1 IV Dm

RC 17,06,2012

Red FAQ™

Discipline: Discrete Mathematics

Lead: Nasteka Aleksandr

Source: lectures (I.E. Krivtsova)

«FAQ™» Group приветствует всех, и благодарит за использование *этого* пособия для подготовки по выбранной дисциплине. Вы видите лишь четвертое издание, но уже в какой-то мере можно сказать, что это интересный и удобный способ для подготовки к предметам, но, безусловно, не основной и является лишь небольшим подспорьем к основным знаниям.

Данный выпуск не появился бы без помощи наших же студентов, поэтому всем, кто сделал хоть что-нибудь для него, Спасибо за вашу поддержку! Удачной подготовки!

Лидер проекта: Настека Александр

Легенда:

Примеры (Отмечены почти все)	●
Определение в лекции	Определение
Важная информация	Текст или Текст
Номер вопроса по общему списку	Вопрос №

Список вопросов.

1. Понятие множества. Отображения множеств.
2. Конечные и бесконечные множества.
3. Операции над множествами.
4. Прямое произведение множеств. Кортеж.
5. Понятие отношения. Отношения и функции.
6. Свойства отношений.
7. Разбиение множеств.
8. Отношение эквивалентности
9. Отношение порядка, частичного порядка
10. Размещения и перестановки.
11. Сочетания.
12. Разбиения. Полиномиальная формула.
13. Алгебраические операции. Понятие алгебры.
14. Группы.
15. Понятие кольца. Кольцо целых чисел.
16. Кольцо вычетов по модулю n. Малая теорема Ферма.
17. Понятие поля. Конечные поля.
18. Понятие решетки. Примеры решеток.
19. Решетки и алгебры.
20. Понятие нечеткого подмножества. Функции принадлежности.
21. Операции над нечеткими подмножествами.
22. Расстояние Хемминга.
23. Понятие высказывания. Логические операции над высказываниями.
24. Формулы алгебры логики.
25. Функции алгебры логики.
26. Дизъюнктивная нормальная форма
27. Конъюнктивная нормальная форма.
28. Проблема разрешимости.
29. Понятие предиката.
30. Логические операции над предикатами.
31. Кванторные операции над предикатами.
32. Формулы логики предикатов.
33. Понятие алгоритма. Свойства алгоритмов.
34. Вычислимые и рекурсивные функции. Тезис Черча.
35. Машина Тьюринга. Тезис Тьюринга.
36. Нормальные алгоритмы Маркова.
37. Трудоемкость алгоритма. Эффективные алгоритмы.
38. Сложность вычислений. Классы сложности: P, NP и NP-полные задачи.
39. Понятие графа. Виды графов.
40. Способы задания графов
41. Операции над графами.
42. Маршруты на графе: цепи и пути.
43. Достижимость. Связность.
44. Понятие дерева. Остовное дерево.
45. Построение дерева полного перебора.
46. Порядковая функция орграфа. Уровневый граф.

Предмет и задачи дискретной математики.

Классическая математика, в основном, занимается изучением свойств объектов непрерывного характера.

Дискретность понимается как антипод непрерывности.

В качестве синонима понятия дискретная математика иногда употребляют термин конечная математика.

Определение 1

Дискретная математика - область математики, занимающаяся изучением свойств структур конечного характера, которые возникают как в самой математике, так и в области ее приложений.

Дискретная математика представляет собой важное направление в математике, имеющее характерные для него предмет исследования, методы и задачи, специфика которых обусловлена в первую очередь, необходимостью отказа от основополагающих понятий классической математики - предела и непрерывности.

Перечислим разделы дискретной математики: множества, комбинаторика, алгебраические структуры, математическая логика, графы.

Вопрос 1. Понятие множества. Отображения множеств

В современной математике и в различных ее приложениях фундаментальную роль играет понятие ***множества***.

Георг Кантор (1845-1918) - немецкий математик, основатель теории множеств:

"**Под** многообразием или **множеством я понимаю** вообще **все многое**, **которое возможно мыслить как единое**, т. е. такую совокупность определенных элементов, которая посредством одного закона может быть соединена в одно целое."

Например, можно говорить о множестве студентов в группе, о множестве натуральных чисел, букв в алфавите и т.д. При этом о множестве можно вести речь только тогда, когда элементы множества различимы между собой.

В современной математической литературе фигурируют аксиоматические теории множеств, в которых понятие множества строго определяется посредством набора аксиом, но при этом используются уже другие неопределяемые понятия.

Обозначение: прописными буквами: ***A, B, C,…,X, … .***

Отдельные объекты, из которых состоит множество, называют ***элементами множества***.
Обозначение: строчными буквами *a, в, c, …*

Для указания того, что некоторый элемент *«a»* является элементом множества *A*, используют символ $\in$ принадлежности множеству: запись $a \in A$ означает, что элемент *a* принадлежит множеству *A*.

Запись $x \notin X$ означает, что элемент *x* не принадлежит множеству *X*.

$x_1, x_2, \ldots, x_n \in X$ сокращение для записи $x_1 \in X, x_2 \in X, \ldots, x_n \in X$.

Общим обозначением множества служит пара фигурных скобок *{ }*, внутри которых перечисляются элементы множества.

Стандартные обозначения множеств:
N - множество натуральных чисел;
Z - множество целых чисел;
Q - множество рациональных чисел;
R - множество действительных чисел;
C - множество комплексных чисел;

Способы задания множеств - *перечисление* и *описание*:

1. *Перечисление* соответствует записи в фигурных скобках всех элементов множества через запятую.

Пример 1:
$Y = \{a, b, c, d\}$ - множество, состоящее из элементов *a, b, c, d*;
$X = \{2,4,6,8,\ldots\}$ - такая запись применима, если вполне ясно, что понимается под многоточием.

2. *Описание* или *рекурсия* состоит в том, что указывается характерное свойство, которым обладают все элементы множества.

Пример 2:
$A = \{x \mid x - \text{четное}\}$ - множество четных чисел (читается: множество *A* состоит из элементов *x*, обладающих свойством *x* - четное);
$B = \{x \mid x^2 - 1 = 0\}$ - множество корней уравнения $\{+1, -1\}$;
Пусть *Z* - множество целых чисел, тогда $\{x \in Z \mid 0 < x \le 7\}$ есть множество $\{1,2,3,4,5,6,7\}$.

Важным понятием теории множеств является понятие *пустого* множества.

Определение 2

Пустым множеством называют множество, не содержащее ни одного элемента.

Обозначение: $\emptyset$.
Пустое множество можно задать следующим образом:

$$\{x \in R \mid x^2 + 1 = 0\} = \emptyset$$

В алгебре множеств пустое множество $\emptyset$ играет роль, аналогичную роли числа 0 в обычной числовой алгебре.

Рассмотрим отношения между множествами.

Определение 3

Два множества называют **равными**, если они состоят из одних и тех же элементов.

Обозначение: $A = B$.

Пример 3
$A = \{3,4,5,6\};\ B = \{4,5,6,3\};\ A = B$.

Определение 4

Множество *A* называют **подмножеством** или **частью множества** *B*, если каждый элемент множества *A* является элементом множества *B*.

Обозначение: $A \subseteq B$. $\subseteq$ - знак нестрогого включения.

В число подмножеств множества *B* входит, как это видно из определения, само это множество.

Кроме того, в теории множеств постулируется, что пустое множество $\emptyset$ есть подмножество любого множества.

Множество всех подмножеств множества *B* называется ***множеством-степенью*** или ***булеаном*** множества *B*. Обозначение: 2^B или *P(A)*.

Непустые подмножества множества *B*, не совпадающие с *B*, называют ***истинными*** или ***собственными*** подмножествами.

Обозначение: $A \subset B$. $\subset$ - знак строгого включения.

Пример 4

1). $B = \{1,2,3\}$ тогда $\{1,2\},\{2,3\},\{3,1\},\{1\},\{2\},\{3\}$ - собственные подмножества множества *B*;

2). $N_{нат} \subset Z_{цел} \subset Q_{рац} \subset R_{дей} \subset C_{компл}$, причем каждое из множеств есть собственное подмножество каждого последующего.

Определение 5

Отображением (или **однозначным отображением**) множества *X* во множество *Y* называется тройка $\langle X,Y,f \rangle$, где *X* и *Y* - два непустых множества, *f* - правило, сопоставляющее каждому элементу $x \in X$ ***однозначно определенный*** элемент $y=f(x) \in Y$.

Обозначение: $f: X \to Y$.

Множество *X* - ***область определения*** отображения; элемент $x \in X$ - аргумент отображения; множество *Y* - область значений функции; элемент *y* - ***образ*** **элемента** *x* при отображении *f*; элемент *x* - ***прообраз*** элемента *y* при отображении *f*. Множество всех прообразов элемента *y* при отображении *f* называется *полным прообразом* элемента *y* при отображении *f* и обозначают $f^{-1}(y)$.

Часто в случае, когда множества *X* и *Y* - числовые, отображение называют ***функцией***. Если только множество *Y* - числовое, то отображение называют ***функционалом***.

Функциональные отображения удобно изображать в виде графов.

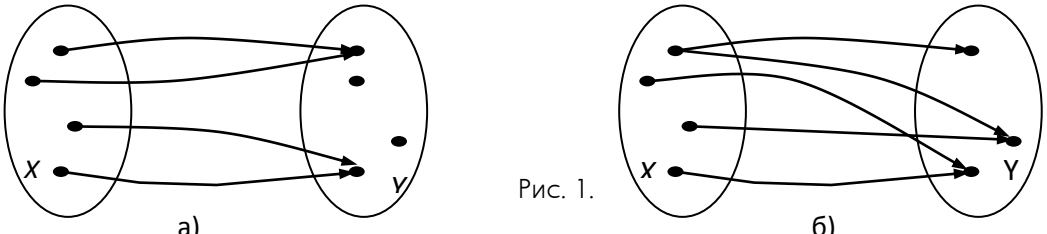


Рис. 1.

Граф на рис.1 (а) представляет функцию, а граф на рис.1 (б) не изображает функцию, т.к. в множестве *X* существуют элементы, которым соответствуют не один, а несколько элементов множества *Y*.

Определение 6

Множество $f(A)=\{f(x): x \in A, A \subseteq X\}$ называется **образом подмножества** *A* при отображении *f*.

Множество $f^{-1}(B)=\{x \in X: f(x) \in B, B \subseteq Y\}$ называется **прообразом подмножества** *B*.

Пример 5

Пусть $X=Y=\{1, 2, 3\}$. Отображение $f: X \to Y$ задано следующим образом:
$f(1)=1$, $f(2)=1$, $f(3)=2$.

Тогда $f(X)=\{1, 2\}$ - образ множества X. У элемента $1 \in Y$ два прообраза - 1 и 2; у элемента $2 \in Y$ один прообраз - 3; у элемента $3 \in Y$ прообразов нет.

Определение 7

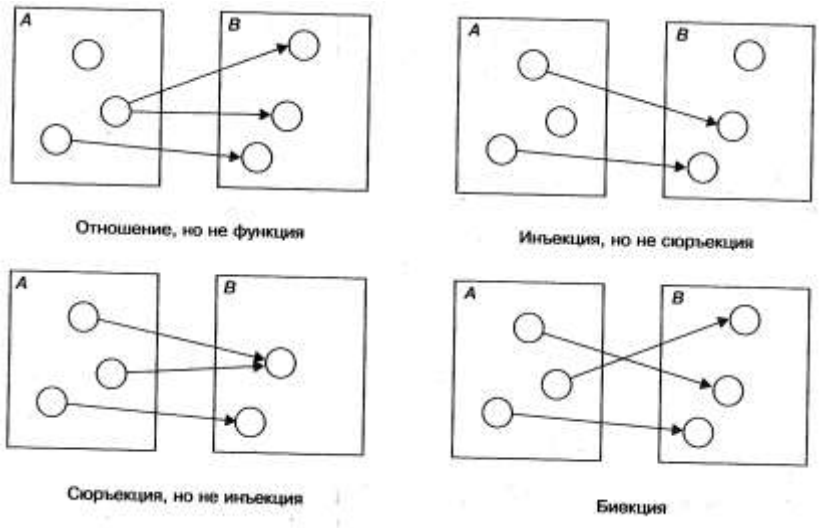
Отображение $f: X \to Y$ называется:

инъективным (или **отображением "в"**), если $\forall\ x_1, x_2 \in X, y \in Y$: $y=f(x_1), y=f(x_2) \Rightarrow x_1 = x_2$;

сюръективным (или отображением "**на**"), если $\forall\ y \in Y\ \exists\ x \in X$: $y = f(x)$;

биективным (или **взаимно-однозначным**), если f сюръективно и инъективно.

Другими словами, отображение называется инъективным, если каждый элемент из области его значений имеет единственный прообраз; сюръективным - если область его значений совпадает со множеством Y. Существование биекции $f: X \to Y$ означает, что каждому элементу множества X соответствует единственный элемент множества Y и наоборот. Тогда и говорят, что f осуществляет ***взаимно-однозначное соответствие*** между множествами X и Y.



Отображения вида $f: X \to X$ называются преобразованиями множества X

Биекцию множества X в себя называют ***автоморфизмом*** множества X.

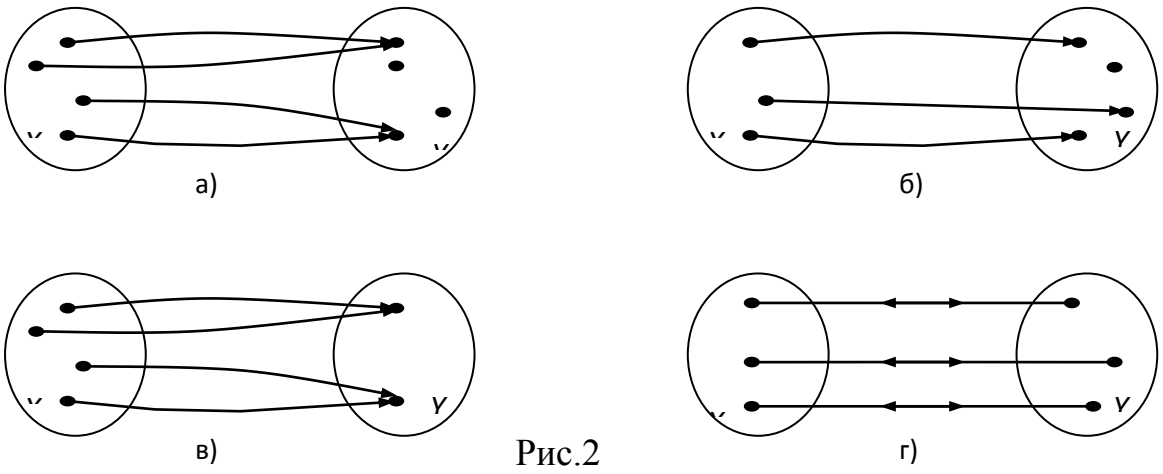


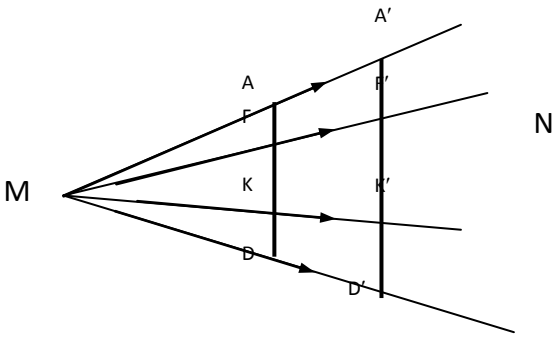
Рис.2

- Отображение множества X ***на*** множество Y: рис. в), г);
- Отображение множества X ***во*** множество Y: рис. а), б).

Является ли отображение «***на***» в то же время и отображением «***в***»? (Да! Обратное утверждение неверно).

Замечание. Одно и то же правило соответствия может быть сюръективным, инъективным или биективным отображением в зависимости от исходных множеств X и Y.

Использование термина «отображение» оказывается особенно полезным при рассмотрении точечных множеств. Например, естественно рассматривать функцию, заданную графом на рис.3 как ***однозначное отображение*** множества точек отрезка AB на множество точек отрезка $A'B'$, устанавливаемое подвижным лучом MN, вращающимся вокруг точки M.



Определение 8

Тождественным отображением множества X в себя называется отображение $e_X : X \to X$ такое, что $\forall x \in X$: $e_X(x)=x$.

Тогда, если $f : X \to Y$, то $e_Y \circ f = f$, $f \circ e_X = f$

Определение 9

Композицией (или **суперпозицией**) двух отображений $f : X \to Y$ и $g : Y \to Z$ называется отображение $g \circ f : X \to Z$ определяемое равенством

$$g \circ f = g(f(x)), \text{ где } x \in X$$

В некоторых учебниках композицию обозначают наоборот $f \circ g$, подчеркивая, что порядок записи функций в композиции совпадает с порядком их применения.

Замечание. Композиция определена не для любых пар отображений. Однако, композиция двух преобразований одного и того же множества определена всегда.

Итак, если множеств X отображено «***на***» или «***в***» множество Y, то говорят, что задана функция $x \xrightarrow{f} y = f(x)$.

Естественно возникает вопрос о возможности отобразить множество Y «на» или «в» множество X, т.е. вопрос о возможности из данного отображения образовать такое, что $\forall y \in Y$ соответствовал единственный прообраз $x \in X$.

Чтобы ответить на этот вопрос, рассмотрим различные виды отображений множества X ***на*** и ***в*** множество Y (см. рис.2). Для того, чтобы получить отображение множества Y ***на*** множество X необходимо следующее:

1. Каждый элемент множества Y должен входить в какую-либо пару множества пар (y, x);
2. Каждому значению y должно быть поставлено в пару ***единственное*** значение x.

Из рассмотренных на рис.2 отображений только отображение г) удовлетворяет названным условиям. Такое отображение называется ***обратимым***.

Пусть $f : X \to Y$ и $g : Y \to X$.

Определение 10

Отображение g называется обратным к отображению f (а f - обратным к g), если

$$f \circ g = e_Y, \quad g \circ f = e_X$$

Обозначение: f^{-1}. Обратное отображение существует не всегда.

Утверждение 1.

Отображение $f: X \to Y$ имеет обратное $f^{-1}: Y \to X$ тогда и только тогда, когда f - биекция.

Замечание. Если обратное отображение существует, то оно единственно.

Вопрос 2. Конечные и бесконечные множества

Рассмотрим понятие количества элементов во множестве, на основе которого можно классифицировать множества: множества бывают конечными и бесконечными; бесконечные множества, в свою очередь, - счетными и несчетными.

Определение 11

Множество называется **конечным**, если число его элементов конечно, т.е. если существует натуральное число n, являющееся числом элементов множества.

Множество, не являющееся конечным, называется **бесконечным**.

Число n элементов конечного множества X называется ***мощностью*** *или* ***порядком*** множества X.

Обозначение: $|X|$.

Множество мощности n называют n - *множеством.*

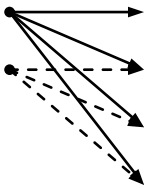
Определение 12

Два множества называются **равномощными** (или **эквивалентными**), если существует биекция одного из них на другое.

Обозначение: $|X|=|Y|$ или $X \sim Y$.

Пусть X и Y два конечных множества, m и n - элементные соответственно. Между ними можно установить взаимно однозначное соответствие, если $m=n$.

Сколько же существует таких взаимно однозначных соответствий для двух «n» элементарных множеств X и Y?



"X" "У"

Первый элемент множества X может быть сопоставлен с любым из n элементов множества Y.

Второй элемент множества X может быть сопоставлен с оставшимися $(n-1)$ элементов множества Y, и т.д.

Таким образом, общее число взаимно однозначных соответствий равно $n(n-1)\cdots 1 = n!$

Рассмотрим бесконечные множества. Оказывается, что бесконечные множества могут иметь разные мощности.

Определение 13

Бесконечное множество, элементы которого возможно пронумеровать натуральными числами, называется **счетным**.

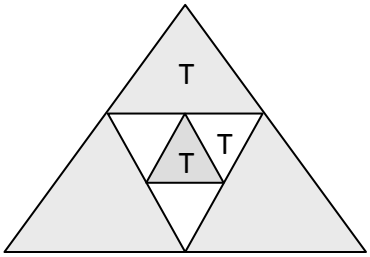
Другими словами, бесконечное множество является счетным, если его элементы возможно привести во взаимно-однозначное соответствие с натуральным рядом чисел N.

Мощность счетного множества обозначают $\aleph_0$ (читается "**алеф-нуль**").

Не все бесконечные множества являются счетными.

Определение 14

Если бесконечное множество невозможно привести во взаимно однозначное соответствие с натуральным рядом чисел, то оно называется **несчетным**.



Пример 7

1) Бесконечное множество равносторонних треугольников, его можно привести в взаимно однозначное соответствие с натуральным рядом чисел, расположив в порядке уменьшения длин сторон $T_1, T_2, T_3, \ldots, T_n, \ldots \Rightarrow$ это **счетное множество;**

2) Простые числа - счетное множество;

3) Натуральные числа - счетное множество;

4) Множество всех целых чисел Z={...-2, -1, 0, 1, 2...}, хотя натуральный ряд представляет собой лишь подмножество этого множества:

N:	1	2	3	4	5	6	…
Z:	0	1	-1	2	-2	3	…

- **счетно;**

5) Множество рациональных чисел Q счетно.

Теорема 1.

Любое бесконечное множество содержит счетное подмножество.

Теорема 2.

Множество 2^N, то есть множество всех подмножеств натуральных чисел, **несчетно.**

Рассмотренное множество $2^N \sim [0, 1] \sim [a, b] \sim R$.

Таким образом, несчетным является множество всех действительных чисел R.

Определение 15

Мощность множества всех действительных чисел R называется **континуумом**.

До сих пор речь шла о равенстве мощностей. Однако мощности разных множеств можно в определенном смысле сравнивать, говоря о большей или меньшей мощности.

Например, мощность любого конечного множества строго меньше мощности $\aleph_0$, а $\aleph_0$, в свою очередь, меньше континуума.

Теорема (Кантора-Берштейна).

Для любых двух множеств X и Y имеет место в точности одно из следующих трех условий: либо $|X| < |Y|$, либо $|Y| < |X|$, либо $|X| = |Y|$.

Таким образом, любые два множества сравнимы по мощности.

Теорема 3.

Для любого множества X верно неравенство $|2^X| > |X|$.

Из теоремы следует, что имеются несчетные множества, мощности сколь угодно большей, чем континуум. Например, множество 2^R всех подмножеств R (булеан R) является множеством мощности большей, чем континуум. Однако неизвестно о существовании множеств промежуточной мощности между счетным N и котинуумом R (*проблема континуума*).

Вопрос 3. Операции над множествами. (Вопрос 4. Кортеж, Вопрос 7. Разбиение мн-в)

Рассмотрим способы получения новых множеств из уже существующих.

Определение 16

Объединением множеств *A* и *B* называют множество, состоящее из всех тех и только тех элементов, которые принадлежат хотя бы одному из множеств *A* и *B*, т.е. принадлежат множеству *A* **или** множеству *B*.

Обозначение: $A \cup B$.

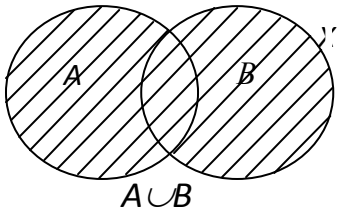
Итак, $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.

Объединение множеств иногда называют *суммой множеств* и обозначают *A+B*.

Пример 8

$A = \{1,2,3,4,5\}, B = \{2,4,6,7\}$. Тогда $A \cup B = \{1,2,3,4,5,6,7\}$

Для наглядного представления операций над множествами используют диаграммы Эйлера-Венна.



Пусть *A* - множество точек левого круга, *B* - множество точек правого круга, то $A \cup B$ есть заштрихованная область.

Понятие объединения можно распространить и на большее число множеств.

Объединение множеств $A_1, A_2, \ldots, A_n$ есть множество, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из этих множеств:

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

Справедливы законы:

1). $A \cup B = B \cup A$ - *коммутативный* или *переместительный*;

2). $(A \cup B) \cup C = A \cup (B \cup C)$ - *ассоциативный* или *сочетательный*.

Очевидно также: $A \cup \emptyset = A$; $A \cup A = A$.

Определение 17

Пересечением множеств *A* и *B* называют множество, состоящее из всех тех и только тех элементов, которые принадлежат как множеству *A* так **и** множеству *B*.

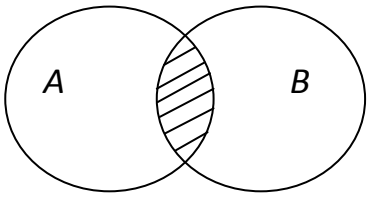
Обозначение: $A \cap B$.

Итак, $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.

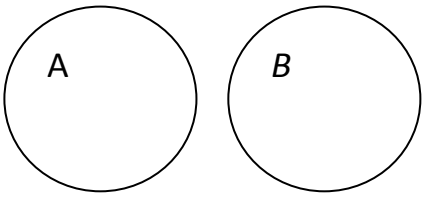
Пример 9

$A=\{1,2,3,4,5\},\ B=\{2,4,6,7\},$ то $A\cap B=\{2,4\}.$

Диаграмма Эйлера-Венна:



$A\cap B$



непересекающиеся множества

Обобщим операцию пересечения на n множеств.

Пересечение множеств $A_1,A_2,\dots,A_n$ есть множество, состоящее из всех тех и только тех элементов, каждый из которых принадлежит всем этим множествам:

$$A_1\cap A_2\cap\cdots\cap A_n=\bigcap_{i=1}^{n}A_i\ .$$

Справедливы законы:

1). $A\cap B=B\cap A$ - *коммутативный* или *переместительный*;

2). $(A\cap B)\cap C=A\cap(B\cap C)$ - *ассоциативный* или *сочетательный*.

Заметим, что $A\cap\emptyset=\emptyset;\ A\cap A=A$

Определение 18

Множества X и *Y* называются **непересекающимися**, если они не имеют общих элементов, т.е. если $A\cap B=\emptyset$.

Пример 10

Пусть $A=\{1,2,3\}$ и $B=\{4,5,6\}$. Тогда $A\cap B=\emptyset$.

Связь между операциями объединения и пересечения:

1). законы дистрибутивности:

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

2). законы поглощения:

$$A\cup(A\cap B)=A$$
$$A\cap(A\cup B)=A.$$

Определение 19

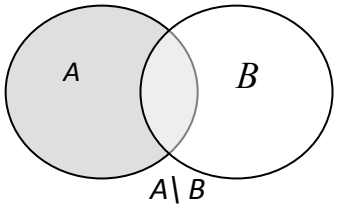
Разностью множеств *A* и *B* называют множество, состоящее из всех тех и только тех элементов, которые принадлежат *A* и не принадлежат *B*.

Обозначение: *A* \ *B*.

Итак, $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$

В примере 9:

$X = \{1,2,3,4,5\}$ $Y = \{2,4,6,7\}$, то $X \setminus Y = \{1,3,5\}$; $Y \setminus X = \{6,7\}$.



$A \setminus B$

Из определения следует, что

$$(A \setminus B) \cup (A \cap B) = A.$$

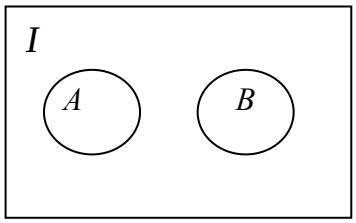
Для рассмотрения следующей операции необходимо ввести понятие универсального множества.

Универсальным множеством или ***универсумом*** в теории множеств является совокупность всех подмножеств.

Обозначение: *I* или *U*.

Другими словами, если все рассматриваемые в ходе данного рассуждения множества являются подмножествами некоторого множества *I*, то это множество *I* называется ***универсальным*** для данного рассмотрения.

Его удобно изображать графически в виде множества точек прямоугольника. Отдельные области внутри этого прямоугольника будут означать различные подмножества универсального множества:



Например, универсальным множеством в теории вероятностей является ПЭС, а случайные события - его подмножества.

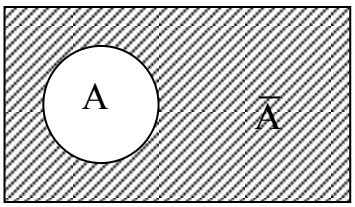
Можно продемонстрировать и другой подход к понятию универсального множества. Как мы видели, роль нуля в алгебре множеств играет пустое множество. Не существует ли множество *I*, которое будет играть *роль* ***единицы***, т.е. удовлетворять условию $A \cap I = A$, аналогичному $a \cdot 1 = a$ в обычной алгебре?

В соответствии с введенным выше понятием, такой "единицей" является универсальное множество.

С другой стороны, универсальное множество обладает интересным свойством, которое не имеет аналогии в обычной алгебре: для любого подмножества *A* справедливо $A \cup I = I$.

Определение 20

Множество $\overline{A}$, определяемое из соотношения $\overline{A} = I \setminus A$, называется **дополнением (абсолютным дополнением)** множества *A* до универсального.



Итак, дополнение множества *A* – это множество всех элементов универсального множества, не принадлежащих *A*:

$$\overline{A} = \{x \mid x \in I \text{ и } x \notin A\}.$$

Справедливы следующие соотношения:

1). $A \cup \overline{A} = I$, $A \cap \overline{A} = \emptyset$, $\overline{\overline{A}} = A$;

2). законы де Моргана:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Замечание. Операция 11 также называется **относительным дополнением** множества *B* до множества *A*.

Каждое из написанных выше равенств верно для любых подмножеств *A, B, C* универсального множества *I*. Они называются *основными тождествами алгебры множеств*. Любое из них может быть доказано: **методом двух**

включений; с помощью диаграмм Эйлера-Венна. Кроме того тождества можно доказывать, используя ранее доказанные тождества для преобразований левой части к правой и наоборот. Такой метод доказательства часто называют **методом эквивалентных преобразований.** Могут быть использованы и другие методы, например **метод характеристических функций.**

Утверждение 3.

Предложения о произвольных множествах A и B попарно эквивалентны:

1). $A \subseteq B$; 2). $A \cap B = A$; 3). $A \cup B = B$.

Наряду с понятием множества как совокупности элементов важным понятием является понятие ***упорядоченного множества*** или ***кортежа***.

Определение 21

Кортежем называется совокупность элементов, в которой каждый элемент занимает определенное место.

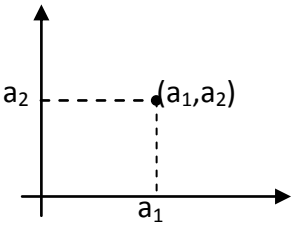
Сами элементы при этом называются **компонентами кортежа** (первая компонента, вторая и т.д.).

Обозначение: используют круглые скобки: $a = (a_1, a_2, \ldots, a_n)$ - это кортеж длины n с элементами $a_1, a_2, \ldots, a_n$.

Например:

1. Множество людей в очереди;
2. Множество слов в фразе;
3. Числа, выражающие декартовы координаты точки в пространстве т.(x,y, z).

Порядок чисел существенен: (1,0,-1), (-1,0,1) - разные точки пространства.



Кортеж (a_1, a_2) - точка на плоскости или вектор, проведенный из начала координат в данную точку. Компоненты a_1 и a_2 - это проекции вектора на оси.

Кортеж (a_1, a_2, a_3) - точка в 3-х мерном пространстве или трехмерный вектор.

Определение 22

Число элементов кортежа называют его **длиной**.

В отличие от обычного множества в кортеже могут быть и одинаковые элементы.

Определение 23

Прямым (декартовым) произведением множеств *A* и *B* называют множество, состоящее из всех тех и только тех упорядоченных пар, первая компонента которых принадлежит множеству *A*, а вторая - множеству *B*.

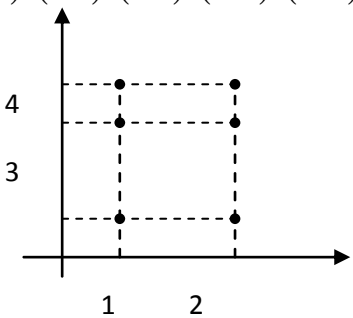
Обозначение: $A \times B$.

Итак, $A \times B = \{(x, y) \mid x \in A, y \in B\}$

Пример 11

$X = \{1,2\}$, $Y = \{1,3,4\}$, тогда $X \times Y = \{(1,1), (1,3), (1,4), (2,1), (2,3), (2,4)\}$.

Графическая интерпретация:



Свойства декартового произведения:

1) $A\times(B\cup C)=(A\times B)\cup(A\times C)$;
2) $A\times(B\cap C)=(A\times B)\cap(A\times C)$;
$A\times\varnothing=\varnothing\times A=\varnothing$.

Однако свойства прямого произведения отличаются от свойств обычного произведения в арифметическом смысле: $A\times B\neq B\times A$ (проверить самостоятельно).

Прямым (декартовым) произведением множеств $A_1,\ldots,A_m$ называется множество всех кортежей длины m. Обозначение: $A_1\times\ldots\times A_m$.

Итак, $A_1\times\ldots\times A_m=\{(a_1,\ldots,a_m)\mid a_1\in A_1,\ldots,a_m\in A_m\}$

Определение 24

***m*–й декартовой степенью множества** A называется декартово произведение m сомножителей $A^m=A\times A\times\ldots\times A$.

В частности, при $m=2$ получаем декартов квадрат, а при $m=3$ – декартов куб множества A.

По определению полагают, что первая декартова степень любого множества A есть само множество A, т.е. $A^1=A$.

Определение 25

Любой кортеж из A^m называется **упорядоченной выборкой** размера m из множества A, или **словом** длины m **в алфавите** A, или **последовательностью** длины m **над множеством** A.

Несложно доказать (по индукции) следующее утверждение.

Утверждение 4.

$$|A_1\times A_2\times\ldots A_m|=\prod_{i=1}^{m}|A_i|$$

Системы подмножеств множества

Определение 26

Покрытием множества A называется совокупность подмножеств $\{A_1,A_2,\ldots,A_n\}$ таких, что объединение всех подмножеств A_i, где $i=1, 2,\ldots, n$ есть данное множество A, то есть $A=A_1\cup A_2\cup\ldots\cup A_n$.

Определение 27

Разбиением множества A называется его покрытие $\{A_1,A_2,\ldots,A_n\}$ если выполняются условия:

1) все подмножества A_i - *непустые*, то есть $\forall i\ \ A_i\neq\emptyset,\quad A_i\subset A$;
2) любые два подмножества A_i,A_j - *непересекающиеся*, то есть $\forall i,j\quad i\neq j,\quad A_i\cap A_j=\emptyset$.

Другими словами, *разбиением* множества A называется совокупность попарно непересекающихся подмножеств A таких, что каждый элемент множества A принадлежит одному и только одному из этих подмножеств.

Пример 12

Дано множество $A=\{1,2,3,4,5\}$.

1). Система подмножеств $A_1=\{1,2\}, A_2=\{3,4\}$ не будет разбиением этого множества, так как $A_1 \cup A_2 \neq A$.

2). Система подмножеств $A_1=\{1,2,3\}, A_2=\{3,4\}, A_3=\{5\}$ также не будет разбиением, так как множества A_1 и A_2 имеют общий элемент 3.

3). ***Разбиением*** этого множества будут, например, такие системы подмножеств: $A_1=\{1,2\}, \quad A_2=\{3,4\}, \quad A_3=\{5\}.$ или $A_1=\{1,2,3\}, \quad A_2=\{4,5\}.$

Подмножества данного множества, образующиеся при покрытии (разбиении), называют ***блоками покрытия (классами разбиения)***; число n - ***порядком покрытия (разбиения)***.

Тривиальным блоком разбиения множества A называется одноэлементный блок.

Например, множество всех натуральных чисел N, допускает разбиение на два класса - класс четных чисел и класс нечетных чисел. Не исключены и крайние случаи: представление множества A в виде объединения его одноэлементных подмножеств или разбиение,

Определение 28

Продолжением разбиения $\{A_1, A_2, \ldots, A_n\}$ множества A называется разбиение $\{B_1, B_2, \ldots, B_m\}$ того же множества, если для любого $i=1, 2,\ldots, m$ найдется такой номер $j=\{1,\ldots,n\}$, что $B_i \subseteq A_j$.

Отсюда следует, что $m \geq n$.

Для разбиения конечного множества A справедливо **правило суммы**:

$$|A|=|A_1|+\ldots+|A_n|,$$

для покрытия - **обобщенное правило суммы**:

$$|A| \leq |A_1|+\ldots+|A_n|.$$

Число разбиений n - множества на k непустых блоков мощностей $n_1, n_2, \ldots, n_k$ вычисляется по формуле:

$$T_n(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$$

Вопрос 5, 6. Понятие отношения. Бинарные отношения и их свойства

Пример 1. Рассмотрим два множества: первое *(X)*, состоящее из 11 студентов и второе *(Y)*, состоящее из 9 городов.

Чтобы получить прямое произведение этих множеств, надо составить все пары: (студент, город). Из множества всех таких пар мы выберем лишь такие пары, которые «связывают» каждого студента с тем городом,

где он бывал. Очевидно, что «список» таких пар (студент, известный город) будет являться подмножеством декартова произведения.

Вот несколько пар этого «списка»: (А - Москва), (А - СПб), (В - Одесса) и т.д.

Такой список удобно заменить таблицей, способной указать все города, в которых побывал студент.

X \ Y	Москва	СПб	Киев	Одесса	Ярославль	Ульяновск	Тула	Рига	Курск
1. А									
2. В									
3. Г									
4. Д									
5. Е									
6. З									
7. И									
8. К									
9. Л									
10. М									
11. Н									

Говорят, что *данная таблица задает определенное отношение между элементами множества X и элементами множества Y.*

Между элементами одного множества тоже можно задавать различные отношения. Если отношение задается между двумя элементами, то такое отношение называют **бинарным**.

Пример 2 бинарных отношений: ●

1. Между числами: равно, не равно, меньше, больше, не меньше, не больше.
2. Между точками прямой: предшествует, следует за.
3. Между множествами: включается, равно, пересекается, не пересекается.

Пусть X - непустое множество.

Определение 1
Бинарным (или **двухместным**) **отношением** Q на множестве X, называется произвольное подмножество упорядоченных пар (x, y) этого множества.

Обозначение: xQy или $(x, y) \in Q$

Элементы x и y называют *координатами* (*компонентами*) отношения Q.

Например, на множестве натуральных чисел N зададим отношение "меньше": $3 < 7$ и $(3,7) \in <$ - обозначает одно и тоже.

Пусть X и Y - два непустых множества.

Определение 2
Бинарным отношением Q на множествах X и Y, называется произвольное подмножество упорядоченных пар (x, y), где $x \in X, y \in Y$.

Вывод:
Каждое бинарное отношение Q на множестве X есть подмножество прямого произведения X^2 - декартова квадрата множества X; на множествах X и Y - подмножество прямого произведения $X \times Y$, то есть $Q \subseteq X \times Y$.

Определение 3

Областью определения бинарного отношения Q называется множество $D_Q = \{x \mid \exists\ y$ такое, что $xQy\}$.

Областью значений бинарного отношения Q называется множество $R_Q = \{y \mid \exists\ x$ такое, что $xQy\}$.

В примере 1: X - множество из всех 11 студентов, Y - множество из всех 9 городов, D_Q - область определения отношения (это множество студентов, исключая студентов Д и Л, ни разу не бывавших ни в одном из указанных городов), R_Q - область значений (множество всех городов, исключая Ригу, где никто из студентов не побывал).

Само множество X называют областью *отправления* отношения, а множество Y - областью *прибытия* отношения.

Пример 3

1). X={2, 4}, Y={1, 2, 3, 4}, отношение Q: Y делится на X.
Зададим перечислением это отношение: Q= {(2, 2), (2, 4), (4, 4)}.
Область определения такого отношения D_Q ={2, 4}, область значений R_Q ={2, 4}.

2). Рассмотрим на множестве действительных чисел R отношение Q: равенство "=". Здесь множества $D_Q = R_Q = R$ (совпадают со множеством действительных чисел);

3). Рассмотрим множество {(1, 2), (2, 4), (3, 3), (2,1)}.
Это бинарное отношение Q на множествах X={1,2, 3}, Y={1, 2, 3, 4}.
$D_Q = X$, $R_Q = Y$.

Отношение может быть определено не только для пар объектов, но и для троек, четверок и т.д., то есть для n объектов.

Определение 3

n-местным (n–арным) отношением на множествах $X_1,\ldots,X_n$ называется произвольное подмножество упорядоченных n-ок $(x_1,\ldots,x_n)$.

Т.о, каждое n-арное отношение Q на множествах X_i, i=1, 2,...,n есть подмножество прямого произведения множеств $X_1 \times \cdots \times X_n$.

Среди отношений на множествах особую роль играют отношения между элементами одного множества. Считают, что для элементов некоторого множества X задано бинарное отношение, если про любые два элемента этого множества известно, находятся они в этом отношении или не находятся.

Способы задания бинарных отношений на конечных множествах:

- список пар, для которых это отношение выполняется;
- матрица отношения;
- граф отношения.

Определение 4

Матрицей бинарного отношения на множестве $X = \{x_1,\ldots,x_n\}$ называется квадратная матрица Q порядка n, в которой элемент q_{ij}, стоящий на пересечении i-й строки и j-го столбца определяется так:

$$q_{ij} = \begin{cases} 1, \text{если } x_i Q\, y_j \\ 0, \text{в противном случае} \end{cases}.$$

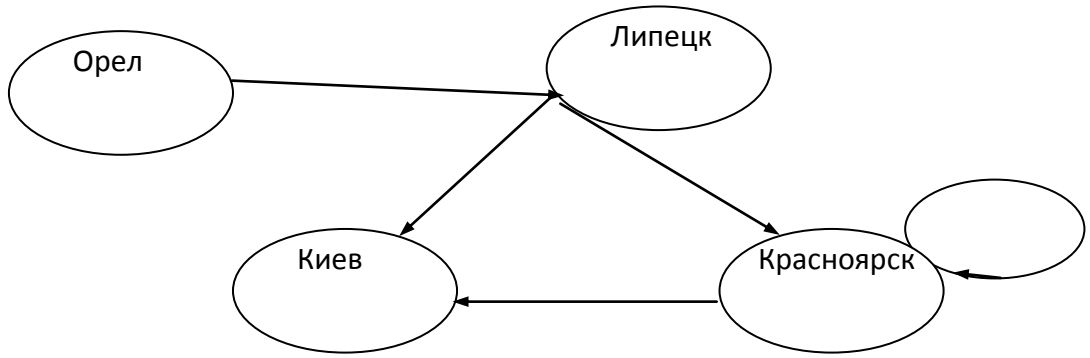
Пример 4

Для конечного множества $X=\{1,2,3,4,5,6\}$ матрица отношения Q: $x \le y$ имеет вид:

Q	1	2	3	4	5	6
1	1	1	1	1	1	1
2	0	1	1	1	1	1
3	0	0	1	1	1	1
4	0	0	0	1	1	1
5	0	0	0	0	1	1
6	0	0	0	0	0	1

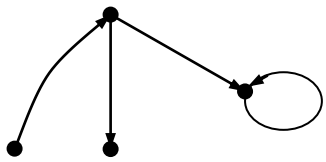
Пример 5

На множестве названий городов *X*={Орел, Липецк, Киев, Красноярск} определим отношение *Q*: последняя буква названия одного города является первой буквой в названии другого.



Красноярск находится в указанном отношении *Q* с самим собой. Это отражается на схеме с помощью одной стрелки «исходящей» из этого слова и «заходящей» в него; здесь две стрелки заменены одной.

Придадим схеме более сжатую форму, обозначив города точками.



Такое множество точек, и связывающих их дуг называют *графом*, а сами точки - *вершинами графа*.

Таким образом, если множество *X* - конечное множество, то отношение *Q*, определенное на этом множестве, можно задавать ориентированным графом.

Граф отношения строится следующим образом:

- если имеет место xQy, то на рисунке изображается стрелка, ведущая от точки, соответствующей элементу *x*, к точке, соответствующей элементу *y*;
- если имеет место xQx, то на рисунке изображается петля, исходящая из точки образа элемента *x* и заходящая в ту же точку.

Итак, граф является геометрической интерпретацией отношения.

Многоместные отношения удобно задавать с помощью *реляционных таблиц*. Такое задание соответствует перечислению множества *n*-ок отношения *Q*:

A_1	A_2	...	A_n
a_1	a_2	...	a_n
a_1	a_1	...	a_1
...	...	...	...

Реляционные таблицы широко используют в компьютерной практике в реляционных базах данных. При этом множества A_i называют *атрибутами* (свойствами), а элементы $a_i \in A_i$ - *доменами* (значениями) атрибутов.

Определение 5

Обратным отношением для отношения Q называется отношение

$$Q^{-1} = \{(x,y): (y,x) \in Q\}.$$

Определение 6

Композицией бинарных отношений Q_1 и Q_2 называется отношение

$$Q_1 \circ Q_2 = \{(x,z): \exists_y \text{ такое, что } (x,y) \in Q_1 \text{ и } (y,z) \in Q_2\}.$$

Утверждение 1

Для любых бинарных отношений выполняются свойства:

1) $(Q^{-1})^{-1} = Q$;
2) $(Q_1 \circ Q_2)^{-1} = (Q_2)^{-1} \circ (Q_1)^{-1}$.

Определение 7

Бинарное отношение f, определенное на паре множеств X и Y, называется **однозначным отображением** или **функцией**, если имеют место следующие свойства:

1. $\forall x \in X$, $\exists y \in Y$: $(x,y) \in f$;
2. $\forall x \in X$, $\forall y,z \in Y$: xfy и $xfz \Rightarrow y = z$.

Обозначение: функция как отображение обозначается $f: X \to Y$.

Другими словами, **функцией** называется соответствие, определяющее $\forall x \in X$ *единственный элемент* $y \in Y$. При этом записывают: $y = f(x)$.

Пример 6

1). Рассмотрим отношение вида $\{(1, 2), (2, 3), (\square,\Delta)\}$.

Такое отношение есть функция на множествах $X = \{1, 2, \square\}$ и $Y = \{2, 3, \Delta\}$.

2). Отношение вида $\{(1, 2), (1, 3), (2,4)\}$ не является функцией: значению $x=2$ соответствует два значения y: 2 и 3.

3). Отношение $\{(x, x^2+2x+1): x \in R\}$ - функция, которую обычно записывают $y=(x+1)^2$.

Определение 8

Отношение f называется ***n*-местной функцией** из X в Y, если f: $X^n \to Y$.

Обозначение: $y=f(x_1, x_2, ..., x_n)$.

Для отображения были введены понятия *инъекции, сюръекции, биекции*.

В силу того, что функция есть отображение, эти понятия применимы и к функции.

Пример 7

Пусть f: $R \to R$.

1) Функция $f(x)=e^x$ - инъективна, но не сюръективна;
2) $f(x)=x^3 - x$ - сюръективна, но не инъективна;
3) $f(x)=2x+1$ - биективна.

Определение 9

Композицией двух функций f и g называется отношение

$$g \circ f = \{(x,z): \exists_y \text{ такое, что } xfy \text{ и } ygz\}.$$

Утверждение 2

Композиция двух функций есть функция. При этом, если $f: X \to Y$, $g: Y \to Z$, то $g \circ f : X \to Z$.

Утверждение 3

Композиция двух биекций есть биекция.

Замечание. Для того, чтобы обратное отношение f^{-1} было функцией, достаточно инъективности функции f.

Поскольку функция есть бинарное отношение, то выполняются следующие свойства:

для инъективных функций f и g:

1). $(f^{-1})^{-1} = f$;

2). $(g \circ f)^{-1} = (f)^{-1} \circ (g)^{-1}$.

для биективной функции f:

1) $(f^{-1} \circ f) = e_x$;

2) $f \circ f^{-1} = e_y$.

Свойства отношений

Существует бесконечное множество отношений самой разнообразной природы. Например, среди отношений родства на множестве людей можно выделить отношения «быть родственником», «быть братом», «быть отцом» и т.д. В математике: «быть кратным», «быть параллельным», «быть обратным» и т.д. Кажется, что невозможно ориентироваться в этом многообразии отношений.

Однако существует несколько замечательных свойств отношений, которые позволяют подразделить все основные отношения на сравнительно небольшое число типов и тем самым изучать не каждое отношение отдельно, а сразу множество отношений одного и того же типа. Рассмотрим эти свойства.

Пример 8

1). A={множество людей}, Q - отношение «быть родственником».

Заметим, что каждый человек является родственником самому себе, т.е. aQa.

2). N - множество натуральных чисел, отношение Q - «быть кратным». Нетрудно заметить, что любое число a кратно самому себе: aQa или $a \vdots a$ (дел. нацело).

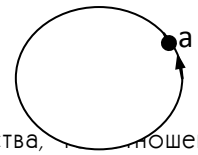
Два различных отношения из рассмотренных примеров, обладают общим свойством: если $a \in A$, то aQa.

Определение 10

Если отношение Q, установленное между элементами одного или нескольких множеств таково, что любой элемент множества находится в данном отношении Q с самим собой, то такое отношение называется **отношением рефлексивности**, а данное свойство - **свойством рефлексивности**.

Итак, для рефлексивного отношения Q выполняется: $\forall a \in A: \quad aQa$ или $\forall a \in A: (a,a) \in A$.

С помощью графа это отношение изобразим так:



Замечание:

Если aQa справедливо не для каждого элемента множества, то отношение Q в этом случае свойством рефлексивности не обладает.

Определение 11

Отношение называется **антирефлексивным**, если ни для какого $a \in A$ не выполняется aQa.

Например, отношение "быть перпендикулярным" на множестве прямых; отношение "<" на множестве действительных чисел.

Определение 12

Отношение называется **нерефлексивным**, если оно ни рефлексивно, ни антирефлексивно.

Отношение, рассмотренное в примере 5, свойством рефлексивности не обладает, так как aQa справедливо лишь для одного элемента из A - Красноярска; оно также не является антирефлексивным, поскольку все-таки выполняется для одного элемента из A - Красноярска.

Пример 9

Рассмотрим опять отношение Q - «быть родственником» на множестве людей. Легко заметить, что если один человек родственник другого, то второй так же является родственником первого, то есть если aQb, то bQa.

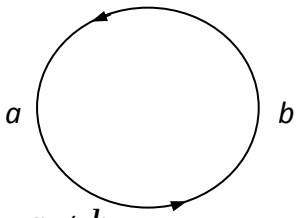
Определение 13

Если отношение Q, установленное между элементами одного или нескольких множеств, такого, что для всех элементов множества выполняется условие $aQb \Rightarrow bQa$, то такое отношение называется **симметричным**, а данное свойство - **свойством симметричности**.

Итак, для симметричного отношения Q выполняется

$\forall a, в \in A$: $aQb \Rightarrow bQa$ или $\forall a, в \in A$: $(a,в) \in Q \Rightarrow (в,a) \in Q$.

С помощью графа это отношение изобразим так:



Определение 14

Отношение называется **антисимметричным**, если наличие его между a и b, $a \neq b$, влечет за собой его отсутствие между b и a.

Например, отношение ">": из $a > b$ следует, что отношение $b > a$ не верно; отношение «a является делителем $в$».

Другими словами, отношение антисимметрично, если $\forall a, в \in A$: $(a,в) \in Q$ и $(в,a) \in Q \Rightarrow a=в$. Например, отношение "≤".

Определение 15

Отношение называется **несимметричным**, если оно не является ни симметричным, ни антисимметричным.

Например, отношение «любит» на множестве людей будет несимметричным: если M любит N $(M\,Q\,N)$, то возможны оба случая: N любит M или N не любит M.

Определение 16

Отношение Q называется **транзитивным**, если для любых a, b, c из aQb и bQc следует aQc.

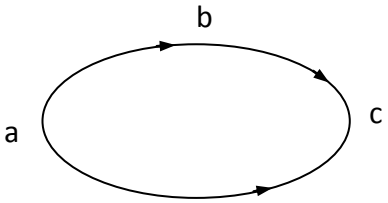
Итак, для транзитивного отношения Q выполняется

$$\forall a,b,c \in A: \; aQb, bQc \Rightarrow aQc$$

или $\forall a,b,c \in A$: $(a,b) \in Q$ и $(b,c) \in Q \Rightarrow (a,c) \in Q$.

Например, отношение «=», «≤» , «жить в одном городе», «быть родственником» - транзитивны. Отношение «быть сыном» не транзитивно.

С помощью графа, отношение транзитивности представлено на рисунке:



Определение 17
Отношение Q называется **интранзитивным**, если наличие его между a и b, b и c влечет его отсутствие между a и c.

Например, отношение «на 2 больше, чем» является интранзитивным, так как если a на 2 больше, чем b и b на 2 больше, чем c, то утверждение «a на 2 больше, чем c» - ложно.

Определение 18
Отношение Q называется **не транзитивным**, если оно не является ни транзитивным, ни интранзитивным.

Например, отношение «≠»; отношение «друг» на множестве людей: a - друг $в$ и $в$ - друг c, то могут быть обе возможности: a друг c или a не друг c.

Для бинарных отношений обычным образом определены теоретико-множественные операции объединения, пересечения и т.д.

Вопрос 8,9. Отношение эквивалентности. Отношение порядка.

В математике важную роль играют два вида специальных бинарных отношений - отношение эквивалентности и отношение порядка.

Рассмотрим отношение эквивалентности.
Отношение эквивалентности является формализацией такой ситуации, когда говорят о сходстве (одинаковости) двух элементов множества.
В предыдущем вопросе мы изучили свойства отношений: рефлексивность, симметричность и транзитивность. Например, отношение «быть родственником» обладает сразу тремя свойствами: рефлексивностью, симметричностью и транзитивностью.

Определение 19
Рефлексивное, симметричное и транзитивное отношение на множестве X называется **отношением эквивалентности** на множестве X.

Обозначение: символ ≡ или ~.

Пример 10 ●
1). В математике ярким примером отношения эквивалентности является отношение *равенства на множестве действительных чисел*: $\mathbb{R}$, Q: =

- любой элемент этого множества равен самому себе, то есть $x = x$;
- если $x = y$, то $y = x$;
- если $x = y$ и $y = z$, то $x = z$.

2). Отношение *подобия* на множестве треугольников: *X* - множество треугольников, *Q*: "подобие".

3). Отношение *«иметь одинаковый остаток от деления на 3»* на множестве натуральных чисел: *N*, *Q*: "одинаковый остаток от деления на 3".

4). Отношение *параллельности* на множестве прямых плоскости: *X* - множество прямых на плоскости, *Q*: ||.

Пример 11

Рассмотрим понятие сравнимости двух чисел по модулю.

Определение. Числа *x* и *y* называются *сравнимыми (равными) по модулю* натурального числа *n*, если разность *x-y* делится на *n*.

Число *n* называется *модулем*, каждое из чисел *x* и *y* - *вычетом* другого по модулю *n*.

Обозначение: x=y (mod *n*).

Итак, $x=y \pmod n \Leftrightarrow (x-y) \vdots n \Leftrightarrow x-y=t \bullet n$, где $t \in Z$ (*t* - некоторое целое число).

Если какое-либо число *z* несравнимо с *y* по модулю *n* (т.е. разность *z-y* не делится на *n*), то *z* называется *невычетом y* по модулю *n*.

Отношение *Q* сравнимости по модулю натурального числа *n* на множестве целых чисел *Z* обладает свойствами:

- рефлексивно: $\forall x \in Z \;\; x-x=0$ и, следовательно, $\vdots n$;
- симметрично: $\forall x, y \in Z \;\; (x-y) \vdots n \Rightarrow (y-x) \vdots n$;
- транзитивно: $\forall x, y, z \in Z \;\; (x-y) \vdots n, (y-z) \vdots n \Rightarrow (x-z) \vdots n$.

Таким образом, *Q* является отношением эквивалентности на *Z*.

Пусть *Q* - отношение эквивалентности на множестве *X*.

Определение 20

Классом эквивалентности, порожденным элементом *x*, называется подмножество множества *X*, состоящее из тех элементов $y \in X$, для которых $x \equiv y$.

Обозначение: [*x*].

Итак, $[x]=\{y \mid y \in X \text{ и } x \equiv y\}$.

Пример 12

1). Отношение равенства на множестве целых чисел *Z*, порождает следующие классы эквивалентности: для любого элемента $x \in Z \;\; [x]=\{x\}$, то есть каждый класс эквивалентности состоит только из одного элемента - числа *x*;

2). Пусть *X* - множество студентов I курса, а отношением эквивалентности является отношение *Q*: «быть в одной группе». Классом эквивалентности является все множество студентов одной группы. Группа, в которой учится студент Иванов, будет классом эквивалентности, эквивалентным студенту Иванову.

3). На множестве целых чисел *Z* отношение *Q*: «равенство по модулю натурального числа *n*» является отношением эквивалентности. Равенство чисел *x* и *y* по модулю *n* означает, что при делении на *n* эти числа дают одинаковые остатки. Отношение *Q* порождает следующие классы эквивалентности: вместе с $\forall x \in Z$ в этом же классе эквивалентности содержатся все числа вида *x* + *t*• *n*, где $t \in Z$. Действительно, $\forall x \in Z$ можно представить в виде *x=q*• *n+r*, где 0≤*r*<*n* - остаток от деления *x* на *n*. Т. о , каждое число попадает в тот же класс эквивалентности по отношению *Q*, что и остаток от его деления на *n*. Очевидно, что остатки 0, 1, 2,..., *n*-1 порождают различные классы эквивалентности по данному отношению [0], [1], [2],...,[*n*-1], которые называются *классами вычетов по модулю n*.

Отметим, что мы установили взаимно-однозначное соответствие между фактор-множеством целых чисел, равных по модулю *n*, и множеством целых чисел от 0 до *n*-1.

Утверждение 1

Пусть *Q* - отношение эквивалентности на *X*. Тогда:

1. $x \in X \Rightarrow x \in [x]$;
2. $x, y \in X, xQy \Rightarrow [x]=[y]$.

т.е. класс эквивалентности порождается любым своим элементом.

Док-во:

Отношение эквивалентности находится в тесной связи с разбиением множества.

Утверждение 2

Всякое разбиение множества X определяет на X отношение эквивалентности : $x \equiv y \Leftrightarrow x$ и y принадлежат одному подмножеству разбиения.

Утверждение 3

Всякое отношение эквивалентности определяет разбиение множества X на классы эквивалентности относительно этого отношения.

Т.о., два последних утверждения позволяют отождествлять отношения эквивалентности и разбиения: любая эквивалентность определяет единственное разбиение и наоборот.

Определение 21

Множество всех классов эквивалентности по данному отношению эквивалентности Q на множестве X называется **фактор-множеством** множества X по отношению Q.

Обозначение: X/Q.

Систему представителей всех классов эквивалентности называют *трансверсалом* множества X по отношению Q. Трансверсал множества по отношению эквивалентности в общем случае определен неоднозначно.

Рассмотрим еще один тип специальных бинарных отношений - отношение порядка.
Интуитивное понятие отношения порядка - предшествование, предпочтение, превосходство, например:

1. Очередь в кассу.
2. Шеренга студентов, выстроенных по росту.
3. Список учебной группы в алфавитном порядке.

Опишем эти отношения, путем перечисления свойств, которыми они обладают.

Определение 22

Отношением частичного порядка на множестве X, называется бинарное отношение Q, обладающее свойствами: рефлексивности, антисимметричности и транзитивности.

Обозначение: символ $\preceq$.

Свойства отношения нестрогого порядка:

1. *рефлексивность*: $x \preceq x$ - истинно;
2. *антисимметричность*: $x \preceq y$ и $y \preceq x \Rightarrow x = y, \quad x, y \in X$;
3. *транзитивность*: $x \preceq y$ и $y \preceq z \Rightarrow x \preceq z$.

Пример 13 ●

1). На множестве действительных чисел R отношение Q: «не больше», «не меньше» ; «a является делителем $в$».
2). Во множестве подмножеств некоторого универсального множества / отношение $A \subseteq B$;
3). Отношение «не выше» на множестве студентов;
4). Схема организации подчинения в учреждении есть отношение частичного порядка на множестве должностей.

Определение 23

Отношение частичного порядка на множестве X, для которого любые два элемента сравнимы, т.е. $\forall x, y \in X$: $x \preceq y$ или $y \preceq x$, называется **отношением линейного порядка**.

Например, в примере 12 отношение 10.1 - отношение линейного порядка; отношение 10.4 таковым не является, так как не любые два служащих учреждения находятся один в подчинении другого

Пусть на множестве X задано отношение частичного порядка. Как можно его задать на множестве $X \times X$?

Один из возможных способов: определим отношение Π условием

$$x,y,z,h \in X: (x,y)\Pi(z,h) \Leftrightarrow x \preceq z \text{ и } y \preceq h.$$

Отношение Π есть отношение частичного порядка, оно называется *отношением Парето*.

Определение 24

Отношением строгого порядка на множестве X, называют отношение Q, обладающее следующими тремя свойствами: антирефлексивности, антисимметричности и транзитивности.

Обозначение: символ $\prec$.

Свойства отношения строгого порядка:

1. $x \prec x$ - ложно, *антирефлексивность*;
2. из $x \prec y \Rightarrow y \prec x$ - не верно, *антисимметричность*,
3. из $x \prec y$ и $y \prec z \Rightarrow x \prec z$ - *транзитивность*.

Итак, $x \prec y$ если $x \preceq y$ и $x \neq y$.

Пример 14

1). На множестве действительных чисел R отношение Q: «больше», «меньше» ;
2). Отношение Q: «старше по званию» на множестве офицеров.

Оба отношения частичного и строгого порядка называют отношением порядка.

Элементы комбинаторики

Предмет и задачи комбинаторики.

Определение

Комбинаторика - раздел математики, посвященный решению задач выбора и расположения элементов некоторого, обычно конечного, множества в соответствии с заданными правилами.

Каждое такое правило определяет способ построения некоторой конструкции из элементов исходного множества, называемой **комбинаторной конфигурацией.**

Поэтому можно сказать, что целью комбинаторного анализа является изучение комбинаторных конфигураций.

Это изучение включает в себя:

- вопросы существования комбинаторных конфигураций,
- алгоритмы их построения,
- оптимизацию таких алгоритмов,
- решение задач пересчета и перечисления.

Простейшими примерами комбинаторных конфигураций являются перестановки, сочетания и размещения (с которыми мы познакомимся в теории вероятностей.)

Комбинаторные задачи:

– если нас интересует, сколько элементов, принадлежащих данному конечному множеству, обладает некоторым свойством или заданным набором свойств, то это **задача пересчета**;

- если необходимо выделить все элементы множества, удовлетворяющие заданным свойствам, то это задача **перечисления**;
- если на исходном конечном множестве элементов определена некоторая целевая функция, причем нас интересуют элементы множества, доставляющие минимальное (или максимальное) значение этой функции, то имеем **задачу оптимизации**.

Перечисленные задачи тесно связаны друг с другом.

Комбинаторика в настоящее время находит широкое применение в алгебре многочленов, теории группы, теории вероятностей, теории графов, в электронике, в быту (замки, сейфы, телефонная сеть и т.п.).

По мере развития комбинаторики выяснилось, что несмотря на внешнее различие изучаемых ею вопросов, многие из них имеют одно и то же математическое содержание.

При подсчете числа комбинаторных конфигураций используют правила суммы и произведения.

Правило суммы

Пусть X - конечное множество, состоящее из m элементов. Тогда говорят, что объект x из X может быть выбран m способами, и пишут: $|X| = m$.

Правило суммы.

Пусть $X_1, \dots, X_\kappa$ - конечные попарно непересекающиеся множества, т.е. $X_i \cap X_j = 0$ при $i \neq j$.

Тогда, очевидно выполняется равенство: $\left| \bigcup_{i=1}^{\kappa} X_i \right| = \sum_{i=1}^{\kappa} |X_i|$.

Замечание.

Для κ=2 оно формулируется следующим образом. Пусть $|X| = m$, $|Y| = n$.

Если объект x может быть выбран m способами, а объект y - другими n способами, то выбор «либо x, либо y» может быть осуществлен $m+n$ способами.

Правило произведения

Для двух множеств X и Y формулируется так: если объект x может быть выбран m способами и после каждого из таких выборов объект y в свою очередь может быть выбран n способами, то выбор упорядоченной пары (x, y) может быть осуществлен $m \cdot n$ способами.

Правило произведения.

Если объект x_1 может быть выбран m_1 способами, после чего объект x_2 может быть выбран m_2 способами и для любого $i,\ 2 \le i \le k-1$ после выбора объектов $x_1, \dots, x_i$ объект x_{i+1} может быть выбран m_{i+1} способами, то выбор упорядоченной последовательности из k объектов $(x_1, x_2, \dots, x_k)$ может быть осуществлен $m_1 \cdot m_2 \cdot \dots \cdot m_\kappa$ способами.

Иными словами,

$$|X_1 \times X_2 \times \dots \times X_n| = |X_1| \cdot |X_2| \cdot \dots \cdot |X_n|.$$

Вопрос 10. Размещения и перестановки

Определение

Пусть задано множество $X=\{x_1, \ldots, x_n\}$. Набор элементов: $x_{i_1}, \ldots, x_{i_r}$ называется **выборкой** объема r из n элементов или иначе **(n, r)-выборкой**.

(Понятие выборки не следует смешивать с понятием подмножества, один и тот же элемент из множества X может в ней встречаться на различных местах). Если речь идет о подмножествах, то здесь все элементы попарно различны и никакого определенного порядка в расположении им не приписывается.

Определение

Выборка называется **упорядоченной**, если порядок следования элементов в ней задан.

Две упорядоченные выборки, различающиеся лишь порядком следования элементов, считаются различными.

Определение

Если порядок следования элементов в выборке не является существенным, то такая выборка называется **неупорядоченной**.

В выборках могут допускаться или не допускаться повторения элементов.

Определение

Упорядоченная (n, r) выборка в которой элементы могут повторяться, называется **(n, r)-размещением с повторениями**.

Если элементы упорядоченной (n, r) выборки попарно различны, то она называется **(n, r)-размещением без повторений** или просто **(n, r)-размещением**.

Обозначение: число размещений (n, r) с повторениями обозначаем через $\overline{A}_n^r$, а без повторений A_n^r.

Пример 1.

$X=\{1, 2, 3\}$. Составьте размещения из 3-х элементов по 2 и найдите их число:

1). (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3) - размещения с повторениями;

2). число таких размещений $\overline{A}_3^2 = 9$;

3). (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2) - размещения без повторений;

4). число размещений без повторений равно $A_3^2=6$.

Вывод:

Размещения отличаются друг от друга либо порядком элементов, либо самими элементами, либо и тем, и другим.

Так как размещения с повторениями из трех элементов по два образованы из множества *X*, то множество таких размещений есть декартов квадрат $X^2 = X \times X$.

Пример 2.

D={5, 8}. Составьте размещение с повторениями из двух элементов по четыре и подсчитайте их число.

Решение: $D^4 = D \times D \times D \times D$.

Искомые размещения имеют вид: (5, 5, 5, 5), (5, 5, 5, 8), (5, 5, 8, 5), (5, 8, 5, 5), (8, 5, 5, 5), (5, 5, 8, 8), (5, 8, 5, 8), (8, 8, 5, 5), (8, 5, 8, 5), (5, 8, 8, 5), (5, 8, 8, 8), (8, 8, 8, 5), (8, 5, 8, 8), (8, 8, 5, 8), (8, 5, 5, 8), (8, 8, 8, 8).

Число таких размещений: $\overline{A}_2^4 = 16$.

Вывод:

Размещения с повторениями можно рассматривать как в случае $n>r$ (пример 1), так и в случае $n \leq r$ (пример 2).

Теорема 1

*Число различных размещений с повторениями из **n** элементов по **r** определяется по формуле*

$$\overline{A}_n^r = n^r.$$

Док-во

Действительно, каждое (***n, r***) размещение с повторениями является упорядоченной последовательностью длины *r*, причем каждый член этой последовательности может быть выбран любым из ***n*** способов, откуда по обобщенному правилу произведения и получаем требуемую формулу: $\overline{A}_n^r = \underbrace{n \cdot n \cdot \ldots \cdot n}_{r} = n^r$.

Пример 3.

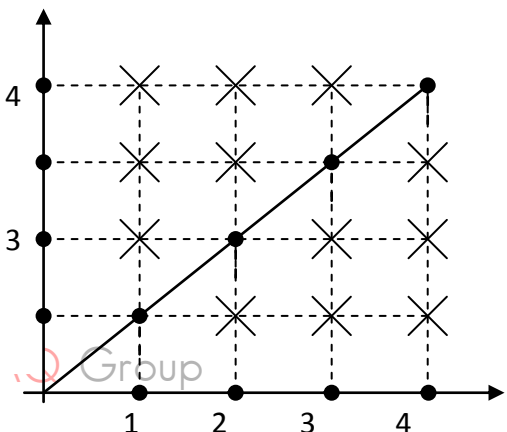
Сколько различных трехзначных чисел можно составить из двух (отличных от нуля) цифр?
Решение: $\overline{A}_2^3 = 2^3 = 8$.

В ряде случаев из множества всех *r* выборок необходимо выделить подмножество таких упорядоченных *r*-выборок, в которых все элементы *попарно различны*. Такие выборки называются **размещениями без повторений**.

Пример 4.

В финале за выход в высшую лигу боролись 4 футбольные команды. Сколько было сыграно матчей, если команды встречались друг с другом дважды.
Решение: *x*={1, 2, 3, 4} (это номера команд).

Образуем пары: (1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (3, 4), (4, 1), (4, 2), (4, 3), (4, 4).



Команда не может играть сама с собой, поэтому из X^2 исключим пары, у которых первый и второй элементы совпадают.

Итак получаем, что число матчей, сыгранных командами равно 12.

Теорема 2

*Число различных размещений без повторений из **n** элементов по **r** вычисляется по формуле*

$$A_n^r = \frac{n!}{(n-r)!} \quad \text{при } n \le r,$$

$$A_n^r = 0 \text{ при } n > r.$$

Док-во:

Пусть множество X состоит из n элементов. Рассмотрим $(a_1, a_2, \ldots, a_r)$ всевозможные r-выборки из множества X, в которых все элементы попарно различны, при этом предполагаем $r \le n$.

Тогда первый член этой последовательности может быть выбран n способами, после каждого выбора первого члена последовательности второй член может быть выбран $n-1$ способами и т.д. r-й член может быть выбран $n-(r-1)=n-r+1$ способами, отсюда по обобщенному правилу произведения получаем требуемую формулу: $A_n^r = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$.

Пример.
Сколькими способами собрание из 30 человек может выбрать председателя и секретаря.

Решение: $A_{30}^2 = 29 \cdot 30 = 870$ (способов).

(n-r+1) n

перестано

Определение
(n, n) размещение без повторений называется **перестановкой множества** X.

Обозначение: P_n.

Теорема 3

*Число различных перестановок без повторений из **n** элементов равно произведению всех последовательных натуральных чисел, начиная от **n** до 1 включительно:*

$$P_n = n!$$

Док-во

По определению $P_n = A_n^n = n(n-1)\cdots 1 = n!$.

Пример.

X={1, 2, 3}. Составьте перестановки без повторений множества X и найдите их число.

1). (1, 2, 3), (1, 3, 2) (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1) - перестановки без повторений; 2). число перестановок $P_3 = 3! = 1 \cdot 2 \cdot 3 = 6$.

Вывод:

Перестановки отличаются друг от друга только порядком элементов.

Пример.

Сколькими способами можно составить список различных фамилий из 5-ти человек?

$P_5 = 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$ (способов).

Вопрос 11. Сочетания.

Определение

Неупорядоченная (n, r) выборка в которой элементы могут повторяться называется **сочетанием с повторениями**.

Если элементы неупорядоченной (n, r) выборки попарно различны, то она называется **сочетанием без повторений** или просто **сочетанием**.

Обозначение: Число сочетаний с повторениями $\overline{C}_n^r$, без повторений C_n^r.

Пример.

X={1, 2, 3}. Составьте:

1). сочетания с повторениями из трех элементов по два: {a, b}, {a, c}, {c, b}, {a, a}, {b, b}, {c, c};

2). число сочетаний с повторениями равно $\overline{C}_n^r$=6;

3). сочетания без повторений из трех элементов по два : {a, b}, {a, c}, {c, b};

4). число сочетаний равно C_3^2=3 .

Замечание

Любое (n, r) сочетание можно рассматривать как r-элементное подмножество

n-элементного множества.

Вывод:

Сочетания различаются только элементами.

Теорема 4

Число сочетаний без повторений из ***n*** *элементов по* ***r*** *вычисляется по формуле*

$$C_n^r = \frac{n!}{r!\cdot(n-r)!} \text{ при } r \le n \text{ и}$$

$$C_n^r = 0 \text{ при } r > n.$$

Док-во:

Рассмотрим случай когда $r \le n$. Подсчитывая число размещений из ***n*** по ***r*** можно получить, что

$$A_n^r = C_n^r \cdot P_r \Rightarrow C_n^r = \frac{A_n^r}{P_r} = \frac{n!}{(n-r)!\cdot r!}. \; C_n^r = \frac{n!}{r!\cdot(n-r)!}$$

.

Замечание. $C_n^0 = 1$ (т.к. имеется только одно пустое подмножество)

$C_n^n = 1$ (т.к. имеется только одно подмножество, содержащее все элементы данного множества)

Теорема 5

Число сочетаний с повторениями из ***n*** *элементов по* ***r*** *вычисляется по формуле*

$$\overline{C}_n^r = C_{n+r-1}^r \text{ (без доказательства).}$$

Пример ●

Число решений в целых неотрицательных числах уравнения

$$X_1+X_2+\ldots+X_n = r$$

равно $\overline{C}_n^r$.

Действительно, каждое решение $\langle a_1, a_2, \ldots, a_n \rangle$ этого уравнения можно считать неупорядоченной выборкой, в которой a_1 элементов первого типа, a_2 элементов второго типа, ..., a_n n-го типа. С-но, число решений равно $\overline{C}_n^r$.

В частности, число целочисленных решений уравнения

$$x_1+x_2+x_3 = 13$$

равно $\overline{C}_3^{13} = C_{15}^{13} = 7 \cdot 15 = 105$.

ПРИМЕРЫ ПРИМЕНЕНИЯ ФОРМУЛ

Пример

Сколькими способами можно выбрать 5 номеров из 36?

$$C_{36}^{5} = \frac{36!}{5! \cdot 31!} = 376.992$$

Пример

Как велико число различных результатов бросаний двух не отличимых друг от друга кубиков?

Решение:

$$\overline{C}_6^2 = C_{6+2-1}^2 = C_7^2 = \frac{7!}{2! \cdot 5!} = \frac{6 \cdot 7}{2} = 21$$ (различный результат бросаний).

Вопрос 12. Полиномиальная формула.

- Пусть X - конечное множество, $|X|=n$.
  Множества $\{X_1, X_2, ..., X_k\}$ - разбиение X:

$$\bigcup_{i=1}^{k} X_i = X, \quad X_i \cap X_j = \varnothing \quad при \quad i \neq j, \quad |X_i| = n_i, \quad i = 1,2,...k$$

причем $n=n_1+n_2+...+n_k$.

- Число разбиений множества X вычисляется по формуле:

$$N(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! n_2! \ldots n_к!}$$

Формула:

$$\overline{P_n}(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! n_2! \ldots n_к!}$$

есть формула для вычисления числа перестановок с повторениями из n элементов, среди которых n_1 равных между собой, n_2 равных между собой, ...,

n_k равных между собой и $n_1+n_2+...+n_k=n$.

Формула:

$$C_{n_1 n_2 \cdots n_k} = \frac{n!}{n_1! n_2! \ldots n_к!}$$

есть формула для вычисления коэффициентов полинома:

$$(x_1+x_2+\ldots+x_k)^n$$

Вопрос 13. *Алгебраические операции. Понятие алгебры.*

Определение 1

Функция $f: X^n \to X$ называется n-местной алгебраической операцией на множестве X.

Операция f называется:

- при $n=1$ - **унарной**;
- при $n=2$ - **бинарной**;
- в общем случае - n-арной (n-местной).

Определение 2

Пусть на множестве X заданы несколько операций:

$f_k : X^{n_k} \to X$, где $k=1, 2,\ldots m,$

n_k - натуральное число, зависящее от k.

Множество с такой структурой называется алгеброй.

Множество X называется носителем алгебры.

Обозначение: $A = \langle X, f_1, f_2,\ldots f_m \rangle$.

Определение 3

Подмножество называется системой образующих (порождающих) или базисом алгебры A, если любой элемент из X можно получить из элементов M при помощи операций алгебры A.

Пусть $\langle X, * \rangle$ -алгебра.

Определение 4

Операция $*$ называется ассоциативной, если

$$\forall x, y, z \in X \quad (x * y) * z = x * (y * z)$$

Определение 5

Операция $*$ называется коммутативной, если

$$\forall x, y \in X \quad x * y = y * x$$

Определение 6

Элемент e называется нейтральным по отношению к операции $*$, если

$$\forall x \in X \quad x * e = e * x = x$$

Теорема

Если нейтральный элемент существует, то он единственный.

Определение 7

Пусть $<X,*>$ - алгебра, причем существует нейтральный элемент e.

Элемент y называется обратным к элементу x, а x - обратным к y, если

$$x*y=y*x=e$$

Определение 8

Для обозначения ассоциативной операции существует два вида записи:

1) аддитивная запись: $x*x*...*x=x+x+...+x=nx$
здесь *нейтральный элемент* называют нулем и обозначают 0,

обратный элемент к x - противоположным и обозначают $-x$, то есть

$x+0=x$, $x+(-x)=0$;

2) мультипликативная запись: $x*x*...*x=x\cdot x\cdot ...\cdot x=x^n$

здесь *нейтральный* элемент называют единицей и обозначают *1*, *обратный элемент* к x обозначают

x^{-1}, то есть $x\cdot 1=x$, $x\cdot x^{-1}=1$.

Определение 9

Пусть $<X,*>$ $<Y,\circ>$ - две алгебры с одинаковым числом алгебраических операций.

Отображение $f: X\to Y$ называется изоморфизмом алгебр, если оно биективно, все операции первой алгебры поставлены в биективное соответствие всем операциям второй алгебры и при этом для соответствующих операций выполняется:

$$f(x*y)=f(x)\circ f(y)$$

где $x,y\in X$; $f(x),f(y)\in Y$.

Вопрос 14. *Группы.*

Определение 10

Множество с заданной на нем одной ассоциативной бинарной операцией называется полугруппой.

Определение 11

Полугруппа с нейтральным элементом (с единицей) называется моноидом или полугруппой с единицей.

Определение 12

Если заданная бинарная операция еще и коммутативна, то полугруппа или моноид называется коммутативной (абелевой).

Определение 13

Алгебра $A=<X,*>$ называется группой, если она моноид, в котором каждый элемент обратим.

Определение 14

Если алгебра $A=<X,*>$ - группа, $Y \subseteq X$

и алгебра $B=<Y,*>$ - группа с той же операцией, что и в A, то она называется подгруппой группы A.

Определение 15

Группа называется циклической, если она имеет единственный образующий элемент x_0, то есть

$$\forall x \in X \quad \exists k \in Z \quad x = x_0^k$$

Пусть $U \neq$ пустому множеству.

Определение 16

Алгебра всех биекций вида $f: U \to U$ с операцией произведения (суперпозиции) биекций называется группой подстановок или перестановок.

Определение 17

Группа подстановок конечного множества U

с числом элементов n называется симметрической группой степени n.

Обозначение: S_n.

Теорема

(*о представлении групп*):

Всякая группа изоморфна подгруппе некоторой группы подстановок.

Вопрос 15. *Понятие кольца. Кольцо целых чисел.*

Определение 1

Кольцом называется алгебра $A=<X,+,\cdot>$

с двумя ассоциативными бинарными операциями - сложением (+) и умножением (·), которая удовлетворяет аксиомам:

1. $<X,+>$ - коммутативная группа (по сложению);

2. $< X, \cdot >$ - полугруппа (по умножению);

3. $\forall x, y, z \in X$ имеет место дистрибутивность

$(x+y)\cdot z = x\cdot z + y\cdot z$

$z\cdot(x+y) = z\cdot x + z\cdot y$

Если при этом существует нейтральный элемент для умножения, то кольцо называется кольцом с единицей.

Если операция умножения коммутативна, то кольцо называется коммутативным.

Кольцо целых чисел

Рассмотрим алгебру $A =< Z, +, \cdot >$.

(1) Алгебра $A =< Z, + >$ - коммутативная группа (по сложению).

(2) Алгебра $A =< Z, \cdot >$ - полугруппа (по умножению).

(3) $\forall x, y, z \in X$ Имеет место дистрибутивность:

$(x+y)\cdot z = x\cdot z + y\cdot z$

$z\cdot(x+y) = z\cdot x + z\cdot y$

ДЕЛИМОСТЬ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Пусть ***a, b, c*** **– целые числа**.

Число $a \neq 0$ делит число b или a является делителем b, если существует такое целое число c, что $b = a\cdot c$.

Обозначение: $a \mid b$ или $b \ \vdots \ a$.

Теорема 1 (свойство евклидовости)

$\forall a, \forall b \neq 0$

существуют единственные целые частное q и остаток r такие, что

$a = b\cdot q + r, \quad 0 \le r < |b|$.

Пусть $a \neq 0, \quad b \neq 0$

Определение 2

Целое число $d > 0$ называется наибольшим общим делителем чисел a и b при выполнении следующих условий:

1) $d \mid a, \ d \mid b$;
2) если $c \mid a$ и $c \mid b$, то $c \mid d$.

Обозначение: (a,b) или НОД(a,b).

Теорема 2

Если целые числа $a\neq0$ и $b\neq0$, то существуют целые числа x и y такие, что

НОД$(a,b)= ax + by$

Линейные уравнения от двух переменных

$ax + by=c$

называются линейными диофантовыми уравнениями

РАЗЛОЖИМОСТЬ ЦЕЛЫХ ЧИСЕЛ НА МНОЖИТЕЛИ

Теорема (о существовании неприводимого разложения)

Любое целое число $a \notin \{-1, 0, 1\}$ может быть записано как $\pm$ произведение конечного числа положительных неразложимых целых чисел:

$a = \pm u_1 \cdot u_2 \cdot \ldots \cdot u_r,$

где $u_i>1$ - неразложимые числа, i=1, 2,…,r

Теорема (о единственности неприводимого разложения)

Любое целое число $a \notin \{-1, 0, 1\}$ может быть записано как $\pm$ произведение простых чисел с точностью до порядка сомножителей:

$$a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

где $p_1< p_2<\ldots< p_k$ - различные простые числа, $\alpha_i \in N$, $i=1, 2,\ldots k.$

Вопрос 16. *Кольцо вычетов по модулю n. Малая теорема Ферма*

Z_n={[0], [1],…,[n-1]} - множество вычетов по модулю n.

Введем на Z_n операции:

- Сложение [a]+[b]=[a+b];
- Умножение [a]·[b]=[a·b];
- Обратный (противоположный) элемент по операции сложения -[a]=[n-a].
- $< Z_n; + >$ - коммутативная группа (по сложению),
- $< Z_n; \cdot >$ - коммутативная полугруппа с единицей (по умножению).

Вывод:

алгебра $< Z_n; +, \cdot >$ - коммутативное кольцо с единицей.

Кольцо $< Z_n; +, \cdot >$ называется кольцом вычетов по модулю n.

Арифметика целых чисел по модулю n может рассматриваться как арифметика остатков или модулярная арифметика.

Теорема Ферма

Если p - простое число и a - произвольное целое число, не делящееся на p, то

$a^{p-1} \equiv 1 \pmod{p}$.

Более удобная формулировка:

если p - простое число, то для произвольного целого a выполняется сравнение:

$a^{p} \equiv a \pmod{p}$.

Следствие

Если n - простое, то в кольце Z_n выполняется равенство:

$a^{-1} = a^{n-2}$.

Вопрос 17 *Понятие поля. Конечные поля.*

Определение 3

Коммутативное кольцо с единицей, в котором для каждого ненулевого элемента существует обратный относительно операции умножения, называется полем.

Конечные поля называются полями Галуа.

Теорема 4

Элемент a кольца Z_n имеет обратный a^{-1} <=> если НОД$(a,n)=1$.

Теорема 5

Кольцо вычетов $\langle Z_n; +, \cdot \rangle$ является полем <=> когда n – простое число.

Вопрос 18. *Понятие решетки. Примеры решеток.*

Определение

Отношением частичного порядка на множестве X, называется бинарное отношение Q, обладающее свойствами: рефлексивности, антисимметричности и транзитивности.

Обозначение: символ $\preceq$.

Определение

Отношением строгого порядка на множестве X, называют отношение Q, обладающее следующими свойствами:

$$\forall x, y \in X \quad x \prec y \Leftrightarrow x \preceq y \quad и \quad x \neq y$$

Определение

Отношение частичного порядка на множестве X, для которого любые два элемента сравнимы, т.е.

$$\forall x, y \in X \quad x \preceq y \quad или \quad y \preceq x$$

называется отношением линейного порядка.

Определение

Непустое множество X с заданным на нем отношением частичного (линейного) порядка Q называется частично (линейно) упорядоченным.

Сокращенно ч.у.м. или л.у.м.

Обозначение: $\langle X, Q \rangle$.

Рассмотрим ч. у. м. $\langle X; \preceq \rangle$.

Определение

Элемент y покрывает элемент x, если

$$x \prec y \quad и \quad не \quad \exists \quad такого \quad z, что \quad x \prec z \prec y$$

Диаграммы Хассе:

- каждый элемент множества изображается точкой на плоскости;
- если y покрывает x, то точки x и y соединяют отрезком, причем x располагают ниже y.

Понятие решетки

Рассмотрим ч. у. м. $\langle X, \preceq \rangle$.

Определение 1

Интервалом $[a, b]$ для a b называется множество всех элементов

$$x \in X \quad таких, \quad что \quad a \preceq x \preceq b.$$

Определение 2

Ч. у. м. называется локально конечным, если любой его интервал является конечным множеством.

Пусть $\langle X; \preceq \rangle$ - ч. у. м.

Определение 3

Элемент $x_m \in X$ называется максимальным (минимальным), если

$$\forall x \in X \quad x_m \preceq x \quad (x \preceq x_m) \Rightarrow \quad x_m = x$$

Определение 4

Элемент $x^* \in X$ называется наибольшим, если

$\forall x \in X \quad x \preceq x^*$

Обозначение: 1 (единица)

Определение 5

Элемент $x^* \in X$ называется наименьшим, если

$\forall x \in X \quad x_* \preceq x$

Обозначение: 0 (нуль)

Теорема

Если наибольший (наименьший) элемент существует, то он единственный.

Определение 6

Элемент $a \in X$ называется верхней (нижней) гранью элементов x и y, если

$$x \preceq a \quad и \quad y \preceq a \quad (a \preceq x \quad и \quad a \preceq y)$$

Определение 7

Элемент a^* называется точной верхней гранью или супремумом элементов x и y, если

$$\forall t \quad x \preceq t \quad и \quad y \preceq t \quad \Rightarrow \quad a^* \preceq t$$

Обозначение: $a^* = sup\{x, y\}$.

Определение 8

Элемент a^* называется точной нижней гранью или инфимумом элементов x и y, если

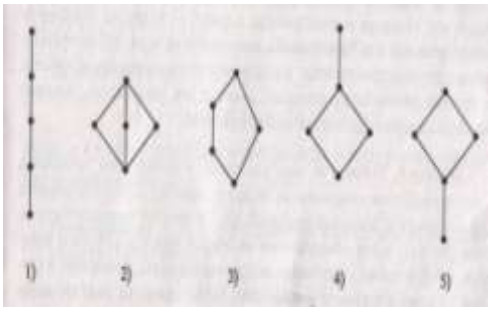
$$\forall t \quad t \preceq x \quad и \quad t \preceq y \quad \Rightarrow \quad t \preceq a_*$$

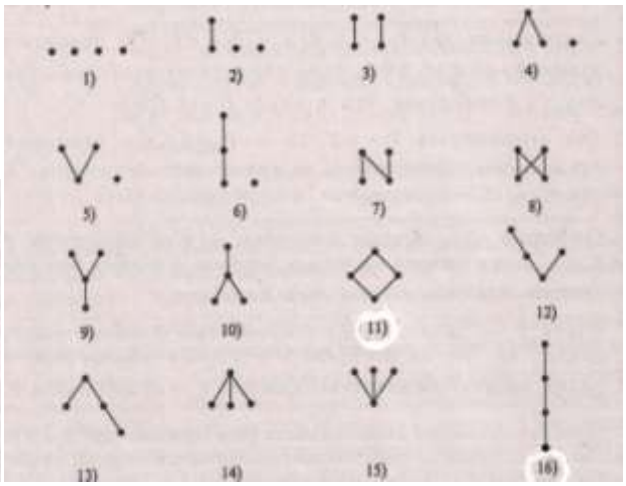
Обозначение: $a_* = inf\{x, y\}$.

Определение 9

Решеткой называется ч.у.м. $\langle X; \preceq \rangle$, в котором каждая пара элементов x и y имеет супремум и инфимум.

Примеры:





Вопрос 19. *Решетки и алгебры.*

Пусть $\langle X; \preceq \rangle$ - решетка.

Для заданных элементов x и $y \in X$ обозначим

элемент $inf\{x,y\} = x \wedge y$

и назовем решетчатым пересечением (конъюнкцией) x и y;

обозначим элемент $sup\{x,y\} = x \vee y$

и назовем решетчатым объединением (дизъюнкцией) x и y.

Решетку $\langle X; \preceq \rangle$ можно рассматривать как алгебру $A = \langle X; \wedge, \vee \rangle$ с двумя бинарными операциями.

Определение 10

Подмножество элементов решетки, замкнутое относительно операций $\wedge u \vee$, то есть содержащее с каждыми двумя элементами их точную верхнюю и нижнюю грани, называется подрешеткой.

Вопрос 20. *Понятие нечеткого подмножества. Функция принадлежности*

Пусть E - некоторое множество.

Определение 1

Нечетким подмножеством A множества E называется множество упорядоченных пар

$$\{x \mid \mu_{\bar{A}}(x)\} \quad \forall x \in E$$

где $\mu_{\bar{A}}(x)$ - степень принадлежности x к A.

Обозначение: $\bar{A}$

Определение 2

Множество E называется базовым (универсальным);

Функция $\mu_{\bar{A}}(x)$ называется функцией принадлежности нечеткого подмножества $\bar{A}$;

Значение функции $\mu_{\bar{A}}(x)$ для каждого конкретного $x \in E$, называется степенью принадлежности элемента x к нечеткому подмножеству $\bar{A}$.

Определение 3

Носителем нечеткого подмножества $\bar{A}$ называется подмножество универсального множества E, для элементов которого функция принадлежности строго больше нуля:

$$S_A = \{x : x \in E, \ \mu_{\bar{A}}(x) > 0\}$$

Обозначение: S_A или *supp A*.

Вопрос 21. *Операции над нечеткими подмножествами.*

- Включение
- Равенство
- Дополнение
- Пересечение
- Объединение

Вопрос 22. *Расстояние Хемминга.*

Обобщенное (линейное) расстояние Хемминга:

$$d(\bar{A}, \bar{B}) = \sum_{i=1}^{n} | \mu_{\bar{A}}(x_i) - \mu_{\bar{B}}(x_i) |$$

Евклидово (квадратичное) расстояние:

$$e(\bar{A}, \bar{B}) = \sqrt{\sum_{i=1}^{n} (\mu_{\bar{A}}(x_i) - \mu_{\bar{B}}(x_i))^2}$$

Элементы математической логики и теории алгоритмов

Определение
Коротко говоря - **математическая логика** - это наука о средствах и методах математических доказательств.

Современную мат. логику определяют как раздел математики, посвященный изучению математических доказательств и вопросов оснований математики.

Вопрос 23. Понятие высказывания. Логические операции над высказываниями.

- Основным (неопределяемым) понятием математической логики является понятие «простого высказывания».

Под ***высказыванием*** обычно понимают всякое повествовательное предложение, утверждающее чего-либо о чем-либо, и при этом мы можем сказать, истинно оно или ложно в данных условиях места и времени. Логическими значениями высказываний являются «истина» и «ложь» (коротко «и», «л» или «1», «0»).

Примеры высказываний:

1) Новгород стоит на Волхове;
2) Париж - столица Англии;
3) Карась не рыба;
4) Число 6 делится на 2 и на 3;
5) Если юноша окончил среднюю школу, то он получает аттестат зрелости.

Высказывания 1), 4), 5) истины, а высказывания 2) и 3) ложны.

Очевидно, предложение «Да здравствуют наши спортсмены!» («Да здравствует 1 Мая!», «Пейте томатный сок!») не являются высказыванием.

Высказывание, представляющее собой одно утверждение, принято называть **простым** или **элементарным**. Примерами элементарных высказываний могут служить высказывания 1) и 2).

Высказывание, которые получаются из элементарных с помощью грамматических связок: «не», «и», «или», «если …, то …», «тогда и только тогда» принято называть **сложными** или **составными**.

Так высказывание 3) получается из простого высказывания «Карась - рыба» с помощью отрицания «не», высказывание 4) образовано из элементарных высказываний «Число 6 делится на 2», «Число 6 делится на 3», соединенных союзом «и». Высказывание 5) получается из простых высказываний «Юноша окончил среднюю школу», «Юноша получает аттестат зрелости» с помощью грамматической связки «если …, то …». Аналогично сложные высказывания могут быть получены из простых высказываний с помощью грамматических связок «или», «тогда и только тогда».

В алгебре логики все высказывания рассматриваются только с точки зрения их логического значения, а от их житейского содержания отвлекаются. Считается, что каждое высказывание либо истинно, либо ложно и ни одно высказывание не может быть одновременно истинным и ложным.

Обозначение: элементарные высказывания обозначать малыми буквами латинского алфавита: x, y, z, …, a, b, c, …; истинное значение высказывания - буквой «И» или цифрой «1», а ложное - буквой «Л» или цифрой «0».

Если высказывание **a** истинно, то будем писать **a=1**, а если **a** ложно, то **a=0**.

Алгебра высказываний изучает способы построения высказываний из уже имеющихся.

Отрицание

Определение
Отрицанием высказывания x называется новое высказывание, которое является истинным, если высказывание x ложно, и ложным, если высказывание x истинно.

Обозначение: $\bar{x}$ (читается «**не** x» или «неверно, что x»).

Логические значения высказывания $\bar{x}$ можно описать с помощью таблицы.

x	$\bar{x}$
1	0
0	1

- Таблицы такого вида принято называть *таблицами истинности*.

Высказывание $\bar{\bar{x}}$ - двойное отрицанием высказывания x. Ясно, что логическое значение высказывания $\bar{\bar{x}}$ и x совпадают.

● Например, для высказывания «Река Волхов вытекает из озера Ильмень» отрицанием будет высказывание «Неверно, что река Волхов вытекает из озера Ильмень» или «Река Волхов **не** вытекает из озера Ильмень», а двойным отрицанием будет высказывание «**Неверно**, что река Волхов **не** вытекает из озера Ильмень».

Конъюнкция (логическое умножение)

Определение
Конъюнкцией двух высказываний x, y называется новое высказывание, которое считается истинным, если оба высказывания x, y истинны, и ложным, если хотя бы одно из них ложно.

Обозначение: x & y или $x \wedge y$ (читается «x **и** y»).

Высказывания x, y называются членами конъюнкции. Логические значения конъюнкции описываются следующей таблицей истинности:

x	y	x & y
1	1	1
1	0	0
0	1	0
0	0	0

Например, для высказываний «6 делится на 2», «6 делится на 3» их конъюнкцией будет высказывание «6 делится на 2 **и** 6 делится на 3», которое очевидно, истинно.

Из определения операции конъюнкции видно, что союз «и» в алгебре логики употребляется в том же смысле, что и в повседневной речи. Но в обычной речи не принято соединять союзом «и» два высказывания далеких друг от друга по содержанию, а в алгебре логики рассматривается конъюнкция двух любых высказываний.

Из определения операции конъюнкции и отрицания ясно, что высказывание $x \& \bar{x}$ всегда ложно.

Дизъюнкция (логическое сложение)

Определение

Дизъюнкцией двух высказываний x, y называется новое высказывание, которое считается истинным, если хотя бы одно из высказываний x, y истинно, и ложным, если они оба ложны.

Обозначение: $x \vee y$ (читается «*x* **или** *y*»).

Высказывания x, y называются членами дизъюнкции. Логические значения дизъюнкции описываются следующей таблицей истинности:

x	y	$x \vee y$
1	1	1
1	0	1
0	1	1
0	0	0

Например, высказывание «В треугольнике DFE угол D или угол E острый» истинно, т. к. обязательно истинно хотя бы одно из высказываний: «В треугольнике DFE угол D острый», «В треугольнике DFE угол E острый».

В повседневной речи союз «или» употребляется в различном смысле: исключающем и не исключающем. В алгебре логики союз «или» всегда употребляется в не исключающем смысле.
Из определения операции дизъюнкции и отрицания ясно, что высказывание $x \vee \bar{x}$ всегда истинно.

Импликация

Определение

Импликацией двух высказываний x, y называется новое высказывание, которое считается ложным, если x истинно, а y - ложно, и истинным во всех остальных случаях.

Обозначение: $x \to y$ (читается «если *x*, то *y*» или «из *x* следует *y*»).

Высказывание x называют *условием* или *посылкой*, высказывание y - *следствием* или *заключением*.

Логические значения операции импликации описываются следующей таблицей истинности:

x	y	$x \to y$
1	1	1
1	0	0
0	1	1
0	0	1

● Например, высказывание «Если число 12 делится на 6, то оно делится на 3», очевидно, истинно, т.к. здесь истинна посылка «Число 12 делится на 6» и истинно заключение «Число 12 делится на 3».

Употребление слов «если …, то …» в алгебре логики отличается от употребления их в обычной речи, где мы, как правило, считаем, что если высказывание x ложно, то высказывание «если x, то y » вообще не имеет смысла. Кроме того, строя предложение вида «Если x, то y » в обычной речи, мы всегда подразумеваем, что предложение y вытекает из предложения x. Употребление слов «если …, то …» в математической логике не требует этого, поскольку в ней смысл высказываний не рассматривается.

Импликация играет важную роль в математических доказательствах, т.к. многие теоремы формулируются в условной форме «Если x, то y ». Если при этом известно, что x истинно и доказана истинность импликации $x \to y$, то мы вправе сделать вывод об истинности заключения y.

Эквиваленция

Определение

Эквиваленцией (или **эквивалентностью**) двух высказываний x, y называется новое высказывание, которое считается истинным, когда оба высказывания x, y либо одновременно истинны, либо одновременно ложны, и ложными во всех остальных случаях.

Обозначение: $x \leftrightarrow y$ (читается «для того чтобы x, необходимо и достаточно, чтобы y» или «x тогда и только тогда, когда y»). Высказывания x, y называют членами эквиваленции.

Логические значения операции описываются следующей таблицей истинности:

x	y	$x \leftrightarrow y$
1	1	1
1	0	0
0	1	0
0	0	1

● Например, эквиваленция «Треугольник SPQ с вершиной S и основанием PQ равнобедренный тогда и только тогда, когда $\angle P = \angle Q$» является истинной, т.к. высказывание «Треугольник SPQ с вершиной S и основанием PQ равнобедренный» и «В треугольнике SPQ с вершиной S и основанием PQ $\angle P = \angle Q$» либо одновременно истинны, либо одновременно ложны.

Эквивалентность играет важную роль в математических доказательствах. Известно, что значительное число теорем формулируется в форме необходимых и достаточных условий, т.е. в форме эквивалентности. В этом случае, зная об истинности или ложности одного из двух членов эквивалентности и доказав истинность самой эквивалентности, мы заключаем об истинности или ложности второго члена эквивалентности.

Вопрос 24. Формулы логики высказываний

С помощью логических операций над высказываниями из заданной совокупности высказываний можно строить различные сложные высказывания. При этом порядок выполнения операций указывается скобками.

● Например, из трех высказываний x, y, z можно построить высказывания: $(x \,\&\, y) \vee \bar{z}$ и $x \to \overline{(y \vee (x \,\&\, z))}$.

Первое из них есть дизъюнкция конъюнкции x, y и отрицания высказывания z, а второе высказывание есть импликация, посылкой которой является высказывание x, а заключением - отрицание дизъюнкции высказывания y и конъюнкции высказываний x, z.

Определение

Всякое сложное высказывание, которое может быть получено из элементарных высказываний посредством применения логических операций отрицания, конъюнкции, дизъюнкции, импликации и эквиваленции, называется **формулой алгебры логики**.

Обозначение: большими буквами латинского алфавита A, B, C, …

Для упрощения записей формул примем следующее соглашение об опускании скобок: опускать внешние скобки, а также все скобки, которые становятся необязательными, если считать, что логические операции выполняются в таком порядке: отрицание , конъюнкция ^, дизъюнкция ∨, импликация =>, эквиваленция <=>.

Определение

Две формулы алгебры логики A и B называются **равносильными**, если они принимают одинаковые логические значения на любом наборе значений входящих в формулы элементарных высказываний.

Обозначение: $A \equiv B$.

Определение

Формула A называется **тождественно истинной (или тавтологией/**если она принимает значение 1 при всех значениях входящих в нее переменных.

Например, тождественно истинна формула

1) $x \vee \bar{x}$

x	$\bar{x}$	$x \vee \bar{x}$
1	0	1
0	1	1

2) $x \to (y \to x)$

x	y	$y \to x$	$x \to (y \to x)$
1	1	1	1
1	0	1	1
0	1	0	1
0	0	1	1

Определение

Формула A называется **тождественно ложной** если она принимает значение 0 при всех значениях входящих в нее переменных.

Например, тождественно ложна формула $x \& \bar{x}$.

Важнейшие равносильности алгебры логики можно разбить на три группы:

I. Основные равносильности:

1. $x \& x \equiv x$
2. $x \vee x \equiv x$

} законы идемпотентности

3. $x \& u \equiv x$
4. $x \vee u \equiv u$
5. $x \& л \equiv л$
6. $x \vee л \equiv x$
7. $x \& \bar{x} \equiv л$ - закон противоречия
8. $x \vee \bar{x} \equiv u$ - закон исключенного третьего
9. $= x \equiv x$ - закон снятия двойного отрицания
10. $x \& (y \vee x) \equiv x$
11. $x \vee (y \& x) \equiv x$

} законы поглощения

II. Равносильности, выражающие одни логические операции через другие:

1. $x \leftrightarrow y \equiv (x \to y)\,\&\,(y \to x)$
2. $x \to y \equiv \bar{x} \vee y$
3. $\overline{x \,\&\, y} \equiv \bar{x} \vee \bar{y}$
4. $\overline{x \vee y} \equiv \bar{x} \,\&\, \bar{y}$

} Законы де Моргана

5. $\overline{\bar{x} \,\&\, \bar{y}} \equiv x \vee y$
6. $\overline{\bar{x} \vee \bar{y}} \equiv x \,\&\, y$

Из равносильностей этой группы следует, что всякую формулу алгебры логики можно заменить равносильной ей формулой, содержащей только две логические операции: конъюнкцию и отрицание или дизъюнкцию и отрицание. Дальнейшее исключение логических операций невозможно.

Однако существует операция, и через нее может быть выражена любая пяти логических операций, которыми мы пользуемся. Такой операцией, является, например, операция «штрих Шеффера». Эта операция обозначается символом $x \mid y$ и определяется следующей таблицей истинности:

x	y	$x \mid y$
1	1	0
1	0	1
0	1	1
0	0	1

читают «x не совместно с y»

Очевидно, что имеют место равносильности:

$$\bar{x} \equiv x \mid x$$

$$x \,\&\, y \equiv (x \mid y) \mid (x \mid y)$$

Из этих двух равносильностей следует, что всякая формула алгебры логики может быть заменена равносильной формулой, содержащей только операцию «штрих Шеффера». Отметим, что $x \mid y \equiv \overline{x \,\&\, y}$.

III. Равносильности выражающие основные законы алгебры логики:

1. $x \,\&\, y \equiv y \,\&\, x$. -коммутативность конъюнкции;
2. $x \vee y \equiv y \vee x$. - коммутативность дизъюнкции;
3. $x \,\&\, (y \,\&\, z) \equiv (x \,\&\, y) \,\&\, z$. - ассоциативность конъюнкции;
4. $x \vee (y \vee z) \equiv (x \vee y) \vee z$. - ассоциативность дизъюнкции;
5. $x \,\&\, (y \vee z) \equiv (x \,\&\, y) \vee (x \,\&\, z)$. - дистрибутивность конъюнкции относительно дизъюнкции;
6. $x \vee (y \,\&\, z) \equiv (x \vee y) \,\&\, (x \vee z)$. - дистрибутивность дизъюнкции относительно конъюнкции;

Последний, шестой закон, часто называют «чудо - законом». Он справедлив только в алгебре высказываний, остальные пять законов известны и в алгебре чисел.

Докажем последний закон III:

Если $x = 1$, то будут истинными формулы $x \vee (y \wedge z), x \vee y, x \vee z$. Но тогда будет истинной и конъюнкция $(x \vee y) \wedge (x \vee y)$.

Таким образом, при $x = 1$ обе части равносильности принимают одинаковые логические значения (истинные).

Самостоятельно доказать для случая x=0:

Пусть теперь *x=0*. Тогда $x \vee (y \wedge z) \equiv (y \wedge z), x \vee y \equiv y$, и $x \vee z \equiv z$, а потому и конъюнкция $(x \vee y) \wedge (x \vee z) \equiv y \wedge z$.

Следовательно, здесь обе части равносильности равносильные одной и той же формуле $y \wedge z$, и поэтому принимают одинаковые логические знания.

Выводы:

- Используя равносильности I, II, III групп можно часть формулы или формулу заменить равносильной ей формулой. Такие преобразования формул называются равносильными.
- Равносильные преобразования используются для доказательства равносильностей, для приведения формул к заданному виду, для упрощения формул.
- Формула A считается проще равносильной ей формулы B, если она содержит меньше букв, меньше логических операций. При этом обычно операции эквивалентность и импликация заменяются операциями дизъюнкции и конъюнкции, а отрицание относят к элементарным высказываниям.

Логическое следование

Рассмотрим так называемое отношение следствия, т.е. случай, когда из одного высказывания логически следует другое.

Примерами отношений такого типа являются отношение между математической теоремой и ее следствием, отношение между условием теоремы и ее заключением.

Определение

Мы говорим, что из высказывания **p** следует высказывание **q**, если **q** истинно всякий раз, когда истинно **p**.

Таким образом, отношение следствия есть частный случай импликации.
Рассмотрим сводную таблицу истинности сложных высказываний:

	p	q	$p \leftrightarrow q$ (+)	$p \rightarrow q$ (+)	$p \vee q$ (•)	$p \wedge q$	$q \rightarrow p$ (•)
1)	1	1	1	1	1	1	1
2)	1	0	0	0	1	0	1
3)	0	1	0	1	1	0	0
4)	0	0	1	1	0	0	1

• 1) и 2)
+ 1) и 4)

В первом и втором случаях, когда p истинно, истинны также $p \vee q$ и $q \rightarrow p$. Поэтому можно сказать, что из p логически следует $p \vee q$, а также $q \rightarrow p$.

Возьмем высказывание $p \leftrightarrow q$. Мы видим, что это высказывание истинно в первом и четвертом случаях, в этих же случаях высказывание $p \rightarrow q$ истинно. Поэтому мы можем сказать, что из $p \leftrightarrow q$ следует $p \rightarrow q$.

Изучение таблицы показывает, что отношение следствия не имеет места для пар высказываний: $p \leftrightarrow q$ и $p \vee q$ и $p \vee q$.

Следует подчеркнуть тот факт, что если импликация двух высказываний есть новое высказывание, то следствие - это *отношение* между этими высказываниями. Вместе с тем отношение следствия между высказываниями *p* и *q* имеет место в том и только в том случае, когда импликация $p \rightarrow q$ тождественно истинна. Исходя из таблицы истинности импликации, мы видим, что случай *p* истинно, а *q* ложно - здесь невозможен. Таким образом, множество импликаций содержит множество высказываний о следовании. Как собственное подмножество, т.е. всякое истинное высказывание о следствии является истинной импликацией; однако не всякая импликация выражает логическое следование.

Пример:

$(2+3=7) \rightarrow (7-2=5)$. Здесь мы имеем истинную импликацию, но не имеем отношения следствия (второе высказывание из первого).

$(2+3=5) \rightarrow (5-2=3)$. Здесь мы имеем истинную импликацию и отношение следования. Во втором случае наряду с импликативной связью высказываний имеет место и смысловая (содержательная) связь. Аналогично двойная импликация $p \leftrightarrow q$ обладает отношением логической эквивалентности, если обе импликации $p \rightarrow q$ и $q \rightarrow p$ выражают отношение логического следования.

Вопрос 25. Функции алгебры логики.

Если каждой высказывательной переменной, входящей в формулу, придавать истинностное значение *И* и *Л*, то формула будет определять истинностную *логическую функцию*, т.е. функцию определенную на множестве {*И, Л*} со значениями в этом множестве. Такая функция может быть представлена таблицей истинности.

Например, формула $(x \wedge y) \to \bar{z}$ *является* ***функцией трех переменных*** $f(x,y,z)$.

Особенностью этой функции является то обстоятельство, что ее аргументы принимают одно из двух значений: ноль или единицу, и при этом функция также принимает одно из двух значений: ноль или единицу.

Определение

Функцией алгебры логики *n* переменных (или **функцией Буля**) называется функция *n* переменных, где каждая переменная принимает два значения: 0 и 1, и при этом функция может принимать только одно из двух значений: 0 или 1.

- Ясно, что тождественно истинные и тождественно ложные формулы алгебры логики представляют собой постоянные функции, а две равносильные формулы выражают одну и ту же функцию.
- Выясним, каково число функций *n* переменных. Очевидно, каждую функцию алгебры логики (как и формулу алгебры логики) можно задать с помощью таблицы истинности, которая будет содержать 2^n строк. Следовательно, каждая функция *n* переменных принимает 2^n значений, состоящих из нулей и единиц. Таким образом, функция *n* переменных полностью определяется набором значений из нулей и единиц длины 2^n. Общее же число наборов, состоящих из нулей и единиц, длины 2^n равно 2^{2^n}. Значит, число различных функций алгебры логики *n* переменных равно 2^{2^n}.
- В частности, различных функций одной переменной четыре, а различных функций двух переменных шестнадцать. Рассмотрим таблицу истинности для различных функций одной переменной. Она, очевидно, имеет вид:

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
1	1	1	0	0
0	1	0	1	0

Для n=1. 2^1=2 (строк) - длина набора; 2^{2^n} *=2^2=4 (число различных функций)*

Из этой таблицы следует, что две функции одной переменной будут постоянными: $f_1(x) \equiv 1$, $f_4(x) \equiv 0$, а $f_2(x) \equiv x$ и $f_3(x) \equiv \bar{x}$.

Вопрос 26. Дизъюнктивная нормальная форма

Функцией алгебры логики *n* переменных (или **функцией Буля**) $f : \{0,1\}^n \to \{0,1\}$ называется функция $f(x_1, x_2, \ldots x_n)$, определенная на множестве двоичных наборов длины *n*, и принимающая на каждом из них значение 0 или 1.

Так как имеется 2^n двоичных наборов длины *n*, на каждом из которых булева функция принимает одно из двух значений, число булевых функций от *n* переменных равно 2^{2^n}.

Множество булевых функций от n переменных обозначают P_2^n, а все множество булевых функций - как P_2. $P_2 = \bigcup_{n=0}^{\infty} P_2^n$.

При этом под функциями, зависящими от нулевого числа переменных, понимаются константы 0 и 1.

Множество P_2 счетно.

Способы представления булевых функций

1. Булева функция $f(x_1, x_2, \dots x_n)$ однозначно задается перечислением всех наборов, на которых она принимает значение 0, либо перечислением всех наборов, на которых она принимает значение 1.
2. *Вектором значений* булевой функции $f(x_1, x_2, \dots x_n)$ называют упорядоченный набор всех значений функции f, при котором значения упорядочены по лексикографическому порядку множества аргументов $\{0,1\}^n$ (по возрастанию двоичных чисел).
3. Булевы функции полностью определяются своими таблицами истинности. В каждой строке табл. истинности вначале задается набор значений переменных - нулей и единиц, а затем - значение функции на этом наборе.

Пример 1. *(голосование)*

Пример 2.
Пусть функция $f(x_1, x_2, \dots x_n)$ задана таблицей истинности:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Заметим, что выбрав лексикографический порядок двоичных наборов, любую функцию можно компактно задать битовой строкой ее значений. Булева функция будет представлена двоичным вектором.

Запишем соответствующую ей формулу алгебры логики. Она может быть получена просто. Действительно, для каждого набора значений переменных, на котором функция $f(x_1, x_2, \dots x_n)$ принимает значение 1. Запишем конъюнкцию элементарных переменных высказываний, взяв за составляющую конъюнкции x_k, если x_k на указанном наборе значений переменных есть 1 и отрицание x_k, если значение x_k есть 0. Дизъюнкция всех записанных конъюнкций и будет искомой формулой.

В нашем примере №2 для наборов (1, 1, 0), (1, 0, 1), (0, 1, 0), (0, 0, 0) функция принимает значение 1.

Запишем конъюнкции: $x_1 \wedge x_2 \wedge \overline{x_3}$, $x_1 \wedge \overline{x_2} \wedge x_3$, $\overline{x_1} \wedge x_2 \wedge \overline{x_3}$, $\overline{x_1} \wedge \overline{x_2} \wedge x_3$.

Искомая формула имеет вид: $x_1 \wedge x_2 \wedge \overline{x_3} \vee x_1 \wedge \overline{x_2} \wedge x_3 \vee \overline{x_1} \wedge x_2 \wedge \overline{x_3} \vee \overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}$.

В результате получилась **формула, которая обладает следующими свойствами:**

1) Каждое логическое слагаемое формулы содержит все переменные, входящие в функцию.
2) Все логические слагаемые формулы различны.
3) Ни одно логическое слагаемое не содержит одновременно переменную и ее отрицание.
4) Ни одно логическое слагаемое формулы не содержит одну и ту же переменную дважды.

Перечисленные свойства 1)-4) называются **свойствами совершенства**.

Если булева функция и формула имеют одну и туже таблицу истинности, то говорят, что *формула представляет функцию*.

Вывод: из приведенных рассуждений видно, что каждую не тождественно ложную функцию представляет единственная формула указанного вида.

Замечание:
Формулу, полученную в примере№1 можно упростить, используя равносильные преобразования.

Отв.: $x \to y \cdot z$ или $\bar{x} \vee y \cdot z$.

Определение 1

Если x - логическая переменная, $\delta \in \{0,1\}$, то выражение вида

$$x^{\delta} = \begin{cases} x, & \text{если } \delta = 1, \\ \bar{x}, & \text{если } \delta = 0. \end{cases}$$

называется **литерой** (или **литералом**).

Литеры x и $\bar{x}$ называются **контрарными**.

Из определения 1 следует, что $x^{\delta} = 1 \Leftrightarrow x = \delta, \quad x^{\delta} = 0 \Leftrightarrow x = \bar{\delta}$.

Определение 2

Элементарной конъюнкцией или **конъюнктом** ранга r называется конъюнкция литер.

Элементарная конъюнкция может быть записана в виде:

$$x_1^{\delta_1} \wedge x_2^{\delta_2} \wedge \ldots \wedge x_r^{\delta_r}.$$

Например, ●

$\Delta = (\delta_1, \delta_2, \ldots, \delta_n)$ - набор нулей и единиц.

Определение

Конституентой единицы набора Δ называется конъюнкт

$$K^1(\delta_1, \delta_2, \ldots, \delta_n) = x_1^{\delta_1} \wedge x_2^{\delta_2} \wedge \ldots \wedge x_n^{\delta_n}.$$

Заметим, что $K^1(\delta_1, \delta_2, \ldots, \delta_n) = 1$ тогда и только тогда, когда $x_1 = \delta_1, x_2 = \delta_2, \ldots, x_n = \delta_n$.

Так как в элементарной конъюнкции для каждой из n переменных есть три возможности: входить с отрицанием, входить без отрицания и не входить, то всего имеется 3^n элементарных конъюнкций.

Пустая конъюнкция, не содержащая ни одного литерала, считается конъюнкцией нулевого ранга и полагается равной константе 1.

Утверждение 1

Элементарная конъюнкция $x_1^{\delta_1} \wedge x_2^{\delta_2} \wedge \ldots \wedge x_n^{\delta_n}$ принимает значение 1 на единственном наборе значений переменных $x_1 = \delta_1, x_2 = \delta_2, \ldots, x_n = \delta_n$

Определение 3

Дизъюнктивной нормальной формой *(ДНФ) формулы A называется равносильная ей формула, представляющая дизъюнкцию элементарных конъюнкций.*

Любая формула может быть представлена в виде ДНФ, причем такое представление не единственно.

Но среди многочисленных ДНФ существует единственная, для которой выполняются перечисленные выше свойства совершенства. Такая ДНФ называется *совершенной дизъюнктивной нормальной формой* (СНДФ) формулы *A*.

Определение

Совершенной дизъюнктивной нормальной формой *(СДНФ) формулы A называется ДНФ, удовлетворяющая свойствам совершенства.*

Определение

Совершенной дизъюнктивной нормальной формой *(СДНФ) формулы A называется дизъюнкция некоторых конституент единицы, среди которых нет одинаковых.*

Вопрос 27. Конъюнктивная нормальная форма

Определение 4

Элементарной дизъюнкцией или **дизъюнктом** ранга *r* называется дизъюнкция литер.

Элементарная дизъюнкция может быть записана в виде:

$$x_1^{\delta_1} \vee x_2^{\delta_2} \vee \ldots \vee x_r^{\delta_r}.$$

Определение

Конституентой нуля набора Δ называется дизъюнкт

$$K^0(\delta_1, \delta_2, \ldots, \delta_n) = x_1^{1-\delta_1} \vee x_2^{1-\delta_2} \vee \ldots \vee x_n^{1-\delta_n}.$$

Заметим, что $K^0(\delta_1, \delta_2, \ldots, \delta_n) = 0$ тогда и только тогда, когда $x_1 = \delta_1, x_2 = \delta_2, \ldots, x_n = \delta_n$.

Пустая дизъюнкция считается дизъюнкцией нулевого ранга и полагается равной константе 0.

Утверждение 2

Элементарная дизъюнкция $x_1^{\delta_1} \vee x_2^{\delta_2} \vee \ldots \vee x_n^{\delta_n}$ принимает значение 0 на единственном наборе значений переменных $x_1 = \overline{\delta_1}, x_2 = \overline{\delta_2}, \ldots, x_n = \overline{\delta_n}$

Определение 5

Конъюнктивной нормальной формой (КНФ) формулы *A* называется равносильная ей формула, представляющая конъюнкцию элементарных дизъюнкций.

Для любой формулы алгебры логики путем равносильных преобразований можно получить ее КНФ, причем не единственную.

Рассмотрим КНФ, которая удовлетворяет **свойствам совершенства**:
1). Все элементарные дизъюнкции содержат все переменные.
2). Все элементарные дизъюнкции различны.
3). Каждая элементарная дизъюнкция не содержит одновременно переменную и ее отрицание.
4). Каждая элементарная дизъюнкция не содержит двух одинаковых переменных.

Определение
Совершенной конъюнктивной нормальной формой *(СКНФ) формулы А называется КНФ, удовлетворяющая свойствам совершенства.*

Например, ●

Для решения задачи нахождения СНДФ и СКДФ булевых функций, сформулируем Теорему о функциональной полноте.

Теорема

Для любой булевой функции $f(x_1, x_2, \dots x_n)$ найдется формула A, представляющая функцию f:

1. если $f(x_1, x_2, \dots x_n)$ не равна тождественно нулю, то существует представляющая ее формула, находящаяся в СДНФ:

$$f(x_1, x_2, \dots, x_n) = \bigvee_{f(\delta_1, \dots, \delta_n)=1} x_1^{\delta_1} \wedge x_2^{\delta_2} \wedge \dots \wedge x_n^{\delta_n}$$

и такое представление единственно с точностью до порядка следования элементарных конъюнкций;

2. если $f(x_1, x_2, \dots x_n)$ не равна тождественно единице, то существует представляющая ее формула, находящаяся в СКНФ:

$$f(x_1, x_2, \dots, x_n) = \bigwedge_{f(\delta_1, \dots, \delta_n)=0} x_1^{\overline{\delta}_1} \vee x_2^{\overline{\delta}_2} \vee \dots \vee x_n^{\overline{\delta}_n}$$

и такое представление единственно с точностью до порядка следования элементарных дизъюнкций.

Итак, для нахождения СДНФ и СКНФ исходной формулы А составляется ее таблица истинности, а затем по ней строится требуемая совершенная нормальная форма.

Вопрос 28. Проблема разрешимости

Все формулы алгебры логики делятся на три класса:

1) тождественно истинные,
2) тождественно ложные,
3) выполнимые.

Определения тождественно истинной и тождественно ложной формул даны выше.

Определение
Формула *А* называется **выполнимой,** если она принимает значение «истина» хотя бы на одном наборе значений входящих в нее переменных и не является тождественно истинной.

В связи с этим возникает задача: к какому классу относится данная формула?
Эта задача носит название *проблемы разрешимости.*

Очевидно, что проблема разрешимости алгебры логики разрешима.

Действительно, для каждой формулы алгебры логики может быть записана таблица истинности, которая и даст ответ на поставленный вопрос.

Однако практическое использование таблицы истинности для формулы $A(x_1, x_2, \ldots, x_n)$ при больших *n* затруднительно.

Существует другой способ, позволяющий, не используя таблицы истинности, определить, к какому классу относится формула *A*. Этот способ основан на приведении формулы к нормальной форме (КНФ или ДНФ) и использовании алгоритма, который позволяет определить, является ли данная формула тождественно истинной или не является. Одновременно с этим решается вопрос о том, будет ли формула *A* выполнимой.

Предположим, что мы имеем критерий тождественной истинности для формул алгебры логики. Рассмотрим механизм его применения.

Применим критерий тождественной истинности к формуле *A*. Если окажется, что формула *A* - тождественно истинная, то задача решена. Если же окажется, что формула *A* не тождественно истинная, то применим критерий тождественной истинности к формуле $\overline{A}$. Если окажется, что формула $\overline{A}$ - тождественно истинная, то ясно, что формула *A* - тождественно ложная, и задача решена. Если же формула $\overline{A}$ не тождественно истинная, то остается единственно возможный результат: формула *A* выполнима.

Установим теперь критерий тождественной истинности произвольной формулы алгебры логики. С этой целью предварительно сформулируем и докажем критерий тождественной истинности элементарной дизъюнкции.

Теорема 1.

Для того, чтобы элементарная дизъюнкция была тождественно истинной, необходимо и достаточно, чтобы в ней содержалась переменная и ее отрицание.

Доказательство. ***Необходимость***. Пусть элементарная дизъюнкция тождественно истинна, но в нее одновременно не входит некоторая переменная и ее отрицание. Придадим каждой переменной, входящей в элементарную дизъюнкцию без знака отрицания, значение «ложь», а каждой переменной, входящей в элементарную дизъюнкцию под знаком отрицания - значение «истина». Тогда, очевидно, вся элементарная дизъюнкция примет значение «ложь», что противоречит условию.

Достаточность. Пусть теперь элементарная дизъюнкция содержит переменную и ее отрицание. Так как $x_i \vee \overline{x_i} \equiv 1$, то и вся элементарная дизъюнкция будет тождественно истинной.

Критерий тождественной истинности элементарной дизъюнкции позволяет сформулировать и доказать критерий тождественной истинности произвольной формулы алгебры логики.

Теорема 2.

Для того, чтобы формула алгебры логики A была тождественно истинна, необходимо и достаточно, чтобы любая элементарная дизъюнкция, входящая в КНФ A, содержала переменную и ее отрицание.

Доказательство. ***Необходимость.*** Пусть *A* - тождественно истинна. Тогда и КНФ *A* - тождественна истинна. Но КНФ $A \equiv A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n$, где A_i - элементарные дизъюнкции $(i = 1,2,\ldots,n)$. Так как КНФ $A \equiv 1$, то $A_i \equiv 1 \ (i = 1,2,\ldots,n)$. Но тогда по теореме 1 каждая элементарная дизъюнкция A_i содержит переменную и ее отрицание.

Достаточность. Пусть любая элементарная дизъюнкция A_i, входящая в КНФ *A*, содержит переменную и ее отрицание. Тогда по теореме 1 $A_i \equiv 1 \ (i = 1,2,\ldots,n)$. При этом и КНФ $A \equiv 1$.

Например, выясним, является ли формула $A \equiv y \vee \bar{y} \,\&\, x \vee \bar{x} \,\&\, \bar{y}$ тождественно истинной.

Так как $A \equiv y \vee \bar{y} \,\&\, (x \vee \bar{x}) \equiv (y \vee \bar{y}) \,\&\, (y \vee x \vee \bar{x})$, то ясно, что каждая элементарная дизъюнкция $y \vee \bar{y}$ и $y \vee x \vee \bar{x}$, входящая в КНФ *A*, содержит переменную и ее отрицание. Следовательно, $A \equiv 1$.

Аналогично можно установить критерий тождественной ложности формулы алгебры логики, используя ее ДНФ.

Теорема 3.

Для того, чтобы элементарная конъюнкция была тождественно ложной, необходимо и достаточно, чтобы в ней содержалась переменная и ее отрицание.

Теорема 4.

Для того, чтобы формула алгебры логики А была тождественно ложной, необходимо и достаточно, чтобы любая конъюнкция, входящая в ДНФ А, содержала переменную и ее отрицание.

Вопрос 29. Понятие предиката

Логика высказываний - очень узкая логическая система. Есть такие типы логических рассуждений, которые не могут быть осуществлены в рамках логики высказываний.

Например:

1. Простое число 2 - четное. Следовательно, существуют простые четные числа.
2. Всякий друг Ивана есть друг Петра. Сидор не есть друг Петра, следовательно, Сидор не есть друг Ивана.

Корректность этих умозаключений основана на внутренней структуре самих предложений и на смысле слов "всякий" и "существуют".

В связи с этим возникает необходимость в расширении логики высказываний.

- Логика предикатов представляет собой дальнейшее развитие алгебры логики.
- Логика предикатов, как и традиционная формальная логика, расчленяет элементарное высказывание на субъект (буквально - подлежащее, хотя оно и может играть роль дополнения) и предикат (буквально - сказуемое, хотя оно может играть роль определения).
- **Субъект** - это то, о чем что-то утверждается в высказывании;
- **Предикат** - это то, что утверждается о субъекте.

Пример:

Например, в высказывании «7 простое число», «7»- субъект, «простое число» - предикат. Это высказывание утверждает, что «7» обладает свойством «быть простым числом».

Если в рассмотренном примере заменить конкретное число 7 переменной *x* из множества натуральных чисел, то получим высказывательную форму «*x* - простое число». При одних значениях *x* (например *x*=13, *x*=17) эта форма дает истинные высказывания, а при других значениях *x* (например, *x*=10, *x*=18) эта форма дает ложные высказывания.

Что собой представляет эта высказывательная форма?

Ясно, что эта высказывательная форма определяет функцию одной переменной - *x*, определенной на множестве *N*, и принимающую значение из множества {1, 0}.

- Здесь предикат становится функцией субъекта и выражает свойство субъекта.

Определение 1

Одноместным предикатом называется произвольная функция переменной *x*, определенная на множестве *M* и принимающая значение из множества {1, 0}.

Множество M, на котором определен предикат *P(x)* называется **областью определения предиката**.

Обозначение: *P(x)*.

Определение 2

Множество всех элементов $x \in M$, при которых предикат принимает значение «истина», называется **множеством истинности** предиката *P(x)*.
Обозначение: I_p.

Т.о. множество истинности предиката *P(x)* - это множество:

$$I_P = \{x : x \in \mathrm{M},\ \mathrm{P}(x) = 1\}.$$

Так, предикат *P(x)* - «*x* - простое число» определен на множестве *N*, то множество I_p для него есть множество всех простых чисел.

Предикат $Q(x)$ - "$\sin x = 0$" определен на множестве *R*, а его множество истинности $I_Q = \{x : k\pi, k \in z\}$.

Приведенные примеры одноместных предикатов выражают свойства предметов.

Определение 3

Предикат *P(x)*, определенный на множестве *M*, называется **тождественно истинным** (**тождественно ложным**), если $I_p = M$ ($I_p = Ш$).

Естественным обобщением понятия одноместного предиката является понятие многоместного предиката, с помощью которого выражаются отношения между предметами.

Примером бинарного отношения (отношения между двумя предметами) является отношение «меньше». Пусть это отношение введено на множестве *Z* целых чисел. Оно может быть охарактеризовано высказывательной формой: «x<y», где x,y ∈ *Z*, то есть является функцией двух переменных *P(x,y)*, определенной на множестве Z×Z с множеством значений на {1, 0}.

Определение 4

***n*-местным предикатом** $P(x_1, x_2, \ldots, x_n)$ называется функция *n* переменных $x_1, x_2, \ldots, x_n$, определенная на множестве $M = M_1 \times M_2 \times \ldots M_n$ и принимающая значения на множестве {1, 0}.

Примеры:

1. *Q(x,y)* - «*x=y*» предикат равенства, определенный на множестве $R^2 = R \times R$;
2. *F(x,y)* - «x || y» - прямая *x* параллельна прямой *y*, определенный на множестве прямых, лежащих на данной плоскости.

Аналогично определяется *n*-местный предикат.

Вопрос 30. Логические операции над предикатами.

Предикаты, так же, как высказывания, принимают два значения *И* и *Л*, поэтому к ним применимы все операции логики высказываний.

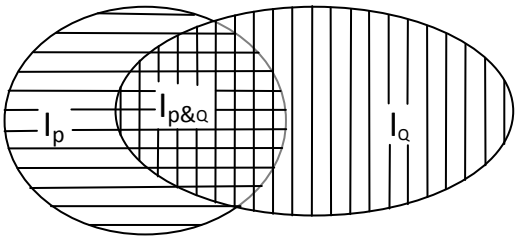
Рассмотрим применение операций логики высказываний к предикатам на примерах одноместных предикатов.

Пусть на некотором множестве *M* определены два предиката *P(x)* и *Q(x)*.

Определение 5

Конъюнкцией двух предикатов *P(x)* и *Q(x)* называется новый предикат, который принимает значение «истина» при тех и только тех значениях x ∈ M, при которых каждый из предикатов принимает значение «истина», и принимает значение «ложь» во всех остальных случаях.

Обозначение: $P(x) \& Q(x)$ или $P(x) \wedge Q(x)$.



Областью истинности предиката $P(x) \wedge Q(x)$ является пересечение $I_p \cap I_Q$.

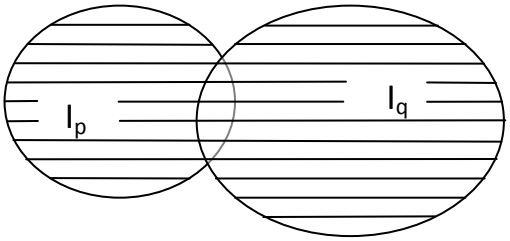
●Например, для предикатов $P(x)$: «*x* четное число» и $Q(x)$: «*x* кратно 3» конъюнкцией $P(x) \& Q(x)$ является предикат «*x* четное число и *x* кратно 3», то есть предикат «*x* делится на 6».

Определение 6

Дизъюнкцией двух предикатов *P(x)* и *Q(x)* называется новый предикат, который принимает значение «ложь» при тех и только тех значениях $x \in M$, при которых каждый из предикатов принимает значение «ложь», и принимает значение «истина» во всех остальных случаях.

Обозначение: $P(x) \vee Q(x)$.

Ясно, что областью истинности предиката $P(x) \vee Q(x)$ является объединение областей истинности предикатов *P(x)* и *Q(x)*, т.е. объединение $I_p \cup I_q$.



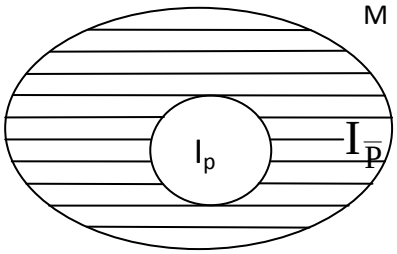
Пример:
P(x): «x - число, кратное 3»;
Q(x): «x - число, кратное 5».
$P(x) \vee Q(x)$: «x - кратно 3 или число x кратно 5».

Определение 7

Отрицанием предиката *P(x)* называется новый предикат *P(x)*, который принимает значение «истина» при всех значениях $x \in M$, при которых предикат *P(x)* принимает значение «ложь», и принимает значение «ложь» при тех значениях $x \in M$, при которых предикат *P(x)* принимает значение «истина».

Обозначение: $\overline{P(x)}$.

Из этого определения следует, что $I_{\overline{P}} = M \setminus I_P$.



Областью истинности предиката $\overline{P(x)}$ является разность между M и областью истинности предиката *P(x)*, т.е. $M \setminus I_P = CI_p$.

Пример: ●
P(x): «*x* - число четное" на множестве *Z*;
$\overline{P}(x)$: «*x* - число нечетное». $I_{\overline{P}} = Z \setminus I_P$.

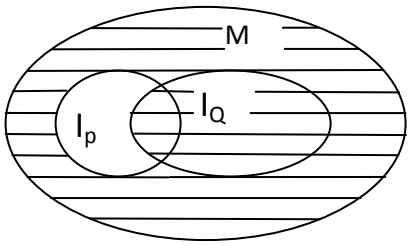
Определение 8

Импликацией предикатов *P(x)* и *Q(x)* называется новый предикат, который является ложным при тех и только тех значениях x ∈ M, при которых одновременно *P(x)* принимает значение «истина», а *Q(x)* - значение «ложь» и принимает значение «истина» во всех остальных случаях.

Обозначение: $P(x) \to Q(x)$.

Так как при каждом фиксированном $x \in M$ справедлива равносильность $P(x) \to Q(x) \equiv \overline{P}(x) \vee Q(x)$, то область истинности импликации

$$I_{P \to Q} = I_{\overline{P}} \cup I_Q .$$



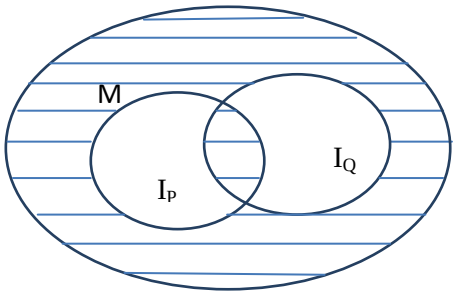
Пример:
P(x): «*x* - четное число;
Q(x): «*x* - кратно 3».
$P(x) \to Q(x)$: «Если *x* четное, то *x* кратно 3».

Определение

Эквивалентностью предикатов P(x) и Q(x) называется новый предикат, который является истинным при тех значениях x ∈ M, при которых одновременно P(x) и Q(x) принимают значение «истина» или одновременно принимают значение «ложь», и считается ложным в остальных случаях.

Обозначение: P(x) ↔ Q(x)

$I_{P \leftrightarrow Q} = (I_{\overline{P}} \cup I_Q) \cap (I_{\overline{q}} \cup I_P)$



Пример:
P(x): «x - число, кратное 3»
Q(x): «x - число, кратное 5»
P(x) ↔ Q(x): «x - число кратное и 3, и 5 (кратное 15) или число не кратное ни 3, ни 5»

Вопрос 31. Кванторные операции над предикатами.

Пусть имеется предикат *P(x)*, определенный на множестве *M*. Если *a* - некоторый элемент из множества *M*, то подстановка его вместо *x* в предикат *P(x)* превращает его в высказывание *P(a)*.

Наряду с образованием из предикатов единичных высказываний в логике предикатов рассматриваются еще две операции, которые превращают одноместный предикат в высказывание.

Квантор всеобщности.

Пусть *P(x)* - предикат, определенный на множестве M.

Определение 9

Под выражением $\forall x P(x)$ понимают высказывание, истинное, когда *P(x)* истинно для каждого элемента *x* из множества M и ложное в противном случае.

Символ $\forall$ называют квантором всеобщности (от английского: All - все).

Это высказывание уже не зависит от *x*. Соответствующее ему словесное выражение будет: «Для всякого *x P(x)* истинно».

Переменную *x* в предикате *P(x)* называют **свободной** (ей можно придавать различные значения из M), в высказывании $\forall x P(x)$ переменную *x* называют **связанной** квантором $\forall$.

Квантор существования

Пусть *P(x)* - предикат, определенный на множестве M.

Определение 10

Под выражением $\exists x P(x)$ понимают высказывание, которое является истинным, если существует элемент $x \in M$, для которого *P(x)* истинно, и ложным в противном случае.

Символ $\exists$ называют **квантором существования**. В высказывании $\exists x P(x)$ переменная *x* связана квантором $\exists$.

Это высказывание уже не зависит от *x*. Соответствующее ему словесное выражение будет: «Существует *x*, при котором *P(x)* истинно».

Приведем пример употребления кванторов.

Пусть на множестве *N* натуральных чисел задан предикат *P(x)*: «Число *x* кратно 5». Используя кванторы, из данного предиката можно получить высказывания:

$\forall x \in N \quad P(x)$ - «Все натуральные числа кратны 5»

$\exists x \in N \quad P(x)$ - «Существует натуральное число, кратное 5»

Очевидно, первое из высказываний ложно, а второе истинно.

Вывод: высказывание $\forall x P(x)$ будет истинным тогда и только тогда, когда *P(x)* тождественно истинный предикат, а высказывание $\exists x P(x)$ будет ложным тогда и только тогда, когда *P(x)* тождественно ложный предикат.

Взаимосвязь кванторных операции с операциями конъюнкции и дизъюнкции

Рассмотрим предикат *P(x)*, определенный на множестве $M = \{a_1, a_2, ..., a_h\}$, содержащем конечное число элементов. Если предикат *P(x)* является тождественно истинным, то истинным будут высказывания: *P(a₁)*, *P(a₂)*, …, *P(aₙ)*. При этом истинными будут высказывание $\forall x P(x)$ и конъюнкция *P(a₁)&P(a₂)& …& P(aₙ)*.

Если же хотя бы для одного элемента $a_k \in M$ $P(a_k)$ окажется ложным, то ложными будут высказывания $\forall x P(x)$ и конъюнкция *P(a₁)&P(a₂)& …& P(aₙ)*.

Следовательно, справедлива равносильность:

$$\forall x P(x) \equiv P(a_1) \& P(a_2) \& \cdots \& P(a_n).$$

Нетрудно показать, что справедлива и равносильность:

$$\exists x P(x) \equiv P(a_1) \vee P(a_2) \vee \cdots \vee P(a_n).$$

Отсюда видно, что кванторные операции можно рассматривать как обобщение операций конъюнкции и дизъюнкции.

Кванторные операции применяются и к многоместным предикатам. Однако заметим, что применение одной кванторной операции к двуместному предикату не превращает его в высказывание, а превращает его в одноместный предикат.

Чтобы превратить двуместный предикат в высказывание с помощью кванторных операций, нужно использовать две кванторные операции по каждой из переменных.

Рассмотрим двухместных предикат *P(x,y) P(ax)*: «x ⋮ y» определенный на множестве *N*. (*x* делится нацело на *y* или *y* - делитель *x*).

Применение кванторных операций к предикату *P(x,y)* приводит к восьми высказываниям:

1.	$\forall y \forall x P(x,y)$	«Для всякого y и для всякого x y является делителем x»	(Ложно)
2.	$\exists y \forall x P(x,y)$	«Существует y, которое является делителем всякого x»	(Истинно)
3.	$\forall y \exists x P(x,y)$	«Для всякого y существует такое x, что x делится на y»	(Истинно)
4.	$\exists y \exists x P(x,y)$	«Существует y и существует x, такие, что y является делителем x»	(Истинно)
5.	$\forall x \forall y P(x,y)$	«Для всякого x и для всякого y y является делителем x»	(Ложно)
6.	$\forall x \exists y P(x,y)$	«Для всякого x существует такое y, что x делится на y»	(Истинно)
7.	$\exists x \exists y P(x,y)$	«Существует x и существует y такое, что y является делителем x»	(Истинно)
8.	$\exists x \forall y P(x,y)$	«Существует x такое, что для всякого y x делится на y»	(Ложно)

Из рассмотренных примеров **ВЫВОД:** в общем случае изменение порядка следования кванторов изменяет смысл высказывания, а значит и его логическое значение (например, высказывания 3 и 8).

Например, если *P(x,y)* есть предикат - неравенство, то есть *x<y*, определенный на множестве натуральных чисел, то высказывание

$$\forall x \in N \, \exists \, y \in N \quad \mathrm{P}(\mathrm{x}, \mathrm{y})$$

гласит: «для любого натурального числа *x* существует натуральное число *y*, такое, что *x<y* ». Это высказывание очевидно, истинно, а высказывание

$$\exists x \in N \, \forall \, y \in N \quad \mathrm{P}(\mathrm{x}, \mathrm{y})$$

гласит: «существует натуральное число *x* такое, что для всех натуральных чисел *y* справедливо *x<y* ». Это высказывание ложно. Действительно, для *y*=1 не существует $x \in N$ меньше 1.

Пример: ●

Установить истинность или ложность высказываний:

1) $\forall x(x \in \{2,5\} \rightarrow (x^2-6x+8=0)), x \in R$

2) $\exists x(x \notin \{2,5\} \rightarrow (x^2-6x+8=0)), x \in R$

1) Обозначим предикаты:

P(x): $x \in \{2,5\}$

Q(x): $x^2-6x+8=0$

Найдём области истинности:

$I_P = \{2,5\}$

$I_Q = \{2,4\}$

Применим импликацию к предикатам:

$I_{P \rightarrow Q} = I_{\overline{P}} \cup I_Q = R \setminus I_P \cup I_Q = \{x \in R: x \notin \{2,5\}\} \cup \{2,4\} = \{x \in R: x \neq 5\}$

Так как $I_{P \rightarrow Q} \neq R$, то $\forall x(P(x) \rightarrow Q(x))$ - ложно.

2) Обозначим предикаты:

P(x): $x \notin \{2,5\}$

Q(x): $x^2-6x+8=0$

Найдём области истинности:

$I_P = \{ x \in R: x \notin \{2,5\}\}$

$I_Q = \{2,4\}$

Применим импликацию к предикатам:

$I_{P \rightarrow Q} = I_{\overline{P}} \cup I_Q = R \setminus I_P \cup I_Q = \{2,5\} \cup \{2,4\} = \{2,4,5\}$

Так как $I_{P \rightarrow Q} \neq \emptyset$, то $\exists x(P(x) \rightarrow Q(x))$ - истинно.

Вопрос 32. Формулы логики предикатов

В логике предикатов будем пользоваться следующей символикой:

1. Символы *p, q, r* …- **переменные высказывания**, принимающие два значения 1 - истина, 0 - ложь.
2. **Предметные переменные** - *x, y, z, …* , которые принимают значения из некоторого множества M; *x; y; z; …* - предметные константы, то есть значение предметных переменных.
3. $P(\cdot), F(\cdot)$ **одноместные предикатные переменные**; $Q(\cdot,\cdot,\cdots,\cdot), \mathrm{R}(\cdot,\cdot,\cdots,\cdot)$ ***n*-местные предикатные переменные**. $P^{\circ}(\cdot), \mathrm{Q}^{\circ}(\cdot,\cdot,\cdots,\cdot)$ - символы **постоянных предикатов**.
4. Символы логических операций: $\wedge, \vee, \rightarrow, \overline{\ }$.
5. Символы кванторных операций: $\forall x, \exists \mathrm{x}$.
6. Вспомогательные символы: скобки, запятые.

Определение формулы логики предикатов

1. Каждое высказывание как предметное, так и постоянное, является формулой (элементарной).
2. Если $F(\cdot,\cdot,\cdots,\cdot)$ - *n*-местная предикатная переменная или постоянный предикат, а $x_1, \mathrm{x}_2, \cdots, \mathrm{x}_n$ предметные переменные или предметные постоянные (не обязательно все различные), то $F(x_1, \mathrm{x}_2, \cdots, \mathrm{x}_n)$ есть формула. Такая формула называется элементарной, в ней предметные переменные являются свободными, не связанными кванторами.
3. Если *A* и *B* - формулы, причем такие, что одна и та же предметная переменная не является в одной из них связанной, а в другой - свободной, то слова $A \vee B, \quad \mathrm{A} \wedge \mathrm{B}, \quad \mathrm{A} \rightarrow \mathrm{B}$ есть формулы. В этих формулах те переменные, которые в исходных формулах были свободными, являются свободными, а те которые были связанными, являются связанными.
4. Если *A* - формула, то $\overline{A}$ - формула, и характер предметных переменных при переходе от формулы *A* к формуле $\overline{A}$ не меняется.
5. Если *A(x)* - формула, в которую предметная переменная *x* входит свободно, то слова $\forall x A(x)$ и $\exists x A(x)$ являются формулами, причем предметная переменная входит в них связанно.
6. Всякое слово, отличное от тех, которые названы формулами в пунктах 1-5, не является формулой.

Примеры.

1. Например, если *P(x)* и *Q(x,y)* - одноместный и двуместный предикаты, а *q, r* - переменные высказывания, то формулами будут слова:

$$q, \quad P(x), \quad P(x) \wedge Q(x^{\circ}, y), \forall \mathrm{x} P(x) \rightarrow \exists x Q(x, y), \quad (\overline{Q(x, y)} \vee q) \rightarrow r.$$

2. Слово: $\forall x Q(x, y) \rightarrow P(x)$ не является формулой. Здесь нарушено условие п.3 т.к. в формулу $\forall x Q(x, y)$ переменная *x* входит связано, а в формулу *P(x)* переменная *x* входит свободно.

3. Из определения формулы логики предикатов ясно, что всякая формула алгебры высказываний является формулой логики предикатов.

Определение 11

Две формулы логики предикатов *A* и *B* называются **равносильными на области *M***, если они принимают одинаковые логические значения при всех значениях входящих в них переменных, отнесенных к области *M*.

Определение 12

Две формулы логики предикатов *A* и *B* называются **равносильными**, если они равносильны на всякой области.

Обозначение: $A \equiv B$.

- Ясно, что все равносильности алгебры высказываний будут верны, если в них вместо переменных высказываний поставить формулы логики предикатов.

Но, кроме того, имеют место равносильности самой логики предикатов. Рассмотрим основные из них.

Пусть *A(x)* и *B(x)* - переменные предикаты, а *c* - переменное высказывание. Тогда

1.	$\overline{\forall x A(x)} \equiv \exists x\, \overline{A(x)}$
2.	$\overline{\exists x A(x)} \equiv \forall x\, \overline{A(x)}$
3.	$\forall x A(x) \equiv \overline{\exists x\, \overline{A(x)}}$

4.	$\exists x A(x) \equiv \overline{\forall x \overline{A(x)}}$
5.	$\forall x A(x) \wedge \forall x B(x) \equiv \forall x [A(x) \wedge B(x)]$

и т. д.

Равносильность (1) означает тот простой факт, что если не для всех *x* истинно *A(x)*, то существует *x*, при котором будет истинной $\overline{A(x)}$.

Равносильность (2) означает тот простой факт, что если не существует *x* при котором *истинно A(x)*, то для всех *x* будет истинной $\overline{A}(x)$.

Равносильности (3) и (4) получаются из равносильностей (1) и (2) соответственно, если от обеих их частей взять отрицания и воспользоваться законом двойного отрицания.

Докажем равносильность (5).

Если предикаты *A(x)* и *B(x)* одновременно тождественно истинные, то будет тождественно истинным и предикат $A(x) \wedge B(x)$, а поэтому будут истинными высказывания: $\forall x A(x)$, $\forall x B(x)$, $\forall x [A(x) \wedge B(x)]$.

То есть в этом случае обе части равносильности (5) принимают значение «истина».

Пусть теперь хотя бы один из предикатов, например *A(x)*, будет не тождественно истинным. Тогда не тождественно истинным будет и предикат $A(x) \wedge B(x)$, а поэтому ложными будут высказывания $\forall x A(x)$, $\forall x A(x) \wedge \forall x B(x)$, $\forall x [A(x) \wedge B(x)]$. То есть и в этом случае обе части равносильности (5) принимают одинаковые (ложные) значения. Этим исчерпывается доказательство равносильности (5).

Отметим в заключении, что формула $\forall x [A(x) \vee B(x)]$ не равносильна формуле $\forall x A(x) \vee \forall x B(x)$, а формула $\exists x [A(x) \wedge B(x)]$ не равносильна формуле $\exists x A(x) \wedge \exists x B(x)$.

Вопрос 33 *Понятие алгоритма. Свойства алгоритмов*

- Рассмотрим функцию *n*-переменных

$$f: N_0^n \to N_0,$$
$$\text{где } N_0 = \{0,1,2,3...\}$$

- расширенное множество натуральных чисел.

Под алгоритмом решения этой задачи понимают процесс преобразования во времени заданных *n* натуральных чисел в число $f(x_1, x_2, ... x_n)$, если этот процесс удовлетворяет требованиям:

- *дискретность;*
- *элементарность;*
- *детерминированность;*
- *массовость;*
- *результативность.*

Вопрос 34 *Вычислимые и рекурсивные функции. Тезис Черча*

Определение 1

Числовая функция эффективно вычислима, если имеется алгоритм вычисления любого ее значения, в противном случае - невычислима.

Определение 2

Множество *M* называется перечислимым, если существует алгоритм, позволяющий перечислить все элементы *M* (возможно с повторениями).

Определение 3
Подмножество M называется разрешимым в X, если существует алгоритм, который для любого $x \in X$ решает проблему: является ли x элементом подмножества M.

Теорема Поста

Множество M разрешимо в X тогда и только тогда, когда M и дополнение - перечислимые множества.

Определение 4
Базовыми (простейшими) называются три следующие функции:

1. $O: N_0 \to N_0$, $O(x)=0$ - оператор аннулирования;
2. $S: N_0 \to N_0$, $S(x)=x+1$ - оператор сдвига (функция Пеано);
3. $I_m^n: \ N_0^n \to N_0, \ I_m^n(x_1, x_2, \dots x_n) = x_m, \ 1 \le m \le n$ - оператор проектирования.

Определение 5
Операция получения новой функции по имеющимся функциям:

$$f_0(x_1, x_2, \dots x_n), \ f_1(y_1, y_2, \dots y_k), \dots, f_n(y_1, y_2, \dots y_k)$$

по правилу:

$$f(y_1, y_2, \dots y_k) = f_0(f_1(y_1, y_2, \dots y_k), \dots, f_n(y_1, y_2, \dots y_k))$$

называется суперпозицией или подстановкой.

Определение 6
Операция получения новой функции по имеющимся функциям:

$$f_0(x_1, x_2, \dots x_n), \quad f_1(x_1, x_2, \dots x_n, k, z)$$

по правилу:

$$f(x_1, x_2, \dots, x_n, y) = \begin{cases} f(x_1, x_2, \dots, x_n, 0) = f_0(x_1, x_2, \dots, x_n), \ k = 0 \\ f(x_1, x_2, \dots, x_n, k) = f_1(x_1, \dots, x_n, k-1, f(x_1, \dots, x_n, k-1)), \\ 1 \le k \le y \end{cases}$$

называется примитивной рекурсией.

Определение 7
Если функция $f(x_1, x_2, \dots x_n)$ определена на всем множестве N_0^n, то она называется общей;

в противном случае функция

$f: D \to N_0, \ D \subset N_0^n$

называется частичной.

Определение 8
Функции, полученные из трех базовых функций при помощи конечного числа операций суперпозиции и примитивной рекурсии, называются примитивно рекурсивными.

Теорема

Всякая примитивно рекурсивная функция является общей, то есть всюду определенной.

Определение 9
Операция построения новой функции из известной функции $f_0(x_1, x_2, \dots x_n, y)$

по правилу: $f(x_1, x_2, \dots, x_n, x_{n+1}) = \min_{y \in N_0}\{y : \ f_0(x_1, x_2, \dots x_n, y) = x_{n+1}\}$ называется минимизацией.

Определение 10
Функция, получающаяся из базовых при помощи конечного числа трех операций - суперпозиции, примитивной рекурсии и минимизации, называется частично рекурсивной.

Тезис Черча

Класс интуитивно вычислимых функций совпадает с классом частично рекурсивных функций.

Вопрос 35 *Машина Тьюринга. Тезис Тьюринга.*

Устройство машины Тьюринга включает:

- *Ленту машины* - устройство для записи входной, промежуточной и выходной информации;
- *Внешний алфавит* - конечное множество символов $A=\{a_0, a_1, \dots, a_n\}$, символ a_0 - пустая клетка; символы $a_i \neq a_0$ - буквы алфавита;
- *Внутренний алфавит* - конечное множество символов

$$Q=\{q_0, q_1, \dots, q_m, R, L, S\},$$

где символы

q_i - символы состояния машины;
q_0 - заключительное состояние;
q_1 - начальное состояние;
R - сдвиг вправо (Right);
L - сдвиг влево (Left);
S - на месте (State);

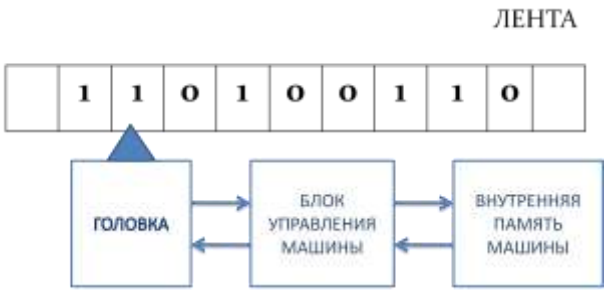
- *Головка машины* - устройство для обработки символов в клетках ленты;
- *Программа машины* - конечный набор команд вида

$$q_i\, a_l \rightarrow q_k a_l P$$

где P - один из символов R, L, S.

Программу машины Тьюринга представляют в виде таблицы:

	A					
	a_0	a_1	…	a_j	…	a_n
q_0						
…						
q_i				$q_k a_l P$		
…						
q_m						



Машина Тьюринга

Определение 11

Машина Тьюринга не применима к слову x, если в процессе применения ее к слову она ни на каком из шагов не приходит в заключительное состояние.

Тезис Тьюринга

Всякий интуитивный алгоритм может быть реализован с помощью некоторой машины Тьюринга.

Вопрос 36. *Нормальные алгоритмы Маркова.*

Определение 12

- Конечное множество символов $A=\{a_0, a_1,\dots,a_n\}$ называется алфавитом;

- символы алфавита A - буквами;

- конечное множество $\tilde{A}=A\cup M$, где $A\cap M\neq\varnothing$ называется расширением алфавита A;

- конечная последовательность символов алфавита $\tilde{A}$ называется словом.

Обозначение: $a_{i1}a_{i2}\dots a_{is}$ - слово;

Λ - пустое слово.

Определение 13

Конкатенацией (соединением) слов $P= a_{i1}a_{i2}\dots a_{is}$ и $Q= a_{j1}a_{j2}\dots a_{jt}$

называется слово $PQ= a_{i1}a_{i2}\dots a_{is}a_{j1}a_{j2}\dots a_{jt}$.

Теорема

Операция конкатенации ассоциативна:

$$\forall P,Q,R \in \tilde{A} \quad (PQ)R = P(QR).$$

Для операции конкатенации слов существует *нейтральный элемент*:

$$\forall P \in \tilde{A} \quad P\Lambda = \Lambda P = P.$$

Пусть $\rightarrow, \bullet \notin \tilde{A}$.

Определение 14

Выражения $P \rightarrow Q$, $P \rightarrow \bullet Q$, где $P,Q \in \Gamma$ называются подстановками слова Q вместо слова P:

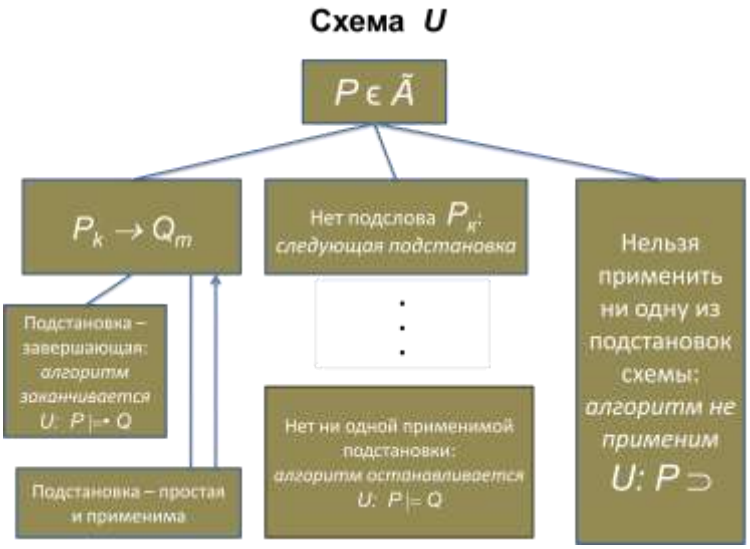
- подстановка $P \rightarrow Q$ называется простой;

- подстановка $P \rightarrow \bullet Q$ - заключительной.

Определение 15

Конечный список подстановок называется схемой нормального алгоритма в алфавите Γ или над алфавитом A.

Обозначение: U.



Марков:

Класс функций, реализуемый нормальными алгоритмами, совпадает с классом функций, реализуемых машиной Тьюринга, и с классом частично рекурсивных функций

Вопрос 37. Трудоемкость алгоритма. Эффективные алгоритмы.

Трудоемкость алгоритма оценивают временем решения наиболее трудной задачи данной размерности n или средним временем решения по всему множеству задач данной размерности.

Определение 1

Трудоемкость алгоритма есть $O(f(n))$, если для всех задач данного класса число элементарных операций алгоритма не превосходит $c \cdot f(n)$, где:

$f(n)$ - некоторая возрастающая с ростом n функция;

c - *не зависящая от* n константа.

Если число операций есть:

$O(n)$, то алгоритм имеет линейную трудоемкость;

$O(n^2)$ - квадратичную;

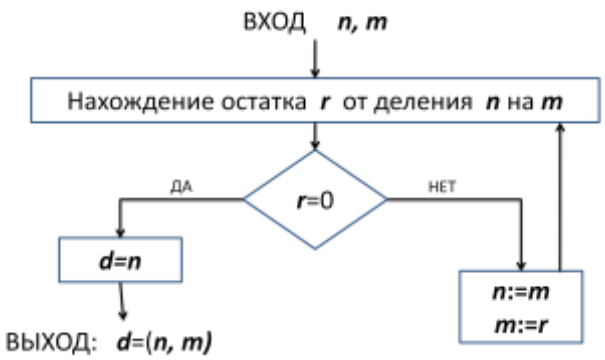
и т.д.

Определение 2

Алгоритмы, трудоемкость которых есть $O(n^k)$ называются полиномиальными или эффективными.

Для большинства эффективных алгоритмов k =1, 2, 3.

Блок-схема алгоритма Евклида



Вопрос 38. Сложность вычислений. Классы сложности: P, NP и NP-полные задачи.

Определение 3

Сложность алгоритма решения задачи - число шагов (элементарных действий), необходимых для получения окончательного результата.

Определение 4

Класс P - это класс таких задач распознавания, для которых существуют эффективные , то есть полиномиальные от длины входа алгоритмы решения.

Определение 5

Класс NP - это множество таких задач распознавания, для которых в случае правильного ответа «да» существуют:

1. полиномиальный от длины входа задачи сертификат для подтверждения этого ответа;
2. эффективный алгоритм проверки этого сертификата.

Определение 6

Задача A полиномиально сводится к задаче B, если по строке x_A, задающей задачу A, за полиномиальное относительно $|x_A|$ время можно построить строку $|x_B|$, задающую задачу B, которая имеет ответ «да» и том и только том случае, если исходная задача A имеет ответ «да».

Обозначение: $A \to B$.

Утверждение 1

Если $A \to B$ и $B \in P$, то $A \in P$.

Утверждение 2

Отношение полиномиальной сводимости транзитивно:

если $A \to B$ и $B \to C$, то $A \to C$.

Определение 7

Задача распознавания $A \in NP$ называется *NP*-полной, если любая задача из NP полиномиально сводится к A.

Определение 1

Теория графов - область дискретной математики, особенностью которой является геометрический подход к изучению объектов.

Вопрос 39. Понятие графа. Виды графов.

Определение 1

Говорят, что определен граф, если задано, вообще говоря, конечное множество

$X=\{x_1, x_2,\dots,x_n\}$ некоторых объектов - вершин графа и множество $A=\{a_1, a_2,\dots,a_k\}$ всех существующих попарных связей вида $a_k=(x_i, x_j)$ между вершинами.

Обозначение: $G=(X,A)$.

Определение 2

- Ненаправленные (неориентированные) связи в графе называются ребрами;

- направленные (ориентированные) связи называются дугами.

Определение 3

- Граф, все связи которого ненаправлены, называется неориентированным (неорграфом);

- граф, все связи которого направлены, называется ориентированным (орграфом).

Определение 4 (по Бержу)

Говорят, что задан граф, если даны:

1) Непустое множество X;
2) Отображение Γ множества X в X.

Обозначение: $G=(X, \Gamma)$.

Определение 5

Подграфом графа $G=(X, \Gamma)$ называется граф, которому принадлежит лишь часть вершин графа G, образующих множество Y, вместе с дугами, соединяющими эти вершины.

Определение 6

Частичным графом по отношению к графу G называется граф, содержащий только часть дуг графа G.

Определение 7

- Граф, в котором пару вершин может соединять не более чем одно ребро называется простым;

- граф с кратными ребрами и петлями называется псевдографом;

- псевдограф без петель называется мультиграфом.

Определение 8

- Граф, состоящий из одной вершины, называется тривиальным;

- вершина, не связанная ни с одной из остальных вершин графа, называется изолированной;

- граф, состоящий из изолированных вершин, называется ноль-графом.

Вопрос 40. Способы задания графов.

- Диаграмма (графическое изображение).
- Теоретико- множественный способ: $G=(X, A)$.
- С помощью прямого отображения: $G=(X, \Gamma)$.
- С помощью обратного отображения: $G=(X, \Gamma^{-1})$.
- Матричный: матрицы смежности и инцидентности.

Определение 9

Прямым отображением Γ вершины x_i называется множество таких вершин $x_j \in X$, для которых в графе G существует дуга (x_i, x_j):

$\Gamma x_i = \{x_j \in X: \exists (x_i, x_j) \in G\}$.

Определение 10

Обратным отображением Γ^{-1} вершины x_i называется множество таких вершин $x_k \in X$, для которых в графе G существует дуга (x_k, x_i):

$\Gamma^{-1} x_i = \{x_k \in X: \exists (x_k, x_i) \in G\}$.

Определение 11

- Две дуги (ребра) графа называются смежными, если они имеют общую вершину;

- любые две вершины графа x_i и x_j называются смежными, если на графе имеется дуга $a=(x_i, x_j)$ (ребро), соединяющая эти вершины;

- при этом говорят, что каждая из вершин x_i, x_j инцидентна дуге a (ребру), а дуга (ребро) инцидентна этим вершинам.

Пусть дан орграф $G=(X, A)$ с n вершинами.

Определение 12

Матрицей смежности графа G называется квадратная матрица D, порядок которой n равен числу вершин графа, а элемент d_{ij} равен числу дуг (x_i, x_j) с началом в вершине x_i и концом в x_j:

$$d_{ij} = \begin{cases} к, \ \ если \ \ существует \ \ к \ \ дуг \ \ (x_i, x_j) \\ \\ 0, \ \ в \ \ противном \ случае \end{cases}$$

Определение 13

- Если дуга a *исходит из вершины* x, то говорят, что дуга a положительно инцидентна этой вершине;

- дуга a называется отрицательно инцидентной вершине x, если она *заходит в эту вершину*.

Определение 14

- Число дуг, инцидентных вершине x, называется степенью вершины x;
- число дуг, положительно инцидентных вершине x, называется полустепенью исхода вершины x;
- число дуг, отрицательно инцидентных вершине x, называется полустепенью захода вершины x.

Определение 15

Матрицей инцидентности графа , не содержащего петель, называется матрица B размерности $n \times m$, где n - число вершин графа, m - число дуг, элементы которой образуются по следующему правилу:

$$b_{ij} = \begin{cases} 1, & \text{если дуга } a_j \textbf{ положительно инцидентна} \text{ вершине } x_i, \text{ т.е. исходит из нее;} \\ -1, & \text{если дуга } a_j \textbf{ отрицательно инцидентна} \text{ вершине } x_i, \text{ т.е. заходит в нее;} \\ 0, & \text{если дуга } a_j \textbf{ не инцидентна} \text{ вершине } x_i. \end{cases}$$

Вопрос 41. Операции над графами.

Пусть даны графы $G_1=(X_1,A_1)$, $G_2=(X_2,A_2)$.

Определение 1

Объединением графов G_1 и G_2 называется граф $G=(X,A)$, множество вершин которого X и множество дуг (ребер) A определяются выражениями:

$X=X_1\cup X_2$, $A=A_1\cup A_2$.

Обозначение: $G=G_1\cup G_2$

Определение 2

Пересечением графов G_1 и G_2 называется граф $G=(X,A)$, множество вершин которого X и множество дуг (ребер) A определяются выражениями:

$X=X_1\cap X_2$, $A=A_1\cap A_2$.

Обозначение: $G=G_1\cap G_2$

Определение 3

Кольцевой суммой графов G_1 и G_2 называется граф $G=(X,A)$, множество вершин которого X и множество дуг (ребер) A определяются выражениями:

$X=X_1\cup X_2$, $A=A_1\oplus A_2$,

где $A_1\oplus A_2=(A_1 | A_2)\cup(A_2 | A_1)$.

Обозначение: $G=G_1\oplus G_2$

Определение 4

Произведением графов $G_1=(Y,A_1)$ и $G_2=(Z,A_2)$ называется граф $G=(X,A)$, множество вершин которого X определяется выражением:

$X=Y\times Z$,

причем

$((y_1,z_1),(y_2,z_2))\in A \Leftrightarrow y_1=y_2$ и $(z_1,z_2)\in A_2$

или $z_1=z_2$ и $(y_1,y_2)\in A_1$.

Обозначение: $G=G_1\times G_2$

Определение 5

Неорграф без петель называется полным, если его любые две различные вершины смежны.

Обозначение: K_n - полный граф с n вершинами.

Обозначим: Q_n n- куб.

Правило построения n - мерного куба:

1. Q_0 - граф без петель, состоящий из одной вершины;
2. $Q_1=K_2$;
3. $Q_n= K_2\times Q_{n-1}$, n>1.

Вершинами n - мерного куба Q_n являются всевозможные n-ки, состоящие из нулей и единиц, а ребра задаются по следующему правилу:

вершины смежны ‹=› соответствующие кортежи различаются ровно одной координатой

Пусть $G=(X,A)$, $a_i \in A$.

Определение 6

- Графом $G-a_i$ называется граф, который получился из графа G путем удаления ребра (дуги) $a_i \in A$;

- удалением ребра (дуги) a_i называется операция перехода от графа G к графу $G-a_i$.

При этом вершины, инцидентные ребру (дуге) a_i, из графа G не удаляются.

Пусть $G=(X,A)$, $x_i \in X$.

Определение 7

- Графом $G-x_i$ называется граф, который получился из графа G путем удаления вершины $x_i \in X$ и всех ребер (дуг), инцидентных этой вершине;

- удалением вершины x_i называется операция перехода от графа G к графу $G-x_i$.

Вопрос 42. Маршруты на графе: цепи и пути.

Пусть $G=(X,A)$ - граф.

Определение 8

- Последовательность $x_1,a_1,x_2,a_2,\dots, a_n,x_{n+1}$,

где $x_1,x_2,\dots,x_{n+1} \in X$, $a_1,a_2,\dots,a_n \in A$ называется маршрутом, соединяющим вершины x_1 и x_{n+1}, если $a_i=(x_i, x_{i+1})$, $i=1,2,\dots,n$;

- число n дуг в маршруте называется его длиной.

Пусть $G=(X,A)$ - неорграф.

Определение 9

- Цепью называется маршрут, все ребра которого различны;

- простой цепью называется цепь, все вершины которой, кроме, быть может, первой и последней, различны.

Определение 10

- Циклическим называется маршрут, если $x_1=x_{n+1}$;

- циклом называется циклическая цепь;

- простым циклом называется циклическая простая цепь;

- ациклическим называется неорграф без циклов;

- обхватом цикла называется минимальная из длин циклов неорграфа.

Пусть $G=(X,A)$ - орграф.

Определение 11

- Путем называется маршрут все дуги которого различны;

- контуром называется путь, если $x_1=x_{n+1}$;

- бесконтурным называется орграф, не имеющий контуров.

Обозначение: $\mu=(x_1,x_2,\dots,x_n)$ или $\mu=(a_1,a_2,\dots,a_k)$.

Вопрос 43. Достижимость. Связность.

Определение 12

- Неорграф G называется связным, если любые две несовпадающие его вершины соединены маршрутом;

- орграф G называется связным, если соответствующий ему неорграф является связным.

Определение 13

Орграф G называется сильно связным (сильным), если любые две несовпадающие его вершины соединены по крайней мере одним маршрутом.

Определение 14

Всякий максимальный по включению вершин (сильно) связный подграф данного графа называется его (сильной) компонентой связности или (сильной) связной компонентой.

Теорема

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

Определение 16

Вершина x_j достижима из вершины x_i в орграфе G, если существует путь из вершины x_i в вершину x_j.

Определение 17

Матрицей достижимости R орграфа G с n вершинами называется квадратная матрица размерности $n\times n$, элемент которой r_{ij} определяется следующим образом:

$$r_{ij}=\begin{cases}1, \text{если вершина } x_j \text{ достижима из } x_i;\\ 0, \text{в противном случае.}\end{cases}$$

Определение 18
Матрицей обратной достижимости (контрдостижимости) Q орграфа G

с n вершинами называется квадратная матрица размерности $n \times n$, элемент которой q_{ij} определяется следующим образом:

$$q_{ij} = \begin{cases} 1, \text{если из вершины} x_j \text{можно достичь вершину} x_i; \\ 0, \text{в противном случае.} \end{cases}$$

Утверждение

Рассмотрим матрицу $S=R*Q$,

где $*$ - поэлементное умножение матриц:

$s_{ij}=r_{ij} \cdot q_{ij}$.

Элемент $s_{ij}=1$ <=> $i=j$ или вершины x_i и x_j взаимно достижимы.

Вопрос 44. Понятие дерева. Остовное дерево.

Определение 1
- Неорграф G называется деревом, если он связен и не имеет циклов;

- орграф G называется деревом, если он связен, имеет одну вершину (корень), в которую не заходит ни одна дуга, а в остальные вершины заходит только по одной дуге в каждую.

Теорема 1

Любые две вершины дерева x_i и x_j связаны одной и только одной простой цепью.

Теорема 2

Дерево с n вершинами имеет $n-1$ ребро.

Свойства деревьев

- 1. Граф G', полученный из G в результате удаления любого ребра, не является деревом. То есть всякое ребро в дереве является *мостом*.
- 2. Граф G', полученный в результате добавления к G новой вершины x_i и ребра $\{x_i, x_j\}$, где x_j - некоторая вершина графа G, является деревом.
- 3. Дерево - минимальный связный граф, то есть граф, который не содержит подграфа, состоящего из всех его вершин и являющегося связным.

Определение 2
Несвязный (неориентированный) граф без циклов называется лесом.

Связные компоненты леса являются деревьями.

Определение 3
Остовным деревом (остовом) графа G называется любой его подграф, содержащий все вершины графа G и являющийся деревом.

Обозначение: T.

Определение 4
Для связного графа G, содержащего n вершин и m ребер, число $\gamma=m-n+1$ называется цикломатическим числом.

Вопрос 45. Построение дерева полного перебора.

Пусть $G=(X,A)$ - орграф.

Определение 5
- Построение дерева с помощью разбиения множества X на подмножества называется ветвлением;

- исходное множество X называется множеством нулевого уровня ветвления.

Определение 6
Дерево, с помощью которого представим процесс ветвления , называется деревом решений или деревом полного перебора.

Определение 7
Орграф называется взвешенным (нагруженным), если каждой его дуге a поставлено в соответствие число $l(a)$, называемое длиной дуги или ее весом.

Определение 8
Длиной пути нагруженного графа G называется сумма длин всех дуг, образующих этот путь.

Вопрос 46. Порядковая функция орграфа. Уровневый граф.

Пусть $G=(X,A)$ - орграф без контуров.

На множестве вершин X определим подмножества:

$$N_0=\{x_i \in X : \Gamma(x_i)=\varnothing\}$$

$$N_1=\{x_i \in X \setminus N_0 : \Gamma(x_i)\subseteq N_0\}$$

$$N_2=\{x_i \in X \setminus (N_0\cup N_1): \Gamma(x_i)\subseteq N_0\cup N_1\}$$

…

$$N_k = \{x_i \in X \setminus (\bigcup_{j=0}^{k-1} N_j) : \ \Gamma(x_i) \subseteq \bigcup_{j=0}^{k-1} N_j\}$$

где k - наименьшее число, такое, что

$$X \setminus (\bigcup_{j=0}^{k-1} N_j) = \varnothing$$

Определение 7

Множества $N_0, N_1, \ldots, N_k$ называются уровнями орграфа G.

Определение 8

Функция $\varphi(x_i)$, определенная на множестве вершин X орграфа G без контуров и ставящая в соответствие каждой вершине $x_i \in X$ номер уровня j, которому она принадлежит, называется порядковой функцией орграфа G.

На подмножествах *A* и *B* некоторого универсума / выполняются

тождества алгебры множеств:

1) $A \cup B = B \cup A$ коммутативность U;
2) $A \cap B = B \cap A$ коммутативность ∩;
3) $A \cup (B \cup C) = (A \cup B) \cup C$ ассоциативность U;
4) $A \cap (B \cap C) = (A \cap B) \cap C$ ассоциативность ∩;
5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ дистрибутивность ∩ относит U;
6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ дистрибутивность U относит ∩;
7) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ закон де Моргана;
8) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ закон де Моргана;
9) $A \cup \emptyset = A$;
10) $A \cap \emptyset = \emptyset$;
11) $A \cap U = A$;
12) $A \cup U = U$;
13) $A \cup \overline{A} = U$;
14) $A \cap \overline{A} = \emptyset$;
15) $A \cup A = A$;
16) $A \cap A = A$;
17) $A \cup (B \cap A) = A$ закон поглощения;
18) $A \cap (B \cup A) = A$ закон поглощения;
19) $\overline{\overline{A}} = A$

Приложение 2 (к Вопросу 23-25)

Таблица равносильностей

I. Основные равносильности:

1. $x \wedge x \equiv x$
2. $x \vee x \equiv x$

} законы идемпотентности

3. $x \wedge u \equiv x$
4. $x \vee u \equiv u$
5. $x \wedge л \equiv л$
6. $x \vee л \equiv x$
7. $x \wedge \bar{x} \equiv л$ - закон противоречия
8. $x \vee \bar{x} \equiv u$ - закон исключенного третьего
9. $\bar{\bar{x}} \equiv x$ - закон снятия двойного отрицания
10. $x \wedge (y \vee x) \equiv x$
11. $x \vee (y \wedge x) \equiv x$

} законы поглощения

II. Равносильности, выражающие одни логические операции через другие:

1. $x \leftrightarrow y \equiv (x \to y) \wedge (y \to x)$
2. $x \to y \equiv \bar{x} \vee y$
3. $\overline{x \wedge y} \equiv \bar{x} \vee \bar{y}$
4. $\overline{x \vee y} \equiv \bar{x} \wedge \bar{y}$

} Законы де Моргана

5. $x \wedge y \equiv \overline{\bar{x} \vee \bar{y}}$
6. $x \vee y \equiv \overline{\bar{x} \wedge \bar{y}}$

III. Равносильности выражающие основные законы алгебры логики:

1. $x \wedge y \equiv y \wedge x.$ -коммутативность конъюнкции;
2. $x \vee y \equiv y \vee x.$ - коммутативность дизъюнкции;
3. $x \wedge (y \wedge z) \equiv (x \wedge y) \wedge z.$ - ассоциативность конъюнкции;
4. $x \vee (y \vee z) \equiv (x \vee y) \vee z.$ - ассоциативность дизъюнкции;
5. $x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z).$ - дистрибутивность конъюнкции относительно дизъюнкции;
6. $x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z).$ - дистрибутивность дизъюнкции относительно конъюнкции;