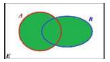
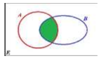
1.операции над множествами. Диаграммы Эйлера-Венна.

Операции на множествами:

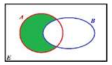
1.Объединение $A \cup B = \{x : x \in A \vee x \in B\}$



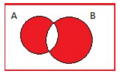
2.Пересечение $A \cap B = \{x : x \in A \wedge x \in B\}$



3.Разность $A - B = \{x : x \in A \wedge x \notin B\}$



4.Геометрическая разность $A \triangle B = \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$



5. Дополнение $\bar{A} = \{x : x \in U \wedge x \notin A\}$

Диаграмма Венна — схематичное изображение всез возможных пересечений нескольких множеств.

2.способы задания множеств. Понятие подмножества.

Чтобы задать множество, нужно указать, какие элементы ему принадлежат. Это можно сделать различными способами.

• **перечислением элементов**: M ={a, b, c, d};

• **указанием характеристического свойства**, которому удовлетворяют элементы данного множества, и только они: M = {x | P(x)} или {x: P(x)} При задании множеств перечислением обозначения элементов обычно заключают в фигурные скобки и разделяют запятыми.

Характеристическое свойство задается с помощью предиката. Предикат P(x) – это логическая функция, принимающая два значения «истина» или «ложь» в зависимости от значения своего аргумента, принадлежащего некоторому множеству

3.Разбиения,покрытия.Булеан,мощность булеана.

Пусть ε={Ei} — некоторое семейство подмножеств множества M, Ei⊂M.
Семейство ε называется **покрытием** множества M, если каждый элемент M принадлежит хотя бы одному из множеств Ei.
Разбиением множества MM называется дизъюнктивное покрытие εε.

Пример

Пусть M={1,2,3}M={1,2,3}, тогда семейство {{1,2},{2,3},{3,1}}{{1,2},{2,3},{3,1}} является покрытием, но не разбиением; {{1},{2},{3}}{{1},{2},{3}} является разбиением (и покрытием)
Множество всех подмножеств множества A называется булеаном множества A и обозначается P(A) или A 2 .
Для конечного множества A мощность его булеана: $|P(A)| = 2^{|A|}$.

4.Понятие прямого произведения множеств, его мощность.

Прямым (декартовым) произведением двух множеств A и B называется множество упорядоченных пар, в котором первый элемент каждой пары принадлежит множеству A, а второй принадлежит множеству B: A× B = {(a,b) | a∈ A ∧ b∈B}.

Если мощность множества A равна n, а мощность множества B равна m, то мощность прямого произведения: | A× B |= n ·m. Соответственно, | A^n |=$|A|^n$.

5.Свойства операций над множествами.

1. Коммутативность. x ∧ y = y ∧ x .

x ⊕ y = y ⊕ x

2. Ассоциативность. (x ∨ y)∨ z = x ∨ (y ∨ z).

(x ~ y) ~ z = y ~ (x ~ z)

3. Дистрибутивность. (x ∨ y) ∧ z = (x ∧ z) ∨ (y ∧ z) .

(x ∧ y) ∨ z = (x ∨ z) ∧ (y ∨ z) .

4. Закон двойного отрицания $x = \bar{\bar{x}}$.

5. Законы де Моргана. x ∨ y = x ∧ y

6. Законы идемпотентности. x∨ x = x, x ∧ x = x

7. Законы поглощения. (x ∨ y) ∧ x = x (x ∧ y) ∨ x = x

6.понятие отношения. Способы задания отношений

Отношение — установление связи между понятиями или объектами. (множество упорядоченных пар, связанных отношением R на множестве AxB.

Способы:

1.Предикатом
2.Матрицей или таблицей
3.Ориентированный граф
4.перечислением

7.область определения, область значений отношений; обратное отношение

Введем несколько понятий, связанных с отношениями.

Пусть R есть отношение на A× B : R ⊆ A× B , (a,b) ∈ R и a∈ A, b∈B.

Область определения отношения: D(R) = {a | (a,b) ∈ R– множество всех первых элементов a упорядоченных пар из R. Для нашего отношения R1 ⊆ A× A, A = {2,3,4,5,6}:

D(R1) ={3,4,5,6}

Множество значений отношения: E(R) = {b | (a,b) ∈ R}– множество всех вторых элементов b упорядоченных пар из R.

E(R1) ={2,3,4,5}.

Обратное отношение: Обратное отношение −1 R на множестве B × A определяется следующим образом:

R^{-1}= {(b, a) |(a, b) ∈R}

Таким образом, (b, a) ∈ R^{-1} тогда и только тогда, когда (a,b) ∈ R , другими словами R^{-1} связывает те же элементы, но в обратном порядке.

8.операции над отношениями. Операции композиции отношений

Поскольку R – это множество упорядоченных пар, то над отношениями можно выполнять операции объединения, пересечения, разности, дополнения.

Для бинарных отношений определена специальная операция, называемая композицией.

Пусть R – отношение между множествами A и B, R ⊆ A× B и S – отношение между множествами B и C, S ⊆ B×C . Композицией отношений S и R называется бинарное отношение между A и C, которое обозначается S o R и определяется следующим образом: S o R ={(a,c)| a∈ A,c∈C ∧ ∃ b∈ B (a,b)∈ R ∧ (b,c)∈S}

Для двух бинарных отношений R и S, заданных на множестве A, их композиция является бинарным отношением на том же множестве.

из записи следует, что отношения применяются справа налево: вначале применяется R, затем S, т.е. справедливо соотношение: (S o R)(a) = S(R(a)).

9.свойства отношений.

Свойства отношений

- **Определение 1**

Пусть $P \subseteq A^2$. Р называют

а) рефлексивным, если $\forall x \in A \quad (x,x) \in P$,

б) антирефлексивным, если $\forall x \in A \quad (x,x) \notin P$,

в) симметричным, если $\forall x, y \in A \quad (x,y) \in P \Rightarrow (y,x) \in P$,

г) антисимметричным, если $\forall x, y \in A \quad \big((x,y) \in P \wedge (y,x) \in P\big) \Rightarrow (x=y)$

д) транзитивным, если $\forall x, y, z \in A \quad \big((x,y) \in P \wedge (y,z) \in P\big) \Rightarrow (x,z) \in P$

е) линейным, если $\forall x, y \in A \quad x \neq y \Rightarrow (x,y) \in P \vee (y,x) \in P$

10.замыкание отношений относительно свойств.

Если отношение R на множестве A не обладает тем или иным свойством P, то его можно попытаться продолжить до отношения R * , которое будет иметь нужное свойство. Под «продолжением» мы понимаем присоединение некоторых упорядоченных пар к подмножеству R ⊂ A× A так, что новое полученное множество уже будет обладать требуемым свойством. Ясно, что исходное множество R будет подмножеством R * . В том случае, если вновь построенное множество R * будет минимальным среди всех расширений R с выделенным свойством, то говорят, что R * является замыканием относительно данного свойства P.

Дано множество A = {a,b,d,l} на котором задано отношение R = {(a,b),(b,d),(d,l)}. Отношение не рефлексивно, не симметрично и не транзитивно. Рефлексивным замыканием будет отношение: R′ = {(a,b),(b,d),(d,l),(a,a),(b,b),(d,d),(l,l)}. Симметричным замыканием будет отношение: R′′ = {(a,b),(b,d),(d,l),(b,a),(d,b),(l,d)}.

Транзитивным замыканием будет отношение: R = {(a,b),(b,d), (d,l),(a,d),(b,l), (a, l)}

11.отношение эквивалентности. классы эквивалентности. Фактор множество.

Рефлексивное, симметричное и транзитивное отношение на множестве A называется отношением эквивалентности. Отношениями эквивалентности, определенными на соответствующих множествах, являются: отношения равенства чисел и множеств, отношение равномощности множеств, отношение подобия треугольников, || прямых на множестве прямых плоскости и т.д.

Пусть R – эквивалентность на множестве A и a ∈ A. Множество всех элементов множества A эквивалентных a, называется классом эквивалентности для a по отношению R и обозначается: [a] = {b∈A | bRa} или [a] ={b∈A|(b,a)∈ R}

Множество всех классов эквивалентности называется фактор множеством множества A по эквивалентности R и обозначается $[A]_R$.

Построим фактор множество для нашего отношения эквивалентности. $[A]_R$={{2,4.6},(3,5}}. Фактор множество, является разбиением множества A и является также подмножеством булеана: $[A]_R \subset 2^A$

12.отношение порядка . отношение частичного порядка. Понятие ЧУ-множества.

Рефлексивное, антисимметричное, транзитивное отношение называется отношением частичного (нестрогого) порядка. Отношение частичного порядка принято обозначать знаком ≤ , это обозначение является условным. Если отношение R на множестве A является отношением частичного порядка, то (A, ≤) называют частично-упорядоченным множеством или ЧУмножеством.

Рассматриваемое нами отношение S ={(a,b)| a,b∈ N ∧ a − делитель b}, определенное на множестве натуральных чисел N, является отношением частичного порядка, а (N, ≤) – ЧУ-множеством.

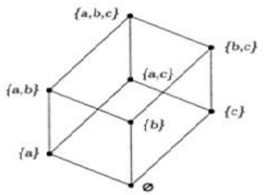
Множество A , на котором задано отношение частичного порядка, называется полностью упорядоченным (линейно упорядоченным, цепью), если каждые два элемента ЧУ-множества (A, ≤) сравнимы.

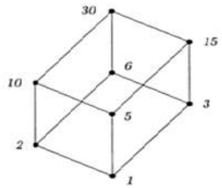
13.сравнимые и несравнимые элементы. Диаграмма Хассе. Наибольший/наименьший и максимальный/минимальный элемент ЧУ-множества.

Два элемента a и b ЧУ-множества (A, ≤) называются сравнимыми по отношению порядка R, если выполняется a ≤ b или b ≤ a.

Несравнимые элементы - Такие **элементы** в частично упорядоченном **множестве**, которые не состоят в отношении частичной упорядоченности

Отношения частичного порядка на множестве удобно задавать диаграммами Хассе. Диаграмма Хассе представляет собой граф (иногда орграф), в котором петли не указываются. Вершины графа изображают элементы частично упорядоченного множества A, и если a ≤ c , для элементов a и c множества A, то вершина a помещается ниже вершины c и соединяется с ней ребром, если не существует такое b ≠ a, с что a ≤ b ≤ c . Если же такое b существует и a ≤ b ≤ c , то линия от a к c не указывается.





1)элемент a∈A называется наибольшим если для всех элементов b ∈A выполняется b ≤ a. Для любых b ∈A

2)элемент a∈A называется наименьшим если для любых b ∈A : a ≤ b

3) элемент a∈A называется максимальным если не существует b ∈A: b больше a, то есть выполняется 3 условия b меньше a, b=a,a и b –несравнимые

4) элемент a∈A называется минимальным если не существует b ∈A: b меньше a

14.Понятие функции. Области определения и значений функции, множество значений функции

Определим функцию как специальное отношение на множестве A× B , на которое наложено дополнительное ограничение. Отношение f на множестве A× B называется функцией из A в B и обозначается f : A → B , если для каждого a∈ A существует единственный элемент b∈B такой, что (a,b) ∈ f .

Множество A называется областью определения функции и обозначается D f . Множество E {b B | a A_ b f (a)} f = ∈ ∃ ∈ = называется множеством значений функции f. Множество B называется областью значений функции

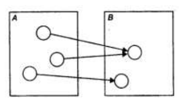
Множество значений функции — множество всех значений, которые функция принимает на области определения

Область значений функции — это множество значений, которые принимает переменная.

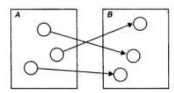
15.Свойства функции: инъекция, сюръекция, биекция.

Функция называется инъективной (инъекцией), если из $f(a_1) = f(a_2)$ следует a1 = a2 . Функция f называется отображением «на» или сюръективной функцией (сюръекцией), если для каждого b∈B существует некоторое a∈ A , такое что f (a) = b .

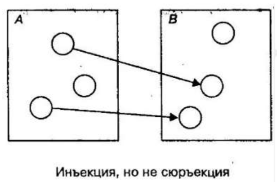
Функция, которая является одновременно и инъективной и сюръективной называется биективной (биекцией). Если f : A → B биективная функция, то говорят, что f осуществляет взаимно однозначное соответствие между множествами A и B.



Сюръекция, не инъекция.



Биекция.



Инъекция, но не сюрьекция

16. Обратная функция, тождественная функция. Сужение функции на множество.

Пусть задана функция f : A → B и f^{-1}– отношение, обратное f . Если отношение f^{-1}является функцией, то ее называют обратной функцией к f и она отображает множество B во множество A f^{-1} :B → A . Функция f имеет обратную тогда и только тогда, когда f – биекция, причем f^{-1}также является биекцией

Тождественной функцией (отображением) множества A на себя называется функция e_A : A→ A , такая что ∀a∈ A_ e_A (a) = a.

17. композиция функций. Свойства операции композиции.

определим для функции операцию композиции. Пусть f : A → B и g : B → C . Тогда композиция двух функций g и f есть функция и она отображает множество A во множество C: g o f : A → C . Если a∈ A , то (g o f)(a) = g(f (a)). Композиция функций как и композиция отношений выполняется справа налево.

Композиция функций ассоциативна. И в общем случае не коммутативна : 1. h o (g o f) = (h o g) o f ;

2. g o f ≠ f o g

композиция биективных функций есть также биективная функция

18. Рекурсивный способ задания функции. Примеры.

Рекурсивная процедура задает функцию, определенную на множестве $Z_{\geq 0}$ (или _N) следующим образом:

1. задается значение f(1) или f(0);

2. значение f(n+1) определяется через суперпозицию f(n) и других, считающихся известными, функций; Зададим, например, функцию f(n) = a^n , определенную на множестве $Z_{\geq 0}$, рекурсивно:

f(0)=1;

f(n+1)=a умножить f(n);

Как видим, указанная функция может быть задана как аналитически (с помощью формулы), так и рекурсивно. Функция факториал f (n) = n!, определенная рекурсивно, имеет вид:

f(0)=1;

f(n+1) =(n+1) умножить f(n);

Последовательности чисел Фибоначчи и Каталана также могут быть заданы рекурсивно.

19.Счётно бесконечные множества. Несчетные бесконечные множества.

За основу для сопоставления бесконечных множеств берется множество натуральных чисел N. Множество A называется счетно бесконечным, если существует взаимно однозначное соответствие между множеством A и множеством натуральных чисел N.

Множество называется счетным, если оно конечно или счетно бесконечно.

Если бесконечное множество A нельзя поставить во взаимно однозначное соответствие с множеством натуральных чисел N, то множество A называется несчетным.

20.Взаимно однозначное соответствие. Мощность множеств.

Взаимно однозначным соответствием между двумя непустыми множествами A и B называется такое правило (или закон) f, по которому каждому элементу a∈ A ставится в соответствие единственный элемент f (a) ∈ B и для любого элемента b∈B существует единственный элемент a∈ A, такой что f (a) = b , другими словами, f задает биекцию между A и B.

Между непустыми конечными множествами A и B существует взаимно однозначное соответствие тогда и только тогда, когда | A |=| B |.

Мощность множества — количество элементов конечного множества.

Мощность множества M={a,b,c} |M|=3

21.Принцип Дирихле. Примеры использования.

Пусть f : A → B – функция, причем A и B – конечные множества. Предположим, что A состоит из n элементов: $a_1, a_2, \ldots a_n$. Принцип Дирихле гласит, что если |A| > |B|, то, по крайней мере, одно значение f встретится более одного раза. Иначе, найдется пара элементов ai ≠ a j , для которых f(a_i) = f(a_j) . Принцип Дирихле иногда называют принципом клеток и формулируют в легко запоминающей форме: Невозможно рассадить 10 кроликов в 9 клетках так, чтобы в каждой клетке сидел один кролик

Пример

В коробке лежат 2 пары одинаковых ботинок. Какое наименьшее число ботинок нужно вынуть не глядя, чтобы среди них обязательно оказалась одна пара? Решение.

В таких задачах мы рассматриваем худший случай: за первые два раза мы вытащили 2 левых или 2 правых ботинка (левый и правый – это лучший случай). Тогда, какой ботинок мы бы не вытащили в третий раз, мы обязательно получим пару одинаковых ботинок. Итак, ответ 3.

22.понятие операции . таблица Кэли для задания операции. свойства операций

Операцией над множеством A называется функция f $f : A^n \to A$. Поскольку мы определили операцию как функцию, то результат операции однозначно определен и т. к. $E_f \subseteq A$ операция замкнута на A. Определенная таким образом операция имеет арность (порядок) n. При n = 1 операция называется унарной, например, операция отрицания. При n = 2 операция называется бинарной. Бинарной операцией на множестве A называется функция f : A× A → A .

Одним из способов задания бинарных операций является таблица Кэли

∧	0	1
0	0	0
1	0	1

свойства бинарных операций. • Бинарная операция называется коммутативной, если справедливо равенство: a*b = b*a, ∀a,b ∈ A . Коммутативными являются операции сложения и умножения на числовых множествах, операции сложения матриц одного порядка. Некоммутативны операции: вычитания на Z, деления на R, разности множеств, векторное произведения векторов• Бинарная операция называется ассоциативной, если справедливо равенство: (a ∗b) ∗c = a ∗ (b ∗ c) , ∀a,b,c ∈ A. Ассоциативными являются операции: сложение и умножение на Z, умножение матриц, объединение и пересечение множеств .Не ассоциативными являются операции разности множеств, векторное умножение векторов пространства.

• Пусть дано множество *A*, на котором определенны две бинарные операции: ∗, •.

Тогда, если для всех $a,b,c \in A$ выполняется:

$a * (b \bullet c) = (a * b) \bullet (a * c)$ *(дистрибутивность слева)*

$(b \bullet c) * a = (b * a) \bullet (c * a)$ (дистрибутивность справа)

23.Принцип математической индукции.

Инструментом для доказательства истинности утверждений относительно всех натуральных чисел является принцип математической индукции. Сформулируем его. Пусть P(n) есть такое утверждение, что: a) P(1) истинно, и b) для каждого k, если P(k) истинно, то P(k+1) истинно. Тогда P(n) истинно для любого натурального числа n. В символической записи принцип математической индукции имеет вид: $(P(1) \wedge ((\forall k)P(k) \to P(k+1)) \to (\forall n)P(n)$. Рассмотрим примеры.

Пример 1. Докажем методом математической индукции, что $7^n - 1$ делится на 6 при любом натуральном показателе n, т. е. имеет место равенство: $7^n - 1 = 6m$, где $m \in N$.

1.При n = 1 имеем: 7^1-1=7-1=6. И, следовательно, P(1) – истинно. **2**.Теперь покажем, что для $\forall k \in N$, если P(k) истинно, то P(k+1) истинно. Предположим, что7^k-1 делится на 6, т. е. 7^k-1 = 6m для некоторого натурального числа m. Запишем утверждение для (k+1) и выполним эквивалентные преобразования. Имеем: 7^{k+1}-1=7(7^k)-1=7($7^k - 1$)+7-1=7($7^k -$ 1)+6=7*6m+6=6(7m+1)=6l , где l = (7m +1) и $l \in N$.

24.понятие булевой функции. основные булевы функции 2-х переменных .

Пусть задано множество B = {0, 1}. Тогда, отображение $f : B^n \to B$ множества B^n на множество B называется булевой функцией n переменных и ее можно записать в виде $f(x_1 \dots x_n)$. Булеву функцию называют также переключательной функцией.

Рассмотрим основные булевы функции.

1) конъюнкция или «логическое и » (логическое умножение). Обозначение: $x \wedge y$, $x \& y$, $x \cdot y$, xy.
2) сложением по модулю два (исключающее или) $x \oplus y$.
3) дизъюнкция или «логическое или» (логическое сложение). Обозначение: $x \vee y$, x + y
4) операцией Пирса или стрелкой Пирса. Обозначение: $x \downarrow y$. Ее можно выразить через операции отрицания и дизъюнкции двух переменных
5) эквивалентность (логическая равнозначность). Обозначение: $x \sim y$.
6) импликация от y к x. Обозначение: $y \to x$

25.Основные эквивалентности для булевых функций.

Коммутативность. $x \vee y = y \vee x$, $x \wedge y = y \wedge x$, $x \oplus y = y \oplus x$, $x \sim y = y \sim x$

2. Ассоциативность. (x ∨ y}∨ z = x ∨ (y ∨ z), $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, $(x \sim y) \sim z = y \sim (x \sim z)$

3. Дистрибутивность. $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$, $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$, $(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z)$.

4. Закон двойного отрицания. x = x .

5. Законы де Моргана. $x \vee y = x \wedge y$. $x \wedge y = x \vee y$

6. Законы идемпотентности. $x \vee x = x$, $x \wedge x = x$

7. Законы поглощения. $(x \vee y) \wedge x = x$, $(x \wedge y) \vee x = x$

8. Другие эквивалентности. $x \vee$ не x =1 ,$x \wedge$ не x = 0 ,$x \vee 1=1$,$x \wedge 0 = 0$,$x \wedge 1= x$,$x \vee 0 = x$

26.Существенные и мнимые переменные. Двойственные функции

Принцип двойственности

- Булева функция f*(x1,x2, ..., xn) называется *двойственной* к функции f(x1,x2, ..., xn), если $f^*(x_1,x_2, \dots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n})}$.

- Например, функция $f^*(x, y) = xy$ является двойственной к функции $f(x, y) = x \vee y$

$$f^*(x, y) = \overline{\overline{\overline{x}} \vee \overline{\overline{y}}} = \overline{\overline{x}} \wedge \overline{\overline{y}} = xy$$

Булева функция $f(x_1, \dots x_{i-1}, x_i, x_{i+1}, \dots, x_n)$ *существенно зависит* от переменной x_i, если существует такой набор значений $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$, что выполняется соотношение:

$$f(a_1, \dots a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots a_{i-1}, 1, a_{i+1}, \dots, a_n)$$

В этом случае x_i называют *существенной* переменной.

В противном случае говорят, что от переменной x_i функция зависит несущественно и x_i является ее *фиктивной* переменной.

27.классы булевых функций. Теорема Поста-Яблонского.

Классы Поста

Классы булевых функций

- **Класс T_0** – класс функций, сохраняющих 0
- **Класс T_1** – класс функций, сохраняющих 1
- **Класс M** – класс монотонных функций
- **Класс S** – класс самодвойственных функций
- **Класс L** – класс линейных функций

Теорема (теорема Поста)

Система булевых функций F является функционально полной тогда и только тогда, когда для любого класса $K \in \{K_0; K_1; S; L; M\}$ найдется функция $f \in F$ такая, что $f \notin K$

Таблица принадлежности булевых функций классам K_0, K_1, S, L, M

Функция	K_0	K_1	S	L	M
$\bar{x}$	–	–	+	+	–
$x_1 \wedge x_2$	+	+	–	–	+
$x_1 \vee x_2$	+	+	–	–	+
$x_1 \to x_2$	–	+	–	–	–
$x_1 \sim x_2$	–	+	–	+	–
$x_1 \oplus x_2$	+	–	–	+	–

Системы булевых функций $\{\bar{x}, x_1 \wedge x_2\}$, $\{\bar{x}, x_1 \vee x_2\}$ являются функционально полными

28.конституэнта единицы. СДНФ булевой функции.

- ***Конституентой единицы*** **называют конъюнкцию, содержащую все переменные или их инверсии, которая обращается в единицу только при одном выборочном наборе переменных.**

Дизъюнкция конституент единицы, равных единице на тех же наборах, что и заданная функция, называется совершенной дизъюнктивной нормальной формой булевой функции, сокращенно СДНФ. Любую булеву функцию $f(x_1 \dots x_n)$, кроме константы 0, можно представить в виде СДНФ и это представление единственно.

Чтобы получить совершенную дизъюнктивную нормальную форму (СДНФ), надо взять все наборы, на которых значение функции равно 1 и записать для каждого из них конъюнкцию переменных и их отрицаний. Если в наборе значение переменной равно 0 – то переменную надо взять с отрицанием, если 1 – без отрицания

29.конституэнта нуля. СКНФ булевой функции.

Конституентой нуля **называют дизъюнкцию, содержащую все переменные или их инверсии, которая обращается в нуль только при одном выборочном наборе переменных.**

Конъюнкция конституент нуля, которые равны нулю на тех же наборах, что и заданная функция, называется совершенной конъюнктивной нормальной формой, сокращенно СКНФ. Любую булеву функцию $f(x_1 \dots x_n)$, кроме константы 1, можно представить в виде СКНФ и это представление единственно.

Чтобы получить совершенную конъюнктивную нормальную форму, надо взять все наборы, на которых значение функции равно 0 и записать для каждого из них дизъюнкцию переменных и их отрицаний. Если в наборе значение переменной равно 0, то переменную надо взять без отрицания, если 1 – с отрицанием.

30.Полином Жегалкина. алгоритм построения.

Справедлива следующая теорема Жегалкина. Любая булева функция может быть представлена в виде полинома, т. е. записана в форме.

$$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{n+1} x_1 x_2 \oplus \dots \oplus a_N x_1 \dots x_n$$

где a_0, a_1, ..., a_N – коэффициенты, равные нулю или единице.

Слагаемое отсутствует, если коэффициент при нем равен нулю. Как мы видим, полином Жегалкина строится с помощью операций: сложение по модулю два, конъюнкции и константы 1. Полином Жегалкина для каждой булевой функции единственен.

Полином Жегалкина можно построить различными способами: используя таблицу истинности (через СДНФ), методом неопределенных коэффициентов, методом треугольника.

31.Понятие элементарной конъюнкции, дизъюнкции. Операции склеивания , неполного склеивания, поглощения.

Элементарной дизъюнкцией называется дизъюнкция переменных или их отрицаний, в которой каждая переменная встречается не более одного раза.

$$x, \quad \bar{x} \vee y, \quad x \vee \bar{y} \vee z.$$

Элементарной конъюнкцией называется конъюнкция переменных или их отрицаний, в которой каждая переменная встречается не более одного раза.

$$x, \quad \bar{x} \cdot y, \quad x \cdot \bar{y} \cdot z.$$

Первая операция, называемая *операцией склеивания*, для элементарных конъюнкций осуществляется по следующему правилу: *дизъюнкцию двух соседних конъюнкций некоторого ранга r можно заменить одной элементарной конъюнкций ранга r-1, являющейся общей частью исходных конъюнкций.*

$xA \vee \bar{x}A = (x \vee \bar{x}) \cdot A = 1 \cdot A = A$,

Вторая из операций называется *операцией поглощения,* и она осуществляется по правилу:

Дизъюнкцию двух элементарных конъюнкций разных рангов, из которых одна является собственной частью другой, можно заменить конъюнкцией, имеющим меньший ранг.

$A \vee A \cdot B = A \cdot 1 \vee A \cdot B = A \cdot (1 \vee B) = A \cdot 1 = A$,

где A и B – некоторые элементарные конъюнкции.

32.Минимизация булевых функций методом Квайна.

Рассмотрим пример.

Найдем *МДНФ* булевой функции, заданной *СДНФ*:

$f_{СДНФ}(x_1, x_2, x_3) = \bar{x}_1\bar{x}_2\bar{x}_3 \vee x_1\bar{x}_2\bar{x}_3 \vee x_1x_2\bar{x}_3 \vee \bar{x}_1x_2x_3 \vee x_1x_2x_3$.

1. Проведем операции *неполного склеивания*, их лучше выполнять последовательно, слева на право.
   1) $\bar{x}_1\bar{x}_2\bar{x}_3 \vee x_1\bar{x}_2\bar{x}_3 = \bar{x}_2\bar{x}_3$.
   2) $x_1\bar{x}_2\bar{x}_3 \vee x_1x_2\bar{x}_3 = x_1\bar{x}_3$.
   3) $x_1x_2\bar{x}_3 \vee x_1x_2x_3 = x_1x_2$.
   4) $\bar{x}_1x_2x_3 \vee x_1x_2x_3 = x_2x_3$.

   У нас *все* конституенты единицы участвовали в склеивании, поэтому операций поглощения нет. Элементарные конъюнкции больше не склеиваются между собой, следовательно, мы получили *простые импликанты.*
2. Из простых импликант строим сокращенную *ДНФ* функции: $f(x_1, x_2, x_3) = \bar{x}_2\bar{x}_3 \vee x_1\bar{x}_3 \vee x_1x_2 \vee x_2x_3$.
3. Строим таблицу покрытия.

Простые импликанты	*Конституенты единицы*				
	$\bar{x}_1\bar{x}_2\bar{x}_3$	$x_1\bar{x}_2\bar{x}$	$x_1x_2\bar{x}_3$	$\bar{x}_1x_2x_3$	x_1x_2x
$\bar{x}_2\bar{x}_3$	*1*	*1*	*0*	*0*	*0*
$x_1\bar{x}_3$	*0*	*1*	*1*	*0*	*0*
x_1x_2	*0*	*0*	*1*	*0*	*1*
x_2x_3	*0*	*0*	*0*	*1*	*1*

Выбираем *существенные* импликанты.

Первая импликанта входит в *МДНФ* обязательно, она единственная, кто покрывает единицу функции на наборе *000* (единственная единица в первой колонке), затем можно выбрать *3-ю* и *4-ю* простые импликанты. Получили *МДНФ*:

$f_{МДНФ_1}(x_1, x_2, x_3) = \bar{x}_2\bar{x}_3 \vee x_1x_2 \vee x_2x_3$.

У нашей функции *две МДНФ*: к первой импликанте можно выбрать *2-ю* и *4-ю*. Получим:

$f_{МДНФ_2}(x_1, x_2, x_3) = x_1\bar{x}_3 \vee \bar{x}_2\bar{x}_3 \vee x_2x_3$.

Как видим, у булевой функции может быть *несколько МДНФ.*

Ранг обеих *МДНФ* $R = 6$

33.Минимизация булевых функций методом Карно-Вейча.

Диаграмма Карно выглядит как прямоугольная таблица с количеством клеток, зависящим от числа переменных булевой функции, для которой она строится. Например: для булевой функции

$f(x_1, x_2, x_3, x_4) =$
$\overline{x_1}\,\overline{x_2}\,\overline{x_3}x_4 \vee x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4} \vee \overline{x_1}\,\overline{x_2}x_3x_4 \vee \overline{x_1}x_2\overline{x_3}x_4 \vee \overline{x_1}x_2x_3x_4 \vee x_1x_2\overline{x_3}x_4 \vee$
$x_1x_2x_3x_4$

Построим диаграмму Карно

x_1x_2 \ x_3x_4	00	01	11	10
00	0	1	1	0
01	0	1	1	0
11	0	1	1	0
10	1	0	0	0

Далее на диаграмме нужно выделить одну или группу (2^n) рядом стоящих единиц, таким образом , чтобы перекрыть одним выделением как можно больше единиц. При этом необходимо учитывать , что верхние и нижние ряды клеток рассматриваются как соседние. Аналогично следует рассматривать соседними левые и правые столбцы клеток. Выделенные группы должны образовывать или одну клетку, или линию, или прямоугольник, или квадрат. И должны быть выделены все единицы на диаграмме.

По выделенным группам составляем конъюнкции (при этом изменяемые переменные в группе в конъюнкции не перечисляются) и дизъюнктивно их объединяем.

Таким образом получаем ДНФ:

$f = \overline{x_1}x_4 \vee x_2x_4 \vee x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4}$.

34.Правило суммы. Правило произведения.

Сформулируем *правило суммы* на языке теории множеств.

Пусть $S_1, S_2, \ldots, S_m$ - *попарно непересекающиеся множества* ($S_i \cap S_j = \varnothing$ для всех $i \neq j$), и пусть для каждого i, множество S_i содержит n_i элементов. Количество вариантов выбора одного элемента из S_1 или S_2 или ... или S_m равно $n_1 + n_2 + \ldots + n_m$.

Запишем приведенное правило в виде формулы:

$|S_1 \cup S_2 \cup \ldots \cup S_m| = |S_1| + |S_2| + \ldots + |S_m|$.

Правило суммы иногда называют правилом *«или»*.

Сформулируем правило суммы для двух объектов ($m = 2$) в иной форме.

Если некоторый объект A можно выбрать m способами, а объект B можно выбрать <u>другими</u> n способами, то выбор либо A, либо B (A или B) можно осуществить m + n способами.

К примеру, если на первой полке стоит *5* книг по физике, а на второй *10* книг по математике, то выбрать книгу из первой *или* второй полки, можно *5 + 10 = 15* способами.

Сформулируем *правило произведения*.

Если объект x_1 может быть выбран n_1 способами, после чего объект x_2 может быть выбран n_2 способами и для любого i, где $2 \le i \le m-1$, после выбора объектов $x_1, \ldots x_i$ объект x_{i+1} может быть выбран n_{i+1} способами, то выбор упорядоченной последовательности $(x_1, x_2, \ldots x_m)$ можно осуществить $n_1 \cdot n_2 \cdot \ldots \cdot n_m$ способами.

Теперь также сформулируем правило произведения для двух объектов.

Если объект A можно выбрать m способами и если после каждого такого выбора объект B можно выбрать n способами, то выбор пары объектов *(A, B)* в указанном порядке можно осуществить $(m \cdot n)$ способами.

Правило произведения иногда называют правилом *«и»*

Вернувшись к нашему примеру с книжными полками, имеем, что выбрать одну книгу с первой полки *и* одну книгу со второй можно $5 \cdot 10 = 50$ способами.

35.Формула включений и исключений в комбинаторике и в теории множеств.

Формула включений и исключений

Другая формулировка

Существует N объектов, каждый из которых обладает или не обладает свойствами $P_1, P_2, \ldots, P_n$

Пусть $N(P_i)$ - количество объектов , обладающих свойством P_i ,

$N(\overline{P_i})$ - количество объектов, не обладающих свойством P_i

Тогда

$$N(\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_n) = N - \sum_{1 \le i \le n} N(P_i) + \sum_{1 \le i_1 < i_2 \le n} N(P_{i_1}, P_{i_2}) + \ldots +$$
$$+ (-1)^k \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} N(P_{i_1}, P_{i_2}, \ldots, P_{i_k}) + \ldots + (-1)^n N(P_1, P_2, \ldots, P_n)$$

36.понятие выборки, примеры различных выборок.

Дадим понятие выборки.

Набор (*комбинация*) из *k*-элементов множества $X = \{x_1, x_2, \ldots, x_n\}$ мощности *n* называется *выборкой объема k из n элементов* или *выборкой из n элементов по k* , или просто *(n,k) выборкой*.

Выборка называется *упорядоченной*, если существенным является не только состав элементов в ней, но и порядок их расположения. Две упорядоченные выборки считаются различными, если они отличаются, либо составом элементов, либо порядком их расположения. Например, упорядоченные выборки *(1,2)* и *(2,1)* считаются различными, хотя и составлены из одних и тех же элементов.

Выборка называется *неупорядоченной*, если порядок следования элементов в ней не существенен. Так, соответственно, *{1,2}* и *{2,1}* считаются одной и той же неупорядоченной выборкой.

Рассмотрим пример, составим всевозможные (3,2)-выборки из элементов множества M = {a,b,c}.

1. (a,a), (a,b), (a,c), (b,b), (b,a), (b,c), (c,c), (c,a), (c,b) – это размещения с повторениями. Их всего 9.

2. (a,b), (b,a), (a,c), (c,a), (b,c), (c,b) – это размещения без повторений. Их, очевидно, всего 6.

3. (a,b), (a,a), (a,c), (b,b), (b,c), (c,c) - сочетания с повторениями. Их всего 6.

4. (a,b), (a,c), (b,c) – сочетания без повторений. Их всего 3.

37.Размещение с повторением и без.

В зависимости от указанных свойств, выборки носят специальные названия.

- *(n,k)-размещением с повторениями* называется упорядоченная *(n,k)* выборка, элементы в которой могут повторяться;
- *(n,k)-размещением без повторений* называется упорядоченная *(n,k)* выборка, элементы которой попарно различны;
- *(n,k)-сочетанием с повторениями* называется неупорядоченная *(n,k)* выборка, элементы которой могут повторяться;
- *(n,k)-сочетанием без повторений* называется неупорядоченная *(n,k)* выборка, элементы которой попарно различны.

Число *(n,k)-размещений с повторениями* обозначается, как $\overline{A_n^k}$ и вычисляется по формуле:

$\overline{A_n^k} = n^k, \forall n, k \in N$.

38.Перестановки.Разупорядочения.

Разупорядочением называется *перестановка n различных упорядоченных символов*, при котором ни один символ не остается на своем месте. Количество разупорядочений на *n* различных упорядоченных символах обозначается D_n.

Например, при $n = 3$, $D_3 = 2$ и разупорядочениями будут перестановки:

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

В общем случае, для $n>1$ количество разупорядочений на *n* символах вычисляется по формуле:

$D_n = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!})$

Размещения без повторений из n элементов по n называются *перестановками* из n элементов без повторений или *перестановками* множества X. Их число обозначается P_n и вычисляется по формуле:

$$P_n = A_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!, \quad 0! = 1.$$

Перестановки удобно представлять матрицами. Например,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

39.Сочетания.

Сочетаниями без повторений из n *элементов по* k называются неупорядоченные k -выборки из n элементов без повторений. Каждое *(n,k)-сочетание без повторений* можно упорядочить $k!$ различными способами и получить $k!$ различных *(n,k)*-размещений без повторений. Таким образом, количество вариантов при сочетании будет меньше количества размещений в $k!$ раз. Их число обозначается C_n^k и вычисляется по формуле:

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}. \quad k \le n$$

Сочетания из n по k без повторений образуют *k-элементарные подмножества* исходного множества мощности n.

В современной терминологии C_n^k обозначается как $\binom{n}{k}$.

Пример:

Сколько трехкнопочных комбинаций существует на кодовом замке (все три кнопки нажимаются одновременно), если на нем всего *10* цифр.

Решение. Так как кнопки нажимаются *одновременно*, то выбор этих трех кнопок – сочетание. Отсюда возможное количество комбинаций:

$$C_{10}^3 = \frac{10!}{(10-3)! \cdot 3!} = \frac{8 \cdot 9 \cdot 10}{6} = 120 \text{ вариантов.}$$

40.Деление с остатком на множестве целых чисел Z. Алгоритмы деления.

Рассмотрим множество Z и рассмотрим на этом множестве *операцию деления с остатком.*

Справедлива следующая *теорема 1*.

Теорема 1.

Для любых целых чисел a и b, $b \neq 0$, существуют *единственные* целые числа q и r, $0 \le r < |b|$, такие, что $a = bq + r$.

При этом $-r$ называют *остатком*, а q − *частным* (*неполным частным* при $r \neq 0$) от деления a на b. Если остаток $r = 0$, то говорят, что b делит a *нацело*, и обозначают $b|a$. Еще раз подчеркнем, что остаток у нас – *целое неотрицательное число*.

Поскольку при изучении сравнений рассматривается деление с остатком целого числа на *целое положительное число* (*натуральное*), перейдем к таким случаям.

Деление *целых положительных чисел* удобно выполнять *столбиком*, этот способ позволяет получить и неполное частное (или просто частное) и остаток.

Чтобы получить неполное частное от деления *целого отрицательного* числа a на *целое положительное* число b нужно взять число, противоположное неполному частному от деления *модулей исходных чисел* и *вычесть из него еди*ницу, после чего остаток r вычислить по формуле $r = a - bq$.

Рассмотрим *примеры*.

Найдем остаток от деления числа *19* на *4*. Имеем: частное, $q = 4$, остаток, $r = 19 - 4 \cdot 4 = 3$.

Теперь найдем остаток от деления *-19* на *4*. Делим модули исходных чисел, получаем *4*, меняем знак и отнимаем единицу, получаем q = -5. Теперь найдем остаток, $r = -19 - 4 \cdot (-5) = 1$.

41.Понятие сравнения. основные свойства сравнений.

Целые числа a и b называются *сравнимыми по модулю* n, если они удовлетворяют одному из условий *теоремы 2*, что обозначается $a \equiv b(\mathrm{mod}\ n)$ или в эквивалентной форме $a - b \equiv 0(\mathrm{mod}\ n)$. Может быть использовано и краткое обозначение: $a \equiv b(n)$.

Данное соотношение между целыми числами называют *сравнением по модулю n.*

Например, $-8 \equiv -3(\mathrm{mod}\ 5) \equiv 7(\mathrm{mod}\ 5) \equiv 12(\mathrm{mod}\ 5) \equiv 2(\mathrm{mod}\ 5)$.

Рассмотрим *основные свойства сравнений.*

1. Пусть $a \equiv b(\mathrm{mod}\ n)$. Тогда $(a \pm c) \equiv (b \pm c)(\mathrm{mod}\ n)$ для любого $c \in Z$. Это соотношение означает, что к обеим частям сравнения можно *добавить*, или *вычесть* из обеих частей, *одно и то же число*. Например: $3 \equiv 11(\mathrm{mod}\ 4)$ отсюда следует, что $6 \equiv 14(\mathrm{mod}\ 4)$ и $1 \equiv 9(\mathrm{mod}\ 4)$.
2. Сравнения можно почленно *складывать* или *вычитать*. Если $a \equiv b(\mathrm{mod}\ n)$ и $c \equiv d(\mathrm{mod}\ n)$, то $(a + c) \equiv (b + d)(\mathrm{mod}\ n)$. Например: $7 \equiv 3(\mathrm{mod}\ 4)$ и $10 \equiv 6(\mathrm{mod}\ 4)$ отсюда следует, что $17 \equiv 9(\mathrm{mod}\ 4) \equiv 1(\mathrm{mod}\ 4)$.
3. Сравнения можно почленно *перемножать*. Если $a \equiv b(\mathrm{mod}\ n)$ и $c \equiv d(\mathrm{mod}\ n)$, то $ac \equiv bd(\mathrm{mod}\ n)$. Перемножим сравнения из предыдущего свойства, имеем $70 \equiv 18(\mathrm{mod}\ 4) \equiv 2(\mathrm{mod}\ 4)$.
4. Сравнения можно почленно возводить в любую *натуральную степень*, m, если $a \equiv b(\mathrm{mod}\ n)$, то $a^m \equiv b^m(\mathrm{mod}\ n)$, $m \in N$. Например, $2 \equiv 7(mod 5)$, отсюда следует что $2^2 \equiv 7^2(mod 5) \equiv 49(mod 5) \equiv 4(mod 5)$.
5. Если в сравнении $a \equiv b(\mathrm{mod}\ n)$ числа a, b и n имеют *общий множитель* d, то на него сравнение можно *сократить*: $a/d \equiv b/d(\mathrm{mod}\ n/d)$. Например, $6 \equiv 10(\mathrm{mod}\ 4)$, отсюда следует, что $3 \equiv 5(\mathrm{mod}\ 2)$.
6. Операция *деления* для сравнений *отсутствует!!!* Если, $a_1 d \equiv b_1 d(\mathrm{mod}\ n)$, то это *не всегда* означает, что $a_1 \equiv b_1(\mathrm{mod}\ n)$. К примеру, $3 \cdot 2 \equiv 5 \cdot 2(\mathrm{mod}\ 4)$, но *3* не сравнимо с *5* по модулю *4* . Однако свойство

42.Отношение сравнимости на множестве целых чисел Z. Классы вычетов.

Свойство сравнимости целых чисел по данному модулю n определяет бинарное отношение $R_{\mathrm{mod}\ n}$ на множестве Z.

Два целых числа находятся в отношении сравнимости $R_{\mathrm{mod}\ n}$, тогда и только тогда, когда они сравнимы друг с другом по модулю n. Отношение сравнимости является *отношением эквивалентности* и для него выполняются свойства:

1. рефлексивно, поскольку $a \equiv a(\mathrm{mod}\ n)$ для каждого $a \in Z$;
2. симметрично, поскольку, если $a \equiv b(\mathrm{mod}_n)$, то $b \equiv a(\mathrm{mod}_n)$ для целых чисел a и b;
3. транзитивно, поскольку, если $a \equiv b(\mathrm{mod}_n)$ и $b \equiv c(\mathrm{mod}_n)$, то $a \equiv c(\mathrm{mod}_n)$.

Классы вычетов с определенными выше операциями сложения и умножения по модулю составного числа n образуют кольцо классов вычетов, если n – простое число, то получаемая алгебраическая система – поле Галуа. Классы вычетов с операцией сложения образуют абелеву группу.