбП равно $\binom{n}{k}=C_n^k=n!/(n-k)!k!$ Док-во: Выпишем элементы (n,k)-сочетания без повторений в нек-ом порядке. Поскольку k элементов можно упорядочить k! способами, то из каждого сочетания можно образовать k! различных перестановок, причем каждая перестановка будет получена только один раз. Значит $P_{n,k}=k!\binom{n}{k} \Rightarrow C_n^k=n!/(n-k)!k!$. **Сл-ия: 1)** $C_n^0=C_n^n=1$; **2)** $C_n^1=C_n^{n-1}=n$; **3)** $C_n^k=C_n^{n-k}$ **4)** $C_n^k=C_{n-1}^{k-1}+C_{n-1}^k$

Теорема: Число (n,k) - СП равно $C^k_{n+k-1}=(n+k-1)!/k!(n-1)!$ Чтобы задать СП из n по k, достаточно указать для каждого числа от 1 до n, сколько раз оно встречается в данном С.] k_i есть кол-во вхождений числа $i\in\{1\ldots n\}$ в С(кратность вхождения). Т.к. общее число элементов в С равно k, то $\Sigma^n_{i=1}k_i=k$. В алфавите $E=\{0,1\}$ поставим в соответствие данному сочетанию слово. В начале слова поставим k_1 нулей, затем единицу, за ней k_2 нулей, единицу и т.д. Все слово будет состоять из n групп нулей, разделенных единицами, причем в i-ой группе число нулей равно k_i . Сл-но, слово будет состоять из k нулей и n-1 единицы, его длина равна n+k-1. Обратно, если взять любое слово, то по нему можно построить (n, k)-СП: нули разбиваются единицами на n групп, число i необходимо включить в СП столько раз, сколько нулей в i-ой группе. Таким образом, $\exists$ (n, k)-СП $\leftrightarrow\alpha\in L(E)$, $l(\alpha)=n+k-1$, в α k нулей. Число таких слов: $\binom{n+k-1}{k}$ или $C^k_{n+k-1}=(n+k-1)!/k!(n-1)!$

Билет 5.

Бином Ньютона: $(x+y)^n=\Sigma^n_{k=0}C^k_n x^{n-k}y^k$. Док-во: по индукции: 1)при n=1 очевидно 2)Предполог. для n и док-ем для n+1: $(x+y)^{n+1}=(x+y)^n(x+y)=x^{n+1}+(C^1_n+C^0_n)x^n y+...+(C^{k+1}{}_n+C^k_n)x^{n-k}y^{k+1}+...+y^{n+1}$. Пользуясь $C^{k+1}{}_n+C^k_n=C^{k+1}{}_{n+1}$(1), получим нужную формулу, в которой n заменено на n+1. (1) док-ся легко:] дан n+1 элемент, из которых составляются С по k+1 элементов. Зафиксируем один из этих элементов; тогда число С, в которые вошел этот элемент, равно C^k_n. А число С в которые он не вошел равно C_n^{k+1} .

Опр: Разбиением множества А на k частей называется семейство его подмножеств, такое, что: 1) $A_i\cap A_j=\varnothing$ при $i\neq j$; 2) $\cup^n_{i=1}A_i=A$; Если порядок частей существенен, говорят , что рассматриваются **упорядоченные разбиение.**

Теорема:Число упорядоч. разбиений n эл-ов по k частей: k^n

Теорема:Число упорядоченных разбиений множества мощности n на k частей мощностей $n_1+...+n_k=n$ равно $\binom{n}{n_1...n_k}=n!/(n_1!...n_k!)$ **(полиномиальный коэффициент)**. Док-во: Первую часть разбиения можно выбрать C_n^{n1} способами, после чего останется $n-n_1$ элементов для выбора. Из них вторую часть разбиения можно выбрать C^{n2}_{n-n1} способами. По принципу последовательного выбора, общее число разбиений равно произведению $\binom{n}{n1}\binom{n-n1}{n2}...\binom{n-n1-...-nk-1}{nk}$. После выполнения сокращений получим $n!/(n_1!...n_k!)$

Теорема. Число слов в алфавите $A=\{a_1...a_k\}$, в которых буква a_i встречается n_i раз, $i=1\ldots k$, $n_1+...+n_k=n$ равно $\binom{n}{n1...nk}$ Док-во: Занумеруем позиции букв в слове числами от 1 до n слева направо.] P_i есть мн-во номеров всех позиций, в которых находится буква a_i, $i=1\ldots k$. Семейство множеств $P_1...P_k$ есть упорядоченное разбиение множества $I_n=\{1...n\}$ и это семейство однозначно определяет слово. Таким образом, $\exists$ взаимно однозначное соответствие между словами, число которых нужно найти, и упорядоченными разбиениями.

Полиномиальная теорема: $(x_1+...+x_k)^n=\Sigma_{n1+...+nk}x_1^{n1}...x_k^{nk}\binom{n}{n1...nk}$ Раскроем скобки, не группируя одинаковые сомножители и не приводя подобные. Множество всех слагаемых, полученных таким образом есть множество всех слов длины n в алфавите $\{x_1...x_k\}$. После группировки одинаковых сомножителей слагаемые этой суммы примут вид $x_1^{n1}...x_k^{nk}$, где $n_1+...+n_k=n$, причем такое слагаемое встретится столько раз, сколько имеется слов, в которых буква x_1 встречается n_1 раз, буква x_2 - n_2 раз и т.д. после приведения подобных коэффициентов при $x_1^{n1}...x_k^{nk}$ согласно предыдущей теореме, будет равен $\binom{n}{n1...nk}$

Билет 6

Метод включения и исключения

Билет 7.

Число разбиений конечного мн-ва(число упорядоч. разбиений без пустых мн-в).

Опр.Х-любое мн-во, представленное в виде семейства q непустых непересекающихся подмн-в $P_1,...,P_n=X$ таких, что $P_1\cup...\cup P_n$. Такое семейство $q=\{P_1,...,P_n\}$ называется **разбиением** мн-ва X.

] A_i - мн-во таких разбиений, у кот-ых i часть пустая. $A_i=\{(P_1,...,P_k)$ - разбиение$|$ $P_i=\varnothing\}$. $A=P_1\cup...\cup P_n$.

$|A_1\cup...\cup A_n|$ - число разбиений, у которых есть пустая часть. Число разбиений без пустых частей = $n^k-|A_1\cup...\cup A_n|$. $|A_{i1}\cap A_{i2}\cap...\cap A_{ij}|=(n-j)^k$. $S_j=\Sigma_{\{i1,...,ij\}\subseteq\{1,...,n\}}|A_{i1}\cap A_{i2}\cap...\cap A_{ij}|$ - одно слагаемое в ф-ле вкл. искл. $S_j=\binom{n}{j}(n-j)^k$. $S_{k,n}=n^k-\binom{n}{1}(n-1)^k+...+(-1)^j\binom{n}{j}(n-j)^k+...+(-1)^n\binom{n}{n}(n-n)^k$. $S_{k,n}=\Sigma^{n-1}_{j=0}(-1)^j\binom{n}{j}(n-j)^k$ - число неупоряд. разб. без пустых частей k - эл-го мн-ва на n-частей. Упорядочить можем n! способами$\Rightarrow S`_{k,n}=(1/n!)\Sigma^{n-1}_{j=0}(-1)^j\binom{n}{j}$(n-

$j)^k$ - число Стирлинга 2 рода.(число упоряд. разб. без пустых частей k - эл-го мн-ва на n-частей). Число отношений экв-ти:$b_k=\Sigma^k_{n=1}(1/n!)\Sigma^{n-1}_{j=0}(-1)^j(^n{}_j)(n-j)^k$ - число Белла
.⊆ ⊂ ⊇ ⊃ ∪ ∩ ¬ ∅ ⊕ ≠ ± ∈ ∉ ∀ ∃ ∍ Σ ∏ ⇔ ⇐ ⇒ ≤¬⊄→

Билет 8.

Графы очень часто используются в различных приложениях, поскольку они возникают как модель при изучении многих объектов. Н.: структура молекулы, схема дорог, блок-схема алгоритма и т.п. **Графом** *G называется любая пара (V,E), где V={v_1,v_2,...} - мн-во элементов любой природы, а E={e_1,e_2,...}-семейство пар элементов из V,* причем допускаются пары вида (v_i,v_i) и одинаковые пары. Если пары в V рассматриваются как неупорядоченные, то граф называется **неоринтированным**, если как упорядоченные, то граф называется **ориентированным**(*орграфом*). Элементы мн-ва V называются **вершинами** графа, а пары из E - его **ребрами**; в орграфе - дуги. Говорят ребро *соединяет* вершины,а дуга *идет* из v_1 в v_2. Говорят, что вершины **смежны**, если в E входит пара из них, а данное ребро **инцидентно** им. Пара вида (v_i,v_i) называется **петлей** в вершине v_i. Если пара (v_i,v_j) встречается более одного раза, то говорят, что (v_i,v_j) - **кратное ребро**. Граф с кратными ребрами называется **мультиграфом(**без них - **простой)**, а еще и с петлями - **псевдографом**. **Обыкновенный граф** - неор, простой, без петел.

Способы задания графов: 1)Мн-ми V и E(перечислением) 2)Изображение(рисунок) 3)Матрицей смежности(a_{ij}={1,(i,j)∈E; 0,(i,j)∉E}); 4)Матрицей инцидентности(для этого надо пронумеровать вершины от 1 до n и ребра от 1 до m: a_{ij}={1, если вершина инцидентна ребру j;0, в противном случае}) 5)Списком смежности: a:b,c,e; b:a,d,c (с кем смежны) и т.д.

Опр. Степенью вершины в неор. графе называется число ребер, инцидентных данной вершине. Вершина степени 0 называется **изолированной.**

Лемма о рукопожатиях. Пусть в графе G p вершин и q ребер. Пусть deg v_i - степень вершины v_i. Тогда $\Sigma^p_{i=1}$deg v_i=2q. (Вычисляя сумму всех степеней мы каждое ребро считаем 2 раза)

Пустой граф O_n=(V,O) - граф не имеющий ребер

Полный граф K_n=(V,V_2) - граф, ребрами которого явл. всевозможные пары его вершин(петель нет)

Теорема:g_n-число графов с n-вершинами. $g_n=2^k$, где k=($^n{}_2$). А если с петлями(т.е. с повторами), то k=n(n+1)/2;

Опр. Граф G_1={V_1,E_1} называется **подграфом(3)** графа G={V,E}, если V_1⊆V, E_1⊆E. 1)**Остовной подграф** - могут удаляться только ребра(V`=V); 2) **Порожденные подграфы** - удаляются вершины и их ребра

Опр. Графы G_1={V_1,E_1} и G_2={V_1,E_1} называются **изоморфными**, если ∃ такая биекция f:V_1→V_2, что вершины x,y образуют (x,y)∈E_1↔(f(x),f(y))∈E_2(*т.е. если можно поменять названия вершин одного графа так, что получится второй*)

Инвариант - числовая хар-ка, которая сохраняется при изоморфизме(число вершин, ребер, степень вершин, набор степеней и т.п.)

Билет 9.

Маршрутом в графе называется последовательность вершин(v_1,...,v_k), где все (v_i,v_{i+1})∈E. **Длина маршрута** - это число ребер в нем(k-1). **Путь** - это маршрут, у которого все ребра различны. **Простой путь** - путь, у которого все вершины разные. **Замкнутый маршрут** - если v_1=v_k. **Цикл** - замкнутый путь. **Простой цикл** - цикл, у которого все вершины разные кроме x_1=x_k

Лемма1.Если в графе есть маршрут соединяющий 2 вершины, то в нем есть и простой путь соединяющий эти вершины. Док-во: Есть м-т x_1,....,x_k , и пусть есть повтор-ся вершины x_i=x_j(i<j). Имеем, x_1,...,x_i,$\underline{x_{i+1},...,x_j}$,$x_{j+1}$,...,$x_k$. Подчеркн. удаляем. Получается x_1,...,$\underline{x_i,x_{j+1}}$,...,x_k - простой путь, т.к. (x_i,x_{j+1})=(x_j,x_{j+1})∈E

Лемма2.Если в графе есть цикл, проходящий через нек-ое ребро, то и есть простой цикл, проходящий через это ребро. Док-во: циклу **Z** соответствует путь **P**, который соединяет вершину **d**. По предыдущей теореме ∃ прстой путь **P**′,соединяющий вершину **d,** но это есть искомый простой цикл **Z** '

Лемма3.Если в графе степень каждой вершины не меньше 2, то в этом графе ∃ цикл.Док-во: Возьмем в графе простой путь наибольшей длины x_1…x_k . Рассмотрим последнее ребро этого пути (**x_{k-1},x_k**). Определим, найдётся ли в графе ребро (x_k,y) такое, что y∉{x_1,..,x_{k-1}}. Не может быть по усл, иначе x_1....x_k не наиб. длины. Отсюда получаем , что y∈{x_1,..,x_{k-1}}. Если положить y=x_i, i≤k-2, то x_i,x_{i+1},…x_i будет циклом.

Опр.Граф называется **связным**, если для любых двух несовпадающих вершин имеется соединяющий их маршрут. **Несвязный граф** состоит из **компонент связности** т.е. максимальные связные подграфы.

Зам.Граф можно разбить на компоненты связности , так как отношение существования маршрута из одной вершины в другую есть отношение эквивалентности, тогда, по теореме о факторизации, множество вершин графа можно разбить на конечное число классов эквивалентности.

Опр.Точка сочленения (**шарнир**) – это вершина , при удалении которой (вместе с инцидентными ей ребрами) увеличивается число компонент связности.

Перешеек-это ребро, при удалении которого увеличивается число компонент связности.

Лемма4.Ребро является перешейком ⇔когда не содержится ни в одном цикле.

Билет 10.
Маршрутом в графе называется последовательность вершин($v_1,...,v_k$), где все $(v_i,v_{i+1})\in E$. **Длина маршрута** - это число ребер в нем(k-1). **Путь** - это маршрут, у которого все ребра различны. **Простой путь** - путь, у которого все вершины разные. **Замкнутый маршрут** - если $v_1=v_k$. **Цикл** - замкнутый путь. **Простой цикл** - цикл, у которого все вершины разные кроме $x_1=x_k$. Граф с кратными ребрами называется **мультиграфом**
Опр:Цикл, соединяющий все ребра мультиграфа, называется **эйлеровым**, и мультиграф, в котором имеется эйлеров цикл, также называется эйлеровым.
Лемма о четных степенях вершин. Если степень каждой вершины конечного графа четна, то на графе существует хотя бы один простой цикл. Док-во: Выберем произвольную вершину графа. Так как ее степень по усл-ю четна, то $\exists$ по крайней мере два ребра, инцидентных выбранной вершине. Выйдем по одной из дуг из вершины. Вершина, в которую мы попадем, также имеет четную степень, а значит, кроме ребра, по которому мы пришли, есть еще ребро, по которому мы можем покинуть эту вершину. После прохождения через эту вершину мы будем отбрасывать ребра входа и выхода этой вершины. После отбрасывания ребер, степень пройденной вершины уменьшается на 2, и в результате остается четной. Таким образом, условие четности вершины гарантирует возможность обхода этой вершины при обходе графа. Двигаясь таким образом по конечному графу и игнорируя ребра, которые мы отбросили, мы не сможем все время оказываться в вершинах, в которых мы не побывали раннее (в силу конечности числа вершин графа). Тогда на одном из шагов обхода мы окажемся в вершине, в которой уже побывали ранее. Отрезок пути, заключенный между первым и вторым прохождением через эту вершину, будет циклом
Теорема (критерий эйлеровости графа). Для того чтобы конечный связный граф был эйлеровым, необходимо и достаточно,чтобы степени всех его вершин были четными числами. Док-во:
($\Longrightarrow$)Двигаясь по эйлеровому циклу, войдя в вершину по одной дуге, мы выходим из нее по другой, т.е. каждой дуге входа соответствует дуга выхода. Каждая такая пара дуг дает вклад, равный 2, в степень вершины, а поскольку эйлеров цикл содержит все дуги, то степень каждой вершины представлена суммой двоек, а значит, четна.
($\Longleftarrow$)Докажем индукцией по числу ребер графа. Основание индукции: n=1=|E|. Единственная дуга такого графа образует эйлеров цикл. Индуктивный переход: Доп-им, что утв-е Т. верно для $\forall$ графа, у которого $|E|\le n_0$. Док-ем, что тогда оно справедливо и для графа, у которого $|E|=n_0+1$. Так как степени всех вершин этого графа четны, то по Л. о четных степенях вершин, на графе существует простой цикл n. Если n проходит через все дуги графа G, то он и есть искомый эйлеров цикл. В противном случае в графе G оказываются непройденными некоторые ребра. Рассмотрим граф, полученный из G удалением дуг цикла n: G´. Каждая его компонента связности есть конечный связный граф с четными степенями вершин и числом дуг, не превосходящим n_0. Тогда, по предположению индукции, на каждой компоненте связности графа G´ существует эйлеров цикл. Обозначим эйлеровы циклы компонент как $n_1,...,n_k$ соответственно. Поскольку исходный граф связен, то цикл n имеет хотя бы по одной общей вершине с компонентами графа G´. Выберем по одной общей с циклом n вершине на каждой компоненте – $x_1,\dots x_k$. Искомый эйлеров цикл на графе G построим следующим образом. Начав обход цикла n из произвольной его вершины, будем двигаться по нему до тех пор, пока не встретим вершину $x_i\in\{x_1,\dots,x_k\}$, и затем от вершины x_i пойдем по эйлерову циклу n_i на соответствующей компоненте графа G´, после чего продолжим движение по циклу n до тех пор, пока не встретим вершину $x_j\in\{x_1,\dots,x_k\}$, снова прервем движение по n и пройдем по эйлерову циклу n_j соответствующей компоненты и т.д. В результате мы пройдем по всем циклам $n_1,...,n_k$, побывав во всех вершинах множества $\{x_1,\dots,x_k\}$
Опр.: Эйлеров путь - путь, который проходит через все ребра. **Необх. и дост. усл-ие $\exists$ эйлерова путь**: стартовая и финишная вершина должны иметь неч-ую степень, все остальные четную.(Сл-ие из пред. теоремы: добавим ребро между этими вершинами, и получится цикл)

Билет 11.
Опр.Граф называется связным, если для любых двух несовпадающих вершин имеется соединяющий их маршрут. Несвязный граф состоит из компонент связности т.е. максимальные связные подграфы. Деревом называется связный граф не имеющий циклов. Лес - не связный граф не имеющийй циклов. Т.о., компонентами связности любого леса являются деревья. Листьями дерева называются вершины со степенью 1. !*Листья имеются во всех деревьях с 2-х или более вершинами*.
Теорема: Для того, чтобы граф был деревом, необходимо и достаточно выполнение двух любых условий из: 1)граф связен; 2)граф не имеет циклов; 3)|E|=|V|-1 Док-во:
(1) и (2) $\Rightarrow$ (3) Докажем, что дерево с n вершинами содержит n-1 ребро. Индукция по n: Основание индукции: **n=2**-очевидно. Индуктивный переход: **n-1$\rightarrow$ n** .] Дерево T содержит n вершин. Удалим из T один лист и инцидентное ему ребро. Получим новое дерево, содержащее **n-1** вершину и, по предположению индукции, **n-2** ребра. Значит, исходное дерево T содержит **(n-2)+1=n-1** ребро.
(1) и (3)$\Rightarrow$ (2) Докажем, что связный граф, в котором |E|=|V|-1 , является деревом (т.е. докажем, что в таком графе нет циклов). Допустим, что в таком графе имеется цикл. Удалим ребро цикла. Это ребро содержится в

цикле, поэтому не является перешейком, следовательно, при удалении этого ребра связность графа не нарушится. Если в исходном графе **G** было m ребер, то в полученном графе **G'** ребер будет **m-1**. Если есть еще циклы, то удалить из каждого по одному ребру, т.е. получится в G` m-k ребер.В полученном графе **G'** не будет циклов, но он является связным по построению, следовательно, **G'** есть дерево по определению. **G'**-дерево, значит, должно быть выполнено условие **m-k=n-1**⇒ k=0⇒**нет циклов** противоречие.
(2) и (3)⇒(1) Докажем, что граф без циклов,в котором |E|=|V|-1, является деревом (т.е. докажем, что этот граф является связным). Рассмотрим лес **F,** имеющий **k** компонент связности $\mathbf{G_1,...,G_k}$ при этом каждый компонент леса является деревом,поэтому выполнены соотношения:$m_1=n_1-1$ .... $m_k=n_k-1$. Просуммируем соотношения $m_1+...+m_k=n_1+...+n_k-k$ **. Т.е. |E|=|V|-k .** Но по условию |E|=|V|-1⇒k=1, значит, в лесу всего один компонент связности, значит этот лес связен.
Теорема. В любом дереве: 1)при удалении любого ребра нарушается связность(все ребра перешейки)(т.к. в дереве нет циклов⇒ ни одно ребро не содержится в цикле⇒по Л. все ребра перешейки 2)при добавлении любого другого ребра образуется цикл 3) для любых 2-х вершин ∃ единств. соед-ий их путь(если было бы 2, то был бы цикл)

Билет 12.
Метрические характеристики связности.
Опр:Длина кратчайшего пути, соединяющего вершины x,y, называется **расстоянием** между этими вершинами и обозначается **d(x,y). d(x,x)=0; d(x,y)=1, x,y**∈E**; d(x,y)** ≡ ∞ **,** если в разных компонент связности. **Аксиомы метрики (аксиомы Фреше): 1**)d(x,y)≥0; 2)d(x,y)=0 ⟺ x=y; 3)d(x,y)= d(y,x); 4)d(x,z)≤ d(x,y)+ d(y,z)(нер-во треуг.)
Опр: Эксцентриситетом вершины называется расстояние от данной вершины до наиболее отдаленной от нее: **ecc a=max{d(a,b), b**∈V **}** Максимальный из всех эксцентриситетов вершин называется **диаметром** графа: **diam G=max{ecc a, a**∈**V}**
Опр.Минимальный из эксцентриситетов вершин графа G называется его **радиусом**: **rad G=min{ecc a, a**∈**V }**
Опр:Вершина a называется **центральной**, если ecc a = rad G. Множество всех центральных вершин называется **центром** графа.
Теорема: <u>∀ графа G: rad G≤ diam G ≤ 2rad G</u> Док-во: min{ecc a, a∈ V } ≤ max{ecc a, a∈ V } ⟹ rad G≤ diam G .] d(a,b)= diam G, *c*-центральная вершина: ecc c= rad G: diam G= d(a,b) ≤ d(a,c)+ d(c,b) ≤2 ecc c= rad G
Теорема о центре дерева. <u>Центр дерева состоит либо из одной вершины(**центральный**), либо из двух(**бицентральный**)</u>.Док-во: 1)n=1 - центр это вершина; n=2 - центр две эти вершины;2)По индукции: для <=n-1 док-но, док-ем для n. Удалим все листья дерева T, тогда получится дерево T_1. ecc(x)(T_1)=ecc(x)(T)-1, но центр C(T_1)=C(T). Т.к. по предположению индукции, C(T_1) состоит либо из 1 либо из 2 вершин, то и у T также.

Билет 13.
Опр:Геометрическим графом называется граф, вершинами которого являются точки, а ребрами - непрерывные прямые. **Плоским графом** называется граф, ребра которого не имеют других общих точек, кроме вершин. Граф называется **планарным**, если он изоморфен некоторому плоскому геометрическому графу. Плоский граф G разбивает плоскость на несколько областей, называемых его **гранями или** др. словами грань, это связанные участки, получ-ся при разрезании пл-ти по ребрам. x и y являются **соединенными**, если существует непрерывная соединяющая их линия, не пересекающая граф. Очевидно, что это есть отношение эквивалентности, поэтому по теореме о факторизации оно разбивает плоскость на множество классов. Число граней не зависит от геометрической реализации графа.
Теорема (формула Эйлера).<u>Для любого связного плоского графа:n-m+r=2,</u> где r-число граней, n=|V|,m=|E| Докажем теорему по индукции числа ребер m с фиксированным числом вершин n. 1)Базис индукции m=n-1 G-связный граф, m=n-1⇒ G-дерево,значит в G нет циклов. Тогда r=1 (только одна грань, внешняя). Отсюда n-m+r=n-(n-1)+1=2. 2)Индуктивный переход.] для m∈[n-1,m_o) теорема справедлива.Покажем,что она справедлива и для m=m_o.G-связный граф с n вершинами и m_o ребрами, образующий r граней. Поскольку m_o>n-1,то G - не дерево,значит в G есть цикл.] В цикл входит ребро e,тогда к нему с двух сторон примыкают разные грани.Удалим из G ребро e,тогда две грани сольются в одну,а полученный граф G_1 останется связным(цикл стал путем,e-не являлось перешейком,поэтому по лемме о перешейке число компонент связности не изменилось). При этом получится планарный граф с n вершинами, m_o-1 ребрами и r-1 гранями.Т.к. m=m_o-1 ,то справедлива (по предположению индукции) формула Эйлера,т.е. n-(m_0-1)+(r-1)=2, или n-m_0+r=2(для первонач. графа)
Сл-ие1: <u>Число граней плоского графа с k компонентами связности определяется формулой r=m+k-n+1</u>.Число граней i-й компоненты связности плоского графа выражается формулой $r_i=m_i-n_i+1$. При суммировании f_i по i=1…k внешняя грань ,будет учитываться k раз, поэтому $f=\Sigma^k_{i=1}f_i-k+1=\Sigma^k_{i=1}(m_i-n_i+2)-k+1=m-n+2k-k+1=m-n+k+1$

Сл-ие2: $\forall$ планарного графа с $n\geq3$ выполняется нер-во: $m\leq 3n-6$. Док-во:1) нет циклов$\Rightarrow$дерево:$m=n-1$,$n-1\leq 3n-6$. 2)цикл есть. занумеруем грани(1,2,...,r).] a_i - число ребер в границе грани i. $S=\Sigma^{r}_{i=1}a_i$, $a_i\geq3\Rightarrow S\geq 3r$. Но $S\leq 2m$(каждую посчитали один или 2 раза) $\Rightarrow 3r\leq 2m\Rightarrow 3(m-n+k+1)\leq 2m\Rightarrow m\leq 3n-3k-3, k\geq1\Rightarrow m\leq 3n-6$
Сл-ие3: $\forall$ Планарного графа, в котором длина циклов строго больше 3 и $n\geq3$, выполняется нер-во $m\leq 2n-4$. Доказательством аналогично следствию 2,отличие заключается в том что мы полагаем $a_i\geq4$,а не $a_i\geq3$.
Сл-ие4: <u>Граф K_5 - непланарен</u>. |V| =5,|V|=10. $10\leq 3*5-6=9$ - противоречие
Сл-ие5: <u>Граф $K_{3,3}$ - непланарен</u>**.** **9**$\leq 2*6-4=8$
$\subseteq \subset \supseteq \supset \cup \cap \varnothing \oplus \neq \pm \in \notin \forall \exists \ni \Sigma \prod \Leftrightarrow \Leftarrow \Rightarrow \leq$
Опр. Подразбиением ребра (a,b) называют его замену на два ребра (a,c) и (c,b), где *c*-новая вершина графа.
Опр: Графы G_1 и G_2 называются гомеоморфными, если они с помощью конечного числа процедур подразделения ребер могут быть превращены в изоморфные. Ясно, что гомеоморфные плоские графы имеют одинаковое число граней.
Теорема Понтрягина-Куратовского: Граф является планарным тогда и только тогда, когда он не содержит подграфа, гомеоморфного K_5 и $K_{33.}$

Билет 14.
Опр: **Двудольным графом** G(V,E) называется граф, множество вершин которого можно разбить на два подмножества $V=V_1\cup V_2$, $V_1\cap V_2=\varnothing$ так, чтобы каждое ребро соединяло вершины из разных подмножеств.
Теорема:<u>C_n(цикл - граф спец.вида) двудольный$\Leftrightarrow$когда содержит четное число вершин.</u> Док-во:Доп-им в цикле нечетн. число вершин. 2p вершин распадуться на два класса, а (2p+1)-ую вершину, если разместить в один класс, то она будет соединена с 2p-й вершиной, а если в другой-то с 1-ой вершиной. Т.о. граф не двудолен.
Теорема Кенига. <u>Граф является двудольным тогда и только тогда, когда в нем нет циклов нечетной длины</u>.
$\Rightarrow$] $(V_1,V_2;E)$ - двудольный граф,] $a_1,..., a_{2k+1}, a_1$ - простой цикл нечетной длины.] $a_1\in V_1, a_2\in V_2$... Т.о., $a_1,a_{2k+1}\in V_1$,(a_1,a_{2k+1}) $\in E$ что противоречит двудольности.
$\Leftarrow$Не ограничивая общности, будем считать что G-связный граф, т.к.каждую компоненту связности можно рассматривать отдельно. Разобьем множество V на $V_1,V_2,V_1\cup V_2=V$, следующим образом. В первую долю мы поместим произвольную вершину a. Далее из множества V\{a} в первую долю поместим вершины, расстояние от которых до a есть четное число, а во вторую - для которых это число нечетное.
Доп-им в одной доле есть две вершины, соединенные ребром. Для определенности: $b,c\in V_2$, $(b,c)\in E$
Рассмотрим два кратчайших пути из a в b и c, т.е. d(a,b)=l(a,…,b), d(a,c)=l(a,…,c). Тогда по построению множества V_2 числа d(a,b),d(a,c) нечетные. Эти кратчайшие пути имеют общие вершины (по крайней мере a).Рассмотрим наиболее удаленную от a общую вершину этих путей, обозначим ее как a` (может оказаться, что a`=*a*). Тогда, длина цикла составленная из: (a`,b)$\cup$(b,c)$\cup$(c,a`) равна
(a',b)+d(b,c)+d(c,a`)=d(a`,b)+1+d(c,a`)=2d(a`,b)+1(нечетная) есть простой цикл нечетной длины, что противоречит начальным условиям теоремы. Аналогично можно рассмотреть случай, когда $b,c\in V_1$ - получим тот же результат.
$K_{p,q}$ - полный двудольный граф

Билет 15.
Опр:Логической (булевой) функцией называют произвольное отображение вида $f:E^n\to E$
($f:\{0,1\}^n\to\{0,1\}$), $f = f(x_1,…,x_n)$ (функция от n переменных)
Операции: 1)Отрицание 2)Конъюнкция 3)Дизъюнкция
Формулы булевой алгебры (высказываний) строятся из логических переменных a,b,c,… и логических констант 0 и 1 с помощью логических операций. 1)Имя переменной – формула (0-формула, 1-формула, x - формула); 2) A-формула $\Rightarrow(\neg A)$ - формула. 3) A,B-формула $\Rightarrow$(A&B),(AvB) - формула
Соглашения при построении формул:1)Опускаем внешние скобки; 2) $\neg x=x^-$ 3) & сильнее v; 4)$x_1\&x_2=x_1x_2$
Свойства элементарных ф-ий(основные тождества):1) x & 0 = 0; x & 1 = x; xv0=x; xv1=1; 2)x&x=x; xvx=x; x&¬x=0; xv¬x=1 3)x= ¬(¬x) 4)Коммутативность: $x_1\&x_2=x_2\&x_1$; $x_1vx_2=x_2vx_1$ 5)Ассоциативность: $x_1\&(x_2\&x_3)=(x_1\&x_2)\&x_3=x_1x_2x_3$; $x_1v(x_2vx_3)=$... 6)Дистрибутивность:$x_1\&(x_2vx_3)=x_1\&x_2vx_1\&x_3$; $x_1v(x_2\&x_3)=(x_1vx_2)\&(x_1vx_3)$ 7)Законы де Моргана: $\neg(x_1\&x_2)=(\neg x_1)v(\neg x_2)$; $\neg(x_1vx_2)=(\neg x_1)\&(\neg x_2)$
8)$x_1vx_1x_2=x_1$,x(xvy)=x - законы Поглащения
Опр: Формулой, **двойственной** к формуле $A(x_1,...,x_n)$, называется формула $A^*(x_1,...,x_n)$, которая получается из A заменой v на &, & на v,1 на 0, 0 на 1.
Лемма. <u>Для любой булевой ф-лы A:A*=¬(A(¬x))</u> Док-во: Пусть k - число опраций в A:1)k=0:a)A=x, A*=x; ¬A(¬x)= ¬(¬x)=x; b)A=0, A*=1; ¬A(¬x)= ¬0=1 c)A=1 ... 2)Для k=n-1 выполняется. Док-ем для k=n: a)проверяем операцию отрицание, т.е. n-операция над B: A=¬B(в B n-1 операция), по предпол. индукции B*=¬B(¬x); A*=¬(B*)=¬(¬B(¬x))= ¬A(¬x) b)проверяем конъюнкцию: $A=B_1\&B_2$, $B_1^*=\neg B_1(\neg x)$, $B_2^*=\neg B_2(\neg x)$; $A^*=B_1^*vB_2^*= \neg B_1(\neg x)v(\neg B_2(\neg x))= \neg(B_1(\neg x)\& B_2(\neg x))=\neg A(\neg x)$ c)$A=B_1vB_2$ .....
Теорема. <u>Если A=B$\Rightarrow$A*=B*;</u> Док-во:A(¬x)=B(¬x) $\Rightarrow$ ¬A(¬x)=¬B(¬x) $\Rightarrow$(по лемме)A*=B*

Билет 16.

x,a - логические переменные(т.е.$x,a\in\{0,1\}$). <u>$x^a=\{x$,если a=1; $\neg x$,если a=0$\}$</u> 1)$x^a=xa \vee (\neg x)(\neg a)$ 2)$x^a=1\Leftrightarrow x=a$ 3)$x_1^{a1}x_2^{a2}...x_n^{an}=1\Leftrightarrow x_i=a_i$ 4)$\neg(x^a)=\neg x^a$

Опр: Элементарной конъюнкцией называется конъюнкция логических переменных и их отрицаний, в которой каждая переменная встречается не более одного раза (включая ее вхождение под знаком отрицания). $x_{i1}^{ai1}x_{i2}^{ai2}\ldots x_{ik}^{aik}$, $\{i_1,\ldots,i_k\}\in\{1,2,\ldots,n\}$ Число переменных k, входящих в конъюнкцию, называют ее рангом. При k=0 ее считают пустой и полагают равной истине, при k=n ее называют **совершенной** (или полной).

Опр. Общий вид **элементарной дизъюнкции**: $x_{i1}^{ai1} \vee x_{i2}^{ai2} \vee ... \vee x_{ik}^{aik}$, $\{i_1,\ldots,i_k\}\in\{1,2,\ldots,n\}$

Опр: ДНФ называют дизъюнкцию неповторяющихся элементарных конъюнкций.

Общий вид ДНФ: $P=K_1 \vee K_2 \vee ... \vee K_s$, K_i -элементарные конъюнкции, $K_i\neq K_j$ при $i\neq j$

Опр: КНФ называют конъюнкцию неповторяющихся элементарных дизъюнкций.

Общий вид КНФ: $P=D_1\&D_2\&...\&D_s$, D_i -элементарные дизъюнкции, $D_i\neq D_j$ при $i\neq j$

Теорема. Для любой булевой формулы не явл. тожд. ложной $\exists$ эквивал. ДНФ. -||- не явл. тожд. истинной -||- КНФ. Док-во:] A=1 - тожд. $1=x \vee (\neg x)$ - ДНФ.] A=0 - тожд. $0=x(\neg x)$ - КНФ. **]** <u>A не тожд. ист. и не тожд. ложна., тогда $\exists$ и КНФ и ДНФ</u> **Док-во:] в A k операций:1)k=0 A=x - ДНФ и КНФ 2)K>0: а)A=$\neg$B;**

$B=K_1 \vee K_2 \vee ... \vee K_p$- ДНФ, $B=D_1\&D_2\&...\&D_q$ - КНФ (по предпол. индукции).

$A=\neg B=\neg(K_1 \vee K_2 \vee ... \vee K_p)=\neg K_1\&...\&\neg K_p$ - КНФ, т.к. : $\neg(x_{i1}^{a1}\&...\&x_{ik}^{ak})=\neg(x_{i1}^{a1}) \vee ... \vee \neg(x_{in}^{an})=x_{i1}^{a1\wedge}...$ - э.д.

б)$A=B_1B_2$; $B_1=K`_1 \vee K`_2 \vee ... \vee K`_p$; $B_1=D`_1\&D`_2\&...\&D`_q$; $B_2=K`_1 \vee K`_2 \vee ... \vee K`_r$; $B_2=D`_1\&D`_2\&...\&D`_s$;

$A=D`_1D`_2...D`_qD``_1D``_2...D``_s$ - КНФ.

$A=(K`_1 \vee K`_2 \vee ... \vee K`_p) \vee (K`_1 \vee K`_2 \vee ... \vee K`_r)=K`_1K``_1 \vee ... \vee K_i`K``_j \vee ... \vee K`_pK``_r=V^p_{i=1}V^r_{j=1}K`_1K`_j$. Если $K`_i=K``_j$ то делаем так:xx=x; $x(\neg x)=0$; $0 \vee x=x$;$x \vee x=x$

Опр. Аналогично ДНФ и КНФ, определяются понятия **СДНФ** и **СКНФ**, в которые входят только совершенные(полные) элементарные кон- и дизъюнкции соответственно.

Теорема. <u>$\forall$ булевской ф-лы не явл. тожд. ложной $\exists$ единств. эквивал. ей СДНФ</u>. Док-во: По предыд. теореме $\exists$ ДНФ, экв-ая данной ф-ле, из которой можно получить СДНФ(напр. $x \vee (\neg x)=1$,$x\&(\neg x))=0$). **Единств.:**] A и B - нек-ые различные СДНФ, эквив-ые ф-ле. Раз они различны, то $\exists$ слагаемое A, которого нет в B: $x_1^{a1}...a_n^{an}$. Рассмотрим случай, когда c=1, т.е. набор занч. перем.:$x_1=a_1,x_2=a_2...$.Ясно, что A=1. Возьмем произвольное слагаемое из B: $x_1^{b1}...x_n^{bn}$, и <u>рассмотрим его значение при данном наборе.</u> Т.к. никакое слагаемое из B не равно выбранному слагаемому из A, то хотя бы один множитель $b_i\neq a_i\Leftrightarrow a_i=(\neg b_i)$ или $b_i=(\neg a_i)$. $x_i^{bi}=x_i^{ai\wedge}=a_i^{ai\wedge}=\neg(a_i^{ai})=\neg 1=0$. Т.к. мы выбирали произв. слагаем. из B, зн. B=0, а A=1 (при данном наборе)

Билет 17.

Опр: Полиномом Жегалкина от переменных $x_1\ldots x_n$ называется ф-ла, полученная из 0,1,$\{x_1\ldots x_n\}$ путем применения конечного числа операций &, $\oplus$ и скобок, определяющих порядок действий. **Моном**: 1или $x_{i1}\ldots x_{ik}$ степени k. **Полином**: 0 или $A_1\oplus\ldots\oplus A_n$, где $A_1 \ldots A_n$ - различные мономы. **Степенью полинома** называют максимальное количество переменных в каждом мономе. n=2: $p(x_1,x_2)=a_0\oplus a_1x_1\oplus a_2x_2\oplus a_{12}x_1x_2$

Теорема: <u>Для любой формулы булевой алгебры существует ее представление полиномом Жегалкина, и притом единственное.</u> Док-во: **($\exists$)** Из предыдущих теорем известно, что для любой формулы существует ее представление в виде ДНФ или КНФ. Если $A\equiv 0$, то A –полином, если $A\equiv 1$, то A –моном. В ином случае получим из A эквивалентную ей ДНФ, а из ДНФ - полином Жегалкина. Для этого докажем, что операции $\vee$, $\neg$ выражаются через операции алгебры Жегалкина. Справедливы формулы: 1)$\neg a=a\oplus 1$ 2)$a \vee b=\neg(\neg a\neg b)=(a\oplus 1)(b\oplus 1)\oplus 1=ab\oplus a\oplus b$. Исключим в ДНФ операции $\vee$, $\neg$ по данным формулам, в результате получим искомый полином. **(!)**] По формуле A были получены полиномы P_1 и P_2 . Т.к. они различны, то некоторое слагаемое $c=x_{i1},\ldots,x_{ik}$ есть в P_1, но отсутствует в P_2. Рассмотрим случай, когда c=1, т.е. $x_{i1}=\ldots=x_{ik}=1$. Рассмотрим такой набор переменных $x_1,\ldots, x_n$, что $x_{i1}=\ldots=x_{ik}=1$, $x_j=0$, $j\notin\{i_1,\ldots,i_k\}$. Построим полином $P=P_1\oplus P_2$. В таком наборе переменных только слагаемое c в P будет истинным, а так как одинаковые слагаемые в P взаимно уничтожаются, то все остальные слагаемые в P будут ложными. Тогда: $P=P_1\oplus P_2=c=1$, $P_1\oplus P_2=1\Rightarrow P_1= P_2\oplus 1=\neg P_2$, то есть $P_1\neq P_2$ - противоречие.

Билет 18.

Опр: Логической (булевой) функцией называют произвольное отображение вида $f:E^n\to E$ ($f:\{0,1\}^n \to\{0,1\}$), $f = f(x_1,\ldots,x_n)$ (функция от n переменных). Число всевозможных наборов 2^n. Число логических ф-ий 2^k, где $k=2^n$.

Теорема. <u>$\forall$ Функции алгебры логики $f(x_1,\ldots,x_n)$ и $\forall k(1\le k\le n)$ справедливо равенство: $f(x_1,\ldots,x_n)=V_{a1\ldots ak}x_1^{a1}...x_k^{ak}f(a_1,...,a_k,x_{k+1},...,x_n)$.</u> Док-во:$\forall$ набора $\sigma=(\sigma_1,\ldots,\sigma_n)$ вычислим значение правой части на этом наборе. Как только хотя бы один из сомножителей будет равен нулю, вся конъюнкция обратится в 0.Таким образом, из ненулевых конъюнкций останется только одна, в которой $\sigma_i=a_i$ и $V_{a1\ldots ak}\sigma_1^{\sigma 1}...\sigma_k^{\sigma k}f(\sigma_1,..., \sigma_k, \sigma_{k+1},...,\sigma_n)$. А поскольку $x^x=1$, то указанное выражение равно в точности $f(\sigma)=f(\sigma_1\ldots\sigma_n)$

Сл-ие1: Любую ф-ию тождественно не равной нулю, можно представить СДНФ. Док-во: $f(x_1,...,x_n)=V_{(a1...an)}x_1^{a1}...x_n^{an}\ f(a_1,...,a_n)= V_{(a1...an):f(a1...an)=0}x_1^{a1}...x_n^{an}\ f(a_1,...,a_n)\ v\ V_{(a1...an):f(a1...an)=1}x_1^{a1}...x_n^{an}\ f(a_1,...,a_n)= V_{(a1...an):f(a1...an)=1}x_1^{a1}...x_n^{an}\ f(a_1,...,a_n)v0=V_{(a1...an):f(a1...an)=1}x_1^{a1}...x_n^{an}$ - СДНФ.

Сл-ие2 Любую лог-ую ф-ю можно представить булевой формулой(СДНФ):

Сл-ие3:Каждую лог-ую ф-ю можно представить формулой, составленной из этих 3-х операций(&,v,¬) Док-во: $\neg f(x_1,...,x_n)=V_{(a1...an):f(a1...an)=1}x_1^{a1}...x_n^{an}=\&_{(a1...an):f(a1...an)=0}(\neg x_1^{a1}v...v\neg x_n^{an})\Rightarrow f(x_1,...,x_n)=\neg V_{(a1...an):f(a1...an)=0}x_1^{a1}...x_n^{an}= \&_{(a1...an):f(a1...an)=0}(\neg x_1^{a1}v...v\neg x_n^{an})$ - СКНФ

Сл-ие4:Всякая ф-ия тождественно не равная единице, можно представить СКНФ.

Сл-ие5:Каждую лог-ую ф-ию можно представить полиномом Жегалкина.

Билет 19.

Опр.Переменную x_i называют **фиктивной** переменной булевой функции $f(x_1,…,x_n)$, если $\forall\ x_1,..,x_{i-1},x_{i+1},…,x_n$ $f(x_1,..,x_{i-1},0,x_{i+1},…,x_n)=f(x_1,..,x_{i-1},1,x_{i+1},…,x_n)$. Переменная, не являяющаяся фиктивной,называется **существенной.(т.е.** $\exists$ такой набор ... $\neq$**)**

Теорема: Если переменная фиктивна, то она не входит в полином Жегалкина.Док-во:] в P входит x_1. $P(x_1,...,x_n)=x_1Q(x_2,...,x_n)\oplus R(x_2,...,x_n)$, $Q\neq 0$(т.к. x_1 входит в P). Возьмем набор, чтобы $Q(a_1,...,a_n)=1$ $(x_1,a_1,...,a_n)=x_1\oplus R(x_2,...,x_n)(R()=c)=x_1\oplus c$. $x_1=0\Rightarrow P=c$, $x_1=1$, $P=1+c=\neg c$ - по опр. сущ-ая переменная.

Билет 20.

Определим **суперпозицию** функций алгебры логики как применение следующих операций: 1)**Подстановка**] $f(x_1,…,x_n)$, $g(y_1,…,y_n)$ -логическая функция: $h=f(x_1,…,x_{i-1}, g(y_1,…,y_n) , x_{i+1,…,}x_n)$ – суперпозиция f и g. 2) **Переименование переменных**:] $f(x_1,…,x_n) = f(y_1,…,y_n)$, т.е. $f(x_1,x_2,x_3)=f(x_3,x_1,x_2)=(x_3,x_1,x_2)$ 3)Введение и удаление фиктивных переменных. Определим символом P_2 мн-во всех логических функций.]$A\subseteq P_2$, $f\subseteq P_2$, f есть **суперпозиция функций** из А,если она может быть получена из нее рассмотренными выше тремя способами.

Опр. Замыканием А называется множество всех функций алгебры логики,которые можно выразить формулами из А (т.е. множество всех суперпозиций функций из А),и обозначается знаком [А]. Множество А называется **замкнутым классом**, если А=[А]. Примеры з. кл.: $[P_2]= P_2$, $A=\{1,x\}:[A]=A$, $A=\{0,\neg x\}:[A]\neq A$

Свойства замыкания: 1)$A\subseteq[A]$, 2)$[[A]]=[A]$, 3)$A\subseteq B\Rightarrow[A]\subseteq[B]$,

Опр. f,g называются **конгруэнтными**, если каждая из них может быть получена из другой только с помощью переименования переменных. Пр:$f(x_1,x_2)=x_1\rightarrow x_2$, $g(x_1,x_2)=x_2\rightarrow x_1$, но $h(x_1)=x_1\rightarrow x_1$ - не конгр. им

Опр. Система функций алгебры логики А называется **полной**, если $[A]= P_2$. $A=\{x_1x_2,x_1\oplus x_2,0,1\}$

Теорема: $A,B\subseteq P_2$, причем $[A]= P_2$, $\forall f\subseteq A,f\subseteq[B] \Rightarrow [B]= P_2$(если А –полная система, $f\subseteq A$ есть суперпозиция функций из В, то В-также полная система) Док-во: $[A]= P_2,\ \forall f\subseteq A$: $f\subseteq[B]\Rightarrow A\subseteq[B]\Rightarrow[A]\subseteq[[B]]\Rightarrow[A]\subseteq[B]$. Итак, $[A]\subseteq[B]$ и $[A]= P_2 \Rightarrow P_2\subseteq[B]$,но $[B]\subseteq P_2\Rightarrow[B]=P_2$ (B - полное)

Билет 21.

Опр. Замыканием А называется множество всех функций алгебры логики,которые можно выразить формулами из А (т.е. множество всех суперпозиций функций из А),и обозначается знаком [А]. Множество А называется **замкнутым классом**, если А=[А]. Примеры з. кл.: $[P_2]= P_2$, $A=\{1,x\}:[A]=A$, $A=\{0,\neg x\}:[A]\neq A$

Свойства замыкания: 1)$A\subseteq[A]$, 2)$[[A]]=[A]$, 3)$A\subseteq B\Rightarrow[A]\subseteq[B]$,

Опр: Формулой, **двойственной** к формуле $A(x_1,...,x_n)$, называется формула, которая получается из А заменой v на &, & на v,1 на 0, 0 на 1($A^*(x_1,...,x_n)= \neg(A(\neg x_1,..., \neg x_n))$.

Опр. Ф-ия самодвойственна $f\in S$, если $f=f^*$(двойственная). Пр. $f=0,f=1\notin S$; $f=x,f=\neg x\in S$.От 2-х переменных $f\in S$ не существует!

Док-ем, что S замкнуто(проверим только одно св-во:подстановку, а переим. перем и введ. и удал. фикт. перем. очевидно): $f,g\in S$. $h(x_1,...,x_n)=f(x_1,...,x_{n-1},g(x_1,...,x_n))$. $h^*(x_1,...,x_n)=\neg h(\neg x_1,...,\neg x_n)=\neg f(\neg x_1,..., \neg x_{n-1}, g(\neg x_1,...,\neg x_n))=\neg f(\neg x_1,..., \neg x_{n-1},\neg(\neg\ \mathbf{g(\neg x_1,...,\neg x_n)}))=\neg f(\neg x_1,..., \neg x_{n-1},\neg g(x_1,...,x_n))=f^*(x_1,...,x_{n-1},g(x_1,...,x_n))=f(x_1,...,x_{n-1},g(x_1,...,x_n))=h(x_1,...,x_n)$

Лемма о несамодвойственной ф-ии:Если $f\notin S$, то из неё подстановкой вместо переменных ф-ий x и ¬x - можно получить const. Док-во:$f(x_1,...,x_n)\notin S\Rightarrow\exists f(a_1,...,a_n)=f(\neg a_1,...,\neg a_n)$. Сделаем подстановку x_i->x^{ai}: $h(x)=(x_1^{a1},...,x_n^{an})$. Док-ем, что h(x)-const. $x^a=x\sim a=a\sim x=a^x$.

$h(0)=f(0^{a1},...,0^{an})=f(a_1^0,...,a_n^0)=f(\neg a_1,...,\neg a_n)=f(a_1,...,a_n)=f(a_1^1,...,a_n^1)=f(1^{a1},...,1^{an})=h(1)\Rightarrow h(x)$=const

Билет 22.

Опр. Замыканием А называется множество всех функций алгебры логики,которые можно выразить формулами из А (т.е. множество всех суперпозиций функций из А),и обозначается знаком [А]. Множество А называется **замкнутым классом**, если А=[А]. Примеры з. кл.: $[P_2]= P_2$, $A=\{1,x\}:[A]=A$, $A=\{0,\neg x\}:[A]\neq A$

Свойства замыкания: 1)$A\subseteq[A]$, 2)$[[A]]=[A]$, 3)$A\subseteq B\Rightarrow[A]\subseteq[B]$,

Опр. **Ф-ия монотонна**, если при $a \preceq b$, $f(a)\le f(b)$, (где $\preceq$ покоординатный порядок:частичный, не всегда можно сравнить, напр. набор (1,0) и (0,1) не сравним. $(1,0)\succeq(0,0)$)
Док-ем, что этот класс ф-ий замкнут: (проверим только одно св-во:подстановку, а переим. перем и введ. и удал. фикт. перем. очевидно).] $f,g\in M$. $h(x_1,...,x_n)=f(x_1,...,x_{n-1},g(x_1,...,x_n))$. $a=(a_1,...,a_n),b=(b_1,...,b_n)$, $a\preceq b\Rightarrow g(a)\le g(b)$. Итак, $(a_1,...,a_{n-1},g(a_1,...,a_n))\preceq(b_1,...,b_{n-1},g(b_1,...,b_n))\Rightarrow f(a_1,...,a_{n-1},g(a_1,...,a_n))\le f(b_1,...,b_{n-1},g(b_1,...,b_n))$ $\Rightarrow h(a)\le h(b)$
Лемма о немонотонной ф-ии: Если $f\notin M$, то тз неё подстановкой const(1,0) можно получить немонотонную ф-ию одной переменной, т.е. **¬x.** Док-во:$a=(a_1,...,a_{i-1},0,a_{i+1},...,a_n),b=(b_1,...,b_{i-1},1,b_{i+1},...,b_n)$. $f(a)>f(b)$, т.е. $f(a)=1;f(b)=0$; Рассм. ф-ию $h(x)=f(a_1,...,a_{i-1},x_i,a_{i+1},...,a_n)$. $h(0)=f(a_1,...,a_{i-1},0,a_{i+1},...,a_n)=f(a)=1$; $h(1)=f(b_1,...,b_{i-1},1,b_{i+1},...,b_n)=f(b)=0\Rightarrow h(x)=\neg x$

Билет 23.
Опр. Замыканием А называется множество всех функций алгебры логики,которые можно выразить формулами из А (т.е. множество всех суперпозиций функций из А),и обозначается знаком [А]. Множество А называется **замкнутым классом**, если А=[А]. Примеры з. кл.: $[P_2]=P_2$, $A=\{1,x\}:[A]=A$, $A=\{0,\neg x\}:[A]\ne A$
Свойства замыкания: 1)$A\subseteq[A]$, 2)$[[A]]=[A]$, 3)$A\subseteq B\Rightarrow[A]\subseteq[B]$,
Опр. Ф-ия линейная, если её можно представить в виде: $f(x_1,...,x_n)=a_0\oplus a_1x_1\oplus...\oplus a_nx_n$, где $a_0,...,a_n\in E_2$. Пр.: 0; $1,a_0=1$; x_1, $a_0=0,a_1=1$; $\neg x_1=x_1\oplus 1$, $a_0=1,a_1=1$; - лин. ф-ии. Но $x_1x_2\notin L$. Всего $L=2^{n+1}$ ф-ий
Док-ем, что класс лин. ф-ий замкнут(По сути надо док-ть 3 св-ва суперп.:Подстановка, Переим. перем., Введение и удаление фикт. перем. Мы док-ем подст., остальное очевидно): $f,g\in L$;
$f(x_1,...,x_n)=a_0\oplus a_1x_1\oplus...\oplus a_nx_n$, $g(x_1,...,x_n)=b_0\oplus b_1x_1\oplus...\oplus b_nx_n$. $h(x_1,...,x_n)=f(x_1,...,x_{n-1},g(x_1,...,x_n))=a_0\oplus a_1x_1\oplus...\oplus a_{n-1}x_{n-1}\oplus a_n(b_0\oplus b_1x_1\oplus...\oplus b_nx_n)=(a_0\oplus a_nb_0)\oplus(a_1\oplus a_nb_1)x_1\oplus...\oplus(a_{n-1}\oplus a_nb_{n-1})x_{n-1}\oplus a_nb_nx_n=c_0\oplus c_1x_1\oplus...\oplus c_nx_n$
Лемма о нелинейной ф-ии. Если f - нелинейная ф-ия, то & явл. суперпозицией 4 ф-ий $\{\neg f, \neg x,0,1\}$Док-во: Т.к. нелинейная, то значит входит какая-нибудь &, напр.x_1x_2. Тогда
$f(x_1,...,x_n)=x_1x_2P_1(x_3,...,x_n)(\ne 0)\oplus x_1P_2(x_3,...,x_n)(=a_1)\oplus x_2P_3(x_3,...,x_n)(=a_2)\oplus P_4(x_3,...,x_n)(=b)$. Возьмем набор, при котором $P_1(y_3,...,y_n)=1$. $f(x_1,x_2,...,x_n)=x_1x_2\oplus a_1x_1\oplus a_2x_2\oplus b$. Сделаем подстановку $x_1\to x_1\oplus a_2$,а $x_2\to x_2\oplus a_1$(т.е. либо x_1 при $a_2=0$, либо $\neg x_1$, при $a_2=1$). Тогда
$f(x_1\oplus a_2,x_2\oplus a_1,y_3...,y_n)=(x_1\oplus a_2)(x_2\oplus a_1)\oplus a_1(x_1\oplus a_2)\oplus a_2(x_2\oplus a_1)\oplus b=x_1x_2\oplus a_1a_2\oplus b=x_1x_2\oplus c\Rightarrow x_1x_2= f(x_1\oplus a_2,x_2\oplus a_1,y_3...,y_n)\oplus c$

Билет 24.
Теорема Поста о полноте(н. и д. усл-ие полноты).Мн-во ф-ий является полным, т.и т.т., когда оно не содержится не в каких из этих классов(T_0,T_1,M,S,L). Док-во:Необх.: Допустим, что это не так, и $X\subseteq M$, $[X]\subseteq[M]=M\ne P_2$(т.к. суперпоз. монот-ых ф-ий, есть ф-ия монотонная, а кол-во таких ф-ий меньше, чем P_2). Получили противоречие. Дост:$X\not\subset T_0,T_1,S,M,L$.] $f_1\notin T_0$, $f_2\notin T_1$, $f_3\notin S$, $f_4\notin M$, $f_5\notin L$. $\{f_1,f_2,f_3,f_4,f_5\}\subseteq X$. Возможны 2 случая:1)$f_1(1,...,1)=1$. Т.к.$f_1(0,...,0)=1$(т.к.$f_1\notin T_0$), то $f_1(x,...,x)=1$ - получили 1. $f_2\notin T_1\Rightarrow f_2(1,...,1)=0$, $f_2(f_1(x,...,x),...,f_1(x,...,x))=0$ - получили 0. Дальше пользуясь $\{f_4,0,1\}\to\neg x$(Л. о не М.). Пользуясь $\{f_5,0,1,\neg x\}\to$&(Л. о не Л.). Т.о. получили $\{\&,\neg\}\subseteq[X]\Rightarrow X$ - полное. 2) $f_1(1,...,1)=0$, но $f_1(0,...,0)=1$(т.к.$f_1\notin T_0$) $\Rightarrow f_1(x,...,x)=\neg x$. Дальше пользуясь $\{f_3,\neg x\}$(Л. о не S) получим const=c. Дальше найдем другую const, пользуясь $f_1(c,..,c)=\neg c$ Пользуясь $\{f_5,0,1,\neg x\}\to$&(Л. о не Л.).

Билет 25.
Опр. **Замыканием А** называется множество всех функций алгебры логики,которые можно выразить формулами из А (т.е. множество всех суперпозиций функций из А),и обозначается знаком [А]. Множество А называется **замкнутым классом**, если А=[А]. Примеры з. кл.: $[P_2]=P_2$, $A=\{1,x\}:[A]=A$, $A=\{0,\neg x\}:[A]\ne A$
Свойства замыкания: 1)$A\subseteq[A]$, 2)$[[A]]=[A]$, 3)$A\subseteq B\Rightarrow[A]\subseteq[B]$,
Опр. Система функций алгебры логики А называется **полной**, если $[A]=P_2$. $A=\{x_1x_2,x_1\oplus x_2,0,1\}$
Опр. Мн-во ф-ий называется **предполным** классом, если оно не полное, но при добавлении ф-ии(не принадл. данному мн-ву) становится полным.
Теорема. T_0,T_1,S,M,L - единственные предполные классы. Док-во:1) Нужно убедиться, что ни один из 5 классов, при добавлении ф-ии, не является подмн-ом другого. $S`=S\cup\{f\},f\notin S$. Допустим, что S` не полный, тогда по т.Поста $S`\subseteq M$(надо проверить на все классы) $\Rightarrow S\subseteq M$, $\neg x\in S,\neg x\notin M\Rightarrow S\not\subset M$. Наше предполож. неверно$\Rightarrow$S` - полное. (!)Предположим, что X - предполный класс$\ne T_0,T_1,...$ .X не явл. полным$\Rightarrow$ по т.Поста (к примеру) $X\subseteq T_1$. Поскольку (по усл.) $X\ne T_0,...$, то $\exists f\in T_1-X(f\in T_1,f\notin X)$. Тогда добавим f в X: $X`=X\cup\{f\}\subseteq T_1$ - не полный класс. Итак, X не полный класс, и при добавлении ф-ии $f\notin X$, мы получили не полный класс, след-но(по опр. предп. кл.)X не предполный.

Опр. Базис - минимальное по включению мн-во ф-ий полной системы, которое само явл. полной. Пр. $\{\&,v,\neg\}$ - полны, не базис. $\{\&,\neg\}$ -полна, базис.

Сл-ие из т.Поста. Всякий базис состоит не более чем из 4-х ф-ий. Док-во:] $f_1\notin T_0$, $f_2\notin T_1$, $f_3\notin S$, $f_4\notin M$, $f_5\notin L$. $\{f_1,f_2,f_3,f_4,f_5\}\subseteq X$. $f_1\notin T_0\Rightarrow f_1(0,..,0)=1$ a)$f_1(1,...,1)=0\Rightarrow f_1\notin M$ $\{f_1,f_2,f_3,f_5\}$ - полное. б)$f_1(1,...,1)=1\Rightarrow f_1\notin S$ (т.к. $f_1(0,...,0)=f_1(1,...,1)$) тогда $\{f_1,f_2,f_4,f_5\}$ - полное

Билет 26.

СФЭ(схема из функц. элементов) - ациклический граф, в котором вершины делятся на 3 категории: 1)*входные*($deg^+(x)=0$)(из неё только выходят) 2)*функциональные*($f(x_1,...,x_k)$, $deg^+(x)=k$) 3)*выходные* $deg^+(a)=1$, $deg^-(a)=0$. Основные элементы - *конъюнктор*(2 вх. 1 вых.), *дизъюнктор*(2 вх. 1 вых.), *инвертор*(1 вх. 1 вых.).

Сложность - число элементов в схеме(чем больше, тем сложнее).

Простейшие методы синтеза.

1)$f(x_1,...,x_n)$ $\neq$const. $f(x_1,...,x_n)=V_{f(a1,...,an)=1}x_1^{a1}...x_n^{an}=K_1v...vK_s$. Строим 3 схемы:а)$x_i^{ai}$, б)$K_i$ в)f . Получаем сложность схемы $L_1(n)$. Оценим её по макс.: $\neg$:n; &:(n-1)S; v:S-1; $S\le 2^n-1$(max кол-во &). Получается: n+(n-1)S+S-1=n(s+1)-1. $L_1(n)<n*2^n$

2)Либо СДНФ, либо СКНФ.] S_1 - число 1, S_0 - число 0. Соотв.: $n(S_1+1)-1$, $n(S_0+1)-1$. min $(S_0,S_1)\le 2^{n-1}$. $L_2(n)<n(2^{n-1}+1)$

3)Теорема о разложении $f(x_1,...,x_n)$ по m переменным. 1)m=1. $f(x_1,...,x_n)=x_nf(x_1,...,x_{n-1},1)V\neg x_nf(x_1,...,x_{n-1},0)$. $f_1(x_1,...,x_{n-1})=f(x_1,...,x_{n-1},1)$, $f_0(x_1,...,x_{n-1})=f(x_1,...,x_{n-1},0)$. Тогда, $f=x_nf_1v\neg x_nf_0$. Строим схему.($x_1,...,x_{n-1}$ пускаем 2 прямоуг. S_1 и S_0 и получаем соотв. f_1 и f_0. x_n пускаем в 2-х напр.: 1.в конънктор, куда идет и f_1, и 2. в инвентор, после которого в конънктор куда идет и f_2. И от 2-х конъюнкт. в дизъюнктор и получаем f). Итак, оценим $L_3(n)$: $L_3(1)=2$, $L_3(n)\le 2L_3(n-1)+4$, $L_3(n-1)\le 2L_3(n-2)+4$, $L_3(n)\le 2^2L_3(n-2)+2*4+4$, $L_3(n-2)\le 2L_3(n-3)+4$, $L_3(n)\le 2^3L_3(n-3)+2^2*4+2*4*4\le....\le 2^kL_3(n-k)+4(2^k-1)$. n-k=1,k=n-1. $L_3(n)\le 2^n+4(2^{n-1}-1)=3*2^n-4\approx 2^n/n$

Сложение нат. чисел.:Вводим w_i={1,если есть перенос из i в i+1; 0, нет}(остаток). $z_i=x_i\oplus y_i\oplus w_{i-1}$; $w_i=x_iy_i\oplus x_iw_{i-1}\oplus y_iw_{i-1}=x_iy_i\oplus(x_i\oplus y_i)w_{i-1}$

Билет 27.

Опр. Литера - это либо x, либо $\neg$x. **Минимальная ДНФ** - ДНФ, в которой наим. число литер. **Импликант** ф-ии f - называется эл-ая конъюнкция K, т.ч. а)$K=1\Rightarrow f=1$ или б)$K\rightarrow f=1$ или в)Kvf=f

Лемма1. Пусть $f=K_1v...vK_s$ - ДНФ. Тогда K_i - импликант f. Док-во: $fvK_i=K_1v...vK_iv...vK_svK_i=K_1v...vK_s=f$(т.к. в ДНФ в одинаковых эл. диз. одна убираются)$\Rightarrow K_i$ - импликант.

Опр. Простой импликант - при вычеркивание из него любой литеры, он перестает быть импликантом.

Лемма2. Мин. ДНФ состоит только из простых импликантов. Док-во: $f=K_1v...vK_s$ - мин. ДНФ.] K_1 - не простой импликант. Покажем, что она не минимальна. $K_1=x^aK_1`$, $K_1`$ - импликант(т.к. K_1 - не простой). $fvK_1`=x^aK_1`vK_2v...vK_svK_1`=K_1`vK_2v...vK_s$(по зак. поглащения) - ДНФ, причем меньше чем была, значит f не минем.

Лемма3.$K_1v...vK_s$- все простые импликанты f, то $f=K_1v...vK_s$ - тождество. Док-во:] $f=K_1v...vK_p$ - min ДНФ, p=s. Если p<s, то будем добавлять до P_s, т.е. $f=fvK_{p+1}$(по опр.импликанта), ...$f=fvK_s$

Опр.Сокращенная ДНФ - дизъюнкция всех простых импл-ов данной ф-ии. ДНФ приведенная - если к ней неприменим закон поглащения.

Теорема:] дана КНФ $f=D_1...D_s$. после раскрытия скобок и приведения(исп. закона поглащения) получается приведенная ДНФ. Док-ем, что это сокращенная ДНФ.] $K=x_{i1}^{a1}x_{i2}^{a2}...x_{ip}^{ap}$ - (простой) импликант. Док-ем, что в D_i входит в качестве слагаемых один из $x_{i1}^{a1},....,x_{ip}^{ap}$(причем в той же степени). Доп-им, что в D_i не входит ни один элемент из K. Тогда возбмем такой набор $x_{i1}=a_1$, $x_{i2}=a_2,...,x_{ip}=a_p\Rightarrow K=1$, и $x_{j1}=\neg b_1,...,x_{jq}=\neg b_q\Rightarrow D_i=0$. Пременные не вошедшие ни в какую из этих групп, могут принимать любые значения. Итак, $D_i=0\Rightarrow f=0$, но $K=1\Rightarrow f=1$. След-но противоречие.

Билет 28.

$A=\{a_1,...,a_n\}$ - алфавит. $a=a_{i1}...a_{is}$ - слово. A* - мн-во всех слов из A. λ - пустое слово. |a| - длина слова a, кол-во букв. $|\lambda|=0$; A^n - мн-во всех слов A длины n. $A^0=\{\lambda\}$, $A^1=A$, $A^*=\cup_{n=0}^{\infty}A^n$.

] $A=\{a_1,...,a_k\}$, $B=\{b_1,...,b_q\}$. Схема кодирования: $a_1\rightarrow u_1$; $a_2\rightarrow u_2,...,a_k\rightarrow u_k$(если $\forall u_i=b_j$ то **кодирование алфавитное**). $U=\{u_1,...,u_k\}$ - код. Тем лучше кодирование, чем меньше |f(a)|/|a| - **коэффициент сжатия.** Доп-им, в слове a: a_1- n_1 раз,....,a_k - n_k раз. $|a|=n_1+...+n_k=n$. $|f(a)|=n_1|u_1|+n_2|u_2|+...+n_k|u_k|$. $|f(a)|/|a=(n_1/n)*|u_1|+...+(n_k/n)*|u_k|=\Sigma_{i=1}^k(n_i/n)|u_i|$. $((n_i/n)$ - доля (частота) a_i в a). $P_1=(n_1/n),...,P_k=(n_k/n)$. $P=(P_1,...,P_k)$. $C(P,U)=\Sigma_{i=1}^kP_i|u_i|$ - коэф-т сжатия.

Опр. Код свободный, если ($U=\{u_1,...,u_n\}$) $u_{i1}...u_{in}=u_{j1},...,u_{jm}$ только тогда, когда n=m и $i_1=j_1,...,i_n=j_n$

Нер-во Мак Миллане: Если U - свободный код, |A|=k, |B|=q, то $\Sigma^k_{i=1}q^{-|ui|}\le 1$.

Задача1. A,B; |A|=k. $P=(P_1,...,P_k)$, $0\le P_i\le 1$. Найти свободный код $U=\{u_1,...,u_k\}$, $u_i\in B^*$, i=1,...,k, такой, на котором minC(P,U)

Префиксный код - такой код, в котором ни одно слово кода, не явл. префиксом другого.

Лемма. Любой префиксный код - свободный. Док-во:] $U=\{u_1,...,u_k\}$. Доп-им он не свободный, т.е. $u_{i1}...u_{in}=u_{j1},...,u_{jm}$, $i_1,...,i_n \neq j_1,...,j_m$. Выберем |a| - min. Доп-им, $i_1 \neq j_1$. Тогда, одно из u_{i1} или u_{j1} явл. префиксом другого, но это протеворечие, что код преф. Зн. наше предпол. не верно. Продолжим дальше, доп-им $i_2 \neq j_2$ .... В итоге все равны⇒свободный.

Билет 29.

Опр. Код свободный, если ($U=\{u_1,...,u_n\}$) $u_{i1}...u_{in}=u_{j1},...,u_{jm}$ только тогда, когда n=m и $i_1=j_1,...,i_n=j_n$

Нер-во Мак Миллане: Если U - свободный код, |A|=k, |B|=q, то $\Sigma^k_{i=1}q^{-|ui|}\leq 1$. Док-во: $S_1=\Sigma_{i=1}{}^k q^{-|ui|}$, $S_n=\Sigma_{a\in A^\wedge n}q^{-|f(a)|}$. Если n=1 S≤1. $a=a_{i1}a_{i2}...a_{in}$. $S_n=\Sigma^k_{i1=1}\Sigma^k_{i2=1}...\Sigma^k_{in=1}q^{-|ui1...uin|}=\Sigma^k_{i1=1}q^{-|ui1|}\Sigma^k_{i2=1}...\ \Sigma^k_{in=1}q^{-|uin|}=(\Sigma^k_{i1=1}q^{-|ui1|})(\Sigma^k_{i2=1})...(\Sigma^k_{in=1})=S^n_1$. $f(a)=u_{i1},u_{i2},...,u_{in}$. $|u_{i1}...u_{in}|=|u_{i1}|+...+|u_{in}|$. Итак: $S_n=S_1{}^n$

Билет 30.

Префиксный код - такой код, в котором ни одно слово кода, не явл. префиксом другого.

Лемма. Любой префиксный код - свободный

Теорема. Пусть набор нат. чисел $l_1,...,l_k$ - удовл-ет нер-ву М, т.е. $\Sigma^k_{i=1}q^{-li}\leq 1$. Тогда ∃ преф-ый код $U=\{u_1,...,u_k\}$, $|u_1|=l_1,...,|u_k|=l_k$. Док-во: Пусть $l_1\leq l_2\leq ...\leq l_k$. 1)Строем $U_1=\{u_1\}$,$|u_1|=l_1$, и так далее до $U_{i-1}=\{u_1,...,u_{i-1}\}$,$|u_1|=l_1$,...,$|u_{i-1}|=l_{i-1}$ - так, чтобы они был префиксными. Док-ем, что добавив u_i слово длины l_i код останется префиксным. Возьмем мн-во всех слов алфавита B длины l_i: $|B^{li}|=q^{li}$. Посчитаем сколько будет запрещенных слов, т.е. слов, у которых префикс один из $u_1...u_{i-1}$. Всего запрещенно $q^{li-l1}+q^{li-l2}+...+q^{li-l(i-1)}<q^{li}$. Док-ем, что: $q^{-l1}+q^{-l2}+...+q^{-l(i-1)}<1$. У нас выполняется нер-во М.М.: $q^{-l1}+...+q^{-l(i-1)}+\underline{q^{-li}+...+q^{-lk}}\leq 1$(то что подч. >0) ⇒ $q^{-l1}+...+q^{-l(i-1)}<1$. Зн. $U_i=\{u_1,...,u_{i-1},u_i\}$ - пр-ый.

Билет 31.

Лемма. ∃ оптимальный преф-ый код $U=\{u_1,...,u_k\}$, в котором длины слов $|u_1|\leq ...\leq |u_k|$ расположенны данным образом. Док-во: Предп.$|u_i|>|u_j|$, где i<j. Тогда $U`=\{u_1,...,u_{i-1},u_j,u_{i+1},...,u_{j-1},u_i,u_{j+1},...,u_k\}$. Тогда C(U,P)-C(U`,P)=$P_i|u_i|+P_j|u_j|-P_i|u_j|-P_j|u_i|=(P_i-P_j)(|u_i|-|u_j|)$>=0. Зн. C(U`,P) ≤C(U,P) при необх. делать далее аналог.

Теорема(редукции). $A=\{a_1,...,a_k\}$. Для исходного алфавита A, построим $V=\{v_1,...,v_{k-2},g_0,g_1\}$ Рассм. $A`=\{a_1,...,a_{k-2},b\}$, $P`=(P_1,...,P_{k-2},P_{k-1}`=P_{k-1}+P_k)$. Пусть $V`=\{v_1,...,v_{k-1},v_{k-2},g\}$ - опт. преф. код для P`(для A`). Если V` - опт. префиксный код для P`, то V - опт. преф. код для P. Док-во: Доп-им V - не явл. оптим. преф. кодом для P. Тогда $U=\{u_1,...,u_{k-2},u_{k-1},u_k\}$ - опт. преф. код для P. Тогда C(U,P)<C(V,P). Ввиду Леммы можно предположить, что ∃ оптимальный преф-ый код $|u_1|\leq ...\leq |u_k|$. u_k=z0; $W=\{u_1,...,u_{k-1},z\}$⇒C(W,P)<C(U,P). Но так не может быть⇒W - не префиксный. Тогда u_i=z1(с помощью этого как-раз нарушилось). $|u_i|=...=|u_{k-1}|=|u_k|$. Пусть i=k-1. (если не так перестав.). Зн. $U=\{u_1,...,u_{k-2},z1,z0\}$. Построим для него $U`=\{u_1,...,u_{k-2},z\}$ - это преф. код для P`. Рассм. C(V,P)-C(V`,P`)=$|g0|*P_{k-1}+|z1|*P_k-|z|(P_{k-1}+P_k)$, |g0|=|g1|=|z|+1. Итак, C(V,P)-C(V`,P`)=$P_{k-1}+P_k$. Аналог. C(U,P)-C(U`,P`)=$P_{k-1}+P_k$⇒C(V`,P`)-C(U`,P`)=C(V,P)-C(U,P)(1). Зн. если (1)>0, то мы приходим к противоречию.

Билет 32.

n-мерный куб - граф, у которого вершина явл. дв-ые наборы дляны n, а вершины(конкр. набор) смежны т. и т.т., когда они различаются в одной позиции(их связывает ребро**).** **Грань** у куба размерности n-k - явл. мн-во вершин, у которых фиксированно значений в k- переменных. **Расстояние Хемминга** d(a,b)-число различий в позициях. **Аксиомы метрики (аксиомы Фреше): 1**)d(x,y)≥0; 2)d(x,y)=0 ⟺ x=y; 3)d(x,y)= d(y,x); 4)d(x,z)≤ d(x,y)+ d(y,z)(нер-во треуг.)

Сфера радиуса k в центре a - $S_k(a)=\{b|d(a,b)=k\}$. **Шар** радиуса k в центре a - $B_k(a)=\{b|d(a,b)\leq k\}$

Граница Хеммига: $B=E^n$. Пусть в коде m слов. Объем каждого шара(каждого слова) радиуса t $\Sigma_{i=0}{}^t({}^n{}_i)$. Всего m-слов⇒Объем всех слов = $m\Sigma_{i=0}{}^t({}^n{}_i)$. Чтобы код исправлял t ошибок из 2 леммы эти шары не должны пересекаться, и меньше объема всех слов: $m\Sigma_{i=0}{}^t({}^n{}_i)\leq 2^n$. ⇒$m\leq 2^n/\Sigma_{i=0}{}^t({}^n{}_i)$. Код называется плотно упакованным, если он лежит на границе Хеммига, т.е. $m=2^n/\Sigma_{i=0}{}^t({}^n{}_i)$

Билет 33.

Кодовое расстояние - min d(x,y): x,y∈V

ψ - декодирующая ф-ия, если $\psi:E^n\rightarrow V\cup\{?\}$. ψ бывает: 1)обнаружив. ошибки $\psi_{обн.}(x)=\{x, x\in V;? x\notin V \}$. Код обнаруживает t ошибок: ∀x∈V, ∀y∉V d(x,y)≤t $\psi_{обн.}(x)$=? 2)испр. ошибки: $\psi_{испр.}(x)=y_0$, $y_0\in V$ и $d(y_0,x)=d(y,x)$, y∈V. Код исправляет t ошибок, если для x∈V, а x`∉V, и d(x,x`)≤t, то $\psi_{испр.}(x`)=x$

Лемма1:Код V обнаруживает t ошибок, когда кодовое расстояние d(x,y)>=t+1

Лемма2: Код исправляет t ошибок, если кодовое расстояние >=2t+1

Граница Хеммига: $B=E^n$. Пусть в коде m слов. Объем каждого шара(каждого слова) радиуса t $\Sigma_{i=0}{}^t({}^n{}_i)$. Всего m-слов⇒Объем всех слов = $m\Sigma_{i=0}{}^t({}^n{}_i)$. Чтобы код исправлял t ошибок из 2 леммы эти шары не должны пересекаться, и меньше объема всех слов: $m\Sigma_{i=0}{}^t({}^n{}_i)\leq 2^n$. ⇒$m\leq 2^n/\Sigma_{i=0}{}^t({}^n{}_i)$. Код называется плотно упакованным, если он лежит на границе Хеммига, т.е. $m=2^n/\Sigma_{i=0}{}^t({}^n{}_i)$

⊆ ⊂ ⊇ ⊃ ∪ ∩ ¬ ∅ ⊕ ≠ ± ∈ ∉ ∀ ∃ ∍ Σ ∏ ⟺ ⇐ ⇒ ≤¬⊄→

Диктовал:
Билет 33
Коды, обнаруживающие и исправляющие ошибки. Граница Хэмминга
Билет 34
Код Хэмминга, исправление одиночной ошибки