

**С. Ф. КОЖУХОВ,
П. И. СОВЕРТКОВ**

СБОРНИК ЗАДАЧ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ

УЧЕБНОЕ ПОСОБИЕ

Издание второе, стереотипное



• САНКТ-ПЕТЕРБУРГ •
• МОСКВА •
• КРАСНОДАР •
2018

ББК 22.176я73

К 58

Кожухов С. Ф., Совертков П. И.

К 58 Сборник задач по дискретной математике: Учебное пособие. — 2-е изд., стер. — СПб.: Издательство «Лань», 2018. — 324 с.: ил. — (Учебники для вузов. Специальная литература).

ISBN 978-5-8114-2588-4

Учебное пособие содержит задачи по темам: множества, комбинаторика и бинарные отношения, булевы функции, графы, кодирование информации, алгоритмы. В пособии приведены краткие теоретические сведения, решено около 200 типовых примеров, содержится большой набор задач для самостоятельного решения, дана контрольная работа. При наличии большого количества новых понятий приведены систематизирующие таблицы, в которых указаны критерии использования понятий.

Предназначено для студентов дневного и заочного отделений, обучающихся по направлениям подготовки и специальностям, входящим в УГС: «Математика и механика», «Физика и астрономия», «Техника и технология строительства», «Информатика и вычислительная техника», «Электроника, радиотехника и системы связи», «Электро- и теплотехника», «Физико-технические науки и технологии» и другим техническим и педагогическим направлениям подготовки и специальностям, где предусмотрен курс дискретной математики.

ББК 22.176я73

Рецензенты:

В. А. ГАЛКИН — доктор физико-математических наук, профессор, директор Политехнического института Сургутского государственного университета;
С. П. ГУЛЬКО — доктор физико-математических наук, профессор, зав. кафедрой теории функций Томского государственного университета.

Обложка

Е. А. ВЛАСОВА

© Издательство «Лань», 2018
© С. Ф. Кожухов, П. И. Совертков, 2018
© Издательство «Лань»,
художественное оформление, 2018

Оглавление

Предисловие	5
Глава 1. Множества, бинарные отношения и булева алгебра	6
§ 1. Множества и отображения	6
§ 2. Комбинаторика и бином Ньютона	21
§ 3. Рекуррентные отношения и производящая функция	31
§ 4. Бинарные отношения	37
§ 5. Булева алгебра	52
Глава 2. Булевы функции	59
§ 6. Логические операции	59
§ 7. Прямая, обратная и противоположная теоремы	65
§ 8. Определение булевых функций	68
§ 9. СДНФ и СКНФ	79
§ 10. Полином Жегалкина	86
§ 11. Карта Карно	91
§ 12. Схемы и булевы функции	97
§ 13. Функционально замкнутые классы. Классы T_0 и T_1	107
§ 14. Класс самодвойственных функций	112
§ 15. Класс линейных функций	116
§ 16. Класс монотонных функций	120
§ 17. Множество симметричных функций	126
§ 18. Множество функций T_{k_0} и $T_{>k_0}$	131
§ 19. Полные системы функций	133
§ 20. Предикаты. Кванторы общности и существования	135
§ 21. Логические уравнения	140
§ 22. Производная булевой функции	144
Глава 3. Графы и орграфы	147
§ 23. Определение графа	147
§ 24. Изоморфные и гомеоморфные графы	151
§ 25. Матрица смежности и матрица инцидентности	157
§ 26. Однородный и полный графы	161
§ 27. Маршруты и числовые характеристики на графе	164
§ 28. Двудольный граф	171
§ 29. Связность графа и нахождение простых цепей	173
§ 30. Эйлеровы и гамильтоновы графы	175
§ 31. Плоские и планарные графы. Теорема Эйлера	184
§ 32. Операции над графами	187
§ 33. Деревья, лес и остов графа	191
§ 34. Фундаментальная система циклов и разрезы графа	198
§ 35. Раскрашивание вершин, ребер и граней графа	201

Глава 4. Кодирование информации.....	209
§ 36. Основы теории делимости	209
§ 37. Сравнения первой степени	214
§ 38. Простейшие способы кодирования информации	224
§ 39. Шифрование аффинным преобразованием	230
§ 40. Код Грея	236
§ 41. Код переменной длины. Код Хаффмана	238
§ 42. Код Хемминга	240
§ 43. Криптосистема с закрытым или открытым ключом	243
§ 44. Группа, кольцо и поле	246
Глава 5. Потоки в сетях. Алгоритмы	252
§ 45. Сети	252
§ 46. Алгоритмы обхода вершин графа	255
§ 47. Выбор кратчайшего пути методом присвоения меток	259
§ 48. Максимальная пропускная способность сети	262
§ 49. Понятие алгоритма	268
§ 50. Вычислимые функции	272
§ 51. Машина Тьюринга	277
Приложение 1. Структура графов	282
Приложение 2. Структура деревьев	292
Приложение 3. Контрольная работа.....	293
Приложение 4. Несколько компьютерных программ	303
Приложение 5. Основные обозначения	309
Ответы	310
Литература	322

Предисловие

Сборник задач содержит различные разделы дискретной математики и предназначен для закрепления теоретического материала, освоенного на лекциях или самостоятельно. В задачнике решено около 200 типовых задач. В начале каждой темы сообщены необходимые теоретические сведения. После решения задач студент может продолжить работу по данной тематике, разрабатывая проект по математическому и компьютерному моделированию. В приложении 4 приведено несколько простейших программ на языке Visual Basic 6.0, оформление которых на этом языке программирования является экономным.

При перечислении графов и деревьев можно использовать классификацию графов и деревьев, приведенную в приложениях 1 и 2.

В приложении 3 дана типовая контрольная работа. В зависимости от объема часов, отведенных на изучение дискретной математики, и в зависимости от специальности содержание контрольной работы может дополняться заданиями из других тем. Вместо итоговой контрольной работы рабочая программа по дискретной математике может содержать проведение контроля знаний и умений по изучаемым модулям. Тогда приведенная контрольная работа разделяется на части.

Если некоторые понятия изучались в других дисциплинах (например: группа, кольцо, поле, сравнения – изучались в курсе алгебры), то содержание практических занятий следует соответственно изменить.

В приложении 5 приведены обозначения символов, используемых как для сокращения записи текстовой информации, так и для обозначения изучаемых объектов.

Простейшие способы кодирования информации можно использовать в профориентационной работе с учащимися.

Нумерация задач в пособии – двойная. Первое число указывает номер параграфа, а второе – номер задачи в параграфе.

В пособии большое количество рисунков и таблиц, поэтому нумерация рисунков и таблиц проводится для каждой главы отдельно.

Авторы пособия выражают благодарность преподавателям Политехнического института СурГУ Назину А.Г. и Мухутдиновой Д.Р. за полезные замечания, способствующие улучшению пособия.

Критические замечания и пожелания по наиболее рациональному решению предложенных в пособии задач можно направлять по e-mail: psovertkov@mail.ru.

Глава 1. Множества, бинарные отношения и булева алгебра

§ 1. Множества и отображения

а) Множества

Понятие *множества* является фундаментальным неопределяемым понятием математики. Множество – это некоторая совокупность объектов, называемых элементами, относительно которых указано характеристическое свойство, их объединяющее. Если элемент a принадлежит множеству A , то записывают $a \in A$ и $a \notin A$ в противном случае. Пустым множеством называется множество \emptyset , не содержащее ни одного элемента.

Множество можно задавать: перечислением элементов, если оно имеет конечное число элементов, формулой или словами, формулируя характеристическое свойство.

Множество A называется *подмножеством* B (A содержится в B ; B содержит A), если каждый элемент A принадлежит B . Обозначение $A \subset B$. Считается, что пустое множество \emptyset является подмножеством любого множества.

Два множества называются *равными*, если каждое из них является подмножеством другого: $A=B \leftrightarrow A \subset B, B \subset A$.

Объединением двух множеств A и B называется множество, каждый элемент которого принадлежит, по крайней мере, одному из данных множеств:

$$A \cup B = \{x : x \in A \text{ или } x \in B\}, \quad x \in A \cup B \leftrightarrow \begin{cases} x \in A, \\ x \in B. \end{cases}$$

Пересечением множеств A и B называется множество, которое состоит из всех элементов, содержащихся в обоих множествах A и B и не содержит никаких других элементов, т.е. любой элемент пересечения принадлежит каждому из данных множеств:

$$A \cap B = \{x : x \in A \text{ и } x \in B\}, \quad x \in A \cap B \leftrightarrow \begin{cases} x \in A, \\ x \in B. \end{cases}$$

Разностью множеств A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат A , но не принадлежат B , т.е.

$$A \setminus B = \{x : x \in A \text{ и } x \notin B\}, \quad x \in A \setminus B \leftrightarrow \begin{cases} x \in A, \\ x \notin B. \end{cases}$$

В конкретных рассуждениях подмножества рассматриваются в некотором достаточно широком множестве U , которое называется *универсальным* множеством (*универсумом*).

Множество $U \setminus A$ называется *дополнением* множества A до U и обозначается $C_U A$ или \bar{A} . Элемент $x \in A$ тогда и только тогда, когда $x \notin \bar{A}$.

$x \in A \cup B$ тогда и только тогда, когда $x \notin \bar{A}, x \notin \bar{B}$.

Используя дополнение множества, разность двух множеств можно представить в виде $A \setminus B = A \cap \bar{B}$.

Симметричной разностью множеств A и B называется множество, которое содержит все элементы множеств A и B , кроме их общих элементов:

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

Для иллюстрации множеств и операций над ними используют диаграммы Венна или круги Эйлера.

Рассмотрим схему (рис. 1), иллюстрирующую основные операции с множествами, для различных расположений множеств.

A, B	$A \cup B$	$A \cap B$	$A \setminus B$	$B \setminus A$	$A \Delta B$
		\emptyset			
				\emptyset	
			\emptyset	\emptyset	\emptyset

Рис. 1

Упорядоченной парой (x, y) называется двухэлементное множество, в котором указано, какой элемент является первым. Две упорядоченные пары (x_1, y_1) , (x_2, y_2) считаются равными тогда и только тогда, когда $x_1 = x_2, y_1 = y_2$.

Декартовым (прямым) произведением множеств X и Y называется множество всех упорядоченных пар (x, y) , таких, что $x \in X, y \in Y$. Обозначение $X \times Y$.

Если $Y=X$, то декартово произведение $X \times X$ называется декартовым квадратом множества X и обозначается X^2 .

Пример 1. $X = \{2, 3, 5\}, Y = \{3, 7\}$.

$X \times Y = \{(2,3), (3,3), (5,3), (2,7), (3,7), (5,7)\}$.

□

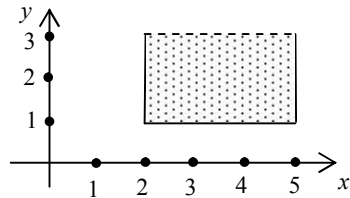


Рис. 2

Пример 2. $A=[2; 5]$, $B=[1; 3]$, тогда $A \times B$ можно изобразить точками прямоугольника без верхнего основания (рис. 2). \square

Пример 3. Пусть $I=[0;1]$ – отрезок, тогда $I \times I = I^2$ можно изобразить точками квадрата. \square

Пример 4. Множество $R \times [a; b]$ можно рассматривать как точки полосы между параллельными прямыми (рис. 3). \square

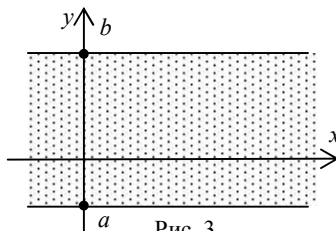


Рис. 3

Прямым произведением n множеств A_1, A_2, \dots, A_n называется множество всех упорядоченных наборов (x_1, x_2, \dots, x_n) , таких, что $x_1 \in A_1, x_2 \in A_2, \dots, x_n \in A_n$:

$$A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) : x_1 \in A_1, x_2 \in A_2, \dots, x_n \in A_n\}.$$

В частности, при $A_1 = A_2 = \dots = A_n$ получаем n -ю степень множества A :

$$A^n = A \times A \times \dots \times A = \{(x_1, x_2, \dots, x_n) : x_1 \in A, x_2 \in A, \dots, x_n \in A\}.$$

Пример 5. Множество $\underbrace{R \times R \times \dots \times R}_n$ состоит из всех упорядоченных наборов

(x_1, \dots, x_n) n действительных чисел и обозначается R^n . \square

Числовые множества:

$N = \{1, 2, 3, 4, \dots\}$ – множество натуральных чисел;

$P = \{2, 3, 5, 7, 11, \dots\}$ – множество простых чисел;

$Z = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ – множество целых чисел;

$Q = \left\{ \frac{m}{n}, m \in Z, n \in (Z \setminus \{0\}) \right\}$ – множество рациональных чисел;

R – множество вещественных (действительных) чисел;

R^+ – множество вещественных (действительных) положительных чисел;

R_0^+ – множество вещественных (действительных) неотрицательных чисел;

C – множество комплексных чисел.

Формулы для операций над множествами:

Для $\forall A, B, C \subset U$ выполняются свойства:

$$A \cup A = A, \quad A \cap A = A \quad (1) \text{ идемпотентность;}$$

$$A \cup B = B \cup A, \quad A \cap B = B \cap A \quad (2) \text{ коммутативность;}$$

$$\left. \begin{aligned} (A \cup B) \cup C &= A \cup (B \cup C), \\ (A \cap B) \cap C &= A \cap (B \cap C) \end{aligned} \right\} (3) \text{ ассоциативность;}$$

$$\left. \begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned} \right\} (4) \text{ дистрибутивность}$$

(общий “множитель” в двух скобках с одной и той же операцией можно выносить за скобки);

$$A \cup (A \cap B) = A, \quad A \cap (A \cup B) = A \quad (5) \text{ поглощение;}$$

$$\begin{aligned}
A \cup \emptyset &= A, & A \cap \emptyset &= \emptyset & (6) \text{ свойства пустого множества;} \\
A \cup U &= U, & A \cap U &= A & (7) \text{ свойства универсального множества;} \\
\overline{\overline{A}} &= A & & & (8) \text{ инволютивность;} \\
\overline{A \cup B} &= \overline{A} \cap \overline{B}, & \overline{A \cap B} &= \overline{A} \cup \overline{B} & (9) \text{ законы де Моргана;} \\
A \cup \overline{A} &= U, & A \cap \overline{A} &= \emptyset & (10) \text{ свойство дополнения;} \\
(A \cap B) \cup (A \cap \overline{B}) &= A, & (A \cup B) \cap (A \cup \overline{B}) &= A & (11) \text{ законы склеивания.}
\end{aligned}$$

При использовании несколько раз одной из операций \cup или \cap и группировки множеств с помощью скобок (...) будем иногда скобки опускать. Например:

$$\begin{aligned}
(A \cup B) \cup C &= A \cup B \cup C, & A \cup (B \cup C) &= A \cup B \cup C, \\
(A \cap B) \cap C &= A \cap B \cap C, & A \cap (B \cap C) &= A \cap B \cap C.
\end{aligned}$$

Множество A называется *конечным*, если оно состоит из конечного числа элементов. Это число называется *мощностью* множества A и обозначается $|A| = \text{card}(A)$, $|\emptyset| = 0$, но $|\{\emptyset\}| = 1$.

Два конечных множества называются *равномощными*, если их мощности равны, т.е. $|A| = |B|$.

Для любых конечных множеств A, B, C выполняются равенства

$$\begin{aligned}
|A \cup B| &= |A| + |B| - |A \cap B|, \\
|A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|
\end{aligned}$$

– формула перекрытий, формула включения и исключения.

В множестве $X = \{a, b, c\}$ из трех элементов можно рассмотреть восемь подмножеств:

$$P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Аналогичным образом для множества из n элементов можно образовать 2^n подмножеств.

С каждым конечным множеством A связаны числовые характеристики: мощность множества $|A|$ и число его подмножеств $2^{|A|}$.

Если множества A и B конечны, то число пар в декартовом произведении $A \times B$ равно произведению чисел элементов этих множеств $|A \times B| = |A| \times |B|$.

Доказательство равенства двух множеств проводится либо с использованием формул операций над множествами, либо исходя из определения операций. При использовании определений операций берется произвольный элемент из первого множества и путем каких-то рассуждений показывается, что он принадлежит второму множеству. Затем берется произвольный элемент из второго множества и путем некоторых рассуждений показывается, что он принадлежит первому множеству.

Пример 6. Доказать равенство $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Решение. *Первый способ* с использованием определений операций над множествами.

Для доказательства равенства двух множеств необходимо доказать два включения $A \setminus (B \cup C) \subset (A \setminus B) \cap (A \setminus C)$ и $(A \setminus B) \cap (A \setminus C) \subset A \setminus (B \cup C)$.

а) Пусть $x \in (A \setminus (B \cup C))$, тогда

$$\rightarrow \left\{ \begin{array}{l} x \in A, \\ x \notin B \cup C. \end{array} \right. \rightarrow \left\{ \begin{array}{l} x \in A, \\ x \notin B, \\ x \notin C. \end{array} \right. \rightarrow \left\{ \begin{array}{l} x \in A \setminus B, \\ x \in A \setminus C. \end{array} \right. \rightarrow x \in (A \setminus B) \cap (A \setminus C).$$

Таким образом, доказано, что если $x \in (A \setminus (B \cup C))$, то $x \in (A \setminus B) \cap (A \setminus C)$, т.е. доказано включение $A \setminus (B \cup C) \subset (A \setminus B) \cap (A \setminus C)$.

б) Пусть $x \in (A \setminus B) \cap (A \setminus C)$, тогда

$$\left\{ \begin{array}{l} x \in A \setminus B, \\ x \in A \setminus C. \end{array} \right. \rightarrow \left\{ \begin{array}{l} x \in A, \\ x \notin B, \\ x \notin C. \end{array} \right. \rightarrow \left\{ \begin{array}{l} x \in A, \\ x \notin (B \cup C). \end{array} \right. \rightarrow x \in (A \setminus (B \cup C)).$$

Таким образом, доказано, что если $x \in (A \setminus B) \cap (A \setminus C)$, то $x \in (A \setminus (B \cup C))$.

Второй способ с использованием формул.

$$\begin{aligned} A \setminus (B \cup C) &= A \cap \overline{B \cup C} \stackrel{(9)}{=} A \cap (\overline{B} \cap \overline{C}) \stackrel{(1)}{=} (A \cap A) \cap (\overline{B} \cap \overline{C}) = \square \\ &= A \cap A \cap \overline{B} \cap \overline{C} \stackrel{(3),(2)}{=} (A \cap \overline{B}) \cap (A \cap \overline{C}) = (A \setminus B) \cap (A \setminus C). \end{aligned}$$

Пример 7. Сколько чисел среди первых 200 натуральных чисел не делятся ни на 2, ни на 3, ни на 5?

Решение. Обозначим через A – множество чисел, делящихся на 2, B – множество чисел, делящихся на 3 и C – делящихся на 5. Тогда $A \cup B \cup C$ – числа, которые делятся хотя бы на одно из чисел 2, 3, 5. Число элементов множества $A \cup B \cup C$ найдем по формуле:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Для множества $A = \{2, 4, \dots, 200\}$ получаем $|A| = 100$, для множества $B = \{3, 6, \dots, 198\}$ следует $|B| = 66$ и для множества $C = \{5, 10, \dots, 200\}$ получаем $|C| = 40$.

Множество чисел, которые одновременно делятся на 2 и 3, т.е. делятся на 6, имеет вид $A \cap B = \{6, 12, \dots, 198\}$, причем $|A \cap B| = 33$.

Аналогично $A \cap C = \{10, 20, \dots, 200\}$, $|A \cap C| = 20$, $B \cap C = \{15, 30, \dots, 195\}$, $|B \cap C| = 13$, $A \cap B \cap C = \{30, 60, \dots, 180\}$, $|A \cap B \cap C| = 6$, $|A \cup B \cup C| = 100 + 66 + 40 - 33 - 20 - 13 + 6 = 146$.

Количество чисел, которые не делятся ни на 2, ни на 3, ни на 5, равно $200 - |A \cup B \cup C|$, т.е. равно 54.

Замечание 1. Методом решета Эратосфена можно удалить из множества $\{1, 2, \dots, 200\}$ натуральные числа, которые делятся на 2 или на 3 или на 5, но этот процесс будет долгим. Применим модифицированный вариант решета Эратосфена. Наименьшее общее кратное чисел 2, 3, 5 равно 30, поэтому количество чисел, не делящихся ни на 2, ни на 3, ни на 5, в множествах $\{1, 2, \dots, 30\}$, $\{31, 32, \dots, 60\}$, \dots , $\{151, 152, \dots, 180\}$, полученных одно из другого сдвигом на 30, будет одинаковым. Действительно, любая пара чисел x и $30k + x$, где k – произвольное число, ведет себя одинаково относительно делимости на 2 или на 3 или на 5. Поэтому достаточно найти искомое количество чисел на множестве $\{1, 2, \dots, 30\}$, затем это количество умножить на число таких периодов и добавить необходимые числа из оставшегося множества $\{181, 182, \dots, 200\}$. Окончательно получаем $8 \cdot 6 + 6 = 54$.

Эти решения требуют приблизительно одинакового времени.

Решение, приведенное выше, иллюстрирует применение теоремы включений и исключений. Последнее решение использует догадку о периодичности значений функции на множестве и ее аддитивности.

Замечание 2. Эти вычисления быстро проверяются для любого значения n с помощью простейшей компьютерной программы, приведенной в приложении.

б) *Отображения*

Пусть X и Y – произвольные множества. Если каждому элементу $x \in X$ сопоставлен некоторый единственный элемент $y \in Y$ по правилу (закону) f , то говорят, что задано отображение f множества X в множество Y и пишут $f: X \rightarrow Y$ или $X \xrightarrow{f} Y$.

Элемент y обозначается через $f(x)$ и называется образом элемента x при отображении f , а элемент x – прообразом элемента y . Если множество $A \subset X$, то через $f(A)$ обозначается множество образов всех элементов множества A и называется образом множества A при отображении f .

Множество всех элементов в X , образы которых при отображении f содержатся в данном множестве $B \subset Y$, называется прообразом (полным прообразом) множества B при отображении f и обозначается $f^{-1}(B)$.

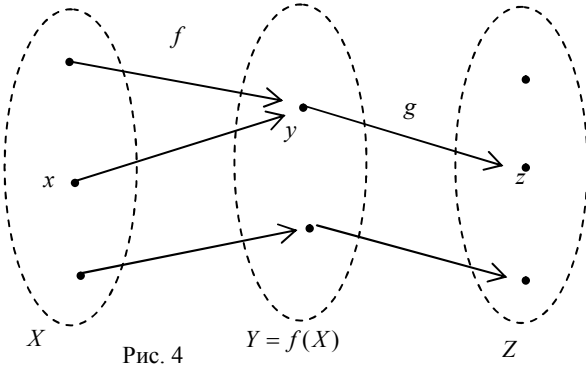
Отображение $f: X \rightarrow Y$ называется отображением множества X на множество Y (сюръективным), если $f(X) = Y$.

Отображение $f: X \rightarrow Y$ называется взаимно-однозначным (инъективным), если любые два различных элемента x_1 и x_2 из X имеют различные образы $f(x_1)$ и $f(x_2)$.

Тождественное отображение $1_X: X \rightarrow X$ определяется равенством $1_X(x) = x$ для любого $x \in X$.

Включением множества $B \subset A$ в множество A называется такое отображение $i: B \rightarrow A$, что $i(x) = x$ для любого $x \in B$.

Образование $f: X \rightarrow Y$ называется биективным (биекцией), если оно инъективно и сюръективно.



На рис. 4 образование f – сюръективно, но не инъективно. Образование инъективно, но не сюръективно.

Образование $f: X \rightarrow Y$ называется обратимым, если существует такое образование $g: Y \rightarrow X$, что $g \cdot f = 1_X$ и $f \cdot g = 1_Y$. Образование g называется обратным к образованию f и обозначается f^{-1} .

Образование $f: X \rightarrow Y$ обратимо тогда и только тогда, когда оно биективное.

Пусть даны образования $f: X \rightarrow Y$ и $g: Y \rightarrow Z$. Образование $h: X \rightarrow Z$, определяемое формулой $h(x) = g[f(x)]$, называется композицией образований f и g и обозначается $g \circ f$. Образование f иногда называют внутренней операцией или первым множителем, а образование g – внешней операцией или вторым множителем. Название определяется близостью к элементу x , на который необходимо действовать образованиями.

Для образований, заданных на рис. 4, $(g \circ f)(x) = z$.

Для любых двух образований композиция образований, вообще говоря, не удовлетворяет условию коммутативности, т.е. $g \circ f \neq f \circ g$. Сравним композиции двух образований на примерах двух функций, выполненных в различном порядке.

Примеры. В следующих приводимых примерах $f: R \rightarrow R$ и $g: R \rightarrow R$.

1. Для $f(x) = x + 2$, $g(x) = x^2$ получаем

$$(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 + 2,$$

$$(g \circ f)(x) = g(f(x)) = g(x + 2) = (x + 2)^2.$$

2. Рассмотрим постоянные, но различные образования: $f(x) = x_1, \forall x$; $g(x) = x_2, \forall x: x_1 \neq x_2$, тогда $(g \circ f)(x) = x_2$, $(f \circ g)(x) = x_1$.

Существуют функции, для которых выполняется коммутативность композиции $g \cdot f = f \cdot g$.

3. Например, для $f(x) = x + 2$, $g(x) = x - 3$ получаем

$$(f \circ g)(x) = f(g(x)) = f(x - 3) = (x - 3) + 2 = x - 1,$$

$$(g \circ f)(x) = g(f(x)) = g(x + 2) = (x + 2) - 3 = x - 1.$$

Обратим внимание на два следующих примера.

4. Для $f(x) = x^3$, $g(x) = \sqrt[3]{x}$ получаем

$$(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x,$$

$$(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x.$$

В этом случае $g \cdot f = f \cdot g$.

5. Для $f(x) = x^2$, $g(x) = \sqrt{x}$ получаем

$$(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x,$$

$$(g \circ f)(x) = g(f(x)) = g(x^2) = \sqrt{x^2} = |x|.$$

Однако, в этом случае нельзя утверждать, что выполняется равенство $g \circ f = f \circ g$. Обычно приводят пояснение, состоящее в том, что $x \neq |x|$. Но причина в другом. Прежде чем составить композицию, необходимо определить область определения выражений, составляющих композицию.

Композиция $(g \circ f)(x) = \sqrt{x^2} = |x|$ определена для любого действительного числа x , а композиция $(f \circ g)(x) = (\sqrt{x})^2 = x$ определена только для $x \geq 0$.

Если каждую из функций $f(x) = x^2$, $g(x) = \sqrt{x}$ задать на множестве $X = \{x \in R : x \geq 0\}$, то в этом случае можно утверждать, что выполняется условие $g \circ f = f \circ g$.

Теорема 1. Композиция отображений подчиняется ассоциативному закону, т.е. если $f: X \rightarrow Y, g: Y \rightarrow Z, h: Z \rightarrow W$, то выполняется равенство $h \circ (g \circ f) = (h \circ g) \circ f$.

Доказательство (рис. 5).

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x).$$

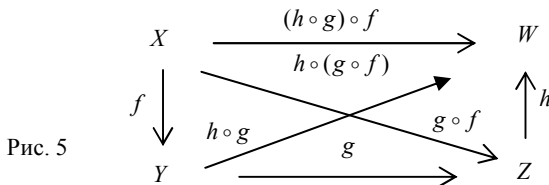


Рис. 5

Для тождественного отображения 1_X и отображения $f: X \rightarrow Y$ выполняются свойства: $f \circ 1_X = f$, $1_Y \circ f = f$.

Пусть X – произвольное множество. Биективное отображение этого множества на себя называется *преобразованием* множества.

Симметрия S_l относительно прямой l , поворот R_O^φ вокруг точки O на угол φ , параллельный перенос T_a на вектор \vec{a} на плоскости являются примерами преобразований плоскости.

Пример. На множестве $X = \{x_1, x_2, x_3\}$ заданы все биективные преобразования $G_X = \{f_0, f_1, f_2, f_3, f_4, f_5\}$:

$$f_0 : f_0(x_1) = x_1, f_0(x_2) = x_2, f_0(x_3) = x_3, \quad f_3 : f_3(x_1) = x_1, f_3(x_2) = x_3, f_3(x_3) = x_2;$$

$$f_1 : f_1(x_1) = x_2, f_1(x_2) = x_3, f_1(x_3) = x_1, \quad f_4 : f_4(x_1) = x_3, f_4(x_2) = x_2, f_4(x_3) = x_1;$$

$$f_2 : f_2(x_1) = x_3, f_2(x_2) = x_1, f_2(x_3) = x_2, \quad f_5 : f_5(x_1) = x_2, f_5(x_2) = x_1, f_5(x_3) = x_3.$$

Составим всевозможные произведения отображений. Запишем их в таблицу, которую называют таблицей Кэли.

Таблица 1

Внутренняя опера- ция \ внешняя операция	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

По ней удобно проверять ассоциативное и коммутативное свойство операции, находить тождественное и обратное отображения.

в) *Метод математической индукции*

Рассмотрим один из важнейших методов поиска закономерностей для дискретной величины n и доказательства утверждений.

Принцип математической индукции:

Пусть $P(n)$ – некоторое утверждение, зависящее от натурального числа n .

Это утверждение справедливо для всякого натурального n , если

1) оно справедливо для $n = 1$;

2) из справедливости утверждение для некоторого $n = k$, следует его справедливость для $n = k + 1$.

Доказательства утверждений с помощью принципа математической индукции называются методом математической индукции.

Пример 8. Найти сумму $S_n = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n(n+1)}$.

Решение.

$$S_1 = \frac{1}{1 \cdot 2} = \frac{1}{2}, S_2 = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} = \frac{2}{3}, S_3 = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} = \frac{3}{4}.$$

Появляется гипотеза, что $S_n = \frac{n}{n+1}$. Проверим ее методом математической индукции, т.е. докажем, что утверждение $S_n = \frac{n}{n+1}$ справедливо для любого натурального числа n .

Для $n=1$ гипотеза верна, т.к. $S_1 = \frac{1}{2}$.

Предположим, что гипотеза верна при $n=k$, т.е.

$$S_k = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{k(k+1)} = \frac{k}{k+1}.$$

Докажем, что гипотеза верна и при $n=k+1$, т.е. что $S_{k+1} = \frac{k+1}{k+2}$.

Действительно,

$$S_{k+1} = S_k + \frac{1}{(k+1)(k+2)} = \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = \frac{k^2 + 2k + 1}{(k+1)(k+2)} = \frac{k+1}{k+2}.$$

На основании принципа математической индукции можно утверждать, что $S_n = \frac{n}{n+1}$ справедливо при любом натуральном n . \square

Замечание. Иногда утверждение доказывается не для всякого натурального числа n , а для всякого натурального числа, превосходящего некоторое число n . Например, любое утверждение для n -угольника имеет смысл только при $n \geq 3$.

Метод математической индукции с базисом a :

Пусть $P(n)$ высказывание, обладающее свойствами:

- 1) $P(a)$ – истинно,
- 2) из справедливости высказывания для произвольного $k \geq a$ следует его справедливость для $k+1$. Тогда высказывание $P(n)$ истинно для каждого $n \geq a$.

Задачи.

1.1. Установите, какие из пар множеств на плоскости связаны отношением включения:

- а) A – множество параллелограммов, B – множество ромбов;
- б) A – множество прямоугольников, B – множество ромбов;
- в) A – множество прямоугольных треугольников с острым углом в 45° , B – множество равнобедренных треугольников;
- г) A – множество ромбов с прямым углом, B – множество прямоугольников с равными сторонами.

1.2. Найдите множества $A \cup B, A \cap B, A \setminus B, B \setminus A, A \Delta B$, если:

- а) $A = \{2, 5, 6, 7, 9\}, B = \{4, 6, 7, 8\}$; г) $A = \mathbb{Z}, B = \mathbb{N}$;
- б) $A = \{5, 7, 9\}, B = \{4, 6, 8\}$; д) $A = \mathbb{R}, B = \mathbb{Q}$;

- в) $A = \{1, 2, 3, 4\}, B = \{3, 4, 5, 6\}$;
 е) $A = \mathbb{Z}, B = \mathbb{Q}$.

1.3. На рис. 6. построены три множества A, B, C , являющиеся кругами на плоскости. Для каждой из штрихованной областей обозначьте соответствующее множество и выразите его, используя операции над множествами A, B, C .

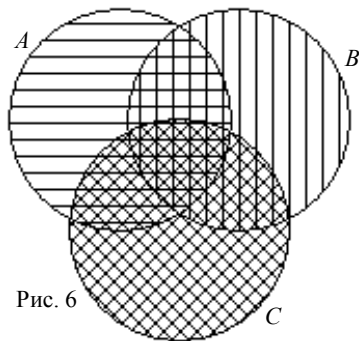


Рис. 6

1.4. Изобразите с помощью диаграмм Венна следующие множества, определяющие предметы, изучаемые на различных факультетах университета:

$A = \{\text{математический анализ, языки программирования, дискретная математика, аналитическая геометрия, английский язык, философия}\}$,

$B = \{\text{физика, математический анализ, история, английский язык, аналитическая геометрия}\}$,

$C = \{\text{экономическая теория, высшая математика, философия, история, английский язык}\}$.

Определите множества: $A \cap B \cap C$, $A \setminus (B \cap C)$, $A \cap (B \Delta C)$, $(A \setminus B) \cap (A \setminus C)$.

1.5. Пусть $\{U = \{n \in \mathbb{Z} : 1 \leq n \leq 12\}, A = \{n : n - \text{делитель числа } 12\}$, $B = \{n : n - \text{простое число}\}$, $C = \{n : n - \text{нечетное число}\}$. Составьте список элементов для множеств $A, B, C, A \cap B, A \cap B \cap C, B \cup C, B \cap \bar{C}, A \setminus C, \overline{A \cap B}, \overline{A \cup C}, A \Delta B$.

1.6. Даны множества A, B и C . С помощью операций запишите множество элементов, которые принадлежат:

- всем трем множествам;
- по крайней мере двум из этих множеств;
- любым двум из этих множеств, но не принадлежат всем трем множествам;
- по крайней мере одному из этих множеств;
- любому из этих множеств, но не принадлежат двум остальным.

1.7. A и B – два множества. В каком случае:

- $A = A \cup B$;
- $A = A \cap B$?

1.8. Всегда ли справедливо равенство $(A \setminus B) \cup B = A$? Если равенство не выполняется, то приведите примеры таких множеств.

1.9. Следует ли из равенства $A = B \cup C$, что $A \setminus C = B$?

1.10. Выполняется ли ассоциативное свойство для операции разности множеств, т.е. $(A \setminus B) \setminus C = A \setminus (B \setminus C)$? Если равенство не выполняется, то приведите примеры.

1.11. Докажите, что:

а) если $A \subset B \cap C$, то $A \subset B$ и $A \subset C$;

б) если $A \cap B \subset C$, то $A \subset \overline{B} \cup C$;

в) если $A \cup B \subset C$, то $A \subset C$ и $B \subset C$;

г) если $A \subset B \cup C$, то $A \cap \overline{B} \subset C$.

1.12. Докажите, что

а) если $A \subset B$, то $\overline{B} \subset \overline{A}$;

б) если $A \subset B$, то $A \cup C \subset B \cup C$;

в) если $A \subset B$, то $A \cap C \subset B \cap C$.

1.13. Докажите, что $(A \cup B) \setminus B = A$ в том и только в том случае, если $A \cap B = \emptyset$.

1.14. Докажите, что $(A \setminus B) \cup B = A$ в том и только в том случае, если $B \subset A$.

1.15. Пусть $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$ – универсальное множество, $A = \{1, 2, 3, 4, 5\}$. Найдите множество B , если известно, что:

а) $B \setminus A = \{6, 7\}$, $A \cap B = \{1, 3, 5\}$; б) $A \setminus B = \{2, 4\}$, $B \setminus A = \{6, 7\}$.

1.16. Докажите свойства симметричной разности множеств:

а) $\emptyset \Delta A = A$, $A \Delta A = \emptyset$; б) $A \Delta B = B \Delta A$; в) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$;

г) $A \Delta (A \Delta B) = B$; д) $A \Delta B = (A \setminus B) \cup (B \setminus A)$; е) $A \Delta B = \overline{A \Delta B}$.

1.17. Докажите, что если $C = A \Delta B$, то $A \Delta C = B$.

1.18. Пусть A и B – подмножества множества X . Докажите равенства:

а) $A \setminus B = A \cap (X \setminus B)$;

б) $X \setminus (A \setminus B) = (X \setminus A) \cup B$;

в) $(X \setminus A) \Delta (X \setminus B) = A \Delta B$.

1.19. Докажите равенства:

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

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

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

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

д) $A \setminus B = A \setminus (A \cap B) = (A \cup B) \setminus B$;

е) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$;

- ж) $(A \setminus B) \setminus C = (A \setminus (B \cup C))$;
- з) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$;
- и) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
- к) $A \setminus (B \cup C) = (A \setminus B) \setminus C$;
- л) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
- м) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$;
- н) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$;
- о) $\overline{A \setminus B} = \overline{A} \cup B$;
- п) $A \cap B = A \setminus (A \setminus B)$;
- р) $(\overline{A} \cup B) \cap A = A \cap B$;
- с) $(A \setminus B) \cap (B \setminus A) = \emptyset$;
- т) $(A \setminus B) \cap (C \setminus D) = (A \cap C) \setminus (B \cap D)$;
- у) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$;
- ф) $A \Delta B = (A \cup B) \cap (\overline{A} \cup \overline{B})$.

1.20. Докажите дистрибутивность относительно операций \cap, Δ и \setminus в следующих равенствах:

- а) $(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C)$;
- б) $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$;
- в) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$;
- г) $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$;
- д) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$;
- е) $(A \Delta B) \setminus C = (A \setminus C) \Delta (B \setminus C)$.

1.21. Минимальный набор операций, через который выражаются все остальные операции над множествами, называется базисом операций. Докажите, что следующие наборы операций являются базисами операций среди введенных ранее операций $\{\cup, \cap, \setminus, \Delta, \overline{}\}$, где $\overline{}$ является операцией дополнения:

а) (\cup, \setminus) ; б) (\cap, Δ) ; в) $(\cap, \overline{})$; г) (\setminus) ; д) базис Шеффера $(\uparrow, \overline{})$, где операция Шеффера для множеств определяется по формуле $A \uparrow B = \overline{A} \cap \overline{B}$.

1.22. Изобразите множество $A \times B$ в прямоугольной декартовой системе координат на плоскости, если:

- а) $A = \{1, 3\}, B = \{1, 2, 4\}$; б) $A = (1; 3), B = (1; 4)$.

1.23. Сколько чисел среди первой тысячи натуральных чисел не делятся ни на 2, ни на 3, ни на 7?

1.24. По итогам экзаменационной сессии из 35 студентов потока оценку «хорошо» по математическому анализу имели 14 студентов, по физике – 15, по геометрии – 18, по математическому анализу и физике – 7, по математическому анализу и геометрии – 9, по физике и геометрии – 6, по всем трем предметам – 4. Сколько студентов получили хотя бы по одной отметке «хорошо»?

1.25. Найти все отображения множества $X = \{a, b, c\}$ в множество $Y = \{c, d\}$. Сколько из них являются:

а) инъективными; б) сюръективными; в) биективными?

1.26. Пусть на множестве R заданы отображения $f(x) = 1 - x, g(x) = \frac{1}{x}, h(x) = \sqrt{x}$. Найдите формулы, задающие следующие композиции: а) $f \circ g \circ h$; б) $g \circ h \circ f$; в) $h \circ f \circ g$.

1.27. Постройте графики следующих числовых функций: $f(x) = \max(x, 0), g(x) = -\min(x, 0), f \circ f, g \circ g, f \circ g, g \circ f$.

1.28. Пусть на R задана функция $y = f(x)$. Представьте в виде композиции данной функции и некоторой функции (порядок их выполнения определите самостоятельно) следующие функции: а) $y = f(x - a)$; б) $y = f(x) + b$; в) $y = k f(x)$; г) $y = f(\omega x)$; д) $y = |f(x)|$; е) $y = f(|x|)$.

В каждом случае сформулируйте правило для перехода от графика функции $y = f(x)$ к графику указанной сложной функции.

$f_1 : X \rightarrow X$



Рис. 7

$f_2 : X \rightarrow X$

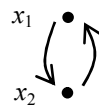


Рис. 8

1.29. На множестве $\{x_1, x_2\}$ заданы все биективные отображения (рис. 7, 8). Составьте таблицу умножения отображений для этих преобразований множества. Запишите аналитически действие каждого отображения на элементы множества. Для каждого преобразования найдите обратное преобразование.

1.30. Пусть $f : A \rightarrow B, A$ и B – конечные множества, состоящие соответственно из a и b элементов. Докажите, что:

а) если f – инъективно, то $a \leq b$;

б) если f – сюръективно, то $a \geq b$;

в) если f – биективно, то $a = b$.

1.31. Пусть $f: A \rightarrow B$, A и B – множества, имеющие одинаковое конечное число элементов. Докажите, что:

- а) если f – инъективно, то f – биективно;
б) если f – сюръективно, то f – биективно.

1.32. Приведите пример функции $f: X \rightarrow Y$ и двух множеств $A, B \in X$, таких, что $f(A \cap B) \neq f(A) \cap f(B)$.

1.33. Дано отображение $f: X \rightarrow Y$.

а) верно ли равенство $f^{-1}(f(A)) = A$ для $\forall A \subset X$;

б) верно ли равенство $f(f^{-1}(B)) = B$ для $\forall B \subset Y$?

1.34. Докажите тождества:

а) $1 + 3 + 5 + \dots + (2n - 1) = n^2$;

б) $1^2 + 3^2 + 5^2 + \dots + (2n - 1)^2 = \frac{n(2n - 1)(2n + 1)}{3}$;

в) $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n + 1)(2n + 1)}{6}$;

г) $1^3 + 2^3 + 3^2 + \dots + n^3 = (1 + 2 + 3 + \dots + n)^2$;

д) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n + 1) = \frac{n(n + 1)(n + 2)}{3}$;

е) $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \dots + n(n + 1)(n + 2) = \frac{n(n + 1)(n + 2)(n + 3)}{4}$;

ж) $\frac{1^2}{1 \cdot 3} + \frac{2^2}{3 \cdot 5} + \frac{3^2}{5 \cdot 7} \dots + \frac{n^2}{(2n - 1)(2n + 1)} = \frac{n(n + 1)}{2(2n + 1)}$;

з) $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \dots + n \cdot n! = (n + 1)! - 1$;

и) $1 \cdot 4 + 2 \cdot 7 + \dots + n(3n + 1) = n(n + 1)^2$.

1.35. Найдите суммы:

а) $S_n = \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n - 1)(2n + 1)}$;

б) $S_n = \frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \dots + \frac{1}{(3n - 2)(3n + 1)}$.

1.36. Докажите, что сумма кубов трех последовательных натуральных чисел делится на 9.

1.37. Докажите, что $2^{2^n} + 1$ оканчивается цифрой 7 для всех $n > 1$.

1.38. Докажите, что следующие соотношения выполняются для любого натурального n :

- а) $(10^n + 18n - 1) : 27$; б) $(n^3 + 11n) : 6$; в) $(n^3 + 5n) : 6$;
 г) $(4^n + 15n - 1) : 9$; д) $(6^{2n+1} + 1) : 7$; е) $(11^{n+2} + 12^{2n+1}) : 133$,

где $m:n$ означает, что натуральное число m нацело делится на натуральное число n .

§ 2. Комбинаторика и бином Ньютона

Комбинаторика – раздел математики, посвященный решению задач выбора и расположения элементов некоторого множества по заданному правилу.

Правило суммы:

Если объект A можно выбрать n_1 способами, а объект B можно выбрать n_2 способами, причем выбор одного объекта не зависит от выбора другого объекта, то выбор « A или B » можно выполнить $n_1 + n_2$ способами.

Правило произведения:

Пусть требуется выполнить одно за другим два действия. Если первое действие можно выполнить n_1 способами, а после этого второе действие – n_2 способами, то два действия можно выполнить $n_1 \cdot n_2$ способами.

Пример 1. Из города A в город B ведет три дороги, а из города B в город C две дороги. Сколько различных маршрутов существует из города A в город C ?

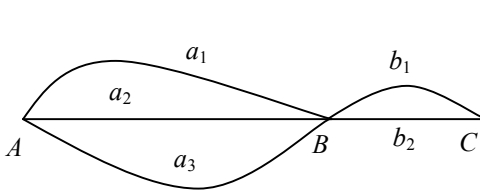


Рис. 9

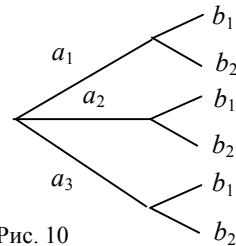


Рис. 10

Схема дорог на рисунке 9 показывает, что в точке A можно выбрать одну из дорог a_1, a_2, a_3 . Зафиксировав свой выбор на первом участке, мы имеем возможность снова в точке B выбрать путь из двух дорог, поэтому получаем 3×2 различных маршрутов: $a_1b_1, a_1b_2; a_2b_1, a_2b_2; a_3b_1, a_3b_2$.

Фактически задача решена на основе применения правила произведения, т.к. для выбора маршрута из города A в город C необходимо выполнить оба действия, т.е. выбрать маршрут из города A в город B , а потом выбрать маршрут из города B в город C .

Рисунок 10 наглядно иллюстрирует, сколькими способами можно выбрать различные маршруты для примера 1. \square

Рассмотрим опыт, состоящий в выборе наугад одного за другим k шаров из n пронумерованных шаров, содержащихся в урне.

Такой опыт называется *выборкой с возвращением*: если после каждого извлечения шара его номер записывается, шар возвращается обратно и, следовательно, может участвовать в дальнейшем отборе. Если из n пронумерованных

шаров выбирают k шаров с возвращением, то всего существует n^k различных упорядоченных выборов. В некоторых выборках элементы могут повторяться.

Эти выборки называются *размещениями с повторением из n элементов по k элементов*, а общее их количество обозначается $\overline{A}_n^k = n^k$.

Размещения с повторениями из трех элементов a, b, c по два элемента:

$aa, ba, ca, ab, bb, cb, ac, bc, cc$. Всего получаем $\overline{A}_3^2 = 3^2 = 9$ наборов.

Если же осуществляются выборки шаров без возвращения в урну, то получаем упорядоченные множества, называемые *размещениями из n элементов по k элементов*. После каждого вытаскивания шара в урне остается на один шар меньше, поэтому первый шар можно вытащить n способами, второй шар $n-1$ способами и т. д., k шар — $(n-k+1)$ способами. Все k шаров можно вытащить $n(n-1)(n-2)\dots(n-k+1)$ способами. Число размещений из n элементов по k элементов равно:

$$A_n^k = n(n-1)(n-2)\dots(n-k+1).$$

Два различных размещения из данных n элементов по k элементов различаются либо составом входящих в них элементов, либо, при одном и том же составе элементов, порядком их расположения.

Размещения из трех элементов a, b, c по два элемента:

ab, ac, ba, bc, ca, cb . Всего получаем $A_3^2 = 3 \cdot 2 = 6$ наборов.

Факториалом натурального числа n называется произведение

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n = \prod_{i=1}^n i = n!. \text{ Для } n=0 \text{ полагают } 0!=1.$$

При возрастании n функция $n!$ очень быстро возрастает (таблица 2).

Таблица 2

n	0	1	2	3	4	5	6	7	8	9	10
$n!$	1	1	2	6	24	120	720	5040	40320	362880	3628800

Размещения из n элементов по n элементов называются *перестановками*, а их количество обозначают P_n , поэтому:

$$A_n^n = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1 = n!, \quad P_n = n!$$

Перестановки для трех элементов: $abc, acb, bac, bca, cab, cba$. Число перестановок в этом случае равно $P_3 = 3! = 6$.

Любые две различные перестановки из n элементов имеют одинаковый состав элементов, но отличаются их порядком. Выборка в перестановке — упорядоченное множество.

Пусть дано конечное множество элементов $\{a, b, c, \dots, l\}$. *Перестановкой с повторениями*, в которой элемент a повторяется α раз, элемент b повторяется β раз, ..., элемент l повторяется ν раз, где $\alpha, \beta, \dots, \nu$ — заданные натуральные числа, называется всякое размещение с повторениями, в котором каждый элемент повторяется указанное число раз.

Число различных перестановок равно $\frac{(\alpha + \beta + \dots + \nu)!}{\alpha! \beta! \dots \nu!}$.

Перестановки с повторениями из трех элементов a, b, c , в которых элемент a повторяется 2 раза, а элементы b, c один раз:

$abc, aacb, abac, abca, acab, acba, baac, baca, bcaa, caab, caba, cbaa$.

Число перестановок с повторениями в этом случае равно $\frac{(2+1+1)!}{2! \cdot 1! \cdot 1!} = \frac{4!}{2!} = 12$.

Если при выборке из n элементов по k без возвращения рассматриваются неупорядоченные множества, то эти размещения называются *сочетаниями*.

В этом случае все размещения, содержащие одинаковые элементы, но отличающиеся порядком, считаются одинаковыми. Количество таких случаев равно количеству перестановок из k элементов. Поэтому число сочетаний из n элементов по k равно

$$C_n^k = \frac{A_n^k}{P_k} = \frac{n(n-1) \cdots (n-k+1)}{k!} = \frac{n!}{k! (n-k)!}.$$

Два сочетания из данных n элементов, взятых по k элементов, различны, если в одном из них содержится хотя бы один элемент, не содержащийся в другом.

Свойства $C_{n-1}^{k-1} + C_{n-1}^k = C_n^k$ и $C_n^0 + C_n^1 + \dots + C_{n-1}^{n-1} + C_n^n = 2^n$.

Пусть имеются предметы n видов и из них составляется набор, содержащий k элементов, причем некоторые элементы могут повторяться. Два набора считаются одинаковыми в том и только в том случае, когда они имеют один и тот же состав. Такие наборы назовем сочетаниями с повторениями из n элементов по k элементов. Число сочетаний с повторениями из n элементов по k обозначается \bar{C}_n^k и вычисляется по формуле $\bar{C}_n^k = C_{k+n-1}^k$.

Пример 2. Сколько существует треугольников, длины сторон которых принимают одно из следующих значений: 5, 6, 7, 8?

Решение. Треугольник существует, если сумма любых двух сторон больше третьей стороны. Любые пара из данных четырех чисел удовлетворяет этому условию, поэтому геометрическое условие на существование треугольника выполняется автоматически и задача с геометрическим содержанием превращается в чисто комбинаторную задачу. В этой задаче некоторые выборки могут содержать одинаковые элементы. Например, равносторонний треугольник (5; 5; 5), равнобедренный треугольник (5; 5; 8). Два равнобедренных треугольника (5; 5; 8) и (5; 8; 5) следует считать одинаковыми. Ответ $\bar{C}_4^3 = C_{3+4-1}^3 = C_6^3 = 20$.

Поясните второй способ решения этой задачи:

$$C_4^3 + C_4^1 \cdot C_3^1 + C_4^1 = 4 + 4 \cdot 3 + 4 = 20. \square$$

При решении комбинаторных задач часто возникает затруднение при выборе размещения, сочетания или перестановки для решения конкретной задачи.

Иногда руководствуются следующим алгоритмом:

1. Обратить внимание на порядок расположения элементов и на повтор элементов в выборке.
2. Если порядок элементов не имеет значения, то это сочетание.
3. Если порядок имеет значение, то это размещение или перестановки, причем это размещение, если не все элементы входят в выборку и перестановки, если все элементы входят в выборку.
4. Количество размещений или сочетаний определяется по таблице 3.

Таблица 3

Влияние порядка Повтор элементов	порядок существенен	порядок не существен
элементы повторяются	Размещения с повторениями $\overline{A}_n^k = n^k$	Сочетания с повторениями $\overline{C}_n^k = \frac{(n+k-1)!}{k!(n-1)!}$
элементы не повторяются	Размещения без повторений $A_n^k = n(n-1)\dots(n-k+1)$	Сочетания без повторений $C_n^k = \frac{n!}{k!(n-k)!}$

Пример 3. В почтовом отделении продаются открытки 10 видов. Сколькими способами можно купить 12 открыток?

Решение. Порядок открыток в предлагаемом наборе несущественен, поэтому набор открыток является сочетанием из 10 по 12, причем с повторением. Число способов купить 12 открыток равно $\overline{C}_{10}^{12} = C_{12+10-1}^{12} = C_{21}^{12}$.

Пример 4. Из трех преподавателей и девяти студентов нужно составить факультетскую команду из 7 человек. Сколькими способами можно составить команду, если в нее должен войти хотя бы один преподаватель?

Решение. В команде может быть: а) 1 преподаватель и 6 студентов; б) 2 преподавателя и 5 студентов; в) 3 преподавателя и 4 студента.

а) Выбор одного преподавателя из трех возможен C_3^1 способами, а шести студентов из девяти – C_9^6 . Используя правило произведения, получаем число способов выбрать одного преподавателя и шести студентов $C_3^1 \cdot C_9^6$.

б) Выбор двух преподавателей из трех возможен C_3^2 способами, а пяти студентов из девяти – C_9^5 . Число способов выбрать двух преподавателей и пяти студентов $C_3^2 \cdot C_9^5$.

в) Выбор трех преподавателей из трех возможен C_3^3 способами, а четырех студентов из девяти – C_9^4 . Число способов выбрать трех преподавателей и четырех студентов $C_3^3 \cdot C_9^4$.

Общее число способов сформировать команду, в состав которой должен войти хотя бы один преподаватель, по правилу суммы равно:

$$C_3^1 \cdot C_9^6 + C_3^2 \cdot C_9^5 + C_3^3 \cdot C_9^4 = 756. \quad \square$$

Формула бинома Ньютона:

$$(a+x)^n = a^n + C_n^1 a^{n-1} x + \dots + C_n^k a^{n-k} x^k + \dots + C_n^{n-1} a x^{n-1} + x^n.$$

Использование формулы бинома Ньютона для доказательства комбинаторных равенств:

а) Полагая в формуле бинома Ньютона $a=1, x=1$, получаем

$$C_n^0 + C_n^1 + C_n^2 + \dots + C_n^n = 2^n.$$

б) По формуле Ньютона

$$(1+x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + \dots + C_n^k x^k + \dots + C_n^n x^n.$$

Дифференцируя равенство, получим

$$n(1+x)^{n-1} = C_n^1 + 2C_n^2 x + \dots + kC_n^k x^{k-1} + \dots + nC_n^n x^{n-1}.$$

Полагая $x=1$, получаем

$$C_n^1 + 2C_n^2 + \dots + kC_n^k + \dots + nC_n^n = n \cdot 2^{n-1}.$$

Множество $X = \{x_1, x_2, \dots, x_n\}$ называется разбитым на подмножества X_1, X_2, \dots, X_k , если выполняются условия:

$$1) X_i \neq \emptyset \text{ для } \forall i; 2) X_i \cap X_j = \emptyset, \forall i, j; 3) \bigcup_i X_i = X.$$

Представление множества $X = X_1 \cup X_2 \cup \dots \cup X_k$ с указанными свойствами называется его разбиением.

Пусть подмножество X_i содержит n_i элементов, тогда $n_1 + n_2 + \dots + n_k = n$.

Пусть $C(n; n_1, n_2, \dots, n_k)$ – число разбиений множества $X = \{x_1, x_2, \dots, x_n\}$ на подмножества X_1, X_2, \dots, X_k , тогда

$$C(n; n_1, n_2, \dots, n_k) = \frac{n!}{n_1! n_2! \dots n_k!}.$$

$$\text{При } k=2 \text{ получаем равенство } C(n; n_1, n_2) = \frac{n!}{n_1! n_2!} = \frac{n!}{n_1! (n-n_1)!} = C_n^{n_1} = C_n^{n_2}.$$

Числа $C(n; n_1, n_2, \dots, n_k)$ являются коэффициентами в полиномиальной формуле, являющейся обобщением формулы бинома Ньютона:

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{n_1, n_2, \dots, n_k} C(n; n_1, n_2, \dots, n_k) x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}.$$

Пример 5. Найти: а) коэффициент при $x^2 y^3 z^4$ в разложении $(x+y+z)^9$;

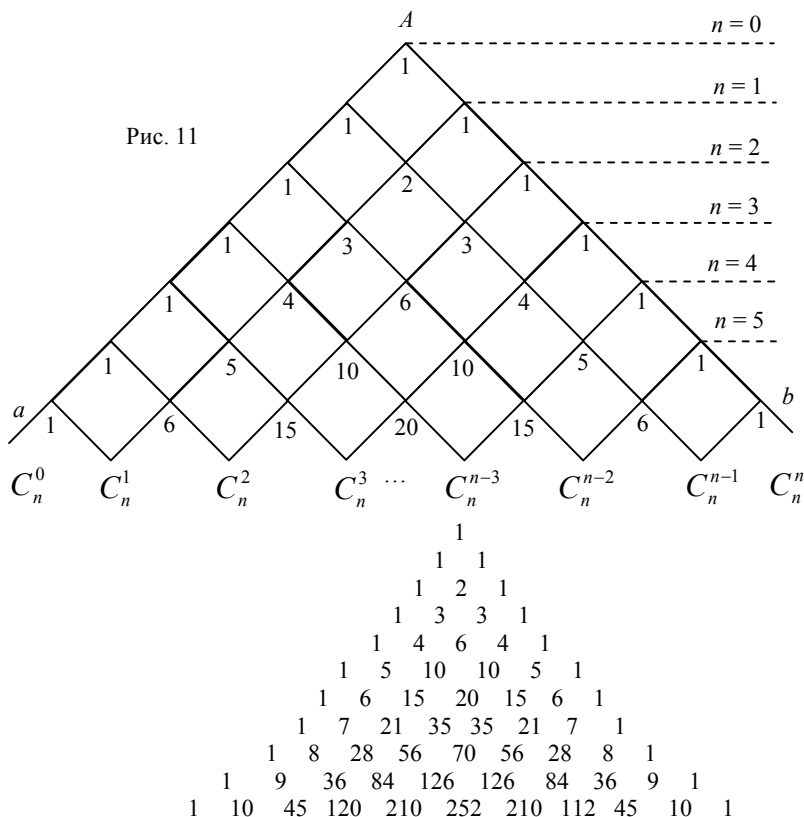
б) коэффициент при $x^2 y^3$ в разложении $(x+y+z)^9$.

$$\text{Решение. а) } C(9; 2, 3, 4) = \frac{9!}{2! \cdot 3! \cdot 4!} = 1260.$$

б) В полиномиальной формуле $(x+y+z)^9$ каждое слагаемое имеет степень, равную девяти. Слагаемое с выражением $x^2 y^3$ в разложении $(x+y+z)^9$ можно

получить из слагаемого $C(9;2,3,4)x^2y^3z^4$, если положить $z=2$, поэтому коэффициент при x^2y^3 в разложении $(x+y+2)^9$ равен $1260 \cdot 16 = 20160$. \square

Для малых значений n коэффициенты C_n^k определяют из треугольника Паскаля. На рис. 11 показан алгоритм составления треугольника Паскаля, а затем приведены значения числа сочетаний $n \leq 10$.



Задачи.

2.1. В группе 25 студентов. Сколькими способами можно выбрать старосту, физорга и культорга, если нет ограничений для избрания и эти должности должны занимать различные студенты? Порядок элементов имеет значение в этой выборке?

2.2. В группе 25 студентов. Сколькими способами можно выбрать бригаду из трех человек для уборки территории? Порядок элементов имеет значение в этой выборке?

2.3. В группе 25 студентов. Сколькими способами можно выбрать бригаду для уборки территории вокруг университета, в которой один из студентов назначается ответственным? Порядок элементов имеет значение в этой выборке?

2.4. Множество X содержит n элементов, а множество Y содержит m элементов.

a) Сколькими способами можно построить отображения множества X в множество Y ?

b) Сколько существует биективных отображений $f: X \rightarrow Y$, если $n = m$?

2.5. Имеется n пронумерованных элементов. Сколько размещений из n элементов по k элементов начинается с первого элемента?

2.6. Сколько делителей имеет число 210?

2.7. Сколько делителей имеет число 30030?

2.8. В группе 15 девушек и 10 парней. Сколько различных пар (парень + девушка) можно составить для танцев? А сколько пар может выйти одновременно танцевать?

2.9. Сколько упорядоченных троек, в которых две соседние буквы не являются одинаковыми, можно составить из 32 букв?

2.10. Лектор имеет три пиджака, пять рубашек, два галстука и трое брюк. Сколько различных костюмов можно составить из этих предметов?

2.11. Студентка имеет шесть платьев, четыре юбки и три блузки, причем узоры и цвета этих объектов различные. Сколько различных нарядов она может составить из своей одежды, если юбка или блузка не надевается поверх платья? Сколько различных нарядов она может составить, если юбку или блузку надеть поверх платья?

2.12. Шесть джентльменов при встрече решили обменяться визитными карточками. Сколько карточек потребуется?

2.13. Шесть студентов при встрече обменялись рукопожатиями (каждый с каждым). Сколько было сделано рукопожатий?

2.14. Сколько различных двузначных чисел можно составить из цифр 0, 1, 2, 3, 4? Число 0 может быть записано на первое место в двузначном числе?

2.15. Сколько различных шестизначных чисел можно составить в машинном коде, используя цифры 0,1? В машинном коде число может начинаться с 0?

2.16. Сколько различных двузначных чисел можно составить, используя шестнадцатеричную систему счисления: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f\}$?

2.17. Сколькими способами можно разложить в три кармана 6 монет различного достоинства?

2.18. Имеется 4 книжных шкафа, в каждом из которых находится 100 книг. Все книги в шкафах различные. Сколькими способами можно выбрать из них пару книг (порядок книг в паре не имеет значения), так, чтобы книги в паре были из различных шкафов?

2.19. Сколько существует двузначных чисел, имеющих обе четные цифры?

2.20. Сколько существует шестизначных наборов билетов, которые читаются одинаково слева направо и справа налево? Как изменится ответ, если рассматривать пятизначные “счастливые билеты”?

2.21. Сколько существует пятизначных чисел, которые делятся на 5?

2.22. Сколькими способами можно обозначить вершины четырехугольника, используя буквы: A, B, C, D, E, F ?

2.23. В урне 36 шаров, пронумерованных различными числами. Сколько различных комбинаций из пяти шаров можно получить, если вынутые шары не возвращаются? Сколько существует вариантов вынуть 5 шаров, если после каждого вытаскивания шара этот шар возвращается в урну?

2.24. Сколько всего существует шестизначных номеров с различными цифрами на автобусных билетах одной серии? Нумерация билета может начинаться с нуля.

2.25. Проживают ли в вашем городе два человека с одинаковыми инициалами? Инициалы предполагаются состоящими из трех букв и они не содержат букв ψ, τ, ν .

2.26. а) Сколькими различными способами можно расположить в ряд 5 человек для выполнения их группового портрета?

б) Сколькими различными способами можно выполнить групповой портрет, если трех человек поставить в заднем ряду, а двух – в переднем ряду?

в) Семья из пяти человек имеет троих детей. Сколькими различными способами можно выполнить групповой портрет, если родителей поставить в заднем ряду, а детей в переднем ряду?

2.27. Имеется 7 карточек, на каждой из которых написано по одной букве. Все буквы различные. Сколько различных “слов” (некоторые из них окажутся бессмысленными) можно составить из семи карточек?

2.28. Пусть на семи карточках написано по одной букве $A, П, П, A, P, A, T$. Сколько различных “слов” можно составить из семи карточек?

2.29. Даны натуральные числа от 1 до 30. Сколькими способами можно выбрать три числа, так, чтобы их сумма была четной?

2.30. Сколькими способами можно рассадить за круглым столом n человек? Два расположения считаются различными, когда в этих двух случаях хоть один сидящий за столом имеет с какой-либо стороны разных соседей.

2.31.а) Сколько различных ожерелий можно составить на нитке из семи бусинок разных размеров?

б) А из шести одинаковых бусинок и еще одной несколько большего размера?

в) А из пяти одинаковых бусинок и двух несколько больших бусинок, но равных?

2.32. Сколькими способами можно составить комиссию в составе 3 человек, выбирая из 5 супружеских пар, если:

а) в комиссию могут входить любые 3 человека;

б) в комиссию не могут входить члены одной семьи?

2.33. В конкурсе на звание лучшей семьи приняло участие 6 семей, причем каждая семья состояла из трех человек (папа, мама и ребенок). Сколькими способами можно рекомендовать три человека для подготовки интервью в средствах массовой информации, если в состав тройки не могут входить члены одной семьи?

2.34. Доказать равенства

а) $C_n^k = C_n^{n-k}$; б) $C_n^k + C_n^{k-1} = C_{n+1}^k$; в) $C_n^k = \frac{n}{k} C_{n-1}^{k-1}$;

г) $C_n^0 - C_n^1 + C_n^2 - C_n^3 + \dots + (-1)^n C_n^n = 0$.

2.35. Сколько существует в выпуклом n -угольнике ($n \geq 4$) точек пересечения диагоналей, считая, что никакие три из них не пересекаются в одной точке?

2.36. На светском балу оказалось, что любые две дамы отличаются количеством колец на руках. Каково наибольшее число дам на балу, если на каждом пальце не более одного кольца?

2.37. Сколькими способами можно расселить 8 студентов по четырем комнатам: трехместной, двум двухместным и одноместной?

2.38. Сколькими способами можно раскрасить 6 шаров в красный, синий и зеленый цвет по 2 шара?

2.39. Сколькими способами можно из 20 студентов выбрать жюри из трех человек, из которых один председатель и один секретарь?

2.40. Сколькими способами можно составить сборную команду из 5 парней и 5 девушек, если имеется 7 парней и 9 девушек?

2.41. Пароль на компьютер должен состоять из пяти символов – вначале двух букв, которые выбираются из 32 букв на нижнем регистре клавиатуры, и затем трех цифр. Сколько различных паролей такого типа существует?

2.42. Пароль на компьютер должен состоять из семи символов – двух букв и трех цифр, причем расположение букв является произвольным. Сколько различных паролей такого типа существует, если буквы выбираются из 32 букв на нижнем регистре клавиатуры?

2.43. Сколько чисел, меньших миллиона, можно составить с помощью цифр 8 и 9?

2.44. Докажите тождества:

а) $\frac{A_n^6 + A_n^5}{A_n^4} = (n-4)^2$; б) $A_n^k = \frac{P_n}{P_{n-k}}$; в) $\frac{A_{n+k}^{n+2} + A_{n+k}^{n+1}}{A_{n+k}^n} = k^2$; г) $A_n^{n-1} = P_n$;

д) $A_n^k \cdot P_{n-k} = n!$; е) $A_n^k = nA_{n-1}^{k-1}$; ж) $A_n^k = A_{n-1}^k + kA_{n-1}^{k-1}$.

2.45. Решите уравнения: а) $5C_n^3 = C_{n+2}^4$; б) $30P_n = P_{n+2}$.

2.46. В партии из N деталей имеется n стандартных деталей. Сколькими способами можно осуществить выборку V элементов, где $V < N$, содержащую v стандартных деталей?

2.47. В учебной группе из 20 человек 8 парней. Сколькими способами можно сформировать команду из пяти человек, в состав которой должны входить 2 парня?

2.48. Используя формулу бинома Ньютона, найдите разложения

а) $(x-2)^7$; б) $(\sqrt{3}-\sqrt{2})^5$; в) $(\sqrt{x}+y)^4$; г) $\left(2x-\frac{1}{x}\right)^6$.

2.49. Найдите двенадцатый член разложения бинома $\left(\frac{1}{\sqrt{3x}}-2x\right)^n$, если биномиальный коэффициент третьего члена разложения равен 105.

2.50. Найти в разложении бинома $\left(z+\frac{1}{z^3}\right)^{16}$ член, не содержащий z .

2.51. Найти в разложении бинома $\left(\sqrt[3]{x}+\frac{1}{x}\right)^{16}$ номер члена, не содержащий x .

2.52. Показатель степени одного бинома на 3 больше показателя другого бинома. Определите эти показатели, если сумма биномиальных коэффициентов в обоих разложениях вместе равна 72.

2.53. Сколько рациональных членов содержится в разложении $(\sqrt{2}-\sqrt[3]{3})^{20}$?

2.54. Напишите разложения по биномиальной формуле:

а) $(x+y+z)^2$; б) $(x+y+z)^3$; в) $(x_1+x_2+x_3+x_4)^2$.

2.55. Докажите равенства

а) $C_n^1 - 2C_n^2 + 3C_n^3 - \dots + (-1)^{n-1} n C_n^n = 0$;

б) $C_n^1 + 2^2 C_n^2 + 3^2 C_n^3 + \dots + n^2 C_n^n = n(n+1)2^{n-2}$.

2.56. Пусть $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Какие из следующих семейств подмножеств множества X являются его разбиениями:

а) $S_1 = \{\{1\}, \{2, 3, 4\}, \{6, 7, 8\}\}$; б) $S_2 = \{\{1, 2, 3, 4, 5\}, \{5, 6, 7, 8\}\}$;

в) $S_3 = \{\{1, 2, 4, 8\}, \{3, 6\}, \{5\}, \{7\}\}$?

2.57. Сколькими способами можно разбить на подмножества множество, состоящее: а) из трех элементов, б) из четырех элементов?

2.58. Найдите коэффициент при $x^2y^3z^2$ в разложении $(x + y + z)^7$.

2.59. Найдите коэффициент при a^4b^2 в разложении $(a + b + 3)^8$.

§ 3. Рекуррентные отношения и производящая функция

В компьютерных вычислениях значительное число вычислений осуществляется по заданному рекуррентному отношению. Для выяснения асимптотики вычисляемой величины лучше использовать аналитическое задание этой величины как функции натурального аргумента.

Этот раздел посвящен методам получения явного задания функции от натурального аргумента, если для функции известно рекуррентное отношение.

$u_{n+k} = F(n, u_n, u_{n+1}, \dots, u_{n+k-1})$ – рекуррентное отношение, которое позволяет вычислять любой член последовательности, если заданы ее k предшествующих членов.

Пример 1. $u_{n+1} = u_n q$, где $q = \text{const} \neq 0$. Рекуррентное отношение определяет геометрическую прогрессию. \square

Пример 2. $u_{n+1} = u_n + d$, где $d = \text{const}$. Рекуррентное отношение определяет арифметическую прогрессию. \square

Пример 3. $u_n = u_{n-1} + u_{n-2}$, $n > 2$, $u_1 = 1$, $u_2 = 1$ – последовательность чисел Фибоначчи, т.е. последовательность чисел

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

Любое положительное целое число имеет единственное представление

$$n = F_{k_1} + F_{k_2} + \dots + F_{k_r} \quad (1)$$

$$k_1 \geq k_2 + 2, k_2 \geq k_3 + 2, \dots, k_{r-1} \geq k_r + 2,$$

где представление осуществляется с помощью “жадного” подхода. В качестве F_{k_1} выбирается наибольшее число Фибоначчи, которое меньше либо равно данному числу n , затем в качестве F_{k_2} выбирается наибольшее число, которое меньше либо равно $n - F_{k_1}$ и т.д.

Равенство (1) представим в виде

$$n = \sum_{k=2}^m b_k F_k, \quad (2)$$

где $b_k = 1$, если число F_k имеется в разложении и $b_k = 0$, если соответствующее число Фибоначчи отсутствует в разложении.

Сопоставим числу (2) машинное слово (b_m, \dots, b_3, b_2) . Получим код числа n в фибоначчевой системе счисления, причем для записи используются только символы 0 или 1.

Числа F_2, F_3, F_4, \dots образуют базис системы счисления Фибоначчи, а равенство (2) является разложением числа n по базису.

Примеры кодов некоторых чисел:

$1_{10}=1=$	00000001,	$7_{10}=5+2=$	00001010,
$2_{10}=2=$	00000010,	$8_{10}=8=$	00010000,
$3_{10}=3=$	00000100,	$9_{10}=8+1=$	00010001,
$4_{10}=3+1=$	00000101,	$19_{10}=13+5+1=$	00101001,
$5_{10}=5=$	00001000,	$45_{10}=34+8+3=$	10010100,
$6_{10}=5+1=$	00001001,	$54_{10}=34+13+5+2=$	10101010.

В этой форме представления чисел две единицы не могут быть расположены рядом. Это свойство используется при кодировании информации. \square

Если u_{n+k} линейно выражается через $u_n, u_{n+1}, \dots, u_{n+k-1}$, т.е.

$u_{n+k} = c_n u_n + c_{n+1} u_{n+1} + \dots + c_{n+k-1} u_{n+k-1}$, где $c_i - const$, то рекуррентная последовательность называется возвратной последовательностью.

Пусть для возвратной последовательности

$$u_n = au_{n-1} + bu_{n-2}, \quad (3)$$

где $n > 2$, $a, b - const, b \neq 0$, известны первые два члена последовательности u_1, u_2 .

Характеристическое уравнение для равенства (3):

$$k^2 - ak - b = 0.$$

Если корни k_1, k_2 уравнения (4) различные, то получаем формулу для общего члена

$$u_n = C_1 k_1^n + C_2 k_2^n, \quad (4)$$

$$\text{где } C_1 = \frac{u_2 - k_2 u_1}{k_1(\alpha - k_2)}, \quad C_2 = -\frac{u_2 - k_1 u_1}{k_2(k_1 - k_2)}.$$

На практике постоянные C_1, C_2 находят из условий

$$u_1 = C_1 k_1 + C_2 k_2, \quad u_2 = C_1 k_1^2 + C_2 k_2^2.$$

Пример 4. Найдем формулу для числа Фибоначчи F_n .

Для рекуррентного отношения $F_n = F_{n-1} + F_{n-2}$ составим характеристическое уравнение $k^2 - k - 1 = 0$.

$$\text{Корни уравнения } k_1 = \frac{1 - \sqrt{5}}{2}, \quad k_2 = \frac{1 + \sqrt{5}}{2}.$$

Постоянные C_1, C_2 находим из равенств

$$1 = C_1 \frac{1 - \sqrt{5}}{2} + C_2 \frac{1 + \sqrt{5}}{2}, \quad 1 = C_1 \left(\frac{1 - \sqrt{5}}{2} \right)^2 + C_2 \left(\frac{1 + \sqrt{5}}{2} \right)^2.$$

$$\text{Откуда следует } C_1 = -\frac{1}{\sqrt{5}}, \quad C_2 = \frac{1}{\sqrt{5}}.$$

Формула n -го члена числа Фибоначчи принимает вид

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Замечание. Если для последовательности известны первые два члена u_0, u_1 , то система для определения постоянных C_1, C_2 принимает более простой вид

$$\begin{cases} u_0 = C_1 + C_2, \\ u_1 = C_1 k_1 + C_2 k_2. \end{cases}$$

Например, для чисел Фибоначчи можно расширить определение, полагая $F_0 = 0$, тогда константы определяются из равенств

$$0 = C_1 + C_2, \quad 1 = C_1 \frac{1-\sqrt{5}}{2} + C_2 \frac{1+\sqrt{5}}{2}. \quad \square$$

Если корни характеристического уравнения равны $k_1 = k_2 = k$, то формула общего члена рекуррентной последовательности принимает вид

$$\boxed{u_n = C_1 k^n + C_2 n k^n.} \quad (5)$$

Постоянные C_1, C_2 находят из условий

$$\begin{cases} u_0 = C_1, \\ u_1 = C_1 k + C_2 k. \end{cases}$$

Выражение вида $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$ называется формальным числовым рядом.

Формальные числовые ряды можно складывать, вычитать, умножать, делить, дифференцировать, составлять их композицию, не беспокоясь о сходимости рядов.

Пусть $\{a_n\} = a_0, a_1, \dots$ произвольная числовая последовательность, тогда формальный числовой ряд $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$ называется производящей функцией этой последовательности.

Разложение функций в формальные степенные ряды

$$\frac{1}{1-ax} = 1 + ax + a^2 x^2 + \dots + a^n x^n + \dots,$$

$$\frac{1}{(1-ax)^2} = 1 + 2ax + 3a^2 x^2 + \dots + (n+1)a^n x^n + \dots,$$

$$\frac{1}{(1-ax)^3} = 1 + 3ax + 6a^2 x^2 + \dots + \frac{(n+1)(n+2)}{2} a^n x^n + \dots,$$

$$\frac{1}{(1-ax)^k} = 1 + C_k^1 ax + C_{k+1}^2 a^2 x^2 + \dots + C_{n+k-1}^n a^n x^n + \dots$$

Метод производящих функций – это переход от оперирования с комбинаторными объектами и числовыми последовательностями к действиям с формальными степенными рядами.

Пример 5. Найти формулу общего члена последовательности, заданной рекуррентным отношением $a_n = 3a_{n-1}$ для $n \geq 1$.

Решение. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$, тогда

$$3x f(x) = 3a_0x + 3a_1x^2 + 3a_2x^3 + \dots + 3a_{n-1}x^n + 3a_nx^{n+1} + \dots$$

$$f(x) - 3x f(x) = a_0 + (a_1 - 3a_0)x + (a_2 - 3a_1)x^2 + \dots + (a_n - 3a_{n-1})x^n + \dots$$

Но $a_n - 3a_{n-1} = 0$ при всех $n \geq 1$, поэтому

$$(1 - 3x)f(x) = a_0, \quad f(x) = \frac{a_0}{1 - 3x} = a_0 \frac{1}{1 - 3x},$$

$$f(x) = a_0(1 + 3x + 3^2x^2 + \dots + 3^n x^n + \dots).$$

Сравнивая коэффициенты при x^n в двух разложениях функции $f(x)$, получаем $a_n = a_0 3^n$.

Замечание. В условии данной задачи рассматривается рекуррентное соотношение для геометрической прогрессии со знаменателем $q = 3$. Формула общего члена получается по известной формуле с поправкой на то, что прогрессия имеет первый член a_0 . \square

Пример 6. Найти формулу общего члена последовательности, заданной рекуррентным отношением $a_n = a_{n-1} + 3$ для $n \geq 1$ и $a_0 = 5$.

Решение. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$, тогда

$$x f(x) = a_0x + a_1x^2 + a_2x^3 + \dots + a_{n-1}x^n + a_nx^{n+1} + \dots$$

При сравнении коэффициентов потребуется производящая функция, у которой все коэффициенты содержат число 3, поэтому рассмотрим разложение

$$\frac{3}{1 - ax} = 3(1 + ax + a^2x^2 + \dots + a^n x^n + \dots),$$

$$f(x) - x f(x) - \frac{3}{1 - x} =$$

$$= a_0 - 3 + (a_1 - a_0 - 3)x + (a_2 - a_1 - 3)x^2 + \dots + (a_n - a_{n-1} - 3)x^n + \dots$$

Но $a_n - a_{n-1} - 3 = 0$ при всех $n \geq 1, a_0 = 5$, поэтому

$$f(x) - x f(x) - \frac{3}{1 - x} = 2, \quad (1 - x)f(x) = 2 + \frac{3}{1 - x}, \quad f(x) = \frac{2}{1 - x} + \frac{3}{(1 - x)^2},$$

$$f(x) = 2(1 + x + x^2 + \dots + x^n + \dots) + 3(1 + 2x + 3x^2 + \dots + (n + 1)x^n + \dots),$$

$$f(x) = 5 + 8x + \dots + (3n + 5)x^n + \dots$$

Сравнивая коэффициенты при x^n в двух разложениях функции $f(x)$, получаем $a_n = 3n + 5$.

Замечание. В условии данной задачи рассматривается рекуррентное соотношение для арифметической прогрессии с разностью $d = 3$. Формула общего члена арифметической прогрессии получается по известной формуле с поправкой на то, что прогрессия имеет первый член a_0 . \square

Пример 7. Найти формулу общего члена последовательности, заданной рекуррентным отношением $a_n = 3a_{n-1} + 4^n$ для $n \geq 1$ и $a_0 = 1$.

Решение. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$, тогда

$$3x f(x) = 3a_0x + 3a_1x^2 + 3a_2x^3 + \dots + 3a_{n-1}x^n + 3a_nx^{n+1} + \dots$$

$$\frac{1}{1-4x} = 1 + 4x + 4^2x^2 + \dots + 4^n x^n + \dots$$

$$f(x) - 3x f(x) - \frac{1}{1-4x} =$$

$$= a_0 - 1 + (a_1 - 3a_0 - 4)x + (a_2 - 3a_1 - 4^2)x^2 + \dots + (a_n - 3a_{n-1} - 4^n)x^n + \dots$$

$$f(x) - 3x f(x) - \frac{1}{1-4x} = 0, \quad f(x) = \frac{1}{(1-4x)(1-3x)}.$$

Представим функцию $\frac{1}{(1-4x)(1-3x)}$ в виде суммы элементарных дробей

$$\frac{1}{(1-4x)(1-3x)} = \frac{A}{1-4x} + \frac{B}{1-3x}.$$

Умножая обе части на $(1-4x)(1-3x)$, найдем

$$1 = A(1-3x) + B(1-4x).$$

Подставляя в равенство $x = 1/3$, получаем $B = 3$.

Аналогично, для $x = 1/4$ найдем $A = 4$.

Следовательно,

$$f(x) = \frac{4}{1-4x} - \frac{3}{1-3x},$$

$$f(x) = 4(1 + 4x + 4^2x^2 + \dots + 4^n x^n + \dots) - 3(1 + 3x + 3^2x^2 + \dots + 3^n x^n + \dots).$$

Сравнивая коэффициенты при x^n в двух разложениях функции $f(x)$, получаем

$$a_n = 4 \cdot 4^n - 3 \cdot 3^n, \quad a_n = 4^{n+1} - 3^{n+1}.$$

Рассмотрим проверку полученного решения.

При $n = 0$ получаем $a_0 = 4^1 - 3^1 = 1$.

Проверим рекуррентное соотношение

$$3a_{n-1} + 4^n = 3(4^n - 3^n) + 4^n = 4^{n+1} - 3^{n+1} = a_n. \quad \square$$

Пример 8. Найти формулу общего члена последовательности, заданной рекуррентным отношением $a_n = 2a_{n-1} + n$ для $n \geq 1$ и $a_0 = 3$.

Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$, тогда

$$2x f(x) = 2a_0x + 2a_1x^2 + 2a_2x^3 + \dots + 2a_nx^{n+1} + \dots,$$

$$\frac{x}{(1-x)^2} = x(1 + 2x + 3x^2 + \dots + (n+1)x^n + \dots),$$

$$\begin{aligned}
 f(x) - 2x f(x) - \frac{x}{(1-x)^2} &= \\
 = a_0 + (a_1 - 2a_0 - 1)x + (a_2 - 2a_1 - 2)x^2 + \dots + (a_n - 2a_{n-1} - n)x^n + \dots \\
 (1-2x)f(x) &= \frac{x}{(1-x)^2} + 3, \quad f(x) = \frac{x}{(1-2x)(1-x)^2} + \frac{3}{1-2x}, \\
 f(x) &= \frac{5}{1-2x} - \frac{1}{1-x} - \frac{1}{(1-x)^2}, \quad f(x) = 5(1+2x+2^2x^2+\dots+2^n x^n+\dots) - \\
 &-(1+x+x^2+\dots+x^n+\dots) - (1+2x+3x^2+\dots+(n+1)x^n+\dots). \\
 a_n &= 5 \cdot 2^n - n - 2. \quad \square
 \end{aligned}$$

К возвратным последовательностям можно применять как метод, определенный формулами (4) и (5) с последующим определением констант, так и метод производящей функции.

Задачи.

3.1. Найдите общий член последовательности, заданный рекуррентным отношением:

- а) $u_n = 6u_{n-1} - 9u_{n-2}$, $u_1 = 3$, $u_2 = 0$;
- б) $u_n = -2u_{n-1} - u_{n-2}$, $u_1 = -1$, $u_2 = -1$;
- в) $u_n = 5u_{n-1} - 6u_{n-2}$, $u_0 = 0$, $u_1 = 1$;
- г) $u_n = 3u_{n-1} - 2u_{n-2}$, $u_0 = 1$, $u_1 = 1$;
- д) $u_n = 2u_{n-1} - u_{n-2}$, $u_0 = 1$, $u_1 = 2$.

3.2. Дан квадрат $ABCD$ (рис. 12). Каждая сторона квадрата делится на две равные части. На полученных отрезках строятся квадраты во внешнюю сторону от данного квадрата и строятся квадраты в угловых точках. Вокруг данного квадрата получилось первое кольцо из квадратов. Далее стороны полученных квадратов снова делятся пополам, и повторяется процесс построения квадратов.

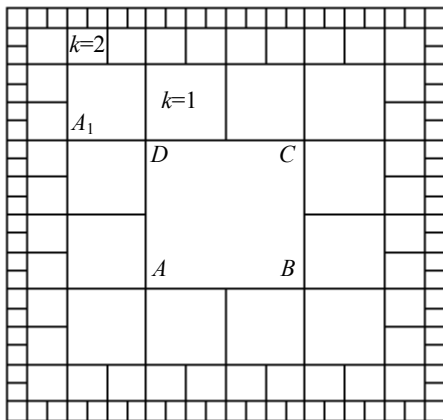


Рис. 12

а) Определите рекуррентное отношение для числа квадратов a_n в горизонтальном ряду в зависимости от номера n ряда. Найдите явное выражение для a_n .

б) Определите рекуррентное отношение для числа квадратов c_n в окаймляющем кольце в зависимости от номера n кольца. Найдите явное выражение для c_n .

3.3. На рис. 13 сторона квадрата, расположенного в центре рисунка, делится на 3 равные части и далее строятся окаймляющие квадраты. Определите рекуррентное отношение для числа квадратов a_n в горизонтальном ряду в зависимости от номера n ряда. Найдите явное выражение для a_n . Определите рекуррентное отношение для числа квадратов c_n в окаймляющем кольце в зависимости от номера n кольца. Найдите явное выражение для c_n .

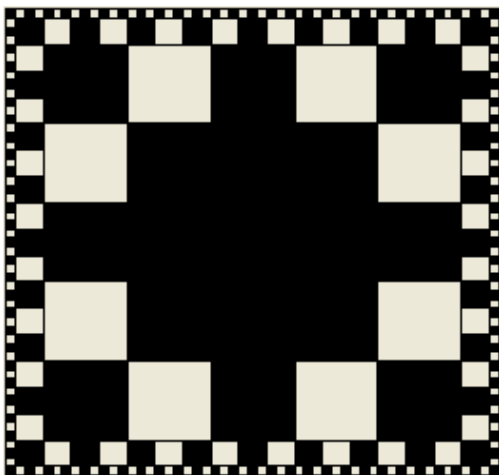


Рис. 13

3.4. Составьте рекуррентное отношение, используя выражение общего члена последовательности:

а) $a_n = 4^n + 5^{n-1}$; в) $a_n = 2^n - n3^n$;

б) $a_n = 2n - 1$; г) $a_n = (-1)^n$.

§ 4. Бинарные отношения

Пусть A_1, A_2 – непустые множества, тогда бинарное отношение определяется на множестве $A_1 \times A_2$ как подмножество в декартовом произведении $A_1 \times A_2$.

Бинарным отношением ρ на множестве A называется любое множество упорядоченных пар, т.е. подмножество в декартовом произведении $A \times A$. Для пары, связанной отношением ρ , применяют обозначения $x\rho y$ или $(x, y) \in \rho$. Если

элемент x не связан отношением ρ с элементом y , то будем записывать $(x, y) \notin \rho$ или $\overline{x\rho y}$.

Областью определения бинарного отношения ρ называется множество $D_\rho = \{x: \exists \text{ такое } y, \text{ что } x\rho y\}$.

Областью значений бинарного отношения ρ называется множество $E_\rho = \{y: \exists \text{ такое } x, \text{ что } x\rho y\}$.

Пример 1. Пусть даны множества $A = \{1, 2, 3, 4\}$ и $B = \{2, 3, 4, 5\}$. В декартовом произведении $A \times B$ выделим подмножество ρ пар (a, b) для которых $a \geq b$. Бинарное отношение задано *характеристическим свойством*. Используя данное свойство, можно *перечислить все элементы* отношения $\rho = \{(2, 2), (3, 2), (3, 3), (4, 2), (4, 3), (4, 4)\}$.

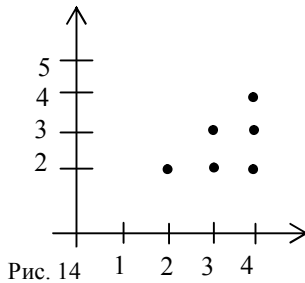


Рис. 14

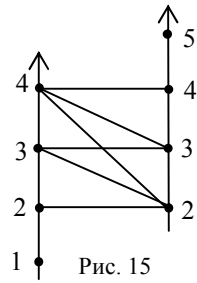


Рис. 15

Построим *график отношения*, изобразив на горизонтальной оси область определения отношения, а на вертикальной оси – область значений отношения (рис. 14). Упорядоченную пару (x, y) отношения изобразим точкой плоскости с этими координатами.

Схема отношения изображается с помощью двух вертикальных прямых. На левой прямой изображают элементы области определения, а на правой прямой множество значений. Упорядоченную пару изображают отрезком или стрелкой (рис. 15). □

Пусть $X = \{x_1, x_2, \dots, x_n\}$, $Y = \{y_1, y_2, \dots, y_m\}$ – два произвольных конечных множества и ρ – бинарное отношение на множестве $X \times Y$. Матрицей отношения

ρ называется матрица $A(\rho) = (a_{ij})$, где $a_{ij} = \begin{cases} 1, & \text{если } x_i\rho y_j, \\ 0, & \text{если } \overline{x_i\rho y_j}. \end{cases}$

Матрица отношения для примера 1 приведена в таблице 4.

Таблица 4

	2	3	4	5
1	0	0	0	0
2	1	0	0	0
3	1	1	0	0
4	1	1	1	0

Замечание. Порядок элементов в множестве не имеет значения, а порядок записи элементов для матрицы имеет значение. В дальнейшем будем считать, что запись элементов для строк матрицы и для столбцов матрицы проводится в том порядке, как они перечислены в множестве. Если множества состоят из целых чисел, то примем обязательным расположением элементов в порядке возрастания.

Пример 2. Пусть дано множество $X = \{1, 2, 3, 4, 5\}$ и на декартовом произведении $X \times X$ задано отношение $\rho = \{(x, y) \mid (2x + y) : 3\}$, т.е. $2x + y$ кратно 3.

Перечислим пары, удовлетворяющие характеристическому свойству: $(1,1), (1,4), (2,2), (2,5), (3,3), (4,1), (4,4), (5,2), (5,5)$.

Это отношение можно, как и в предыдущем примере, задать графиком, схемой, матрицей. Для отношения на декартовом квадрате множества можно рассмотреть задание с помощью графа. \square

Граф строится следующим образом. На плоскости изображаем точками элементы множества и соединяем стрелкой от элемента x к элементу y , если эти элементы связаны данным отношением (рис. 16). \square



Рис. 16

Обратным отношением для ρ называется отношение $\rho^{-1} = \{(x, y) : (y, x) \in \rho\}$.

Пример 3. $\rho = \{(1,2), (5,7), (5,9)\}$.

Решение. $D_\rho = \{1,5\}$, $E_\rho = \{2,7,9\}$, $\rho^{-1} = \{(2,1), (7,5), (9,5)\}$. \square

Композицией бинарных отношений ρ_1 и ρ_2 называется отношение $\rho_2 \cdot \rho_1 = \{(x, z) : \exists \text{ такое } y, \text{ что } (x, y) \in \rho_1, (y, z) \in \rho_2\}$. Точка между отношениями при обозначении композиции иногда не ставится.

Композиция бинарных отношений ρ_1 и ρ_2 определена тогда и только тогда, когда множество значений отношения ρ_1 содержится в области определения бинарного отношения ρ_2 , т.е. $E_{\rho_1} \subset D_{\rho_2}$.

Пример 4. $\rho_1 = \{(1,2), (5,7), (3,3), (20,10)\}$, $\rho_2 = \{(2,4), (7,6), (7,9), (3, 0), (10,10), (15, 1)\}$, $\rho_2 \cdot \rho_1 = \{(1,4), (5,6), (5,9), (3,0), (20,10)\}$. \square

Для любых бинарных отношений выполняются свойства:

$$(\rho^{-1})^{-1} = \rho, (\rho_2 \cdot \rho_1)^{-1} = \rho_1^{-1} \rho_2^{-1}, (\rho_1 \rho_2) \rho_3 = \rho_1 (\rho_2 \rho_3).$$

Отношение ρ на множестве X называется *рефлексивным*, если для любого элемента $x \in X$ выполняется $x\rho x$, т.е. любой элемент $x \in X$ находится сам с собой в отношении ρ .

Отношение ρ на множестве X называется *антирефлексивным*, если любой элемент $x \in X$ не находится сам с собой в отношении ρ , т.е. $x \overline{\rho} x$.

Если отношение ρ не является ни рефлексивным, ни антирефлексивным, то будем называть его *нерефлексивным*. Нерефлексивность означает, что $\exists x \in X : x\rho x$ и $\exists y \in X : y \overline{\rho} y$.

Отношение ρ на множестве X называется *симметричным*, если для любых элементов $x, y \in X$ из $x\rho y$ следует $y\rho x$.

Отношение ρ на множестве X называется *антисимметричным*, если для любых элементов $x, y \in X$ из $x\rho y$ и $y\rho x$ следует $x = y$.

Если отношение ρ не является ни симметричным, ни антисимметричным, то будем называть его *несимметричным*.

Отношение ρ на множестве X называется *транзитивным*, если для любых элементов $x, y, z \in X$ из $x\rho y, y\rho z$ следует $x\rho z$.

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

Рефлексивное, антисимметричное и транзитивное отношение на множестве X называется *отношением частичного порядка* на множестве X .

Антирефлексивное, антисимметричное и транзитивное отношение на множестве X называется *отношением строгого порядка* на множестве X и обозначается $<$.

Отношение частичного порядка на множестве X называется *отношением линейного порядка*, если для любых элементов $x, y \in X$ выполняется $x < y$ или $y < x$. Для линейного порядка будем использовать также символ $<$.

Рассмотрим непустое конечное множество X , на котором задано отношение частичного порядка $<$. Для различных элементов x, y , удовлетворяющих условию $x < y$, будем говорить, что элемент y покрывает элемент x , если не существует такого элемента z , что $x < z < y$.

Изобразим элементы множества X на плоскости точками, и если y покрывает x , то точки x и y соединяем отрезком, причем точку y располагаем выше точки x . Полученную схему называют *диаграммой Хассе*.

Пример 5. Дано множество $X = \{a, b, c\}$. На совокупности всех его подмножеств $P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ введем отношение “быть подмножеством”. Построить диаграмму Хассе этого отношения.

Решение. Множества $\{a\}, \{b\}, \{c\}$ покрывают множество \emptyset , поэтому изображаем их выше множества \emptyset (рис. 17). Множества $\{a, b\}, \{a, c\}$ покрывают множество $\{a\}$, множества $\{a, b\}, \{b, c\}$ покрывают множество $\{b\}$, множества $\{a, c\}, \{b, c\}$ покрывают множество $\{c\}$ и, наконец, каждое из множеств $\{a, b\}, \{a, c\}, \{b, c\}$ покрывает единственное множество $\{a, b, c\}$.

Замечание. При построении диаграммы Хассе для одного и того же множества и его отношения можно получить различные изображения, но их структура будет одинаковой. \square

Рассмотрим характеристику бинарных отношений с помощью матриц отношений.

Матрица $A = (a_{ij})$ размера $m \times n$ называется булевой, если каждый элемент матрицы равен 0 или 1.

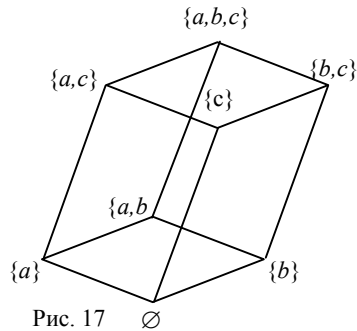


Рис. 17 \emptyset

Для булевых матриц $A = (a_{ij})$ и $B = (b_{ij})$ считаем, что $A \leq B$ тогда и только тогда, когда для любых $i, j = 1, 2, \dots, n$ выполняется неравенство $a_{ij} \leq b_{ij}$.

Булевым произведением матрицы $A = (a_{ij})$ на матрицу $B = (b_{ij})$ (обозначение $A \circ B$) называется булева матрица $C = (c_{ij})$, в которой любой элемент c_{ij} вычисляется по формуле $c_{ij} = \max(\min(a_{i1}, b_{1j}), \min(a_{i2}, b_{2j}), \dots, \min(a_{in}, b_{nj}))$.

$$\text{Например, } \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Свойства бинарных отношений представлены в таблице 5.

Таблица 5

Бинарное отношение	Характеристическое свойство матрицы
Рефлексивное отношение	Все элементы главной диагонали равны 1
Антирефлексивное отношение	Все элементы главной диагонали равны 0
Нерефлексивное отношение	На главной диагонали находятся как единицы, так и нули
Симметричное отношение	Матрица симметрична относительно главной диагонали
Антисимметричное отношение	Матрица не содержит симметричные относительно главной диагонали единицы
Несимметричное отношение	Матрица содержит симметричные элементы относительно главной диагонали (среди которых должны быть обязательно симметричные единицы), а также в матрице есть элементы, не симметричные относительно главной диагонали
Транзитивное отношение с матрицей $A(\rho)$	$A(\rho) \circ A(\rho) \leq A(\rho)$

Классом эквивалентности, порожденным элементом x в множестве X с отношением ρ , называется подмножество множества X , состоящее из тех элементов $y \in X$, для которых $x \rho y$. Класс эквивалентности, порожденный элементом x , обозначается $[x]$.

Теорема. Класс эквивалентности порождается любым своим элементом, т.е. если $x \rho y$, то $[x] = [y]$.

Сокупность классов эквивалентности множества X по отношению ρ называется фактор-множеством X по отношению ρ и обозначается X/ρ .

Фактор-множество является разбиением множества X , порожденным отношением эквивалентности и, наоборот, для любого разбиения множества можно

указать отношение эквивалентности, для которого фактор-множество совпадает с этим разбиением.

Пример 6. Пусть дано натуральное число n . На множестве целых чисел введем отношение $a\rho b$ тогда и только тогда, когда $(a-b):n$. Обозначение этого отношения $a \equiv b \pmod{n}$, произношение – a сравнимо с b по модулю n и название этого отношения – вычеты по модулю n , сравнения по модулю n .

Для отношения “сравнение по модулю 5” на множестве целых чисел получаем классы

$$\begin{aligned} [1] &= \{\dots -9, -4, 1, 6, 11, \dots\}, \\ [2] &= \{\dots -8, -3, 2, 7, 12, \dots\}, \\ [3] &= \{\dots -7, -2, 3, 8, 13, \dots\}, \\ [4] &= \{\dots -6, -1, 4, 9, 13, \dots\}, \\ [5] &= \{\dots -5, 0, 5, 10, 15, \dots\}, \\ [0] &= \{\dots -10, -5, 0, 5, 10, \dots\}. \end{aligned}$$

Отношение “сравнение по модулю n ” является отношением эквивалентности, т.е. выполняются свойства:

- а) $a \equiv a \pmod{n}$;
- б) если $a \equiv b \pmod{n}$, то $b \equiv a \pmod{n}$;
- в) если $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$.

Из теоремы следует, что сравнение по модулю n разбивает множество целых чисел на n классов, которые можно обозначить следующим образом: $[0], [1], \dots, [n-1]$. Для этих классов используется также обозначение: $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$.

Для сравнения по модулю n фактор-множество Z/ρ состоит из n элементов: $Z/\rho = \{[0], [1], \dots, [n-1]\}$. \square

Пример 7. На множестве $A = \{1, 2, 3, \dots, 10\}$ задано бинарное отношение $x\rho y \leftrightarrow \exists k \in Z : x = 2^k y$. Доказать, что ρ – отношение эквивалентности и найти фактор-множество по этому отношению.

Решение. Прежде всего нужно понять смысл бинарного отношения, а иногда и переформулировать другими словами для лучшего понимания. В данном примере первый элемент x в упорядоченной паре $(x; y)$ связан бинарным отношением со вторым элементом в этой паре, если элемент x может быть получен из элемента y умножением на степень с основанием 2 и целым показателем. Например, $3\rho 6$, т.к. $3 = 2^{-1} \cdot 6$, но $3 \overline{\rho} 5$.

Множество A содержит 10 элементов, множество A^2 содержит 100 упорядоченных пар, поэтому в этом примере проверку свойств отношения эквивалентности целесообразно проводить по определению для произвольных элементов.

1) Для любого элемента $x \in A$ выполняется условие $x\rho x$, т.к. $x = 2^0 x$, поэтому бинарное отношение является рефлексивным.

2) Проверим свойство симметричности. Пусть для некоторых элементов x, y выполняется условие $x\rho y$, тогда существует такое целое число k , что вы-

полняется равенство $x = 2^k y$. Из этого равенства выразим y , т.е. $y = 2^{-k} x$. Обозначим $m = -k$, тогда $y = 2^m x$. Следовательно, нашлось такое целое число m , что число y выражается через число x с помощью умножения на степень с основанием 2 и целым показателем, т.е. $y \rho x$. Бинарное отношение является симметричным.

3) Проверим транзитивность бинарного отношения. Пусть для некоторых элементов x, y выполняется условие $x \rho y$, а также для элемента y и некоторого элемента z выполняется условие $y \rho z$, тогда $\exists k \in \mathbb{Z} : x = 2^k y$ и $\exists m \in \mathbb{Z} : y = 2^m z$. Из двух равенств методом замены получаем $x = 2^k \cdot (2^m z) = 2^{k+m} z$. Обозначим $n = k + m$, тогда $x = 2^n z$. Следовательно, нашлось такое целое число n , что число x получается из числа z умножением на степень с основанием 2 и целым показателем, поэтому $x \rho z$ и бинарное отношение является транзитивным.

4) Начинаем формировать классы эквивалентности. В класс $[2]$, порожденный числом 2, включаем, прежде всего, само число 2, т.к. выполняется рефлексивность отношения. Далее включаем те элементы y , которые связаны с элементом 2 бинарным отношением, поэтому $[2] = \{2, 4, 8, 1\}$. Аналогично $[4] = \{4, 8, 2, 1\}$. Два множества $[2]$ и $[4]$ имеют одинаковый состав элементов, поэтому эти классы $[2]$ и $[4]$ совпадают, т.е. являются одним и тем же классом эквивалентности. Этот факт можно объяснить другим способом и в дальнейшем использовать его для упрощения перечисления классов. Класс эквивалентности $[4]$ содержит элемент 4. Элемент 4 содержится и в построенном классе $[2]$. Используя свойство «Если два класса эквивалентности имеют общий элемент, то они совпадают», получаем $[4] = [2]$. Аналогично $[8] = [2]$, $[3] = \{3, 6\} = [6]$, $[5] = \{5, 10\} = [10]$, $[7] = \{7\}$, $[9] = \{9\}$. Обращаем внимание на то, что каждый элемент данного множества оказался в одном из классов.

Окончательно перечислим классы эквивалентности:

$$[2] = \{1, 2, 4, 8\}, [3] = \{3, 6\}, [5] = \{5, 10\}, [7] = \{7\}, [9] = \{9\}.$$

Фактор-множество $A/\rho = \{[2], [3], [5], [7], [9]\}$ содержит в качестве элементов построенные классы эквивалентности. Каждый класс можно задать с помощью любого элемента, входящего в этот класс. Например, фактор-множество можно задать другим способом $A/\rho = \{[2], [6], [10], [7], [9]\}$.

Данное множество A можно представить в виде объединения классов эквивалентности $A = [2] \cup [3] \cup [5] \cup [7] \cup [9]$. \square

Пример 8. На множестве действительных чисел задано отношение $x \rho y \Leftrightarrow (x - y)(x + 2y)(y + 2x) = 0$. Является ли это отношение отношением эквивалентности?

Решение. Запишем условие в виде

$$x\rho y \leftrightarrow \begin{cases} x = y, \\ x = -2y, \\ y = -2x. \end{cases}$$

Последняя запись означает, что первый элемент x упорядоченной пары $(x; y)$ находится в бинарном отношении ρ со вторым элементом y , если эти элементы равны или если один из них получается из второго умножением на (-2) .

Формулировка бинарного отношения получилась симметричной относительно двух элементов, а значит, бинарное отношение симметрично.

Рефлексивность бинарного отношения очевидна, т.к. любое число равно самому себе.

Проверим транзитивность. Пусть для трех элементов x, y, z выполняются условия $x\rho y$ и $y\rho z$, т.е.

$$\begin{cases} x = y, \\ x = -2y, \\ y = -2x. \end{cases} \text{ и } \begin{cases} y = z, \\ y = -2z, \\ z = -2y. \end{cases} \quad (1)$$

Для выполнения транзитивности нужно проверить выполнение условия $x\rho z$ или эквивалентного условия

$$\begin{cases} x = z, \\ x = -2z, \\ z = -2x. \end{cases} \quad (2)$$

Используя две данные квадратные скобки (1), можно рассмотреть по правилу произведения 9 пар уравнений, выбирая по одному уравнению из каждой совокупности уравнений. Например, из равенств $x = y$ и $y = z$ следует равенство $x = z$. Если $x = y$ и $y = -2z$, то $x = -2z$. Вначале кажется, что если выполняются равенства (1), то выполняется и условие (2). Но из пары равенств $x = -2y$ и $y = -2z$ возникает новое условие $x = 4z$, которого нет в совокупности (2). Делать вывод о том, что нарушается транзитивность отношения, преждевременно. Например, если $x = 0, y = 0, z = 0$, то условие транзитивности для этих трех элементов выполняется.

Для подтверждения того, что получено новое условие, отличное от (2), достаточно привести подтверждающий пример, т.е. контрпример того, что выполняется транзитивность бинарного отношения.

Действительно, $3\rho(-6), (-6)\rho 12$, но $\overline{3\rho 12}$. Данное отношение не является транзитивным, а значит, и не является отношением эквивалентности. \square

Задачи.

4.1. Докажите, что отношение “равенства” на множестве вещественных чисел: $(x, y) \in \rho \leftrightarrow x = y$ является отношением эквивалентности.

4.2. Докажите, что отношение подобия на множестве треугольников является рефлексивным, симметричным и транзитивным отношением, а значит, отношением эквивалентности.

4.3. Докажите, что отношение “меньше” на множестве вещественных чисел является транзитивным отношением, но не является рефлексивным и симметричным. Как изменятся свойства, если рассмотреть отношение «меньше либо равно»?

4.4. Перечислите все свойства отношения “перпендикулярности отрезков” на множестве сторон прямоугольника.

4.5. Какими из свойств (рефлексивность, симметричность, антисимметричность, транзитивность) обладают следующие бинарные отношения:

а) отношение «сидеть за одной партой» в множестве студентов группы;

б) отношение «иметь общую границу» в множестве государств;

в) отношение «быть равноудаленным от Сургута» в множестве городов;

г) отношение «иметь общие остановки» в множестве автобусных маршрутов г. Сургута;

д) отношение делимости на множестве целых чисел, не содержащем нуля;

е) отношение делимости на множестве простых чисел;

ж) отношение взаимной простоты на множестве простых чисел;

з) A, B, C – точки на прямой, причем точка C является серединой отрезка AB . Для элементов множества $X = \{A, B, C\}$ введено отношение: $x\rho y \Leftrightarrow$ когда точки x и y симметричны относительно точки C . Составьте матрицу отношения для элементов этого множества.

4.6. Пусть даны множества $A = \{1, 2, 3, 4\}$ и $B = \{2, 3, 4, 5\}$. В декартовом произведении $A \times B$ выделим подмножество ρ_2 пар (a_2, b_2) , для которых $a_2 < b_2$. Задайте это отношение другими способами.

4.7. Определите, являются ли данные бинарные отношения:

– рефлексивными, антирефлексивными, нерефлексивными;

– симметричными, антисимметричными, несимметричными;

– транзитивными, нетранзитивными?

Определите, есть ли среди них отношения эквивалентности или частичного порядка.

I. В множестве натуральных чисел N :

а) $\rho = \{(x, y) : x < 3y\}$;

б) $\rho = \{(x, y) : x = y^2\}$;

в) $\rho = \{(x, y) : |x - y| = 3\}$;

г) $\rho = \{(x, y) : \text{НОД}(x, y) = 1\}$;

д) $\rho = \{(x, y) : (x - y) \vdots 3\}$.

II. В множестве целых чисел Z :

е) $\rho = \{(x, y) : x \neq y\}$;

ж) $\rho = \{(x, y) : x^2 \geq y^2\}$;

з) $\rho = \{(x, y) : x - y = 3\}$;

и) $\rho = \{(x, y) : (x - y) \vdots 7\}$.

III. В множестве действительных чисел R :

к) $\rho = \{(x, y) : xy \geq 0\}$;

л) $\rho = \{(x, y) : x^2 = y^2\}$;

м) $\rho = \{(x, y) : |x| = |y|\}$;

н) $\rho = \{(x, y) : |x + y| > 1\}$;

о) $\rho = \{(x, y) : |x| + |y| \geq 0\}$.

4.8. На каждом из следующих множеств X задано отношение ρ . Является ли ρ отношением эквивалентности? Если является, то найти фактор-множество X/ρ :

а) $X = \{1, 2, 3, \dots, 8, 9\}$, $(a, b) \in \rho \leftrightarrow \exists k \in Z : a = 3^k b$;

б) $X = \{1, 2, 3, \dots, 11, 12\}$, $(a, b) \in \rho \leftrightarrow \exists k \in Z : a = 4^k b$.

4.9. На множестве трехчленных последовательностей, члены которых могут быть 0 или 1, определено отношение $(a_1 a_2 a_3) \rho (b_1 b_2 b_3) \leftrightarrow a_i = b_i$ для нечетных i .

а) Докажите, что ρ – отношение эквивалентности.

б) Найдите фактор-множество X/ρ .

4.10. На множестве $R \setminus \{0\}$ задано отношение $x \rho y \leftrightarrow xy > 0$.

а) Докажите, что ρ – отношение эквивалентности;

б) найдите фактор-множество X/ρ .

4.11. Дано множество $X = \{1, 2, 3, 4\}$. На множестве $X \times X$ задано отношение $(x_1; y_1) \rho (x_2; y_2) \leftrightarrow x_1 + y_1 = x_2 + y_2$.

а) Покажите, что ρ – отношение эквивалентности;

б) найдите фактор-множество X/ρ .

4.12. Дано множество $X = \{2, 3, 4\}$. На множестве $X \times X$ задано отношение $(x_1; y_1) \rho (x_2; y_2) \leftrightarrow x_1 + x_2 = y_1 + y_2$. Найдите матрицу отношения.

Является ли это отношение рефлексивным, симметричным, транзитивным?

4.13. На множестве N введено отношение

$$x\rho y \leftrightarrow 2\left(\frac{x}{y}\right)^2 - 5\frac{x}{y} + 2 \leq 0.$$

а) Является ли ρ отношение эквивалентности?

б) Найдите матрицу этого отношения для элементов подмножества $X = \{1, 2, 3, 4\}$.

4.14. На множестве N задано отношение $a\rho b \leftrightarrow 3\left(\frac{a}{b}\right)^2 - 10\frac{a}{b} + 3 \leq 0$.

а) Является ли ρ отношение эквивалентности?

б) Найдите матрицу этого отношения для элементов подмножества $X = \{1, 2, 3, 4\}$.

4.15. Пусть $f(x, y) = (x - y)(y + 3x)(3y + x)$. На множестве действительных чисел задано отношение $x\rho y \leftrightarrow f(x, y) = 0$.

а) Является ли ρ отношение эквивалентности?

б) Найдите матрицу этого отношения для элементов подмножества $X = \{0, 1, 2, 3\}$.

4.16. На множестве $Z \setminus \{0\}$ задано отношение $a\rho b \leftrightarrow a + b = 0$ или $a - b = 0$.

а) Является ли ρ отношение эквивалентности?

б) Найдите матрицу этого отношения для элементов подмножества $X = \{-1, 0, 1, 2\}$.

4.17. На множестве R^2 задано отношение

$$(x_1; y_1)\rho (x_2; y_2) \leftrightarrow |x_1| - |y_1| = |x_2| - |y_2|.$$

а) Докажите, что ρ является отношением эквивалентности.

б) Опишите классы эквивалентности.

4.18. На множестве $X = \{1, 2, 3, 4, 5\}$ задано отношение $\rho = \{(x, y) \mid (2y + x) : 3\}$. Является ли это отношение – отношением эквивалентности? Постройте классы эквивалентности по этому отношению. Найдите матрицу отношения.

4.19. На множестве A упорядоченных пар неотрицательных целых чисел задано отношение $(a, b)\rho(c, d) \leftrightarrow ad = bc$. Является ли оно отношением эквивалентности? Если является, то найдите фактор-множество A/ρ по этому отношению.

4.20. Сколько отношений эквивалентности можно построить на множестве $X = \{1, 2, 3, 4\}$?

4.21. Множество X состоит из n элементов, где $n > 1$. Отношение на множестве X рефлексивно и состоит из $n+1$ пар. Какими из основных свойств обладает это отношение?

4.22. Отношение ρ задано на множестве X и состоит из пяти пар. Сколько элементов может содержать множество X , если отношение рефлексивно?

4.23. Множество X содержит больше одного элемента. Какими свойствами обладает на множестве X отношение $\rho = A \times A \setminus \{(a, a)\}$, где a – некоторый фиксированный элемент множества X ?

4.24. Множество X содержит больше двух элементов. Какими свойствами обладает на множестве X отношение $\rho = A \times A \setminus \{(a, b)\}$, где a и b – некоторые фиксированные различные элементы множества X ?

4.25. Какими свойствами бинарных отношений обладают следующие отношения на множестве F всех вещественных функций, заданных на $[0, 1]$:

а) $f(x) \rho g(x) \leftrightarrow f(x) \leq g(x)$ для $\forall x \in [0, 1]$;

б) $f(x) \rho g(x) \leftrightarrow \exists c \in [0, 1]: f(c) = g(c)$;

в) $f(x) \rho g(x) \leftrightarrow f(0) = g(0), f(1) = g(1)$?

4.26. На множестве R^+ положительных действительных чисел задано отношение $a \rho b \leftrightarrow \log_b a \leq 1$. Каковы свойства данного отношения?

4.27. На множестве действительных чисел задано отношение $a \rho b \leftrightarrow tg a \leq tg b$. Какими свойствами обладает это отношение?

4.28. Пусть A множество всех подмножеств множества $\{a, b, c, d\}$. На множестве A задано отношение $x \rho y$, если x и y содержат одинаковое количество элементов. Является ли оно отношением эквивалентности? Если является, то найдите фактор-множество A/ρ по этому отношению.

4.29. На множестве $X = \{1, 2, 3, 4\}$ для каждого случая задано бинарное отношение с помощью матрицы. Изучите свойства каждого из этих бинарных отношений.

а) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$; в) $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$;

$$\begin{array}{l}
 \text{г)} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}; \text{ д)} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \text{ е)} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}; \\
 \text{ж)} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}; \text{ з)} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}; \text{ и)} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.
 \end{array}$$

4.30. Отношение ρ задано булевой матрицей A на множестве $B = \{a, b, c, d, e, f\}$:

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Запишите элементы ρ и определите свойства этого отношения. Измените элементы матрицы так, чтобы ρ стало:

- симметричным, рефлексивным, транзитивным;
- несимметричным, рефлексивным, транзитивным;
- антисимметричным, антирефлексивным, транзитивным;
- симметричным, рефлексивным, нетранзитивным.

4.31. Сколько различных бинарных отношений можно задать на множестве из трех элементов? А на множестве из n элементов, где n – натуральное число?

4.32. На множестве из четырех элементов (рис. 18) задано бинарное отношение $x\rho y$, если от



Рис. 18

x к y идет стрелка. Изучите его свойства и найдите матрицу отношения.

4.33. Даны множества $X = \{a, b, c, d\}$ и $Y = \{e, f, g, h\}$ (рис. 19) и задано бинарное отношение $x\rho y$, если от x к y идет стрелка. Найдите матрицу отношения на декартовом произведении $X \times Y$ и матрицу отношения на декартовом произведении $Y \times X$.

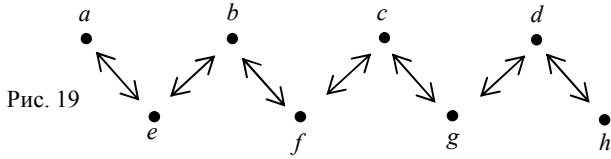


Рис. 19

4.34. На множестве $X = \{1, 2, 3\}$ задано бинарное отношение (рис. 20). Изучите его свойства и напишите матрицу отношения.

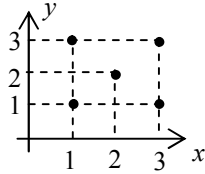


Рис. 20

4.35. На множестве всех подмножеств множества X задано отношение $A \rho B \leftrightarrow A \setminus B = \emptyset$. Будет ли это отношение частичным порядком?

4.36. Пусть A – непустое конечное множество. На множестве всех его подмножеств введем отношение $X \rho Y \leftrightarrow |X| \leq |Y|$. Является ли это отношение частичным порядком?

4.37. Докажите, что:

а) отношение \leq является отношением частичного порядка на множестве вещественных чисел;

б) в множестве подмножеств множества U отношение $A \subset B$ является отношением частичного порядка.

4.38. Докажите, что:

а) отношение \leq является отношением линейного порядка на множестве вещественных чисел;

б) отношение \subset не является линейным порядком на совокупности подмножеств.

4.39. Пусть на множестве X задано отношение частичного порядка ρ . На множестве $X \times X$ определим *отношение Парето*: $(a, b) \Pi (c, d) \leftrightarrow a \rho c$ и $b \rho d$. Изучите свойства этого отношения.

4.40. Постройте диаграмму Хассе для отношения делимости на множестве $X = \{1, 2, 3, 5, 11, 6, 15, 30, 33\}$ и найдите максимальный элемент.

4.41. Рассмотрим попарно взаимно простые числа a, b, c, d . На множестве $X = \{\{a\}, \{ab\}, \{ac\}, \{ad\}, \{abc\}, \{abd\}, \{acd\}, \{abcd\}\}$ введем порядок $x < y \leftrightarrow y : x$. Постройте диаграмму Хассе этого отношения.

4.42. На множестве функций с действительными аргументами и действительными значениями можно ввести частичный порядок, считая, что $f < g$, если $f(x) \leq g(x)$ при всех $x \in R$. Докажите, что этот порядок не является линейным.

4.43. На буквах русского языка традиционно определяется алфавитный порядок $A < B < B < Г < .. < Я$. Поясните, что это линейный порядок.

4.44. На словах русского языка определен *лексикографический* порядок: если слово x является началом слова y , то $x < y$. Например, слон $<$ слоны. Если ни одно из слов не является началом другого, посмотрим на первую по порядку букву, с которой слова начинаются, тогда слово, где эта буква раньше в алфавитном порядке, и будет предшествовать. Например, лев $<$ мышь, слон $<$ танк. Изучите свойства этого отношения.

4.45. На множестве всех прямоугольников введите следующие отношения порядка и изучите их свойства:

а) $(x_1, y_1) < (x_2, y_2) \leftrightarrow x_1 \leq x_2, y_1 \leq y_2$,

т.е. прямоугольник со сторонами x_1, y_1 вкладывается в прямоугольник со сторонами x_2, y_2 (рис. 21);

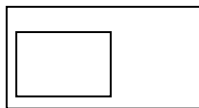


Рис. 21

б) $(x_1, y_1) < (x_2, y_2) \leftrightarrow x_1 y_1 = y_1 y_2$, т.е. прямоугольники имеют равные площади;

в) $(x_1, y_1) < (x_2, y_2) \leftrightarrow x_1 \leq x_2$, т.е. сравнение по первой стороне;

г) $(x_1, y_1) < (x_2, y_2) \leftrightarrow \sqrt{x_1^2 + y_1^2} \leq \sqrt{x_2^2 + y_2^2}$, т.е. сравнение по длине диагонали.

4.46. На множестве всех картонных коробок с измерениями a, b, c введите несколько порядков и исследуйте их свойства.

4.47. На множестве $X = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ введены бинарные отношения $x \rho_1 y \leftrightarrow x = 2y$ и $x \rho_2 y \leftrightarrow x = 3y$. Определите следующие бинарные отношения и приведите примеры некоторых упорядоченных пар для этих отношений:

а) объединение отношений $\rho_1 \cup \rho_2$;

б) пересечение отношений $\rho_1 \cap \rho_2$;

в) разность отношений $\rho_1 \setminus \rho_2$;

г) разность отношений $\rho_2 \setminus \rho_1$;

д) дополнение отношения ρ_1 , т.е. $\bar{\rho}_1$.

4.48. Бинарные ρ_1 и ρ_2 отношения заданы матрицами:

$$A(\rho_1) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad A(\rho_2) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Найдите матрицы отношений $\rho_1 \cup \rho_2$, $\rho_1 \cap \rho_2$, $\rho_1 \setminus \rho_2$, $\rho_2 \setminus \rho_1$, $\overline{\rho_1}$, $\overline{\rho_2}$.

4.49. Пусть a, b, c, d – прямые проходящие через стороны квадрата $ABCD$ (рис. 22). На множестве $X = \{a, b, c, d\}$ заданы матрицы двух бинарных отношений

$$A(\rho_1) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad A(\rho_2) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

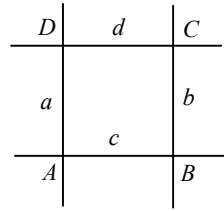


Рис. 22

Сформулируйте на геометрическом языке, что означают эти бинарные отношения.

4.50. Пусть X – конечное множество и f – отображение этого множества в себя. На множестве X задано бинарное отношение: $x\rho y \leftrightarrow y = f(x)$. Какие свойства выполняются для матрицы бинарного отношения, если:

- а) f – отображение;
- б) f – сюръективное отображение;
- в) f – инъективное отображение;
- г) f – биективное отображение?

§ 5. Булева алгебра

Отображение $f: B \times B \rightarrow B$ называется бинарной алгебраической операцией, а отображение $f: B \rightarrow B$ называется унарной алгебраической операцией.

Множество B с заданными двумя бинарными операциями ($a \vee b$ и $a \wedge b$), одной унарной алгебраической операцией \bar{a} и фиксированными элементами 0 и 1 (которые называются универсальными границами) называется булевой алгеброй, если для любых элементов $a, b, c \in B$ выполняются условия:

- 1) $a \vee b = b \vee a$, $a \wedge b = b \wedge a$ – законы коммутативности;
- 2) $(a \vee b) \vee c = a \vee (b \vee c)$, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
– законы ассоциативности;
- 3) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
– законы дистрибутивности;
- 4) $a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$ – законы поглощения;
- 5) $a \vee a = a$, $a \wedge a = a$ – законы идемпотентности;
- 6) $\overline{\overline{a}} = a$ – закон двойного отрицания;
- 7) $a \vee \bar{a} = 1$, $a \wedge \bar{a} = 0$, $a \vee 0 = a$, $a \wedge 0 = 0$, $a \vee 1 = 1$, $a \wedge 1 = a$
– законы универсальных границ;

8) $\overline{a \vee b} = \bar{a} \wedge \bar{b}$, $\overline{a \wedge b} = \bar{a} \vee \bar{b}$ – законы де Моргана.

Обозначение булевой алгебры $B = \langle B, \vee, \wedge, \bar{}, 0, 1 \rangle$.

Для упрощения записи в выражении, содержащем одну операцию, будем опускать скобки. Например:

$$(a \vee b) \vee c = a \vee b \vee c, ((a \vee b) \vee c) \vee d = a \vee b \vee c \vee d,$$

$$(a \wedge b) \wedge c = a \wedge b \wedge c, ((a \wedge b) \wedge c) \wedge d = a \wedge b \wedge c \wedge d.$$

Пример 1. Пусть M – произвольное множество и $P(M)$ – множество всех его подмножеств, тогда $\langle P(M); \cup, \cap, \bar{}, \emptyset, M \rangle$ является булевой алгеброй, которая называется булевой алгеброй подмножеств. \square

Пример 2. Пусть m – натуральное число, не делящееся ни на один квадрат простого числа и M – множество всех делителей числа m , включая 1 и m . На множестве M введены операции:

$$a \vee b = \text{НОК}(a, b) \text{ и } a \wedge b = \text{НОД}(a, b).$$

Определить самостоятельно булево дополнение произвольного элемента a , т.е. \bar{a} , универсальные границы 0 и 1. Доказать, что M с введенными операциями является булевой алгеброй.

Решение. Вспомним простейшие свойства о делимости чисел.

Если $a = p^k$, где p – простое число, k – натуральное число, то число a имеет $k+1$ делителей, включая 1 и число a .

Если $a = p_1^{k_1} p_2^{k_2}$, где p_1 и p_2 – простые различные числа, k_1 и k_2 – натуральные числа, то число a имеет $(k_1+1)(k_2+1)$ делителей, включая 1 и число a .

Если число m не делится ни на один квадрат простого числа, то оно является простым числом или каноническое разложение данного числа m содержит только произведение простых чисел в первых степенях: $m = p_1 \cdot p_2 \cdot \dots \cdot p_n$.

Решая задачу в общем виде, полезно видеть пример с конкретным числом. Например, $m = 210 = 2 \cdot 3 \cdot 5 \cdot 7$, $M = \{1, 2, 3, 5, 7, 6, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}$.

При определении наибольшего общего кратного двух чисел a и b нужно помнить, что эти числа являются делителями числа m , а поэтому $\text{НОК}(a, b)$ не превосходит самого числа m . Результат данной алгебраической операции принадлежит множеству M , на котором задана операция.

Для конкретного числа $m = 210$ приведем иллюстрирующие примеры: $6 \vee 21 = \text{НОК}(6, 21) = 42$, $6 \vee 35 = \text{НОК}(6, 35) = 210$.

Операция \wedge также замкнута на множестве M , т.е. результат операции принадлежит самому множеству M . Иллюстрирующие примеры: $6 \wedge 21 = \text{НОД}(6, 21) = 3$, $6 \wedge 35 = \text{НОД}(6, 35) = 1$.

Фиксированный элемент 0, т.е. нижнюю границу, найдем из равенств:

$$a \vee 0 = a \leftrightarrow \text{НОК}(a, ?) = a, \quad a \wedge 0 = 0 \leftrightarrow \text{НОД}(a, ?) = ?.$$

Очевидно, что элемент 0 является числом 1, т.е. нижняя граница – это самый минимальный делитель числа m .

Фиксированный элемент 1, т.е. верхнюю границу, найдем из равенств:

$$a \vee 1 = 1 \leftrightarrow \text{НОК}(a, ?) = ?, \quad a \wedge 1 = a \leftrightarrow \text{НОД}(a, ?) = a.$$

Очевидно, что элемент 1 является числом m , т.е. верхняя граница – это самый максимальный делитель числа m .

Дополнение элемента определим из равенств

$$a \vee \bar{a} = 1 \leftrightarrow \text{НОК}(a, ?) = m, \quad a \wedge \bar{a} = 0 \leftrightarrow \text{НОД}(a, ?) = 1.$$

Дополнением элемента a является элемент $\bar{a} = \frac{m}{a}$. Заметим, что этот элемент является делителем числа m , а значит, принадлежит множеству M .

Чтобы найти дополнение к элементу a , можно в каноническом разложении данного числа m найти дополняющие множители к каноническому разложению рассматриваемого числа a .

Пример для $m = 210$ и $a = 42$.

$$\text{Первый способ. } \bar{42} = \frac{210}{42} = 5.$$

$$\text{Второй способ. } m = 210 = 2 \cdot 3 \cdot 5 \cdot 7, \quad a = 42 = 2 \cdot 3 \cdot 7, \quad \bar{42} = 5.$$

Далее условия 1) – 8) булевой алгебры для введенных операций легко проверяются, если для делителей числа m и операций использовать канонические разложения.

Пусть $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_s^{\beta_s}$, тогда

$$a \vee b = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_k^{\gamma_k}, \quad a \wedge b = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot \dots \cdot p_k^{\lambda_k}, \quad \text{где}$$

$\gamma_i = \max(\alpha_i, \beta_i)$, $\lambda_i = \min(\alpha_i, \beta_i)$, причем числа α_i и β_i принимают значения 1 в первоначальном разложении чисел a и b , но при образовании результата операции можно считать, что степень отсутствующего множителя в одном из элементов принимает нулевое значение.

Пример 3. n -мерный вектор $a = (a_1, a_2, \dots, a_n)$ называется булевым вектором длины n , если каждая его координата принимает значение 0 или 1. Пусть A_n множество всех векторов длины n . Тогда $A_n = \{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}$. Для булевых векторов $a = (a_1, a_2, \dots, a_n)$ и $b = (b_1, b_2, \dots, b_n)$ определим операции:

$$a \vee b = (\max(a_1, b_1), \max(a_2, b_2), \dots, \max(a_n, b_n)),$$

$$a \wedge b = (\min(a_1, b_1), \min(a_2, b_2), \dots, \min(a_n, b_n)),$$

$$\bar{a} = (1 - a_1, 1 - a_2, \dots, 1 - a_n).$$

Определим универсальные границы $0 = (0, 0, \dots, 0)$, $1 = (1, 1, \dots, 1)$, тогда $\langle A_n; \vee, \wedge, \bar{}, 0, 1 \rangle$ является булевой алгеброй, которая называется алгеброй булевых векторов. \square

Пример 4. Булевой функцией от n переменных называется любое отображение $f : A_n \rightarrow \{0,1\}$. Все булевы функции от двух переменных представлены в таблице 6.

Таблица 6

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Всего существует 2^n наборов аргументов, поэтому функцию от n переменных можно задать булевым вектором значений на этих наборах, т.е. $g(x_1, x_2, \dots, x_n) = (g_1, g_2, \dots, g_{2^n})$. На множестве F_n всех булевых функций от n переменных введем операции.

Для булевых функций $g(g_1, g_2, \dots, g_{2^n})$ и $h(h_1, h_2, \dots, h_{2^n})$ определим операции

\vee и \wedge как операции с булевыми векторами, т.е.

$$g \vee h = (\max(g_1, h_1), \max(g_2, h_2), \dots, \max(g_{2^n}, h_{2^n})),$$

$$g \wedge h = (\min(g_1, h_1), \min(g_2, h_2), \dots, \min(g_{2^n}, h_{2^n})).$$

В качестве универсальных границ выберем функции

$$0(x_1, x_2, \dots, x_n) = \underbrace{(0, 0, \dots, 0)}_{2^n}, \quad 1(x_1, x_2, \dots, x_n) = \underbrace{(1, 1, \dots, 1)}_{2^n}.$$

Множество F_n с введенными операциями и универсальными границами является булевой алгеброй, которая называется алгеброй булевых функций от n переменных. \square

Пример 5. Пусть множество $B = \{x_1, x_2, \dots, x_n\}$ состоит из n упорядоченных элементов и A – подмножество множества B . Характеристической функцией подмножества A в множестве B называется отображение, которое подмножеству A сопоставляет булев вектор длины n , т.е. $\chi_B^A = (\chi_B^A(x_1), \chi_B^A(x_2), \dots, \chi_B^A(x_n))$, где

$$\chi_B^A(x_i) = \begin{cases} 1, & x_i \in A, \\ 0, & x_i \notin A. \end{cases}$$

Для множества $B = \{x_1, x_2, x_3\}$ рассмотрим подмножества: $A = \emptyset$, $C = \{x_2\}$, $D = \{x_1, x_3\}$, тогда соответствующие булевы векторы

$$\chi_B^A = (000), \quad \chi_B^C = (010), \quad \chi_B^D = (101).$$

Пусть в множестве $M = \{x_1, x_2, \dots, x_n\}$ заданы подмножества A и B , которым соответствуют булевы векторы $\chi_M^A = (\alpha_1, \alpha_2, \dots, \alpha_n) = a$, $\chi_M^B = (\beta_1, \beta_2, \dots, \beta_n) = b$, тогда $\chi_M^{A \cup B} = (\max(\alpha_1, \beta_1), \max(\alpha_2, \beta_2), \dots, \max(\alpha_n, \beta_n)) = a \vee b$,

$$\chi_M^{A \cap B} = (\min(\alpha_1, \beta_1), \min(\alpha_2, \beta_2), \dots, \min(\alpha_n, \beta_n)) = a \wedge b,$$

$$\chi_M^{A \setminus B} = (\min(\alpha_1, 1 - \beta_1), \min(\alpha_2, 1 - \beta_2), \dots, \min(\alpha_n, 1 - \beta_n)) = a \setminus b,$$

где операция разности приведена в таблице 7.

Таблица 7

α_i	β_i	$\alpha_i \setminus \beta_i$
0	0	0
0	1	0
1	0	1
1	1	0

Дано множество $M = \{1,2,3,4,5,6,7,8,9\}$ и три его подмножества $A = \{3,5,6,8,9\}$, $B = \{3,6,7,8\}$, $C = \{1,2,5,8,9\}$. Найти значения характеристической функции для подмножеств A , B , C и множества $X = [A \setminus (B \cap C)] \setminus [B \setminus (A \cap C)]$. Из каких элементов состоит множество X ?

Решение. Для данных подмножеств и некоторых вспомогательных подмножеств составляем булевы векторы. Последовательности желательно выписывать так, чтобы соответствующие разряды в разных последовательностях находились на одной вертикальной линии. Это упрощает выполнение логических операций с соответствующими разрядами:

$$f(A) = (001011011),$$

$$f(B) = (001001110),$$

$$f(C) = (110010011),$$

$$f(B \cap C) = (000000010),$$

$$f(A \setminus (B \cap C)) = (001011001),$$

$$f(A \cap C) = (000010011),$$

$$f(B \setminus (A \cap C)) = (001001100),$$

$$f(X) = (000010001).$$

Значения функции можно оформить другим способом с помощью табл. 8.

Таблица 8

M	1	2	3	4	5	6	7	8	9
Подмножество	Булев вектор								
A	0	0	1	0	1	1	0	1	1
B	0	0	1	0	0	1	1	1	0
C	1	1	0	0	1	0	0	1	1
$B \cap C$	0	0	0	0	0	0	0	1	0
$A \setminus (B \cap C)$	0	0	1	0	1	1	0	0	1
$A \cap C$	0	0	0	0	1	0	0	1	1
$B \setminus (A \cap C)$	0	0	1	0	0	1	1	0	0
$X = [A \setminus (B \cap C)] \setminus [B \setminus (A \cap C)]$	0	0	0	0	1	0	0	0	1

По булевому вектору множества X строим искомое множество $X = \{5,9\}$.

Задачи.

5.1. Докажите следующие соотношения для любой булевой алгебры

а) $(a \wedge b) \vee (c \wedge d) = (a \vee c) \wedge (a \vee d) \wedge (b \vee c) \wedge (b \vee d)$;

б) $(a \vee b) \wedge (c \vee d) = (a \wedge c) \vee (a \wedge d) \vee (b \wedge c) \vee (b \wedge d)$;

$$в) (a \vee b) \wedge (\bar{a} \vee b) = b;$$

$$г) (a \vee b) \wedge (\bar{a} \vee c) = (a \wedge c) \vee (\bar{a} \wedge b) \vee (b \wedge c);$$

$$д) \overline{(a \wedge b) \vee (c \wedge \bar{b})} = (\bar{a} \wedge b) \vee (\bar{c} \wedge \bar{b}) \vee (\bar{a} \wedge \bar{c}).$$

5.2. Пусть $B = \{3, 4\}$ и для элементов множества B определены операции $a \vee b = \max(a, b)$, $a \wedge b = \min(a, b)$, $\bar{3} = 4$, $\bar{4} = 3$. Пусть меньшая универсальная граница равна 3, а наибольшая универсальная граница равна 4, т.е. имеет место символическая запись $0 = 3$, $1 = 4$. Докажите, что $B = \langle B, \max, \min, \bar{\cdot}, 3, 4 \rangle$ является булевой алгеброй.

5.3. Дано множество $U = \{x_1, \dots, x_{10}\}$. Подмножества X, Y, Z заданы характеристическими функциями: $X = \{1, 1, 0, 1, 0, 1, 1, 0, 1, 0\}$, $Y = \{1, 0, 1, 1, 1, 0, 1, 1, 0, 1\}$, $Z = \{1, 0, 1, 0, 0, 1, 1, 1, 0, 0\}$. Определите характеристические функции множеств

$$а) A = [(X \cup Y) \setminus Z] \setminus [(X \setminus Z) \cup (Y \setminus Z)];$$

$$б) B = (\bar{X} \cup Y) \cap (\bar{Y} \cup Z) \cap (\bar{Z} \cup X);$$

$$в) C = [X \setminus (Y \cap Z)] \cup [Y \setminus (X \cap Z)];$$

$$г) D = [(X \cap Z) \setminus (X \cap \bar{Z})] \cup (Y \cap Z).$$

5.4. Используя характеристические функции подмножеств, докажите равенства

$$а) \overline{A \setminus B} = \bar{A} \cup B;$$

$$б) A \cap B = A \setminus (A \setminus B);$$

$$в) (\bar{A} \cup B) \cap A = A \cap B;$$

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

$$д) (A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C);$$

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

$$ж) A \setminus (B \cup C) = (A \setminus B) \setminus C;$$

$$з) (A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C);$$

$$и) A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C).$$

5.5. Дано множество $M = \{a, b, c, d, e, f, g, h, i\}$ и его подмножества $A = \{a, b, e, f, i\}$, $B = \{b, c, d, g, h\}$, $C = \{a, d, g, h, i\}$. Из каких элементов состоит множество $X = (A \setminus B) \cup (B \cap C) \cup (\bar{B} \setminus C)$?

5.6. Определите соотношения между множествами

а) $A \setminus (B \cap C)$ и $(A \setminus B) \cup (A \setminus C)$;

б) $(A \cap B) \setminus C$ и $A \cup B$;

в) $A \cap B \cap C$ и $(A \Delta B) \setminus A$;

г) $(B \cup C) \cap (B \cup A)$ и $(\bar{A} \cup C) \cap A$;

д) $B \setminus (A \cup C)$ и $(A \cap C) \setminus B$.

5.7. Покажите, что в любой булевой алгебре универсальные границы 0 и 1 определены однозначно. Используя это, покажите, что в примере 2, если m делится на квадраты, то построения затем структур в примере не будет булевой алгеброй.

5.8. Покажите, что в любой булевой алгебре B следующие условия эквивалентны:

а) $a \wedge b = a$; б) $a \vee b = b$; в) $\bar{b} \wedge \bar{a} = \bar{b}$; г) $\bar{b} \vee \bar{a} = \bar{a}$.

5.9. Пусть дано частично упорядоченное множество $\langle X, \leq \rangle$ и в нем подмножество $S \subseteq X$. Элемент $a \in X$ называется верхней (нижней) гранью подмножества S , если выполняются условия:

1) $x \leq a$ ($a \leq x$) для любого элемента $x \in S$;

2) если $b \in X$ таков, что $x \leq b$ ($b \leq x$) для всех $x \in S$, то $a \leq b$ ($b \leq a$).

Верхняя и нижняя грани множества S обозначаются как $\sup_x S$ (супремум) и $\inf_x S$ (инфимум) соответственно.

В булевой алгебре B введем отношение ρ , полагая $a \rho b$ тогда и только тогда, когда $a \wedge b = a$. Покажите, что ρ есть частичный порядок, причем относительно данного порядка $\sup \{a, b\} = a \vee b$ и $\inf \{a, b\} = a \wedge b$.

Относительно этого порядка в булевой алгебре для любого элемента x имеет место $0 \leq x \leq 1$, чем объясняется название 0, 1 – универсальные границы.

Охарактеризуйте данный частичный порядок для алгебр подмножеств $P(M)$, булевых векторов A_n и булевых функций F_n .

Глава 2. Булевы функции

§ 6. Логические операции

Высказыванием (*утверждением*) называется такое предложение, которое истинно или ложно, но не то и другое вместе.

Таблица 1

A	\bar{A}
0	1
1	0

Высказывания A и B в этом параграфе имеют логический тип, означают истину или ложь и обозначены символами 1 или 0.

Отрицанием высказывания A называется высказывание, которое истинно тогда и только тогда, когда высказывание A ложно.

Обозначение отрицания: \bar{A} или $\neg A$ (таблица 1). Читается “не A ”.

Дизъюнкцией двух высказываний A и B называется высказывание, которое ложно тогда и только тогда, когда оба высказывания ложны (другими словами: высказывание истинно, когда по крайней мере одно из высказываний – истинно). Обозначение $A \vee B$ (таблица 2). Читается “ A или B ”.

Конъюнкцией двух высказываний A и B называется высказывание, которое истинно тогда и только тогда, когда оба высказывания истинны (другими словами: высказывание истинно, когда каждое из высказываний – истинно). Обозначения $A \wedge B$ или AB (таблица 2). Читается “ A и B ”.

Импликацией высказываний A и B называется высказывание, которое ложно тогда и только тогда, когда A истинно, а B ложно. Обозначение импликации $A \rightarrow B$ (таблица 2). Высказывание A называется *посылкой (условием)*, а высказывание B – *заключением (следствием)*. Высказывание A является *достаточным условием* для B , а высказывание B является *необходимым условием* для A . Читается “если A то B ” или “из A следует B ”.

Эквивалентность высказываний A и B называется высказывание, которое истинно тогда и только тогда, когда оба высказывания принимают одинаковые логические значения. Обозначение эквивалентности $A \leftrightarrow B$ или $A \sim B$ (таблица 2). Читается “ A эквивалентно B ” или “ A тогда и только тогда, когда B ” или “для A необходимо и достаточно B ”.

Суммой по модулю 2 высказываний A и B называется высказывание, которое истинно тогда и только тогда, когда оба высказывания принимают различные логические значения (только одно из высказываний истинно). Обозначение $A \oplus B$ (таблица 2). Читается “сумма A и B по модулю 2”.

Таблица 2

A	B	$A \vee B$	$A \wedge B$	$A \rightarrow B$	$A \leftrightarrow B$	$A \oplus B$
0	0	0	0	1	1	0
0	1	1	0	1	0	1
1	0	1	0	0	0	1
1	1	1	1	1	1	0

Порядок выполнения операций: приоритет имеет отрицание, затем конъюнкция, дизъюнкция, следование и, наконец, эквивалентность. Для выделения приоритета операций используют скобки.

Запись выражения $\neg A \wedge B \vee C \wedge D$ совпадает с $((\neg A) \wedge B) \vee (C \wedge D)$.

Законы логики высказываний:

$A \vee A = A, \quad A \wedge A = A$ (1) идемпотентность;

$A \vee B = B \vee A, \quad A \wedge B = B \wedge A$ (2) коммутативность;

$A \vee (B \vee C) = (A \vee B) \vee C, \quad A \wedge (B \wedge C) = (A \wedge B) \wedge C$ (3) ассоциативность;

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C), \quad A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ (4) дистрибутивность;

– общий “множитель” в двух скобках с одной и той же операцией можно

выносить за скобки;

$A \vee (A \wedge B) = A, \quad A \wedge (A \vee B) = A$ (5) поглощение;

$A \vee 0 = A, \quad A \wedge 0 = 0$ (6) свойство ложного;

$A \vee 1 = 1, \quad A \wedge 1 = A$ (7) свойство истинного;

$\overline{\overline{A}} = A$ (8) двойное отрицание;

$\overline{A \vee B} = \overline{A} \wedge \overline{B}, \quad \overline{A \wedge B} = \overline{A} \vee \overline{B}$ (9) формулы де Моргана;

$\overline{A \vee B \vee C} = \overline{A} \wedge \overline{B} \wedge \overline{C}, \quad \overline{A \wedge B \wedge C} = \overline{A} \vee \overline{B} \vee \overline{C}$ (9a);

$A \vee \overline{A} = 1, \quad A \wedge \overline{A} = 0$ (10) формулы дополнения;

$A = (A \wedge B) \vee (A \wedge \overline{B}), \quad A = (A \vee B) \wedge (A \vee \overline{B})$ (11) формулы расщепления;

$A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A)$ (12);

$A \leftrightarrow B = AB \vee \overline{A}\overline{B}$ (13);

$A \rightarrow B = \overline{A} \vee B = \overline{A \wedge \overline{B}}$ (14);

$A \vee B = \overline{\overline{A} \rightarrow B}$ (15);

$A \wedge B = \overline{A \rightarrow \overline{B}}$ (16);

$A \vee (\overline{A}B) = A \vee B, \quad A(\overline{A} \vee B) = AB$ (17);

$AB \vee \overline{B}\overline{C} \vee AC = A \vee \overline{B}\overline{C}$ (18);

$(A \vee B)(\overline{B} \vee \overline{C})(A \vee C) = A(\overline{B} \vee \overline{C})$ (19).

Формулой называется представление сложного высказывания с помощью простых логических высказываний, соединенных логическими символами: $\vee, \wedge, \neg, \rightarrow, \leftrightarrow, \oplus$ и символов скобок (...).

Таблица, в которой указаны всевозможные наборы значений высказываний и значения формулы на этих наборах, называется таблицей истинности.

Две формулы $A(X_1, X_2, \dots, X_n)$ и $B(X_1, X_2, \dots, X_n)$ называются равносильными, если они принимают одинаковые значения при одних и тех же значениях переменных X_1, X_2, \dots, X_n . Записывается это как $A(X_1, X_2, \dots, X_n) = B(X_1, X_2, \dots, X_n)$, причем $A = B$ тогда и только тогда, когда формула $A \leftrightarrow B$ истинна для любых значений переменных.

Пример 1. Докажите, что следующие формулы $f_1 = \overline{\overline{x}yz} \vee \overline{x\overline{y}z}$ и $f_2 = \overline{(\overline{yx} \vee \overline{yz})} \overline{xy} \vee yz \vee xz$ равносильны.

Решение. Первый способ. $f_1 = \overline{x} \overline{y} z \vee x \overline{y} z = \overline{y} z (\overline{x} \vee x) = \overline{y} z 1 = \overline{y} z$.

$$\begin{aligned} f_2 &= (\overline{y} x \vee \overline{y} z) \overline{(x y \vee y z \vee x z)} = (\overline{y} x \vee \overline{y} z) (\overline{x y} \overline{y z} \overline{x y}) = \\ &= \overline{y} (x \vee z) ((\overline{x} \vee \overline{y}) (\overline{y} \vee \overline{z}) (\overline{x} \vee \overline{z})) = \overline{y} (x \vee z) (\overline{x} \vee \overline{z}) (\overline{x} \vee \overline{y}) (\overline{y} \vee \overline{z}) = \\ &= \overline{y} (x \vee z) (\overline{x} \vee \overline{z}) (\overline{x} \vee \overline{y}) (\overline{y} \vee \overline{z}) = \overline{y} (x \overline{x} \vee x \overline{y} \vee x \overline{z} \vee x \overline{y} \overline{z} \vee \overline{x} \overline{y} \vee \overline{x} \overline{z} \vee \overline{x} \overline{y} \overline{z} \vee \overline{y} \overline{z}) = \\ &= \overline{y} (x \overline{x} \vee z) (\overline{x} \overline{z} \vee \overline{y}) = \overline{y} z (\overline{x} \overline{z} \vee \overline{y}) = \overline{y} z \overline{x} \overline{z} \vee \overline{y} z \overline{y} = \overline{y} z. \end{aligned}$$

Второй способ. Достаточно проверить равносильность этих формул, приравняв одну из переменных 1, а затем 0. Например, при $z=1$ получаем $f_1 = \overline{x} \overline{y} \vee x \overline{y} = (\overline{x} \overline{y} \vee x \overline{y}) = \overline{y}$, $f_2 = (\overline{y} x \vee \overline{y}) \overline{x y \vee y} = \overline{y} \overline{y} = \overline{y}$.

При $z=0$ получаем $f_1 = 0$, $f_2 = (\overline{y} x) \overline{x y \vee x} = (\overline{y} x) \overline{x} = 0$.

Равносильность формул доказана. \square

Формула $f(X_1, X_2, \dots, X_n)$ называется *выполнимой*, если существует набор высказываний A_1, A_2, \dots, A_k , который обращает эту формулу в истинное высказывание.

Формула $f(X_1, X_2, \dots, X_n)$ называется *опровержимой*, если существует набор высказываний A_1, A_2, \dots, A_k , который обращает эту формулу в ложное высказывание.

Формула называется *тождественно истинной (тавтологией)*, если она обращается в истинное высказывание при всех наборах значений переменных.

Формула называется *тождественно ложной (противоречием)*, если она обращается в ложное высказывание при всех наборах значений переменных.

Формула $G(x_1, x_2, \dots, x_n)$ называется *логическим следствием* формул $F_1(x_1, x_2, \dots, x_n), \dots, F_m(x_1, x_2, \dots, x_n)$, если она обращается в истинное высказывание на всяком наборе значений переменных, для которого в истинные высказывания обращаются все формулы F_1, \dots, F_m . Обозначение: $F_1, \dots, F_m \rightarrow G$.

Законы логического вывода – это тавтологии, т.е. высказывания, истинные при любых значениях переменных:

1. $A \vee \overline{A} = 1$ – закон *исключенного третьего*: или A истинно, или A ложно (третьего не дано).

2. $A \wedge \overline{A} = 0$ – закон *противоречия* (невозможно, чтобы выполнялось A и его отрицание; A и его отрицание не могут выполнять одновременно).

3. $A \rightarrow (\overline{\overline{A}})$ – закон *двойного отрицания*.

4. $(A \rightarrow B) \leftrightarrow (\overline{B} \rightarrow \overline{A})$ – закон *контрапозиции*.

Правила логического вывода:

1. $((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$ – *правило транзитивности, упрощенное правило силлогизма*: если “из A следует B ” и если “из B следует C ”, то “из A следует C ”.

Используется другая запись:

$$\frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C}.$$

2. $((A \rightarrow B) \wedge A) \rightarrow B$ – правило *modus ponens*, утверждающий модус, если “из A следует B ” и выполняется A , то выводится B

$$\frac{A \rightarrow B, A}{B}.$$

3. $((A \rightarrow B) \wedge \bar{B}) \rightarrow \bar{A}$ – правило *modus tollens*, отрицающий модус, если “из A следует B ” и “не B ” то выводится “не A ”, если из A следует B , но высказывание B неверно, то неверно A

$$\frac{A \rightarrow B, \bar{B}}{\bar{A}}.$$

4. $(A \vee B) \wedge \bar{A} \rightarrow B$ – если “ A или B ” и “не A ”, то выводится B ; если истинно A или B и неверно A , то верно B

$$\frac{A \vee B, \bar{A}}{B}.$$

5. $(A \rightarrow \bar{A}) \rightarrow \bar{A}$ – принцип приведения к абсурду: если из A следует “не A ”, то из этого выводится “не A ”.

6. $(A \wedge B) \rightarrow A$ – если выполняются утверждения A и B , то конечно выполняется A .

7. $A \rightarrow (A \vee B)$ – если выполняется утверждение A , то конечно выполняется A или B

$$8. (A \rightarrow B) \rightarrow ((A \vee C) \rightarrow (B \vee C)).$$

$$9. (A \rightarrow B) \rightarrow ((A \wedge C) \rightarrow (B \wedge C)).$$

Задачи.

6.1. Являются ли высказываниями следующие предложения:

а) диагонали ромба взаимно перпендикулярны;

б) $\sin x$ не больше 1;

в) число 0,000002 очень мало;

г) $\sqrt{3}$ – число нечетное;

д) 5 сентября следующего года в г. Сургуте будет дождь;

е) длина окружности радиуса R равна $3R$?

6.2. Сформулируйте отрицания следующих высказываний:

а) $A = \{\sqrt{3} > 2\}$;

б) $B = \{\sqrt{5} - \text{простое число}\}$;

в) число 2 является делителем числа 10.

6.3. Даны высказывания: $A = \{\text{Студент Петров изучает английский язык}\}$, $B = \{\text{Студент Петров успевает по дискретной математике}\}$.

Дайте словесную формулировку высказываниям:

а) $A \wedge \bar{B}$; б) $A \rightarrow B$; в) $\bar{B} \vee \bar{A}$.

6.4. Истинно или ложно высказывание A , если высказывание

а) $(A \text{ и } 2 \cdot 3 < 7)$ – истинно; в) $(A \text{ или } 2 \cdot 2 \geq 7)$ – ложно;

б) $(A \text{ или } 2 \cdot 3 > 7)$ – истинно; г) $(A \text{ и } 3 \cdot 3 \leq 9)$ – ложно?

6.5. Истинно или ложно высказывание:

а) если 18 делится на 6, то 18 делится на 3;

б) если 11 делится на 6, то 11 делится на 2;

в) если 15 делится на 6, то 15 делится на 3;

г) если 15 делится на 5, то 15 делится на 10?

6.6. Истинно или ложно высказывание A , если следующее высказывание истинно:

а) если A , то 6 – нечетное число; г) если $12:4$, то A или $5:2$;

б) если $4 > 2$, то $6:2$ и A ; д) если A или $6:3$, то $8:4$ и A ?

в) если $11 > 11$ и A , то $5 > 7$;

6.7. Постройте отрицания следующих сложных высказываний:

а) число a делится на 5 и число b делится на 5;

б) число a не делится на 5 и число b не делится на 5;

в) число a делится на 5 или число b не делится на 5;

г) число a не делится на 5 и число b делится на 5;

д) число a делится на 5 или число b не делится на 5.

6.8. Докажите, что $x \wedge 0$, $x \wedge 0 \wedge (y \rightarrow z)$ являются тождественно ложными формулами, а $x \vee 1$, $x \vee 1 \vee (y \rightarrow z)$ являются тождественно истинными формулами.

6.9. Докажите, что формулы $x \wedge 1$, $x \vee 0$ являются как выполнимыми, так и опровержимыми.

6.10. Упростите формулы $\overline{x_1 \vee x_1 x_2}$, $\overline{x_1 \vee x_2 \wedge x_1}$ двумя способами, снимая отрицания.

6.11. Расставьте скобки так, чтобы получилась формула:

а) $\neg A \rightarrow B \vee C \rightarrow D$; б) $A \wedge B \rightarrow \bar{C} \rightarrow D$.

6.12. Уберите скобки: $(A \rightarrow ((\neg(B \rightarrow C)) \vee (B \wedge (D \rightarrow A))))$.

6.13. Докажите равенства:

а) $(A \vee B)(C \vee D) = AC \vee AD \vee BC \vee BD$;

б) $(AB) \vee (CD) = (A \vee C)(A \vee D)(B \vee C)(B \vee D)$;

в) $AB \vee A\bar{B} = A$;

г) $(A \vee B)(A \vee \bar{B}) = A$;

- д) $A \vee AB \vee AC \vee \dots \vee AW = A$;
 е) $A(A \vee B)(A \vee C) \dots (A \vee W) = A$;
 ж) $AB \vee \overline{ABC} \vee \overline{BAC} \vee \overline{AC} = A$;
 з) $\overline{XY} \vee \overline{X\overline{Y}}(X \vee \overline{Y}) = X\overline{Y}$;
 и) $\overline{(X \vee Y) \rightarrow \overline{Y \vee Z}} = Y \vee XZ$.

6.14. Укажите, какое выражение равносильно выражению

$$\overline{A \vee \overline{B} \vee C}:$$

- 1) $\overline{A} \vee B \vee \overline{C}$; 2) $A \wedge \overline{B} \wedge C$; 3) $\overline{A} \vee \overline{B} \vee \overline{C}$; 4) $\overline{A} \wedge B \wedge \overline{C}$.

6.15. Докажите тождественную ложность формулы

$$f(x_1, x_2) = [x_1 \leftrightarrow \overline{(x_2 \vee x_1)}] \leftrightarrow [x_1 \leftrightarrow (x_2 \vee x_1)].$$

6.16. Докажите тождественную истинность формулы

$$f(x_1, x_2, x_3) = (x_1 \rightarrow x_2) \vee [x_2 \leftrightarrow (x_3 \rightarrow x_1)].$$

6.17. Постройте таблицу истинности для формул:

а) $A = [(P \wedge Q) \rightarrow (\overline{P} \wedge \overline{Q})] \rightarrow (P \wedge Q)$;

б) $B = (P \rightarrow R) \rightarrow [(P \rightarrow (R \rightarrow Q)) \rightarrow (P \rightarrow R)]$.

6.18. Упростите:

а) $(A \vee B)(BA)$; б) $\overline{A \vee B}(\overline{A} \vee \overline{B})$; в) $(A \rightarrow \overline{B})(A \rightarrow C)$;

г) $(A \vee B) \rightarrow (A \vee C)$; д) $(A \rightarrow B) \rightarrow AC$; е) $\overline{A}(A \vee B)$;

ж) $(A \rightarrow B)(B \rightarrow A)(A \vee B)$; з) $(A \rightarrow B)(B \rightarrow \overline{A})(A \vee B)$;

и) $\overline{(A \rightarrow B)(B \rightarrow \overline{A})}$; к) $(P \vee Q)(Q \vee P)$;

л) $(P \vee Q) \vee (R \vee P)$; м) $(P \vee Q)(QP)$;

н) $\overline{(P \vee Q)(\overline{P} \vee \overline{Q})}$; о) $(P \rightarrow \overline{Q})(P \rightarrow R)$;

п) $PQ \rightarrow \overline{P}$; р) $(P \vee Q) \rightarrow (P \vee R)$; с) $(P \rightarrow Q) \rightarrow (PR)$;

т) $(\overline{AB})(B \vee C)(A \vee (BC))$; у) $(\overline{XY} \vee \overline{XYZ})(\overline{X} \vee \overline{XY} \vee \overline{Y})$;

ф) $(AB \vee (A \vee B)) \vee \overline{A \vee B}$; х) $((A \vee B)AB) \vee \overline{A \vee B}$;

ц) $\overline{(AB(A \vee B)) \vee (AB \vee (A \vee B))}$; ч) $(AB(A \vee B)\overline{AB})\overline{AB(A \vee B)}$.

6.19. Докажите справедливость следующих правил логического вывода:

а) Правило противоречия: если из A следует B и из A следует \bar{B} , то неверно A

$$\frac{A \rightarrow B, A \rightarrow \bar{B}}{A};$$

б) правило сечения $\frac{A \rightarrow B, (B \wedge C) \rightarrow D}{(A \wedge C) \rightarrow D}$;

в) правила дилемм

$$\frac{A \rightarrow C, B \rightarrow C, A \vee B}{C}, \frac{A \rightarrow B, C \rightarrow D, A \vee C}{B \vee D};$$

г) правило объединения посылок $\frac{A \rightarrow (B \rightarrow C)}{(AB) \rightarrow C}$;

д) правило разъединения посылок $\frac{(AB) \rightarrow C}{A \rightarrow (B \rightarrow C)}, \frac{(AB) \rightarrow C}{B \rightarrow (A \rightarrow C)}$;

е) правило пересечения заключений $\frac{(A \rightarrow B), (A \rightarrow C)}{(A \rightarrow BC)}$.

6.20. Покажите, что следующие рассуждения не являются правильными. При каких значениях переменных нарушается правило логического вывода:

а) $\frac{A \rightarrow B, B}{A}$; б) $\frac{A \rightarrow B, \bar{A}}{\bar{B}}$; в) $\frac{A \vee B, A}{\bar{B}}$?

6.21. Докажите, что множество классов равносильных формул относительно операций $\vee, \wedge, \bar{}$ образует булеву алгебру, которая называется алгеброй высказываний.

§ 7. Прямая, обратная и противоположная теоремы

Структуру каждой теоремы можно выразить следующим образом: “Если высказывание A истинно, то высказывание B также истинно” или “из истинности высказывания A следует истинность высказывания B ”. Символическая запись

$$A \rightarrow B. \quad (1)$$

Условие A называется *достаточным* для выполнения B , а условие B – *необходимым* для A .

Теорема 1. В равнобедренном треугольнике углы при основании равны.

Высказывания A и B можно записать в виде: $A = \{\text{треугольник является равнобедренным, т.е. имеет две равных стороны}\}$, $B = \{\text{в треугольнике два угла равны}\}$. □

Для сложного высказывания (1) построим следующие составные высказывания:

$$B \rightarrow A, \quad (2)$$

$$\overline{A} \rightarrow \overline{B}, \quad (3)$$

$$\overline{B} \rightarrow \overline{A}. \quad (4)$$

Высказывания (1) и (2) называются *взаимно обратными*. Аналогично, (3) и (4) являются взаимно обратными высказываниями.

Теорема 2. Если в треугольнике два угла равны, то треугольник является равнобедренным.

Теорема 2 является обратной к теореме 1, и, наоборот, теорема 1 является обратной к теореме 2.

Высказывание 1. Сумма двух четных чисел является четным числом.

Высказывание 2. Если сумма двух чисел является четным числом, то каждое из чисел является четным.

Высказывания 1 и 2 являются взаимно обратными, но высказывание 2 не является истинным.

Если истинны оба взаимно обратных высказывания, то говорят о *взаимно обратных теоремах*.

Высказывания (1) и (3) называются *взаимно противоположными*. Аналогично, высказывания (2) и (4) называются взаимно противоположными. Если взаимно противоположные высказывания являются истинными, то говорят о *взаимно противоположных теоремах*.

Теорема 3. Если в треугольнике две стороны не равны, то и противолежащие им углы также не равны.

Теорема 4. Если в треугольнике два угла не равны, то и противолежащие им стороны также не равны.

Среди теорем 1–4 укажите все пары взаимно обратных и взаимно противоположных теорем.

Составим таблицу истинности (таблица 3) высказываний (1)–(4).

Таблица 3

A	B	$A \rightarrow B$	$B \rightarrow A$	\overline{A}	\overline{B}	$\overline{A} \rightarrow \overline{B}$	$\overline{B} \rightarrow \overline{A}$
0	0	1	1	1	1	1	1
0	1	1	0	1	0	0	1
1	0	0	1	0	1	1	0
1	1	1	1	0	0	1	1

Из таблицы видно, что высказывания $A \rightarrow B$ и $\overline{B} \rightarrow \overline{A}$ равносильны. Аналогично, высказывания $B \rightarrow A$ и $\overline{A} \rightarrow \overline{B}$ равносильны.

Равносильность высказываний $A \rightarrow B$ и $\overline{B} \rightarrow \overline{A}$ называется *законом контрапозиции*.

Существуют следующие способы доказательства теоремы $A \rightarrow B$:

1. **Прямое рассуждение.** Предположим, что A истинно. Используя правило логического вывода, т.е. используя истинность импликации $A \rightarrow B$, получаем единственно возможное заключение: B – истинно.

2. **Обратное рассуждение.** На основе закона контрапозиции вместо утверждения $A \rightarrow B$ доказываем равносильное утверждение $\bar{B} \rightarrow \bar{A}$ и приходим к противоречию с данным условием A .

Действительно. Предположим, что B – ложно, тогда \bar{B} истинно. Используя правило логического вывода, т.е. истинность импликации, получаем, что \bar{A} истинно, но тогда A ложно. Это противоречит тому, что A по условию истинно.

3. **Метод “от противного”.** Предполагаем, что A истинно, а B ложно, но тогда импликация $A \rightarrow B$ должна быть ложной. Используя правило логического вывода, мы должны получить противоречие в выводе, т.е. в логической цепочке рассуждений. Фактически это сводится к тому, что для более простого объекта получаем два противоречивых утверждения.

Оба метода (обратное рассуждение и “от противного”) имеют общее начало – допускаем, что утверждение B ложно. В обратном рассуждении ищем противоречие с данным условием. В методе “от противного” ищем противоречие в импликации.

Задачи.

7.1. Для сформулированных выше высказываний 1 и 2 постройте противоположные высказывания, используя формулу снятия отрицания с конъюнкции $\overline{A \cap B} = \bar{A} \cup \bar{B}$. Какие из построенных утверждений являются истинными?

7.2. Реализуйте различные способы доказательств теоремы 1 и высказывания 1.

7.3. Выделите условие и заключение в следующих высказываниях и запишите в виде $A \rightarrow B$. Сформулируйте обратное утверждение и определите его истинность:

- а) если произведение двух целых чисел – число нечетное, то сумма этих чисел есть число четное;
- б) все вписанные углы, опирающиеся на одну и ту же дугу равны между собой;
- в) если в треугольнике один угол прямой, то два другие – острые;
- г) в треугольнике каждая сторона меньше суммы двух других, но больше их разности.

7.4. Для следующих случаев сформулируйте высказывание $A \rightarrow B$ и обратное к нему. Определите истинность этих высказываний:

- а) $A = \{\text{четырёхугольник является прямоугольником}\}$,
 $B = \{\text{диагонали четырёхугольника равны}\}$;
- б) $A = \{\text{натуральное число } a \text{ делится на } 9\}$,
 $B = \{\text{сумма цифр натурального числа } a \text{ делится на } 3\}$;
- в) $A = \{\text{четырёхугольник является ромбом}\}$,
 $B = \{\text{диагонали четырёхугольника делят его углы пополам}\}$.

7.5. Для теоремы “В параллелограмме диагонали, пересекаясь, делятся пополам” определите необходимое условие теоремы и достаточное

условие теоремы. Сформулируйте обратное утверждение, противоположное утверждение, обратное к противоположному и противоположное к обратному утверждения. Какие из этих утверждений справедливы?

7.6. Для признака “Если последние две цифры натурального числа делятся на 4, то число делится на 4” определите необходимое условие теоремы, достаточное условие теоремы. Сформулируйте обратное утверждение, противоположное утверждение, обратное к противоположному и противоположное к обратному утверждения. Какие из этих утверждений справедливы?

7.7. Для теоремы “Диагонали ромба взаимно перпендикулярны” определите необходимое условие теоремы, достаточное условие теоремы. Сформулируйте обратное утверждение, противоположное утверждение, обратное к противоположному и противоположное к обратному утверждения. Какие из этих утверждений справедливы?

§ 8. Определение булевых функций

а) Наборы переменных

Если в наборе переменные принимают фиксированные булевы значения 0 или 1, то их записывают подряд в скобках, не отделяя запятыми, т.к. этот набор можно рассматривать как число, записанное в двоичной системе счисления.

Если переменные набора являются произвольными, то при их обозначении переменные в скобках отделяют запятыми.

Наборы переменных $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ называются соседними, если они отличаются только одной координатой. Например, $(\alpha_1, \alpha_2, \dots, \alpha_n)$ и $(\bar{\alpha}_1, \alpha_2, \dots, \alpha_n)$ – соседние наборы.

Наборы переменных $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ называются противоположными, если они отличаются всеми координатами, т.е. $(\beta_1, \beta_2, \dots, \beta_n) = (\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)$.

Расстоянием Хэмминга между наборами $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ называется число $\rho(\alpha, \beta) = \sum_1^n |\alpha_i - \beta_i|$, т.е. число координат, в которых наборы отличаются.

Например, для наборов $\alpha = (10101010)$, $\beta = (11110001)$, $\rho(\alpha, \beta) = 5$.

Номером набора $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ называется число $N(\alpha) = \sum_{i=1}^n \alpha_i \cdot 2^{n-i}$.

Например, для $\alpha = (1101)$ получаем номер $N(\alpha) = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 4 + 1 = 13$, равный значению этого числа в десятичной системе координат. Кстати, записав номер набора в двоичной системе счисления $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1101_2$, получаем сам набор.

Таким образом, каждому двоичному набору сопоставляется десятичный номер и каждому десятичному числу, т.е. номеру, можно сопоставить его двоичное разложение, а значит, набор переменных при заданном числе булевых переменных.

б) *Способы задания булевой функции:*

1. *Словесный способ* задания функции, если функция определяется правилом ее составления. Например, в составе комиссии нечетное число экспертов. Решение комиссии считается принятым, если за него проголосовало большинство экспертов комиссии.

2. *Аналитический способ*, если функция задана формулой $y = f(x_1, x_2, \dots, x_n)$. Например, словесный способ задания функции

Таблица 4

x_1	x_2	f
0	0	0
0	1	1
1	0	1
1	1	0

для комиссии с тремя экспертами можно записать аналитически $f = x_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 x_2 x_3$.

3. *Табличный способ* состоит в том, что задаются значения функции в таблице на всех наборах переменных. Функция задается таблицей истинности (таблица 4).

Для двух переменных можно составить таблицу истинности (таблица 5) всех различных булевых функций.

Таблица 5

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

$$f_0 = 0, f_1 = X \wedge Y, f_2 = \bar{X} \rightarrow \bar{Y}, f_3 = X, f_4 = \bar{Y} \rightarrow X, f_5 = Y, \\ f_6 = X \oplus Y, f_7 = X \vee Y, f_8 = X \downarrow Y, f_9 = X \leftrightarrow Y, f_{10} = \bar{Y}, \\ f_{11} = Y \rightarrow X, f_{12} = \bar{X}, f_{13} = X \rightarrow Y, f_{14} = X | Y, f_{15} = 1.$$

Обращаем внимание на то, что для каждой функции можно составить бесконечное число равносильных алгебраических выражений, применяя законы алгебры логики. Но в действительности существует 16 различных булевых функций от двух переменных, т.е. законов, которые четырем упорядоченным наборам (00), (01), (10), (11) сопоставляют наборы значений.

Таблица 6

f	0	1	1	0	0	1	0	1
x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1

Если число переменных $n \geq 3$, то таблица истинности для одной функции в тексте занимает много места и значения функции записывают матрицей-строкой. Например, $f = (01100101)$ для функции от

трех переменных. В этом случае подразумевается, что все наборы переменных упорядочены в лексикографическом порядке и каждому из этих наборов соответствует определенное значение функции. Для некоторых задач полезно под значениями функции подписать эти наборы переменных (таблица 6).

Для записи значений функции от n переменных вместе со значениями наборов переменных в виде вертикальной (таблица 4) или горизонтальной (таблица 5) таблиц потребуется записать $n 2^n$ цифр.

Таблица 7

				0	0	...	1	x_{k+1}
				0	0	...	1	x_{k+2}
			
x_1	x_2	...	x_k	0	1	...	1	x_n
0	0	...	0	0	0	...	0	
0	0	...	1	0	0	...	0	
...	0	
1	1	...	1	0	0	...	1	

Для $n \geq 3$ значения функции с соответствующими наборами удобнее записывать в виде следующей таблицы.

Слева записываются в строки наборы для k переменных. Сверху записываются в столбцы наборы переменных для $n-k$ переменных.

На пересечении значений строк и столбцов записываются значения функции для наборов $(x_1, x_2, \dots, x_k, x_{n-k}, \dots, x_n)$.

В таблице 7 представлена функция $f(x_1, x_2, \dots, x_n) = x_1 \wedge x_2 \wedge \dots \wedge x_n$.

В таблице 8 задана функция $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_3 \oplus x_4$ для $k = 2$.

Таблица 8

			0	0	1	1	x_3
			0	1	0	1	x_4
x_1	x_2	0	0	1	1	0	
0	0	0	1	1	0		
0	1	1	0	0	0		
1	0	1	0	0	1		
1	1	0	1	1	0		

Изменяя число строк и число столбцов при фиксированном значении числа переменных n , можно получать различные таблицы. Для записи значений функции от n переменных вместе со значениями наборов переменных в виде таблицы 4 потребуется $k 2^k + (n-k) 2^{n-k} + 2^n$ цифр.

4. Для функции $f(x_1, x_2, \dots, x_n)$ от n переменных каждый фиксированный набор переменных $(\underbrace{- \dots -}_n)$ содержит n разрядов, т.е. $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_n)$. Учитывая, что каждый разряд может принимать значение 0 или 1, получаем всего 2^n наборов переменных, на которых нужно задать функцию. Например, для $n = 3$ получаем $2^3 = 8$ различных наборов переменных.

Таким образом, каждую функцию $f(x_1, x_2, \dots, x_n)$ от n переменных можно задать упорядоченным набором $(\underbrace{- \dots -}_{2^n})$ из 2^n разрядов, т.е.

$\alpha_f = (\alpha_0, \alpha_1, \dots, \alpha_{2^n-1})$. Каждый разряд принимает значение 0 или 1, поэтому всего существует 2^{2^n} функций.

Для $n = 3$ получаем $2^8 = 256$ функций. Задание функции строкой значений $f = (f_0 f_1 f_2 f_3 f_4 f_5 f_6 f_7)$ является перечислением значений функции на наборах переменных:

$$f(0,0,0) = f_0, f(0,0,1) = f_1, f(0,1,0) = f_2, f(0,1,1) = f_3, \\ f(1,0,0) = f_4, f(1,0,1) = f_5, f(1,1,0) = f_6, f(1,1,1) = f_7.$$

Задание функции строкой значений равносильно рассмотрению функции $f = \overline{f_0 x_1 x_2 x_3} \vee \overline{f_1 x_1 x_2 x_3} \vee \overline{f_2 x_1 x_2 x_3} \vee \overline{f_3 x_1 x_2 x_3} \vee \overline{f_4 x_1 x_2 x_3} \vee \overline{f_5 x_1 x_2 x_3} \vee \overline{f_6 x_1 x_2 x_3} \vee \overline{f_7 x_1 x_2 x_3}$.

5. *Графический способ* задания булевой функции используется при $n = 2$ (рис. 1). График булевой функции $z = f(x, y)$ используется только для вершин ломаной линии. Внутренние точки звеньев ломаной при $0 < x < 1$ или $0 < y < 1$ не используются в дискретной математике. Наглядное изображение булевой функции в виде ломаной позволяет привлечь геометрические характеристики (кривизну и кручение ломаной), которые способствуют выдвижению гипотезы об объединении нескольких кривых в класс кривых с некоторым свойством.

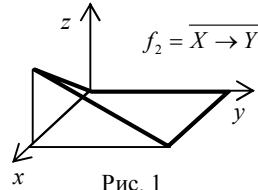


Рис. 1

Визуализация булевой функции от двух переменных может быть представлена на базисном квадрате с вершинами $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$. Вершина (x, y) изображается закрашенной точкой, если $f(x, y) = 1$. На рис. 2 представлена функция $f = x \oplus y$.

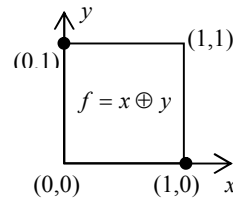


Рис. 2

Если на базисном квадрате изобразить две булевых функции $f_1(x, y)$ и $f_2(x, y)$, расположив закрашенные точки рядом, то на этом квадрате можно быстро определить сложную функцию $f_1 * f_2$. Звездочка означает некоторую данную логическую операцию. В этом случае нужно применить эту операцию поразрядно к значениям данных функций f_1 и f_2 , т.е. к вершинам квадрата. Симметрии базисного квадрата также позволяют выдвигать гипотезы об объединении нескольких функций в класс с некоторым свойством.

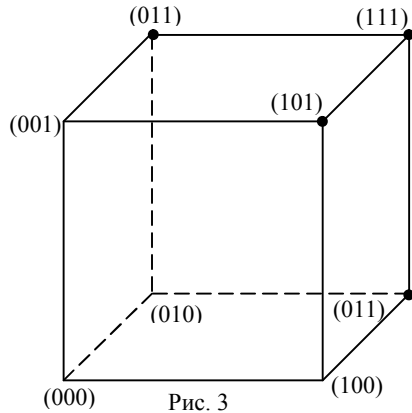


Рис. 3

Для функции от трех переменных аналогично значения булевой функции можно изображать точками на вершинах куба (рис. 3).

На рис. 3 изображена функция, когда решение комиссии из трех человек считается принятым, если за него проголосовало большинство экспертов комиссии, т.е. функция $f = x_1x_2x_3 \vee x_1x_2\bar{x}_3 \vee x_1\bar{x}_2x_3 \vee x_1x_2x_3$.

6. Булеву функцию от двух переменных можно изобразить орграфом. От элемента x к элементу y изображается стрелка или петля, если $f(x, y) = 1$. На рис. 4 изображена булева функция $f = x \rightarrow y$.

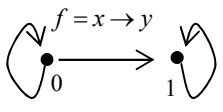


Рис. 4

в) *Композиция функций*

Пусть даны булевы функции $z = f(x, y)$, $x = \varphi(u, v)$, $y = \psi(t, w)$, тогда функция, полученная в результате подстановки, т.е. функция $f(\varphi(u, v), \psi(t, w)) = F(u, v, t, w)$, называется композицией (суперпозицией или сложной функцией).

Например, если $z = x \vee y$, $x = uv$, $y = t \rightarrow w$, то $F = uv \vee (t \rightarrow w)$.

Если $z = x \vee y$, $x = x \rightarrow y$, $y = x \oplus y$, то $F = (x \rightarrow y) \vee (x \oplus y)$.

Если $z = f(x, y)$, $x = x$, $y = x$, то $F = f(x, x)$. В этом случае иногда говорят, что применена операция переименования переменной, т.е. из первоначальной функции получена новая функция при $y = x$.

Рассмотрим составление композиции функций и ее упрощение.

Пусть функции от трех переменных заданы строкой значений:

$$f(x, y, z) = (1, 0, 0, 1, 0, 0, 1, 0), g(x, y, z) = (1, 1, 1, 1, 0, 0, 0, 0), h(x, y, z) = (0, 0, 1, 1, 0, 1, 0, 0).$$

Требуется составить композицию $f_k = f(g, z, h)$, полученную из функции

$$f_k(x, y, z) = f(g(x, y, z), z, h(x, y, z)).$$

Таблица 9

f_k	0	1	0	0	1	1	1	1
f	1	0	0	1	0	0	1	0
g	1	1	1	1	0	0	0	0
z	0	1	0	1	0	1	0	1
h	0	0	1	1	0	1	0	1
x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1

Составим таблицу истинности для данных функций и композиции функций (таблица 9).

Вначале заполняются три нижние строки для переменных x, y, z , затем заполняются строки для внутренних функций g, z, h и данной функции f .

Пример вычисления значений композиции функций

$$f_k(0, 0, 0) = f(g(0, 0, 0), 0, h(0, 0, 0)) = f(1, 0, 0) = 0.$$

Если от заданий функций строкой в выше приведенном примере перейти к аналитическому заданию этих функций, то получим следующие формулы и преобразования:

$$\begin{aligned}
 f(x, y, z) &= \overline{xy}z \vee \overline{xy}z \vee \overline{x}y\overline{z} \vee \overline{x}y\overline{z}, g(x, y, z) = \overline{x}, h(x, y, z) = \overline{xy} \vee xz, \\
 f_k(x, y, z) &= f(g(x, y, z), z, h(x, y, z)) = \overline{\overline{xz} \overline{xy} \vee xz \vee xz} (\overline{xy} \vee xz) \vee \overline{\overline{xz} \overline{xy} \vee xz} = \\
 &= \overline{xz} (\overline{xy} \overline{xz}) \vee (\overline{xz} \overline{xy} \vee xz \overline{xz}) \vee \overline{xz} (\overline{xy} \overline{xz}) = \\
 &= \overline{xz} (x \vee \overline{y}) (\overline{x} \vee \overline{z}) \vee 0 \vee xz \vee \overline{xz} (x \vee \overline{y}) (\overline{x} \vee \overline{z}) =
 \end{aligned}$$

$$= \overline{\overline{x}} \overline{yz} \vee xz \vee xz \vee \overline{xz} \vee \overline{xy} \overline{z} = \overline{\overline{x}} \overline{yz} \vee x = x \vee \overline{yz}.$$

Любая логическая функция $f(x_1, \dots, x_n)$ может быть представлена в следующем виде:

$$f(x_1, x_2, \dots, x_n) = \overline{x_1} f(0, x_2, \dots, x_n) \vee x_1 f(1, x_2, \dots, x_n),$$

$$f(x_1, \dots, x_n) = \overline{x_1} \overline{x_2} f(0, 0, x_3, \dots, x_n) \vee \overline{x_1} x_2 f(0, 1, x_3, \dots, x_n) \vee$$

$$\vee x_1 \overline{x_2} f(1, 0, x_3, \dots, x_n) \vee x_1 x_2 f(1, 1, x_3, \dots, x_n),$$

$$f(x_1, x_2, x_3) = \overline{x_1} \overline{x_2} \overline{x_3} f(0, 0, 0) \vee \overline{x_1} \overline{x_2} x_3 f(0, 0, 1) \vee \overline{x_1} x_2 \overline{x_3} f(0, 1, 0) \vee \overline{x_1} x_2 x_3 f(0, 1, 1) \vee$$

$$\vee x_1 \overline{x_2} \overline{x_3} f(1, 0, 0) \vee x_1 \overline{x_2} x_3 f(1, 0, 1) \vee x_1 x_2 \overline{x_3} f(1, 1, 0) \vee x_1 x_2 x_3 f(1, 1, 1).$$

Равенства доказываются подстановкой в обе части всех наборов переменных.

г) Фиктивная переменная

Переменная x_i в функции $f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n)$ называется фиктивной (несущественной), если $f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) = f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$. В этом случае функция $f(x_1, \dots, x_n)$ фактически зависит от $n-1$ переменных и может быть представлена функцией $g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$.

Ввести фиктивную переменную в данную функцию $f(x, y)$ можно использованием очевидных равенств $f(x, y) \vee 0 = f(x, y)$ и $f(x, y) \wedge 1 = f(x, y)$, в которых нужно представить 0 и 1 в виде булевых функций от новой переменной.

В качестве таких функций можно, например, выбрать:

$$0 = z\overline{z}, 0 = z \oplus z, 0 = z \rightarrow z, 0 = (z \oplus z)(z \leftrightarrow z), 0 = (z \rightarrow z)(z \vee \overline{z}),$$

$$0 = z(z \rightarrow \overline{z}), 0 = xz(\overline{x} \vee \overline{z}), 0 = (x \vee z)\overline{x}\overline{z},$$

$$1 = z \vee \overline{z}, 1 = z \leftrightarrow z, 1 = z \rightarrow z, 1 = (x \oplus z) \vee (x \leftrightarrow z), 1 = (x \rightarrow z) \vee (x \vee \overline{z}),$$

$$1 = (xz) \vee (x \rightarrow \overline{z}), 1 = (xz) \vee (\overline{x} \vee \overline{z}), 1 = (x \vee z) \vee (\overline{x}\overline{z}).$$

Пример 1. Пусть $\varphi(x, y)$ – произвольная булева функция, а операция $*$ является булевой операцией \vee или \oplus . Доказать, что для функции $f(x, y) = \varphi(x, y) * \overline{\varphi(x, y)}$ переменная x является фиктивной переменной.

Решение. Подстановкой $x = 0$ и $x = 1$ проверяем равенство $\varphi(x, y) = \overline{x}\varphi(0, y) * x\varphi(1, y)$. Заменяя x на \overline{x} , получаем равенство $\overline{\varphi(x, y)} = x\varphi(0, y) * \overline{x}\varphi(1, y)$.

$$\varphi(x, y) * \overline{\varphi(x, y)} = \left((\overline{x} * x)\varphi(0, y) \right) * \left((x * \overline{x})\varphi(1, y) \right) = \varphi(0, y) * \varphi(1, y).$$

Функция $\varphi(0, y) * \varphi(1, y)$ не зависит от переменной x , следовательно, переменная x является фиктивной для функции $\overline{x}\varphi(0, y) * x\varphi(1, y)$. \square

Пример 2. Для произвольной коммутативной логической операции $*$, удовлетворяющей условию $f(x) * g(x) = g(x) * f(x)$, докажите равенство

$$f(x, y)g(\overline{x}, y) * f(\overline{x}, y)g(x, y) = f(1, y)g(0, y) * f(0, y)g(1, y). \quad (1)$$

Решение.

$$f(x, y)g(\bar{x}, y) * f(\bar{x}, y)g(x, y) \Big|_{x=1} = f(1, y)g(\bar{1}, y) * f(\bar{1}, y)g(1, y) = \\ = f(1, y)g(0, y) * f(0, y)g(1, y),$$

$$f(x, y)g(\bar{x}, y) * f(\bar{x}, y)g(x, y) \Big|_{x=0} = f(0, y)g(\bar{0}, y) * f(\bar{0}, y)g(0, y) = \\ = f(0, y)g(1, y) * f(1, y)g(0, y) = f(1, y)g(0, y) * f(0, y)g(1, y).$$

Задачи.

8.1. Среди наборов переменных найдите соседние наборы и противоположные наборы

$$\alpha = (1010), \beta = (0110), \gamma = (0100), \delta = (1001), \lambda = (0101).$$

8.2. Наборы α и β – соседние, наборы β и γ – соседние, наборы α и γ – противоположные. Сколько переменных содержит набор α ?

8.3. Найдите номер набора (0101). Выпишите все наборы для четырех переменных для стандартного расположения переменных и убедитесь, что набор (0101) находится на соответствующем месте (нумерация наборов начинается с 0).

8.4. Изобразите набор $\alpha = (111)$ вершиной куба.

а) Найдите все наборы, удаленные от набора α на расстоянии, равном 1. Почему такие наборы можно назвать соседними к набору α ? Изобразите эти наборы вершинами графа.

б) Найдите все наборы, удаленные от набора α на расстоянии, равном 2. Изобразите эти наборы вершинами графа.

в) Найдите все наборы, удаленные от набора α на расстоянии, равном 3. Почему такие наборы можно назвать противоположными к набору α ? Изобразите эти наборы вершинами графа. Изобразите несколько ломаных линий на поверхности, соединяющих противоположные вершины куба. Найдите среди них кратчайшие ломаные линии.

8.5. Набор $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ связан бинарным отношением с набором $\beta = (\beta_1, \beta_2, \dots, \beta_n)$, если эти наборы являются соседними. Какими свойствами обладает это бинарное отношение?

8.6. Набор $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ связан бинарным отношением с набором $\beta = (\beta_1, \beta_2, \dots, \beta_n)$, если эти наборы являются противоположными. Какими свойствами обладает это бинарное отношение?

8.7. Проверьте, что следующие функции содержат фиктивную переменную, и выразите эти функции только через существенные переменные:

$$\text{а) } (x \vee y) \oplus (\bar{x} \vee y); \quad \text{б) } (xy) \oplus (\bar{xy}); \quad \text{в) } (x \oplus y) \oplus (\bar{x} \oplus y);$$

- г) $(x \rightarrow y) \oplus (\bar{x} \rightarrow y)$; д) $(x \leftrightarrow y) \oplus (\bar{x} \leftrightarrow y)$;
 е) $(x \downarrow y) \oplus (\bar{x} \downarrow y)$; ж) $(x|y) \oplus (\bar{x}|y)$; з) $\overline{(x \rightarrow y)} \oplus \overline{x \rightarrow y}$.

8.8. Проверьте, что следующие функции содержат фиктивную переменную, и выразите эти функции только через существенные переменные:

- а) $(x \vee y) \vee (\bar{x} \vee y)$; б) $(xy) \vee (\bar{x}y)$; в) $(x \oplus y) \vee (\bar{x} \oplus y)$;
 г) $(x \rightarrow y) \vee (\bar{x} \rightarrow y)$; д) $(x \leftrightarrow y) \vee (\bar{x} \leftrightarrow y)$;
 е) $(x \downarrow y) \vee (\bar{x} \downarrow y)$; ж) $(x|y) \vee (\bar{x}|y)$; з) $\overline{(x \rightarrow y)} \vee \overline{x \rightarrow y}$.

8.9. Содержит ли фиктивную переменную функция $(x \rightarrow y) \rightarrow (\bar{x} \rightarrow y)$?

8.10. Дана функция $f(x, y) = (x \rightarrow y) \oplus (x \leftrightarrow y)$. Запишите пять выражений этой функции введением фиктивной переменной z , т.е. как функции от переменных x, y, z .

8.11. Докажите тождество $f(0, y) \oplus f(1, y) \oplus f(x, y) = f(\bar{x}, y)$.

8.12. Найдите вектор значений для каждой из следующих функций:

- а) $f_1(x, y) = x \oplus y$; е) $f_6(x, y, z) = y \rightarrow x$;
 б) $f_2(x, y, z) = x \oplus y$; ж) $f_7(x, y, z) = \overline{((y \rightarrow x) \vee z)} \vee y$;
 в) $f_3(x, y, z) = y \oplus z$; з) $f_8(x, y, z) = (x \oplus y) \wedge (y \rightarrow z)$;
 г) $f_4(x, y, z) = x \oplus z$; и) $f_9(x, y, z) = (x \vee \bar{y}) \oplus (y \rightarrow \bar{z})$.
 д) $f_5(x, y, z) = x \rightarrow y$;

8.13. Найдите аналитическое задание следующих функций от трех переменных (таблица 10).

Таблица 10

x_1	x_2	x_3	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	0	1	0	0	0	0	1
0	0	1	0	0	0	1	0	1	1
0	1	0	0	1	0	1	1	1	1
0	1	1	0	0	0	1	1	0	1
1	0	0	0	1	0	1	0	0	0
1	0	1	0	0	0	1	0	1	0
1	1	0	0	1	1	1	1	1	1
1	1	1	1	0	1	1	1	0	1

8.14. Найдите аналитическое задание следующих функций от трех переменных:

$$f_1=(11001100), f_2=(11111110), f_3=(11110101), f_4=(11000011);$$

$$f_5=(10101001), f_6=(11111111), f_7=(00000000), f_8=(01101001).$$

8.15. Проверьте, что операция сложения по модулю два (сумма Жегалкина) обладает следующими свойствами:

а) $x \oplus y = \overline{xy} \vee x\overline{y}$; б) $x \oplus y = y \oplus x$;

в) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;

г) $x \oplus y = \overline{x} \leftrightarrow \overline{y} = \overline{\overline{x}} \leftrightarrow y = x \leftrightarrow \overline{\overline{y}}$;

д) $(x \oplus y)z = xz \oplus yz$;

е) $(x_1 \oplus x_2 \oplus \dots \oplus x_n)y = x_1y \oplus x_2y \oplus \dots \oplus x_ny$;

ж) $x \oplus x = 0$; з) $x \oplus 0 = x$; и) $x \oplus 1 = \overline{x}$; к) $x \oplus \overline{x} = 1$;

л) $x_1 \oplus x_2 \oplus \dots \oplus x_n =$

$$= \begin{cases} 0, & \text{если среди } x_1, x_2, \dots, x_n \text{ четное число единиц,} \\ 1, & \text{если среди } x_1, x_2, \dots, x_n \text{ нечетное число единиц.} \end{cases}$$

(функция $f(x_1, x_2, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ называется функцией четности);

м) если $z = x \oplus y$, то $x = z \oplus y$;

н) если $x \oplus z = y \oplus z$, то $x = y$;

о) $x \oplus y = \overline{xy} \vee x\overline{y}$;

п) $x \oplus y = x \vee y$, тогда и только тогда, когда $xy = 0$;

р) $xy \oplus xz \oplus yz = xy \vee xz \vee yz$;

с) $\overline{x_1 \oplus x_2} = \overline{x_1} \oplus \overline{x_2} = \overline{x_1} \oplus \overline{x_2} = \overline{\overline{x_1} \vee \overline{x_2}} = \overline{\overline{x_1} \vee \overline{x_2}} = (\overline{x_1} \vee \overline{x_2})(x_1 \vee x_2)$;

т) $(x_1 \oplus x_2)(x_1 \oplus x_3) = x_1 \overline{x_2} \overline{x_3} \vee x_1 x_2 x_3$.

8.16. Докажите, что булевы функции следующим образом выражаются через сумму Жегалкина и константу 1:

а) $\overline{x} = x \oplus 1$; б) $x \vee y = (x \oplus 1)(y \oplus 1) = xy + x + y$;

в) $x \rightarrow y = xy \oplus x \oplus 1$; г) $\overline{x \rightarrow y} = xy + x$;

д) $x \leftrightarrow y = x \oplus y \oplus 1$; е) $\overline{x \leftrightarrow y} = x \oplus y$;

ж) $(x \leftrightarrow y) \leftrightarrow z = x \oplus y \oplus z$; з) $x \downarrow y = xy \oplus x \oplus y \oplus 1$;

и) $x \uparrow y = xy \oplus 1$; к) $\overline{xy} \vee x\overline{y} = x \oplus y$; л) $\overline{x \vee y} \vee xy = x \oplus y \oplus 1$.

8.17. Докажите, что операция штрих Шеффера ($x|y = \overline{xy}$) обладает следующими свойствами:

- а) $x|0 = 1$; б) $x|1 = x|x = \bar{x}$; в) $x|\bar{x} = 1$; г) $x|y = y|x$;
 д) $\overline{x|y} = \bar{x} \downarrow \bar{y}$; е) $\overline{x|y} = \overline{\bar{x} \vee \bar{y}}$; ж) $x|(x \vee y) = \bar{x}$;
 з) $x \vee (x|y) = y \vee (x|y)$; и) $x \rightarrow y = x|(y|y)$;
 к) $x \vee y = (x|x)|(y|y)$; л) $xy = \overline{(x|x)|(y|y)}$.

8.18. Докажите, что булевы функции следующим образом выражаются через штрих Шеффера $|$:

- а) $\bar{x} = x|x$; б) $xy = (x|y)|(x|y)$; в) $x \vee y = (x|x)|(y|y)$;
 г) $x \rightarrow y = x|(y|y)$; д) $\overline{x \rightarrow y} = (x|(y|y)|(x|(y|y))$;
 е) $x \downarrow y = ((x|x)|(y|y))|((x|x)|(y|y))$;
 ж) $x \oplus y = (x|(y|y))|(y|(x|x))$; з) $f(x) \equiv 1 = (x|x)|x = x|(x|x)$;
 и) $f(x, y) \equiv 0 = ((x|x)|x)|((y|y)|y)$;
 к) $f(x, y) \equiv 1 = ((x|(x|x))|(y|(y|y))|((x|(x|x))|(y|(y|y))))$;
 л) $x \leftrightarrow y = ((x|(y|y))|(y|(x|x))|((x|(y|y))|(y|(x|x))))$;
 м) $f(x, y) = x = (x|(y|(y|y))|((x|(y|(y|y))))$.

8.19. Докажите, что операция стрелка Пирса ($x \downarrow y = \overline{x \vee y}$) обладает следующими свойствами:

- а) $x \downarrow 0 = \bar{x}$; б) $x \downarrow 1 = 0$; в) $x \downarrow x = \bar{x}$; г) $x \downarrow \bar{x} = 0$;
 д) $(x \downarrow x) \downarrow x = 0$; е) $x \downarrow y = y \downarrow x$; ж) $\overline{x \downarrow y} = \bar{x} \overline{y}$;
 з) $\overline{x \downarrow y} = x \vee y = \overline{\bar{x} \bar{y}}$; и) $x \downarrow xy = \bar{x}$.

8.20. Докажите, что булевы функции следующим образом выражаются через стрелку Пирса \downarrow :

- а) $\bar{x} = x \downarrow x$; б) $xy = (x \downarrow x) \downarrow (y \downarrow y)$;
 в) $x|y = ((x \downarrow x) \downarrow (y \downarrow y)) \downarrow ((\bar{x} \downarrow y) \downarrow (x \downarrow \bar{y}))$;
 г) $x \vee y = (x \downarrow y) \downarrow (x \downarrow y)$;

$$\text{д) } x \rightarrow y = ((x \downarrow x) \downarrow y) \downarrow ((x \downarrow x) \downarrow y);$$

$$\text{е) } x \leftrightarrow y = ((x \downarrow x) \downarrow y) \downarrow ((x \downarrow (y \downarrow y)));$$

$$\text{ж) } f(x) \equiv 0 = x \downarrow (x \downarrow x);$$

$$\text{з) } f(x) \equiv 1 = (x \downarrow (x \downarrow x)) \downarrow (x \downarrow (x \downarrow x));$$

$$\text{и) } f(x, y) \equiv 0 = y \downarrow ((x \downarrow (x \downarrow x)) \downarrow (x \downarrow (x \downarrow x)));$$

$$\text{к) } f(x, y) \equiv 1 = (x \downarrow (x \downarrow x)) \downarrow (y \downarrow (y \downarrow y));$$

$$\text{л) } f(x, y) = \bar{x} = x \downarrow ((x \downarrow x) \downarrow (y \downarrow y));$$

$$\text{м) } x \oplus y = [((x \downarrow x) \downarrow y) \downarrow ((x \downarrow (y \downarrow y)))] \downarrow [((x \downarrow x) \downarrow y) \downarrow ((x \downarrow (y \downarrow y)))] .$$

8.21. Докажите равенство

$$(((A \wedge B) \rightarrow C) \rightarrow (A \rightarrow (B \rightarrow C))) = ((\bar{A} \rightarrow (A \rightarrow B)) \vee C).$$

8.22. Даны две булевы функции $f(x, y)$ и $g(x, y)$. Составьте и упростите композиции:

$$F_1(x, y) = f(g(x, y), y), \quad F_2(x, y) = f(x, g(x, y)),$$

$$F_3(x, y) = f(g(x, y), g(x, y)), \quad F_4(x, y) = g(f(x, y), y),$$

$$F_5(x, y) = g(x, f(x, y)), \quad F_6(x, y) = g(f(x, y), f(x, y)), \text{ если:}$$

$$\text{а) } f(x, y) = x \rightarrow y, \quad g(x, y) = x;$$

$$\text{б) } f(x, y) = x \oplus y, \quad g(x, y) = 1;$$

$$\text{в) } f(x, y) = x \vee y, \quad g(x, y) = \overline{xy}.$$

8.23. Приведите примеры функций от двух переменных, для которых выполняются равенства:

$$\text{а) } f(x, y) = f(f(x, y), y); \quad \text{б) } f(x, y) = f(x, f(x, y));$$

$$\text{в) } f(x, y) = f(f(x, y), f(x, y)).$$

8.24. Применяя равносильные преобразования, докажите тождественную истинность формулы

$$((x \rightarrow z)(y \rightarrow z)) \rightarrow ((x \vee y) \rightarrow z).$$

8.25. Докажите следующие теоремы о разложении булевой функции:

$$\text{а) } f(x_1, x_2, \dots, x_n) = x_1 f(1, x_2, \dots, x_n) \vee \bar{x}_1 f(0, x_2, \dots, x_n).$$

Указание. Проверьте это равенство при $x_1 = 0$ и при $x_1 = 1$;

$$\text{б) } f(x_1, x_2, \dots, x_n) = x_1 f(1, x_2, \dots, x_n) \oplus \bar{x}_1 f(0, x_2, \dots, x_n),$$

Указание. Используйте свойство: если $xy = 0$, то $x \oplus y = x \vee y$.

8.26. а) Запишите равенство (1) из примера 2 для некоторых конкретных коммутативных операций *.

б) Запишите равенство (1) для булевой функции $g(x, y) = 1$.

Таблица 11

x	y	z	f
1	1	1	1
1	1	0	1
1	0	1	1

8.27. Дан фрагмент таблицы истинности функции f (таблица 11).

Выберите функцию для этого фрагмента:

а) $x \vee \bar{y} \vee z$; б) $x \wedge y \wedge z$; в) $x \wedge y \wedge \bar{z}$; г) $\bar{x} \vee y \vee \bar{z}$.

8.28. Изобразите орграфами все булевы функции f_0, f_1, \dots, f_{15} от двух переменных.

§ 9. СДНФ и СКНФ

Элементарной конъюнкцией (элементарным произведением) называется конъюнкция, состоящая только из переменных или их отрицаний, а также одна переменная или отрицание одной переменной. В каждой элементарной конъюнкции ни одна переменная не содержится одновременно со своим отрицанием. Например: $x, y, x\bar{y}z$.

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

Из переменных x_1, x_2, \dots, x_n можно составить элементарное произведение $K = x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}$, где σ_i принимает значение 0 или 1, $i = 1, 2, \dots, n$. Такое произведение будем называть просто конъюнкцией. Число n называется *рангом* конъюнкции. Если $n = 0$, то конъюнкция называется пустой и полагается равной 1.

Дизъюнктивной нормальной формой (ДНФ) называется дизъюнкция элементарных конъюнкций. Например: $x\bar{y}z \vee xy \vee z \vee zxy$.

Пусть ДНФ функции представлена в виде $D = K_1 \vee K_2 \vee \dots \vee K_m$ через элементарные конъюнкции K_i , тогда число $r = r(K_1) + r(K_2) + \dots + r(K_m)$ называется *рангом* ДНФ. Ранг ДНФ равен количеству символов переменных в ДНФ.

Дизъюнктивная нормальная форма функции $f(x_1, x_2, \dots, x_n)$ называется *совершенной* (СДНФ), если:

- все элементарные конъюнкции попарно различны,
- каждая элементарная конъюнкция содержит все переменные, причем на k месте стоит переменная x_k или ее отрицание \bar{x}_k , где $1 \leq k \leq n$.

Пример СДНФ: $x_1 x_2 x_3 x_4 \vee x_1 \bar{x}_2 x_3 x_4 \vee x_1 x_2 \bar{x}_3 x_4, xyz \vee x\bar{y}z \vee \bar{x}yz$. □

Носителем булевой функции $f(x_1, x_2, \dots, x_n)$ называется совокупность всех булевых векторов $(\alpha_1, \alpha_2, \dots, \alpha_n) \in E^n$, для которых $f(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$. Носитель функции обозначается N_f .

Таблица 12

f	0	1	1	0	0	1	0	1
x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1

Для функции в таблице 12 носителем функции является множество, состоящее из четырех векторов:

$$N_f = \{(001), (010), (101), (111)\}.$$

Рассмотрим булеву функцию от n переменных, которая задана единственным набором переменных, на котором она принимает значение 1.

Составим конъюнкцию от всех переменных следующим образом: переменные равные нулю в данном наборе возьмем с инверсией, а переменные равные 1 без знака инверсии.

Например: на единственном наборе $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1$ функция принимает значение 1, а на остальных наборах значение функции равно 0. Тогда $f = \overline{x_1} \wedge \overline{x_2} \wedge x_3 \wedge x_4$.

Таблица 13

x_1	x_2	x_3	f
0	1	1	1
1	0	1	1
1	0	0	1
1	1	1	1
все остальные наборы			0

Произвольная булева функция, заданная перечислением всех наборов переменных, при которых она принимает значение, определяется следующим образом: для каждого из этих наборов составляется конъюнкция, а затем образуется дизъюнкция всех этих конъюнкций.

Пример 1. Для функции, заданной таблицей 13, получаем $f = \overline{x_1}x_2x_3 \vee x_1\overline{x_2}x_3 \vee x_1x_2\overline{x_3} \vee x_1x_2x_3$ – совершенная дизъюнктивная нормальная форма, построенная на данных наборах аргументов. \square

Теорема 1. Любая n -местная булева функция, не равная тождественно 0, может быть представлена формулой в СДНФ. Формула определяется однозначно с точностью до перестановки дизъюнктивных членов.

Дизъюнктивная нормальная форма называется *минимальной*, если она содержит наименьшее общее число вхождений переменных среди всех ей равносильных ДНФ. Минимальную ДНФ можно найти, перебрав конечное число равносильных ей ДНФ и выбрав ту, которая содержит минимальное число вхождений переменных.

Элементарной дизъюнкцией (элементарной суммой) называется дизъюнкция, состоящая только из переменных или их отрицаний, а также одна переменная или отрицание одной переменной. Например: $x \vee \overline{y} \vee z, x \vee \overline{y}, x, \overline{z}$.

Конъюнктивной нормальной формой (КНФ) называется конъюнкция элементарных дизъюнкций. Например: $(x \vee \overline{y} \vee z)(x \vee \overline{y})(x \vee \overline{y} \vee z)$.

Конъюнктивная нормальная форма (КНФ) называется *совершенной* (СКНФ), если:

- все элементарные дизъюнкции попарно различны,
- каждая элементарная дизъюнкция содержит все переменные, причем на k месте стоит переменная x_k или ее отрицание \bar{x}_k , где $1 \leq k \leq n$.

Пример СКНФ: $(x \vee y \vee z)(x \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z})$.

Рассмотрим булеву функцию от n переменных, которая задана единственным набором переменных, на котором она принимает значение 0.

Составим дизъюнкцию от всех переменных следующим образом: переменные равные нулю в данном наборе возьмем без знака инверсии, а переменные, равные 1, – со знаком инверсии.

Например, если на единственном наборе $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1$ функция принимает значение 0, а на остальных наборах значение функции равно 1. Тогда $f = x_1 \vee x_2 \vee \bar{x}_3 \vee \bar{x}_4$.

Таблица 14

x_1	x_2	x_3	f
0	1	0	0
1	1	0	0
0	0	0	0
все остальные наборы			1

Произвольная булева функция, заданная перечислением всех наборов переменных, при которых она принимает значение 0, определяется следующим образом: для каждого из этих наборов составляется дизъюнкция, а затем образуется конъюнкция всех этих дизъюнкций.

Пример 2. Для функции, заданной таблицей 14, получаем $f = (x_1 \vee x_2 \vee x_3)(x_1 \vee x_2 \vee x_3)(x_1 \vee x_2 \vee x_3)$ – совершенная конъюнктивная нормальная форма, построенная на данных наборах переменных. \square

Теорема 2. Любая n -местная булева функция, не равная тождественно 1, может быть представлена формулой в СКНФ. Формула определяется однозначно с точностью до перестановки конъюнктивных членов.

Пример 3. Найти СДНФ формулы $f(x, y, z) = \overline{xy} \rightarrow \overline{x \vee z}$:

Таблица 15

x	y	z	\overline{xy}	$\overline{x \vee z}$	f
0	0	0	1	1	1
0	0	1	1	0	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	1	0	0
1	0	1	1	0	0
1	1	0	0	0	1
1	1	1	0	0	1

- а) составив таблицу истинности;
- б) применяя законы логики.

Решение.

а) из таблицы 15 получаем

$$f(x, y, z) = \overline{x} \overline{y} \overline{z} \vee \overline{x} \overline{y} z \vee \overline{x} y \overline{z} \vee \overline{x} y z;$$

$$\text{б) } \overline{xy} \rightarrow \overline{x \vee z} = xy \vee \overline{xz} =$$

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

$$= xyz \vee xy\bar{z} \vee \overline{xy}z \vee \overline{xy}\bar{z}. \square$$

Пример 4. Найти СКНФ формулы $f(x, y, z) = \overline{x}y \rightarrow (\overline{z} \leftrightarrow y)$:

а) составив таблицу истинности; б) применяя законы логики.

Таблица 16

x	y	z	$x \vee \overline{y}$	$\overline{x \vee \overline{y}}$	$\overline{z} \leftrightarrow y$	f
0	0	0	1	0	0	1
0	0	1	1	0	1	1
0	1	0	0	1	1	1
0	1	1	0	1	0	0
1	0	0	1	0	0	1
1	0	1	1	0	1	1
1	1	0	1	0	1	1
1	1	1	1	0	0	1

Решение.

а) из таблицы 16 получаем

$$f(x, y, z) = x \vee \overline{y} \vee \overline{z};$$

б) $f(x, y, z) =$

$$= (x \vee \overline{y}) \vee (\overline{z} \leftrightarrow y) =$$

$$= x \vee \overline{y} \vee (\overline{z} \vee zy) =$$

$$= x \vee (\overline{y} \vee zy) \vee \overline{z} =$$

$$= x \vee \overline{y} \vee yz = x \vee (\overline{y} \vee yz) =$$

$$= x \vee \overline{y} \vee \overline{z}.$$

Пример 5. Функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(f_0, f_1, 0, 0, f_2, f_3, 0, 0)$, найти формулу.

Решение. Функция от двух переменных равна

$$f(x, y) = f_0 \overline{x} \overline{y} \vee f_1 x \overline{y} \vee f_2 x y \vee f_3 x y.$$

Функция от трех переменных равна

$$f(x, y, z) = f_0 \overline{x} \overline{y} \overline{z} \vee f_1 \overline{x} \overline{y} z \vee f_2 x \overline{y} \overline{z} \vee f_3 x \overline{y} z = \overline{y} (f_0 \overline{x} \overline{z} \vee f_1 \overline{x} z \vee f_2 x \overline{z} \vee f_3 x z).$$

$$f(x, y, z) = \overline{y} f(x, z).$$

Если для функции $f(x_1, x_2, \dots, x_n)$ число переменных больше или равно 4, то вместо задания вектора значений на каждом наборе переменных используют перечисление номеров носителей функции.

Пример 6. Для функции $f(x_1, x_2, x_3, x_4) = (1010000000000001)$ используют запись $f(x_1, x_2, x_3, x_4) = (0, 2, 15)$.

Для заданной функции $f(x_1, x_2, \dots, x_5) = (5, 17, 33)$ нахождение СДНФ можно выполнить следующим образом:

$$5_{10} = 4 + 1 = (00101)_2, \quad 19_{10} = 16 + 2 + 1 = (10011)_2,$$

$$33_{10} = 16 + 8 + 4 + 2 + 1 = (11111)_2,$$

$$f(x_1, x_2, \dots, x_5) = \overline{x_1} \overline{x_2} \overline{x_3} \overline{x_4} x_5 \vee x_1 \overline{x_2} \overline{x_3} \overline{x_4} x_5 \vee x_1 x_2 \overline{x_3} x_4 x_5. \quad \square$$

Задачи.

9.1. Используя одну переменную, можно составить три различных конъюнкции: $1, x, \overline{x}$. Используя n переменных, можно составить 3^n различных конъюнкций. Найдите все различные конъюнкции для:

а) $n = 2$, б) $n = 3$.

9.2. (устно). Перечислите наборы переменных, для которых функция принимает значение 0:

- а) $x \rightarrow y$; б) $x \vee y \vee z$; в) $x y z$; г) $(x \vee y) z$; д) $(x y) \vee z$;
 е) $(x \rightarrow y) \rightarrow z$; ж) $x \rightarrow (y \rightarrow z)$; з) $(x \leftrightarrow y) \leftrightarrow z$; и) $x \leftrightarrow (y \leftrightarrow z)$.

9.3. (устно). Перечислите наборы переменных, для которых функция принимает значение 1:

- а) $x \rightarrow y$; б) $x \vee y \vee z$; в) $x y z$; г) $(x \vee y) z$; д) $(x y) \vee z$;
 е) $(x \rightarrow y) \rightarrow z$; ж) $x \rightarrow (y \rightarrow z)$; з) $(x \leftrightarrow y) \leftrightarrow z$; и) $x \leftrightarrow (y \leftrightarrow z)$.

9.4. Для следующих булевых функций найдите носители:

- а) $f = (10101010)$; б) $f = (0000000011111111)$;
 в) $f = 1 \oplus x \oplus y \oplus z$; г) $f(x, y, z) = x \vee \bar{x}$.

9.5. Даны две булевы функции $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$.

Докажите следующие равенства для носителей функций:

- а) $N_{f \wedge g} = N_f \cap N_g$; б) $N_{f \vee g} = N_f \cup N_g$; в) $N_{\bar{f}} = \overline{N_f} = E^n \setminus N_f$;
 г) для функций f и g , заданных в таблице 17, найдите $N_{f \wedge g}, N_{f \vee g}, N_{\bar{f}}, N_{\bar{g}}$.

Таблица 17

f	1	0	0	1	0	1	0	0
g	0	1	1	0	0	1	0	1
x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1

9.6. Привести следующие формулы к СДНФ:

- а) $(Z \rightarrow X) \wedge (Y \rightarrow X)$; б) $(Z \wedge Y) \rightarrow (Y \rightarrow X)$.

9.7. Докажите, что вектор значений $(\varphi_1, \varphi_1, \varphi_2, \varphi_2, \varphi_3, \varphi_3, \varphi_4, \varphi_4)$ функции от трех переменных можно представить как вектор значений функции двух переменных, т.е. первоначальное задание функции содержит фиктивную переменную.

9.8. Докажите, что вектор значений $(\varphi_1, \varphi_2, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_3, \varphi_4)$ функции от трех переменных можно представить как вектор значений функции двух переменных, т.е. первоначальное задание функции содержит фиктивную переменную.

9.9. Докажите, что вектор значений $(\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_1, \varphi_2, \varphi_3, \varphi_4)$ функции от трех переменных можно представить как вектор значений функции двух переменных, т.е. первоначальное задание функции содержит фиктивную переменную.

9.10. Какие фиктивные переменные содержат функции:

$$f_1 = (11001111), f_2 = (00111100), f_3 = (10100101), f_4 = (11011101).$$

9.11. Найдите СДНФ булевой функции от трех переменных, носителями которой являются все вершины грани куба, заданной условием $x_2 = 0$.

9.12. Булева функция принимает значения 1 только в носителе (1010) и в противоположной вершине четырехмерного куба. Найдите СДНФ этой функции.

9.13. С помощью эквивалентных преобразований приведите формулу к СДНФ. По полученной СДНФ запишите вектор значений функции

а) $(x \vee y) \rightarrow (\bar{z} \leftrightarrow y)$; б) $(\overline{x \leftrightarrow y \rightarrow z})y$.

9.14. Докажите следующие правила поглощения для трехчленной дизъюнктивной нормальной формы, каждый член которой содержит по две переменных:

а) $xz \vee xy \vee \bar{y}z = xy \vee \bar{y}z$

(если в трехчлен входит только одна переменная как сама, так и ее отрицание, то исчезает тот член, который не содержит эту переменную);

б) $\bar{x}y \vee \bar{x}\bar{z} \vee yz = \bar{x}\bar{z} \vee yz$; в) $\bar{x}y \vee \bar{x}\bar{z} \vee yz = \bar{x}y \vee \bar{y}z$;

г) $xy \vee xz \vee \bar{y}\bar{z} = x \vee \bar{y}\bar{z}$; д) $\bar{x}y \vee \bar{y}z \vee \bar{x}\bar{z} = \bar{x} \vee \bar{y}z$

(если в трехчлен входит только две переменных как сами, так и их отрицания, то в формуле соединяем дизъюнкцией третью переменную с тем слагаемым, который не содержит эту переменную);

е) $x\bar{y} \vee xz \vee y\bar{z} = x \vee y\bar{z}$.

9.15. Булева функция от $2k+1$ переменных равна 1, если m переменных, где $m \geq k+1$, принимают значения 1 и равна 0 – в противном случае. Эта функция называется *мажоритарной*, а множество всех мажоритарных функций обозначается $\{Maj_{2k+1}\}$.

а) Докажите, что число носителей мажоритарной функции от $2k+1$ переменных (т.е. число наборов, на которых функция равна 1) равно 2^{2k} .

б) Докажите, что вектор значений мажоритарной функции от трех переменных равен $(f_0, f_1, f_2, 1, f_4, 1, 1, 1)$. Сколько существует мажоритарных функций от трех переменных?

в) Проверьте, что функция голосования для жюри из трех человек (см. п. 8) является мажоритарной функцией.

9.16. Дана функция двух переменных $f(x, y) = (f_0, f_1, f_2, f_3)$. Изучите закономерность образования некоторых простейших функций от трех переменных, полученных из данной функции (таблица 18).

Таблица 18

0	0	0	0	1	1	1	1	x
0	0	1	1	0	0	1	1	y
0	1	0	1	0	1	0	1	z
f_0	f_1	f_2	f_3	0	0	0	0	$\varphi(x, y, z) = \bar{x} f(y, z)$
0	0	0	0	f_0	f_1	f_2	f_3	$\varphi(x, y, z) = x f(y, z)$
f_0	f_1	f_2	f_3	1	1	1	1	$\varphi(x, y, z) = \bar{x} f(y, z) \vee x$
1	1	1	1	f_0	f_1	f_2	f_3	$\varphi(x, y, z) = x f(y, z) \vee \bar{x}$
f_0	0	f_1	0	f_2	0	f_3	0	$\varphi(x, y, z) = \bar{z} f(x, y)$
0	f_0	0	f_1	0	f_2	0	f_3	$\varphi(x, y, z) = z f(x, y)$
f_0	1	f_1	1	f_2	1	f_3	1	$\varphi(x, y, z) = \bar{z} f(x, y) \vee z$
1	f_0	1	f_1	1	f_2	1	f_3	$\varphi(x, y, z) = z f(x, y) \vee \bar{z}$
f_0	f_1	0	0	f_2	f_3	0	0	$\varphi(x, y, z) = \bar{y} f(x, z)$
0	0	f_0	f_1	0	0	f_2	f_3	$\varphi(x, y, z) = y f(x, z)$
f_0	f_1	1	1	f_2	f_3	1	1	$\varphi(x, y, z) = \bar{y} f(x, z) \vee y$
1	1	f_0	f_1	1	1	f_2	f_3	$\varphi(x, y, z) = y f(x, z) \vee \bar{y}$
f_0	f_1	f_2	f_3	f_0	f_1	f_2	f_3	$\varphi(x, y, z) = f(y, z)$
f_0	f_0	f_1	f_1	f_2	f_2	f_3	f_3	$\varphi(x, y, z) = f(x, y)$
f_0	f_1	f_0	f_1	f_2	f_3	f_2	f_3	$\varphi(x, y, z) = f(x, z)$

Используя таблицу, запишите аналитическое выражение для следующих значений функции:

- а) (00010000); к) (11011111); ф) (00110011);
б) (00100000); л) (11101111); х) (11001100);
в) (00110000); м) (10101010); ц) (00000011);
г) (01000000); н) (10001010); ч) (00111111);
д) (00000111); о) (01010001); ш) (11111100);
е) (00001000); п) (00010101); щ) (11110011);
ж) (00001001); р) (01100110); ы) (00001111);
з) (00001010); с) (10011001); э) (01010101);
и) (11111011); т) (01110111); ю) (11110000);
й) (11111100); у) (01100110); я) (00110011).

9.17. Для следующих функций найдите СДНФ и упростите полученные выражения:

- а) $f(x_1, x_2, \dots, x_5) = (0, 16)$; г) $f(x_1, x_2, \dots, x_5) = (3, 19)$;

- б) $f(x_1, x_2, \dots, x_5) = (1, 17)$; д) $f(x_1, x_2, \dots, x_5) = (4, 20)$;
 в) $f(x_1, x_2, \dots, x_5) = (2, 18)$; е) $f(x_1, x_2, \dots, x_5) = (5, 21)$;
 ж) $f(x_1, x_2, \dots, x_5) = (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30)$;
 з) $f(x_1, x_2, \dots, x_5) = (1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31)$.

§ 10. Полином Жегалкина

Свойства операции сложения по модулю два:

$$x \oplus y = x \leftrightarrow y = \overline{xy} \vee \overline{xy}, \quad x \oplus y = y \oplus x, \quad (x \oplus y) \oplus z = x \oplus (y \oplus z),$$

$$x \oplus x = 0, \quad x \oplus 0 = x, \quad x \oplus 1 = \overline{x}, \quad x(y \oplus z) = xy \oplus xz,$$

$$x \oplus x = 0, \quad x \oplus 0 = x, \quad x \oplus 1 = \overline{x},$$

$$x \vee y = xy \oplus x \oplus y, \quad \text{причем } x \vee y = x \oplus y \leftrightarrow xy = 0,$$

$$x \vee y \vee z = xy \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z,$$

$$x \rightarrow y = xy \oplus x \oplus 1, \quad x \leftrightarrow y = x \oplus y \oplus 1, \quad x \downarrow y = xy \oplus x \oplus y \oplus 1.$$

Алгеброй Жегалкина называется множество булевых функций с операциями конъюнкции и сложения по модулю 2. В алгебре Жегалкина выполняются равенства:

- 1) $xy = yx$, $x \oplus y = y \oplus x$;
- 2) $(xy)z = x(yz)$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;
- 3) $x(y \oplus z) = xy \oplus xz$;
- 4) $xx = x$, $x \oplus x = x$;
- 5) $x \cdot 1 = x$, $x \cdot 0 = x$;
- 6) $x \oplus 1 = \overline{x}$, $x \oplus 0 = x$;
- 7) $x \vee y = xy \oplus x \oplus y$, причем $x \vee y = x \oplus y \leftrightarrow xy = 0$.

Полиномом Жегалкина называется сумма по модулю 2 произведений переменных x_1, x_2, \dots, x_n .

Теорема. Любую булеву функцию можно представить единственным образом в виде полинома Жегалкина.

Пример 1. Рассмотрим различные способы нахождения полинома Жегалкина для функции $f(x, y, z) = (y \rightarrow x) \rightarrow \overline{xyz}$.

Способ 1. *Нахождение полинома Жегалкина с использованием формул.*

$$(y \rightarrow x) \rightarrow \overline{xyz} = (yx \oplus y \oplus 1) \rightarrow \overline{xyz} = (yx \oplus y \oplus 1) \overline{xyz} \oplus (yx \oplus y \oplus 1) \oplus 1 =$$

$$= yxx\overline{yz} \oplus yx\overline{yz} \oplus xy\overline{z} \oplus yx \oplus y \oplus 1 \oplus 1 = 0 \oplus 0 \oplus xy\overline{z} \oplus yx \oplus y =$$

$$= x(y \oplus 1)(z \oplus 1) \oplus yx \oplus y = xyz \oplus xy \oplus xz \oplus x \oplus yx \oplus y.$$

$$(y \rightarrow x) \rightarrow \overline{xyz} = xyz \oplus xz \oplus x \oplus y.$$

Таблица 19

x	y	z	$y \rightarrow x$	\overline{xyz}	$f(x, y, z)$
0	0	0	1	0	0
0	0	1	1	0	0
0	1	0	0	0	1
0	1	1	0	0	1
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	0	0
1	1	1	1	0	0

переменных можно заменить сложением по модулю 2 этих наборов, т.е.

$$f(x, y, z) = \overline{x}y\overline{z} \oplus \overline{xyz} \oplus x\overline{y}z = ((x \oplus 1)y(z \oplus 1)) \oplus ((x \oplus 1)yz) \oplus (x(y \oplus 1)(z \oplus 1)) = xyz \oplus xy \oplus yz \oplus y \oplus \overline{xyz} \oplus yz \oplus xyz \oplus xy \oplus xz \oplus x.$$

$$(y \rightarrow x) \rightarrow \overline{xy}z = xyz \oplus xz \oplus x \oplus y.$$

Способ 3. *Нахождение полинома Жегалкина с использованием треугольника Паскаля.*

В верхнюю строку треугольника Паскаля записываем строку значений функции на всех наборах (табл. 20). В каждую следующую строку записываем значения, складывая последовательно по модулю 2 два соседних элемента предыдущей строки. Рассмотрим левую сторону треугольника. Единицам этой стороны соответствуют наборы значений переменных данной функции. Соединив знаком \oplus слагаемые, получим полином Жегалкина. Если набору (000) соответствует 1 в левой стороне треугольника, то добавим слагаемое 1.

Таблица 20

x	y	z	$f(x, y, z)$	Треугольник Паскаля	Левая сторона	Слагаемое
0	0	0	0	0 0 1 1 1 0 0 0	0	1
0	0	1	0	0 1 0 0 1 0 0	0	z
0	1	0	1	1 1 0 1 1 0	1	y
0	1	1	1	0 1 1 0 1	0	yz
1	0	0	1	1 0 1 1	1	x
1	0	1	0	1 1 0	1	xz
1	1	0	0	0 1	0	xy
1	1	1	0	1	1	xyz

$$(y \rightarrow x) \rightarrow \overline{xy}z = y \oplus x \oplus xz \oplus xyz.$$

Способ 4. *Метод неопределенных коэффициентов.*

Запишем в общем виде полином Жегалкина от трех переменных:

$$f(x, y, z) = a_0 \oplus a_1x \oplus a_2y \oplus a_3z \oplus a_4xy \oplus a_5xz \oplus a_6yz \oplus a_7xyz.$$

Вычислим значения данной функции на каждом наборе переменных или составим таблицу истинности для данной функции. Подставим также значения переменных в общий вид полинома и приравняем соответствующие значения функции:

$$f(0, 0, 0) = a_0 = 0, \quad f(0, 0, 1) = a_0 \oplus a_3 = 0, \quad f(0, 1, 0) = a_0 \oplus a_2 = 1,$$

Способ 2. *Нахождение полинома Жегалкина с использованием СДНФ.*

Составим таблицу истинности данной функции (табл. 19).

Представим данную функцию в виде СДНФ:

$$f(x, y, z) = \overline{x}y\overline{z} \vee \overline{xyz} \vee x\overline{y}z.$$

Используя свойство $X \vee Y = X \oplus Y \leftrightarrow XY = 0$, получаем, что дизъюнкцию любых наборов

$$f(0,1,1) = a_0 \oplus a_2 \oplus a_3 \oplus a_6 = 1, \quad f(1,0,0) = a_0 \oplus a_1 = 1,$$

$$f(1,0,1) = a_0 \oplus a_1 \oplus a_3 \oplus a_5 = 0, \quad f(1,1,0) = a_0 \oplus a_1 \oplus a_2 \oplus a_4 = 0,$$

$$f(1,1,1) = a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0.$$

Решая эту систему уравнений для операций по модулю 2, получим $a_0 = 0, a_3 = 0, a_2 = 1, a_6 = 0, a_1 = 1, a_5 = 1, a_4 = 0, a_7 = 1$.

Подставляя значения коэффициентов в общий вид, получаем $(y \rightarrow x) \rightarrow xy\bar{z} = x \oplus y \oplus xz \oplus xyz$. \square

Пример 2. Найти общий вид полинома Жегалкина мажоритарной функции от трех переменных.

Вычислим значения полинома Жегалкина на всех наборах переменных

$$f(0,0,0) = a_0, \quad f(0,0,1) = a_0 \oplus a_3, \quad f(0,1,0) = a_0 \oplus a_2,$$

$$f(0,1,1) = a_0 \oplus a_2 \oplus a_3 \oplus a_6 = 1, \quad f(1,0,0) = a_0 \oplus a_1,$$

$$f(1,0,1) = a_0 \oplus a_1 \oplus a_3 \oplus a_5 = 1, \quad f(1,1,0) = a_0 \oplus a_1 \oplus a_2 \oplus a_4 = 1,$$

$$f(1,1,1) = a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 1.$$

В уравнениях

$$a_0 \oplus a_2 \oplus a_3 \oplus a_6 = 1, \quad a_0 \oplus a_1 \oplus a_3 \oplus a_5 = 1, \quad a_0 \oplus a_1 \oplus a_2 \oplus a_4 = 1,$$

$$a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 1, \text{ считая коэффициенты } a_0, a_1, a_2, a_3$$

– свободными переменными, найдем остальные коэффициенты:

$$a_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2, \quad a_5 = 1 \oplus a_0 \oplus a_1 \oplus a_3,$$

$$a_6 = 1 \oplus a_0 \oplus a_2 \oplus a_3, \quad a_7 = a_1 \oplus a_2 \oplus a_3.$$

Общий вид полинома Жегалкина мажоритарной функции

$$f(x, y, z) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 z \oplus (1 \oplus a_0 \oplus a_1 \oplus a_2)xy \oplus$$

$$\oplus (1 \oplus a_0 \oplus a_1 \oplus a_3)xz \oplus (1 \oplus a_0 \oplus a_2 \oplus a_3)yz \oplus (a_1 \oplus a_2 \oplus a_3)xyz. \square$$

Булеву функцию для полинома Жегалкина можно задавать строкой коэффициентов $f = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)_{\oplus}$. Символ внизу строки будем использовать, чтобы различать задание функции двумя способами.

Вычислим значения данной функции на каждом наборе перемен для данной функции. Подставим также значения переменных в общий вид полинома и приравняем соответствующие значения функции:

$$f(0,0,0) = f_0 = a_0, \quad f(0,0,1) = f_1 = a_0 \oplus a_3, \quad f(0,1,0) = f_2 = a_0 \oplus a_2,$$

$$f(0,1,1) = f_3 = a_0 \oplus a_2 \oplus a_3 \oplus a_6, \quad f(1,0,0) = f_4 = a_0 \oplus a_1,$$

$$f(1,0,1) = f_5 = a_0 \oplus a_1 \oplus a_3 \oplus a_5, \quad f(1,1,0) = f_6 = a_0 \oplus a_1 \oplus a_2 \oplus a_4,$$

$$f(1,1,1) = f_7 = a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7.$$

Получили формулы перехода от коэффициентов разложения полинома Жегалкина $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)_{\oplus}$ к коэффициентам разложения по СДНФ $(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)$:

$$\begin{aligned}
 f_0 &= a_0, & f_1 &= a_0 \oplus a_3, & f_2 &= a_0 \oplus a_2, & f_3 &= a_0 \oplus a_2 \oplus a_3 \oplus a_6, & f_4 &= a_0 \oplus a_1, \\
 f_5 &= a_0 \oplus a_1 \oplus a_3 \oplus a_5, & f_6 &= a_0 \oplus a_1 \oplus a_2 \oplus a_4, \\
 f_7 &= a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7.
 \end{aligned}
 \tag{1}$$

Выразим коэффициенты a_i через коэффициенты f_j :

$$\begin{aligned}
 a_0 &= f_0, & a_1 &= f_0 \oplus f_4, & a_2 &= f_0 \oplus f_2, & a_3 &= f_0 \oplus f_1, & a_4 &= f_0 \oplus f_2 \oplus f_4 \oplus f_6, \\
 a_5 &= f_0 \oplus f_1 \oplus f_4 \oplus f_5, & a_6 &= f_0 \oplus f_1 \oplus f_2 \oplus f_3, \\
 a_7 &= f_0 \oplus f_1 \oplus f_2 \oplus f_3 \oplus f_4 \oplus f_5 \oplus f_6 \oplus f_7.
 \end{aligned}
 \tag{2}$$

Полученные формулы являются формулами перехода от коэффициентов разложения по СДНФ $(f_0 f_1 f_2 f_3 f_4 f_5 f_6 f_7)$ к коэффициентам полинома Жегалкина $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)_{\oplus}$.

Полином Жегалкина для данной функции можно найти четырьмя способами:

- используя формулы математической логики,
- используя СДНФ для данной функции и затем снятием отрицаний с переменных по формуле $\overline{x} = x \oplus 1$,
- используя СДНФ для данной функции и переходом к треугольнику Паскаля,
- методом неопределенных коэффициентов.

Если использовать формулы (2) для найденной СДНФ, то получаем пятый способ нахождения полинома Жегалкина.

Аналогично обозначим для функции от двух переменных $f(x, y)$:

$$f(0,0) = f_0, f(0,1) = f_1, f(1,0) = f_2, f(1,1) = f_3, \quad f(x, y) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 xy.$$

Булеву функцию от двух переменных можно задавать строкой значений (f_0, f_1, f_2, f_3) и можно задавать строкой коэффициентов $(a_0, a_1, a_2, a_3)_{\oplus}$.

Связь между координатами осуществляется по формулам

$$\left\{ \begin{array}{l} f_0 = a_0, \\ f_1 = a_0 \oplus a_2, \\ f_2 = a_0 \oplus a_1, \\ f_3 = a_0 \oplus a_1 \oplus a_2 \oplus a_3. \end{array} \right. \quad \text{или} \quad \left\{ \begin{array}{l} a_0 = f_0, \\ a_1 = f_0 \oplus f_2, \\ a_2 = f_0 \oplus f_1, \\ a_3 = f_0 \oplus f_1 \oplus f_2 \oplus f_3. \end{array} \right.$$

Задачи.

10.1. Найдите полином Жегалкина для следующих функций:

а) $f = (x \leftrightarrow y) \vee xz$; г) $f = \overline{xy} \oplus \overline{xz} \oplus \overline{z}$; ж) $f = (11110000)$;

б) $f = (x \vee y) \rightarrow \overline{xz}$; д) $f = (01010101)$; з) $f = (00001111)$.

в) $f = xy \vee xz \vee yz$; е) $f = (10101010)$;

10.2. Найдите СДНФ для следующих полиномов Жегалкина:

а) $f = 1 \oplus x_1 \oplus x_2 + x_1 x_3$; б) $f = x_1 \oplus x_3 \oplus x_1 x_3 \oplus x_1 x_2 x_3$;

в) $f = x_1 \oplus x_2 \oplus x_3 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_1 x_2 x_3$.

10.3. При нахождении полинома Жегалкина для функции $f(x_1, x_2, \dots, x_n)$ методом неопределенных коэффициентов получаем систему 2^n уравнений с 2^n неизвестными. Чему равен определитель этой системы?

10.4. Для функции $f(x, y, z)$ от трех переменных дан вектор значений $(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)$ этой функции, составленный из коэффициентов разложения функции в СДНФ, и вектор значений $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)_{\oplus}$ этой функции, составленный из коэффициентов полинома Жегалкина. Найдите вектор коэффициентов СДНФ и вектор коэффициентов полинома Жегалкина для следующих функций от двух переменных:

а) $\varphi_1(x, y) = f(x, y, 0)$; ж) $\varphi_7(x, y) = f(x, y, y)$;

б) $\varphi_2(x, y) = f(x, y, 1)$; з) $\varphi_8(x, y) = f(x, y, x)$;

в) $\varphi_3(x, z) = f(x, 0, z)$; и) $\varphi_9(x, z) = f(x, x, z)$;

г) $\varphi_4(x, z) = f(x, 1, z)$; й) $\varphi_{10}(x, y) = f(x, y, \bar{y})$;

д) $\varphi_5(y, z) = f(0, y, z)$; к) $\varphi_{11}(x, y) = f(x, \bar{y}, y)$;

е) $\varphi_6(y, z) = f(1, y, z)$; л) $\varphi_{12}(x, y) = f(x, \bar{y}, \bar{y})$.

10.5. а) Функция задана строкой коэффициентов полинома Жегалкина $f(x, y) = (g_0, g_1, g_3, g_4)_{\oplus}$. Найдите полином Жегалкина функции $f(x, 0) \oplus f(0, y)$.

б) Функция задана строкой коэффициентов полинома Жегалкина $f(x, y, z) = (g_0, g_1, \dots, g_7)_{\oplus}$. Найдите полином Жегалкина функции $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z)$.

в) Функция задана строкой коэффициентов полинома Жегалкина $f(x_1, x_2, x_3, x_4) = (g_0, g_1, \dots, g_{15})_{\oplus}$.

Сформулируйте гипотезу о виде полинома Жегалкина функции $f(x_1, x_2, x_3, 0) \oplus f(x_1, x_2, 0, x_4) \oplus f(x_1, 0, x_3, x_4) \oplus f(0, x_2, x_3, x_4)$ и проверьте эту гипотезу.

10.6. Найдите полином Жегалкина функции $f(x, y, z)$, удовлетворяющей условию $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z) = f(x, y, z)$.

10.7. Найдите полином Жегалкина функции $f(x, y, z)$, удовлетворяющей условию $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z) \equiv 0$.

§ 11. Карта Карно

Таблица 21

	y	\bar{y}
x		
\bar{x}		

Карта Карно для функции от двух переменных выделена жирной линией прямоугольника с клетками (таблица 21). Сверху и слева таблицы записаны переменные, которые влияют на запись конъюнкции в конкретную клетку.

Карта Карно для функции от трех переменных выделена жирной линией прямоугольника с клетками (таблицы 22 или 23). Сверху, снизу и слева таблицы записаны переменные, которые влияют на запись конъюнкции в конкретную клетку.

Таблица 22

	y	\bar{y}	
x			
\bar{x}			
	\bar{z}	z	\bar{z}

Таблица 23

	$x_2 x_3$	$x_2 \bar{x}_3$	$\bar{x}_2 x_3$	$\bar{x}_2 \bar{x}_3$
x_1				
\bar{x}_1				

Карта Карно для функции от четырех переменных (таблицы 24 – 26).

Таблица 24

	y	\bar{y}		
x				\bar{t}
				t
\bar{x}				\bar{t}
	\bar{z}	z	\bar{z}	

Таблица 25

	$x_3 x_4$	$x_3 \bar{x}_4$	$\bar{x}_3 x_4$	$\bar{x}_3 \bar{x}_4$
$x_1 x_2$				
$x_1 \bar{x}_2$				
$\bar{x}_1 x_2$				
$\bar{x}_1 \bar{x}_2$				

Таблица 26

	$x_2 x_3 x_4$	$x_2 \bar{x}_3 x_4$	$x_2 x_3 \bar{x}_4$	$x_2 \bar{x}_3 \bar{x}_4$	$\bar{x}_2 x_3 x_4$	$\bar{x}_2 \bar{x}_3 x_4$	$\bar{x}_2 x_3 \bar{x}_4$	$\bar{x}_2 \bar{x}_3 \bar{x}_4$
x_1								
\bar{x}_1								

Строки и столбцы карты Карно нумеруются конъюнкциями. Главное требование – каждая последующая конъюнкция отличается от предыдущей конъюнкции ровно одним символом. Края карты можно склеивать как по вертикали, так и по горизонтали. И тогда крайние конъюнкции также отличаются одним символом.

Запись логической функции в карту Карно.

Таблица 27

	y		\bar{y}	
x		1		1
\bar{x}	1			
	\bar{z}	z	\bar{z}	z

а) Пусть логическая функция представлена в форме СДНФ.

Пример 1. $f = xyz \vee \bar{x}\bar{y}\bar{z} \vee x\bar{y}z$. Для функции от трех переменных используем карту Карно для трех переменных (таблица 27). Для каждой конъюнкции определяем клетку на карте Карно, используя сферу влияния переменных и отмечая наличие конъюнкции

в этой клетке единицей. □

б) Пусть булева функция задана строкой значений на наборах переменных. Среди значений находим значения функции, равные 1, и определяем конъюнкции, на которой данная функция примет значение, равное единице.

Таблица 28

	y		\bar{y}	
x			1	1
\bar{x}		1		1
	\bar{z}	z	\bar{z}	z

Пример 2. $f = (10011100)$. Функция от трех переменных принимает значения, равные 1, на наборах (000), (011), (100), (101). Носителями данной функции являются $\bar{x}y\bar{z}, x\bar{y}z, x\bar{y}\bar{z}, x\bar{y}z$. Отмечаем на карте Карно (таблица 28) соответствующие клетки. □

в) Пусть логическая функция представлена в ДНФ, содержащей конъюнкции различных рангов. Для каждой конъюнкции определяем клетки, на которые влияют переменные в каждой конъюнкции.

Пример 3. $f = x \vee \bar{x}y \vee x\bar{y}z \vee x\bar{y}z\bar{t}$. Функция содержит 4 переменных, поэтому заполняем карту Карно для четырех переменных (таблица 29). Переменная x влияет на клетки двух верхних строк, поэтому заполняем восемь клеток единицами.

Таблица 29

	y		\bar{y}		
x	1	1	1	1	\bar{t}
	1	1	1	1	t
\bar{x}	1	1		1	
	1	1	1	1	\bar{t}
	\bar{z}	z	\bar{z}	z	

Конъюнкция $\bar{x}y$ влияет на 4 клетки, расположенные в левом нижнем квадрате размером 2×2 , поэтому заполняем их единицами.

Конъюнкция $x\bar{y}z$ влияет на 2 клетки, расположенные внизу четвертого столбца, поэтому заполняем их единицами.

Для конъюнкции $x\bar{y}z\bar{t}$ заполняем одну клетку в нижней строке. □

Замечание. При нанесении функций на карту Карно возможно наложение областей влияния различных конъюнкций. Если в клетку была вписана единица, то второй раз в эту клетку единицу не вписываем, т.к. дизъюнкция двух одинаковых конъюнкций является снова эта конъюнкция.

Пример 4. $f = \bar{x}t \vee y\bar{z} \vee x\bar{y}z\bar{t}$. Для конъюнкции $\bar{x}t$ заполняем верхнюю строку единицами (таблица 30). Для конъюнкции $y\bar{z}$ заполняем левый столбец таблицы. Зоны влияния этих двух конъюнкций пересекаются в левой верхней клетке. При заполнении второй конъюнкции в левом столбце нет необходимости снова отмечать эту клетку. Отмечаем остальные клетки левого столбца единица-

ми. Продолжая нанесение функции на карту, переходим к третьему члену $x\bar{y}z\bar{t}$ заданной функции. Эта конъюнкция расположена в верхней, левой клетке, и отмечать ее в третий раз также не нужно. □

Минимизация булевой функции с помощью карты Карно

Таблица 30

	y		\bar{y}		
x	1	1	1	1	\bar{t}
	1	1			t
\bar{x}	1	1			\bar{t}
	\bar{z}	z		\bar{z}	

Две клетки на карте Карно называются соседними, если они расположены рядом в одной строке либо рядом в одном столбце, либо расположены на концах одной строки или столбца.

Как отмечалось выше – любые две конъюнкции в соседних клетках отличаются одной переменной, а именно, в одной клетке расположена эта переменная, а в другой ее отрицание. Дизъюнкцию этих конъюнкций можно упростить.

Например, $x\bar{y}z \vee x\bar{y}z\bar{t} = xz(y \vee \bar{y}) = xz$. Таким образом, для упрощения СДНФ нужно произвести склейки соседних клеток. Иногда эту операцию можно применить к большей группе клеток.

Таблица 31

	y	\bar{y}
x	1	1
\bar{x}		1

Правила склейки конъюнкций на карте Карно:

1) любые две соседние единицы можно склеить, т.е. определяем сферу влияния элементарной конъюнкции для этой пары единиц. Ранг новой конъюнкции на единицу меньше, чем число переменных в карте Карно.

Например, в таблице 31, объединяя две верхних клетки, получим x, объединяя две клетки в правом столбце, получим \bar{y} . В итоге получаем ДНФ: $f = x \vee \bar{y}$.

Таблица 32

	y		\bar{y}	
x	1		1	1
\bar{x}	1			
	\bar{z}	z		\bar{z}

Будем использовать нумерацию элементов для матрицы. Объединяя элементы a_{11} и a_{14} матрицы (в таблице 32), получим конъюнкцию $x\bar{z}$, объединяя элементы a_{13} и a_{14} , получим конъюнкцию $x\bar{y}$, объединяя элементы a_{11} и a_{21} , получим $y\bar{z}$.

В итоге получаем ДНФ: $f = x\bar{z} \vee x\bar{y} \vee y\bar{z}$.

Таблица 33

	y		\bar{y}		
x	1	1	1	1	\bar{t}
				1	t
\bar{x}	1	1	1	1	
	1	1		1	\bar{t}
	\bar{z}	z		\bar{z}	

2) Любые четыре единицы на карте Карно четвертого порядка (таблица 33) объединяются, если они либо расположены рядом в одной строке, либо расположены рядом в одном столбце, либо образуют квадрат размером 2×2 , внутри которого нет других клеток. Определяем сферу влияния элементарной конъюнкции для этой группы единиц. Ранг новой конъюнкции на две единицы меньше, чем число переменных в карте Карно $f = x\bar{t} \vee y\bar{z} \vee x\bar{y}$.

Замечание. Если при склеивании двух единиц есть возможность включить их в некоторую четверку единиц, среди которых некоторые уже были раньше учтены, то необходимо это сделать – конъюнкция при этом только упростится.

В таблице 34 вначале объединяем четверку единиц в левом верхнем углу и получаем xy . Склеивая единицы в клетках a_{13} и a_{23} , получаем конъюнкцию третьего ранга $x\bar{y}z$. Но если включить эти единицы в квадрат, то получим конъюнкцию второго ранга xz . Она является более простым выражением. Покажем равносильность полученных формул $xy \vee x\bar{y}z$ и $xy \vee xz$ при двух способах склейки: $xy \vee x\bar{y}z = x(y \vee \bar{y}z) = x(y \vee z) = xy \vee xz$.

Таблица 34

	y	\bar{y}		
x	1	1	1	\bar{t}
	1	1	1	t
\bar{x}				
				\bar{t}
	\bar{z}	z		\bar{z}

Таблица 35

	y	\bar{y}		
x	1		1	\bar{t}
				t
\bar{x}				
	1		1	\bar{t}
	\bar{z}	z		\bar{z}

Обращаем внимание на следующий случай в таблице 35, где также на схеме имеем квадрат вида 2×2 из соседних клеток. Для этого достаточно заполнить окрестность угловой точки четырьмя такими картами. Получаем минимальную дизъюнктивную форму $\bar{z}\bar{t}$.

3) Любые восемь единиц на карте Карно четвертого порядка можно склеить, если они расположены в зоне влияния одной переменной или ее отрицания. Ранг новой конъюнкции на три единицы меньше, чем число переменных в карте Карно. Для таблицы 36 $f = y$.

Таблица 36

	y	\bar{y}		
x		1	1	\bar{t}
		1	1	t
\bar{x}		1	1	
		1	1	\bar{t}
	\bar{z}	z		\bar{z}

4) Если вся карта заполнена единицами, то функция тождественно равна единице.

Существуют различные способы минимизации ДНФ. Например, метод минимизирующих карт изложен в пособиях [16, 19].

Для двух, трех и четырех переменных часто используют карту Карно.

Алгоритм минимизации логической функции на карте Карно для четырех переменных:

1) Находим группу из 16 соседних единиц и записываем функцию $f = 1$.

2) Находим группы из восьми соседних единиц и записываем переменную.

3) Находим группы из четырех соседних единиц и записываем конъюнкции второго ранга.

4) Находим пары соседних единиц и составляем третьего ранга.

5) Используя приоритеты 1), 2), 3) находим минимальный набор элементарных конъюнкций, который охватывает все единицы в таблице, и составляем ДНФ.

На таблицах 37, 38 показаны различные способы склейки единиц для минимизации одной и той же функции:

$$f_1 = xz \vee xy \vee \bar{y}t \vee \bar{x}y\bar{t}, \quad f_2 = xz \vee \bar{y}z \vee \bar{y}t \vee \bar{x}y\bar{t}.$$

Таблица 37

	y	\bar{y}		
x		1	1	\bar{t}
	1	1	1	t
\bar{x}		1	1	t
	1		1	\bar{t}
	\bar{z}	z		\bar{z}

Таблица 38

	y	\bar{y}		
x		1	1	\bar{t}
	1	1	1	t
\bar{x}		1	1	t
	1		1	\bar{t}
	\bar{z}	z		\bar{z}

Задачи.

11.1. а) Запишите на карту Карно функцию $f(x, y, z)$ с носителем $N_f = \{(0011), (0010), (1101), (1100)$ и найдите для нее минимальную ДНФ.

б) Составьте для данного носителя СДНФ и приведите ее минимальной ДНФ.

11.2 . Запишите на карту Карно следующие функции и найдите для каждой функции минимальную ДНФ:

а) $f = xyz \vee \bar{x}y\bar{z} \vee x\bar{y}\bar{z};$

г) $f = (11110000);$

б) $f = x \vee \bar{y} \vee xz \vee xy\bar{z};$

д) $f = (1010101010101010);$

в) $f = x \vee z \vee xz \vee xy\bar{z}t;$

е) $f = (x \rightarrow y) \oplus (z \rightarrow t).$

11.3. Для следующих функций найдите минимальную ДНФ:

а)

	y	\bar{y}		
x			1	\bar{t}
	1	1	1	t
\bar{x}			1	t
				\bar{t}
	\bar{z}	z		\bar{z}

б)

	y	\bar{y}		
x		1	1	\bar{t}
	1	1	1	t
\bar{x}	1	1		t
	1	1		\bar{t}
	\bar{z}	z		\bar{z}

в)

	y	\bar{y}	
x	1	1	\bar{t}
	1	1	t
\bar{x}		1	
		1	\bar{t}
\bar{z}	z		\bar{z}

г)

	y	\bar{y}	
x	1	1	1
	1		t
\bar{x}		1	
	1	1	\bar{t}
\bar{z}	z		\bar{z}

11.4. Каким свойством обладает булева функция от четырех переменных, если карта Карно симметрична относительно:

- вертикальной средней линии;
- горизонтальной средней линии;
- относительно центра таблицы?

11.5. Каким свойством обладает булева функция от четырех переменных, если карта Карно антисимметрична, т.е. в симметричных клетках расположены 0 (который не записывается) и 1 относительно:

- вертикальной средней линии;
- горизонтальной средней линии;
- относительно центра таблицы?

11.6. Каким свойством обладает минимальная ДНФ булевой функции, если функция содержит фиктивную переменную?

11.7. Как заполнится карта Карно, если функция от четырех переменных содержит фиктивную переменную?

11.8. Функция $f(x_1, x_2, x_3, x_4)$ принимает значение 1 тогда и только тогда, когда хотя бы две переменные принимают значения 1. Минимизируйте функцию с помощью карты Карно.

11.9. Функция $f(x_1, x_2, x_3, x_4)$ принимает значение 1 тогда и только тогда, когда хотя бы две переменные принимают значения 0. Минимизируйте функцию с помощью карты Карно.

§ 12. Схемы и булевы функции

а) Релейно-контактные схемы

Под релейно-контактной схемой будем понимать устройство из проводников и переключателей. Каждому переключателю на схеме поставим в соответствие логическую переменную, принимающую значение 1, если переключатель замкнут и значение 0, если он разомкнут. Все переключатели на схеме, обозначенные одной и той же переменной, подключены к одному реле, которое может изменить положение “включено” на положение “выключено” и наоборот.

На схеме с двумя переключателями, соединенными параллельно (рис. 5), сигнал будет проходить, если хотя бы один переключатель замкнут, что соответствует *дизъюнкции* $x \vee y$.

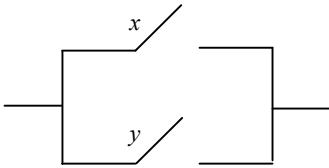


Рис. 5

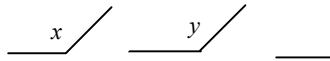


Рис. 6

На схеме с двумя переключателями, соединенными последовательно (рис. 6), сигнал будет проходить, если оба переключателя замкнуты, что соответствует *конъюнкции* $x \wedge y$.

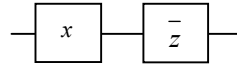


Рис. 7

Две схемы будем считать *эквивалентными* (равносильными), если при одном и том же состоянии входных сигналов будут соответственно одинаковые сигналы на выходе системы. Из двух эквивалентных схем более *простой* будем считать ту, которая содержит меньше переключателей.

В дальнейшем переключатель x , находящийся в состоянии “замкнуто”, и переключатель z , находящийся в положении “разомкнуто”, будем обозначать более простым способом (рис. 7). Иногда контур переменной на схеме не изображается.

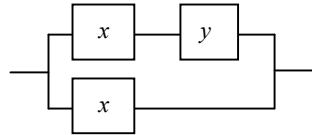


Рис. 8

Булева функция, соответствующая схеме, называется функцией проводимости.

Пример 1. Для схемы на рис. 8 составить функцию проводимости, упростить эту функцию и построить для нее более простую схему.

Решение. Входной сигнал разделяется на две параллельные ветви, что соответствует дизъюнкции некоторых переменных. В верхней ветви переключатели соединены последовательно, что соответствует конъюнкции двух переменных.

На данной схеме реализуется булева функция $(x \wedge y) \vee x$.

Применяя закон поглощения, получаем

$$(x \wedge y) \vee x = x.$$

Эквивалентная, но более простая схема, представлена на рис. 9. Схема на рис. 9 содержит меньшее число переключателей. Рассмотрите различные состояния переключателей x и y на рисунке 8 и покажите, что выходной сигнал определяется только состоянием выключателя x и не зависит от состояния выключателя y . □

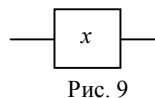


Рис. 9

Пример 2. Сколько и каких переключателей будет иметь схема после упрощения (рис. 10)?

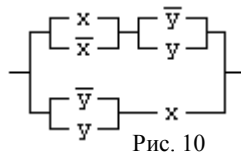


Рис. 10

Решение. Схеме соответствует булева функция

$$f(x, y) = ((x \vee \bar{x})(\bar{y} \vee y)) \vee ((y \vee \bar{y})x) = (1 \wedge 1) \vee 1x = 1 \vee x = 1.$$

Для любых значений переменных x и y в схеме проходит сигнал, поэтому упрощенная схема не содержит ни одного выключателя. □

Пример 3. Жюри из трех человек принимает положительное решение большинством голосов “за”. Построить схему устройства для голосования.

Таблица 39

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x, y, z)$	0	0	0	1	0	1	1	1

Решение. Пусть в случае голосования “за” экспертом x жюри поступает сигнал $x = 1$, а в случае “против” поступает сигнал 0.

Составим функцию принятия решения (таблица 39).

Найдем СДНФ для этой функции:

$$\bar{x}yz \vee x\bar{y}z \vee xy\bar{z} \vee xyz.$$

11), реализующую эту функцию.

Функция содержит 12 символов для переменных (не считая знаки отрицаний, дизъюнкций и конъюнкций), что соответствует двенадцати переключателям на схеме.

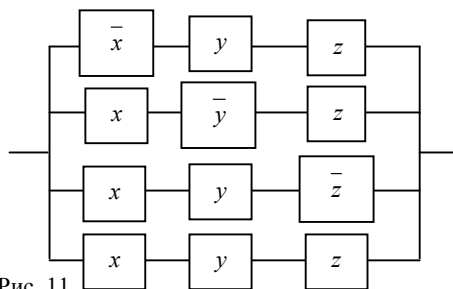


Рис. 11

Упростим булеву функцию

$$\begin{aligned} \bar{x}yz \vee x\bar{y}z \vee xy\bar{z} \vee xyz &= \bar{x}yz \vee xyz \vee x\bar{y}z \vee xyz \vee xy\bar{z} \vee xyz = \\ &= (\bar{x} \vee x)yz \vee x(\bar{y} \vee y)z \vee xy(\bar{z} \vee z) = xy \vee xz \vee yz. \end{aligned}$$

Составим схему полученной функции (рис. 12).

Устройство содержит 6 переключателей.

Кстати, функцию можно упростить следующим образом:

$$xy \vee xz \vee yz = xy \vee (x \vee y)z.$$

Построим схему с меньшим числом переключателей (рис. 13). □

Уменьшение числа переключателей на схеме является важной задачей электротехники и электроники, а значит, важной задачей минимизации булевой функции в дискретной математике.

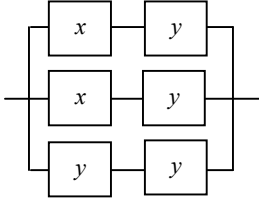


Рис. 12

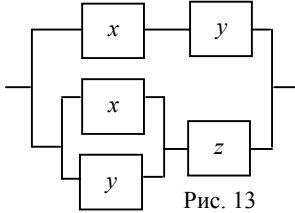


Рис. 13

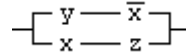


Рис. 14

Пример 4. Определить наборы значений переменных, при которых работает схема на рис. 14.

Решение. Данной схеме соответствует функция $f(x, y, z) = y\bar{x} \vee xz$. Составим таблицу истинности (табл. 40).

Выбирая значения переменных, на которых функция принимает значения 1, получаем условия работы схемы: $f(0, 1, 0) = 1 = f(0, 1, 1)$, $f(1, 0, 1) = 1 = f(1, 1, 1)$. □

Таблица 40

x	y	z	$y\bar{x}$	xz	$f = y\bar{x} \vee xz$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	1	0	1
0	1	1	1	0	1
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	0	0	0
1	1	1	0	1	1

схеме

Простейшим логическим элементом на схемах является **инвертор** (рис. 15 или рис. 16), выполняющий функцию отрицания (инверсию). У этого элемента один вход и один выход. Если на вход поступает сигнал, соответствующий 1, то на выходе будет 0 и наоборот.

Логический элемент, выполняющий конъюнкцию двух переменных (рис. 17 или рис. 18), называется **конъюнктом**.

На выходе этого элемента будет сигнал 1 только в том случае, когда на все входы поступает сигнал 1.

Если хотя бы на одном входе будет ноль, то на выходе также будет ноль.

Логический элемент, выполняющий дизъюнкцию входящих сигналов $x \vee y$ (рис. 19 или рис. 20), называется

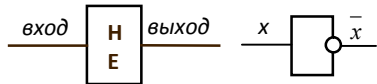


Рис. 15

Рис. 16

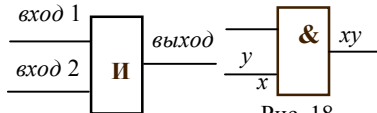


Рис. 17

Рис. 18

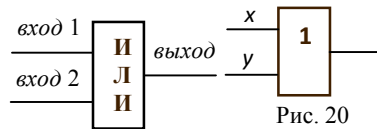


Рис. 19

Рис. 20

дизъюнктом. Если хотя бы на один вход дизъюнктора поступает сигнал 1, то на выходе будет сигнал 1.

Будем использовать специальные графические обозначения (рис. 16, 18, 20) соответственно для отрицания, конъюнкции и дизъюнкции согласно ГОСТ ЕСКД. Конъюнкторы и дизъюнкторы могут иметь более двух входов.

Пример 5. Для схемы на рис. 21:

- а) расставьте значения на выходе каждого логического элемента;
- б) упростите полученную логическую функцию;
- в) постройте новую схему для упрощенной логической функции.

Решение. а) рис. 22.

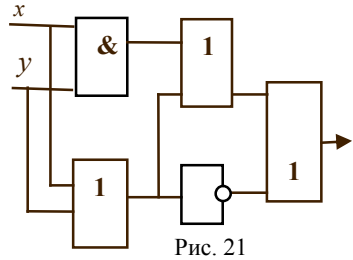


Рис. 21

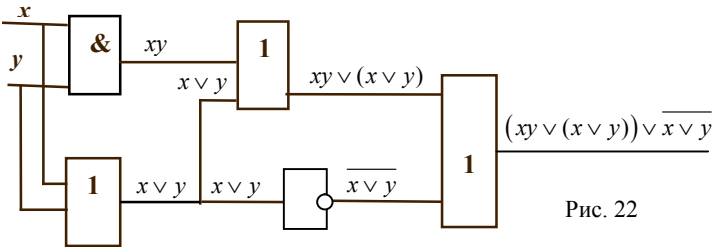


Рис. 22

б) Упростим выражение

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

Для данной схемы можно рассмотреть равносильную функцию $f(x, y) = 1$.

в) Кроме данной схемы, эту функцию можно реализовать и несколькими другими схемами.

Приведем более простую схему (рис. 23), с одним входом. □

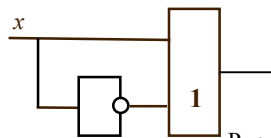


Рис. 23

Пример 6. Дана схема (рис. 24), для которой известны некоторые значения входных и выходных сигналов.

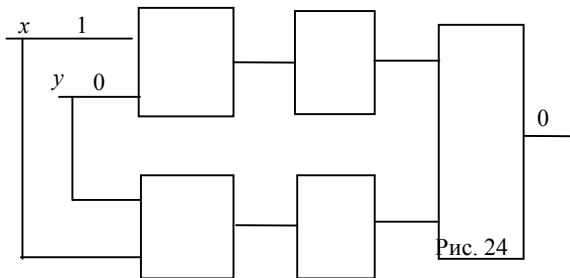
а) Расставьте логические элементы, реализующие дизъюнкцию, конъюнкцию или отрицание, таким образом, чтобы схема работала;

б) для каждого решения, реализующего схему, составьте логическое выражение и упростите его;

в) для упрощенного логического выражения постройте более простую схему, эквивалентную данной схеме.

Решение. На схеме можно выделить три вида информации: входные сигналы, набор электронных элементов и выходные сигналы.

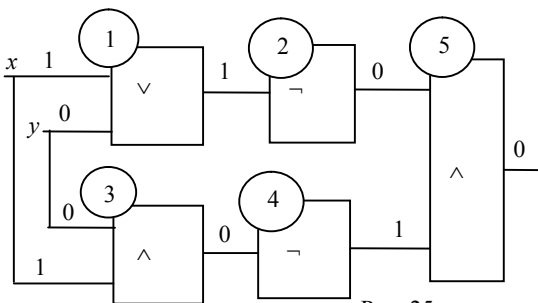
а) Возможно решение простыми подстановками в пустые клетки соответствующих элементов.



Если в клетку приходит один сигнал, то этот блок реализует операцию – отрицание. В каждую клетку, в которую приходит два сигнала, можно подставить элемент, реализующий дизъюнкцию или конъюнкцию. Для трех таких клеток получаем $2 \cdot 2 \cdot 2 = 8$ вариантов. Некоторые из этих вариантов могут привести к противоречию с заданными сигналами на входе и выходе.

Но метод перебора можно упростить, если осуществить целенаправленный поиск.

Занумеруем элементы и начинаем анализ с последнего элемента. Он может быть дизъюнкцией или конъюнкцией. Выбрав одну из этих функций, например конъюнкцию (рис. 25), получаем, что на вход пятого элемента должен прийти один из следующих наборов (0;0), (0;1) или (1;0). Порядок символов в паре следующий: первый элемент пары означает значение сигнала на выходе со второго элемента, а второй символ в паре – значение сигнала на выходе с четвертого элемента.



Если на вход пятого элемента подан набор (0,1), т.е. со второго элемента пришло значение 0, а с четвертого элемента пришло значение 1, то с первого элемента вышло – 1, а с третьего – 0. Следовательно, первый элемент должен быть дизъюнкцией, а третий элемент – конъюнкцией.

Для рассмотренного варианта решения запишем последовательность найденных операций в порядке нумерации элементов ($\vee \neg \wedge \neg \wedge$).

Аналогично рассматриваются остальные варианты.

Чтобы избежать ошибок при перечислении, нужно компактно записывать решение. Будем записывать каждый вариант, последовательно отмечая значения сигналов на выходе или входе блоков и логические функции в каждую клетку. Во втором и четвертом блоках можно записать один раз логическую операцию “нет” (рис. 26).

После рассмотрения всех вариантов необходимо собрать вначале первые символы в каждой четверке, затем вторые, третьи и, наконец, четвертые символы. Запишем все решения в виде последовательностей операций: $(\vee\wedge\wedge\wedge)$, $(\wedge\vee\wedge\wedge)$, $(\vee\vee\wedge\wedge)$, $(\vee\vee\vee\vee)$.

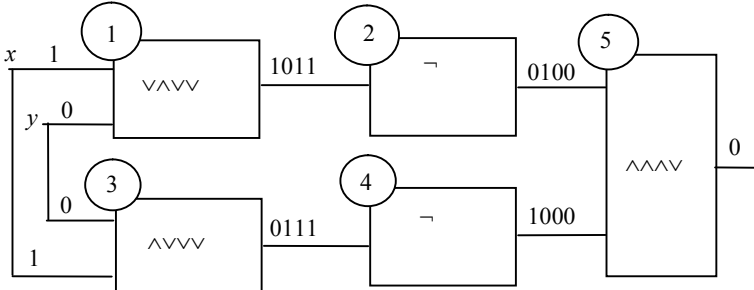


Рис. 26

б) Составим логическое выражение для каждого варианта схемы и упростим его, используя законы логики:

$$x \vee x = x \quad (1), \quad xx = x \quad (2), \quad x \vee y = y \vee x \quad (3), \quad xy = yx \quad (4),$$

$$x(y \vee z) = xy \vee xz \quad (5), \quad \overline{x \vee y} = \overline{x} \overline{y} \quad (6), \quad \overline{xy} = \overline{x} \vee \overline{y} \quad (7).$$

Для набора операций $(\vee\wedge\wedge\wedge)$, учитывая их последовательность из схемы, получаем

$$\overline{x \vee y} \overline{xy} \stackrel{(6),(7)}{=} \overline{xy(x \vee y)} \stackrel{(5)}{=} \overline{xyx \vee xyx} \stackrel{(4),(2)}{=} \overline{xy \vee xy} \stackrel{(1)}{=} \overline{xy} \stackrel{(7)}{=} \overline{xy} = x \vee y.$$

Схема на рис. 27 реализует упрощенную логическую функцию.

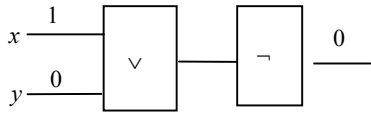


Рис. 27

Аналогично

$$\overline{xy} \overline{x \vee y} \stackrel{(4)}{=} \overline{xy(x \vee y)} = \overline{xy \vee xy} \stackrel{(2)}{=} \overline{xy \vee xy} = \overline{xy \vee xy},$$

$$\overline{x \vee y} \overline{xy \vee xy} \stackrel{(1)}{=} \overline{x \vee y}.$$

Можно ли сразу определить упрощенную логическую функцию, реализующую данную схему? Частично да, на основе информации о входных и выходных сигналах.

По таблице логических функций от двух переменных можно найти восемь логических функций, принимающие значение 0 на наборе (0,1).

Вначале кажется, что получено противоречие. При решении задачи после упрощения получена одна функция, а из таблицы следует, что должно получиться восемь функций.

Противоречия нет, т.к. в задаче задана схема, в которой кроме значений входных и выходных сигналов имеется информация о количестве логических элементов. В схеме должно быть два отрицания и три элемента, которые реали-

зуют дизъюнкцию или конъюнкцию, причем указано их взаиморасположение. Дополнительная информация сузила класс функций и вместо восьми функций появилась одна функция.

Данная схема (рис. 24) симметрична относительно горизонтальной прямой. Это замечание сразу сокращает вдвое количество функций для поиска.

Некоторые задачи такого типа можно решать, используя эвристики, т.е. сокращением количества вариантов перебора на основе некоторых догадок.

Рассмотрим второй способ решения задачи с использованием эвристики.

Из симметрии коммутативных свойств логических операций (3), (4) следует, что первый и третий элементы на схеме (рис. 24) с одинаковыми логическими операциями формируют одинаковый выходной сигнал. При переборе всех вариантов с одинаковыми операциями в этих элементах подробно рассматриваем линию первого и второго элементов и автоматически повторяем выходной сигнал с четвертого элемента, равный значению выходного сигнала со второго элемента.

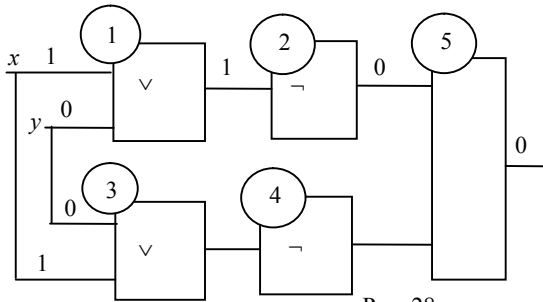


Рис. 28

На схеме (рис. 28) пятый элемент можно реализовать, используя две логические операции – дизъюнкцию и конъюнкцию. Получаем два решения: $(\vee \vee \neg \wedge)$, $(\vee \vee \neg \vee)$.

Для двух конъюнкций в первом и третьем элементах на схеме (рис. 29) получаем противоречие для пятого элемента, поэтому такая расстановка конъюнкций не реализуется.

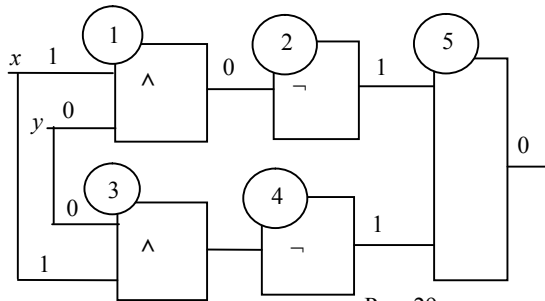


Рис. 29

Из симметрии операций относительно двух пар $0 \vee 1 = 1$, $1 \vee 0 = 1$ и $0 \wedge 1 = 1$, $1 \wedge 0 = 1$ следует, что, переставив операции в первом и втором элементах, мы получим на выходе схемы один и тот же результат. Поэтому достаточно подробно рассмотреть один из вариантов. Например, для варианта на рис. 30 задаем в первом и третьем элементах соответственно функции \vee , \wedge . По схеме далее опреде-

ляем набор функций – ($\vee \wedge \neg$). Переставляя функции в первом и во втором элементах автоматически получаем следующее решение ($\wedge \neg \vee \wedge$).

Итак, идея симметрии элементов внутри одной операции и идея перестановки операций для данной схемы (снова симметрия) позволяет значительно сократить число переборов вариантов.

В этом примере эвристики, основанные на свойствах логических операций и фундаментальном понятии - симметрии, сократили вдвое количество возможных вариантов для проверки. \square

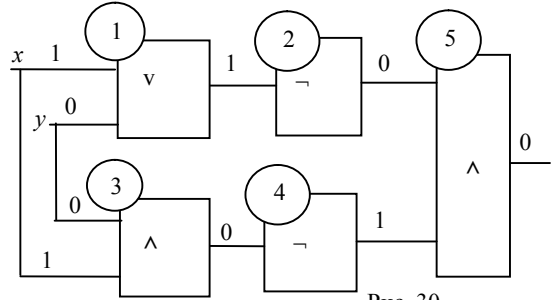
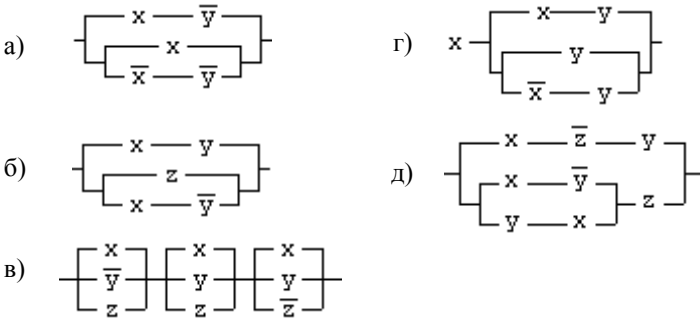


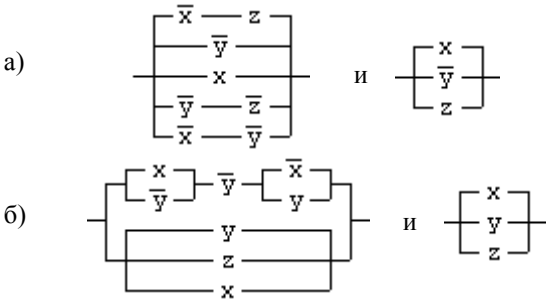
Рис. 30

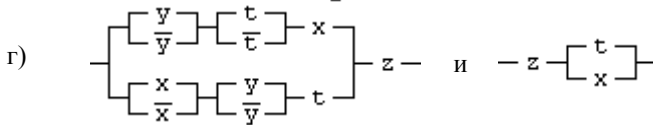
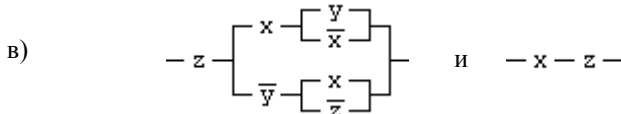
Задачи.

12.1. Для данной схемы найдите функцию проводимости, упростите ее и постройте соответствующую схему:

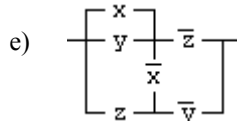
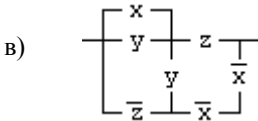
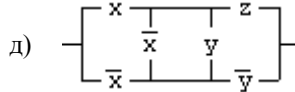
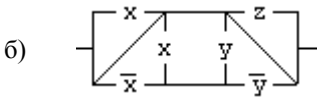
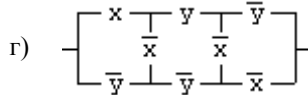
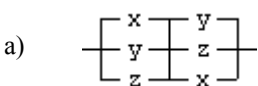


12.2. Эквивалентны ли следующие схемы:





12.3. Упростите (если это возможно) следующие релейно-контактные схемы, называемые мостиками:



12.4. Постройте релейно-контактную схему с данной функцией проводимости. Приведите пример набора переменных, для которого схема передает сигнал.

а) $xy \vee xz \vee yz$;

д) $x \rightarrow y$;

б) $(x\bar{y} \vee z \vee \bar{x})(\bar{x}\bar{y})$;

е) $x \vee xy \vee xyz \vee xyzt$;

в) $x(x \vee y)(x \vee y \vee z)(x \vee y \vee z \vee t)$;

ж) $\bar{x} \vee \bar{x}y \vee \bar{x}yz \vee \bar{x}yzt$;

г) $(x \vee y \vee \bar{y}z)\bar{x}$;

з) $x \oplus y$.

12.5. Для функции $f = (11011011)$ постройте релейно-контактную схему. Минимизируйте функцию с помощью карты Карно и постройте упрощенную схему.

12.6. В следующих задачах введите понятие переключателя. Постройте наиболее простую релейно-контактную схему с четырьмя переключателями x, y, z, t , которая проводит ток при выполнении следующего условия:

а) Дверь сейфа открывается тогда и только тогда, когда каждый из четырех членов правления банка дает разрешение на открытие двери.

б) Входная дверь секретной лаборатории открывается, когда хотя бы два сотрудника лаборатории дают разрешение на открытие лаборатории.

в) Погружение водолазов на большую глубину прекращается тогда и только тогда, когда остается не более одного работоспособного комплекта для погружения.

г) Работа спасательного судна считается возможной, если из четырех членов команды водолазы x и y дают согласие на начало работы.

д) Выход из строя двух автомобилей x и z из четырех на базе послужило основанием для проведения расследования.

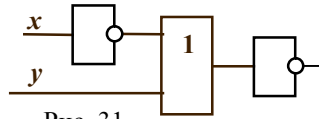


Рис. 31

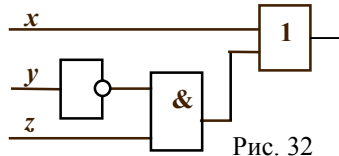


Рис. 32

12.7. Какую логическую функцию реализует схема на рис. 31?

12.8. Постройте таблицу истинности для логической схемы (рис. 29) и запишите формулу для данной схемы.

12.9. Составьте выражение логической функции для каждой из схем на рис. 33–35, упростите выражение и запишите одной логической функцией.

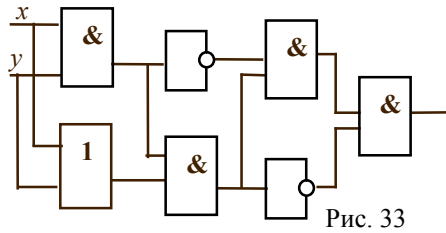


Рис. 33

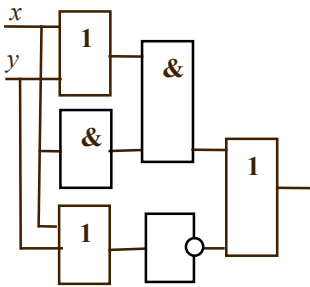


Рис. 34

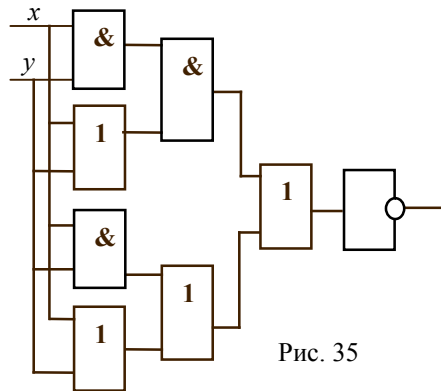


Рис. 35

12.10. Определите все варианты входных значений x и y , чтобы работала схема на рис. 36.

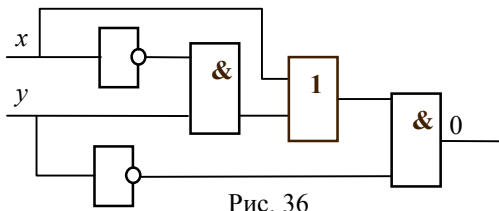


Рис. 36

12.11. Дана схема (рис. 37), для которой известны некоторые значения входных и выходных сигналов.

а) Расставьте логические элементы, реализующие дизъюнкцию, конъюнкцию или отрицание таким образом, чтобы схема работала;

б) для каждого решения, реализующего схему, составьте логическое выражение и упростите его;

в) для упрощенного логического выражения постройте более простую схему, эквивалентную данной схеме.

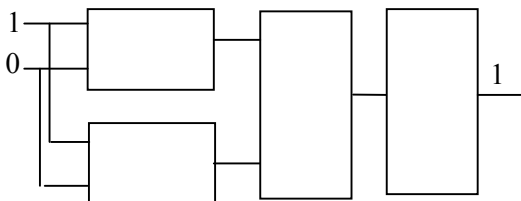


Рис. 37

12.12. Составьте схему, содержащую пустые клетки и стрелки, указывающие направление сигналов. Расставьте на входе и выходе схемы наборы сигналов таким образом, чтобы схема не проводила сигнал.

12.13. Постройте схему, реализующую данную функцию:

а) $f(x, y) = \overline{x \vee y} \cdot x \vee y$; б) $f(x, y) = (x \downarrow y)(x \downarrow y)$; в) $\overline{\overline{x \vee y} \cdot x \vee y}$.

§ 13. Функционально замкнутые классы. Классы T_0 и T_1

Множество булевых функций называется *функционально замкнутым классом*, если вместе с функциями этого множества оно содержит все их композиции.

Замыканием набора K булевых функций называется множество всех композиций этого набора. Обозначение замыкания – $[K]$.

Класс функций является функционально замкнутым, если его замыкание совпадает с этим классом.

Пример 1. Найти замыкание множества функций $K = \{f_1(x, y) = y, f_2(x, y) = x \vee y, f_3(x, y) = x \rightarrow y\}$.

Решение. Составим композиции:

$$F_1(x, y) = f_2(x, f_3(x, y)) = x \vee (x \rightarrow y) = x \vee (\bar{x} \vee y) = (x \vee \bar{x}) \vee y = 1, \quad F_1 \notin K,$$

$$F_2(x, y) = f_2(f_3(x, y), y) = (x \rightarrow y) \vee y = (\bar{x} \vee y) \vee y = \bar{x} \vee y = x \rightarrow y, \quad F_2 \in K,$$

$$F_3(x, y) = f_3(f_2(x, y)) = (x \vee y) \rightarrow y = \overline{x \vee y} \vee y = (\bar{x} \bar{y}) \vee y = \\ = (\bar{x} \vee y)(\bar{y} \vee y) = (\bar{x} \vee y) = x \rightarrow y, \quad F_3 \in K,$$

$$F_4(x, y) = f_3(x, f_2(x, y)) = x \rightarrow (x \vee y) = \bar{x} \vee (x \vee y) = (\bar{x} \vee x) \vee y = 1, \quad F_4 \notin K,$$

$$F_5(x, y) = f_3(y, y) = y \rightarrow y = 1, \quad F_5 \notin K,$$

$$F_6(x, y) = f_2(y, y) = y \vee y = y, \quad F_6 \in K.$$

Аналогично продолжая составлять композиции, можно заметить, что множество K нужно дополнить функцией $f(x, y) = 1$, чтобы получить замыкание.

Объединяя данное множество функций и всевозможные композиции, получим замыкание $[K] = \{y, x \vee y, x \rightarrow y, 1\}$. \square

Пример 2. Доказать, что множество булевых функций, удовлетворяющих условию $f(x_1, x_2, \dots, x_n) \geq x_n$, образует замкнутый класс.

Решение. Если $x_n = 0$, то значение функции $f(x_1, x_2, \dots, 0)$ может быть произвольным. Если $x_n = 1$, то значение функции $f(x_1, x_2, \dots, x_{n-1}, 1) = 1$. Таким образом, множество функций K характеризуется одним условием $f(x_1, x_2, \dots, x_{n-1}, 1) = 1$.

Пусть функции $f(x_1, x_2, \dots, x_n)$ и $h(x_1, x_2, \dots, x_n)$ удовлетворяют условию $f(x_1, x_2, \dots, x_{n-1}, 1) = 1$, $h(x_1, x_2, \dots, x_{n-1}, 1) = 1$. Для сложной функции

$$F(x_1, x_2, \dots, x_{n-1}, x_n) = f(x_1, x_2, \dots, x_{i-1}, h(x_1, x_2, \dots, x_n), x_{i+1}, \dots, x_n)$$

получаем

$$F(x_1, x_2, \dots, x_{n-1}, 1) = f(x_1, x_2, \dots, x_{i-1}, h(x_1, x_2, \dots, x_{n-1}, 1), x_{i+1}, \dots, 1) = \\ = f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, 1) = 1.$$

$F(x_1, x_2, \dots, x_{n-1}, 1) \in K$. Аналогично для подстановок в другие переменные.

Множество данных функций образует замкнутый класс.

Замечание. Множество функций $f(x, y)$, удовлетворяющих условию $f(x, 1) = 1$, состоит из четырех функций $\{y, x \vee y, x \rightarrow y, 1\}$, изученных в предыдущем примере. \square

Пример 3. Доказать, что множество функций $a_0(a_1 \vee x_1)(a_2 \vee x_2) \dots (a_n \vee x_n)$ для всевозможных значений a_i , где $i = 0, 1, \dots, n$ образует замкнутый класс.

Решение. Если $a_0 = 0$, то $f(x_1, x_2, \dots, x_n) = 0$.

$a_0 = a_1 = \dots = a_n = 1$, то $f(x_1, x_2, \dots, x_n) = 1$.

Если $a_i = 1$, то $(a_i \vee x_i) = (1 \vee x_i) = 1$ и функция не содержит скобку $(a_i \vee x_i)$.

Если $a_i = 0$, то $(a_i \vee x_i) = (0 \vee x_i) = x_i$ и функция вместо скобки $(a_i \vee x_i)$ содержит множитель x_i .

Таким образом, получаем множество всех функций:

$$0, 1, x_1, x_2, \dots, x_n, x_1x_2, x_1x_3, \dots, x_1x_n, \dots, x_1x_2 \dots x_n.$$

Переобозначая любую переменную, т.е. полагая $x_i = x_j$, получим функцию из этого множества.

Любая композиция этих функций снова является функцией из этого множества. Следовательно, данное множество является замкнутым множеством. \square

Классом T_0 называется множество функций, удовлетворяющих условию $f(0, 0, \dots, 0) = 0$. Переименование переменной не выводит из этого класса. Для любых двух функций из этого класса получаем $f_1(0, f_2(0, 0, \dots, 0), 0, \dots, 0) = 0$, поэтому этот класс функций является функционально замкнутым.

Для двух переменных существует восемь различных булевых функций в классе T_0 : $0, X, Y, X \wedge Y, X \vee Y, X \oplus Y, \overline{X} \rightarrow \overline{Y}, \overline{Y} \rightarrow \overline{X}$.

Функция от n переменных из класса T_0 имеет вид $\underbrace{(0 \dots \dots)}_{2^n}$, поэтому

класс T_0 содержит $2^{2^n - 1}$ функций. Для $n = 3$ класс T_0 содержит $2^7 = 128$ функций.

Классом T_1 называется множество функций, удовлетворяющих условию $f(1, 1, \dots, 1) = 1$. Переименование переменной не выводит из этого класса. Для любых двух функций из этого класса получаем $f_1(1, f_2(1, 1, \dots, 1), 1, \dots, 1) = 1$, поэтому этот класс функций является функционально замкнутым.

Класс функций, не сохраняющих единицу (ноль), не является замкнутым классом. Примером функции, не сохраняющей единицу, является функция $f(x) = \overline{x}$. Эта функция также не сохраняет ноль. Но композиция $f(f(x)) = \overline{\overline{x}} = x$ сохраняет и единицу и ноль.

Функция от n переменных из класса T_1 имеет вид $\underbrace{(\dots \dots \dots 1)}_{2^n}$, поэтому

класс T_1 содержит $2^{2^n - 1}$ функций. Для $n = 3$ класс T_1 содержит $2^7 = 128$ функций.

Теорема. Пусть функции $f_0(x_1, x_2, \dots, x_n)$ и $f_1(x_1, x_2, \dots, x_n)$ удовлетворяют условиям $f_0(0, 0, \dots, 0) = 1, f_0(1, 1, \dots, 1) = 1, f_1(1, 1, \dots, 1) = 0$ (первое равенство означает, что функция f_0 не сохраняет 0, а третье равенство означает, что функция f_1 не сохраняет 1), тогда из этих функций можно получить константы 0 и 1 с помощью формул

$$1 = f_0(x, x, \dots, x) = \varphi(x),$$

$$0 = f_1(f_0(x, x, \dots, x), f_0(x, x, \dots, x), \dots, f_0(x, x, \dots, x)) = \psi(x).$$

Задачи.

13.1. Постройте замыкание следующих множеств функций:

а) $K = \{f_1(x, y) = \overline{x}, f_2(x, y) = \overline{y}\}$;

б) $K = \{0, f_1(x, y) = \overline{x}, f_2(x, y) = \overline{y}\}$;

в) $K = \{xy\}$; г) $K = \{x \vee y\}$.

13.2. Сколько функций $f(x_1, x_2, \dots, x_n)$ в классе T_0 удовлетворяет условиям:

а) $f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 0$;

б) $f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 1$;

в) $f(0, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 1$;

г) $f(1, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 1$?

13.3. Сколько функций $f(x_1, x_2, \dots, x_n)$ в классе T_1 удовлетворяет условиям:

а) $f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 0$; в) $f(0, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 1$;

б) $f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 1$; г) $f(1, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 1$?

13.4. а) Докажите, что для двух переменных существует восемь различных булевых функций в классе T_1 :

$xy, x, y, x \vee y, x \leftrightarrow y, y \rightarrow x, x \rightarrow y, 1$.

б) Докажите, что для $n = 3$ класс T_1 содержит $2^7 = 128$ функций. Приведите несколько примеров таких функций.

13.5. Покажите, что для функции $f(x_1, x_2, \dots, x_n)$ из класса T_0 можно построить несколько функций $g_i(x_1, x_2, \dots, x_{n+1})$ из класса T_0 , так что $g_i(x_1, x_2, \dots, x_n, 0) = f(x_1, x_2, \dots, x_n)$.

13.6. Покажите, что для функции $f(x_1, x_2, \dots, x_n)$ из класса T_1 можно построить несколько функций $g_i(x_1, x_2, \dots, x_{n+1})$ из класса T_1 , так что $g_i(x_1, x_2, \dots, x_n, 1) = f(x_1, x_2, \dots, x_n)$.

13.7. Постройте карты Карно для каждой функции от двух переменных из класса T_1 .

13.8. Перечислите все функции от двух переменных, которые принадлежат как классу T_0 , так и классу T_1 .

13.9. Приведите несколько функций от трех переменных, которые принадлежат классу T_0 и классу T_1 .

13.10. Приведите пример функций, не сохраняющих 0, из которых композицией можно получить функцию, сохраняющую 0.

13.11. Приведите пример функций, не сохраняющих 1, из которых композицией можно получить функцию, сохраняющую 1.

13.12. Используя следующие функции, получите константы 0 и 1:

а) $f_0(x, y) = x \leftrightarrow y, f_1(x, y) = y$; б) $f_0(x, y) = y \rightarrow x, f_1(x, y) = x \oplus y$.

13.13. Приведите пример мажоритарной функции f , удовлетворяющей условию:

а) $f \in T_0$; б) $f \notin T_0$; в) $f \in T_1$; г) $f \notin T_1$.

13.14. Приведите пример функции, не принадлежащей классу T_0 и:

- а) заданной аналитически;
- б) заданной вектором значений.

13.15. Приведите пример функции, не принадлежащей классу T_1 и:

- а) заданной аналитически;
- б) заданной вектором значений.

13.16. Докажите, что булева функция $f(x_1, x_2, \dots, x_n)$, записанная в СДНФ принадлежит классу T_1 , тогда и только тогда, когда она содержит элементарную конъюнкцию x_1, x_2, \dots, x_n без инверсий. Используя это свойство, определите, какие из следующих функций принадлежат классу T_1 :

- а) (01010101); в) $f(x_1, x_2, \dots, x_5) = (1, 5, 31)$;
- б) (10101010); г) $f(x_1, x_2, \dots, x_5) = (0, 5, 30)$.

13.17. Докажите, что булева функция $f(x_1, x_2, \dots, x_n)$, записанная в ДНФ, принадлежит классу T_1 тогда и только тогда, когда она содержит хотя бы одну элементарную конъюнкцию без инверсий. Используя это свойство, определите, какие из следующих функций принадлежат классу T_1 :

- а) $\bar{x}\bar{y} \vee \bar{y}\bar{z} \vee \bar{x}\bar{z} \vee \bar{x}\bar{y}\bar{z}$; б) $\bar{x} \vee \bar{x}\bar{y} \vee \bar{y}\bar{z} \vee \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}\bar{z}$.

13.18. Докажите, что булева функция $f(x_1, x_2, \dots, x_n)$, записанная в КНФ, принадлежит классу T_1 , если в каждую ее дизъюнкцию входит хотя бы одна неинверсная переменная. Используя это свойство, определите, какие из следующих функций принадлежат классу T_1 :

- а) $(\bar{x} \vee \bar{y})\bar{z}$; б) $\bar{x} \vee \bar{y} \vee \bar{z}$; в) $(\bar{x} \vee \bar{y} \vee z)(x \vee y \vee \bar{z})$.

13.19. Докажите, что булева функция $f(x_1, x_2, \dots, x_n)$, записанная в СДНФ, принадлежит классу T_0 тогда и только тогда, когда она не содержит элементарную конъюнкцию $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$ с инверсиями всех переменных. Используя это свойство, определите, какие из следующих функций принадлежат классу T_0 :

- а) (01010101); в) $f(x_1, x_2, \dots, x_5) = (1, 5, 31)$;
- б) (10101010); г) $f(x_1, x_2, \dots, x_5) = (0, 5, 30)$.

13.20. Докажите, что булева функция $f(x_1, x_2, \dots, x_n)$, записанная в ДНФ, принадлежит классу T_0 , если в ее записи нет ни одной конъюнкции, содержащей только переменные с инверсиями. Используя это свойство, определите, какие из следующих функций принадлежат классу T_0 :

- а) $\bar{x}\bar{y} \vee \bar{y}\bar{z} \vee \bar{x}\bar{z} \vee \bar{x}\bar{y}\bar{z}$; б) $\bar{x} \vee \bar{x}\bar{y} \vee \bar{y}\bar{z} \vee \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}\bar{z}$; в) $x \vee \bar{y}\bar{z}$.

13.21. Докажите, что функция, заданная в КНФ, принадлежит классу T_0 , если в ее записи имеется хотя бы одна неинверсная переменная, находящаяся за скобками. Используя это свойство, определите, какие из следующих функций принадлежат классу T_0 :

а) $(x \vee z)yt$; б) $(\overline{x \vee y})(z \vee t)$.

13.22. Даны функции $f_1 \in T_0, f_2 \in T_0$. Принадлежат ли классу T_0 функции:

а) $f_1 \vee f_2$; б) $f_1 \wedge f_2$; в) $f_1 \oplus f_2$; г) $f_1 \rightarrow f_2$; д) $f_1 \leftrightarrow f_2$; е) $\overline{f_1}$?

Влияет ли на ответ количество переменных, от которых зависят каждая из данных функций?

13.23. Даны функции $f_1 \in T_1, f_2 \in T_1$. Принадлежат ли классу T_1 функции:

а) $f_1 \vee f_2$; б) $f_1 \wedge f_2$; в) $f_1 \oplus f_2$; г) $f_1 \rightarrow f_2$; д) $f_1 \leftrightarrow f_2$; е) $\overline{f_1}$?

Влияет ли на ответ количество переменных, от которых зависит каждая из данных функций?

13.24. Дана $f(x, y)$, принадлежащая классу T_0 . Какие из следующих функций принадлежат классу T_0 :

а) $f(x, y) \oplus z$; б) $f(x, y) \oplus \overline{z}$; в) $f(x, y)z$; г) $f(x, y)\overline{z}$;
 д) $f(x, y) \vee z$; е) $f(x, y) \rightarrow z$; ж) $f(x, y) \leftrightarrow z$; з) $\overline{f(x, y)}$?

13.25. Дана $f(x, y)$, принадлежащая классу T_1 . Какие из следующих функций принадлежат классу T_1 :

а) $f(x, y) \oplus z$; б) $f(x, y) \oplus \overline{z}$; в) $f(x, y)z$; г) $f(x, y)\overline{z}$;
 д) $f(x, y) \vee z$; е) $f(x, y) \rightarrow z$; ж) $f(x, y) \leftrightarrow z$; з) $\overline{f(x, y)}$?

§ 14. Класс самодвойственных функций

Для данной функции $f(x_1, x_2, \dots, x_n)$ функция $f^* = \overline{f(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n})}$ называется *двойственной*.

Примеры 1–6:

1. $f_1 = x_1 \vee x_2, f_1^* = \overline{\overline{x_1 \vee x_2}} = \overline{\overline{x_1} \wedge \overline{x_2}} = x_1 \wedge x_2$;

2. $f_1 = x_1 \wedge x_2, f_1^* = \overline{\overline{x_1 \wedge x_2}} = \overline{\overline{x_1} \vee \overline{x_2}} = x_1 \vee x_2$;

3. $f_3(x_1, x_2) = x_1, f_3^* = \overline{\overline{x_1}} = x_1, f_3^* = f_3$;

4. $f_4(x_1, x_2) = \overline{x_2}, f_4^* = \overline{\overline{\overline{x_2}}} = \overline{x_2}, f_4^* = f_4$;

5. $f_5(x_1, x_2) = 0$, $f_5^* = \bar{0} = 1$. Обращаем внимание в этом случае на то, что отрицание применяется только к функции, т.к. аналитическая запись функции не содержит переменных.

Обоснуем полученный факт другим способом.

$$f_5 = 0 = x \wedge \bar{x}, f_5^* = \overline{x \wedge \bar{x}} = \overline{x \vee \bar{x}} = x \vee \bar{x} = 1.$$

6. $f_6(x_1, x_2) = 1$, $f_6^* = \bar{1} = 0$. Отрицание применяется только к функции, т.к. аналитическая запись функции не содержит переменных.

Обоснуем полученный факт другим способом.

$$f_6 = 1 = X \vee \bar{X}, f_6^* = \overline{X \vee \bar{X}} = \overline{X} \wedge \bar{\bar{X}} = X \wedge \bar{X} = 0.$$

$$7. f_7(X_1, X_2) = X_1 \oplus X_2, f_7^* = \overline{X_1 \oplus X_2} = \overline{X_1} \oplus \overline{X_2} \oplus 1 = \\ = X_1 \oplus 1 \oplus X_2 \oplus 1 \oplus 1 = X_1 \oplus X_2 \oplus 1, f_7^* = f_7 \oplus 1.$$

Теорема. Пусть $f(f_1(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n)) = \Phi(x_1, x_2, \dots, x_n)$, тогда $\Phi^*(x_1, x_2, \dots, x_n) = f^*(f_1^*(x_1, x_2, \dots, x_n), \dots, f_k^*(x_1, x_2, \dots, x_n))$.

Из теоремы вытекает принцип двойственности: пусть имеется некоторая формула над множеством $\{0, 1, x, \bar{x}, x_1 \vee x_2, x_1 \wedge x_2\}$, тогда заменив 0 на 1 и, наоборот, 1 на 0, \vee на \wedge , \wedge на \vee , получим двойственную формулу. Если для исходной формулы выполнялось тождество, то и для соответствующих формул выполняется тождество.

Пример 7. Пусть доказано утверждение $x \vee \bar{x} = 1$. Применяя замены \vee на \wedge , 1 на 0, получим утверждение $x \wedge \bar{x} = 0$, справедливость которого автоматически следует из принципа двойственности.

Применение принципа двойственности позволяет сократить число доказательств при выводе тождеств.

Функция $f(x_1, x_2, \dots, x_n)$ называется *самодвойственной*, если

$$f(x_1, x_2, \dots, x_n) = f^*(x_1, x_2, \dots, x_n) \text{ или } f(x_1, x_2, \dots, x_n) = \overline{\overline{f(x_1, x_2, \dots, x_n)}} \text{ или равносильно } \overline{f(x_1, x_2, \dots, x_n)} = f(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}).$$

Если все значения функции различны относительно средней линии таблицы истинности, то функция – самодвойственная.

Множество всех самодвойственных функций является замкнутым классом.

Примеры самодвойственных функций:

$$x_1, \bar{x}_1, x_1 \oplus x_2 \oplus x_3, x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5.$$

Класс самодвойственных функций обозначим \mathcal{S} . Он является функционально замкнутым, что следует из теоремы.

Для двух переменных существует четыре различные булевы функции в классе \mathcal{S} .

Функция от n переменных из класса \mathcal{S} имеет вид $(f_0, f_2, \dots, f_{2^{n-1}}, \overline{f_{2^{n-1}}}, \dots, \overline{f_2}, \overline{f_0})$, поэтому класс \mathcal{S} содержит $2^{2^{n-1}}$ функций. Для $n = 3$ класс \mathcal{S} содержит 16 функций.

Самодвойственные функции от трех переменных $f(x, y, z)$:

$$f_{15} = x, f_{23} = xy \vee xz \vee yz, f_{43} = xy \vee xz \vee yz, f_{51} = y, f_{77} = xz \vee xy \vee yz, f_{85} = z, \\ f_{105} = xyz \vee \overline{xy} \vee \overline{x} \vee \overline{y} \vee \overline{z}, f_{113} = yz \vee \overline{xy} \vee \overline{xz}, f_{142} = xy \vee \overline{xz} \vee \overline{yz}, \\ f_{150} = xyz \vee \overline{xy} \vee \overline{x} \vee \overline{y} \vee \overline{z}, f_{170} = z, f_{178} = xy \vee \overline{xz} \vee \overline{yz}, f_{204} = y, \\ f_{212} = \overline{xy} \vee \overline{xz} \vee \overline{yz}, f_{232} = \overline{xy} \vee \overline{xz} \vee \overline{yz}, f_{240} = \overline{x}.$$

Проверим по определению, что функция f_{23} является самодвойственной:

$$f_{23}^* = \overline{\overline{xy \vee xz \vee yz}} = \overline{\overline{xy} \vee \overline{xz} \vee \overline{yz}} = (x \vee y) (x \vee z) (y \vee z) = \\ = (x \vee xz \vee yx \vee yz) (y \vee z) = xy \vee xzy \vee yx \vee yz \vee xz \vee xz \vee yxz \vee yz = \\ = xy \vee xzy \vee yz \vee xz = xy \vee yz \vee xz.$$

Теорема. Пусть функция $f_0(x_1, x_2, \dots, x_n)$ удовлетворяет условиям $f_0(0, 0, \dots, 0) = 1, f_0(1, 1, \dots, 1) = 0$ (первое равенство означает, что функция f_0 не сохраняет 0) и функция $f_c(x_1, x_2, \dots, x_n)$ не самодвойственная, тогда из этих функций можно получить константы 0 и 1.

Алгоритм получения констант:

1. $\varphi(x) = f_0(x, x, \dots, x) = \overline{x}$,

2. Существует набор $(\alpha_1, \alpha_2, \dots, \alpha_n)$, для которого:

$$f_c(\alpha_1, \alpha_2, \dots, \alpha_n) = f_c(\overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_n}) = \text{const} = c.$$

3. Составляем функции $f_c(x^{\alpha_1}, x^{\alpha_2}, \dots, x^{\alpha_n}) = c, \varphi(f_c(x^{\alpha_1}, x^{\alpha_2}, \dots, x^{\alpha_n})) = \overline{c}$ и для всех i , для которых $\alpha_i = 0$, заменяем x^{α_i} на $\varphi(x)$.

Пример 8. Из функции $f(x, y, z)$ (табл. 41) получить константы 0 и 1.

Таблица 41

x	y	z	$f(x, y, z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Из таблицы видно, что для данной функции выполняются равенства $f_0(0, 0, \dots, 0) = 1, f_0(1, 1, \dots, 1) = 0$. Эта функция также не является самодвойственной. Например, существует два набора $(0, 0, 1)$ и $(1, 1, 0)$, расположенных симметрично относительно средней горизонтальной линии таблицы, проходящей через наборы переменных, на которых функция принимает равные значения: $f(0, 0, 1) = 1 = f(1, 1, 0)$.

Две указанные функции $f_0(x, y, z)$ и $f_c(x, y, z)$, рассмотренные в теореме, совпадают с одной данной функцией $f(x, y, z)$.

Вначале получаем отрицание переменной $\varphi(x) = f(x, x, \dots, x) = \overline{x}$.

Для набора $(\alpha_1, \alpha_2, \alpha_3) = (1, 1, 0)$ составляем функцию

$$1 = f(x^1, x^1, x^0) = f(x, x, \overline{x}) = f(x, x, f(x, x, x)).$$

Применяя отрицание, получим

$$0 = \varphi(f(x, x, f(x, x, x))) = f(f(x, x, f(x, x, x)), f(x, x, f(x, x, x)), f(x, x, f(x, x, x))).$$

Замечание 1. Аналогично можно рассмотреть набор $(\alpha_1, \alpha_2, \alpha_3) = (0, 0, 1)$ и составить функцию $1 = f(x^0, x^0, x^1) = f(\bar{x}, \bar{x}, x) = f(f(x, x, x), f(x, x, x), x)$. Далее аналогично применяем отрицание.

Замечание 2. Для данной функции существует еще два набора $(0, 1, 1)$ и $(1, 0, 0)$, расположенные симметрично относительно средней горизонтальной линии таблицы, на которых функция принимает равные значения: $f(0, 1, 1) = 0 = f(1, 0, 0)$.

Аналогично можно построить константы

$$0 = f(x^0, x^1, x^1) = f(\bar{x}, x, x) = f(f(x, x, x), x, x)$$

$$\text{или } 0 = f(x^1, x^0, x^0) = f(x, \bar{x}, \bar{x}) = f(x, f(x, x, x), f(x, x, x)).$$

Отметим, что константу 1 лучше получить, используя вектор $(1, 1, 0)$, а константу 0 – используя вектор $(0, 1, 1)$. \square

Задачи.

14.1. Перечислите все самодвойственные функции от одной переменной.

14.2. Перечислите все самодвойственные функции от двух переменных.

14.3. Сколько существует самодвойственных функций от n переменных?

14.4. Докажите, что число значений самодвойственной функции от n переменных, равных 0, равно числу значений, равных 1.

14.5. Докажите, что операция перехода к двойственной функции обладает следующими свойствами:

$$\text{а) } (f^*)^* = f; \quad \text{г) } (f \vee g)^* = f^* g^*; \quad \text{ж) } (f \rightarrow g)^* = \overline{g^* \rightarrow f^*};$$

$$\text{б) } (\bar{f})^* = \overline{(f^*)}; \quad \text{д) } (f \oplus g)^* = f^* \leftrightarrow g^*; \quad \text{з) } (f|g)^* = f^* \downarrow g^*;$$

$$\text{в) } (fg)^* = f^* \vee g^*; \quad \text{е) } (f \leftrightarrow g)^* = f^* \oplus g^*; \quad \text{и) } (f \downarrow g)^* = f^* | g^*.$$

14.6. Функции $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ самодвойственные. Докажите, что если $f(1, x_2, \dots, x_n) = g(1, x_2, \dots, x_n)$, то $f = g$.

14.7. Какие из функций класса \mathcal{S} от трех переменных принадлежат классу T_0 ?

14.8. Какие из функций класса \mathcal{S} от трех переменных принадлежат классу T_1 ?

14.9. Сколько функций $f(x_1, x_2, \dots, x_n)$ в классе \mathcal{S} удовлетворяет условиям:

$$\text{а) } f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 0; \quad \text{в) } f(0, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 0;$$

$$\text{б) } f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 1; \quad \text{г) } f(1, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 1?$$

14.10. Приведите пример функций, которые не являются самодвойственными, но из которых путем композиции можно получить самодвойственную функцию.

14.11. Функция $f(x_1, x_2, x_3)$ задана вектором значений (11010110). Покажите, что функция не является самодвойственной и получите из нее константы 0 и 1.

14.12. Даны самодвойственные функции $f(x_1, x_2, \dots, x_n)$ и $F(t, x_{n+1})$. Докажите, что сложная функция от $n+1$ переменной $\varphi(x_1, x_2, \dots, x_n, x_{n+1}) = F(f(x_1, x_2, \dots, x_n), x_{n+1})$ также является самодвойственной.

14.13. Приведите пример мажоритарной функции f , удовлетворяющей условию: а) $f \in S$; б) $f \notin S$.

14.14. Дана самодвойственная функция $f(x, y)$. Какие из следующих функций являются самодвойственными:

- а) $f(x, y) \wedge z$; б) $f(x, y) \wedge \bar{z}$; в) $f(x, y) \vee z$; г) $f(x, y) \rightarrow z$;
 д) $f(x, y) \oplus z$; е) $f(x, y) \leftrightarrow z$; ж) $\overline{f(x, y)}$?

§ 15. Класс линейных функций

Функция $f(x_1, x_2, \dots, x_n)$ называется *линейной*, если

$$f(x_1, x_2, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n, \text{ где } a_i \in \{0, 1\}, \text{ т.е. ее полином Жегалкина не содержит произведений переменных.}$$

Множество линейных функций обозначается через L .

Пусть $f(x_1, x_2, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$,

$$g(x_1, x_2, \dots, x_n) = b_0 \oplus b_1 x_1 \oplus b_2 x_2 \oplus \dots \oplus b_n x_n, \text{ } f \in L, g \in L, \text{ тогда:}$$

$$f \oplus g = (a_0 \oplus b_0) \oplus (a_1 \oplus b_1) x_1 \oplus (a_2 \oplus b_2) x_2 \oplus \dots \oplus (a_n \oplus b_n) x_n \in L, 0 \in L, 1 \in L.$$

Переименование переменной не выводит из этого класса. Для суперпозиции получаем

$$f(x_1, \dots, x_{i-1}, g(x_1, \dots, x_n), x_{i+1}, \dots, x_n) =$$

$$a_0 \oplus a_1 x_1 \oplus \dots \oplus a_{i-1} x_{i-1} \oplus a_i (b_0 \oplus b_1 x_1 \oplus \dots \oplus b_n x_n) \oplus a_{i+1} x_{i+1} \oplus \dots \oplus a_n x_n \in L.$$

Следовательно, множество L является функционально замкнутым классом.

Линейные функции от двух переменных имеют вид

$$f(x, y) = a_0 \oplus a_1 x \oplus a_2 y.$$

Составим таблицу 42 для коэффициентов.

Таблица 42

a_0	a_1	a_2	$a_0 \oplus a_1 x \oplus a_2 y$
0	0	0	0
0	0	1	y
0	1	0	x
0	1	1	$x \oplus y$
1	0	0	1
1	0	1	$1 \oplus y = \bar{y}$
1	1	0	$1 \oplus x = \bar{x}$
1	1	1	$1 \oplus x \oplus y = x \oplus y = x \leftrightarrow y$

Таким образом, класс L функций от двух переменных содержит восемь линейных функций: $0, x, y, \bar{x}, \bar{y}, x \oplus y, x \leftrightarrow y, 1$

Класс L функций от n переменных содержит 2^{n+1} функций.

Достаточный признак нелинейности функции. Если булева функция $f(x_1, x_2, \dots, x_n)$ принимает

значение 1 на нечетном числе булевых векторов (x_1, x_2, \dots, x_n) , то она нелинейная.

Существуют нелинейные функции, принимающие значение 1 на четном числе булевых векторов.

Например, $f(x, y, z) = xyz \vee \bar{x}\bar{y}\bar{z} = xy \oplus xz \oplus x = (00001001)$.

Класс всех нелинейных функций не является замкнутым, т.е. существуют такие нелинейные функции, композиция которых линейна.

Пример 1. Пусть $f(x, y) = x \downarrow y = x \vee \bar{y}$, $\varphi(x, y) = x | y = \bar{x} \bar{y}$. Составим таблицу истинности этих функций (таблица 43).

Таблица 43

x	y	$f(x, y)$	$\varphi(x, y)$
0	0	1	1
0	1	0	1
1	0	0	1
1	1	0	0

Обе функции принимают нечетное число раз значение 1, поэтому они нелинейные. \square

Построим следующую композицию этих функций $F(x, y) = f(x, \varphi(x, y))$, т.е.

$$f(x, \varphi(x, y)) = x \vee \overline{\bar{x}\bar{y}} = \bar{x}xy = \bar{x}xy = (x\bar{x})y = 0,$$

$F(x, y) = 0$ – линейная функция. Следовательно,

композиция нелинейных функций оказалась линейной функцией.

Лемма о нелинейных функциях. Если функция $f(x_1, x_2, \dots, x_n)$ нелинейная, то подстановкой констант и использования отрицания из этой функции можно получить дизъюнкцию, и конъюнкцию.

Алгоритм получения дизъюнкции и конъюнкции из нелинейной функции:

1. Для функции $f(x_1, x_2, \dots, x_n)$ ищем полином Жегалкина.
2. Среди всех произведений в полиноме Жегалкина выбираем самое короткое произведение K .
3. Среди переменных, входящих в произведение K , выбираем любые две переменные x, y , а всем остальным переменным, входящим в это короткое произведение, придаем значение 1. Остальным переменным, не входящим в K , придаем значение 0. После подстановки этих констант получим функцию $\varphi(x, y) = xy \oplus \alpha x \oplus \beta y \oplus \gamma$ от двух переменных, в которой коэффициенты α, β, γ принимают значения 0 или 1.

4. В зависимости от коэффициентов α, β, γ получаем дизъюнкцию и конъюнкцию расстановкой констант. Можно использовать таблицу 44.

Таблица 44

α	β	γ	Полином Жегалкина	Формула	\vee	\wedge
0	0	0	xy	$x \wedge y$	$\overline{\varphi(\overline{x}, \overline{y})}$	$\varphi(x, y)$
0	0	1	$xy \oplus 1$	$\overline{x \wedge y}$	$\varphi(\overline{x}, \overline{y})$	$\overline{\varphi(x, y)}$
0	1	0	$xy \oplus y$	$\overline{x} \wedge y$	$\overline{\varphi(x, \overline{y})}$	$\overline{\varphi(\overline{x}, y)}$
0	1	1	$xy \oplus y \oplus 1$	$x \vee \overline{y}$	$\varphi(x, \overline{y})$	$\overline{\varphi(\overline{x}, y)}$
1	0	0	$xy \oplus x$	$x \wedge \overline{y}$	$\overline{\varphi(\overline{x}, y)}$	$\varphi(x, \overline{y})$
1	0	1	$xy \oplus x \oplus 1$	$\overline{x} \vee y$	$\varphi(\overline{x}, y)$	$\overline{\varphi(x, \overline{y})}$
1	1	0	$xy \oplus x \oplus y$	$x \vee y$	$\varphi(x, y)$	$\overline{\varphi(\overline{x}, \overline{y})}$
1	1	1	$xy \oplus x \oplus y \oplus 1$	$\overline{x \vee y}$	$\overline{\varphi(x, y)}$	$\varphi(\overline{x}, \overline{y})$

Таблица 45

f	0	0	0	1	0	1	1	0
x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1

Пример 2. Показать, что следующая функция (таблица 45) нелинейная, и получить из нее конъюнкцию и дизъюнкцию расстановкой констант и знака отрицания.

Решение. Функция нелинейная, т.к. она принимает значение 1 нечетное число

раз. Найдем полином Жегалкина, используя СДНФ.

$$f(x, y, z) = \overline{xyz} \vee x\overline{yz} \vee xy\overline{z} = ((x \oplus 1)yz) \oplus (x(y \oplus 1)z) \oplus (xy(z \oplus 1)) = \\ = xyz \oplus yz \oplus x\overline{yz} \oplus xz \oplus xy\overline{z} \oplus xy = xyz \oplus yz \oplus xz \oplus xy.$$

В полиноме Жегалкина три коротких произведения yz, xz, xy . Выбираем одно из них, например yz .

Таблица 46

y	z	yz	$f(0, y, z)$	$y \vee z$	$\overline{f(0, \overline{y}, \overline{z})}$
0	0	0	0	0	0
0	1	0	0	1	1
1	0	0	0	1	1
1	1	1	1	1	1

Остальным переменным, т.е. переменной x , придаем значение 0. Получаем $f(0, y, z) = yz$ и $\overline{f(0, \overline{y}, \overline{z})} = y \vee z$.

Сделаем проверку результата в таблице 46, используя

значения $f(0, y, z)$ из таблицы 45. \square

Задачи.

15.1. Проверьте, что каждая булева функция от одной переменной является линейной.

15.2. Докажите, что булева функция $f = (f_0, f_1, f_2, f_3)$ от двух переменных является линейной тогда и только тогда, когда $f_3 = f_0 \oplus f_1 \oplus f_2$.

15.3. Докажите, что если функция $f(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)$ от трех переменных является линейной, то $f_3 = f_0 \oplus f_1 \oplus f_2$, $f_5 = f_0 \oplus f_1 \oplus f_4$, $f_6 = f_0 \oplus f_2 \oplus f_4$, $f_7 = f_1 \oplus f_2 \oplus f_4$. Обратите внимание на суммирование нижних индексов, т.е. линейная функция имеет вид $(f_0, f_1, f_2, f_0 \oplus f_1 \oplus f_2, f_4, f_0 \oplus f_1 \oplus f_4, f_0 \oplus f_2 \oplus f_4, f_1 \oplus f_2 \oplus f_4)$.

15.4. Докажите равенство $\sum_{i=0}^7 f_i = 0$ для линейной функции от трех переменных, используя задачу 15.3. Докажите это же равенство, используя достаточный признак нелинейности функции.

15.5. Докажите, что если функция $f(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)$ от трех переменных является линейной, то

$$(f_2, f_3) = (f_0, f_1) \text{ или } (f_2, f_3) = (\overline{f_0}, \overline{f_1}) \text{ и}$$

$$(f_4, f_5, f_6, f_7) = (f_0, f_1, f_2, f_3) \text{ или } (f_4, f_5, f_6, f_7) = (\overline{f_0}, \overline{f_1}, \overline{f_2}, \overline{f_3}).$$

15.6. Докажите, что полином Жегалкина $a_0 \oplus a_1x \oplus a_2y \oplus a_3z \oplus a_4xy \oplus a_5xz \oplus a_6yz \oplus a_7xyz$ является линейной функцией тогда и только тогда, когда выполняется равенство $a_4 \vee a_5 \vee a_6 \vee a_7 = 0$.

15.7. Среди перечисленных функций найдите нелинейные булевы функции и получите из них конъюнкцию и дизъюнкцию расстановкой констант и знака отрицания:

а) $f = 1 \oplus x \oplus z \oplus xz \oplus xyz$; д) $f = (x \leftrightarrow y) \oplus (z \leftrightarrow t) \oplus 1$;

б) $f = 1 \oplus x \oplus y$; е) $f = (01101001)$;

в) $f = x \vee xz \vee xyz$; ж) $f = (10011011)$.

г) $f = x \rightarrow y$;

15.8. Функция $f(x, y, z)$ принимает значение 0 тогда и только тогда, когда только две переменные принимают значения 0. Покажите, что функция не является линейной и путем подстановки констант и использования отрицания получите из нее конъюнкцию и дизъюнкцию.

15.9. Используя полином Жегалкина, перечислите все линейные функции от трех переменных. Задайте эти функции строкой значений.

15.10. Какие из функций класса L от двух переменных принадлежат классу T_0 ?

15.11. Какие из функций класса L от двух переменных принадлежат классу T_1 ?

15.12. Какие из функций класса L от двух переменных принадлежат классу S ?

15.13. Докажите, что для любой булевой функции $f(x, y)$ функция $f(x, x)$, полученная подстановкой $y = x$, является линейной.

15.14. Приведите пример нелинейной функции от трех переменных, в которой отождествлением двух переменных можно получить только нелинейную функцию.

15.15. Приведите пример нелинейных функций, из которых композицией можно получить нелинейную функцию.

15.16. Сколько функций $f(x_1, x_2, \dots, x_n)$ в классе L удовлетворяет условиям:

а) $f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 0$; б) $f(0, 0, \dots, 0) = 0, f(1, 1, \dots, 1) = 1$;

в) $f(0, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 0$; г) $f(1, 0, \dots, 0) = 1, f(1, 1, \dots, 1) = 1$?

15.17. Покажите, что для функции $f(x_1, x_2, \dots, x_n)$ из класса L можно построить функцию $g(x_1, x_2, \dots, x_{n+1})$ из класса L , так что $g(x_1, x_2, \dots, x_n, 0) = f(x_1, x_2, \dots, x_n)$.

15.18. Приведите пример нелинейной мажоритарной функции.

15.19. Докажите, что существует единственная линейная мажоритарная функция от трех переменных.

15.20. Докажите, что функция, двойственная линейной функции, является линейной.

15.21. Дана линейная функция $f(x, y)$. Какие из следующих функций являются линейными:

а) $f(x, y) \oplus z$; б) $f(x, y) \oplus \bar{z}$; в) $f(x, y) \wedge z$; г) $f(x, y) \wedge \bar{z}$;

д) $f(x, y) \vee z$; е) $f(x, y) \rightarrow z$; ж) $f(x, y) \leftrightarrow z$; з) $\overline{f(x, y)}$?

§ 16. Класс монотонных функций

Набор булевых переменных $\alpha = (\alpha_1, \dots, \alpha_n)$ предшествует набору булевых переменных $\beta = (\beta_1, \dots, \beta_n)$, если $\alpha_i \leq \beta_i$ для любого i . Обозначение $\alpha < \beta$. Например, $(0, 1, 0, 0) < (1, 1, 1, 0)$. Обращаем внимание на корректное употребление этого понятия. Например, набор $\alpha = (1, 0, 1)$ не предшествует набору $\beta = (1, 0, 0)$, но $\beta < \alpha$. Набор $\alpha = (1, 0, 1)$ не предшествует набору $\beta = (0, 1, 1)$, т.к. эти наборы несравнимы по данному определению.

Функция $f(x_1, x_2, \dots, x_n)$ называется *монотонной*, если для любых двух наборов α и β переменных, удовлетворяющих условию $\alpha < \beta$, выполняется неравенство $f(\alpha) \leq f(\beta)$. Множество всех монотонных функций обозначается M и образует функционально замкнутый класс.

Для двух переменных все наборы значений аргументов можно упорядочить следующим образом: $(0,0) < (0,1) < (1,1)$ и $(0,0) < (1,0) < (1,1)$, но два набора $(0,1)$ и $(1,0)$ не являются упорядоченными. Для соответствующих значений монотонной функции должно быть

$$f(0,0) \leq f(0,1) \leq f(1,1) \text{ и } f(0,0) \leq f(1,0) \leq f(1,1).$$

Для значений функции на наборах $(0,1)$ и $(1,0)$ не накладывается ограничений.

Таблица 47

x	y	f_0	f_1	f_3	f_5	f_7	f_{15}
0	0	0	0	0	0	0	1
0	1	0	0	0	1	1	1
1	0	0	0	1	0	1	1
1	1	0	1	1	1	1	1

Класс монотонных функций \mathcal{M} от двух переменных состоит из функций (таблица 47):

$$f_0(x, y) = 0, f_1(x, y) = x \wedge y,$$

$$f_3(x, y) = x, f_5(x, y) = y,$$

$$f_7(x, y) = x \vee y, f_{15}(x, y) = 1.$$

Число монотонных функций для различных значений n :

$$|M_1| = 3, |M_2| = 6, |M_3| = 20, |M_4| = 168, |M_5| = 7581, |M_6| = 7828354.$$

Изображение куба с наклоном (рис. 38) позволяет наглядно представить упорядоченные тройки булевых векторов, т.е. все цепи на поверхности куба, соединяющие две противоположные вершины и изучать монотонные булевы функции от трех переменных:

$$(0,0,0) < (0,0,1) < (0,1,1) < (1,1,1), (0,0,0) < (0,0,1) < (1,0,1) < (1,1,1),$$

$$(0,0,0) < (0,1,0) < (0,1,1) < (1,1,1), (0,0,0) < (0,1,0) < (1,1,0) < (1,1,1),$$

$$(0,0,0) < (1,0,0) < (1,0,1) < (1,1,1), (0,0,0) < (1,0,0) < (1,1,0) < (1,1,1).$$

В этом случае необходимо выполнить 12 проверок неравенств для значений функции, т.к. некоторые из приведенных выше условий повторяются.

Применим метод половинного деления для упрощения проверки функции на монотонность [3, с. 76].

Пусть функция $f(x_1, \dots, x_n)$ задана вектором значений $f = (f_0, f_1, \dots, f_{2^n-1})$. Разделим вектор f на две части одинаковой длины:

$$f^1 = (f_0, f_1, \dots, f_{2^{n-1}-1}) \text{ и}$$

$$f^2 = (f_{2^{n-1}}, f_{2^{n-1}+1}, \dots, f_{2^n-1}).$$

Если упорядочивание $f^1 < f^2$ не выполнено, то функция не является монотонной. Если упорядочивание выполняется, то разделим каждый вектор f^1 и f^2 на пары векторов одинаковой длины и аналогично проверим упорядочивание для каждой новой пары. Аналогично, продолжим разбиения и проверку. Если отно-

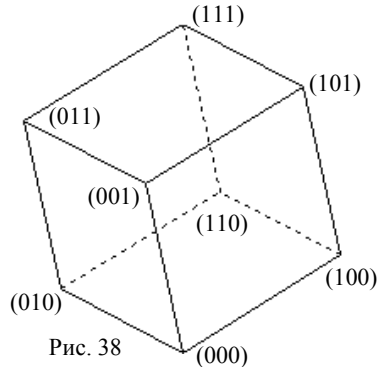


Рис. 38

шения предшествования для значений функции будут выполняться для всех соответствующих пар, то функция будет монотонной. Для проверки предшествования нужно первую половину вектора сдвинуть на вторую половину вектора и сравнить соответствующие координаты.

Например, для функции трех переменных, заданной вектором значений $(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)$, нужно проверить условия: $f_0 \leq f_1, f_2 \leq f_3, f_4 \leq f_5, f_6 \leq f_7, (f_0, f_1) \prec (f_2, f_3), (f_4, f_5) \prec (f_6, f_7), (f_0, f_1, f_2, f_3) \prec (f_4, f_5, f_6, f_7)$.

В этом случае необходимо выполнить 12 проверок неравенств для значений функции.

Лемма о немонотонной функции. Если функция $f(x_1, x_2, \dots, x_n)$ немонотонная, то подстановкой констант из этой функции можно получить отрицание.

Доказательство. Для немонотонной функции $f(x_1, x_2, \dots, x_n)$ существует два набора $\alpha = (\alpha_1, \dots, \alpha_n)$ и $\beta = (\beta_1, \dots, \beta_n)$, такие, что $\alpha \prec \beta$, но $f(\alpha) > f(\beta)$, т.е. $f(\alpha) = 1, f(\beta) = 0$.

Пусть наборы α и β являются соседними, т.е. отличаются одной координатой. Например, $\alpha = (\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n), \beta = (\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n)$, тогда $f(\alpha_1, \dots, \alpha_{i-1}, x_i, \alpha_{i+1}, \dots, \alpha_n) = \bar{x}_i$.

Пусть наборы α и β не являются соседними, и пусть они отличаются k координатами. Без ограничения общности можно считать, что они отличаются первыми k координатами, т.е. $\alpha = (0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n), \beta = (1, \dots, 1, \alpha_{k+1}, \dots, \alpha_n)$.

Построим упорядоченную цепочку векторов, в которой каждый вектор отличается от соседних векторов ровно одной координатой:

$$(0, 0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n) \prec (1, 0, 0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n) \prec (1, 1, 0, 0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n) \prec \dots \prec (1, 1, 1, 0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n) \prec \dots \prec (1, 1, 1, \dots, 1, \alpha_{k+1}, \dots, \alpha_n).$$

На каждом векторе цепочки вычислим значение функции. Поскольку на первом векторе $(0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n)$ значение функции равно 1, а на последнем векторе $(1, \dots, 1, \alpha_{k+1}, \dots, \alpha_n)$ значение равно 0, то найдется два соседних вектора, отличающихся одной координатой (например, x_i), причем на предшествующем векторе $(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_{k+1}, \dots, \alpha_n)$ значение функции равно 1, а на последующем векторе $(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_{k+1}, \dots, \alpha_n)$ равно 0. В этом случае подстановкой констант $x_1 = \alpha_1, \dots, x_{i-1} = \alpha_{i-1}, x_{i+1} = \alpha_{i+1}, \dots, x_n = \alpha_{n-1}$ получим отрицание $f(\alpha_1, \dots, \alpha_{i-1}, x_i, \alpha_{i+1}, \dots, \alpha_n) = \bar{x}_i$.

Пример 1. Покажите, что следующие функции немонотонные, и получите из них отрицания:

а) $f(x, y, z, t) = x \oplus y \oplus z \oplus t$; б) $f(x, y, z, t) = x \rightarrow (y \rightarrow (z \rightarrow t))$.

Решение. а) Используя определение операции сложения по модулю 2, можно легко найти два соседних набора $\alpha = (0, 1, 0, 0)$ и $\beta = (1, 1, 0, 0)$, для которых

$\alpha < \beta$ и $f(\alpha) = 1, f(\beta) = 0$. Следовательно, функция $x \oplus y \oplus z \oplus t$ не является монотонной, причем $f(x, 1, 0, 0) = \bar{x}$. Кстати $f(x, 1, 0, 0) = x \oplus 1 = \bar{x}$.

Следует заметить, что отрицание можно получить из данной функции подстановкой констант вместо других переменных.

б) Рассмотрим два набора $\alpha = (0, 0, 0, 0)$ и $\beta = (1, 1, 1, 0)$, для которых $\alpha < \beta$ и $f(\alpha) = 1, f(\beta) = 0$.

Построим цепочку возрастающих векторов:

$$(0, 0, 0, 0) < (1, 0, 0, 0) < (1, 1, 0, 0) < (1, 1, 1, 0).$$

Вычисляем значения функции на векторах

$$f(0, 0, 0, 0) = 1, f(1, 0, 0, 0) = 1, f(1, 1, 0, 0) = 1, f(1, 1, 1, 0) = 0.$$

Выделим два соседних набора $(1, 1, 0, 0)$ и $(1, 1, 1, 0)$, на которых нарушается определение монотонности функции. Получим отрицание $f(1, 1, z, 0) = \bar{z}$.

$$\text{Кстати, } f(1, 1, z, 0) = 1 \rightarrow (1 \rightarrow (z \rightarrow 0)) = 1 \rightarrow (1 \rightarrow \bar{z}) = 1 \rightarrow \bar{z} = \bar{z}. \square$$

Пример 2. Среди следующих функций $f_1 = (01010101)$, $f_2 = (01010101)$, $f_3 = (00001111)$ определить монотонные функции. Для немонотонной функции получить отрицание.

Таблица 48

x	y	z	f_1	f_2	f_3
0	0	0	0	0	1
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	1	1	0

Решение.

а) Монотонность функции f_1 проверяется легко. Если булева функция принимает равные значения на двух наборах (даже если первый из двух наборов не предшествует второму набору), определение монотонности для этих наборов выполняется.

Расположение наборов переменных в таблице 48 таково, что каждый набор либо предшествует любому набору, расположенному ниже в таблице, либо не связан отношением “предшествовать” с ним. Но набор переменных, расположенный ниже, не предшествует набору, расположенному выше.

При движении по столбцу значений функции f_1 сверху вниз булева функция не убывает.

б) Если при движении по столбцу значений сверху вниз значения функции изменяются с 1 на 0, то появляется гипотеза, что определение монотонности нарушается, либо на этих наборах не нужно проверять определение монотонности, т.к. первый из двух рассматриваемых наборов не предшествует второму набору. Вначале кажется, что функция f_2 не является монотонной, т.к. неравенство $f(\alpha) \leq f(\beta)$ нарушается при переходе со второго набора к третьему, с четвертого набора к пятому, с шестого набора к седьмому, кстати от второго набора к пятому и т.д. Но можно ли применять определение монотонной функции к второму и третьему наборам? Набор (001) не предшествует набору (010), поэтому не нужно сравнивать значения $f(0, 0, 1)$ и $f(0, 1, 0)$. Аналогично убеждаемся, что и для остальных пар не нужно сравнивать значения функции. Таким образом, данная функция является монотонной.

Второй способ определения монотонности функции f_2 .

Из таблицы легко заметить, что $f_2(x, y, z) = z$, тогда:

– для любых двух наборов $(x_1, y_1, 0)$ и $(x_2, y_2, 0)$ выполняется равенство $f_2(x_1, y_1, 0) = 0 = f_2(x_2, y_2, 0)$;

– для любых двух наборов $(x_1, y_1, 1)$ и $(x_2, y_2, 1)$ выполняется равенство $f_2(x_1, y_1, 1) = 1 = f_2(x_2, y_2, 1)$;

– для любых двух наборов $(x_1, y_1, 0)$ и $(x_2, y_2, 1)$ выполняется неравенство $f_2(x_1, y_1, 0) < f_2(x_2, y_2, 1)$.

Таким образом, для любых двух наборов выполняется определение монотонности для функции f_2 .

в) Функция f_3 не монотонная, т.к. $(0, 0, 0) \prec (0, 1, 0)$, но $f(0, 1, 0) > f(0, 0, 0)$.

Два набора $(0, 0, 0)$ и $(0, 1, 0)$ отличаются второй координатой, поэтому, сравнивая значения функции на этих наборах, получаем $f(0, y, 0) = \bar{y}$. Наборы $(0, 0, 0)$ и $(1, 0, 0)$ отличаются первой координатой, поэтому $f(x, 0, 0) = \bar{x}$. Аналогично получаем отрицания переменных $f(x, 1, 1) = \bar{x}$, $f(1, y, 1) = \bar{y}$.

Задачи.

16.1. Докажите, что функция $f(x_1, x_2, \dots, x_n)$, равная одной из переменных, является монотонной.

16.2. Докажите, что функция $f(x_1, x_2, \dots, x_n)$, равная отрицанию одной из переменных, не является монотонной.

16.3. Какие из следующих функций являются монотонными:

- а) $x \vee y \vee z$; б) (01010101) ; в) xuz ;
г) (0001000100110011) ; д) $x \oplus y \oplus z$.

16.4. Какие из функций класса M от двух переменных принадлежат классу: а) T_0 ; б) T_1 ; в) L ; г) S ?

16.5. Функция $f(x_1, x_2, x_3)$ является конъюнкцией любого числа переменных (без отрицаний переменных):

а) перечислите элементы носителя функции, если функция является второй переменной;

б) перечислите элементы носителя функции, если функция является конъюнкцией первой и третьей переменной;

в) докажите, что конъюнкция любого числа переменных является монотонной функцией.

16.6. Докажите, что монотонными являются те и только те функции, которые являются константами 0 или 1 либо допускают представление в виде ДНФ без инверсий.

16.7. Дана функция $((x \leftrightarrow y) \rightarrow (\bar{y} \leftrightarrow z)) \vee (x \rightarrow z)$. Определить, будет ли эта функция монотонной, самодвойственной и составить для нее полином Жегалкина.

16.8. Покажите, что функция $f = (11110101)$ не является монотонной. Подстановкой констант получите из нее отрицание.

16.9. Приведите пример функций, которые не являются монотонными, но из которых путем композиции можно получить монотонную функцию.

16.10. Сколько функций $f(x_1, x_2, x_3)$ в классе M удовлетворяет условиям:

а) $f(0,0,0) = 0, f(1,1,1) = 0$; б) $f(0,0,0) = 0, f(1,1,1) = 1$;

в) $f(0,0,0) = 1, f(1,1,1) = 1$; г) $f(1,0,0) = 1, f(1,1,1) = 1$?

16.11. Функция от трех переменных $f(x, y, z) = (f_0 f_1 \dots f_7)$ является монотонной. Докажите, что функция от четырех переменных $g(x, y, z, t) = (f_0 f_1 \dots f_7 f_0 f_1 \dots f_7)$, полученная из функции f повторной записью ее значений, также является монотонной. Какую фиктивную переменную содержит эта функция?

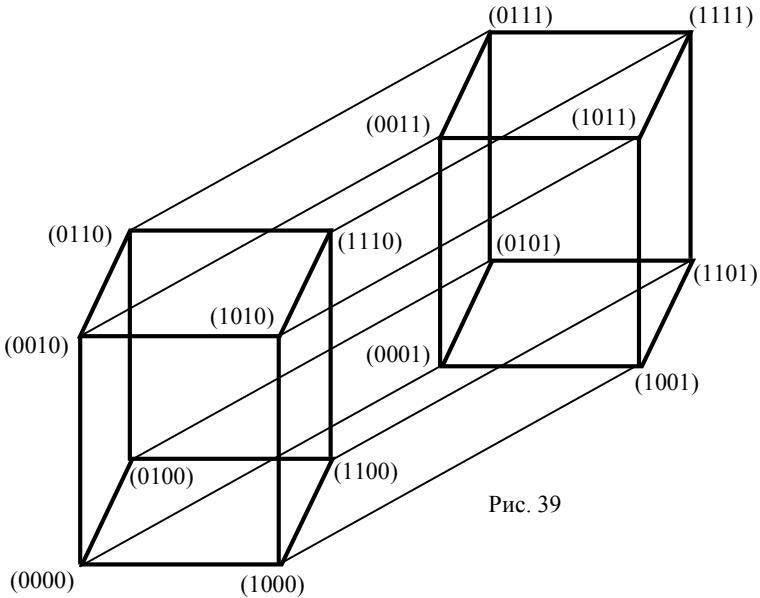


Рис. 39

16.12. На рис. 39 изображен четырехмерный куб и указаны координаты вершин. Приведите пример цепи, т.е. последовательности вершин, от вершины (0000) к вершине (1111), в которой каждая вершина, за ис-

ключением последней вершины, предшествует последующей вершине. Задайте несколько монотонных функций от четырех переменных.

16.13. Приведите пример мажоритарной функции f , удовлетворяющей условию: а) $f \in M$; б) $f \notin M$.

16.14. Дана монотонная функция $f(x, y)$. Какие из следующих функций являются монотонными:

- а) $f(x, y) \wedge z$; б) $f(x, y) \wedge \bar{z}$; в) $f(x, y) \vee z$; г) $f(x, y) \rightarrow z$;
 д) $f(x, y) \oplus z$; е) $f(x, y) \leftrightarrow z$; ж) $\overline{f(x, y)}$?

16.15. Функция $f(x, y, z)$ принадлежит одному из следующих классов: а) T_0 ; б) T_1 ; в) L ; г) S ; д) M . Принадлежит ли этому классу функция $f(x, y, const)$ от двух переменных?

§ 17. Множество симметричных функций

В некоторых матричных задачах психологических тестов предлагается девять квадратов (клеток) размером 3×3 , т.е. матрица третьего порядка. В каждой клетке имеется определенный узор из некоторого набора элементов.

Вдоль строк и вдоль столбцов матрицы нужно обнаружить определенную зависимость узоров. Правая, нижняя клетка является пустой, в которую нужно записать результат. Задача решающего – обнаружить закономерность в двух данных полных строках и в двух данных полных столбцах и заполнить узор в пустую клетку так, чтобы он оказался логическим завершением последовательности вдоль строки и вдоль столбца, на пересечении которых она находится.

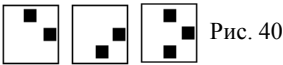


Рис. 40

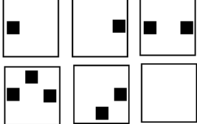


Рис. 41

A	B	$A \vee B$
C	D	$C \vee D$
$A \vee C$	$A \vee D$	

Рассмотрим квадраты в первой и второй полных строках (рис. 40). Третий столбец этой матрицы получается при наложении первого и второго столбцов.

Рассмотрим квадраты в первом и втором полных столбцах. Последняя строка также получается при наложении первой и второй строк. Получаем правило построения зависимости: элемент в результирующей клетке встречается в том и только в том случае, если он содержится, по крайней мере, в одной из двух клеток. Но это дизъюнкция двух высказываний, зашифрованных узором. Обозначим дизъюнкцию двух высказываний A и B через $A \vee B$ (рис. 41).

Обозначим содержание квадратов матрицы второго порядка, расположенной в верхнем левом углу, через A, B, C, D . Эту матрицу в дальнейшем будем называть основной. Используя найденную зависимость для третьего столбца, получим результат для пустой клетки $(A \vee B) \vee (C \vee D)$. Применяя полученную

зависимость для третьей строки, получаем результат $(A \vee C) \vee (B \vee D)$, $(A \vee C) \vee (B \vee D)$. Используя законы логики, получаем равносильность формул.

Рассмотрим следующую матричную задачу (рис. 42). Принцип построения зависимости: элемент принадлежит результирующему квадрату тогда и только тогда, когда он принадлежит каждому из двух рассматриваемых квадратов. Это конъюнкция данных высказываний AB , зашифрованных узором.

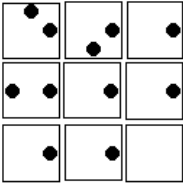


Рис. 42

A	B	AB
C	D	CD
AC	BD	

Рис. 43

Получаем матрицу с элементами (рис. 43). Используя полученную зависимость, получаем два выражения $(AB)(CD)$ и $(AC)(BD)$ для пустой клетки, которые равносильны.

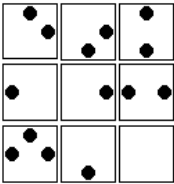


Рис. 44

A	B	$A \oplus B$
C	D	$C \oplus D$
$A \oplus C$	$B \oplus D$	

Рис. 45

Для матричной задачи (рис. 44) замечаем, что общие элементы на одинаковых местах в обоих квадратах отбрасываются. Элементы уникальные для каждой клетки, т.е. которые встречаются только в одной клетке, остаются. Если наличие символа в квадрате обозначим 1, а отсутствие символа через 0, получаем сумму по модулю 2 (рис. 45), т.е. $A \oplus B: 1 \oplus 1 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 0 \oplus 0 = 0$. Для пустой клетки получаем выражения $(A \oplus B) \oplus (C \oplus D)$ и $(A \oplus C) \oplus (B \oplus D)$. По таблице истинности убеждаемся в равносильности формул.

Для матрицы (рис. 46) замечаем, что результирующий столбец (строка) является отрицанием первого рассмотренного столбца (строки), т.е. $f(A, B) = \bar{A}$. Получаем матрицу (рис. 47). Определите содержание девятого столбца, перемещаясь в двух направлениях.

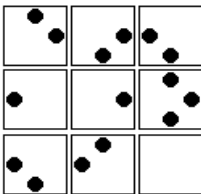


Рис. 46

A	B	\bar{A}
C	D	\bar{C}
\bar{A}	\bar{B}	

Рис. 47

Для матричной задачи (рис. 48) замечаем, что элемент в результирующем квадрате встречается тогда и только тогда, когда он либо отсутствует в обоих квадратах, либо он встречается в обоих квадратах, т.е. получаем равносильность в матрице (рис. 49).

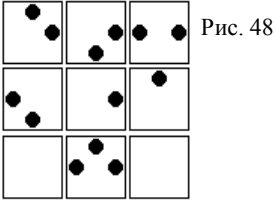


Рис. 48

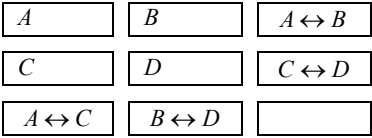


Рис. 49

Заполняя по вертикали, получаем $(A \leftrightarrow B) \leftrightarrow (C \leftrightarrow D)$.

Заполняя по горизонтали, получаем $(A \leftrightarrow C) \leftrightarrow (B \leftrightarrow D)$.

Равносильность формул следует из равенств

$$\begin{aligned} (A \leftrightarrow B) \leftrightarrow (C \leftrightarrow D) &= (A \oplus B \oplus 1) \oplus (C \oplus D \oplus 1) \oplus 1 = \\ &= A \oplus B \oplus C \oplus D \oplus 1 \oplus 1 = A \oplus B \oplus C \oplus D = \\ &= A \oplus C \oplus B \oplus D \oplus 1 \oplus 1 = (A \oplus C \oplus 1) \oplus (B \oplus D \oplus 1) \oplus 1 = (A \leftrightarrow C) \leftrightarrow (B \leftrightarrow D). \end{aligned}$$

Психологический тест подразумевает коммутативность диаграммы, т.е.

$$f(f(A,B), f(C,D)) = f(f(A,C), f(B,D)). \tag{1}$$

Теорема 1. Десять булевых функций $f_0(A,B) = 0$, $f_1(A,B) = AB$, $f_3(A,B) = A$, $f_5(A,B) = B$, $f_6(A,B) = A \oplus B$, $f_7(A,B) = A + B$, $f_9(A,B) = A \leftrightarrow B$, $f_{10}(A,B) = \bar{B}$, $f_{12}(A,B) = \bar{A}$, $f_{15}(A,B) = 1$ удовлетворяют условию (1).

Множество функций, удовлетворяющих этому условию, обозначим **K**.

Функция называется *симметричной*, если при любой перестановке в наборе аргументов она сохраняет значение. Класс симметричных булевых функций обозначим *Sim*. Для функции от двух аргументов достаточно потребовать выполнения равенства $f(0,1) = f(1,0)$.

Распределение функций от двух переменных по классам и множествам представлено в таблице 49.

Таблица 49

Функции \ Классы	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
T_0	+	+	+	+	+	+	+	+								
T_1		+		+		+		+		+		+		+		+
S				+		+					+		+			
M	+	+		+		+		+								+
L	+			+		+	+			+	+		+			+
Sim	+	+					+	+	+	+					+	+
K	+	+		+		+	+	+		+	+		+			+

Классы *Sim* и *K* отделены пустой строкой таблицы по той причине, что они не образуют функционально замкнутые классы. Классы T_0 , T_1 , S , M , L играют важную роль в дискретной математике.

Пересечение функционально замкнутых классов дано в таблице 50.

Таблица 50

\cap	T_0	T_1	L	S	M
T_0	$0, x, y, xy,$ $x \vee y, x \oplus y$ $\overline{x \rightarrow y}, \overline{y \rightarrow x}$	$x, y, xy, x \vee y$	$0, x, y$	x, y	$0, x, y, xy,$ $x \vee y$
T_1	$x, y, xy, x \vee y$	$x, y, xy, x \vee y$ $x \rightarrow y, y \rightarrow x$ $x \leftrightarrow y, 1$	$x, y, x \leftrightarrow y, 1$	x, y	$x, y, xy,$ $x \vee y, 1$
L	$0, x, y$	$x, y, x \leftrightarrow y, 1$	$0, x, y, \bar{x}, \bar{y},$ $x \oplus y, x \leftrightarrow y, 1$	x, y, \bar{x}, \bar{y}	$0, x, y, 1$
S	x, y	x, y	x, y, \bar{x}, \bar{y}	x, y, \bar{x}, \bar{y}	x, y
M	$0, x, y, xy,$ $x \vee y$	$x, y, xy,$ $x \vee y, 1$	$0, x, y, 1$	x, y	$0, x, y, xy,$ $x \vee y, 1$

Задачи.

17.1. Используя логические операции, найдите закономерность в следующих матричных задачах и заполните пустые клетки. Проверьте найденную закономерность по столбцам и по строкам.

а

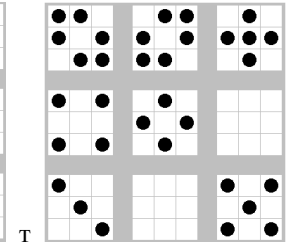
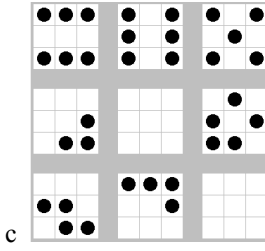
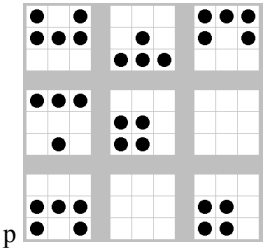
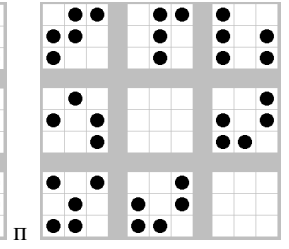
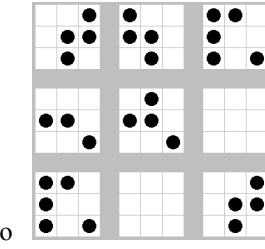
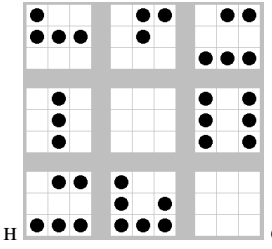
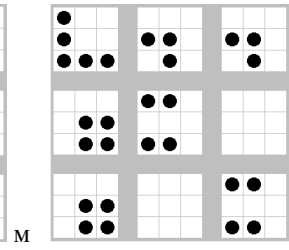
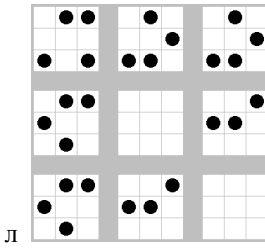
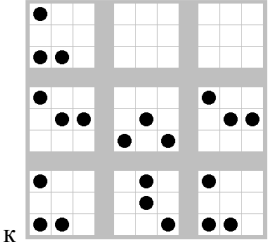
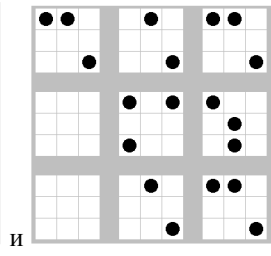
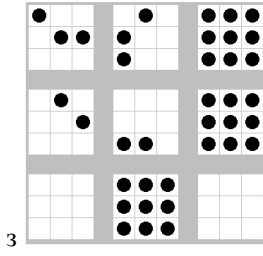
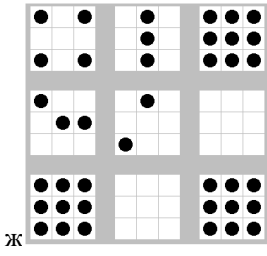
б

в

г

д

е



§ 18. Множество функций T_{k0} и $T_{>k0}$

Рассмотрим функции от трех переменных $f(x, y, z)$.

Функция называется принадлежащей множеству T_{10} , если на любом наборе переменных, содержащем ровно одно нулевое значение, функция принимает нулевое значение.

Для функции трех переменных получаем информацию о значениях функции (таблица 51).

Кодируя значения функции на всех наборах строкой, получаем $f(x, y, z) = (, , , 0, , 0, 0,)$. Используя значения 0 или 1, пять свободных разрядов можно заполнить 2^5 способами, поэтому множество функций T_{10} содержит 32 функции.

Таблица 51

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x, y, z)$				0		0	0	

Функция называется принадлежащей множеству T_{20} , если на любом наборе переменных, содержащем ровно два нулевых значения, функция принимает нулевое значение.

Для функции трех переменных получаем информацию о значениях функции (таблица 52).

Таблица 52

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x, y, z)$		0	0		0			

Кодируя значения функции на всех наборах строкой, получаем $f(x, y, z) = (, 0, 0, , 0, , ,)$. Используя значения 0 или 1, пять свободных разрядов можно заполнить 2^5 способами, поэтому множество функций T_{20} тоже

содержит 32 функции.

Функция называется принадлежащей множеству T_{30} , если на любом наборе переменных, содержащем ровно три нулевых значения, функция принимает нулевое значение.

Таблица 53

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x, y, z)$	0							

Для функции трех переменных получаем информацию о значениях функции (таблица 53).

Получаем значения функции на всех наборах $f(x, y, z) = (0, , , , , ,)$. Используя значениями 0 или 1, семь свободных разрядов можно заполнить 2^7 способами, поэтому множество функций T_{30} содержит 128 функций. Очевидно, что множество T_{30} – это класс T_0 .

Функция называется принадлежащей множеству $T_{\geq 20}$, если на любом наборе переменных, содержащем хотя бы два нулевых значения, функция принимает нулевое значение.

Для функции трех переменных получаем информацию о значениях функции (таблица 54).

Таблица 54

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x,y,z)$	0	0	0		0			

Кодируя значения функции на всех наборах строкой, получаем $f(x,y,z)=(0,0,0,0,0,0,0,0)$. Используя значения 0 или 1, четыре свободных разряда можно заполнить 2^4 способами, поэтому множество функций $T_{\geq 20}$

содержит 16 функций.

Функция называется принадлежащей множеству $T_{\geq 10}$, если на любом наборе переменных, содержащем хотя бы одно нулевое значение, функция принимает нулевое значение.

Таблица 55

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x,y,z)$	0	0	0	0	0	0	0	

Для функции трех переменных получаем информацию о значениях функции (таблица 55). Получаем значения функции на всех наборах $f(x,y,z)=(0,0,0,0,0,0,0,0)$. Используя значениями 0 или 1, один свободный разряд можно заполнить двумя способами, поэтому множество функций $T_{\geq 10}$

содержит 2 функции: 0 и XYZ.

В таблице 56 перечислены все функции этого класса.

Таблица 56

000	001	010	011	100	101	110	111	$f(x,y,z)$
$\overline{x}\overline{y}\overline{z}$	$\overline{x}\overline{y}z$	$\overline{x}y\overline{z}$	$\overline{x}yz$	$x\overline{y}\overline{z}$	$x\overline{y}z$	$xy\overline{z}$	xyz	
0	0	0	0	0	0	0	0	f_0
0	0	0	1	0	0	0	0	f_{16}
0	0	0	0	0	1	0	0	f_4
0	0	0	1	0	1	0	0	f_{20}
0	0	0	0	0	0	1	0	f_2
0	0	0	1	0	0	1	0	f_{18}
0	0	0	0	0	1	1	0	f_6
0	0	0	1	0	1	1	0	f_{22}
0	0	0	0	0	0	0	1	f_1
0	0	0	1	0	0	0	1	f_{17}
0	0	0	0	0	1	0	1	f_5
0	0	0	1	0	1	0	1	f_{21}
0	0	0	0	0	0	1	1	f_3
0	0	0	1	0	0	1	1	f_{19}
0	0	0	0	0	1	1	1	f_7
0	0	0	1	0	1	0	1	f_{23}

Используя совершенную дизъюнктивную нормальную форму, получаем $f_0(x,y,z) = 0$, $f_2 = xy\overline{z}$, $f_4 = x\overline{y}z$,

$$\begin{aligned}
f_{20} &= \overline{xyz} \vee x\overline{y}z = (\overline{xy} \vee x\overline{y})z = (x \oplus y)z, \\
f_{18} &= \overline{xyz} \vee xy\overline{z} = (\overline{xz} \vee x\overline{z})y = (x \oplus z)y, \\
f_6 &= x\overline{yz} \vee xy\overline{z} = x(\overline{yz} \vee y\overline{z}) = x(y \oplus z), \\
f_{22} &= \overline{xyz} \vee x\overline{y}z \vee xy\overline{z}, \quad f_1 = xyz, \quad f_{17} = \overline{xyz} \vee xyz = (\overline{x} \vee x)yz = yz, \\
f_5 &= x\overline{yz} \vee xy\overline{z} = xz(\overline{y} \vee y) = xz, \\
f_{21} &= \overline{xyz} \vee x\overline{y}z \vee xy\overline{z} = (\overline{xyz} \vee xy\overline{z}) \vee (x\overline{y}z \vee xy\overline{z}) = yz \vee xz = (x \vee y)z, \\
f_3 &= xy\overline{z} \vee xyz = xy(\overline{z} \vee z) = xy, \\
f_{19} &= \overline{xyz} \vee xy\overline{z} \vee xyz = (\overline{xyz} \vee xyz) \vee (xy\overline{z} \vee xyz) = yz \vee xy = (x \vee z)y, \\
f_7 &= x\overline{yz} \vee xy\overline{z} \vee xyz = (x\overline{yz} \vee xyz) \vee (xy\overline{z} \vee xyz) = xz \vee xy = x(y \vee z), \\
f_{23} &= \overline{xyz} \vee x\overline{y}z \vee xy\overline{z} \vee xyz = (\overline{xyz} \vee xyz) \vee (x\overline{y}z \vee xyz) \vee (xy\overline{z} \vee xyz) = xy \vee yz \vee xz.
\end{aligned}$$

Задачи.

18.1. Приведите примеры функций, заданных формулой, из следующих множеств: а) T_{10} ; б) T_{20} ; в) T_{30} ; г) $T_{\geq 20}$.

18.2. Являются ли следующие множества замкнутыми классами:

а) T_{10} ; б) T_{20} ; в) T_{30} ; г) $T_{\geq 20}$?

§ 19. Полные системы функций

Система булевых функций $\{f_1, f_2, \dots, f_m\}$ называется полной, если любая булева функция может быть выражена через функции f_1, f_2, \dots, f_m с помощью суперпозиций, т.е. составления сложных высказываний:

а) переименованием некоторой переменной $f = f_i(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_k)$, где y может совпасть с любой переменной,

б) подстановкой какой-либо из функций вместо какой-нибудь переменной $f = f_i(x_1, \dots, x_{i-1}, f_j(x_1, \dots, x_k), x_{i+1}, \dots, x_k)$.

Пример. Следующая система функций $\{\overline{}, \wedge, \vee\}$ является полной.

Теорема 1. Если система функций $\{f_1, f_2, \dots, f_m\}$ полная, и любая из функций f_1, f_2, \dots, f_m может быть выражена с помощью суперпозиции через функции g_1, \dots, g_r , то система $\{g_1, \dots, g_r\}$ также полная.

Теорема 2. Следующие системы функций являются полными:

а) $\{\overline{}, \vee\}$; б) $\{\overline{}, \wedge\}$; в) $\{\overline{}, \rightarrow\}$; г) $\{\oplus, \wedge, 1\}$.

Доказательство. а) Из теорем о возможности представления любой функции в СДНФ следует, что с помощью операций $\overline{}, \wedge, \vee$ можно выразить любую булеву функцию, т.е. эта система функций полна.

б) Пусть $f_1 = \overline{}$, $f_2 = \wedge$, $f_3 = \vee$, $g_1 = \overline{}$, $g_2 = \vee$, тогда $f_1 = g_1$, $f_2(x, y) = x \wedge y = \overline{\overline{x \vee y}} = g_2(g_1(x), g_1(y))$, $f_3 = g_2$. По теореме 1 система функций $\{\overline{}, \vee\}$ является полной.

Рассмотрите аналогично остальные случаи.

Система булевых функций Σ называется функционально *полной*, если любая булева функция представима в виде суперпозиции функций из Σ .

Теорема Поста. Система булевых функций Σ функционально полна тогда и только тогда, когда в Σ содержится хотя бы одна функция, не сохраняющая 0, хотя бы одна функция, не сохраняющая 1, хотя бы одна несамодвойственная функция, хотя бы одна нелинейная функция и хотя бы одна немонотонная функция.

Классы функций T_0, T_1, S, L, M являются неполными и попарно различными.

Таблица 57

f	T_0	T_1	S	L	M
$X \oplus Y$	+	-	-	+	-
$X \vee Y$	+	+	-	-	+
1	-	+	-	+	+

Пример. Докажите полноту системы функций $\{\oplus, \vee, 1\}$, используя теорему Поста.

Решение (таблица 57).

Будем использовать свойства функций классов

$$f \in T_0 \leftrightarrow f(0, 0, \dots, 0) = 0,$$

$$f \in T_1 \leftrightarrow f(1, 1, \dots, 1) = 1,$$

$$f \in S \leftrightarrow \overline{f(x_1, x_2, \dots, x_n)} = f(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}),$$

$$f \in L \leftrightarrow f = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n,$$

$$f \in M \leftrightarrow (\forall \alpha, \beta: \alpha < \beta \rightarrow f(\alpha) \leq f(\beta)).$$

Функция $f_3(x, y) = 1$ не принадлежит классу T_0 , т.к. $f_3(0, 0) = 1$.

Функция $f_1(x, y) = x \oplus y$ не принадлежит классу T_1 , т.к. $f_1(1, 1) = 0$.

Таблица 58

x	y	$x \oplus y$	xy
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Функция $x \oplus y$ не принадлежит классу S , т.к. ее таблица истинности (таблица 58) не симметрична относительно средней линии.

Функция $f_2(x, y) = xy$ не принадлежит классу L .

Функция $x \oplus y$ не является монотонной, т.к. для наборов $(1, 0)$ и $(1, 1)$ выполняется упорядочивание $(1, 0) < (1, 1)$, но $f_2(1, 0) > f_2(1, 1)$. \square

Задачи.

19.1. Можно ли с помощью композиции из указанных функций получить все булевы функции?

$$f_1(x_1, x_2) = x_1 \oplus x_2, f_2(x_1, x_2) = x_1 \wedge x_2, f_3(x_1, x_2) = 1.$$

19.2. Можно ли любую формулу алгебры высказываний записать только через операции:

$$\text{а) } \rightarrow, \oplus, \text{ б) } \downarrow, \text{ в) } | \text{ ?}$$

19.3. Докажите, что через функцию $f = (1, 1, 1, 1, 0, 0, 0)$ можно выразить все булевы функции.

19.4. Докажите, что \rightarrow нельзя выразить через \wedge и \vee .

19.5. Можно ли произвольную булеву функцию $f(x, y)$ от двух переменных выразить через две булевы функции $g(x)$ и $h(y)$, используя только один раз логическую операцию в следующем виде:

$$\text{а) } f(x, y) = g(x) \wedge h(y); \text{ г) } f(x, y) = g(x) \rightarrow h(y);$$

- б) $f(x, y) = g(x) \vee h(y)$; д) $f(x, y) = g(x) \leftrightarrow h(y)$;
 в) $f(x, y) = g(x) \oplus h(y)$; е) $f(x, y) = g(x) \downarrow h(y)$?

§ 20. Предикаты. Кванторы общности и существования

Предикатом называется некоторое предложение, зависящее от переменных, которое превращается в высказывание при замене переменных на значения из заданного множества.

Пример 1. $P(x) : x$ – натуральное четное число;

$Q(x, y) : x, y$ – действительные числа и $x^2 + y^2 = 25$. \square

Точное определение предиката следующее.

Пусть M – произвольное множество. n -местным предикатом, заданным на множестве M , называется любая функция $P(x_1, \dots, x_n)$, отображающая n -ую степень M^n во множество $\{L, I\}$ (или $\{0, 1\}$). По определению все переменные у предиката называются свободными, а их количество – это местность предиката. Высказывание полагается 0-местным предикатом.

Предикат называется *тождественно истинным* на множестве M (*тождественно ложным*), если при любой подстановке вместо переменных x_1, \dots, x_n конкретных элементов из множества M он превращается в истинное (соответственно ложное) высказывание.

Предикат $P(x_1, \dots, x_n)$ называется *выполнимым* на множестве M (*опровержимым*), если существует такой набор значений переменных, при котором высказывание $P(x_1, \dots, x_n)$ истинно (соответственно ложно).

Пример 2. $P(x) = 1$ тогда и только тогда, когда $(x - 1)^2 > 0$. Если M – множество всех действительных чисел, то $P(x)$ – выполнимый предикат. Если же M – множество всех действительных чисел, кроме $x = 1$, то $P(x)$ – тождественно истинный предикат. \square

Областью истинности предиката $P(x_1, \dots, x_n)$ называется множество упорядоченных наборов $(a_1, \dots, a_n), a_i \in M$, для которых $P(a_1, \dots, a_n) = 1$. Аналогично определяется область ложности предиката. Для задания предиката достаточно задать область истинности или область ложности. При этом либо записывают область истинности как множество всех n -ок (x_1, \dots, x_n) , на которых $P(x_1, \dots, x_n) = 1$, либо указывают свойство, описывающее элементы x_i из этих n -ок.

Пример 3. $P(x, y) = \{(x, y) : x + y = 4; x, y \in R\}$,

$Q(x, y) = \{(x, y) : \lg(xy) = \lg x + \lg y; x, y \in R, x > 0, y > 0\}$.

Обычно это записывают в виде

$P(x, y) : x + y = 4; x, y \in R$;

$Q(x, y) : \lg(xy) = \lg x + \lg y; x, y \in R, x > 0, y > 0$. \square

Предикаты P и Q , заданные на одной и той же области M , называются *равносильными*, если они принимают одинаковые значения “истина-ложь” на одних и тех же значениях переменных из области M . Записывают это как $P \equiv Q$.

Пример 4. $P(x, y) : x + y = 4, x, y \in R$ и $Q(x, y) : \log_4(x + y) = 1, x, y \in R$.

Очевидно, что $P(x, y) \equiv Q(x, y)$. \square

Предикат $Q(x_1, \dots, x_n)$ называется *следствием* предиката $P(x_1, \dots, x_n)$, если для любых значений переменных (a_1, \dots, a_n) из того, что $P(a_1, \dots, a_n) = 1$ следует, что $Q(a_1, \dots, a_n) = 1$. Записывают это как $P \rightarrow Q$. Предикат P называется достаточным условием для предиката Q , а предикат Q необходимым условием для предиката P . Очевидно, что $P \equiv Q$ тогда и только тогда, когда $P \rightarrow Q$ и $Q \rightarrow P$.

Пример 5. $Q : x^2 - 5x + 6 = 0, x \in R$ и $P(x) : x - 2 = 0, x \in R$. Тогда $P \rightarrow Q$. Действительно, если разрешимо уравнение $x - 2 = 0$ (т.е. $P(x)$ принимает значение 1), то уравнение $x^2 - 5x + 6 = 0$ также разрешимо. \square

Так как предикаты, заданные на одной и той же области, при подстановке вместо переменных конкретных значений превращаются в высказывания, то на предикатах можно ввести логические операции: $\vee, \wedge, \rightarrow, \leftrightarrow, \neg$.

Пусть $P(x_1, \dots, x_n, y_1, \dots, y_m)$ – $(n + m)$ -местный предикат, а $Q(y_1, \dots, y_m, z_1, \dots, z_k)$ – $(m + k)$ -местный предикат. Под выражением $P \wedge Q$ понимается такой $(n + m + k)$ -местный предикат $R(x_1, \dots, x_n, y_1, \dots, y_m, z_1, \dots, z_k)$, который на наборе $(a_1, \dots, a_n, b_1, \dots, b_m, c_1, \dots, c_k)$ принимает значение 1 тогда и только тогда, когда $P(a_1, \dots, a_n, b_1, \dots, b_m) = 1$ и $Q(b_1, \dots, b_m, c_1, \dots, c_k) = 1$.

Аналогично определяются операции $\vee, \rightarrow, \leftrightarrow, \neg$.

Пример 6. Пусть на множестве целых чисел заданы предикаты: $P(x, y) : xy$ – четное число, $Q(y, z) : y + z$ – четное число.

Тогда $P(x, y) \vee Q(y, z)$ есть трехместный предикат $R(x, y, z)$, для которого $R(a, b, c) = 1$ тогда и только тогда, когда либо ab четно, либо $b + c$ четно.

В то же время, если $Q(x, y) : x + y$ – четное число, то $P(x, y) \vee Q(x, y)$ – двуместный предикат $R(x, y)$, для которого $R(a, b) = 1$ тогда и только тогда, когда ab или $a + b$ четные числа. \square

Пусть $P(x, x_1, \dots, x_n)$ – некоторый $(n + 1)$ -местный предикат, в котором выделена свободная переменная x . Под выражением $\forall x P(x, x_1, \dots, x_n)$ понимается такой n -местный предикат $R(x_1, \dots, x_n)$, который на наборе (a_1, \dots, a_n) принимает значение 1 тогда и только тогда, когда одноместный предикат $P(x, a_1, \dots, a_n)$ тождественно истинен. Знак \forall называется квантором общности. После его применения переменная x становится связанной (перестает быть свободной).

Под выражением $\exists x P(x, x_1, \dots, x_n)$ понимается такой n -местный предикат $R(x_1, \dots, x_n)$, который на наборе (a_1, \dots, a_n) принимает значение 0 тогда и только

тогда, когда предикат $P(x, a_1, \dots, a_n)$ тождественно ложный. Знак \exists называется квантором существования. После его применения переменная x становится также связанной.

Если $P(x)$ – одноместный предикат, то $\forall x P(x)$ и $\exists x P(x)$ – высказывания.

Пример 7. Пусть на множестве целых чисел заданы предикаты:

$P(x) : x$ – делится на 2, $Q(x) : x$ – делится на 5.

Тогда $P(x) \wedge Q(x)$ означает, что x делится и на 2, и на 5, т.е. делится на 10.

В таком случае $\forall x(P(x) \wedge Q(x))$ означает, что любое целое число делится на 10, т.е. это ложное высказывание. В то же время $\exists x(P(x) \wedge Q(x))$ – истинное высказывание, т.к. существует целое число x (например, 20), которое делится и на 2, и на 5. \square

В алгебре высказываний были введены логические операции, а затем определили формулы алгебры высказываний как сложные высказывания, полученные из простейших (переменных высказываний) с помощью введенных логических операций. Аналогично можно определить формулы логики предикатов:

1) Все высказывания и предикаты, заданные на области M , являются формулами;

2) Если A, B – формулы, в которых одна и та же переменная одновременно свободна или связана в A и B , то $A \vee B, A \wedge B, A \rightarrow B, A \leftrightarrow B, \bar{A}$ формулы, в которых связность-свобода переменных сохраняется;

3) Если $A(x)$ – некоторая формула, в которой выделена свободная переменная x , то $\forall x A(x)$ и $\exists x A(x)$ – формулы, в которых x – связанная переменная, связность-свобода остальных переменных остаются прежними.

В дальнейшем запись $P(x)$ означает, что эта формула зависит от каких-то переменных и выделенная переменная x свободна. Аналогично означает запись $Q(x, y)$.

Две формулы P и Q логики предикатов, заданные на области M , называются равносильными на области M , если они принимают одинаковые значения истинности на одних и тех же значениях переменных из M . Записывают как $P \equiv Q$. Две формулы называются просто равносильными, если они равносильны на любой области.

Очевидно, что все равносильности алгебры высказываний (коммутативность, дистрибутивность и т.п.) имеют место и в логике предикатов. Но здесь еще появляются дополнительные равносильности, связанные с введением операций \forall и \exists .

Пример 8.

$$\overline{\forall x P(x)} \equiv \exists x \overline{P(x)}. \quad (1)$$

Действительно, пусть левая часть при каком-то наборе значений переменных принимает значение I . Тогда $\forall x P(x) = I$, что означает $P(x) \equiv I$. Тогда $\overline{P(x)} \equiv \bar{I}$, а значит, $\exists x \overline{P(x)}$ принимает значение I .

Пусть теперь левая часть принимает значение I , т.е. $\forall x P(x) = I$. По определению тогда $P(x) \neq I$, т.е. $P(x_0) = L$ для некоторого x_0 . В таком случае $\overline{P(x_0)} \equiv I$, т.е. $P(x) \neq L$. Тогда $\exists x P(x) = I$. \square

Имеют место следующие равносильности:

$$\overline{\exists x P(x)} \equiv \forall x \overline{P(x)}; \quad (2)$$

$$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y); \quad (3)$$

$$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y); \quad (4)$$

$$\forall x (P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x)); \quad (5)$$

$$\exists x (P(x) \vee Q(x)) \equiv (\exists x P(x)) \vee (\exists x Q(x)); \quad (6)$$

$$\exists x (P(x) \wedge Q) \equiv (\exists x P(x)) \wedge Q; \quad (7)$$

$$\forall x (P(x) \wedge Q) \equiv (\forall x P(x)) \wedge Q; \quad (8)$$

$$\exists x (P(x) \vee Q) \equiv (\exists x P(x)) \vee Q; \quad (9)$$

$$\forall x (P(x) \vee Q) \equiv (\forall x P(x)) \vee Q. \quad (10)$$

В (7)–(10) переменная x свободна в $P(x)$, а в формуле Q переменная x не содержится.

$$\forall x P(x) \equiv \forall y P(y); \quad (11)$$

$$\exists x P(x) \equiv \exists y P(y). \quad (12)$$

Здесь $P(y)$ получается заменой переменной x на некоторую переменную y , которая в формулу $P(x)$ не входит.

Задачи.

20.1. Изобразите на координатной плоскости область истинности следующих предикатов $P(x, y)$:

а) $P(x, y) : x \leq 2$; б) $P(x, y) : \overline{x \leq 2}$; в) $P(x, y) : (x \leq 2) \vee (y \geq 1)$;

г) $P(x, y) : (x \leq 2) \wedge (y \geq 1)$; д) $P(x, y) : (y \geq 1) \rightarrow (x \leq 2)$;

е) $P(x, y) : (x \leq 2) \rightarrow (y \geq 1)$; ж) $P(x, y) : (x \leq 2) \leftrightarrow (y \geq 1)$;

з) $P(x, y) : (xy < 1) \rightarrow (x^2 + y^2 \leq 4)$;

и) $P(x, y) : (x < y) \vee (y > x^2 - 3x + 2)$.

20.2. На множестве действительных чисел заданы предикаты: $Z(x) : (x - \text{целое число})$ и $Q(x) : (x - \text{рациональное число})$.

Используя кванторы \exists , \forall и операцию отрицания $\overline{\quad}$, запишите формулой следующие высказывания и определите их истинность:

а) существует целое число, которое не является рациональным числом;

б) любое целое число является рациональным числом;

в) существует рациональное число, которое является целым числом;

г) не существует рациональное число, которое не является целым числом.

20.3. Аналогично доказательству равносильности (1), докажите равносильность (2) – (12).

20.4. Приведите пример двуместного предиката $P(x, y)$ такого, что $\forall x \exists y P(x, y) \neq \exists y \forall x P(x, y)$ (см. равносильности (3) и (4)).

20.5. Приведите пример одноместных предикатов $P(x)$ и $Q(x)$ таких, что:

а) $\forall x (P(x) \vee Q(x)) \neq (\forall x P(x)) \vee (\forall x Q(x))$;

б) $\exists x (P(x) \wedge Q(x)) \neq (\exists x P(x)) \wedge (\exists x Q(x))$

(см. равносильности (5) и (6)).

20.6. Пусть $P(x)$ – формула, в которой выделена свободная переменная x , а C – высказывание. Докажите следующие равносильности:

а) $C \rightarrow (\forall x P(x)) \equiv \forall x (C \rightarrow P(x))$;

б) $\forall x (P(x) \rightarrow C) \equiv (\exists x P(x)) \rightarrow C$;

в) $C \rightarrow (\exists x P(x)) \equiv \exists x (C \rightarrow P(x))$;

г) $\exists x (P(x) \rightarrow C) \equiv (\forall x P(x)) \rightarrow C$.

20.7. На множестве людей нашей планеты определен двуместный предикат $P(x, y)$: x старше y . Сформулируйте словесно следующие высказывания и определите их истинность:

а) $\forall x \exists y P(x, y)$; д) $\exists x \exists y P(x, y)$;

б) $\exists x \forall y P(x, y)$; е) $\exists y \exists x P(x, y)$;

в) $\forall y \exists x P(x, y)$; ж) $\forall x \forall y P(x, y)$;

г) $\exists y \forall x P(x, y)$; з) $\forall y \forall x P(x, y)$.

20.8. Приведите примеры различных уравнений с параметром a , удовлетворяющие следующему условию:

а) для любого значения параметра a существует решение уравнения ...;

б) существует значение параметра a , при котором уравнение ... не имеет решения;

в) существует значение параметра a , при котором любое число является решением уравнения ...;

г) для любого значения параметра a уравнение ... не имеет решений;

д) существует значение параметра a , при котором уравнение ... имеет два решения;

е) для любого значения параметра a любое число является решением уравнения ...

§ 21. Логические уравнения

Уравнение $a \oplus x = b$ имеет единственное решение $x = b \oplus a$.

Уравнение $a \leftrightarrow x = b$ имеет единственное решение:

$$x = \begin{cases} 1, & \text{если } a \leftrightarrow b, \\ 0, & \text{если } a \not\leftrightarrow b. \end{cases}$$

Уравнение $a \wedge x = b$ имеет решение $x = \begin{cases} b, & \text{если } a = 1, \\ 0 \text{ или } 1, & \text{если } a = 0, b = 0, \\ \emptyset, & \text{если } a = 0, b = 1. \end{cases}$

Уравнение $a \vee x = b$ имеет решение $x = \begin{cases} b, & \text{если } a = 0, \\ 0 \text{ или } 1, & \text{если } a = 1, b = 1, \\ \emptyset, & \text{если } a = 1, b = 0. \end{cases}$

Для уравнения $a \rightarrow x = b$ получаем решение

$$x = \begin{cases} 0 \text{ или } 1, & \text{если } a = 0, b = 1, \\ 1, & \text{если } a = 0, b = 1 \text{ или } a = 1, b = 1, \\ \emptyset, & \text{если } a = 0, b = 0. \end{cases}$$

Пример 1. Сколько существует различных наборов значений логических переменных $x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4, y_5$, которые удовлетворяют всем ниже перечисленным условиям

$$(x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1,$$

$$(y_1 \rightarrow y_2) \wedge (y_2 \rightarrow y_3) \wedge (y_3 \rightarrow y_4) \wedge (y_4 \rightarrow y_5) = 1,$$

$$(x_1 \rightarrow y_1) \wedge (x_2 \rightarrow y_2) = 1?$$

Решение. Из первого уравнения получаем вспомогательную систему

$$(x_1 \rightarrow x_2) = 1, (x_2 \rightarrow x_3) = 1, (x_3 \rightarrow x_4) = 1, (x_4 \rightarrow x_5) = 1.$$

Рассмотрим уравнение $(x_i \rightarrow x_{i+1}) = 1$, где $i = 1, 2, 3, 4$. Пара переменных (x_i, x_{i+1}) принимает значения (00), (01), (11). Среди этих пар нет пары (10).

Изменяя номер i , получаем, что если некоторая переменная x_i приняла значение 1, то все последующие переменные также примут значения 1, т.е. если $x_i = 1$, то $x_k = 1$ для всех $k > i$.

Первое уравнение имеет следующие решения

00000, 00001, 00011, 00111, 01111.11111.

Аналогично, второе уравнение имеет 6 решений

00000, 00001, 00011, 00111, 01111.11111.

Изобразим решения каждого уравнения (рис. 50).

x_1	x_2	x_3	x_4	x_5
0	0	0	0	0
0	0	0	0	1
0	0	0	1	1
0	0	1	1	1
0	1	1	1	1
1	1	1	1	1



y_1	y_2	y_3	y_4	y_5
0	0	0	0	0
0	0	0	0	1
0	0	0	1	1
0	0	1	1	1
0	1	1	1	1
1	1	1	1	1

Рис. 50

О
бъединя
ния набо
ры
 x_1, x_2, x_3, x_4, x_5
и
 y_1, y_2, y_3, y_4, y_5
полу-

чим пары наборов, часть из которых представлена с помощью стрелок на рис. 50. Третье уравнение накладывает условие, по которому объединяются не все выше приведенные наборы, а часть из них.

Запишем третье уравнение в виде $x_1 \rightarrow y_1 = 1$ и $x_2 \rightarrow y_2 = 1$.

Перечислим все наборы (x_1, x_2, y_1, y_2) , которые удовлетворяют этим условиям. Порядок расположения четырех переменных выбран так, чтобы переменные потом легко находились в выше приведенных кластерах:

(0000), (0001), (~~0010~~), (0011), (0101), (0111), (~~1010~~), (~~1011~~), (1111).

Среди девяти наборов три набора вычеркнуты, т.к. числа в наборах (x_1, x_2) и (y_1, y_2) не могут убывать.

Алгоритм соединения двух наборов наглядно представим в виде схемы (рис. 51).

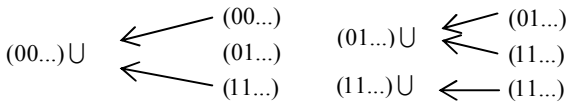


Рис. 51

Если выбрать пару $(x_1, x_2) = (00)$ в первой таблице, то из второй таблицы можно добавить все 6 наборов. В первой таблице существует четыре набора, первые два элемента в которых являются нулевыми, а значит, в этом случае можно составить $4 \times 6 = 24$ объединенных набора.

Если выбрать пару $(x_1, x_2) = (01)$ в первой таблице, то из второй таблицы можно добавить всего 2 набора. Если выбрать пару $(x_1, x_2) = (11)$ в первой таблице, то из второй таблицы можно добавить единственный набор. В этом случае получаем только один объединенный набор.

Системе логических уравнений удовлетворяет $24 + 2 + 1 = 27$ наборов. \square

Пример 2. Сколько существует различных наборов значений логических переменных $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$, которые удовлетворяют всем ниже перечисленным условиям:

$$(x_1 \vee x_2) \rightarrow (x_3 \vee x_4) = 1, (x_3 \vee x_4) \rightarrow (x_5 \vee x_6) = 1, (x_5 \vee x_6) \rightarrow (x_7 \vee x_8) = 1.$$

Решение. Обозначим $x_1 \vee x_2 = y_1, x_3 \vee x_4 = y_2, x_5 \vee x_6 = y_3, x_7 \vee x_8 = y_4$.

Исходная система примет вид $y_1 \rightarrow y_2 = 1, y_2 \rightarrow y_3 = 1, y_3 \rightarrow y_4 = 1$.

Последняя система имеет решения 1111, 0111, 0011, 0001, 0000.

Рассмотрим каждый из наборов в отдельности. Учитывая замену, каждый из этих наборов дает систему для x_1, x_2, \dots, x_8 , причем множества решений этих систем не пересекаются. Поэтому количество решений исходной системы равно сумме количеств решений систем, полученных из различных решений вспомогательной системы.

Для набора 1111 получаем систему:

$$x_1 \vee x_2 = 1, x_3 \vee x_4 = 1, x_5 \vee x_6 = 1, x_7 \vee x_8 = 1.$$

Каждое из уравнений имеет 3 решения. Уравнения системы независимы, поэтому количество решений системы равно произведению количеств решений для каждого из уравнений. Поэтому система имеет $3^4 = 81$ решений. Для набора 0111 получаем систему: $x_1 \vee x_2 = 0, x_3 \vee x_4 = 1, x_5 \vee x_6 = 1, x_7 \vee x_8 = 1$.

Первое уравнение имеет 1 решение, каждое из остальных уравнений имеет 3 решения. Поэтому система имеет $3^3 = 27$ решений.




Аналогично для наборов 0011, 0001 и 0000 получаем соответственно $3^2 = 9$, $3^1 = 3$ и $3^0 = 1$ решений. Исходная система имеет $81 + 27 + 9 + 3 + 1 = 121$ решение. \square




Задачи.




21.1. Исследуйте логические уравнения:




а) $A \downarrow X = B$; б) $A | X = B$.

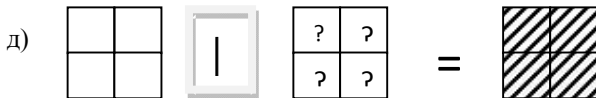
21.2. Из прозрачной бумаги (кальки) изготовлены следующие матрицы. Найдите решения уравнений.

а)  \vee  $=$ 

б)  \wedge  $=$ 

в)  \oplus  $=$ 

г)  \downarrow  $=$ 



21.3. Сколько различных решений имеет уравнение:

а) $(x \vee y) \rightarrow (y \wedge z \wedge t) = 0$; б) $(x \wedge y) \rightarrow (y \vee z \vee t) = 0$; в) $(x \rightarrow y) \rightarrow z = 0$?

21.4. Сколько существует различных наборов значений логических переменных $x_1, x_2, x_3, x_4, x_5, x_6$, которые удовлетворяют перечисленному ниже условию:

$$(x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) \wedge (x_5 \rightarrow x_6) = 1 ?$$

21.5. Сколько существует различных наборов значений логических переменных $x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4$, которые удовлетворяют системе:

а)
$$\begin{cases} (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1, \\ (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) = 1; \end{cases}$$

б)
$$\begin{cases} (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1, \\ (y_1 \rightarrow y_2) \wedge (y_2 \rightarrow y_3) \wedge (y_3 \rightarrow y_4) \wedge (y_4 \rightarrow y_5) = 1, \\ x_1 \vee y_1 = 1; \end{cases}$$

в)
$$\begin{cases} (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1, \\ (y_1 \rightarrow y_2) \wedge (y_2 \rightarrow y_3) \wedge (y_3 \rightarrow y_4) \wedge (y_4 \rightarrow y_5) = 1, \\ x_3 \wedge y_3 = 1; \end{cases}$$

г)
$$\begin{cases} (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1, \\ (y_1 \rightarrow y_2) \wedge (y_2 \rightarrow y_3) \wedge (y_3 \rightarrow y_4) \wedge (y_4 \rightarrow y_5) = 1, \\ x_1 \wedge y_1 = 1; \end{cases}$$

д)
$$\begin{cases} (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1, \\ (y_1 \rightarrow y_2) \wedge (y_2 \rightarrow y_3) \wedge (y_3 \rightarrow y_4) \wedge (y_4 \rightarrow y_5) = 1; \end{cases}$$

е)
$$\begin{cases} (x_1 \rightarrow x_2) \wedge (x_2 \rightarrow x_3) \wedge (x_3 \rightarrow x_4) \wedge (x_4 \rightarrow x_5) = 1, \\ (y_5 \rightarrow y_4) \wedge (y_4 \rightarrow y_3) \wedge (y_3 \rightarrow y_2) \wedge (y_2 \rightarrow y_1) = 1, \\ y_1 \rightarrow x_1 = 1? \end{cases}$$

§ 22. Производная булевой функции

Производной функции $f(x_1, x_2, \dots, x_i, \dots, x_n)$ по переменной x_i называется функция

$$\frac{\partial}{\partial x_i} f(x_1, x_2, \dots, x_i, \dots, x_n) = f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \oplus f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n),$$

где $f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$ – функция, полученная из данной функции $f(x_1, x_2, \dots, x_i, \dots, x_n)$ подстановкой $x_i = 1$, $f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$ – функция, полученная из данной функции $f(x_1, x_2, \dots, x_i, \dots, x_n)$ подстановкой $x_i = 0$.

Для этой производной используется также обозначение f'_{x_i} .

Из равенства $x \oplus y = \bar{x}y \vee x\bar{y}$ следует

$$\frac{\partial}{\partial x_i} f(x_1, \dots, x_i, \dots, x_n) = \overline{f(x_1, \dots, 1, \dots, x_n)} f(x_1, \dots, 0, \dots, x_n) \vee f(x_1, \dots, 1, \dots, x_n) \overline{f(x_1, \dots, 0, \dots, x_n)}$$

Свойства производной

$$\frac{\partial(const)}{\partial x} = 0, \quad \frac{\partial}{\partial x} \left(\frac{\partial f}{\partial x} \right) = 0, \quad \frac{\partial}{\partial x_i} \left(\frac{\partial f}{\partial x_j} \right) = \frac{\partial}{\partial x_j} \left(\frac{\partial f}{\partial x_i} \right), \quad \frac{\partial \bar{f}}{\partial x} = \frac{\partial f}{\partial x}, \quad (x f(y))'_x = f(y),$$

$$(f \oplus g)'_x = f'_x \oplus g'_x, \quad (fg)'_x = f'_x g \oplus f g'_x \oplus f'_x g'_x, \quad (f \vee g)'_x = f'_x \bar{g} \oplus \bar{f} g'_x \oplus f'_x g'_x.$$

Пример 1. Найти производную по переменной x от функции

$$f(x, y, z) = xyz \vee \bar{x}yz \vee \bar{z}t.$$

Решение. Первый способ, используя определение производной

$$\begin{aligned} \frac{\partial f}{\partial x} &= (1y\bar{z} \vee 1yz \vee \bar{z}\bar{t}) \oplus (0y\bar{z} \vee 0yz \vee \bar{z}\bar{t}) = (y\bar{z} \vee \bar{z}\bar{t}) \oplus (yz \vee \bar{z}\bar{t}) = \\ &= \overline{y\bar{z} \vee \bar{z}\bar{t}} (yz \vee \bar{z}\bar{t}) \vee (y\bar{z} \vee \bar{z}\bar{t}) \overline{yz \vee \bar{z}\bar{t}} = \overline{y\bar{z}\bar{z}\bar{t}} (yz \vee \bar{z}\bar{t}) \vee (y\bar{z} \vee \bar{z}\bar{t}) (\overline{yz\bar{z}\bar{t}}) = \\ &= ((\bar{y} \vee z)(z \vee t)(yz \vee \bar{z}\bar{t})) \vee (y\bar{z} \vee \bar{z}\bar{t})(\bar{y} \vee \bar{z})(z \vee t) = \\ &= (\bar{y}\bar{z} \vee y\bar{t} \vee zz \vee zt)(yz \vee \bar{z}\bar{t}) \vee (y\bar{z} \vee \bar{z}\bar{t})(\bar{y}\bar{z} \vee y\bar{t} \vee \bar{z}\bar{z} \vee \bar{z}\bar{t}) = \\ &= yz \vee yzt \vee y\bar{z}\bar{t} = yz \vee yt(z \vee \bar{z}) = yz \vee yt = y(z \vee t). \end{aligned}$$

Второй способ.

Используем свойства производной и свойство: если $xy = 0$, то $x \vee y = x \oplus y$.

$$\begin{aligned} (xyz \vee \bar{x}yz \vee \bar{z}\bar{t})'_x &= [(xyz \vee \bar{x}yz) \vee \bar{z}\bar{t}]'_x = [(xyz \oplus \bar{x}yz) \vee \bar{z}\bar{t}]'_x = \\ &= [y(x\bar{z} \oplus \bar{x}z) \vee \bar{z}\bar{t}]'_x = (y(x\bar{z} \oplus \bar{x}z))'_x \bar{z}\bar{t} \oplus y(x\bar{z} \oplus \bar{x}z)(\bar{z}\bar{t})'_x \oplus \\ &\oplus (y(x\bar{z} \oplus \bar{x}z))'(\bar{z}\bar{t})'_x = y[(0\bar{z} \oplus 0z) \oplus (1\bar{z} \oplus \bar{1}z)](z \vee t) \oplus 0 \oplus 0 = y[z \oplus \bar{z}](z \vee t) = y(z \vee t). \end{aligned}$$

Третий способ. Используем равенство

$$\begin{aligned}
 x \vee y \vee z &= xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z \\
 f(x, y, z) &= xyz \vee \overline{xy}z \vee \overline{x}yz \vee \overline{z}t = xyz\overline{z}t \oplus \overline{xy}z\overline{z}t \oplus \overline{x}yz\overline{z}t \oplus \overline{z}t \oplus \overline{xy}z \oplus \overline{x}yz \oplus \overline{z}t = \\
 &= \overline{xy}z\overline{t} \oplus \overline{xy}z \oplus \overline{x}yz \oplus \overline{z}t. \quad (\overline{xy}z \oplus \overline{x}yz \oplus \overline{z}t)'_x = (\overline{xy}z\overline{t} \oplus \overline{xy}z \oplus \overline{x}yz \oplus \overline{z}t)'_x = \\
 &= \overline{yz}\overline{t} \oplus \overline{yz} \oplus yz = y(\overline{z}\overline{t} \oplus \overline{z} \oplus z) = y(\overline{z}\overline{t} \oplus 1) = \overline{yz}\overline{t} = y(z \vee t). \quad \square
 \end{aligned}$$

Дифференцирование булевой функции с помощью карты Карно

Записываем остаточную функцию $f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$ на карту Карно, затем остаточную функцию $f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$ и проводим сложение единиц в каждой клетке по модулю 2. Желательно минимизировать полученную ДНФ.

Пример 2. Найти производную по переменной x от функции

$$f(x, y, z) = \overline{xy}z \vee \overline{xy}z \vee \overline{z}t.$$

Решение. Остаточные функции $f(1, y, z) = 1y\overline{z} \vee 1yz \vee \overline{z}t = \overline{yz} \vee \overline{z}t$ и $f(0, y, z) = 0y\overline{z} \vee 0yz \vee \overline{z}t = yz \vee \overline{z}t$ зависят от трех переменных. Записываем их на карту Карно для трех переменных (таблица 59). Функцию $f(1, y, z) = \overline{yz} \vee \overline{z}t$ записываем сверху соответствующей клетки, а функцию $f(0, y, z) = yz \vee \overline{z}t$ записываем внизу клетки. Сложив по модулю 2 получаем карту Карно (таблица 60), для которой минимальная ДНФ имеет вид $f = yz \vee yt$. \square

Таблица 59

	zt	\overline{zt}	$\overline{z}t$	$\overline{z}\overline{t}$
y	1	1	1	1
\overline{y}			1	1

Таблица 60

	zt	\overline{zt}	$\overline{z}t$	$\overline{z}\overline{t}$
y	1	1		1
\overline{y}				

Пример 3. Докажите равенства

$$а) \frac{\partial}{\partial x} f(x, y) = \overline{\frac{\partial}{\partial x} f(x, y)}; \quad б) \frac{\partial}{\partial x} f(x, y) = \overline{\frac{\partial}{\partial x} \overline{f(x, y)}}.$$

Решение.

$$а) \frac{\partial}{\partial x} f(x, y) = \overline{\frac{\partial}{\partial x} \overline{f(x, y)}} = \overline{f(\overline{0}, y) \oplus f(\overline{1}, y)} = \overline{f(1, y) \oplus f(0, y)} = \overline{\frac{\partial}{\partial x} f(x, y)},$$

$$\begin{aligned}
 б) \frac{\partial}{\partial x} \overline{f(x, y)} &= \overline{f(0, y) \oplus f(1, y)} = \overline{(f(0, y) \oplus 1) \oplus ((f(1, y) \oplus 1))} = \\
 &= \overline{f(0, y) \oplus f(1, y) \oplus 1 \oplus 1} = \overline{f(0, y) \oplus f(1, y)} = \frac{\partial}{\partial x} f(x, y). \quad \square
 \end{aligned}$$

Задачи.

22.1. Используя определения производной, докажите следующие равенства:

а) $\frac{\partial}{\partial x} 0 = 0$; б) $\frac{\partial}{\partial x} 1 = 0$; в) $(fg)'_x = f'_x g \oplus fg'_x \oplus f'_x g'_x$;

г) производная по переменной x от функции, не зависящей от этой переменной, равна нулевой функции; д) $(f \oplus g)'_x = f'_x \oplus g'_x$;

е) $(f \vee g)'_x = (fg)'_x \oplus f'_x \oplus g'_x$; ж) $(f \vee g)'_x = f'_x \bar{g} \oplus \bar{f} g'_x \oplus f'_x g'_x$.

22.2. Найдите производную от следующих функций по переменной x : а) $x y z$; б) $x \vee \bar{x}$; в) $x \wedge \bar{x}$; г) $y z$.

22.3. Используя карту Карно, найдите производную от функции $f = x_1 x_2 x_3 \vee x_2 x_3 x_5 \vee x_2 x_4 x_5 \vee x_2 x_3 x_5$ по переменной x_3 .

22.4. Найдите производные

а) $(x \vee x)'$; г) $(x \rightarrow x)'$; ж) $(x \leftrightarrow y)'_x$; й) $(x \downarrow y)'_y$;

б) $(x \wedge x)'$; д) $(x \rightarrow y)'_x$; з) $(x \leftrightarrow y)'_y$; к) $(x|y)'_x$;

в) $(\bar{x})'$; е) $(x \rightarrow y)'_y$; и) $(x \downarrow y)'_x$; л) $(x|y)'_y$.

22.5. Докажите равенства

а) $f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 0, \dots, x_n) \vee x_i \frac{\partial f(x_1, \dots, x_i, \dots, x_n)}{\partial x_i}$;

б) $f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, 1, \dots, x_n) \vee \bar{x}_i \frac{\partial f(x_1, \dots, x_i, \dots, x_n)}{\partial x_i}$.

22.6. Докажите равенства

а) $(x \vee y)'_x = \bar{y}$; б) $(x \vee y \vee z)'_x = \bar{y} \vee \bar{z}$; в) $(x \vee f(y, z))'_x = \overline{f(y, z)}$.

22.7. Докажите равенства

а) $f(x_1, x_2, \dots, x_n) = f(0, x_2, \dots, x_n) \oplus x_1 \frac{df(x_1, x_2, \dots, x_n)}{dx_1}$;

б) $f(x_1, x_2, \dots, x_n) = f(1, x_2, \dots, x_n) \oplus \bar{x}_1 \frac{df(x_1, x_2, \dots, x_n)}{dx_1}$.

22.8. СИ. Можно ли любую функцию от трех переменных представить в виде композиции функций двух переменных в виде:

а) $f(x, y, z) = \varphi(m(x, y), n(y, z))$;

б) $f(x, y, z) = \varphi(h(m(x, y), n(y, z)), l(x, z))$?

Глава 3. Графы и оргграфы

§ 23. Определение графа

Пусть $V = \{v_1, v_2, \dots, v_n\}$ – непустое множество, элементы которого назовем *вершинами*. Рассмотрим некоторое семейство E пар элементов из V вида $\{v_i, v_j\}$.

Конкретный набор $\{v_i, v_j\}$ будем называть *ребром*, соединяющим вершины v_i и v_j .

Пара $\{v_i, v_i\}$ называется *петлей*. Если в E имеются одинаковые пары, то они называются *кратными ребрами*. Количество одинаковых пар называется *кратностью* ребра.

Для наглядности вершины изображают в виде точек плоскости (пространства), а ребра – непрерывными линиями, соединяющими эти вершины.

Множество (V, E) с кратными ребрами и петлями (рис. 1) называется *псевдографом*. Псевдограф без петель называется графом с кратными ребрами или *мультиграфом*.

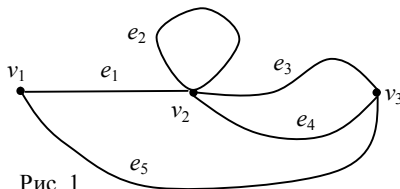


Рис. 1

Если в наборе E нет кратных ребер и петель, то множество (V, E) называется графом, т.е. *графом* называется совокупность двух множеств – непустого множества V вершин и множества E ребер, т.е. пар некоторых различных элементов из V . Обозначение графа $G = G(V, E) = \{V, E\}$.

Граф, содержащий одну вершину, называется *тривиальным*.

На рисунке 2 изображен граф.

Множество вершин – $V = \{v_1, v_2, v_3, v_4, v_5\}$, множество ребер – $E = \{e_1 = \{v_1, v_2\}, e_2 = \{v_2, v_3\}, e_3 = \{v_2, v_4\}, e_4 = \{v_3, v_4\}\}$.

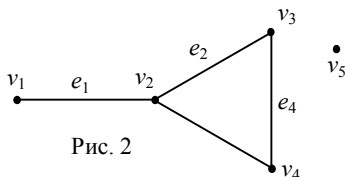


Рис. 2

Замечания. Иногда в литературе для графа допускаются петли (петля – ребро, соединяющее одну и ту же вершину) и кратные ребра, т.е. несколько ребер, соединяющих две точки.

Если пары в E являются упорядоченными, то граф называется ориентированным (*орграфом*), а ребра называются *дугами*. Дуги в ориентированном графе записывают в круглых скобках, а ребра в неориентированном графе – в фигурных скобках. На ориентированном графе дуги изображают стрелками, начало которой находится в первой вершине ребра (v_1, v_2) , а конец – во второй.

На рисунке 3 изображен ориентированный псевдограф $D = \{V, E\}$. Множество вершин $V = \{v_1, v_2, v_3, v_4\}$. Множество дуг $E = \{e_1 = (v_1, v_2), e_2 = (v_2, v_1), e_3 = (v_2, v_2), e_4 = (v_2, v_3)\}$.

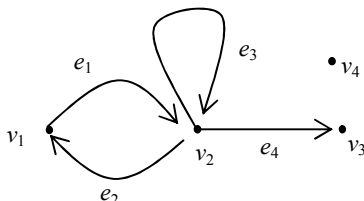


Рис. 3

Если $e = \{v_1, v_2\}$ – ребро графа, то вершины v_1, v_2 называются концами ребра e или ребро e соединяет вершины v_1, v_2 .

Если $e = (v_1, v_2)$ – дуга орграфа, то вершина v_1 называется *началом*, а вершина v_2 называется *концом дуги e* или дуга e выходит из вершины v_1 и приходит в вершину v_2 .

Если вершина v является концом ребра e , то v и e называются *инцидентными*.

Вершины v_1, v_2 графа $G = \{V, E\}$ называются *смежными*, если $\{v_1, v_2\} \in E$. Два ребра графа называются *смежными*, если они имеют общую вершину.

Пусть дан граф G и V – множество его вершин.

Дополнением \bar{G} графа G называется граф, имеющий то же самое множество вершин V , причем две вершины в \bar{G} смежные тогда и только тогда, когда они не смежные в G .

На рисунке 4 изображены граф G и его дополнение \bar{G} .

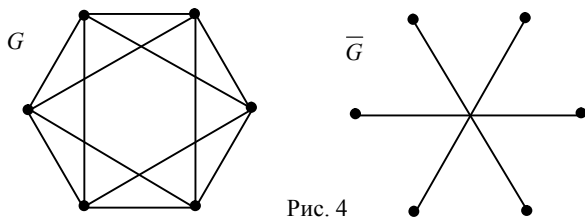


Рис. 4

Число вершин графа обозначим $n = n(G) = |V|$.

Число ребер графа обозначим $m = m(G) = |E|$.

Степенью вершины v_i графа G называется число $\deg(v_i)$ ребер графа, инцидентных этой вершине.

Вершина графа, со степенью равной нулю, называется *изолированной*, а со степенью равной 1, называется *висячей*.

На рисунке 2 вершина v_5 – изолированная вершина, вершина v_1 – висячая, $\deg(v_2) = 3, \deg(v_3) = 2, \deg(v_4) = 2$.

Теорема 1. Сумма степеней вершин графа равна удвоенному количеству ребер, т.е. $\sum_{v_i \in V} \deg(v_i) = 2m(G)$.

Вершина с четной степенью называется *четной*, а вершина графа с нечетной степенью называется *нечетной*.

Теорема 2. Число нечетных вершин любого графа – четно.

Для неориентированного псевдографа полагают, что петля добавляет число ребер в вершине, равное двум.

Степенью входа (выхода) вершины v_i орграфа D называется число $\text{indeg}(v_i)$ ($\text{outdeg}(v_i)$) дуг орграфа, входящих в вершину (выходящих из вершины).

Теорема 3. Для любого орграфа $\sum_{v_i \in V} \text{indeg}(v_i) + \sum_{v_i \in V} \text{outdeg}(v_i) = m(D)$.

Пример 1. Вершинами графа назовем множество $V = \{(x_1, x_2, \dots, x_n)\}$ всех упорядоченных наборов n булевых переменных. Например, для $n = 3$ получаем вершины: (000), (001), (010), (011), (101), (101), (110), (111).

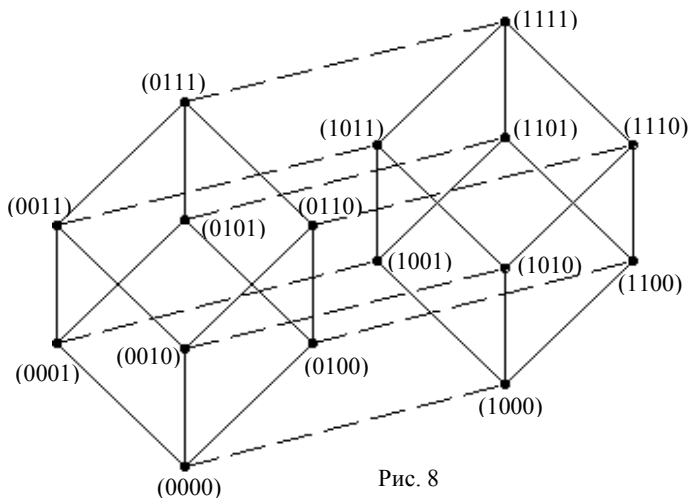
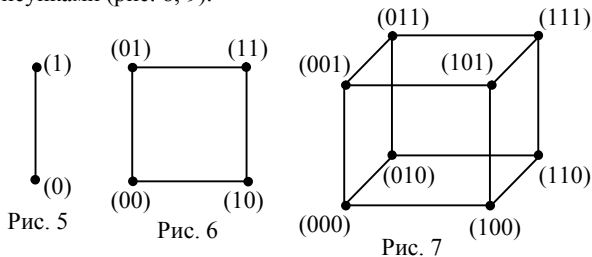
Две вершины графа называются смежными, если наборы этих вершин являются соседними, т.е. отличаются одной переменной. Ребрам графа называется пара смежных вершин. Множество всех вершин и ребер называется n -мерным кубом и обозначается B^n . Число вершин n -мерного куба равно 2^n .

Степень каждой вершины равна n , т.к. для произвольной вершины (x_1, x_2, \dots, x_n) существует ровно n смежных вершин:

$$(\bar{x}_1, x_2, \dots, x_n), (x_1, \bar{x}_2, \dots, x_n), \dots, (x_1, x_2, \dots, \bar{x}_n).$$

Две вершины куба называются *противоположными*, если наборы этих вершин являются противоположными.

На рис. 5–7 изображены соответственно одномерный, двумерный и трехмерный кубы. Четырехмерный куб в трехмерном пространстве изображают различными рисунками (рис. 8, 9).



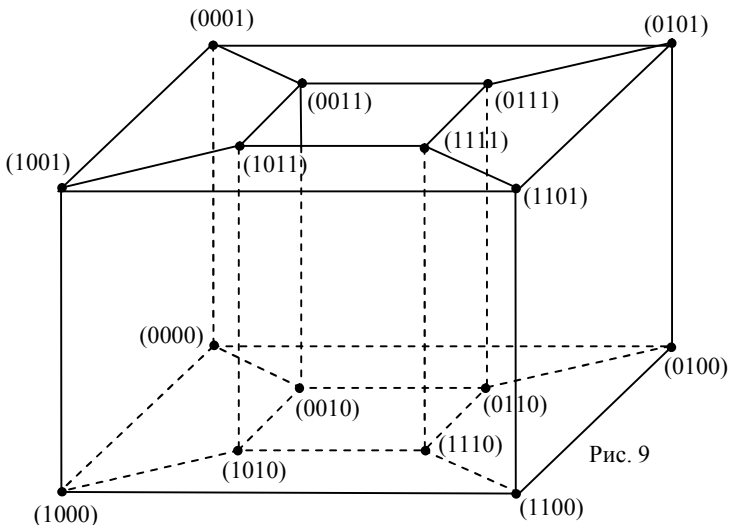


Рис. 9

Задачи.

23.1. Постройте граф, вершины которого обозначают города, с которыми связан ваш город (населенный пункт) автобусным или авиационным сообщением.

23.2. Постройте оргграф, вершины которого обозначают этапы строительства дома, и укажите последовательность этапов.

23.3. В группе 28 студентов. Может ли быть так, что 9 из них имеют по 3 друга в этой группе, 11 – по 4 друга, а 8 – по 5 друзей?

23.4. Может ли в государстве, в котором из каждого города выходит 7 дорог, быть ровно 100 дорог?

23.5. Докажите, что число всех людей, когда-либо пожавших руку другим людям нечетное число раз, является четным.

23.6. Докажите, что во всяком графе с n вершинами, где $n \geq 2$, всегда найдется две или более вершины с одинаковыми степенями.

23.7. В шахматном турнире участвует 20 команд. Докажите, что в любой момент времени найдется две команды, сыгравшие одинаковое число матчей.

23.8. Докажите, что для любого значения $n \geq 3$ существует n -вершинный граф без петель и кратных ребер, содержащий $n-1$ вершин с неравными друг другу степенями.

23.9. Каждая вершина правильного шестиугольника соединена с каждой из остальных вершин отрезком красного или синего цвета. Докажите, что найдется треугольник со сторонами одного цвета.

23.10. Докажите методом математической индукции, что число ребер n -мерного куба равно $n2^{n-1}$.

23.11. Постройте дополнения к данным графам на рис. 10.

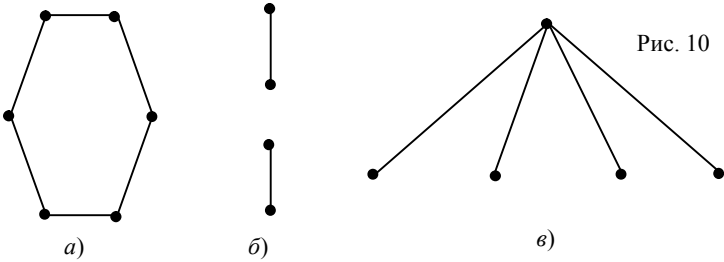


Рис. 10

23.12. Пусть m – число ребер графа G , \bar{m} – число ребер его дополнения \bar{G} , n – число вершин графа G . Найдите зависимость m и \bar{m} .

24.13. Докажите, что дополнение к дополнению графа G есть первоначальный граф G .

24.14. Докажите, что среди любых шести человек найдутся либо трое попарно знакомых, либо трое попарно незнакомых.

§ 24. Изоморфные и гомеоморфные графы

Граф $G_1(V_1, E_1)$ называется *изоморфным* графу $G_2(V_2, E_2)$ (обозначение $G_1 \sim G_2$), если существует биективное отображение $\varphi: V_1 \rightarrow V_2$, сохраняющее отношение смежности, т.е. $\{v, u\} \in E_1 \leftrightarrow \{\varphi(v), \varphi(u)\} \in E_2$.

Из определения изоморфизма графов следует, что изоморфные графы отличаются лишь обозначением вершин. На рисунке 11 представлены три изоморфных графа.

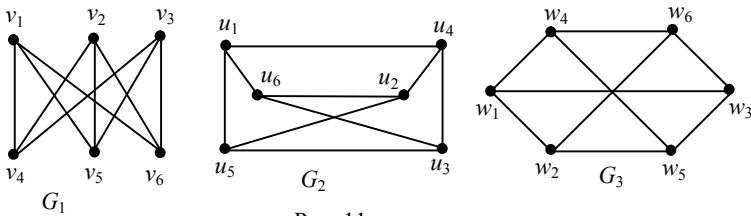


Рис. 11

Изоморфизм графов есть отношение эквивалентности:

1) $G \sim G$, т.е. каждый граф изоморфен себе. Биекцией является тождественное отображение.

2) Из $G_1 \sim G_2$ следует $G_2 \sim G_1$, т.е. выполняется симметричность. Действительно, из существования биекции $\varphi: G_1 \rightarrow G_2$, сохраняющей отношение смежности, следует существование обратной биекции $\varphi^{-1}: G_2 \rightarrow G_1$, сохраняющей отношение смежности.

3) Из $G_1 \sim G_2$, $G_2 \sim G_3$ следует $G_1 \sim G_3$, т.е. выполняется транзитивность изоморфизма.

Графы рассматривают с точностью до изоморфизма, т.е. рассматривают классы эквивалентности графов по отношению изоморфизма.

Переход от одного изоморфного графа к другому изоморфному графу часто представляют с помощью непрерывной деформации графа, сохраняющей отношение смежности. На рисунке 12 пунктирной линией показана траектория вершины графа при деформации графа. Три изображенных графа являются изоморфными.

В дальнейшем для краткости записей вершины будем часто обозначать их номерами. Для изоморфных графов это удобнее, т.к. изоморфные графы отличаются лишь обозначением вершин.

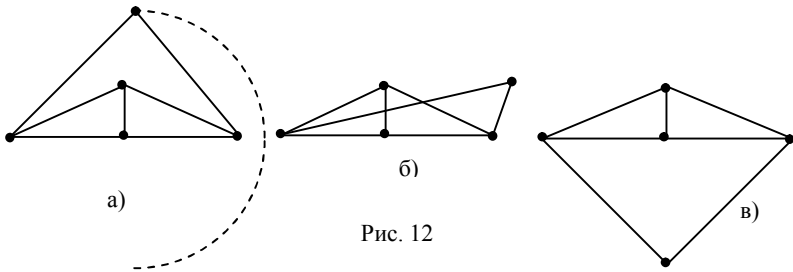


Рис. 12

Числовая характеристика, одинаковая для всех изоморфных графов, называется *инвариантом графа*. Примеры инвариантов графа: $n, m, \deg(i)$. В настоящее время не известно набора инвариантов, определяющих граф с точностью до изоморфизма. В приложении 1 этого задачника представлена структуры неизоморфных графов с числом вершин не более 6.

Если два графа изоморфны, то у них одинаковое количество вершин данной степени. На рисунке 13 представлены два графа, для которых $n, m, \deg(i)$ совпадают, но графы не изоморфны.

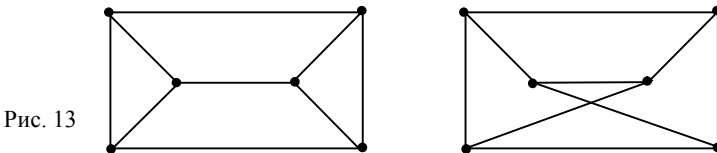


Рис. 13

Изоморфизм графа в себя называется *автоморфизмом*. Совокупность автоморфизмов относительно композиции образует группу, т.к. если $\varphi_1 : G \rightarrow G$ и $\varphi_2 : G \rightarrow G$ – автоморфизмы графа G , то их композиция и обратные к ним являются также автоморфизмами. Тожественное отображение графа в себя является автоморфизмом и выполняет роль единичного элемента в группе.

Число неизоморфных графов с n вершинами и m ребрами представлено в таблице 1.

Таблица 1

$m \backslash n$	1	2	3	4	5	6	7	8
0	1	1	1	1	1	1	1	1
1		1	1	1	1	1	1	1
2			1	2	2	2	2	2
3				3	4	5	5	5
4					2	6	9	10
5						1	6	15
6							1	6
7								4
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
Итого	1	2	4	11	24	156	1044	12 344

Операция подразделения ребра $\{u, v\}$ графа $G = \{V, E\}$ состоит в удалении из E ребра $\{u, v\}$ и добавлении к V новой вершины w и добавлении к E ребер $\{u, w\}, \{w, v\}$.

На рисунке 14 графы G_1, G_2 получены из графа G подразбиением ребра $\{u, v\}$. Графы G_1 и G_2 изоморфны.

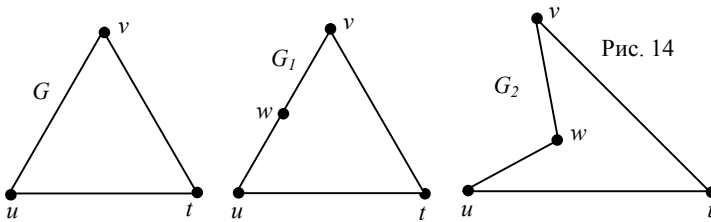


Рис. 14

Каждое подразбиение ребра увеличивает число вершин графа на единицу, увеличивает число ребер графа на единицу, но не изменяет степени вершин первоначального графа. Для вновь введенной вершины подразбиения степень равна 2. Таким образом, первоначальный граф и граф, полученный при подразбиении ребра, не изоморфны.

Граф G_1 называется *подразбиением графа G* , если граф G_1 может быть получен из графа G последовательным применением операции подразбиения ребер (рис. 15).

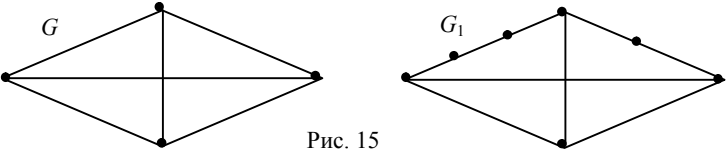


Рис. 15

Графы G_1 и G_2 называются *гомеоморфными*, если существуют их подразбиения, которые изоморфны.

Графы на рисунке 16 гомеоморфны, т.к. если на графе G_1 осуществить подразбиение ребра $\{v, u\}$, а на графе G_2 осуществить подразбиение ребра $\{w, t\}$, то получим изоморфные графы.

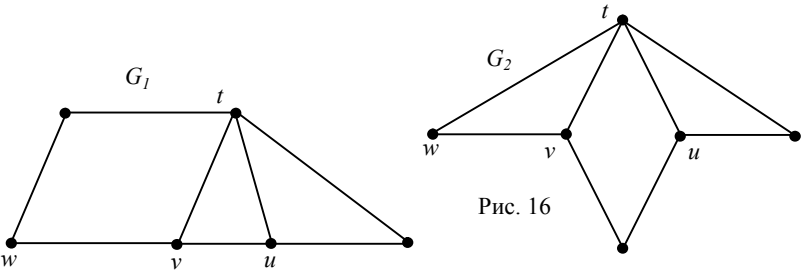


Рис. 16

Графы на рис. 17 гомеоморфны. Области, которые ограничивают эти многоугольники, также называются гомеоморфными.

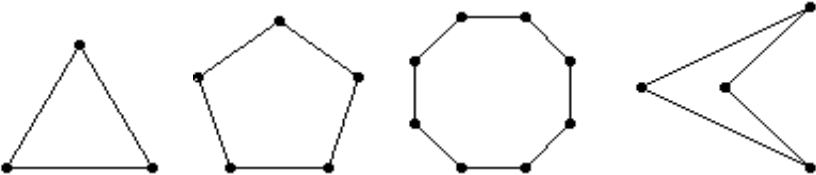


Рис. 17

Граф называется *самополнительным*, если он изоморфен своему дополнению.

На рис. 18 сплошными линиями изображены самодополнительные графы G . Пунктирными линиями изображены их дополнения \overline{G} , которые, кстати, также являются самодополнительными графами.

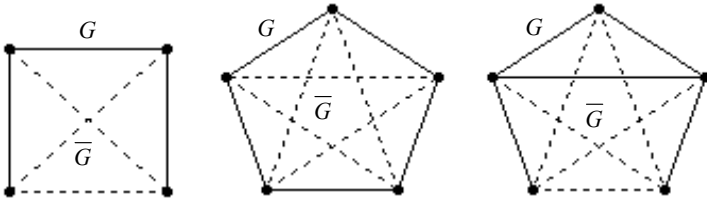


Рис. 18

Задачи.

24.1. Докажите изоморфизм графов на рис. 19.

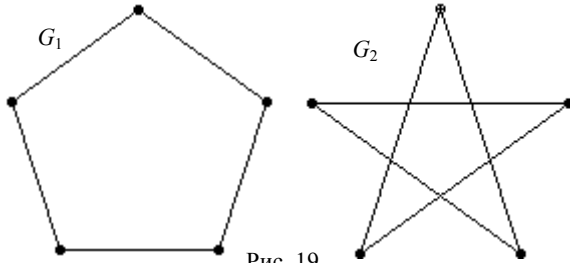


Рис. 19

24.2. Среди следующих графов G_1, G_2, \dots, G_6 (рис. 20) найдите изоморфные графы.

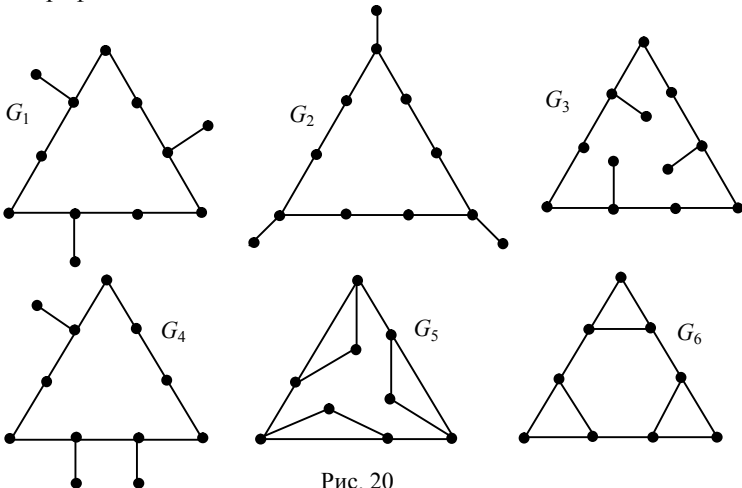


Рис. 20

24.3. Изоморфны ли графы $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$, если $V_2 = \{a, b, c, d, e, f\}$, $E_2 = \{(a, b), (b, c), (c, a), (d, e), (e, f), (f, d)\}$ и $V_1 = \{1, 2, 3, 4, 5, 6\}$, $E_1 = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (6, 1)\}$?

24.4. Перечислите все автоморфизмы каждого следующего графа (рис. 21), которые переводят множество вершин $\{a, b, c\}$ в это же множество.

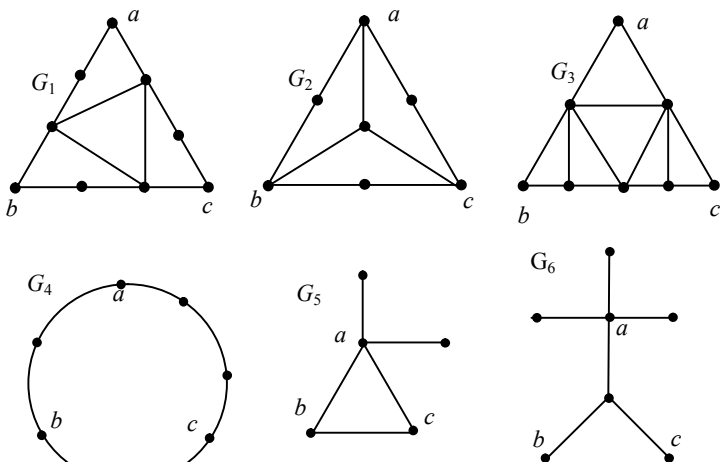


Рис. 21

24.5. Дан граф G_1 (рис. 22). Постройте графы G_2, G_3, G_4 , гомеоморфные графу G_1 , никакие два из которых не изоморфны между собой.

24.6. Докажите, что если графы G_1 и G_2 изоморфны, то их дополнения – изоморфны.

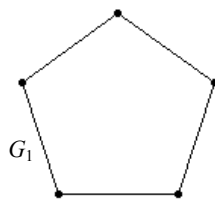


Рис. 22

§ 25. Матрица смежности и матрица инцидентности

Пусть $G(V, E)$ – граф, состоящий из множества V вершин и множества E ребер и пусть n – число вершин, m – число ребер.

Матрицей смежности графа G называется квадратная матрица $A(G) = [a_{ij}]$ размером $n \times n$, у которой

$$a_{ij} = \begin{cases} 1, & \text{если } \{v_i, v_j\} \in E, \text{ т.е. существует ребро, соединяющее } v_i \text{ с } v_j, \\ 0, & \text{если } \{v_i, v_j\} \notin E. \end{cases}$$

Матрицей инцидентности графа называется матрица $B(G) = [b_{ij}]$ размером $n \times m$, для которой $b_{ij} = \begin{cases} 1, & \text{если } v_i \in e_j, \\ 0, & \text{если } v_i \notin e_j. \end{cases}$

Пусть орграф не имеет петель и не имеет двойных ребер.

Матрицей смежности орграфа D называется квадратная матрица $A(G) = [a_{ij}]$ размером $n \times n$, у которой

$$a_{ij} = \begin{cases} 1, & \text{если } (v_i, v_j) \in E, \text{ т. е. существует путь из } v_i \text{ в } v_j, \\ 0, & \text{если } (v_i, v_j) \notin E, \text{ т. е. нет пути из } v_i \text{ в } v_j. \end{cases}$$

Матрицей инцидентности орграфа называется матрица $B(D) = [b_{ij}]$ размером $n \times m$, для которой

$$b_{ij} = \begin{cases} 1, & \text{если вершина } v_i \text{ является концом дуги } e_j, \\ -1, & \text{если вершина } v_i \text{ является началом дуги } e_j, \\ 0, & \text{если } v_i \notin e_j. \end{cases}$$

Пример 1. Для графа (рис. 23) составим таблицу (табл.2), отмечая соответствующие ребра, а затем матрицу смежности A .

Таблица 2

	v_1	v_2	v_3	v_4	v_5
v_1	0	1	0	0	0
v_2	1	0	1	1	0
v_3	0	1	0	1	0
v_4	0	1	1	0	0
v_5	0	0	0	0	0

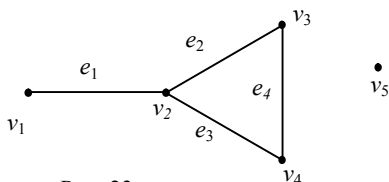


Рис. 23

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Для графа составим таблицу (табл. 3), отмечая соответствующие инцидентности, т.е. принадлежность вершины ребру, а затем матрицу инцидентности B :

Таблица 3

	e_1	e_2	e_3	e_4
v_1	1	0	0	0
v_2	1	1	1	0
v_3	0	1	0	1
v_4	0	0	1	1
v_5	0	0	0	0

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Пример 2. Для графа (рис. 24) составим таблицу (табл. 4), отмечая соответствующие ребра, а затем матрицу смежности:

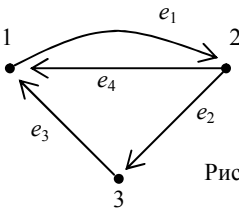


Рис. 24

Таблица 4

	1	2	3
1	0	1	0
2	1	0	1
3	0	1	0

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Для данного графа составим таблицу (табл. 5), отмечая соответствующие инцидентности, а затем матрицу инцидентности:

Таблица 5

	e_1	e_2	e_3	e_4
1	-1	0	1	1
2	1	-1	0	-1
3	0	1	-1	0

$$B = \begin{pmatrix} -1 & 0 & 1 & 1 \\ 1 & -1 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

Для запоминания знаков в матрице инцидентности будем рассуждать следующим образом. Приход стрелки в точку будем интерпретировать как приток капитала и отмечать единицей, а выход стрелки из точки интерпретировать как отток капитала и обозначать -1 .

Если номера дуг не имеют значения и ребра заданы парами вершин, то матрицу инцидентности можно задать для орграфа на рис. 2 следующим образом (табл. 6).

Таблица 6

Ребра \ Вершины	(1,2)	(2,1)	(2,3)	(3,1)
1	-1	1	0	1
2	1	-1	-1	0
3	0	0	1	-1

По матрице смежности графа (орграфа) всегда можно определить ребра графа (дуги орграфа) как пары инцидентных им вершин. Но если ребра (дуги) были пронумерованы, то восстановить их номера по матрице смежности невозможно. В этом случае матрица инцидентности позволяет получить больше информации.

Отметим важную идею. Графы и орграфы можно задавать матрицами и свети изучение графов и орграфов к изучению соответствующих матриц. Это часто используется, но для некоторых графов информация быстрее определяется непосредственно с графа, чем из матрицы. Графический и матричный способы дополняют друг друга.

Таблица 7

v_1	v_2	v_2	v_3	v_5
v_2	v_3	v_4	v_4	

Для графа на рис. 23 получаем таблицу 7, в которой, если пара $\{v_i, v_j\}$ записана, то пара $\{v_j, v_i\}$ уже не записывается.

Таблица 8

1	2	2	3
2	1	3	1

Для орграфа на рис. 24. получаем таблицу 8. В первой строке записывается вершины выхода дуги, а во второй строке вершина прихода дуги.

Задачи.

25.1. Составьте матрицы смежности для графов (рис. 25).

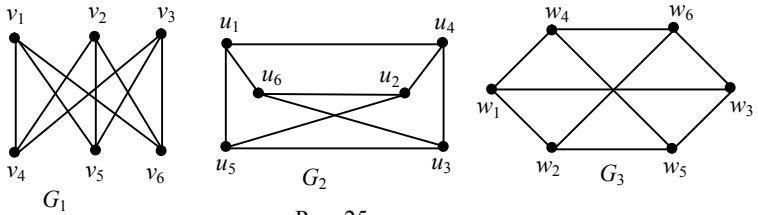


Рис. 25

25.2. Для следующих матриц смежности постройте графы

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, A_5 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, A_6 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

25.3. Какой смысл имеет сумма элементов в строке (в столбце) матрицы смежности?

25.4. Составьте матрицы инцидентности для графов (рис. 26):

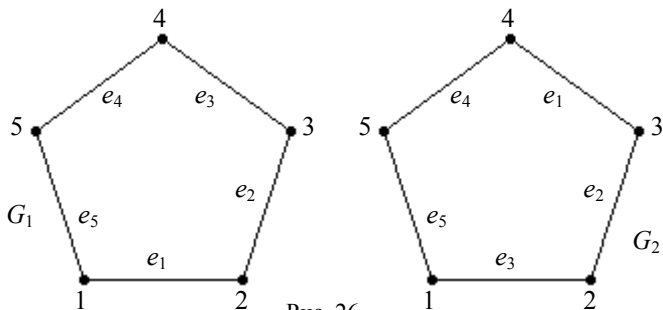


Рис. 26

25.5. Как изменится матрица инцидентности, если переставить два ребра на графе?

25.6. Составьте матрицу смежности и матрицу инцидентности для орграфа (рис. 27). Как изменятся матрицы, если изменить направления всех дуг на противоположные направления?

25.7. Охарактеризуйте матрицу смежности и матрицу инцидентности орграфа, если любые две вершины соединены дугами в двух противоположных направлениях.

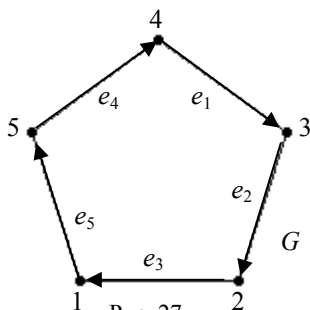


Рис. 27

25.8. Чему равна сумма элементов в каждом столбце матрица инцидентности орграфа?

25.9. Чему равна сумма элементов в каждой строке матрицы инцидентности?

25.10. Составьте матрицу смежности и матрицу инцидентности 4-мерного куба.

25.11. Найдите связь между матрицей смежности графа и матрицей смежности его дополнения.

§ 26. Однородный и полный графы

Граф называется *однородным*, если степени всех его вершин равны между собой, т.е. для $\forall i, \deg(v_i) = \text{const} = \delta$. Иногда говорят, что граф однородный степени δ или короче δ -валентный граф.

Для однородного графа $n\delta = 2m$.

Однородный граф называется *кубическим*, если степень каждой вершины равна 3 (рис. 28).

Схема вершин и ребер на кубе является примером кубического графа.

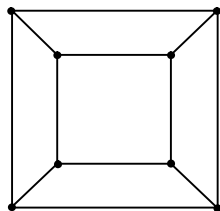


Рис. 28

Пример 1. Построить (с точностью до изоморфизма) все однородные графы с пятью вершинами.

Решение. Графы для четных степеней легко построить (рис. 29)

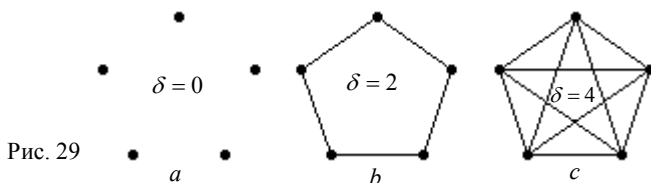


Рис. 29

Графы со степенями $\delta=1$ и $\delta=3$ не удается построить, и тогда возникает гипотеза, что такие графы не существуют. Действительно, из равенства для графа с пятью вершинами $m = \frac{5\delta}{2}$ следует, что число ребер графа в этих случаях является дробным числом, что невозможно. Используя приложение 1, выясните, все ли однородные графы построены с точностью до изоморфизма.

Граф называется *полным*, если каждая пара его различных вершин соединена одним ребром. Полный граф, имеющий n вершин, обозначается K_n .

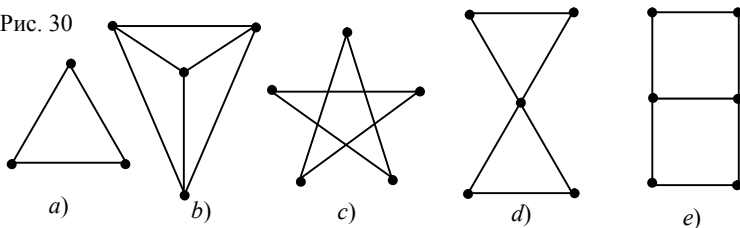
Степень любой вершины полного графа равна $n-1$, т.к. каждая вершина соединена с $n-1$ остальными вершинами графа.

Для полного графа выполняется равенство $n(n-1) = 2m$.

Задачи.

26.1. На рисунке 30 определите однородные и полные графы.

Рис. 30



26.2. Охарактеризуйте класс всех графов, изображенных на рис. 31. Найдите среди них два изоморфных графа.

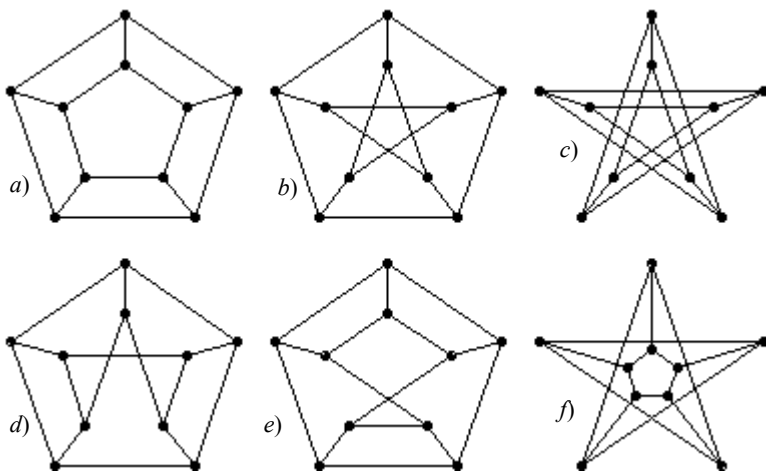


Рис. 31

26.3. Охарактеризуйте графы, изображенные на рис. 32. Найдите среди них изоморфные графы.

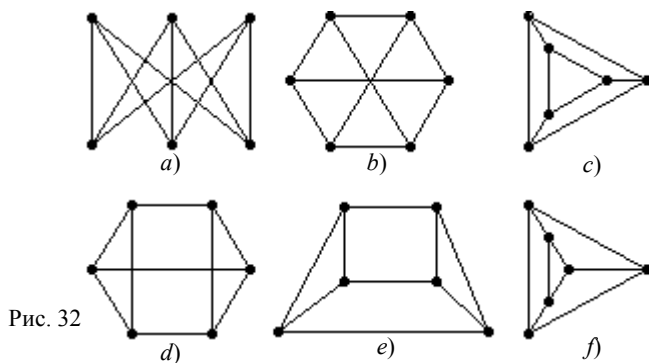


Рис. 32

26.4. Дано шесть точек. Постройте все однородные графы с точностью до изоморфизма, вершины которых находятся в этих точках. Проверьте результат, используя приложение 1 в конце задачника.

26.5. Найдите число n вершин графа и степени δ вершин однородного графа, если он содержит 7 ребер. Изобразите эти графы.

26.6. Сколько ребер имеет полный 10-вершинный граф?

26.7. Найдите степень вершины полного графа, имеющего 91 ребро.

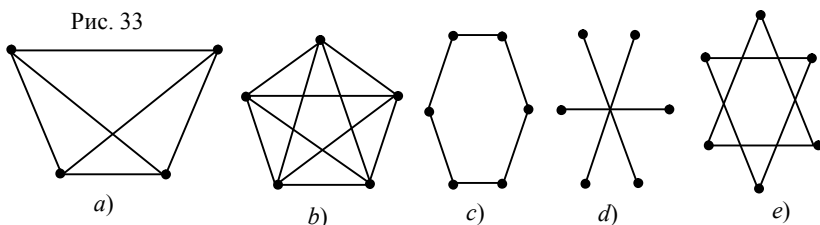
26.8. Существует ли однородный граф с заданным количеством m ребер? Для простого числа m изобразите все однородные графы.

26.9. Каким свойством обладает матрица смежности для однородного графа?

26.10. Постройте кубический граф с четырьмя вершинами.

26.11. Докажите, что каждый кубический граф имеет четное число вершин.

26.12. На рисунке 33 определите полные графы.



Существует ли полный граф с заданным количеством m ребер? Приведите примеры полных графов для некоторых значений m .

26.13. Выразите число ребер и степень вершины полного графа через число m .

26.14. В полном графе степень одной вершины равна δ . Выразите число вершин и число ребер через число δ .

26.15. Докажите, что каждый полный граф является однородным. Справедливо ли обратное утверждение?

26.16. Задайте полный граф с пятью вершинами, используя матрицу смежности.

26.17. Докажите теорему Кенига. Каждый кубический граф имеет четное число вершин.

26.18. Можно ли построить однородный граф с четным числом вершин, состоящий из двух компонент?

26.19. Найдите дополнение полного графа K_n .

26.20. Граф G имеет n вершин и m ребер. Сколько ребер имеет дополнение этого графа, т.е. граф \overline{G} ?

26.21. Докажите, что если число вершин графа равно $4k + 2$, где k – натуральное число, то граф не является самодополнительным.

26.22. Докажите, что если самодополнительный граф имеет n вершин, то число его ребер равно $\frac{n(n-1)}{4}$.

§ 27. Маршруты и числовые характеристики на графе

а) *Маршруты, цепи и циклы*

Для графа $G = \{V, E\}$ *маршрутом* называется последовательность

$$v_1 e_1 v_2 v_3 \dots e_k v_{k+1}, \quad (1)$$

где $k \geq 1, v_i \in V, e_j \in E$, в которой чередуются вершины и ребра и каждое ребро e_j имеет вид $\{v_j, v_{j+1}\}$.

Для орграфа $D = \{V, E\}$ эта последовательность называется *путем*.

Вершина v_1 называется начальной, вершина v_{k+1} – конечной, а остальные вершины – внутренними.

Одна и та же вершина может оказаться одновременно начальной, внутренней и конечной. Последовательность вершин в маршруте определяет на ребрах, входящих в маршрут, ориентацию.

Последовательность (1) можно однозначно восстановить по последовательности $e_1 e_2 \dots e_k$.

Это иногда используется для краткой записи маршрута.

Если в последовательности (1) ребра $e_1 e_2 \dots e_k$ имеют кратности, равные 1, то последовательность можно восстановить по последовательности вершин

$$v_1 v_2 \dots v_{k+1}.$$

Это также используется для краткой записи маршрута.

Пусть $x_1 x_2 \dots x_k$ – маршрут в графе G и для некоторой последовательности номеров i_1, i_2, \dots, i_r , где $r \geq 1, 1 \leq i_1 < i_2 < \dots < i_r \leq k$ последовательность $x_{i_1} x_{i_2} \dots x_{i_r}$ снова является маршрутом в графе G , тогда $x_{i_1} x_{i_2} \dots x_{i_r}$ называется *подмаршрутом* маршрута $x_1 x_2 \dots x_k$.

Число ребер (дуг) в маршруте (пути) называется длиной *маршрута* (пути).

Маршрут называется *замкнутым*, если его начальная вершина совпадает с конечной, т.е. $v_1 = v_{k+1}$.

При подсчете числа вхождения вершин в замкнутый маршрут начальную и конечную вершины будем считать за одно вхождение этой вершины в маршрут.

Для замкнутого маршрута $x_1 x_2 \dots x_n$ будем считать, что последовательности $x_1 x_2 \dots x_n, x_2 x_3 \dots x_n x_1, x_3 x_4 \dots x_n x_2, x_n x_1 \dots x_{n-1}$ – различные записи одного и того же маршрута.

Незамкнутый маршрут, в котором все ребра попарно различны называется *цепью*. Цепь, в которой все вершины попарно различны, называется *простой цепью*.

Замкнутый маршрут, в котором все ребра попарно различны, называется *циклом* (*контуром*). Цикл (контур), в котором все вершины попарно различны, называется *простым*.

Для графа на рисунке 34:

$v_1v_2e_3v_4v_3$ – маршрут длины 3, простая цепь, т.к. все ребра различны и все вершины различны;

$v_3e_2v_3e_4v_4e_3v_2$ – замкнутый маршрут длины 3, простой цикл;

$v_1e_1v_2e_3v_3e_4e_3v_2$ – маршрут длины 4, цепь, но не является простой цепью, т.к. вершина v_2 встречается дважды;

$v_1e_1v_2e_3v_3e_2v_2$ – маршрут длины 3, не является цепью, т.к. ребро e_2 встречается дважды.

Для орграфа D на рисунке 35:

$v_1e_1v_2v_3$ – путь длины 2, простая цепь;

$v_2e_3v_2$ – простой контур длины 1;

$v_1e_2v_2e_3v_2e_4v_3$ – цепь длины 3, но не является простой цепью.

Граф, состоящий из одного простого цикла с n вершинами, обозначают через C_n , а простую цепь с n вершинами – через P_n . Цикл C_3 называется треугольником.

Рассмотрим два маршрута $\pi_1 = v_1e_1v_2 \dots e_{k-1}v_k$ и $\pi_2 = v_k e_k v_{k+1} \dots e_{r-1}v_r$. Композицией этих маршрутов называется маршрут $\pi_1 \circ \pi_2 = v_1 e_1 v_2 \dots e_{k-1} v_k e_k v_{k+1} \dots e_{r-1} v_r$.

Обозначим $A^k = [a_{ij}^{(k)}]$ – k -ю степень матрицы смежности графа (орграфа).

Теорема. Элемент $a_{ij}^{(k)}$ матрицы A^k ориентированного псевдографа $D = \{V, E\}$ равен числу всех путей длины k из вершины v_i в вершину v_j .

Пример. Для псевдографа, заданного на рисунке 36, найти число всех путей длины 2 и длины 3, соединяющих v_1 с v_2 .

Матрица смежности $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$,

$$A^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Элемент $a_{12}^{(2)}$ матрицы A^2 равен 1 и показывает, что должен существовать один путь длины 2 из вершины v_1 в вершину v_2 .

Рисунок 37 демонстрирует такой путь.

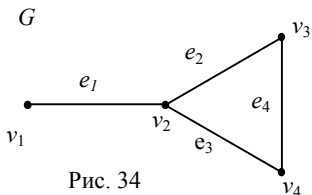


Рис. 34

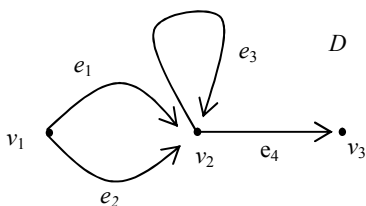


Рис. 35

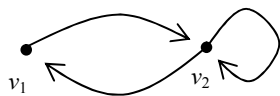


Рис. 36

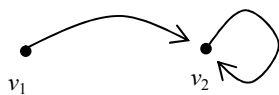


Рис. 37

Элемент $a_{22}^{(2)} = 2$. Рисунок 38 демонстрирует два пути из вершины v_1 в вершину v_2 длиной 2:

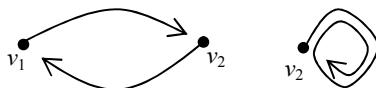


Рис. 38

$$A^3 = A^2 A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}.$$

б) Числовые характеристики на графе

Расстоянием $d(v_i, v_j)$ между вершинами v_i и v_j графа называется минимальная длина простой цепи, соединяющей эти вершины. Кратчайшая простая цепь, соединяющая вершины, называется геодезической линией или просто – геодезической.

Диаметром графа называется величина $d = \max_{v_i, v_j \in V} d(v_i, v_j)$.

Диаметр графа – это длина самой длинной геодезической графа.

Для графа на рисунке 6:

$$d(1, 5) = 3, \quad d(1, 7) = 3,$$

$$d(10, 5) = 5, \quad d = 5.$$

Существуют две самые длинные геодезические, длины которых равны диаметру графа: 10, 9, 8, 7, 6, 5 и 10, 9, 8, 7, 6, 5.

$$\text{Число } r(v_i) = \max_{v_k \in V} d(v_i, v_k)$$

называется *максимальным удалением* в графе от вершины v_i .

Радиусом графа называется число $r = \min_{v_i \in V} r(v_i)$.

Любая вершина $v_i \in V$ такая, что $r(v_i) = r$ называется *центром графа*.

Обхват графа G – обозначение $g(G)$ – это длина кратчайшего простого цикла графа (если он есть).

Окружение графа G (обозначение $c(G)$) – длина самого длинного простого цикла графа.

Если в графе нет циклов, то обхват и окружения не определены.

Для графа на рис. 39:

$$r(1) = 4, \quad r(2) = 4, \quad r(3) = 3, \quad r(4) = 4, \quad r(5) = 5, \quad r(6) = 4, \quad r(7) = 3,$$

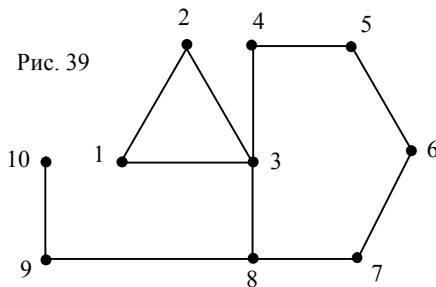
$$r(8) = 3, \quad r(9) = 4, \quad r(10) = 5, \quad r = 3.$$

Вершины 3, 7 и 8 на графе могут быть выбраны в качестве центров данного графа.

Обхват графа на рис. 6 равен 3 и определяется циклом 1, 2, 3, 1.

Окружение графа на рис. 6 равно 6 и определяется циклом 8, 3, 4, 5, 6, 7, 8.

Рис. 39



в) Поиск пути с минимальным количеством ребер

В теории графов одной из важнейших задач является поиск пути на графе из одной данной вершины к другой данной вершине.

Рассмотрим алгоритм поиска пути на графе из вершины a_0 в вершину a_7 , состоящий из минимального количества ребер на рис. 40.

1-й шаг поиска – определяем вершины 1-го поколения, т.е. множество вершин, в которые можно попасть из начальной вершины. Каждой такой вершине поставим в соответствие метку, т.е. вершину, из которой пришла дуга (заполняем метки первого поколения в таблице 9).

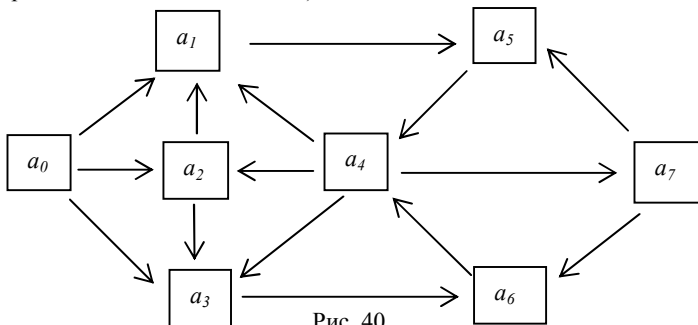


Рис. 40

Таблица 9

вершины	метки 1-го поколения
a_0	
a_1	a_0
a_2	a_0
a_3	a_0
a_4	
a_5	
a_6	
a_7	

Таблица 10

вершины	метки 1-го поколения	метки 2-го поколения
a_0		
a_1	a_0	
a_2	a_0	
a_3	a_0	
a_4		
a_5		a_1
a_6		a_3
a_7		

2-й шаг поиска – находим вершины 2-го поколения. Расставляем метки некоторым из оставшихся неотмеченных вершин, просматривая все вершины, полученные на предыдущем этапе. Если вершина отмечена меткой, то новые метки не ставим (таблица 10).

Аналогично продолжим этот процесс, пока не будет помечена в первый раз конечная вершина (таблица 11).

Таблица 11

вершины	метки 1-го поколения	метки 2-го поколения	метки 3-го поколения	метки 4-го поколения
a_0				
a_1	a_0			
a_2	a_0			
a_3	a_0			
a_4			a_5, a_6	
a_5		a_1		
a_6		a_3		
a_7				a_4

Для наглядности метки разных поколений расположены в разных столбцах, но принят их записывать в один столбец (таблица 12).

Находим искомый маршрут, отправляясь от конечной вершины.

Таблица 12

вершины	метки
a_0	
a_1	a_0
a_2	a_0
a_3	a_0
a_4	a_5, a_6
a_5	a_1
a_6	a_3
a_7	a_4

Для вершины a_7 находим метку a_4 , для вершины a_4 находим метки a_5, a_6 . В этом месте происходит “раздвоение маршрута”.

Если выбираем вершину a_5 , то получаем метку a_1 , а для вершины a_1 – метку a_0 . Таким образом, получаем последовательность $a_7 a_4 a_5 a_4 a_0$.

Если выбираем вершину a_6 , то получаем метку a_3 , а для вершины a_3 – метку a_0 . Таким образом, получаем последовательность $a_7 a_4 a_6 a_3 a_0$.

Переворачивая последовательности, получим два маршрута из минимального количества ребер: $a_0 a_1 a_5 a_4 a_7$, $a_0 a_3 a_6 a_4 a_7$.

Замечание. На графе с небольшим количеством ребер, заданном рисунком, кратчайший маршрут может быть определен визуально быстрее, чем составление таблицы.

Задачи.

27.1. Найдите диаметр, радиус и центры графов на рис. 41, 42:

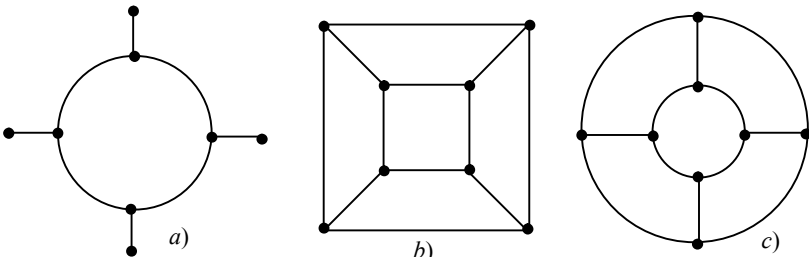


Рис. 41

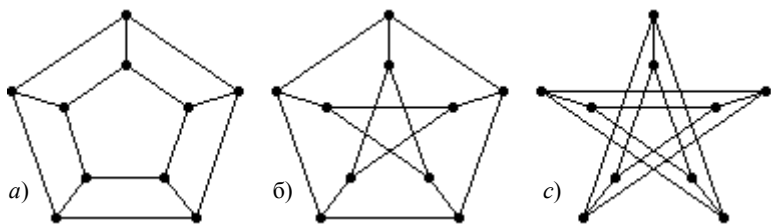


Рис. 42

27.2. Укажите способ построения графа, имеющего единственный центр и радиус которого равен заданному натуральному числу r .

27.3. Укажите способ построения графа, диаметр которого равен заданному натуральному числу d .

27.4. Постройте граф, имеющий 9 вершин, диаметр которого равен 5, радиус графа равен 3, причем граф имеет единственный центр в вершине 9.

27.5. Найдите диаметр n -мерного куба.

27.6. Граф содержит $n+1$ вершину. Всегда ли существует цепь в графе, содержащая n ребер?

27.7. Для следующих орграфов найдите путь минимальной длины из вершины 11 в вершину 3 (рис. 43, 44).

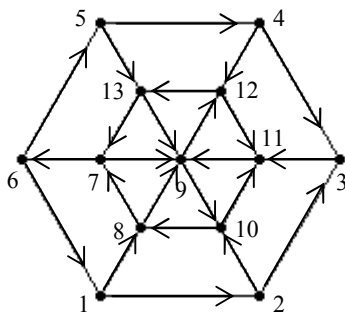


Рис. 43

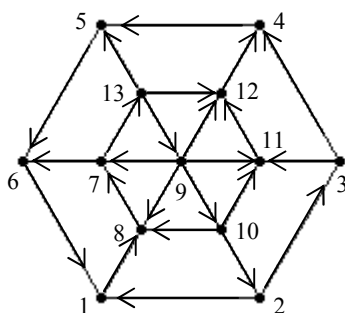


Рис. 44

27.8. Сколько путей существует на орграфе

а) из вершины A в вершину H (рис. 45),

б) из вершины A в вершину L (рис. 46),

в) из вершины A в вершину P (рис. 47),

г) из вершины A в вершину P (рис. 48)?

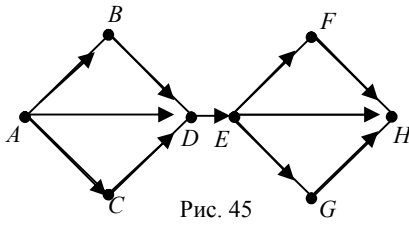


Рис. 45

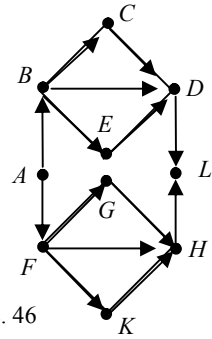


Рис. 46

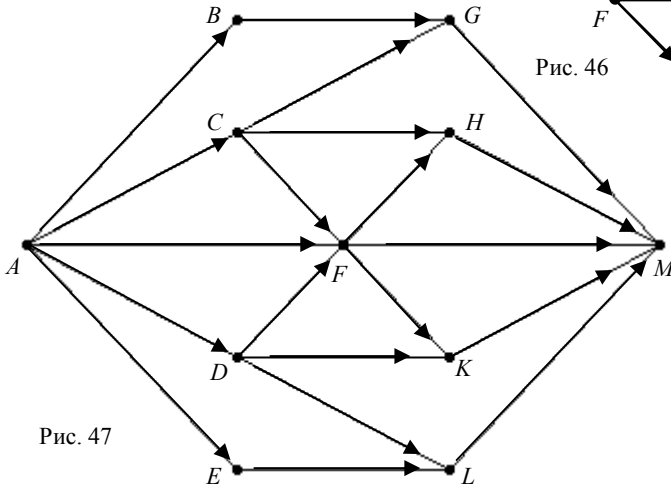


Рис. 47

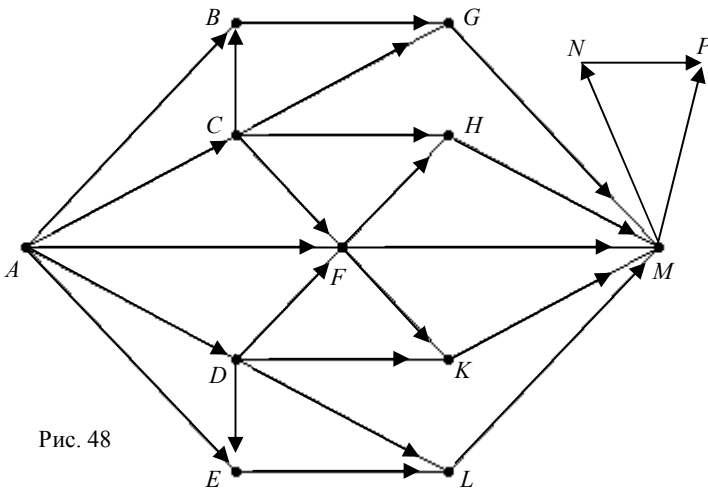


Рис. 48

§ 28. Двудольный граф

Пусть множество вершин V графа G состоит из двух непустых непересекающихся множеств V_1, V_2 , т.е. $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \emptyset$, $V_1 \neq \emptyset$, $V_2 \neq \emptyset$.

Если каждое ребро графа G соединяет некоторую вершину множества V_1 с какой-то вершиной множества V_2 , то граф называется *двудольным*.

Пусть множество V_1 состоит из n_1 вершин, множество V_2 состоит из n_2 вершин, тогда двудольный граф обозначается G_{n_1, n_2} (рис. 49-51).

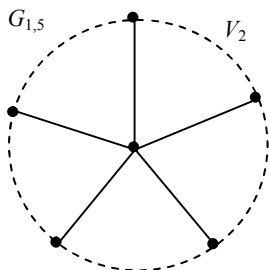


Рис. 49

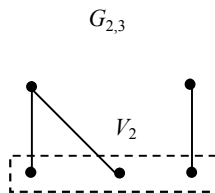


Рис. 50

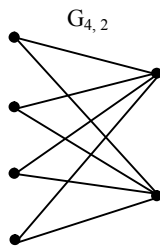


Рис. 51

Двудольный граф называется *полным*, если каждая вершина множества V_1 соединена с каждой вершиной множества V_2 . Обозначение полного двудольного графа K_{n_1, n_2} .

На рисунках 49 и 51 представлены полные двудольные графы.

Полный двудольный граф вида $K_{1, n}$ называется *звездным* графом. На рисунке 49 изображен звездный граф $K_{1,5}$.

В теории графов большое значение имеет граф вида $K_{3,3}$.

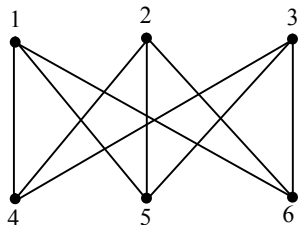


Рис. 52

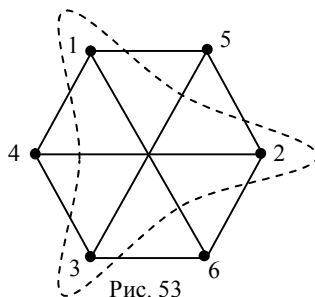


Рис. 53

На рисунках 52 и 53 представлено два изображения графа $K_{3,3}$. Для каждого рисунка множество вершин двудольных графов можно представить в виде $V = \{1, 2, 3, 4, 5, 6\}$, $V_1 = \{1, 2, 3\}$, $V_2 = \{4, 5, 6\}$.

Степень каждой вершины множества V_1 полного двудольного графа K_{n_1, n_2} равна n_2 , т.к. из такой вершины выходят ребра во все вершины множества V_2 . Аналогично, степень каждой вершины множества V_2 полного двудольного графа K_{n_1, n_2} равна n_1 , т.к. из такой вершины выходят ребра во все вершины множества V_1 . Поэтому количество ребер полного двудольного графа равно $m = n_1 n_2$.

Дополнением полного двудольного графа является граф, состоящий из двух компонент. Одна компонента это полный граф с n_1 вершинами. Вторая компонента – это полный граф с n_2 вершинами.

Двудольный граф G_{n_1, n_2} и его дополнение при объединении образуют полный граф с $n_1 + n_2$ вершинами. Число ребер такого графа равно:

$$\frac{(n_1 + n_2)(n_1 + n_2 - 1)}{2}.$$

Вычитая из этого числа количество ребер двудольного графа, получим количество ребер дополнения полного двудольного графа:

$$\frac{n_1^2 + n_2^2 - n_1 - n_2}{2}.$$

Эту величину можно подсчитать другим способом. Для каждой компоненты количество ребер равно

$$m_1 = C_{n_1}^2 = \frac{n_1(n_1 - 1)}{2}, \quad m_2 = C_{n_2}^2 = \frac{n_2(n_2 - 1)}{2}, \quad m = m_1 + m_2.$$

Теорема. Граф является двудольным тогда и только тогда, когда все его простые циклы имеют четную длину [18, с. 198].

Задачи.

- 28.1. Постройте двудольные графы $G_{1,6}$, $G_{2,2}$, $G_{2,5}$.
- 28.2. Постройте неизоморфные двудольные графы $G_{2,3}$ и $G'_{2,3}$.
- 28.3. Постройте полные двудольные графы $K_{2,3}$, $K_{3,4}$.
- 28.4. Постройте с точностью до изоморфизма двудольные графы типа $G_{1,5}$.
- 28.5. Постройте несколько однородных двудольных графов.
- 28.6. Докажите, что n -мерный куб можно рассматривать как двудольный граф.
- 28.7. Сколько ребер имеет полный двудольный граф $G_{7,4}$?
- 28.8. В полном двудольном графе степень каждой вершины множества V_1 равна 8, а степень каждой вершины множества V_2 равна 6. Сколько ребер содержит граф $G_{8,6}$?

§ 29. Связность графа и нахождение простых цепей

Две вершины графа называются *связными*, если существует простая цепь на графе, соединяющая их. Граф называется *связным*, если любая пара его вершин может быть соединена цепью.

Граф Давида (рис. 54) и граф, состоящий только из вершин, т.е. без ребер, являются примерами несвязных графов.

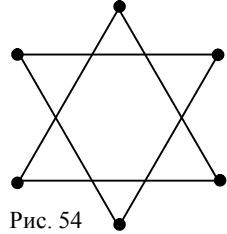


Рис. 54

Связный подграф G_1 графа G называется *связной компонентой* графа G , если не существует подграфа $G_2 \subset G$, такого, что $G_1 \subset G_2 \subset G$.

Пример. На рис. 55 граф имеет три связных компоненты G_1, G_2 и G_3 .

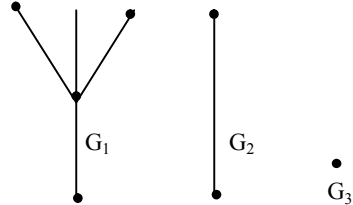


Рис. 55

Вершина графа называется *точкой сочленения*, если ее удаление увеличивает число компонент связности графа.

В любом нетривиальном графе есть по крайней мере две вершины, которые не являются точками сочленения. Например, концы диаметра графа.

Мостом называется ребро, удаление которого увеличивает число компонент связности.

Блоком в графе называется связный подграф, не имеющий точек сочленения.

На рис. 56:

- вершины 3 и 4 - точки сочленения и других точек сочленения нет;
- ребро $\{3,4\}$ - мост и других мостов нет;
- подграфы $\{1,2,3\}$, $\{1,2\}$, $\{2,3\}$, $\{1,3\}$, $\{4,5,6\}$, $\{4,5\}$, $\{5,6\}$, $\{4,6\}$ - примеры блоков.

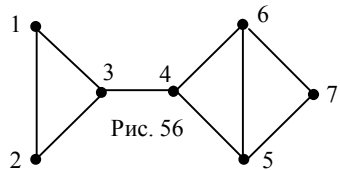


Рис. 56

Рассмотрим задачу о нахождении всех простых цепей, соединяющих две данные вершины графа.

Для графа, изображенного на рис. 57, найдем все цепи с начальной вершиной 1 и конечной вершиной 5.

На первом этапе перечислим все возможности выйти из вершины 1:

1-2, 1-4, 1-6.

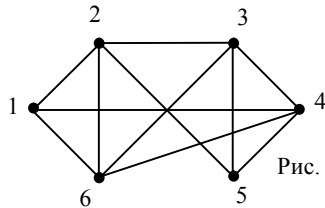


Рис. 57

Конечную вершину пока не достигли.

На втором этапе полученные вершины 2, 4, 6 используем для построения маршрутов длиной два. Возврат в вершину 1 не рассматриваем, т.к. мы определяем простые цепи. Вершины в маршруте не должны повторяться.

Все маршруты длиной 2 с начальной вершиной 1:

$1-2-3, 1-4-3, 1-6-2,$
 $\underline{1-2-5}, \underline{1-4-5}, 1-6-3,$
 $1-2-6, 1-4-6, 1-6-4.$

Мы нашли две простые цепи длиной 2. Они подчеркнуты в таблице.

Все маршруты длиной 3 с начальной вершиной 1:

$1-2-3-4, 1-4-3-2, 1-6-2-3, 1-6-4-3,$
 $\underline{1-2-3-5}, \underline{1-4-3-5}, \underline{1-6-2-5}, \underline{1-6-4-5},$

$1-2-3-6, 1-4-3-6, 1-6-3-2,$

$1-2-6-3, 1-4-6-2, 1-6-3-4,$

$1-2-6-4, 1-4-6-3, \underline{1-6-3-5}.$

Все маршруты длиной 4 с начальной вершиной 1:

$\underline{1-2-3-4-5}, 1-2-6-4-3, 1-4-6-2-3, \underline{1-6-2-3-5},$

$1-2-3-4-6, \underline{1-2-6-4-5}, \underline{1-4-6-2-5}, \underline{1-6-3-2-5},$

$1-2-3-6-4, \underline{1-4-3-2-5}, 1-4-6-3-2, \underline{1-6-3-4-5},$

$1-2-6-3-4, 1-4-3-2-6, \underline{1-4-6-3-5}, 1-6-4-3-2,$

$\underline{1-2-6-3-5}, 1-4-3-6-2, 1-6-2-3-4, \underline{1-6-4-3-5}.$

Все маршруты длиной 5 с начальной вершиной 1:

$\underline{1-2-3-6-4-5}, \underline{1-4-3-6-2-5}, \underline{1-6-2-3-4-5},$

$\underline{1-2-6-3-4-5}, \underline{1-4-6-2-3-5}, \underline{1-6-4-3-2-5},$

$\underline{1-2-6-4-3-5}, \underline{1-4-6-3-2-5}.$

Всего в графе 25 простых цепей из вершины 1 в вершину 5. Среди них: 2 цепи длиной 2, 5 цепей длиной 3, 10 цепей длиной 4 и 8 цепей длиной 5. Цепи длиной 5 содержат все вершины графа.

Задачи.

29.1. Постройте граф, содержащий m ребер, причем каждое ребро является мостом.

29.2. Постройте граф, содержащий два ребра и один блок.

29.3. Постройте граф, содержащий m ребер и m блоков.

29.4. Докажите, что если число ребер графа, не имеющего петель и кратных ребер, с n вершинами ($n > 2$) больше C_n^2 , то граф связан.

29.5. Докажите, что граф (без петель и кратных ребер) с n вершинами, степень каждой из которых не менее $(n-1)/2$ – связан.

29.6. Докажите, что n -мерный куб является связным графом.

29.7. Найдите все простые цепи из вершины 6 в вершину 5 на рис.

57.

29.8. Сколько компонент связности имеют графы (рис. 58)?

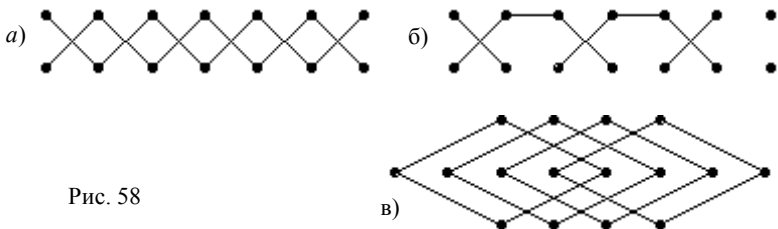


Рис. 58

29.9. В графе 30 вершин, степени всех вершин равны 1. Сколько компонент связности имеет граф?

29.10. Сколько точек сочленения и сколько мостов содержат графы на рис. 59? Определите среди них изоморфные графы.

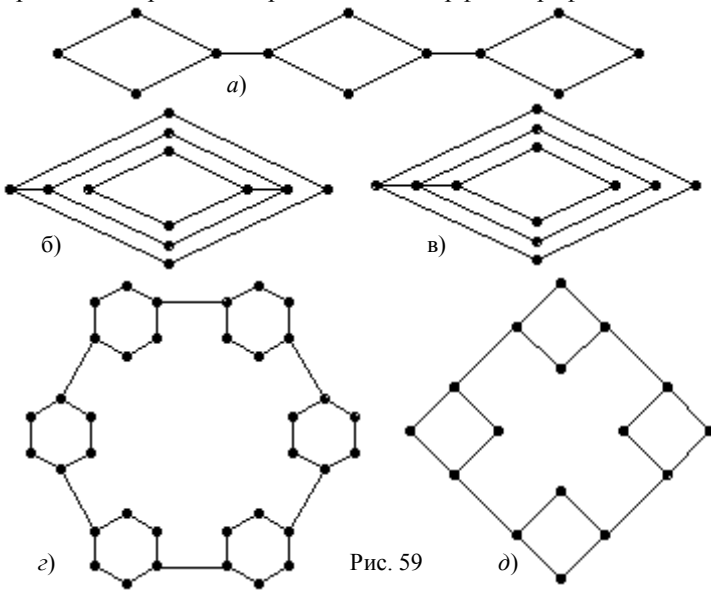


Рис. 59

29.11. Пусть $v_i \rho v_j \leftrightarrow$ существует маршрут с началом v_i и концом v_j . Покажите, что ρ – отношение эквивалентности, и что класс эквивалентности есть связная компонента.

29.12. Докажите, что расстояние $d(u, v)$ между вершинами связного графа G является метрикой, т.е. удовлетворяет следующим свойствам:

- 1) $d(u, v) \geq 0$ для $\forall u, v \in G$, причем $d(u, v) = 0 \leftrightarrow u = v$;
- 2) $d(u, v) = d(v, u)$ для $\forall u, v \in G$;
- 3) $d(u, v) + d(v, w) \geq d(u, w)$ для $\forall u, v, w \in G$.

§ 30. Эйлеровы и гамильтоновы графы

Схема города Кёнигсберга от 1736 г. (рис. 60) показывает, что он расположен на берегах реки Преголи и двух островах. Рассмотрим задачу об определении такого маршрута, чтобы пройти по каждому мосту один раз.

Изобразим берега реки и два острова с помощью вершин графа, мосты с помощью ребер, тогда получаем модель данной задачи на рис. 61. Эта модель игнорирует переходы по берегу от одного моста к другому мосту, переходы по

одному острову, но выделяет главный элемент для данной задачи: расположение мостов.

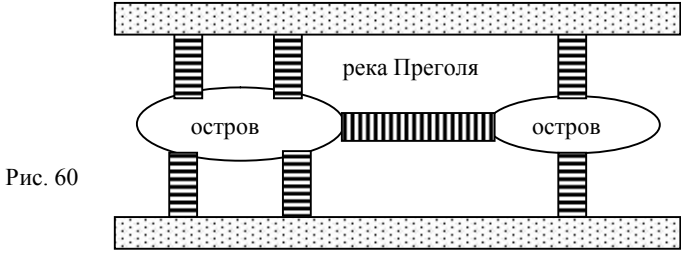


Рис. 60

Попытки обойти весь граф, пройдя по каждому ребру только один раз, и вернуться в исходную точку не удаются. Леонард Эйлер доказал, что такая задача неразрешима для данного графа.

Цикл, содержащий все ребра графа по одному разу, называется *эйлеровым* циклом, замкнутой эйлеровой цепью. Граф, содержащий эйлеров цикл, называется эйлеровым графом.

Граф называется *полуэйлеровым*, если существует цепь (не обязательно простая), содержащая все ребра по одному разу.

Теорема 1. Если в связном графе все вершины имеют четную степень, то этот граф содержит эйлеров цикл, и наоборот, если граф содержит эйлеров цикл, то все его вершины четны [29, 31].

Граф на рисунке 2 имеет все нечетные вершины, поэтому на нем невозможно провести эйлеров цикл.

Теорема 2. Если в связном графе две вершины нечетны, а все остальные четны, то граф содержит эйлерову разомкнутую цепь.

Линию, которую можно провести непрерывным ходом рисования, не проходя участки дважды и не отрывая карандаш от листа бумаги, называется *уникурсальной*. Иногда ее определяют следующим образом. *Уникурсальная линия* – это плоская линия, которую можно обойти, побывав дважды только в точках самопересечения. На рисунке 62 представлена уникурсальная линия.

Теорема 3. Для того чтобы линия была уникурсальной, необходимо и достаточно, чтобы у нее либо не было нечетных вершин, либо было только две нечетные вершины.

Обход уникурсальной линии, имеющей две нечетные вершины, начинается в одной из нечетных вершин и заканчивается в другой нечетной вершине.

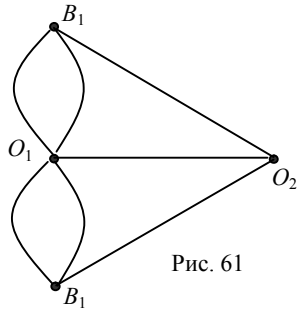


Рис. 61

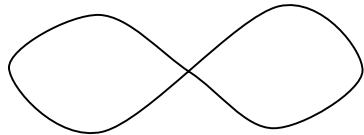


Рис. 62

Правильный додекаэдр – это многогранник, имеющий 12 граней, причем каждая грань является правильным пятиугольником. У. Р. Гамильтон (1805–1865) создал игру – головоломку под названием “Путешествие по свету”. Гамильтон поставил в соответствие каждой вершине додекаэдра название одного из крупных городов: Берлин, Брюссель, Париж, Пекин, Дели и т.д. Играющий должен был найти замкнутый маршрут на додекаэдре, побывав в каждом городе точно по одному разу.

Структуру вершин и ребер додекаэдра можно изобразить на плоскости следующим графом (рис. 63).

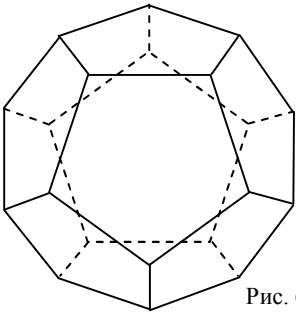


Рис. 63

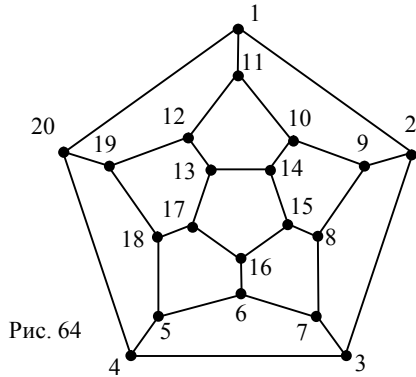


Рис. 64

Цикл, проходящий по одному разу через каждую вершину графа, называется *гамильтоновым циклом*. Граф, содержащий гамильтонов цикл, называется *гамильтоновым*. Гамильтонов цикл на графе 64 определяется указанной последовательностью вершин.

Для графа на рис. 65 гамильтонов цикл показан на рис. 66.

Граф, который содержит простую цепь, проходящую через каждую его вершину, называется *полугамильтоновым*.

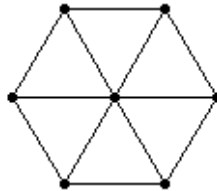


Рис. 65

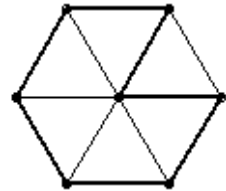


Рис. 66

Некоторые признаки гамильтоновых графов:

а) если n – число вершин графа и степень каждой вершины графа не меньше числа $n/2$, то граф – гамильтонов,

б) если n – число вершин графа и сумма степеней для любых двух несмежных вершин графа не меньше n , то граф – гамильтонов.

Пример 1 (теорема Кенига). Доказать, что в полном орграфе существует гамильтонов путь.

Решение. В орграфе G с n вершинами рассмотрим путь $P = v_1v_2 \dots v_{k-1}v_k$, где $k \leq n-1$, максимальной длины и являющийся простой цепью. Если этот путь содержит все вершины, то он является гамильтоновым путем. Предположим, что

существует вершина a , не принадлежащая этому пути. В полном орграфе эта вершина соединена дугами со всеми остальными вершинами орграфа. Орграф не может содержать дугу (v_k, a) , т.к. в этом случае существует путь большей длины $Pa = v_1v_2\dots v_{k-1}v_k a$, а это противоречит выбору пути P максимальной длины. Следовательно, (a, v_k) . Орграф не может содержать дугу (v_{k-1}, a) (рис. 67), т.к. в этом случае существует путь большей длины $v_1v_2\dots v_{k-1}av_k$. Следовательно, (a, v_{k-1}) . Рассматривая последовательно вершины пути P в обратном направлении от вершины v_k до вершины v_1 , получим последовательность дуг выходящих из вершины a , т.е. $(a, v_k), (a, v_{k-1}), \dots, (a, v_2), (a, v_1)$ (рис. 68). Снова получаем путь большей длины $av_1v_2\dots v_{k-1}v_k$, что противоречит выбору пути максимальной длины. Следовательно, максимальный путь P содержит все вершины орграфа и является гамильтоновым.

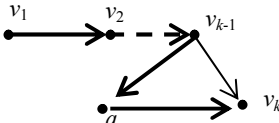


Рис. 67

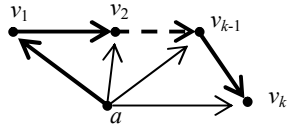


Рис. 68

Рассмотрим применение гамильтоновых путей в машиностроении.

Оптимальная последовательность обработки деталей на двух станках

Имеются токарный станок A , фрезерный станок B и две детали, каждая из которых должна быть вначале обработана на токарном, а затем на фрезерном станке. Токарный и фрезерный станки могут обрабатывать следующую деталь сразу же после обработки предыдущей детали, причем фрезерный станок может обрабатывать деталь только после ее обработки на токарном станке. Время обработки деталей на станках приведено в таблице 1. В какой последовательности требуется обрабатывать детали, чтобы общее время обработки двух деталей оказалось минимальным?

Таблица 13

	1-я деталь	2-я деталь
A	a_1	a_2
B	b_1	b_2

Решение. Пусть вначале обрабатывается первая деталь, тогда:

$a_1 + b_1$ соответствует окончанию обработки первой детали на фрезерном станке,

$a_1 + a_2$ соответствует окончанию обработки второй детали на токарном станке.

Вторую деталь можно начать обрабатывать на фрезерном станке только тогда, когда обе эти операции закончены, т.е. в момент $\max(a_1 + b_1, a_1 + a_2) = a_1 + \max(a_2, b_1)$. Обработка обеих деталей закончится в момент $t_1 = a_1 + \max(a_2, b_1) + b_2$.

Аналогично, если вначале обрабатывается вторая деталь, то момент окончания обработки обеих деталей $t_2 = a_2 + \max(a_1, b_2) + b_1$.

Если $a_1 + \max(a_2, b_1) + b_2 \leq a_2 + \max(a_1, b_2) + b_1$, то обработку деталей выгоднее начать с первой детали.

Используя равенства

$$a_1 + b_2 = \max(a_1, b_2) + \min(a_1, b_2), \quad a_2 + b_1 = \max(a_2, b_1) + \min(a_2, b_1),$$

получаем условие

$$\min(a_1, b_2) \leq \min(a_2, b_1), \quad (1)$$

при котором обработку деталей выгоднее начать с первой детали.

Если рассматривается задача с n деталями, которые также обрабатываются на двух станках, то можно показать [11, с. 459], что из деталей i и j раньше нужно начать обработку детали i если выполняется условие

$$\min(a_i, b_j) \leq \min(a_j, b_i). \quad (2)$$

Изобразим каждую деталь вершиной орграфа и построим дугу от вершины i до вершины j , если выполняется неравенство (2). Любая пара вершин соединена дугами, т.е. оргграф граф является полным. По теореме Кенига в таком графе всегда существует гамильтонов путь. Кратчайший гамильтонов путь на оргграфе и определяет оптимальную последовательность обработки деталей.

Одним из алгоритмов нахождения гамильтонова пути в таком графе состоит в поиске следующей последовательности действий:

- 1) Находим степени выхода $\delta^-(x_i)$ вершин, т.е. количество дуг с начальной вершиной x_i ;
- 2) Располагая вершины в порядке убывания степеней выхода $\delta^-(x_i)$, получим гамильтонов путь.

Пример. Время обработки пяти деталей на станках дано в таблице 14. Найти оптимальную последовательность обработки деталей.

Таблица 14

Детали	1	2	3	4	5
Станок А	1	5	4	2	3
Станок В	3	2	4	6	5

Решение. Для каждой пары вершин проверяем выполнение неравенства 2 и определяем дуги графа (таблица 15).

Таблица 15

Пара вершин	Неравенство	Дуга
1 и 2	$\min(1, 2) < \min(5, 3)$	{1, 2}
1 и 3	$\min(1, 4) < \min(4, 3)$	{1, 3}
1 и 4	$\min(1, 6) < \min(2, 3)$	{1, 4}
1 и 5	$\min(1, 5) < \min(3, 3)$	{1, 5}
2 и 3	$\min(5, 4) > \min(4, 2)$	{3, 2}
2 и 4	$\min(5, 6) > \min(2, 2)$	{4, 2}
2 и 5	$\min(5, 5) > \min(3, 2)$	{5, 2}
3 и 4	$\min(4, 6) > \min(2, 4)$	{4, 3}
3 и 5	$\min(4, 5) > \min(3, 4)$	{5, 3}
4 и 5	$\min(2, 5) < \min(3, 6)$	{4, 5}

Построим оргграф с пятью вершинами и найденными дугами (рис. 69).

Определяем степени выхода вершин:

$$\delta^-(1) = 4, \delta^-(2) = 0, \delta^-(3) = 1,$$

$$\delta^-(4) = 3, \delta^-(5) = 2.$$

По убывающей последовательности степеней вершин: 4, 3, 2, 1, 0 определяем последовательность вершин гамильтонова графа: 1, 4, 5, 3, 2 (рис. 69).

Для гамильтонова пути 1, 4, 5, 3, 2 строим диаграмму работы механизмов *A* и *B* (рис. 70). Общее время обработки деталей равно 21, из которых одна единица времени вызвана простоем механизма *B*.

Для сравнения на рис. 71 построена диаграмма работы механизмов для последовательности обработки деталей 1, 2, 3, 4, 5, предложенной в данной таблице 14. Время обработки деталей в этом случае равно 25. Время простоя механизма *B* в этом случае увеличивается на 4 единицы времени.

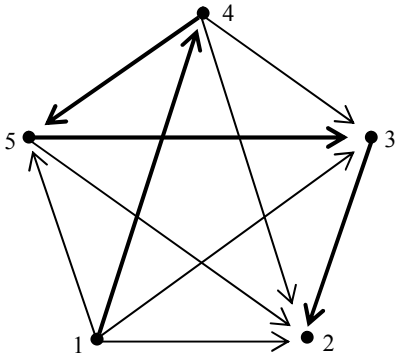


Рис. 69

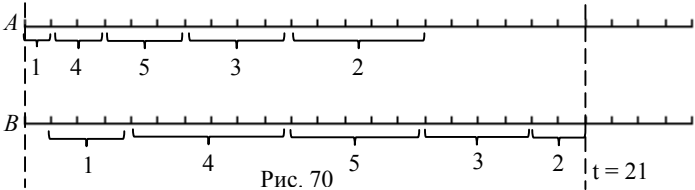


Рис. 70

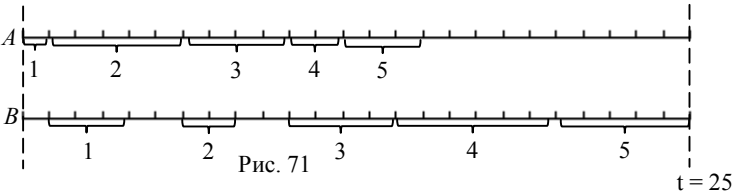


Рис. 71

Задачи.

30.1. На рисунке 72 определите уникурсальные линии. Определите четность внутренней точки уникурсальной линии. Какая четность может быть у вершины, из которой начинается обход линии? Какая четность может быть у вершины, в которой заканчивается обход линии?

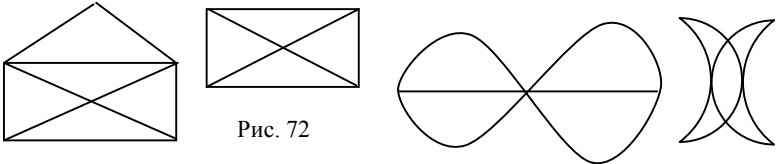


Рис. 72

30.2. Дан граф на рис. 73. Можно ли провести непрерывную линию, которая пересечет все ребра графа во внутренних точках только по одному разу?

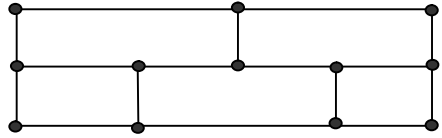


Рис. 73

30.3. Среди следующих графов (рис. 74) определите эйлеровы графы. На эйлеровом графе укажите эйлеров цикл.

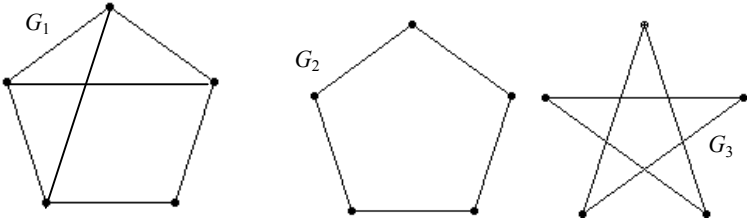


Рис. 74

30.4. На рисунке 64 укажите гамильтонов цикл, если первыми двумя вершинами маршрута являются вершины 1, 11.

30.5. Гамильтонов цикл на додекаэдре является эйлеровым циклом?

30.6. Граф в задаче о прохождении всех мостов в Кенигсберге является гамильтоновым?

30.7. Докажите, что полный граф, имеющий не менее трех вершин, является гамильтоновым.

30.8. Является ли граф, имеющий висячую вершину, гамильтоновым? Может ли полугамильтонов граф содержать две висячие вершины?

30.9. Являются ли графы на рисунке 75, гамильтоновыми?

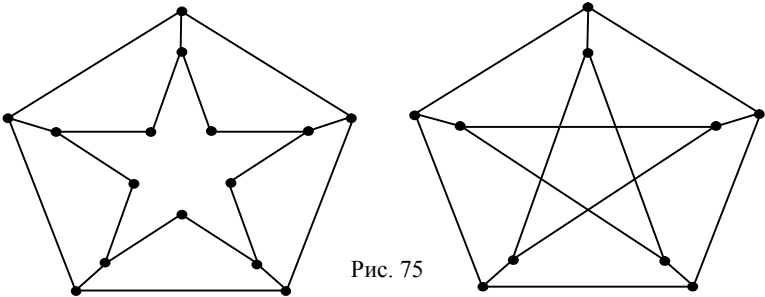


Рис. 75

30.10. Существует пять платоновых тел, т.е. правильных многогранников: тетраэдр, куб, октаэдр, додекаэдр, икосаэдр. Икосаэдр изображен на рис. 76. Постройте графы остальных пяти платоновых тел. Какие из них являются гамильтоновыми, а какие эйлеровыми графами?

30.11. Граф содержит изолированную вершину.

а) Может ли такой граф быть эйлеровым?

б) Может ли такой граф быть гамильтоновым?

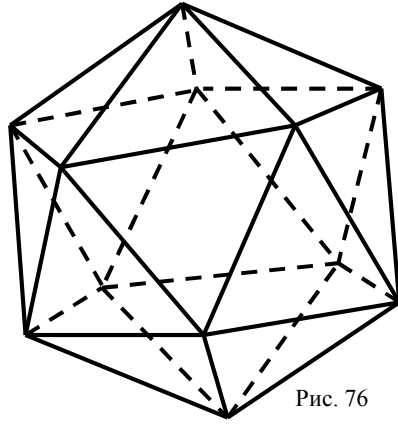


Рис. 76

30.12. Дан звездный граф $G_{1,n}$.

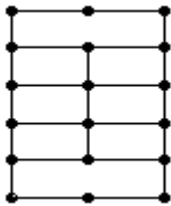
а) Может ли он быть эйлеровым графом?

б) Может ли он быть гамильтоновым графом?

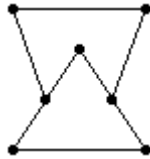
30.13. Дан полный граф с пятью вершинами. Покажите на нем несколько различных гамильтоновых циклов.

30.14. Дан полный двудольный граф $G_{3,3}$. Покажите на нем несколько различных гамильтоновых циклов.

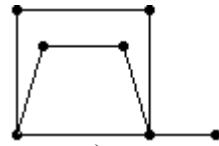
30.15. Поясните, почему следующие графы (рис. 77) являются полугамильтоновыми.



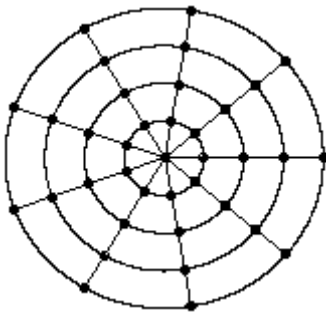
а)



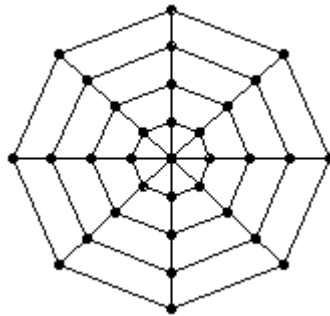
б)



в)



г)



д)

Рис. 77

30.16. Докажите, что полный граф K_n имеет гамильтонов цикл.

30.17. Докажите, что если граф содержит висячую вершину, то он не является гамильтоновым.

30.18. Гамильтонов граф является полугамильтоновым графом? А на оборот?

30.19. Существует ли двудольный граф, содержащий:

а) эйлеров цикл; б) гамильтонов цикл?

30.20. Сколько гамильтоновых циклов существует на графах (рис. 78).

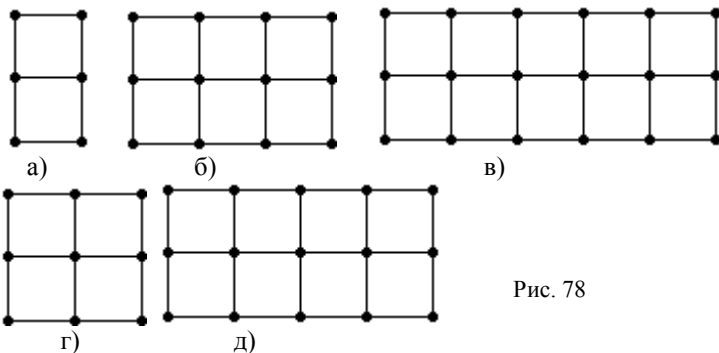


Рис. 78

Таблица 16

Аттестуемые	1	2	3	4	5
Эксперт A	40	50	29	30	48
Эксперт B	30	45	48	20	15

двух экспертов проводят аттестацию пяти сотрудников отдела. Эксперт A проверяет соответствие представленных документов утвержденным критериям должностей и уточняет в беседе с аттестуемым его видение перспективы развития отдела. Эксперт B , после получения проверенной документации на аттестуемого, проверяет его профессиональные знания и навыки. Время собеседования и время тестирования пяти сотрудников дано в таблице 16. Найдите оптимальную последовательность работы с аттестуемыми, чтобы минимизировать время работы экспертной комиссии.

Таблица 17

Больной	1	2	3	4	5
Подготовка	10	50	40	20	30
Операция	30	20	40	60	50

Для каждой операции рекомендован средний норматив времени на подготовку к операции и средний норматив выполнения операции в таблице 17. Найдите оптимальную последовательность выполнения операций.

30.21. Два эксперта проводят аттестацию пяти сотрудников отдела. Эксперт A проверяет соответствие представленных документов утвержденным критериям должностей и уточняет в беседе с аттестуемым его видение перспективы развития отдела. Эксперт B , после получения проверенной документации на аттестуемого, проверяет его профессиональные знания и навыки.

30.22. На вторник в стационаре назначены пять различных операций. Каждый из больных вначале проходит подготовку к операции, а затем выполняется операция.

§ 31. Плоские и планарные графы. Теорема Эйлера

Граф называется *плоским*, если он изображен на плоскости таким образом, что любые его ребра пересекаются только в вершине графа.

Схема вершин и ребер параллелепипеда может быть изображена плоским графом (рис. 79).

Схема вершин и ребер любой усеченной пирамиды может быть изображена плоским графом (рис. 80).

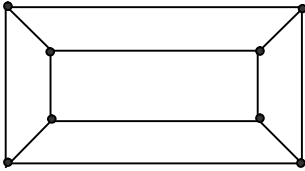


Рис. 79

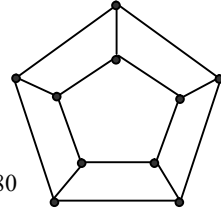


Рис. 80

Граф, изоморфный плоскому графу, называется *планарным*.

Всякий плоский граф является планарным, но обратное утверждение не всегда справедливо.

На рисунке 81 изображен плоский граф, а на рисунке 82 – планарный граф.

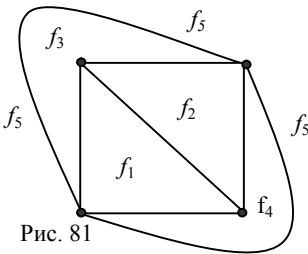


Рис. 81

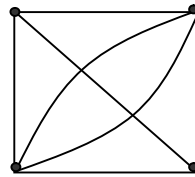


Рис. 82

Часть плоскости, ограниченную замкнутой линией, будем называть *гранью*. Каждая петля ограничивает некоторую область, которая может быть названа гранью псевдографа. Два кратных ребра мультиграфа ограничивают область, которая может быть названа гранью. Любой многоугольник разбивает плоскость на две области, одну область называют внутренней, а вторую – внешней относительно многоугольника. Обе эти области будем называть гранями графа. Граф на рисунке 81 имеет четыре внутренних области: f_1, f_2, f_3, f_4 и одну внешнюю f_5 , т.е. граф имеет 5 граней.

Величина $\chi = n - m + f$, где n – число вершин, m – число ребер, f – число граней графа, называется *эйлеровой характеристикой* графа.

Для плоских графов на рисунках 79–81 эйлерова характеристика равна 2.

Теорема 1. Эйлерова характеристика связного плоского графа равна 2, т.е.

$$\chi = n - m + f = 2.$$

Теорема 2. Если плоский граф не является связным и состоит из k компонент, то справедлива формула $\chi = n - m + f = k + 1$.

При монтаже радиоэлектронных устройств печатным способом соединение элементов желательнее располагать таким образом, чтобы они не пересекались, чтобы избежать изоляции между слоями. Поэтому становится актуальным вопрос о возможности изобразить данный граф в виде плоского графа, т.е. выясняется вопрос о планарности данного графа.

Критерий Понтрягина – Куратовского: граф является планарным тогда и только тогда, когда он не содержит подграфов, гомеоморфных графам K_5 или $K_{3,3}$.

Любой граф с числом вершин $n = 1, 2, 3, 4$ является планарным. Всякий граф с пятью вершинами является планарным, если он не является полным графом.

Теорема 3. Пусть заданы числа n, m, f , где $n \in N, f \in N, m \in N \cup \{0\}$, $n = m + f + 2$. Тогда существует связный плоский граф, для которого n – число вершин, m – число ребер, f – число граней.

Доказательство. В связном плоском графе с n вершинами число ребер удовлетворяет условию $m \geq n - 1$, следовательно, $m - n + 1 \geq 0$.

Число m представим в виде $m = (n - 1) + (m - n + 1)$.

Если $n = 1$, то граф, состоящий из одной точки, удовлетворяет условию теоремы.

Если $n \geq 2$, то вначале построим звездный граф $G_{1, n-1}$ (рис. 83), расположив вершину 1 в центре произвольной окружности, остальные вершины 2, 3, ..., $n - 1$ на окружности и построим $n - 1$ ребер графа, соединяющих вершину 1 с остальными вершинами.

Далее построим $m - n + 1$ кратных ребер, соединяющих вершины 2 и 3, причем ребра имеют общие точки только в этих вершинах. Полученный граф удовлетворяет условиям теоремы.

Задачи.

31.1. Докажите, что граф, изображающий структуру вершин и ребер выпуклого замкнутого многогранника, можно изобразить плоским графом. Найдите эйлерову характеристику такого графа.

31.2. Сколько граней содержат графы на рис. 84–86. Поясните выполнимость формулы $\chi = n - m + f = k + 1$ для этих графов.

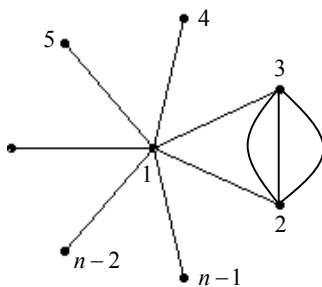


Рис. 83

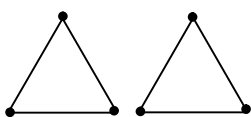


Рис. 84

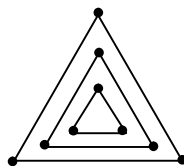


Рис. 85

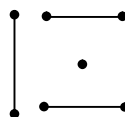


Рис. 86

31.3. Какие из следующих графов (рис. 87) являются плоскими, а какие планарными?

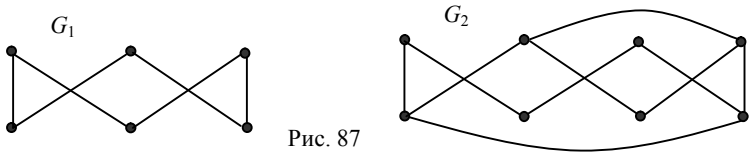


Рис. 87

31.4. Какое наименьшее число ребер нужно удалить на графе Петерсона, чтобы получить планарный граф?

31.5. Какое наименьшее число граней может быть у плоского 5-вершинного графа, не имеющего петель и кратных ребер?

31.6. Докажите, что полный граф с пятью вершинами не является плоским.

31.7. Планарный граф имеет 12 вершин со степенями 3. Сколько у него ребер и граней? Постройте такой граф.

31.8. Проверьте каждый из следующих графов (рис. 88) на планарность. Ответ поясните.

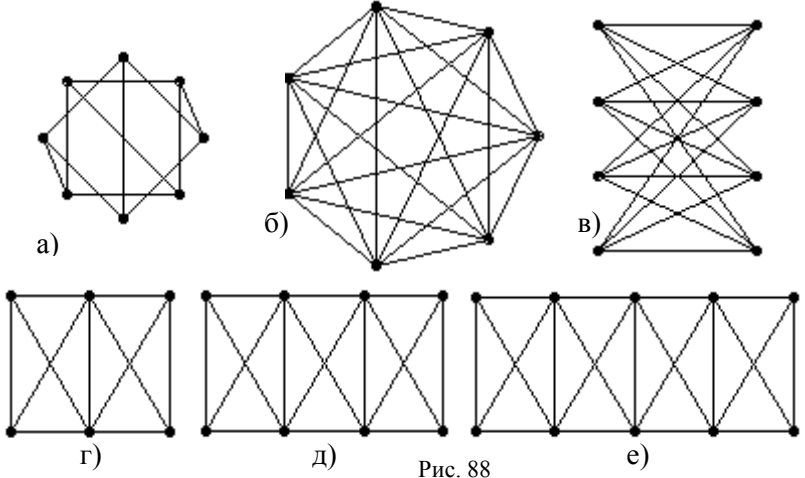


Рис. 88

31.9. Какое наибольшее число граней может содержать связный, плоский мультиграф (псевдограф) с n вершинами и m ребрами?

31.10. Какое наименьшее число граней может содержать плоский граф с n вершинами?

31.11. В связном плоском графе 20 граней и 30 ребер. Сколько в нем вершин?

31.12. В связном плоском графе 30 вершин и 29 ребер. Сколько в нем граней?

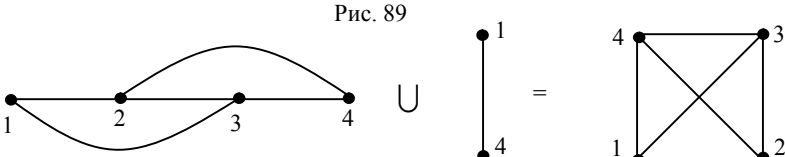
31.13. В связном плоском графе число ребер равно 20, число вершин равно числу граней. Сколько в нем вершин?

31.14. Кубический граф является планарным графом?

§ 32. Операции над графами

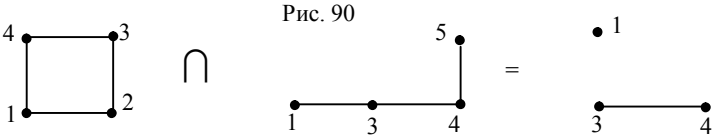
Объединением двух графов $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ называется граф $G = \{V, E\}$, где $V = V_1 \cup V_2$, $E = E_1 \cup E_2$.

Пример 1 на рис. 89.



Пересечением двух графов $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ называется граф $G = \{V, E\}$, где $V = V_1 \cap V_2$, $E = E_1 \cap E_2$.

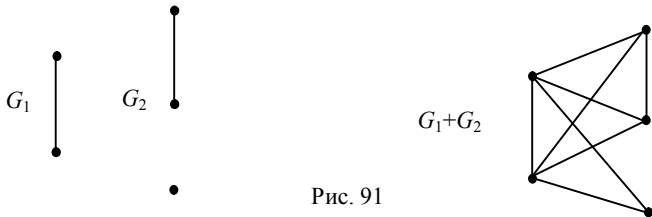
Пример 2 на рис. 90.



Граф $G' = (V', E')$ называется *подграфом* графа $G = (V, E)$, если $V' \subset V$, $E' \subset E$.

Пусть графы $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ имеют непересекающиеся множества вершин V_1 и V_2 и непересекающиеся множества ребер E_1 и E_2 .

Соединением двух графов $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ называется граф $G_1 + G_2$, множество вершин которого $V = V_1 \cup V_2$, а множество ребер состоит из ребер графа G_1 , ребер графа G_2 и всех ребер, соединяющих вершины из V_1 и V_2 .



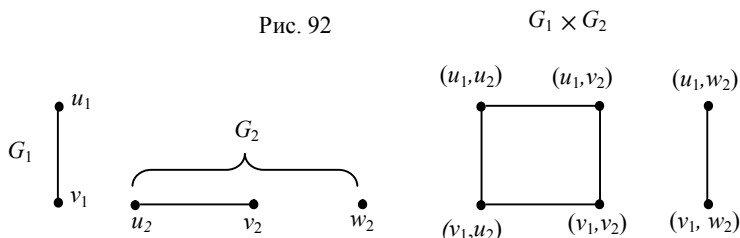
Пример 3 на рис. 91.

Если две вершины u и v связаны на графе ребром, то будем записывать следующим образом $u \text{ adj } v$ [adjacent – смежный].

Произведением двух графов $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ называется граф $G_1 \times G_2$, множество вершин которого $V = V_1 \times V_2$, причем две вершины $u = (u_1, u_2)$, $v = (v_1, v_2)$ являются смежными тогда и только тогда, когда либо $u_1 = v_1$, $u_2 \text{ adj } v_2$, либо $u_2 = v_2$, $u_1 \text{ adj } v_1$, т.е.

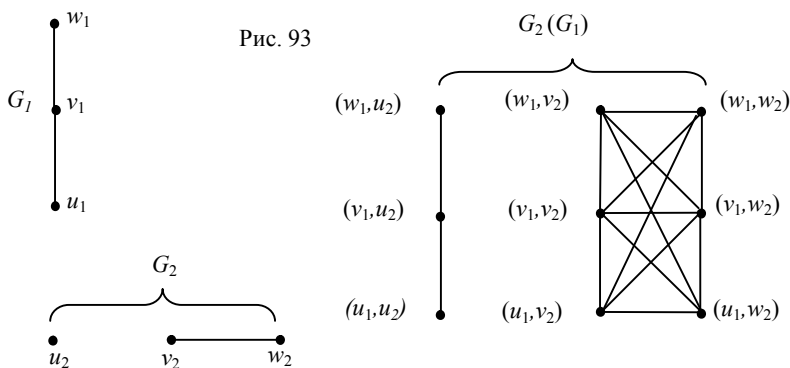
$$(u_1, u_2) \text{ adj } (v_1, v_2) \Leftrightarrow \left[\begin{array}{l} (u_1 = v_1) \wedge (u_2 \text{ adj } v_2) \\ (u_2 = v_2) \wedge (u_1 \text{ adj } v_1) \end{array} \right]$$

Пример 4 на рис. 92.



Композицией двух графов $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ называется граф $G = G_2(G_1)$, множество вершин которого $V = V_1 \times V_2$, причем две вершины $u = (u_1, u_2)$, $v = (v_1, v_2)$ являются смежными тогда и только тогда, когда либо $u_2 \text{ adj } v_2$, либо $u_2 = v_2$, $u_1 \text{ adj } v_1$.

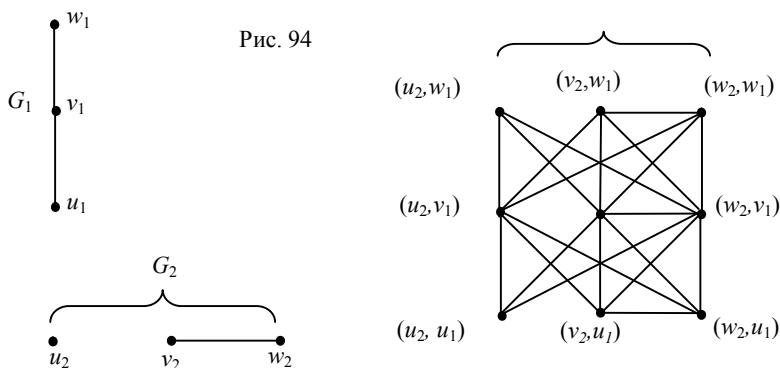
Пример 5 на рис. 93.



Композиция графов $G = G_2(G_1)$ означает следующее: на граф G_1 действует граф G_2 по следующему алгоритму (рис. 94):

- рисуем столько копий графа G_1 , сколько вершин в графе G_2 ,
- любые две вершины копий с разными номерами соединяем ребром, если в графе G_2 вершины с такими номерами были соединены ребром, т.е. в этом случае все точки одной копии соединяются с каждой точкой другой копии ребрами.

Сравните композицию $G_2(G_1)$ с композицией $G_1(G_2)$.



Задачи.

- 32.1. Найдите объединение и пересечение графа и его дополнения.
- 32.2. Найдите объединение и пересечение графа G с этим же графом.
- 32.3. Для двух графов выполняется свойство $G_1 \cup G_2 = G_1$. Найдите граф G_2 .
- 32.4. Для двух графов выполняется свойство $G_1 \cap G_2 = G_1$. Найдите граф G_2 .
- 32.5. Постройте какой-нибудь граф с шестью вершинами. Представьте его несколькими способами как объединение двух графов.
- 32.6. Для операции объединения графов выполняются свойства коммутативности и ассоциативности? А для пересечения графов?
- 32.7. Даны четыре графа $G_1, G_2, G_1 \cup G_2, G_1 \cap G_2$. Какой из этих графов является подграфом другого графа?

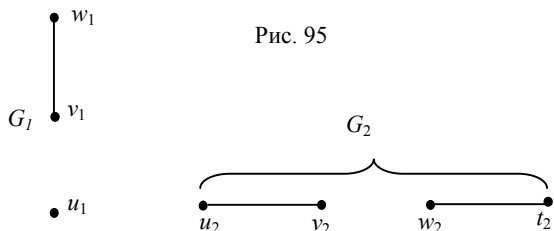


Рис. 95

32.8. Для следующих графов (рис. 95) найдите $G_1 + G_2$, $G_1 \times G_2$, $G_2(G_1)$, $G_1(G_2)$.

32.9. Докажите, что если графы $G_1 = \{V_1, E_1\}$ и $G_2 = \{V_2, E_2\}$ имеют непересекающиеся множества вершин V_1 и V_2 и непересекающиеся множества ребер E_1 и E_2 , причем n_1, m_1 количество вершин и ребер в первом графе, а n_2, m_2 количество вершин ребер во втором графе, то для операций количество вершин и количество ребер вычисляется по таблице 18.

Таблица 18

Операции	Число вершин	Число ребер
$G_1 \cup G_2$	$n_1 + n_2$	$m_1 + m_2$
$G_1 + G_2$	$n_1 + n_2$	$m_1 + m_2 + n_1 n_2$
$G_1 \times G_2$	$n_1 n_2$	$n_1 m_2 + n_2 m_1$
$G_2(G_1)$	$n_1 n_2$	$n_1^2 m_2 + n_2 m_1$

32.10. Докажите, что если оба графа G_1 и G_2 имеют по изолированной вершине, то графы $G_1 \times G_2$, $G_2(G_1)$, $G_1(G_2)$ также имеют изолированные вершины.

32.11. Докажите, что если графы G_1 и G_2 изоморфны, то графы $G_1 \times G_3$ и $G_2 \times G_3$ также изоморфны.

32.12. Докажите, что объединение графа и его дополнения является полным графом.

32.13. Докажите, что пересечение графа $G = (V, E)$ и его дополнения является графом с множеством вершин V и не содержит ребер.

§ 33. Деревья, лес и остов графа

Связный граф называется *деревом*, если он не имеет циклов.

Число неизоморфных деревьев с n вершинами приведено в таблице 19.

Таблица 19

n	1	2	3	4	5	6	7	8	9	10
t_n	1	1	1	2	3	6	11	23	47	105

В приложении 2 построены деревья с числом вершин не более 8.

Если нумерация вершин и положение вершин графа зафиксированы, то можно построить n^{n-2} (формула Кэли) деревьев с n вершинами.

Для $n = 3$ получаем три дерева (рис. 96), которые все изоморфны.



Рис. 96

Для $n = 4$ получаем 16 деревьев (рис. 97). Все эти деревья изоморфны двум существенно различным деревьям (сравните с рисунками деревьев в приложении 2).

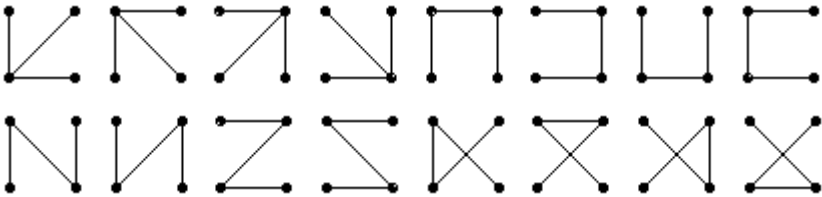
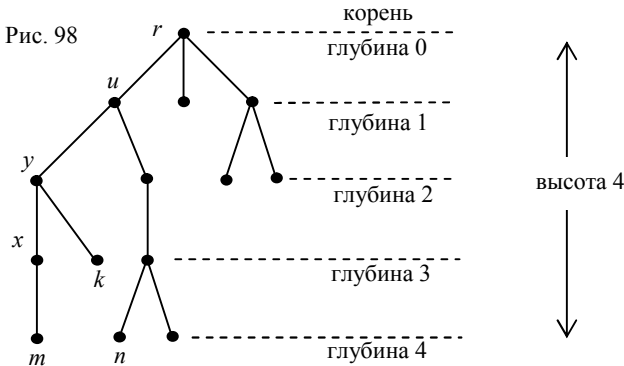


Рис. 97

Если в дереве выделена одна из вершин, то она называется *корнем* дерева, а само дерево – *деревом с корнем*. Рассмотрим терминологию, принятую в теории алгоритмов для дерева с корнем r (рис. 98).



Пусть x – произвольная вершина дерева с корнем. Существует единственный путь из корня r в вершину x . Все вершины, находящиеся на этом пути, называются

ся *предками* вершины x . Если вершина y является предком вершины x , то вершина x называется *потомком* y .

Для каждой вершины u можно рассмотреть дерево с корнем u , состоящее из всех потомков u . Оно называется *поддеревом* данного дерева.

Если (y, x) – последнее ребро на пути из корня в вершину x , то y называется родителем x , а x называется ребенком для y . Корень является вершиной дерева, у которой нет родителя.

Листом дерева называется вершина дерева, не имеющая детей, т.е. вершина, в которой завершается маршрут поиска. На рис. 98 вершины m, k являются листьями.

Лист дерева может быть определен как висячая (концевая) вершина, т.к. в ней степень равна 1.

Ребро, инцидентное концевой вершине, называется *концевым*.

Задание корня дерева, введение понятий “родитель”, “ребенок” фактически определяют ориентацию на графе от корня к листьям или наоборот. В дальнейшем будем считать, что на дереве с корнем задана ориентация дуг от корня к листьям, а корень дерева расположен выше всех вершин.

Вершина, имеющая детей, называется *внутренней*. На рисунке 98 вершины x, y, u – внутренние.

Длина пути от корня (в нашем случае от самой верхней вершины) до произвольной вершины называется *глубиной* вершины.

Максимальная глубина вершины дерева называется *высотой* дерева.

Длина E внешнего пути дерева (внешняя сумма длин) определяется как сумма глубин всех листьев.

Длина I внутреннего пути дерева (внутренняя сумма длин) определяется как сумма глубин всех внутренних вершин.

Для этих характеристик выполняется равенство $E = I + 2k$, где k – число внутренних вершин.

Рассмотрим конечное дерево G . Вершинами типа 1 называются его концевые вершины. Удалим из дерева G все вершины типа 1 и инцидентные им концевые ребра. В оставшемся дереве G' концевые вершины называются вершинами типа 2 для данного дерева G . Аналогично определяются вершины 3, 4 и т.д. типов. В конечном дереве найдутся вершины максимального типа.

На рисунке 99 возле вершин расставлены типы этих вершин. Маленькими черточками на рисунке отмечены последовательные удаления ребер для каждого типа точек.

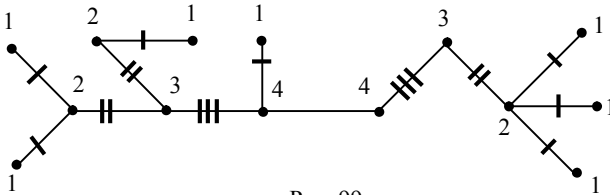


Рис. 99

Имеют место следующие простые теоремы о деревьях.

Теорема 1. Любые две вершины дерева соединены только одной простой цепью.

Теорема 2. Дерево, имеющее n вершин, содержит $n - 1$ ребер.

Теорема 3. Соединив любые две вершины дерева, получим цикл в новом графе.

Остовом связного графа называется любой его подграф, содержащий все вершины данного графа и являющийся деревом.

На рисунке 100 изображен граф G и несколько его остовов.

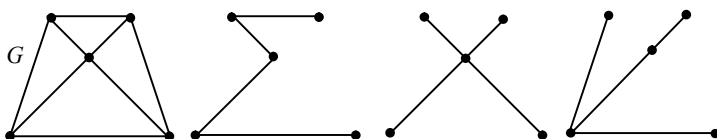


Рис. 100

Граф, все компоненты связности которого являются деревьями, называется *лесом*.

Теорема 4. Лес, имеющий n вершин и состоящий из k компонент, содержит $n - k$ ребер.

Пусть G – граф, имеющий n вершин, m ребер и k компонент, тогда величина $\gamma(G) = m - n + k$ называется *цикломатическим числом* графа.

Для связного графа $k = 1$ и цикломатическое число равно $m - n + 1$.

Геометрический смысл цикломатического числа заключается в следующем. Если компонента содержит цикл, то удаление любого ребра из цикла разрушает этот цикл, но сохраняет связность компоненты. Применим эту процедуру к каждому циклу, пока не останется циклов. Получим остов графа. Количество необходимых удалений ребер равно $m - (n - k) = m - n + k$, т.е. равно цикломатическому числу графа. Таким образом, число $\gamma(G)$ показывает, какое количество ребер необходимо удалить на графе, чтобы получить остов графа.

Корневой граф, изображенный на любом рисунке, можно задать аналитически *кодом* дерева.

Каждому дереву с m ребрами поставим в соответствие вектор длины $2m$ из нулей и единиц. Обход дерева начинается с корня. Первый проход ребра обозначаем нулем, а повторный проход по этому ребру обозначаем единицей. Из возможных вариантов выхода из вершины выбираем вначале продолжение обхода по крайнему левому из непройденных ребер. После прихода в вершину, являющуюся листом, возвращаемся назад. Если есть непройденное ребро правее, то двигаемся по нему от корня, в противном случае возвращаемся на одно ребро к корню. Заканчивается обход в корне дерева. Каждый код дерева содержит равные количества нулей и еди-

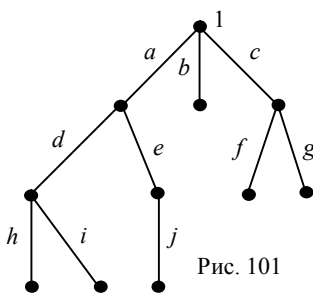


Рис. 101

ниц.

Пример 1. Для графа с корнем 1 на рис. 101 обозначим ребра произвольным образом.

Обход графа задается следующей последовательностью: *adhhiidejjeabbcffggc*.

Кодируем последовательность следующим образом – если символ, обозначающий ребро, встречается первый раз, то записываем 0, а если повторяется, то записываем 1.

Код дерева 00010110011101001011.

Замечание. Обозначение ребер не является обязательным. В примере было применено обозначение ребер, чтобы пояснить последовательность обхода ребер. Дерево можно сразу кодировать числовой последовательностью.

Построение дерева по коду выполняется по следующему алгоритму.

Выбираем точку, которую назовем корнем дерева. Двигаемся по числовой последовательности слева направо. Если рассматриваемая цифра равна нулю, то рисуем новое ребро, а если единице, то возвращаемся в обратном направлении по последнему нарисованному ребру. Каждое ребро рисуется таким образом, чтобы не получался цикл.

Рассмотрим кодирование дерева *методом Пруфера*.

Пусть дано дерево, вершины которого обозначены 1, 2, 3, ..., *n*. Среди висячих вершин находим вершину с наименьшим номером. Удаляем эту вершину с инцидентным ей ребром и записываем номер оставшейся вершины удаленного ребра в код. Повторяем эту операцию с висячими вершинами. Процесс заканчивается, когда остается ребро с двумя вершинами. Число записанных вершин в коде Пруфера на 2 меньше, чем число вершин в данном дереве.

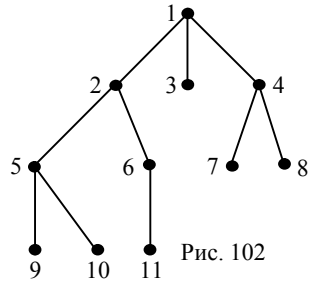


Рис. 102

Если граф имеет *n* вершин, то код Пруфера содержит *n* – 2 числа.

В коде Пруфера отсутствуют висячие вершины данного дерева.

Пример 2. Построить код дерева на рис. 102.

Решение приведено в таблице 20.

Таблица 20

Висячие вершины	Удаляем вершину	Кодирование
3,7,8,9,10,11	3	K=1...
7,8,9,10,11	7	K=14...
8,9,10,11	8	K=144...
4, 9,10,11	4	K=1441...
1, 9,10,11	1	K=14412...
9,10,11	9	K=144125...
10,11	10	K=1441255...
5,11	5	K=14412552...
2,11	2	K=144125526

Код Пруфера данного графа $K=144125526$.

Замечание. Если дерево содержит большое количество вершин, то появляющиеся числа в коде разделяются запятыми, чтобы однозначно понимать номера записанных вершин.

Пример 2. Построить дерево по данному коду Пруфера $K=144125526$.

Код содержит 9 чисел, следовательно, дерево содержит 11 вершин: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. В коде нет номеров висячих вершин. Запишем их номера в возрастающем порядке

$$W=\{3, 7, 8, 9, 10, 11\}.$$

Составим из цифр кода множество, элементы которого могут повторяться и записаны в том же порядке, как и в коде

$$K=(1, 4, 4, 1, 2, 5, 5, 2, 6).$$

Выбираем в множестве K элементы слева направо, а в множестве W наименьшее число.

На первом шаге вершина $1 \in K$ соединяется с вершиной $3 \in W$. Вершину 1, записанную первый раз в множестве K , удаляем из множества K , а из множества W удаляем вершину 3.

Оформим действия в таблице 21.

Таблица 21

Множество K	Множество W	Новое ребро	Примечания
(1, 4, 4, 1, 2, 5, 5, 2, 6)	{3, 7, 8, 9, 10, 11}	(1, 3)	
(4, 4, 1, 2, 5, 5, 2, 6)	{7, 8, 9, 10, 11}	(4, 7)	
(4, 1, 2, 5, 5, 2, 6)	{8, 9, 10, 11}	(4, 8)	Вершина 4 больше не повторяется в K , переводим ее в W .
(1, 2, 5, 5, 2, 6)	{4, 9, 10, 11}	(1, 4)	Вершина 1 больше не повторяется в K , переводим ее в W .
(2, 5, 5, 2, 6)	{1, 9, 10, 11}	(2, 1)	
(5, 5, 2, 6)	{9, 10, 11}	(5, 9)	
(5, 2, 6)	{10, 11}	(5, 10)	Вершина 5 больше не повторяется в K , переводим ее в W .
(2, 6)	{5, 11}	(2, 5)	Вершина 2 больше не повторяется в K , переводим ее в W .
(6)	{2, 11}	(6, 2)	Вершина 6 больше не повторяется в K , переводим ее в W .
	{6, 11}	(6, 11)	

Задачи.

33.1. Изобразите дерево для графа на рисунке 102, если

- корень выбран в вершине 3;
- корень выбран в вершине 7;

в) корень выбран в вершине 11.

33.2. Сравните длины внешних путей для каждого из вышепостроенных деревьев с корнем в задаче 33.1.

33.3. Сравните длины внутренних путей для каждого из вышепостроенных деревьев с корнем в задаче 33.1.

33.4. В дереве как частном случае графа можно определить центр графа. Имеется ли связь между центром дерева и вершиной максимального типа дерева? Сколько может быть вершин максимального типа?

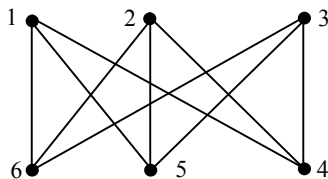


Рис. 103

33.5. Для графа (рис. 103) постройте несколько остовов графа.

33.6. Изобразите дерево с восьмью вершинами, причем степень каждой вершины не превосходит 2.

а) Какую вершину надо объявить корнем, чтобы высота дерева была наибольшей?

б) Какую вершину надо объявить корнем, чтобы высота дерева была наименьшей?

33.7. Дерево имеет девять вершин, причем две вершины имеют степень 3, а степени остальных вершин не превосходят 2. Сколько существует неизоморфных деревьев такого типа?

33.8. Постройте лес, каждое дерево которого содержит 5 вершин и деревья не изоморфны.

33.9. Постройте лес, высота деревьев которого не более 5, причем любые два дерева отличаются числом вершин.

33.10. В связном графе 20 вершин. Сколько ребер содержит его произвольный остов?

33.11. В связном графе 18 вершин и 30 ребер. Сколько ребер необходимо удалить, чтобы получить остов этого графа?

33.12. В дереве 30 ребер. Сколько ребер необходимо удалить, чтобы получить лес из 20 деревьев?

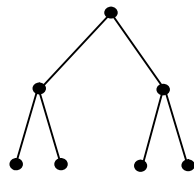


Рис. 104

33.13. На рис. 104 представлено полное бинарное дерево с корнем высотой 2, в котором степень выхода каждой вершины, не являющейся листом, равна 2 и все листья находятся на одной глубине.

а) Найдите код обхода всех вершин дерева с корнем;

б) найдите код обхода вершин аналогичного бинарного полного дерева с корнем высотой 3;

в) полное бинарное дерево с корнем любой высоты можно изобразить так, что дерево имеет ось симметрии. Как это свойство отражается на коде такого дерева?

33.14. На рис. 105 представлено полное тринарное дерево с корнем высотой 2, в котором степень выхода каждой вершины, не являющейся листом, равна 3 и все листья находятся на одной глубине.

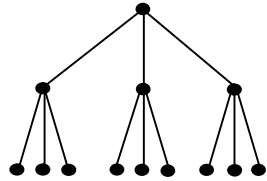


Рис. 105

а) Найдите код обхода всех вершин дерева с корнем;

б) найдите код обхода вершин аналогичного тринарного полного дерева с корнем высотой 3;

в) полное тринарное дерево с корнем любой высоты можно изобразить так, что дерево имеет ось симметрии. Как это свойство отражается на коде такого дерева?

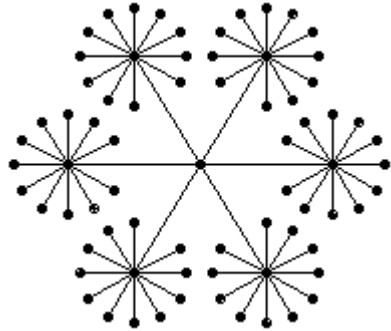


Рис. 106

33.15. Найдите код обхода всех вершин дерева (рис. 106) с корнем в центре цветка.

33.16. Найдите коды Пруфера следующих деревьев (рис. 107):

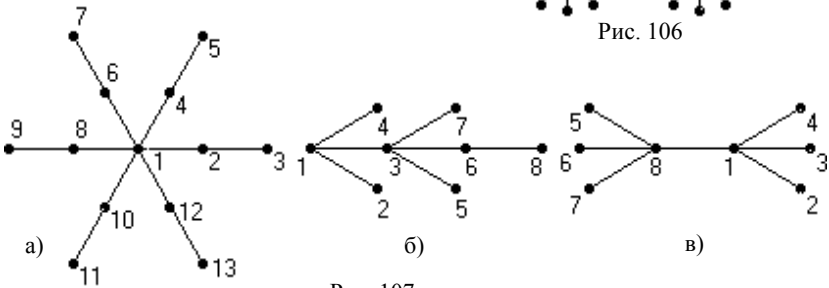


Рис. 107

33.17. Чем отличаются коды Пруфера деревьев на рис. 108?

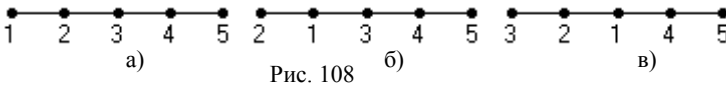


Рис. 108

33.18. Найдите код Пруфера для звезды $G_{1,7}$, если нумерация вершин начинается в центре звезды.

33.19. По коду Пруфера (1, 2, 2, 2, 4, 3) укажите номера висячих вершин.

33.20. Существуют ли дерево, все вершины которого являются висячими?

33.21. Верно ли, что всякое дерево является планарным графом?

33.22. Два дерева $G_1(V_1, E_1)$ и $G_2(V_2, E_2)$ имеют ровно одну общую вершину. Является ли деревом граф $G_1 \cup G_2$?

33.23. Два дерева $G_1(V_1, E_1)$ и $G_2(V_2, E_2)$ имеют ровно две общие вершины. Является ли деревом граф $G_1 \cup G_2$? А если эти общие вершины в каждом дереве являются листьями?

§ 34. Фундаментальная система циклов и разрезы графа

Рассмотрим граф G , содержащий циклы (рис. 109). Удалим из каждого цикла по одному ребру таким образом, чтобы получился остов. На рисунке 110 изображен один из возможных остовов графа.

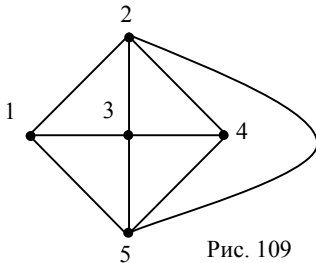


Рис. 109

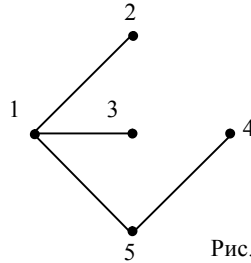


Рис. 110

Множество удаленных ребер обозначим через U . Для графа на рисунке 109: $U = \{\{2,3\}, \{2,4\}, \{3,4\}, \{3,5\}\}$. Возвратим одно ребро из U и получим цикл (рис. 111). Удалим это ребро и вернем из множества U другое ребро; получим другой цикл (рис. 112). Повторяя аналогично с остальными ребрами множества U получим систему циклов. Множество всех таких циклов называется *фундаментальной системой циклов* данного графа G , порожденной выбранным остовом (рис. 111–115). При изменении остова графа фундаментальная система циклов, вообще говоря, изменяется, хотя иногда может и сохраниться. Для связного графа число циклов равно $m - n + 1$, m – число ребер графа, где n – число вершин.

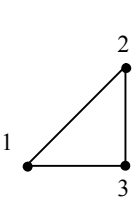


Рис. 111

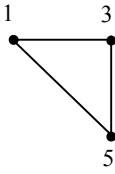


Рис. 112

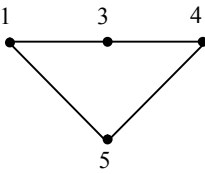


Рис. 113

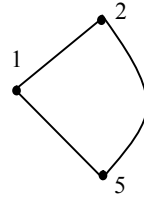


Рис. 114

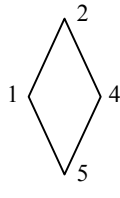


Рис. 115

Множество ребер графа называется *разделяющим*, если после его удаления получаем несвязный граф.

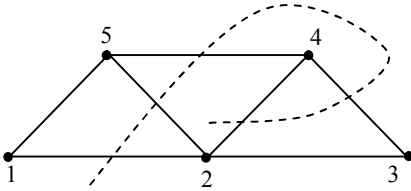


Рис. 116

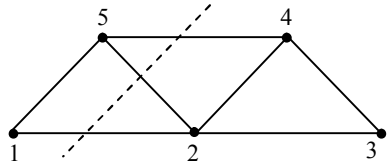


Рис. 117

Например, множество $R = \{\{1,2\}, \{2,5\}, \{5,4\}, \{4,3\}, \{4,2\}\}$ является разделяющим для графа на рисунке 116. Пунктирная линия показывает удаленные ребра. Число элементов этого разделяющего множества можно сократить. Например, множества $R_1 = \{\{1,2\}, \{2,5\}, \{5,4\}, \{4,3\}\}$, $R_2 = \{\{1,2\}, \{2,5\}, \{5,4\}, \{4,2\}\}$ также являются разделяющими для данного графа.

Разрезом называется разделяющее множество, у которого нет собственного подмножества, являющегося разделяющим для данного графа. На рисунке 117 показан один из возможных разрезов графа: $R_3 = \{\{1,2\}, \{2,5\}, \{5,4\}\}$.

В дереве любое ребро есть разрез. Пусть G – связный граф и T – некоторое остовное дерево. Удалим в T одно ребро. Дерево разобьется на две связные компоненты. Эти компоненты в графе G связаны каким-то набором ребер, который будет разрезом для графа G . Удаляя по очереди ребра у дерева T , получим систему разрезов графа G , которая называется фундаментальной системой разрезов графа G относительно остовного дерева T .

Для перечисления всех разрезов графа на рис 9 построим двойственный граф к данному графу (рис. 118). В каждой области, включая внешнюю область для графа, отметим по точке.

Получим множество вершин $\{a, b, c, d\}$ двойственного графа. Каждые две вершины из разных областей с общей границей соединим ребрами, пересе-

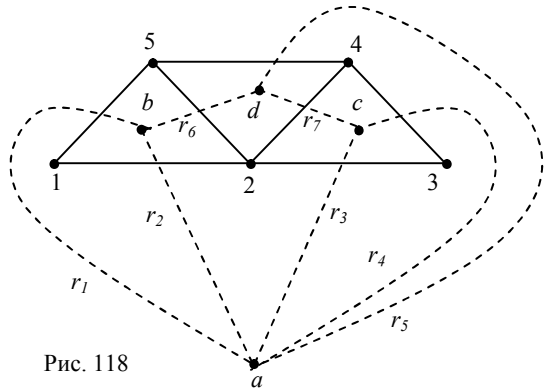
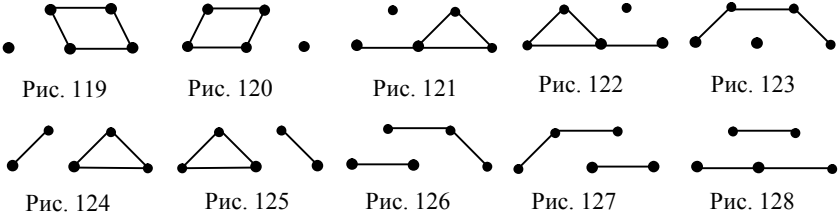


Рис. 118

кающими ребро, лежащее на границе. Получаем множество ребер $\{r_1, r_2, r_3, r_4, r_5, r_6, r_7\}$ двойственного графа.

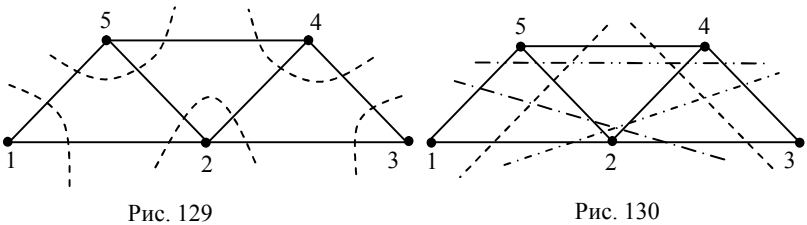
Таблица 22

цикл	разрез	компоненты графа
$\{\Gamma_1, \Gamma_2\}$	$\{\{1,5\}, \{1,2\}\}$	рис. 119
$\{\Gamma_3, \Gamma_4\}$	$\{\{2,3\}, \{3,4\}\}$	рис. 120
$\{\Gamma_1, \Gamma_6, \Gamma_5\}$	$\{\{1,5\}, \{5,2\}, \{5,4\}\}$	рис. 121
$\{\Gamma_5, \Gamma_7, \Gamma_4\}$	$\{\{5,4\}, \{2,4\}, \{4,3\}\}$	рис. 122
$\{\Gamma_2, \Gamma_6, \Gamma_7, \Gamma_3\}$	$\{\{1,2\}, \{2,5\}, \{2,4\}, \{2,3\}\}$	рис. 123
$\{\Gamma_2, \Gamma_6, \Gamma_5\}$	$\{\{1,2\}, \{2,5\}, \{5,4\}\}$	рис. 124
$\{\Gamma_3, \Gamma_7, \Gamma_5\}$	$\{\{2,3\}, \{2,4\}, \{4,5\}\}$	рис. 125
$\{\Gamma_1, \Gamma_6, \Gamma_7, \Gamma_3\}$	$\{\{1,5\}, \{5,2\}, \{2,4\}, \{2,3\}\}$	рис. 126
$\{\Gamma_2, \Gamma_6, \Gamma_7, \Gamma_4\}$	$\{\{1,2\}, \{5,2\}, \{2,4\}, \{4,3\}\}$	рис. 127
$\{\Gamma_1, \Gamma_6, \Gamma_7, \Gamma_4\}$	$\{\{1,5\}, \{5,2\}, \{2,4\}, \{4,3\}\}$	рис. 128



Перечисляем все простые циклы двойственного графа: вначале содержащие внутри себя по одной вершине исходного графа, затем по две вершине исходного графа. На этом процесс нужно остановить, т.к. для графа с пятью вершинами множества, содержащие три или четыре вершины, уже оказались сформированными. Получаем следующие случаи в таблице 22.

Замечание. Иногда двойственный граф не используют, а разрезы показывают линиями с двумя концевыми точками во внешней области графа (рис. 129, 130). Каждая линия показывает один разрез.



Задачи.

34.1. Для следующих графов (рис. 131) постройте несколько остовных деревьев и найдите относительно каждого фундаментальные системы циклов и разрезов. Для этих графов найдите все разрезы.

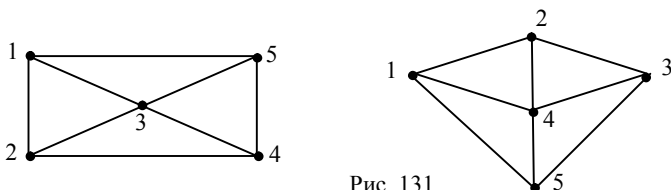


Рис. 131

34.2. Для графов на рис. 131 постройте двойственные графы.

34.3. Существует ли граф, в разрез которого входят все ребра?

34.4. Сколько в графе (рис. 132) разрезов, содержащих два ребра? Три ребра? Четыре ребра?

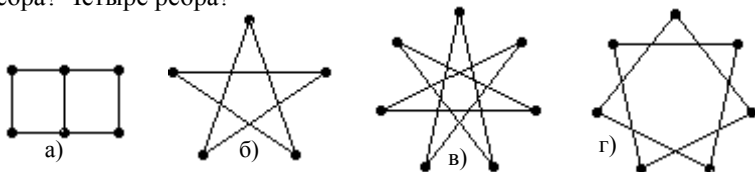


Рис. 132

§ 35. Раскрашивание вершин, ребер и граней графа

Пусть задан плоский граф $G(V, E, F)$, имеющий множество вершин V , множество ребер E и множество граней F .

Грани графа правильно раскрашены, если каждой грани присвоен определенный цвет и любым двум смежным граням присвоены различные цвета.

Задача. Для данного плоского графа определить минимальное число цветов для раскраски граней.

В 1879 г. А. Кэли высказал гипотезу о том, что любую географическую карту можно правильно раскрасить четырьмя красками.

О необходимости четырех красок можно убедиться на плоском графе (рис. 133), имеющем 6 вершин.

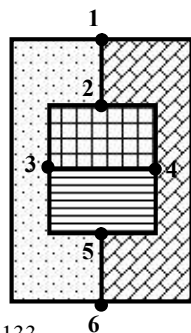


Рис. 133

Гипотеза Кэли не доказана и не опровергнута.

Теорема 1 (о пяти красках). Любой плоский граф допускает правильную раскраску граней в 5 цветов [9, с. 132].

Теорема 2. (теорема о двух красках). Для того, чтобы плоский граф допускал правильную раскраску граней в два цвета, необходимо и достаточно, чтобы все вершины этого графа были четными [9, с. 136].

Пример такой раскраски на рис. 134.

Теорема 3 (теорема о трех красках). Для того чтобы плоский кубический граф допускал правильную раскраску граней в 3 цвета, необходимо и достаточно, чтобы каждая его грань была ограничена четным числом ребер [9, с. 138].

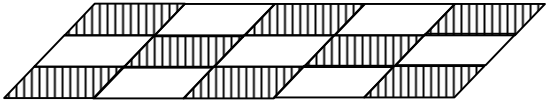


Рис. 134

Пусть дан граф $G(V, E)$. Вершины графа правильно раскрашены, если каждой вершине присвоен определенный цвет, причем любым двум смежным вершинам присвоены различные цвета, т.е. ребра соединяют вершины разного цвета.

Если граф содержит петли, т.е. псевдограф, то его невозможно правильно раскрасить.

Мультиграф называется p -хроматическим, если он допускает правильную раскраску вершин в p цветов.

На рис. 135 один и тот же граф G раскрашен различными способами, поэтому данный граф можно назвать 2-хроматическим, 3-хроматическим или 4-хроматическим.

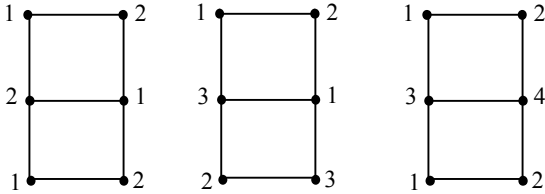


Рис. 135

Наименьшее значение p , при котором граф G является p -хроматическим, называется хроматическим числом графа. Для графа на рис. 136 хроматическое число равно 3, т.е. $\chi(G) = 3$.

Для графа, имеющего только изолированные вершины, $\chi(G) = 1$.

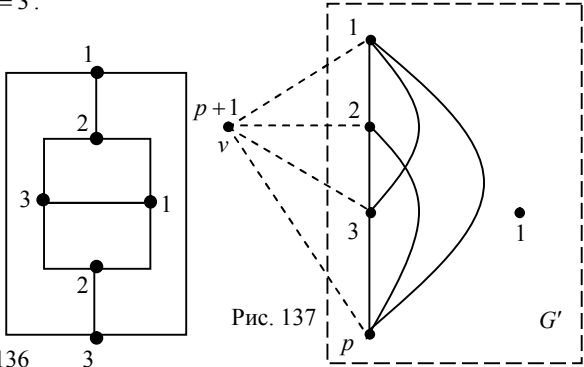


Рис. 137

Рис. 136

Для полного графа хроматическое число равно его числу вершин.

Пример 1. Доказать, что если наибольшая из степеней вершин графа G равна p , то этот граф $(p+1)$ -раскрашиваем.

Решение. Доказательство проведем методом математической индукции по числу вершин графа. Для графа с одной или двумя вершинами утверждение справедливо. Пусть граф имеет n вершин. Удалим из графа произвольную вершину v с наибольшей степенью вместе с инцидентными ей ребрами (рис. 137). В оставшемся графе G' с $(n-1)$ вершинами степени вершин также не превосходят число p . По предположению индукции этот подграф $(p+1)$ -раскрашиваем, причем в нем существует p вершин, смежных с вершиной v . На рис. 137 показана раскраска смежных вершин. Раскрасим вершину v цветом, отличным от цветов смежных вершин, тогда данный граф $(p+1)$ -раскрашиваем. \square

Рассмотрим плоский граф $G(V, E, F)$ (рис. 138), имеющий множество вершин V , множество ребер E и множество граней F . Построим двойственный граф $G'(V', E', F')$. При двойственном отображении:

- грани графа G отображаются в вершины графа G' ;
- вершины графа G отображаются в грани графа G' .

Задача о раскраске вершин графа G эквивалентна задаче о раскраске граней графа G' .

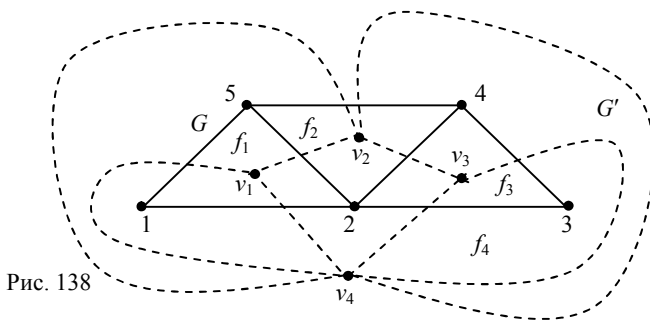


Рис. 138

Гипотеза. Для раскраски вершин графа G достаточно 4 красок.

Теорема 1₁. Любой плоский граф допускает раскраску вершин в 5 цветов.

Теорема 2₁. Для того чтобы плоский граф допускал раскраску вершин в 2 цвета, необходимо и достаточно, чтобы каждая грань графа была ограничена четным числом ребер.

Теорема 3₁. Для того чтобы плоская триангуляция (разбиение на треугольники) допускала раскраску вершин в 3 цвета, необходимо и достаточно, чтобы каждая ее вершина была четной.

Ребра графа правильно раскрашены, если каждому ребру присвоен определенный цвет, причем любые два смежных ребра раскрашены в разные цвета.

Граф называется *реберно k -раскрашенным*, если его ребра можно раскрасить k красками так, что любые два смежных ребра раскрашены в разные цвета. Если граф G реберно k раскрашиваем, но не является реберно $(k-1)$ -раскрашиваемым, то число k называется реберно-хроматическим числом графа и обозначается $\chi_c(G) = k$.

Если наибольшая из степеней вершин графа равна δ , то его ребра невозможно раскрасить менее чем δ цветов, причем $\chi_e(G) \geq \delta$.

Пример 2. Доказать, что для двудольного графа реберно-хроматическое число равно $\chi_e(K_{m,n}) = \max(m, n)$.

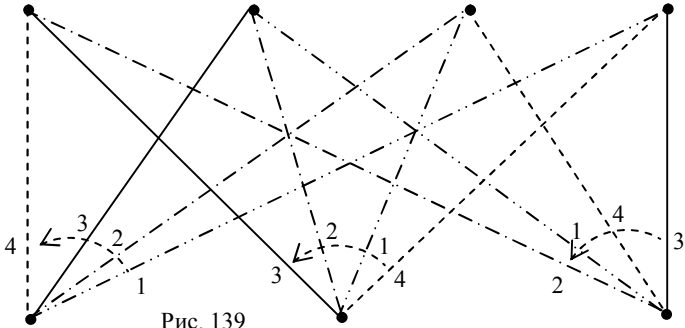


Рис. 139

Решение. Будем считать, что $m \geq n$. Изобразим любой двудольный граф аналогично рис. 139. Порядок раскрашивания ребер в каждой вершине можно представить в виде циклического сдвига по окружности в одном и том же направлении. \square

Пример 3. Докажите, что для полного графа с n вершинами реберно-хроматическое число равно:

$$\chi_e(K_n) = \begin{cases} n, & \text{если } n \text{ - нечетно и } n \neq 1; \\ n-1, & \text{если } n \text{ - четно.} \end{cases}$$

Для нечетного n изобразим граф в виде правильного многоугольника (рис. 140). Любая диагональ многоугольника, соединяющая две вершины, разбивает множество всех остальных вершин многоугольника на два множества. Одно из них содержит нечетное число вершин, а второе множество – четное число вершин. В множестве с четным числом вершин содержится две вершины, являющиеся концами стороны, параллельной этой диагонали. Достаточно параллельным переносом переместить диагональ до совпадения со стороной. Каждая диагональ многоугольника параллельна некоторой стороне. Все диагонали распадаются на классы диагоналей, параллельных сторонам многоугольника. Раскрашиваем все стороны многоугольника в n различных цветов, а затем все диагонали одного класса красим в тот же цвет, что и параллельная им сторона. Граф оказался реберно n -раскрашенным (рис. 140). Заметим, что в каждой вершине все ребра окрашены в $n-1$ цвет, причем в ней нет цвета той стороны, напротив которой расположена эта вершина.

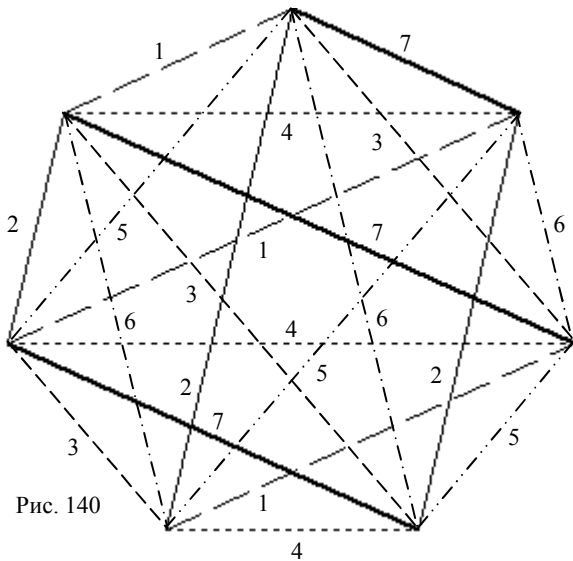


Рис. 140

Для четного числа n полный граф K_n можно рассматривать как объединение полного графа K_{n-1} , отдельной вершины v и всех ребер, соединяющих эту вершину с вершинами графа K_{n-1} (рис. 141). Раскрасим в графе K_{n-1} все ребра указанным выше способом, а каждое ребро, соединяющее вершину v с остальными вершинами графа K_{n-1} , раскрасим “недостающим” цветом, т.е. цветом стороны в графе K_{n-1} , напротив которого лежит вторая вершина ребра (рис. 141). □

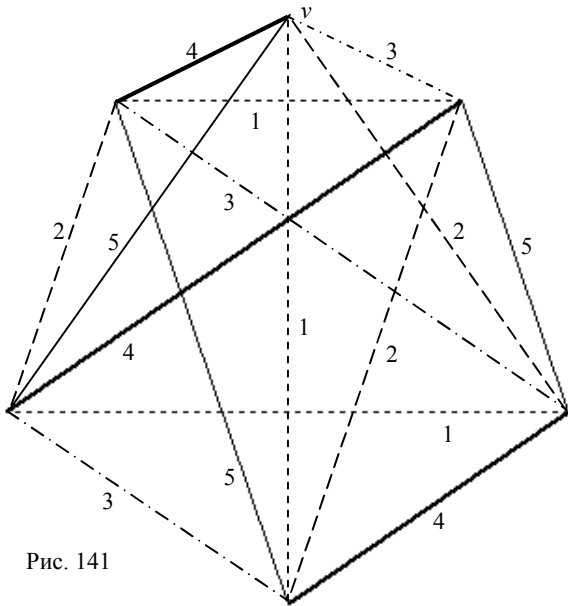


Рис. 141

Теорема Тейта. Плоский кубический двусвязный граф допускает раскраску граней четырьмя цветами тогда и только тогда, когда он допускает правильную раскраску ребер в три цвета [9, с. 147].

К раскрашенным графам приводят различные задачи, которые на первый взгляд никакого отношения к раскраске графов не имеют.

Пример 4. *Задача составления расписания.* Необходимо прочитать некоторое количество лекций определенным количеством преподавателей за наименьший промежуток времени. Пусть каждая лекция длится одно и то же время (например, 1 час). Некоторые лекции не могут читаться одновременно, например, когда эти лекции читает один и тот же преподаватель.

Построим граф $G = \{V, E\}$, где V – множество всех лекций, а две вершины смежные тогда и только тогда, когда соответствующие лекции не могут читаться одновременно. Очевидно, что всякая правильная раскраска определяет допустимое расписание: лекции, вершины которых окрашены в один цвет, читаются одновременно, в разные цвета – в одно и то же время не читаются. Оптимальное расписание будет соответствовать минимальной раскраске, а минимальное число часов, необходимое для прочтения всех лекций, равно $\chi(G)$.

Пример 5. *Задача распределения оборудования.* Есть некоторое множество работ, и имеется некоторый набор механизмов для выполнения этих работ. Считаем, что каждая работа выполняется за одно и то же время и при этом ни один механизм не может участвовать одновременно в выполнении нескольких работ. Требуется распределить механизмы так, чтобы общее время выполнения всех работ было минимальным.

Построим граф $G = \{V, E\}$, где $V = \{v_1, v_2, \dots, v_n\}$ – множество всех работ. Две вершины считаются смежными тогда и только тогда, когда для выполнения работ v_i и v_j требуется хотя бы один общий механизм. При правильной раскраске графа G работы, соответствующие вершинам одного цвета, могут выполняться одновременно. Минимальная раскраска графа G будет соответствовать наименьшему времени, требуемому для выполнения работ.

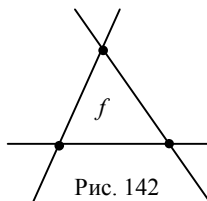
Пример 6. *Задача проектирования коробки скоростей.* Коробка скоростей – это механизм, который изменяет частоту оборотов вала. Это изменение выполняется за счет того, что различные шестеренки, находящиеся внутри коробки, сцепляются специальным образом. Одна из задач перед конструкторами – минимизировать размеры коробки. Это зачастую достигается за счет уменьшения количества валов, на которых размещены шестеренки.

Построим граф $G = \{V, E\}$, где V – множество всех шестеренок, $(v, u) \in E$ тогда и только тогда, когда шестеренки v и u не могут находиться на одном валу (например, они должны сцепляться между собой или они слишком тяжелы для одного вала). Правильная раскраска такого графа говорит о том, что одинаково раскрашенные вершины соответствуют шестеренкам, находящимся на одном валу, а шестеренки, соответствующие разнораскрашенным вершинам, находятся на разных валах. Хроматическое число $\chi(G)$ соответствует минимальному количеству валов в проектируемой коробке скоростей.

Задачи.

35.1. Докажите, что если степень \deg вершины графа является нечетным числом ребер и $\deg \geq 3$, то правильная раскраска граней графа вокруг этой вершины невозможна.

35.2. Докажите, что если некоторая грань графа (рис. 142) ограничена нечетным числом ребер и $m \geq 3$, то правильная раскраска граней графа невозможна. Рассмотрите случай, когда m – четно, и приведите соответствующие примеры.



35.3. Для следующих графов (рис. 143) определите правильную раскраску вершин, ребер и граней.

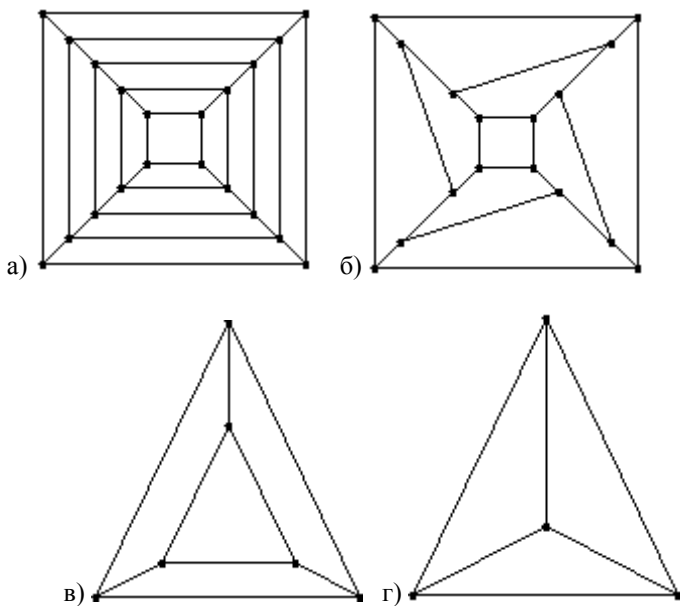


Рис. 143

35.3. Найдите реберно-хроматическое число следующих графов:

- а) звездного графа $K_{1,n}$;
- б) n -угольной пирамиды;

в) однородного графа с n вершинами, имеющего степени вершин, равные 2.

35.4. Докажите, что граф является 2-хроматическим тогда и только тогда, когда он двудольный.

35.5. Докажите, что граф является 2-хроматическим тогда и только тогда, когда он не содержит циклов нечетной длины.

35.6. Докажите, что всякое дерево является 2-хроматическим графом. Докажите, что всякое дерево является двудольным графом.

35.7. Какое минимальное количество различных механизмов нужно для выполнения шести работ, если граф распределения механизмов приведен на рис. 144? Укажите правильную раскраску вершин графа и минимальное время для выполнения всех работ. Механизмы удовлетворяют условиям задачи распределения механизмов.

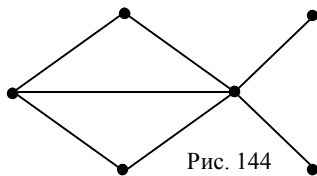


Рис. 144

35.8. В летней математической школе запланировано провести лекции по алгебре (А), геометрии (Г), математическому анализу (МА), дискретной математике (Д), кодированию информации (К) и олимпиадным задачам (О). Приглашенные преподаватели могут прочитать лекции соответственно по тематикам: (А, Г, О), (О, Д, К), (МА, Г, О, А), (К, Д, А), (МА, К). Перечисленные наборы удовлетворяют условию задачи составления расписания. Преподаватели приезжают одновременно утром и уезжают также одновременно после прочтения последней лекции. Укажите оптимальную последовательность лекций, при которой время пребывания преподавателей в школе окажется минимальным.

Глава 4. Кодирование информации

§ 36. Основы теории делимости

Целое число, которое делит целые числа a_1, a_2, \dots, a_n , называется их общим делителем. Положительный общий делитель чисел a_1, a_2, \dots, a_n , делящийся на любой общий делитель, называется наибольшим общим делителем и обозначается (a_1, a_2, \dots, a_n) или $\text{НОД}(a_1, a_2, \dots, a_n)$.

Натуральное число p , большее 1, называется *простым*, если оно имеет только два различных делителя: единицу и само p .

Натуральное число называется *составным*, если оно имеет больше двух различных натуральных делителя.

Число 1 имеет только один натуральный делитель, поэтому оно не простое и не составное число.

Приведем таблицу простых чисел в пределах первой тысячи, которыми мы будем иногда пользоваться.

Таблица 1

2	47	109	191	269	353	439	523	617	709	811	907
3	53	113	193	271	359	443	541	619	719	821	911
5	59	127	197	277	367	449	547	631	727	823	919
7	61	131	199	281	373	457	557	641	733	827	929
11	67	137	211	283	379	461	563	643	739	829	937
13	71	139	223	293	383	463	569	647	743	839	941
17	73	149	227	307	389	467	571	653	751	853	947
19	79	151	229	311	397	479	577	659	757	857	953
23	83	157	233	313	401	487	587	661	761	859	967
29	89	163	239	317	409	491	593	673	769	863	971
31	97	167	241	331	419	499	599	677	773	877	977
37	101	173	251	337	421	503	601	683	787	881	983
41	103	179	257	347	431	509	607	691	797	883	991
43	107	181	263	349	433	521	613	701	809	887	997

Пусть a, b – натуральные числа и $a > b$. Если при делении числа a на число b частное равно q , а остаток равен r , где $0 \leq r < b$, то выполняется равенство $a = bq + r$. Если $r = 0$, то a делится на b , и это записывают как $a : b$.

Если a делится на b , то b и будет наименьшим общим делителем этих чисел.

Если a не делится на b , то для нахождения наибольшего общего делителя двух натуральных чисел применяется алгоритм Евклида, который состоит в следующем.

Пусть a и b – натуральные числа и $a > b$, тогда

$$a = bq_1 + r_1, \text{ где } 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, \text{ где } 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \text{ где } 0 < r_3 < r_2,$$

.....

$$r_{n-2} = r_{n-1}q_n + r_n, \text{ где } 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_n q_{n+1}.$$

Последний отличный от нуля остаток r_n является наибольшим общим делителем чисел a и b , т.е. $r_n = (a, b)$.

Если d – наибольший общий делитель чисел a и b , то существуют такие целые числа x и y , что $ax + by = d$.

Пример. Найти наибольший общий делитель чисел 403 и 143 и найти линейное представление общего делителя через эти числа.

Решение.

$$403 = 143 \cdot 2 + 117,$$

$$143 = 117 \cdot 1 + 26,$$

$$117 = 26 \cdot 4 + 13,$$

$$26 = 13 \cdot 2.$$

Последний отличный от нуля остаток равен 13, поэтому $(403, 143) = 13$.

$$\begin{aligned} 13 &= 117 - 26 \cdot 4 = 117 - (143 - 117) \cdot 4 = 117 \cdot 5 - 143 \cdot 4 = \\ &= (403 - 143 \cdot 2) \cdot 5 - 143 \cdot 4 = 403 \cdot 5 - 143 \cdot 14. \end{aligned}$$

$$13 = 403 \cdot 5 + 143 \cdot (-14).$$

Чтобы найти наибольший общий делитель трех и более чисел, сначала находят НОД какой-нибудь пары из них, а затем НОД найденного делителя и третьего числа и т.д.

Два числа называются взаимно простыми, если наибольший общий делитель этих чисел равен единице.

Два числа a и b являются взаимно простыми тогда и только тогда, когда существуют такие целые числа x_0 и y_0 , что $ax_0 + by_0 = 1$.

Таблица признаков делимости

Таблица 2

m	Признак делимости натурального числа n на число m
2	последняя цифра числа n четная
3	сумма цифр числа n делится на 3
4	две последние цифры числа n образуют число, кратное 4
5	последняя цифра числа n ноль или 5
6	число n делится на 2 и на 3
11	разность между суммой цифр, стоящих на четных местах, и суммой цифр, стоящих на нечетных местах, делится на 11
7, 11, 13	разность между числом, образованным тремя последними цифрами числа n , и числом, образованным остальными цифрами, делится на m
8	три последние цифры образуют число, делящееся на 8
9	сумма цифр числа n делится на 9
10	число n оканчивается нулем
25	последние две цифры числа n образуют число, делящееся на 25

Представление натурального числа n в виде $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, где p_1, p_2, \dots, p_k – простые числа, $p_1 < p_2 < \dots < p_k$ и $\alpha_1 > 0, \alpha_2 > 0, \dots, \alpha_k > 0$ называется каноническим.

Если $a = p^k$, где p – простое число, k – натуральное число, то число a имеет $k+1$ делителей, включая 1 и число a .

Если $a = p_1^{k_1} p_2^{k_2}$, где p_1 и p_2 – простые различные числа, k_1 и k_2 – натуральные числа, то число a имеет $(k_1+1)(k_2+1)$ делителей, включая 1 и число a .

Если $\frac{a}{b}$ – обыкновенная несократимая дробь (правильная или неправильная), то с помощью алгоритма Евклида эту дробь можно представить в виде конечной непрерывной (цепной) дроби:

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}}$$

где $a = bq_0 + r_1$, где $0 < r_1 < b$,

$b = r_1q_1 + r_2$, где $0 < r_2 < r_1$,

$r_1 = r_2q_2 + r_3$, где $0 < r_3 < r_2$,

.....

$r_{n-2} = r_{n-1}q_{n-1} + r_n$, где $0 < r_n < r_{n-1}$,

$r_{n-1} = r_nq_n$.

Обозначение цепной дроби $(q_0; q_1, q_2, \dots, q_n)$.

Дроби

$$\frac{P_0}{Q_0} = \frac{q_0}{1}, \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1}, \frac{P_2}{Q_2} = q_0 + \frac{1}{q_1 + \frac{1}{q_2}}, \dots$$

$$\frac{P_n}{Q_n} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}}$$

называются подходящими дробями.

Если условно ввести $P_{-2} = 0, P_{-1} = 1, Q_{-2} = 1, Q_{-1} = 0$, то для вычисления подходящих дробей существует алгоритм:

$$\frac{P_i}{Q_i} = \frac{P_{i-1}q_i + P_{i-2}}{Q_{i-1}q_i + Q_{i-2}}$$

Для данной дроби $\frac{a}{b}$ и подходящих дробей выполняются неравенства

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \dots < \frac{a}{b} < \dots < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.$$

Пример 1.

$$\frac{35}{16} = 2 + \frac{1}{5 + \frac{1}{3}}, \text{ т.к.}$$

$$\begin{array}{r} \underline{35 \overline{) 16}} \\ \underline{32} \\ 3 \end{array}$$

$$\frac{35}{16} = (2; 5, 3). \quad \square$$

$$\begin{array}{r} 3 \overline{) 1} \\ \underline{3} \\ 0 \end{array}$$

Пример 2. Записать число $\frac{99}{170}$ в виде цепной дроби и найти подходящие дроби.

Решение. Применим алгоритм Евклида:

$$99 = 170 \cdot 0 + 99, \quad 170 = 99 \cdot 1 + 71, \quad 99 = 71 \cdot 1 + 28,$$

$$71 = 28 \cdot 2 + 15, \quad 28 = 15 \cdot 1 + 13, \quad 15 = 13 \cdot 1 + 2,$$

$$13 = 2 \cdot 6 + 1, \quad 2 = 1 \cdot 2.$$

Собирая частные в равенствах, получаем

$$\frac{99}{170} = (0; 1, 1, 2, 1, 1, 6, 2).$$

Найдем подходящие дроби

$$\frac{P_0}{Q_0} = \frac{q_0}{1} = \frac{0}{1}, \quad \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = 0 + \frac{1}{1} = \frac{1}{1}, \quad \frac{P_2}{Q_2} = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = 0 + \frac{1}{1 + \frac{1}{1}} = \frac{1}{2}.$$

Далее подходящие дроби можно находить по рекуррентным формулам

$$\frac{P_3}{Q_3} = \frac{P_2 q_3 + P_1}{Q_2 q_3 + Q_1} = \frac{1 \cdot 2 + 1}{2 \cdot 2 + 1} = \frac{3}{5}, \quad \frac{P_4}{Q_4} = \frac{P_3 q_4 + P_2}{Q_3 q_4 + Q_2} = \frac{3 \cdot 1 + 1}{5 \cdot 1 + 2} = \frac{4}{7},$$

$$\frac{P_5}{Q_5} = \frac{P_4 q_5 + P_3}{Q_4 q_5 + Q_3} = \frac{4 \cdot 1 + 3}{7 \cdot 1 + 5} = \frac{7}{12}, \quad \frac{P_6}{Q_6} = \frac{P_5 q_6 + P_4}{Q_5 q_6 + Q_4} = \frac{7 \cdot 6 + 4}{12 \cdot 6 + 7} = \frac{46}{79},$$

$$\frac{P_6}{Q_6} = \frac{P_5 q_6 + P_4}{Q_5 q_6 + Q_4} = \frac{7 \cdot 6 + 4}{12 \cdot 6 + 7} = \frac{46}{79}, \quad \frac{P_7}{Q_7} = \frac{P_6 q_7 + P_5}{Q_6 q_7 + Q_5} = \frac{46 \cdot 2 + 7}{79 \cdot 2 + 12} = \frac{99}{170}.$$

Слева и справа от данной дроби располагаем подходящие дроби

$$0 < \frac{1}{2} < \frac{4}{7} < \frac{46}{79} < \frac{99}{170} = \frac{99}{170} < \frac{7}{12} < \frac{3}{5} < 1.$$

Замечание 1. Подходящие дроби можно использовать для выстраивания цепочки несократимых дробей, содержащих данное число.

Замечание 2. Иногда цепочку дробей, содержащих данное число, можно построить более простым способом, но среди найденных дробей могут содержаться сократимые дроби.

Например, увеличивая или уменьшая знаменатель дроби, получим

$$\frac{99}{174} < \frac{99}{173} < \frac{99}{172} < \frac{99}{171} < \frac{99}{170} < \frac{99}{169} < \frac{99}{168} < \frac{99}{167} < \frac{99}{166}.$$

Сокращая дроби, получим цепочку дробей для данного числа:

$$\frac{33}{58} < \frac{99}{173} < \frac{99}{172} < \frac{11}{19} < \frac{99}{170} < \frac{99}{169} < \frac{33}{56} < \frac{99}{167} < \frac{99}{166}.$$

В этом случае придется применять несколько раз алгоритм поиска наибольшего общего делителя для сокращения дробей. \square

Функцией Эйлера $\varphi(n), n \in \mathbb{N}$ при $n > 1$ называется количество натуральных чисел, меньших n и взаимно простых с n . Для $n = 1$ полагают $\varphi(1) = 1$.

Пример 3.

Для $n = 9$ имеем шесть чисел 1, 2, 4, 5, 7, 8, взаимно простых с 9, поэтому $\varphi(9) = 6$.

Для $n = 12$ получаем числа 1, 5, 7, 11, поэтому $\varphi(12) = 4$.

Для $n = 2^k$ каждое нечетное число, меньшее n , является взаимно простым с числом 2^k . Таких чисел 2^{k-1} , поэтому $\varphi(2^k) = 2^{k-1}$.

Для $n = 3^k$ выпишем в ряд все числа от 1 до 3^k и вычеркнем все числа, кратные 3. Вычеркнутых чисел окажется $3^k / 3 = 3^{k-1}$.

Количество оставшихся чисел равно функции Эйлера $\varphi(3^k) = 2 \cdot 3^{k-1}$.

Если n – простое число, то $\varphi(n) = n - 1$. \square

Теорема 1. Пусть $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ – каноническое разложение числа n , то

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Пример 4. Применение теоремы для некоторых чисел.

$$12 = 2^2 \cdot 3, \quad \varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4,$$

$$n = 2^k, \quad \varphi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = 2^{k-1}. \quad \square$$

Теорема 2. Если n и m – взаимно простые числа, то

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Число m называется наименьшим общим кратным (НОК) целых чисел a_1, a_2, \dots, a_n , если выполняются условия:

- 1) $m : a_1, m : a_2, \dots, m : a_n$;
- 2) если $m' : a_1, m' : a_2, \dots, m' : a_n$, где m' – любое целое число, то $m' : m$.

Положительное НОК чисел a_1, a_2, \dots, a_n обозначают $[a_1, a_2, \dots, a_n]$.

Если простое число p входит в канонические разложения чисел a и b с показателями соответственно α и β , то p входит в каноническое разложение числа (a, b) с показателем $\min(\alpha, \beta)$, а в каноническое разложение числа $[a, b]$ с показателем $\max(\alpha, \beta)$.

Задачи.

36.1. Найдите количество делителей следующих чисел:

а) 3^5 ; б) 7^5 ; в) 125; г) 32; д) 15; е) 12; ж) 45; з) 250.

36.2. Найдите значение функции Эйлера для следующих чисел:

а) 5; б) 8; в) 15; г) 12; д) 41; е) 81.

36.3. Найти наибольший общий делитель данных чисел и найти линейное представление общего делителя через эти числа:

а) 34 и 85; б) 18 и 27; в) 437 и 621.

36.4. Докажите, что если $\text{НОД}(a, b)$ выражен через данные числа a и b в виде $\text{НОД}(a, b) = ax + by$, то x и y – взаимно простые числа.

36.5. Докажите что в разложении $\text{НОД}(a, b) = ax + by$ коэффициенты x и y не определяются единственным образом.

36.6. Докажите, что если $\text{НОД}(a, b) = 1$, то $\text{НОД}(a + nb, b) = 1$.

36.7. Докажите, что если $d = (a, b)$, то a/d и b/d взаимно просты.

36.8. Докажите, что для положительных целых чисел выполняется равенство $(a, b)[a, b] = ab$.

36.9. Докажите, что если для целых чисел a, b, c : $(a, b) = d_1, (d_1, c) = d_2$, то $(a, b, c) = d_2$.

36.10. Докажите, что если для целых чисел a, b, c : $[a, b] = m_1, (m_1, c) = m_2$, то $(a, b, c) = m_2$.

36.11. СИ. Изучите понятие подходящих дробей для иррациональных чисел в пособии [19, с. 34–38].

§ 37. Сравнения первой степени

Напомним, что на множестве целых чисел для натурального числа m , где $m > 1$ вводили отношение, которое является отношением эквивалентности, число a сравнимо с числом b по модулю m тогда и только тогда, когда $(a - b) : m$. Обозначение $a \equiv b \pmod{m}$. Множество всех целых чисел, сравнимых с числом x по модулю m , называется классом эквивалентности (классом вычетов), порожденным элементом x , и обозначается \bar{x} .

Пусть при делении целых чисел n_1 и n_2 на натуральное число m получены соответственно частные k_1, k_2 и остатки r_1, r_2 , т.е.

$$n_1 = k_1 \cdot m + r_1, \quad 0 \leq r_1 < m, \quad n_2 = k_2 \cdot m + r_2, \quad 0 \leq r_2 < m,$$

тогда

$$n_1 + n_2 = (k_1 + k_2)m + (r_1 + r_2),$$

$$n_1 \cdot n_2 = (\dots)m + (r_1 \cdot r_2),$$

$$(n_1)^k = (\dots)m + (r_1)^k.$$

Таким образом:

– чтобы найти остаток от деления суммы двух чисел $n_1 + n_2$ на число m , достаточно найти сумму остатков при делении каждого из чисел n_1, n_2 на число m и полученную сумму разделить на m ;

– чтобы найти остаток от деления произведения двух чисел $n_1 \cdot n_2$ на число m , достаточно найти произведение остатков при делении каждого из чисел n_1, n_2 на число m и полученное произведение разделить на m ;

– чтобы найти остаток от степени n_1^k на число m , достаточно найти степень остатка при делении основания n_1 на число m и полученное число разделить на m .

Обозначая $r(n)_m$ – остаток при делении числа n на число m , полученные свойства можно записать в виде:

$$r(n_1 + n_2)_m = r(r(n_1)_m + r(n_2)_m)_m; \quad r(n_1 \cdot n_2)_m = r(r(n_1)_m \cdot r(n_2)_m)_m;$$

$$r(n^k)_m = r\left(\left(r(n)_m\right)^k\right)_m.$$

Пример 1. С каким числом сравнимо число 3^{2003} по модулю 7?

Решение. Найдем остатки при делении первых степеней основания 3 на число 7 (таблица 3).

Таблица 3

3^n	3	9	27	81	243	729	2187
Остатки при делении 3^n на число 7	3	2	6	4	5	1	3

Вычисление степеней в некоторых случаях может оказаться трудоемким. Этот процесс можно упростить, если использовать следующее свойство.

Пусть $a^n = km + t$, тогда $a^{n+1} = kma + ta$, $r(a^{n+1})_m = r(ta)_m$, т.е. чтобы найти остаток при делении следующей степени на число m , нужно остаток, полученный на предыдущем этапе умножить на основание a и записать новый остаток при делении на число m (таблица 4).

Таблица 4

3^n	3	3^2	3^3	3^4	3^5	3^6
Вспомогательная операция		$3 \cdot 3$	$2 \cdot 3$	$6 \cdot 3$	$4 \cdot 3$	$5 \cdot 3$
Остатки при делении на 7	3	2	6	4	5	1

$$r(3^{2003})_7 = r(3^{6 \cdot 335 + 3})_7 = r(3^{6 \cdot 335} \cdot 3^3)_7 = r(3^{6 \cdot 335})_7 \cdot r(3^3)_7 = 6, \quad 3^{2003} \equiv 6 \pmod{7}. \quad \square$$

Пример 2. Доказать, что $2003^{2004} + 2004^{2003}$ делится на 5.

Решение. Докажем, при делении числа $2003^{2004} + 2004^{2003}$ на число 5 получим остаток, равный 0.

$$r(2003^{2004} + 2004^{2003})_5 = r(2003^{2004})_5 + r(2004^{2003})_5,$$

$$r(2003^{2004})_5 = r((2000+3)^{2004})_5 = r(3^{2004})_5.$$

Выделим период при делении числа 3^{2004} на 5 (таблица 5).

Таблица 5

3^n	3	3^2	3^3	3^4	3^5
Остатки при делении 3^n на число 5	3	4	2	1	3

$$r(3^{2004})_5 = r((3^4)^{501})_5 = r(1^{501})_5 = 1. \quad r(2004^{2003})_5 = r((2000+4)^{2003})_5 = r(4^{2003})_5.$$

Выделим период при делении числа 4^{2003} на 5 (таблица 6).

Таблица 6

4^n	4	4^2	4^3
Остатки при делении 4^n на число 5	4	1	4

$$r(4^{2003})_5 = r((4^2)^{1000} \cdot 4)_5 = r((4^2)^{1000})_5 \cdot r(4)_5 = r(1^{1000})_5 \cdot 4 = 4.$$

$$r(2003^{2004} + 2004^{2003})_5 = r(1+4)_5 = 0. \quad \square$$

Для классов вычетов по данному модулю m определены операции:

сложения $\overline{a+b} = \overline{a} + \overline{b}$ и умножения $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$.

Эти операции обладают свойствами:

$$- \overline{a+b} = \overline{b+a}, \quad \overline{a \cdot b} = \overline{b \cdot a};$$

$$- (\overline{a+b}) + \overline{c} = \overline{a} + (\overline{b+c}), \quad (\overline{a \cdot b}) \cdot \overline{c} = \overline{a \cdot (b \cdot c)};$$

$$- \overline{a+0} = \overline{a}, \quad \overline{a \cdot 0} = \overline{0};$$

$$- \overline{a(b+c)} = \overline{a \cdot b} + \overline{a \cdot c};$$

$$- \overline{a+m-a} = \overline{0}, \quad \text{поэтому } \overline{m-a} = \overline{-a};$$

$$- \overline{a \cdot 1} = \overline{a}.$$

Таблицы сложения и умножения для вычетов по модулю 6.

Таблица 7

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Таблица умножения показывает, что уравнение $\bar{2} \cdot \bar{x} = \bar{1}$ в классе вычетов по модулю 6 не имеет решения, т.к. при умножении получаем числа, кратные 2.

Класс вычетов \bar{a} называется обратимым, если существует класс \bar{b} , такой что $\bar{a} \cdot \bar{b} = \bar{1}$. Класс \bar{b} называется обратным к классу \bar{a} и обозначается \bar{a}^{-1} .

Таблица 8

•	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Для того чтобы класс вычетов \bar{a} по модулю m был обратим, необходимо и достаточно, чтобы числа a и m были взаимно просты [7].

Таблица иллюстрирует утверждение теоремы. Числа 1 и 6, 5 и 6 взаимно просты, и таблица подтверждает, что уравнения $\bar{1} \cdot \bar{x} = \bar{1}$, $\bar{5} \cdot \bar{x} = \bar{1}$ имеют решения. Числа 2 и 6, 3 и 6, 4 и 6 не являются взаимно простыми, поэтому классы $\bar{2}$, $\bar{3}$, $\bar{4}$ не имеют обратных.

Для фиксированного натурального числа m множество классов $\bar{0}, \bar{1}, \dots, \overline{m-1}$ с введенными операциями сложения и умножения классов обозначается Z_m . Классы вычетов используются в криптографии при кодировании и декодировании информации.

Сравнением первой степени с неизвестной x называется уравнение вида $ax \equiv b \pmod{m}$, где $a \not\equiv 0 \pmod{m}$.

Решением сравнения (1) называется любое число, удовлетворяющее уравнению (1).

Теорема 1. Если число c удовлетворяет уравнению (1), то любое число c_1 вида $c_1 = c + mt$, $t \in Z$, т.е. $c_1 \equiv c \pmod{m}$ также удовлетворяет уравнению (1).

Доказательство. По условию теоремы число c удовлетворяет уравнению (1), поэтому $ac \equiv b \pmod{m}$. Разность $ac - b$ кратна m , поэтому $ac - b = mk$, $ac + amt - b = mk + amt$, $a(c + mt) - b = m(k + at)$, $ac_1 - b = m(k + at)$, $(ac_1 - b):m$, $ac_1 \equiv b \pmod{m}$.

Из теоремы следует, что если уравнение имеет решением число c , то все числа класса вычетов \bar{c} по модулю m также удовлетворяют уравнению. Поэтому сравнения естественно решать с точностью до класса вычетов.

Решить сравнение первой степени – значит найти все классы вычетов по модулю m , любой из которых удовлетворяет уравнению, а это более подробно означает, что при подстановке любого числа из этих классов в уравнение получаются числа, сравнимые по модулю m .

Теорема 2. (алгоритм решения уравнения $ax \equiv b(\text{mod } m)$).

а) Если $(a, m) = 1$, то существует и единственное решение $\bar{x} = \left(\bar{a}\right)^{\varphi(m)-1} \bar{b}$.

б) Если $(a, m) = d \neq 1$ и b не делится на d , то уравнение не имеет решения.

в) Если $(a, m) = d \neq 1$, $b: d$, то существует d решений вида

$$\bar{x}_0 = \bar{a}_1^{-\varphi(m_1)-1} \bar{b}_1, \bar{x}_k = \bar{x}_0 + \bar{m}_1 k, k = 0, 1, \dots, (d-1), a_1 = \frac{a}{d}, b_1 = \frac{b}{d}, m_1 = \frac{m}{d}.$$

Комментарий к условию в) теоремы. Если $(a, m) = d \neq 1$, $b: d$, то все коэффициенты данного уравнения нужно разделить на наибольший общий делитель, т.е. рассмотреть уравнение $a_1 x \equiv b_1(\text{mod } m_1)$. Вначале необходимо его решить,

что подтверждает выражение $\bar{x}_0 = \bar{a}_1^{-\varphi(m_1)-1} \bar{b}_1$, затем записать серию решений, обращая внимание на то, что сравнения должны записываться по модулю m .

Пример 3. Решить сравнения:

а) $5x \equiv 4(\text{mod } 6)$; б) $2x \equiv 3(\text{mod } 6)$; в) $8x \equiv 4(\text{mod } 6)$.

Решение.

а) $(5, 6) = 1$ находимся в условии а) теоремы, т.к. $\varphi(6) = 2$, $\bar{x} = \bar{5}^{-2} \bar{4}$. По таблице умножения вычетов по модулю 6 упрощаем $\bar{5} \cdot \bar{4} = \bar{2}$. Ответ может быть представлен в виде $x \equiv 2(\text{mod } 6)$ или $\bar{2} \in Z_6$. Кстати, наличие таблицы умножения вычетов по модулю 6 позволяет решить уравнение без использования теоремы. В горизонтальной строке, соответствующей множителю $\bar{5}$, находим $\bar{4}$, определяем столбец, где находится это число, и определяем неизвестный множитель $\bar{2}$.

Обращаем внимание на корректную запись ответа. Запись $\bar{2}$ не уточняет, по какому модулю рассматривается этот класс.

Если по модулю 5, то получаем множество $\bar{2} = \{\dots - 8, -3, 2, 7, 12, \dots\}$.

Если по модулю 6, то получаем множество $\bar{2} = \{\dots - 10, -4, 2, 8, 14, \dots\}$.

В пределах решения одного примера иногда встречается такая запись, но при переносе результата в другое место обязательно нужно указывать модуль сравнения, используя нижний индекс.

б) $(2, 6) = 2 = d$, но число 3 не делится на 2. Выполняется условие б) теоремы, поэтому уравнение не имеет решений.

Это легко проверить по таблице умножения. Умножая $\bar{2}$ на любое число, получаем четные числа, они представлены классами $\bar{0}, \bar{2}, \bar{4}$, которые не равны классу $\bar{3}$.

в) $(8,6)=2=d$, число 4 делится на 2, т.е. выполняется условие в) теоремы. Данное уравнение имеет 2 решения.

Разделив все числа в данном уравнении на наибольший общий делитель, получим уравнение $4x \equiv 2 \pmod{3}$.

Это уравнение имеет решение $x \equiv 2 \pmod{6}$, т.к. $(4, 3)=1$. Вспоминая о сравнении по модулю 6 в первоначальном уравнении, находим второе решение $x \equiv 2 + 3 \pmod{6}$, т.е. $x \equiv 5 \pmod{6}$.

Замечание. Данное уравнение можно было сразу упростить, т.к. $\bar{8} = \bar{2}$, поэтому получаем эквивалентное уравнение $2x \equiv 4 \pmod{6}$. Найдите решения этого уравнения по таблице умножения. \square

Теорема 3 (Китайская теорема об остатках). Пусть в системе

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \vdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

m_1, m_2, \dots, m_n – попарно взаимно простые числа, т.е. $\text{НОД}(m_i, m_j) = 1$ для любых i и j , где $i \neq j$, тогда система имеет единственное решение $\bar{x} = \sum_{k=1}^n M_k z_k$ в классе по модулю, равному числу m_1, m_2, \dots, m_n ,

где $M_k = \frac{\prod_{i=1}^n m_i}{m_k}$ и z_k – решение сравнения $M_k z_k \equiv b_k \pmod{m_k}$ для каждого k .

Пример 4. Найти решение системы сравнений

$$\begin{cases} x \equiv 5 \pmod{8}, \\ x \equiv 7 \pmod{11}. \end{cases}$$

Решение. Числа $m_1 = 8$ и $m_2 = 11$ являются взаимно простыми, поэтому можем применить теорему 3.

$$\text{Находим } M_1 = \frac{8 \cdot 11}{8} = 11, M_2 = \frac{8 \cdot 11}{11} = 8.$$

Для вспомогательных сравнений $11z_1 \equiv 5 \pmod{8}$, $8z_2 \equiv 7 \pmod{11}$ находим соответственно решения $z_1 = \bar{7}_{11}$, $z_2 = \bar{5}_8$.

Составляем выражение $M_1 z_1 + M_2 z_2 = 8 \cdot 5 + 11 \cdot 7 = 117$ и записываем ответ в классе по модулю $8 \cdot 11$, т.е. $x = \bar{29}_{88}$.

Пример 5. Группа обезьян пытается разложить кокосовые орехи в кучки. Если обезьяны разложат орехи в кучки по пять штук, то останется четыре ореха. Если разложат в кучки по четыре ореха, то останется три ореха. Если разложат в кучки по семь орехов, останется 2 ореха. Какое минимальное число орехов было?

Решение. Пусть x – искомое число орехов, тогда варианты разложения можно представить системой

$$\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 3 \pmod{4}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

Находим $M_1 = \frac{5 \cdot 4 \cdot 7}{5} = 28$, $M_2 = 35$, $M_3 = 20$.

Для вспомогательных сравнений $28z_1 \equiv 4 \pmod{5}$, $35z_2 \equiv 3 \pmod{4}$, $20z_3 \equiv 2 \pmod{7}$ находим соответственно решения $z_1 = 8$, $z_2 = 1$, $z_3 = 5$.

Составляем выражение $M_1z_1 + M_2z_2 + M_3z_3 = 28 \cdot 8 + 35 \cdot 1 + 20 \cdot 5 = 359$ и записываем ответ в классе по модулю $5 \cdot 4 \cdot 7$, т.е. $x = \overline{359}_{140} = \overline{79}_{140}$. Минимальное положительное число в этом классе равно 79. \square

Рассмотрим задачу о нахождении всех целых решений (x, y) уравнения первой степени с целыми коэффициентами

$$ax + by = c. \quad (1)$$

Алгоритм решения сравнения первой степени позволяет ответить на вопрос, когда и сколько решений имеет сравнение

$$ax \equiv c \pmod{b}. \quad (2)$$

Пусть x_0 – решение сравнения (2). Тогда $ax_0 \equiv c \pmod{b}$. Следовательно, $(ax_0 - c):b$, $ax_0 - c = b(-y_0)$, где $(-y_0)$ – некоторое целое число. Следовательно, $ax_0 + by_0 = c$, т.е. (x_0, y_0) – решение уравнения (1). Эти рассуждения справедливы и в обратную сторону.

Таким образом, уравнение первой степени сводится к решению сравнения первой степени.

Теорема 4. Если $(a, b) = d$, то уравнение $ax + by = c$ имеет целочисленные решения в том и только в том случае, когда c делится на d .

На практике этой связью между уравнениями пользуются редко. Например, чтобы найти одно из решений уравнения $ax + by = c$ используют алгоритм Евклида или используют цепные дроби. Но чаще одно из решений такого уравнения находят устно для некоторых коэффициентов.

Все решения уравнения находятся по следующей теореме [7].

Теорема 5. Если (x_0, y_0) – одно из целочисленных решений уравнения $ax + by = c$ и $(a, b) = d$, то общее решение этого уравнения имеет вид

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

Замечание. Проверьте, что решение уравнения можно записать в виде

$$x = x_0 - \frac{b}{d}t, \quad y = y_0 + \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

Пример 6. Решить уравнения:

а) $5x - 3y = 9$; б) $6x + 10y = 7$; в) $14x - 20y = 26$.

Решения. а) $(5, 3) = 1$. Уравнение имеет решения вне зависимости от значений правой части.

Частное решение найдем методом подбора. Слагаемое $5x$, где x – целое, означает, что нужно рассматривать числа, кратные 5. Например, 5, 10, 15, 20,...

Слагаемое $3y$ также ориентирует на рассмотрение чисел, кратных 3, т.е. 3, 6, 9, 13,...

Разность числа из одного ряда и числа из другого ряда должна быть равна 9. Такую пару легко обнаружить: $15 - 6 = 9$. Итак, получаем частное решение: $x_0 = 3$, $y_0 = 2$. Все решения данного уравнения $x = 3 - 3t$, $y = 2 - 5t$, $t \in R$.

б) $(6, 10) = 2$, но правая часть уравнения не делится на 2. Поэтому данное уравнение не имеет решений по теореме 1.

Поясним это другим способом, преобразуя данное уравнение $2(3x + 5y) = 7$. Для любых целых значений x , y левая часть уравнения кратна 2, а правая часть не кратна 2. Получили противоречие.

в) $(14, 20) = 2$. Правая часть делится на 2, данное уравнение имеет решение.

Разделив данное уравнение на 2, получим более простое уравнение, эквивалентное данному уравнению:

$$7x - 10y = 13. \quad (3)$$

Будем искать частное решение с помощью алгоритма Евклида.

Рассмотрим другое более простое уравнение, полученное заменой правой части на 1, т.е.

$$7x - 10y = 1. \quad (4)$$

Если мы найдем решение уравнения (4), то, умножая это уравнение на 13, получим решение уравнения (3).

Применим к коэффициентам уравнения (4) при неизвестных (не обращая внимания пока на знаки) алгоритм Евклида

$$10 = 7 \cdot 1 + 3, \quad 7 = 3 \cdot 2 + 1.$$

Из этих равенств выразим 1 (это правая часть уравнения (4)) через коэффициенты уравнения:

$$1 = 7 - 3 \cdot 2, \quad 3 = 10 - 7 \cdot 1, \quad 1 = 7 - (10 - 7) \cdot 2 = 7 \cdot 3 - 10 \cdot 2.$$

Равенство $1 = 7 \cdot 3 - 10 \cdot 2$ позволяет найти частное решение уравнения (4), но его не обязательно выписывать.

Умножая последнее равенство на 13 и сохраняя данные коэффициенты 7 и 10, получим $13 = 7 \cdot 39 - 10 \cdot 26$.

Из этого равенства получаем частное решение $x_0 = 39$, $y_0 = 26$ уравнения (3).

Общее решение уравнения (3): $x = 39 - 10t$, $y = 26 - 7t$, $t \in Z$.

Данное уравнение $14x - 20y = 26$ имеет это же решение, которое, кстати, можно записать в другом виде $x = 39 + 10t$, $y = 26 + 7t$, $t \in Z$. \square

Рассмотрим второй способ решения примера 4, используя определение сравнений и не используя китайскую теорему об остатках.

Пример 7.

Найти решение системы сравнений

$$\begin{cases} x \equiv 5 \pmod{8}, \\ x \equiv 7 \pmod{11}. \end{cases}$$

Уравнение $x \equiv 5 \pmod{8}$ имеет решение $x = \overline{5}_8$ или $x = 5 + 8t$, где $t \in Z$.

Уравнение $x \equiv 7 \pmod{11}$ имеет решение $x = \overline{7}_{11}$ или $x = 7 + 11u$, где $u \in Z$.

Из равенства $5 + 8t = 7 + 11u$ получаем уравнение $8t - 11u = 2$. Находим вначале частное решение этого уравнения в целых числах $t = 3, u = 2$, а затем легко обнаружить и общее решение уравнения $t = 3 + 11k, u = 2 + 8k$. Подставляя t или u найдем $x = 29 + 88k$. \square

Пример 8. Рассмотрим второй способ решения примера 5 с обезьянами и орехами, используя определение сравнений и не используя китайскую теорему об остатках.

Решить систему сравнений

$$\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 3 \pmod{4}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

Решение. Уравнение $x \equiv 4 \pmod{5}$ имеет решение $x = 4 + 5t$, где $t \in Z$.

Уравнение $x \equiv 3 \pmod{4}$ имеет решение $x = 3 + 4u$, где $u \in Z$.

Уравнение $x \equiv 2 \pmod{7}$ имеет решение $x = 2 + 7v$, где $v \in Z$.

Сравнивая значение x , получаем систему

$$\begin{cases} 4u - 5t = 1, \\ 7v - 4u = 1. \end{cases}$$

Первое уравнение системы имеет решение $u = 4 + 5m, t = 3 + 4m, m \in Z$.

Второе уравнение системы имеет решение $v = 3 + 4n, u = 5 + 7n, n \in Z$.

Сравнивая значения для u , получаем уравнение $5m - 7n = 1$, которое имеет решение $m = -4 + 7k, n = -3 + 5k, k \in Z$. Подставляя эти значения в промежуточные выражения, получим $x = -61 + 140k$ или $x = \overline{-61}_{140}$. \square

Теорема 6. (малая теорема Ферма). Если p – простое число и a – целое, взаимно простое с p , т.е. $(a, p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$.

Теорема 7. (теорема Эйлера) Если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Пример 9, иллюстрирующий теорему.

$$a = 2, n = 9, (2, 9) = 1, \varphi(9) = 6, 2^6 \equiv 1 \pmod{9},$$

$$a = 5, n = 12, (5, 12) = 1, \varphi(12) = 4, 5^4 \equiv 1 \pmod{12}. \quad \square$$

Теорема 8. (теорема Ферма – Эйлера). Если p и q – различные простые числа, а m – любое целое число, которое не делится на p и q , то $m^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Задачи.

37.1. Докажите, что если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то:

а) $a + c \equiv b + d \pmod{n}$ (сравнения по одному и тому же модулю можно складывать);

б) $a - c \equiv b - d \pmod{n}$ (сравнения по одному и тому же модулю можно вычитать);

в) $ak \equiv bk \pmod{n}$ (обе части сравнения можно умножать на одно и то же число);

г) $ac \equiv bd \pmod{n}$ (сравнения по одному и тому же модулю можно перемножать);

д) $a^n \equiv b^n \pmod{n}$ (сравнение можно возводить в степень).

37.2. Докажите, что если $ac \equiv bc \pmod{n}$, то $a \equiv b \pmod{n}$ при условии, что числа n и c взаимно простые (обе части сравнения можно сократить на число, взаимно простое с модулем n).

37.3. Докажите, что если $a \equiv b \pmod{mn}$, то $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$.

37.4. Докажите, что если a – нечетное целое число, то $a^2 \equiv 1 \pmod{8}$.

37.5. Найдите все значения x , удовлетворяющие уравнению $x \equiv 2 \pmod{11}$.

37.6. Найдите наибольшее отрицательное число x , удовлетворяющее уравнению $x \equiv 2 \pmod{7}$.

37.7. Найдите наименьшее положительное число x , удовлетворяющее уравнению $x \equiv -3 \pmod{7}$.

37.8. Найдите наименьшее положительное число x , удовлетворяющее уравнению $3^{89} \equiv x \pmod{7}$.

37.9. а) Постройте таблицу сложения и таблицу умножения для классов вычетов по модулю 7;

б) используя эти таблицы, решите уравнения:

$$x + \bar{2} \equiv \bar{6}, x \cdot \bar{2} \equiv \bar{6}, x + \bar{2} \equiv \bar{0}, x \cdot \bar{2} \equiv \bar{1}.$$

37.10. Пусть p – простое число и $(a, p) = 1$. Покажите, что сравнение $ax \equiv 1 \pmod{p}$ имеет решение $x \equiv a^{p-2} \pmod{p}$.

37.11. Решите сравнения: а) $2x \equiv 6 \pmod{8}$; б) $2x \equiv 4 \pmod{8}$.

37.12. Решите систему уравнений $x \equiv 7 \pmod{8}, x \equiv 5 \pmod{11}$.

37.13. Решите уравнения в целых числах:

а) $23x + y = 2302$, б) $25x - y = 2499$.

37.14. Сколькими способами можно набрать сумму в 51 р. двухрублевыми и пятирублевыми монетами?

37.15. Проходит ли через точки с целочисленными координатами прямая, заданная уравнением $3x + 2y = 4$?

37.16. Представьте число 263 в виде суммы двух натуральных слагаемых, одно из которых кратно 3, а второе кратно 4.

37.17. Решите систему сравнений

$$x \equiv 5 \pmod{3}, x \equiv 7 \pmod{2}, x \equiv 3 \pmod{5}.$$

37.18. Найдите остаток при делении: а) 3^4 на 5; б) 3^6 на 7; в) 5^6 на 7.

37.19. Докажите малую теорему Ферма: если p – простое число, m – любое число, которое не делится на p , то $m^{p-1} \equiv 1 \pmod{p}$, т.е. число m^{p-1} при делении на p дает остаток 1.

§ 38. Простейшие способы кодирования информации

Процесс кодирования сообщения называется *шифрованием* (зашифровкой), а обратный процесс декодирования называется *расшифрованием* (расшифровкой).

Кодированное сообщение называется шифрованным (шифровкой), а применяемый метод называется *шифром*.

Основное требование к шифру состоит в том, чтобы расшифровка и зашифровка были возможны при наличии некоторой дополнительной информации или устройства, которые называется *ключом*.

Процесс декодирования шифровки без ключа называется *дешифрованием* или *раскрытием ключа*.

Область знаний о шифрах, методах их создания и раскрытия называется *криптографией*.

Криптография существенно использует факты теории чисел, возродила новый интерес к этой древней науке и породила новую область знаний – прикладную теорию чисел.

Свойство шифра противостоять раскрытию называется *криптостойкостью* (надежностью) и обычно измеряется сложностью алгоритма дешифрования.

В I веке н.э. Юлий Цезарь во время войны с галлами применил шифр, заменяющий первую букву латинского алфавита

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

на четвертую, вторую на пятую, т.е. осуществлялся циклический сдвиг букв на 3 позиции вправо.

Переданное сообщение YHQL YLGL YLFL следует расшифровать VENI VIDI VICI. Сообщение переводится – пришел, увидел, победил.

Сдвиг букв можно осуществить по более сложному правилу, например по ключу 1432. Это означает, что первая буква сообщения сдвигается по алфавиту на один знак, вторая буква на четыре знака, третья буква на три знака, а четвертая буква на два знака. Далее сдвиг букв повторяется. Сообщение «Иванов, передай решение задачи!» шифруется следующим образом:

1 4 3 2 1 4 3 2 1 4 3 2 1 4 3 2 1 4 3 2 1 4 3 2 1 4
 Иванов, передай решение задачи!
 Й ё г п п ё, т ж с и ж в к ф з ь ё с л ж и д ж в ш м!

Этот прием кодирования разгадать сложнее. Для этого приема кодирования одна и та же буква в разных местах текста может оказаться зашифрованной по-разному.

Криптографические системы делятся на два основных класса в соответствии с тем, как при их использовании поступают с исходным текстом.

Если буквы не зашифрованного текста только меняются местами, т.е. осуществляется их перестановка, то система называется *транспозицией*.

Если буквы заменяются некоторыми эквивалентами – другими буквами, цифрами или какими-либо иными знаками, но их порядок при этом остается неизменным, то система называется *подстановкой*. В одной шифровке могут применяться транспозиция и подстановка.

Каждая транспозиция использует некоторую геометрическую фигуру, в которую вписывают исходный текст по ходу одного маршрута, а затем считывают по ходу другого маршрута.

Фразу “с двадцатого апреля запускаем завод” запишем (таблица 9) в прямоугольник по строкам, двигаясь слева направо, справа налево, слева направо и т.д. (рис. 1). Клетки, для которых не хватило букв, заполняем произвольными буквами.

Таблица 9

С	Д	В	А	Д	Ц	А	Т
Л	Е	Р	П	А	О	Г	О
Я	З	А	П	У	С	К	А
Х	Д	О	В	А	З	М	Е

Считываем информацию по столбцам, двигаясь справа налево, а в столбцах сверху вниз и снизу вверх (рис. 2). В силу международных правил, контролирующих стоимость передачи телеграфных сообщений, окончательный текст криптограммы обычно разбивается на группы по 5 символов.

Получаем ТОАЕМ КГАЦО СЗАУА ДАППВ ОАРВД ЕЗДХЯ ЛС. Это пример *маршрутной транспозиции*.



Рис. 1



Рис. 2

Таблица 10

С ₃	У ₅	Р ₂	Г ₁	У ₆	Т ₄
П	Р	О	Т	И	В
Н	И	К	З	А	В
Л	А	Д	Е	Л	А
В	Т	О	М	О	Б
И	Л	Ь	Н	Ы	М
М	О	С	Т	О	М

Пример *постолбцовой транспозиции*.
 Текст вписывается в таблицу обычным способом, считывается по порядку, зашифрованным некоторым ключом. Например, словом “Сургут” (таблица 10). Буквы в ключе упорядочиваем в алфавитном порядке. Две одинаковые буквы упорядочиваем в порядке написания в слове. Фраза “противник завладел автомобильным мостом” шифруется следующим образом:
 ТЗЕМН ТОКДО ЁСПНЛ ВИМВВ АБММР ИАТЛО ИАЛЮБ О.

Таблица Виженера устроена следующим образом. В первой строке записывается весь алфавит (таблица 11). В каждой следующей строке осуществляется циклический сдвиг на одну букву. Получаем квадратную таблицу 31×31 (без букв: Ъ, Ё).

Таблица 11

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю

Над сообщением (Сбежим с пары в столовую) записываем слово – ключ “Радужный” с повторением. Для шифровки текста находим очередную букву в ключевой строке и ее место в вертикальном алфавите. Для соответствующей буквы в сообщении находим знак в горизонтальном алфавите. На пересечении столбца и строки получаем букву для шифрования. Достоинство таблицы Виженера в том, что одна и та же буква шифруется различными символами.

РАДУЖНЫЙ РАДУЖНЫЙ РАДУ
СБЕЖИМ СПАРЫ В СТОЛОВУЮ

Шифрованное сообщение

В Б Й Щ О Щ Н Ш А Р А Х Ч А К Ф Я В Ч С.

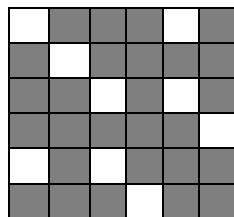


Рис. 3

К перестановкам относится шифр “*решето Кардано*”. Это прямоугольная карточка с отверстиями (рис. 3). При наложении на лист бумаги текст вписывает-

ся в отверстия. При последовательных поворотах карточки вокруг центра на 90° в направлении вращения часовой стрелки вписываются следующие буквы.

Текст для шифрования “Встреча 10 04 в 18 00 Музей Пароль Репин упал” после вписывания в решетку Кардано принимает вид (таблица 12).

Рассмотрим вопросы, предъявляемые к шифру, на примере решетки Кардано:

Таблица 12

О	З	Р	В	4	Е
С	В	Т	Е	Й	П
И	П	1	А	8	Р
Р	Н	Е	У	Ч	О
О	А	М	О	П	Л
1	А	Б	У	О	Л

а) как построить решетку для шифрования в квадрате размером $2n \times 2n$, где $n \geq 1$?

б) сколько различных решеток может быть для квадрата фиксированного размера?

в) какова вероятность расшифровать текст противником?

На рис. 4 квадрат разделен на 4 области, кото-
рые получаются одна из другой поворотом вокруг
центра квадрата на углы, кратные
 $\pi/2$. Существует ли более про-
стое деление большого квадрата
на 4 области, так чтобы каждая
область из другой получалась
указанными поворотами?

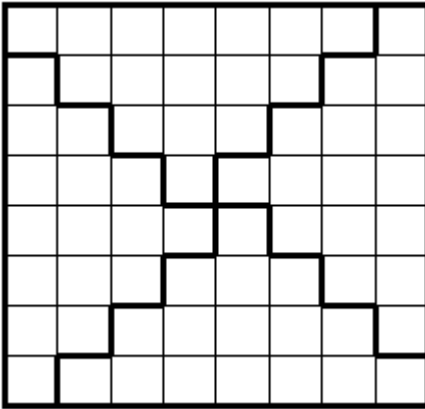


Рис. 4

Число квадратов в каждой области равно

$$(2n - 1) + (2n - 3) + \dots + 3 + 1 = n^2.$$

Кстати, число квадратов в каждой области можно вычислить, если разделить общее число квадратов на четыре, т.е.

$$\frac{(2n)^2}{4} = n^2.$$

Если в большом квадрате выбран маленький квадрат (один из $4n^2$ квадратов) в качестве окна решетки для вписывания текста, то все остальные три квадрата, полученные поворотом, исключаются для выбора остальных окон решетки.

Первое окно в большом квадрате может быть в любом из $4n^2$ квадратов. Второе окно можно выбрать в любом из $4n^2 - 4$ квадратов, третье окно в любом из $4n^2 - 8$ квадратов. Последнее окно может быть выбрано в любом из 4 квадратов.

По правилу произведения число способов, с помощью которых можно выбрать окна, с учетом нумерации окон равно:

$$4n^2 \times 4(n^2 - 1) \times 4(n^2 - 2) \times \dots \times 2 \times 1 = 4^{n^2} n!.$$

Учитывая, что нумерация окон при изготовлении решетки не имеет значения, нужно полученное число решеток разделить на число перестановок из n^2 элементов, т.е. на $n!$

Число решеток в квадрате размером $2n \times 2n$ равно 4^{n^2} .

Для квадрата 8×8 число шифров равно 4294967296. В качестве одного из шифров можно выбрать все n^2 окон в одной из четырех построенных областей.

В этом случае шифровка может быть легко прочитана. Если исключить решетки с несколькими примыкающими окнами, останется несколько сотен миллионов решеток. Вероятность раскрытия шифра окажется малой при $n = 4$.

Криптограммы часто расшифровывают, учитывая частоту букв в алфавите.

Расположение букв русского алфавита по их относительной частоте на 1000 символов приведено в таблице 13.

Таблица 13

№			№		
1	о	0,090	14	я	0,018
2	е-ё	0,072	15	ы, з	0,016
3	а, и	0,062	16	б, ь-ъ	0,014
4	н, т	0,053	17	г	0,013
5	с	0,045	18	ч	0,012
6	р	0,040	19	й	0,010
7	в	0,038	20	х	0,009
8	л	0,035	21	ж	0,007
9	к	0,028	22	ш, ю	0,006
10	м	0,026	23	ц	0,004
11	д	0,025	24	щ, э	0,003
12	п	0,023	25	ф	0,002
13	у	0,021			

Следует отметить, что в профессиональных сообщениях из различных наук частота букв для каждой науки имеет свою специфику.

Замаскировать частоту появления букв можно многосимвольной подстановкой, т.е. заменой сочетания букв из сообщения группой символов. Рассмотрим классическую двухсимвольную систему, *шифр Плейфера*, модифицированную для русского алфавита.

В матрицу 5×6 (таблица 14) вписываем ключевое слово, например “Нижневартовск”. Повторяющиеся буквы опускаем и дописываем остальные буквы алфавита, за исключением букв *Ъ, Ъ, Ъ*, без которых любой текст можно понять.

Таблица 14

Н	И	Ж	Е	В	А
Р	Т	О	С	К	Б
Г	Д	З	Л	М	П
У	Ф	Х	Ц	Ч	Ш
Щ	Ъ	Ы	Э	Ю	Я

Незашифрованное сообщение делим на пары букв. Если встречаем две одинаковые буквы подряд, то вставляем между ними нерабочую букву *Х*. Например, для фразы “На рассвете наступаем” получаем пары

НА РА СХ СВ ЕТ ЕН АС ТУ ПА ЕМ.

Если две буквы пары находятся в одной строке (или одном столбце) прямоугольника, то при шифровании каждая из них заменяются соседней справа (или снизу), причем совокупность букв в каждой строке и в каждом столбце рассматривается как цикл. Например, пара НА меняется на пару ИН.

Если буквы не находятся в одной строке (столбце), то они расположены в противоположных углах некоторого прямоугольника. Тогда они заменяются буквами, стоящими в двух других противоположных углах прямоугольника, причем каждая из них заменяется той, с которой она находится в одной строке. Например, пара РА меняется на пару БН.

Получаем шифровку ИН БН ОЦ КЕ ИС ВИ ЕБ РФ ШБ ВЛ.

Рассмотрим пример нераскрываемого шифра “одноразовый шифровальный блокнот”. Два человека договариваются об определенной книге, имеющейся у каждого из них. Например, Ильф и Петров “Двенадцать стульев. Золотой теленок.”– Р/Д., 1998 – 526 с.

Они договариваются о ключе (261, 3), т.е. о странице 261 и 3-й строке:

“О том, что он лучше других мальчиков, Ипполит узнал во время вступительного экзамена по арифметике”.

Занумеруем буквы алфавита и цифры до десяти:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Х Ц Ч Ш Щ Ъ Ы Э Ю Я 1 2 3 4 5 6 7 8 9 0
21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40

Указанную фразу из книги записываем в виде последовательности чисел:

14 18 14 12 23 18 14 14 13 11 19 23 24 5 ...

Нумеруем нужное сообщение “Завтра скупаем весь сахар”:

7 0 2 18 16 0 17 10 19 15 0 5 12 2 5 17 26 17 0 21 0 16

Шифруем сообщение по правилу

$$a_n + c_n \equiv b_n \pmod{40}, 0 \leq b_n \leq 40, \text{ где}$$

a_n – последовательность номеров передаваемого сообщения,

c_n – последовательность из книги,

b_n – зашифрованная последовательность.

Получаем шифровку:

21 18 16 28 0 18 31 24 32 26 19 28 17 ...

Расшифровка вторым человеком осуществляется по правилу:

$$a_n \equiv (b_n - c_n) \pmod{40}.$$

Задачи.

38.1. Зашифруйте фразу «Списывание – порок, недостойный на дискретке» шифром Цезаря. Для шифрования используйте 40-символьный алфавит, содержащий 30 букв и 10 цифр. Напишите компьютерную программу для расшифровки сообщения, закодированного шифром Цезаря.

38.2. Как следует изменить шифровку фразы в задаче 38.1, если при шифровании необходимо выполнить сдвиг на 4 позиции вправо?

38.3. Напишите компьютерную программу для кодирования текста с ключевым словом «1432».

38.4. Зашифруйте фразу «Хорошо-то хорошо, только ничего хорошего» методом маршрутной транспозиции. Подберите рациональные размеры прямоугольника, чтобы эта фраза вместились в него целиком и оставалось немного пустых клеток в прямоугольнике после заполнения словами. Укажите в нем другой маршрут транспозиции.

38.5. Зашифруйте с помощью постолбцовой транспозиции фразу «Мою шифровку не прочтет преподаватель» с помощью ключевого слова «Москва». Подберите рациональные размеры прямоугольника, чтобы эта фраза вместились в него целиком и пустых клеток в прямоугольнике после заполнения словами оставалось немного.

38.6. Зашифруйте фразу «Кодирование – самая интересная тема дискретной» с помощью таблицы Виженера, используя ключевое слово

«Владивосток». Передайте эту шифровку своему другу и попросите расшифровать.

38.7. Зашифруйте фразу «Приглашаю Вас в кафе вторник 18 00» с помощью решета Кардано.

38.8. Зашифруйте фразу «Этот факультатив ориентирует меня на профессию» с помощью шифра Плейфера.

38.9. Используя ключ “Сургут”, зашифруйте таблицей Плейфера фразу “Рассмотрим производную”.

38.10. Выберите в этом задачнике строку, содержащую текст, и, используя ее, зашифруйте методом одноразового блокнота фразу «Я обязательно найду свой способ шифрования».

38.11. Используя ключевую фразу “Дискретная математика”, зашифруйте с помощью одноразового блокнота фразу “Я сдал экзамен”.

38.12. а) Определите число шифров для решета Кардано в квадрате размером 6×6 .

б) Постройте несколько решеток для решета Кардано в квадрате размером 8×8 .

в) Сколько различных решеток Кардано можно построить в квадрате размером 7×7 ?

§ 39. Шифрование аффинным преобразованием

Занумеруем буквы русского алфавита (без букв й, ъ, ё) числами от 0 до 29:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Шифр Юлия Цезаря, сдвигающий буквы вправо на 3 единицы, задается формулой

$$y \equiv (x + 3) \pmod{30}. \quad (1)$$

Знак сравнения в формуле (1) означает, что число y равно остатку при делении числа $x + 3$ на число 30.

Например, фраза “Люблю я кофе поутру” шифруется абракадаброй “Обдобо нсуи тсьхуц”.

Расшифровка текста осуществляется

$$x \equiv (y - 3) \pmod{30}.$$

Этот шифр является частным случаем сдвига

$$y \equiv (x + d) \pmod{30}, \text{ где } d \in \mathbb{N}, 1 \leq d \leq 30. \quad (2)$$

Предположим, что d меняется в каждой шифровке по некоторому закону. Например, $d = 32 - k$, где k – дата отправки шифровки.

Если d для расшифровывающей стороны неизвестно, то это число легко найти, осуществляя сдвиг полученного сообщения влево на 1, 2, ..., 31 “разря-

дов”. Из 31 полученной “расшифровки” где-то можем получить осмысленный текст.

Более скрытой системой шифрования является использование преобразования текста по аффинному закону

$$y \equiv (ax + d) \pmod{30}, \quad (3)$$

где (a, d) – заранее оговоренная пара целых чисел, удовлетворяющая условию $(a, n) = 1$ ($a; n) = 1$, n – число символов, используемых в алфавите сообщения.

Пример 1. Для аффинного преобразования

$$y \equiv (7x + 12) \pmod{30} \quad (4)$$

сообщение “ключ под ковриком” нужно передать шифровкой “рчнос холл роуэироя”.

Расшифровка текста, зашифрованного аффинным преобразованием (3), осуществляется по формуле

$$x \equiv a^{-1}y - a^{-1}d \pmod{30}, \quad (5)$$

где a^{-1} – обратный элемент к a в классе вычетов по модулю n , т.е. в Z_n . Справедливость формулы (5) проверяется непосредственной подстановкой

$$y = a(a^{-1}y - a^{-1}d) + b.$$

Для преобразования (4) получаем:

$$7^{-1} = 13, \text{ т.к. } 7 \cdot 13 \equiv 1 \pmod{30},$$

$$x \equiv 13y + 6 \pmod{30}. \quad (6)$$

Пусть нам известно, что перехваченное сообщение зашифровано аффинным преобразованием (4). Нам необходимо определить ключ $(a; d)$, чтобы прочесть сообщение.

Применим частотный анализ. Допустим, что в шифровке достаточно большого объема часто встречающимся буквам “ц, ь” соответствуют часто встречающиеся буквы “о, е”. Подставляя численные значения этих букв в преобразование (3), получим систему

$$\begin{cases} a \cdot 13 + d \equiv 21 \pmod{30}, \\ a \cdot 5 + d \equiv 25 \pmod{30}. \end{cases}$$

Вычитая второе уравнение из первого уравнения, получим

$$8a = -4, \quad 8a = 26 \Rightarrow a = 7.$$

Подставляя в любое уравнение системы, получим $d = 20$.

Сообщение может быть дешифровано формулой $y \equiv 7x + 20 \pmod{30}$. □

Возможно, что этот алгоритм придется применить несколько раз, т.к. частоту букв сложно определить для текста небольшого объема.

Анализ декодирования ключа показывает, что его можно раскрыть при наличии несложной информации.

Рассмотрим небольшую модификацию метода аффинных преобразования для кодирования.

Сообщения из двух (трех) символов назовем биграммой (триграммой).

Любой биграмме xy поставим в соответствие число по правилу

$k = nx + y$, где n – число символов в используемом алфавите.

Имеем неравенства

$$0 \leq x \leq n-1, 0 \leq nx + y \leq n^2 - 1, 0 \leq k \leq n^2 - 1.$$

Преобразуем полученное число аффинным преобразованием (3)

$$k' \equiv ak + d \pmod{n^2}, (a, n) = 1.$$

Шифруем полученное число символами, используя разложение

$$k' = nx' + y'.$$

Получаем шифровку $x'y'$ биграммы.

Расшифровка осуществляется в обратную сторону, причем

$$k \equiv a^{-1}k' - a^{-1}d \pmod{n^2}.$$

Пример 2. Зашифровать слово “НЕ”, используя биграмму и преобразование

(4).

Решение. Биграмме “НЕ” поставим в соответствие число

$$k = 30 \cdot 12 + 5 = 365.$$

Преобразуем число 365 с помощью аффинного преобразования

$$k' = 7 \cdot 365 + 12 \pmod{900}, k' \equiv 767 \pmod{900}.$$

Шифруем число 767

$$767 = 25 \cdot 30 + 17, (25 \ 17) \rightarrow \text{БТ}.$$

Слово “НЕ” зашифровано словом “БТ”. □

Шифрующая матрица

На множестве действительных чисел R каждая невырожденная матрица

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ где } a, b, c, d \in R, D = ad - bc \neq 0$$

имеет обратную матрицу

$$A^{-1} = \begin{pmatrix} dD^{-1} & -bD^{-1} \\ -cD^{-1} & aD^{-1} \end{pmatrix}.$$

В кольце Z_{30} с операциями $+$ и \times справедлив аналогичный результат. Это утверждение следует из следующей теоремы.

Теорема. Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, где $a, b, c, d \in Z_n$, $D = ad - bc$, тогда следующие утверждения эквивалентны:

а) НОД $(D, n) = 1$;

б) матрица A имеет обратную;

в) если хотя бы один из элементов $x, y \in Z_n$ отличен от нуля, то

$$A \begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix};$$

г) матрица A задает взаимно однозначное отображение множества $Z_n \times Z_n$ на себя.

Найдем обратную матрицу к матрице

$$A = \begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix}, \text{ для которой } a_{ij} \in Z_{30}, D = 17.$$

Числа 30 и 17 взаимно простые, поэтому матрица имеет обратную матрицу.

Обратным элементом к числу 17 в кольце Z_{30} является число 23, т.к.

$$17 \cdot 23 \equiv 1 \pmod{30}. \text{ Поэтому } 17^{-1} = 23.$$

Для обратной матрицы получаем

$$A^{-1} = \begin{pmatrix} 5 \cdot 23 & -9 \cdot 23 \\ -2 \cdot 23 & 7 \cdot 23 \end{pmatrix} = \begin{pmatrix} 115 & -207 \\ -46 & 161 \end{pmatrix} \equiv \begin{pmatrix} 25 & 3 \\ 14 & 11 \end{pmatrix} \pmod{30}.$$

Проверка

$$A \cdot A^{-1} = \begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 25 & 3 \\ 14 & 11 \end{pmatrix} = \begin{pmatrix} 301 & 120 \\ 120 & 61 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{30},$$

$$A^{-1} \cdot A = \begin{pmatrix} 25 & 3 \\ 14 & 11 \end{pmatrix} \begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 181 & 240 \\ 120 & 181 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{30}.$$

Шифрующую матрицу A будем использовать для шифровки биграмм следующим образом:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix},$$

т.е. биграмму $\begin{pmatrix} x \\ y \end{pmatrix}$ преобразуем в биграмму $\begin{pmatrix} x' \\ y' \end{pmatrix}$ по правилу $AX = X'$.

Дешифровка осуществляется применением обратной матрицы

$$A^{-1}X' = X.$$

Пример 3. Зашифровать биграмму “ДА” матрицей A .

Шифрование: $\begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 28 \\ 8 \end{pmatrix}$. Заменяя числа соответствующими буквами, получаем шифровку “ЮИ”.

Расшифровывание: $\begin{pmatrix} 25 & 3 \\ 14 & 11 \end{pmatrix} \begin{pmatrix} 28 \\ 8 \end{pmatrix} = \begin{pmatrix} 724 \\ 480 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 0 \end{pmatrix} \pmod{30}$ приводит к замене “ЮИ” \rightarrow “ДА”.

Чтобы зашифровать любое сообщение шифрующей матрицей, разбиваем сообщение на пары, записываем последователь биграмм столбцами в матрицу X .

Зашифруем, например, название города “Сургут”:

Запишем слово в матрицу $\begin{pmatrix} С & Р & У \\ У & Г & Т \end{pmatrix}$. Заменяя буквы соответствующими

числами, получим

$$\begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 16 & 15 & 18 \\ 18 & 3 & 17 \end{pmatrix} = \begin{pmatrix} 274 & 132 & 279 \\ 122 & 45 & 121 \end{pmatrix} \equiv \begin{pmatrix} 4 & 12 & 9 \\ 2 & 15 & 1 \end{pmatrix} \pmod{30}.$$

Получаем шифровку “ДВНРЛБ”.

В этом примере одна и та же буква У оказалась зашифрованной различными символами. □

Каждый способ шифрования характеризуется криптостойкостью. В рассмотренном способе шифрования секрет шифрования составляют следующие характеристики.

1. Сколько букв используется в алфавите. Количество букв русского алфавита могли выбрать 31, 32, 33. Могли добавить “пробел” для лучшего понимания текста, а также для дезориентации перехватчика информации. Пробел между словами часто встречается в тексте, поэтому есть вероятность, что при частотном анализе букв пробел воспримут как наиболее часто встречающуюся букву “о”.

2. Нумерацию букв можно осуществить разными способами, известными только передающему информацию и принимающему информацию.

3. Выбор шифрующей матрицы. Она, кстати, могла меняться каждый день по некоторому ранее заключенному договору.

Рассмотрим раскрытие шифрующей матрицы. Будем предполагать, что все остальные условия остались прежними.

Пусть мы имеем ограниченную информацию и хотим ее дешифровать. Предположим, что шифрование проводилось одной и той же матрицей.

Пусть мы имеем две биграммы X_1 и X_2 открытого текста и две биграммы X'_1, X'_2 шифрованного текста, тогда

$$AX_1 = X'_1, AX_2 = X'_2.$$

Объединим X_1 и X_2 в одну матрицу X , объединим X'_1, X'_2 в другую матрицу X' , тогда

$$AX = X' \quad (1)$$

или $A = X'X^{-1}$, если матрица X имеет обратную матрицу.

Пример 4. Пусть известно, что Иванов Николай подписывает сообщения своим именем. Перехваченное сообщение заканчивается шифрованным именем “АШБР”.

Решение. Подпись из четырех символов указывает, что использовалось имя из четырех букв. Предположим, что имя “Коля” использовалось для подписи, тогда

$$X = \begin{pmatrix} 9 & 10 \\ 13 & 29 \end{pmatrix}, D = 11, D^{-1} = 11, X^{-1} = \begin{pmatrix} 19 & 10 \\ 7 & 9 \end{pmatrix}.$$

$$X' = \begin{pmatrix} 0 & 1 \\ 23 & 15 \end{pmatrix} A = \begin{pmatrix} 0 & 1 \\ 23 & 15 \end{pmatrix} \begin{pmatrix} 19 & 10 \\ 7 & 9 \end{pmatrix} = \begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix}.$$

$$\text{Проверка } AX = \begin{pmatrix} 7 & 9 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 9 & 10 \\ 13 & 29 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 23 & 15 \end{pmatrix}.$$

Условие задачи содержит неопределенность. В качестве имени возможно использовалось сокращение “Нико”. Указанный выше алгоритм встречает затруднение, т.к. определитель матрицы

$$X = \begin{pmatrix} 12 & 9 \\ 8 & 13 \end{pmatrix} \text{ равен нулю.}$$

Если подставить значения матрицы X и X' в матричное уравнение (1), то получим систему уравнений с нулевым определителем. Она имеет конечное множество решений в множестве Z_{30} . Методом перебора ее можно решить, но лучше использовать дополнительную информацию.

Замечание. Выбор числа $n = 30$ в алфавите не является удачным, т.к. условие НОД $(D, n) = 1$ не допускает к рассмотрению шифрующие матрицы, определитель которых содержит в качестве множителей числа 2, 3, 5, 6, 12, 15, 18, 30.

Число 31 в этом отношении лучше, т.к. в этом случае НОД $(D, n) = 1$ для любого значения определителя шифрующей матрицы. Увеличьте число символов в алфавите до 31 и проведите шифрование в этом алфавите. \square

Задачи.

39.1. Расшифруйте сообщение “рчюс холл роыэироя”, используя формулу (6).

39.2. Проведите расшифровку слова “ЪТ” в обратную сторону для примера 2.

39.3. Дано аффинное преобразование $y \equiv (13x + 25) \pmod{30}$. Зашифруйте слово “Река”:

а) применяя аффинное преобразование к каждому символу,

б) применяя аффинное преобразование к биграммам.

39.4. Проведите расшифровку полученного сообщения “ДВНРЛБ” для примера 39.3.

39.5. Зашифруйте с помощью шифрующей матрицы в примере 3 сообщение “Встречай вторник”.

39.6. Для кодирующей матрицы $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ найдите декодирующую матрицу. Закодируйте фразу “Я умею шифровать” и проведите декодирование полученной “фразы”.

39.7. Для кодирующей матрицы $\begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix}$ найдите декодирующую матрицу. Закодируйте фразу “Сохрани шифр в тайне” и проведите декодирование полученной “фразы”.

§ 40. Код Грея

В современной технике широко используются датчики поворота механизма, назначение которых состоит в определении информации об угле поворота механизма. На валу закрепляется диск с нанесенной кодировкой в двоичной системе счисления. Закрепленные фотоэлементы определяют угол поворота $\frac{2k\pi}{2^n}$, где $n \geq 1, 0 \leq k \leq 2^n - 1$.

Диск разделен на 2^n секторов. Рассмотрим n концентрических окружностей. На пересечении концентрических окружностей и секторов нанесены темные дуги. Кодировка нумерации секторов для $n = 3$ с помощью двоичной позиционной системы счисления представлена на рис. 5. Младший разряд изображается на внешнем кольце, а старший разряд на внутреннем кольце. Темной дуге соответствует 1, а светлой дуге (вернее, отсутствующей дуге) соответствует 0.

Кодировка хорошо считывается фотоэлементами в пределах одного сектора, но при переходе от одного сектора к другому сектору на границе секторов могут возникнуть помехи.

Разработан код Грея, в котором коды каждых двух соседних чисел, расположенных по кругу, отличаются только в одном разряде.

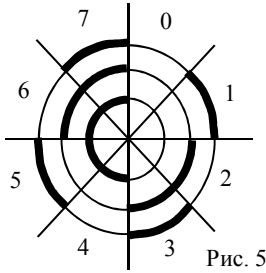


Рис. 5

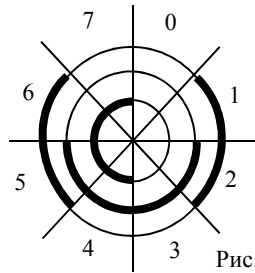


Рис. 6

Пусть $a = a_n a_{n-1} \dots a_2 a_1$ – запись числа в двоичной позиционной системе счисления. Сложив это число по модулю 2 с самим собой, сдвинутым предварительно вправо на 1 разряд, получим новую кодировку старого числа:

$$\oplus \begin{array}{l} a = a_n a_{n-1} \dots a_2 a_1 \\ \underline{a_n \dots a_3 a_2} \end{array}, \text{ где}$$

$$b = b_n b_{n-1} \dots b_2 b_1$$

$$b_i = a_i \oplus a_{i+1}, \quad i \leq n-1; \quad b_n = a_n. \quad (1)$$

Например, для $n = 3$ получаем таблицу 15.

Таблица 15

Десятичная запись числа	0	1	2	3	4	5	6	7
Двоичная позиционная запись	000	001	010	011	100	101	110	111
Код Грея	000	001	011	010	110	111	101	100

6. Кодирование углов поворота с помощью кода Грея представлена на рисунке 6. Коды Грея – это перестановка обычного двоичного позиционного кодирования, но коды Грея уже не являются позиционной системой счисления.

Если информацию, считанную датчиком, нужно перевести в классическую позиционную систему, то, прибавив к обеим частям равенств (1) выражение a_{i+1} , получим:

$$b_i \oplus a_{i+1} = (a_i \oplus a_{i+1}) \oplus a_{i+1} = a_i \oplus (a_{i+1} \oplus a_{i+1}) = a_i$$

$$a_i = b_i \oplus a_{i+1}, \quad a_n = b_n. \quad (2)$$

Или

$$a_n = b_n,$$

$$a_{n-1} = b_{n-1} \oplus a_n = b_n \oplus b_{n-1},$$

$$a_{n-2} = b_{n-2} \oplus a_{n-1} = b_n \oplus b_{n-1} \oplus b_{n-2},$$

.....

$$a_1 = b_n \oplus b_{n-1} \oplus \dots \oplus b_2 \oplus b_1.$$

Пример 1. Перевести число 101101_G , записанное кодом Грея, в двоичный позиционный код и потом сделать проверку, переводя двоичный код в код Грея.

Решение. Рис. 7 показывает, что левая цифра опускается вниз, а для остальных чисел применяется сложение по модулю два в направлении, указанном стрелкой.



Рис. 7

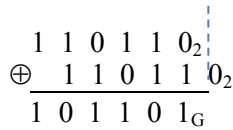


Рис. 8

Рис. 8 показывает, что под данным числом в двоичной системе счисления записывается это же число, но сдвинутое вправо на один разряд, и далее применяется сложение по модулю 2. □

Задачи.

40.1. Зашифруйте кодом Грея числа $a=101010$, $b=010101$, $c=101101$, представленные в двоичной позиционной системе счисления.

40.2. Зашифруйте числа $a=101010$, $b=010101$, $c=101101$, записанные кодом Грея, в позиционную двоичную систему счисления.

40.3. Используя устройство, реализующее сложение по модулю 2, постройте схему, переводящую число из двоичной позиционной системы в код Грея.

40.4. Используя устройство, реализующее сложение по модулю 2, постройте схему, переводящую число из кодировки Грея в двоичную позиционную систему счисления.

§ 41. Коды переменной длины. Код Хаффмана

При кодировании символов в таблице ASCII для каждого разряда отводится восемь разрядов, т.е. 8 битов или 1 байт. В этом случае коды всех символов имеют одинаковую длину.

Для передачи информации больших объемов и для увеличения скорости передачи информации разработаны специальные методы, которые кодировали чаще встречающиеся символы более коротким кодом.

Азбука Морзе является примером рационального кодирования информации. В ней часто встречающиеся буквы закодированы меньшим количеством символов.

<i>A</i> ·—	<i>B</i> —···	<i>V</i> ·—	<i>Г</i> —···	<i>Д</i> —··	<i>E</i> ·	<i>Ж</i> ····—	<i>З</i> —····
<i>И</i> ··	<i>Й</i> ·—···	<i>K</i> ··—	<i>Л</i> ····	<i>M</i> —	<i>H</i> ··	<i>O</i> —···	
<i>П</i> ····	<i>P</i> ···	<i>C</i> ···	<i>T</i> —	<i>У</i> ··—	<i>Ф</i> ····	<i>X</i> ····	<i>Ц</i> ····
<i>Ч</i> ····	<i>Ш</i> ····	<i>Щ</i> ····	<i>Ы</i> ····	<i>Ъ, Ь</i> ····	<i>Э</i> ····	<i>Ю</i> ····	<i>Я</i> ····
1·—····	2····	3····	4····	5····	6····		
7····	8····	9····	0····	[.]····	[,]····		
[/]····	[:]····	[!]····	["]····	[()]····	[-]····		
[/]····	[']····	[шт]····	[кп]····				

шт – начало передачи, *кп* – конец передачи.

Азбука Морзе, используя два символа: точку и тире, в действительности является трехсимвольным алфавитом, т.к. для распознавания символа необходимо понимать, где кончается один символ и где начинается новый символ, т.е. необходим символ “паузы” – пробел.

Шеннон и Фэнно предложили конструкцию кода переменной длины, в котором не нужно было предусматривать специальный символ для паузы. Ими был предложен *префиксный код*, в котором никакая кодовая последовательность одного символа не является началом кодовой последовательности другого символа.

Один из простейших и эффективных способов кодирования информации с помощью кодов переменной длины был предложен Хаффманом (1952 г.).

Суть метода кодирования заключается в следующем. Заданы некоторые элементы с вероятностями. Элементы с наименьшими вероятностями объединяются в пары, пока не получим две большие группы. Коды одной большой группы начинаются с 1, а коды другой большой группы с 0. Каждую группу разбиваем на две подгруппы и т.д., пока в каждой группе не останется по одному символу. На каждом шаге цифры 1 или 0 дописываются к предыдущим кодам.

Пример 1. Рассмотрим метод для алфавита из пяти символов $a(0,35), b(0,23), c(0,17), d(0,13), e(0,12)$.

Объединяя элементы d и e , получим $a(0,35), b(0,23), c(0,17), de(0,25)$.

Объединяя элементы b и c , получим $a(0,35), bc(0,40), de(0,25)$.

Объединяя элементы a и de , получим: $a\ de\ (0,60), bc(0,40)$.

Для кодирования выберем стратегию: группу с большей вероятностью кодировать единицей, а с меньшей вероятностью нулем. Кодлируем две группы: $a\ de - 1, bc - 0$.

Пару ade разбиваем на две группы согласно объединениям и кодлируем $a - 11, de - 10$; разбивая пару bc , получим $b - 01, c - 00$.

Разбивая на следующем шаге, получаем кодировку $a - 11, b - 01, c - 00, d - 101, e - 100$.

На рисунке 9 представлен граф объединения букв алфавита. Из графа легко определяется код каждого символа алфавита.

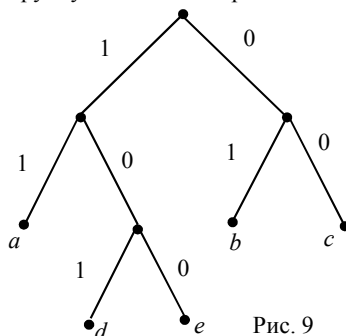


Рис. 9

Если для кодирования выберем другую стратегию: группу с большей вероятностью кодировать нулем, а с меньшей вероятностью единицей, то получим кодировку: $a - 00, b - 10, c - 11, d - 010, e - 011$.

Одна кодировка получается из другой поразрядной инверсией.

Обращаем внимание на то, что ни один код символа не является началом кода другого символа. Следующие наборы однозначно восстанавливают зашифрованное сообщение: $1101100 - sea, 10001000 - baba$. □

Рассмотрим пример алфавита, содержащего 7 букв:

$a (0,40), b (0,24), c (0,15), d (0,09), e (0,06), f (0,04), g (0,02)$.

Объединяя элементы в пары, чтобы сумма вероятностей была наименьшей на каждом этапе, получим:

$a (0,40), b (0,24), c (0,15), d (0,09), e (0,06), fg (0,06),$

$a (0,40), b (0,24), c (0,15), d (0,09), efg (0,12),$

$a (0,40), b (0,24), c (0,15), defg (0,21),$

$a (0,40), b (0,24), cdefg (0,36),$

$a (0,40), bcdefg (0,60)$.

Кодировка алфавита:

$a - 0, b - 10, c - 110, d - 1110, e - 11110, f - 111110, g - 111111. (1)$

Рассмотрим другой пример группировки того же множества. Все элементы на первом шаге разделим на две группы с равными вероятностями $ae f (0,50), bcdg (0,50)$ и закодируем эти группы 0 или 1.

На следующем этапе также по возможности разделим каждую группу на две подгруппы с более близкими вероятностями:

$a (0,40)$ и $ef (0,10); b g (0,26)$ и $cd (0,24)$.

Разделив на третьем этапе, получим кодировку:

$a - 00, b - 100, c - 110, d - 111, e - 010, f - 010, g - 111. (2)$

Первоначальный обзор кодировок (1) и (2) создает впечатление, что кодировка (2) лучше кодировки (1), т.к. для записи алфавита в (2) требуется 20 разрядов, в (1) требуется 27 разрядов. Но это ошибочное мнение, т.к. нужно учитывать частоту появления букв в тексте. □

Рассмотрим текст, содержащий 100 букв. В среднем в нем буква a появится 40 раз, буква b – 24 раза и т.д. Учитывая это, найдем среднюю длину закодированного текста для 100 букв алфавита:

– в случае (1): $40 \cdot 1 + 24 \cdot 2 + 15 \cdot 3 + 9 \cdot 4 + 6 \cdot 5 + 4 \cdot 6 + 2 \cdot 6 = 235$,

– в случае (2): $40 \cdot 2 + 24 \cdot 3 + 15 \cdot 3 + 9 \cdot 3 + 6 \cdot 3 + 4 \cdot 3 + 2 \cdot 3 = 260$.

Полезно эти результаты сравнить с классическим кодированием кодами постоянной длины. Семь символов в двоичной системе можно закодировать кодами длиной 3: 000, 001, 010, 011, 100, 101, 110. Для текста из 100 букв потребуется 300 позиций.

Из трех методов кодировки более рациональным является метод группировки в пары с наименьшей вероятностью.

Задачи.

41.1. Используя коды переменной длины, рассмотрите различные кодировки для алфавита: $a(0,51)$, $b(0,25)$, $c(0,13)$, $d(0,06)$, $e(0,03)$, $f(0,02)$.

41.2. Используя код Хаффмана для алфавита $a(0,49)$, $k(0,23)$, $c(0,13)$, $p(0,12)$, $b(0,03)$, зашифруйте слова: карась, краб, бар, раб, рак.

§ 42. Код Хемминга

Из-за помех, ошибок, шума или преднамеренного искажения с некоторой стороны возможно искажение информации. Рассмотрим код Хемминга, который позволяет исправлять несколько разрядов поступившего искаженного сообщения.

Введем меру отличия передаваемого сообщения от принятого сообщения.

Расстояние Хемминга между двумя числовыми последовательностями $u = (u_1, u_2, \dots, u_n)$ и $v = (v_1, v_2, \dots, v_n)$ равно числу разрядов, в которых последовательности различаются.

Например, $d(10111, 10001)=2$, $d(11110, 00001)=5$.

Набор следующих кодовых слов длиной 4 обозначается E_4 : 0000, 0011, 0101, 1001, 0101, 1010, 1100, 1111.

В каждом слове содержится четное число единиц. Для набора важной характеристикой является минимальное расстояние между различными кодовыми словами, т.е.

$$d = \min_{u \neq v} d(u, v).$$

Расстояние Хемминга d для набора E_4 равно 2.

Искажение любого одного разряда в этом наборе слов превращает их в слова, отличные от данного набора. Например, слово 0100 содержит нечетное число единиц и могло быть получено из слова 0000 искажением второго разряда или из слова 0101 искажением четвертого разряда. Расстояние Хемминга от искаженного слова до набора E_4 равно 1. Код E_4 можно использовать для исправления одной ошибки.

Код Хемминга длиной 7: 0000000, 0010111, 10001011, 1100101, 1110010, 0111001, 1011100, 0101110. Расстояние Хемминга d для этого набора равно 4.

Код исправляет любую одну ошибку и обнаруживает двойную ошибку.

Рассмотрим построение *кода Хемминга*, исправляющего одну ошибку для слов заданной длины.

Если в n -разрядном коде содержится нечетное число единиц, то добавим еще одну единицу, записав ее справа от младшего разряда.

Если в n -разрядном коде содержится четное число единиц, то добавим нуль на указанное место. Таким образом, переработанный код из $n + 1$ разрядов будет всегда содержать четное число единиц.

Если при искажении одного разряда произошла замена $0 \rightarrow 1$ или $1 \rightarrow 0$, то число единиц в принятом коде будет нечетным, что является признаком искажения передаваемого кода.

Схема формирования $n + 1$ разрядного кода и определения четности очень проста (рис. 10) и использует операцию сложения по модулю 2.

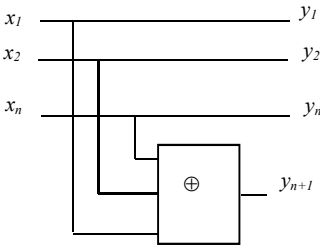


Рис. 10

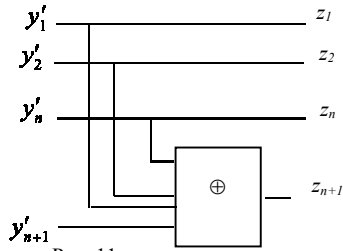


Рис. 11

$$y_i = x_i, \text{ для } i = 1, 2, \dots, n, \quad y_{n+1} = x_1 \oplus x_2 \oplus \dots \oplus x_n.$$

Принимающее устройство (рис. 11) обнаруживает искажение кода.

Если не произошло искажение кода, то получаем

$$z_{n+1} = y'_{n+1} \oplus y'_1 \oplus y'_2 \oplus \dots \oplus y'_n = (x_1 \oplus \dots \oplus x_n) \oplus x_1 \oplus \dots \oplus x_n = 0.$$

Если $z_{n+1} = 0$, то код $z_n z_{n-1} \dots z_1$ является правильным либо в нем произошло четное число искажений. Практика показывает, что наиболее вероятны ошибки в одном разряде.

Если $z_{n+1} = 1$, то в принятом коде содержится ошибка, но устройство не может определить, в каком разряде произошла ошибка.

Для определения номера разряда с ошибкой расширим данный код из n разрядов на m разрядов и будем передавать сообщение $n+m$ – разрядным кодом.

В каждом из этих разрядов может произойти сбой, поэтому нам нужно занумеровать все $n+m$ разрядов, используя дополнительные контрольные m разрядов. Следовательно, нужно наложить условие $2^m \geq m + n + 1$. Единице в неравенстве соответствует случай, когда код не содержит ошибок.

Например, для $n = 10$ выберем $m = 4$, т.е. для передаваемого сообщения $x_{10} x_9 \dots x_1$ рассмотрим четыре дополнительных контрольных числа y_4, y_3, y_2, y_1 и запишем их в разряды с номерами 1, 2, 4, 8, т.е. степени числа 2.

Получим 14-разрядный код

$$\begin{matrix} x_{10} & x_9 & x_8 & x_7 & x_6 & x_5 & y_4 & x_4 & x_3 & x_2 & y_3 & x_1 & y_2 & y_1 \\ 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1. \end{matrix} \quad (1)$$

Рассмотрим последовательности чисел:

V_1 : 1, 3, 5, 7, 9, 11, 13, 15... – все числа, у которых в двоичной системе счисления разряд № 1 равен 1,

V_2 : 2, 3, 6, 7, 10, 11, 14, 15... – все числа, у которых в двоичной системе счисления разряд № 2 равен 1,

V_3 : 4, 5, 6, 7, 12, 13, 14, 15... – все числа, у которых в двоичной системе счисления разряд № 3 равен 1,

V_4 : 8, 9, 10, 11, 12, 13, 14, 15... – все числа, у которых в двоичной системе счисления разряд № 4 равен 1.

Значения контрольных разрядов для кода (1) определим следующим образом

$y_1 = x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_9$, т.е. все разряды последовательности V_1 кроме первого члена,

$y_2 = x_1 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_{10}$, т.е. все разряды последовательности V_2 кроме первого члена,

$$y_3 = x_2 \oplus x_3 \oplus x_4 \oplus x_8 \oplus x_9 \oplus x_{10}, \quad y_4 = x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10}.$$

Пусть код (1) принят. Для определения разряда, содержащего ошибку, найдем значения переменных

$$z_1 = y_1 \oplus x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_9,$$

$$z_2 = y_2 \oplus x_1 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_{10},$$

$$z_3 = y_3 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_8 \oplus x_9 \oplus x_{10},$$

$$z_4 = y_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10}.$$

Если произошла ошибка в одном разряде при передаче информации, то число $z_4 z_3 z_2 z_1$ укажет номер того разряда, где произошла ошибка. Если $z_4 z_3 z_2 z_1 = 0$, то ошибки в принятом коде нет.

Пример. Рассмотрим код до передачи:

$$x = 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1,$$

и нумерацию разрядов: 10 9 8 7 6 5 4 3 2 1.

Значения переменных:

$$x_{10} = 1, \quad x_9 = 0, \quad x_8 = 1, \quad x_7 = 0, \quad x_6 = 1, \quad x_5 = 1, \quad x_4 = 0, \quad x_3 = 1, \quad x_2 = 0, \quad x_1 = 1.$$

Найдем контрольные цифры:

$$y_1 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0, \quad y_2 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 0,$$

$$y_3 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 1, \quad y_4 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 0.$$

Получаем расширенный код для передачи:

$$1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0$$

$$14 \ 13 \ 12 \ 11 \ 10 \ 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1.$$

Допустим, что в одиннадцатом разряде произошел сбой, тогда приемное устройство примет сигнал

$$1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0$$

$$14 \ 13 \ 12 \ 11 \ 10 \ 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1$$

$$x_{10}, \quad x_9, \quad x_8, \quad x_7, \quad x_6, \quad x_5 \quad y_4 \quad x_4, \quad x_3, \quad x_2 \quad y_3 \quad x_1 \quad y_2 \quad y_1.$$

$$\text{Вычислим } z_1 = 1, \quad z_2 = 1, \quad z_3 = 0, \quad z_4 = 1.$$

Адрес поврежденного разряда $z_4 z_3 z_2 z_1 = 1011_2 = 11_{10}$. Инвертируя этот разряд и удаляя контрольные цифры, получаем исправленное сообщение.

Если искажение сигнала произошло в контрольном разряде, то для исправления можно отбросить все контрольные разряды.

Задачи.

42.1. Для каждого из нижеуказанных кодов:

- определите число m контрольных разрядов для кода Хаффмана;
- найдите значения контрольных переменных y_1, y_2, \dots, y_m ;
- составьте расширенный код для передачи;
- считая искажение сигнала при передаче в $n-2$ разряде, составьте принятый код;
- найдите значения переменных z_1, z_2, \dots, z_m и определите номер поврежденного сигнала;
- сравните полученный номер и указанный номер поврежденного символа:

а) (1010); б) (110011001); в) (0101010101010101).

§ 43. Криптограмма с закрытым или открытым ключом

а) Криптосистема с закрытым ключом

Напоминаем, что через $\varphi(n), n \in N$ при $n > 1$ обозначена функция Эйлера, равная количеству натуральных чисел, меньших n и взаимно простых с n .

Пусть абоненты A и B решили установить переписку без передачи ключей. Они договариваются о достаточно большом простом числе p , чтобы $p-1$ хорошо разлагалось на не очень большие простые множители. Например, $p=19$, $\varphi(19)=18$.

Каждый из абонентов случайно выбирает взаимно простое число с $p-1$.

Например, A выбирает число a , B выбирает число b .

$A: a=5, B: b=7$.

Абонент A находит α из уравнения

$$a\alpha \equiv 1 \pmod{\varphi(p)}, \quad 0 < \alpha < p-1, \quad 5\alpha \equiv 1 \pmod{18}, \quad \alpha = 11$$

(a, α) – секретный ключ абонента A . $A: (5, 11)$

Абонент B находит β из уравнения

$$b\beta \equiv 1 \pmod{\varphi(p)}, \quad 0 < \beta < p-1, \quad 7\beta \equiv 1 \pmod{18}, \quad \beta = 13$$

(b, β) – секретный ключ абонента B . $B: (7, 13)$

Пусть A составляет сообщение m , $0 < m < p-1$ абоненту B , шифрует это сообщение своим первым секретным числом ключа $m_1 \equiv m^a \pmod{p}, 0 < m_1 < p$ и посылает сообщение абоненту B :

$$m = 16, \quad m_1 \equiv 16^5 \pmod{19}, \quad m_1 = 4, \quad A \xrightarrow{4} B.$$

Абонент B , получив сообщение, также шифрует его первым числом своего ключа $m_2 \equiv m_1^b \pmod{p}$, $0 < m_2 < p$ и посылает сообщение абоненту A :

$$m_2 \equiv 4^7 \pmod{19}, \quad m_2 = 6, \quad B \xrightarrow{6} A.$$

Абонент A , получив сообщение m_2 , шифрует его снова вторым числом своего ключа $m_3 \equiv m_2^\alpha \pmod{p}$, $0 < m_3 < p$ и посылает его абоненту B :

$$m_3 \equiv 6^{11} \pmod{19}, \quad m_3 = 17, \quad A \xrightarrow{17} B.$$

Абонент B расшифровывает эту шифровку с помощью второго числа своего ключа $m_4 \equiv m_3^\beta \pmod{p}$, $0 < m_4 < p$, $m_4 \equiv 17^{13} \pmod{19}$, $m_4 = 16$.

Оказывается, что полученное сообщение m_4 является отправленным сообщением m . Это следует из свойств сравнений и способов определения чисел a, α, b, β : $m_4 \equiv m_2^{\alpha\beta} \pmod{p} \equiv m_1^{b\alpha\beta} \pmod{p} \equiv m^{ab\alpha\beta} \pmod{p} \equiv m^{a\alpha b\beta \pmod{p-1}} \pmod{p}$.

В 1976 г. Уитфилд Диффи и Мартин Хеллман опубликовали новый принцип криптосистем, который не требует сохранять тайну передачи ключа и метода шифрования. Эти шифры позволяют легко зашифровать и расшифровать текст (при наличии компьютера), и их можно использовать многократно.

б) Обмен ключами

A и B договариваются о двух целых числах p и m , где p – большое простое число, а m заключено между 1 и $(p-1)$. Значения чисел p и m не нужно держать в секрете.

Абонент A произвольно выбирает секретное число a , а абонент B произвольно выбирает число b . Числа a и b выбираются из диапазона от 1 до $(p-1)$, и каждое из них взаимно просто с числом $(p-1)$. Абоненты не сообщают свои секретные числа ни друг другу, ни кому-либо из третьих лиц.

Абонент A вычисляет выражение $k_A \equiv m^a \pmod{p}$ и посылает его абоненту B , который возводит полученное число в степень b и вычисляет $k_{AB} \equiv (k_A)^b \pmod{p}$.

Абонент B вычисляет выражение $k_B \equiv m^b \pmod{p}$ и посылает его абоненту A , который возводит полученное число в степень a и вычисляет $k_{BA} \equiv (k_B)^a \pmod{p}$.

Полученные и дополнительно обработанные числа k_{AB} и k_{BA} обоими абонентами оказываются равными, т.к.

$$k_{AB} = (k_A)^b \pmod{p} = (m^a)^b \pmod{p} = (m^b)^a \pmod{p} = (k_B)^a \pmod{p} = k_{BA}.$$

Число $K \equiv m^{ab} \pmod{p}$ можно использовать в качестве общего ключа, причем ни один из абонентов не знает секретного числа другого.

Пример 1. Пусть $p = 47$, $m = 3$. Секретные числа абонентов A и B равны соответственно $a = 11$ и $b = 17$. Выбранные числа a и b взаимно просты с числом $p-1 = 46$.

Абоненты вычисляют значения и обмениваются полученными значениями:

$$k_A \equiv 3^{11} \pmod{47} \quad \text{и} \quad k_B \equiv 3^{17} \pmod{47}.$$

Вычисления можно провести на калькуляторе или с помощью простейшей компьютерной программы.

Покажем вычисления с помощью модульной арифметики (таблица 16).

Таблица 16

3^m	3	3^2	3^3	3^4	3^5	3^6	3^7	3^8
Вспомогательная операция		$3 \cdot 3$	$9 \cdot 3$	$27 \cdot 3$	$34 \cdot 3$	$8 \cdot 3$	$24 \cdot 3$	$25 \cdot 3$
Остатки при делении на 47	3	9	27	34	8	24	25	1

$$3^{11} \equiv 3^8 \cdot 3^3 \equiv 1 \cdot 27 \equiv 27 \pmod{47}, \quad 3^{17} \equiv 3^8 \cdot 3^8 \cdot 3^1 \equiv 3 \pmod{47}.$$

Абонент A посылает число $k_A = 27$, а абонент B посылает число $k_B = 3$.

Далее каждый из абонентов определяет значение ключа.

Абонент A обрабатывает полученное число

$$k_{BA} = 3^{11} \pmod{47} = 27 \pmod{47}.$$

Абонент B обрабатывает полученное число

$$k_{AB} = 27^{17} \pmod{47} \equiv 3^{17} \cdot 3^{17} \cdot 3^{17} \pmod{47} = 3 \cdot 3 \cdot 3 \pmod{47} = 27 \pmod{47}.$$

Значение общего ключа $K = 27$.

в) Криптосистема с открытым ключом

Пусть A и B решили начать секретную переписку с открытым ключом. Каждый из них, независимо от другого, выбирает два больших простых числа, находит их произведение, функцию Эйлера от этого произведения и выбирает случайное число, меньшее этого вычисленного значения функции Эйлера и взаимно простое с ним:

$$A: p_1, p_2, r_A = p_1 p_2, \varphi(r_A), (a, \varphi(r_A)) = 1, 0 < a < \varphi(r_A),$$

$$A: p_1 = 11, p_2 = 19, r_A = 209, \varphi(r_A) = \varphi(11)\varphi(19) = 180, a = 7.$$

$$B: q_1, q_2, r_B = q_1 q_2, \varphi(r_B), (b, \varphi(r_B)) = 1, 0 < b < \varphi(r_B),$$

$$B: q_1 = 7, q_2 = 17, r_B = 119, \varphi(r_B) = \varphi(7)\varphi(17) = 96, b = 5.$$

Печатается электронная книга, доступная всем желающим.

Абонент A печатает результат произведения двух простых чисел, но сами числа p_1, p_2 сохраняет в тайне и печатает открытый ключ a . A: 209, 7

Абонент B печатает результат произведения двух простых чисел, но сами числа q_1, q_2 сохраняет в тайне и печатает открытый ключ b . B: 119, 5

A находит свой секретный ключ из условия

$$a\alpha \equiv 1 \pmod{\varphi(r_A)}, 0 < \alpha < \varphi(r_A) \quad 7\alpha \equiv 1 \pmod{180}, \alpha = 103.$$

B находит свой секретный ключ из условия

$$b\beta \equiv 1 \pmod{\varphi(r_B)}, 0 < \beta < \varphi(r_B) \quad 5\beta \equiv 1 \pmod{96}, \beta = 77.$$

A хочет послать сообщение m , где $0 < m < r_B$, т.е. шифрует сообщение

$$m_1 \equiv m^b \pmod{r_B}, 0 < m_1 < r_B,$$

$$m = 8, m_1 \equiv 8^5 \pmod{119}, m_1 = 43.$$

B расшифровывает сообщение своим секретным ключом

$$m_2 \equiv m_1^\beta \pmod{r_B}, 0 < m_2 < r_B, m_2 \equiv 43^{77} \pmod{153}, m_2 = 8.$$

Доказательство следует из следующих преобразований:

$$m_2 \equiv m_1^\beta \pmod{r_B} \equiv (m^b)^\beta \pmod{r_B} \equiv m^{b\beta} \pmod{r_B},$$

$$b\beta \equiv 1 \pmod{\phi(r_B)}, m_2 \equiv m \pmod{r_B}, 0 < m < r_B, 0 < m_2 < r_B, m = m_2.$$

Вначале кажется, что секретный ключ можно легко найти, а значит, дешифровать сообщение. В настоящее время известны эффективные алгоритмы разложения числа на множители для достаточно больших чисел. Однако для разложения на множители чисел, содержащих 200 и более цифр, нет достаточно эффективных алгоритмов. Поэтому секрет в этом случае составляет умение разложить число, объявленное для открытого ключа, на простые множители.

Задачи для работы в парах.

43.1. Для каждого из следующих простых чисел p :

- студент A выбирает число a , студент B выбирает число b , взаимно простые с числом $p - 1$;
 - определите свои секретные ключи;
 - пусть абонент A выбирает сообщение $m = 15$;
 - обменяйтесь сообщениями $A \xrightarrow{m_1} B, B \xrightarrow{m_2} A, A \xrightarrow{m_3} B$;
 - пусть абонент B расшифрует полученное сообщение;
 - сравните расшифровку m_4 с первоначальным сообщением m :
- а) $p = 7$, б) $p = 11$, в) $p = 23$.

43.2. Что произойдет в рассмотренной схеме шифрования и расшифрования, если выбранное число b абонентом B окажется совпавшим с числом a абонента A ?

43.3. Абоненты A и B выбрали простое число p для переписки. Абонент C перехватил одно сообщение m_1 , догадался о числе p (оно оказалось днем рождения одного из абонентов или последним числом в феврале) и способе шифрования с помощью закрытых ключей. Может ли абонент C дешифровать сообщение m ?

§ 44. Группа, кольцо и поле

Рассмотрим бинарную операцию \circ на множестве M , которая любым двум элементам a, b из M сопоставляет единственный элемент $a \circ b$ из M .

Множество M с бинарной операцией называется *полугруппой*, если для любых элементов выполняется ассоциативное свойство: $a \circ (b \circ c) = (a \circ b) \circ c$.

Примеры.

1. Множество R с операцией $+$ является полугруппой.

2. Множество R с операцией \times является полугруппой.

Множество M с бинарной операцией называется *моноидом*, если для любых элементов выполняется:

1) ассоциативное свойство: $a \circ (b \circ c) = (a \circ b) \circ c$;

2) существует элемент e , принадлежащий M , такой, что для любого элемента a множества M выполняется равенство

$$a \circ e = e \circ a = a \text{ – существование единицы.}$$

Моноид – это полугруппа с единицей.

Теорема 1. В группе единичный элемент единственный.

Множество M с бинарной операцией называется *группой*, если для любых элементов выполняется:

1) ассоциативное свойство $a \circ (b \circ c) = (a \circ b) \circ c$;

2) существует элемент $e \in M$, такой, что для любого элемента a множества M выполняется равенство $a \circ e = e \circ a = a$;

3) для любого элемента $a \in M$ существует такой элемент $a^{-1} \in M$, что выполняется равенство $a \circ a^{-1} = a^{-1} \circ a = e$.

Группа – это моноид, в котором для любого элемента существует обратный элемент.

Теорема 2. Для каждого элемента группы обратный элемент является единственным.

Теорема 3. В группе выполняются следующие соотношения:

1) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$; 3) $a \circ b = a \circ c \Rightarrow b = c$;

2) $(a^{-1})^{-1} = a$; 4) $b \circ a = c \circ a \Rightarrow b = c$.

Подмножество H в группе G называется *подгруппой*, если:

1) единичный элемент принадлежит H ;

2) для любых элементов $h_1, h_2 \in H \rightarrow h_1 \circ h_2 \in H$, т.е. H замкнуто относительно данной операции;

3) для любого элемента $h \in H \rightarrow h^{-1} \in H$.

Подгруппа называется *собственной*, если $H \neq \{e\}, H \neq G$.

Группа, состоящая из степеней одного из своих элементов, называется *циклической*, а элемент, из степеней которых состоит группа, называется образующим элементом.

Пусть X – множество из n элементов. Группа всех биекций множества X на себя называется *симметрической группой порядка n* и обозначается S_n .

Обозначим элементы $1, 2, \dots, n$. Каждая биекция $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ называется

подстановкой.

Пример.

$$S_3: a_1 = \begin{pmatrix} 123 \\ 123 \end{pmatrix}, a_2 = \begin{pmatrix} 123 \\ 231 \end{pmatrix}, a_3 = \begin{pmatrix} 123 \\ 312 \end{pmatrix}, a_4 = \begin{pmatrix} 123 \\ 132 \end{pmatrix}, a_5 = \begin{pmatrix} 123 \\ 213 \end{pmatrix}, a_6 = \begin{pmatrix} 123 \\ 321 \end{pmatrix}.$$

Теорема Кэли. Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической матрицы S_n .

Симметрией фигуры на плоскости (в пространстве) называется движение плоскости (пространства), которое переводит фигуру в себя.

Например, для бесконечной полосы (рис. 12) симметриями фигуры являются: симметрия относительно оси полосы, т.е. прямой b , симметрии относительно

произвольной прямой c , перпендикулярной границе полосы, параллельные переносы на произвольный вектор \vec{a} , параллельный границе полосы.

Теорема 1. Совокупность всех симметрий фигуры образует группу относительно композиции отображений.

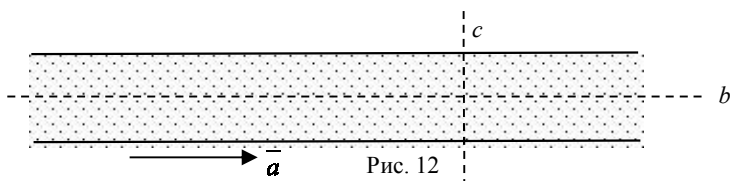


Рис. 12

Число элементов группы G , состоящей из конечного числа элементов, называется порядком группы и обозначается через $|G|$.

Деревья являются частными случаями графов, поэтому для деревьев распространяется понятия изоморфизма и автоморфизма.

Напомним, что два графа изоморфны, если между их вершинами можно установить биективное отображение, сохраняющее отношение смежности, и изоморфизм графа на себя называется автоморфизмом.

Совокупность всех автоморфизмов дерева образует группу относительно композиции автоморфизмов.

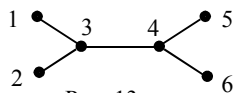


Рис. 13

Группа автоморфизмов графа на рис. 13 состоит из шести элементов:

$$f_1: 1 \rightarrow 1, 2 \rightarrow 2, 3 \rightarrow 3, 4 \rightarrow 4, 5 \rightarrow 5, 6 \rightarrow 6;$$

$$f_2: 1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3, 4 \rightarrow 4, 5 \rightarrow 5, 6 \rightarrow 6;$$

$$f_3: 1 \rightarrow 1, 2 \rightarrow 2, 3 \rightarrow 3, 4 \rightarrow 4, 5 \rightarrow 6, 6 \rightarrow 5;$$

$$f_4: 1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3, 4 \rightarrow 4, 5 \rightarrow 6, 6 \rightarrow 5;$$

$$f_5: 1 \rightarrow 5, 2 \rightarrow 6, 3 \rightarrow 4, 4 \rightarrow 3, 5 \rightarrow 1, 6 \rightarrow 2;$$

$$f_6: 1 \rightarrow 6, 2 \rightarrow 5, 3 \rightarrow 4, 4 \rightarrow 3, 5 \rightarrow 2, 6 \rightarrow 1.$$

Отображение f_1 является тождественным отображением. Общее число автоморфизмов можно быстро определить геометрическим образом. Для вершин 1 и 2 и сохранения остальных вершин на местах существует два автоморфизма – тождественное и симметрия относительно моста графа, соединяющего вершины 3 и 4. Для элементов 5 и 6 и сохранения остальных элементов на местах также существует два автоморфизма. Вершины 3 и 4 имеют одинаковые степени, поэтому рассмотрим автоморфизмы, переставляющие эти вершины, причем вершины 1 и 2 должны отобразиться в вершины 5 и 6. Существует два таких автоморфизма.

Дерево называется *асимметричным*, если его группа автоморфизмов состоит из единственного элемента, т.е. является тождественным отображением дерева на себя. На рис. 14 построены все неизоморфные асимметричные деревья с восьмью вершинами.

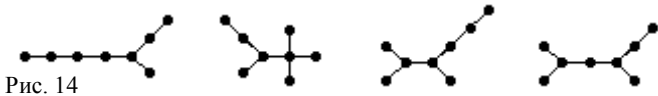


Рис. 14

Существуют графы, не являющиеся асимметричными, т.е. для графа существует автоморфизм, отличный от тождественного отображения. Они могут быть заданы рисунками, не имеющими симметрий с точки зрения геометрии (рис. 15), но их можно изобразить изоморфными графами с элементами геометрических симметрий.

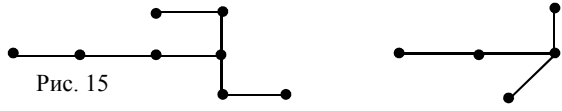


Рис. 15

Пусть на множестве M определены две бинарные операции $+$, \times , которые назовем “сложением” и “умножением”.

Множество M с двумя бинарными операциями $+$, \times называется *кольцом*, если выполняются свойства:

- 1) $(a + b) + c = a + (b + c)$ – ассоциативность сложения;
- 2) существует элемент $0 \in M$, такой, что для любого элемента $a \in M$ выполняется равенство $a + 0 = 0 + a = a$ – существование нуля;
- 3) для всякого $a \in M$ существует элемент $-a \in M$, такой, что $a + (-a) = 0$ – существование обратного элемента;
- 4) $a + b = b + a$ – коммутативность сложения;
- 5) $(a \times b) \times c = a \times (b \times c)$ – ассоциативность умножения;
- 6) $a \times (b + c) = (a \times b) + (a \times c)$ – дистрибутивность слева и $(b + c) \times a = (b \times a) + (c \times a)$ справа относительно сложения.

В некоторых пособиях ассоциативность умножения исключается в определении кольца, тогда рассматривается неассоциативное кольцо.

Кольцо является коммутативной группой относительно сложения.

Кольцо называется *коммутативным*, если $a \times b = b \times a$.

Коммутативное кольцо называется *кольцом с единицей*, если существует $1 \in M, a \times 1 = 1 \times a = a$.

Примеры.

1. Множество действительных чисел, множество рациональных чисел и множество целых чисел с операциями сложения и умножения чисел являются примерами колец с единицей.

2. Множество четных чисел с операциями сложения и умножения чисел является кольцом, в котором нет единицы.

3. Множество векторов трехмерного пространства с операциями сложения векторов и векторного умножения векторов не является кольцом, т.к. не выполняется ассоциативность для векторного умножения.

Теорема 1. В кольце выполняются свойства:

- 1) $0 \times a = a \times 0 = 0$;
- 2) $a \times (-b) = (-a) \times b = -(a \times b)$;

$$3) (-a) \times (-b) = a \times b.$$

Множество M с двумя бинарными операциями $+$, \times называется *полем*, если выполняются свойства:

$$1) (a+b)+c = a+(b+c) \text{ – ассоциативность сложения;}$$

2) существует элемент $0 \in M$, такой, что для любого элемента $a \in M$ выполняется равенство $a+0=0+a=a$ – существование нуля;

3) для всякого $a \in M$ существует элемент $-a \in M$, такой, что $a+(-a)=0$ – существование обратного элемента;

$$4) a+b = b+a \text{ – коммутативность сложения;}$$

$$5) (a \times b) \times c = a \times (b \times c) \text{ – ассоциативность умножения;}$$

6) существует элемент $e \in M$ такой, что для любого элемента $a \in M$ выполняется равенство: $a \circ e = e \circ a = a$ существование единицы;

7) для любого ненулевого элемента $a \in M$ существует такой элемент $a^{-1} \in M$, что выполняется равенство $a \times a^{-1} = a^{-1} \times a = 1$ – существование обратного элемента по умножению;

$$8) a \times b = b \times a \text{ – коммутативность умножения;}$$

$$9) a \times (b+c) = (a \times b) + (a \times c) \text{ – дистрибутивность относительно сложения.}$$

Поле – это коммутативное кольцо с 1, в котором любой ненулевой элемент имеет обратный относительно умножения. Таким образом, все элементы поля относительно сложения образуют коммутативную группу, и все ненулевые элементы относительно умножения также образуют коммутативную группу.

Примеры.

1. Множество действительных чисел и множество рациональных чисел с операциями сложения и умножения чисел являются примерами полей, но множество целых чисел не является полем относительно этих операций.

2. Если натуральное число m является простым числом, то Z_m является полем, а если m – составное число, то не является полем (см. ниже задачу 44.6).

Теорема 2. В поле выполняются свойства:

$$1) (-a) = a \times (-1), \quad 3) a \neq 0, (a^{-1})^{-1} = a,$$

$$2) -(a+b) = (-a) + (-b), \quad 4) a \times b = 0 \rightarrow a = 0 \vee b = 0.$$

Задачи.

44.1. Докажите, что множество матриц типа $m \times n$ с операцией сложения является моноидом. Определите единицу в этом моноиде.

44.2. Докажите, что множество квадратных матриц второго порядка является моноидом относительно операции умножения матриц. Определите единицу в этом моноиде.

44.3. Докажите, что множество (nZ, \cdot) целых чисел, делящихся на n , ($n > 1$) с операцией умножения является коммутативной полугруппой без единицы.

44.4. Пусть $A = \{a_1, a_2, \dots, a_n\}$ – множество символов, т.е. алфавит. Конечную последовательность символов назовем словом в алфавите A .

На множестве Π слов в алфавите A введем бинарную операцию – “склеивание”, т. е. двум словам $a = a_{i_1} \dots a_{i_k}, b = a_{j_1} \dots a_{j_n}$ поставим в соответствие слово $ab = a_{i_1} \dots a_{i_k} a_{j_1} \dots a_{j_n}$. Докажите, что Π является полугруппой, которая называется свободной полугруппой, порожденной множеством A .

44.5. Докажите, что совокупность многочленов, степень которых меньше либо равна данному числу $n, n \in \mathbb{N}$, является группой относительно сложения многочленов.

44.6. Докажите, что классы вычетов $\overline{0}, \overline{1}, \dots, \overline{n-1}$ в множестве Z_n относительно сложения и умножения классов образуют коммутативное кольцо с единицей. Это кольцо является полем тогда и только тогда, когда n – простое число.

44.7. Докажите, что совокупность всех движений плоскости, переводящих правильный треугольник в себя, образует группу. Перечислите все элементы группы.

44.8. Постройте группу симметрий следующих фигур (рис. 16).

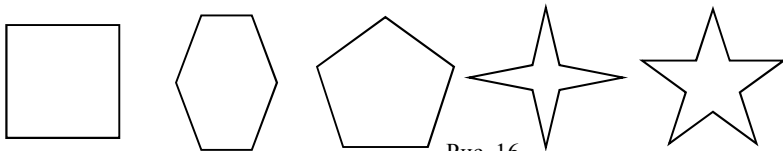


Рис. 16

44.9. Постройте все неизоморфные асимметричные деревья с семью вершинами.

44.10. Постройте асимметричное дерево, содержащее наименьшее число вершин.

44.11. Пусть S_{Ox}, S_{Oy} – симметрии относительно осей Ox и Oy соответственно. Постройте несколько графов с различным числом вершин, автоморфизмы которых содержат следующие отображения: S_{Ox}, S_{Oy} и тождественное отображение. Могут ли эти графы содержать другие элементы в группе автоморфизмов?

44.12. Пусть \vec{a} – данный вектор. Постройте бесконечный граф, группа автоморфизмов которого содержит параллельные переносы $T_{k\vec{a}}$, где $k \in \mathbb{Z}$.

44.13. Пусть n – натуральное число. Постройте несколько графов, группа автоморфизмов которых содержит повороты $R_O^{k\varphi}$, где $\varphi = \frac{2\pi}{n}, k = 0, 1, \dots, n-1$.

44.14. СИ. Изучите конечные поля в пособии [17] и их применение для кодирования информации.

Глава 5. Потоки в сетях. Алгоритмы

§ 45. Сети

Граф называется *нагруженным*, если каждому ребру x поставлено в соответствие некоторое действительное число $l(x)$, называемое весом ребра. В большинстве случаев это число является положительным. Для пути P нагруженного графа обозначим через $l(P)$ сумму весов, входящих в путь ребер, при этом каждое ребро считается столько раз, сколько оно входит в путь. Эта характеристика называется весом пути. Путь из вершины u в вершину v называется минимальным, если он имеет наименьший вес среди всех путей, соединяющих эти вершины. Граф (орграф) с заданными весами ребер называется сетью или нагруженным графом (орграфом).

Квадратная матрица $C(G)$ с элементами $c_{ij} = \begin{cases} l(v_i, v_j), & \text{если } (v_i, v_j) \in E \\ 0, & \text{если } i = j \\ \infty, & \text{если } (v_i, v_j) \notin E \end{cases}$ называется

с матрицей весов дуг нагруженного графа.

1. Задача о коммивояжере

Задача о коммивояжере (странствующем торговце, представителе торговой фирмы и предлагавшем покупателям товары по образцам, прейскурантам, каталогам) имеет два варианта формулировок.

Первый вариант. Требуется посетить n определенных городов, побывав хотя бы один раз в каждом городе, проделав путь наименьшей длины. Этот вариант разрешает маршруту пройти несколько раз через один и тот же город. Если длина пути между двумя городами значительно превосходит обходные пути, а такой случай возможен, например, в горах, то такая трактовка имеет смысл. Иногда схема дорог также обязывает коммивояжера пройти через некоторые города несколько раз (рис. 1).

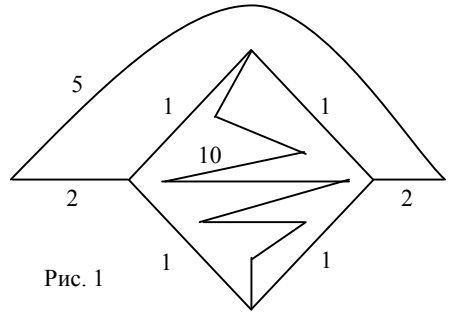


Рис. 1

Второй вариант: Требуется посетить n определенных городов, побывав только один раз в каждом городе и проделав путь наименьшей длины. Рассмотрим задачу о коммивояжере в последней формулировке. Предполагается, что коммивояжер должен вернуться в первоначальный город. Задача сводится к поиску гамильтонова цикла наименьшей длины.

Граф на рис. 2 имеет следующую матрицу:

$$\begin{pmatrix} 0 & 10 & \infty & \infty \\ 10 & 0 & 20 & \infty \\ \infty & 20 & 0 & 12 \\ \infty & \infty & 12 & 0 \end{pmatrix}$$

Рассмотрим задачу о коммивояжере для графа на рис. 3.

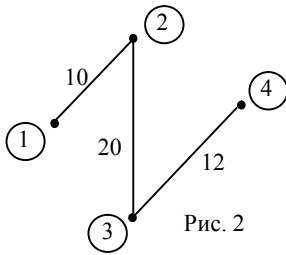


Рис. 2

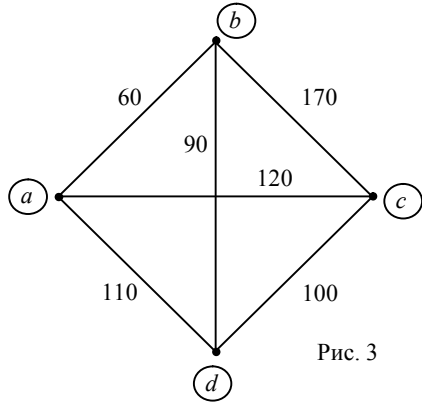


Рис. 3

Перечислим все простые цепи:

$a-b-d-c-a$, $a-b-c-d-a$,

$a-c-b-d-a$, $a-c-d-b-a$,

$a-d-c-b-a$, $a-d-b-c-a$.

Три из них являются различными $a-b-d-c-a$, $a-b-c-d-a$, $a-c-b-d-a$, т.к. остальные цепи являются путями, пройденными в обратном направлении.

Вычисляем длину каждого пути:

Цикл $a-b-d-c-a$: $l_1=60+90+100+120=470$,

цикл $a-b-c-d-a$: $l_2=60+170+100+110=430$,

цикл $a-c-b-d-a$: $l_3=120+170+90+110=490$.

Выбираем кратчайший путь $a-b-c-d-a$.

Общего способа решения задачи о коммивояжере для произвольного графа не известно, хотя для некоторых частных случаев известны признаки существования минимального пути. Для графа с небольшим количеством вершин задачу можно решить методом перебора всех путей.

Маршруты коммивояжера нагляднее изображаются на пирамиде (рис. 4).

Изобразим начальную точку вершиной пирамиды, а в плоскости основания все остальные точки. Выбрав маршрут из верхней точки, выполняем перебор маршрутов на плоскости и завершаем маршрут в вершине a .

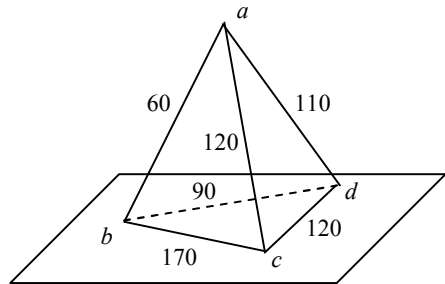


Рис. 4

2. Остов дерева минимального веса

Пусть задан нагруженный граф. Например, на рис. 5 вершины графа занумерованы и каждому ребру поставлено в соответствие число по формуле $l(i, j) = \min(i, j)$.

Остов дерева минимального веса находится по следующему алгоритму.

Шаг 1. Выберем в графе G ребро минимальной веса. Добавляя инцидентные ему вершины, получим подграф G_2 (нумерация подграфов по числу вершин). Положим $i = 2$.

Шаг 2. Если $i = n(G)$, то задача решена и G_i – искомый остов минимального веса.

Шаг 3. Строим граф G_{i+1} , добавляя к графу G_i ребро минимальной длины из всех ребер графа G , не принадлежащих G_i . Одна вершина этого ребра должна принадлежать графу G_i , а другая не принадлежать G_i . Добавим к ребру инцидентную ему вершину и не принадлежащую G_i . Полагаем $i = i + 1$ и переходим к шагу 2.

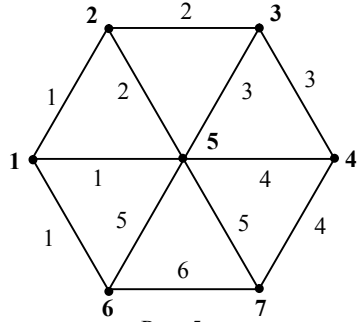


Рис. 5

Для графа на рис. 1 получаем последовательность графов по рассмотренному алгоритму (рис. 6).

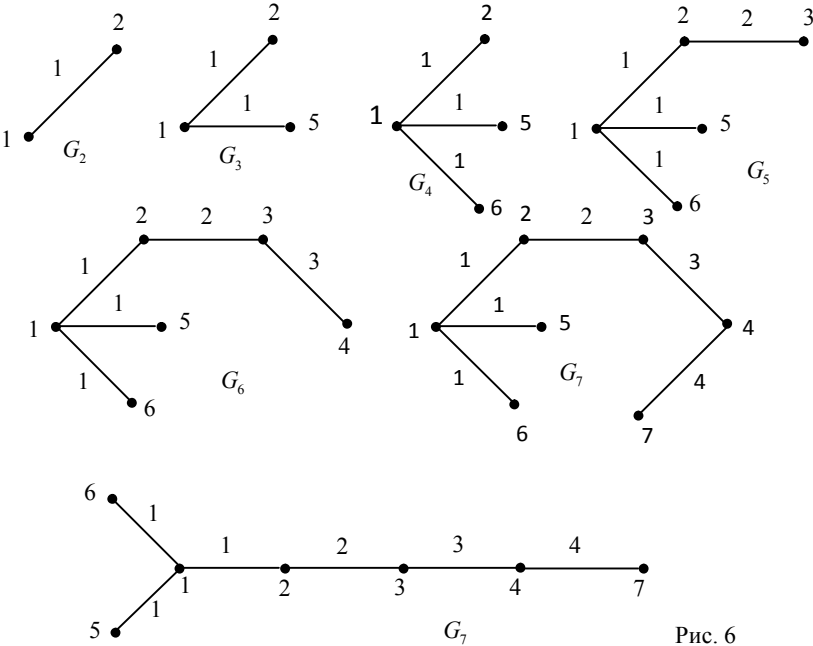


Рис. 6

Цикломатическое число данного графа равно $\gamma(G) = m - n + 1 = 12 - 7 + 1 = 6$. и показывает количество удаленных ребер из исходного графа, чтобы получить остов графа.

Задачи.

45.1. Найдите кратчайший маршрут для коммивояжёра (рис. 7, 8).

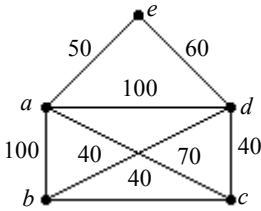


Рис. 7

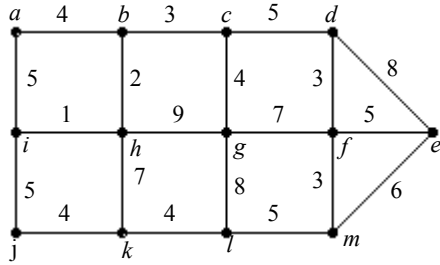


Рис. 8

Имеет ли смысл уточнять, из какого города начинается маршрут коммивояжёра?

45.2. Найдите остов дерева минимального веса для следующих графов (рис. 9, 10).

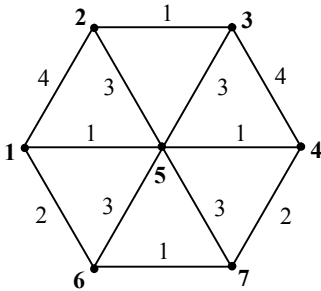


Рис. 9

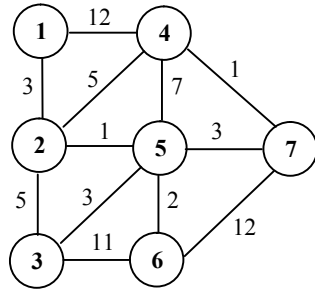


Рис. 10

§ 46. Алгоритмы обхода вершин графа

Решение задач на сетях предполагает поиск вершин графа, удовлетворяющих определенным условиям, причем, в большинстве случаев, образующих некоторую цепь или простую цепь.

Рассмотрим два метода, использующих следующие идеи:

- 1) Стек (магазин, выход из тупика) – “первым пришел, последним вышел” (рис. 11).
- 2) Очередь – “первым пришел, первым вышел” (рис. 12).

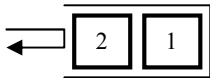


Рис. 11

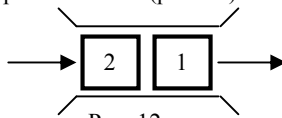


Рис. 12

1. Алгоритм поиска в глубину в графе

Стратегия данного метода – идти “вглубь” графа пока это возможно, (т.е. непросмотренные вершины), возвращаться и искать другой путь, когда нет непросмотренных вершин. Поиск продолжается, пока не просмотрены все вершины графа, достижимые из данной вершины.

Шаг 1. Начало работы. Все вершины считаются непросмотренными. Выбираем произвольную вершину v_0 , записываем ее в стек и отмечаем как просмотренную.

Шаг 2. Вершину, находящуюся на вершине стека, обозначим через v . Ищем непросмотренную вершину u , смежную с вершиной v . Если такой вершины нет, то переходим на следующий шаг. В противном случае отмечаем найденную вершину u как просмотренную и записываем ее в стек (слева от ранее расположенной в стеке). Повторяем текущий шаг.

Шаг 3. Удаляем текущую вершину из стека. Если стек пуст, то все вершины графа просмотрены. Алгоритм заканчивает работу. Иначе переходим на предыдущий шаг.

Пример 1. Рассмотрим применение алгоритма для графа на рис. 13. Стек заполняется с правой стороны влево. Заполнение стека показано в таблице 1.

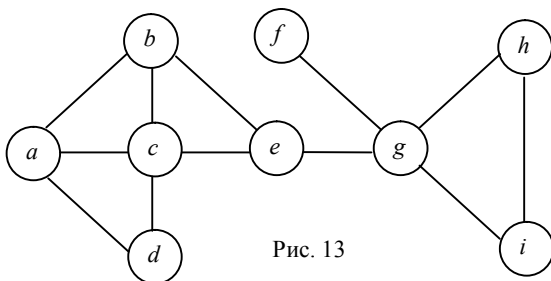


Рис. 13

Таблица 1

Текущая вершина	Действие	Состояние стека
a	Добавляем вершину a в стек	a
b	Добавляем вершину b в стек	ba
e	Добавляем вершину e в стек	eba
g	Добавляем вершину g в стек	$gcba$
f	Добавляем вершину f в стек	$fgcba$
f	Удаляем вершину f из стека	gcb
g	Добавляем вершину h в стек	$hgcb$
h	Добавляем вершину i в стек	$ihgcb$
i	Удаляем вершину i из стека	$hgcb$
h	Удаляем вершину h из стека	gcb
g	Удаляем вершину g из стека	eba
e	Удаляем вершину e из стека	ba
b	Добавляем вершину c в стек	cba
c	Добавляем вершину d в стек	$dcba$
d	Удаляем вершину d из стека	cba
c	Удаляем вершину c из стека	ba
b	Удаляем вершину b из стека	a
a	Удаляем вершину a из стека	Стек пуст

Порядок просмотра вершин графа: $a \rightarrow b \rightarrow e \rightarrow g \rightarrow f \rightarrow h \rightarrow i \rightarrow c \rightarrow d$.

Если удаленную вершину записывать перечеркнутым символом, то процесс заполнения стека можно компактно записывать одной строкой:

$\alpha \ \cancel{b} \ \cancel{c} \ \cancel{d} \ c \ \cancel{e} \ \cancel{g} \ \cancel{h} \ \cancel{i} \ h \ \cancel{f} \ g \ e \ b \ a$.

Такая запись позволяет однозначно восстановить процесс обхода вершин на данном графе. Кстати, такая запись позволяет частично восстановить сам граф с точностью до “переплетения кос”. На восстановленном графе могут исчезнуть ребра между вершинами, которые не оказались смежными в маршруте. □

2. Алгоритм поиска в ширину на графе

Стратегия метода – просматривать все вершины, достижимые из начальной вершины, т.е. все смежные вершины, затем смежные смежных вершин.

Шаг 1. Начало работы. Все вершины считаются непросмотренными. Выбираем произвольную вершину v_0 , записываем ее в очередь и отмечаем как просмотренную.

Шаг 2. Вершину, находящуюся на выходе из очереди (т.е. справа), обозначим через v . Ищем непросмотренную вершину u , смежную с вершиной v . Если такой вершины нет, то переходим на следующий шаг. В противном случае отмечаем найденную вершину u как просмотренную и записываем ее в очередь (слева от ранее расположенной в очереди). Повторяем текущий шаг.

Таблица 2

Вершина в начале очереди	Действие	Состояние очереди
	Добавляем вершину a в очередь	a
a	Добавляем вершину b в очередь	ba
a	Добавляем вершину c в очередь	cba
a	Добавляем вершину d в очередь	$dcba$
a	Удаляем вершину a из очереди	dcb
b	Добавляем вершину e в очередь	$edcb$
b	Удаляем вершину b из очереди	edc
c	Удаляем вершину c из очереди	ed
d	Удаляем вершину d из очереди	e
e	Добавляем вершину g в очередь	ge
e	Удаляем вершину e из очереди	g
g	Добавляем вершину f в очередь	fg
g	Добавляем вершину h в очередь	hfg
g	Добавляем вершину i в очередь	$ihfg$
g	Удаляем вершину g из очереди	ihf
f	Удаляем вершину f из очереди	ih
h	Удаляем вершину h из очереди	i
i	Удаляем вершину i из очереди	Очередь пуста

Шаг 3. Удаляем текущую вершину из очереди. Если очередь пуста, то все вершины графа просмотрены. Алгоритм заканчивает работу. Иначе переходим на предыдущий шаг.

§ 47. Выбор кратчайшего пути методом присвоения меток

Дан граф на рис. 19, вершины которого изображают населенные пункты, а веса ребер – расстояния между населенными пунктами. Требуется найти кратчайший маршрут от вершины 1 до вершины 5.

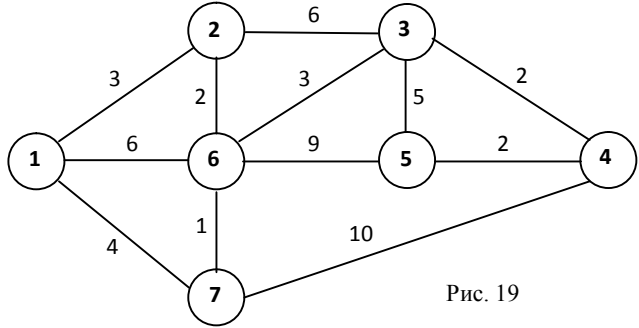


Рис. 19

Каждой вершине припишем метку, состоящую из пары чисел. Первое число – это минимальное расстояние от этой вершины до начальной вершины 1. Второе число – это номер предыдущей вершины маршрута к данной вершине.

Из начальной вершины 1 выходит три ребра. Выходя из вершины 1, закрашиваем ее и записываем метки к вершинам 2, 6 и 7 (рис. 20).

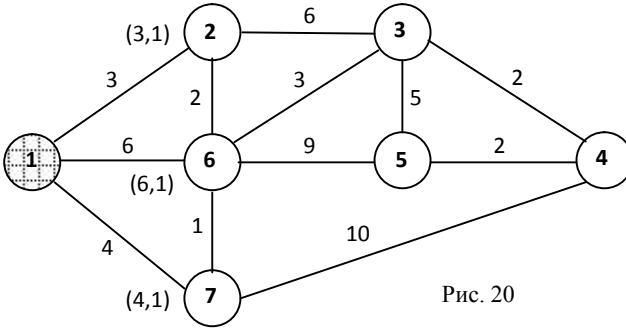


Рис. 20

Среди меток (3, 1), (6, 1) и (4, 1) для незакрашенных вершин находим метку с наименьшим первым числом, т.е. метку (3, 1). Фактически определяем маршрут наименьшей длины. Вершина 2 становится стартовой для дальнейшего присвоения меток.

Из вершины 2 выходит два ребра в незакрашенные вершины 3 и 6. Закрашиваем вершину 2 (рис. 21) и записываем метки для вершин 3 и 6.

Вершина 3 получает метку (9, 2). Первое число метки получено суммированием первого числа метки (3, 1) с длиной ребра $\{2; 3\}$, т.е. $9=3+6$. Второе число метки указывает номер предыдущей вершины.

Для вершины 6 получаем метку (5, 2). Сравниваем ее с полученной ранее меткой (6, 1). Выбираем из двух претендентов метку с наименьшим первым числом. Удаляем

предыдущую метку или зачеркиваем ее и записываем метку с наименьшим маршрутом до начальной вершины.

Замечание. Иногда метка возле вершины уточняется несколько раз и становится постоянной после закрашивания этой вершины.

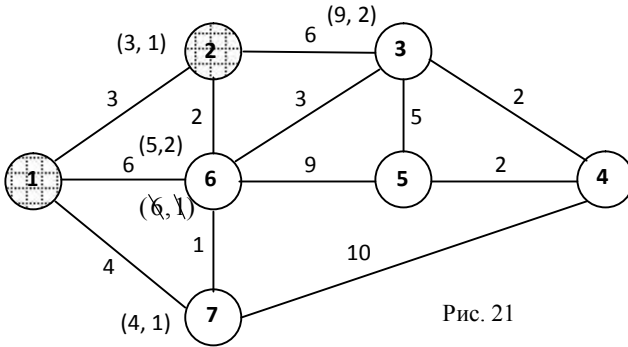


Рис. 21

Среди меток (9, 2), (5, 2) и (4, 1) для незакрашенных вершин находим метку с наименьшим первым числом, т.е. метку (4, 1). Вершина 7 становится стартовой для дальнейшего присвоения меток.

Закрашиваем вершину 7 (рис. 22) и записываем метки для вершин 6 и 4.

Вершина 6 получает метку (5, 7). Первое число метки получено суммированием первого числа метки (4, 1) с длиной ребра {7; 6}, т.е. $5 = 4 + 1$. Но вершина 6 имеет метку (5, 2). Первые числа в этих метках равны. Записываем возле вершины 6 и эту метку. Две метки с одинаковыми первыми числами возле одной вершины означают, что существует два маршрута одинаковой длины из начальной вершины в эту вершину. Один маршрут – 1, 2, 6, а другой маршрут – 1, 7, 6.

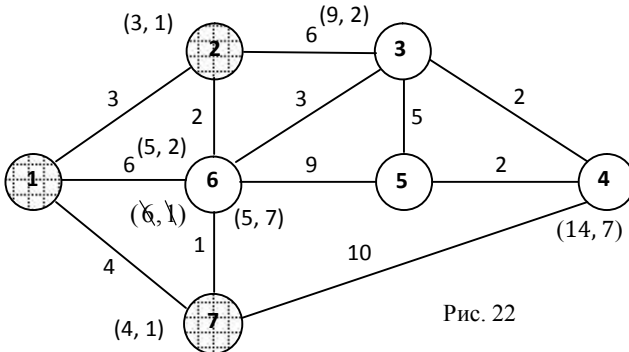


Рис. 22

Среди незакрашенных вершин 3, 4 и 6 с метками выбираем вершину 6, которая имеет метки с наименьшими первыми числами.

Закрашиваем вершину 6 (рис. 23) и расставляем метки в вершины 3 и 5.
 Для вершины 3 получаем метку (8, 6). Сравниваем ее с меткой (9, 2) при этой вершине. Заменяем прежнюю метку новой меткой (8, 6), т.к. $8 < 9$.
 Для вершины 5 получаем метку (14, 6).

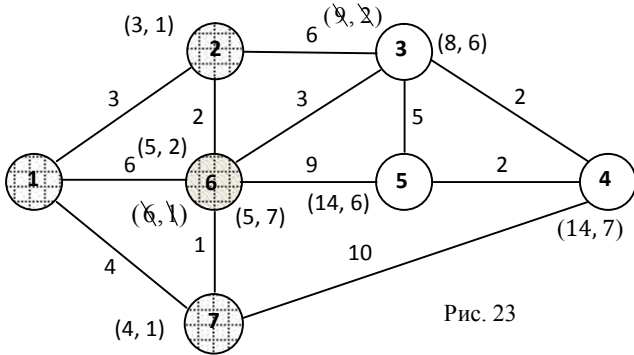


Рис. 23

Среди незакрашенных вершин 3, 4 и 5 с метками выбираем вершину 3.
 Закрашиваем вершину 3 (рис. 24) и записываем метки к вершинам 4 и 5.
 Для вершины 5 получаем метку (13, 3). Сравнивая ее с прежней меткой (14, 6), заменяем прежнюю метку на метку (13, 3).
 Для вершины 4 получаем метку (10, 3).

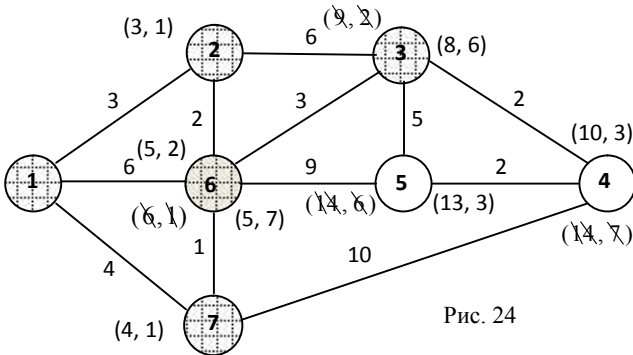


Рис. 24

Среди незакрашенных вершин 4 и 5 выбираем вершину 4.
 Закрашиваем вершину 4. Для вершины 5 получаем метку (12, 4). Сравнивая с прежней меткой, (13, 3), исключаем прежнюю метку и записываем новую метку (12, 4) возле вершины 5.
 Всем вершинам присвоены метки, которые показывают кратчайшие маршруты от начальной точки (рис. 25).
 Чтобы перечислить кратчайшие маршруты, пройдем обратным ходом из конечной вершины 5 в начальную вершину 1. Второе число каждой метки показывает, в какую вершину нужно вернуться по ранее пройденному маршруту.

Получаем вершины в обратном порядке: 5, 4, 3, 6, 2, 1 или 5, 4, 3, 6, 7, 1.

Записывая эти последовательности вершин в обратном порядке, получим искомые маршруты: 1, 2, 6, 3, 4, 5 и 1, 7, 6, 3, 4, 5.

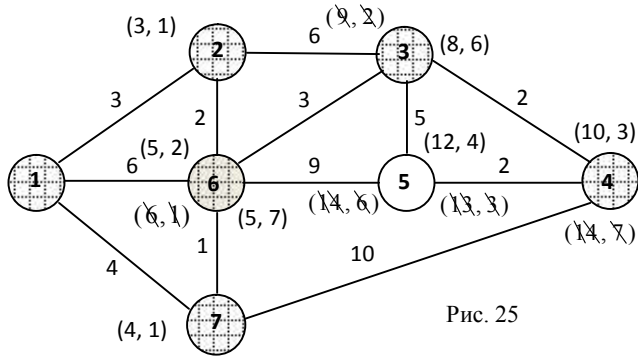


Рис. 25

Задачи.

47.1. Для графа на рис. 26 найдите кратчайший маршрут из вершины 1 в вершину 7.

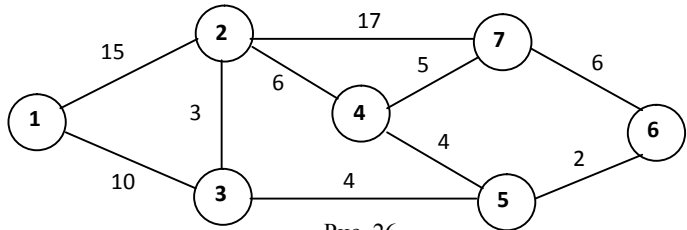


Рис. 26

§ 48. Максимальная пропускная способность сети

Рассмотрим орграф, в котором имеется одна вершина, степень входа которой равна нулю (такая вершина называется источником сети), и в котором имеется одна вершина, степень выхода которой равна нулю (такая вершина называется стоком сети).

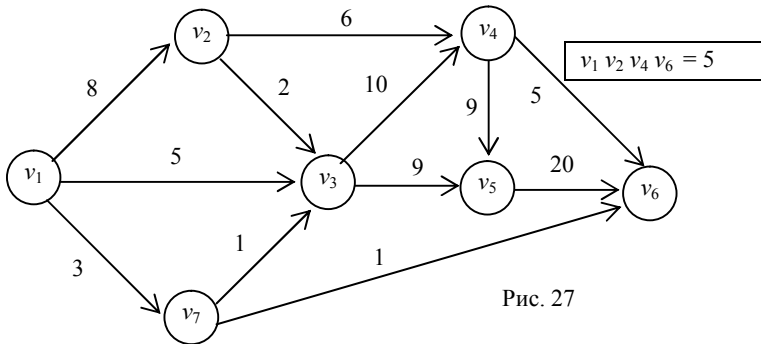


Рис. 27

Пример 1. На рисунке 27 вершина v_1 изображает месторождение нефти и является источником, вершина v_6 – потребителем нефти, т.е. стоком. Остальные вершины орграфа – перекачивающие станции. Числа возле ребер, являющиеся весами ребер, обозначают пропускную способность трубопровода за некоторую единицу времени. Найдем максимальную пропускную способность сети из вершины v_1 в вершину v_6 .

Решение. Любая цепь из вершины v_1 в вершину v_6 имеет несколько последовательных дуг. Максимальная пропускная способность цепи определяется наименьшим значением некоторой дуги среди всех дуг этой цепи. Перечисляя различные цепи, определим максимальную способность всей сети.

Шаг 1. Для цепи $v_1v_2v_4v_6$ на рис. 27 максимальная пропускная способность равна $\min(8, 6, 5) = 5$. Уменьшим на эту величину пропускные способности всех дуг рассматриваемой цепи. Дугу v_4v_6 с новой нулевой пропускной способностью удалим из сети.

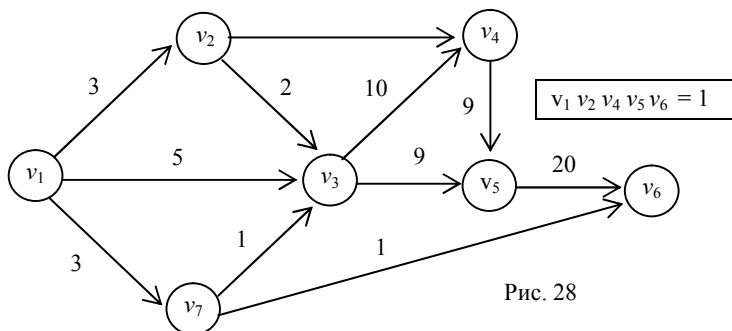


Рис. 28

П

получим вспомогательную сеть для поиска других цепей (рис. 28).

Для цепи $v_1v_2v_4v_5v_6$ на рис. 28 максимальная пропускная способность равна 1. Уменьшив на эту величину значения пропускных способностей всех дуг цепи $v_1v_2v_4v_5v_6$, получим вспомогательную сеть на рис. 29.

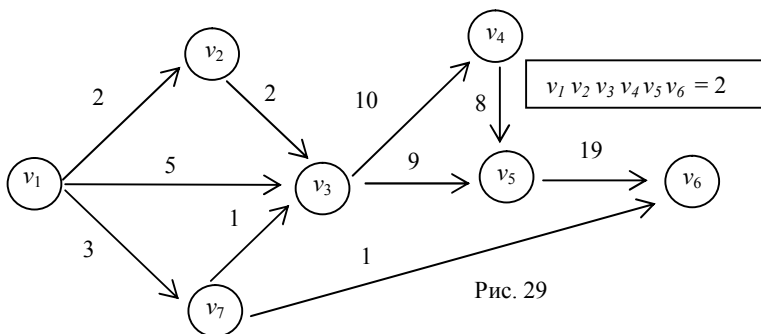


Рис. 29

Для цепи $v_1v_2v_3v_4v_5v_6$ на рис. 29 максимальная пропускная способность равна 2.

Уменьшив на эту величину значения пропускных способностей всех дуг цепи $v_1v_2v_3v_4v_5v_6$, получим вспомогательную сеть на рис. 30.

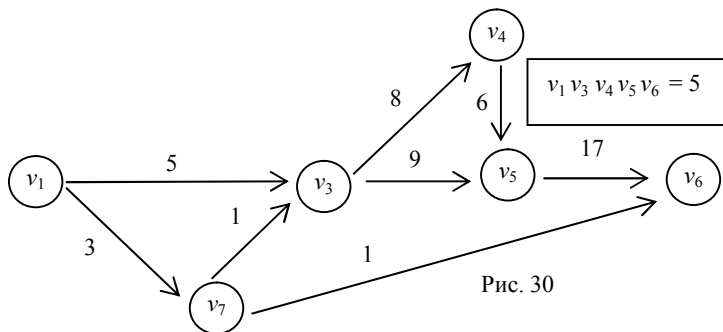


Рис. 30

Для цепи $v_1 v_3 v_4 v_5 v_6$ на рис. 30 максимальная пропускная способность равна 5. Уменьшив на эту величину значения пропускных способностей всех дуг цепи $v_1 v_3 v_4 v_5 v_6$, получим вспомогательную сеть на рис. 31.

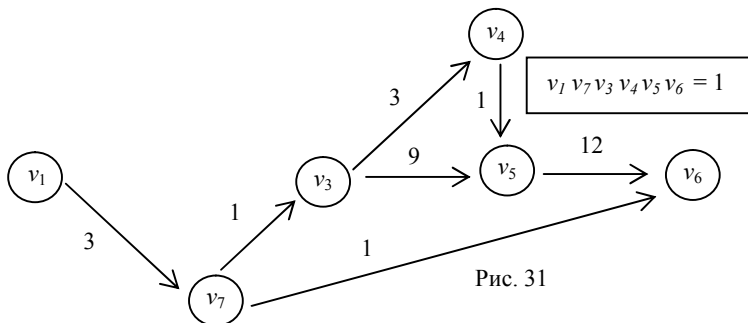


Рис. 31

Для цепи $v_1 v_7 v_3 v_4 v_5 v_6$ на рис. 31 максимальная пропускная способность равна 1. Уменьшив на эту величину значения пропускных способностей всех дуг цепи $v_1 v_7 v_3 v_4 v_5 v_6$, получим вспомогательную сеть на рис. 32.

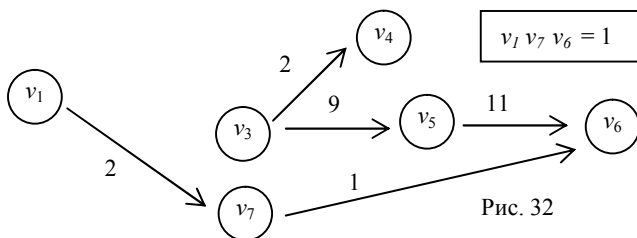


Рис. 32

Для цепи $v_1 v_7 v_6$ на рис. 32 максимальная пропускная способность равна 1. Уменьшив на эту величину значения пропускных способностей всех дуг цепи $v_1 v_7 v_6$, получим вспомогательную сеть на рис. 33.

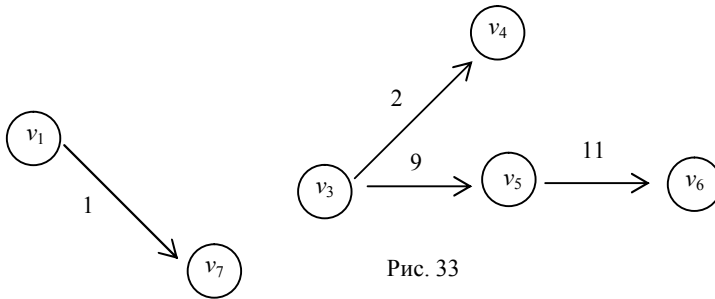


Рис. 33

Суммируя пропускные способности $5 + 1 + 2 + 5 + 1 + 1 = 15$ рассмотренных путей, получим пропускную способность всей сети – 14.

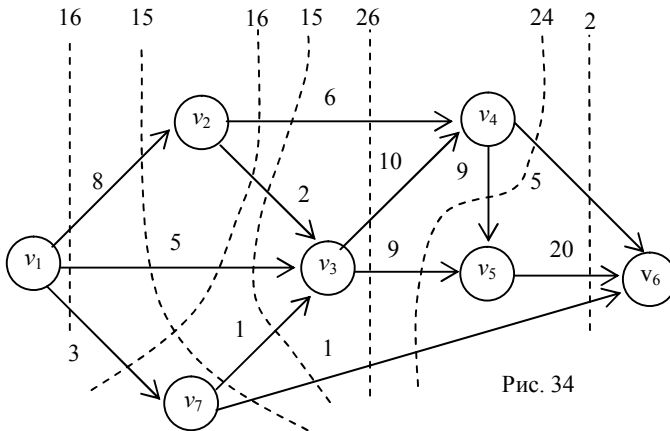


Рис. 34

Пропускную способность сети можно получить, если найти все разрезы сети и определить разрез с минимальной пропускной способностью.

На рис. 34 представлено несколько разрезов с указанием пропускных способностей.

Замечание. Если сеть имеет сложное строение, то проведенный разрез может пересекать дуги с противоположными направлениями (рис. 35). При определении пропускной способности разреза нужно учитывать числа с добавлением знаков.

Изложенный выше метод является относительно простым, но затрудняет в итоге увидеть распределение максимальной пропускной способности сети по дугам.

Рассмотрим второй способ реализации изложенного метода. В дальнейшем изображение на рис. 36 означает следующее.

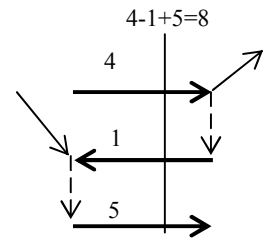


Рис. 35

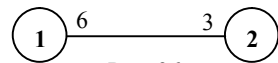


Рис. 36

Поток от узла 1 к узлу 2 равен 6, а в обратном направлении от узла 2 к узлу 1 поток равен 3. Например, автомобильная дорога имеет две полосы от 1 к 2, а в обратном направлении одну полосу, что существенно влияет на поток автомобилей при непрерывном потоке автомобилей.

Пример 2. Найти максимальный поток в сети (рис. 37) от узла 1 к узлу 3.

1. Выбираем один из путей, который имеет направление от вершины 1 к вершине 3, причем поток должен иметь ненулевое значение. Для пути 1-2-3 поток равен 2 и определяется минимальной пропускной способностью от узла 2 к узлу 3. Мощности всех потоков по направлению этого пути уменьшаем на величину $P=2$, а в обратном направлении увеличиваем на 2. Получаем схему на рис. 38.

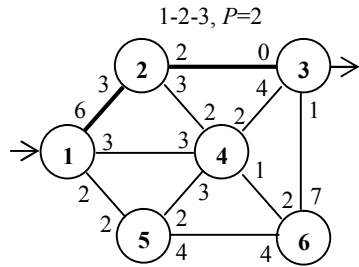


Рис. 37

2. Выбираем путь 1-2-4-3 (рис. 38) с мощностью, равной 2. Мощности всех потоков по направлению этого пути уменьшаем на величину $P=2$, а в обратном направлении увеличиваем на 2. Мощность на выходе из вершины 3 увеличиваем на 2. Получаем схему на рис. 39.

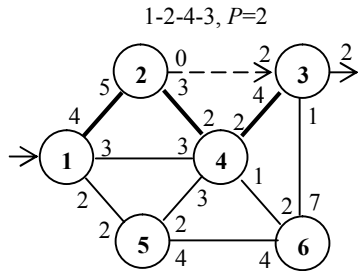


Рис. 38

3. Для пути 1-2-4-6-3 (рис. 39) мощность потока равна 1. Увеличиваем общую мощность потока на 1. Аналогично получаем схему на рис. 40.

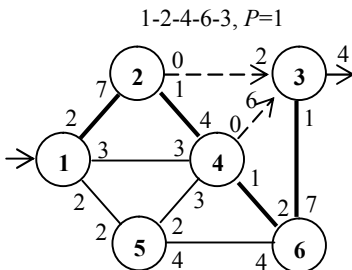


Рис. 39

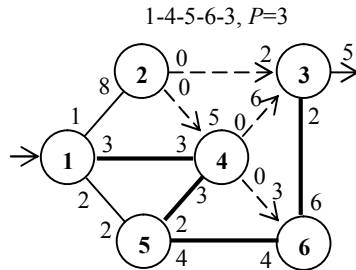


Рис. 40

4. Для пути 1-4-5-6-3 мощность потока равна 3. Получаем схему на рис. 41.

5. Для пути 1-5-6-3 мощность потока равна 1. Получаем схему на рис. 42. Больше не существует путей из узла 1 в узел 3 с положительным потоком. Сравнивая первоначальную схему с последней схемой, найдем разности весов, выходящих из каждой вершины, и получим распределение общего потока (рис. 43).

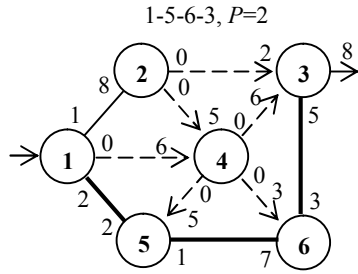


Рис. 41

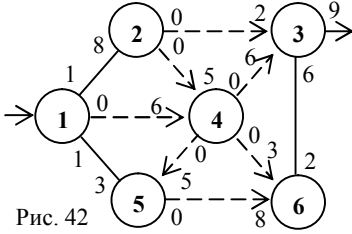


Рис. 42

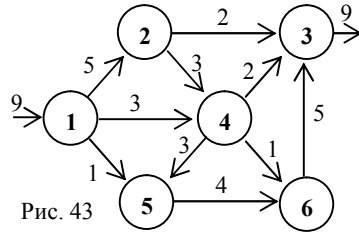


Рис. 43

Задачи.

Найдите максимальную пропускную способность сети из вершины 1 в вершину 7 (рис. 44–47):

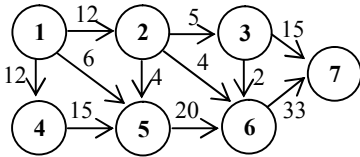


Рис. 44

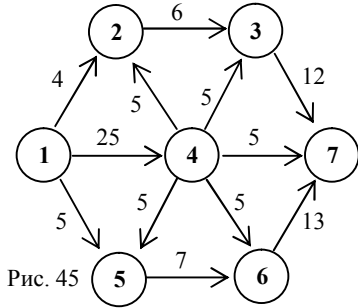


Рис. 45

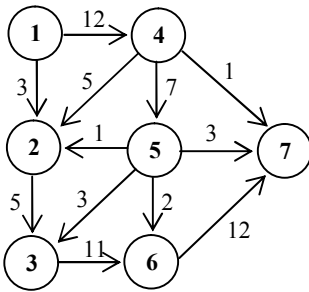


Рис. 46

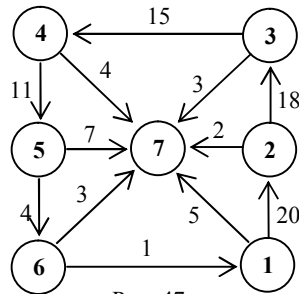


Рис. 47

§ 49. Понятие алгоритма

Введем рабочее определение алгоритма.

Алгоритм – это точная конечная система предписаний, определяющих содержание и порядок действий исполнителя над некоторыми объектами (исходными и промежуточными данными) для получения искомого результата.

Свойства алгоритма:

Дискретность. Выполнение алгоритма разбивается на конечную последовательность действий. Только выполнив одно действие, можно приступить к выполнению другого действия. Выполнить каждое отдельное действие предписывает указание в алгоритме, называемое командой.

Детерминированность. Способ решения однозначно определен. Если алгоритм многократно применяется к одному и тому же набору исходных данных, то каждый раз получатся одни и те же промежуточные и выходные данные.

Понятность. Исполнитель должен однозначно воспринимать смысл предстоящих действий.

Результативность. При точном исполнении команд алгоритма процесс должен закончиться за конечное число действий и должен быть получен ответ на вопрос задачи. В качестве одного из возможных ответов может быть вывод о том, что задача не имеет решения.

Массовость. Алгоритм применяется для решения любой задачи определенного класса задач, который называется областью применения алгоритма.

Различные способы описания алгоритма:

- текстовая форма записи;
- символьная запись;
- запись алгоритма на некотором алгоритмическом языке;
- представление алгоритма в виде машины Тьюринга или машины Поста.

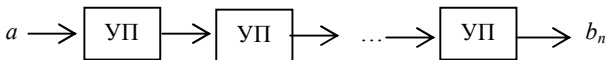
Если алгоритм содержит большое число команд, то применяют укрупнение и команды объединяются в алгоритмические конструкции: последовательные, ветвящиеся, циклические и рекурсивные. Для записи любого алгоритма достаточно трех основных конструкций: последовательных, ветвящихся и циклических.

Примеры алгоритмов.

Пример 1. Вычисление суммы первых n членов данной числовой последовательности: a_1, a_2, \dots, a_n .

Пример 2. Вычисление факториала числа n .

Пример 3. Блок УП имеет один вход и один выход. Поступившее число в блок УП вначале умножается на 2, а затем прибавляется 2. Схема состоит из n блоков УП, соединенных последовательно (рис. 48). На вход системы поступает число a . Какое число будет на выходе из схемы?



Решение.

Рис. 48

Для поиска общей формулы рассмотрим частные случаи:

$$n = 1 \rightarrow b_1 = a \cdot 2 + 2,$$

$$n = 2 \rightarrow b_2 = (a \cdot 2 + 2) \cdot 2 + 2 = a \cdot 2^2 + 2^2 + 2,$$

$$n = 3 \rightarrow b_3 = (a \cdot 2^2 + 2^2 + 2) \cdot 2 + 2 = a \cdot 2^3 + 2^3 + 2^2 + 2,$$

$$n = 4 \rightarrow b_4 = (a \cdot 2^3 + 2^3 + 2^2 + 2) \cdot 2 + 2 = a \cdot 2^4 + 2^4 + 2^3 + 2^2 + 2.$$

Появляется гипотеза $b_n = a \cdot 2^n + 2^n + 2^{n-1} + \dots + 2^2 + 2$.

Сумма $2^n + 2^{n-1} + \dots + 2^2 + 2$ является суммой членов геометрической прогрессии, и она равна $2^{n+1} - 2$. Следовательно $b_n = 2^n a + 2^{n+1} - 2$.

Докажем это равенство методом математической индукции.

При $n = 1$ равенство выполняется.

Допустим, что гипотеза верна при $n = k$, т.е. $b_k = 2^k a + 2^{k+1} - 2$.

Докажем равенство при $n = k + 1$.

Действительно, $b_{k+1} = b_k \cdot 2 + 2 = (2^k a + 2^{k+1} - 2) \cdot 2 + 2 = 2^{k+1} a + 2^{k+2} - 2$.

На основании метода математической индукции можно утверждать, что формула $b_n = 2^n a + 2^{n+1} - 2$ справедлива при любом натуральном n .

Пример 4. У исполнителя Вычислитель две команды. Одна команда увеличивает число на 2, а вторая удваивает его. Программа для Удвоителя — это некоторая последовательность этих команд. Сколько есть программ, которые число 4 преобразуют в число 30?

Решение. Очевидно, что из числа 4 можно получить только четные числа, поэтому нечетные числа можно не рассматривать. Будем решать поставленную задачу последовательно для чисел 4, 6, 8, ..., 30.

Вначале попытаемся наглядно изобразить команды при получении первых чисел (рис. 49).

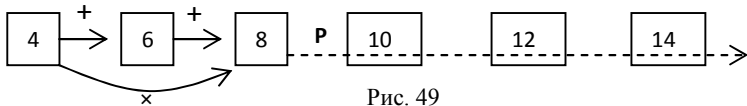


Рис. 49

Число 8 можно получить из числа 4 двумя способами, применяя команды добавления числа 2 или удвоения числа. Пусть выбрана одна из программ P , часть которой на рис. 49 изображена пунктирной стрелкой и выходящей из числа 8.

Соединяя эту часть с предшествующими частями $4 \xrightarrow{+} 6 \xrightarrow{+} 8$ или $4 \xrightarrow{x} 8$, получаем две программы.

Пусть выбрана одна из программ P , часть которой на рис. 50 изображена пунктирной стрелкой и выходящей из числа 10.

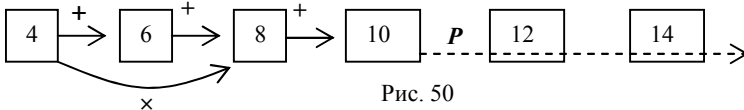


Рис. 50

Соединяя эту часть с предшествующими частями, приходящими в число 10, получаем две программы.

Пусть выбрана одна из программ P , часть которой на рис. 51 изображена пунктирной стрелкой и выходящей из числа 12.

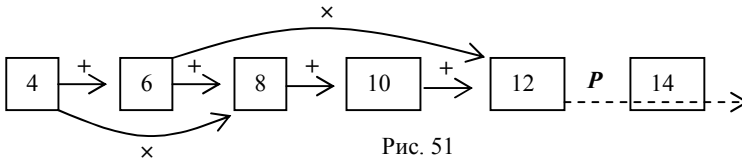


Рис. 51

Число 12 можно получить из числа 10 с помощью двух программ, а также число 12 можно получить из числа 6 с помощью одной программы. В результате число 12 можно получить с помощью трех программ.

Итак, при определении числа программ, с помощью которых можно получить некоторое число, нужно знать, из каких предшествующих чисел может быть получено данное число.

Количество программ, которые преобразуют число 4 в число n , обозначим через $R(n)$. Число 4 у нас уже есть, значит, его можно получить с помощью “пустой” программы. Любая непустая программа увеличит исходное число, т.е. даст число больше 4. Значит, $R(4)=1$. Для каждого следующего четного числа рассмотрим, из каких четных чисел оно может быть получено за одну команду исполнителя. Для удобства составим таблицу 3.

Таблица 3

Число	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Из чего получается	–	4	6, 4	8	10, 6	12	14, 8	16	18, 10	20	22, 12	24	26, 14	28
Количество программ														

Средняя строка таблицы 3 показывает, из каких чисел можно получить данное число за одно действие. В нижнюю строку запишем количество программ, с помощью которых можно получить данное число.

Для заполнения нижней строки, используем следующее правило.

Пусть число n за одно действие можно получить из чисел n_1, n_2 . Тогда $R(n)=R(n_1)+R(n_2)$. Если число n можно получить только из одного число n_1 , то $R(n)=R(n_1)$.

Используя эти формулы, заполняем нижнюю строку таблицы 4, двигаясь от меньших чисел к большим.

Таблица 4

Число	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Из чего получается	–	4	6, 4	8	10, 6	12	14, 8	16	18, 10	20	22, 12	24	26, 14	28
Количество программ	1	1	2	2	3	3	5	5	7	7	10	10	13	13

Ответ: 13 .

Задачи.

49.1. Блок УП имеет один вход и один выход. Поступившее число в блок УП вначале умножается на 2, а затем прибавляется 2. Блок ПУ имеет один вход и один выход. К поступившему числу в блок ПУ вначале добавляется 2, а затем результат умножается на 2.

а) Схема состоит из m блоков ПУ, соединенных последовательно. На вход системы поступает число a . Какое число будет на выходе из схемы?

б) Какое число поступило на вход, если результат работы одной схемы из n блоков УП, соединенных последовательно и работы другой схемы из m блоков УП, соединенных последовательно, оказались одинаковыми?

49.2. У исполнителя Кузнечик две команды.

Одна из них увеличивает число на 7, вторая – уменьшает его на 5 (отрицательные числа допускаются). Программа для Кузнечика – это последовательность команд.

Сколько различных чисел можно получить из числа 1 с помощью программы, которая содержит ровно 7 команд?

49.3. У исполнителя Множитель две команды: одна из них увеличивает число в 5 раз, вторая – уменьшает его в 3 раза. Программа для Множителя – это последовательность команд. Сколько различных чисел можно получить из числа 81 с помощью программы, которая содержит ровно 4 команды?

49.4. У исполнителя Накопитель две команды. Одна из них увеличивает число на 5, вторая – увеличивает на 10. Программа для Накопителя – это последовательность команд. Сколько различных чисел можно получить из числа 1 с помощью программы, которая содержит ровно 7 команд?

49.5. У исполнителя Множитель две команды. Одна из них увеличивает число в 5 раз, вторая – увеличивает его в 3 раза. Программа для исполнителя Множитель – это последовательность команд.

Сколько различных чисел можно получить из числа 81 с помощью программы, которая содержит ровно 4 команды?

49.6. У исполнителя Плюсик две команды. Одна из них увеличивает число на 6, вторая – уменьшает его на 3. Плюсик умеет производить действия только с положительными числами. Если в ходе вычислений появляется отрицательное число, он выходит из строя и стирает написанное на экране. Программа для Плюсика – это последовательность команд.

Сколько различных чисел можно получить из числа 1 с помощью программы, которая содержит ровно 10 команд?

49.7. У исполнителя две команды:

– команда В вычитает число 2 из поступившего числа;

– команда У умножает поступившее число на 3.

Укажите алгоритм с наименьшим числом команд для получения числа 13 из числа 11.

§ 50. Вычислимые функции

Действие любого алгоритма сводится к вычислению некоторой функции $f(x_1, x_2, \dots, x_n)$ натуральных аргументов. Естественно такую функцию назвать *алгоритмически вычислимой*, если существует алгоритм для вычисления ее значений. Для удобства в этом параграфе будем считаться, что 0 – это натуральное число.

Простейшими числовыми функциями являются функции следующего вида:

а) $O(x) = 0$ – оператор аннулирования;

б) $\lambda(x) = x + 1$ – оператор сдвига;

в) $I_m^n(x_1, x_2, \dots, x_n) = x_m, 1 \leq m \leq n$ – оператор проектирования.

Все эти функции всюду определены и алгоритмически вычислимы.

Если имеем функции $f(x_1, x_2, \dots, x_m), f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$, то можно построить их суперпозицию

$$F(x_1, x_2, \dots, x_n) = f(f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)).$$

Таким образом, имеем оператор $S^{m+1}(f, f_1, f_2, \dots, f_m)$, который функциям f, f_1, f_2, \dots, f_m ставит в соответствие их суперпозицию F . Любой такой оператор (т. е. оператор суперпозиции) назовем *оператором подстановки*. Очевидно, что если функции f, f_1, f_2, \dots, f_m всюду определены и алгоритмически вычислимы, то функция F тоже всюду определена и алгоритмически вычислима.

Пусть даны n -местная функция $g(x_1, x_2, \dots, x_n)$ и $(n+2)$ -местная функция $h(x_1, x_2, \dots, x_n, y, z)$. Говорят, что $(n+1)$ -местная функция $f(x_1, x_2, \dots, x_n, y)$ получена из данных функций с помощью *примитивной рекурсии*, если выполнены условия:

1) $f(x_1, x_2, \dots, x_n, 0) = g(x_1, x_2, \dots, x_n)$;

2) $f(x_1, x_2, \dots, x_n, y+1) = h(x_1, x_2, \dots, x_n, y, f(x_1, x_2, \dots, x_n, y))$.

Если итоговая функция f одноместная, то под 0-местной функцией g понимается некоторая константа a . И в этом случае условия 1), 2) выглядят следующим образом:

1) $f(0) = a$; 2) $f(x+1) = h(x, f(x))$.

Отметим, что функция f всегда определена и притом однозначно.

Таким образом, имеем оператор $R(g, h) = f$, который называется *оператором примитивной рекурсии*. Если функции g и h всюду определены и алгоритмически вычислимы, то функция f также всюду определена и алгоритмически вычислима.

Числовая функция $f(x_1, x_2, \dots, x_n)$ называется *примитивно рекурсивной*, если она может быть получена из простейших числовых функций $O(x), \lambda(x), I_m^n(x_1, \dots, x_n)$ с помощью конечного числа операторов подстановки и примитивной рекурсии. Понятно, что простейшие функции примитивно рекурсивны.

Любая примитивно рекурсивная функция всюду определена и алгоритмически вычислима.

Пример 1. Пусть даны функции $g(x) = x$ и $h(x, y, z) = x + z$. Какая функция $f(x, y)$ получается из них с помощью примитивной рекурсии?

Решение. По схеме примитивной рекурсии имеем

$$f(x, 0) = g(x) = x = a_0,$$

$$f(x, 1) = f(x, 0 + 1) = h(x, 0, f(x, 0)) = h(x, 0, a_0) = h(x, 0, x) = x + x = 2x = a_1,$$

$$f(x, 2) = f(x, 1 + 1) = h(x, 1, f(x, 1)) = h(x, 1, a_1) = h(x, 1, 2x) = x + 2x = 3x = a_2,$$

$$f(x, 3) = f(x, 2 + 1) = h(x, 2, f(x, 2)) = h(x, 2, a_2) = f(x, 2, 3x) = x + 3x = 4x.$$

Можно заметить закономерность $f(x, y) = (y + 1)x$.

Покажем, что эта функция удовлетворяет условиям схемы примитивной рекурсии, что ввиду вышеуказанной однозначности и даст искомый результат. Итак, имеем

$$1) f(x, 0) = (0 + 1)x = x = g(x);$$

$$2) f(x, y + 1) = [(y + 1) + 1]x = (y + 1)x + x = f(x, y) + x = h(x, y, f(x, y)). \quad \square$$

Если функции g и h примитивно рекурсивны, то и функция $f = R(g, h)$ тоже примитивно рекурсивна. Это позволяет доказывать примитивную рекурсивность различных числовых функций.

Пример 2. Покажем, что функция $f(x_1, \dots, x_n) = a$, где $a = const$ есть примитивно рекурсивная функция. Имеем

$$a = \underbrace{\lambda(\lambda(\dots(\lambda(0))\dots))}_a = \underbrace{\lambda(\lambda(\dots(\lambda(O(x_1))\dots))}_a = \underbrace{\lambda(\lambda(\lambda(\dots(\lambda(O(I_1^n(x_1, \dots, x_n)))\dots))}_a),$$

т.е. функция f получается из простейших с помощью конечного числа операторов подстановки. По определению f примитивно рекурсивна. \square

Пример 3. Показать, что обычная операция сложения $f(x, y) = x + y$ есть примитивно рекурсивная функция.

Решение. Рассмотрим функции $g(x) = x = I_1^1(x)$ и $H(x, y, z) = z + 1 = \lambda(z)$, которые примитивно рекурсивны. Покажем, что $f(x, y)$ получается из них с помощью примитивной рекурсии. Имеем

$$1) f(x, 0) = x + 0 = x = g(x),$$

$$2) f(x, y + 1) = x + (y + 1) = (x + y) + 1 = f(x, y) + 1 = h(x, y, f(x, y)). \quad \square$$

Обычная разность не является примитивно рекурсивной функцией, т.к. она не всюду определена. В теории алгоритмов используется так называемая усеченная разность

$$x \dot{-} y = \begin{cases} x - y, & \text{если } x \geq y, \\ 0, & \text{если } x < y. \end{cases}$$

Любое натуральное число x можно поделить на любое натуральное число y с остатком, т.е. $x = qy + r$, $0 \leq r < y$. Имеем две функции:

$$\left[\frac{x}{y} \right] - \text{неполное частное от деления } x \text{ на } y;$$

$rest(x, y)$ – остаток от деления x на y .

$$\text{Доопределим эти функции, положив } \left[\frac{x}{0} \right] = x \text{ и } rest(x, 0) = x.$$

Функции $\left[\frac{x}{y} \right]$, $rest(x, y)$ и $x \div y$ примитивно рекурсивны (см. задачи 50.7 и 50.3).

Пусть задана функция $g(x_1, x_2, \dots, x_n, y)$. Обозначим через $\mu_y(g(x_1, \dots, x_n, y) = 0)$ наименьший корень уравнения $g(x_1, x_2, \dots, x_n, y) = 0$ относительно y , если он существует. Таким образом, если $\mu_y(g(x_1, \dots, x_n, y) = 0) = a$, то $g(x_1, \dots, x_n, a) = 0$ и $g(x_1, \dots, x_n, b)$ для всех $b < a$ определены и $g(x_1, \dots, x_n, b) \neq 0$. Имеем функцию $f((x_1, \dots, x_n) = \mu_y(g(x_1, \dots, x_n, y) = 0))$. Эта функция не всюду определена, т.к. во-первых, уравнение $g(x_1, \dots, x_n, y) = 0$ при каком-то наборе переменных x_1, \dots, x_n вообще может не иметь решений. А во-вторых, если оно имеет какое-то решение, например $g(x_1, x_2, \dots, x_n, a) = 0$, мы не можем определить его минимальность, т.к. для некоторых $b < a$ значение $g(x_1, x_2, \dots, x_n, b) = 0$ может быть не определено. Если же значение функции определено, скажем $f(x_1, x_2, \dots, x_n) = a$, то это означает, что $g(x_1, \dots, x_n, a) = 0$ и для всех $b < a$ значения $g(x_1, \dots, x_n, b)$ определены и отличны от нуля.

Говорят, что построенная выше функция $f((x_1, \dots, x_n) = \mu_y(g(x_1, \dots, x_n, y) = 0))$ получается из функции $g(x_1, \dots, x_n, y)$ с помощью операции минимизации, т.е. имеем оператор $M(g) = f$, который называется оператором минимизации.

Функция $f(x_1, \dots, x_n)$ называется *частично рекурсивной*, если она может быть получена из простейших с помощью конечного числа операторов подстановки, примитивной рекурсии и минимизации.

Очевидно, что примитивно рекурсивные функции являются частично рекурсивными. Если к набору частично рекурсивных функций применим оператор подстановки, примитивной рекурсии или минимизации, то получим снова частично рекурсивную функцию.

Частично рекурсивная функция, вообще говоря, не всюду определена. Как уже отмечалось, обычная разность $f(x, y) = x - y$ не является примитивно рекурсивной, но функция $f(x, y) = x - y$ частично рекурсивная (докажите).

Теорема о мажорируемости неявных функций. Пусть для функции $g(x_1, \dots, x_n, y)$ уравнение $g(x_1, \dots, x_n, y) = 0$ разрешимо по y при любых значениях x_1, \dots, x_n . Если $\alpha(x_1, \dots, x_n)$ — такая примитивно рекурсивная функция, что $f((x_1, \dots, x_n) = \mu_y(g(x_1, \dots, x_n, y) = 0)) \leq \alpha(x_1, \dots, x_n)$, то функция $f(x_1, \dots, x_n)$ примитивно рекурсивная.

Тезис Черча. Функция $f(x_1, \dots, x_n)$ алгоритмически вычислима тогда и только тогда, когда она частично рекурсивна.

Таким образом, согласно тезису Черча, вопрос существования алгоритма для решения какой-то задачи сводится к вопросу: “Можно или нельзя требуемую вычислительную процедуру описать с помощью какой-то частично рекурсивной функции?” Используя этот подход, были решены многие алгоритмические проблемы.

Например, десятая проблема Гильберта. Пусть дан многочлен $F(x_1, x_2, \dots, x_n)$ с целыми коэффициентами. Проблема: построить алгоритм, позволяющий для любого такого многочлена определять, разрешимо ли уравнение $F(x_1, x_2, \dots, x_n) = 0$ в целых числах.

Не существует алгоритма, позволяющего для любого целочисленного многочлена $F(x_1, x_2, \dots, x_n)$ определять, разрешимо ли уравнение $F(x_1, x_2, \dots, x_n) = 0$ в целых числах (Матиясевич Ю.В.).

Проблема тождественной истинности. Фактически любое утверждение в математике можно записать в виде формулы логики предикатов. Проблема: построить алгоритм, позволяющий для любой формулы логики предикатов определять ее тождественную истинность.

Не существует алгоритма, позволяющего определять тождественную истинность любой формулы логики предикатов.

Задачи.

50.1. Определите, какая функция $f(x, y)$ получится из функций $g(x)$ и $h(x, y, z)$ с помощью рекурсии:

а) $g(x) = 3$, $h(x, y, z) = xz$;

б) $g(x) = x^2$, $h(x, y, z) = x + z$;

в) $g(x) = x$, $h(x, y, z) = xz$;

г) $g(x) = 0$, $h(x, y, z) = |z - x|$;

д) $g(x) = 1$, $h(x, y, z) = x^z$;

е) $g(x) = x$, $h(x, y, z) = z^x$;

ж) $g(x) = 0$, $h(x, y, z) = x + y - z$;

з) $g(x) = x$, $h(x, y, z) = zy$;

и) $g(x) = 5$, $h(x, y, z) = zy$.

50.2. Покажите, что функции $f(x, y) = xy$ и $f(x, y) = x^y$ примитивно рекурсивны.

50.3. Покажите, что усеченная разность является примитивной функцией. (Указание: покажите сначала примитивную рекурсивность функции $x \div 1$.)

50.4. Докажите, что следующие функции примитивно рекурсивны:

$$\text{а) } sg(x) = \begin{cases} 0, & x = 0, \\ 1, & x \neq 0. \end{cases} \quad \text{б) } \overline{sg}(x) = \begin{cases} 1, & x = 0, \\ 0, & x \neq 0. \end{cases}$$

50.5. Пусть примитивно рекурсивны $f_1(x_1, \dots, x_n), \dots, f_{k+1}(x_1, \dots, x_n)$ и $\alpha_1(x_1, \dots, x_n), \dots, \alpha_k(x_1, \dots, x_n)$, причем для любых $i \neq j$ функции $\alpha_i(x_1, \dots, x_n)$ и $\alpha_j(x_1, \dots, x_n)$ одновременно в 0 не обращаются ни при каких значениях переменных $i, j = 1, 2, \dots, k$. Покажите примитивную рекурсивность функции

50.11. Пусть $2, 3, 5, 7, \dots, p_n, \dots$ – простые числа, записанные в порядке возрастания, и пусть $p(n) = p_n$ – n -ое простое число. Покажите, что $p(n)$ примитивно рекурсивна. (Указание. Предварительно методом математической индукции докажите неравенство $p_n < 2^{2^n}$.)

§ 51. Машина Тьюринга

Машина Тьюринга состоит из трех частей.

1. *Управляющее устройство*, которое может находиться в одном из состояний, образующих конечное множество $Q = \{q_0, q_1, \dots, q_n\}$. Среди состояний выделены начальное состояние q_1 и заключительное q_0 . В начальном состоянии машина находится перед началом работы, попав в заключительное состояние, машина останавливается.
2. *Лента*, разбитая на ячейки, в каждой из которых находится один из символов конечного алфавита $A = \{a_1, a_2, \dots, a_m\}$. Лента бесконечна в обе стороны, однако в любой момент времени только конечное число ячеек заполнено символами из алфавита. Остальные ячейки пусты, т.е. заполнены пустым символом λ . Важна не фактическая бесконечность ленты, а ее неограниченность, т.е. возможность записать на ней сколь угодно большие слова, но конечные.
3. Устройство обращения к ленте, т.е. некая считывающая и пишущая *головка*. Она в каждый момент времени обзрывает ровно одну ячейку, в зависимости от символа в этой ячейке a_j и состояния q_i управляющего устройства, записывает в данную ячейку новый символ a'_j (возможно, тот же самый), переходит в новое состояние q'_i (возможно, то же самое) и сдвигается на одну ячейку вправо (R), влево (L) или остается на месте (E).

Это записывается в виде

$$q_i a_j \rightarrow q'_i a'_j d, \quad (*)$$

где d – одно из действий R, L или E .

Словом в алфавите $A = \{a_1, a_2, \dots, a_m\}$ называется любая конечная последовательность букв в алфавите. Любая конечная последовательность слов алфавита A называется *словарным вектором*.

Память машины Тьюринга – это конечное множество состояний (внутренняя память) и лента (внешняя память). Элементарные шаги машины – это считывание и запись символов, сдвиг головки на ячейку вправо-влево, а также переход управляющего устройства из одного состояния в другое. Полное состояние машины Тьюринга, по которому можно определить ее дальнейшее поведение, определяется ее внутренним состоянием, состоянием ленты и положением головки на ней. Полное состояние машины называется ее конфигурацией K , которая определяется тройкой $\alpha q_i \beta$, где q_i – текущее внутреннее состояние, α – слово слева от головки, β – слово справа от головки (точнее, α и β – словарные векторы). Причем слева от α и справа от β все ячейки пусты.

Стандартная начальная конфигурация – это конфигурация вида $q_1\alpha$, а конечная – вида $q_0\alpha$. Ко всякой незаключительной конфигурации K применима ровно одна команда вида $q_ia_j \rightarrow q'_ia'_jd$. При этом конфигурация K переходит в новую конфигурацию K' , что записывается в виде $K \rightarrow K'$.

Если имеется последовательность конфигураций $K_1 \rightarrow K_2 \rightarrow \dots \rightarrow K_n$, то говорят, что машина в процессе своей работы перешла от конфигурации K_1 к конфигурации K_n .

Набор всех команд вида (*) называется программой работы машины. Эту программу часто записывают в виде таблицы, которую иногда называют функциональной схемой.

Пример 1. Пусть $A = \{a_1, a_2, a_3, a_4\}$ и $Q = \{q_0, q_1, q_2, q_3\}$. Команды рассматриваемой машины запишем в виде таблицы 5.

Таблица 5

$A \backslash Q$	a_1	a_2	a_3	a_4
q_1	q_2a_2R			q_3a_3R
q_2	q_3a_2L	q_3a_4L		
q_3	q_2a_4R		q_1a_2E	q_0a_2L

Пустые клетки означают, что, например, в состоянии q_1 в процессе работы на символ a_2 машина не попадет.

K_1 :

a_4	a_1	a_2
-------	-------	-------

 \rightarrow
 q_1

K_2 :

a_3	a_1	a_2
-------	-------	-------

 \rightarrow
 q_3

K_3 :

a_3	a_4	a_2
-------	-------	-------

 \rightarrow
 q_2

K_4 :

a_3	a_4	a_4
-------	-------	-------

 \rightarrow
 q_3

K_5 :

a_3	a_2	a_4
-------	-------	-------

 – стоп.
 q_0

Таким образом, данная машина переработала слово $a_4a_1a_2$ в слово $a_3a_2a_4$. Не изображая ленту, данную работу можно записать в виде последовательности:

$q_1a_4a_1a_2 \rightarrow a_3q_3a_1a_2 \rightarrow a_3a_4q_2a_2 \rightarrow a_3q_3a_4a_4 \rightarrow q_0a_3a_2a_4$. \square

Исходными данными машины Тьюринга являются записанные на ленте слова (словарные векторы) в алфавите $A_{исх}$. Для любого словарного вектора над $A_{исх}$ машина работает бесконечно либо перерабатывает его в совокупность слов, разделенных некоторым знаком, над некоторым алфавитом результатов $A_{рез}$. В процессе работы машины на ленте могут появиться какие-то новые символы, не входящие ни в $A_{исх}$, ни в $A_{рез}$, которые образуют новый промежуточный алфавит $A_{пр}$. На практике, как правило, $A_{исх} = A_{рез} = A$. Новые символы из $A_{пр}$ в итоге в $A_{рез}$ отсутствуют.

Пусть дан некоторый словарный вектор $(\alpha_1, \alpha_2, \dots, \alpha_n)$, где α_i – слово в алфавите A . Запись на ленте этого вектора называется правильной (или машинной), если она имеет вид $\alpha_1 * \alpha_2 * \dots * \alpha_n$, где $*$ – специальный символ-разделитель, не входящий в A . Внутри правильно записанного словарного вектора пустых ячеек λ нет. Если в процессе работы машине приходится внутри машинной записи словарного вектора стирать какую-либо букву, то тогда вместо пустой ячейки λ в нее заносится некоторый новый символ, добавляя его в $A_{пр}$.

Пусть f – функция, отображающая множество векторов над $A_{исх.}$ во множество векторов над $A_{рез.}$

Определение. Говорят, что машина Тьюринга T правильно вычисляет функцию f , если выполнены условия:

а) для любых словарных векторов V и W таких, что $f(V) = W$, машина, начав работать в конфигурации $q_1 V^*$ заканчивает работу в конфигурации $q_0 W^*$, где V^* и W^* – машинная запись словарных векторов V и W соответственно;

б) для любого словарного вектора V , если значение $f(V)$ не определено, то машина, начав работать в конфигурации $q_1 V^*$, никогда не остановится.

Если для словарной функции f существует машина Тьюринга, правильно ее вычисляющая, то говорят, что функция f вычислима по Тьюрингу. Две машины T_1 и T_2 называются эквивалентными, если они правильно вычисляют одну и ту же словарную функцию.

Машина Тьюринга T называется машиной с правой полулентой, если для любого правильно записанного словарного вектора $\alpha_1 * \alpha_2 * \dots * \alpha_n$ головка машины влево от первой буквы слова α_1 не забегает. Аналогично, T машина с левой полулентой, если в процессе ее работы вправо от последней буквы слова α_n головка не забегает.

Теорема. Для любой машины T существует эквивалентная ей машина как с правой полулентой, так и левой.

Эти машины обычно обозначают, как T^R – эквивалентная T машина с правой полулентой и T^L – с левой полулентой.

Как отмечалось в предыдущем параграфе, действие любого алгоритма сводится к вычислению некоторой функции натуральных аргументов. Как правило, в этом случае натуральные числа представляются в так называемом унарном коде, т.е. $A_{исх.} = \{1\}$.

Тогда натуральное число x представляется в виде $\underbrace{111\dots 1}_x$, которое удобно обозначать в

виде 1^x . Числовая функция $f(x_1, x_2, \dots, x_n)$ вычислима по Тьюрингу, если существует машина T , такая, что $q_1 1^{x_1} * 1^{x_2} * \dots * 1^{x_n} \Rightarrow q_0 1^y$, когда $f(x_1, x_2, \dots, x_n) = y$, и T работает бесконечно, начиная с $q_1 1^{x_1} * 1^{x_2} * \dots * 1^{x_n}$, если значение функции $f(x_1, x_2, \dots, x_n)$ не определено. В этом случае число 0 представляется в виде пустой ячейки λ и записывается либо в виде $q *$, либо $q * \lambda *$. При необходимости можно в $A_{исх.}$ ввести какой-либо новый символ, обозначающий ноль.

Таблица 6

$Q \backslash A$	1	*	λ
q_1	$q_2 \lambda R$	$q_0 \lambda R$	
q_2	$q_2 1 R$	$q_3 1 L$	
q_3	$q_3 1 L$		$q_0 \lambda R$

Пример 2. Во введенном ранее представлении сложить числа x и y – это значит, слово $1^x * 1^y$ переработать в слово 1^{x+y} , т.е. удалить разделитель $*$ и сдвинуть одно число к другому. Это можно осуществить с помощью следующей машины (таблица 6). Здесь команда $q_1 * \rightarrow q_0 \lambda R$ задана для случая, когда

$x = 0$, т.е. исходное слово имеет вид $*1^y$.

Пусть, например, надо найти сумму $4 + 3$. Машина Тьюринга работает следующим образом:

$$q_1 1^4 * 1^3 \rightarrow q_1 1111 * 111 \rightarrow q_2 111 * 111 \rightarrow 1q_2 11 * 111 \rightarrow 11q_2 1 * 111 \rightarrow 111q_2 * 111 \rightarrow \\ \rightarrow 11q_3 11111 \rightarrow 1q_3 111111 \rightarrow q_3 1111111 \rightarrow q_3 \lambda 1111111 \rightarrow q_0 1111111 .$$

Эту машину обычно обозначают T_+ . Она складывает два числа. Если заменим команду $q_3 \lambda \rightarrow q_0 \lambda R$ на команду $q_3 \lambda \rightarrow q_1 \lambda R$ и добавим команды $q_1 \lambda \rightarrow q_4 \lambda L$, $q_4 1 \rightarrow q_4 1 L$, $q_4 \lambda \rightarrow q_0 R$, то получим машину Тьюринга, складывающую несколько чисел. \square

Таблица 7

$Q \backslash A$	1	λ	*	0
q_1	$q_2 0 R$	$q_0 \lambda R$	$q_1 * L$	$q_1 1 L$
q_2	$q_2 1 R$	$q_3 * R$	$q_3 * R$	
q_3	$q_3 1 R$	$q_4 1 L$		
q_4	$q_4 1 L$		$q_4 * L$	$q_1 0 R$

Пример 3. Рассмотрим следующую машину (таблица 7).

Эта машина работает со словом 1^x . Например, пусть имеем слово 1^3 , тогда

$$q_1 1^3 \rightarrow q_1 111 \rightarrow 0q_2 11 \rightarrow 01q_2 1 \rightarrow 011q_2 \lambda \rightarrow 011 * q_3 \lambda \rightarrow 011 * q_4 * 1 \rightarrow 01q_4 1 * 1 \rightarrow \\ \rightarrow 0q_4 11 * 1 \rightarrow q_4 011 * 1 \rightarrow 0q_1 11 * 1 \rightarrow 00q_2 1 * 1 \rightarrow 001q_2 * 1 \rightarrow 001 * q_3 1 \rightarrow 001 * 1q_3 \lambda \rightarrow \\ \rightarrow 001 * q_4 11 \rightarrow 001q_4 * 11 \rightarrow 00q_4 1 * 11 \rightarrow 0q_4 01 * 11 \rightarrow 00q_1 1 * 11 \rightarrow 000q_2 * 11 \rightarrow \\ \rightarrow 000 * q_3 11 \rightarrow 000 * 1q_3 1 \rightarrow 000 * 11q_3 \lambda \rightarrow 000 * 1q_4 11 \rightarrow 000 * q_4 111 \rightarrow \\ \rightarrow 000q_4 * 111 \rightarrow 00q_4 0 * 111 \rightarrow 000q_1 * 111 \rightarrow 00q_1 0 * 111 \rightarrow 0q_1 01 * 11 \rightarrow \\ \rightarrow q_1 011 * 111 \rightarrow q_1 \lambda 111 * 111 \rightarrow \rightarrow q_0 111 * 111 \rightarrow q_0 1^3 * 1^3 .$$

Данная машина копирует слово 1^x , т.е. $q_1 1^x \Rightarrow q_0 1^x * 1^x$. Здесь добавляется в алфавит $A_{\text{пр}}$ дополнительный символ 0, который затем удаляется. Несколько изменив указанные команды, можно, во-первых, не только отдельно взятое слово копировать, но и копировать любой словарный вектор. Во-вторых, копию словарного вектора создавать не только рядом с исходным вектором, но и переносить ее в любое нужное место на ленте. Такая машина обычно обозначается как $T_{\text{коп}}$.

Пример 4. Пусть $Q = \{q_1, q_2, q_3, q_4\}$ – команды построенной машины $T_{\text{коп}}$, а $Q' = \{q'_1, q'_2, q'_3\}$ – команды построенной системы T_+ . В машине $T_{\text{коп}}$ команду $q_1 \lambda \rightarrow q_0 \lambda R$ заменим командой $q_1 \lambda \rightarrow q'_1 \lambda R$. Получим новую машину с набором ко-

манд $\{q_1, q_2, q_3, q_4, q'_1, q'_2, q'_3\}$. Нетрудно видеть, что новая машина вычисляет функцию $f(x) = 2x$. Она называется композицией двух машин и обозначается как $T_+(T_{\text{кон}})$.

Задачи.

51.1. В алфавите $A = \{1\}$ постройте машины Тьюринга для следующих функций:

- а) $f(x, y) = xy$; б) $f(x, y) = x^y$; в) $f(x, y) = x \div y$;
- г) $f(x, y) = \text{rest}(xy)$ и $f(x, y) = \left\lfloor \frac{x}{y} \right\rfloor$;
- д) $f(x) = \lfloor \sqrt{x} \rfloor$.

51.2. В алфавите $A = \{1, И, Л\}$, где *И* – истина, *Л* – ложь, постройте машину Тьюринга, вычисляющую следующие предикаты:

- а) $P(x, y) = И \leftrightarrow x \leq y$;
- б) $P(x, y) = И \leftrightarrow x$ делится на y ;
- в) $P(x, y) = И \leftrightarrow x$ – простое число ;
- г) $P(x, y) = И \leftrightarrow x, y$ – взаимно просты .

51.3. В алфавите $A = \{1\}$ постройте машины Тьюринга, вычисляющие простейшие числовые функции $O(x)$, $\lambda(x)$, $I^n_m(x_1, x_2, \dots, x_n)$.

51.4. Пусть машина T_1 вычисляет функцию $f_1(x, y)$, машина T_2 – функцию $f_2(x, y)$ и T – функцию $f(x, y)$ в алфавите $A = \{1\}$. Постройте машину Тьюринга, вычисляющую функцию $F(x, y) = f(f_1(x, y), f_2(x, y))$.

51.5. Пусть в алфавите $A = \{1\}$ машина T_g вычисляет функцию $g(x)$, а T_h – функцию $h(x, y, z)$. Постройте машину Тьюринга, вычисляющую функцию $f(x, y)$, которая получается из функций $g(x)$ и $h(x, y, z)$ с помощью оператора примитивной рекурсии.

51.6. Пусть в алфавите $A = \{1\}$ машина Тьюринга T_g вычисляет функцию $g(x, y)$. Постройте машину Тьюринга, вычисляющую функцию $f(x)$, которая получается из $g(x, y)$ путем минимизации по y .

Тезис Тьюринга-Черча. Функция $f(x_1, x_2, \dots, x_n)$ вычислима по Тьюрингу тогда и только тогда, когда она частично рекурсивна.

51.7. В алфавите $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ постройте машину Тьюринга, вычисляющую функции:



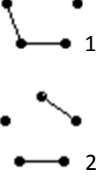
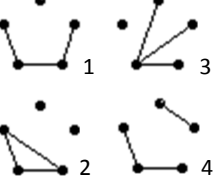
- а) $f(n) = n + 3$; б) $f(n) = 3n$; в) $f(n, m) = n + m$; г) $f(n, m) = n \div m$;
- д) постройте в этом алфавите $T_{\text{кон}}$; е) $f(n, m) = nm$.

Приложение 1. Структура графов







Для работы с графами полезно иметь по одному представителю из класса изоморфных графов $G(n, m)$, имеющих n вершин и m ребер. Если для графа с n вершинами и m ребрами существует несколько неизоморфных графов, то для них введена нумерация внизу графа.

	$m = 0$	$m = 1$	$m = 2$	$m = 3$	$m = 4$	$m = 5$	$m = 6$
$n = 1$							
$n = 2$							
$n = 3$							
$n = 4$			 	 	 	 	







$n = 5$

$m = 0$	$m = 1$	$m = 2$	$m = 3$
			



$n = 5$

$m = 4$	$m = 5$
  	  

$n = 5$

$m = 6$	$m = 7$	$m = 8$
 1	 4	
 2	 2	
 3	 3	

$n = 5$

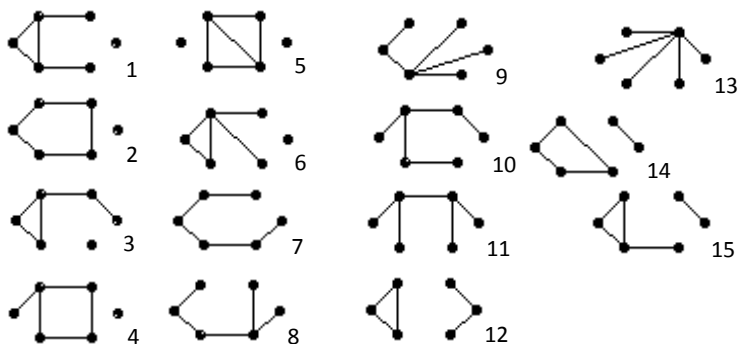
$m = 9$	$m = 10$
	

$n = 6$

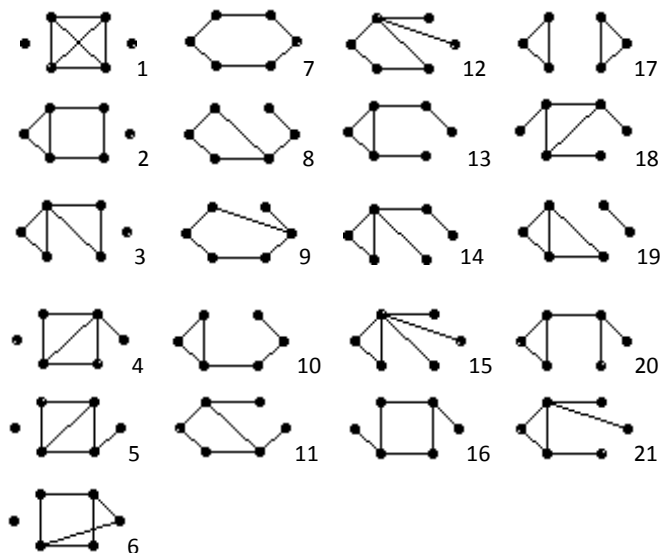
$m = 0$	$m = 1$	$m = 2$	$m = 3$

$n = 6, m = 4$

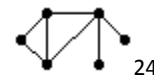
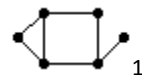
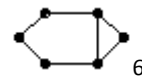
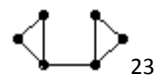
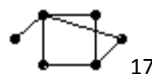
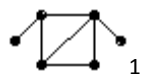
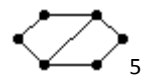
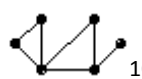
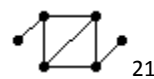
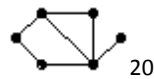
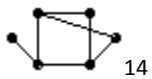
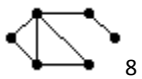
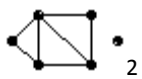
$n = 6, m = 5$



$n = 6, m = 6$



$n = 6, m = 7$



$n = 6, m = 8$



1



7



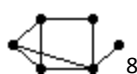
13



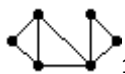
19



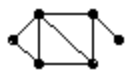
2



8



14



20



3



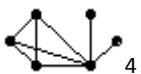
9



15



21



4



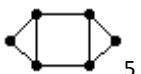
10



16



22



5



11



17



23



6



12

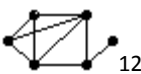
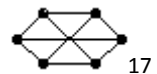
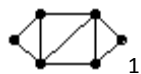
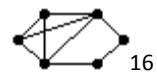
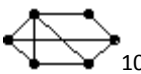
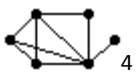
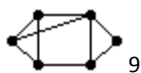
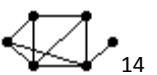
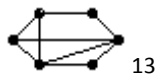
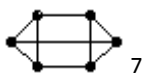


18

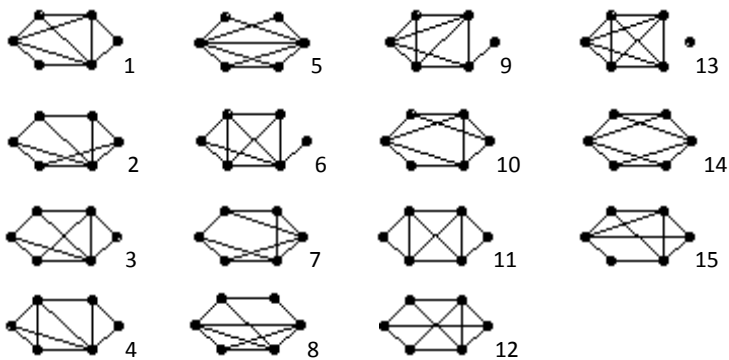


24

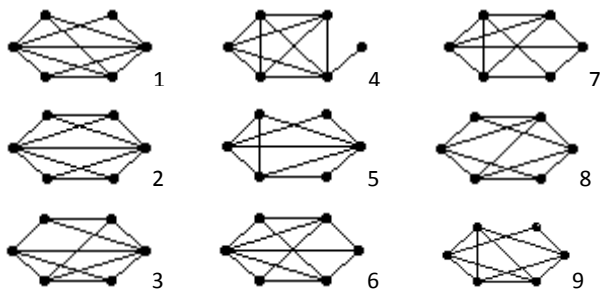
$n = 6, m = 9$

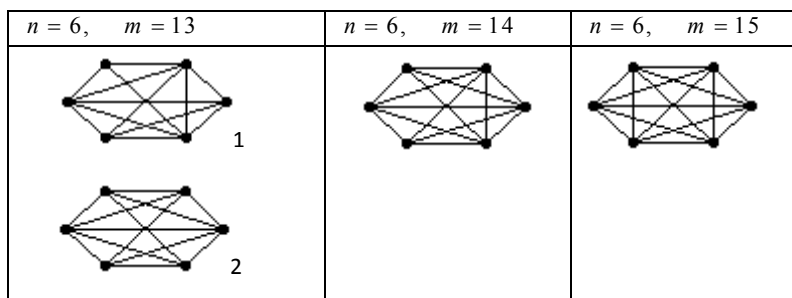
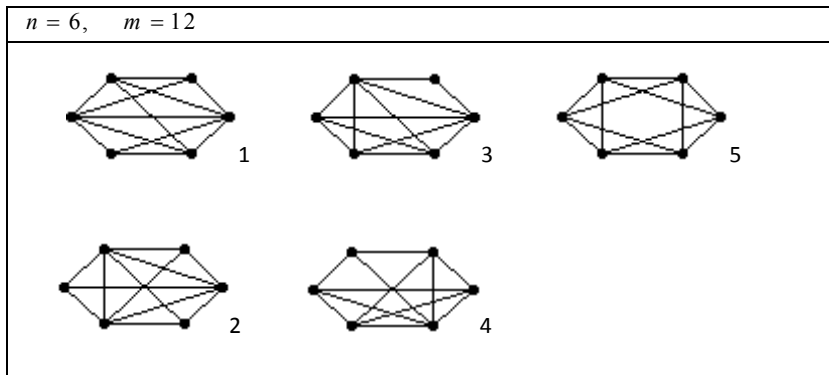


$n = 6, m = 10$



$n = 6, m = 11$





Приложение 3. Контрольная работа

Вариант № 1.

- Докажите равенство $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$.
- Сколькими способами можно составить сборную команду из 4 парней и 5 девушек, если имеется 6 парней и 7 девушек.
- Пусть A множество всех подмножеств множества $\{a, b, c, d\}$. На множестве A задано отношение $x \rho y$, если x и y содержат одинаковое количество элементов. Является ли оно отношением эквивалентности? Если является, то найдите фактор-множество A / ρ по этому отношению.
- Изобразите на плоскости множество истинности предиката $G = \{((x, y) : x^2 + y^2 < 4) \rightarrow ((x, y) : y \geq x)\}$.
- Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(f_0, f_1, f_2, f_3, 0, 0, 0, 0)$, найдите формулу.
- Для функции $((p \leftrightarrow q) \rightarrow r) \vee \bar{q}$ найдите СДНФ.
- Найдите минимальную ДНФ, если функция задана вектором значений $(0, 1, 0, 1, 1, 1, 1, 1)$.
- Найти полином Жегалкина для функции $\overline{x \rightarrow y} (y\bar{z} \vee \bar{y}z)$.
- Можно ли записать все формулы алгебры высказываний с помощью операций \leftrightarrow и \oplus ?
- Постройте эйлеров граф, содержащий 6 вершин и не менее 10 ребер. Обозначьте вершины и укажите эйлеров цикл.
- Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = 10y_{n-1} - 25y_{n-2}, y_0 = 2, y_1 = 15$.
- Для графа на рис. 1 вес ребра равен $l(i, j) = i + j$.
 - найдите остовное дерево минимального веса;
 - для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
 - найдите кратчайший маршрут от вершины 2 до вершины 7;
 - граф превратите в орграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
 - определите диаметры и центры дерева.

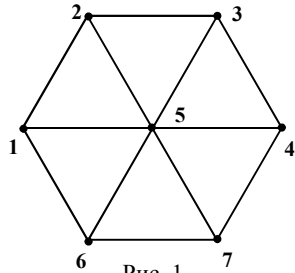


Рис. 1

- Для функции $F(A, B, C, D) = ABD \vee \bar{B}\bar{C}D \vee \bar{A}\bar{B}C\bar{D}$ найдите $\frac{\partial F}{\partial D}$.

Вариант № 2.

1. Дано множество $X = \{a, b, c, d\}$. Постройте какое-нибудь инъективное отображение $f: X \rightarrow X$.
2. Сколько существует шестизначных номеров с различными цифрами на автобусных билетах одной серии, если номер билета может начинаться с 0?
3. На множестве A упорядоченных пар неотрицательных целых чисел задано отношение $(a, b)\rho(c, d) \Leftrightarrow ad = bc$. Является ли оно отношением эквивалентности? Если является, то найдите фактор-множество A/ρ по этому отношению.
4. Изобразите на плоскости множество истинности предиката $R = \{(x, y) : y \geq |x - 2|\} \oplus \{(x, y) : y \geq 1\}$.
5. Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(f_0, f_1, f_2, f_3, 1, 1, 1, 1)$, найдите формулу.
6. Для функции $f = (\overline{X} \rightarrow Y) \wedge (Y \leftrightarrow Z)$ найдите СДНФ.
7. Найдите минимальную ДНФ, если функция задана вектором значений $(0, 1, 0, 1, 0, 1, 0, 1)$.
8. Найдите полином Жегалкина для функции $\overline{x} \vee (y \rightarrow z) \vee \overline{xz}$.
9. Булева функция $f(x_1, x_2, x_3)$ задана вектором значений $(1, 0, 1, 1, 0, 1, 1, 0)$. Принадлежит ли эта функция классам T_0, T_1, M, S ?
10. Постройте гамильтонов граф, содержащий 6 вершин. Обозначьте вершины и укажите гамильтонов цикл.
11. Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = -7y_{n-1} - 12y_{n-2}$, $y_0 = -1, y_1 = 5$.
12. Для графа на рис. 2 вес ребра равен $l(i, j) = i + j - 2$.
 - а) найдите остовное дерево минимального веса;
 - б) для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
 - в) найдите кратчайший маршрут от вершины 2 до вершины 7;
 - г) граф превратите в орграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
 - д) определите диаметры и центры дерева.
13. Для функции $F(A, B, C, D) = BCD \vee \overline{CD} \vee \overline{AB} \overline{BC} \overline{D}$ найдите $\frac{\partial F}{\partial A}$.

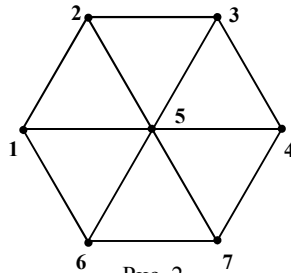


Рис. 2

Вариант № 3.

- Докажите равенство $(A \cap B) \cup B = B$.
- В группе 20 студентов. Сколькими способами можно выбрать старосту, физорга и культорга, если эти должности должны занимать разные студенты?
- На множестве $X = \{1, 2, 3, 4, 6, 8, 12, 16\}$ дано отношение $x \rho y \leftrightarrow \exists n \in Z : x = 4^n y$.
 - Докажите, что ρ отношение эквивалентности.
 - Найдите фактор-множество X/ρ .

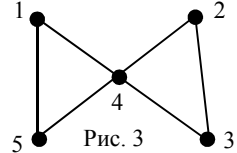


Рис. 3

- Изобразите на плоскости множество истинности предиката $G = \{((x, y) : x^2 + y^2 > 4) \rightarrow ((x, y) : y \leq x)\}$.
- Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(0, 0, 0, 0, f_0, f_1, f_2, f_3)$, найдите формулу.
- Для функции $\overline{(p \rightarrow q)} \vee (q \leftrightarrow r)$ найдите СДНФ.
- Найдите минимальную ДНФ, если функция задана вектором значений $(1, 1, 1, 1, 0, 1, 0, 1)$.
- Найти полином Жегалкина для функции $(\bar{x} \leftrightarrow y) \vee (x \rightarrow z)$.
- Можно ли записать все формулы алгебры высказываний с помощью операций \rightarrow, \vee ?
- Дан граф G (рис. 3). Постройте два гомеоморфных ему графа, которые не изоморфны графу G .
- Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = -12y_{n-1} - 36y_{n-2}, y_0 = 1, y_1 = 0$.

- Для графа на рис. 4 вес ребра равен $l(i, j) = \max(i, j)$.

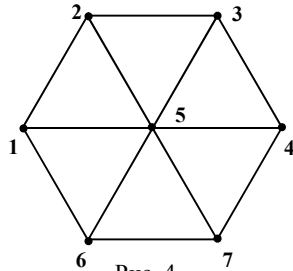


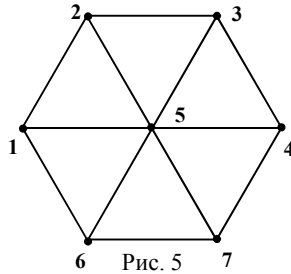
Рис. 4

- найдите остовное дерево минимального веса;
 - для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
 - найдите кратчайший маршрут от вершины 2 до вершины 7;
 - граф превратите в оргграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
 - определите диаметры и центры дерева.
- Для функции $F(A, B, C, D) = ABCD \vee \bar{A}\bar{B}\bar{C} \vee \bar{A}C\bar{D}$ найдите $\frac{\partial F}{\partial B}$.

Вариант № 4.

1. Дано множество $X = \{a, b, c, d\}$. Постройте сюръективное отображение $f: X \rightarrow X$.
2. Сколько существует автобусных шестизначных билетов, которые одинаково читаются слева направо и наоборот. Номер билета может начинаться с 0.
3. На множестве $R \setminus \{0\}$ задано отношение $x\rho y \leftrightarrow xy > 0$. Докажите, что ρ отношение эквивалентности и найдите фактор-множество X/ρ .
4. Изобразите на плоскости множество истинности предиката $G = \{(x, y) : xy < 9\} \rightarrow \{(x, y) : y \geq x + 1\}$.
5. Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(1, 1, 1, 1, f_0, f_1, f_2, f_3)$, найдите формулу.
6. Для функции $((\bar{p} \leftrightarrow q)(p \rightarrow r) \vee p)$ найдите СДНФ.
7. Найдите минимальную ДНФ, если функция задана вектором значений $(1, 1, 0, 1, 0, 1, 0, 1)$.
8. Найти полином Жегалкина для функции $(\bar{x} \leftrightarrow y)(y\bar{z} \oplus \bar{y}z)$.
9. Можно ли записать все формулы алгебры высказываний с помощью операций \neg, \leftrightarrow ?
10. Для двудольного полного графа $G_{2,5}$ найдите цикломатическое число и укажите один какой-нибудь остов этого графа.
11. Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = 7y_{n-1} + 8y_{n-2}, y_0 = -1, y_1 = 11$.
12. Для графа на рис. 5 вес ребра равен $l(i, j) = \min(i, j)$.

- а) найдите остовное дерево минимального веса;
- б) для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
- в) найдите кратчайший маршрут от вершины 2 до вершины 7;
- г) граф превратите в оргграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
- д) определите диаметры и центры дерева.



13. Для функции $F(A, B, C, D) = CD \vee \overline{B}\overline{C}D \vee A\overline{B}\overline{C}\overline{D}$ найдите $\frac{\partial F}{\partial C}$.

Вариант № 5.

- Докажите равенство $(C \cap A) \cup (B \cap C) = (A \cup B) \cap C$.
- На столе преподавателя лежит 25 экзаменационных билетов. Студент берет билет, смотрит номер и возвращает в стопку билетов. Билеты перемешиваются. Сколькими способами можно посмотреть три билета?
- Дано множество $X = \{2, 3, 4, 5\}$. На множестве $X \times X$ задано отношение $(x_1; y_1) \rho (x_2; y_2) \leftrightarrow x_1 + x_2 = y_1 + y_2$.
 - Найдите матрицу отношения.
 - Является ли это отношение рефлексивным, симметричным, транзитивным?
- Изобразите на плоскости множество истинности предиката

$$G = \{((x, y) : (x-1)(y-2) \geq 0) \wedge ((x, y) : y \geq x^2)\}.$$

- Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(f_0, f_1, 0, 0, f_2, f_3, 0, 0)$, найдите формулу.
- Для функции $f = ((Y|Z) \oplus X) \leftrightarrow X$ найдите СДНФ.
- Найдите минимальную ДНФ, если функция задана вектором значений $(1, 0, 1, 0, 1, 1, 0)$.
- Найти полином Жегалкина для функции $(\bar{x} \oplus y) (\bar{z} | \bar{y} z)$.

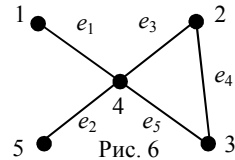


Рис. 6

- Можно ли записать все формулы алгебры высказываний с помощью операций \oplus, \downarrow ?
- Для графа (рис.6) найдите матрицу инцидентности.
- Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = 16y_{n-2}, y_0 = 3, y_1 = 16$.
- Для графа на рис. 7 вес ребра равен $l(i, j) = i \cdot j$.

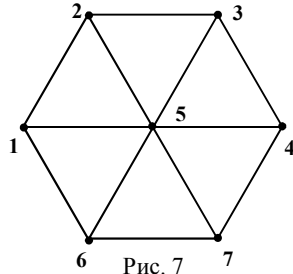


Рис. 7

- найдите остовное дерево минимального веса;
 - для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
 - найдите кратчайший маршрут от вершины 2 до вершины 7;
 - граф превратите в оргграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
 - определите диаметры и центры дерева.
- Для функции $f(x, y, z, t) = x y z \vee \bar{x} \bar{y} z \vee \bar{x} y \bar{z}$ найдите f'_x .

Вариант № 6.

1. Дано множество $X = \{a, b, c, d\}$. Постройте отображение $f : X \rightarrow X$, которое не является инъективным.
2. Сколькими способами можно обозначить вершины четырехугольника, имея в наличии 20 букв латинского алфавита, если порядок обозначения вершин не имеет значения?
3. Дано множество $X = \{2, 3, 4, 5\}$ и отношение $x\rho y \leftrightarrow (2y + x) : 3$. Найдите матрицу отношения.
4. Изобразите на плоскости множество истинности предиката $G = \{((x, y) : \ln(xy) = 0) \leftarrow ((x, y) : x^2 + y^2 < 0)\}$.
5. Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(0, 0, f_0, f_1, 0, 0, f_2, f_3)$, найдите формулу.

6. Для функции $f = (X \vee Y) \leftrightarrow Z \oplus X$ найдите СДНФ.
7. Найдите минимальную ДНФ, если функция задана вектором значений $(0, 1, 1, 1, 0, 1, 1, 1)$.
8. Найти полином Жегалкина для функции $(x \oplus yz) (\bar{z} \downarrow \bar{y}z)$.

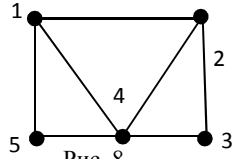


Рис. 8

9. Можно ли записать все формулы алгебры высказываний с помощью операций \leftrightarrow, \vee ?
10. Дан граф G на рис. 8. Постройте два гомеоморфных ему графа, которые не изоморфны графу G .
11. Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = 8y_{n-1} - 7y_{n-2}, y_0 = 2, y_1 = -10$.

12. Для графа на рис. 9 вес ребра равен $l(i, j) = \min(i + j, 3)$.

- а) найдите остовное дерево минимального веса;
- б) для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
- в) найдите кратчайший маршрут от вершины 2 до вершины 7;
- г) граф превратите в оргграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
- д) определите диаметры и центры дерева.

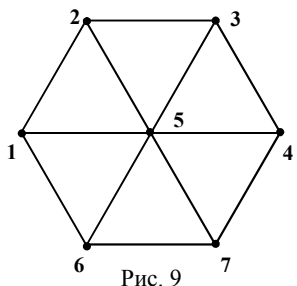


Рис. 9

13. Для функции $f(x, y, z, t) = yz \vee \bar{x}\bar{z}t \vee \bar{x}yt$ найдите f' .

Вариант №7.

- Докажите равенство $A \cap (\overline{A \cup B}) = A \cap \overline{B}$.
- В группе 25 студентов. Сколькими способами можно сформировать бригаду из трех человек для подготовки аудитории к новому учебному году?
- На множестве государств задано отношение «иметь общую границу». Является ли оно рефлексивным, симметричным или транзитивным?
- Изобразите на плоскости множество истинности предиката $G = \{(x, y) : (x - 1)^2 + (y - 1)^2 = 2\} \vee \{(x, y) : y = 2 - x\}$.
- Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(0, f_0, 0, f_1, 0, f_2, 0, f_3)$, найдите формулу.

6. Для функции $f = \overline{(X \rightarrow Y \oplus Z)} \wedge Z$ найдите СДНФ.

7. Найдите минимальную ДНФ, если функция задана вектором значений $(1, 0, 1, 1, 1, 0, 1, 1)$.

8. Найти полином Жегалкина для функции $(x \rightarrow y) \rightarrow (x \rightarrow z)$.

9. Можно ли записать все формулы алгебры высказываний с помощью операций $\vee, |$?

10. Найдите диаметр, радиус и центры графа (рис. 10).

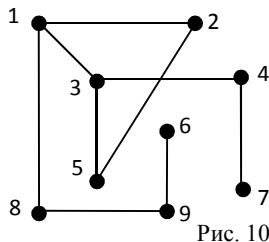


Рис. 10

11. Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = 8y_{n-1} - 7y_{n-2}$, $y_0 = 0, y_1 = 1$.

12. Для графа на рис. 11 вес ребра равен $l(i, j) = 2i + j$.

а) найдите остовное дерево минимального веса;

б) для полученного дерева найдите фундаментальную систему циклов и систему разрезов;

в) найдите кратчайший маршрут от вершины 2 до вершины 7;

г) граф превратите в орграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;

д) определите диаметры и центры дерева.

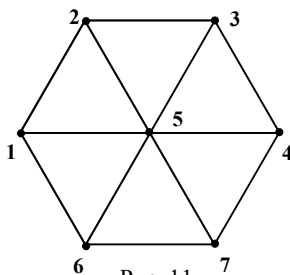


Рис. 11

13. Для функции $f(x, y, z, t) = x y z t \vee \overline{y z t} \vee \overline{x y z}$ найдите f' .

Вариант № 8.

1. Дано множество $X = \{a, b, c, d\}$. Постройте отображение $f: X \rightarrow X$, которое не является сюръективным.
2. В группе 11 парней и 9 девушек. Для участия в конкурсе группа должна выставить команду из 9 парней и 7 девушек. Сколькими способами можно сформировать команду?
3. На множестве государств задано отношение «иметь общую границу». Является ли оно рефлексивным, симметричным или транзитивным?
4. Изобразите на плоскости множество истинности предиката $G = \{(x, y) : x^2 + y^2 \geq 0\} \cap \{(x, y) : \sqrt{xy} \geq 0\}$.
5. Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(1, f_0, 1, f_1, 1, f_2, 1, f_3)$, найдите формулу.
6. Для функции $f = ((X \downarrow Y) \oplus Z) \leftrightarrow X$ найдите СДНФ.
7. Найдите минимальную ДНФ, если функция задана вектором значений $(1, 1, 0, 1, 0, 1, 1, 0)$.
8. Можно ли записать все формулы алгебры высказываний с помощью операций \oplus, \rightarrow ?
9. Найти полином Жегалкина для $\bar{x} \rightarrow (y \vee \bar{z})$.

10. Постройте граф по его матрице инцидентности $B = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

11. Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = 6y_{n-1} - 9y_{n-2}$, $y_0 = 1, y_1 = 2$.

12. Для графа на рис. 12 вес ребра равен $l(i, j) = i + 2j$.

- а) найдите остовное дерево минимального веса;
- б) для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
- в) найдите кратчайший маршрут от вершины 2 до вершины 7;
- г) граф превратите в оргграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
- д) определите диаметры и центры дерева.

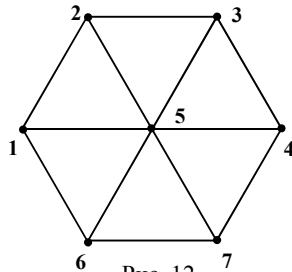


Рис. 12

13. Для функции $f(x, y, z, t) = x\bar{y}z\bar{t} \vee x\bar{y}z\bar{t} \vee \bar{x}yzt$ найдите f' .

Вариант № 9.

- Докажите равенство $(C \cup D) \cap \bar{C} = D \cap \bar{C}$.
- Решите уравнение $30P_n = P_{n+2}$.
- Дано множество $X = \{1, 2, 3, 4\}$. На множестве $X \times X$ задано отношение $(x_1; y_1) \rho (x_2; y_2) \Leftrightarrow x_1 + y_1 = x_2 + y_2$.
 - Является ли ρ отношение эквивалентности?
 - Найдите фактор-множество X/ρ , если оно существует.
- Изобразите на плоскости множество истинности предиката $G = \{(x, y) : e^{xy} > 0\} \oplus \{(x, y) : 2^x < 8\}$.
- Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(1, 1, f_0, f_1, 1, 1, f_2, f_3)$, найдите формулу.
- Для функции $f = ((X \oplus Y) \rightarrow Z) \wedge Y$ найдите СДНФ.
- Найдите минимальную ДНФ, если функция задана вектором значений $(1, 1, 0, 1, 0, 1, 1, 1)$.
- Найти полином Жегалкина для функции $(x \oplus y) \leftrightarrow (x \oplus z)$.

- Можно ли записать все формулы алгебры высказываний с помощью операций $\downarrow, \vee, \rightarrow$?
- Для графа (рис. 13) найдите диаметр, радиус и центры графа.
- Найти явное выражение для функции, заданной рекуррентным соотношением

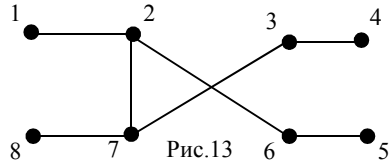


Рис. 13

$$y_n = 14y_{n-1} - 49y_{n-2}, \quad y_0 = 0, y_1 = 1.$$

- Для графа на рис. 14 вес ребра равен $l(i, j) = ij + |i - j|$.
 - найдите остовное дерево минимального веса;
 - для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
 - найдите кратчайший маршрут от вершины 2 до вершины 7;
 - граф превратите в оргграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
 - определите диаметры и центры дерева.

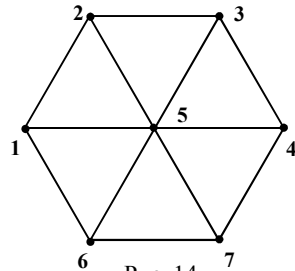


Рис. 14

- Для функции $f(x, y, z, t) = \overline{xyzt} \vee x\overline{yzt} \vee \overline{xyzt}$ найдите f'_x .

Вариант № 10.

1. Дано множество $X = \{a, b, c, d\}$. Сколько существует биективных отображение множества X в себя?
2. Решите уравнение $5C_n^3 = C_{n+2}^4$.
3. На множестве последовательностей, членами которых могут быть 0 или 1, определено отношение $(a_1 a_2 a_3) \rho (b_1 b_2 b_3) \leftrightarrow a_i = b_i$ для нечетных i .
 - а) Докажите, что ρ отношение эквивалентности.
 - б) Найдите фактор-множество X/ρ .
4. Изобразите на плоскости множество истинности предиката $G = \{((x, y) : (x - 2)(y - 1) \leq 0) \wedge ((x, y) : |x - 1| \leq 1)\}$.
5. Булева функция от двух переменных задана формулой $f(x, y)$ и имеет вектор значений (f_0, f_1, f_2, f_3) . Для функции от трех переменных, заданной вектором значений $(f_0, 1, f_1, 1, f_2, 1, f_3, 1)$, найдите формулу.
6. Для функции $f = ((X \oplus Z) \vee Y) \wedge Z$ найдите СДНФ.
7. Найдите минимальную ДНФ, если функция задана вектором значений $(0, 1, 1, 1, 0, 1, 1, 1)$.
8. Найдите полином Жегалкина для функции $(x \leftrightarrow y) \oplus (x \leftrightarrow z)$.
9. Является ли полной система функций \vee, \leftrightarrow .

10. Постройте орграф по его матрице инцидентности $B = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

11. Найти явное выражение для функции, заданной рекуррентным соотношением $y_n = -14y_{n-1} - 49y_{n-2}$, $y_0 = 1, y_1 = 0$.
12. Для графа на рис. 15 вес ребра равен $l(i, j) = i + |i - j|$.

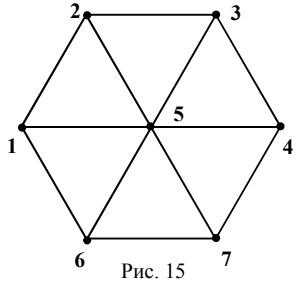


Рис. 15

- а) найдите остовное дерево минимального веса;
- б) для полученного дерева найдите фундаментальную систему циклов и систему разрезов;
- в) найдите кратчайший маршрут от вершины 2 до вершины 7;
- г) граф превратите в орграф, заменив каждое ребро с весом дугой, направленной от вершины с меньшим номером к вершине с большим номером. Найдите максимальную пропускную способность сети от вершины 1 к вершине 7;
- д) определите диаметры и центры дерева.
13. Для функции $f(x, y, z, t) = x y z \bar{t} \vee \bar{x} y z \bar{t} \vee x y z \bar{t}$ найдите f'_y .

Приложение 4. Несколько компьютерных программ

Справочный материал об операторах в Visual Basic 6

Способы задания цветов:

- QBColor (0) или vbBlack – черный;
- QBColor (1) – темно-синий;
- QBColor (2) – темно-зеленый;
- QBColor (3) – темно-голубой;
- QBColor (4) – темно-красный;
- QBColor (5) – темно-сиреневый;
- QBColor (6) – коричневый;
- QBColor (7) – светло-серый;
- QBColor (8) – темно-серый;
- QBColor (9) или vbBlue – синий;
- QBColor (10) или vbGreen – зеленый;
- QBColor (11) или vbCyan – голубой;
- QBColor (12) или vbRed – красный;
- QBColor (13) или vbMagenta – сиреневый;
- QBColor (14) или vbYellow – желтый;
- QBColor (15) или vbWhite – белый.

Значения свойств DrawStyle и DrawWidth:

- DrawStyle = 0 – сплошная заливка;
- DrawStyle = 1 – штриховая линия;
- DrawStyle = 2 – пунктирная линия;
- DrawStyle = 3 - штрихпунктирная линия;
- DrawStyle = 4 - штрих двойной пунктир;
- DrawStyle = 5 – прозрачная заливка линии.
- DrawWidth = i – толщина линии.

По умолчанию DrawWidth = 1

CLS – оператор, очищающий экран.

Form1.Scale (0, Form1.Height)-(Form1.Width, 0) – оператор перехода на экране компьютера к декартовой системе координат.

Символ	Значение	Символ	Значение
+	сложение	COS (x)	cos x
-	вычитание	SIN (x)	sin x
*	умножение	TAN (x)	tg x
/	деление	ATN (x)	arc tg x
\	целочисленное деление	EXP (x)	e^x
^	возведение в степень	LOG (x)	ln x
MOD	нахождение остатка при делении	SQR (x)	\sqrt{x}
		ABS (x)	$ x $

$\pi = 4 * \text{ATN}(1)$ – вычисление числа π в программе.

LINE $(x_1, y_1) - (x_2, y_2)$, ..., B | BF , & $H000$
коорд. противоположных вершин цвет прямоугольник закрашка прямоугольника штрих – линия

- оператор рисования отрезка (прямоугольника при указании B)

CIRCLE (x, y), ..., ..., ..., ..., ..., \dots - оператор рисо-
координаты центра радиус цвет дуги начало дуги конец дуги коэффициент сжатия

вания окружности (дуги эллипса при указании начала и конца дуги).

PSET (x, y) – оператор, рисующий точку (x, y) на экране.

PSet (x, y), **QBColor**(15): **Print** "b="; **Int**(b) – оператор, устанавливающий точку белым цветом с координатами x, y на экране компьютера и оператор, печатающий рядом целую часть значения переменной b .

Print s – оператор печати значения переменной s .

FOR $i = 1$ **TO** 10 **STEP** 0.1 – начинается цикл

.....

NEXT i – закрывается цикл

- оператор цикла по переменной i , принимающей значение от 0 до 10 с шагом – изменения 0,1.

IF $x > 0$ **THEN** $a = \text{SQR}(x)$

ELSE

PRINT *значение квадратного корня не существует*

- условный оператор, который при выполнении условия $x > 0$ вычисляет значение квадратного корня из неотрицательного числа или сообщает о невозможности вычисления квадратного корня из отрицательного числа.

Print Screen (клавиша на клавиатуре) – копирование содержания экранного окна в буфер.

Dim M(0 To 7) As Integer – объявление одномерного целочисленного массива, изменяющегося от 0 до 7 включительно.

Dim M(8,9) – объявление двумерного массива.

Dim A(1 To 10, -5 To 4) As Double - объявление двумерного массива десятичных чисел двойной точности.

Private Sub ... определение локальной процедуры

End Sub

1. Программа поиска натуральных чисел, удовлетворяющих нескольким условиям делимости (§ 1):

Private Sub Command1_Click()

$n = 200$; $k = 0$

For $i = 1$ **To** n

If ($i \bmod 2 = 0$) **Or** ($i \bmod 3 = 0$) **Or** ($i \bmod 5 = 0$) **Then** $s = s + 1$ **Else** $k = k + 1$

Next i

Print k

End Sub. □

2. Программа для композиции функций, заданных строками (§ 8):

Private Sub Command1_Click()

Dim $f(0 \text{ To } 7)$ 'массив для функции f : **Dim** $g(0 \text{ To } 7)$: **Dim** $e(0 \text{ To } 7)$

Dim $h(0 \text{ To } 7)$: **Dim** $fk(0 \text{ To } 7)$ 'массив для композиции функций

(Задайте свои функции строками значений)

```
f(0) = 1: f(1) = 0: f(2) = 0: f(3) = 1: f(4) = 0: f(5) = 0: f(6) = 1: f(7) = 0
g(0) = 1: g(1) = 1: g(2) = 1: g(3) = 1: g(4) = 0: g(5) = 0: g(6) = 0: g(7) = 0
h(0) = 0: h(1) = 0: h(2) = 1: h(3) = 1: h(4) = 0: h(5) = 1: h(6) = 0: h(7) = 1
For x = 0 To 1 'вложенный цикл для перечисления наборов переменных
For y = 0 To 1 'и вычисления значений функции на этих наборах
For z = 0 To 1
e(i) = z 'заполнение массива функции
k = 4 * g(i) + 2 * e(i) + h(i) 'десятичная нумерация для наборов значений
                               внутренних функций
fk(i) = f(k) 'вычисление значений композиции функций
i = i + 1 'десятичная нумерация наборов переменных
Next z, y, x 'закрытие трех циклов
Print "fk= "; fk(0); fk(1); fk(2); fk(3); fk(4); fk(5); fk(6); fk(7) 'печать fk(i)
Print "f= "; f(0); f(1); f(2); f(3); f(4); f(5); f(6); f(7) 'печать f(i)
Print "g= "; g(0); g(1); g(2); g(3); g(4); g(5); g(6); g(7) 'печать g(i)
Print "e= "; e(0); e(1); e(2); e(3); e(4); e(5); e(6); e(7) 'печать e(i)
Print "h= "; h(0); h(1); h(2); h(3); h(4); h(5); h(6); h(7) 'печать h(i)
Print "x= "; 0; 0; 0; 0; 1; 1; 1; 1 'печать наборов переменных в столбец
Print "y= "; 0; 0; 1; 1; 0; 0; 1; 1: Print "z= "; 0; 1; 0; 1; 0; 1; 0; 1: End Sub
```

3. Программа, которая для введенной функции от трех переменных выдает последовательности $(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)$ и $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)_{\oplus}$ (§ 10):

```
Private Sub Command1_Click()
Dim f(0 To 7) 'массив для коэффициентов разложения в СДНФ
Dim a(0 To 7) 'массив для коэффициентов полинома Жегалкина
For x = 0 To 1 'вложенный цикл для перечисления наборов переменных
For y = 0 To 1 'и вычисления значений функции на этих наборах
For z = 0 To 1
i = 4 * x + 2 * y + z 'десятичная нумерация для наборов переменных
f(i) = (x And y) Or z 'данная функция Замените на свою функцию
Next z, y, x 'одновременное закрытие трех циклов
a(0) = f(0) 'вычисление коэффициентов полинома Жегалкина
a(3) = f(1) Xor f(0): a(2) = f(2) Xor f(0): a(1) = f(4) Xor f(0)
a(6) = f(3) Xor f(2) Xor f(1) Xor f(0): a(5) = f(5) Xor f(4) Xor f(1) Xor f(0)
a(4) = f(6) Xor f(4) Xor f(2) Xor f(0)
a(7) = f(7) Xor f(6) Xor f(5) Xor f(4) Xor f(3) Xor f(2) Xor f(1) Xor f(0)
Print "x="; 0; 0; 0; 0; 1; 1; 1; 1 'печать наборов переменных в столбец
Print "y="; 0; 0; 1; 1; 0; 0; 1; 1: Print "z="; 0; 1; 0; 1; 0; 1; 0; 1
Print
Print "f="; f(0); f(1); f(2); f(3); f(4); f(5); f(6); f(7) 'печать f(i)
Print "a="; a(0); a(1); a(2); a(3); a(4); a(5); a(6); a(7) 'печать a(i)
End Sub
```

4. Программа “Класс S - 2 переменные” для перечисления самодвойственных функций от двух переменных (§ 14):

```
Private Sub Command1_Click()
```



```

Print
For r3 = 0 To 1: For r2 = 0 To 1: For r1 = 0 To 1: For r0 = 0 To 1
    nf = r0 * 2 ^ 3 + r1 * 2 ^ 2 + r2 * 2 + r3
    M(0) = r0: M(1) = r1: M(2) = r2: M(3) = r3
For X = 0 To 1: For Y = 0 To 1
    If ((M(1) - M(0)) >= 0 And (M(3) - M(1)) >= 0 And (M(2) - M(0)) >= 0 And
(M(3) - M(2)) >= 0) Then k = k + 1 Else GoTo 1
    Next Y: Next X
    Print r0; r1; r2; r3; "..."; "f"; nf
1
Next r0: Next r1: Next r2: Next r3
Print
Print 0; 0; 1; 1; "..."; "X": Print 0; 1; 0; 1; "..."; "Y"
End Sub

```

7. Программа “Класс - **Sim**” определения всех булевых симметричных функций от двух аргументов (§ 17):

```

Private Sub Command1_Click()
Dim m(0 To 3)
k = 0
Print:
For r3 = 0 To 1: For r2 = 0 To 1: For r1 = 0 To 1: For r0 = 0 To 1
    nf = r0 * 2 ^ 3 + r1 * 2 ^ 2 + r2 * 2 + r3
    m(0) = r0: m(1) = r1: m(2) = r2: m(3) = r3
For X = 0 To 1: For Y = 0 To 1
    If m(1) = m(2) Then k = k + 1 Else GoTo 1
    Next Y: Next X
    Print r0; r1; r2; r3; "..."; "f"; nf
1
Next r0: Next r1: Next r2: Next r3
Print
Print 0; 0; 1; 1; "..."; "X": Print 0; 1; 0; 1; "..."; "Y"
End Sub

```

8. Программа для определения всех симметричных функций от трех аргументов. В программе предусмотрите подсчет количества таких функций и вывод на печать этого количества функций (§ 17):

```

Private Sub Command1_Click()
Dim M(0 To 7)
s = 0: k = 0
For r0 = 0 To 1: For r1 = 0 To 1: For r2 = 0 To 1: For r3 = 0 To 1
For r4 = 0 To 1: For r5 = 0 To 1: For r6 = 0 To 1: For r7 = 0 To 1
    nf = r0 * 2 ^ 7 + r1 * 2 ^ 6 + r2 * 2 ^ 5 + r3 * 2 ^ 4 + r4 * 2 ^ 3 + r5 * 2 ^ 2 + r6 *
2 + r7
    M(0) = r0: M(1) = r1: M(2) = r2: M(3) = r3
    M(4) = r4: M(5) = r5: M(6) = r6: M(7) = r7
For X = 0 To 1: For Y = 0 To 1: For Z = 0 To 1

```

```

    If ((M(1) = M(2)) And (M(2) = M(4)) And (M(3) = M(5)) And (M(5) = M(6)))
Then k = k + 1 Else GoTo 1
Next Z, Y, X
s = s + 1
Print r0; r1; r2; r3; r4; r5; r6; r7; ".."; "f"; nf
1
Next r7, r6, r5, r4, r3, r2, r1, r0
Print
Print 0; 0; 0; 0; 1; 1; 1; 1; ".."; "X": Print 0; 0; 1; 1; 0; 0; 1; 1; ".."; "Y"
Print 0; 1; 0; 1; 0; 1; 0; 1; ".."; "Z": Print "s"; "="; s 'число функций
End Sub

```

9. Программа **“Класс К – 2 переменные”** определения всех булевых функций от двух аргументов, удовлетворяющих условию коммутативности диаграммы (§ 17):

```

Private Sub Command1_Click()
Dim M(0 To 3)
k = 0
For r3 = 0 To 1: For r2 = 0 To 1: For r1 = 0 To 1: For r0 = 0 To 1
nf = r0 * 2 ^ 3 + r1 * 2 ^ 2 + r2 * 2 + r3
M(0) = r0: M(1) = r1: M(2) = r2: M(3) = r3
For A = 0 To 1: For B = 0 To 1: For C = 0 To 1: For D = 0 To 1
f1 = M(2 * A + B): f2 = M(2 * C + D)
fp = M(2 * f1 + f2): f3 = M(2 * A + C)
f4 = M(2 * B + D): fl = M(2 * f3 + f4)
If fp = fl Then k = k + 1 Else GoTo 1
Next D: Next C: Next B: Next A
Print r0; r1; r2; r3; ".."; "f"; nf
1
Next r0: Next r1: Next r2: Next r3
Print
Print 0; 0; 1; 1; 1; 1; 1; 1; ".."; "X": Print 0; 1; 0; 1; 1; 1; 1; 1; ".."; "Y"
End Sub

```

10. Программа **“Cezar”** для шифрования сообщения шифром Цезаря (§ 38):

```

Private Sub Command1_Click()
Dim s, ss, res As String: Dim i As Byte
s = Text1.Text: res = ""
For i = 1 To Len(s)
ss = Mid(s, i, 1): Select Case ss
Case "A" To "W", "a" To "w"
ss = Chr(Asc(ss) + 3): res = res & ss
Case "X" To "Z", "x" To "z"
ss = Chr(Asc(ss) - 23): res = res & ss
End Select
Next i
Text2.Text = res: End Sub

```

Приложение 5. Основные обозначения

\exists – существует, некоторый;	$A \times B$ – произведение множеств A и B ;
\forall – любой, произвольный;	$\dot{\vdots}$ – кратно, делится без остатка;
$n!$ – факториал числа n ;	\vdash – такой, что;
\in – принадлежит;	\vee – дизъюнкция (читается “или”);
\notin – не принадлежит;	\wedge – конъюнкция (читается “и”);
$ A $ – мощность множества A ;	\oplus – сложение по модулю два;
\emptyset – пустое множество;	\downarrow – стрелка Пирса;
\subset – содержится;	$ $ – штрих Шеффера;
\cup – объединение (читается или);	\rightarrow – следует;
\cap – пересечение (читается и);	
НОД (a, b) или (a, b) – наибольший общий делитель чисел a и b ;	
НОК (a, b) или $[a, b]$ – наименьшее общее кратное;	
A_n^k – число размещений из n элементов по k элементов;	
C_n^k – число сочетаний из n элементов по k элементов;	
P_n – число перестановок из n элементов;	
\bar{A} – отрицание высказывания A (читается “не A ”);	
\leftrightarrow – тогда и только тогда, если и только если, эквивалентно;	
ДНФ – дизъюнктивная нормальная форма;	
СДНФ – совершенная дизъюнктивная нормальная форма;	
КНФ – конъюнктивная нормальная форма;	
СКНФ – совершенная конъюнктивная нормальная форма;	
$(f_0, f_1, \dots, f_{2^n-1})$ – упорядоченный набор значений булевой функции	
$\alpha < \beta$ – набор α предшествует набору β ;	
$(g_0, g_1, \dots, g_{2^n-1})_{\oplus}$ – упорядоченный набор коэффициентов полинома Жегалкина;	
$G(V, E)$ – граф G , имеющий множество вершин V и множество ребер E ;	
$\deg(v_i)$ – степень вершины v_i ;	
K_n – полный граф с n вершинами;	
G_{n_1, n_2} – двудольный граф, одно множество вершин которого содержит n_1 вершин,	
а второе множество содержит n_2 вершин;	
K_{n_1, n_2} – полный двудольный граф, одно множество вершин которого содержит n_1	
вершин, а второе множество содержит n_2 вершин;	
$\chi(G)$ – эйлерова характеристика графа G ;	
$\gamma(G)$ – хроматическое число графа G ;	
\square – окончание решения примера;	
СИ – материал для самостоятельного исследования.	

§ 1. 1.10. Ассоциативное свойство не выполняется для произвольных множеств A, B, C . Например, для $A = \{a, b, c\}$, $B = C = \{c\}$, $A \setminus (B \setminus C) = \{a, b, c\}$ и $(A \setminus B) \setminus C = \{a, b\}$. **1.15.** д) $A \setminus B = \overline{A} \uparrow B$, $A \cap B = (A \uparrow A) \uparrow (B \uparrow B)$. **1.18.** 29. **1.20.**

а) $S_n = \frac{n}{2n+1}$; б) $S_n = \frac{n}{3n+1}$. **1.32.** $f: R \rightarrow [0; 1]$, $f(x) = \sin x$, $A = [0; \pi/2]$, $B = [2\pi; 2\pi + \pi/2]$, $f(A) = [0; 1]$, $f(B) = [0; 1]$, $f(A \cap B) = \emptyset$, $f(A) \cap f(B) = [0; 1]$.

1.33. а) Для следующего примера равенство не выполняется. $X = \{a, b, c\}$, $Y = \{d, e\}$, $f(a) = d = f(b)$, $f(c) = e$, $A = \{b, c\}$, $f(A) = \{d, e\}$, $f^{-1}(f(A)) = X \neq A$;

б) Для следующего примера равенство не выполняется. $X = \{a, b\}$, $Y = \{c, d, e\}$, $f(a) = d$, $f(b) = e$, $B = \{c, d, e\}$, $f^{-1}(B) = \{a, b\}$, $f(f^{-1}(A)) = \{d, e\} \neq B$. **1.36.** а)

Утверждение справедливо при $n=1$. Пусть справедливо $(10^k + 18k - 1):27$ при $n=k$, тогда $10^{k+1} + 18(k+1) - 1 = (10^k + 18k - 1)10 - 162k + 27$. Выражение $10^k + 18k - 1$ делится на 27 по предположению. Выражение $-162k + 27$ также делится на 27, следовательно $(10^{k+1} + 18(k+1) - 1):27$.

§ 2. 2.1. $25 \cdot 24 \cdot 23 = 13800$. **2.2.** $C_{25}^3 = 2300$. **2.3.** $C_{25}^1 C_{24}^2$. **2.4.** а) Пусть $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_m\}$. Элементу x_1 можно поставить в соответствие любой элемент из множества Y , поэтому первое действие по определению образа $f(x_1)$ можно выполнить m способами. Аналогично для остальных элементов множества X . По правилу произведения получаем m^n т.е. общее число отображений равно $|Y|^{|X|}$; б) число биективных отображений равно $n!$. **2.5.** A_{n-1}^{k-1} . **2.6.**

$1 + C_4^1 + C_4^2 + C_4^3 + C_4^4$. **2.7.** $1 + C_6^1 + C_6^2 + C_6^3 + C_6^4 + C_6^5 + C_6^6$. **2.9.** $32 \cdot 31^2$. **2.14.** 20.

2.15. 2^6 . **2.17.** Первую монету можно положить в любой из трех карманов. Вторую монету можно положить аналогично и т.д. Всего 3^6 способов. **2.20.** 1000.

Типографский станок, изменяя нумерацию билетов, печатает также номер 000000. **2.26.** б) $5!$. в) $3!2!$. **2.28.** При перестановке двух одинаковых букв значение слова не изменяется, поэтому получаем $\frac{7!}{2!3!}$.

2.29. Сумма чисел будет четной, если все слагаемые четные или одно слагаемое четное и два слагаемых нечетные. Из пятнадцати четных чисел три числа можно выбрать C_{15}^3 способами, так как порядок слагаемых не учитывается. Из пятнадцати нечетных чисел два числа можно выбрать C_{15}^2 способами и после каждого такого выбора необходимо выбрать из 15 четных чисел по одному четному числу C_{15}^1 способами. По правилу произведения число выборок, содержащих два нечетных числа и одно четное число, равно $C_{15}^2 C_{15}^1$. Применяя правило суммы, найдем общее число выборок $C_{15}^3 + C_{15}^2 C_{15}^1 = 2030$. **2.32.** а) $C_{10}^3 = 120$; б) Первым действием определим семь, из

которых будем выбирать 3 человека для комиссии, т.е. $C_5^3 = 10$ способов. После этого в каждой из семей можно выбрать представителя – мужа или жену. Значит, второе действие можно выполнить $2 \cdot 2 \cdot 2 = 8$ способами. По правилу произведения получаем $10 \cdot 8 = 80$ способов составить комиссии. **2.36.** Рассмотрим множество всех дам с одним кольцом. Одно кольцо может находиться на любом из 10 пальцев, т.е. число дам с одним кольцом равно C_{10}^1 , аналогично число дам с двумя кольцами – C_{10}^2 . Максимальное число дам равно $C_{10}^0 + C_{10}^1 + \dots + C_{10}^{10} = 1024$.

2.37. $C(8; 3, 2, 2, 1) = 1680$. **2.38.** $C(6; 2, 2, 2) = 90$. **2.41.** 1024 000. **2.42.** $C_5^2 \cdot 1024000$.

2.43. $2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 126$. **2.46.** Первое действие – отбор стандартных деталей для выборки. Существует C_n^v способов выбрать v стандартных деталей для выборки из n стандартных деталей в партии. Второе действие – отбор нестандартных деталей. Существует C_{N-n}^{V-v} способов выбрать $V-v$ нестандартных деталей для выборки из $N-n$ стандартных деталей в партии. По правилу произведения получаем $C_n^v C_{N-n}^{V-v}$. **2.49.** Биномиальный коэффициент третьего члена разложения равен $C_n^2 = 105$, следовательно, $n = 15$. Двенадцатый член разложения

бинома равен $-C_{15}^{11} \left(\frac{1}{\sqrt{3x}} \right)^4 (2x)^{11}$. **2.54.** б) $x^3 + y^3 + z^3 + 3x^2y + 3x^2z + 3y^2z + 3y^2x + 3z^2x + 3z^2y + 6xyz$. **2.55.** а) После вычислений и сокращений вынести за

скобки n ; б) пусть $f(x) = (1+x)^n = \sum_{k=0}^n C_n^k x^k$, тогда $\sum_{k=1}^n k^2 C_n^k = (x f'(x))' \Big|_{x=1} = n(n+1)2^{n-2}$. **2.58.** 210. **2.59.** 7560.

§ 3. **3.1.** а) $u_n = (2-n)3^n$; б) $u_n = (3-2n)(-1)^n$; в) $u_n = 3^n - 2^n$; г) $u_n = 1$; д) $u_n = n+1$. **3.2.** $a_k = 2a_{k-1} + 2$, где $k \geq 1$, $b_0 = 1$, $a_k = 3 \cdot 2^k - 2$, $c_k = 4a_k - 4$, где $k \geq 1$, $c_k = 12(2^k - 1)$. **3.3.** $a_k = 2 \cdot 3^k - 1$.

§ 4. **4.38.** Подмножества $A = \{a, b\}$, $C = \{c, f\}$ не являются сравнимыми.

4.40. Рис. 16. **4.48.** Для первого бинарного отношения $x\rho_1y$, если прямая x совпадает с прямой y или параллельна прямой y . Для второго бинарного отношения $x\rho_2y$, если прямая x перпендикулярна прямой y .

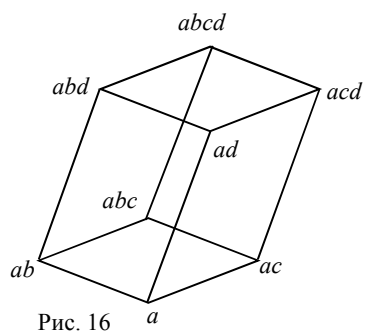


Рис. 16

§ 5. **5.5.** $X = \{b, d, e, f, g, h\}$. 5.7. Пусть 0_1 и 0_2 – две нижние границы, удовлетворяющие условиям $a \vee 0_1 = a$, $a \vee 0_2 = a$ для любого элемента a булевой

алгебры, тогда $0_1 = 0_1 \vee 0_2 = 0_2 \vee 0_1 = 0_2$. Следовательно, $0_1 = 0_2$. **5.18.** Из условия а) получаем условие б): $a \vee b = (a \wedge b) \vee b = b \vee (a \wedge b) = b \vee (b \wedge a) = b \vee b = b$.

§ 6. 6.13 з) $\overline{XY \vee \overline{XY}}(X \vee \overline{Y}) = \overline{XY} \overline{\overline{XY}}(X \vee \overline{Y}) = (\overline{X} \vee \overline{Y})(X \vee \overline{Y})(X \vee \overline{Y}) =$
 $= (\overline{X} \vee \overline{Y})(X \vee \overline{Y})(X \vee Y) = \overline{Y}(\overline{X} \vee X)(X \vee Y) = \overline{Y}(X \vee Y) = \overline{XY}$; и) $\overline{(X \vee Y)} \rightarrow \overline{Y \vee Z} =$
 $= \overline{\overline{X \vee Y} \vee \overline{Y \vee Z}} = \overline{(X \vee Y)(Y \vee Z)} = \overline{Y \vee XZ}$. **6.18.** а) $(A \vee B)(BA) = ABA \vee BBA =$

$= AB \vee AB = AB$; б) $(P \rightarrow Q) \rightarrow (PR) = (\overline{P} \vee Q) \rightarrow PR = \overline{\overline{P} \vee Q} \vee PR = P(\overline{Q} \vee R)$;

в) $(\overline{AB})(B \vee C)(A \vee (BC)) = (\overline{AB} \vee \overline{ABC})(A \vee (BC)) = \overline{AB}(A \vee (BC)) = \overline{ABC}$;

г) $(\overline{XY} \vee \overline{XYZ})(\overline{X} \vee \overline{XY} \vee \overline{Y}) = (\overline{X} \vee \overline{Y})(\overline{X} \vee (\overline{XY} \vee \overline{Y})) = (\overline{X} \vee \overline{Y})(\overline{X} \vee (\overline{X} \vee \overline{Y}) \vee \overline{Y}) =$
 $= (\overline{X} \vee \overline{Y})(\overline{X} \vee \overline{XY}) = (\overline{X} \vee \overline{Y})\overline{X} = \overline{X}$; д) 1. х) $A \leftrightarrow B$; и) $A \downarrow B$; л) $A | B$.

6.19. а) $(A \rightarrow B)(A \rightarrow \overline{B}) = (\overline{A} \vee B)(\overline{A} \vee \overline{B}) = \overline{A} \vee (B\overline{B}) = \overline{A}$.

§ 8. 8.12. ж) (00000000); з) (00011100). **8.18.** ж) $(x|(y|y))|(y|(x|x)) =$
 $= (x|y)|(y|x) = \overline{xy} | \overline{yx} = \overline{\overline{xy} \vee \overline{yx}} = \overline{xy \vee yx} = x \oplus y$. **8.19.** ж) $x \downarrow y = \overline{x \vee y} = \overline{x} \overline{y} = \overline{x} \overline{y}$.

8.20. г) $(x \downarrow y) \downarrow (x \downarrow y) = \overline{x \downarrow y} = \overline{\overline{x \vee y}} = x \vee y$. **8.22.** в) $F_1 = f(\overline{xy}, y) = \overline{xy} \vee y = 1$,
 $F_2 = f(x, \overline{xy}) = x \vee \overline{xy} = 1$, $F_3 = f(\overline{xy}, \overline{xy}) = \overline{xy}$, $F_4 = g(x \vee y, y) = \overline{(x \vee y)y} = \overline{y}$,
 $F_5 = g(x, x \vee y) = \overline{x(x \vee y)} = \overline{x \vee x \vee y} = \overline{x \vee (xy)} = \overline{x}$, $F_6 = \overline{(x \vee y)(x \vee y)} = \overline{x \vee y} = \overline{x} \overline{y}$,

8.23. а) $0, 1, x, y, x \vee y, xy$. **8.24.** $f = \overline{(x \rightarrow z)(y \rightarrow z)} \vee ((x \vee y) \rightarrow z) =$
 $= \overline{(xz) \vee (yz)} \vee \overline{(x \vee y \vee z)} = \overline{((x \vee y)z)} \vee \overline{(x \vee y \vee z)} = \overline{x \vee y \vee z} \vee \overline{(x \vee y \vee z)} = 1$.

§ 9. 9.5. Для рисунка 20 задачи получаем
 $((x \vee y)xy) \vee \overline{x \vee y} = (\overline{xy} \vee yx) \vee (\overline{xy}) = \overline{xy} \vee \overline{xy} = x \leftrightarrow y$.

9.13. а) $(x \vee y) \rightarrow (\overline{z} \sim y) = \overline{x \vee y} \vee ((\overline{zy}) \vee (zy)) = (x \vee y)(\overline{zy}) \vee (zy) = (x \vee y)((\overline{zy})(zy)) =$
 $= (x \vee y)((\overline{z \vee y})(\overline{z \vee y})) = (x \vee y)(\overline{z \vee y})(\overline{z \vee y}) = (xz \vee xy \vee yz \vee y\overline{y})(\overline{z \vee y}) =$
 $= xyz \vee x\overline{y}\overline{z} \vee xyz \vee x\overline{y}\overline{z}$, $f = (00011001)$; б) $(\overline{x \leftrightarrow y} \rightarrow \overline{z})y = (\overline{\overline{xy} \vee \overline{xy}} \rightarrow \overline{z})y =$
 $= ((xy \vee \overline{xy}) \vee \overline{z})y = xyz \vee xy\overline{z} \vee \overline{xy}\overline{z}$. $f = (00100011)$. **9.14.** а) $xz \vee xy \vee \overline{yz} =$
 $= x(y \vee y)z \vee xy \vee \overline{yz} = xyz \vee x\overline{y}z \vee xy \vee \overline{yz} = xyz \vee xy \vee x\overline{y}z \vee \overline{yz} = xy \vee \overline{yz}$.

г) $xy \vee xz \vee \overline{yz} = x(y \vee z) \vee \overline{yz} = x(y \vee z) \vee \overline{y \vee z} = x \vee y \vee z = x \vee \overline{yz}$. **9.15. а)** Рассмотрим двоичный набор $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_{2k+1})$, где $\alpha_1 + \alpha_2 + \dots + \alpha_{2k+1} \geq k+1$, на кото-

ром мажоритарная функция принимает значение 1, т.е. $Maj_{2k+1}(\alpha_1, \alpha_2, \dots, \alpha_{2k+1})=1$. Каждому такому набору однозначно соответствует набор $\bar{\alpha} = (\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_{2k+1})$, $\bar{\alpha}_1 + \bar{\alpha}_2 + \dots + \bar{\alpha}_{2k+1} \leq k$, на котором $Maj_{2k+1}(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_{2k+1})=0$. Следовательно, мажоритарная функция принимает единичные значения на половине всех наборов.

§ 10. 10.4. ж) $f = f_0 \bar{x} \bar{y} \bar{z} \vee f_1 \bar{x} \bar{y} z \vee f_2 \bar{x} y \bar{z} \vee f_3 \bar{x} y z \vee f_4 x \bar{y} \bar{z} \vee f_5 x \bar{y} z \vee f_6 x y \bar{z} \vee f_7 x y z$,
 $\varphi_1(x, y) = f_0 \bar{x} y \bar{y} \vee f_1 \bar{x} y y \vee f_2 \bar{x} y \bar{y} \vee f_3 \bar{x} y y \vee f_4 x y \bar{y} \vee f_5 x y y \vee f_6 x y \bar{y} \vee f_7 x y y$,
 $\varphi_2(x, y) = f_0 \bar{x} \bar{y} \vee f_3 \bar{x} y \vee f_4 x \bar{y} \vee f_7 x y$, $\varphi_7(x, y) = (f_0, f_3, f_4, f_7)$. $f(x, y, z) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 z \oplus a_4 x y \oplus a_5 x z \oplus a_6 y z \oplus a_7 x y z$, $\varphi_7(x, y) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 z \oplus a_4 x y \oplus a_5 x z \oplus a_6 y z \oplus a_7 x y z$, $\varphi_7(x, y) = a_0 \oplus a_1 x \oplus (a_2 \oplus a_3 \oplus a_6) y \oplus (a_4 \oplus a_5 \oplus a_7) x y$,
 $\varphi_7(x, y) = (a_0, a_1, a_2 \oplus a_3 \oplus a_6, a_4 \oplus a_5 \oplus a_7)_{\oplus}$. **10.5. б)** Используя разложение $f(x, y, z) = g_0 \oplus g_1 x \oplus g_2 y \oplus g_3 z \oplus g_4 x y \oplus g_5 x z \oplus g_6 y z \oplus g_7 x y z$, получаем $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z) = g_0 \oplus g_1 x \oplus g_2 y \oplus g_4 x y \oplus g_0 \oplus g_1 x \oplus g_3 z \oplus g_5 x z \oplus g_0 \oplus g_2 y \oplus g_3 z \oplus g_6 y z$. Полином Жегалкина данной функции примет вид $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z) = g_0 \oplus g_4 x y \oplus g_5 x z \oplus g_6 y z$. **10.6.** Данное равенство запишем в виде $(g_0, 0, 0, 0, g_4, g_5, g_6, 0)_{\oplus} = (g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7)_{\oplus}$. Из единственности представления функции в виде полинома Жегалкина следует $g_1 = 0, g_2 = 0, g_3 = 0, g_7 = 0$. Функция, удовлетворяющая условию $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z) = f(x, y, z)$, имеет полином $f(x, y, z) = g_0 \oplus g_4 x y \oplus g_5 x z \oplus g_6 y z$. **10.7.** Равенство запишем в виде $(g_0, 0, 0, 0, g_4, g_5, g_6, 0)_{\oplus} = (0, 0, 0, 0, 0, 0, 0, 0)_{\oplus}$. Из единственности представления функции в виде полинома Жегалкина следует $g_0 = 0, g_4 = 0, g_5 = 0, g_6 = 0$. Если $f(x, y, 0) \oplus f(x, 0, z) \oplus f(0, y, z) = 0$, то полином Жегалкина имеет вид $f(x, y, z) = g_1 x \oplus g_2 y \oplus g_3 z \oplus g_7 x y z$.

§ 11. 11.1. а) $f = x y \bar{z} \vee \bar{x} \bar{y} z$; б) $f = \bar{x} y z t \vee x \bar{y} z t \vee x y z t \vee x y \bar{z} t = (\bar{x} y z t \vee \bar{t}) \vee (x y z t \vee t) = \bar{x} \bar{y} z \vee x y \bar{z}$.

§ 12. 12.1. а) $x \vee \bar{y}$.

§ 13. 13.1. а) $[K] = \{x, y, \bar{x}, \bar{y}\}$; б) $[K] = \{0, 1, x, y, \bar{x}, \bar{y}\}$; в) $[K] = \{x, y, x y\}$; г) $[K] = \{0, x, y, x \oplus y\}$. **13.2. а)** $2^{2^n - 2}$; б) $2^{2^n - 2}$; в) 0.

§ 14. 14.5. ж) $(f(x_1, x_2, \dots, x_n) \rightarrow g(x_1, x_2, \dots, x_n))^* = \overline{f(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)} \rightarrow g(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) = \overline{f(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) \vee g(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)} = \overline{f(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)} \overline{g(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)} = f^*(x_1, x_2, \dots, x_n) g^*(x_1, x_2, \dots, x_n) = f^*(x_1, x_2, \dots, x_n) \vee g^*(x_1, x_2, \dots, x_n) =$

$$= \overline{g^*(x_1, x_2, \dots, x_n)} \vee \overline{f^*(x_1, x_2, \dots, x_n)} = g^*(x_1, x_2, \dots, x_n) \rightarrow f^*(x_1, x_2, \dots, x_n).$$

14.6. Если $x_1 = 1$, то $f(x_1, x_2, \dots, x_n) = g(x_1, x_2, \dots, x_n)$ по условию. Если $x_1 = 0$, то

$$\begin{aligned} f(0, x_2, \dots, x_n) &= \overline{f(1, \overline{x_2}, \dots, \overline{x_n})} = \overline{g(1, \overline{x_2}, \dots, \overline{x_n})} = g(0, x_2, \dots, x_n), \text{ тогда } f(x_1, x_2, \dots, x_n) = \\ &= g(x_1, x_2, \dots, x_n). \end{aligned} \quad \mathbf{14.12.} \quad \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{x_{n+1}}) = F\left(\overline{f(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}), \overline{x_{n+1}}}\right) = \\ &= F\left(\overline{f(x_1, x_2, \dots, x_n)}, \overline{x_{n+1}}\right) = \overline{F(f(x_1, x_2, \dots, x_n), x_{n+1})} = \overline{\varphi(x_1, x_2, \dots, x_n, x_{n+1})}.$$

§ 15. 15.2. Функция $f(x, y) = a_0 \oplus a_1x \oplus a_2y \oplus a_3xy$ является линейной $\leftrightarrow a_3 = 0$. Но $a_3 = f_0 \oplus f_1 \oplus f_2 \oplus f_3$ (§11). Уравнение $f_0 \oplus f_1 \oplus f_2 \oplus f_3 = 0$ имеет единственное решение $f_3 = f_0 \oplus f_1 \oplus f_2$. **15.5.** $f_2 = f_0 \oplus (f_0 \oplus f_2), f_3 = f_1 \oplus (f_0 \oplus f_2)$ поэтому наборы (f_0, f_1) и (f_2, f_3) совпадают или отличаются в каждом разряде. Аналогично, $f_{i+4} = f_i \oplus (f_0 \oplus f_4), i = 0, 1, 2, 3$, поэтому наборы (f_0, f_1, f_2, f_3) и (f_4, f_5, f_6, f_7) одинаковые или противоположные. **15.14.** $xy + xz + yz$. **15.10. а)** 2^{n-1} . **15.17.** $g(x_1, x_2, \dots, x_n, x_{n+1}) = f(x_1, x_2, \dots, x_n) \oplus x_{n+1}$.

15.19. Для мажоритарной функции $f = a_0 \oplus a_1x \oplus a_2y \oplus a_3z \oplus (1 \oplus a_0 \oplus a_1 \oplus a_2)xy \oplus (1 \oplus a_0 \oplus a_1 \oplus a_3)xz \oplus (1 \oplus a_0 \oplus a_2 \oplus a_3)yz \oplus (a_1 \oplus a_2 \oplus a_3)xyz$ найдем линейные функции, полагая $1 \oplus a_0 \oplus a_1 \oplus a_2 = 0, 1 \oplus a_0 \oplus a_1 \oplus a_3 = 0, 1 \oplus a_0 \oplus a_2 \oplus a_3 = 0, a_1 \oplus a_2 \oplus a_3 = 0$. Система имеет единственное решение $a_0 = 1, a_1 = 0, a_2 = 0, a_3 = 0$, поэтому существует единственная линейная мажоритарная функция $f(x, y, z) = 1$.

§ 16. 16.13. Фиктивной переменной является t , т.к. $g(x, y, z, 0) = g(x, y, x, 1)$.

16.14. а) Для функции $\varphi(x, y, z) = f(x, y) \wedge z$ рассмотрим два произвольных набора переменных (x_1, y_1, z_1) и (x_2, y_2, z_2) , удовлетворяющих условию $(x_1, y_1, z_1) < (x_2, y_2, z_2)$, тогда $(x_1, y_1) < (x_2, y_2)$ и $z_1 \leq z_2$. Подстановкой $f(x_1, y_1) = 0$ или $f(x_1, y_1) = 1$ легко проверяется неравенство $f(x_1, y_1) \wedge z_1 \leq f(x_1, y_1) \wedge z_2$. Из монотонности функции $f(x, y)$ следует $f(x_1, y_1) \leq f(x_2, y_2)$. Подстановкой $z_2 = 0$ или $z_2 = 1$ снова проверяется неравенство $f(x_1, y_1) \wedge z_2 \leq f(x_2, y_2) \wedge z_2$. Тогда $\varphi(x_1, y_1, z_1) = f(x_1, y_1) \wedge z_1 \leq f(x_1, y_1) \wedge z_2 \leq f(x_2, y_2) \wedge z_2 = \varphi(x_2, y_2, z_2)$. Следовательно, функция $f(x, y) \wedge z$ является монотонной; б) для монотонной функции $f(x, y) \equiv 0$ функция $\varphi(x, y, z) = f(x, y) \wedge z \equiv 0$ также является монотонной. Рассмотрим монотонную функцию $f(x, y)$, где $f(x, y) \neq 0$, тогда существует набор (x_1, y_1) , для которого $f(x_1, y_1) = 1$. Рассмотрим наборы $(x_1, y_1, 0)$ и $(x_1, y_1, 1)$, удовлетворяющие условию $(x_1, y_1, 0) < (x_1, y_1, 1)$, тогда $\varphi(x_1, y_1, 0) = f(x_1, y_1) \wedge 0 = 0, \varphi(x_1, y_1, 1) = f(x_1, y_1) \wedge 1 = f(x_1, y_1) = 1, \varphi(x_1, y_1, 1) = f(x_1, y_1) \wedge 1 = 1$. Но $\varphi(x_1, y_1, 0) > \varphi(x_1, y_1, 1)$. Итак, если для монотонной функции

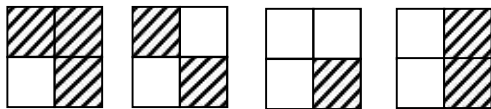
$f(x, y)$ существует набор (x_1, y_1) , на котором $f(x_1, y_1) = 1$, то функция $f(x, y) \wedge \bar{z}$ не является монотонной.

§19. 19.5. а) Пусть $f(x, y) = a_0 \oplus a_1x \oplus a_2y \oplus a_3xy$, $g(x) = g_0 \oplus g_1x$, $h(y) = h_0 \oplus h_1y$. Равенство $f(x, y) = g(x) \wedge h(y)$ примет вид $a_0 \oplus a_1x \oplus a_2y \oplus a_3xy = (g_0 \oplus g_1x)(h_0 \oplus h_1y) = g_0h_0 \oplus g_0h_1y \oplus g_1h_0x \oplus g_1h_1xy$. Из единственности представления функции в виде полинома Жегалкина получаем $g_0h_0 = a_0, g_1h_0 = a_1, g_0h_1 = a_2, g_1h_1 = a_3$. Для функции $f(x, y) = (1011)_{\oplus}$ получаем систему $g_0h_0 = 1, g_1h_0 = 0, g_0h_1 = 1, g_1h_1 = 1$. Уравнение $g_0h_0 = 1$ имеет единственное решение $g_0 = 1, h_0 = 1$. Уравнение $g_1h_1 = 1$ имеет единственное решение $g_1 = 1, h_1 = 1$. Полученные решения противоречат уравнению $g_1h_0 = 0$. Существует функция $f(x, y) = 1 \oplus y \oplus xy$, представление которой в виде $f(x, y) = g(x) \wedge h(y)$ невозможно.

§ 20. 20.4. а) $x + 1 = a$; б) $ax = 1$; в) $ax = 0$; г) $ax - ax = 1$; д) $ax^2 = 4$;

е) $ax - ax = 0$.

§ 21. 21.2. а)



21.3. 7.

§ 22. 22.1. а) $\frac{\partial}{\partial x} 0 = \frac{\partial(x\bar{x})}{\partial x} = 0\bar{0} \oplus \bar{1}1 = 0 \oplus 0 = 0$; в) $(f(x, y)g(x, y))'_x =$

$= f(0, y)g(0, y) \oplus f(1, y)g(1, y), f'_x g \oplus f g'_x \oplus f'_x g'_x = (f(0, y) \oplus f(1, y))g(x, y) \oplus$

$\oplus f(x, y)(g(0, y) \oplus g(1, y)) \oplus (f(0, y) \oplus f(1, y))(g(0, y) \oplus g(1, y))$. Проверка равенства при $x = 0$ и при $x = 1$; г) $\frac{\partial}{\partial x} f(y, z) = f(y, z)|_{x=1} \oplus f(y, z) \oplus f(y, z) = 0$;

д) $(f(x, y) \oplus g(x, y))'_x = (f(1, y) \oplus g(1, y)) \oplus (f(0, y) \oplus g(0, y)) = f(1, y) \oplus f(0, y) \oplus$

$\oplus g(1, y) \oplus g(0, y) = f'_x(x, y) \oplus g'_x(x, y)$; е) $(f \vee g)'_x = (fg \oplus f \oplus g)'_x = (fg)'_x \oplus f'_x \oplus g'_x$.

22.3. $\bar{x}_2 \bar{x}_3 \vee \bar{x}_2 x_4 \vee \bar{x}_2 x_3$. **22.5.** а) $f(x_1, \dots, 0_i, \dots, x_n) \vee x_i \frac{\partial f(x_1, \dots, x_i, \dots, x_n)}{\partial x_i} = f(x_1, \dots, 0_i, \dots, x_n) \oplus$

$\oplus x_i \left((f(x_1, \dots, 1_i, \dots, x_n) \oplus f(x_1, \dots, 0_i, \dots, x_n)) \right)$. При $x_i = 1$ получаем $f(x_1, \dots, 0_i, \dots, x_n) \vee$

$\vee x_i \frac{\partial f(x_1, \dots, x_i, \dots, x_n)}{\partial x_i} = f(x_1, \dots, 0_i, \dots, x_n) \oplus 1 \left((f(x_1, \dots, 1_i, \dots, x_n) \oplus f(x_1, \dots, 0_i, \dots, x_n)) \right) = f(x_1, \dots, 1_i, \dots, x_n)$

При $x_i = 0$ получаем $f(x_1, \dots, 0_i, \dots, x_n) \vee x_i \frac{\partial f(x_1, \dots, x_i, \dots, x_n)}{\partial x_i} =$

$= f(x_1, \dots, 0_i, \dots, x_n) \oplus 0 \left((f(x_1, \dots, 1_i, \dots, x_n) \oplus f(x_1, \dots, 0_i, \dots, x_n)) \right) = f(x_1, \dots, 0_i, \dots, x_n)$.

22.6. б) $(x \vee f(y, z))'_x = (xf(y, z) \oplus x \oplus f(y, z))'_x = f(y, z) \oplus 1 = \overline{f(y, z)}$.

§ 23. 23.3. Нет. Если бы это было возможно, то можно построить граф с 28 вершинами, 9 из них имели бы степень 3, 11 – степень 4, 8 – степень 5. Такой граф имеет 17 нечетных вершин, что противоречит теореме о числе нечетных вершин графа. 23.4. Нет. Если в государстве n городов, то дорог – $7n/2$. Это число не может быть равно 100. 23.6. В графе с n вершинами каждая из вершин может иметь одну из следующих степеней: $0, 1, 2, \dots, (n-1)$. Предположим,

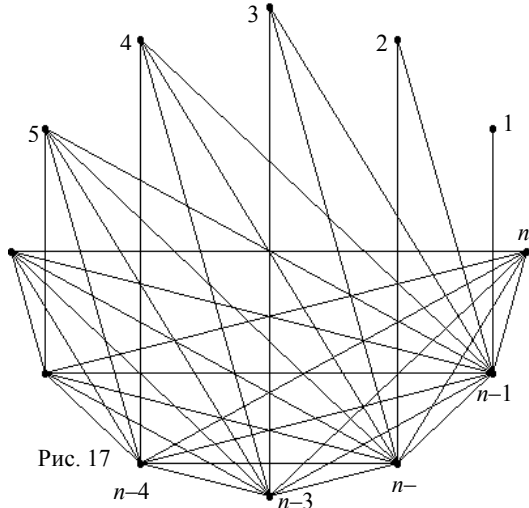


Рис. 17

что все его вершины имеют разные степени, т.е. $\delta(v_1) = 0, \delta(v_2) = 1, \dots, \delta(v_n) = n - 1$. Тогда вершина $v_1 = 0$ изолированная, которая не соединена ребром ни с какой вершиной. А тогда вершина v_n имеет степень, меньшую либо равную числу $n-2$. В графе с n вершинами не может быть вершин со степенями 0 и $n-1$. Следовательно, в графе найдутся, по крайней мере, две вершины, имеющие одинаковые степени. 23.8. Сформулируйте алгоритм построения такого графа, исследуя рис. 17. 23.9. Из каждой вершины графа выходит пять ребер. Из них хотя бы 3 ребра одного цвета. Вторые концы этих ребер образуют треугольник. Если его стороны одного цвета, то утверждение доказано. Если две стороны треугольника имеют разные цвета, то одна из сторон треугольника окрашена в тот же цвет, что три отрезка, выходящие из одной вершины. Эта сторона с двумя из этих отрезков образует одноцветный треугольник.

§ 24. 24.4. Для графа G_6 (рис. 18) вершина a должна отображаться в себя, т.к. только она имеет степень вершины, равную 4. Аналогично, вершина s отображается в себя. Изолированная вершина b может отображаться в себя или в вершину c . Рассмотрим вначале автоморфизмы, при которых вершины $\{a, b, c\}$ остаются неподвижными

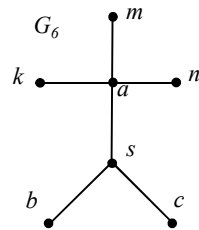


Рис. 18

- $f_1 : a \rightarrow a, b \rightarrow b, c \rightarrow c, k \rightarrow k, m \rightarrow m, n \rightarrow n, s \rightarrow s,$
- $f_2 : a \rightarrow a, b \rightarrow b, c \rightarrow c, k \rightarrow k, m \rightarrow n, n \rightarrow m, s \rightarrow s,$
- $f_3 : a \rightarrow a, b \rightarrow b, c \rightarrow c, k \rightarrow m, m \rightarrow k, n \rightarrow n, s \rightarrow s,$
- $f_4 : a \rightarrow a, b \rightarrow b, c \rightarrow c, k \rightarrow n, m \rightarrow m, n \rightarrow k, s \rightarrow s,$

$$f_5 : a \rightarrow a, b \rightarrow b, c \rightarrow c, k \rightarrow m, m \rightarrow n, n \rightarrow k, s \rightarrow s,$$

$$f_6 : a \rightarrow a, b \rightarrow b, c \rightarrow c, k \rightarrow n, n \rightarrow m, m \rightarrow k, s \rightarrow s.$$

Аналогично можно задать 6 автоморфизмов, при которых вершины b и c меняются местами:

$$f_7 : a \rightarrow a, b \rightarrow c, c \rightarrow b, k \rightarrow k, m \rightarrow m, n \rightarrow n, s \rightarrow s,$$

$$f_8 : a \rightarrow a, b \rightarrow c, c \rightarrow b, k \rightarrow k, m \rightarrow n, n \rightarrow m, s \rightarrow s,$$

$$f_9 : a \rightarrow a, b \rightarrow c, c \rightarrow b, k \rightarrow m, m \rightarrow k, n \rightarrow n, s \rightarrow s,$$

$$f_{10} : a \rightarrow a, b \rightarrow c, c \rightarrow b, k \rightarrow n, m \rightarrow m, n \rightarrow k, s \rightarrow s,$$

$$f_{11} : a \rightarrow a, b \rightarrow c, c \rightarrow b, k \rightarrow m, m \rightarrow n, n \rightarrow k, s \rightarrow s,$$

$$f_{12} : a \rightarrow a, b \rightarrow c, c \rightarrow b, k \rightarrow n, n \rightarrow m, m \rightarrow k, s \rightarrow s.$$

24.14. Используя графы, переформулируем задачу следующим образом. Доказать, что если G – граф с шестью вершинами, то либо G , либо его дополнение \bar{G} содержат треугольник. Пусть v – произвольная вершина графа G . Она смежна с остальными пятью вершинами в графе G или в его дополнении. Найдется три вершины u_1, u_2, u_3 в графе или в его дополнении, смежные с вершиной v . Можно считать, что они расположены в графе G . Если какая-то пара из трех вершин u_1, u_2, u_3 смежна, то они вместе с вершиной v образуют треугольник. Если все пары из этой тройки не смежны в G , то вершины u_1, u_2, u_3 образуют треугольник в \bar{G} .

§ 26. 26.5. $n = 2, \delta = 7$ – мультиграф с двумя вершинами или $n = 7, \delta = 2$ – семиугольник. 26.22. Сумма числа m ребер графа G и числа ребер его дополнения \bar{G} равна числу ребер полного графа K_{4k+2} . Графы G и \bar{G} имеют одинаковое количество ребер, т.к. они изоморфны. Для суммы ребер получаем противоречие $m + m = \frac{(4k+2)(4k+1)}{2} = (2k+1)(4k+1)$, ос-

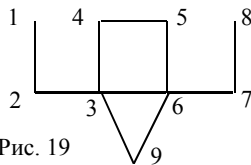


Рис. 19

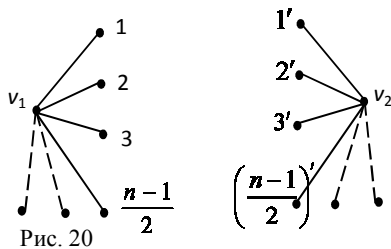
нованное на четности чисел в равенстве.

§ 27. 27.4. Граф на рис. 19. 27.6. В полном звездном графе $K_{1,n}$ при $n \geq 3$ такой цепи не существует.

§ 29. 29.4. Указание. Если граф содержит одну изолированную вершину, то число ребер графа не превосходит числа C_{n-1}^2 . Если граф содержит две компоненты, одна из которых содержит k вершин, а вторая $n-k$ вершин, то число ребер графа не превосходит числа $C_k^2 + C_{n-k}^2$, но $C_k^2 + C_{n-k}^2 < C_n^2$ при $0 < k < n$. 29.5. Пусть в графе существует две вершины v_1 и v_2 , которые не связаны цепью (рис. 20). Каждая из этих вершин соединена по условию не менее чем с $(n-1)/2$ вершинами, причем эти вершины различны (если какие-то из этих вершин совпадают, то существует путь между вершинами v_1 и v_2). Тогда граф содержит не менее

$$1 + \frac{n}{2} + 1 + \frac{n}{2} = n + 2 \text{ вершин, что противоречит условию.}$$

§ 30. 30.16. Пусть v_1, v_2, \dots, v_n – вершины графа K_n . Любые две вершины графа соединены ребром, поэтому существует маршрут $v_1, v_2, \dots, v_n, v_1$, проходящий через каждую вершину графа по одному разу. **30. 21.** (3,2,1,4,5).



§ 31. 31.3. Оба графа не являются плоскими, но являются планарными. **31.5.** Плоский граф имеет наибольшее число граней, если он имеет наибольшее число ребер. Наибольшее число ребер имеет полный граф G_5 , но он не является плоским. Удалив одно из ребер этого графа (рис. 21) и преобразовав его, получим плоский граф, имеющий 6 граней.

31.6. В полном графе все вершины соединены с остальными вершинами.

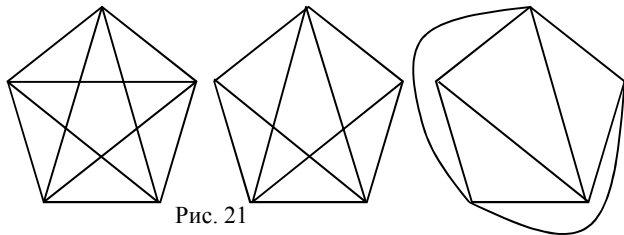


Рис. 21

Предположим

противное, т.е. граф является плоским и тогда по теореме Эйлера число граней равно $f = 2 - 5 + 10 = 7$. Граф не содержит кратных ребер, поэтому в графе нет граней, ограниченных двумя ребрами. Представим число граней в виде $f = f_3 + f_4 + \dots + f_k$, где f_3 – число граней, ограниченных тремя ребрами, f_4 – число граней, ограниченных четырьмя ребрами и т.д. Каждое ребро является границей двух граней, поэтому для числа ребер получаем $2m = 20 = 3f_3 + 4f_4 + \dots + kf_k$,

$3f = 21 = 3f_3 + 3f_4 + \dots + 3f_k$. Выполняется неравенство $3f_3 + 3f_4 + \dots + 3f_k \leq 3f_3 + 4f_4 + \dots + kf_k$, но это противоречит условию $21 < 20$. Противоречие доказывает, что такой граф не является плоским.

31.8. а) планарный, т.к. может быть изображен в виде (рис. 22); б) не планарный, т.к. содержит подграф K_5 ; в) не планарный, т.к. содержит подграф $K_{3,3}$.

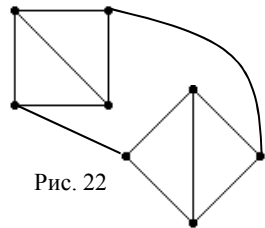


Рис. 22

§ 33. 33.23. Если деревья (1, 2, 3, 4) и (5, 2, 3, 6) с обходом всех вершин объединить, то получим снова дерево. Если деревья (1, 2, 3) и (1, 4, 3) с обходом всех вершин объединить, то получим цикл, который не является деревом. Если два дерева имеют две общие вершины, являющиеся листьями на каждом дереве, то на одном дереве существует путь, соединяющий эти вершины, и на другом дереве существует аналогичный путь. Объединение этих путей является циклом, поэтому в этом случае объединение двух деревьев не является деревом.

§ 36. 36.1. НОД(34,85)=17, 17=34·(-2)+85·1. 36.4. Если $ax+by = \text{НОД}(a,b)$,

то $\frac{a}{\text{НОД}(a,b)}x + \frac{b}{\text{НОД}(a,b)}y = 1$. Любой делитель чисел x и y является делителем числа 1. Следовательно, x и y – взаимно простые числа. 36.5. $\text{НОД}(a,b) = ax+by = a(x-b)+b(y+a)$. 36.6. Из $\text{НОД}(a,b)=1$ следует $ax+by=1$, $x, y \in \mathbb{Z}$.

Тогда $(a+nb)x+b(y-nx)=1$, $x, (y-nx) \in \mathbb{Z}$.

§ 37. 37.1.a) $a \equiv b \pmod{n} \leftrightarrow a = b + nk$, $c \equiv d \pmod{n} \leftrightarrow c = d + nl$, где

$k, l \in \mathbb{Z}$, $a+c = b+d+n(k+l) \leftrightarrow a+c \equiv b+d \pmod{n}$ 37.4. Пусть $a = 2n+1$,

$n \in \mathbb{Z}$, тогда $a^2 - 1 = 4n^2 + 4n = 4n(n+1)$. Но из двух соседних целых чисел одно

является четным, поэтому $4n(n+1):8$, $a^2 \equiv 1 \pmod{8}$. 37.8. $3^{89} \pmod{7} = 5$.

37.13. Если пара (x,y) означает x двухрублевых монет и y пятирублевых монет, то пять способов (23; 1), (18; 3), (13; 5), (8; 7), (3; 9). 37.18. Рассмотрим множество всех остатков по модулю p для чисел, которые не делятся на p : 1, 2, 3, ..., $(p-1)$.

Умножая каждое из этих чисел на m , получим $m, 2m, 3m, \dots, (p-1)m$. Любая пара из этого множества не дает по модулю p один и тот же остаток, т.к. если предположить противное $xm \equiv ym \pmod{p}$, то число $(x-y)m$ делится на p . Но число m не делится на p , а различные числа x и y оба меньше p , поэтому их разность также не делится на p . Следовательно, числа $m, 2m, 3m, \dots, (p-1)m$ различны по модулю p . Это множество фактически совпадает с множеством 1, 2, 3, ..., $(p-1)$. Тогда $m \cdot 2m \cdot 3m \cdot \dots \cdot (p-1)m \equiv 1 \times 2 \times 3 \times \dots \times (p-1) \pmod{p}$, $m \cdot 2m \cdot 3m \cdot \dots \cdot (p-1)m \equiv (p-1)! \pmod{p}$. Число $(p-1)!$ не имеет общих делителей с p , поэтому, разделив последнее равенство на $(p-1)!$, получим $m^{p-1} \equiv 1 \pmod{p}$.

§ 39. 39.6. $\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ 39.7. $\begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix}$.

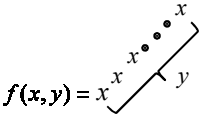
§ 45. 45.1. Для рис. 7 задачи кратчайший маршрут $eachbde$.

§ 49. 49.1. а) $c_n = a \cdot 2^n + 4(2^n - 1)$; в) $a = \frac{2(2^{m+1} - 2^n - 1)}{2^n - 2^m}, n \neq m$. 49.2. 8.

49.3. 5. 49.4. 8. 49.5. 5. 49.7. ВВВУВ.

§ 50. 50.1. а) $f(x,y) = 3x^y$; б) $f(x,y) = xy + x^2$; в) $f(x,y) = x^{y+1}$;

г) $f(x,y) = \begin{cases} 0, & y - \text{четное}, \\ x, & y - \text{нечетное}. \end{cases}$; д)



е) $f(x,y) = x^{xy}$; ж) $f(x,y) = \begin{cases} x+n, & y = 2n+1, \\ n, & y = 2n. \end{cases}$; з) $f(x,y) = \begin{cases} x, & y = 0, \\ 0, & y \neq 0. \end{cases}$

50.5. Указание. $f = f_1 \overline{sg}(\alpha_1) + \dots + f_k \overline{sg}(\alpha_k) + f_{k+1} \overline{sg}(\alpha_1 \alpha_2 \dots \alpha_k)$. **50.7.** Равенство

$x = \left[\frac{x}{y} \right] y + \text{rest}(x, y)$ равносильно равенству $\text{rest}(x, y) = x \dot{-} \left[\frac{x}{y} \right] y$, так что доста-

точно показать примитивную рекурсивность функции $\left[\frac{x}{y} \right]$. Если $y \neq 0$ и

$\left[\frac{x}{y} \right] = n$, то $ny \leq x < (n+1)y$. Значит, в последовательности $1 \cdot y \dot{-} x, 2 \cdot y \dot{-} x, \dots, n \cdot y \dot{-} x, \dots, x \cdot y \dot{-} x$ первые n членов равны нулю, а остальные отличны от нуля.

Тогда в последовательности $\overline{sg}(1 \cdot y \dot{-} x), \overline{sg}(2 \cdot y \dot{-} x), \dots, \overline{sg}(n \cdot y \dot{-} x), \dots, \overline{sg}(x \cdot y \dot{-} x)$

первые n членов равны 1, а остальные – нули. В таком случае $\left[\frac{x}{y} \right] = n = \sum_{i=1}^x \overline{sg}(iy \dot{-} x)$.

Покажите справедливость формулы для $y = 0$. **50.8.** а) $d(x, y) = \overline{sg}(\text{rest}(x, y))$; б)

$nd(x) = \sum_{i=1}^x id(x, i)$; в) $p(x) = \overline{sg}(|nd(x) - (x+1)|)$; г) Пусть $x \leq y$, тогда

$\varphi(x, y) = \overline{sg}\left(\sum_{i=1}^x (d(x, i)d(y, i))\right)$. **50.9.** Если $\lceil \sqrt{x} \rceil = n$, т.е. $n^2 \leq x \leq (n+1)^2$, то n –

наименьший корень уравнения $1 \dot{-} \overline{sg}((y+1)^2 \dot{-} x) = 0$ (уравнение относительно y). Следовательно, $\lceil \sqrt{x} \rceil = n = \mu_y(1 \dot{-} \overline{sg}((y+1)^2 \dot{-} x) = 0)$. Так как $\lceil \sqrt{x} \rceil \leq x$, то можно применить теорему о мажорируемости неявных функций. **50.10.**

$f(n) = a_n = \lceil 10^n \sqrt{2} \rceil \dot{-} 10 \lceil 10^{n-1} \sqrt{2} \rceil$.

§ 51. 51.1. а) Исходя из того, что $xy = \underbrace{x + x + \dots + x}_y$ слово 1^x копируем y раз

с помощью машины $T_{\text{коп}}$. Затем к слову $\underbrace{1^x * 1^x * \dots * 1^x}_y$ применяем машину T_+ ,

складывающую несколько чисел. Получаем машину T_x , умножающую два числа;

б) Указание. Так как $x^y = \underbrace{x \cdot x \cdot \dots \cdot x}_y$, то также как в п. а) копируем 1^x , а затем

применяем нужное число раз машину умножения T_x из п. а); г) Нахождение

$\text{rest}(x, y)$ заключается в том, что в $\underbrace{11\dots 1}_x$ укладывается слово $\underbrace{11\dots 1}_y$. То, что

остается после целого укладывания, и будет остатком. Укладка производится следующим образом:

$$q_1 \underbrace{111\dots 1}_x * \underbrace{111\dots 11}_y \rightarrow \dots \rightarrow \underbrace{111\dots 1}_x \underbrace{111\dots 10}_y \rightarrow \dots \rightarrow \underbrace{011\dots 1}_x \underbrace{111\dots 10}_y \rightarrow \dots$$

→ $\underbrace{011\dots1}_x * \underbrace{111\dots00}_y \rightarrow \dots \rightarrow \underbrace{00\dots00}_y \underbrace{11\dots1}_{x-y} * \underbrace{00\dots0}_y \rightarrow \dots \rightarrow \underbrace{11\dots1}_{x-y} * \underbrace{11\dots1}_y \rightarrow \dots \rightarrow$ до тех пор, пока не получим $000\dots0 * \underbrace{11\dots0}_y$. Тогда количество нулей до разделителя * и

будет остатком $rest(x, y)$. Для получения $\left[\frac{x}{y} \right]$ надо от слова $\underbrace{111\dots1}_x * \underbrace{111\dots1}_y$ перейти к $\Delta \underbrace{111\dots1}_x * \underbrace{111\dots1}_y$ и при каждой укладке $\underbrace{111\dots1}_y$ в $\underbrace{111\dots1}_x$ перед разделителем Δ ставить 1. Количество единиц перед Δ и будет $\left[\frac{x}{y} \right]$. **51.2.** а) Если

головка в начальной команде q_1 смотрит на ячейку с символом *, т.е. $q_1 * 1^y$, то ставится H , а все остальное стирается. Если же $q_1 1^x * 1^y$, то в состоянии q_1 головка движется вправо, все оставляя без изменения, пока не дойдет до пустой ячейки. В этом случае $q_1 \lambda \rightarrow q_2 \lambda L$. Если после этого получим $q_2 *$, пишется L и все остальное стирается. Если же имеем $q_2 1$, то $q_2 1 \rightarrow q_3 \lambda L$ и в состоянии q_3 головка движется влево, все пропуская, пока не достигнет пустой ячейки. Тогда $q_3 \lambda \rightarrow q_4 \lambda R$, а $q_4 1 \rightarrow q_1 \lambda R$, и все повторяется снова уже в положении $1^{x-1} * 1^{y-1}$ до тех пор, пока либо не попадем в состояние $q_1 *$ (и тогда будет H), либо в состояние $q_2 *$ (и тогда будет L). **51.4–51.6.** Для построения необходимой машины надо T_1, T_2, T_g, T_h заменить эквивалентными машинами либо $T_1^L, T_2^L, T_g^L, T_h^L$ (с левой полулентой), либо машинами $T_1^R, T_2^R, T_g^R, T_h^R$ (с правой полулентой). **51.7.** а)

	0	1	2	3	4	5	6	7	8	9	λ
q_1	$q_1 0R$	$q_1 1R$	$q_1 2R$	$q_1 3R$	$q_1 4R$	$q_1 5R$	$q_1 6R$	$q_1 7R$	$q_1 8R$	$q_1 9R$	$q_2 \lambda L$
q_2	$q_3 3L$	$q_3 4L$	$q_3 5L$	$q_3 6L$	$q_3 7L$	$q_3 8L$	$q_3 9L$	$q_4 0L$	$q_4 1L$	$q_4 2L$	
q_3	$q_3 0L$	$q_3 1L$	$q_3 2L$	$q_3 3L$	$q_3 4L$	$q_3 5L$	$q_3 6L$	$q_3 7L$	$q_3 8L$	$q_3 9L$	$q_0 \lambda R$
q_4	$q_3 1L$	$q_3 2L$	$q_3 3L$	$q_3 4L$	$q_3 5L$	$q_3 6L$	$q_3 7L$	$q_3 8L$	$q_3 9L$	$q_4 0L$	$q_0 1E$

в) По аналогии с п. а) построить T_{+1} (прибавляющую 1) и T_{-1} (вычитающую 1). Далее, находясь в конфигурации $m * n$, последовательно вычитаем 1 из n (применяя T_{-1}) и прибавляем к m единицу (с помощью T_{+1}). Переходим к конфигурации $(m+1) * (n-1)$ и т. д., пока не достигнем конфигурации $;; (m+n) * 0$; д) Пусть $a_0, a_1, a_2, \dots, a_y$ - это числа $0, 1, 2, \dots, 9$. Зададим 10 команд t_i следующего типа:

$t_i a_j \rightarrow t_i a_j R$, $t_i \lambda \rightarrow t_i' a_i R$, а 10 команд t_i' действуют следующим образом:
 $t_i' a_j \rightarrow t_i' a_j L$, $t_i' \square \rightarrow a_i q_1 R$, $q_i a_i \rightarrow t_i \square R$.

Литература

1. *Аршинов, М.Н.* Коды и математика (Библиотечка “Квант”. Вып. 30) / М.Н. Аршинов, Л.Е. Садовский. – М.: Наука, 1983.
2. *Болтянский, В.Г.* Беседы о математике. Кн.1. Дискретные объекты / В.Г. Болтянский, А.П.Савин. – М.: МЦНМО, 2002.
3. *Гаврилов, Г.П.* Задачи и упражнения по дискретной математике: учеб. пособие / Г.П. Гаврилов, А.А. Сапоженко. – М.: ФИЗМАТЛИТ, 2006.
4. *Горбатов, В.А.* Дискретная математика / В.А Горбатов, А.В. Горбатов, М.В. Горбатова. - М.: АСТ, 2003.
5. *Грэхем, Р.* Конкретная математика / Р. Грэхем, Д. Кнут, О. Паташник. – М.: Мир, 1998.
6. *Иванов, Б.Н.* Дискретная математика. Алгоритмы и программы: учебное пособие / Б.Н. Иванов. – М.: Лаборатория базовых знаний, 2002.
7. *Казачек, Н.А.* Алгебра и теория чисел. Ч.III / Н.А. Казачек [и др.] – М.: Просвещение, 1974.
8. Задачи по дискретной математике: Булева алгебра и комбинаторика: учебное пособие / под редакцией С.Ф. Кожухова – Сургут: ИЦ СурГУ, 2008.
9. *Коннов, В.В.* Геометрическая теория графов / В.В. Коннов, Г.А. Клековкин, Л.П. Коннова. – М.: Народное образование, 1999.
10. *Коришунов, Ю.М.* Математические основы кибернетики: учебное пособие. – М.: Энергоатомиздат, 1987.
11. *Кузнецов, О.П.* Дискретная математика для инженеров – СПб.: Лань, 2005.
12. *Лавров, А. И.* Задачи по теории множеств, математической логике и теории алгоритмов / А.И. Лавров, Л.Л. Максимова. – М.: Наука, 2004.
13. *Мадер, В.В.* Школьнику об алгебре логики – М.: Просвещение, 1993.
14. *Михайлов, А.Б.* Математический язык в задачах / Михайлов А.Б. [и др.] – СПб.: Изд-во РГПУ им. А. И. Герцена, 2001.
15. *Морозов, В.В.* Исследование операций в задачах и упражнениях / В.В. Морозов, А.Г. Сухарев, В.В. Федоров. – М.: Высшая школа, 1986.
16. *Нефедов, В.Н.* Курс дискретной математики / В.Н. Нефедов, В.А. Осипова. – М.: Изд. МАИ, 1992.
17. *Нечаев, В.И.* Элементы криптографии. Основы теории защиты информации – М.: Высшая школа, 1999.
18. *Новиков, Ф.А.* Дискретная математика для программистов – СПб.: Питер, 2001.
19. *Поздняков, С.Н.* Дискретная математика: учебник / С.Н. Поздняков, С.В. Рыбкин. – М.: Издательский центр «Академия», 2008.
20. *Хаггарти, Р.* Дискретная математика для программистов / Р. Хаггарти. – М.: Техносфера, 2003.
21. *Харари, Ф.* Теория графов – М.: Мир, 1973.
22. *Шевелев, Ю.П.* Дискретная математика – СПб.: Лань, 2008.

*Сергей Федорович КОЖУХОВ,
Петр Игнатьевич СОВЕРТКОВ*

**СБОРНИК ЗАДАЧ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ**

УЧЕБНОЕ ПОСОБИЕ

Издание второе, стереотипное

Зав. редакцией
естественнонаучной литературы *М. В. Рудкевич*

ЛР № 065466 от 21.10.97
Гигиенический сертификат 78.01.10.953.П.1028
от 14.04.2016 г., выдан ЦГСЭН в СПб

Издательство «ЛАНЬ»
lan@lanbook.ru; www.lanbook.com;
196105, Санкт-Петербург, пр. Юрия Гагарина, д. 1, лит. А.
Тел.: (812) 412-92-72, 336-25-09.
Бесплатный звонок по России: 8-800-700-40-71

Подписано в печать 06.02.18.
Бумага офсетная. Гарнитура Школьная. Формат 60×90^{1/16}.
Печать офсетная. Усл. п. л. 20,50. Тираж 100 экз.

Заказ № 103-18.

Отпечатано в полном соответствии
с качеством предоставленного оригинал-макета
в АО «Т8 Издательские Технологии».
109316, г. Москва, Волгоградский пр., д. 42, к. 5.