Дискретная математика

Материал лекций для студентов 2 курса специальности 09.02.07 Информационные системы и программирование

Литература

- *М. С. Спирина, П. А. Спирин. Дискретная математика. – М. : Асабета. 2018.*
- *С. А. Канцедал. Дискретная математика. – М. : И. Д. «Форум» - ИНФРА-М. 2017.*
- *Б. М. Владимирский и др. Математика. – СПб. : Лань. 2020.*
- *Ф. И. Кострикин. Введение в алгебру. – М. : Наука. 1977.*
- *Э. Фрид. Элементарное введение в абстрактную алгебру. – М. : Мир. 1979.*
- *Р. Басакер, Т. Саати. Конечные графы и сети. – М. : Наука. 1974.*

Литература

- *Н. Угринович, Л. Босова, Н. Михайлова. Практикум по информатике и информационным технологиям. - М. : Лаборатория базовых знаний. 2018.*
- *М. В. Воронов, Г. П. Мещерякова. Математика для гуманитарных факультетов. – Ростов-на –Дону: феникс. 2019.*
- *О. Е. Акимов. Дискретная математика. Логика. Группы. Графы. – М. : Лаборатория базовых знаний. 2019.*

МАТЕМАТИЧЕСКАЯ ЛОГИКА. ФОРМАЛЬНАЯ ЛОГИКА.

Основные понятия

- ***Логика*** *– наука, изучающая законы и формы мышления; учение о способах рассуждений и доказательстве.*

  Законы мира, сущность предметов, общее в них мы познаем посредством абстрактного мышления. Основными формами абстрактного мышления являются понятия, суждения и умозаключения.
- ***Понятие*** *– форма мышления, в которой отражаются существенные признаки отдельного предмета или класса однородных предметов.*

  Понятия в языке выражаются словами.
- ***Содержание понятия*** *– совокупность существенных признаков, отражённых в этом понятии.*
- ***Объём понятия*** *– множество предметов, каждому из которых принадлежат признаки, составляющие содержание понятия.*

Основные понятия

- ***Суждение*** *– форма мышления, в которой что-либо утверждается или отрицается о предмете, признаках или их отношениях.*
- ***Умозаключение*** *– форма мышления, посредством которой из одного или нескольких суждений, называемых посылками, мы по определённым правилам вывода получаем суждение, которое называется заключением.*

  Если некоторые события обязательно имеют место при определённом условии, то это является достаточным.

  Если некоторое событие не может иметь место без определённого условия, то это условие является необходимым.

Алгебра высказываний (Булева алгебра)

- ***Алгебра*** *– наука об общих операциях, аналогичных сложению и умножению, которые могут выполняться не только над цифрами, но и над другими математическими объектами.*

  В Булевой алгебре – алгебре логики – объектами являются высказывания.

- ***Высказывание*** *– любое предложение какого-либо языка, содержание которого можно определить как истинное или ложное.*

  В естественном языке высказывания выражаются повествовательными предложениями. Восклицательные и вопросительные предложения высказываниями не являются.

  Высказывание называется простым, если никакая его часть сама не является высказыванием. Высказывание, состоящие из простых высказываний, называется сложным или составным.

  Истинному высказыванию ставится в соответствие 1 логическое значение истина; ложному высказыванию – 0 или ложь.

Основные логические операции

- *КОНЪЮНКЦИЯ – логическое умножение. Если хотя бы одно из высказываний ложно, то ложна и их конъюнкция.*
- *и (рус.), and (англ.), &, ^*

a	b	a & b
0	0	0
0	I	0
I	0	0
I	I	I

Основные логические операции

- *ДИЗЪЮНКЦИЯ – логическое сложение. Если хотя бы одно из высказываний истинно, то истинна и их дизъюнкция.*
- *или (рус.), are (англ.), v*

a	b	a v b
0	0	0
0	I	I
I	0	I
I	I	I

Основные логические операции

- *ИНВЕРСИЯ – логическое отрицание.*
- *не (рус.), **not** (англ.)*

a	***not a***
0	1
1	0

Основные логические операции

- *ИМПЛИКАЦИЯ – если a, то b. Из лжи следует всё, из истинны следует только истина.*

a	b	a =>b
0	0	I
0	I	I
I	0	0
I	I	I

Основные логические операции

- *ЭКВИВАЛЕНЦИЯ – тогда и только тогда.*

a	b	a<=>b
0	0	I
0	I	0
I	0	0
I	I	I

Основные логические операции

- *ШТРИХ ШЕФФЕРА – не и.*

a	**b**	***a|b***
0	0	I
0	I	I
I	0	I
I	I	0

Основные логические операции

- *СТРЕЛКА ПИРСА – не или.*

a	b	$a \downarrow b$
0	0	I
0	I	0
I	0	0
I	I	0

Основные логические операции

- РАЗНОСТЬ

a	b	$a - b$
0	0	0
0	I	0
I	0	I
I	I	0

- ПРЯМАЯ СУММА

a	b	$a \oplus b$
0	0	0
0	I	I
I	0	I
I	I	0

Основные логические операции

- *Логические действия в составном высказывании выполняются в порядке приоритета; наивысший приоритет у инверсии.*

Логические выражения и таблицы истинности

- *Таблицу, показывающую какое значение принимает составное высказывание при любом из возможных наборов значений входящего в него простого высказывания, называют таблицей истинности составного высказывания.*

Алгоритм построения таблицы истинности

1) Сосчитать количество входящих в составное высказывание простых высказываний n.
2) Определить количество строк в таблице $m=2^n$
3) Подсчитать количество логических операций в формуле. Установить последовательность действий с учётом скобок и приоритетов.
4) Определить количество столбцов в таблице (число переменных + число операций)
5) Заполнить первые n столбцов, соответствующих переменным.
6) Поочерёдно заполнить столбцы, соответствующие операциям.

Пример

a	b	c	1	2	3	4	5	6	7	8	9
0	0	0									
0	0	1									
0	1	0									
0	1	1									
1	0	0									
1	0	1									
1	1	0									
1	1	1									

Пример

a	b	c	d	1	2	3	4	5	6	7	8	9							
0	0	0	0																
0	0	0	1																
0	0	1	0																
0	0	1	1																
0	1	0	0																
0	1	0	1																
0	1	1	0																
0	1	1	1																
1	0	0	0																
1	0	0	1																
1	0	1	0																
1	0	1	1																
1	1	0	0																
1	1	0	1																
1	1	1	0																
1	1	1	1																

Законы алгебры логики

название	для И	для ИЛИ
двойного отрицания	$\overline{\overline{A}} = A$	
исключения третьего	$A \cdot \overline{A} = 0$	$A + \overline{A} = 1$
операции с константами	$A \cdot 0 = 0, \;\; A \cdot 1 = A$	$A + 0 = A, \;\; A + 1 = 1$
повторения	$A \cdot A = A$	$A + A = A$
поглощения	$A \cdot (A + B) = A$	$A + A \cdot B = A$
переместительный	$A \cdot B = B \cdot A$	$A + B = B + A$
сочетательный	$A \cdot (B \cdot C) = (A \cdot B) \cdot C$	$A + (B + C) = (A + B) + C$
распределительный (дистрибутивный)	$A + B \cdot C = (A + B) \cdot (A + C)$	$A \cdot (B + C) = A \cdot B + A \cdot C$
правила де Моргана	$\overline{A \cdot B} = \overline{A} + \overline{B}$	$\overline{A + B} = \overline{A} \cdot \overline{B}$

Упрощение логических выражений

Шаг 1. Заменить операции $\oplus \rightarrow \leftrightarrow$ на их выражения через **И**, **ИЛИ** и **НЕ**:

$$A => B = \bar{A} \vee B;$$
$$A <=> B = A \& B \vee \bar{A} \& \bar{B} = (\bar{A} \vee B) \& (A \vee \bar{B});$$
$$A \downarrow B = \bar{A} \& \bar{B};$$
$$A \mid B = \bar{A} \vee \bar{B};$$
$$A - B = \overline{(A => B)};$$
$$A + B = \overline{(A <=> B)};$$

Шаг 2. Раскрыть инверсию сложных выражений по формулам де Моргана:

Шаг 3. Используя законы логики, упрощать выражение, стараясь применять закон исключения третьего.

Упрощение логических выражений

$$X = (B \to A) \cdot \overline{(A + B)} \cdot (A \to C)$$

раскрыли →

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

формула де Моргана

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

распределительный

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

исключения третьего

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

повторения

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

поглощения

$$= \overline{B} \cdot \overline{A}$$

Решение логических задач

Дизъюнктивные и конъюнктивные нормальные формы

- *Элементарной конъюнкцией называется логическое произведение различных логических переменных или их отрицаний.*
- *Элементарной дизъюнкцией называется логическая сумма различных логических переменных или их отрицаний.*
- *Дизъюнктивной нормальной формой (ДНФ) называется произвольная дизъюнкция элементарных конъюнкций.*

  Число входящих в ДНФ конъюнкций называется длиной ДНФ.

  Если длина равна нулю, то ДНФ называется пустой и равной тождественно ложному выражению.
- *Конъюнктивной нормальной формой (КНФ) называется произвольная конъюнкция различных элементарных дизъюнкций.*

Алгоритм построения нормальных форм с помощью логических преобразований

1. Избавляемся от импликации, эквиваленции, стрелки Пирса, штриха Шеффера по формулам

$A => B = \bar{A} \vee B$;

$A <=> B = A \& B \vee \bar{A} \& \bar{B} = (\bar{A} \vee B) \& (A \vee \bar{B})$;

$A \downarrow B = \bar{A} \& \bar{B}$;

$A \mid B = \bar{A} \vee \bar{B}$;

$A - B = \overline{(A => B)}$;

$A + B = \overline{(A <=> B)}$;

2. *С помощью правил Де Моргана преобразовываем полученное выражение так, чтобы знак отрицания стоял только над булевыми переменными, но не над действиями.*

3. *При построении дизъюнктивной нормальной формы (ДНФ) формула, полученная после второго шага, преобразуется с помощью первого дистрибутивного закона, а при построении КНФ – с помощью второго дистрибутивного закона.*

Совершенные нормальные формы (СНФ)

Пусть в логическую функцию входит n переменных или их отрицаний.

Дизъюнктивная нормальная форма называется совершенной, если ранг каждой её элементарной конъюнкции равен n. (СДНФ)

Аналогично определяем совершенную конъюнктивную нормальную форму (СКНФ).

Для каждой, отличной от тождественного нуля булевой функции, существует её совершённая дизъюнктивная нормальная форма.

Для каждой, отличной от тождественной единицы булевой функции, существует её совершённая дизъюнктивная нормальная форма.

Первый метод *- с помощью логических преобразований:*

Вначале по алгоритму строим нормальную форму, а затем добавляем к каждой элементарной конъюнкции (дизъюнкции) недостающие переменные с помощью законов исключения констант, противоречия и исключенного третьего и, применяя дистрибутивный закон, получаем совершенную нормальную форму.

- Пример: учебник Спириной М.С., стр. 173

Второй метод - *с помощью таблицы истинности:*

СКНФ строим по «нулям» таблицы истинности функции.

СДНФ строим по «единицам».

Построение СДНФ

A	B	X	
0	0	1 •	$\overline{A} \cdot \overline{B}$
0	1	1 •	$\overline{A} \cdot B$
1	0	0	
1	1	1 •	$A \cdot B$

Шаг 1. Отметить строки в таблице, где **X = 1**.

Шаг 2. Для каждой из них записать логическое выражение, которое истинно только для этой строки.

Шаг 3. Сложить эти выражения и упростить результат.

распределительный

$$X = \overline{A} \cdot \overline{B} + \overline{A} \cdot B + A \cdot B = \overline{A} \cdot (\overline{B} + B) + A \cdot B$$

$$= \overline{A} + A \cdot B = (\overline{A} + A) \cdot (\overline{A} + B) = \overline{A} + B$$

исключения третьего

распределительный

исключения третьего

Построение СКНФ

A	B	X
0	0	1
0	1	1
1	0	0
1	1	1

$A \cdot \overline{B}$

Шаг 1. Отметить строки в таблице, где **X = 0**.

Шаг 2. Для каждой из них записать логическое выражение, которое истинно только для этой строки.

Шаг 3. Сложить эти выражения и упростить результат, который равен $\overline{X}$.

Шаг 4. Сделать инверсию.

$$\overline{X} = A \cdot \overline{B} \Rightarrow X = \overline{A \cdot \overline{B}} = \overline{A} + B$$

Когда удобнее применять 2-ой способ?

Пример. Построение СДНФ.

A	B	C	X	
0	0	0	1 •	$\overline{A}\cdot\overline{B}\cdot\overline{C}$
0	0	1	1 •	$\overline{A}\cdot\overline{B}\cdot C$
0	1	0	1 •	$\overline{A}\cdot B\cdot\overline{C}$
0	1	1	1 •	$\overline{A}\cdot B\cdot C$
1	0	0	0	
1	0	1	1 •	$A\cdot\overline{B}\cdot C$
1	1	0	0	
1	1	1	1 •	$A\cdot B\cdot C$

$$X=\overline{A}\cdot\overline{B}\cdot\overline{C}+\overline{A}\cdot\overline{B}\cdot C$$
$$+\overline{A}\cdot B\cdot\overline{C}+\overline{A}\cdot B\cdot C$$
$$+A\cdot\overline{B}\cdot C+A\cdot B\cdot C$$
$$=\overline{A}\cdot\overline{B}\cdot(\overline{C}+C)$$
$$+\overline{A}\cdot B\cdot(\overline{C}+C)$$
$$+A\cdot C\cdot(\overline{B}+B)$$
$$=\overline{A}\cdot\overline{B}+\overline{A}\cdot B+A\cdot C$$
$$=\overline{A}\cdot(\overline{B}+B)+A\cdot C$$
$$=\overline{A}+A\cdot C$$
$$=(\overline{A}+A)\cdot(\overline{A}+C)=\overline{A}+C$$

Пример. Построение СКНФ.

A	B	C	X	
0	0	0	1	
0	0	1	1	
0	1	0	1	
0	1	1	1	
1	0	0	0 •	$A \cdot \overline{B} \cdot \overline{C}$
1	0	1	1	
1	1	0	0 •	$A \cdot B \cdot \overline{C}$
1	1	1	1	

$$\overline{X} = A \cdot \overline{B} \cdot \overline{C} + A \cdot B \cdot \overline{C}$$

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

$$= A \cdot \overline{C}$$

$$X = \overline{A \cdot \overline{C}} = \overline{A} + C$$

Полином Жегалкина

Элементарная конъюнкция называется монотонной, если она не содержит отрицаний переменных.

Полиномом Жегалкина называется сумма по модулю два или прямая сумма попарно различных монотонных элементарных конъюнкций.

Метод неопределённых коэффициентов

Этим методом пользуются тогда, когда функция задана своей таблицей истинности.

Для функции, содержащей n логических переменных, записывается общий вид с 2^n неопределенными коэффициентами.

$$f=a_0 \oplus a_1 A \oplus a_2 B \oplus a_3 C \oplus a_4 D \oplus a_{12} A\&B \oplus a_{13} A\&C \oplus a_{14} A\&D \oplus a_{23} B\&C \oplus a_{24} B\&D \oplus a_{34} C\&D \oplus a_{123} A\&B\&C \oplus a_{124} A\&B\&D \oplus a_{134} A\&C\&D \oplus a_{234} B\&C\&D \oplus a_{1234} A\&B\&C\&D$$

Пример

a	b	c	d	f
0	0	0	0	I
0	0	0	I	0
0	0	I	0	0
0	0	I	I	0
0	I	0	0	I
0	I	0	I	I
0	I	I	0	0
0	I	I	I	0
I	0	0	0	0
I	0	0	I	0
I	0	I	0	I
I	0	I	I	0
I	I	0	0	I
I	I	0	I	0
I	I	I	0	0
I	I	I	I	I

Решение

$$
\begin{cases}
a_0 = 1 \\
a_0 + a_4 = 0 \\
a_0 + a_3 = 0 \\
a_0 + a_3 + a_4 + a_{34} = 0 \\
a_0 + a_2 = 1 \\
a_0 + a_2 + a_4 + a_{24} = 1 \\
a_0 + a_2 + a_3 + a_{23} = 0 \\
a_0 + a_2 + a_3 + a_4 + a_{23} + a_{24} + a_{34} + a_{234} = 0 \\
a_0 + a_1 = 0 \\
a_0 + a_1 + a_4 + a_{14} = 0 \\
a_0 + a_1 + a_3 + a_{13} = 1 \\
a_0 + a_1 + a_3 + a_4 + a_{13} + a_{14} + a_{34} + a_{134} = 0 \\
a_0 + a_1 + a_2 + a_{12} = 1 \\
a_0 + a_1 + a_2 + a_4 + a_{14} + a_{12} + a_{24} + a_{124} = 0 \\
a_0 + a_1 + a_2 + a_3 + a_{12} + a_{13} + a_{23} + a_{123} = 0 \\
a_0 + a_1 + a_2 + a_3 + a_4 + a_{12} + a_{13} + a_{14} + a_{23} + a_{24} + a_{34} + a_{123} + a_{124} + a_{134} + a_{234} + a_{1234} = 1
\end{cases}
$$

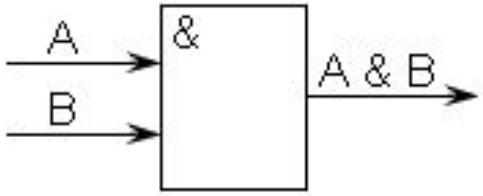
Ответ

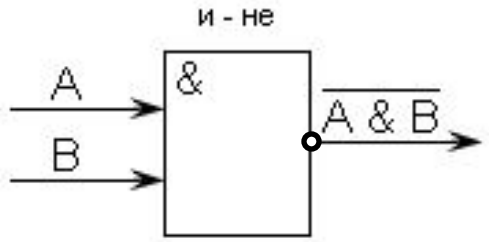
$$
\begin{cases}
a_0 = 1 \\
a_1 = 1 \\
a_2 = 0 \\
a_3 = 1 \\
a_4 = 1 \\
a_{12} = 1 \\
a_{13} = 0 \\
a_{14} = 1 \\
a_{23} = 1 \\
a_{24} = 1 \\
a_{34} = 1 \\
a_{123} = 1 \\
a_{124} = 0 \\
a_{134} = 0 \\
a_{234} = 1 \\
a_{1234} = 0
\end{cases}
$$

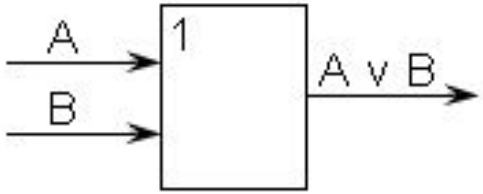
*Ответ: f=**1**⊕A ⊕ C ⊕ D⊕A&B⊕A&D ⊕ B&C ⊕ B&D ⊕ C&D⊕A&B&C⊕B&C&D*

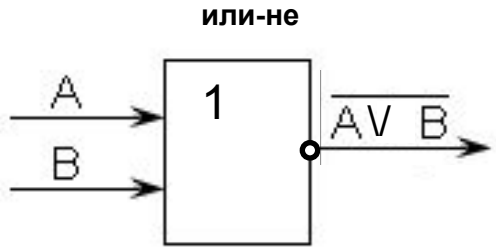
Комбинационные схемы

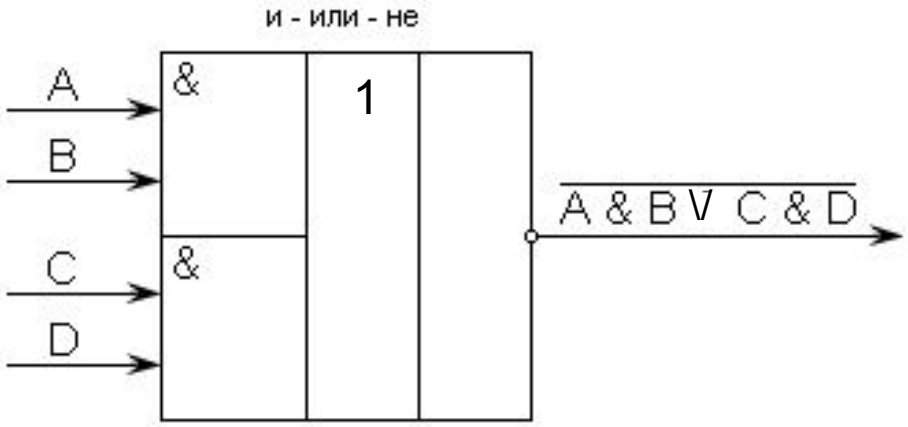
Комбинационная схема – электронная схема, реализующая какую-либо Булеву функцию, то есть если на вход схемы подать какую-нибудь комбинацию нулей и единиц (обычно 0 и 1 – различные уровни напряжения), то на выходе схемы появится напряжение, соответствующее значению логических функций на заданном наборе переменных.









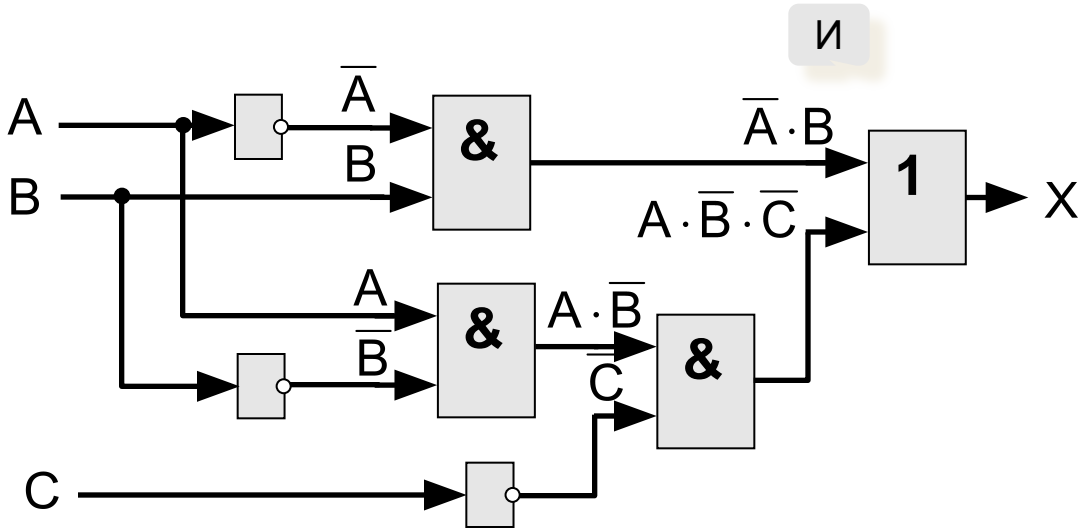


На этих элементах реализуют минимизированные нормальные формы (МНФ).

Составление схем

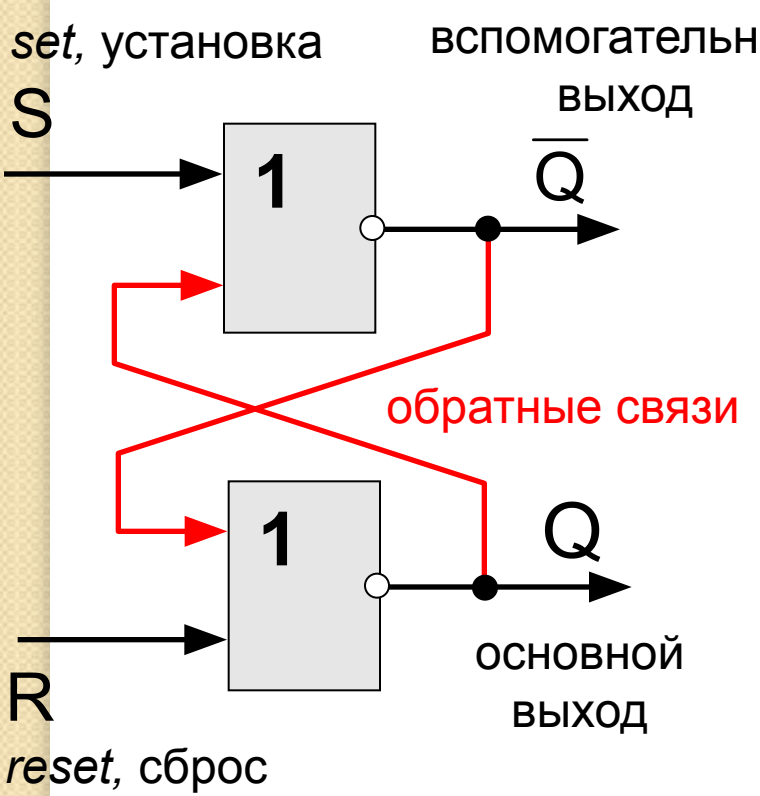
последняя операция - ИЛИ

$$X = \overline{A} \cdot B + A \cdot \overline{B} \cdot \overline{C}$$



Триггер (англ. *trigger* – защёлка)

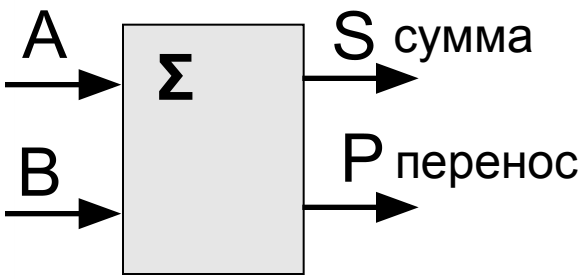
Триггер – это логическая схема, способная хранить 1 бит информации (1 или 0). Строится на 2-х элементах **ИЛИ-НЕ** или на 2-х элементах **И-НЕ.**



S	R	Q	$\overline{Q}$	режим
0	0	Q	$\overline{Q}$	**хранение**
0	1	0	1	**сброс**
1	0	1	0	**установка 1**
1	1	1	1	**запрещен**

Полусумматор

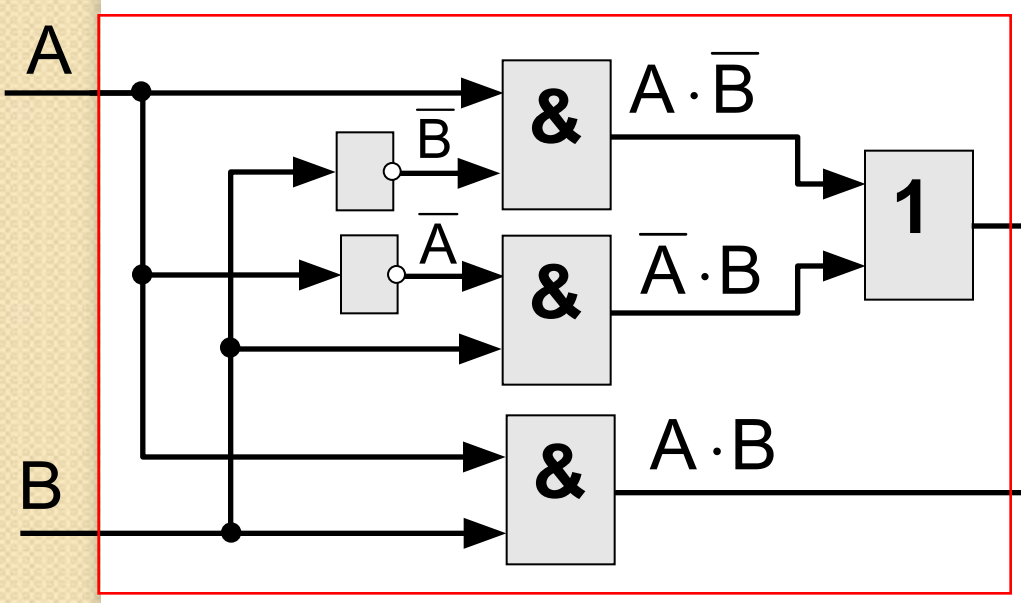
Полусумматор – это логическая схема, способная складывать два одноразрядных двоичных числа.



$$P = A \cdot B$$

$$S = A \oplus B = A \cdot \overline{B} + \overline{A} \cdot B$$

A	B	P	S
0	0	0	0
0	1	0	1
0	0	0	1
0	1	1	0

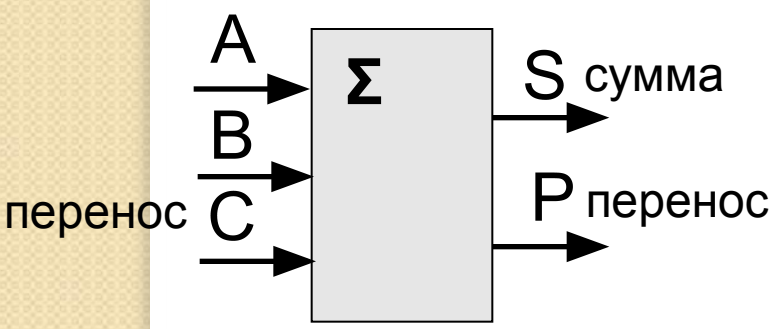


$$S = A \cdot \overline{B} + \overline{A} \cdot B$$

Схема на 4-х элементах?

Сумматор

Сумматор – это логическая схема, способная складывать два одноразрядных двоичных числа с переносом из предыдущего разряда.



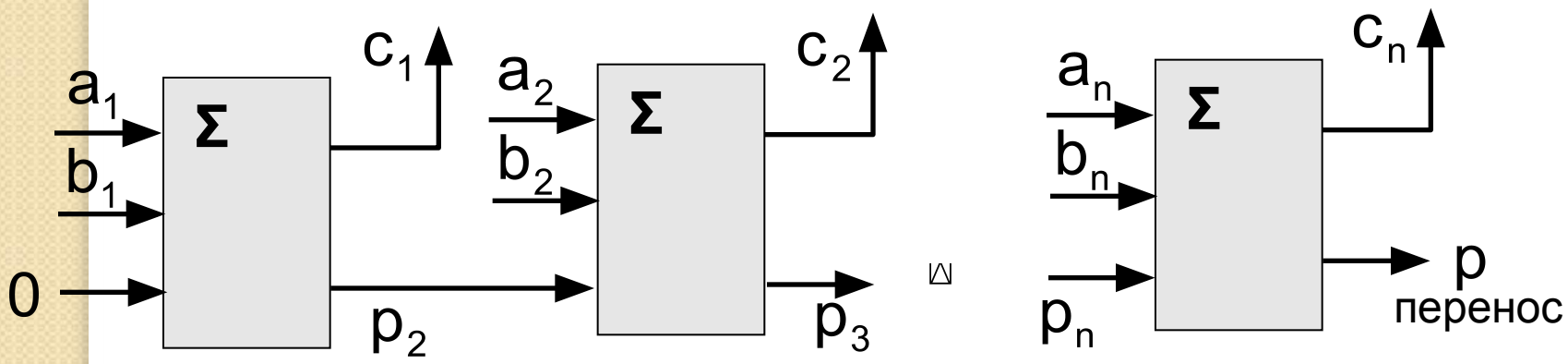
A	B	C	P	S
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Многоразрядный сумматор

это логическая схема, способная складывать два n-разрядных двоичных числа.

$$
\begin{array}{rl}
 & A = \quad a_n \; a_{n-1} \; \square \; a_1 \\
+ & B = \quad b_n \; b_{n-1} \; \square \; b_1 \\
\hline
 & C = p \; c_n \; c_{n-1} \; \square \; c_1
\end{array}
$$

перенос



Переключательные схемы

В компьютерах и других автоматических устройствах широко применяются электрические схемы, содержащие сотни и тысячи переключательных элементов: реле, выключателей и т.п. Разработка таких схем весьма трудоёмкое дело. Оказалось, что здесь с успехом может быть использован аппарат алгебры логики.

Переключательная схема — это схематическое изображение некоторого устройства, состоящего из переключателей и соединяющих их проводников, а также из входов и выходов, на которые подаётся и с которых снимается электрический сигнал.

Каждый переключатель имеет только два состояния: замкнутое и разомкнутое. Переключателю X поставим в соответствие логическую переменную x, которая принимает значение 1 в том и только в том случае, когда переключатель X замкнут и схема проводит ток; если же переключатель разомкнут, то x равен нулю.

Будем считать, что два переключателя X и $\bar{X}$ связаны таким образом, что когда X замкнут, то $\bar{X}$ разомкнут, и наоборот. Следовательно, если переключателю X поставлена в соответствие логическая переменная x, то переключателю $\bar{X}$ должна соответствовать переменная $\bar{x}$.

Всей переключательной схеме также можно поставить в соответствие логическую переменную, равную единице, если схема проводит ток, и равную нулю — если не проводит. Эта переменная является функцией от переменных, соответствующих всем переключателям схемы, и называется функцией проводимости.

Найдем функции проводимости F некоторых переключательных схем:

а) 

Схема не содержит переключателей и проводит ток всегда, следовательно **F=1**;

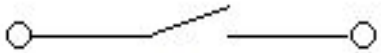
б) 

Схема содержит один постоянно разомкнутый контакт, следовательно **F=0**;

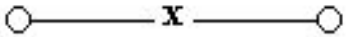
в) 

Схема проводит ток, когда переключатель x замкнут, и не проводит, когда x разомкнут, следовательно, **F(x) = x**;

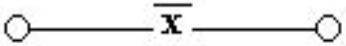
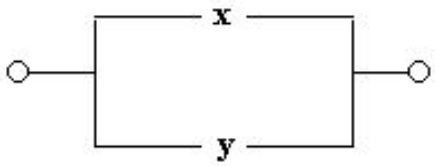
г) 

Схема проводит ток, когда переключатель x разомкнут, и не проводит, когда x замкнут, следовательно, **F(x) =** $\overline{x}$;

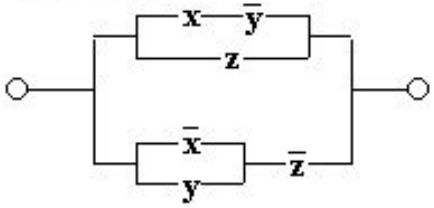
д)

Схема проводит ток, когда оба переключателя замкнуты, следовательно, **F(x) = x · y**;



е)

Схема проводит ток, когда хотя бы один из переключателей замкнут, следовательно, **F(x)=x v y;**



ж)

Схема состоит из двух параллельных ветвей и описывается функцией .

$$F(x, y, z) = (x \cdot \bar{y}) \vee z \vee (\bar{x} \vee y) \cdot \bar{z}$$

При рассмотрении переключательных схем возникают две основные задачи: **синтез и анализ схемы.**

СИНТЕЗ СХЕМЫ по заданным условиям ее работы сводится к следующим трём этапам:

составлению функции проводимости по таблице истинности, отражающей эти условия;

упрощению этой функции;

построению соответствующей схемы.

АНАЛИЗ СХЕМЫ сводится к

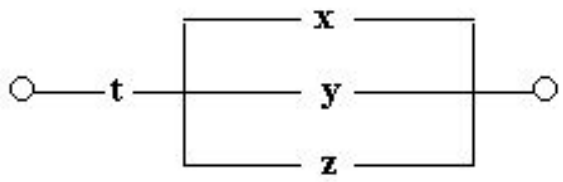
определению значений её функции проводимости при всех возможных наборах входящих в эту функцию переменных.

получению упрощённой формулы.

Примеры.

1. Построим схему, содержащую 4 переключателя x, y, z и t, такую, чтобы она проводила ток тогда и только тогда, когда замкнут контакт переключателя t и какой-нибудь из остальных трёх контактов.

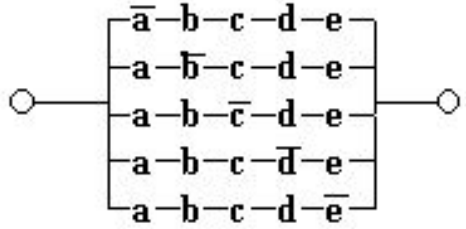
Решение. В этом случае можно обойтись без построения таблицы истинности. Очевидно, что функция проводимости имеет вид $F(x, y, z, t) = t \cdot (x \vee y \vee z)$, а схема выглядит так:



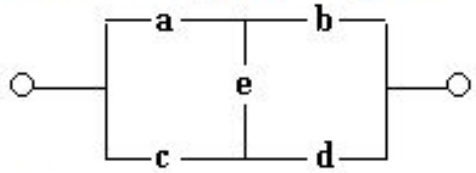
2. Построим схему с пятью переключателями, которая проводит ток в том и только в том случае, когда замкнуты ровно четыре из этих переключателей.

Решение : $F(a, b, c, d, e) = \bar{a} \cdot b \cdot c \cdot d \cdot e \vee a \cdot \bar{b} \cdot c \cdot d \cdot e \vee a \cdot b \cdot \bar{c} \cdot d \cdot e \vee a \cdot b \cdot c \cdot \bar{d} \cdot e \vee a \cdot b \cdot c \cdot d \cdot \bar{e}$

Схема имеет вид:

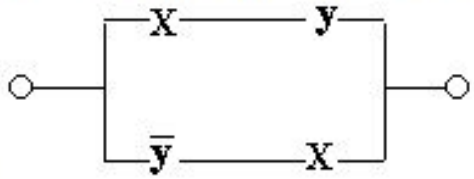


3. Найдем функцию проводимости схемы:



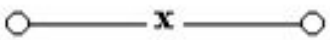
Решение. Имеется четыре возможных пути прохождения тока при замкнутых переключателях a, b, c, d, e : через переключатели a, b; через переключатели a, e, d; через переключатели c, d и через переключатели c, e, b. Функция проводимости **F(a, b, c, d, e) = a · b v a · e · d v c · d v c · e · b.**

4. Упростим переключательные схемы:

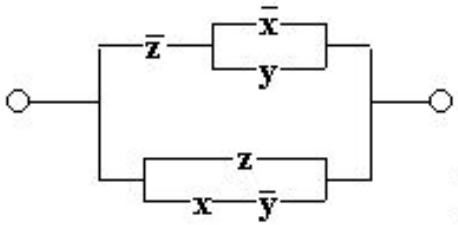


а)

Решение: $F(x, y) = x \cdot y \vee \bar{y} \cdot x = x \cdot (y \vee \bar{y}) = x \cdot 1 = x$

Упрощенная схема: 

б)

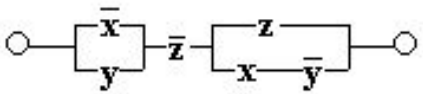


Решение : $F(x, y, z) = \bar{z} \cdot (\bar{x} \vee y) \vee (z \vee x \cdot \bar{y}) = 1$

Здесь первое логическое слагаемое $\bar{z} \cdot (\bar{x} \vee y)$ является отрицанием второго логического слагаемого $(z \vee x \cdot \bar{y})$, а дизъюнкция переменной с ее инверсией равна 1.

Упрощенная схема :

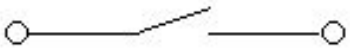
в)



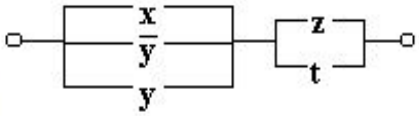
Решение : $F(x, y, z) = (\bar{x} \vee y) \cdot \bar{z} \cdot (z \vee x \cdot \bar{y}) = (\bar{x} \cdot \bar{z} \vee y \cdot \bar{z}) \cdot (z \vee x \cdot \bar{y}) =$

$= \bar{x} \cdot \bar{z} \cdot z \vee \bar{x} \cdot \bar{z} \cdot x \cdot \bar{y} \vee y \cdot \bar{z} \cdot z \vee y \cdot \bar{z} \cdot x \cdot \bar{y} = 0 \vee 0 \vee 0 \vee 0 = 0$

Упрощенная схема:

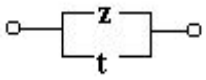


г)

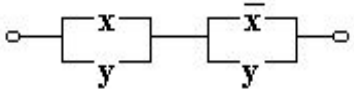


Решение : $F(x,y,z,t) = (x \vee \bar{y} \vee y) \cdot (z \vee t) = 1 \cdot (z \vee t) = z \vee t$

Упрощенная схема:

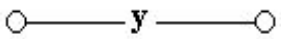


д)

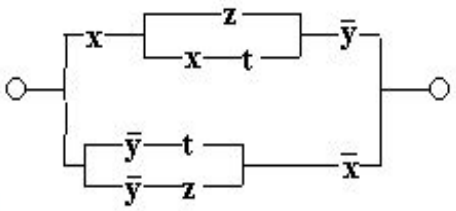


Решение : $F(x,y) = (x \vee y) \cdot (\bar{x} \vee y) = y$ (по закону склеивания)

Упрощенная схема:



е)

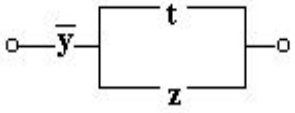


Решение:

$$F(x,y,z,t) = x \cdot (z \vee x \cdot t) \cdot \bar{y} \vee (\bar{y} \cdot t \vee \bar{y} \cdot z) \cdot \bar{x} = x \cdot \bar{y} \cdot z \vee x \cdot \bar{y} \cdot x \cdot t \vee \bar{x} \cdot \bar{y} \cdot (t \vee z) =$$

$$= x \cdot \bar{y} \cdot (z \vee t) \vee \bar{x} \cdot \bar{y} \cdot (t \vee z) = (t \vee z) \cdot (x \cdot \bar{y} \vee \bar{x} \cdot \bar{y}) = (t \vee z) \cdot \bar{y} \cdot (x \vee \bar{x}) = \bar{y} \cdot (t \vee z)$$

Упрощенная схема:



Минимизированные нормальные формы. Карты Карно.

Эти формы получают из СНФ путём исключения некоторых элементов конъюнкций.

Одним из наиболее простых и наглядных способов получения МНФ являются карты Карно.

X_3X_4 \ X_1X_2	00	01	11	10
00				
01				
11				
10				

Свойства карты Карно

- *При переходе от столбца к столбцу и от строки к строке меняется значение только одной логической переменной.*
- *Карта Карно являет собой цилиндр, как по вертикали, так и по горизонтали. Столбцы или строки можно переставлять циклически, то есть столбцы 10 и 00 также являются соседними.*

Алгоритм записи минимизированной функции с помощью карт Карно

- 1. Определить контуры по следующему правилу: в одну группу связываются те 2,4,8 (и т.д.) ячейки, содержащие единицы, которые находятся в левом и правом краях одной строки или в верхней и нижней частях одного столбца. Т.е. охватывается максимальное количество ячеек.

- 2. Для каждого контура записать конъюнкцию только тех переменных, которые при переходе от столбца к столбцу и от строки к строке не поменяли своего значения.
- 3. Сложить полученные конъюнкции. Таким образом будет записана минимальная ДНФ.

Для записи минимальной КНФ выполняются п.1-п.3 алгоритма, только контуры определяются по ячейкам, содержащим нули. И после записи дизъюнкции, выполняется инверсия.

Решение логических задач. Метод рассуждений

Задача 1. Министры иностранных дел России, США и Китая обсудили за закрытыми дверями проекты договора, представленные каждой из стран. Отвечая затем на вопрос журналистов: "Чей именно проект был принят?", министры дали такие ответы:

Россия — "Проект не наш (1), проект не США (2)";
США — "Проект не России (1), проект Китая (2)";
Китай — "Проект не наш (1), проект России (2)".

Один из них оба раза говорил правду; второй – оба раза говорил неправду, третий один раз сказал правду, а другой раз — неправду. Кто что сказал?

проект США (?)

	(1)	(2)
Россия	+	–
США	+	–
Китай		

проект Китая (?)

	(1)	(2)
Россия	+	+
США	+	+
Китай		

проект России (?)

	(1)	(2)
Россия	–	+
США	–	–
Китай	+	+

Решение логических задач. Табличный метод

Задача 2. Дочерей Василия Лоханкина зовут Даша, Анфиса и Лариса. У них разные профессии и они живут в разных городах: одна в Ростове, вторая – в Париже и третья – в Москве. Известно, что

- Даша живет не в Париже, а Лариса – не в Ростове,
- парижанка – не актриса,
- в Ростове живет певица,
- Лариса – не балерина.

- Много вариантов.
- Есть точные данные.

Париж	Ростов	Москва		Певица	Балерина	Актриса
0	**1**	**0**	Даша	**1**	**0**	**0**
1	**0**	**0**	Анфиса	**0**	**1**	**0**
0	**0**	**1**	Лариса	**0**	**0**	**1**

В каждой строке и в каждом столбце может быть только одна единица!

Задача Эйнштейна

Условие: Есть 5 домов разного цвета, стоящие в ряд. В каждом доме живет по одному человеку отличной от другого национальности. Каждый жилец пьет только один определенный напиток, курит определенную марку сигарет и держит животное. Никто из пяти человек не пьет одинаковые напитки, не курит одинаковые сигареты и не держит одинаковых животных.

Известно, что:

1. Англичанин живет в красном доме.
2. Швед держит собаку.
3. Датчанин пьет чай.
4. Зеленой дом стоит слева от белого.
5. Жилец зеленого дома пьет кофе.
6. Человек, который курит *Pallmall*, держит птицу.
7. Жилец среднего дома пьет молоко.
8. Жилец из желтого дома курит *Dunhill*.
9. Норвежец живет в первом доме.
10. Курильщик *Marlboro* живет около того, кто держит кошку.
11. Человек, который содержит лошадь, живет около того, кто курит *Dunhill*.
12. Курильщик *Winfield* пьет пиво.
13. Норвежец живет около голубого дома.
14. Немец курит *Rothmans*.
15. Курильщик *Marlboro* живет по соседству с человеком, который пьет воду.

Вопрос: У кого живет рыба?

Решение логических задач. Использование алгебры логики

Задача 3. Следующие два высказывания истинны:

1. Неверно, что если корабль **A** вышел в море, то корабль **C** – нет.
2. В море вышел корабль **B** или корабль **C**, но не оба вместе.

Определить, какие корабли вышли в море.

Решение:

… если корабль **A** вышел в море, то корабль **C** – нет. $A \to \overline{C} = 1$

1. Неверно, что если корабль **A** вышел в море, то корабль **C** – нет. $A \to \overline{C} = 0$ $\overline{A \to \overline{C}} = 1$

2. В море вышел корабль **B** или корабль **C**, но не оба вместе. $B \oplus C = 1$

$$\left(\overline{A \to \overline{C}}\right) \cdot (B \oplus C) = 1 \qquad \left(\overline{\overline{A} + \overline{C}}\right) \cdot (B \cdot \overline{C} + \overline{B} \cdot C) = 1$$

$$A \cdot C \cdot (B \cdot \overline{C} + \overline{B} \cdot C) = 1$$

$$A \cdot C \cdot \overline{B} = 1$$

$A = 1,\ B = 0,\ C = 1$

Использование алгебры логики

Задача 4. Когда сломался компьютер, его хозяин сказал «Память не могла выйти из строя». Его сын предположил, что сгорел процессор, а винчестер исправен. Мастер по ремонту сказал, что с процессором все в порядке, а память неисправна. В результате оказалось, что двое из них сказали все верно, а третий – все неверно. Что же сломалось?

Решение:

A – неисправен процессор, **B –** память, **C –** винчестер

хозяин: $B = 0,\ \overline{B} = 1$ сын: $A \cdot \overline{C} = 1$ мастер: $\overline{A} \cdot B = 1$

Если ошибся хозяин: $X_1 = \overline{\overline{B}} \cdot A \cdot \overline{C} \cdot \overline{A} \cdot B = 1$

Если ошибся сын: $X_2 = \overline{B} \cdot \overline{A \cdot \overline{C}} \cdot \overline{A} \cdot B = 1$

Если ошибся мастер: $X_3 = \overline{B} \cdot A \cdot \overline{C} \cdot \overline{\overline{A} \cdot B} = 1$

$X_3 = \overline{B} \cdot A \cdot \overline{C} \cdot (A + \overline{B}) = 1$

$X_3 = \overline{B} \cdot A \cdot \overline{C} = 1$

$A = 1$

$B = 0$

$C = 0$

В общем случае: $X_1 + X_2 + X_3 = 1$

Несколько решений!

Методы доказательств

При построении любой теории выдвигается несколько высказываний, истинность которых не нужно доказывать.

Эти доказательства называются аксиомами теории. Все те высказывания, которые могут быть выведены из аксиом путем логических преобразований называются теоремами.

Последовательность высказываний, каждое из которых либо является аксиомой, либо выводится из предыдущего высказывания называется доказательством теоремы.

Любую теорему можно записать в виде импликации A=>B.

A – посылка логического выражения,

B – следствие.

Посылка A –условие теоремы, следствие B – заключение.

Теорема верна, если эта импликация является тождественно истинным выражением.

Тождественно истинное выражение называется тавтология.

Тавтологии играет роль закона, определяющего правильность умозаключений. Некоторые тавтологии легли в основу методов доказательств.

Метод последовательных импликаций.

$A=>A_1=>A_2=>\ldots A_n=>B.$

В основу этого метода лег закон ценных высказываний или закон силлогизма.

(A=>C)&(C=>B)=>(A=>B)

Метод «от противного».

Метод основан на законе контрапозиции.

(A=>B)<=>(not(B)=>not(A))

Метод необходимого и достаточного.

(A=>B)<=>(A=>B)&(not(B)=>not(A))

Метод математической индукции

Предположим, что для каждого элемента $n \in N$ *выполняется некоторое утверждение* $M(n)$. *Предположим также, что мы располагаем правилом, позволяющим установить истинность утверждений* $M(i)$ *для данного* i *при условии, что утверждение* $M(k)$ *истинно для всех* $k < i$ *(в частности подразумевается, что мы можем проверить истинность* $M(1)$*).*

Тогда утверждение M(n) истинно для любого натурального n.

Пример:

Доказать, что

$$1 + 2 + 3 + \cdots + n = \sum_{i=0}^{n} i = \frac{n(n+1)}{2} = s(n)$$

Доказательство:

1. *Проверка утверждения для нескольких малых значений n.*

S(1)=1(1+1)/2=1

S(2)=1+2=2(2+1)/2=3*

2. *Предполагается, что формула справедлива для всех натуральных чисел ≤n.*
3. *Докажем, что утверждение справедливо для n+1:*

S(n+1)=1+2+3+…+n+(n+1)=s(n)+(n+1)=n(n+1)/2+(n+1)= =(n+1)(n/2+1)=(n+1)(n+2)/2=s(n+1);

Учебник с.271 задача 27 , с.273 задача 29

Д/З: с.287 №5.12 (в, г), 5.13 (в, г)

ТЕОРИЯ МНОЖЕСТВ

Теория множеств

Множество – совокупность объектов любой природы, воспринимаемой как единое целое. Объекты, составляющие множество, называются его элементами.

Любые два элемента множества должны быть существенно различны, то есть в одном множестве не могут содержаться два не различных элемента. Сами множества будем обозначать прописными латинскими буквами их элементы строчными. Запись обозначает: a является элементом множества A.

Если множество содержит конечное и небольшое количество элементов его можно задать простым перечислением.

$A = \{2,3,5\}$

Множество можно также задавать с помощью предикатов.

$B=\{x: P(x)\}$ *– множество B это множество элементов x таких что предикат P(x) истинен.*

Множество, не имеющее ни одного элемента, называется пустыми множеством и обозначается Ø.

Множество B называется подмножеством множества A, если любой элемент множества B в тоже время является элементом множества A.

$\varnothing \; B \subseteq A$

Если множество A имеется хотя бы один элемент не входящий в множество B то множество B называется собственным подмножеством множества A. $B \subset A$

Пустое множество является подмножеством любого множества.

$N \subset Z \subset R \subset C$

Два множества называются равными, если первое множество является подмножеством второго и второе является подмножеством первого.

$A=B <=> (A \subseteq B) \& (B \subseteq A)$

Множество, не являющееся счетным и имеющее минимальную мощность называется континуумом, его координатное число алеф-1.

Любое множество имеет как минимум два подмножества: пустое подмножество и самого себя. Эти подмножества называются несобственными.

Если множество конечно и содержит n элементов, то у него 2^n различных подмножеств.

Мощность множества характеризуется количеством его элементов, называется кардинальным числом множества и обозначается Card(A) или |A|.

Если во множестве конечное число элементов, то его мощность равна числу этих элементов.

Если число элементов бесконечно, но их можно пронумеровать, то есть поставить во взаимно однозначное соответствие со множеством натуральных чисел, то такое множество называется счетным и его мощность обозначается алеф-о.

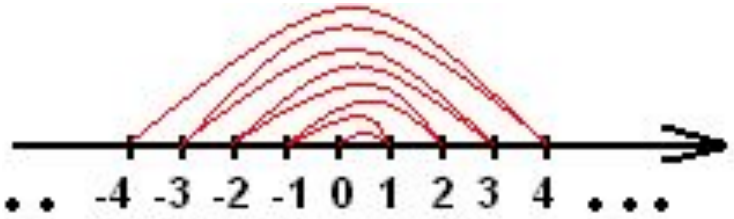
Конечное или счетное множество называется дискретным.

Теорема 1.

Множество целых чисел счетное.

Доказательство:

Нужно пронумеровать все элементы множества:



0=1

-1=2

1=3

-2=4

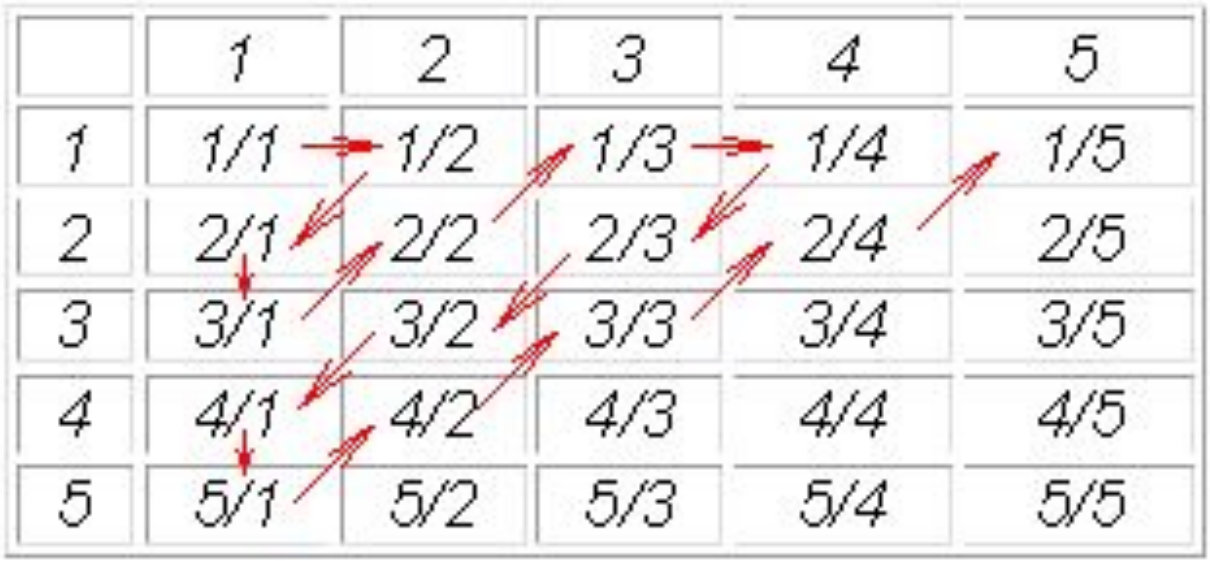
2=5

-3=6

Теорема 2.

Множество рациональных чисел счетное.

Доказательство:



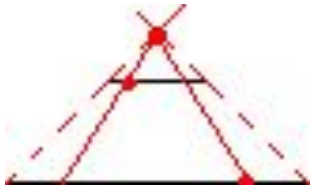
Теорема 3.

Мощность любого отрезка прямой равна мощности всей прямой.

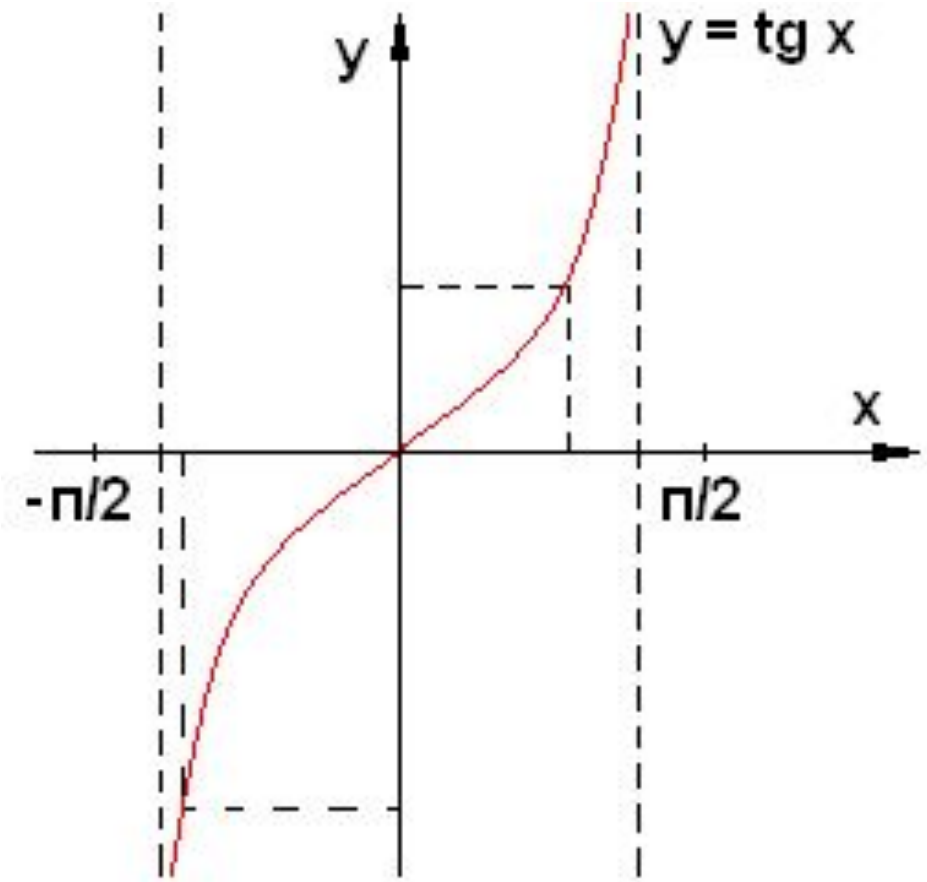
<u>Вспомогательная теорема (лемма)</u>:

Любые два отрезка равномощны:

1. *Если длины двух отрезков равны, то их можно наложить друг на друга при этом естественным образом устанавливается соответствие между точками отрезков.*
2. *Если один отрезок больше другого, то расположим их на параллельных прямых. Проведем лучи через концы отрезков. Точка пересечения этих лучей устанавливает соответствие между отрезками, а именно если через эту точку и произвольную точку первой прямой провести луч то он пересечет вторую прямую в какой-то точке, которая и будет соответствовать выбранной точке первой прямой. Аналогично можно провести луч через точку пересечения и произвольную точку второй прямой.*



Доказательство:



Действия над множествами.

$A \cup B$ – объединение множеств.

$A \cap B$ – пересечение множеств.

$A \setminus B$ – разность множеств.

$\bar{A} = U \setminus A$ – дополнение множества

$A \Delta B = (A \setminus B) \cup (B \setminus A)$ – симметричная разность

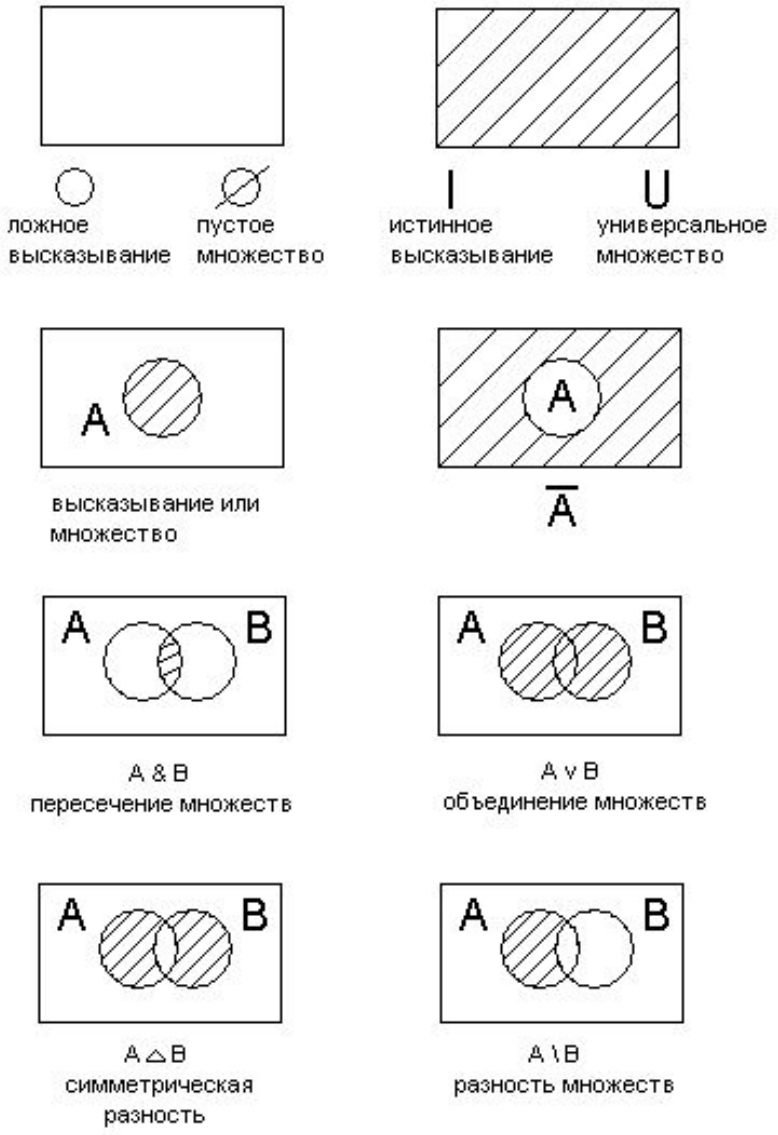
Декартово произведение двух множеств – *множество упорядоченных пар таких, что первый элемент пары – произвольный элемент первого множества, а второй элемент - второго.*

$$C = A \times B = \{(a, b) : (a \in A) \& (b \in B)\}$$

Если множество B равно множеству A, то мы можем говорить о декартовой степени множества.

$A^n = A \times A \times A \times \ldots \times A$ (n-раз)

Диаграммы Эйлера – Венна



Алгебра предикатов

Предикат – переменное высказывание, заданное на некотором множестве, причем значение высказывания (истинность или ложность) зависит от значений его аргументов. Количество аргументов называется местностью предиката.

P(x) – одноместный предикат;

Q(x,y) – двуместный предикат.

Всякий предикат определяет подмножество заданного множества, в каждой точке которого предикат принимает значение «истина».

С помощью операций конъюнкции, дизъюнкции и инверсии из исходного предиката можно построить новый предикат, следующим образом:

1. *Предикат* $R = \overline{P}$, *если на всех элементах заданного множества на котором предикат* P *истинен, предикат* R *– ложен.*
2. *Конъюнкция предикатов* P *и* Q, *определенная на одном и том же множестве* M. *Предикат* $R=P\&Q$ *истинен на любом элементе множества* M *тогда и только тогда, когда на этом элементе предикаты* P *и* Q *истинны.*
3. *Дизъюнкция предикатов* P *и* Q, *определенных на одном и том же множестве* M, *является предикат* $R=P \vee Q$, *истинный на любом элементе множества* M *тогда и только тогда, когда на этом элементе истинен либо предикат* P, *либо предикат* Q, *либо оба сразу.*

Помимо логических операций над предикатами в алгебре предикатов важную роль играют операции, которые называются кванторами.

∀ *- квантор всеобщности, (читается «для всех»).*

∃ *- квантор существования (читается «существует, найдется»).*

Операция кванторизации связывает одну переменную в предикат. После этой операции n-местный предикат становиться n-1-местным, а одноместный предикат становиться высказыванием.

Предикат P(x,y) – число x делится на число y без остатка.

ОТНОШЕНИЯ. ОТОБРАЖЕНИЯ.

Отношения

Для любых двух множеств X и Y всякое подмножество их декартовых произведений называется бинарным отношением между X и Y, а если y=x, то бинарным отношением на X.

Отношение эквивалентности

Бинарное отношение называется *отношением эквивалентности* (~) ($X \sim Y$), если выполняется три условия:

1. Рефлективность. $x \sim x$ (каждый элемент эквивалентен сам себе)
2. Симметричность. $x \sim x_1 \Rightarrow x_1 \sim x$
3. Транзитивность. $(x \sim x_1) \& (x_1 \sim x_2) \Rightarrow (x \sim x_2)$

Любое отношение эквивалентности, заданное на некотором множестве X, разбивает это множество на непересекающиеся классы эквивалентности, объединение которых дает все множество X.

Классы эквивалентности – это такие подмножества множества X, что любые два элемента, принадлежащие одному классу, эквивалентны между собой и любые два элемента, принадлежащие разным классам – не эквивалентны между собой, и наоборот.

Разбиение множества на несколько непересекающихся множеств, дающее в объединении все множество, определены некоторым отношением эквивалентности.

Множество классов эквивалентности – называется фактор-множеством множества M по отношению эквивалентности. M/~

Любой элемент класса эквивалентности полностью его определяет и называется представителем класса эквивалентности.

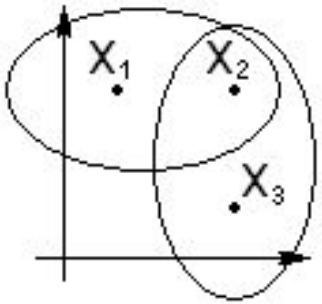
Антирефлективность – *в антирефлективных отношениях из условия, что* x_1 *и* x_2 *связаны отношением* R, *следует что* $x_1 \neq x_2$, *то есть* x_1, x_2 $R \Rightarrow x_1 \neq x_2$.

Асимметричность – *отношение* R, *заданное на множестве* M *называется ассиметричным, если - из этих двух соотношений* $(x_1;x_2) \in R$ *и* $(x_2;x_1) \in R$ *может выполняться не более одного.*

Антисимметричность – *отношение* R *называется антисимметричным, если оба эти соотношения* $(x_1;x_2) \in R$ *и* $(x_2;x_1) \in R$ *выполняются, то* $x_1 = x_2$.

Отношение толерантности

Рефлективное, симметричное и антитранзитивное отношение называется отношением толерантности.



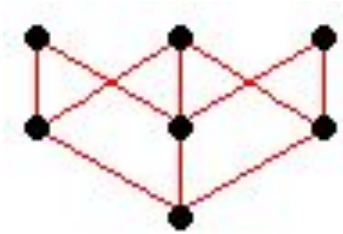
Отношение толерантности точек на плоскости – «отношение» - быть на расстоянии не менее, чем 1 сантиметра друг от друга.

Отношение порядка

Рефлективное, антисимметричное и транзитивное отношение называется отношением порядка.

Вместо $(x_1;x_2) \in R$ пишут $x_1 \le x_2$.

Если для любой пары элементов x_1, x_2 можно установить $x_1 \le x_2$ или $x_2 \le x_1$, то такое множество называется линейно-упорядоченным. Если этого установить нельзя то частично-упорядоченным.



Если x_i лежит ниже x_j и соединен с ней маршрутом

Наименьшее значение частично-упорядоченного множества, которое можно сравнить с любым другим элементом множества называется infimum.

$$x_0 = \inf M = \{x_0 : \forall x \in M \;\; x_0 \leq x\}$$

Наибольшим значением частично-упорядоченного множества называется superemum.

$$x_0 = \sup M = \{x_0 : \forall x \in M \;\; x \leq x_0\}$$

Максимальных или минимальных элементов в любом частично-упорядоченном множестве может быть несколько.

Наибольший или наименьший элемент, если существует, то единственный.

Антирефлективное, антисимметричное, транзитивное отношение называется отношением строго порядка.

Понятие отображения

Отображение играет центральную роль в математике.

Для заданных множеств X и Y отображение f сопоставляет каждому элементу множества X некоторый элемент множества Y.

Множество X называется областью определения. Все те элементы множества Y, в которое отображаются элементы множества X образуют подмножество множества Y, которое называется областью значений.

Символически отображение записывается следующим образом: f: X->Y, если элемент x отображается в элемент y, то это записывается так: f: $X \rightarrow Y$, $Y=f(x)$, $Y=fx$

Если множество Y совпадает с множеством X, то говорят, что это отображение преобразует X в себя.

Образом множества X при отображении f называется следующее подмножество множества X:

$$imf = \{f(x) \in Y : \forall x \in X\}$$

Прообразом элемента y при отображении f называется следующее подмножество множества X:

$$f^{-1}(y) = \{x \in X : f(x) = y\}$$

Отображение называют сюръективным, если образом отображения являются все множество Y, то есть у каждого элемента множества Y есть хотя бы один прообраз Im = Y

Отображение называется инъективным, если у каждого элемента множества Y не более одного прообраза, то есть если $x_1 \neq x_2$, то значит $f(x_1) \neq f(x_2)$

Отображение, одновременно являющееся и сюръективным и инъективным называется биективным или взамнооднозначным.

Единичное или тождественное отображение называется отображение, переводящее каждый элемент множества X сам в себя.

Композиции отображения

Рассмотрим два отображения

$G: X \to Y$

$F: Y \to Z$

Их произведение или суперпозицией называется отображение:

$(f \circ g): X \to Z \qquad f(g(x))$

Теорема№1.

Суперпозиция отображения ассоциативна.

$F \circ (g \circ h) = (f \circ g) \circ h$

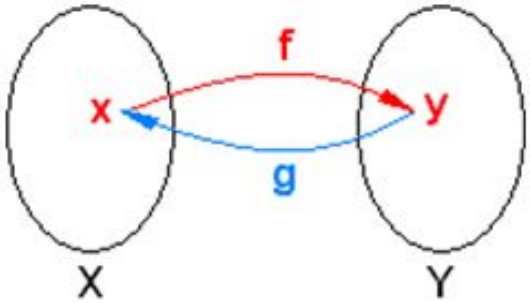
Если отображение f и g обладают следующими свойствами $f \circ g = e_x \quad g \circ f = e_y$, *то эти отображения называются взаимообратными.*

Теорема №2.

Отображение имеет обратное отображение тогда и только тогда, когда оно биективно.

Теорема №3.

*Если произведение f * g является тождественным отображением, то g инъективно, а f сюръективно.*



Доказательство:

1. *g – инъективно.*

Доказательство «от противного».

Предположим что g не является инъективным. Такого быть не может, потому что при отображении f y элемента x не может быть двух различных образов.

2. *f – сюръективно.*

При отображении g во множество x должен отображаться каждый элемент множества y, то есть каждый элемент множества y является образом хотя бы одного элемента множества x.

ТЕОРИЯ ГРУПП

Теория групп

Пусть имеется произвольное множество X.

$$a \in X, b \in X, c \in X$$

Бинарной операцией называется отображение $f: X \times X \to X$.

Таким образом, каждой паре элементов ставится в соответствие некий элемент $(a,b) \to C$. Это же соответствие можно написать также следующим образом $f(a,b)=c$; $a\ f\ b=c$.

Вообще говоря, на любом множестве X можно ввести множество различных операций. Эти операции будем обозначать $a \circ b$ или $a*b$; * - любая операция.

Например на множестве целых числе можно ввести такие операции:

$M \circ n=m+n-mn$

$M*n=-m+n$

Говорят, что операция f определяет на множестве X алгебраическую структуру, или, что упорядоченная пара (x,f) является алгебраической системой.

Бинарная операция называется ассоциативной, если

$a \circ (b \circ c)=(a \circ b) \circ c$

Бинарная операция называется коммутативной, если

$a \circ b=b \circ a$

Множества с заданной на нем бинарной ассоциативной операцией называются полугруппой.

Пусть задана алгебраическая система (X,o), элемент e x называется единичным, если

$\forall x \in X : e \circ x = x \circ e = X.$

Теорема:

Если в алгебраической системе существует единичный элемент, то он единственен.

Доказательство:

Докажем «от противного».

Пусть в алгебраической системе существует два различных единичных элемента e_1 *и* e_2, $e_1 \neq e_2$. *Перемножим эти два элемента. В результате получается:*

$e_1 * e_2 = e_2 = e_1$

следовательно e_1 *и* e_2 *одинаковые (противоречие).*

Полугруппа с единицей называется моноидом.

Элемент a моноида (X,o,e) называется обратимым, если найдется такой элемент на множестве X, что a o b=b o a=e.

Элемент b называется обратным элементом для элемента a и обозначается a^{-1}.

Элемент b естественно тоже обратим и $b^{-1}=a$, то есть $(a^{-1})^{-1}=a$.

Если каждый элемент моноида обратим, то такой моноид называется группой.

Группа с коммутативной операцией– Абелева группа.

Теорема: *если в полугруппе имеется левый единичный элемент и для каждого элемента существует левый обратный элемент, то все левые обратные элементы являются и правыми обратными элементами того же элемента, то есть просто обратными. Левый единичный элемент является правым элементом и значит просто единичным.*

Запишем условие теоремы в предикатах.

Обозначим полугруппу {G,o}

1) $\exists e \in G: \forall a \in G;$ E o a=a=>a o e=a

2) $\forall a \in G \exists b \in G: b \; o \; a = e \Rightarrow a \; o \; b = e$

Доказательство:

1. *Докажем сначала второе утверждение.*

Так как $b \circ a = e$, то, умножив это равенство на b получим:

$$b \circ a \circ b = e \circ b = b$$

По второму утверждению для любого элемента в том числе и для b имеется обратимый элемент. Пусть это элемент c.Умножим на c последнее равенство слева.

$$c \circ (b \circ a \circ b) = c \circ b = e$$

Так как множество c это полугруппа, то операция $\circ$ ассоциативна. Значит

$$(c \circ b) \circ (a \circ b) = e$$

$$e \circ (a \circ b) = e$$

$$a \circ b = e$$

что и требовалось доказать.

2. *Докажем первое утверждение.*

Мы уже доказали, что a o b=b o a=e, a=e o a=(a o b) o a

a(b o a)=a o e

Рассуждения называют теоретически-групповыми, если:

Нигде не обсуждается природа множества.

Нигде не обсуждается природа операций над множествами.

Элементы комбинаторики

1. *Размещение* к–предметов, отобранных из n-предметов является количеством способов отобрать из n-предметов к-предметов, причем отобранные множества предметов считаются различными, если они различаются хотя бы одним элементом или если все элементы одинаковы, то порядком их появления.

Число размещений из n-предметов по k-предметов обозначается A_n^k =n!/(n-k)!

2. *Перестановка* - размещение из n-предметов по n-предметов, то есть просто размещение всех предметов в ряд.

Количество перестановок n-предметов обозначается P_n=n!

3) *Сочетание*. Если при размещении k-предметов из n-предметов не учитывается порядок их появления, то есть два набора из k-предметов считается одинаковым, если их элементы совпадают, невзирая на порядок их появления, то такое количество наборов называется сочетанием из n по k и обозначается:

C_n^k =n!/(n-k)!/k!

Подстановки

Подстановкой или выполнением подстановки называется замена одной подстановки другой.

Подстановка обозначается заглавными латинскими буквами.

$$P = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Для того чтобы полностью определить подстановку нужно:

1. Определить конечное множество элементов, над которыми производится подстановка. Это конечное множество называется областью определения подстановки.
2. Определить алгоритм, по которому для какого-то элемента области определения подстановки можно указать элемент, в которой его переводит подстановка.

Если $a_i < 2{,}5$, то оно переводится в a_i+2, иначе a_i переводится в $5-a_i$

Две подстановки считаются одинаковыми, если их области определения совпадают и каждый элемент их совместной области определения переводится в один и тот же элемент.

Любые два столбика в подстановке можно поменять местами при этом получается одинаковые подстановки. Таким образом любую подстановку можно записать в следующем виде: в первой строке числа расположены строго по возрастанию.

$$P=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix}$$

$$Q=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{pmatrix}$$

Умножением подстановок называется их последовательное выполнение.

$$PQ=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$$

Исследуем упорядоченную пару множества подстановок и введенную в нем операцию умножения.

I. *Является ли эта пара алгебраической системой?*

   При умножении подстановок получается с той же областью определения. Значит эта пара является алгебраической системой.

2. *Является ли эта операция ассоциативной?*

$(PQ)R=P(QR)$

$$P=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$

$$Q=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

$$R=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$$

$$PQ=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

$$(PQ)R=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$$

$$QR=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$$

$$P(QR)=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$$

Подстановку P запишем в виде:

$$P=\begin{pmatrix}1 & 2 & 3 & 4\\ a1 & a2 & a3 & a4\end{pmatrix}$$

Переставляя местами столбцы, подстановки Q и R можно записать следующим образом:

$$Q=\begin{pmatrix}a1 & a2 & a3 & a4\\ b1 & b2 & b3 & b4\end{pmatrix}$$

$$R=\begin{pmatrix}b1 & b2 & b3 & b4\\ c1 & c2 & c3 & c4\end{pmatrix}$$

Отсюда очевидно, что умножение ассоциативно и это полугруппа.

1. *Имеется ли единичный элемент?*

$$e=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}=\begin{pmatrix}a1 & a2 & a3 & a4\\ a1 & a2 & a3 & a4\end{pmatrix}$$

$e*p=p*e=p$

значит это моноид.

2. *Существует ли для каждого элемента обратный элемент?*

$$P^{-1}=\begin{pmatrix}a1 & a2 & a3 & a4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

$P * P^{-1}=P^{-1} * P=e$

Является группой.

Разложение подстановок. Циклы и транспозиции.

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 8 & 7 & 2 & 0 & 9 & 1 & 4 & 6 \end{pmatrix}$$

Перепишем эту подстановку в другом виде.

$$P = \begin{pmatrix} 0 & 3 & 7 & 1 & 5 \\ 3 & 7 & 1 & 5 & 0 \end{pmatrix} \begin{pmatrix} 2 & 8 & 4 \\ 8 & 4 & 2 \end{pmatrix} \begin{pmatrix} 6 & 9 \\ 9 & 6 \end{pmatrix}$$

Будем считать, что все эти три подстановки имеют одну и ту же область определения, а те элементы, которые не указаны, переходят сами в себя.

Проверим, что исходные подстановки можно представить в виде произведения этих 3-х подстановок.

$$P_1 = \begin{pmatrix} 0 & 3 & 7 & 1 & 5 & 2 & 4 & 6 & 8 & 9 \\ 3 & 7 & 1 & 5 & 0 & 2 & 4 & 6 & 8 & 9 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 0 & 3 & 7 & 1 & 5 & 2 & 8 & 4 & 6 & 9 \\ 0 & 3 & 7 & 1 & 5 & 8 & 4 & 2 & 6 & 9 \end{pmatrix}$$

$$P_1 * P_2 = \begin{pmatrix} 0 & 3 & 7 & 1 & 5 & 2 & 4 & 6 & 8 & 9 \\ 3 & 7 & 1 & 5 & 0 & 8 & 2 & 6 & 4 & 9 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 6 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 7 & 8 \\ 9 & 6 & 0 & 1 & 2 & 3 & 4 & 5 & 7 & 8 \end{pmatrix}$$

$$P_1 * P_2 * P_3 = \begin{pmatrix} 0 & 3 & 7 & 1 & 5 & 2 & 4 & 6 & 8 & 9 \\ 3 & 7 & 1 & 5 & 0 & 8 & 2 & 9 & 4 & 6 \end{pmatrix}$$

В подстановках над одним и тем же множеством чисел первую строку можно сделать одинаковой для всех подстановок, а значит, ее можно не указывать.

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 8 & 7 & 2 & 0 & 9 & 1 & 4 & 6 \end{pmatrix} =$$

$$= (3 \quad 5 \quad 8 \quad 7 \quad 2 \quad 0 \quad 9 \quad 1 \quad 4 \quad 6) =$$

$$= \begin{pmatrix} 0 & 3 & 7 & 1 & 5 \\ 3 & 7 & 1 & 5 & 0 \end{pmatrix} \begin{pmatrix} 2 & 8 & 4 \\ 8 & 4 & 2 \end{pmatrix} \begin{pmatrix} 6 & 9 \\ 9 & 6 \end{pmatrix} =$$

$$= (0 \quad 3 \quad 7 \quad 1 \quad 5)(2 \quad 8 \quad 4)(6 \quad 9)$$

Обычно таким образом записывается разбиение подстановки на циклы.

Любой цикл можно представить в виде произведения циклов длины двух транспозиций.

$$(1\ \ 2\ \ 3\ \ 4\ \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$(2\ \ 1\ \ 3\ \ 4\ \ 5)$$

$$(2\ \ 3\ \ 1\ \ 4\ \ 5)$$

$$(2\ \ 3\ \ 4\ \ 1\ \ 5)$$

$$(2\ \ 3\ \ 4\ \ 5\ \ 1)$$

$$(1\ \ 2\ \ 3\ \ 4\ \ 5) = (1\ \ 2)(1\ \ 3)(1\ \ 4)(1\ \ 5)$$

Подгруппы

Рассмотрим множество вещественных чисел $(R,+)$ – это пара является группой.

$(Z,+)$ – тоже группа

$Z \leq R$

В тоже время, множество целых чисел является подмножеством рациональных чисел.

Группа целых чисел по операции сложения является подгруппой и группой вещественных чисел по операции сложения.

Две группы называются изоморфными, если между их множествами существуют взаимно однозначное соответствие (биекция) и операции соответствуют так, что если $a*b=c$, то $f(a)$ о $f(b)=f(c)$.

Теорема Кепи.

Любая конечная группа изоморфна группе подстановок.

Группа и конечные автоматы.

Что бы задать автомат, прежде всего нужно указать три множества:

1. *Множество сигналов на входе X.*
2. *Множество состояний a.*
3. *Множество сигналов на выходе Y.*

Кроме того необходимо задать две функции:

Одна функция: каждому сигналу на входе и каждому внутреннему состоянию ставит в соответствие новое внутреннее состояние,

А вторая функция: каждому сигналу на входе и каждому внутреннему состоянию ставит в соответствие определенный сигнал на выходе.

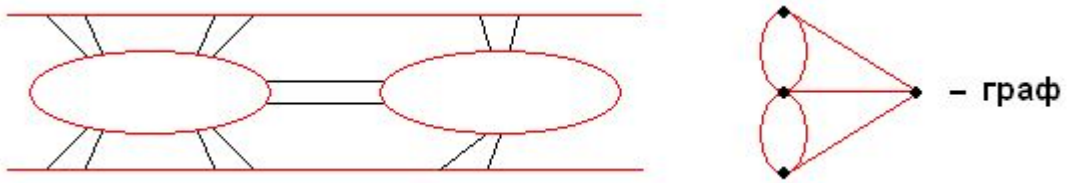
Функционирование автоматов можно изучать, описывая не только его реакцию на отдельные сигналы, подаваемые на вход, но и на серии сигналов. Это позволяет подходить к сигналам на входе, как к образующим свободные полугруппы. Сигналы на выходе также можно рассматривать, как образующие свободные полугруппы. Таким образом, свободные полугруппы позволяют сравнительно просто описывать работу автомата.

ТЕОРИЯ ГРАФОВ

Теория графов

Историческим началом теории графов явилась статья Леонардо Эйлера, вышедшая в 1736 году. В ней разбиралась задача о Кенигсбергских мостах.

ЗАДАЧА:



Можно ли, отправившись в путь с одного из островов или какого-либо берега реки, обойти оба острова и оба берега, пройдя по каждому мосту ровно один раз и вернуться в исходную точку?

ОТВЕТ: нельзя.

Графом называется упорядоченная пара (G,U).

Множество G называется множеством вершин графа, множество U - подмножество декартового произведения U≤G×G – множество ребер графа. Если множество U это множество упорядоченных пар, то есть в каждую вершину ребро входит либо входит либо выходит из вершины, то граф называется ориентированным графом или орграфом.

Если среди множества U имеются пары вида (V,V), то есть ребро, которое выходит из вершины и возвращается в нее, то такое ребро называют петлей, а граф называют графом с петлями. Если во множестве U есть повторяющиеся элементы, то граф называется графом с кратными ребрами.

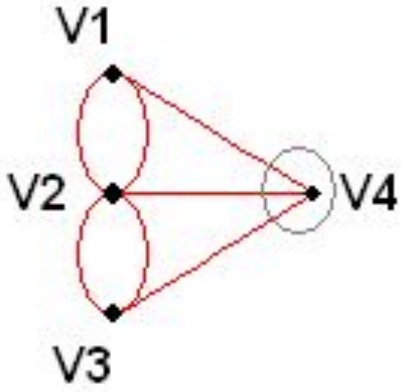
Если какую-либо пару вершин соединяет больше одного ребра, то такой граф называют мультиграфом.

Множество U удобно задавать в виде матрицы смежности для неориентированного графа или матрицы инциденций – для ориентированного графа.

Эти матрицы являются квадратными матрицами, число строк и столбцов равно количеству вершин. На пересечении i-строки и j-столбца матрицы смежности стоит число, равное количеству дуг, соединяющих вершины i и j.

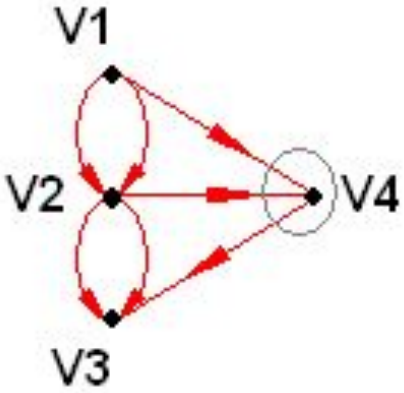
В матрице инциденций входящие дуги считаются со знаком "-", выходящие - "+". Элементы множества U для неориентированного графа называются ребрами, а для ориентированного – дугами.

0	2	0	1
2	0	2	1
0	2	0	1
1	1	1	0



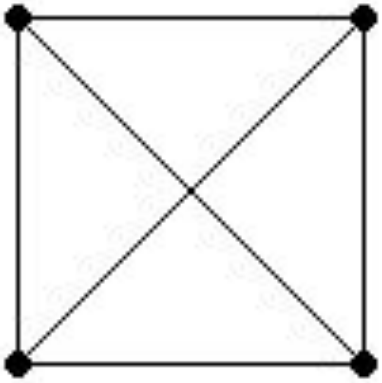
Матрица смежности всегда симметрична относительно главной диагонали.

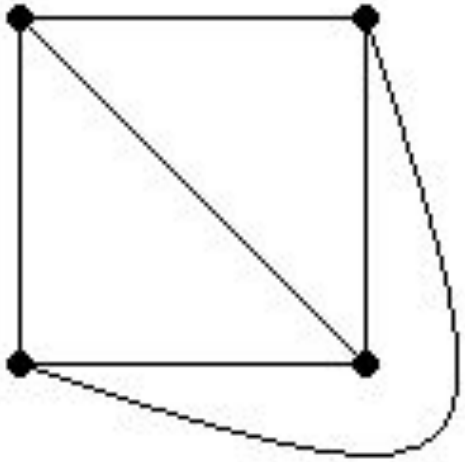
0	-2	0	-1
2	0	-2	-1
0	2	0	1
1	1	-1	0



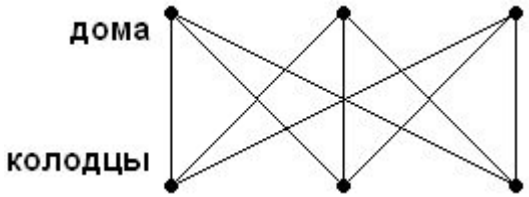
Если 2 графа различаются только нумерацией вершин, но сохраняют при этом отношение инцидентности, то такие 2 графа называются изоморфными.

Если какой-то граф можно изобразить на плоскости таким образом, что его ребра не пересекаются, то такой граф называется планарным.





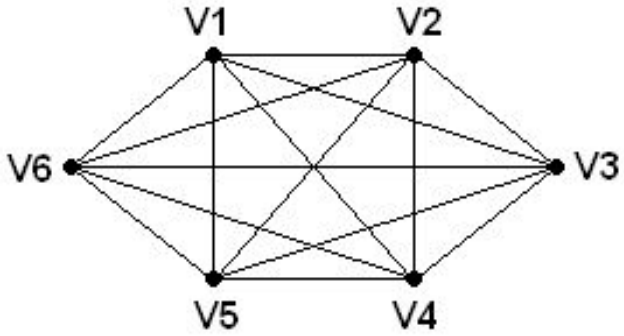
Задача о трех домах и трех колодцах.



Соседи перессорились и решили проложить тропинки заново, чтобы не пересекаться друг с другом.

Обыкновенный граф (граф без петель и кратных ребер) называется полным и обозначается K, где n – количество вершин, если каждая его пара вершин соединены ребром.

Граф K_6



Если множество вершин графа можно разбить на 2 непересекающихся подмножества, так что каждая пара вершин, принадлежащих одному и тому же подмножеству не соединена ребром и каждая пара вершин, принадлежащая разным подмножествам, соединена ребром, то такой граф называется полным двудольным графом и обозначается $K_{m,n}$, где m и n – количество вершин в подмножествах.

Граф в задаче о домах и колодцах полный двудольный граф $K_{3,3}$.

Если имеется граф с множеством вершин G и ребер U(G,U), то G_1 подмножество множества G($G_1 \subseteq G$) и U_1 подмножество множества U($U_1 \subseteq U$), причем если две вершины x1 и x2 принадлежат множеству G_1 и эти две вершины были соединены ребром в графе (G,U), то это ребро принадлежит и множеству U_1, тогда граф (G_1, U_1)называется частью графа (G,U).

Если множество G_1 совпадает с множеством G и U_1 собственное подмножество и $G_1 = G\ U_1 \subset U$, то есть все вершины исходного графа входят в его часть, а ребра не все, то такой граф называется суграфом данного графа

Если $G_1 \subset G$ не все вершины входят в часть графа, а те вершины, которые были соединены в графе G, будут соединены и в графе G_1, то такая часть графа называется подграфом.

Маршруты на графах

Последовательность вершин (не обязательно различных) $V_0, V_1, \ldots, V_n$ называется маршрутом, если каждая пара вершин $(V_{i-1}; V_i)$ $i=1\text{-}n$ соединена ребром.

Если $V_0 = V_n$, то такой маршрут называется замкнутым, в частности маршрут может состоять из одного ребра.

Если маршрут имеет вид $V_0\ V_0$, то это ребро-петля.

Если вершины V_0 и V_n можно соединить каким-либо маршрутом, то эти две вершины называются связанными.

Если каждую пару вершин графа можно соединить маршрутом (то есть каждая пара вершин связана), то такой граф называется связным.

Если все ребра в маршруте различны – называется цепью.

Если и все вершины различны, то - простой или элементарной цепью.

Замкнутая цепь называется циклом.

В ориентированном графе маршрут является ориентированным, так что передвигаться по дугам можно только в направлении стрелок.

Ориентированный маршрут, в котором дуги не повторяются, называется путём и замкнутый путь – контуром.

Если в ориентированном графе каждая упорядоченная пара вершин соединена путем, то такой граф называется сильно связным.

Если в ориентированном графе каждая пара вершин соединена каким-либо маршрутом без учета направления дуг, то такой граф слабо связный.

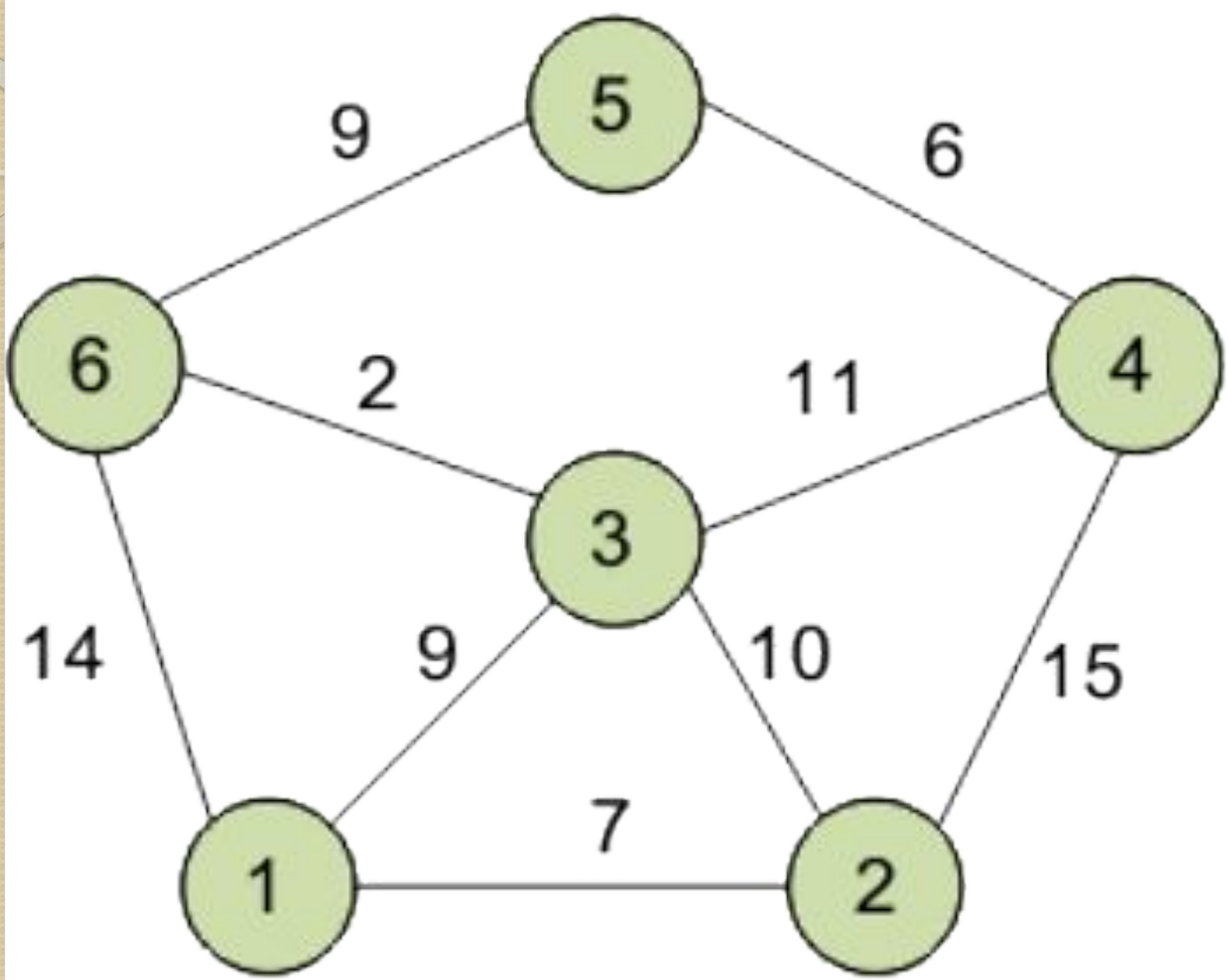
Если в данном графе существует цикл, содержащий все ребра графа, то такой граф называется Эйлеровым и сам цикл Эйлеровым циклом.

Определить, является ли граф Эйлеровым, просто: для этого необходимо и достаточно, чтобы степень каждой его вершины (валентность) была четной.

Алгоритм Дейкстры нахождения кратчайшего пути

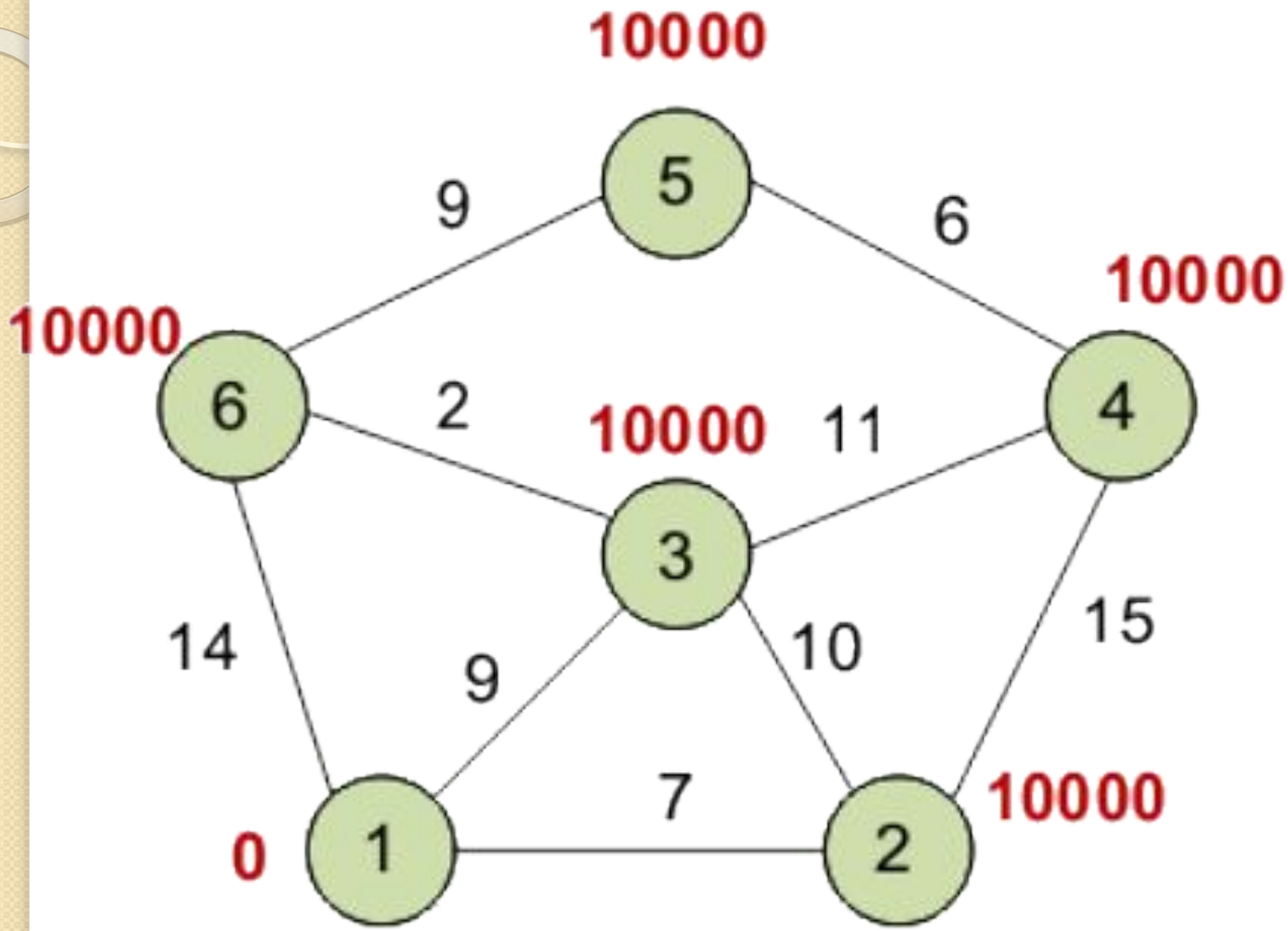
Формулировка задачи

Пусть требуется найти кратчайшие расстояния от 1-й вершины до всех остальных.
Кружками обозначены вершины, линиями – пути между ними (ребра графа). В кружках обозначены номера вершин, над ребрами обозначен их вес – длина пути. Рядом с каждой вершиной красным обозначена метка – длина кратчайшего пути в эту вершину из вершины 1.


5
9
6
6
2
11
4
3
14
9
10
15
7
1
2

Инициализация

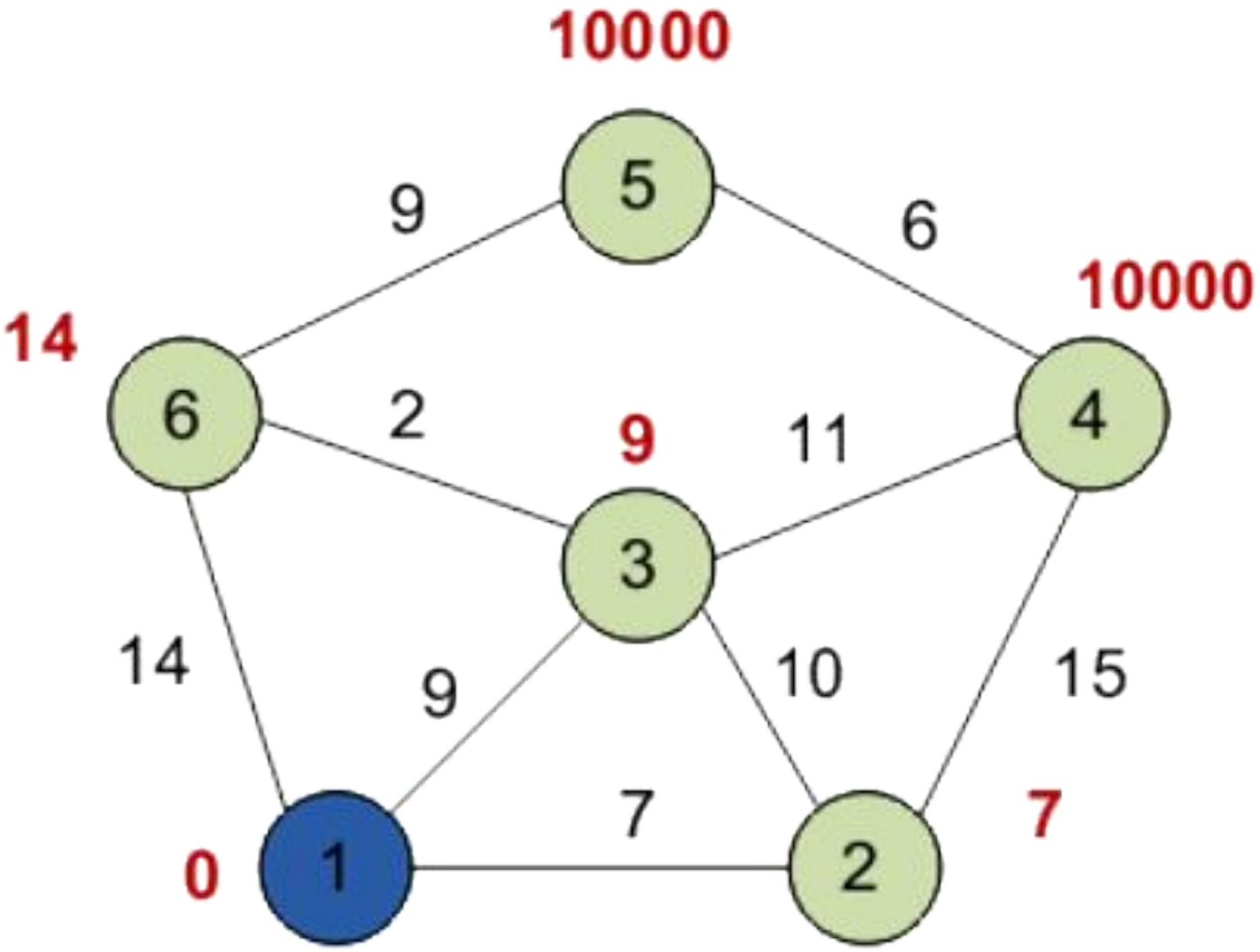
Метка самой вершины 1 полагается равной 0, метки остальных вершин – недостижимо большое число (в идеале - бесконечность). Это отражает то, что расстояния от вершины 1 до других вершин пока неизвестны. Все вершины графа помечаются как непосещенные.


10000
5
9
6
10000
10000
6
2
10000
11
4
3
14
9
10
15
7
10000
0
1
2

Первый шаг

Минимальную метку имеет вершина 1. Её соседями являются вершины 2, 3 и 6. Обходим соседей вершины по очереди.
Первый сосед вершины 1 – вершина 2, потому что длина пути до неё минимальна. Длина пути в неё через вершину 1 равна сумме кратчайшего расстояния до вершины 1, значению её метки, и длины ребра, идущего из 1-й в 2-ю, то есть 0 + 7 = 7. Это меньше текущей метки вершины 2 (10000), поэтому новая метка 2-й вершины равна 7.

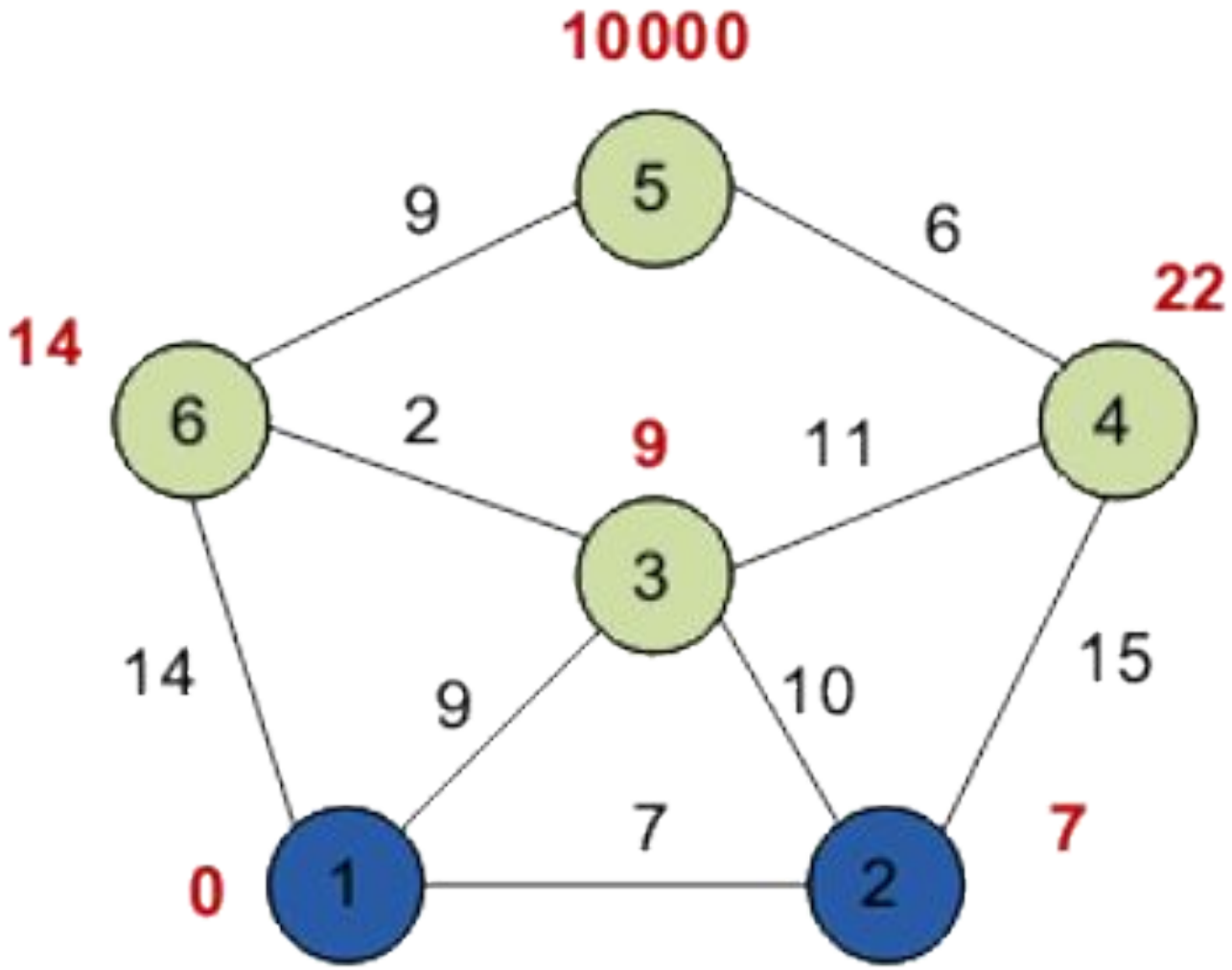
Аналогично находим длины пути для всех других соседей (вершины 3 и 6).
Все соседи вершины 1 проверены. Текущее минимальное расстояние до вершины 1 считается окончательным и пересмотру не подлежит. Вершина 1 отмечается как посещенная.


10000
5
9
6
10000
14
6
2
9
11
4
3
14
9
10
15
7
7
0
1
2

Второй шаг

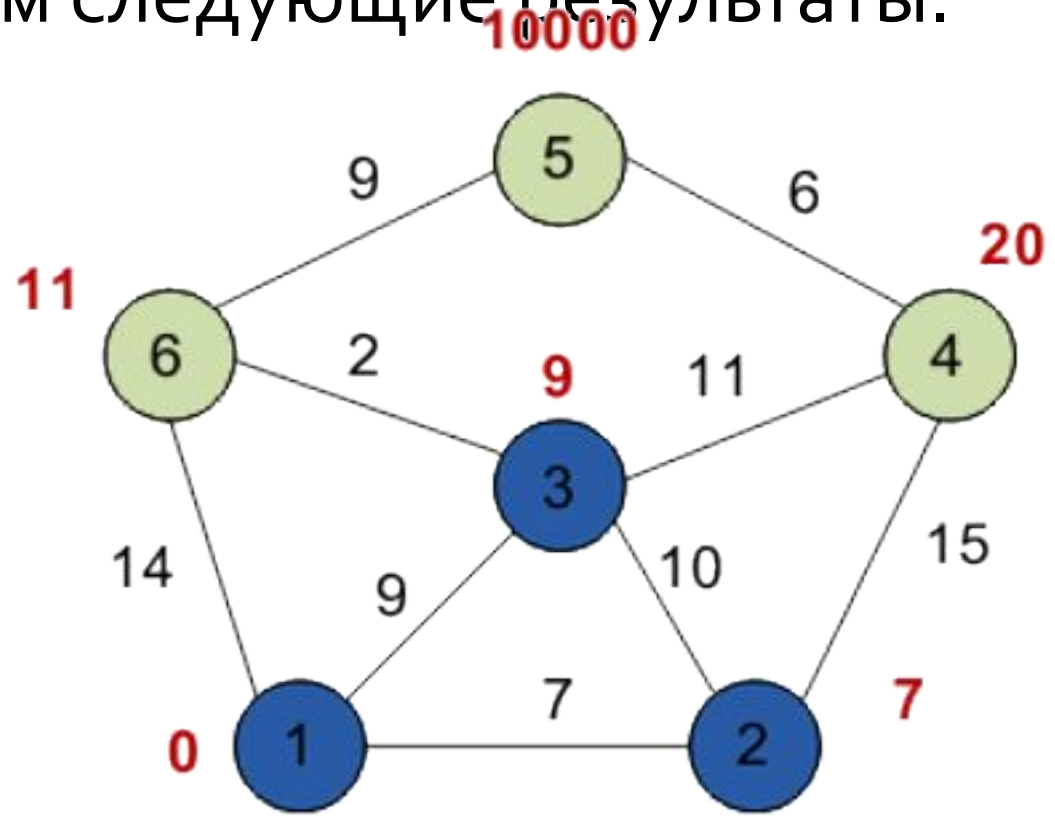
Шаг 1 алгоритма повторяется. Снова находим «ближайшую» из непосещенных вершин. Это вершина 2 с меткой 7.
Снова пытаемся уменьшить метки соседей выбранной вершины, пытаясь пройти в них через 2-ю вершину. Соседями вершины 2 являются вершины 1, 3 и 4.
Вершина 1 уже посещена. Следующий сосед вершины 2 — вершина 3, так как имеет минимальную метку из вершин, отмеченных как не посещённые. Если идти в неё через 2, то длина такого пути будет равна 17 (7 + 10 = 17). Но текущая метка третьей вершины равна 9, а 9 < 17, поэтому метка не меняется.

Ещё один сосед вершины 2 — вершина 4. Если идти в неё через 2-ю, то длина такого пути будет равна 22 (7 + 15 = 22). Поскольку 22<10000, устанавливаем метку вершины 4 равной 22.
Все соседи вершины 2 просмотрены, помечаем её как посещенную.

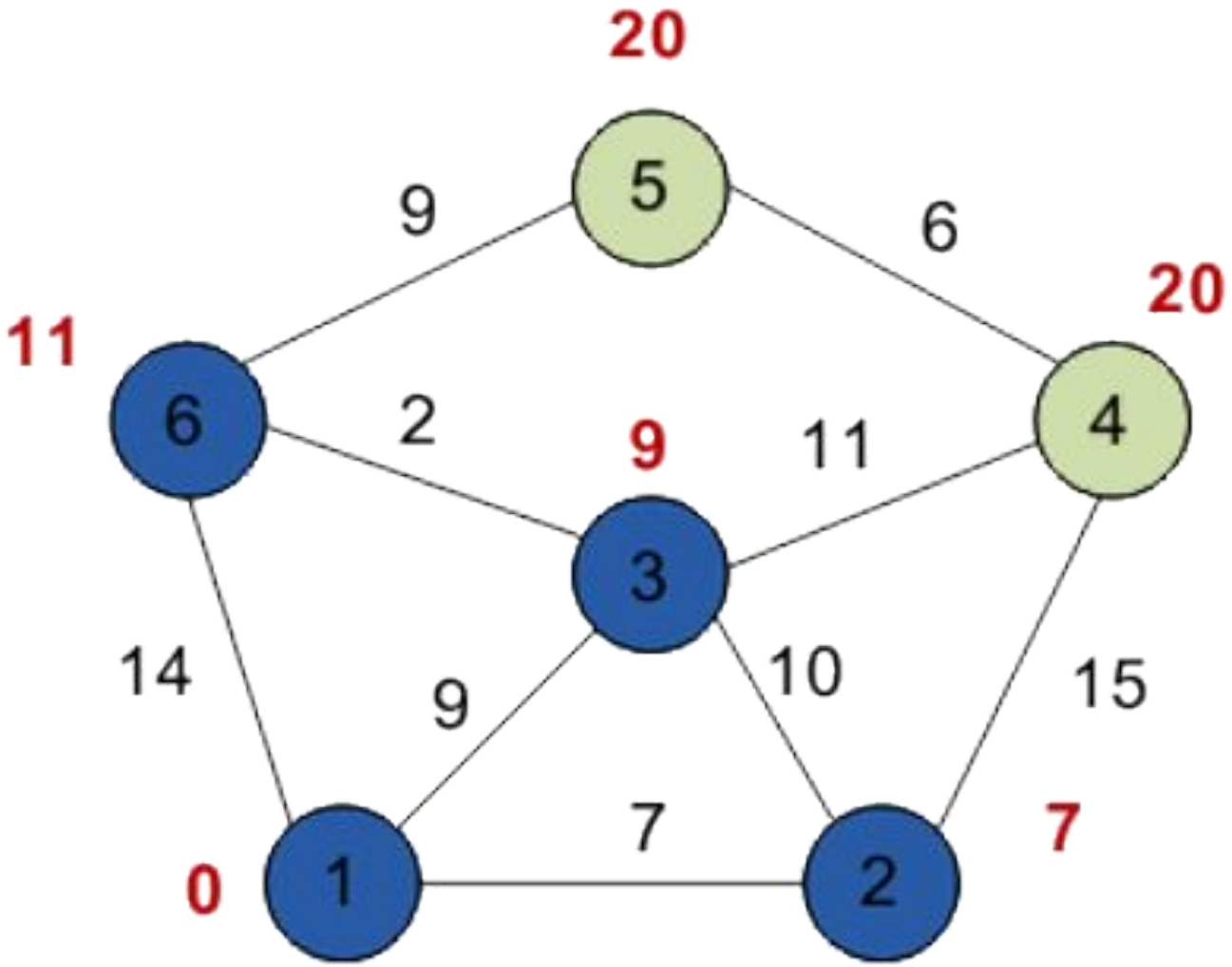

10000
5
9
6
22
14
6
2
9
11
4
3
14
9
10
15
7
7
0
1
2

Третий шаг

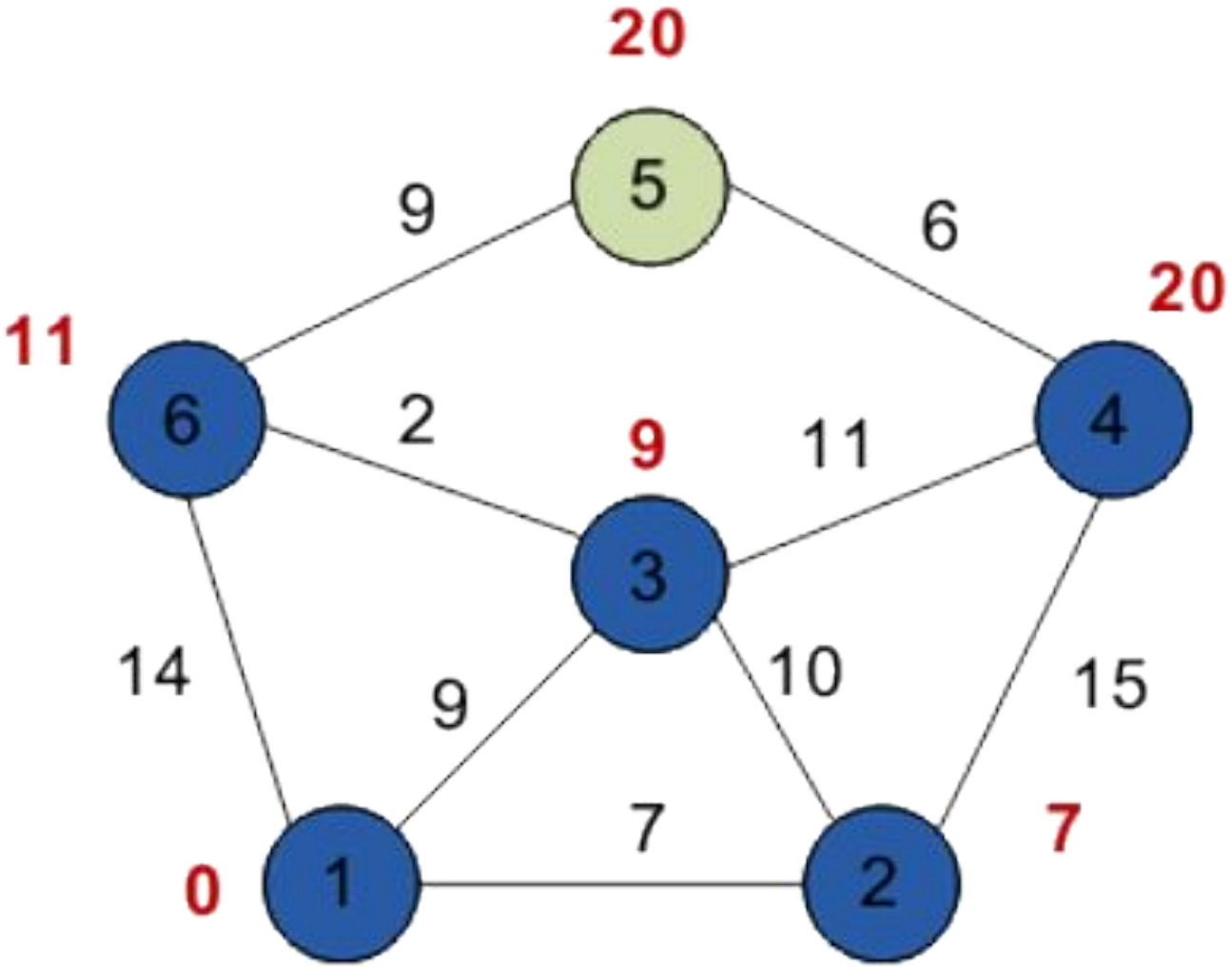
Повторяем шаг алгоритма, выбрав вершину 3. После её «обработки» получим следующие результаты.



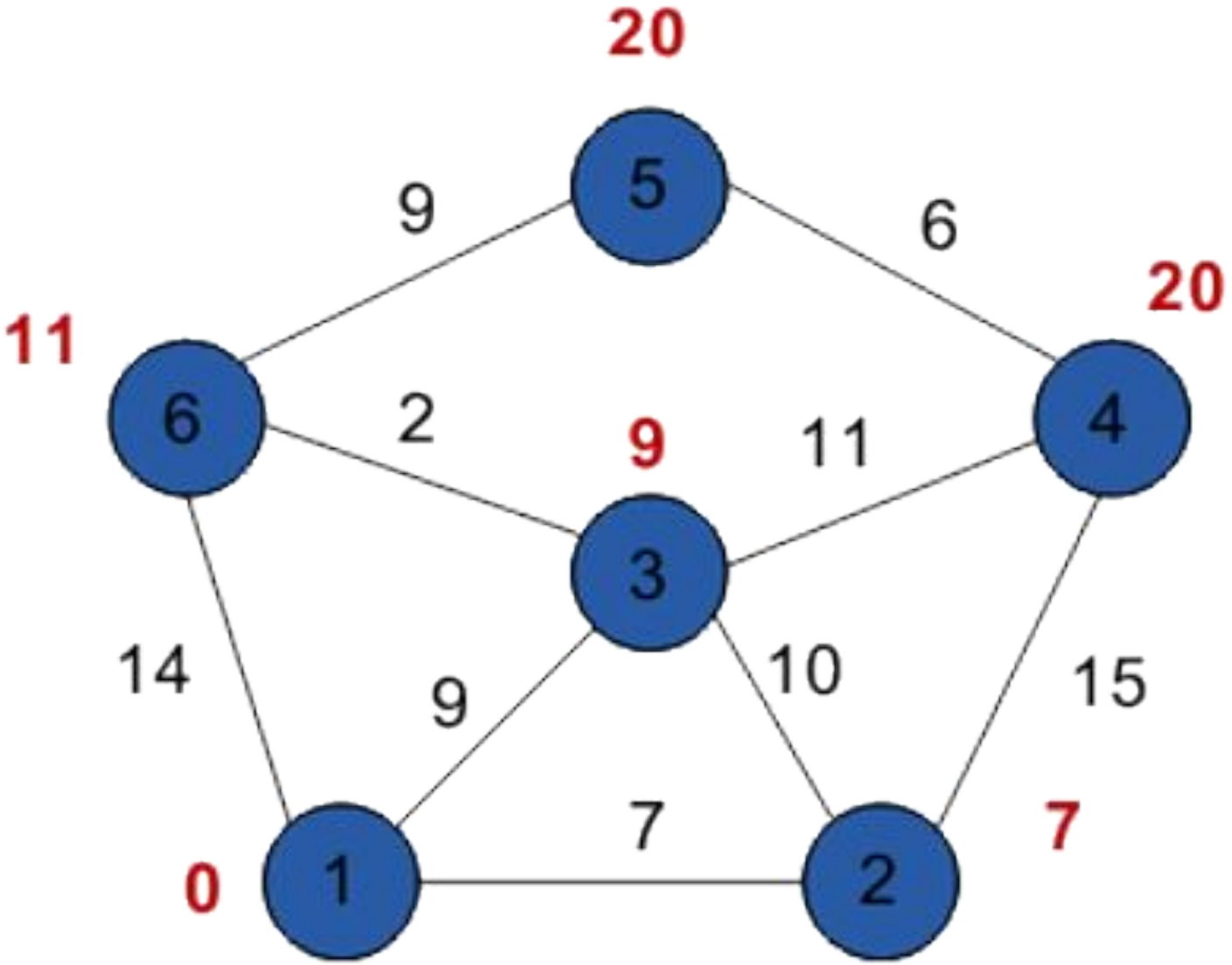
Четвертый шаг



Пятый шаг



Шестой шаг

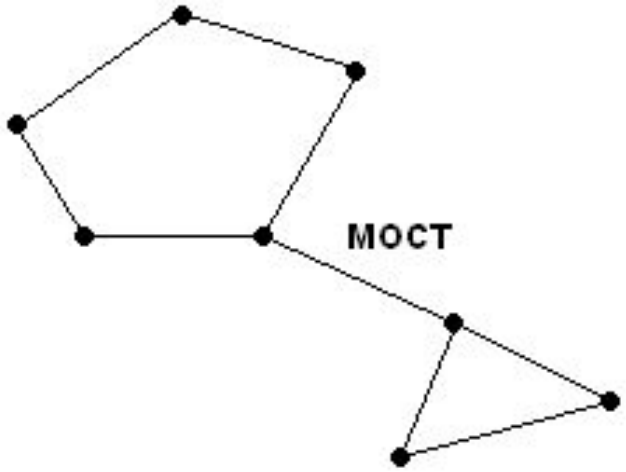


Ответ

Таким образом, кратчайшим путем из вершины 1 в вершину 5 будет путь через вершины **1 - 3 - 6 - 5**, поскольку таким путем мы набираем минимальный вес, равный 20.

Деревья

Ребро связного графа называется мостом, если после его удаления граф теряет связность, то есть распадается на два отдельных связных компонента.



Деревом называется конечный связной граф без циклов.

Основная теорема о деревьях.

Следовательно, утверждения эквивалентны.

1. *Граф G является деревом, то есть связным графом без циклов.*
2. *G не содержит циклов и количество его ребер на одно меньше количества его вершин.*
3. *G связан и количество его ребер на одно меньше числа вершин.*
4. *G связен и каждое его ребро является мостом.*
5. *Любые две вершины графа G можно соединить единственным простым маршрутом.*
6. *G не содержит циклов добавление к нему любого ребра приводит к образованию единственного простого цикла.*

Задача о минимальном покрывающем дереве

Алгоритм Прима.

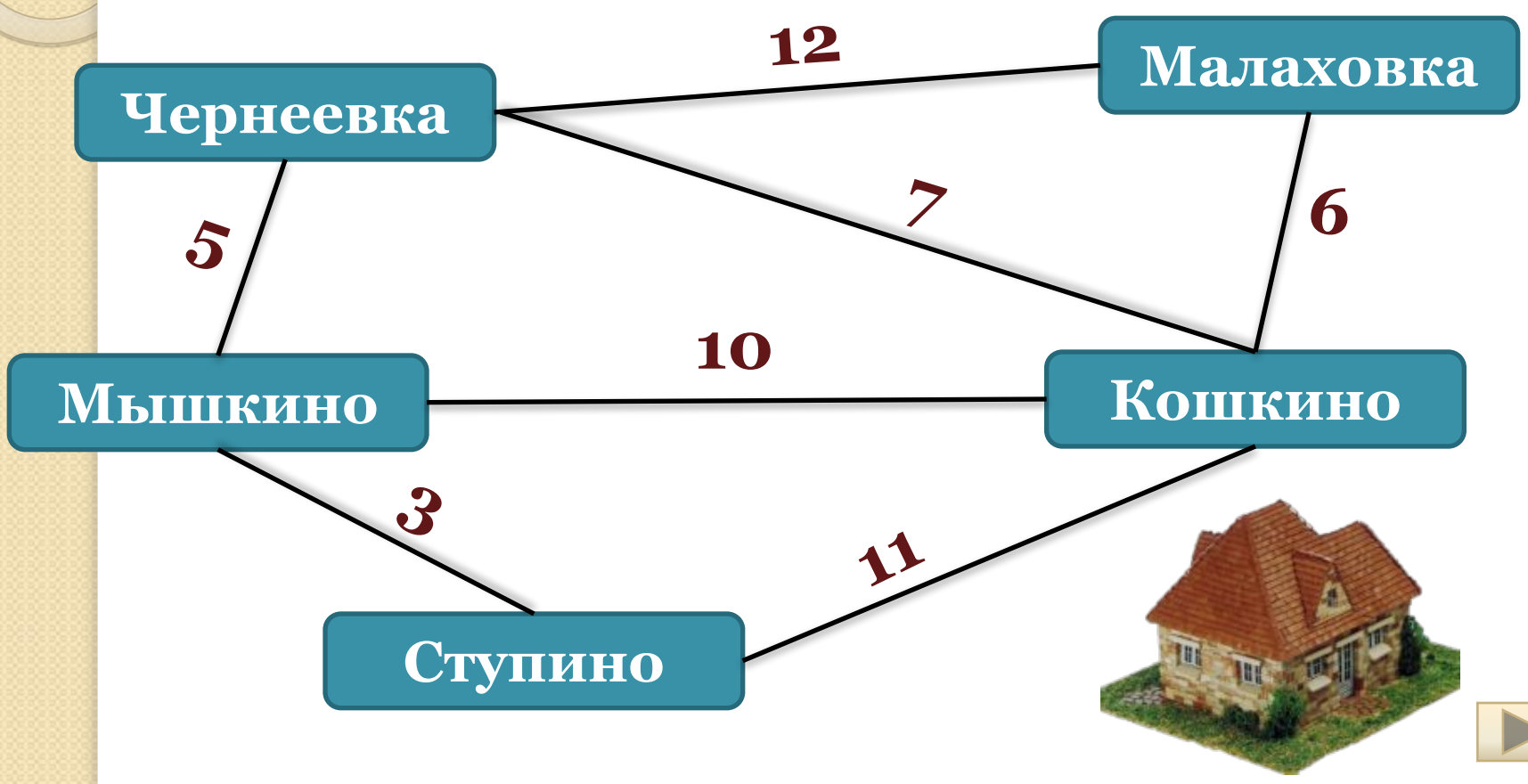
1. *Пронумеруем ребра графа в порядке возрастания весов.*
2. *Помечаем каким-нибудь образом ребро минимального веса.*
3. *Рассмотрим следующее по весу ребро: если хотя бы одна из его вершин не принадлежит множеству вершин, помеченных ребер, то помечаем это ребро и переходим к рассмотрению следующего ребра.*
4. *Если обе вершины рассмотренного ребра являются вершинами уже помеченных ребер, то нужно проверить – не образует ли рассматриваемое ребро циклов с помеченными ребрами, если не образует, то помечаем его и переходим к рассмотрению следующего ребра.*
5. *Процесс продолжаем до тех пор, пока не будет помечены n-1 ребра.*

Задача 1

В некотором районе было решено провести газопровод между пятью деревнями. От Кошкино до Мышкино идти 10 км, от Мышкино до Ступино – 3 км, от Кошкино до Малаховки – 6 км, от Малаховки до Черняевки – 12 км, от Кошкино до Ступино – 11 км, от Мышкино до Чернеевки – 5 км, от Кошкино до Чернеевки – 7 км. Как необходимо провести трубу, чтобы она соединяла все пять деревень, и затраты при этом были минимальными?

Задача 1

Построим граф, моделирующий дороги, соединяющие деревни.



Задача 1

Задача сводится к построению остовного связного дерева минимального веса.

Рассчитаем цикломатическое число.

m (количество ребер) равно **7**

n (количество вершин) рано **5**

$$\gamma = 7 - 5 + 1 = 3$$

Т.е. три деревни напрямую соединены газовой трубой не будут.

(переходы по щелчку)

Алгоритм Прима

Пусть дан взвешенный неориентированный граф.

Для построения минимального остовного дерева необходимо:

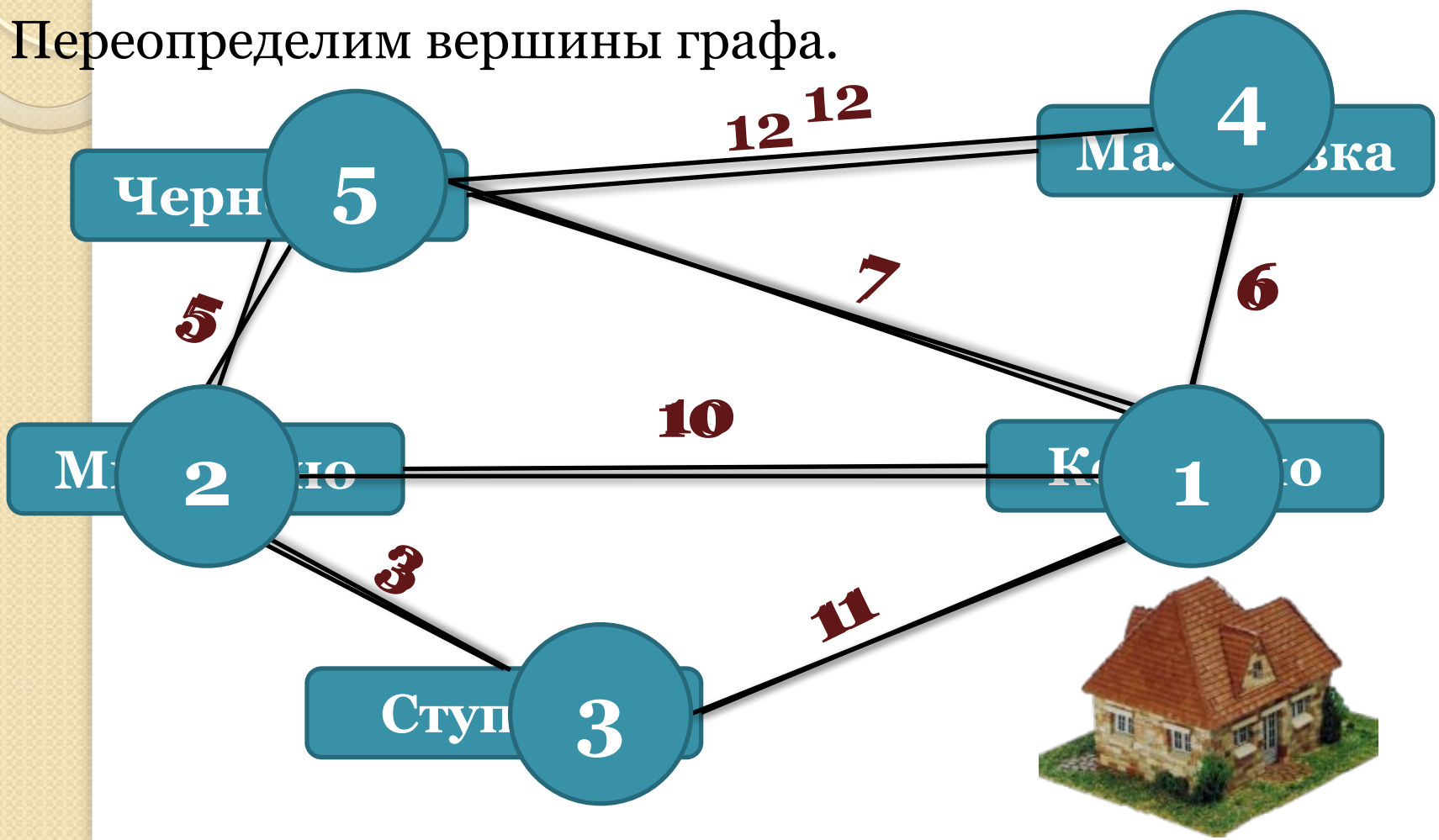
1. Представить граф в виде матрицы смежности
2. Найти в матрице наименьший элемент, соответствующий ребру, соединяющему i-ю и j-ю вершины графа
3. Вычеркнуть элементы i-й и j-й строки матрицы
4. Пометить i-й и j-й столбцы матрицы
5. В помеченных столбцах i и j найти наименьший элемент, отличный от уже найденного
6. Повторять пункты 3-5 до тех пор, пока не будут задействованы все вершины графа

(переходы по щелчку)

Задача 1

Решим задачу по алгоритму Прима.

Переопределим вершины графа.



(переходы по щелчку)

Задача 1

Представим граф в виде матрицы смежности.

	1	2	3	4	5
1	0	10	11	6	7
2	10	0	3	0	5
3	11	3	0	0	0
4	6	0	0	0	12
5	7	5	0	12	0

Найдем минимальный элемент.

Он равен **3**

(переходы по щелчку)

Задача 1

Вычеркнем 2-ю и 3-ю строки таблицы. А столбцы 2 и 3 выделим.

	1	2	3	4	5
1	0	10	11	6	7
2			**3**		
3					
4	6	0	0	0	12
5	7	**5**	0	12	0

Найдем минимальный элемент в выделенных столбцах.

Он равен **5**

(переходы по щелчку)

Задача 1

Вычеркнем 5-ю строку таблицы. А столбец 5 выделим.

	1	2	3	4	5
1	0	10	11	6	7
2			3		
3					
4	6	0	0	0	12
5		5			

Найдем минимальный элемент в выделенных столбцах.

Он равен 7

(переходы по щелчку)

Задача 1

Вычеркнем 1-ю строку таблицы. А столбец 1 выделим.

	1	2	3	4	5
1					7
2			3		
3					
4	6	0	0	0	12
5		5			

Найдем минимальный элемент в выделенных столбцах.

Он равен **6**

(переходы по щелчку)

Задача 1

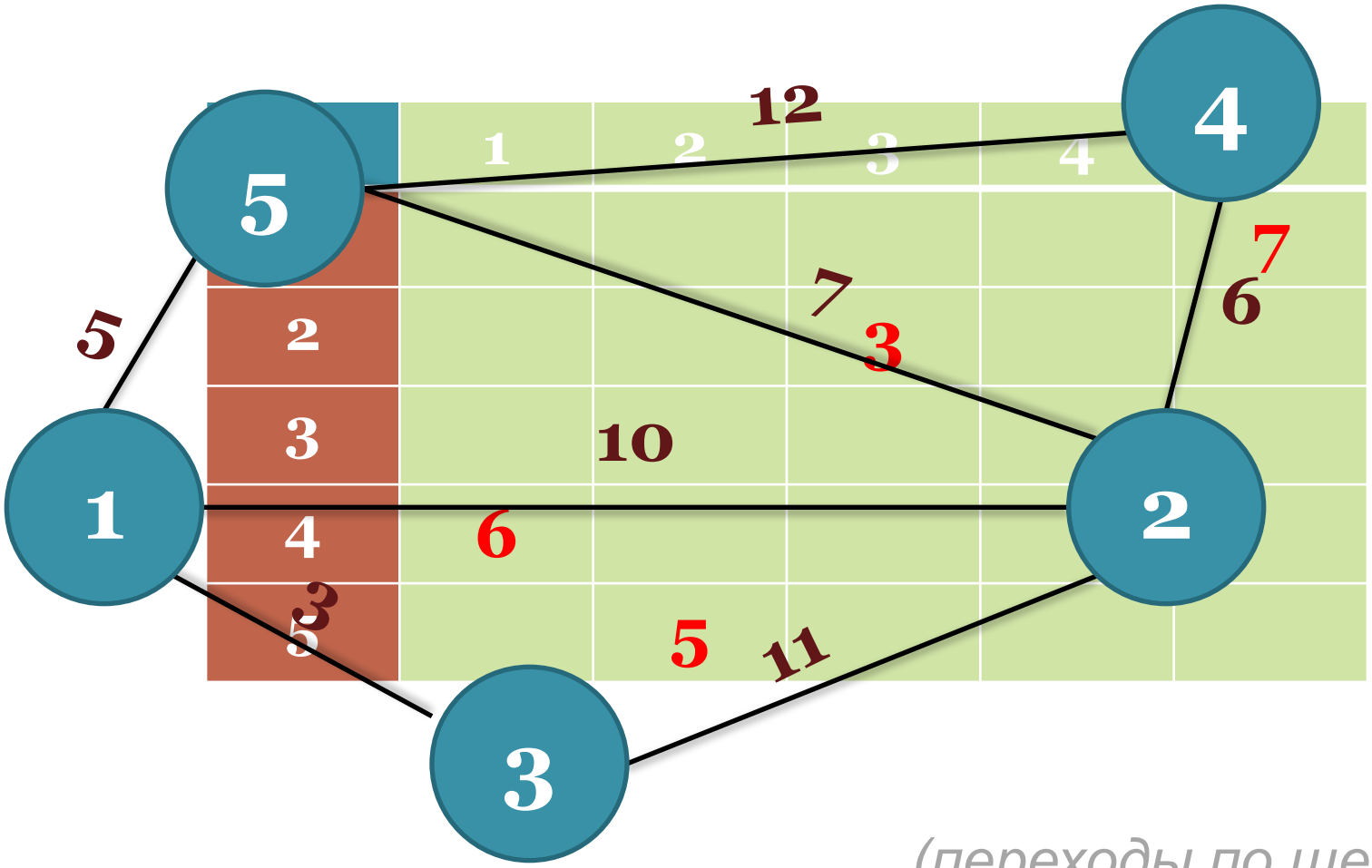
Вычеркнем 4-ю строку таблицы. А столбец 4 выделим.

	1	2	3	4	5
1					7
2			3		
3					
4	6				
5		5			

(переходы по щелчку)

Задача 1

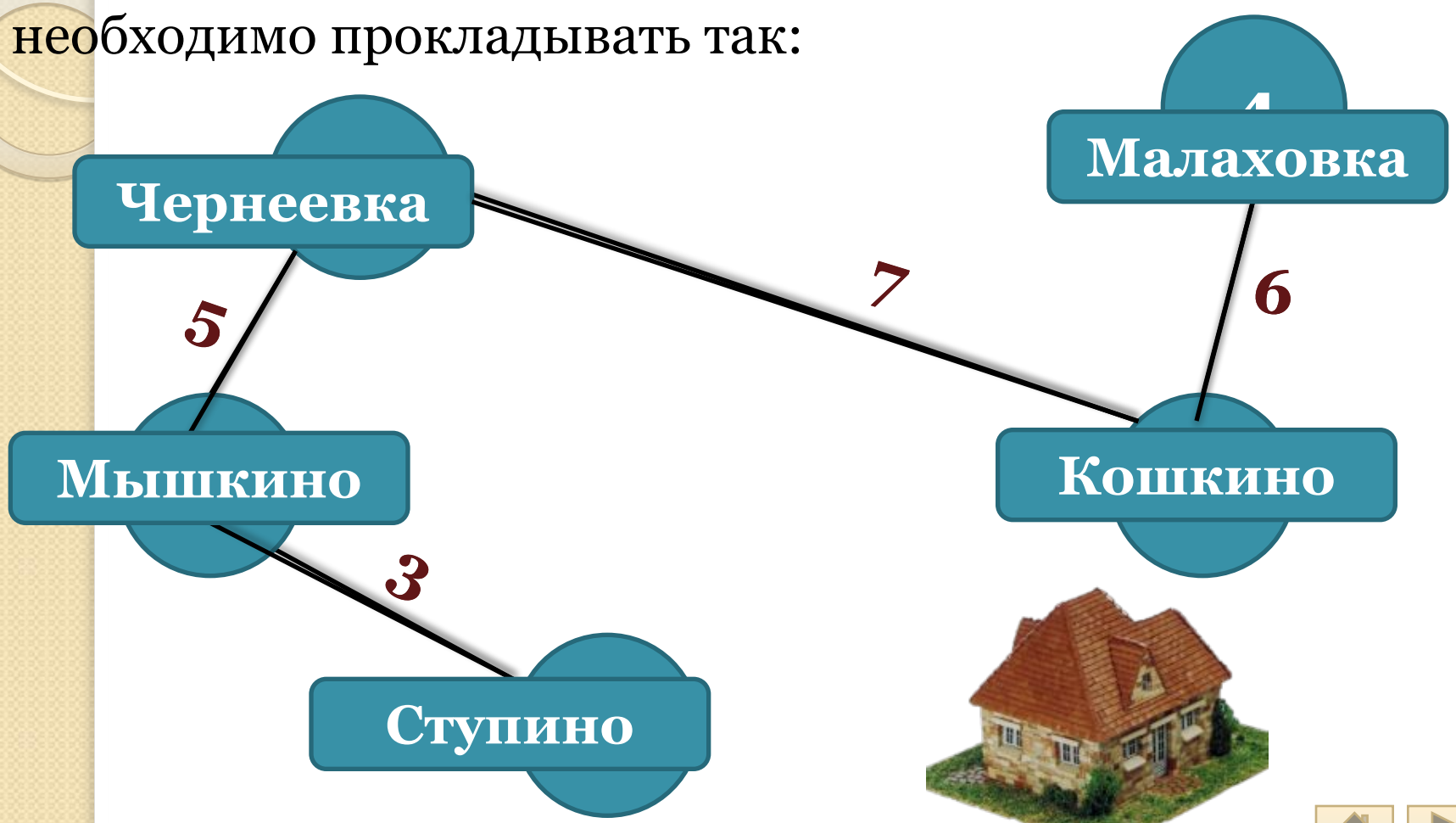
Получаем связное остовное дерево минимальное веса.



(переходы по щелчку)

Задача 1

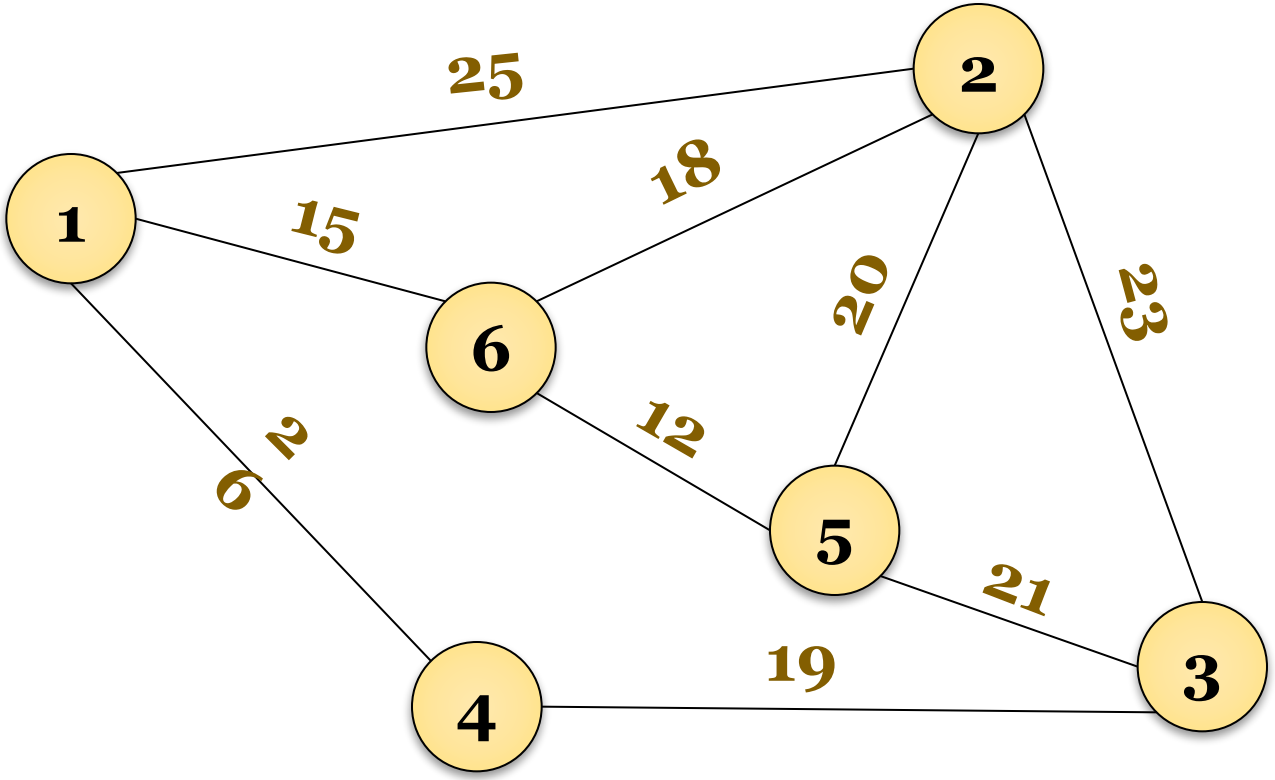
Ответ: газопровод с минимальными затратами необходимо прокладывать так:



Протяженность газопровода – **21 км**.

Задача 2

Даны города, часть которых соединена между собой дорогами. Необходимо проложить туристический маршрут минимальной длины, проходящий через все города.



Задача 2

Задача сводится к построению остовного связного дерева минимального веса.

Рассчитаем цикломатическое число.

m (количество ребер) равно **9**

n (количество вершин) рано **6**

$$\gamma = 9 - 6 + 1 = 4$$

Т.е. четыре дороги, соединяющие города, не будут включены в туристический маршрут.

(переходы по щелчку)

Алгоритм Крускала

1. Удалить все ребра и получить остовной подграф с изолированными вершинами.
2. Отсортировать ребра по возрастанию.
3. Ребра последовательно, по возрастанию их весов, включаются в остовное дерево. Возможны случаи:

а) обе вершины включаемого ребра принадлежат одноэлементным подмножествам, тогда они объединяются в новое, связное подмножество;

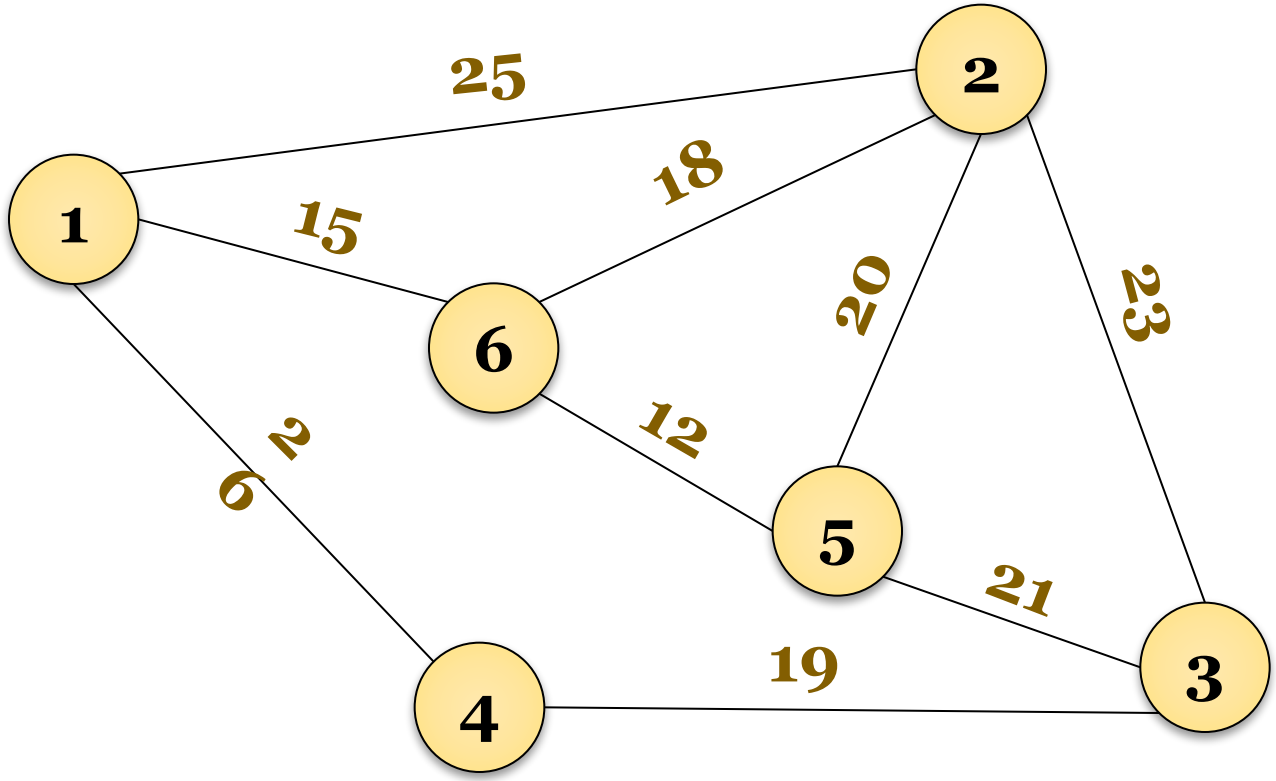
б) одна из вершин принадлежит связному под-множеству, другая нет, тогда включаем вторую в подмножество, которому принадлежит первая;

в) обе вершины принадлежат разным связным подмножествам, тогда объединяем подмножества;

г) обе вершины принадлежат одному

Задача 2

Для определения туристического маршрута минимальной длины воспользуемся алгоритмом Крускала.

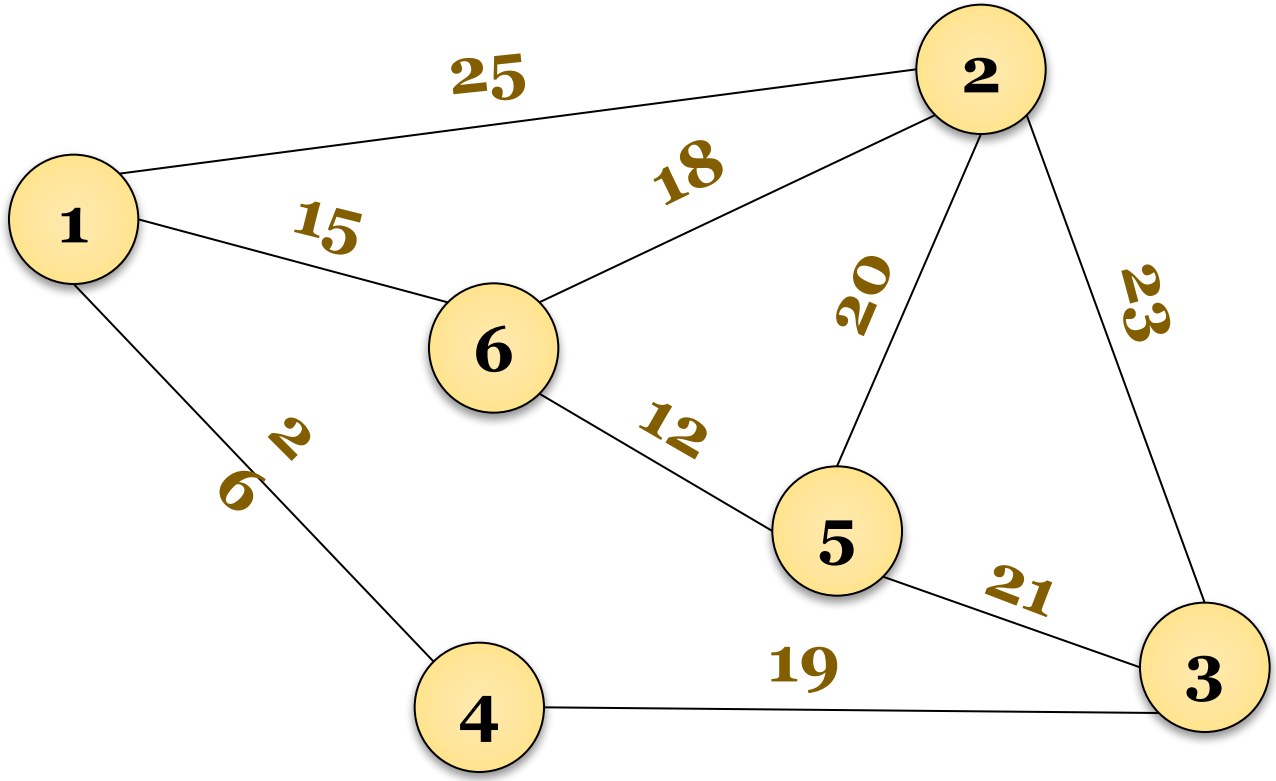


Задача 2

Шаг 1

Построим остовной подграф, содержащий только изолированные вершины.

Получаем шесть одноэлементных подмножеств.



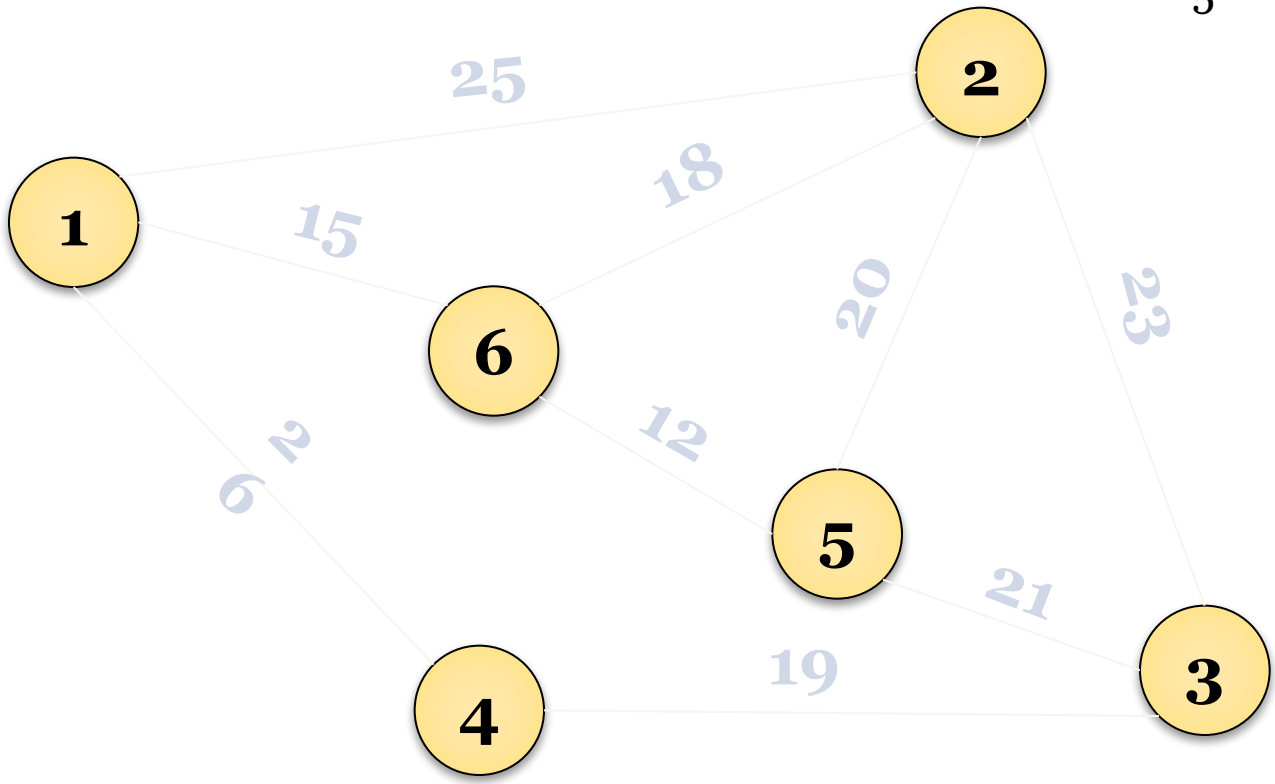
пуск

Задача 2

Шаг 2

Найдем ребро минимального веса и добавим его в остовной подграф.

Образуется связное подмножество вершин $\{V_5, V_6\}$.

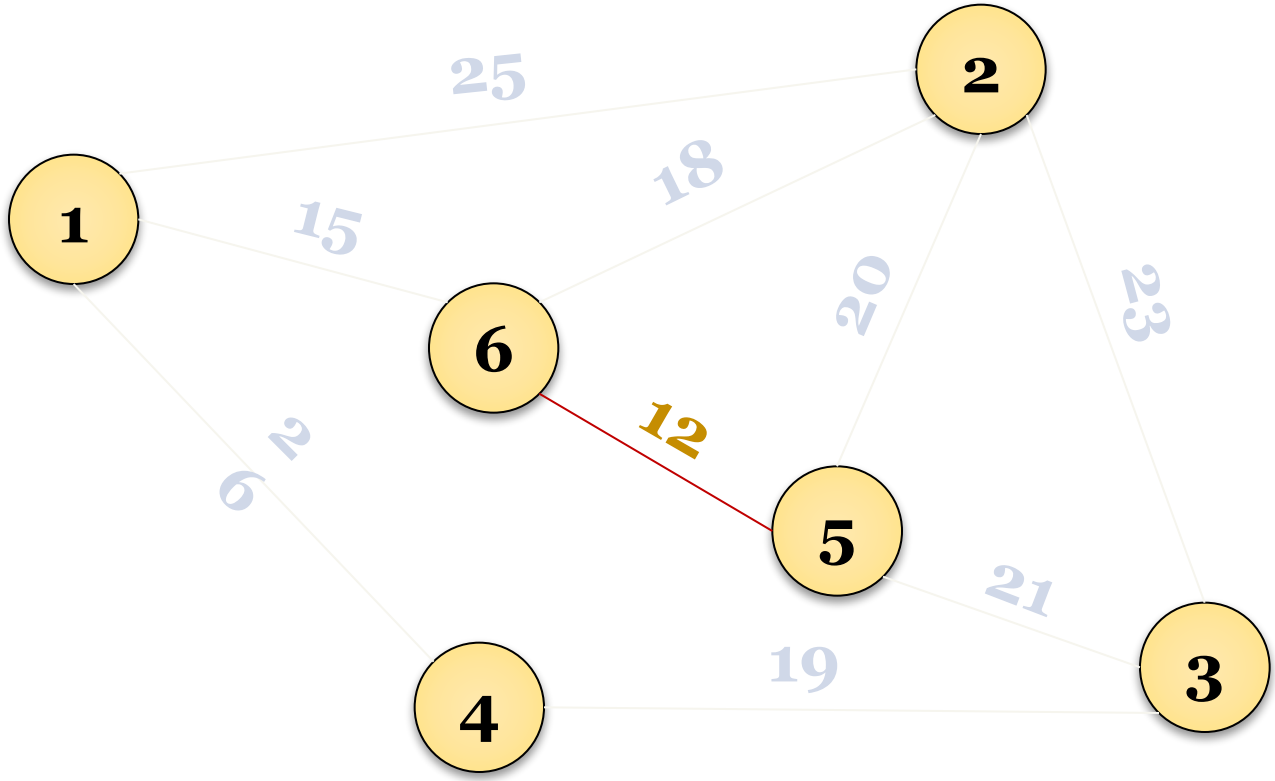


Задача 2

Шаг 3

Среди оставшихся ребер найдем ребро минимального веса и добавим его в остовной подграф.

Добавляем в подмножество вершин еще одну $\{V_5, V_6, V_1\}$.

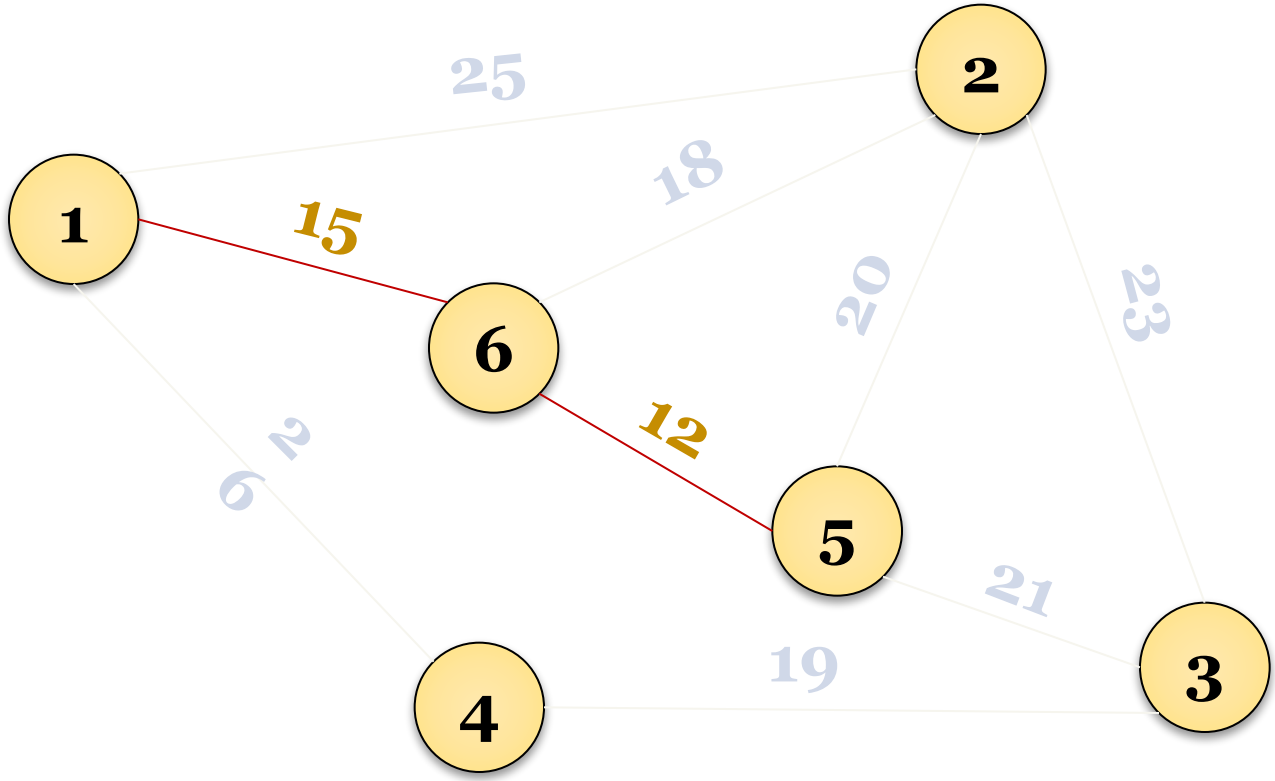


Задача 2

Шаг 4

Среди оставшихся ребер найдем ребро минимального веса и добавим его в остовной подграф.

Добавляем в подмножество вершин еще одну $\{V_5, V_6, V_1, V_2\}$.

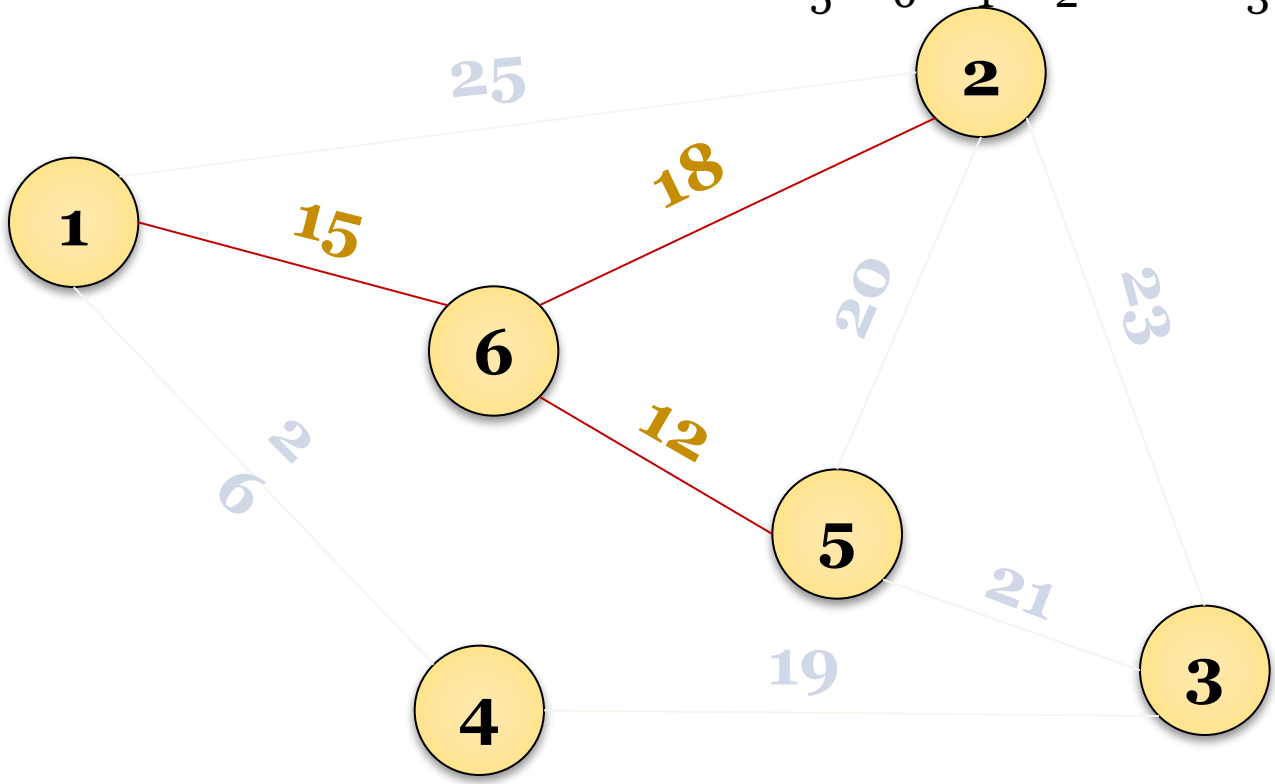


Задача 2

Шаг 5

Среди оставшихся ребер найдем ребро минимального веса и добавим его в остовной подграф.

Образуется два подмножества $\{V_5,V_6,V_1,V_2\}$ и $\{V_3,V_4\}$.



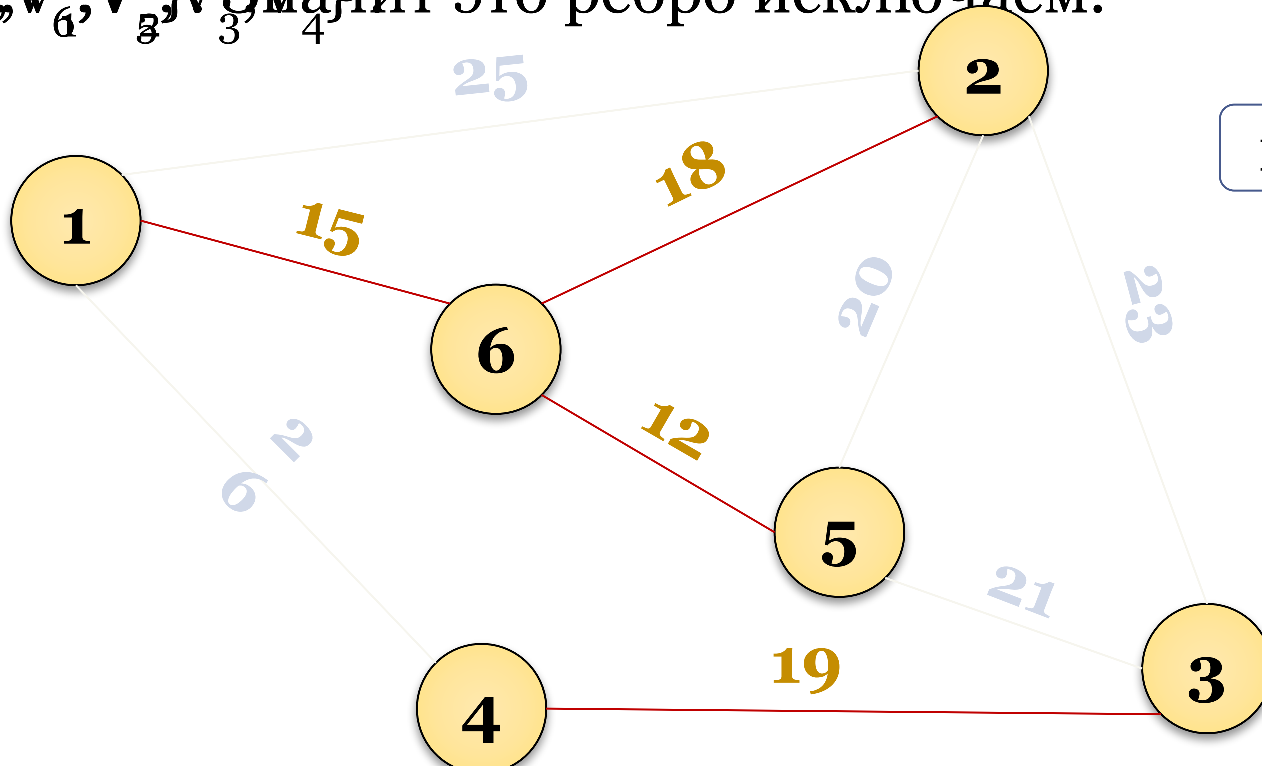
Задача 2

Шаг 6

Среди оставшихся ребер найдем ребро минимального веса и добавим его в остовной подграф.

Но обе вершины принадлежат одному связному множеству $\{V_5, V_2, V_6, V_3\}$ значит это ребро исключаем.

Подмножества объединились в одно связное подмножество $\{V_5, V_6, V_1, V_2, V_3, V_4\}$



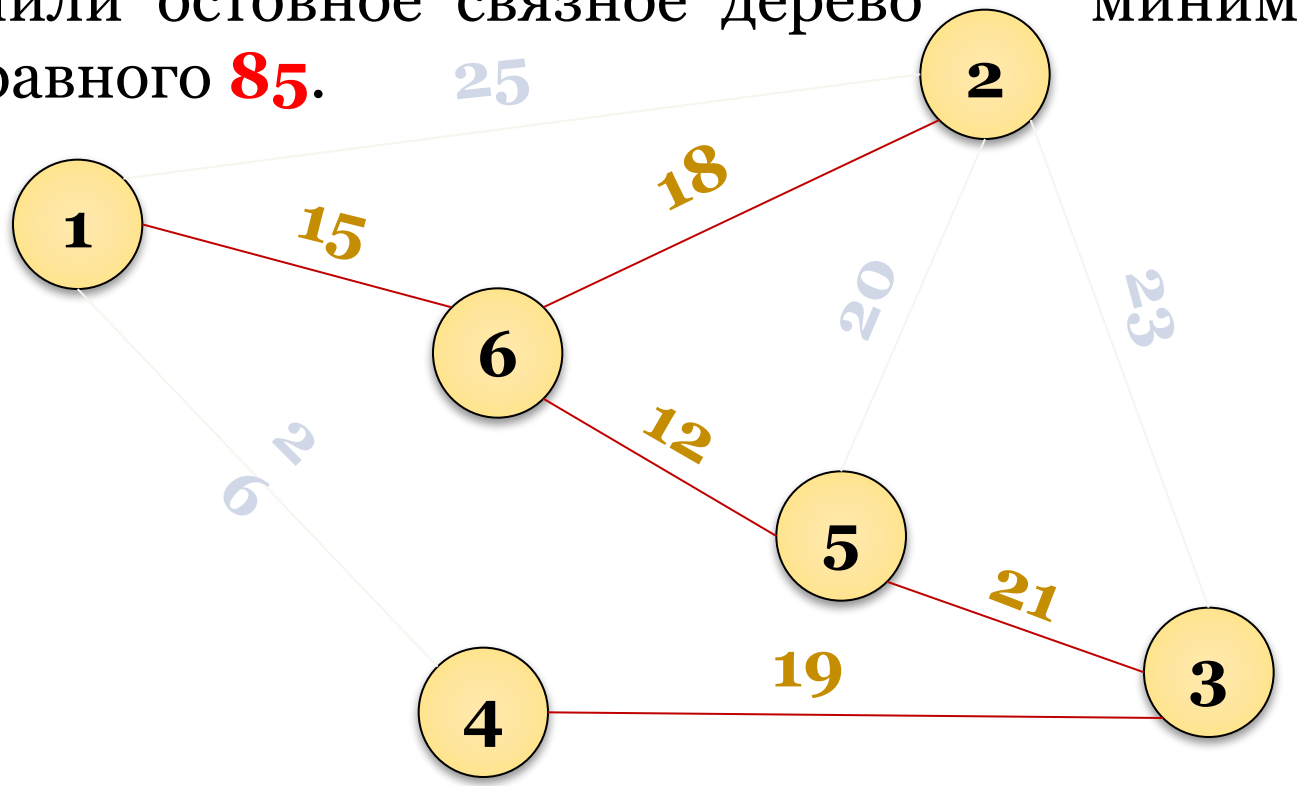
пуск (2)

Задача 2

Итог

Остальные ребра включать в граф не надо, т.к. все их вершины уже принадлежат одному связному множеству.

Получили остовное связное дерево минимального веса, равного **85**.



АЛГОРИТМЫ И РЕКУРСИВНЫЕ ФУНКЦИИ

Алгоритмы и рекурсивные функции

Алгоритм – процесс последовательного построения величин, идущий в дискретном времени таким образом, что в начальный момент времени задается исходная конечная система величин, а в каждый следующий момент система величин получается по определенному закону (программе) из системы величин, имевших в предыдущий момент времени (дискретность алгоритма).

Система величин, получаемых в какой-то (не начальный) момент времени однозначно определяется системой величин, полученных в предшествующий момент времени (детерминированность алгоритма).

Закон получения последующей системы величин из предыдущей должен быть простым и локальным (элементарность шагов алгоритма). Если способ получения последующей величины из какой-либо заданной величины не дает результат, то должно быть указано, что надо считать результатом алгоритма (направленность алгоритма).

Начальная система величин может выбираться из какого-то потенциально бесконечного множества (массовость алгоритма).

Алгоритм Евклида:

1.Заданы два числа a_1 и a_2; будем считать, что ни a_1, ни a_2 не равны нулю; a_1 и a_2 принадлежат N.

2. Делим a_1 на a_2 и находим остаток от деления a_3, если a_3=0, то делим a_2 на a_3, находим остаток от деления a_4, если a_4=0, то a_3 – наибольший делитель, если нет, то делим a_3 на a_4 и так далее.

Интуитивно понятное, неопределенное, а описываемое понятие алгоритма вполне удовлетворяло математиков до начала 20 века, с его помощью легко было доказать существование алгоритма решения той или иной задачи, просто построив этот алгоритм. Когда перед математиками стали задачи, в которых нужно доказать, что алгоритм их решения не существует, потребовалось строгое определение понятия алгоритма. Эта задача была решена в середине 30-х годов 20-го века в работах Гильберта, Геделя, Тьюринга и Поста.

Уточнение понятия алгоритма было произведено 2-мя способами:

1.Через рекурсию функций.

2. Через машину Тьюринга-Поста.

Определение с помощью машин Тьюринга-Поста понятие алгоритма очень специальное, но цель – показать, как самые сложные процессы можно моделировать на весьма простых устройствах.

С помощью теории алгоритма, возникшей из внутренних проблем теоретической математике, впоследствии было решено много практических задач из разных областей знаний.

Другая область применения теории алгоритмов – вычисление машины, на которой легко моделировать машины Тьюринга-поста.

Машина Тьюринга-Поста

Машина Тьюринга-Поста состоит из следующих частей:

1. *Конечная лента, разбитая на конечное число ячеек. В процессе работы машины к существующим ячейкам машина может пристраивать новые ячейки как влево, так и вправо, так что конечно лента может писаться потенциально неограниченно в обе стороны. Каждая ячейка может находиться в одном из конечных множеств состояний a_0, a_1, …a_n – эти величины называются внешним алфавитом машины.*

В процессе работы машины может изменять состояние ячеек, но может и не изменять их.

Таким образом, если в какой-то момент времени лента имеет r ячеек, то состояния лены полностью описывается словом $a_{j1} a_{j2} \ldots a_{jr}$.

2. *Внутренняя память машины – это некоторое устройство, которое в каждый момент находиться в одном из возможных состояний, причем множество этих состояний конечное и фиксированное для каждой машины. Состояние внутренней памяти обозначается символом ($q_1, q_2, \ldots q_n$), не входящие во внешний алфавит машины. Одно из таких внутренних состояний машины является выделение, обычно обозначающиеся q_0, и называется стоп сигналом.*
3. *Управляющая головка – некоторое устройство, которое перемещается вдоль лены или, наоборот, лента перемещается вдоль него, так что в любой момент времени в устройстве находится ровно 1 ячейка.*

4.*Механическое устройство предполагает, что машина снабжена особым механизмом, которое в зависимости от состояний воспроизведения ячейки и состояния внутренней памяти, может изменять состояние внутренней памяти и одновременно либо изменять состояний воспринимаемой ячейки, либо сдвигать управляющую головку влево в соседнюю слева ячейку, либо вправо, при этом, если воспринимаемая ячейка является самой крайней слева и головку нужно сдвинуть влево, то механическое устройство пристраивает слева пустую ячейку.*

Если в какой-то момент времени внутреннее состояние машины переходит в q_0*, то дальнейшее их изменение не происходит.*

Совокупность всех этих данных можно записать одним машинным словом $a_{j_1}, a_{j_2} \ldots q_i a_{j_k} \ldots a_{j_l}$*, в которое входит только один символ из алфавита* q*. Этот символ может быть самым правым, так как после него обязательно должно быть записано состояние воспринимаемой ячейки.*

МЕТОДЫ КОДИРОВАНИЯ

Методы кодирования

Теория кодирования – раздел теории информатики, изучающей способы отождествления сообщений с отображением их сигнатур.

Задачей теории кодирования является отождествление истинной информации с каналом связи.

Объектом кодирования служит как дискретная, так и непрерывная информация. Понятие кодирования означает преобразование информации в форму, удобную для передачи по определенным каналам связи.

Обратная операция – декодирование заключается в восстановлении принятого сообщения из закодированного вида в общепринятый, достаточный для потребителя.

В теории кодирования существует ряд направлений:

1. *Статистическое или эффективное кодирование.*
2. *Помехоустойчивое кодирование.*
3. *Корректирующие коды.*
4. *Циклические коды, арифметические коды и так далее.*
5. *Защита информации.*

Кодирование имеет значение не только в конспиративных целях для шифровки информации, так в математике с помощью кодирования изучают одни объекты, заменяя изучением других более доступных или уже известных, например метод координат, введенный Декартом, дает возможность изучить геометрические объекты через их аналитическое выражение в виде чисел, букв и их комбинаций формул.

Исследование кодов получило новый импульс после создания в 1948 году Клодом Шинером новой науки теории информатики. В основе теории информатики лежит гипотеза о статистических характеристиках истинных сообщений.

Проблемой защиты информации занимается наука криптология, состоящая из криптографии и криптоанализа. Криптология занимается поиском и исследованием математических методов преобразования информации.

Криптоанализ исследует принцип расшифровки сообщений без знания ключа.

Современная криптография включает в себя разделы: симметричные криптоносители, криптосистемы с открытым ключом, системы электронной подписи управления ключами.

Криптографические методы используются для передачи секретной информации по таким каналам связи, как например электронная почта - с целью установления истинности передаваемого сообщения. А также с целью хранения информации на носителях в зашифрованном виде.

Крипто-аналитики часто пользуются математическими методами при работе с информацией, так методы декодирования включают в себя решение уравнений и систем уравнений.