

**А.А.НАБЕБИН**

**СБОРНИК ЗАДАНИЙ  
ПО  
ДИСКРЕТНОЙ  
МАТЕМАТИКЕ**

**Научный мир**

**А.А.НАБЕБИН**

*На фронтах Великой отечественной войны  
погиб каждый второй коммунист. Им,  
павшим за Родину, за счастье людей труда,  
посвящается*

**С Б О Р Н И К З А Д А Н И Й  
П О  
Д И С К Р Е Т Н О Й  
М А Т Е М А Т И К Е**

**Издание второе  
исправленное, переработанное**

**Москва  
Научный мир  
2021**

УДК 519.1 + 510.6  
ББК 22.176 + 22.12  
Н 13

**Набебин А.А.**

Н 13 Сборник заданий по дискретной математике. – М.: Научный мир, 2021. – 299 с.

Пособие содержит набор индивидуальных заданий с примерами решений для студентов по курсу дискретной математики и предназначено для обеспечения самостоятельной работы студентов по освоению курса.

Пособие предназначено для студентов высших учебных заведений, специализирующихся в областях прикладной математики, вычислительной техники, программирования, информатики.

---

Учебное издание

Алексей Александрович Набебин

**СБОРНИК ЗАДАНИЙ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ**

Научный мир  
Тел/факс +7 (495)691-28-17  
E-mail: [naumir@benran.ru](mailto:naumir@benran.ru) Internet <http://bookish.iring.ru>

Подписано к печати 12.01.2009  
Формат 60x90/16  
Гарнитура Таймс. Печать офсетная. Печ.л. 17.5  
Тираж 1000 экз. Заказ 113

Издание отпечатано  
в ООО «ИПЦ Маска»  
Москва, Научный проезд, дом 20, стр.2

---

ISBN 978-5-91522-072-9

© Научный мир, 2020

© Набебин А.А., 2020

## **ПРЕДИСЛОВИЕ**

Учебное пособие составлено в соответствии с программой курса "Дискретная математика" Государственного образовательного стандарта высших технических учебных заведений Российской Федерации.

Рабочие материалы пособия использовались в преподавании курсов "Дискретная математика" и "Математическая логика и теория алгоритмов" в Московском энергетическом институте, Российском государственном социальном университете, Высшей школе экономики, Московском государственном политехническом университете.

Пособие состоит из двух частей. В первой части (главы с первой по шестую: 1) множества, функции, отношения; 2) модулярная арифметика; 3) комбинаторика; 4) математическая логика; 5) графы, 6) конечные автоматы) даны наборы индивидуальных заданий. Каждый набор содержит 30 индивидуальных заданий. Во второй части (главы с седьмой по одиннадцатую) даны примеры решения задач. В главе 12 приведен пакет программ в среде MATHCAD, без использования которого работа в модулярной арифметике и особенно в полях Галуа была бы весьма затруднительна. В написании Mathcad программ принимали участие студенты МЭИ А.В.Горбачев (факторизация), И.В.Исаев (дискретный логарифм), К.В.Кранов (дискретный квадратный корень).

Связанные с вопросами криптографии задачи модулярной арифметики в практике имеют дело с большими целыми числами, выходящими за пределы величин целых чисел, допустимых в алгоритмических языках программирования. Mathcad, например, допускает целые (10-ричные) числа длины не более 15 цифр. Для работы с большими целыми числами с длиной десятеричной записи в 100 и более цифр приходится писать специальный программный процессор. Поэтому индивидуальные задачи предлагаются с целыми числами в пределах, допустимых средой Mathcad.

В книге "Логика и Пролог в дискретной математике" приведены Пролог-программы для некоторых алгоритмов из теории графов, комбинаторики и конечных автоматов.

В составлении задач принимали участие С.М.Авдошин, Н.В.Андреев, А.А.Болотов, А.А. Жданова, К.В.Коляда, Ю.П.Кораблин, Л.И.Ляшенко, Д.Г.Мещанинов, А.В.Полехов, А.Ю.Пресняков, Ю.Н.Филиппович, А.Б.Фролов.

Пособие предназначено для студентов высших технических учебных заведений, специализирующихся в области прикладной математики, вычислительной техники, программирования, информатики по направлению "Информатика и вычислительная техника" специальности "Программное обеспечение вычислительной техники и автоматизированных систем", а также специальности "Информационные системы и технологии".

# 1. МНОЖЕСТВА, ФУНКЦИИ, ОТНОШЕНИЯ

**Задача 1.** Пусть  $A, B, C$  есть произвольные подмножества некоторого множества  $U$  (универсума). Пусть  $\bar{A} = U - A$ ,  $A \triangleleft B = (A - B) \cup (B - A)$ . Иногда  $\bar{A}$  обозначают через  $\neg A$ .

**Утверждение.** Верно соотношение  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ .

**Доказательство.** Пусть элемент  $a \in \overline{A \cup B}$  произволен. Тогда

$a \notin A \cup B$ ,  $a \notin A$ ,  $a \notin B$ ,  $a \in \bar{A}$ ,  $a \in \bar{B}$ ,  $a \in \bar{A} \cap \bar{B}$ , откуда  $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$ .

Пусть теперь  $a \in \bar{A} \cap \bar{B}$ . Тогда

$a \in \bar{A}$ ,  $a \in \bar{B}$ ,  $a \notin A$ ,  $a \notin B$ ,  $a \notin A \cup B$ ,  $a \in \overline{A \cup B}$ , откуда  $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$ .

Следовательно,  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ .

Доказать следующие соотношения.

## Варианты.

1.1.  $A - (A - B) = A \cap B$ .

1.2.  $A - (B - C) = (A - B) - C$ .

1.3.  $A \triangleleft B = B \triangleleft A$ .

1.4.  $A \triangleleft (A \triangleleft B) = B$ .

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

1.6.  $A - (B \cup C) = A - B \cap A - C$ .

1.7.  $A - (B \cap C) = A - B \cup A - C$ .

1.8.  $A \cap (B - C) = (A \cap B) - (A \cap C)$ .

1.9.  $A \cap (B - C) = (A \cap B) - C$ .

1.10.  $A - (B - C) = (A - C) - (B - C)$ .

1.11.  $(A \cup B) - C = (A - C) \cup (B - C)$ .

1.12.  $A - (B - C) = (A - B) \cup (A \cap C)$ .

1.13.  $A \triangleleft (B \triangleleft C) = (A \triangleleft B) \triangleleft C$ .

1.14.  $A \cap (B - C) = (A \cap B) - (A \cap C)$ .

1.15.  $A \cup B = A \triangleleft (B - (A \cap B))$ .

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

1.17.  $A \cup B \subseteq C \Leftrightarrow A \subseteq C \& B \subseteq C$ .

1.18.  $A \subseteq B \cap C \Leftrightarrow A \subseteq B \& A \subseteq C$ .

1.19.  $A \cap B \subseteq C \Leftrightarrow A \subseteq \neg B \cup C$ .

1.20.  $A \subseteq B \cup C \Leftrightarrow A \cap \neg B \subseteq C$ .

1.21.  $(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A$ .

1.22.  $A \subseteq B \rightarrow A \cap C \subseteq B \cap C$ .

1.23.  $A \subseteq B \rightarrow (A - C) \subseteq (B - C)$ .

1.24.  $A \subseteq B \rightarrow (C - B) \subseteq (C - A)$ .

1.25.  $A - \neg B \Leftrightarrow A \cap B = \emptyset \& A \cup B = U$ .

1.26.  $A \subseteq B \rightarrow \neg B \subseteq \neg A$ .

1.27.  $A - B = A \triangleleft (A \cap B)$ .

1.28.  $A \cup B = A \cap B \rightarrow A = B$ .

1.29.  $(A - B) \cup B = A \Leftrightarrow B \subseteq A$ .

1.30.  $A \subseteq B \rightarrow A \cup C \subseteq B \cup C$ .

**Задача 2.** Частично упорядоченное множество  $(A, \leq)$ ,  $A = \{0, 1, 2, 3, \dots, 20\}$ , задано диаграммой (рис.1.1). Множество  $B \subseteq A$ .

1. Начертить диаграмму для  $B$ .
2. Найти наибольший и наименьший элементы (универсальные границы в  $A$ ).
3. Найти максимальные и минимальные элементы в  $A$ .
4. Найти верхний конус для  $B$  (множество всех верхних граней для  $B$ ).
5. Найти нижний конус для  $B$  (множество всех нижних граней  $B$ ).
6. Найти точную верхнюю грань для  $B$ .
7. Найти точную нижнюю грань для  $B$ .

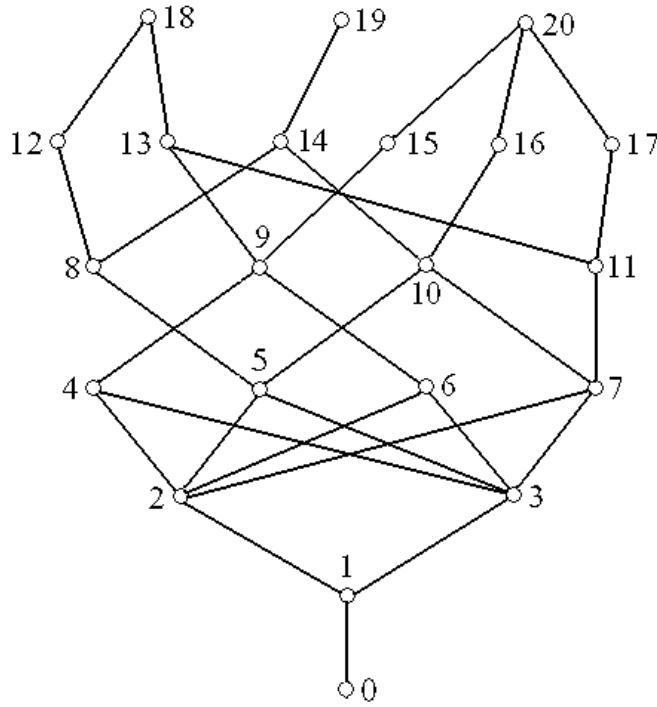


Рис.1.1

**Пример.**  $A = \{0, 1, \dots, 20\}$ ,  $B = \{5, 6, 9, 10\}$ . ЧУМ  $(A, \leq)$  изображено на рис.1.1.  $M$  есть наибольший элемент в  $A$  (верхняя универсальная граница), если  $a \leq M \quad \forall a \in A$ .

$m$  есть наименьший элемент в  $A$  (нижняя универсальная граница), если  $m \leq a \quad \forall a \in A$ .

Элемент  $a$  максимален в  $A$ , если  $\neg \exists x \in A \ x > a$ .

Элемент  $a$  минимален в  $A$ , если  $\neg \exists x \in A \ x < a$ .

Элемент  $a$  есть верхняя грань для  $B$ , если  $\forall b \in B \ a \geq b$ .

Элемент  $a$  есть нижняя грань для  $B$ , если  $\forall b \in B \ a \leq b$ .

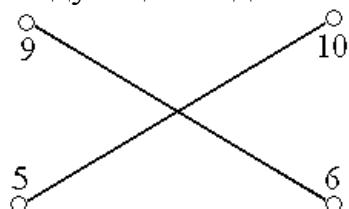
Верхний конус  $B^\Delta$  для  $B$  есть совокупность всех верхних граней для  $B$ .

Нижний конус  $B^\nabla$  для  $B$  есть совокупность всех нижних граней для  $B$ .

Точная верхняя грань для  $B$  есть наименьший элемент  $b^\Delta$  в  $B^\Delta$ .

Точная нижняя грань для  $B$  есть наибольший элемент  $b^\nabla$  в  $B^\nabla$ .

1. Диаграмма для  $B$  имеет следующий вид.



2. Наибольший элемент (верхняя универсальная граница в  $A$ ) не существует.

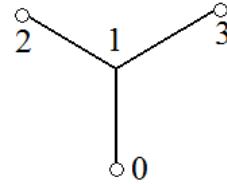
Наименьший элемент (нижняя универсальная граница в  $A$ ) есть 0.

3.  $\{18, 19, 20\}$  есть множество максимальных элементов.

$\{0\}$  есть множество минимальных элементов.

4. Верхний конус для  $B$  есть  $B^\Delta = \{2, 0\}$ .

5. Нижний конус для  $B$  есть  $B^\vee = \{0, 1, 2, 3\}$ . Он имеет следующий вид.



6. Точная верхняя грань для  $B$  (наименьший элемент в  $B^\Delta$ ) есть  $\{2, 0\}$ .

7. Точная нижняя грань для  $B$  (наибольший элемент в  $B^\vee$ ) не существует.

### Варианты множества $B$ .

- |                             |                              |                             |
|-----------------------------|------------------------------|-----------------------------|
| <b>2.1.</b> {2,5,7,9,10}.   | <b>2.2.</b> {3,4,5,9,11}.    | <b>2.3.</b> {2,7,9,10,11}.  |
| <b>2.4.</b> {2,6,8,11,12}.  | <b>2.5.</b> {3,4,9,10,16}.   | <b>2.6.</b> {4,5,10,11,12}. |
| <b>2.7.</b> {4,5,10,13,14}. | <b>2.8.</b> {4,6,10,12,17}.  | <b>2.9.</b> {5,6,7,12,13}.  |
| <b>2.10.</b> {2,4,7,9,17}.  | <b>2.11.</b> {2,5,6,12,13}.  | <b>2.12.</b> {2,7,9,10,11}. |
| <b>2.13.</b> {1,7,8,9,17}.  | <b>2.14.</b> {1,2,3,8,9}.    | <b>2.15.</b> {1,2,3,8,14}.  |
| <b>2.16.</b> {1,3,5,6,11}.  | <b>2.17.</b> {2,3,5,6,15}.   | <b>2.18.</b> {2,3,4,7,8}.   |
| <b>2.19.</b> {2,3,9,11,15}. | <b>2.20.</b> {4,5,6,7,11}.   | <b>2.21.</b> {2,3,4,7,9}.   |
| <b>2.22.</b> {2,4,6,8,9}.   | <b>2.23.</b> {2,9,11,15,16}. | <b>2.24.</b> {3,4,5,8,9}.   |
| <b>2.25.</b> {4,5,6,7,16}.  | <b>2.26.</b> {5,6,7,9,11}.   | <b>2.27.</b> {4,5,7,14,19}. |
| <b>2.28.</b> {4,5,7,14,19}. | <b>2.29.</b> {5,6,8,11,20}.  | <b>2.30.</b> {0,1,7,15,20}. |

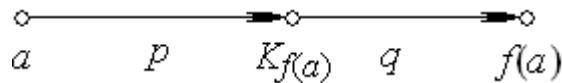
**Задача 3.** Пусть  $A=\{0,1,2,\dots,9\}$ ,  $B=\{0,1,2,3,4,5\}$ . Данна функция  $f(x) : A \rightarrow B$ . Начертить ее график и найти для нее область определения, область значений, прообраз каждого ее значения, ядерную эквивалентность и каноническое разложение.

Пусть  $f : A \rightarrow B$  есть некоторая функция. Определим на  $A$  отношение  $\sigma \in A \times A$ , положив  $\forall a \in A \ \forall b \in A (a \sim b \leftrightarrow f(a) = f(b))$ . Отношение  $\sigma$  есть отношение эквивалентности, так как выполняются следующие свойства:

- 1)  $a \sim a$ , ибо  $f(a) = f(a)$ .
- 2)  $a \sim b \rightarrow b \sim a$ , ибо  $f(a) = f(b) \rightarrow f(b) = f(a)$ .
- 3)  $a \sim b \ \& \ b \sim c \rightarrow a \sim c$ , ибо  $f(a) = f(b) \ \& \ f(b) = f(c) \rightarrow f(a) = f(c)$ .

Введенное отношение  $\sigma$  называется ядерной эквивалентностью для отображения  $f$ . Классы эквивалентности  $A/\sigma$  есть полные прообразы элементов множества  $B$  при отображении  $f$ , то есть  $A_b = f^{-1}(b)$ .

Отображение  $f$  можно разложить в композицию двух отображений согласно следующему рисунку:



Имеет место равенство  $f = q \circ p$ , то есть  $f(a) = q(p(a))$ .

Представление  $f = q \circ p$  называется каноническим разложением (представлением) функции  $f$ .

**Пример.** Пусть  $A=\{0,1,2,\dots,9\}$ ,  $B=\{0,1,2,3,4,5\}$ .

Получить каноническое разложение функции

$$f: A \rightarrow B, f = 0112105533 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 1 & 0 & 5 & 5 & 3 & 3 \end{pmatrix}.$$

Область определения  $D(f) = A$ . Область значений  $Im(f) = \{0,1,2,3,5\}$ . Классы эквивалентности:

$$K_0 = [0]_\sigma = f^{-1}(0) = \{0,5\}, q(K_0) = 0,$$

$$K_1 = [1]_\sigma = f^{-1}(1) = \{1,2,4\}, q(K_1) = 1,$$

$$K_2 = [2]_\sigma = f^{-1}(2) = \{3\}, q(K_2) = 2,$$

$$K_3 = [3]_\sigma = f^{-1}(3) = \{8,9\}, q(K_3) = 3,$$

$$K_5 = [5]_\sigma = f^{-1}(5) = \{6,7\}, q(K_5) = 5.$$

Функции  $p$  и  $q$  задаются следующим образом.

$$p(a) = K_{f(a)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ K_0 & K_1 & K_2 & K_1 & K_0 & K_5 & K_5 & K_3 & K_3 \end{pmatrix},$$

$$D(p) = A, Im(p) = \{K_0, K_1, K_2, K_3, K_5\}; q(K_a) = a = \begin{pmatrix} K_0 & K_1 & K_2 & K_3 & K_5 \\ 0 & 1 & 2 & 3 & 5 \end{pmatrix},$$

$$D(q) = \{K_0, K_1, K_2, K_3, K_5\}, Im(q) = \{0,1,2,3,5\}.$$

Каноническое представление функции  $f(a) = q(p(a))$ .

**Замечание.** Каноническое представление функции можно использовать в криптографии. Например, вместо текста

$$b_1 b_2 b_3 b_4 b_5 b_6 b_7 = 2355131 \text{ в алфавите } Im(f) = \{0,1,2,3,5\}$$

посыпаем шифротекст  $a_1 a_2 a_3 a_4 a_5 a_6 a_7$ , где всякое  $a_i \in K_i$ , например,

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 = 3967284, \text{ что дешифруется как}$$

$$f(a_1) f(a_2) f(a_3) f(a_4) f(a_5) f(a_6) f(a_7) = 235513.$$

**Варианты.** Получить каноническое разложение функции  $f: A \rightarrow B$ .

$A = \{0,1,\dots,14\}$ ,  $B = \{0,1,2,3,4,5\}$ . Значение функции  $f$  определяется номером варианта.

**3.1.** 310344501110451. **3.2.** 231434002301230. **3.3.** 220330511113242.

**3.4.** 321213141122123. **3.5.** 121231234121231. **3.6.** 210311023230443.

**3.7.** 545435544333453. **3.8.** 051411445533012. **3.9.** 010101012323231.

**3.10.** 346112301102210. **3.11.** 321233402121012. **3.12.** 343504030405454.

**3.13.** 233342351204502. **3.14.** 001113423034012. **3.15.** 103304250123423.

**3.16.** 012323234312032. **3.17.** 104203201204321. **3.18.** 323213213232310.

**3.19.** 110023245013245. **3.20.** 312323123231223. **3.21.** 240204040204040.

**3.22.** 531335153531555. **3.23.** 051212205005210. **3.24.** 450003205403231.

**3.25.** 023454320102030. **3.26.** 234143244312121. **3.27.** 010101000203431.

**3.28.** 054005545434502. **3.29.** 324132433151230. **3.30.** 023415233143200.

**Задача 4.** Решетка  $L$  задана своей диаграммой. Является ли она модулярной. Найти дополнения (если они есть) для элементов  $a, d, h, l$ .

Аксиомы решетки  $L$ .

1.  $a \vee a = a, a \wedge a = a.$
2.  $a \vee b = b \vee a, a \wedge b = b \wedge a.$
3.  $a \vee (b \vee c) = (a \vee b) \vee c, a \wedge (b \wedge c) = (a \wedge b) \wedge c.$
4.  $a \vee (a \wedge b) = a, a \wedge (a \vee b) = a.$

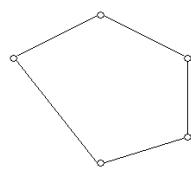
Дистрибутивность.

$$5. a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Модулярность.

$$5'. a \wedge (b \vee (a \wedge c)) = (a \wedge b) \vee (a \wedge c), a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c).$$

Пусть решетка  $L_1$  имеет следующий вид.



Решетка  $L$  модулярна  $\leftrightarrow$  решетка  $L_1$  не является ее подрешеткой.

Решетка, имеющая наименьший и наибольший элементы 0 и 1 называется решеткой с универсальными границами, обладающими следующими свойствами.

$$6. a \vee 1 = 1, a \vee 0 = a; a \wedge 1 = a, a \wedge 0 = 0.$$

Всякая конечная решетка имеет универсальные границы.

Дополнение элемента  $a$  решетки есть такой элемент  $\neg a$ , для которого  $a \vee \neg a = 1, a \wedge \neg a = 0$ .

Решетка задачи 4.30 модулярной не является.

Элементы  $c, d, h, j, e, k, f, l$  обратны к  $a$ .

Элементы  $e, k, f, l, a, b, j, g, i, m$  обратны к  $d$ .

Элементы  $e, k, f, l, a, b, j, g, i, m$  обратны к  $h$ .

Элементы  $c, d, h, j, e, k, a, b, g, i, m$  обратны к  $l$ .

**Варианты.**

4.1

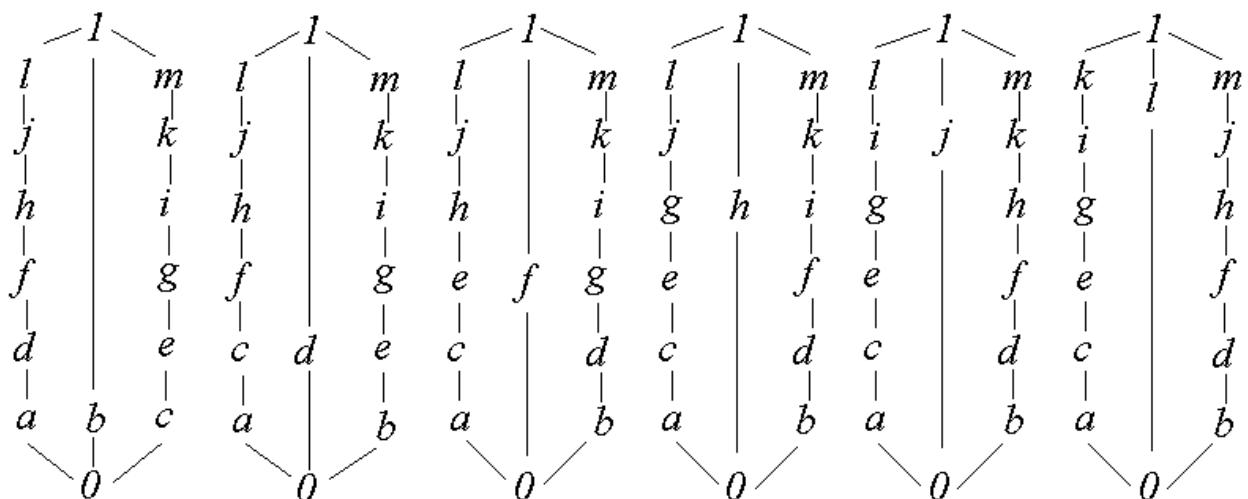
4.2

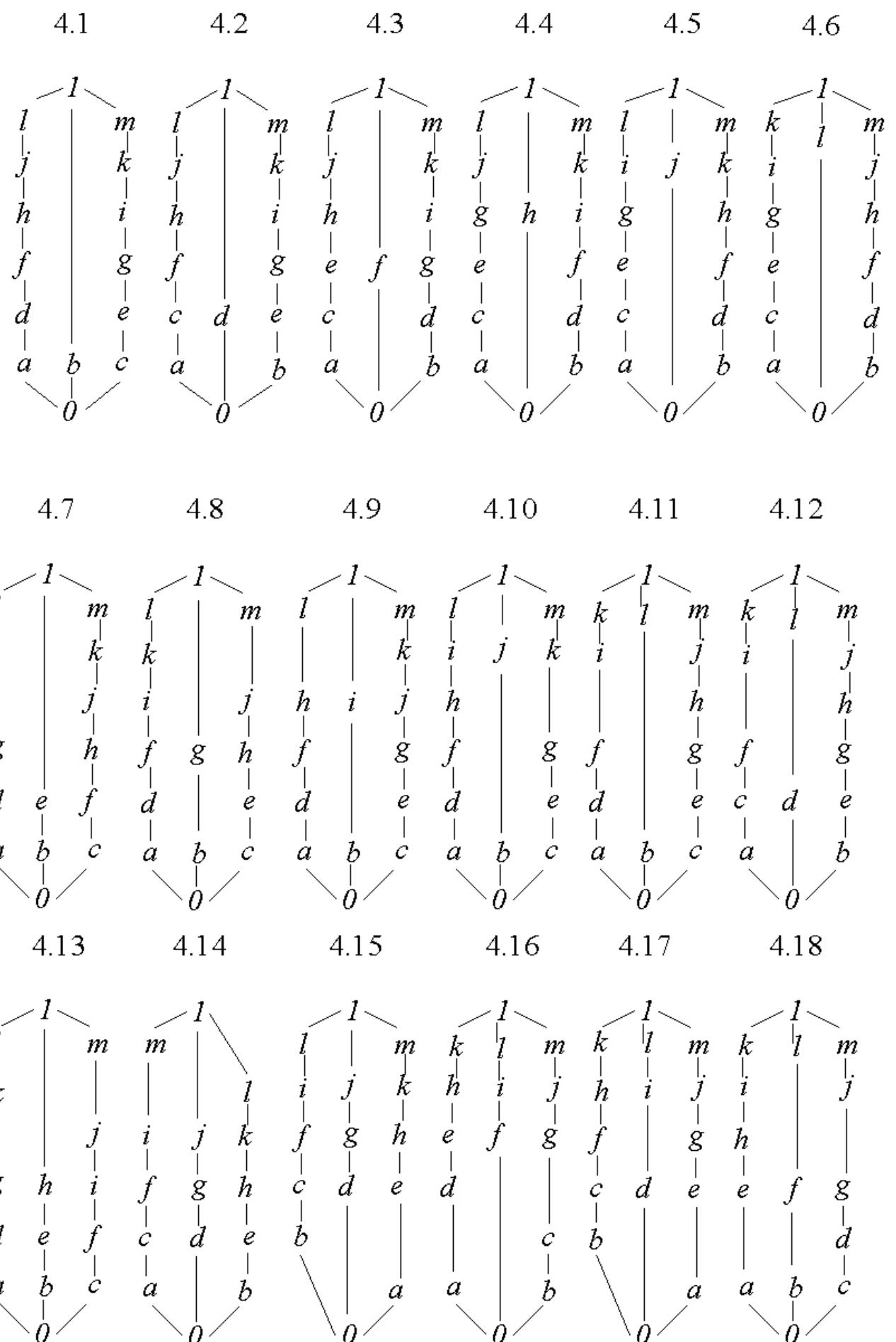
4.3

4.4

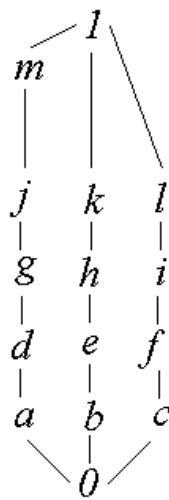
4.5

4.6

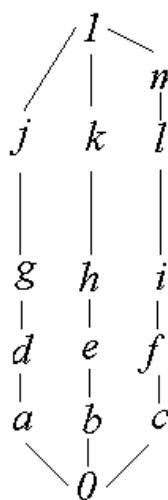




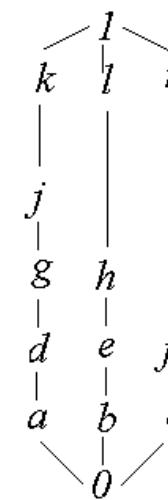
4.19



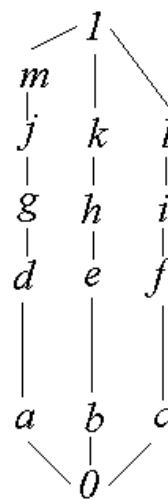
4.20



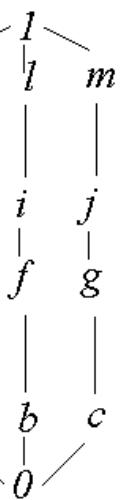
4.21



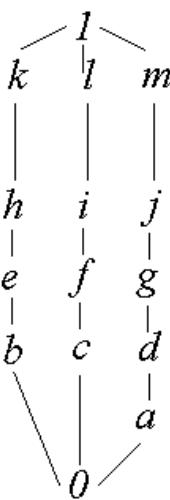
4.22



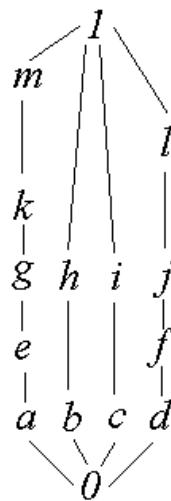
4.23



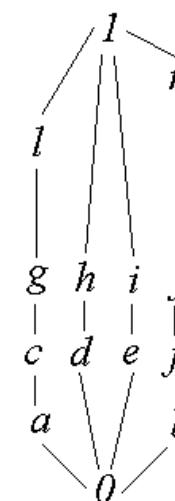
4.24



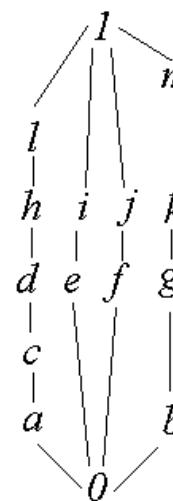
4.25



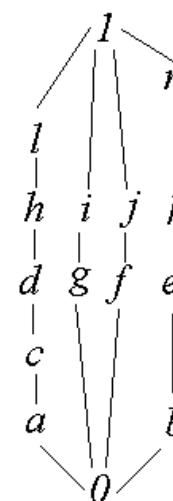
4.26



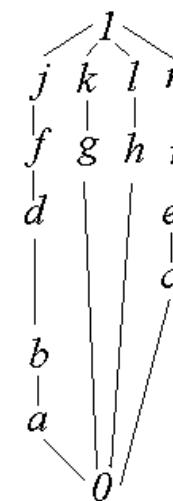
4.27



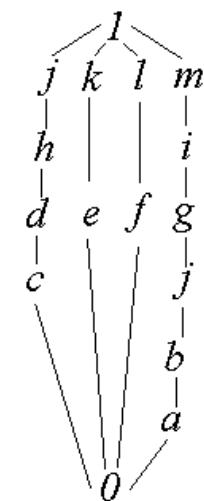
4.28



4.29



4.30



**Задача 5.** Найти все тупиковые и все наименьшие покрытия строк двоичной матрицы.

Пусть  $A = (a_{ij})$ ,  $i = 1, 2, \dots, m$ ,  $j = 1, 2, \dots, n$ , есть двоичная матрица, у которой  $m$  строк и  $n$  столбцов.

Столбец  $j$  двоичной матрицы  $A = (a_{ij})$  покрывает строку  $i$ , если  $a_{ij} = 1$ . Множество столбцов  $S$  называется *покрытием* строк двоичной матрицы  $A$ , если каждая строка из  $A$  покрыта некоторым столбцом из  $S$ . Покрытие  $S$  строк двоичной матрицы  $A$  называется *тупиковым*, если при удалении из  $S$  хотя бы одного столбца оставшееся множество столбцов покрытием уже не является. Покрытие, содержащее наименьшее число столбцов, называется *наименьшим*.

**Алгоритм нахождения всех тупиковых и наименьших покрытий**

1. Столбцу с номером  $j$  сопоставить символ  $x_j$ .

2. Построить решеточное выражение (функцию покрытий)

$$L = \bigwedge_{i=1}^n \left( \bigvee_{j=1}^m a_{ij} x_{ij} \right).$$

В решеточном выражении  $n$  скобок. Первая скобка  $(x_{1,j_1} \vee \dots \vee x_{1,j_k})$

означает, что строка 1 имеет единицы на местах  $j_1, \dots, j_k$  и потому покрыта столбцами  $x_{j_1}, \dots, x_{j_k}$ . Аналогично для покрытия строк 2, 3 …,  $m$ .

3. Перемножить скобки согласно аксиомам дистрибутивной решетки и получить ДНФ  $F_1$ .

4. В  $F_1$  произвести поглощение множителей по свойству  $x \cdot x = x$  в каждом слагаемом и получить ДНФ  $F_2$ .

5. В  $F_2$  произвести поглощение слагаемых по свойству  $x \vee xy = x$ , то есть меньшее слагаемое поглощает большее, если меньшее входит в большее как множество.

6. В полученной минимальной ДНФ  $F_3$  каждое слагаемое  $x_{j_1}, \dots, x_{j_k}$  дает тупиковое покрытие множеством столбцов  $\{j_1, \dots, j_k\}$ .

7. Выбираем из них все наименьшие.

$$\begin{array}{ccccccc} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 1 & 1 & 1 \\ 3 & 0 & 0 & 1 & 1 & 0 & 0 \\ 4 & 0 & 0 & 1 & 1 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}$$

1. Решеточное выражение (по строкам матрицы  $A$ )

$$L = (x_1 \vee x_2 \vee x_6)(x_2 \vee x_4 \vee x_5 \vee x_6)(x_3 \vee x_4)(x_3 \vee x_4 \vee x_5)(x_5 \vee x_6) = \\ x_1 x_3 x_5 \vee x_2 x_3 x_5 \vee x_2 x_4 x_5 \vee x_3 x_6 \vee x_4 x_6 \vee x_1 x_4 x_5.$$

2. Тупиковые покрытия множествами столбцов

$$\{x_1, x_3, x_5\}, \{x_2, x_3, x_5\}, \{x_2, x_4, x_5\}, \{x_3, x_6\}, \{x_4, x_6\}, \{x_1, x_4, x_5\}.$$

3. Наименьшие покрытия  $\{x_3, x_6\}, \{x_4, x_6\}$ .

### Варианты.

5.1.

5.2.

5.3.

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	1	1	0
0	0	0	0	1	1

1	1	1	0	0	0
0	1	0	1	1	1
0	0	1	1	0	1
0	0	1	1	1	0
0	0	0	0	1	1

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.4.**

1	1	0	0	0	1
0	1	1	1	1	1
1	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.5.**

1	1	1	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	0	1

**5.6.**

1	1	0	0	0	1
0	1	0	0	1	1
1	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.7.**

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
1	0	0	0	1	1

**5.8.**

1	1	0	0	0	1
0	1	0	0	1	1
0	0	1	1	0	0
0	0	1	0	1	0
1	0	0	1	1	1

**5.9.**

1	1	0	0	0	0
1	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.10.**

1	1	1	1	1	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.11.**

1	1	0	0	0	1
1	1	1	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.12.**

1	1	0	0	0	1
0	1	0	1	1	1
1	1	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.13.**

1	1	0	0	0	1
0	1	0	1	1	1
1	1	1	1	1	1
0	0	1	0	1	0
0	0	0	1	1	1

**5.14.**

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
1	1	1	1	1	1
0	0	0	1	1	1

**5.15.**

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
1	1	1	1	1	1

**5.16.**

1	1	0	0	0	1
0	0	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	1
0	0	0	1	1	1

**5.17.**

1	1	1	1	1	1
1	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.18.**

1	1	0	0	0	1
1	1	1	1	1	1
1	0	1	1	1	1
0	0	1	0	1	0
0	0	0	1	1	1

**5.19.**

**5.20.**

**5.21.**

1	1	0	0	0	1
0	1	0	1	1	1
1	1	1	1	1	1
1	0	1	0	1	0
0	0	0	1	1	1

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
1	1	1	1	1	1
1	1	0	1	1	1

0	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
1	1	1	1	1	1

**5.22.**

**5.23.**

**5.24.**

1	1	0	0	0	1
0	0	0	1	1	1
0	0	1	1	1	0
0	0	1	0	1	0
0	0	0	1	1	1

1	1	1	0	0	0
0	0	0	1	1	1
0	0	1	1	0	0
0	0	1	0	0	0
0	0	0	1	1	1

1	1	0	1	0	1
0	1	0	1	0	0
0	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	1

**5.25.**

**5.26.**

**5.27.**

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	1
0	0	1	0	0	1
0	0	0	1	1	1

1	1	0	0	0	1
0	1	0	0	1	1
0	0	1	1	0	0
0	0	1	1	1	0
0	0	0	1	1	1

1	1	0	0	0	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	1	0
1	0	0	0	1	1

**5.28.**

**5.29.**

**5.30.**

0	1	1	1	0	1
0	1	0	1	1	0
1	0	1	0	0	0
0	0	1	0	1	0
0	0	0	1	1	1

1	1	0	0	1	1
0	1	0	1	1	1
0	0	1	1	0	0
0	0	1	0	0	0
1	0	0	1	1	1

1	1	0	0	0	1
1	1	0	1	1	1
1	0	1	1	0	0
0	0	1	0	1	0
0	0	0	1	1	0

**Задача 6.** В булевой алгебре  $(A, \leq)$  всех подмножеств данного множества, упорядоченных по включению, с операциями  $\max(A,B) = A \cup B$ ,  $\min(A,B) = A \cap B$  найти булев полином для заданной функции  $f: 2^A \rightarrow \{0,1\}$  и получить представление множества  $Z = \{0,2,3\}$  из  $A = \{0,1,2,3\}$  булевым многочленом относительно независимых множеств.

$$f(z) = 0101100101011001 = \begin{cases} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{cases}.$$

$$U = \{0, 1, 2, 3\}, Z = \{0, 2, 3, 7, 10, 14\}.$$

Порождение множества всех подмножеств множества  $\{0,1,2,3\}$ .

A	0123	$2^U$	0 1 2 3 $x_1 x_2 x_3 x_4$	f(z)	Z
0	0000	$\emptyset$	0 0 0 0	0	1
1	0001	{3}	0 0 0 1	1	0
2	0010	{2}	0 0 1 0	0	1
3	0011	{2,3}	0 0 1 1	1	1
4	0100	{1}	0 1 0 0	1	0
5	0101	{1,3}	0 1 0 1	0	0
6	0110	{1,2}	0 1 1 0	0	0
7	0111	{1,2,3}	0 1 1 1	1	1
8	1000	{0}	1 0 0 0	0	0
9	1001	{0,3}	1 0 0 1	1	0
10	1010	{0,2}	1 0 1 0	0	1
11	1011	{0,2,3}	1 0 1 1	1	0
12	1100	{0,1}	1 1 0 0	0	0
13	1101	{0,1,3}	1 1 0 1	0	0
14	1110	{0,1,2}	1 1 1 0	0	1
15	1111	{0,1,2,3}	1 1 1 1	1	0
			$A_1 A_2 A_3 A_4$		

Порождающие множества (в объединении дающих все множество A).

$$A_1 = \{8, 9, 10, 11, 12, 13, 14, 15\},$$

$$A_2 = \{4, 5, 6, 7, 12, 13, 14, 15\},$$

$$A_3 = \{2, 3, 6, 7, 10, 11, 14, 15\},$$

$$A_4 = \{1, 3, 5, 7, 9, 11, 13, 15\}.$$

Вектор  $\mathbf{x}(z) = (x_1(z), x_2(z), x_3(z), x_4(z))$ .

Обозначения:

$$A^\sigma = \begin{cases} A^1 = A, & \text{если } \sigma = 1, \\ A^0 = \bar{A} = -A = U - A, & \text{если } \sigma = 0. \end{cases} \quad x^\sigma = \begin{cases} x^1 = x, & \text{если } \sigma = 1, \\ x^0 = \bar{x} = -x, & \text{если } \sigma = 0. \end{cases}$$

$$\mathbf{c} = (c_1, c_2, c_3, c_4).$$

Функция алгебры логики (СДНФ)

$$\varphi(x_1, x_2, x_3, x_4) = \bigvee_{f(c)=1} x_1^{c_1} x_2^{c_2} x_3^{c_3} x_4^{c_4} =$$

$$\bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \vee \bar{x}_1 \bar{x}_2 x_3 x_4 \vee \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \vee \bar{x}_1 x_2 x_3 x_4 \vee x_1 \bar{x}_2 \bar{x}_3 x_4 \vee x_1 \bar{x}_2 x_3 x_4 \vee x_1 x_2 \bar{x}_3 x_4.$$

Булев полином

$$f(z) = \varphi(\mathbf{x}(z)) = \varphi(x_1(z), x_2(z), x_3(z), x_4(z)) =$$

$$\bigvee_{f(a)=1} x_1(z)^{x_1(a)} x_2(z)^{x_2(a)} x_3(z)^{x_3(a)} x_4(z)^{x_4(a)} =$$

$$\bar{x}_1(z) \bar{x}_2(z) \bar{x}_3(z) x_4(z) \vee \bar{x}_1(z) \bar{x}_2(z) x_3(z) x_4(z) \vee \bar{x}_1(z) x_2(z) \bar{x}_3(z) \bar{x}_4(z) \vee$$

$$\bar{x}_1(z) x_2(z) x_3(z) x_4(z) \vee x_1(z) \bar{x}_2(z) \bar{x}_3(z) x_4(z) \vee x_1(z) \bar{x}_2(z) x_3(z) x_4(z) \vee$$

$$x_1(z) x_2(z) x_3(z) x_4(z).$$

Представление Z через независимые множества.

$$Z = \bigcup_{a \in Z} (A_1^{x_1(a)} \cap A_2^{x_2(a)} \cap A_3^{x_3(a)} \cap A_4^{x_4(a)}) =$$

$$\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4 \cup \bar{A}_1 \cap \bar{A}_2 \cap A_3 \cap \bar{A}_4 \cup \bar{A}_1 \cap \bar{A}_2 \cap A_3 \cap A_4 \cup \bar{A}_1 \cap A_2 \cap A_3 \cap A_4 \cup$$

$$A_1 \cap \bar{A}_2 \cap A_3 \cap \bar{A}_4 \cup A_1 \cap A_2 \cap A_3 \cap \bar{A}_4.$$

### Варианты.

- 6.1.** 1001001110011011.    **6.2.** 0010100011011111.  
**6.3.** 1101111100100010.    **6.4.** 1001100110111001.  
**6.5.** 1110110011001100.    **6.6.** 1101110110001010.  
**6.7.** 1010100011011101.    **6.8.** 1110110011001100.  
**6.9.** 1101001000111011.    **6.10.** 1010000011011111.  
**6.11.** 1010100001110111.    **6.12.** 1010101001011101.  
**6.13.** 0110111011000110.    **6.14.** 1110010011101100.  
**6.15.** 0111110100101010.    **6.16.** 0010100011111101.  
**6.17.** 1100011011101100.    **6.18.** 1111001000111011.  
**6.19.** 001101111100111.    **6.20.** 1010001101110011.  
**6.21.** 1110011111100001.    **6.22.** 0010001001010111.  
**6.23.** 1101110110001010.    **6.24.** 0111001001111010.  
**6.25.** 1011011100001011.    **6.26.** 1010001111011011.  
**6.27.** 1101101011010010.    **6.28.** 1010100001111111.  
**6.29.** 0111110110001010.    **6.30.** 0101100011110010.

**Задача 7.** Построить на координатной плоскости отношения  $r$  и  $s$ . Найти свертку отношений  $r \circ s$  и построить ее на координатной плоскости.

**Пример.** Свертка.  $\rho = \begin{bmatrix} 0 & 2 & 0 \\ 1 & 2 & 1 \\ 0 & 3 & 2 \\ 1 & 1 & 3 \end{bmatrix}$ ,  $\sigma = \begin{bmatrix} 0 & 1 \\ 0 & 2 \\ 1 & 3 \\ 2 & 0 \end{bmatrix}$ ,  $\rho^* \sigma = \begin{bmatrix} 0 & 2 & 1 \\ 0 & 2 & 2 \\ 1 & 2 & 3 \\ 0 & 3 & 0 \end{bmatrix}$ .

### Варианты.

- 7.1.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,+\infty)$ ,  
 $r = \{(x,y) : y=x+3\}$ ,  $s = \{(x,y) : y \geq \sin x\}$ .
- 7.2.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times \mathbb{R}$ ,  
 $r = \{(x,y) : y=x+3\}$ ,  $s = \{(x,y) : x^2+y^2 \leq 25\}$ .
- 7.3.**  $r \subseteq (0,2) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (-1,1)$ ,  
 $r = \{(x,y) : y=x/3\}$ ,  $s = \{(x,y) : y=x^2\}$ .
- 7.4.**  $r \subseteq (-1,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,0.5)$ ,  
 $r = \{(x,y) : y=x\}$ ,  $s = \{(x,y) : y=3x\}$ .
- 7.5.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,1)$ ,  
 $r = \{(x,y) : x^2 \leq y^2\}$ ,  $s = \{(x,y) : x^2+y^2=4\}$ .
- 7.6.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,1)$ ,  
 $r = \{(x,y) : x=5y+3\}$ ,  $s = \{(x,y) : x^2+y^2 \leq 4\}$ .

**7.7.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (2,4)$ ,

$$r = \{(x,y) : y=2x+3\}, \quad s = \{(x,y) : y=\cos x\}.$$

**7.8.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 \leq 4\}, \quad s = \{(x,y) : y=x^2+2\}.$$

**7.9.**  $r \subseteq (-2,2) \times (-2,2)$ ,  $s \subseteq (-2,2) \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 = 3\}, \quad s = \{(x,y) : x=5y+1\}.$$

**7.10.**  $r \subseteq (-2,2) \times (-2,2)$ ,  $s \subseteq (-2,2) \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 \geq 3\}, \quad s = \{(x,y) : y=5x^2-1\}.$$

**7.11.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0, +\infty)$ ,

$$r = \{(x,y) : y=x+3\}, \quad s = \{(x,y) : y \leq \sin x\}.$$

**7.12.**  $r \subseteq (-1,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,5)$ ,

$$r = \{(x,y) : y=2x^2\}, \quad s = \{(x,y) : y=3x\}.$$

**7.13.**  $r \subseteq (0,2) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (-1,1)$ ,

$$r = \{(x,y) : y=x^3\}, \quad s = \{(x,y) : y=x^2\}.$$

**7.14.**  $r \subseteq (-1,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,0.5)$ ,

$$r = \{(x,y) : y=x^2\}, \quad s = \{(x,y) : y=3/x\}.$$

**7.15.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,1)$ ,

$$r = \{(x,y) : 2x \leq y^2\}, \quad s = \{(x,y) : x^2+y^2 = 4\}.$$

**7.16.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,1)$ ,

$$r = \{(x,y) : x=y+3\}, \quad s = \{(x,y) : x^2+y^2 \leq 4\}.$$

**7.17.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (2,4)$ ,

$$r = \{(x,y) : y=2x\}, \quad s = \{(x,y) : y=\cos x\}.$$

**7.18.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 \leq 4\}, \quad s = \{(x,y) : y=x^2-2\}.$$

**7.19.**  $r \subseteq (-2,2) \times (-2,2)$ ,  $s \subseteq (-2,2) \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 = 1\}, \quad s = \{(x,y) : x=5y+1\}.$$

**7.20.**  $r \subseteq (-2,2) \times (-2,2)$ ,  $s \subseteq (-2,2) \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 \geq 1\}, \quad s = \{(x,y) : y=5x-1\}.$$

**7.21.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,+\infty)$ ,

$$r = \{(x,y) : y=2x\}, \quad s = \{(x,y) : y \geq \sin x\}.$$

**7.22.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times \mathbb{R}$ ,

$$r = \{(x,y) : y=x+3\}, \quad s = \{(x,y) : x^2+y^2 \leq 16\}.$$

**7.23.**  $r \subseteq (0,2) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (-1,1)$ ,

$$r = \{(x,y) : y=1/x-3x\}, \quad s = \{(x,y) : y=x^2\}.$$

**7.24.**  $r \subseteq (-1,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,0.5)$ ,

$$r = \{(x,y) : y=x^2-x\}, \quad s = \{(x,y) : y=3/x\}.$$

**7.25.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,1)$ ,

$$r = \{(x,y) : 2x \leq y^2\}, \quad s = \{(x,y) : 2x^2+y^2=4\}.$$

**7.26.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (0,1)$ ,

$$r = \{(x,y) : x=y+3\}, \quad s = \{(x,y) : 2x^2+y^2 \leq 4\}.$$

**7.27.**  $r \subseteq (0,1) \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times (2,4)$ ,

$$r = \{(x,y) : y=1/x+2x\}, \quad s = \{(x,y) : y=\cos x\}.$$

**7.28.**  $r \subseteq \mathbb{R} \times \mathbb{R}$ ,  $s \subseteq \mathbb{R} \times \mathbb{R}$ ,

$$r = \{(x,y) : 2x^2+y^2 \leq 4\}, \quad s = \{(x,y) : y=x^2-2\}.$$

**7.29.**  $r \subseteq (-2,2) \times (-2,2)$ ,  $s \subseteq (-2,2) \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2=1\}, \quad s = \{(x,y) : x^2=5y+1\}.$$

**7.30.**  $r \subseteq (-2,2) \times (-2,2)$ ,  $s \subseteq (-2,2) \times \mathbb{R}$ ,

$$r = \{(x,y) : x^2+y^2 \geq 1\}, \quad s = \{(x,y) : y=5x^2-1/y\}.$$

**Задача 8.** Привести пример бесконечного отношения эквивалентности  $r$ , вложенного в  $A \times A$  и порождающего ровно  $n$  классов эквивалентности.

Показать, что приведенное отношение соответствует определению отношения эквивалентности.  $\mathbb{N}, \mathbb{Q}, \mathbb{R}$  есть множества соответственно натуральных, рациональных, вещественных чисел.

Пусть  $A$  есть произвольное множество.

**Определение.** Бинарное отношение  $\sigma \subseteq A \times A$  есть *отношение эквивалентности* (обозначение  $a \sim b$ ), если оно удовлетворяет следующим аксиомам:  $\forall a,b,c \in A$

1.  $a \sim a$ , рефлексивность,
2.  $a \sim b \rightarrow b \sim a$ , коммутативность,
3.  $a \sim b \ \& \ b \sim c \rightarrow a \sim c$ , транзитивность.

**Обозначение.**  $a \sim b$ ,  $\sigma(a,b)$ ,  $(a,b) \in \sigma$ ,  $a \sigma b$ .

**Определение.** *Разбиение* множества  $A$  есть семейство попарно непересекающихся подмножеств из  $A$ , в объединении (в сумме) дающих все  $A$ :  $A = \bigcup_{i \in I} A_i$ ,  $A_i \cap A_j = \emptyset \ \forall i \neq j$ . Подмножества  $A_i$  называются смежными классами разбиения.

**Пример.**  $A = \{0,1,2,3,4,5\} = \{0,1,5\} \cup \{2\} \cup \{3,4\}$ .

**Теорема.** 1. Каждому отношению эквивалентности, определенному на множестве  $A$ , соответствует некоторое разбиение множества  $A$ .

2. Каждому разбиению множества  $A$  соответствует некоторое отношение эквивалентности.

Коротко: между классом всех определенных на множестве  $A$  эквивалентностей и классом всех разбиений множества  $A$  существует взаимно однозначное соответствие.

**Замечание.** 1. Разбиение множества  $A$  на одноэлементные подмножества  $A = \bigcup_{a \in A} \{a\}$  и разбиение  $A$ , состоящее из одного только множества  $A$ , называются тривиальными (несобственными) разбиениями.

2. Разбиение  $A$  на одноэлементные подмножества соответствует отношению эквивалентности, которое есть равенство.

3. Разбиение множества  $A$  состоящее из одного только множества  $A$ , соответствует отношению эквивалентности, содержащему все множество  $A \times A$ .

### Варианты.

**8.1.**  $A = \mathbb{R}, n=3.$

**8.2.**  $A = \mathbb{R}, n=4.$

**8.3.**  $A = \mathbb{R}, n=5.$

**8.4.**  $A = \mathbb{R}, n=2.$

**8.5.**  $A = (0,10], n=3.$

**8.6.**  $A = (0,10], n=4.$

**8.7.**  $A = (0,10], n=5.$

**8.8.**  $A = (0,10], n=10.$

**8.9.**  $A = [0,10001), n=3.$

**8.10.**  $A = [0,10001), n=4.$

**8.11.**  $A = [0,10001), n=5.$

**8.12.**  $A = [0, 10001), n=6.$

**8.13.**  $A = [-3,3], n=3.$

**8.14.**  $A = [-3,3], n=4.$

**8.15.**  $A = [-3,3], n=5.$

**8.16.**  $A = [-3,3], n=6.$

**8.17.**  $A = [1,10], n=5.$

**8.18.**  $A = [1,10), n=3.$

**8.19.**  $A = [1,10], n=4.$

**8.20.**  $A = [1,10), n=7.$

**8.21.**  $A = \mathbb{Q}, n=3.$

**8.22.**  $A = \mathbb{Q}, n=4.$

**8.23.**  $A = \mathbb{Q}, n=5.$

**8.24.**  $A = \mathbb{Q}, n=7.$

**8.25.**  $A = \mathbb{Q}, n=9.$

**8.26.**  $A = \mathbb{N}, n=3.$

**8.27.**  $A = \mathbb{N}, n=4.$

**8.28.**  $A = \mathbb{N}, n=5.$

**8.29.**  $A = \mathbb{N}, n=7.$

**8.30.**  $A = \mathbb{N}, n=9.$

**Задача 9.** Найти решение линейного неоднородного рекуррентного уравнения с постоянными коэффициентами.

**Определение.** Уравнения  $(R_0)$  и  $(R_1)$

$$L(x(k)) = a_n \cdot x(k+n) + a_{n-1} \cdot x(k+n-1) + \dots + a_0 \cdot x(k) = \begin{cases} 0, & (R_0) \\ f(k), & (R_1) \end{cases}$$

где  $a_i \in \mathbb{R}, i=0,1,\dots,n; a_n \neq 0; f(k) \neq 0$  есть известная функция,  $x(k)$  есть неизвестная функция, называются линейными рекуррентными уравнениями (ЛРУ) порядка  $n$ , однородным и неоднородным соответственно с постоянными коэффициентами. Коэффициент  $a_n(k)$  называется старшим. Уравнение со старшим коэффициентом 1 называется нормированным уравнением.

Уравнения  $(R_0)$  и  $(R_1)$  называют также стационарными ЛРУ (СЛРУ) однородным и неоднородным соответственно.

**Определение.** Выражение

$$L(\lambda) = a_n \cdot \lambda^n + a_{n-1} \cdot \lambda^{n-1} + a_{n-2} \cdot \lambda^{n-2} + \dots + a_1 \cdot \lambda + a_0$$

называется *характеристическим полиномом*, а выражение  $L(\lambda)=0$  *характеристическим уравнением* для однородного СЛРУ ( $R_0$ ) (равно как и для неоднородного СЛРУ ( $R_1$ )).

**Теорема.** Если

$\lambda_1, \dots, \lambda_p$  есть вещественные корни характеристического уравнения;

$l_1, \dots, l_p$  есть их кратности;

$\mu_1, \dots, \mu_s$  есть группа комплексных корней  $\mu_j = \alpha_j + i\beta_j$ ,  $j=1,2,\dots,s$ ;

$\bar{\mu}_1, \dots, \bar{\mu}_s$  есть группа комплексно сопряженных корней  $\bar{\mu}_j = \alpha_j - i\beta_j$ ,

$j=1,2,\dots,s$ ;

$r_1, \dots, r_s$  есть их кратности;

$\rho_j, \varphi_j$  есть модуль и аргумент комплексного числа  $\mu_j$ ,  $j=1,\dots,s$ ,  
то функции

$$x_j(k) = k^{m_j} \cdot \lambda_j^k, \quad j=1,\dots,p; \quad m_j=0,\dots,l_{j-1},$$

$$y_j(k) = k^{m_j} \cdot \rho_j^k \cdot \cos(\varphi_j \cdot k), \quad j=1,\dots,s; \quad m_j=0,\dots,r_j-1,$$

$$z_j(k) = k^{m_j} \cdot \rho_j^k \cdot \sin(\varphi_j \cdot k), \quad j=1,\dots,s; \quad m_j=0,\dots,r_j-1,$$

составляют ФСР для однородного СЛРУ ( $R_0$ ).

**Замечание.** 1. Если  $x_1(k), \dots, x_n(k)$  есть ФСР для однородного СЛРУ ( $R_0$ ), то его общее решение

$$x_{\text{оо}}(k) = C_1 x_1(k) + \dots + C_n x_n(k),$$

где произвольные постоянные  $C_1, \dots, C_n$  пробегают  $\mathbb{R}$  независимо друг от друга.

Если  $x_{\text{чн}}$  есть какое-либо частное решение неоднородного СЛРУ ( $R_1$ ), то его общее решение

$$x_{\text{ои}}(k) = x_{\text{чн}}(k) + C_1 x_1(k) + \dots + C_n x_n(k).$$

2. Частное решение неоднородного СЛРУ  $R_1$  с правой частью – квазиполиномом  $f(k) = P_m(k) \cdot \lambda^k$  может быть найдено в виде  $k^r Q_m(k) \cdot \lambda^k$ , где  $r$  – кратность корня  $\lambda$  характеристического уравнения.

3. Уравнение

$$a_n x(k+n) + a_{n-1} x(k+n-1) + \dots + a_{n-r} x(k+n-r) = f(k), \quad k = 0, 1, 2, \dots$$

допускает понижение порядка. Это уравнение имеет характеристическое уравнение

$$\begin{aligned} a_n \lambda^n + a_{n-1} \lambda^{n-1} + a_{n-2} \lambda^{n-2} + \dots + a_{n-r} \lambda^{n-r} = \\ \lambda^{n-r} (a_n \lambda^r + a_{n-1} \lambda^{r-1} + a_{n-2} \lambda^{r-2} + \dots + a_{n-r+1} \lambda + a_{n-r}) = 0 \end{aligned}$$

с корнем  $\lambda = 0$  кратности  $n-r$ . Решение исходного уравнения совпадает с решением уравнения

$$a_n y(k+r) + a_{n-1} y(k+r-1) + \dots + a_{n-r} y(k) = f(k-(n-r)), \quad k = n-r, n-r+1, \dots$$

порядка  $r$  с характеристическим уравнением

$$a_n \lambda^r + a_{n-1} \lambda^{r-1} + a_{n-2} \lambda^{r-2} + \dots + a_{n-r+1} \lambda + a_{n-r} = 0$$

без нулевых корней.

В самом деле, из первого уравнения

$$x(k+n) = (f(k) - a_{n-1}x(k+n-1) - \dots - a_{n-r}x(k+n-r))/a_n, \quad k=0,1,2,\dots$$

Из второго уравнения

$$y(k+r) = (f(k-(n-r)) - a_{n-1}y(k+r-1) - \dots - a_{n-r}y(k))/a_n, \quad k=n-r, n-r+1,\dots$$

При указанных значениях  $k$  обе последовательности одинаковы. Вместо второго уравнения удобней решить уравнение

$$z(k+r) = (f(k) - a_{n-1}z(k+r-1) - \dots - a_{n-r}z(k))/a_n, \quad k=0,1,2,\dots$$

и тогда  $y(k+r) = z(k)$ ,  $k=0,1,2,\dots$

Поэтому  $x(k) = z(k-r)$ ,  $k=n-r, n-r+1, n-r+2,\dots$

**Пример.**  $x(k+5) - 6 \cdot x(k+4) + 9 \cdot x(k+3) = 3k-1$ ,  $k=0,1,2,\dots$

$$x(0) = 1, x(1) = 0, x(2) = 1, x(3) = 3, x(4) = 0.$$

Характеристическое уравнение

$$\lambda^5 - 6\lambda^4 + 9\lambda^3 = 0, \quad \lambda^3(\lambda^2 - 6\lambda + 9) = 0, \quad \lambda^3(\lambda - 3)^2 = 0.$$

Корни:  $\lambda=0$  кратности 3,  $\lambda=3$  кратности 2.

Переходим к эквивалентному уравнению

$$y(k+2) - 6 \cdot y(k+1) + 9 \cdot y(k) = 3(k-3) - 1 = 3k-10, \quad k=3,4,\dots, \quad (*)$$

$$y(0) = 1, y(1) = 0, y(2) = 1, y(3) = 3, y(4) = 0.$$

Решение  $y(k)$  уравнения (\*), начиная с  $k=3$ , совпадет с решением  $z(k)$  уравнения

$$z(k+2) - 6z(k+1) + 9z(k) = 3k-1, \quad k=0,1,2,\dots, \quad (**)$$

$z(0) = 3, z(1) = 0$ , в том смысле, что решение  $y(k+3) = z(k)$ ,  $k=0,1,2,\dots$

Характеристическое уравнение для уравнения (\*\*)

$$\lambda^2 - 6\lambda + 9 = 0, \quad (\lambda - 3)^2 = 0.$$

Корень  $\lambda=3$  кратности 2.

$$z_{\text{он}}(k) = z_{\text{чн}}(k) + z_{\text{оо}}(k) = z_{\text{чн}}(k) + C_1 \cdot 3^k + C_2 k \cdot 3^k.$$

$$z_{\text{чн}}(k) = z(k) = ak+b, \quad z(k+1) = a(k+1) + b = ak + a + b,$$

$$z(k+2) = a(k+2) + b = ak + 2a + b.$$

Подставляем  $z(k)$ ,  $z(k+1)$ ,  $z(k+2)$  в уравнение

$z(k+2) - 6z(k+1) + 9z(k) = 3k-1$  и получаем:

$$ak + 2a + b - 6(ak + a + b) + 9(ak + b) = 3k - 1,$$

$$4ak - 4a + 4b = 3k - 1, \quad \begin{cases} 4a = 3, \\ -4a + 4b = -1, \end{cases} \quad \begin{cases} a = 3/4, \\ b = -2/4, \end{cases} \quad z_{\text{чн}}(k) = \frac{3}{4}k + \frac{2}{4},$$

$$z_{\text{он}}(k) = \frac{3k+2}{4} + C_1 \cdot 3^k + C_2 k \cdot 3^k. \quad \text{Найдем } C_1, C_2.$$

$$z_{\text{он}}(0) = \frac{3 \cdot 0 + 2}{4} + C_1 \cdot 3^0 + C_2 \cdot 0 \cdot 3^0 = 2/4 + C_1 + C_2 \cdot 0 \cdot 3^0 = 3,$$

$$z_{\text{он}}(1) = \frac{3 \cdot 1 + 2}{4} + C_1 \cdot 3^1 + C_2 \cdot 1 \cdot 3^1 = 5/4 + 3C_1 + 3C_2 = 0,$$

$$C_1 = 10/4, \quad 3C_2 = -5/4 - 3C_1 = -5/4 - 30/4 = -35/4; \quad C_1 = 10/4, \quad C_2 = -\frac{35}{4 \cdot 3},$$

$$z(k) = \frac{3k+2}{4} + \frac{10}{4} \cdot 3^k - \frac{35}{4 \cdot 3} k \cdot 3^k, \quad k=0,1,2,\dots$$

*Ответ.*  $x(0) = 1, x(1) = 0, x(2) = 1,$

$$x(k) = z(k-3) = \frac{3(k-3)+2}{4} + \frac{10}{4} \cdot 3^{k-3} - \frac{35}{4 \cdot 3} (k-3) \cdot 3^{k-3}, \quad k=3,4,5,\dots$$

### Варианты.

Начальные условия:

$x(0)=1, x(1)=0, x(2)=1$  для уравнения порядка 3;

$x(0)=1, x(1)=0, x(2)=1, x(3)=2$  для уравнения порядка 4;

$x(0)=1, x(1)=0, x(2)=1, x(3)=1, x(4)=2$  для уравнения порядка 5;

**9.1.**  $x(k+3) + 3x(k+2) + 2x(k+1) = 1-k^2.$

**9.2.**  $x(k+3) - x(k+2) = 6k^2 + 3k.$

**9.3.**  $x(k+3) - x(k+1) = k^2 + k.$

**9.4.**  $x(k+4) - 3x(k+3) + 3x(k+2) - x(k+1) = 2k.$

**9.5.**  $x(k+4) - x(k+3) = 5(k+2)^2.$

**9.6.**  $x(k+4) - x(k+3) + x(k+2) = 2k(1-k).$

**9.7.**  $x(k+4) + 2x(k+3) + x(k+2) = k^2 + k - 1.$

**9.8.**  $x(k+5) - x(k+4) = 2k + 3.$

**9.9.**  $3x(k+4) + x(k+3) = 6k - 1.$

**9.10.**  $x(k+4) + 2x(k+3) + x(k+2) = 4k^2.$

**9.11.**  $x(k+3) + x(k+2) = 5k^2 - 1.$

**9.12.**  $x(k+4) + 4x(k+3) + 4x(k+2) = -k^2 + k$

**9.13.**  $7x(k+3) - x(k+2) = 12k.$

**9.14.**  $x(k+3) + 3x(k+2) + 2x(k+1) = 3k^2 + 2k.$

**9.15.**  $x(k+3) - x(k+1) = 3k^2 - 2k + 1.$

**9.16.**  $x(k+3) - x(k+2) = 4k^2 - 3k + 2.$

**9.17.**  $x(k+4) - 3x(k+3) + 3x(k+2) - x(k+1) = k-3.$

**9.18.**  $x(k+4) + 2x(k+3) + x(k+2) = 12k^2 - 6k.$

**9.19.**  $x(k+3) - 4x(k+2) = 32 - 384k^2.$

**9.20.**  $x(k+4) + 2x(k+3) + x(k+2) = 2 - 3k^2.$

**9.21.**  $x(k+3) + x(k+2) = 49 - 24k^2.$

**9.22.**  $x(k+3) - 2x(k+2) = 3k^2 + k - 4.$

**9.23.**  $x(k+3) - 13x(k+2) + 12x(k+1) = k - 1.$

**9.24.**  $x(k+4) + x(k+3) = k.$

**9.25.**  $x(k+3) - x(k+2) = 6k + 5.$

**9.26.**  $x(k+3) + 3x(k+2) + 2x(k+1) = k^2 + 2k + 3.$

**9.27.**  $x(k+3) - 5x(k+2) + 6x(k+1) = (k-1)^2.$

**9.28.**  $x(k+4) - 6x(k+3) + 9x(k+2) = 3k - 1.$

**9.29.**  $x(k+3) - 13x(k+2) + 12x(k+1) = 18k^2 - 39.$

**9.30.**  $x(k+4) + x(k+3) = 12k + 6.$

## 2. КОМБИНАТОРИКА

### *Формулы для размещения, перестановки, сочетаний*

$$A_n^r = \frac{n!}{(n-r)!}. \quad P_n = n! \quad \hat{A}_n^r = n^r. \quad \hat{P}_n = n^n. \quad C_n^r = C_n^{n-r} = \frac{n!}{r!(n-r)!}.$$

$$\hat{C}_n^r = C_{n+r-1}^r. \quad P_n(k_1, k_2, \dots, k_r) = \frac{n!}{k_1! k_2! \dots k_r!}. \quad A_n^r(k_1, k_2, \dots, k_n) = \frac{r!}{k_1! k_2! \dots k_n!}.$$

$$(1+t)^n = \sum_{r=0}^n C_n^r t^r. \quad (a+b)^n = \sum_{r=0}^n C_n^r a^r b^{n-r}. \quad 2^n = \sum_{r=0}^n C_n^r.$$

$$(1-t)^n = \sum_{r=0}^n (-1)^r C_n^r t^r. \quad 0 = \sum_{r=0}^n (-1)^r C_n^r.$$

$$\left( \sum_{r=0}^k a_r \right)^n = \sum_{n_1+n_2+\dots+n_k=r} \frac{n!}{n_1!n_2!\dots n_k!} a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}.$$

**Задача 1.** Преподаватель принимает зачет в группе из  $N+10$  человек. Найти число вариантов очередности опроса студентов.  $N$  есть номер фамилии студента в аудиторном журнале. *Ответ.*  $P(N+10)$ .

**Задача 2.** В каталоге библиотеки приведены наименования  $N+100$  различных журналов. Найти число способов выбора пяти попарно различных журналов? *Ответ.*  $C(N+10, 5)$ .

**Задача 3.** У англичан принято давать детям несколько имен. Сколькими способами можно назвать ребенка, если ему дают три имени, а общее число имен равно  $N+300$ ? Способы, отличающиеся лишь порядком имен, считать различными. *Ответ.*  $A(N+300, 3)$ .

**Задача 4.** Сколькими способами можно выбрать 7 делегатов на конференцию от коллектива в  $N+200$  человек? *Ответ.*  $C(N+200, 7)$ .

**Задача 5.** Группа из  $N+10$  студентов должна сдать 5 экзаменов. Каково число возможных расписаний сдачи экзаменов? *Ответ.* 5!

**Задача 6.** В районе имеется  $N+10$  памятников. Время позволяет осмотреть только 3 из них. Укажите число возможных маршрутов. Порядок прохождения маршрутов существенен. *Ответ.*  $A(N+10, 3)$ .

**Задача 7.** Студентам предложено на выбор  $N+5$  гуманитарных курсов. Сколькими способами студент может выбрать 3 из них? *Ответ.*  $C(N+5, 3)$ .

**Задача 8.** Сколькими способами можно рассадить  $N+20$  студентов (по одному за каждым компьютером) в дисплейном классе, оснащенном 20 компьютерами? Номера компьютеров существенны. *Ответ.*  $A(N+20, 20)$ .

**Задача 9.** В соревновании участвуют  $N+15$  спортсменов. Укажите число вариантов очередности их выступления. *Ответ.*  $P(N+15)$ .

**Задача 10.** В отделе работает  $N+12$  сотрудников, которые могут уходить в отпуск только по одному. Сколько вариантов распределения отпусков в год возможно? *Ответ.*  $A(N+12, 12)$ .

**Задача 11.** В киоске имеется  $N + 10$  сортов мороженого одинаковой стоимости. Сколькими способами можно купить 3 порции мороженого попарно различных сортов? *Ответ.*  $C(N+10, 3)$ .

**Задача 12.** Группа из  $N + 23$  человека должна выполнить лабораторную работу. Сколькими способами можно разбить группу на бригады по 3 человека в бригаде? *Ответ.*  $C(N+23, 3)$ .

### *Правило суммы и правило произведения*

**Задача 13.** Составить график отпусков на январь, февраль, март. В январе в отпуск должны уйти  $r = N + 10$  человек, в феврале  $s = N + 8$ , в марте  $t = N + 15$ . Сколькими способами можно составить график, если в отделе  $n = 150$  человек? *Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . Число способов составления графиков не зависит от порядка месяцев, ибо справедлива следующая последовательность равенств.

$$C(n, r) \cdot C(n-r, s) = C(n, s) \cdot C(n-s, r) \Leftrightarrow$$

$$\frac{n!}{r!(n-r)!} \cdot \frac{(n-r)!}{s!(n-r-s)!} = \frac{n!}{s!(n-s)!} \cdot \frac{(n-s)!}{r!(n-s-r)!} \Leftrightarrow$$

$$\frac{n!}{r!s!(n-r-s)!} \cdot \frac{n!}{s!r!(n-s-r)!}.$$

**Задача 14.** Сколькими способами путем выбора из  $n = N + 100$  человек можно составить комиссию, состоящую из  $r = 1$  председателя,  $s = 3$  заместителей и  $t = 5$  рядовых членов?

*Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . (См. зад. 13).

**Задача 15.** Для премирования  $n = N + 12$  сотрудников куплены следующие книги: “Памятники Москвы”,  $r = 3$  экземпляра, “Фонтаны Петергофа”,  $s = 4$  экземпляра, “Вологодские кружева”,  $t = 5$  экземпляров. Сколькими способами можно распределить книги?

*Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . (См. зад. 13).

**Задача 16.** На  $n = N + 100$  сотрудников выделено 11 путевок:  $r = 2$  в санаторий “Дорохово”,  $s = 5$  в санаторий “Энергия”,  $t = 4$  в санаторий “Звенигород”. Сколькими способами можно распределить путевки?

*Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . (См. зад. 13).

**Задача 17.** Для охраны здания требуется наряд из 8 человек.  $r = 2$  из них – для охраны входа,  $s = 2$  для охраны сейфа и архива,  $t = 4$  для патрулирования. Сколькими способами можно сформировать такой наряд, имея  $n = N + 20$  человек? *Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . (См. зад. 13).

**Задача 18.** В учреждении  $n = N + 300$  сотрудников. Сколько вариантов назначения администрации возможно, если администрация должна состоять из  $r = 1$  директора,  $s = 1$  главного инженера и  $t = 3$  заместителей?

*Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . (См. зад. 13).

**Задача 19.** Для охраны здания надо выделить наряд из 8 человек:  $r = 2$  для охраны входа, по одному:  $s = 1 + 1 = 2$  для охраны сейфа и архива (с учетом распределения обязанностей),  $t = 4$  для патрулирования. Сколькоими способами можно выделить такой наряд имея в распоряжении  $n = N + 20$  человек? *Ответ.*  $C(n, r) \cdot A(n-r, s) \cdot C(n-r-s, t)$ .

**Задача 20.** Сколькоими способами можно распределить 6 именных стипендий между  $N + 100$  отличниками, если имеется 1 стипендия имени  $M_1$ , 2 стипендии имени  $M_2$ , 3 стипендии имени  $M_3$ ?

*Ответ.*  $C(n, r) \cdot C(n-r, s) \cdot C(n-r-s, t)$ . (См. зад. 13).

### Разные задачи

**Задача 21.** В некотором языке программирования имя переменной может состоять из  $n = N + 7$  десятичных цифр и латинских букв, причем имя переменной может быть любой последовательностью из букв и цифр (с повторами символов) любой длины  $l$ ,  $1 \leq l \leq n$ . Сколько различных имен переменных возможно в этом языке? *Ответ.*  $n^1 + n^2 + n^3 + \dots + n^n$ .

**Задача 22.**  $N + 5$  мальчиков и  $N + 5$  девочек с попарно различными именами должны быть рассажены в ряд. Сколькоими способами можно это сделать, если

- а) все мальчики должны сидеть на самых левых местах?
- б) никакие два мальчика не должны сидеть рядом?
- с) Маша и Петя должны сидеть рядом?

*Ответ.*

- а) мм...мдд...д,  $P(N+5) \cdot P(N+5)$ ;
- б) мдмд...мд, дмдм...дм,  $2 \cdot P(N+5) \cdot P(N+5)$ ;
- в) Петя и Маша (ПМ), а также МП среди  $2N+8$  позиций мальчиков и девочек (см. ниже первый ряд позиций) могут занимать позиции от 0 до  $2N+8$  (см. ниже второй ряд позиций). Это  $(P(2N+8)) \cdot (2N+9) \cdot 2$  возможностей.

$$\begin{matrix} 1 & 2 & \dots & 2N+8 \\ 0 & 1 & 2 & \dots & 2N+8 \end{matrix}$$

**Задача 23.** Сколькоими способами можно расставить  $N + 10$  мальчиков и  $N + 5$  девочек так, чтобы никакие две девочки не стояли рядом:

- а) в линию? б) в круг?

*Ответ.* а)  $P(N+10) \cdot A((N+10)+2, N+5)$ ; б)  $P(N+10) \cdot A(N+10, N+5)$ .

**Задача 24.** Сколькоими способами можно упорядочить  $N + 30$  символов так, чтобы между символами  $N$  и  $N + 1$  стояло ровно 5 других символов?

*Ответ.* Числа множества  $\{1, 2, \dots, N+30\} - \{N, N+1\}$  могут занимать позиции от 1 до  $N+28$  (см. ниже первый ряд позиций). Это  $P(N+28)$  возможностей их перестановок. Число  $N$  может занимать позиции от 0 до  $N+22$  (см. ниже второй ряд чисел). Это  $N+23$  возможностей его положения. Третий ряд позиций ниже это соответствующие позиции числа  $N+1$ , когда между  $N$  и

$N+1$  стоят пять других чисел. Число  $N$  может стоять раньше  $N+1$ . Это еще  $N+23$  возможностей их положения. По правилу умножения это  $P(N+28) \cdot 2(N+23)$  возможностей.

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & \dots & N+23 & N+24 & N+25 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots & N+22 \\ & & 6 & \dots & N+23 & N+24 & N+25 & N+26 & N+27 & N+28 \end{array}$$

**Задача 25.** а) Сколько способами могут быть упорядочены буквы в слове *parallelogram*, с приписанной к нему вашей фамилией, записанной в латинице?

б) Сколько способами они могут быть упорядочены, если буквы  $l$  не должны стоять рядом?

*Ответ.* Слово  $w = parallelogram$  без приписанной к нему фамилии состоит из букв  $p,a,r,l,e,o,g,m$ , число повторений которых в слове соответственно равны  $1,3,2,3,1,1,1,1$ .

а) число способов упорядочения равно

$$K_1 = P_{13}(1,3,2,3,1,1,1,1) = \frac{13!}{1! \cdot 3! \cdot 2! \cdot 3! \cdot 1! \cdot 1! \cdot 1! \cdot 1!}.$$

б) слово *paraeogram* есть слово  $w$  без буквы  $l$ . Оно состоит из семи букв  $p,a,r,e,o,g,m$ , число повторений которых в слове соответственно равны  $1,3,2,1,1,1,1$ . Число перестановок этих семи букв

$$K_2 = P_{10}(1,3,2,1,1,1,1) = \frac{10!}{1! \cdot 3! \cdot 2! \cdot 1! \cdot 1! \cdot 1! \cdot 1!}.$$

Три буквы  $l$  должны быть разделены в слове *paraeogram* хотя бы одной буквой. Ниже указаны слово (строка 1), позиции его букв (строка 2) и позиции между ними (строка 3). Буквы  $l$  могут занимать любые три позиции третьей строки от 0 до 10. Это  ${}_{11}C_3$  возможностей. По правилу умножения число способов упорядочения равно  $K_2 \cdot {}_{11}C_3$ .

$p \quad a \quad r \quad a \quad e \quad o \quad g \quad r \quad a \quad m$	$\begin{matrix} \text{буквы слова } parallelogram \text{ без } l \\ \text{их позиции} \end{matrix}$
$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10$	
$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10$	$\begin{matrix} \text{позиции между ними} \end{matrix}$

**Задача 26.** Пусть повторения цифр запрещены. Сколько  $(N + 4)$ -разрядных чисел могут быть сформированы из цифр 2, 3, 5, 6, 8, 9, если:

- а) ограничений нет?
- б) числа меньше 500?
- в) числа четные?
- г) числа нечетные?
- д) числа делятся на 3?
- е) числа делятся либо только на 2, либо только на 3?
- ж) числа делятся на 2 или на 3?
- з) числа делятся одновременно на 2 и на 3?

*Ответ.* а)  $n_a = {}_6A_4$ .

б) числа начинаются с 2 или с 3.  $n_b = 2 \cdot {}_5A_3$ .

- в) числа четные заканчиваются на 2,6,8.  $n_{\text{в}} = 3 \cdot {}_5A_3$ .  
 г) числа нечетные заканчиваются на 3,5,9.  $n_{\text{г}} = 3 \cdot {}_5A_3$ .  
 д) пусть знак  $\vdash$  означает «делится на». Число  $\vdash 3$ , если сумма его цифр делится на 3. Это любая перестановка чисел 2,5,8,а, где  $a \in \{3,6,9\}$ .

Число  $n_{\text{д}} = 3 \cdot P_4$ .

з) пусть знак  $c(\vdash m)$  означает число (cardinality) чисел, которые  $\vdash m$ . Пусть знаки  $\&$  и  $\vee$  означают «и» и «или» соответственно. Числа, которые  $\vdash 3 \& \vdash 2$  получатся, если из чисел, которые  $\vdash 3$ , оставим лишь четные числа, то есть заканчивающиеся на 6, 8, 2. Это числа вида  $abc6, def8, ghi2, jkl2, mno2$ , где  $abc, def, ghi, jkl, mno$  есть любая перестановка цифр 258, 253, 358, 658, 958 соответственно. Тогда  $n_3 = c(\vdash 3 \& \vdash 2) = 5 \cdot P_3$ .

- ж)  $n_{\text{ж}} = c(\vdash 3 \vee \vdash 2) = c(\vdash 3) + c(\vdash 2) - c(\vdash 3 \& \vdash 2) = 3 \cdot P_4 + 3 \cdot {}_5A_3 - 5 \cdot P_3$ .  
 е) пусть знак  $\oplus$  означает «исключающее или». Тогда  $n_{\text{е}} = c(\vdash 3 \oplus \vdash 2) = c(\vdash 3) + c(\vdash 2) - 2 \cdot c(\vdash 3 \& \vdash 2) = 3 \cdot P_4 + 3 \cdot {}_5A_3 - 2 \cdot 5 \cdot P_3 = 3 \cdot P_4 + 3 \cdot {}_5A_3 - 10 \cdot P_3$ .

**Задача 26-1.** Пусть повторения цифр не запрещены. Сколько  $(N + 4)$ -разрядных чисел могут быть сформированы из цифр 2, 3, 5, 6, 8, 9, если:

- а) ограничений нет?  
 б) числа меньше  $5 \cdot 10^{N+24}$ ?  
 в) числа четные?  
 г) числа нечетные?  
 д) числа, имеющие в своей десятичной записи  $N$  двоек, не имеющие пятерок и восьмерок и делящиеся на 3?

**26.1.** Ответ. а)  ${}_{N+24} \hat{A}_6 = 6^{N+4}$ . б) это числа, начинающиеся с 2 и 3. Их число равно  $2 \cdot 6^{N+23}$ . в) числа четные заканчиваются на 2,6,8. Их число равно  $3 \cdot {}_{N+23} \hat{A}_6 = 3 \cdot 6^{N+23}$ .

- г) числа нечетные заканчиваются на 3,5,9. Их число равно  $3 \cdot {}_{N+23} \hat{A}_6 = 3 \cdot 6^{N+23}$ .  
 д) число  $x \vdash 3$ , если сумма его цифр  $\vdash 3$ . Сгруппируем сумму цифр в  $x$  в две суммы  $S_1 + S_2$ , где  $S_1$  есть сумма двоек в  $x$ , и  $S_2$  есть сумма всех троек, шестерок, девяток в  $x$ .  $S_2 \vdash 3$ . Пусть в  $x N$  двоек,  $i_1$  троек,  $i_2$  шестерок,  $i_3$  девяток, причем  $i_1 + i_2 + i_3 = N + 24 - N = 24$ . Число чисел с  $N$  двойками,  $i_1$  тройками,  $i_2$  шестерками,  $i_3$  девятками есть число перестановок из  $N+24$  цифр 2,3,6,9 спецификации  $(N, i_1, i_2, i_3)$ , причем  $N + i_1 + i_2 + i_3 = N+24$ . Их число равно  $P_{N+24}(N, i_1, i_2, i_3) = \frac{(N+24)!}{N! \cdot i_1! \cdot i_2! \cdot i_3!}$ .

Если сумма  $2N$  всех двоек в  $x$  не кратна 3, то число обсуждаемых чисел равно нулю. Если  $2N \vdash 3$ , то число обсуждаемых чисел равно

$$\sum_{i_1+i_2+i_3=24} P_{N+24} = \sum_{i_1+i_2+i_3=24} \frac{(N+24)!}{N! \cdot i_1! \cdot i_2! \cdot i_3!}.$$

**Задача 27.** В анкете предлагается  $N + 15$  вопросов, на которые можно ответить “да”, “нет”, “затрудняюсь ответить”. Сколькими способами можно ответить на вопросы анкеты? *Ответ.*  $3^{N+15}$ .

**Задача 28.** Палиндром это слово, которое одинаково читается как слева направо, так и справа налево. Сколько палиндромов из  $N + 7$  букв можно составить в латинице, не заботясь о смысле слова?

*Ответ.*  $26^{\frac{(N+7)}{2}}$ , если  $N+7$  четно;  $26^{\frac{(N+6)}{2}} \cdot 26$ , если  $N+7$  нечетно.

**Задача 29.** Сколько шести-символьных слов можно сформировать из  $N + 26$  букв и цифр, если:

- первые два символа есть буквы, а следующие четыре есть цифры?
- в слове может быть только две буквы, которые не должны стоять в слове рядом. *Ответ.* а)  $26A_2 \cdot 10^4$ ; б)  $10^{N+24} \cdot {}_{N+25}C_2 \cdot 26^2$ .

**Задача 30.** Найти число положительных натуральных чисел не больших  $1000 + 2N + 1$ :

- не делящихся ни на одно из чисел 3, 5, 7, 11, 13;
- делящихся в точности на два числа;
- делящихся на не менее чем два числа.

$N$  есть номер фамилии студента в аудиторном журнале.

**Пример.** Найти число положительных натуральных чисел не больших  $N=1000$  и

- не делящихся ни на одно из чисел 3, 5, 7,
- делящихся в точности на два числа из {3, 5, 7},
- делящихся на не менее чем два числа из {3, 5, 7}.

*Решение.* Используем формулы включений и исключений для числа предметов  $N$  и числа свойств  $n$ .

$$\begin{aligned} N(0) &= \sum_{r=0}^m (-1)^r \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} N(i_1, i_2, \dots, i_r); \\ N_{=k} &= \sum_{j=0}^{n-k} (-1)^j C_{k+j}^j \sum_{1 \leq i_1 < i_2 < \dots < i_{k+j} \leq n} N(i_1, i_2, \dots, i_{k+j}); \\ N_{\geq k} &= \sum_{j=0}^{n-k} (-1)^j C_{k-1+j}^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_{k+j} \leq n} N(i_1, i_2, \dots, i_{k+j}); \end{aligned}$$

Свойство 1: число  $k$  делится на 3.

Свойство 2: число  $k$  делится на 5.

Свойство 3: число  $k$  делится на 7.

Пусть  $M$  есть множество чисел между 1 и  $N$ , обладающих одним из перечисленных свойств или их сочетанием.

Свойство	Множество $M$ чисел	Число чисел в $M$
1	$\{3k : k = 1, 2, \dots, 333\}$	$N(1) = 333$
2	$\{5k : k = 1, 2, \dots, 200\}$	$N(2) = 200$

3	$\{7k : k = 1, 2, \dots, 142\}$	$N(3) = 142$
1,2	$\{15k : k = 1, 2, \dots, 66\}$	$N(1,2) = 66$
1,3	$\{21k : k = 1, 2, \dots, 47\}$	$N(1,3) = 47$
2,3	$\{35k : k = 1, 2, \dots, 28\}$	$N(2,3) = 28$
1,2,3	$\{105k : k = 1, 2, \dots, 9\}$	$N(1,2,3) = 9$

$$\begin{aligned}
N(0) &= 1000 - \sum_{1 \leq i \leq 3} N(i) + \sum_{1 \leq i < j \leq 3} N(i,j) - N(1,2,3) = \\
&1000 - (333 + 200 + 142) + (66 + 47 + 28) - 9 = 457. \\
N_{=2} &= \sum_{j=0}^{3-2} (-1)^j C_{2+j}^j \sum_{1 \leq i_1 < i_2 < \dots < i_{2+j} \leq 3} N(i_1, i_2, \dots, i_{2+j}) = \\
&(-1)^0 C_2^0 \sum_{1 \leq i < j \leq 3} N(i, j) + (-1)^1 C_3^1 N(1,2,3) = 1 \cdot (66 + 47 + 28) - 3 \cdot 9 = 114. \\
N_{\geq 2} &= \sum_{j=0}^{3-2} (-1)^j C_{2-1+j}^j \sum_{1 \leq i_1 < i_2 < \dots < i_{2+j} \leq 3} N(i_1, i_2, \dots, i_{2+j}) = \\
&(-1)^0 C_1^0 \sum_{1 \leq i < j \leq 3} N(i, j) + (-1)^1 C_2^1 N(1,2,3) = 1 \cdot (66 + 47 + 28) - 2 \cdot 9 = 123.
\end{aligned}$$

### 3. МОДУЛЯРНАЯ АЛГЕБРА

**Задача 1.** Даны целые числа  $a = 100+N$  ( $N$  есть номер фамилии студента в аудиторном журнале) и  $b=11$ . Найти целые,  $q_1, q_2, r_1, r_2$ ,  $0 \leq r_1, r_2 < b$ , для которых  $a = bq_1 + r_1$ ,  $-a = bq_2 + r_2$ .

**Пример.** Даны целые числа  $a = 321$  и  $b = 11$ . Найти целые  $q_1, q_2, r_1, r_2$ ,  $0 \leq r_1, r_2 < b$ , для которых  $a = bq_1 + r_1$ ,  $-a = bq_2 + r_2$ .

*Решение.*  $321 = 11*29 + 2$ ,  $q_1=29$ ;  $r_1=2$ ,  $0 \leq r_1 < b=11$ ,  
 $-321 = 11*(-29) - 2 = 11(-29) - 2 + 11 - 11 = 11(-29-1) + 9 = 11(-30) + 9$ ,  $q_2=-30$ ;  
 $r_2=9$ ,  $0 \leq r_2 < b=11$ .

**Задача 2.** Записать данные числа в восьмеричной, шестеричной, десятичной системах счисления.

- |                                       |                                       |
|---------------------------------------|---------------------------------------|
| <b>2.1.</b> $(1111001011110001)_2$ .  | <b>2.2.</b> $(1001110000111011)_2$ .  |
| <b>2.3.</b> $(1100111001110010)_2$ .  | <b>2.4.</b> $(1101000111000101)_2$ .  |
| <b>2.5.</b> $(1100010110100110)_2$ .  | <b>2.6.</b> $(1001110100011010)_2$ .  |
| <b>2.7.</b> $(1100110000011110)_2$ .  | <b>2.8.</b> $(1111000100111011)_2$ .  |
| <b>2.9.</b> $(1000110101110110)_2$ .  | <b>2.10.</b> $(1011101011000101)_2$ . |
| <b>2.11.</b> $(1011101100011110)_2$ . | <b>2.12.</b> $(1111011001011010)_2$ . |
| <b>2.13.</b> $(1001111010111010)_2$ . | <b>2.14.</b> $(1101101010011101)_2$ . |
| <b>2.15.</b> $(1011101011011100)_2$ . | <b>2.16.</b> $(1011000101111100)_2$ . |
| <b>2.17.</b> $(1001110101111100)_2$ . | <b>2.18.</b> $(1011011101111100)_2$ . |
| <b>2.19.</b> $(1101110001110111)_2$ . | <b>2.20.</b> $(1111110010001101)_2$ . |
| <b>2.21.</b> $(111101111100010)_2$ .  | <b>2.22.</b> $(1000110101000101)_2$ . |
| <b>2.23.</b> $(1110001010111001)_2$ . | <b>2.24.</b> $(1100010101000111)_2$ . |
| <b>2.25.</b> $(1011100110000110)_2$ . | <b>2.26.</b> $(1100011101110011)_2$ . |
| <b>2.27.</b> $(1000011001110011)_2$ . | <b>2.28.</b> $(1101011001110011)_2$ . |
| <b>2.29.</b> $(1111010001010110)_2$ . | <b>2.30.</b> $(1101011001010110)_2$ . |

**Пример.** Записать числа в восьмеричной, шестеричной, десятеричной системах счисления.

*Решение.*  $n = 11\ 101\ 110\ 010\ 101_2 = 35625_8$ .

$n = 11\ 111\ 1101\ 0101_2 = 3FD5_{16}$ .

$n = 11001001_2 = 2^7 + 2^6 + 2^3 + 1 = 201_{10}$ .

**Задача 3.** Записать десятичные числа  $n=100+N$ ,  $m=200+N$  в семеричной и двоичной системах счисления.  $N$  есть номер фамилии студента в аудиторном журнале.

**Пример.** Записать десятичные числа  $n=160$  и  $199$  в семеричной и двоичной системах счисления.

#### 8.1. Алгоритм вычисления $h$ -ричной записи $10$ -ричного числа $a$

**ВХОД.** Натуральные числа  $a > 0$  и  $h \geq 2$ .

**ВЫХОД.**  $h$ -ричная запись числа  $a = (a_t a_{t-1} \dots a_1 a_0)_h$ .

1.  $i := 0$ .

2. Пока  $q \neq 0$ , выполняется следующее.

2.1.  $r := \text{mod}(a, h)$ ,  $q := (a-r)/h$ .

2.2.  $a := q$ ,  $a_i := r$ .

2.3.  $i := i+1$ .

3. Вернуть  $a$ .

*Решение.* По основанию  $h$  число  $a_{10} = (a_t a_{t-1} \dots a_1 a_0)_h$ .

$i := 0$ ,  $a := 160$ ,

$r := \text{mod}(a, h) = \text{mod}(160, 7) = 6$ ,  $q := (a-r)/h = (160-6)/7 = 22$ ,

$a_0 := r = 6$ ,  $i := i+1 = 0+1 = 1$ ;  $a := q = 22$ ,

$r := \text{mod}(a, h) = \text{mod}(22, 7) = 1$ ,  $q := (a-r)/h = (22-1)/7 = 3$ ,

$a := q = 3$ ,  $a_1 := r = 1$ ,  $i := i+1 = 1+1 = 2$ .

$r := \text{mod}(a, h) = \text{mod}(3, 7) = 3$ ;  $q := q := (a-r)/h = (3-3)/7 = 0$ .

$a := q = 0$ ,  $a_2 := r = 3$ ,  $i := i+1 = 2+1 = 3$ .

Результаты вычислений приведены в таблицах 7.1, 7.2, 7.3, 7.4.

$$h = 7, a = 160_{10} = 316_7$$

Таблица 7.1

$i$	$a$	$r$	$q$	$a_i$
0	160	6	22	6
1	22	1	3	1
2	3	3	0	3

$$h = 7, a = 199_{10} = 403_7$$

Таблица 7.2

$i$	$a$	$r$	$q$	$a_i$
0	199	3	28	3
1	28	0	4	0
2	4	4	0	4

$$h = 2, a = 160_{10} = 10100000_2$$

Таблица 7.3

$i$	$a$	$r$	$q$	$a_i$
0	160	0	80	0
1	80	0	40	0
2	40	0	20	0
3	20	0	10	0
4	10	0	5	0
5	5	1	2	1
6	2	0	1	0
7	1	1	0	1

$$h = 2, a = 199_{10} = 11000111_2$$

Таблица 7.4

$i$	$a$	$r$	$q$	$a_i$
0	199	1	99	1
1	99	1	49	1
2	49	1	24	1
3	24	0	12	0
4	12	0	6	0
5	6	0	3	0
6	3	1	1	1
7	1	1	0	1

*Ответ.*  $a = 160_{10} = 316_7 = 10100000_2$ ,

$a = 199_{10} = 403_7 = 11000111_2$ .

**Задача 4.** Сложить и перемножить числа из задачи 3 в системе счисления по основанию семь.

**Пример.** Сложить и перемножить числа  $(160)_{10}$  и  $(199)_{10}$  в системе счисления по основанию семь (табл. 7.5 и 7.6).

*Решение.*  $160_{10} = 316_7$ ;  $199_{10} = 403_7$ .

Таблица 7.5

+7	0	1	2	3	4	5	6
----	---	---	---	---	---	---	---

Таблица 7.6

$\times_7$	0	1	2	3	4	5	6
------------	---	---	---	---	---	---	---

0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	10
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	12
4	4	5	6	10	11	12	13
5	5	6	10	11	12	13	14
6	6	10	11	12	13	14	15

0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	11	13	15
3	0	3	6	12	15	21	24
4	0	4	11	15	22	26	33
5	0	5	13	21	26	34	42
6	0	6	15	24	33	42	56

**Пример** вычисления умножения в 7-ричной системе счисления.

$$\begin{array}{r}
 1 \\
 2 \\
 3 \\
 4 + 0 0 0 \\
 5 \quad 12 \ 4 \ 24 \\
 6 \quad 1 \ 1 \ 4 \ 0 \ 2 \\
 \hline
 7 \quad 13 \ 8 \ 33 \ 5 \ 18 \text{ сумма} \\
 8 \ 1 \ 6 \ 1 \ 5 \ 5 \ 4 \ 7
 \end{array}$$

Вычисления производятся в следующем порядке.

1. Строки 1 и 2 есть семеричные записи чисел  $316_7$  и  $403_7$ .
2. Строки 3, 4, 5 есть 10-ричные произведения чисел 3, 1, 6 на 3, 0, 4.
3. Строки 6, 7, 8 заполняются в следующем порядке.
4. В строке 7 последнее число есть 18. Находим частное 2 и остаток 4 при делении 18 на 7. Остаток 4 есть последнее 7-ричное число в строке 8. В строке 6 частное 2 записывается в предпоследний разряд строки 6.
5. В строках 3, 4, 6 складываются 3, 0, 2 и результат 5 записывается в предпоследний разряд строки 7.
6. В строках 7 и 8 к числу 5 последовательно применяем пункты 4 и 5 и переходим к предыдущему разряду до полного исчерпания разрядов.

*Ответ.*  $316_7 + 403_7 = 1071_7$ ,  $316_7 \cdot 403_7 = 161554_7$ .

**Задача 5.** В двоичной системе счисления разделить число из задачи 2 на число  $101101_2$ .

**Пример.** В двоичной системе счисления разделить число  $n = 11001001_2$  на число  $m = 101101_2$ .

*Решение.*

$$\begin{array}{r}
 - 11001001 \Big| 100111 \\
 - 100111 \\
 \hline
 - 101101 \\
 - 100111 \\
 \hline
 110
 \end{array}$$

$$\text{Ответ. } \frac{n}{m} = 101 \frac{110}{100111}.$$

**Задача 6.** Найти число цифр в десятичном числе  $n$  по основаниям 2, 3, 5, 7, 8, 12, 16. В качестве числа написать свою фамилию и взять из записи начальный отрезок длины 5. Если длина записи меньше пяти, то дописать букву «ю» необходимое число раз. Пусть получили слово  $s$  (длины 5). Все 32 буквы русского алфавита пронумеруем по порядку от 1 до 32. Пробел есть 0. Тогда слово  $s$  можно рассматривать как число в системе счисления по основанию 33. Число  $n$  получается переводом  $s_{32}$  в десятичное число.

**Пример.** Найти число цифр в десятичном числе  $n = 8735284215_{10}$  по основаниям 2, 3, 5, 7, 8, 12, 16.

*Решение.* Если число  $n$  удовлетворяет неравенствам  $b^{k-1} \leq n \leq b^k$ , то  $n$  имеет  $k$  цифр по основанию  $b$ . Логарифмируем неравенства по основанию  $b$  и получаем  $k-1 \leq \log_b n < k$ . Отсюда  $k = \lfloor \log_b n \rfloor + 1 = \lfloor \ln n / \ln b \rfloor + 1$ .

$$\left\lfloor \frac{\ln 8735284215}{\ln 2} \right\rfloor + 1 = 34, \quad \left\lfloor \frac{\ln 8735284215}{\ln 3} \right\rfloor + 1 = 21, \quad \left\lfloor \frac{\ln 8735284215}{\ln 5} \right\rfloor + 1 = 15,$$

$$\left\lfloor \frac{\ln 8735284215}{\ln 7} \right\rfloor + 1 = 12, \quad \left\lfloor \frac{\ln 8735284215}{\ln 8} \right\rfloor + 1 = 12, \quad \left\lfloor \frac{\ln 8735284215}{\ln 12} \right\rfloor + 1 = 10,$$

$$\left\lfloor \frac{\ln 8735284215}{\ln 16} \right\rfloor + 1 = 9.$$

<i>Ответ.</i>	$b$	2	3	5	7	8	12	16
	$k$	34	21	15	12	12	10	9

**Задача 7.** Разложить данное число  $n$  на простые множители и найти число делителей  $f(n)$  числа  $n$ .

- 7.1.** 5402250. **7.2.** 3601500. **7.3.** 1296540.  
**7.4.** 6472500. **7.5.** 3241350. **7.6.** 1440600.  
**7.7.** 3864360. **7.8.** 1575000. **7.9.** 1653750  
**7.10.** 1470000. **7.11.** 1587600. **7.12.** 5556600.  
**7.13.** 3858750. **7.14.** 7717500. **7.15.** 1111320.  
**7.16.** 1984500. **7.17.** 1389150. **7.18.** 4802000.  
**7.19.** 1728720. **7.20.** 6174000. **7.21.** 1984500.  
**7.22.** 2058000. **7.23.** 1481760. **7.24.** 3704400.  
**7.25.** 1543500. **7.26.** 1440600. **7.27.** 8103375.  
**7.28.** 8482700. **7.29.** 4630500. **7.30.** 2160900.

**Пример.** Разложить данное число  $n = 1728720$  на простые множители и найти число делителей  $f(n)$  числа  $n$ .

*Решение.*

1728720	2
---------	---

864360	2
432180	2
216090	2
108045	3
36015	3
12005	5
2401	7
343	7
49	7
7	7
1	

$$n = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^4.$$

Число  $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$  имеет  $(a_1 + 1)(a_2 + 1) \dots (a_k + 1)$  различных делителей.

$$f(n) = (4+1)(2+1)(1+1)(4+1) = 150.$$

**Задача 8.** Найти наибольший общий делитель  $d$  и наименьшее общее кратное чисел  $a$  и  $b$ . Число  $a$  взять из задачи 6, число  $b=780$ . Найти те  $u$  и  $v$ , для которых  $d = ua + vb$ .

**Пример.** Найти наибольший общий делитель  $d$  и наименьшее общее кратное чисел  $a = 4864$ ,  $b = 3458$ . Найти такие целые  $u$  и  $v$ , для которых  $d = au + bv$ .

### *Алгоритм Евклида вычисления нод ( $a,b$ )*

ВХОД. Натуральные числа  $a$  и  $b$ ,  $a \geq b$ .

ВЫХОД. нод( $a,b$ ).

1. Пока  $b \neq 0$ , выполнять следующее.

$$1.1. q := \lfloor a/b \rfloor, r := a - qb, a := b, b := r.$$

2. Вернуть  $a$ .

### *Расширенный алгоритм Евклида вычисления $d=\text{нод}(a,b)$ , и целых чисел $u,v$ , для которых $d = ua + vb$*

ВХОД. Натуральные числа  $a$  и  $b$ ,  $a \geq b$ .

ВЫХОД.  $d = \text{нод}(a,b)$  и целые  $u,v$ , для которых  $d = ua + vb$ .

1. Если  $b = 0$ , то  $d := a$ ,  $u := 1$ ,  $v := 0$  и вернуть  $(d,u,v)$ .

2.  $u_2 := 1$ ,  $u_1 := 0$ ,  $v_2 := 0$ ,  $v_1 := 1$ .

3. Пока  $b > 0$  выполнять следующее.

$$3.1. q := \lfloor a/b \rfloor, r := a - qb, u := u_2 - q u_1, v := v_2 - q v_1.$$

$$3.2. a := b, b := r, u_2 := u_1, u_1 := u, v_2 := v_1, v_1 := v.$$

4.  $d := a$ ,  $u := u_2$ ,  $v := v_2$ , вернуть  $(d, u, v)$ .

*Решение.* Производим следующие вычисления.

**Инициализация.**

**Шаг 0.**  $a := 4864, b := 3458, u_2 := 1, u_1 := 0, v_2 := 0, v_1 := 1$ .

Далее продолжаем согласно алгоритму.

**Шаг 1.**  $\lfloor a/b \rfloor = \lfloor 4864/3458 \rfloor = 1, r = a - q \cdot b = 4864 - 3458 \cdot 1 = 1406;$

$$u := u_2 - q \cdot u_1 = 1 - 1 \cdot 0 = 1, v := v_2 - q \cdot v_1 = 0 - 1 \cdot 1 = -1;$$

$$a := b = 3458, b := r = 1406;$$

$$u_2 := u_1 = 0, u_1 := u = 1; v_2 := v_1 = 1, v_1 := v = -1.$$

**Шаг 2.**  $\lfloor a/b \rfloor = \lfloor 3458/1406 \rfloor = 2, r = a - q \cdot b = 3458 - 1406 \cdot 2 = 646;$

$$u := u_2 - q \cdot u_1 = 0 - 2 \cdot 1 = -2, v := v_2 - q \cdot v_1 = 1 - 2 \cdot (-1) = 3;$$

$$a := b = 1406, b := r = 646;$$

$$u_2 := u_1 = 1, u_1 := u = -2; v_2 := v_1 = -1, v_1 := v = 3.$$

**Шаг 3.**  $\lfloor a/b \rfloor = \lfloor 1406/646 \rfloor = 2, r = a - q \cdot b = 1406 - 646 \cdot 2 = 114;$

$$u := u_2 - q \cdot u_1 = 1 - 2 \cdot (-2) = 5, v := v_2 - q \cdot v_1 = -1 - 2 \cdot 3 = -7;$$

$$a := b = 646, b := r = 114;$$

$$u_2 := u_1 = -2, u_1 := u = 5; v_2 := v_1 = 3, v_1 := v = -7.$$

**Шаг 4.**  $\lfloor a/b \rfloor = \lfloor 646/114 \rfloor = 2, r = a - q \cdot b = 646 - 114 \cdot 5 = 76;$

$$u := u_2 - q \cdot u_1 = -2 - 5 \cdot 5 = -27, v := v_2 - q \cdot v_1 = 3 - 5 \cdot (-7) = 38;$$

$$a := b = 114, b := r = 76;$$

$$u_2 := u_1 = 5, u_1 := u = -27; v_2 := v_1 = -7, v_1 := v = 38.$$

**Шаг 5.**  $\lfloor a/b \rfloor = \lfloor 114/76 \rfloor = 2, r = a - q \cdot b = 114 - 76 \cdot 1 = 38;$

$$u := u_2 - q \cdot u_1 = 5 - 1 \cdot (-27) = 32, v := v_2 - q \cdot v_1 = -7 - 1 \cdot 38 = -45;$$

$$a := b = 76, b := r = 38;$$

$$u_2 := u_1 = -27, u_1 := u = 32; v_2 := v_1 = 38, v_1 := v = -45.$$

**Шаг 6.**  $\lfloor a/b \rfloor = \lfloor 76/38 \rfloor = 2, r = a - q \cdot b = 76 - 38 \cdot 2 = 0;$

$$u := u_2 - q \cdot u_1 = -27 - 2 \cdot 32 = -85, v := v_2 - q \cdot v_1 = 38 - 2 \cdot (-45) = 128;$$

$$a := b = 38, b := r = 0;$$

$$u_2 := u_1 = 32, u_1 := u = -85; v_2 := v_1 = -45, v_1 := v = 128.$$

Продолжаем вычисления и их результаты заносим в табл. 7.7.

Таблица 7.7

$n$	$q$	$r$	$u$	$v$	$a$	$b$	$u_2$	$u_1$	$v_2$	$v_1$
0	—	—	—	—	4864	3458	1	0	0	1
1	1	1406	1	-1	3458	1406	0	1	1	-1
2	2	646	-2	3	1406	646	1	-2	-1	3
3	2	114	5	-7	646	114	-2	5	3	-7
4	5	76	-27	38	114	76	5	-27	-7	38
5	1	38	32	-45	76	38	-27	32	38	-45
6	2	0	-91	128	<b>38</b>	0	<b>-32</b>	-91	<b>-45</b>	128

Ответ.  $d = \text{нод}(a, b) = \text{нод}(4864, 3458) = 38, u = 32, v = -45$ .

**Задача 9.** Найти непрерывные и подходящие дроби для числа  $a/b, a \geq b$ . Числа  $a$  и  $b$  взять из задачи 6.

**Пример.** Найти непрерывные и подходящие дроби для числа  $a/b, a > b, a$

$= 105, b = 38.$

*Решение.*  $105 = 38 \cdot 2 + 29, \quad q_1 = 2,$

$$38 = 29 \cdot 1 + 9, \quad q_2 = 1,$$

$$29 = 9 \cdot 3 + 2, \quad q_3 = 3,$$

$$9 = 2 \cdot 4 + 1, \quad q_4 = 4,$$

$$2 = 1 \cdot 2, \quad q_5 = 2.$$

Непрерывная дробь числа  $105/38$  приведена в табл.7.8.

Таблица 7.8

$$\frac{105}{38} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{q_5}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

Подходящие дроби  $\delta_s$ :

$$\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \dots$$

### Алгоритм вычисления подходящих дробей

$$P_0 = 1, \quad Q_0 = 0, \quad P_1 = q_1, \quad Q_1 = 1, \quad \delta_1 = \frac{P_1}{Q_1},$$

$$\delta_s = \frac{P_s}{Q_s}, \text{ где } \begin{cases} P_s = q_s P_{s-1} + P_{s-2} \\ Q_s = q_s Q_{s-1} + Q_{s-2} \end{cases}, \quad s=2,3,4,\dots$$

В нашем примере  $P_0 = 1, Q_0 = 0, P_1 = q_1 = 2, Q_1 = 1,$

$$\begin{cases} P_0 = 1, P_1 = q_1 = 2, \\ Q_0 = 0, Q_1 = 1, \end{cases} \quad \delta_1 = \frac{P_1}{Q_1} = \frac{2}{1} = 2;$$

$$\begin{cases} P_2 = q_2 P_1 + P_0 = 1 \cdot 2 + 1 = 3, \\ Q_2 = q_2 Q_1 + Q_0 = 1 \cdot 1 + 0 = 1, \end{cases} \quad \delta_2 = \frac{P_2}{Q_2} = \frac{3}{1} = 3;$$

$$\begin{cases} P_3 = q_3 P_2 + P_1 = 3 \cdot 3 + 2 = 11, \\ Q_3 = q_3 Q_2 + Q_1 = 3 \cdot 1 + 1 = 4, \end{cases} \quad \delta_3 = \frac{P_3}{Q_3} = \frac{11}{4};$$

$$\begin{cases} P_4 = q_4 P_3 + P_2 = 4 \cdot 11 + 3 = 47, \\ Q_4 = q_4 Q_3 + Q_2 = 4 \cdot 4 + 1 = 17, \end{cases} \quad \delta_4 = \frac{P_4}{Q_4} = \frac{47}{17};$$

$$\begin{cases} P_5 = q_5 P_4 + P_3 = 2 \cdot 47 + 11 = 105, \\ Q_5 = q_5 Q_4 + Q_3 = 2 \cdot 17 + 4 = 38, \end{cases} \quad \delta_5 = \frac{P_5}{Q_5} = \frac{105}{38}.$$

**Задача 10.** Написать неотрицательную наименьшую полную, наименьшую по модулю, приведенную системы вычетов по модулю  $n=15$ . Для полной и приведенной системы вычетов написать таблицы сложения, умножения. Написать каноническое разложение числа  $n$  и вычислить для него функцию Эйлера  $\phi(n)$ . Для системы вычетов  $\mathbb{Z}_n - \{0\}$  написать по умножению

таблицу обратных элементов, таблицу степеней до показателя  $\varphi(n)$ , указать порядок каждого элемента и указать генератор (по умножению), если он существует.

В вариантах задания дано число  $n$ .

- 10.1.** 12. **10.2.** 14. **10.3.** 16. **10.4.** 18. **10.5.** 20.
- 10.6.** 21. **10.7.** 22. **10.8.** 24. **10.9.** 25. **10.10.** 26.
- 10.11.** 27. **10.12.** 28. **10.13.** 30. **10.14.** 31. **10.15.** 32.
- 10.16.** 34. **10.17.** 35. **10.18.** 36. **10.19.** 38. **10.20.** 39.
- 10.21.** 40. **10.22.** 41. **10.23.** 42. **10.24.** 44. **10.25.** 45.
- 10.26.** 46. **10.27.** 48. **10.28.** 49. **10.29.** 52. **10.30.** 54.

### **8.7. Алгоритм вычисления мультипликативного обратного элемента $a^{-1} \pmod{n}$ в $\mathbb{Z}_n^*$**

Для натуральных  $a$  и  $n$  можно найти такие целые  $u$  и  $v$ , что  $a \cdot u + n \cdot v = \text{нод}(a, n)$ . Если  $\text{нод}(a, n) = 1$ , то  $a \cdot u + n \cdot v = 1$ . Два одинаковых числа при делении на  $n$  дают один и тот же остаток. Так как 1 при делении на  $n$  дает остаток 1, то  $a \cdot u + n \cdot v$  при делении на  $n$  тоже даст остаток 1, откуда  $a \cdot u + n \cdot v \equiv 1 \pmod{n}$ . Из левой части сравнения вычтем кратное модуля  $n \cdot v$  и получим, что  $a \cdot u \equiv 1 \pmod{n}$ . Тогда  $u = a^{-1} \pmod{n}$ .

**ВХОД.** Натуральные числа  $a$ ,  $n$ .

**ВЫХОД.**  $a^{-1} \pmod{n}$  в  $\mathbb{Z}_n$ .

1. С помощью расширенного алгоритма Евклида найти  $d = \text{нод}(a, n)$  и те целые  $u$  и  $v$ , для которых  $au + nv = d$ .
2. Если  $d > 1$ , то  $a^{-1} \pmod{n}$  не существует. Иначе обратный элемент  $a^{-1} = u$ .

### **8.8. Алгоритм вычисления порядка элемента циклической группы $\mathbb{Z}_p^*$ при простом $p$ (перебор)**

**ВХОД.** Натуральное число  $a$  и простое число  $p$ .

**ВЫХОД.** Порядок  $\text{ord}(a)$  элемента  $a$  в  $\mathbb{Z}_p^*$ .

1.  $b := a$ ,  $k := 1$ .
2. Пока  $b > 1$  и  $k \leq p-1$ , выполнить следующее.
  - 3.1.  $b := b \cdot a \pmod{p}$ , (остаток при делении  $b \cdot a$  на  $p$ ).
  - 3.2.  $k := k + 1$ .
4. Если  $b > 1$ , то порядок  $\text{ord}(a)$  не существует. Иначе вернуть  $k$ .

### **8.9. Алгоритм вычисления генератора циклической группы $\mathbb{Z}_p^*$ при простом $p$ (перебор)**

**ВХОД.** Простое число  $p$ .

**ВЫХОД.** Генератор циклической группы  $\mathbb{Z}_p^*$ .

1. Выбрать случайный элемент  $a$  в  $\mathbb{Z}_p^*$ .
2.  $b := a$ ,  $k := 1$ .
3. Пока  $b \neq 1$  и  $k \leq p$ , выполнить следующее.

3.1.  $b := b \cdot a \pmod{p}$ .

3.2.  $k := k + 1$ .

4. Если  $b = 1$  и  $k = p - 1$ , вернуть  $a$ . Иначе перейти к пункту 1.

**Пример.**  $n = 15$ .

*Решение.* 1. Полная система вычетов

$$\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}.$$

2. Наименьшая по модулю система вычетов:

$$\{-7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7\}.$$

3. Приведенная система вычетов  $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ .

4. Сложение по модулю 15 для полной системы вычетов  $\mathbb{Z}_{15}$  (табл.7.9).

Таблица 7.9

$+_{15}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	0	1	2	3	4	5	6	7	8	9	10	11	12	13

5. Умножение по модулю 15 для полной системы вычетов  $\mathbb{Z}_{15}$  (табл.7.10).

Таблица 7.10

$\times_{15}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	0	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5

11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

6. Сложение и умножение по модулю 15 для приведенной системы вычетов  $\mathbb{Z}_{15}^*$  приведены в табл. 7.11.

Таблица 7.11

$+_{15}$	1	2	4	7	8	11	13	14
1	2	3	5	8	9	12	14	0
2	3	4	6	9	10	13	0	1
4	5	6	8	11	12	0	2	3
7	8	9	11	14	0	3	5	6
8	9	10	12	0	1	4	6	7
11	12	13	0	3	4	7	9	10
13	14	0	2	5	6	9	11	12
14	0	1	3	6	7	10	12	13

$\times_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Множество  $\mathbb{Z}_{15}^*$  не замкнуто относительно сложения.

Множество  $\mathbb{Z}_{15}^*$  замкнуто относительно умножения.

7.  $n = 15 = 3^1 \cdot 5^1$ . Функция Эйлера для числа  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$  есть

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}).$$

$$\varphi(15) = (3^1 - 3^0)(5^1 - 5^0) = 2 \cdot 4 = 8.$$

8. Ниже указаны обратные элементы по модулю 15 для системы вычетов  $\mathbb{Z}_n - \{0\}$ . ( $a^{-1}$  обратен для  $a$ , если  $a \cdot a^{-1} = 1$ ).

$a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$a^{-1}$	1	8	-	4	-	-	13	2	-	-	11	-	7	14

9. В табл. 7.12 приведены степени элементов и их порядки по модулю 15 для полной системы вычетов  $\mathbb{Z}_{15}$  до наименьшего  $i \geq 1$ , для которого  $a^i = 1$ .

Таблица 7.12

Степень $a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2		4	9	1	10	6	4	4	6	10	1	9	4	1
3			8	12		5	6	13	2	9	10		3	7
4				1	6		10	6	1	1	6	10		6
5					3		5	6		9	10		12	
6						9		10		6	10		9	
7							12	5		9	10		3	
8								6	10		6		6	
ord( $a$ )	1	4	-	2	-	-	4	4	-	-	2	-	4	2

Генератор для  $\mathbb{Z}_{15} - \{0\}$  отсутствует.

**Задача 11.** Найти степень  $5^{613+N} \pmod{1135}$ , где  $N$  есть номер, под которым стоит фамилия студента в аудиторном журнале.

**Пример.** Найти степень  $5^{596} \pmod{1234}$ .

*Решение.* Если  $k = k_t k_{t-1} \dots k_1 k_0 = \sum_{i=0}^t k_i 2^i$  есть бинарное представление натурального числа  $k$ , то  $a^k = a^{\sum_{i=0}^t k_i 2^i} = a^{k_0 2^0 + k_1 2^1 + \dots + k_t 2^t} = a^{k_0 2^0} \cdot a^{k_1 2^1} \cdot \dots \cdot a^{k_t 2^t} = (a^{2^0})^{k_0} \cdot (a^{2^1})^{k_1} \cdot \dots \cdot (a^{2^t})^{k_t} = \prod_{i=0}^t (a^{2^i})^{k_i}$ .

### *Алгоритм вычисления модулярной степени в $\mathbb{Z}_n$*

ВХОД. Натуральные числа  $a, k, n$ .

ВЫХОД. Степень  $a^k \pmod{n}$ .

1.  $b := 1$ . Если  $k=0$ , то вернуть  $b$ .
2.  $A := a$ .
3. Если  $k_0 = 1$ , то  $b := a$ .
4. Для  $i$  от 1 до  $t$  выполнить следующее:
  - 4.1.  $A := A^2 \pmod{n}$ .
  - 4.2. Если  $k_i = 1$ , то  $b := A \cdot b \pmod{n}$ .
5. Вернуть  $b$ .

В нашем примере  $a^k = 5^{596} \pmod{1234}$ ;

$a = 5, k = 596_{10} = (k_9 k_8 \dots k_1 k_0)_2 = 1001010100_2$ .

*Решение.*

$$k = 596_{10} = 1001010100_2$$

- 1)  $b := 1, k = 0$
- 2)  $k_0 = 0, A := a = 5$   
 $b = 1$
- 3)  $k_1 = 0$   
 $A := A^2 \pmod{n} = 5^2 \pmod{1234} = 25$   
 $b = 1$
- 4)  $k_2 = 1$   
 $A := A^2 \pmod{n} = 25^2 \pmod{1234} = 625$   
 $b := b \cdot A \pmod{n} = 1 \cdot 625 \pmod{1234} = 625$
- 5)  $k_3 = 0$   
 $A := A^2 \pmod{n} = 625^2 \pmod{1234} = 681$   
 $b = 625$
- 6)  $k_4 = 1$   
 $A := A^2 \pmod{n} = 681^2 \pmod{1234} = 1011$   
 $b := b \cdot A \pmod{n} = 625 \cdot 1011 \pmod{1234} = 67$
- 7)  $k_5 = 0$   
 $A := A^2 \pmod{n} = 1011^2 \pmod{1234} = 369$   
 $b = 67$

$$8) k_6 = 1$$

$$A := A^2 \pmod{n} = 369^2 \pmod{1234} = 421$$

$$b := b \cdot A \pmod{n} = 67 \cdot 421 \pmod{1234} = 1059$$

$$9) k_7 = 0$$

$$A := A^2 \pmod{n} = 421^2 \pmod{1234} = 779$$

$$b = 1059$$

$$10) k_8 = 0$$

$$A := A^2 \pmod{n} = 779^2 \pmod{1234} = 947$$

$$b = 1059$$

$$11) k_9 = 1$$

$$A := A^2 \pmod{n} = 947^2 \pmod{1234} = 925$$

$$b := b \cdot A \pmod{n} = 1059 \cdot 925 \pmod{1234} = 1013$$

Вычисления сведены в табл. 7.13.

Таблица 7.13

$i$	0	1	2	3	4	5	6	7	8	9
$k_i$	0	0	1	0	1	0	1	0	0	1
$A$	5	25	625	681	1011	369	421	779	947	925
$b$	1	1	625	625	67	67	1059	1059	1059	1013

Ответ.  $5^{596} \pmod{1234} = 1013$ .

**Задача 12.** Решить (подбором) сравнения.

$$12.1. x^4 + 2x^2 + 3x + 4 \equiv 0 \pmod{5}. \quad 12.2. x^4 + 2x^3 + 3x + 4 \equiv 0 \pmod{5}.$$

$$12.3. x^4 + 2x^3 + 3x^2 + 4 \equiv 0 \pmod{5}. \quad 12.4. x^4 + x^2 + 3x + 4 \equiv 0 \pmod{5}.$$

$$12.5. 2x^4 + x^3 + 3x + 4 \equiv 0 \pmod{5}. \quad 12.6. 2x^4 + x^3 + 3x^2 + 4 \equiv 0 \pmod{5}.$$

$$12.7. 2x^4 + 3x^3 + x + 4 \equiv 0 \pmod{5}. \quad 12.8. 2x^4 + 3x^3 + x + 4 \equiv 0 \pmod{5}.$$

$$12.9. 2x^4 + 3x^3 + x^2 + 4 \equiv 0 \pmod{5}. \quad 12.10. 2x^4 + 3x^3 + x^2 + 4x \equiv 0 \pmod{5}.$$

$$12.11. 2x^4 + 3x^3 + 4x + 1 \equiv 0 \pmod{5}. \quad 12.12. 2x^4 + 3x^3 + 4x + 1 \equiv 0 \pmod{5}.$$

$$12.13. 2x^4 + 3x^3 + 4x^2 + 1 \equiv 0 \pmod{5}. \quad 12.14. x^4 + 3x^3 + 2x + 4 \equiv 0 \pmod{5}.$$

$$12.15. x^4 + x^3 + 2x + 4 \equiv 0 \pmod{5}. \quad 12.16. x^4 + 3x^3 + 2x + 4 \equiv 0 \pmod{5}.$$

$$12.17. 3x^4 + x^3 + 2x + 4 \equiv 0 \pmod{5}. \quad 12.18. 3x^4 + x^3 + 2x + 4 \equiv 0 \pmod{5}.$$

$$12.19. 3x^4 + x^3 + 2x^2 + 4 \equiv 0 \pmod{5}. \quad 12.20. 3x^4 + 2x^2 + x + 4 \equiv 0 \pmod{5}.$$

$$12.21. 3x^4 + 2x^3 + x + 4 \equiv 0 \pmod{5}. \quad 12.22. 3x^4 + 2x^2 + x + 4 \equiv 0 \pmod{5}.$$

$$12.23. 3x^4 + 2x^2 + 4x + 1 \equiv 0 \pmod{5}. \quad 12.24. 3x^4 + 2x^3 + 4x + 1 \equiv 0 \pmod{5}.$$

$$12.25. 3x^4 + 2x^3 + 4x^2 + 1 \equiv 0 \pmod{5}. \quad 12.26. 3x^4 + 2x^3 + 4x^2 + x \equiv 0 \pmod{5}.$$

$$12.27. x^4 + 3x^2 + 4x + 2 \equiv 0 \pmod{5}. \quad 12.28. x^4 + 3x^3 + 4x + 2 \equiv 0 \pmod{5}.$$

$$12.29. x^4 + 3x^3 + 4x^2 + 2 \equiv 0 \pmod{5}. \quad 12.30. x^4 + 3x^3 + 4x^2 + 2x \equiv 0 \pmod{5}.$$

**Пример.** Решить (подбором) сравнение.

$$1. f(x) = x^5 + x + 1 \equiv 0 \pmod{7}.$$

$x$	0	1	2	3	4	5	6
-----	---	---	---	---	---	---	---

$f(x)$	1	3	35	247	1029	3131	7783
$f(x) \pmod{7}$	1	3	0	2	0	2	6

В полной системе вычетов  $0,1,2,3,4,5,6$  сравнению удовлетворяют числа  $x = 2, x = 4$ . Тогда сравнение имеет два решения:  $x \equiv 2 \pmod{7}$ ;  $x \equiv 4 \pmod{7}$ .

2.  $f(x) = x^3 - 2x + 6 \equiv 0 \pmod{11}$ .

$x$	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	6	5	10	27	62	121	210	335	502	717	986
$f(x) \pmod{11}$	6	5	10	5	7	0	1	5	7	2	7

В полной системе вычетов  $0,1,\dots,10$  сравнению удовлетворяет число  $x = 5$ . Сравнение имеет одно решение  $x \equiv 5 \pmod{11}$ .

3.  $f(x) = x^4 + 2x^3 + 6 \equiv 0 \pmod{8}$ .

$x$	0	1	2	3	4	5	6	7
$f(x)$	6	9	38	141	390	881	1734	3093
$f(x) \pmod{8}$	6	1	6	5	76	1	6	5

В полной системе вычетов  $0,1,\dots,7$  нет чисел, удовлетворяющих сравнению. Сравнение решений не имеет.

**Задача 13.** Решить (подбором) систему из двух сравнений с одним неизвестным. Первое сравнение взять из задачи 12. В качестве второго взять  $x^3 + x^2 \equiv 0 \pmod{2}$ .

**Пример.** Решить (подбором) систему из двух сравнений с одним неизвестным.

1.  $\begin{cases} f(x) = x^2 + x + 7 \equiv 0 \pmod{9}, \\ g(x) = x^3 - x + 3 \equiv 0 \pmod{9}. \end{cases}$  НОК(9,9) = [9,9] = 9.

$x$	0	1	2	3	4	5	6	7	8
$f(x)$	7	9	13	19	27	37	49	63	79
$g(x)$	3	3	9	27	63	123	213	339	507
$f(x) \pmod{9}$	7	0	4	1	0	1	4	0	7
$g(x) \pmod{9}$	3	3	0	0	0	6	6	0	3

В полной системе вычетов  $0,1,\dots,8$  по  $\pmod{9}$  обоим сравнениям удовлетворяют числа  $x=4, x=7$ . Система имеет два решения:

$x \equiv 4 \pmod{9}; x \equiv 7 \pmod{9}$ .

2.  $\begin{cases} f(x) = x^3 - 3x + 2 \equiv 0 \pmod{6}, \\ g(x) = 2x^2 + x + 2 \equiv 0 \pmod{4}. \end{cases}$  НОК(6,4) = [6,4] = 12.

$x$	0	1	2	3	4	5	6	7	8	9	10	11
$f(x)$	2	0	0	2	6	12	20	30	42	56	72	90
$g(x)$	2	5	12	23	38	57	80	107	138	173	212	255
$f(x) \pmod{6}$	2	0	0	2	0	0	2	0	0	2	0	0

$g(x) \pmod{94}$	2	1	0	3	2	1	0	3	2	1	0	3
------------------	---	---	---	---	---	---	---	---	---	---	---	---

В полной системе вычетов  $0, 1, \dots, 11$  по  $\pmod{12}$  обоим сравнениям удовлетворяют числа  $x=2, x=10$ . Система имеет два решения:

$$x \equiv 2 \pmod{12}; x \equiv -1 \pmod{12}.$$

**Задача 14.** Решить (подбором) систему из двух сравнений с двумя неизвестными. В качестве первого сравнения взять сравнение из задачи 12, заменив в нем все  $x$  кроме первого на  $y$ . В качестве второго сравнения взять  $x^3 + y + 1 \equiv 0 \pmod{2}$ .

**Задача 14.** Решить (подбором) систему из двух сравнений с двумя неизвестными.

$$\begin{cases} f(x, y) = x^2 - y^2 + 2 \equiv 0 \pmod{6}, \\ g(x, y) = x^3 + x + y + 1 \equiv 0 \pmod{3}. \end{cases} \quad \text{НОК}(6, 3) = [6, 3] = 6.$$

$f(x, y)$

$x \setminus y$	0	1	2	3	4	5
0	2	1	-2	-7	-14	-23
1	3	2	-1	-6	-13	-22
2	6	5	2	-3	-10	-19
3	11	10	7	2	-5	-14
4	18	17	14	9	2	-7
5	27	26	23	18	11	2

$g(x, y)$

$x \setminus y$	0	1	2	3	4	5
0	1	2	3	4	5	6
1	3	4	5	6	7	8
2	11	12	13	14	15	16
3	31	32	33	34	35	36
4	69	70	71	72	73	74
5	131	132	133	134	135	136

$f(x, y) \pmod{6}$

$x \setminus y$	0	1	2	3	4	5
0	2	1	4	5	4	1
1	3	2	5	0	5	2
2	0	5	2	3	2	5
3	5	4	1	2	1	4
4	0	5	2	3	2	5
5	3	2	5	0	5	2

$g(x, y) \pmod{3}$

$x \setminus y$	0	1	2	3	4	5
0	1	2	0	1	2	0
1	0	1	2	0	1	2
2	2	0	1	2	0	1
3	1	2	0	1	2	0
4	0	1	2	0	1	2
5	2	0	1	2	0	1

Число наборов  $(a, b)$ ,  $0 \leq a, b \leq 5$ , равно 36. Наборы  $(1, 3)$  и  $(4, 0)$  удовлетворяют системе. Система имеет два решения:

$$1) x \equiv 1 \pmod{6}, y \equiv 3 \pmod{6}; 2) x \equiv 4 \pmod{6}, y \equiv 0 \pmod{6}.$$

**Задача 15.** Решить (методом Гаусса) систему из трех сравнений.

**15.1.**

**15.2.**

**15.3.**

**15.4.**

**15.5.**

$$x \equiv 2 \pmod{7} \quad x \equiv 4 \pmod{7} \quad x \equiv 2 \pmod{7} \quad x \equiv 2 \pmod{7} \quad x \equiv 1 \pmod{7}$$

$$x \equiv 1 \pmod{11} \quad x \equiv 1 \pmod{11} \quad x \equiv 5 \pmod{11} \quad x \equiv 1 \pmod{11} \quad x \equiv 2 \pmod{11}$$

$$x \equiv 3 \pmod{13} \quad x \equiv 2 \pmod{13} \quad x \equiv 1 \pmod{13} \quad x \equiv 6 \pmod{13} \quad x \equiv 7 \pmod{13}$$

**15.6.**

**15.7.**

**15.8.**

**15.9.**

**15.10.**

$$x \equiv 4 \pmod{7} \quad x \equiv 3 \pmod{7} \quad x \equiv 6 \pmod{7} \quad x \equiv 1 \pmod{7} \quad x \equiv 5 \pmod{7}$$

$$x \equiv 1 \pmod{11} \quad x \equiv 1 \pmod{11} \quad x \equiv 3 \pmod{11} \quad x \equiv 3 \pmod{11} \quad x \equiv 4 \pmod{11}$$

$$x \equiv 3 \pmod{13} \quad x \equiv 5 \pmod{13} \quad x \equiv 1 \pmod{13} \quad x \equiv 7 \pmod{13} \quad x \equiv 1 \pmod{13}$$

- 15.11.**  $x \equiv 6 \pmod{7}$     $x \equiv 4 \pmod{7}$     $x \equiv 1 \pmod{7}$     $x \equiv 5 \pmod{7}$     $x \equiv 1 \pmod{7}$   
**15.12.**  $x \equiv 4 \pmod{11}$     $x \equiv 7 \pmod{11}$     $x \equiv 5 \pmod{11}$     $x \equiv 7 \pmod{11}$     $x \equiv 6 \pmod{11}$   
**15.13.**  $x \equiv 1 \pmod{13}$     $x \equiv 1 \pmod{13}$     $x \equiv 6 \pmod{13}$     $x \equiv 1 \pmod{13}$     $x \equiv 7 \pmod{13}$   
**15.14.**  $x \equiv 2 \pmod{7}$     $x \equiv 3 \pmod{7}$     $x \equiv 2 \pmod{7}$     $x \equiv 3 \pmod{7}$     $x \equiv 2 \pmod{7}$   
**15.15.**  $x \equiv 3 \pmod{11}$     $x \equiv 2 \pmod{11}$     $x \equiv 3 \pmod{11}$     $x \equiv 2 \pmod{11}$     $x \equiv 4 \pmod{11}$   
**15.16.**  $x \equiv 4 \pmod{13}$     $x \equiv 5 \pmod{13}$     $x \equiv 6 \pmod{13}$     $x \equiv 7 \pmod{13}$     $x \equiv 5 \pmod{13}$   
**15.17.**  $x \equiv 2 \pmod{7}$     $x \equiv 3 \pmod{7}$     $x \equiv 2 \pmod{7}$     $x \equiv 3 \pmod{7}$     $x \equiv 2 \pmod{7}$   
**15.18.**  $x \equiv 3 \pmod{11}$     $x \equiv 2 \pmod{11}$     $x \equiv 3 \pmod{11}$     $x \equiv 2 \pmod{11}$     $x \equiv 4 \pmod{11}$   
**15.19.**  $x \equiv 4 \pmod{13}$     $x \equiv 5 \pmod{13}$     $x \equiv 6 \pmod{13}$     $x \equiv 7 \pmod{13}$     $x \equiv 5 \pmod{13}$   
**15.20.**  $x \equiv 6 \pmod{7}$     $x \equiv 4 \pmod{7}$     $x \equiv 6 \pmod{7}$     $x \equiv 5 \pmod{7}$     $x \equiv 2 \pmod{7}$   
**15.21.**  $x \equiv 2 \pmod{11}$     $x \equiv 7 \pmod{11}$     $x \equiv 5 \pmod{11}$     $x \equiv 2 \pmod{11}$     $x \equiv 7 \pmod{11}$   
**15.22.**  $x \equiv 4 \pmod{13}$     $x \equiv 2 \pmod{13}$     $x \equiv 2 \pmod{13}$     $x \equiv 7 \pmod{13}$     $x \equiv 6 \pmod{13}$   
**15.23.**  $x \equiv 4 \pmod{7}$     $x \equiv 3 \pmod{7}$     $x \equiv 4 \pmod{7}$     $x \equiv 5 \pmod{7}$     $x \equiv 3 \pmod{7}$   
**15.24.**  $x \equiv 3 \pmod{11}$     $x \equiv 4 \pmod{11}$     $x \equiv 3 \pmod{11}$     $x \equiv 3 \pmod{11}$     $x \equiv 5 \pmod{11}$   
**15.25.**  $x \equiv 5 \pmod{13}$     $x \equiv 6 \pmod{13}$     $x \equiv 7 \pmod{13}$     $x \equiv 6 \pmod{13}$     $x \equiv 7 \pmod{13}$   
**15.26.**  $x \equiv 5 \pmod{7}$ ,  $x \equiv 7 \pmod{11}$ ,  $x \equiv 3 \pmod{13}$ .  
**15.27.**  $x \equiv 3 \pmod{11}$ ,  $x \equiv 4 \pmod{13}$ ,  $x \equiv 2 \pmod{7}$ .  
**15.28.**  $x \equiv 4 \pmod{13}$ ,  $x \equiv 2 \pmod{11}$ ,  $x \equiv 3 \pmod{7}$ .  
**15.29.**  $x \equiv 6 \pmod{7}$ ,  $x \equiv 7 \pmod{11}$ ,  $x \equiv 6 \pmod{13}$ .  
**15.30.**  $x \equiv 7 \pmod{13}$ ,  $x \equiv 6 \pmod{7}$ ,  $x \equiv 3 \pmod{11}$ .  
**15.31.**  $x \equiv 6 \pmod{7}$ ,  $x \equiv 7 \pmod{11}$ ,  $x \equiv 3 \pmod{13}$ .

*Алгоритм Гаусса для системы сравнений  
 $x \equiv c_1 \pmod{m_1}, \dots, x \equiv c_k \pmod{m_k}$   
с попарно взаимно простыми модулями*

$$x \equiv (\sum_{s=1}^k M_s N_s c_s) \pmod{M},$$

где  $M = m_1 m_2 \dots m_k$ ,  $M_s = M/m_s$ ,  $N_s \equiv M_s^{-1} \pmod{m_s}$ ,  $s=1,2,\dots,k$ .

**Пример.** Решить систему сравнений (методом Гаусса).

$$x \equiv 1 \pmod{4}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}.$$

*Решение.*  $c_1 = 1$ ,  $c_2 = 3$ ,  $c_3 = 2$ . Модули  $m_1 = 4$ ,  $m_2 = 5$ ,  $m_3 = 7$  попарно взаимно просты. Система совместна. Далее вычисляем следующее.

$$M = m_1 m_2 m_3 = 4 \cdot 5 \cdot 7 = 140; M_1 = \frac{M}{m_1} = m_2 m_3 = 5 \cdot 7 = 35,$$

$$M_2 = \frac{M}{m_2} = m_1 m_3 = 4 \cdot 7 = 28, M_3 = \frac{M}{m_3} = m_1 m_2 = 4 \cdot 5 = 20.$$

Сравнения  $M_1 N_1 \equiv 1 \pmod{m_1}$ ,  $M_2 N_2 \equiv 1 \pmod{m_2}$ ,  $M_3 N_3 \equiv 1 \pmod{m_3}$  есть  $35N_1 \equiv 1 \pmod{4}$ ,  $28N_2 \equiv 1 \pmod{5}$ ,  $20N_3 \equiv 1 \pmod{7}$ .

Решим первое сравнение  $35N_1 - 1 \equiv 0 \pmod{4}$ ,

$N_1$	0	1	2	3
$35N_1 - 1$	-1	34	69	104
$35N_1 - 1 \pmod{4}$	3	2	1	0

$N_1 = 3$ . Аналогично находим  $N_2 = 2$ ,  $N_3 = 6$ . Тогда

$$x_0 = M_1 N_1 c_1 + M_2 N_2 c_2 + M_3 N_3 c_3 = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 6 \cdot 2 = 513.$$

Находим  $x \equiv x_0 \pmod{M}$ ,  $x \equiv 513 \pmod{140}$ ,  $x \equiv 93 \pmod{140}$ .

*Ответ.*  $x \equiv 93 \pmod{140}$ .

**Задача 16.** Решить систему из трех сравнений.

**16.1.**

$$x \equiv 2 \pmod{7} \quad x \equiv 4 \pmod{7} \quad x \equiv 2 \pmod{7} \quad x \equiv 2 \pmod{7} \quad x \equiv 1 \pmod{7}$$

$$x \equiv 1 \pmod{9} \quad x \equiv -1 \pmod{9} \quad x \equiv 5 \pmod{9} \quad x \equiv 1 \pmod{9} \quad x \equiv 1 \pmod{9}$$

$$x \equiv 4 \pmod{15} \quad x \equiv 2 \pmod{15} \quad x \equiv 2 \pmod{15} \quad x \equiv 7 \pmod{15} \quad x \equiv 7 \pmod{15}$$

**16.6.**

**16.7.**

**16.8.**

**16.9.**

**16.10.**

$$x \equiv 4 \pmod{7} \quad x \equiv 3 \pmod{7} \quad x \equiv 6 \pmod{7} \quad x \equiv 1 \pmod{7} \quad x \equiv 5 \pmod{7}$$

$$x \equiv -3 \pmod{9} \quad x \equiv -1 \pmod{9} \quad x \equiv 3 \pmod{9} \quad x \equiv -2 \pmod{9} \quad x \equiv 4 \pmod{9}$$

$$x \equiv 3 \pmod{15} \quad x \equiv 5 \pmod{15} \quad x \equiv 7 \pmod{15} \quad x \equiv 7 \pmod{15} \quad x \equiv 1 \pmod{15}$$

**16.11.**

**16.12.**

**16.13.**

**16.14.**

**16.15.**

$$x \equiv 6 \pmod{7} \quad x \equiv 4 \pmod{7} \quad x \equiv 1 \pmod{7} \quad x \equiv 5 \pmod{7} \quad x \equiv 1 \pmod{7}$$

$$x \equiv 4 \pmod{9} \quad x \equiv 7 \pmod{9} \quad x \equiv -5 \pmod{9} \quad x \equiv 7 \pmod{9} \quad x \equiv 8 \pmod{9}$$

$$x \equiv 1 \pmod{15} \quad x \equiv 1 \pmod{15} \quad x \equiv 7 \pmod{15} \quad x \equiv 1 \pmod{15} \quad x \equiv 2 \pmod{15}$$

**16.16.**

**16.17.**

**16.18.**

**16.19.**

**16.20.**

$$x \equiv 2 \pmod{7} \quad x \equiv 3 \pmod{7} \quad x \equiv 2 \pmod{7} \quad x \equiv 3 \pmod{7} \quad x \equiv 2 \pmod{7}$$

$$x \equiv 8 \pmod{9} \quad x \equiv 2 \pmod{9} \quad x \equiv 3 \pmod{9} \quad x \equiv 1 \pmod{9} \quad x \equiv -4 \pmod{9}$$

$$x \equiv 2 \pmod{15} \quad x \equiv 5 \pmod{15} \quad x \equiv 6 \pmod{15} \quad x \equiv 8 \pmod{15} \quad x \equiv 5 \pmod{15}$$

**16.21.**

**16.22.**

**16.23.**

**16.24.**

**16.25.**

$$x \equiv 6 \pmod{7} \quad x \equiv 4 \pmod{7} \quad x \equiv 6 \pmod{7} \quad x \equiv 5 \pmod{7} \quad x \equiv 2 \pmod{7}$$

$$x \equiv -2 \pmod{9} \quad x \equiv -7 \pmod{9} \quad x \equiv -5 \pmod{9} \quad x \equiv -2 \pmod{9} \quad x \equiv -7 \pmod{9}$$

$$x \equiv 4 \pmod{15} \quad x \equiv 2 \pmod{15} \quad x \equiv 2 \pmod{15} \quad x \equiv 7 \pmod{15} \quad x \equiv 8 \pmod{15}$$

**16.26.**

**16.27.**

**16.28.**

**16.29.**

**16.30.**

$$x \equiv 4 \pmod{7} \quad x \equiv 3 \pmod{7} \quad x \equiv 4 \pmod{7} \quad x \equiv 5 \pmod{7} \quad x \equiv 3 \pmod{7}$$

$$x \equiv -5 \pmod{9} \quad x \equiv -5 \pmod{9} \quad x \equiv -4 \pmod{9} \quad x \equiv -7 \pmod{9} \quad x \equiv -5 \pmod{9}$$

$$x \equiv 7 \pmod{15} \quad x \equiv 7 \pmod{15} \quad x \equiv 8 \pmod{15} \quad x \equiv 2 \pmod{15} \quad x \equiv 1 \pmod{15}$$

**16.31.**  $x \equiv 6 \pmod{7}$ ,  $x \equiv 7 \pmod{9}$ ,  $x \equiv 3 \pmod{15}$ .

### *Произвольные модули*

Рассмотрим систему сравнений  $(S)$   $\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}. \end{cases}$  Пусть  $d = (m_1, m_2)$ ,  $M = [m_1, m_2]$ . Для каждого целого  $t$  значение  $x = c_1 + m_1 t$  удовлетворяет первому сравнению из  $(S)$ . Надо найти такое  $t$ , при котором  $x$  удовлетворяет второму сравнению из  $(S)$ , то есть  $c_1 + m_1 t \equiv c_2 \pmod{m_2}$ . Задача сведена к решению сравнения  $m_1 t \equiv c_2 - c_1 \pmod{m_2}$ . Если  $d \nmid (c_2 - c_1)$ , то это сравнение (и сравнение  $(S)$ ) не имеет решений. Если  $d \mid (c_2 - c_1)$ , то сравнение имеет одно решение  $t \equiv a \pmod{m_2/d}$ , или  $t = a + (m_2/d)t_1$  при некотором целом  $a$ . Поэтому  $x = c_1 + m_1(a + (m_2/d)t_1) = c_1 + m_1a + m_1(m_2/d)t_1 = a_1 + Mt_1$  с  $a_1 = c_1 + m_1a$ , откуда  $x \equiv a_1 \pmod{M}$  есть решение сравнения  $(S)$ .

Рассмотрим систему сравнений

$$a_1x \equiv b_1 \pmod{m_1}, \dots, a_sx \equiv b_s \pmod{m_s}. \quad (4.10')$$

Если  $(a_i, m_i) = d_i$ ,  $d_i \nmid b_i$  для некоторого  $1 \leq i \leq s$ , то система (4.10') не имеет решений. Если для  $i = 1, \dots, s$  целое  $d_i | b_i$ , то каждое сравнение можно решить относительно  $x$ , и система (4.10') эквивалентна системе

$$x \equiv c_1 \pmod{m_1/d_1}, \dots, x \equiv c_s \pmod{m_s/d_s}. \quad (4.11)$$

Система (4.11) или не имеет решений, или если решения существуют, то можно найти решение системы (4.11), последовательно решая системы двух сравнений, в результате чего получим решение для (4.11), которое образует класс по модулю  $[m_1/d_1, \dots, m_s/d_s]$ .

**Пример.** Система (1)  $\begin{cases} 6x \equiv 5 \pmod{7}, \\ 7x \equiv 8 \pmod{9}, \\ 2x \equiv 7 \pmod{15} \end{cases}$

*Решение.* Решаем сравнение  $6x - 5 \equiv 0 \pmod{7}$ ,  $f(x) = 6x - 5$ .

$x$	0	1	2	3	4	5	6
$f(x)$	-5	1	7	13	19	32	31
$f(x) \pmod{7}$	-5	1	0	6	5	6	3

$$x \equiv 2 \pmod{7}.$$

Решаем сравнение  $7x - 8 \equiv 0 \pmod{9}$ ,  $f(x) = 7x - 8$ .

$x$	0	1	2	3	4	5	6	7	8
$f(x)$	-8	-1	6	13	20	27	34	41	48
$f(x) \pmod{9}$	-8	-1	6	4	2	0	7	5	3

$$x \equiv 5 \pmod{9}.$$

Решаем сравнение  $2x - 7 \equiv 0 \pmod{15}$ ,  $f(x) = 2x - 7$ .

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(x)$	-7	-5	-3	1	1	3	5	7	9	11	13	15	17	19	21
$f(x) \pmod{9}$	-7	-5	-3	1	1	3	5	7	9	11	13	0	2	4	6

$$x \equiv 11 \pmod{15}.$$

Система (1)  $\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 5 \pmod{9}, \\ x \equiv 11 \pmod{15} \end{cases}$  эквивалентна системе (2)  $\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 5 \pmod{9}, \\ x \equiv 11 \pmod{15} \end{cases}$ . Решаем систему 2.

$c_1=2, c_2=5, c_3=11$ . Модули  $m_1=7, m_2=9, m_3=15$  не являются попарно взаимно простыми:  $d=(9,15)=3 \neq 1$ . Решаем систему из двух первых сравнений

$$\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 5 \pmod{9}. \end{cases} \quad (3)$$

$d=\text{нод}(7,9)=1 \mid (7-9)=-2$ . Система (3) совместна.

Если  $d \nmid (c_1 - c_2)$ , то система несовместна.

Из второго сравнения в (3)

$$x=5+9t \quad (4)$$

(4) подставляем в первое сравнение в (3):

$$x=5+9t \equiv 2 \pmod{7}, 9t \equiv -3 \pmod{7}, 9t-7t \equiv -3 \pmod{7}, 2t \equiv -3 \pmod{7},$$

$2t \equiv 4 \pmod{7}$ ,  $t \equiv 2 \pmod{7}$ ,  $t=2+7y$  подставляем в (4):

$$x = 5+9t = 5+9(2+7y) = 23+63y,$$

$$x = 23+63y \quad (5)$$

Равенство (5) эквивалентно

$$x \equiv 23 \pmod{63} \quad (5a),$$

которое вместе с третьим сравнением в (2) дает систему

$$(6) \begin{cases} x \equiv 23 \pmod{63}, \\ x \equiv 11 \pmod{15}. \end{cases} \quad (6)$$

В (6)  $d=(63,15)=3$  |  $(23-11)=12$ . Система (6) совместна.

Подставляем  $x = 23 + 63y$  из (5a) во второе сравнения в (6) и получаем

$$x = 23 + 63y \equiv 11 \pmod{15}, 63y \equiv -12 \pmod{15}, 3y \equiv 3 \pmod{15}, y \equiv 1 \pmod{5}.$$

Подставляем  $y=1+5z$  в (5):  $x = 23 + 63(1+5z) = 86+315z$ ,  $x = 86+315z$ .

*Ответ.*  $x \equiv 86 \pmod{315}$ .

**Задача 17.** Решить систему из трех сравнений.

**17.1.**

**17.2.**

**17.3.**

**17.4.**

**17.5.**

$$\begin{array}{lllll} 3x \equiv 2 \pmod{7} & 4x \equiv 4 \pmod{7} & 5x \equiv 2 \pmod{7} & 6x \equiv 2 \pmod{7} & 4x \equiv 1 \pmod{7} \\ 4x \equiv 1 \pmod{9} & 2x \equiv -1 \pmod{9} & 7x \equiv 5 \pmod{9} & 5x \equiv 1 \pmod{9} & 4x \equiv 1 \pmod{9} \\ 3x \equiv 4 \pmod{13} & 5x \equiv 2 \pmod{13} & 6x \equiv 2 \pmod{13} & 4x \equiv 7 \pmod{13} & 5x \equiv 7 \pmod{13} \end{array}$$

**17.6.**

**17.7.**

**17.8.**

**17.9.**

**17.10.**

$$\begin{array}{lllll} 5x \equiv 4 \pmod{7} & 5x \equiv 3 \pmod{7} & 6x \equiv 6 \pmod{7} & 5x \equiv 1 \pmod{7} & 4x \equiv 5 \pmod{7} \\ 7x \equiv -3 \pmod{9} & 7x \equiv -1 \pmod{9} & 2x \equiv 3 \pmod{9} & 5x \equiv -2 \pmod{9} & 2x \equiv 4 \pmod{9} \\ 4x \equiv 3 \pmod{13} & 4x \equiv 5 \pmod{13} & 6x \equiv 7 \pmod{13} & 5x \equiv 7 \pmod{13} & 7x \equiv 1 \pmod{13} \end{array}$$

**17.11.**

**17.12.**

**17.13.**

**17.14.**

**17.15.**

$$\begin{array}{lllll} 3x \equiv 6 \pmod{7} & 6x \equiv 4 \pmod{7} & 5x \equiv 1 \pmod{7} & 4x \equiv 5 \pmod{7} & 6x \equiv 1 \pmod{7} \\ 4x \equiv 4 \pmod{9} & 7x \equiv 7 \pmod{9} & 2x \equiv -5 \pmod{9} & 4x \equiv 7 \pmod{9} & 5x \equiv 8 \pmod{9} \\ 4x \equiv 1 \pmod{13} & 3x \equiv 1 \pmod{13} & 2x \equiv 7 \pmod{13} & 3x \equiv 1 \pmod{13} & 4x \equiv 2 \pmod{13} \end{array}$$

**17.16.**

**17.17.**

**17.18.**

**17.19.**

**17.20.**

$$\begin{array}{lllll} 3x \equiv 2 \pmod{7} & 4x \equiv 3 \pmod{7} & 3x \equiv 2 \pmod{7} & 6x \equiv 3 \pmod{7} & 5x \equiv 2 \pmod{7} \\ 7x \equiv 8 \pmod{9} & 5x \equiv 2 \pmod{9} & 4x \equiv 3 \pmod{9} & 2x \equiv 1 \pmod{9} & 7x \equiv -4 \pmod{9} \\ 5x \equiv 2 \pmod{13} & 4x \equiv 5 \pmod{13} & 3x \equiv 6 \pmod{13} & 6x \equiv 8 \pmod{13} & 5x \equiv 5 \pmod{13} \end{array}$$

**17.21.**

**17.22.**

**17.23.**

**17.24.**

**17.25.**

$$\begin{array}{lllll} 3x \equiv 6 \pmod{7} & 6x \equiv 4 \pmod{7} & 4x \equiv 6 \pmod{7} & 5x \equiv 5 \pmod{7} & 6x \equiv 2 \pmod{7} \\ 2x \equiv -2 \pmod{9} & 5x \equiv -7 \pmod{9} & 7x \equiv -5 \pmod{9} & 4x \equiv -2 \pmod{9} & 2x \equiv -7 \pmod{9} \\ 5x \equiv 4 \pmod{13} & 7x \equiv 2 \pmod{13} & 3x \equiv 2 \pmod{13} & 5x \equiv 7 \pmod{13} & 6x \equiv 8 \pmod{13} \end{array}$$

**17.26.**

**17.27.**

**17.28.**

**17.29.**

**17.30.**

$$\begin{array}{lllll} 3x \equiv 6 \pmod{7} & 4x \equiv 3 \pmod{7} & 5x \equiv 4 \pmod{7} & 6x \equiv 5 \pmod{7} & 4x \equiv 3 \pmod{7} \\ 2x \equiv -5 \pmod{9} & 7x \equiv -5 \pmod{9} & 4x \equiv -4 \pmod{9} & 5x \equiv -7 \pmod{9} & 7x \equiv -5 \pmod{9} \end{array}$$

$$4x \equiv 7 \pmod{13} \quad 5x \equiv 7 \pmod{13} \quad 3x \equiv 8 \pmod{13} \quad 5x \equiv 2 \pmod{13} \quad 5x \equiv 1 \pmod{13}$$

$$\boxed{17.31. \quad 5x \equiv 6 \pmod{7}, \quad 2x \equiv 7 \pmod{9}, \quad 7x \equiv 3 \pmod{13}.}$$

**Пример.** Решить систему из трех сравнений

$$\begin{cases} 7x \equiv 3 \pmod{11}, \\ 15x \equiv 5 \pmod{35}, \\ 3x \equiv 2 \pmod{5}. \end{cases}$$

*Решение.* Исходная система эквивалентна системе

$$\begin{cases} 7x \equiv 3 \pmod{11}, \\ 3x \equiv 1 \pmod{7}, \\ 3x \equiv 2 \pmod{5}. \end{cases}$$

Решаем сравнение  $7x - 3 \equiv 0 \pmod{11}$ ,  $f(x) = 7x - 3$ .

$x$	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	-3	4	11	18	25	32	39	46	53	60	67
$f(x) \pmod{11}$	-3	4	0	7	5	10	6	2	9	5	1

$$x \equiv 2 \pmod{11}.$$

Решаем сравнение  $3x - 1 \equiv 0 \pmod{7}$ ,  $f(x) = 3x - 1$ .

$x$	0	1	2	3	4	5	6
$f(x)$	-1	2	5	8	11	14	17
$f(x) \pmod{7}$	-1	2	5	1	4	0	3

$$x \equiv 5 \pmod{7}.$$

Решаем сравнение  $3x - 2 \equiv 0 \pmod{5}$ ,  $f(x) = 3x - 2$ .

$x$	0	1	2	3	4
$f(x)$	-2	1	4	7	10
$f(x) \pmod{7}$	-2	1	4	2	0

$$x \equiv 4 \pmod{5}.$$

Исходная система сравнений эквивалентна системе

$$\begin{cases} x \equiv 2 \pmod{11}, \\ x \equiv 5 \pmod{7}, \\ x \equiv 4 \pmod{5}. \end{cases}$$

Последнюю систему решаем методом Гаусса.

$$c_1 = 2, c_2 = 5, c_3 = 4; m_1 = 11, m_2 = 7, m_3 = 5, M = m_1 m_2 m_3 = 11 \cdot 7 \cdot 5 = 385;$$

$$M_1 = \frac{M}{m_1} = m_2 m_3 = 7 \cdot 5 = 35, M_2 = \frac{M}{m_2} = m_1 m_3 = 11 \cdot 5 = 55,$$

$$M_3 = \frac{M}{m_3} = m_1 m_2 = 11 \cdot 7 = 77. \text{ Сравнения}$$

$M_1 N_1 \equiv 1 \pmod{m_1}, M_2 N_2 \equiv 1 \pmod{m_2}, M_3 N_3 \equiv 1 \pmod{m_3}$  есть  
 $35N_1 \equiv 1 \pmod{11}, 55N_2 \equiv 1 \pmod{7}, 77N_3 \equiv 1 \pmod{5}$ , откуда  
 $2N_1 \equiv 1 \pmod{11}, 6N_2 \equiv 1 \pmod{7}, 2N_3 \equiv 1 \pmod{5}$ , которым удовлетворяют  
 $N_1 = 6, N_2 = -1, N_3 = 3$ . Тогда  $x_0 = M_1 N_1 c_1 + M_2 N_2 c_2 + M_3 N_3 c_3 =$   
 $35 \cdot 6 \cdot 2 - 55 \cdot 1 \cdot 5 + 77 \cdot 3 \cdot 4 = 1069$ . Отсюда  $x_0 \equiv 1069 \pmod{385}$ .

*Ответ.*  $x_0 \equiv 299 \pmod{385}$ .

**Задача 18.** Определить с помощью символа Лежандра, имеет ли решение сравнение  $x^2 \equiv a \pmod{p}$ , 1)  $a = 68$ , 2)  $a = -68$ , простое число  $p$  определяется вариантом задания.

- 18.1.** 631. **18.2.** 641. **18.3.** 643. **18.4.** 647. **18.5.** 653.  
**18.6.** 659. **18.7.** 661. **18.8.** 673. **18.9.** 677. **18.10.** 683.  
**18.11.** 691. **18.12.** 701. **18.13.** 709. **18.14.** 719. **18.15.** 727.  
**18.16.** 733. **18.17.** 739. **18.18.** 743. **18.19.** 751. **18.20.** 757.  
**18.21.** 761. **18.22.** 769. **18.23.** 773. **18.24.** 787. **18.25.** 797.  
**18.26.** 809. **18.27.** 811. **18.28.** 821. **18.29.** 823. **18.30.** 827.

**Определение.** Пусть  $p$  есть нечетное простое число и  $a$  есть некоторое целое число. Символ Лежандра (символ  $a$  по  $p$ )

$$\begin{aligned} \left( \frac{a}{p} \right) &= \begin{cases} 0, & \text{если } p|a, \\ 1, & \text{если } a \text{ есть квадратичный вычет по } \pmod{p}, \\ -1, & \text{если } a \text{ есть квадратичный невычет по } \pmod{p}. \end{cases} \\ &= \begin{cases} 0, & \text{если } p|a, \\ 1, & \text{если сравнение } x^2 \equiv a \pmod{p} \text{ имеет (два) решения,} \\ -1, & \text{если сравнение } x^2 \equiv a \pmod{p} \text{ не имеет решений.} \end{cases} \\ &= \begin{cases} 0, & \text{если } p|a, \\ 1, & \text{если существует } x \equiv \sqrt{a} \pmod{p}, \\ -1, & \text{если не существует } x \equiv \sqrt{a} \pmod{p}. \end{cases} \end{aligned}$$

**Свойства символа Лежандра.**

- (1)  $\left( \frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p}; \left( \frac{1}{p} \right) = 1$ , ибо  $x^2 \equiv 1 \pmod{p}$  имеет решения  $x=1, x=-1$ .
- $$\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}, \quad \left( \frac{-1}{p} \right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{4}, \\ -1, & \text{если } p \equiv 3 \pmod{4}. \end{cases}$$
- (2)  $\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \cdot \left( \frac{b}{p} \right)$ . Если  $a \in \mathbb{Z}_p^*$ , то  $\left( \frac{a^2}{p} \right) = \left( \frac{a}{p} \right) \cdot \left( \frac{a}{p} \right) = 1$ .

(3) Если  $a \equiv b \pmod{p}$ , то  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

(4)  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{если } p \equiv 1 \text{ или } 7 \pmod{8}, \\ -1, & \text{если } p \equiv 3 \text{ или } 5 \pmod{8}. \end{cases}$

(5) Закон квадратичной взаимности. Если  $q$  есть нечетное простое число и  $q \neq p$ , то  $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$ .

**Пример.** Пусть  $p$  есть нечетное простое число и  $a$  есть некоторое целое число. Определить, имеет ли решение сравнение  $x^2 \equiv a \pmod{p}$ .

1.  $x^2 \equiv 68 \pmod{113}$ . *Решение.* Символ Лежандра

$$\begin{aligned} \left(\frac{68}{113}\right) &= \left(\frac{2^2 \cdot 17}{113}\right) =_{(2)} \left(\frac{2^2}{113}\right) \cdot \left(\frac{17}{113}\right) =_{(2,5)} 1 \cdot \left(\frac{113}{17}\right) \cdot (-1)^{\frac{(17-1)(113-1)}{4}} = \\ \left(\frac{113}{17}\right) &= [113 \equiv 11 \pmod{17}] =_{(3)} \left(\frac{11}{17}\right) =_{(5)} \left(\frac{17}{11}\right) \cdot (-1)^{\frac{(11-1)(17-1)}{4}} = \\ \left(\frac{17}{11}\right) &= [17 \equiv 6 \pmod{11}] =_{(3)} \left(\frac{6}{11}\right) = \left(\frac{2 \cdot 3}{11}\right) =_{(2)} \left(\frac{2}{11}\right) \cdot \left(\frac{3}{11}\right) =_{(4)} \\ (-1)^{\frac{11^2-1}{8}} \cdot \left(\frac{3}{11}\right) &= -1 \cdot \left(\frac{11}{3}\right) \cdot (-1)^{\frac{(3-1)(11-1)}{4}} = \left(\frac{11}{3}\right) = [11 \equiv 2 \pmod{3}] =_{(3)} \\ \left(\frac{2}{3}\right) &= (-1)^{\frac{3^2-1}{8}} = -1. \end{aligned}$$

*Ответ.* Сравнение решений не имеет.

2.  $x^2 \equiv 310 \pmod{521}$ . *Решение.* Символ Лежандра

$$\begin{aligned} \left(\frac{310}{521}\right) &= \left(\frac{2 \cdot 5 \cdot 31}{521}\right) =_{(2)} \left(\frac{2}{521}\right) \cdot \left(\frac{5}{521}\right) \cdot \left(\frac{31}{521}\right) = (-1)^{\frac{521^2-1}{8}} \cdot \left(\frac{5}{521}\right) \cdot \left(\frac{31}{521}\right) =_{(5)} \\ \left(\frac{521}{5}\right) \cdot (-1)^{\frac{(5-1)(521-1)}{4}} \cdot \left(\frac{521}{31}\right) &\cdot (-1)^{\frac{(31-1)(521-1)}{4}} = \left(\frac{521}{5}\right) \cdot \left(\frac{521}{31}\right) = \\ \left[ \begin{array}{l} 521 \equiv 1 \pmod{5} \\ 521 \equiv 25 \pmod{31} \end{array} \right] &=_{(3)} \left(\frac{1}{5}\right) \cdot \left(\frac{25}{31}\right) =_{(1)} \left(\frac{5^2}{31}\right) =_{(2)} 1. \end{aligned}$$

*Ответ.* Сравнение имеет два решения.

3.  $x^2 \equiv -174 \pmod{521}$ . *Решение.* Символ Лежандра

$$\begin{aligned} \left(\frac{-174}{619}\right) &= \left(\frac{-1 \cdot 2 \cdot 3 \cdot 29}{619}\right) =_{(2)} \left(\frac{-1}{619}\right) \cdot \left(\frac{2}{619}\right) \cdot \left(\frac{3}{619}\right) \cdot \left(\frac{29}{619}\right) =_{(1,2)} \\ -\left(\frac{2}{619}\right) \cdot \left(\frac{3}{619}\right) \cdot \left(\frac{29}{619}\right) &=_{(4,5)} \\ -(-1)^{\frac{619^2-1}{8}} \cdot \left(\frac{619}{3}\right) \cdot (-1)^{\frac{(3-1)(619-1)}{4}} \cdot \left(\frac{619}{29}\right) &(-1)^{\frac{(5-1)(521-1)}{4}} = \end{aligned}$$

$$\begin{aligned}
& -(-1)(-1) \cdot 1 \cdot \left( \frac{619}{3} \right) \cdot \left( \frac{619}{29} \right) = \begin{bmatrix} 619 \equiv 1 \pmod{3} \\ 619 \equiv 10 \pmod{29} \end{bmatrix} =_{(3)} -\left( \frac{1}{3} \right) \cdot \left( \frac{10}{29} \right) =_{(1)} \\
& -\left( \frac{2 \cdot 5}{29} \right) =_{(3)} -\left( \frac{2}{29} \right) \cdot \left( \frac{5}{29} \right) =_{(4,5)} -(-1)^{\frac{29^2-1}{8}} \cdot \left( \frac{29}{5} \right) \cdot (-1)^{\frac{(5-1)(29-1)}{4}} = \\
& \left( \frac{29}{5} \right) = [29 \equiv 4 \pmod{5}] =_{(3)} \left( \frac{4}{5} \right) = \left( \frac{2^2}{5} \right) =_{(2)} 1.
\end{aligned}$$

*Ответ.* Сравнение имеет два решения.

**Задача 19.** Определить с помощью символа Лежандра, имеет ли решение сравнение  $x^2 \equiv a \pmod{p}$ . Вычислять символ Лежандра  $\left( \frac{a}{p} \right)$ , рассматривая его как символ Якоби. 1)  $a = 506$ , 2)  $a = -506$ , простое число  $p$  определяется вариантом задания.

**19.1.** 1447.    **19.2.** 1451.    **19.3.** 1453.    **19.4.** 1459.

**19.5.** 1471.    **19.6.** 1481.    **19.7.** 1483.    **19.8.** 1487.

**19.9.** 1489.    **19.10.** 1493.    **19.11.** 1499.    **19.12.** 1511.

**19.13.** 1523.    **19.14.** 1531.    **19.15.** 1543.    **19.16.** 1549.

**19.17.** 1553.    **19.18.** 1559.    **19.19.** 1567.    **19.20.** 1571.

**19.21.** 1579.    **19.22.** 1583.    **19.23.** 1597.    **19.24.** 1601.

**19.25.** 1607.    **19.26.** 1609.    **19.27.** 1613.    **19.28.** 1619.

**19.29.** 1621.    **19.30.** 1627.

**Определение.** Пусть  $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} \geq 3$ , где  $p_i$  есть простые числа, среди которых могут быть одинаковые. Символ Якоби

$$\left( \frac{a}{n} \right) = \left( \frac{a}{p_1} \right)^{e_1} \left( \frac{a}{p_2} \right)^{e_2} \dots \left( \frac{a}{p_s} \right)^{e_s}, \text{ где } \left( \frac{a}{p_i} \right) \text{ есть символ Лежандра.}$$

**Замечание.** Символ Якоби вычисляется быстрее символа Лежандра.

**Свойства символа Якоби.** Пусть  $m \geq 3, n \geq 3$  и  $a, b \in \mathbb{Z}$ .

$$(1) \left( \frac{a}{n} \right) = 0, 1 \text{ или } -1, \quad \left( \frac{a}{n} \right) = 0 \Leftrightarrow \text{нод}(a, n) \neq 1.$$

$$(2) \left( \frac{ab}{n} \right) = \left( \frac{a}{n} \right) \cdot \left( \frac{b}{n} \right). \text{ Если } a \in \mathbb{Z}_p^*, \text{ то } \left( \frac{a^2}{p} \right) = 1.$$

$$(3) \left( \frac{a}{mn} \right) = \left( \frac{a}{m} \right) \cdot \left( \frac{b}{n} \right).$$

$$(4) \text{ Если } a \equiv b \pmod{p}, \text{ то } \left( \frac{a}{n} \right) = \left( \frac{b}{n} \right).$$

$$(5) \left( \frac{1}{n} \right) = 1.$$

$$(6) \left( \frac{-1}{n} \right) = (-1)^{\frac{n-1}{2}}, \left( \frac{-1}{n} \right) = \begin{cases} 1, & \text{если } n \equiv 1 \pmod{4}, \\ -1, & \text{если } n \equiv 3 \pmod{4}. \end{cases}$$

$$(7) \left( \frac{2}{n} \right) = (-1)^{\frac{n^2-1}{8}}, \left( \frac{2}{n} \right) = \begin{cases} 1, & \text{если } n \equiv 1 \text{ или } 7 \pmod{8}, \\ -1, & \text{если } n \equiv 3 \text{ или } 5 \pmod{8}. \end{cases}$$

$$(8) \text{Закон квадратичной взаимности. } \left( \frac{m}{n} \right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left( \frac{n}{m} \right).$$

$$(9) \text{Если } a = 2^e b, \text{ где } b \text{ нечетно, то } \left( \frac{a}{n} \right) = \left( \frac{2^e}{n} \right) \cdot \left( \frac{n \pmod{b}}{b} \right) \cdot (-1)^{\frac{(b-1)(n-1)}{4}}.$$

### **Алгоритм вычисления символа Якоби (и символа Лежандра)**

JACOBI( $a, n$ )

ВХОД. Нечетное число  $n \geq 3$  и число  $a$ ,  $0 \leq a < n$ .

ВЫХОД. Символ Якоби  $\left( \frac{a}{n} \right)$  (и следовательно символ Лежандра при простом  $n$ ).

1. Если  $a = 0$ , то вернуть 0.
2. Если  $a = 1$ , то вернуть 1.
3. Записать  $a$  как  $a = 2^e a_1$ , где  $a_1$  нечетно.
4. Если  $e$  четно, то  $s := 1$ . В противном случае

$$s := 1, \text{ если } n \equiv 1 \text{ или } 7 \pmod{8}; \\ s := -1, \text{ если } n \equiv 3 \text{ или } 5 \pmod{8}.$$

5. Если  $n \equiv 3 \pmod{4}$  и  $a_1 \equiv 3 \pmod{4}$ , то  $s := -s$ .
6.  $n_1 := n \pmod{a_1}$ .
7. Если  $a_1 = 1$ , то вернуть  $s$ ; в противном случае вернуть  $s \cdot \text{JACOBI}(n_1, a_1)$ .

**Пример.** Определить с помощью символа Лежандра, имеет ли решение сравнение  $x^2 \equiv a \pmod{p}$ . Вычислять символ Лежандра  $\left( \frac{a}{p} \right)$ , рассматривая его как символ Якоби.

1.  $x^2 \equiv 506 \pmod{1103}$ . Решение. Символ Якоби

$$\left( \frac{506}{1103} \right) = \left( \frac{2 \cdot 253}{1103} \right) =_{(2)} \left( \frac{2}{1103} \right) \cdot \left( \frac{253}{1103} \right) =_{(7,8)}$$

$$(-1)^{\frac{1103^2-1}{8}} \cdot \left( \frac{1103}{253} \right) \cdot (-1)^{\frac{(253-1)(1103-1)}{4}} = 1 \cdot 1 \cdot \left( \frac{1103}{253} \right) = [1103 \equiv 91 \pmod{253}] =_{(4)}$$

$$\left( \frac{91}{253} \right) =_{(8)} \left( \frac{253}{91} \right) \cdot (-1)^{\frac{(91-1)(253-1)}{4}} = \left( \frac{253}{91} \right) = [253 \equiv -20 \pmod{91}] =_{(4)}$$

$$\left( \frac{-20}{91} \right) = \left( \frac{-1}{91} \right) \cdot \left( \frac{20}{91} \right) = (-1)^{\frac{91-1}{2}} \cdot \left( \frac{2^2}{91} \right) \cdot \left( \frac{5}{91} \right) = (-1) \cdot 1 \cdot \left( \frac{91}{5} \right) \cdot (-1)^{\frac{(5-1)(91-1)}{4}} =$$

$$-\left(\frac{91}{5}\right) = [91 \equiv -1 \pmod{5}] \stackrel{(4)}{=} -\left(\frac{1}{5}\right) = -1.$$

*Ответ.* Сравнение не имеет решений.

2.  $x^2 \equiv 903 \pmod{2111}$ . *Решение.* Символ Якоби

$$\begin{aligned} \left(\frac{506}{1103}\right) &\stackrel{(8)}{=} \left(\frac{2111}{903}\right) \cdot (-1)^{\frac{(903-1)(2111-1)}{4}} = -\left(\frac{2111}{903}\right) = \\ &[211 \equiv 305 \pmod{903}] \stackrel{(4)}{=} \left(\frac{305}{903}\right) \stackrel{(8)}{=} \left(\frac{903}{305}\right) \cdot (-1)^{\frac{(305-1)(903-1)}{4}} = \end{aligned}$$

$$-\left(\frac{903}{305}\right) = [903 \equiv -12 \pmod{305}] \stackrel{(4)}{=} -\left(\frac{-12}{305}\right) = -\left(\frac{-1}{305}\right) \cdot \left(\frac{12}{305}\right) \stackrel{(6)}{=}$$

$$-(-1)^{\frac{305-1}{2}} \cdot \left(\frac{2^2 \cdot 3}{305}\right) \stackrel{(2)}{=} -\left(\frac{2^2}{305}\right) \cdot \left(\frac{3}{305}\right) = -\left(\frac{3}{305}\right) \stackrel{(8)}{=}$$

$$-\left(\frac{305}{3}\right) \cdot (-1)^{\frac{(305-1)(903-1)}{4}} = -\left(\frac{305}{3}\right) = [305 \equiv 3 \pmod{3}] \stackrel{(4)}{=} -\left(\frac{2}{3}\right) =$$

$$-(-1)^{\frac{3^2-1}{8}} = 1. \text{ Ответ. Сравнение имеет два решения.}$$

**Задача 20.** Полиномы  $f(x), g(x) \in \mathbb{Z}_5[x]$ . Найти их наибольший делитель  $d(x) = \text{нод}(f(x), g(x))$  и те полиномы  $u(x), v(x) \in \mathbb{Z}_5[x]$ , для которых  $d(x) = f(x)u(x) + g(x)v(x)$ .

**20.1.**  $x^8 + 2x^4 + 1, x^5 + 4x^3 + x^2 + 3x + 3$ .

**20.2.**  $x^8 + 2x^7 + 2x^6 + 2x^4 + x^3 + x^2 + x + 4, x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$ .

**20.3.**  $x^8 + 2x^7 + 4x^6 + 2x^5 + 4x^3 + x + 3x^4 + x^2 + 1, x^5 + x^4 + 2x^2 + 3x^3 + 4x + 2$ .

**20.4.**  $x^8 + 4x^7 + 4x^6 + 3x^5 + 4x^3 + 3x + 3x^4 + x^2 + 1, x^5 + 2x^4 + 3x^2 + 3x^3 + 4x + 2$ .

**20.5.**  $x^8 + 4x^7 + x^6 + 2x^5 + 3x^4 + 2x^2 + 4x + 4, x^5 + 2x^4 + 3x^2 + x + 4$ .

**20.6.**  $x^8 + x^7 + 4x^6 + 2x^5 + 3x^4 + x^3 + x^2 + 2x + 1, x^5 + 3x^4 + 4x^2 + 4x^3 + x + 3$ .

**20.7.**  $x^8 + x^7 + x^6 + 3x^5 + x + 3x^4 + 2x^2 + 4, x^5 + 3x^4 + 4x^2 + 2x + 4$ .

**20.8.**  $x^8 + 3x^7 + 2x^6 + 2x^4 + 4x^3 + x^2 + 2x + 4, x^5 + 4x^4 + 2x^3 + 1$ .

**20.9.**  $x^8 + 3x^7 + 4x^6 + 3x^5 + 3x^4 + x^3 + x^2 + 4x + 1, x^5 + 4x^4 + 3x^3 + x + 2$ .

**20.10.**  $4x^8 + 3x^4 + 4, 2x^5 + 3x^3 + 2x^2 + x + 1$ .

**20.11.**  $4x^8 + 2x^6 + x^4 + 3x^2 + 4, 2x^5 + 2x^2 + x^3 + 4x + 4$ .

**20.12.**  $4x^8 + 4x^7 + x^6 + 3x^5 + 2x^4 + 4x^3 + 4x^2 + 3x + 4, 2x^5 + x^4 + 3x^3 + 2x + 1$ .

**20.13.**  $4x^8 + 4x^7 + 4x^6 + 2x^5 + 2x^4 + 3x^2 + 4x + 1, 2x^5 + x^4 + 3x^2 + 4x + 3$ .

**20.14.**  $4x^8 + 3x^7 + 3x^6 + 3x^4 + 4x^3 + 4x^2 + 2x + 1, 2x^5 + 2x^4 + 4x^3 + 4x^2 + 4x + 2$ .

**20.15.**  $4x^8 + 3x^7 + 6x^6 + 3x^5 + 2x^4 + x^3 + 4x^2 + 4x + 4, 2x^5 + 2x^4 + 4x^2 + x^3 + x + 4$ .

**20.16.**  $4x^8 + 2x^7 + 3x^6 + 3x^4 + x^3 + 4x^2 + 3x + 1, 2x^5 + 3x^4 + 4x^3 + 2$ .

**20.17.**  $4x^8 + 2x^7 + x^6 + 2x^5 + 2x^4 + 4x^3 + 4x^2 + x + 4, 2x^5 + 3x^4 + x^3 + 2x + 4$ .

**20.18.**  $4x^8 + x^7 + x^6 + 2x^5 + x^3 + 2x^4 + 4x^2 + 2x + 4, 2x^5 + 4x^4 + x^2 + 3x^3 + 1$ .

**20.19.**  $4x^8 + x^7 + 4x^6 + 3x^5 + 2x^4 + 3x^2 + x + 1, 2x^5 + 4x^4 + x^2 + 2x + 3$ .

**20.20.**  $4x^8 + 2x^6 + x^4 + 3x^2 + 4, 3x^5 + 3x^2 + 4x^3 + x + 1$ .

- 20.21.**  $4x^8 + 3x^4 + 4, 2x^5 + x^3 + 2x^2 + 4x + 4.$
- 20.22.**  $4x^8 + x^7 + 4x^6 + 3x^5 + 2x^4 + x + 1, 3x^5 + x^4 + 4x^2 + 3x + 2.$
- 20.23.**  $4x^8 + x^7 + x^6 + 2x^5 + x^3 + 2x^4 + 4x^2 + 2x + 4, 3x^5 + x^4 + 4, 2x^3 + 4.$
- 20.24.**  $4x^8 + 2x^7 + x^6 + 2x^5 + 2x^4 + 4x^3 + 4x^2 + x + 4, 3x^5 + 2x^4 + 4x^3 + 3x + 1.$
- 20.25.**  $4x^8 + 2x^7 + 3x^6 + 3x^4 + x^3 + 4x^2 + 3x + 1, 3x^5 + 2x^4 + 4x + 2.$
- 20.26.**  $4x^8 + 3x^7 + x^6 + 3x^5 + 3x^4 + 2x^4 + x^3 + 4x^2 + 4x + 4, 3x^5 + 3x^4 + 6x^2 + 4x^3 + 3x + 1.$
- 20.27.**  $4x^8 + 3x^7 + 3x^6 + 4x^3 + 4x^2 + 2x + 1, 3x^5 + 3x^4 + x^2 + x^3 + x + 3.$
- 20.28.**  $4x^8 + 4x^7 + 4x^6 + 2x^5 + 3x^2 + 4x + 1, 3x^5 + 4x^4 + 2x^2 + x + 2.$
- 20.29.**  $4x^8 + 4x^7 + x^6 + 3x^5 + 2x^4 + 4x^3 + 4x^2 + 3x + 4, 3x^5 + 4x^4 + 2x^2 + 2x^3 + 3x + 4.$
- 20.30.**  $x^8 + 2x^7 + 2x^6 + 2x^4 + x^3 + x^2 + 3x + 4, x^5 + 3x^3 + x^2 + 2x + 2.$

### *Алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$*

ВХОД. Ненулевые полиномы  $f(x), h(x) \in \mathbb{Z}_p[x]$ .

ВЫХОД. Наибольший общий делитель для  $f(x)$  и  $h(x)$ .

1. Пока  $h(x) \neq 0$  выполнять следующее:

$$r(x) := f(x) \pmod{h(x)}, f(x) := h(x), h(x) := r(x).$$

2. Если  $p > 2, a \neq 1$  есть старший коэффициент  $f(x)$ , то  $f(x) := f(x)/a \pmod{p}$ .

3. Вернуть  $f(x)$ .

### *Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$*

ВХОД. Ненулевые полиномы  $f(x), h(x) \in \mathbb{Z}_p[x]$ .

ВЫХОД.  $d(x) = \text{нод}(f(x), h(x))$  и два полинома  $u(x), v(x) \in \mathbb{Z}_p[x]$ , для которых  $d(x) = u(x)f(x) + v(x)h(x)$ .

1. Если  $h = 0$  то  $d := f, u := 1, v := 0$ , возвратить  $(d, u, v)$ .

2.  $u_2 := 1, u_1 := 0, v_1 := 0, v_2 := 1$ .

3. Пока  $h \neq 0$  выполнять следующее.

$$3.1. q := \lfloor f/h \rfloor, r := f - hq, u := u_2 - qu_1, v := v_2 - qv_1.$$

$$3.2. f := h, h := r, u_2 := u_1, u_1 := u, v_2 := v_1, v_1 := v.$$

4.  $d := f, u := u_2, v := v_2$ .

5. Если  $p > 2, a \neq 1$  есть старший коэффициент  $f(x)$ , то  $d := d \cdot a^{-1} \pmod{p}$ ,

$$u := u \cdot a^{-1} \pmod{p}, v := v \cdot a^{-1} \pmod{p}.$$

6. Вернуть  $(d, u, v)$ .

**Пример 1.** (Расширенный алгоритм Евклида для полиномов из  $\mathbb{Z}_5[x]$ ).

Пусть  $f(x) = 4x^8 + 3x^7 + 4x^6 + 2x^5 + 4x^4 + 2x^3 + 4x^2 + 3x + 4$ ,

$h(x) = 3x^7 + x^6 + 4x^4 + 3x^3 + x^2 + 4x + 4$  есть полиномы из  $\mathbb{Z}_5[x]$ . Найти

$d(x) = \text{нод}(f(x), h(x))$  и полиномы  $u(x), v(x) \in \mathbb{Z}_5[x]$ , для которых

$d(x) = u(x)f(x) + v(x)h(x)$ .

*Решение.*

#### **Исходное присваивание.**

$$f(x) = 4x^8 + 3x^7 + 4x^6 + 2x^5 + 4x^4 + 2x^3 + 4x^2 + 3x + 4,$$

$$h(x) = 3x^7 + x^6 + 4x^4 + 3x^3 + x^2 + 4x + 4,$$

$$u_2(x) := 1, u_1(x) := 0, v_2(x) := 0, v_1(x) := 1.$$

#### **Итерация 1.**

$$q(x) := \lfloor f(x)/h(x) \rfloor = \lfloor (4x^8 + 3x^7 + 4x^6 + 2x^5 + 4x^4 + 2x^3 + 4x^2 + 3x + 4) / (3x^7 + x^6 + 4x^4 + 3x^3 + x^2 + 4x + 4) \rfloor = 1$$

$$(3x^7+x^6+4x^4+3x^3+x^2+4x+4) \rfloor = 3x,$$

$$\begin{array}{r} -\frac{4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4}{4x^8+3x^7+0x^6+2x^5+4x^4+3x^3+2x^2+2x} \\ \hline 4x^6+0x^5+0x^4+4x^3+2x^2+1x+4 \end{array}$$

$$r(x) := f(x) - h(x)q(x) = (4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4) - (3x^7+x^6+4x^4+3x^3+x^2+4x+4) \cdot (3x) = 4x^6+4x^3+2x^2+x+4,$$

$$u(x) := u_2(x) - q(x)u_1(x) = 1 - (3x) \cdot (0) = 1,$$

$$v(x) := v_2(x) - q(x)v_1(x) = 0 - (3x) \cdot (1) = 2x,$$

$$f(x) := h(x) = 3x^7+x^6+4x^4+3x^3+x^2+4x+4,$$

$$h(x) := r(x) = 4x^6+4x^3+2x^2+x+4,$$

$$u_2(x) := u_1(x) = 0, u_1(x) := u(x) = 1,$$

$$v_2(x) := v_1(x) = 1, v_1(x) := v(x) = 2x.$$

### Итерация 2.

$$q(x) := \lfloor f(x)/h(x) \rfloor = \lfloor (3x^7+x^6+4x^4+3x^3+x^2+4x+4)/(4x^6+4x^3+2x^2+x+4) \rfloor = 2x+4,$$

$$\begin{array}{r} -\frac{3x^7+1x^6+0x^5+4x^4+3x^3+1x^2+4x+4}{3x^7+0x^6+0x^5+3x^4+4x^3+2x^2+3x+0} \\ \hline 4x^6+4x^3+2x^2+1x+4 \\ -\frac{1x^6+0x^5+1x^4+4x^3+4x^2+1x+4}{1x^6+0x^5+0x^4+1x^3+3x^2+4x+1} \\ \hline 1x^4+3x^3+1x^2+2x+3 \end{array}$$

$$r(x) := f(x) - h(x)q(x) =$$

$$(3x^7+x^6+4x^4+3x^3+x^2+4x+4) - (4x^6+4x^3+2x^2+x+4) \cdot (2x+4) = x^4+3x^3+x^2+2x+3,$$

$$u(x) := u_2(x) - q(x)u_1(x) = 0 - (2x+4) \cdot (1) = 3x+1, v(x) := v_2(x) - q(x)v_1(x) = 1 - (2x+4) \cdot (2x) = x^2+2x+1,$$

$$f(x) := h(x) = 4x^6+4x^3+2x^2+x+4, h(x) := r(x) = x^4+3x^3+x^2+2x+3,$$

$$u_2(x) := u_1(x) = 1, u_1(x) := u(x) = 3x+1,$$

$$v_2(x) := v_1(x) = 2x, v_1(x) := v(x) = x^2+2x+1.$$

### Итерация 3.

$$q(x) := \lfloor f(x)/h(x) \rfloor = \lfloor (4x^6+4x^3+2x^2+x+4)/(x^4+3x^3+x^2+2x+3) \rfloor = 4x^2+3x+2,$$

$$\begin{array}{r} -\frac{4x^6+0x^5+0x^4+4x^3+2x^2+1x+4}{4x^6+2x^5+4x^4+3x^3+2x^2} \\ \hline 1x^4+3x^3+x^2+2x+3 \\ -\frac{3x^5+1x^4+1x^3+0x^2+1x+4}{3x^5+4x^4+3x^3+1x^2+4x} \\ \hline 2x^4+3x^3+4x^2+2x+4 \\ -\frac{2x^4+1x^3+2x^2+4x+1}{2x^3+2x^2+3x+3} \end{array}$$

$$r(x) := f(x) - h(x)q(x) =$$

$$(4x^6+4x^3+2x^2+x+4) - (x^4+3x^3+x^2+2x+3) \cdot (4x^2+3x+2) = 2x^3+2x^2+3x+3,$$

$$u(x) := u_2(x) - q(x)u_1(x) = 1 - (4x^2+3x+2) \cdot (3x+1) = 3x^3+2x^2+x+4,$$

$$v(x) := v_2(x) - q(x)v_1(x) = 2x - (4x^2 + 3x + 2) \cdot (2x) = x^4 + 4x^3 + 3x^2 + 3,$$

$$f(x) := h(x) = x^4 + 3x^3 + x^2 + 2x + 3, h(x) := r(x) = 2x^3 + 2x^2 + 3x + 3,$$

$$u_2(x) := u_1(x) = 3x + 1, u_1(x) := u(x) = 3x^3 + 2x^2 + x + 4,$$

$$v_2(x) := v_1(x) = x^2 + 2x + 1, v_1(x) := v(x) = x^4 + 4x^3 + 3x^2 + 3.$$

#### Итерация 4.

$$q(x) := \lfloor f(x)/h(x) \rfloor = \lfloor (x^4 + 3x^3 + x^2 + 2x + 3)/(2x^3 + 2x^2 + 3x + 3) \rfloor = 3x + 1,$$

$$\begin{array}{r} x^4 + 3x^3 + 1x^2 + 2x + 3 \\ \hline x^4 + 1x^3 + 4x^2 + 4x \\ \hline 2x^3 + 2x^2 + 3x + 3 \\ \hline 2x^3 + 2x^2 + 3x + 3 \\ \hline 0 \end{array}$$

$$r(x) := (x^4 + 3x^3 + x^2 + 2x + 3) - (2x^3 + 2x^2 + 3x + 3) \cdot (3x + 1) = 0,$$

$$u(x) := u_2(x) - q(x)u_1(x) = (3x + 1) - (3x + 1) \cdot (3x^3 + 2x^2 + x + 4) = x^4 + x^3 + 2,$$

$$v(x) := v_2(x) - q(x)v_1(x) =$$

$$(x^2 + 2x + 1) - (3x + 1) \cdot (x^4 + 4x^3 + 3x^2 + 3) = 2x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 3,$$

$$f(x) := h(x) = 2x^3 + 2x^2 + 3x + 3, h(x) := r(x) = 0,$$

$$u_2(x) := u_1(x) = 3x^3 + 2x^2 + x + 4, u_1(x) := u(x) = x^4 + x^3 + 2,$$

$$v_2(x) := v_1(x) = x^4 + 4x^3 + 3x^2 + 3,$$

$$v_1(x) := v(x) = 2x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 3.$$

Так как  $h(x) = 0$ , то  $d(x) := f(x) = 2x^3 + 2x^2 + 3x + 3$ ,

$$u(x) := u_2(x) = 3x^3 + 2x^2 + x + 4, v(x) := v_2(x) = x^4 + 4x^3 + 3x^2 + 3.$$

Так как  $p = 5 > 2$  и  $d(x)$  имеет старший коэффициент  $a = 2$ , то

$$d(x) := d(x) \cdot 2^{-1} \pmod{p} = d(x) \cdot 3 \pmod{p} = x^3 + x^2 + 4x + 4,$$

$$u(x) := u(x) \cdot 2^{-1} \pmod{p} = u(x) \cdot 3 \pmod{p} = 4x^3 + x^2 + 3x + 2,$$

$$v(x) := v(x) \cdot 2^{-1} \pmod{p} = v(x) \cdot 3 \pmod{p} = 3x^4 + 2x^3 + 4x^2 + 4.$$

*Ответ.*  $d(x) = x^3 + x^2 + 4x + 4$ ,  $u(x) = 4x^3 + x^2 + 3x + 2$ ,  $v(x) = 3x^4 + 2x^3 + 4x^2 + 4$ .

**Пример 2.** (Расширенный алгоритм Евклида для полиномов из  $\mathbb{Z}_2[x]$ ).

Пусть  $f(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$ ,  $h(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$  есть полиномы из  $\mathbb{Z}_2[x]$ . Найти  $d(x) = \text{нод}(f(x), h(x))$  и полиномы  $u(x), v(x) \in \mathbb{Z}_2[x]$ , для которых  $d(x) = u(x)f(x) + v(x)h(x)$ .

*Решение.*

**Исходное присваивание.**

$$u_2(x) := 1, u_1(x) := 0, v_2(x) := 0, v_1(x) := 1.$$

#### Итерация 1.

$$q(x) := \lfloor f(x)/h(x) \rfloor = x + 1,$$

$$\begin{array}{r} 1x^{10} + 1x^9 + 1x^8 + 0x^7 + 1x^6 + 1x^5 + 1x^4 + 0x^3 + 0x^2 + 0x + 1 \\ \hline 1x^{10} + 0x^9 + 0x^8 + 1x^7 + 1x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 1x \\ \hline 1x^9 + 1x^8 + 1x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x + 1 \\ \hline 1x^9 + 0x^8 + 0x^7 + 1x^6 + 1x^5 + 0x^4 + 1x^3 + 1x^2 + 0x + 1 \\ \hline 1x^8 + 1x^7 + 1x^6 + 0x^5 + 0x^4 + 0x^3 + 1x^2 + 1x + 0 \end{array}$$

$$\begin{aligned}
r(x) &:= f(x) - h(x)q(x) = \\
&(x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + 1) - (x^9 + x^6 + x^5 + x^3 + x^2 + 1) \cdot (x+1) = \\
&x^8 + x^7 + x^6 + x^2 + x, \\
u(x) &:= u_2(x) - q(x)u_1(x) = 1 - (x+1) \cdot (0) = 1, \\
v(x) &:= v_2(x) - q(x)v_1(x) = 0 - (x+1) \cdot (1) = x+1, \\
f(x) &:= h(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1, h(x) := r(x) = x^8 + x^7 + x^6 + x^2 + x, \\
u_2(x) &:= u_1(x) = 0, u_1(x) := u(x) = 1, \\
v_2(x) &:= v_1(x) = 1, v_1(x) := v(x) = x+1.
\end{aligned}$$

### Итерация 2.

$$\begin{aligned}
q(x) &:= \lfloor f(x)/h(x) \rfloor = x+1, \\
&- \frac{1x^9+0x^8+0x^7+1x^6+1x^5+0x^4+1x^3+1x^2+0x+1}{1x^9+1x^8+1x^7+0x^6+0x^5+0x^4+1x^3+1x^2+0x+0} \left| \begin{array}{c} 1x^8+1x^7+1x^6+1x^2+1x \\ 1x+1 \end{array} \right. \\
&- \frac{1x^8+1x^7+1x^6+1x^5+0x^4+0x^3+0x^2+0x+1}{1x^8+1x^7+1x^6+0x^5+0x^4+0x^3+1x^2+1x+0} \\
&\quad \frac{1x^5+0x^4+0x^3+1x^2+1x+1}{1x^5+0x^4+0x^3+1x^2+1x+1}
\end{aligned}$$

$$\begin{aligned}
r(x) &:= f(x) - h(x)q(x) = \\
&(x^9 + x^6 + x^5 + x^3 + x^2 + 1) - (x^8 + x^7 + x^6 + x^2 + x) \cdot (x+1) = x^5 + x^2 + x + 1, \\
u(x) &:= u_2(x) - q(x)u_1(x) = 0 - (x+1) \cdot (1) = x+1, \\
v(x) &:= v_2(x) - q(x)v_1(x) = 1 - (x+1) \cdot (x+1) = x, \\
f(x) &:= h(x) = x^8 + x^7 + x^6 + x^2 + 1, h(x) := r(x) = x^5 + x^2 + x + 1, \\
u_2(x) &:= u_1(x) = 1, u_1(x) := u(x) = x+1, \\
v_2(x) &:= v_1(x) = x+1, v_1(x) := v(x) = x^2.
\end{aligned}$$

### Итерация 3.

$$\begin{aligned}
q(x) &:= \lfloor f(x)/h(x) \rfloor = x^3 + x^2 + x + 1, \\
&- \frac{1x^8+1x^7+1x^6+0x^5+0x^4+0x^3+1x^2+1x+0}{1x^8+0x^7+0x^6+1x^5+1x^4+1x^3+0x^2+0x+0} \left| \begin{array}{c} 1x^5+1x^2+1x+1 \\ 1x^3+1x^2+1x+1 \end{array} \right. \\
&- \frac{1x^7+1x^6+1x^5+1x^4+1x^3+1x^2+1x+0}{1x^7+0x^6+0x^5+1x^4+1x^3+1x^2+0x+0} \\
&\quad \frac{1x^6+1x^5+0x^4+0x^3+0x^2+1x+0}{1x^6+0x^5+0x^4+1x^3+1x^2+1x+0} \\
&\quad - \frac{1x^5+0x^4+1x^3+1x^2+0x+0}{1x^5+0x^4+0x^3+1x^2+1x+1} \\
&\quad \frac{1x^3+0x^2+1x+1}{1x^3+0x^2+1x+1}
\end{aligned}$$

$$\begin{aligned}
r(x) &:= f(x) - h(x)q(x) = \\
&(x^8 + x^7 + x^6 + x^2 + 1) - (x^5 + x^2 + x + 1) \cdot (x^3 + x^2 + x + 1) = x^3 + x + 1, \\
u(x) &:= u_2(x) - q(x)u_1(x) = 1 - (x^3 + x^2 + x + 1) \cdot (x+1)x, \\
v(x) &:= v_2(x) - q(x)v_1(x) = \\
&(x+1) - (x^3 + x^2 + x + 1) \cdot (x^2) = x^5 + x^4 + x^3 + x^2 + x + 1, \\
f(x) &:= h(x) = x^5 + x^2 + x + 1, h(x) := r(x) = x^3 + x + 1, \\
u_2(x) &:= u_1(x) = x+1, u_1(x) := u(x) = x^4,
\end{aligned}$$

$$v_2(x) := v_1(x) = x^2, \quad v_1(x) := v(x) = x^5 + x^4 + x^3 + x^2 + x + 1.$$

**Итерация 4.**

$$q(x) := \lfloor f(x)/h(x) \rfloor = x^2 + 1,$$

$$\begin{array}{r} 1x^5+0x^4+0x^3+1x^2+1x+1 \\ - 1x^5+0x^4+1x^3+1x^2+0x+0 \\ \hline - 1x^3+0x^2+1x+1 \\ - 1x^3+0x^2+1x+1 \\ \hline 0 \end{array}$$

$$r(x) := f(x) - h(x)q(x) = (x^5 + x^4 + x^3 + x^2 + x + 1) - (x^3 + x^2 + x + 1) \cdot (x^2 + 1) = 0,$$

$$u(x) := u_2(x) - q(x)u_1(x) = x + 1 - (x^2 + 1) \cdot (x^4) = x^6 + x^4 + x + 1,$$

$$v(x) := v_2(x) - q(x)v_1(x) =$$

$$x^2 - (x^2 + 1) \cdot (x^5 + x^4 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^2 + x + 1,$$

$$f(x) := h(x) = x^3 + x + 1, \quad h(x) := r(x) = 0,$$

$$u_2(x) := u_1(x) = x^4, \quad u_1(x) := u(x) = x^6 + x^4 + x + 1,$$

$$v_2(x) := v_1(x) = x^5 + x^4 + x^3 + x^2 + x + 1, \quad v_1(x) := v(x) = x^7 + x^6 + x^2 + x + 1.$$

Ответ.  $d(x) = \text{нод}(f(x), h(x)) = x^3 + x + 1,$

$$u(x) = x^4, \quad v(x) = x^5 + x^4 + x^3 + x^2 + x + 1.$$

**Задача 21.** Полином  $f(x) \in \mathbb{Z}_p[x]$  степени  $m$  над простым полем  $\mathbb{Z}_p$ ,  $p=5$ ,  $m=2$ , задан как определяемое вариантом натуральное число  $a$ . Например, для  $a = 108_{10} = 413_5$  полином  $f(x) = 4 \cdot x^2 + 1 \cdot x + 3 = 4x^2 + x + 3$ .

- a) по заданному числу  $a$  найти полином  $f(x) \in \mathbb{Z}_p[x]$ .
  - b) построить таблицу значений для  $f(x)$  и проверить, будет ли полином  $f(x)$  над полем  $\mathbb{Z}_p$  неприводим.
  - c) написать все элементы поля  $GF(p^m) = \mathbb{Z}_p[x]/(f(x))$  из  $q = p^m$  из  $p^m$  остатков от деления полиномов из  $\mathbb{Z}_p[x]$  на модуль  $f(x)$ .
  - d) для поля  $GF(p^m) = \mathbb{Z}_p[x]/(f(x))$  из  $q = p^m$  остатков от деления полиномов из  $\mathbb{Z}_p[x]$  на  $f(x)$  построить таблицы для сложения и умножения элементов  $a_1x + a_0$ ,  $a_1 = 3$ ,  $a_0 \in \mathbb{Z}_5$ , на все элементы поля  $GF(p^m)$ .
  - e) для каждого элемента  $a_1x + a_0$ ,  $a_1 = 3$ ,  $a_0 \in \mathbb{Z}_5$ , указать обратный (по умножению) элемент.
- 21.1.** 27. **21.2.** 28. **21.3.** 31. **21.4.** 32. **21.5.** 38.  
**21.6.** 39. **21.7.** 43. **21.8.** 44. **21.9.** 46. **21.10.** 47.  
**21.11.** 51. **21.12.** 54. **21.13.** 56. **21.14.** 58. **21.15.** 62.  
**21.16.** 64. **21.17.** 67. **21.18.** 69. **21.19.** 71. **21.20.** 73.  
**21.21.** 76. **21.22.** 79. **21.23.** 82. **21.24.** 84. **21.25.** 86.  
**21.26.** 88. **21.27.** 91. **21.28.** 93. **21.29.** 97. **21.30.** 99.

### **Мультипликативный обратный элемент в $GF(p^m)$**

**ВХОД.** Ненулевой полином  $g(x) \in GF(p^m)$ . (Элементы поля  $GF(p^m)$  представляются как элементы в  $\mathbb{Z}_p[x]/(f(x))$ , где  $f(x) \in \mathbb{Z}_p[x]$  есть неприводимый полином степени  $m$  над  $\mathbb{Z}_p$ ).

**ВЫХОД.**  $g(x)^{-1} \in GF(p^m)$ .

1. С помощью расширенного алгоритма Евклида для полиномов найти два полинома  $u(x)$  и  $v(x) \in \mathbb{Z}_p[x]$ , для которых  $g(x)u(x) + f(x)v(x) = 1$ .

2. Вернуть  $u(x)$ .

### **Модулярная степень в $GF(p^m)$**

**ВХОД.**  $g(x) \in GF(p^m)$  и целое  $0 \leq k < p^m - 1$  с бинарным представлением  $k = \sum_{i=0}^t k_i 2^i$ . (Поле  $GF(p^m)$  есть  $\mathbb{Z}_p[x]/(f(x))$ , где  $f(x) \in \mathbb{Z}_p[x]$  есть неприводимый полином степени  $m$  над  $\mathbb{Z}_p$ ).

**ВЫХОД.**  $g(x)^k \pmod{f(x)}$ .

1.  $u(x) := 1$ . Если  $k=0$ , то вернуть  $u(x)$ .

2.  $G(x) := g(x)$ .

3. Если  $k_0 = 1$ , то  $u(x) := G(x)$ .

4. Для  $i$  от 1 до  $t$  выполнить следующее:

4.1.  $G(x) := G(x)^2 \pmod{f(x)}$ .

4.2. Если  $k_i = 1$ , то  $u(x) := G(x) \cdot u(x) \pmod{f(x)}$ .

5. Вернуть  $u(x)$ .

**Утверждение.** Пусть  $p$  есть простое число и пусть  $k$  есть положительное целое число.

1. Произведение всех нормированных неприводимых полиномов в  $\mathbb{Z}_p[x]$ , степень которых делит  $k$ , равно  $x^{p^k} - x$ .

2. Пусть  $f(x)$  есть полином степени  $m$  из  $\mathbb{Z}_p[x]$ . Тогда  $f(x)$  неприводим над  $\mathbb{Z}_p$ , если и только если  $\text{нод}(f(x), x^{p^k} - x) = 1$  для каждого  $i$ ,  $1 \leq i \leq \lfloor m/2 \rfloor$ .

### **Тестирование полинома из $\mathbb{Z}_p[x]$ на неприводимость**

**ВХОД.** Простое число  $p$  и нормированный полином  $f(x)$  степени  $m$  из  $\mathbb{Z}_p[x]$ .

**ВЫХОД.** Ответ на вопрос: "Является ли полином  $f(x)$  неприводим над  $\mathbb{Z}_p$ ?"

1.  $u(x) := x$ .

2. Для  $i$  от 1 до  $\lfloor m/2 \rfloor$  выполнить следующее.

2.1.  $u(x) := u(x)^p \pmod{f(x)}$ .

2.2.  $d(x) := \text{нод}(f(x), u(x) - x)$ .

2.3. Если  $d(x) \neq 1$ , то вернуть "приводимый".

3. Вернуть "неприводимый".

### **Порождение случайного неприводимого полинома из $\mathbb{Z}_p[x]$**

**ВХОД.** Просто число  $p$  и положительное целое  $m$ .

**ВЫХОД.** Неприводимый полином  $f(x)$  степени  $m$  в  $\mathbb{Z}_p[x]$ .

1. Случайно выбираем целые  $a_0, a_1, \dots, a_{m-1}$  между 0 и  $p-1$  с  $a_0 \neq 0$ . Пусть  $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_2x^2 + a_1x + a_0$ .

2. Тестируем полином  $f(x)$  на неприводимость. Если полином  $f(x)$  приводим над  $\mathbb{Z}_p$ , перейти к пункту 1.

3. Вернуть  $f(x)$ .

#### **Тестирование неприводимого полинома на примитивность**

**ВХОД.** Простое число  $p$ ; целое  $m \geq 1$ ; различные простые делители  $r_1, r_2, \dots, r_t$  числа  $p^m - 1$ ; нормированный неприводимый полином  $f(x)$  степени  $m$  в  $\mathbb{Z}_p[x]$ .

**ВЫХОД.** Ответ на вопрос: "Примитивен ли полином  $f(x)$ ?"

1. Для  $i$  от 1 до  $t$  выполнить следующее.

$$1.1. l(x) := x^{(p^m-1)/r_i} \pmod{f(x)}$$

1.2. Если  $l(x) = 1$ , то вернуть "Непримитивный".

2. Вернуть "Примитивный".

#### **Порождение случайного нормированного примитивного полинома из $\mathbb{Z}_p[x]$**

**ВХОД.** Простое число  $p$ ; целое  $m \geq 1$ ; различные простые делители  $r_1, r_2, \dots, r_t$  числа  $p^m - 1$ .

**ВЫХОД.** Нормированный примитивный полином  $f(x)$  степени  $m$  в  $\mathbb{Z}_p[x]$ .

1. Генерируем случайный нормированный неприводимый полином  $f(x)$  степени  $m$  в  $\mathbb{Z}_p[x]$ .

2. Тестируем полином  $f(x)$  на примитивность. Если полином  $f(x)$  не примитивен над  $\mathbb{Z}_p$ , перейти к 1.

3. Вернуть  $f(x)$ .

#### **Вычисление порядка элемента конечной мультипликативной группы (алгоритм Гаусса)**

**ВХОД.** Мультипликативная конечная группа  $G$  порядка  $n$ , элемент  $a \in G$ , факторизация  $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ .

**ВЫХОД.** Порядок  $t$  элемента  $a$ .

1.  $t := n$ .

2. Для  $i$  от 1 до  $k$  выполнить следующее.

$$2.1. t := t / p_i^{e_i}.$$

$$2.2. a_1 := a^{t/p_i}.$$

2.3. Пока  $a_1 \neq 1$ , выполнить:  $a_1 := a_1^{p_i}$ ,  $t := t \cdot p_i$ .

3. Вернуть  $t$ .

#### **Вычисление генератора конечной мультипликативной**

### циклической группы (алгоритм Гаусса)

**ВХОД.** Циклическая конечная группа  $G$  порядка  $n$ , факторизация  $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ .

**ВЫХОД.** Генератор  $a$  для  $G$ .

1. Выбрать случайный элемент  $a$  в  $G$
2. Для  $i$  от 1 до  $k$  выполнить следующее
  - 2.1.  $b := a^{n/p_i}$ .
  - 2.2. Если  $b = 1$ , то перейти к пункту 1.
3. Вернуть  $a$ .

**Пример.** Задан полином  $f(x) \in \mathbb{Z}_p[x]$  степени  $m$  над простым полем  $\mathbb{Z}_p$ ,  $p=5$ ,  $m=2$ . Полином задан как натуральное число  $a$ . Если, например,  $a = 108_{10} = 413_5$ , то полином  $f(x) = 4 \cdot x^2 + 1 \cdot x + 3 = 4x^2 + x + 3$ .

- a) найти полином  $f(x) \in \mathbb{Z}_p[x]$ .
- b) построить таблицу значений для  $f(x)$  и проверить, будет ли полином  $f(x)$  над полем  $\mathbb{Z}_p$  неприводим.
- c) написать все элементы поля  $GF(p^m) = \mathbb{Z}_p[x]/(f(x))$  из  $q = p^m$  остатков классов при делении полиномов из  $\mathbb{Z}_p[x]$  на  $f(x)$  с операциями сложения и умножения полиномов по модулю  $f(x)$ .
- d) для поля  $GF(p^m) = \mathbb{Z}_p[x]/(f(x))$  построить таблицы для сложения и умножения элементов  $a_1x + a_0$ ,  $a_1 = 3$ ,  $a_0 \in \mathbb{Z}_5$  на все элементы поля  $GF(p^m)$ .
- e) для каждого элемента  $a_1x + a_0$ ,  $a_1 = 3$ ,  $a_0 \in \mathbb{Z}_5$ , указать обратный (по умножению) элемент.

*Решение.*

- a)  $a = 112_{10} = 422_5$ . Полином  $f(x) = 4x^2 + 2x + 2$ .
- b)  $f(0) = 2$ ,  $f(1) = 4 \cdot 1^2 + 2 \cdot 1 + 2 = 8 = 3 \pmod{5}$ ,  
 $f(2) = 4 \cdot 2^2 + 2 \cdot 2 + 2 = 22 = 2 \pmod{5}$ ,  $f(3) = 4 \cdot 3^2 + 2 \cdot 3 + 3 = 44 = 4 \pmod{5}$ ,  
 $f(4) = 4 \cdot 4^2 + 2 \cdot 4 + 3 = 74 = 4 \pmod{5}$ .

Ниже следует таблица значений для  $f(x)$ .

$x$	0	1	2	3	4
$f(x)$	2	3	2	4	4

$f(x) \neq 0 \quad \forall x \in \mathbb{Z}_5$ . Полином  $f(x)$  над полем  $\mathbb{Z}_5$  неприводим.

c) множество  $F$  всех элементов поля  $GF(q)$  определяется множеством всех остатков при делении полиномов из  $\mathbb{Z}_p[x]$  на полином  $f(x) = 4x^2 + 2x + 2$ . Всякий такой остаток есть полином первого порядка  $a_1x + a_0$ , где  $a_1, a_0 \in \mathbb{Z}_5$ . Таких остатков 25. Будем задавать их вектором  $(a_1 a_0)$ , где  $a_1, a_0 \in \mathbb{Z}_5$ .

- |                                 |                                   |
|---------------------------------|-----------------------------------|
| 0. $(00) = 0 \cdot x + 0 = 0$ . | 13. $(23) = 2 \cdot x + 3$ .      |
| 1. $(01) = 0 \cdot x + 1 = 1$ . | 14. $(24) = 2 \cdot x + 4$ .      |
| 2. $(02) = 0 \cdot x + 2 = 2$ . | 15. $(30) = 3 \cdot x + 0 = 3x$ . |
| 3. $(03) = 0 \cdot x + 3 = 3$ . | 16. $(31) = 3 \cdot x + 1$ .      |

- |                                    |                                  |
|------------------------------------|----------------------------------|
| 4. $(04) = 0 \cdot x + 4 = 4.$     | 17. $(32) = 3 \cdot x + 2.$      |
| 5. $(10) = 1 \cdot x + 0 = x.$     | 18. $(33) = 3 \cdot x + 3.$      |
| 6. $(11) = 1 \cdot x + 1 = x + 1.$ | 19. $(34) = 3 \cdot x + 4.$      |
| 7. $(12) = 1 \cdot x + 2 = x + 2.$ | 20. $(40) = 4 \cdot x + 0 = 4x.$ |
| 8. $(13) = 1 \cdot x + 3 = x + 3.$ | 21. $(41) = 4 \cdot x + 1.$      |
| 9. $(14) = 1 \cdot x + 4 = x + 4.$ | 22. $(42) = 4 \cdot x + 2.$      |
| 10. $(20) = 2 \cdot x + 0 = 2x.$   | 23. $(43) = 4 \cdot x + 3.$      |
| 11. $(21) = 2 \cdot x + 1.$        | 24. $(44) = 4 \cdot x + 4.$      |
| 12. $(22) = 2 \cdot x + 2.$        |                                  |

d) табл.7.14 для сложения и умножения в поле  $\mathbb{Z}_5$ .

Таблица 7.14

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

d) табл.7.15 для сложения в поле  $GF(q)$ ,  $q = p^m = 5^2 = 25$ .

$$a+b = a_1a_0 + b_1b_0 = (a_1x+a_0) + (b_1x+b_0) = (a_1+b_1)x + (a_0+b_0).$$

Например,

$$(32) + (24) = (3x + 2) + (2x + 4) = 5x + 6 \pmod{5} = 0x + 1 = 01.$$

Подробные вычисления.

### (30)

- $(30) + (00) = (3x + 0) + (0x + 0) = 3x + 0 \pmod{5} = 3x + 0 = (30)$
- $(30) + (01) = (3x + 0) + (0x + 1) = 3x + 1 \pmod{5} = 3x + 1 = (31)$
- $(30) + (02) = (3x + 0) + (0x + 2) = 3x + 2 \pmod{5} = 3x + 2 = (32)$
- $(30) + (03) = (3x + 0) + (0x + 3) = 3x + 3 \pmod{5} = 3x + 3 = (33)$
- $(30) + (04) = (3x + 0) + (0x + 4) = 3x + 4 \pmod{5} = 3x + 4 = (34)$
- $(30) + (10) = (3x + 0) + (1x + 0) = 4x + 0 \pmod{5} = 4x + 0 = (40)$
- $(30) + (11) = (3x + 0) + (1x + 1) = 4x + 1 \pmod{5} = 4x + 1 = (41)$
- $(30) + (12) = (3x + 0) + (1x + 2) = 4x + 2 \pmod{5} = 4x + 2 = (42)$
- $(30) + (13) = (3x + 0) + (1x + 3) = 4x + 3 \pmod{5} = 4x + 3 = (43)$
- $(30) + (14) = (3x + 0) + (1x + 4) = 4x + 4 \pmod{5} = 4x + 4 = (44)$
- $(30) + (20) = (3x + 0) + (2x + 0) = 5x + 0 \pmod{5} = 0x + 0 = (00)$
- $(30) + (21) = (3x + 0) + (2x + 1) = 5x + 1 \pmod{5} = 0x + 1 = (01)$
- $(30) + (22) = (3x + 0) + (2x + 2) = 5x + 2 \pmod{5} = 0x + 2 = (02)$
- $(30) + (23) = (3x + 0) + (2x + 3) = 5x + 3 \pmod{5} = 0x + 3 = (03)$
- $(30) + (24) = (3x + 0) + (2x + 4) = 5x + 4 \pmod{5} = 0x + 4 = (04)$
- $(30) + (30) = (3x + 0) + (3x + 0) = 6x + 0 \pmod{5} = 1x + 0 = (10)$
- $(30) + (31) = (3x + 0) + (3x + 1) = 6x + 1 \pmod{5} = 1x + 1 = (11)$
- $(30) + (32) = (3x + 0) + (3x + 2) = 6x + 2 \pmod{5} = 1x + 2 = (12)$
- $(30) + (33) = (3x + 0) + (3x + 3) = 6x + 3 \pmod{5} = 1x + 3 = (13)$

$$\begin{aligned}
(30) + (34) &= (3x + 0) + (3x + 4) = 6x + 4 \pmod{5} = 1x + 4 = (14) \\
(30) + (40) &= (3x + 0) + (4x + 0) = 7x + 0 \pmod{5} = 2x + 0 = (20) \\
(30) + (41) &= (3x + 0) + (4x + 1) = 7x + 1 \pmod{5} = 2x + 1 = (21) \\
(30) + (42) &= (3x + 0) + (4x + 2) = 7x + 2 \pmod{5} = 2x + 2 = (22) \\
(30) + (43) &= (3x + 0) + (4x + 3) = 7x + 3 \pmod{5} = 2x + 3 = (23) \\
(30) + (44) &= (3x + 0) + (4x + 4) = 7x + 4 \pmod{5} = 2x + 4 = (24)
\end{aligned}$$

**(31)**

$$\begin{aligned}
(31) + (00) &= (3x + 1) + (0x + 0) = 3x + 1 \pmod{5} = 3x + 1 = (31) \\
(31) + (01) &= (3x + 1) + (0x + 1) = 3x + 2 \pmod{5} = 3x + 2 = (32) \\
(31) + (02) &= (3x + 1) + (0x + 2) = 3x + 3 \pmod{5} = 3x + 3 = (33) \\
(31) + (03) &= (3x + 1) + (0x + 3) = 3x + 4 \pmod{5} = 3x + 4 = (34) \\
(31) + (04) &= (3x + 1) + (0x + 4) = 3x + 5 \pmod{5} = 3x + 0 = (30) \\
(31) + (10) &= (3x + 1) + (1x + 0) = 4x + 1 \pmod{5} = 4x + 1 = (41) \\
(31) + (11) &= (3x + 1) + (1x + 1) = 4x + 2 \pmod{5} = 4x + 2 = (42) \\
(31) + (12) &= (3x + 1) + (1x + 2) = 4x + 3 \pmod{5} = 4x + 3 = (43) \\
(31) + (13) &= (3x + 1) + (1x + 3) = 4x + 4 \pmod{5} = 4x + 4 = (44) \\
(31) + (14) &= (3x + 1) + (1x + 4) = 4x + 5 \pmod{5} = 4x + 0 = (40) \\
(31) + (20) &= (3x + 1) + (2x + 0) = 5x + 1 \pmod{5} = 0x + 1 = (01) \\
(31) + (21) &= (3x + 1) + (2x + 1) = 5x + 2 \pmod{5} = 0x + 2 = (02) \\
(31) + (22) &= (3x + 1) + (2x + 2) = 5x + 3 \pmod{5} = 0x + 3 = (03) \\
(31) + (23) &= (3x + 1) + (2x + 3) = 5x + 4 \pmod{5} = 0x + 4 = (04) \\
(31) + (24) &= (3x + 1) + (2x + 4) = 5x + 5 \pmod{5} = 0x + 0 = (00) \\
(31) + (30) &= (3x + 1) + (3x + 0) = 6x + 1 \pmod{5} = 1x + 1 = (11) \\
(31) + (31) &= (3x + 1) + (3x + 1) = 6x + 2 \pmod{5} = 1x + 2 = (12) \\
(31) + (32) &= (3x + 1) + (3x + 2) = 6x + 3 \pmod{5} = 1x + 3 = (13) \\
(31) + (33) &= (3x + 1) + (3x + 3) = 6x + 4 \pmod{5} = 1x + 4 = (14) \\
(31) + (34) &= (3x + 1) + (3x + 4) = 6x + 5 \pmod{5} = 1x + 0 = (10) \\
(31) + (40) &= (3x + 1) + (4x + 0) = 7x + 1 \pmod{5} = 2x + 1 = (21) \\
(31) + (41) &= (3x + 1) + (4x + 1) = 7x + 2 \pmod{5} = 2x + 2 = (22) \\
(31) + (42) &= (3x + 1) + (4x + 2) = 7x + 3 \pmod{5} = 2x + 3 = (23) \\
(31) + (43) &= (3x + 1) + (4x + 3) = 7x + 4 \pmod{5} = 2x + 4 = (24) \\
(31) + (44) &= (3x + 1) + (4x + 4) = 7x + 5 \pmod{5} = 2x + 0 = (20)
\end{aligned}$$

**(32)**

$$\begin{aligned}
(32) + (00) &= (3x + 2) + (0x + 0) = 3x + 2 \pmod{5} = 3x + 2 = (32) \\
(32) + (01) &= (3x + 2) + (0x + 1) = 3x + 3 \pmod{5} = 3x + 3 = (33) \\
(32) + (02) &= (3x + 2) + (0x + 2) = 3x + 4 \pmod{5} = 3x + 4 = (34) \\
(32) + (03) &= (3x + 2) + (0x + 3) = 3x + 5 \pmod{5} = 3x + 0 = (30) \\
(32) + (04) &= (3x + 2) + (0x + 4) = 3x + 6 \pmod{5} = 3x + 1 = (31) \\
(32) + (10) &= (3x + 2) + (1x + 0) = 4x + 2 \pmod{5} = 4x + 2 = (42) \\
(32) + (00) &= (3x + 2) + (1x + 1) = 4x + 3 \pmod{5} = 4x + 3 = (43) \\
(32) + (12) &= (3x + 2) + (1x + 2) = 4x + 4 \pmod{5} = 4x + 4 = (44) \\
(32) + (13) &= (3x + 2) + (1x + 3) = 4x + 5 \pmod{5} = 4x + 0 = (40)
\end{aligned}$$

$$\begin{aligned}
(32) + (14) &= (3x + 2) + (1x + 4) = 4x + 6 \pmod{5} = 4x + 1 = (41) \\
(32) + (20) &= (3x + 2) + (2x + 0) = 5x + 2 \pmod{5} = 0x + 2 = (02) \\
(32) + (21) &= (3x + 2) + (2x + 1) = 5x + 3 \pmod{5} = 0x + 3 = (03) \\
(32) + (22) &= (3x + 2) + (2x + 2) = 5x + 4 \pmod{5} = 0x + 4 = (04) \\
(32) + (23) &= (3x + 2) + (2x + 3) = 5x + 5 \pmod{5} = 0x + 0 = (00) \\
(32) + (24) &= (3x + 2) + (2x + 4) = 5x + 6 \pmod{5} = 0x + 1 = (01) \\
(32) + (30) &= (3x + 2) + (3x + 0) = 6x + 2 \pmod{5} = 1x + 2 = (12) \\
(32) + (31) &= (3x + 2) + (3x + 1) = 6x + 3 \pmod{5} = 1x + 3 = (13) \\
(32) + (32) &= (3x + 2) + (3x + 2) = 6x + 4 \pmod{5} = 1x + 4 = (14) \\
(32) + (33) &= (3x + 2) + (3x + 3) = 6x + 5 \pmod{5} = 1x + 0 = (10) \\
(32) + (34) &= (3x + 2) + (3x + 4) = 6x + 6 \pmod{5} = 1x + 1 = (11) \\
(32) + (40) &= (3x + 2) + (4x + 0) = 7x + 2 \pmod{5} = 2x + 2 = (22) \\
(32) + (41) &= (3x + 2) + (4x + 1) = 7x + 3 \pmod{5} = 2x + 3 = (23) \\
(32) + (42) &= (3x + 2) + (4x + 2) = 7x + 4 \pmod{5} = 2x + 4 = (24) \\
(32) + (43) &= (3x + 2) + (4x + 3) = 7x + 5 \pmod{5} = 2x + 0 = (20) \\
(32) + (44) &= (3x + 2) + (4x + 4) = 7x + 6 \pmod{5} = 2x + 1 = (21)
\end{aligned}$$

### (33)

$$\begin{aligned}
(33) + (00) &= (3x + 3) + (0x + 0) = 3x + 3 \pmod{5} = 3x + 3 = (33) \\
(33) + (01) &= (3x + 3) + (0x + 1) = 3x + 4 \pmod{5} = 3x + 4 = (34) \\
(33) + (02) &= (3x + 3) + (0x + 2) = 3x + 5 \pmod{5} = 3x + 0 = (30) \\
(33) + (03) &= (3x + 3) + (0x + 3) = 3x + 6 \pmod{5} = 3x + 1 = (31) \\
(33) + (04) &= (3x + 3) + (0x + 4) = 3x + 7 \pmod{5} = 3x + 2 = (32) \\
(33) + (10) &= (3x + 3) + (1x + 0) = 4x + 3 \pmod{5} = 4x + 3 = (43) \\
(33) + (11) &= (3x + 3) + (1x + 1) = 4x + 4 \pmod{5} = 4x + 4 = (44) \\
(33) + (12) &= (3x + 3) + (1x + 2) = 4x + 5 \pmod{5} = 4x + 0 = (40) \\
(33) + (13) &= (3x + 3) + (1x + 3) = 4x + 6 \pmod{5} = 4x + 1 = (41) \\
(33) + (14) &= (3x + 3) + (1x + 4) = 4x + 7 \pmod{5} = 4x + 2 = (42) \\
(33) + (20) &= (3x + 3) + (2x + 0) = 5x + 3 \pmod{5} = 0x + 3 = (03) \\
(33) + (21) &= (3x + 3) + (2x + 1) = 5x + 4 \pmod{5} = 0x + 4 = (04) \\
(33) + (22) &= (3x + 3) + (2x + 2) = 5x + 5 \pmod{5} = 0x + 0 = (00) \\
(33) + (23) &= (3x + 3) + (2x + 3) = 5x + 6 \pmod{5} = 0x + 1 = (01) \\
(33) + (24) &= (3x + 3) + (2x + 4) = 5x + 7 \pmod{5} = 0x + 2 = (02) \\
(33) + (30) &= (3x + 3) + (3x + 0) = 6x + 3 \pmod{5} = 1x + 3 = (13) \\
(33) + (31) &= (3x + 3) + (3x + 1) = 6x + 4 \pmod{5} = 1x + 4 = (14) \\
(33) + (32) &= (3x + 3) + (3x + 2) = 6x + 5 \pmod{5} = 1x + 0 = (10) \\
(33) + (33) &= (3x + 3) + (3x + 3) = 6x + 6 \pmod{5} = 1x + 1 = (11) \\
(33) + (34) &= (3x + 3) + (3x + 4) = 6x + 7 \pmod{5} = 1x + 2 = (12) \\
(33) + (40) &= (3x + 3) + (4x + 0) = 7x + 3 \pmod{5} = 2x + 3 = (23) \\
(33) + (41) &= (3x + 3) + (4x + 1) = 7x + 4 \pmod{5} = 2x + 4 = (24) \\
(33) + (42) &= (3x + 3) + (4x + 2) = 7x + 5 \pmod{5} = 2x + 0 = (20) \\
(33) + (43) &= (3x + 3) + (4x + 3) = 7x + 6 \pmod{5} = 2x + 1 = (21) \\
(33) + (44) &= (3x + 3) + (4x + 4) = 7x + 7 \pmod{5} = 2x + 2 = (22)
\end{aligned}$$

**(34)**

- $$(34) + (00) = (3x + 4) + (0x + 0) = 3x + 4 \pmod{5} = 3x + 4 = (34)$$
- $$(34) + (01) = (3x + 4) + (0x + 1) = 3x + 5 \pmod{5} = 3x + 0 = (30)$$
- $$(34) + (02) = (3x + 4) + (0x + 2) = 3x + 6 \pmod{5} = 3x + 1 = (31)$$
- $$(34) + (03) = (3x + 4) + (0x + 3) = 3x + 7 \pmod{5} = 3x + 2 = (32)$$
- $$(34) + (04) = (3x + 4) + (0x + 4) = 3x + 8 \pmod{5} = 3x + 3 = (33)$$
- $$(34) + (10) = (3x + 4) + (1x + 0) = 4x + 4 \pmod{5} = 4x + 4 = (44)$$
- $$(34) + (11) = (3x + 4) + (1x + 1) = 4x + 5 \pmod{5} = 4x + 0 = (40)$$
- $$(34) + (12) = (3x + 4) + (1x + 2) = 4x + 6 \pmod{5} = 4x + 1 = (41)$$
- $$(34) + (13) = (3x + 4) + (1x + 3) = 4x + 7 \pmod{5} = 4x + 2 = (42)$$
- $$(34) + (14) = (3x + 4) + (1x + 4) = 4x + 8 \pmod{5} = 4x + 3 = (43)$$
- $$(34) + (20) = (3x + 4) + (2x + 0) = 5x + 4 \pmod{5} = 0x + 4 = (04)$$
- $$(34) + (21) = (3x + 4) + (2x + 1) = 5x + 5 \pmod{5} = 0x + 0 = (00)$$
- $$(34) + (22) = (3x + 4) + (2x + 2) = 5x + 6 \pmod{5} = 0x + 1 = (01)$$
- $$(34) + (23) = (3x + 4) + (2x + 3) = 5x + 7 \pmod{5} = 0x + 2 = (02)$$
- $$(34) + (24) = (3x + 4) + (2x + 4) = 5x + 8 \pmod{5} = 0x + 3 = (03)$$
- $$(34) + (30) = (3x + 4) + (3x + 0) = 6x + 4 \pmod{5} = 1x + 4 = (14)$$
- $$(34) + (31) = (3x + 4) + (3x + 1) = 6x + 5 \pmod{5} = 1x + 0 = (10)$$
- $$(34) + (32) = (3x + 4) + (3x + 2) = 6x + 6 \pmod{5} = 1x + 1 = (11)$$
- $$(34) + (33) = (3x + 4) + (3x + 3) = 6x + 7 \pmod{5} = 1x + 2 = (12)$$
- $$(34) + (34) = (3x + 4) + (3x + 4) = 6x + 8 \pmod{5} = 1x + 3 = (13)$$
- $$(34) + (40) = (3x + 4) + (4x + 0) = 7x + 4 \pmod{5} = 2x + 4 = (24)$$
- $$(34) + (41) = (3x + 4) + (4x + 1) = 7x + 5 \pmod{5} = 2x + 0 = (20)$$
- $$(34) + (42) = (3x + 4) + (4x + 2) = 7x + 6 \pmod{5} = 2x + 1 = (21)$$
- $$(34) + (43) = (3x + 4) + (4x + 3) = 7x + 7 \pmod{5} = 2x + 2 = (22)$$
- $$(34) + (44) = (3x + 4) + (4x + 4) = 7x + 8 \pmod{5} = 2x + 3 = (23)$$

Таблица 7.15

+	0	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	4
	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1
3	3	3	3	3	3	4	4	4	4	0	0	0	0	0	1	1	1	1	2	2	2	2
0	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1
3	3	3	3	3	3	4	4	4	4	0	0	0	0	0	1	1	1	1	2	2	2	2
1	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2
3	3	3	3	3	3	4	4	4	4	0	0	0	0	0	1	1	1	1	2	2	2	2
2	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
3	3	3	3	3	3	4	4	4	4	0	0	0	0	0	1	1	1	1	2	2	2	2
3	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
3	3	3	3	3	3	4	4	4	4	0	0	0	0	0	1	1	1	1	2	2	2	2
4	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

е) табл.7.16 для умножения в поле  $GF(q)$ ,  $q = p^m = 5^2 = 25$ .

$$a \cdot b = a_1 a_0 \cdot b_1 b_0 = (a_1 x + a_0) \cdot (b_1 x + b_0) = \\ (a_1 b_1)x^2 + (a_1 b_0 + a_0 b_1)x + (a_0 b_0) \pmod{f(x)}.$$

Например,

$$(32) \cdot (24) = (3x + 2) \cdot (2x + 4) = 6x^2 + 12x + 4x + 8 = 6x^2 + 16x + 8 \pmod{5} = \\ 1x^2 + 1x + 3 \pmod{4x^2 + 2x + 2} = 3x = 3x + 0 = (30).$$

$$\begin{array}{r} - \frac{1x^2+1x+3}{1x^2+3x+3} \mid \frac{4x^2+2x+2}{4} \\ \hline 3x \end{array}$$

**Далее подробные вычисления.**

$$(30) \cdot (00) = (3 \cdot 0)x^2 + (3 \cdot 0 + 0 \cdot 0)x + (0 \cdot 0) = 0x^2 + 0x + 0 \pmod{5} = \\ 0x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 0x + 0 = (00).$$

$$\begin{array}{r} - \frac{0x^2+0x+0}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\ \hline 0 \end{array}$$

$$(30) \cdot (01) = (3 \cdot 0)x^2 + (3 \cdot 1 + 0 \cdot 0)x + (0 \cdot 1) = 0x^2 + 3x + 0 \pmod{5} = \\ 0x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 3x + 0 = (30).$$

$$\begin{array}{r} - \frac{0x^2+3x+0}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\ \hline 3x \end{array}$$

$$(30) \cdot (02) = (3 \cdot 0)x^2 + (3 \cdot 2 + 0 \cdot 0)x + (0 \cdot 2) = 0x^2 + 6x + 0 \pmod{5} = \\ 0x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 1x + 0 = (10).$$

$$\begin{array}{r} - \frac{0x^2+1x+0}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\ \hline 1x \end{array}$$

$$(30) \cdot (03) = (3 \cdot 0)x^2 + (3 \cdot 3 + 0 \cdot 0)x + (0 \cdot 3) = 0x^2 + 9x + 0 \pmod{5} = \\ 0x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 4x + 0 = (40).$$

$$\begin{array}{r} - \frac{0x^2+4x+0}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\ \hline 4x \end{array}$$

$$(30) \cdot (04) = (3 \cdot 0)x^2 + (3 \cdot 4 + 0 \cdot 0)x + (0 \cdot 4) = 0x^2 + 12x + 0 \pmod{5} = \\ 0x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 2x + 0 = (20).$$

$$\begin{array}{r} - \frac{0x^2+2x+0}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\ \hline 2x \end{array}$$

$$(30) \cdot (10) = (3 \cdot 1)x^2 + (3 \cdot 0 + 0 \cdot 1)x + (0 \cdot 0) = 3x^2 + 0x + 0 \pmod{5} = \\ 3x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 1x + 1 = (11).$$

$$\begin{array}{r} - \frac{3x^2+0x+0}{3x^2+4x+4} \mid \frac{4x^2+2x+2}{2} \\ \hline 1x+1 \end{array}$$

$$(30) \cdot (11) = (3 \cdot 1)x^2 + (3 \cdot 1 + 0 \cdot 1)x + (0 \cdot 1) = 3x^2 + 3x + 0 \pmod{5} = \\ 3x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 4x + 1 = (41).$$

$$\begin{array}{r} - \frac{3x^2+3x+0}{3x^2+4x+4} \left| \begin{array}{c} 4x^2+2x+2 \\ 2 \\ 4x+1 \end{array} \right. \end{array}$$

$$(30) \cdot (12) = (3 \cdot 1)x^2 + (3 \cdot 2 + 0 \cdot 1)x + (0 \cdot 2) = 3x^2 + 6x + 0 \pmod{5} = \\ 3x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 2x + 1 = (21).$$

$$\begin{array}{r} - \frac{3x^2+1x+0}{3x^2+4x+4} \left| \begin{array}{c} 4x^2+2x+2 \\ 2 \\ 2x+1 \end{array} \right. \end{array}$$

$$(30) \cdot (13) = (3 \cdot 1)x^2 + (3 \cdot 3 + 0 \cdot 1)x + (0 \cdot 3) = 3x^2 + 9x + 0 \pmod{5} = \\ 3x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 0x + 1 = (01).$$

$$\begin{array}{r} - \frac{3x^2+4x+0}{3x^2+4x+4} \left| \begin{array}{c} 4x^2+2x+2 \\ 2 \\ 1 \end{array} \right. \end{array}$$

$$(30) \cdot (14) = (3 \cdot 1)x^2 + (3 \cdot 4 + 0 \cdot 1)x + (0 \cdot 4) = 3x^2 + 12x + 0 \pmod{5} = \\ 3x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 3x + 1 = (31).$$

$$\begin{array}{r} - \frac{3x^2+2x+0}{3x^2+4x+4} \left| \begin{array}{c} 4x^2+2x+2 \\ 2 \\ 3x+1 \end{array} \right. \end{array}$$

$$(30) \cdot (20) = (3 \cdot 2)x^2 + (3 \cdot 0 + 0 \cdot 2)x + (0 \cdot 0) = 6x^2 + 0x + 0 \pmod{5} = \\ 1x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 2x + 2 = (22).$$

$$\begin{array}{r} - \frac{1x^2+0x+0}{1x^2+3x+3} \left| \begin{array}{c} 4x^2+2x+2 \\ 4 \\ 2x+2 \end{array} \right. \end{array}$$

$$(30) \cdot (21) = (3 \cdot 2)x^2 + (3 \cdot 1 + 0 \cdot 2)x + (0 \cdot 1) = 6x^2 + 3x + 0 \pmod{5} = \\ 1x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 0x + 2 = (02).$$

$$\begin{array}{r} - \frac{1x^2+3x+0}{1x^2+3x+3} \left| \begin{array}{c} 4x^2+2x+2 \\ 4 \\ 2 \end{array} \right. \end{array}$$

$$(30) \cdot (22) = (3 \cdot 2)x^2 + (3 \cdot 2 + 0 \cdot 2)x + (0 \cdot 2) = 6x^2 + 6x + 0 \pmod{5} = \\ 1x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 3x + 2 = (32).$$

$$\begin{array}{r} - \frac{1x^2+1x+0}{1x^2+3x+3} \left| \begin{array}{c} 4x^2+2x+2 \\ 4 \\ 3x+2 \end{array} \right. \end{array}$$

$$(30) \cdot (23) = (3 \cdot 2)x^2 + (3 \cdot 3 + 0 \cdot 2)x + (0 \cdot 3) = 6x^2 + 9x + 0 \pmod{5} =$$

$$1x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 1x + 2 = (12).$$

$$\begin{array}{r} 1x^2+4x+0 \\ 1x^2+3x+3 \\ \hline 1x+2 \end{array}$$

$$(30) \cdot (24) = (3 \cdot 2)x^2 + (3 \cdot 4 + 0 \cdot 2)x + (0 \cdot 4) = 6x^2 + 12x + 0 \pmod{5} = 1x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 4x + 2 = (42).$$

$$\begin{array}{r} 1x^2+2x+0 \\ 1x^2+3x+3 \\ \hline 4x+2 \end{array}$$

$$(30) \cdot (30) = (3 \cdot 3)x^2 + (3 \cdot 0 + 0 \cdot 3)x + (0 \cdot 0) = 9x^2 + 0x + 0 \pmod{5} = 4x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 3x + 3 = (33).$$

$$\begin{array}{r} 4x^2+0x+0 \\ 4x^2+2x+2 \\ \hline 3x+3 \end{array}$$

$$(30) \cdot (31) = (3 \cdot 3)x^2 + (3 \cdot 1 + 0 \cdot 3)x + (0 \cdot 1) = 9x^2 + 3x + 0 \pmod{5} = 4x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 1x + 3 = (13).$$

$$\begin{array}{r} 4x^2+3x+0 \\ 4x^2+2x+2 \\ \hline 1x+3 \end{array}$$

$$(30) \cdot (32) = (3 \cdot 3)x^2 + (3 \cdot 2 + 0 \cdot 3)x + (0 \cdot 2) = 9x^2 + 6x + 0 \pmod{5} = 4x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 4x + 3 = (43).$$

$$\begin{array}{r} 4x^2+1x+0 \\ 4x^2+2x+2 \\ \hline 4x+3 \end{array}$$

$$(30) \cdot (33) = (3 \cdot 3)x^2 + (3 \cdot 3 + 0 \cdot 3)x + (0 \cdot 3) = 9x^2 + 9x + 0 \pmod{5} = 4x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 2x + 3 = (23).$$

$$\begin{array}{r} 4x^2+4x+0 \\ 4x^2+2x+2 \\ \hline 2x+3 \end{array}$$

$$(30) \cdot (34) = (3 \cdot 3)x^2 + (3 \cdot 4 + 0 \cdot 3)x + (0 \cdot 4) = 9x^2 + 12x + 0 \pmod{5} = 4x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 0x + 3 = (03).$$

$$\begin{array}{r} 4x^2+2x+0 \\ 4x^2+2x+2 \\ \hline 3 \end{array}$$

$$(30) \cdot (40) = (3 \cdot 4)x^2 + (3 \cdot 0 + 0 \cdot 4)x + (0 \cdot 0) = 12x^2 + 0x + 0 \pmod{5} = 2x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 4x + 4 = (44).$$

$$\begin{array}{r} \underline{-\frac{2x^2+0x+0}{2x^2+1x+1}} \\ \hline 4x+4 \end{array}$$

$$(30) \cdot (41) = (3 \cdot 4)x^2 + (3 \cdot 1 + 0 \cdot 4)x + (0 \cdot 1) = 12x^2 + 3x + 0 \pmod{5} = \\ 2x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 2x + 4 = (24).$$

$$\begin{array}{r} \underline{-\frac{2x^2+3x+0}{2x^2+1x+1}} \\ \hline 3 \\ 2x+4 \end{array}$$

$$(30) \cdot (42) = (3 \cdot 4)x^2 + (3 \cdot 2 + 0 \cdot 4)x + (0 \cdot 2) = 12x^2 + 6x + 0 \pmod{5} = \\ 2x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 0x + 4 = (04).$$

$$\begin{array}{r} \underline{-\frac{2x^2+1x+0}{2x^2+1x+1}} \\ \hline 3 \\ 4 \end{array}$$

$$(30) \cdot (43) = (3 \cdot 4)x^2 + (3 \cdot 3 + 0 \cdot 4)x + (0 \cdot 3) = 12x^2 + 9x + 0 \pmod{5} = \\ 2x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 3x + 4 = (34).$$

$$\begin{array}{r} \underline{-\frac{2x^2+4x+0}{2x^2+1x+1}} \\ \hline 3 \\ 3x+4 \end{array}$$

$$(30) \cdot (44) = (3 \cdot 4)x^2 + (3 \cdot 4 + 0 \cdot 4)x + (0 \cdot 4) = 12x^2 + 12x + 0 \pmod{5} = \\ 2x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 1x + 4 = (14).$$

$$\begin{array}{r} \underline{-\frac{2x^2+2x+0}{2x^2+1x+1}} \\ \hline 3 \\ 1x+4 \end{array}$$

**(31)**

$$(31) \cdot (00) = (3 \cdot 0)x^2 + (3 \cdot 0 + 1 \cdot 0)x + (1 \cdot 0) = 0x^2 + 0x + 0 \pmod{5} = \\ 0x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 0x + 0 = (00).$$

$$\begin{array}{r} \underline{-\frac{0x^2+0x+0}{0x^2+0x+0}} \\ \hline 0 \end{array}$$

$$(31) \cdot (01) = (3 \cdot 0)x^2 + (3 \cdot 1 + 1 \cdot 0)x + (1 \cdot 1) = 0x^2 + 3x + 1 \pmod{5} = \\ 0x^2 + 3x + 1 \pmod{4x^2 + 2x + 2} = 3x + 1 = (31).$$

$$\begin{array}{r} \underline{-\frac{0x^2+3x+1}{0x^2+0x+0}} \\ \hline 0 \\ 3x+1 \end{array}$$

$$(31) \cdot (02) = (3 \cdot 0)x^2 + (3 \cdot 2 + 1 \cdot 0)x + (1 \cdot 2) = 0x^2 + 6x + 2 \pmod{5} = \\ 0x^2 + 1x + 2 \pmod{4x^2 + 2x + 2} = 1x + 2 = (12)$$

$$\begin{array}{r} 0x^2+1x+2 \\ \hline 0x^2+0x+0 \\ \hline 1x+2 \end{array}$$

$$(31) \cdot (03) = (3 \cdot 0)x^2 + (3 \cdot 3 + 1 \cdot 0)x + (1 \cdot 3) = 0x^2 + 9x + 3 \pmod{5} = \\ 0x^2 + 4x + 3 \pmod{4x^2 + 2x + 2} = 4x + 3 = (43).$$

$$\begin{array}{r} 0x^2+4x+3 \\ \hline 0x^2+0x+0 \\ \hline 4x+3 \end{array}$$

$$(31) \cdot (04) = (3 \cdot 0)x^2 + (3 \cdot 4 + 1 \cdot 0)x + (1 \cdot 4) = 0x^2 + 12x + 4 \pmod{5} = \\ 0x^2 + 2x + 4 \pmod{4x^2 + 2x + 2} = 2x + 4 = (24).$$

$$\begin{array}{r} 0x^2+2x+4 \\ \hline 0x^2+0x+0 \\ \hline 2x+4 \end{array}$$

$$(31) \cdot (10) = (3 \cdot 1)x^2 + (3 \cdot 0 + 1 \cdot 1)x + (1 \cdot 0) = 3x^2 + 1x + 0 \pmod{5} = \\ 3x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 2x + 1 = (21).$$

$$\begin{array}{r} 3x^2+1x+0 \\ \hline 3x^2+4x+4 \\ \hline 2x+1 \end{array}$$

$$(31) \cdot (11) = (3 \cdot 1)x^2 + (3 \cdot 1 + 1 \cdot 1)x + (1 \cdot 1) = 3x^2 + 4x + 1 \pmod{5} = \\ 3x^2 + 4x + 1 \pmod{4x^2 + 2x + 2} = 0x + 2 = (02).$$

$$\begin{array}{r} 3x^2+4x+1 \\ \hline 3x^2+4x+4 \\ \hline 2 \end{array}$$

$$(31) \cdot (12) = (3 \cdot 1)x^2 + (3 \cdot 2 + 1 \cdot 1)x + (1 \cdot 2) = 3x^2 + 7x + 2 \pmod{5} = \\ 3x^2 + 2x + 2 \pmod{4x^2 + 2x + 2} = 3x + 3 = (33).$$

$$\begin{array}{r} 3x^2+2x+2 \\ \hline 3x^2+4x+4 \\ \hline 3x+3 \end{array}$$

$$(31) \cdot (13) = (3 \cdot 1)x^2 + (3 \cdot 3 + 1 \cdot 1)x + (1 \cdot 3) = 3x^2 + 10x + 3 \pmod{5} = \\ 3x^2 + 0x + 3 \pmod{4x^2 + 2x + 2} = 1x + 4 = (14).$$

$$\begin{array}{r} 3x^2+0x+3 \\ \hline 3x^2+4x+4 \\ \hline 1x+4 \end{array}$$

$$(31) \cdot (14) = (3 \cdot 1)x^2 + (3 \cdot 4 + 1 \cdot 1)x + (1 \cdot 4) = 3x^2 + 13x + 4 \pmod{5} = \\ 3x^2 + 3x + 4 \pmod{4x^2 + 2x + 2} = 4x + 0 = (40).$$

$$\begin{array}{r} - \ 3x^2+3x+4 \Big| 4x^2+2x+2 \\ \underline{3x^2+4x+4} \Big| 2 \\ \quad \quad \quad 4x \end{array}$$

$$(31) \cdot (20) = (3 \cdot 2)x^2 + (3 \cdot 0 + 1 \cdot 2)x + (1 \cdot 0) = 6x^2 + 2x + 0 \pmod{5} = \\ 1x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 4x + 2 = (42).$$

$$\begin{array}{r} - \ 1x^2+2x+0 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \Big| 4 \\ \quad \quad \quad 4x+2 \end{array}$$

$$(31) \cdot (21) = (3 \cdot 2)x^2 + (3 \cdot 1 + 1 \cdot 2)x + (1 \cdot 1) = 6x^2 + 5x + 1 \pmod{5} = \\ 1x^2 + 0x + 1 \pmod{4x^2 + 2x + 2} = 2x + 3 = (23).$$

$$\begin{array}{r} - \ 1x^2+0x+1 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \Big| 4 \\ \quad \quad \quad 2x+3 \end{array}$$

$$(31) \cdot (22) = (3 \cdot 2)x^2 + (3 \cdot 2 + 1 \cdot 2)x + (1 \cdot 2) = 6x^2 + 8x + 2 \pmod{5} = \\ 1x^2 + 3x + 2 \pmod{4x^2 + 2x + 2} = 0x + 4 = (04).$$

$$\begin{array}{r} - \ 1x^2+3x+2 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \Big| 4 \\ \quad \quad \quad 4 \end{array}$$

$$(31) \cdot (23) = (3 \cdot 2)x^2 + (3 \cdot 3 + 1 \cdot 2)x + (1 \cdot 3) = 6x^2 + 11x + 3 \pmod{5} = \\ 1x^2 + 1x + 3 \pmod{4x^2 + 2x + 2} = 3x + 0 = (30).$$

$$\begin{array}{r} - \ 1x^2+1x+3 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \Big| 4 \\ \quad \quad \quad 3x \end{array}$$

$$(31) \cdot (24) = (3 \cdot 2)x^2 + (3 \cdot 4 + 1 \cdot 2)x + (1 \cdot 4) = 6x^2 + 14x + 4 \pmod{5} = \\ 1x^2 + 4x + 4 \pmod{4x^2 + 2x + 2} = 1x + 1 = (11).$$

$$\begin{array}{r} - \ 1x^2+4x+4 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \Big| 4 \\ \quad \quad \quad 1x+1 \end{array}$$

$$(31) \cdot (30) = (3 \cdot 3)x^2 + (3 \cdot 0 + 1 \cdot 3)x + (1 \cdot 0) = 9x^2 + 3x + 0 \pmod{5} = \\ 4x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 1x + 3 = (13).$$

$$\begin{array}{r} - \ 4x^2+3x+0 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \Big| 1 \\ \quad \quad \quad 1x+3 \end{array}$$

$$(31) \cdot (31) = (3 \cdot 3)x^2 + (3 \cdot 1 + 1 \cdot 3)x + (1 \cdot 1) = 9x^2 + 6x + 1 \pmod{5} = \\ 4x^2 + 1x + 1 \pmod{4x^2 + 2x + 2} = 4x + 4 = (44).$$

$$\begin{array}{r} - \ 4x^2+1x+1 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \Big| 1 \\ \phantom{-} \quad 4x+4 \end{array}$$

$$(31) \cdot (32) = (3 \cdot 3)x^2 + (3 \cdot 2 + 1 \cdot 3)x + (1 \cdot 2) = 9x^2 + 9x + 2 \pmod{5} = \\ 4x^2 + 4x + 2 \pmod{4x^2 + 2x + 2} = 2x + 0 = (20).$$

$$\begin{array}{r} - \ 4x^2+4x+2 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \Big| 1 \\ \phantom{-} \quad 2x \end{array}$$

$$(31) \cdot (33) = (3 \cdot 3)x^2 + (3 \cdot 3 + 1 \cdot 3)x + (1 \cdot 3) = 9x^2 + 12x + 3 \pmod{5} = \\ 4x^2 + 2x + 3 \pmod{4x^2 + 2x + 2} = 0x + 1 = (01).$$

$$\begin{array}{r} - \ 4x^2+2x+3 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \Big| 1 \\ \phantom{-} \quad 1 \end{array}$$

$$(31) \cdot (34) = (3 \cdot 3)x^2 + (3 \cdot 4 + 1 \cdot 3)x + (1 \cdot 4) = 9x^2 + 15x + 4 \pmod{5} = \\ 4x^2 + 0x + 4 \pmod{4x^2 + 2x + 2} = 3x + 2 = (32).$$

$$\begin{array}{r} - \ 4x^2+0x+4 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \Big| 1 \\ \phantom{-} \quad 3x+2 \end{array}$$

$$(31) \cdot (40) = (3 \cdot 4)x^2 + (3 \cdot 0 + 1 \cdot 4)x + (1 \cdot 0) = 12x^2 + 4x + 0 \pmod{5} = \\ 2x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 3x + 4 = (34).$$

$$\begin{array}{r} - \ 2x^2+4x+0 \Big| 4x^2+2x+2 \\ \underline{2x^2+1x+1} \Big| 3 \\ \phantom{-} \quad 3x+4 \end{array}$$

$$(31) \cdot (41) = (3 \cdot 4)x^2 + (3 \cdot 1 + 1 \cdot 4)x + (1 \cdot 1) = 12x^2 + 7x + 1 \pmod{5} = \\ 2x^2 + 2x + 1 \pmod{4x^2 + 2x + 2} = 1x + 0 = (10).$$

$$\begin{array}{r} - \ 2x^2+2x+1 \Big| 4x^2+2x+2 \\ \underline{2x^2+1x+1} \Big| 3 \\ \phantom{-} \quad 1x \end{array}$$

$$(31) \cdot (42) = (3 \cdot 4)x^2 + (3 \cdot 2 + 1 \cdot 4)x + (1 \cdot 2) = 12x^2 + 10x + 2 \pmod{5} = \\ 2x^2 + 0x + 2 \pmod{4x^2 + 2x + 2} = 4x + 1 = (41).$$

$$\begin{array}{r} - \ 2x^2+0x+2 \Big| 4x^2+2x+2 \\ \underline{2x^2+1x+1} \Big| 3 \\ \phantom{-} \quad 4x+1 \end{array}$$

$$(31) \cdot (43) = (3 \cdot 4)x^2 + (3 \cdot 3 + 1 \cdot 4)x + (1 \cdot 3) = 12x^2 + 13x + 3 \pmod{5} = \\ 2x^2 + 3x + 3 \pmod{4x^2 + 2x + 2} = 2x + 2 = (22).$$

$$\begin{array}{r} - \frac{2x^2+3x+3}{2x^2+1x+1} \left| \begin{array}{r} 4x^2+2x+2 \\ 3 \\ 2x+2 \end{array} \right. \end{array}$$

$$(31) \cdot (44) = (3 \cdot 4)x^2 + (3 \cdot 4 + 1 \cdot 4)x + (1 \cdot 4) = 12x^2 + 16x + 4 \pmod{5} = 2x^2 + 1x + 4 \pmod{4x^2 + 2x + 2} = 0x + 3 = (03).$$

$$\begin{array}{r} - \frac{2x^2+1x+4}{2x^2+1x+1} \left| \begin{array}{r} 4x^2+2x+2 \\ 3 \\ 3 \end{array} \right. \end{array}$$

**(32)**

$$(32) \cdot (00) = (3 \cdot 0)x^2 + (3 \cdot 0 + 2 \cdot 0)x + (2 \cdot 0) = 0x^2 + 0x + 0 \pmod{5} = 0x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 0x + 0 = (00).$$

$$\begin{array}{r} - \frac{0x^2+0x+0}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 0 \end{array} \right. \end{array}$$

$$(32) \cdot (01) = (3 \cdot 0)x^2 + (3 \cdot 1 + 2 \cdot 0)x + (2 \cdot 1) = 0x^2 + 3x + 2 \pmod{5} = 0x^2 + 3x + 2 \pmod{4x^2 + 2x + 2} = 3x + 2 = (32).$$

$$\begin{array}{r} - \frac{0x^2+3x+2}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 3x+2 \end{array} \right. \end{array}$$

$$(32) \cdot (02) = (3 \cdot 0)x^2 + (3 \cdot 2 + 2 \cdot 0)x + (2 \cdot 2) = 0x^2 + 6x + 4 \pmod{5} = 0x^2 + 1x + 4 \pmod{4x^2 + 2x + 2} = 1x + 4 = (14).$$

$$\begin{array}{r} - \frac{0x^2+1x+4}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 1x+4 \end{array} \right. \end{array}$$

$$(32) \cdot (03) = (3 \cdot 0)x^2 + (3 \cdot 3 + 2 \cdot 0)x + (2 \cdot 3) = 0x^2 + 9x + 6 \pmod{5} = 0x^2 + 4x + 1 \pmod{4x^2 + 2x + 2} = 4x + 1 = (41).$$

$$\begin{array}{r} - \frac{0x^2+4x+1}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 4x+1 \end{array} \right. \end{array}$$

$$(32) \cdot (04) = (3 \cdot 0)x^2 + (3 \cdot 4 + 2 \cdot 0)x + (2 \cdot 4) = 0x^2 + 12x + 8 \pmod{5} = 0x^2 + 2x + 3 \pmod{4x^2 + 2x + 2} = 2x + 3 = (23).$$

$$\begin{array}{r} - \frac{0x^2+2x+3}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 2x+3 \end{array} \right. \end{array}$$

$$(32) \cdot (10) = (3 \cdot 1)x^2 + (3 \cdot 0 + 2 \cdot 1)x + (2 \cdot 0) = 3x^2 + 2x + 0 \pmod{5} = 3x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 3x + 1 = (31).$$

$$\begin{array}{r} - \frac{3x^2+2x+0}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 3x+1 \end{array} \right. \end{array}$$

$$(32) \cdot (11) = (3 \cdot 1)x^2 + (3 \cdot 1 + 2 \cdot 1)x + (2 \cdot 1) = 3x^2 + 5x + 2 \pmod{5} = 3x^2 + 0x + 2 \pmod{4x^2 + 2x + 2} = 1x + 3 = (13).$$

$$\begin{array}{r} - \frac{3x^2+0x+2}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 1x+3 \end{array} \right. \end{array}$$

$$(32) \cdot (12) = (3 \cdot 1)x^2 + (3 \cdot 2 + 2 \cdot 1)x + (2 \cdot 2) = 3x^2 + 8x + 4 \pmod{5} = 3x^2 + 3x + 4 \pmod{4x^2 + 2x + 2} = 4x + 0 = (40).$$

$$\begin{array}{r} - \frac{3x^2+3x+4}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 4x \end{array} \right. \end{array}$$

$$(32) \cdot (13) = (3 \cdot 1)x^2 + (3 \cdot 3 + 2 \cdot 1)x + (2 \cdot 3) = 3x^2 + 11x + 6 \pmod{5} = 3x^2 + 1x + 1 \pmod{4x^2 + 2x + 2} = 2x + 2 = (22).$$

$$\begin{array}{r} - \frac{3x^2+1x+1}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 2x+2 \end{array} \right. \end{array}$$

$$(32) \cdot (14) = (3 \cdot 1)x^2 + (3 \cdot 4 + 2 \cdot 1)x + (2 \cdot 4) = 3x^2 + 14x + 8 \pmod{5} = 3x^2 + 4x + 3 \pmod{4x^2 + 2x + 2} = 0x + 4 = (04).$$

$$\begin{array}{r} - \frac{3x^2+4x+3}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 4 \end{array} \right. \end{array}$$

$$(32) \cdot (20) = (3 \cdot 2)x^2 + (3 \cdot 0 + 2 \cdot 2)x + (2 \cdot 0) = 6x^2 + 4x + 0 \pmod{5} = 1x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 1x + 2 = (12).$$

$$\begin{array}{r} - \frac{1x^2+4x+0}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 1x+2 \end{array} \right. \end{array}$$

$$(32) \cdot (21) = (3 \cdot 2)x^2 + (3 \cdot 1 + 2 \cdot 2)x + (2 \cdot 1) = 6x^2 + 7x + 2 \pmod{5} = 1x^2 + 2x + 2 \pmod{4x^2 + 2x + 2} = 4x + 4 = (44).$$

$$\begin{array}{r} - \frac{1x^2+2x+2}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 4x+4 \end{array} \right. \end{array}$$

$$(32) \cdot (22) = (3 \cdot 2)x^2 + (3 \cdot 2 + 2 \cdot 2)x + (2 \cdot 2) = 6x^2 + 10x + 4 \pmod{5} = 1x^2 + 0x + 4 \pmod{4x^2 + 2x + 2} = 2x + 1 = (21).$$

$$\begin{array}{r} - \quad 1x^2+0x+4 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \quad 4 \\ \quad \quad \quad 2x+1 \end{array}$$

$$(32) \cdot (23) = (3 \cdot 2)x^2 + (3 \cdot 3 + 2 \cdot 2)x + (2 \cdot 3) = 6x^2 + 13x + 6 \pmod{5} = 1x^2 + 3x + 1 \pmod{4x^2 + 2x + 2} = 0x + 3 = (03).$$

$$\begin{array}{r} - \quad 1x^2+3x+1 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \quad 4 \\ \quad \quad \quad 3 \end{array}$$

$$(32) \cdot (24) = (3 \cdot 2)x^2 + (3 \cdot 4 + 2 \cdot 2)x + (2 \cdot 4) = 6x^2 + 16x + 8 \pmod{5} = 1x^2 + 1x + 3 \pmod{4x^2 + 2x + 2} = 3x = (30).$$

$$\begin{array}{r} - \quad 1x^2+1x+3 \Big| 4x^2+2x+2 \\ \underline{1x^2+3x+3} \quad 4 \\ \quad \quad \quad 3x \end{array}$$

$$(32) \cdot (30) = (3 \cdot 3)x^2 + (3 \cdot 0 + 2 \cdot 3)x + (2 \cdot 0) = 9x^2 + 6x + 0 \pmod{5} = 4x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 4x + 3 = (43).$$

$$\begin{array}{r} - \quad 4x^2+1x+0 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \quad 1 \\ \quad \quad \quad 4x+3 \end{array}$$

$$(32) \cdot (31) = (3 \cdot 3)x^2 + (3 \cdot 1 + 2 \cdot 3)x + (2 \cdot 1) = 9x^2 + 9x + 2 \pmod{5} = 4x^2 + 4x + 2 \pmod{4x^2 + 2x + 2} = 2x + 0 = (20).$$

$$\begin{array}{r} - \quad 4x^2+4x+2 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \quad 1 \\ \quad \quad \quad 2x \end{array}$$

$$(32) \cdot (32) = (3 \cdot 3)x^2 + (3 \cdot 2 + 2 \cdot 3)x + (2 \cdot 2) = 9x^2 + 12x + 4 \pmod{5} = 4x^2 + 2x + 4 \pmod{4x^2 + 2x + 2} = 0x + 2 = (02).$$

$$\begin{array}{r} - \quad 4x^2+2x+4 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \quad 1 \\ \quad \quad \quad 2 \end{array}$$

$$(32) \cdot (33) = (3 \cdot 3)x^2 + (3 \cdot 3 + 2 \cdot 3)x + (2 \cdot 3) = 9x^2 + 15x + 6 \pmod{5} = 4x^2 + 0x + 1 \pmod{4x^2 + 2x + 2} = 3x + 4 = (34).$$

$$\begin{array}{r} - \quad 4x^2+0x+1 \Big| 4x^2+2x+2 \\ \underline{4x^2+2x+2} \quad 1 \\ \quad \quad \quad 3x+4 \end{array}$$

$$(32) \cdot (34) = (3 \cdot 3)x^2 + (3 \cdot 4 + 2 \cdot 3)x + (2 \cdot 4) = 9x^2 + 18x + 8 \pmod{5} = 4x^2 + 3x + 3 \pmod{4x^2 + 2x + 2} = 1x + 1 = (11).$$

$$\begin{array}{r} - \frac{4x^2+3x+3}{4x^2+2x+2} \mid \frac{4x^2+2x+2}{1} \\ \underline{4x^2+2x+2} \mid 1 \\ 1x+1 \end{array}$$

$$(32) \cdot (40) = (3 \cdot 4)x^2 + (3 \cdot 0 + 2 \cdot 4)x + (2 \cdot 0) = 12x^2 + 8x + 0 \pmod{5} = 2x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 2x + 4 = (24).$$

$$\begin{array}{r} - \frac{2x^2+3x+0}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \underline{2x^2+1x+1} \mid 3 \\ 2x+4 \end{array}$$

$$(32) \cdot (41) = (3 \cdot 4)x^2 + (3 \cdot 1 + 2 \cdot 4)x + (2 \cdot 1) = 12x^2 + 11x + 2 \pmod{5} = 2x^2 + 1x + 2 \pmod{4x^2 + 2x + 2} = 0x + 1 = (01).$$

$$\begin{array}{r} - \frac{2x^2+1x+2}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \underline{2x^2+1x+1} \mid 3 \\ 1 \end{array}$$

$$(32) \cdot (42) = (3 \cdot 4)x^2 + (3 \cdot 2 + 2 \cdot 4)x + (2 \cdot 2) = 12x^2 + 14x + 4 \pmod{5} = 2x^2 + 4x + 4 \pmod{4x^2 + 2x + 2} = 3x + 3 = (33).$$

$$\begin{array}{r} - \frac{2x^2+4x+4}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \underline{2x^2+1x+1} \mid 3 \\ 3x+3 \end{array}$$

$$(32) \cdot (43) = (3 \cdot 4)x^2 + (3 \cdot 3 + 2 \cdot 4)x + (2 \cdot 3) = 12x^2 + 17x + 6 \pmod{5} = 2x^2 + 2x + 1 \pmod{4x^2 + 2x + 2} = 1x + 0 = (10).$$

$$\begin{array}{r} - \frac{2x^2+2x+1}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \underline{2x^2+1x+1} \mid 3 \\ 1x \end{array}$$

$$(32) \cdot (44) = (3 \cdot 4)x^2 + (3 \cdot 4 + 2 \cdot 4)x + (2 \cdot 4) = 12x^2 + 20x + 8 \pmod{5} = 2x^2 + 0x + 3 \pmod{4x^2 + 2x + 2} = 4x + 2 = (42).$$

$$\begin{array}{r} - \frac{2x^2+0x+3}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \underline{2x^2+1x+1} \mid 3 \\ 4x+2 \end{array}$$

**(33)**

$$(33) \cdot (00) = (3 \cdot 0)x^2 + (3 \cdot 0 + 3 \cdot 0)x + (3 \cdot 0) = 0x^2 + 0x + 0 \pmod{5} = 0x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 0x + 0 = (00).$$

$$\begin{array}{r} - \frac{0x^2+0x+0}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\ \underline{0x^2+0x+0} \mid 0 \\ 0 \end{array}$$

$$(33) \cdot (01) = (3 \cdot 0)x^2 + (3 \cdot 1 + 3 \cdot 0)x + (3 \cdot 1) = 0x^2 + 3x + 3 \pmod{5} = 0x^2 + 3x + 3 \pmod{4x^2 + 2x + 2} = 3x + 3 = (33).$$

$$\begin{array}{r}
 -\frac{0x^2+3x+3}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\
 \hline
 3x+3
 \end{array}$$

$$(33) \cdot (02) = (3 \cdot 0)x^2 + (3 \cdot 2 + 3 \cdot 0)x + (3 \cdot 2) = 0x^2 + 6x + 6 \pmod{5} = \\ 0x^2 + 1x + 1 \pmod{4x^2 + 2x + 2} = 1x + 1 = (11).$$

$$\begin{array}{r}
 -\frac{0x^2+1x+1}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\
 \hline
 1x+1
 \end{array}$$

$$(33) \cdot (03) = (3 \cdot 0)x^2 + (3 \cdot 3 + 3 \cdot 0)x + (3 \cdot 3) = 0x^2 + 9x + 9 \pmod{5} = \\ 0x^2 + 4x + 4 \pmod{4x^2 + 2x + 2} = 4x + 4 = (44).$$

$$\begin{array}{r}
 -\frac{0x^2+4x+4}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\
 \hline
 4x+4
 \end{array}$$

$$(33) \cdot (04) = (3 \cdot 0)x^2 + (3 \cdot 4 + 3 \cdot 0)x + (3 \cdot 4) = 0x^2 + 12x + 12 \pmod{5} = \\ 0x^2 + 2x + 2 \pmod{4x^2 + 2x + 2} = 2x + 2 = (22).$$

$$\begin{array}{r}
 -\frac{0x^2+2x+2}{0x^2+0x+0} \mid \frac{4x^2+2x+2}{0} \\
 \hline
 2x+2
 \end{array}$$

$$(33) \cdot (10) = (3 \cdot 1)x^2 + (3 \cdot 0 + 3 \cdot 1)x + (3 \cdot 0) = 3x^2 + 3x + 0 \pmod{5} = \\ 3x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 4x + 1 = (41).$$

$$\begin{array}{r}
 -\frac{3x^2+3x+0}{3x^2+4x+4} \mid \frac{4x^2+2x+2}{2} \\
 \hline
 4x+1
 \end{array}$$

$$(33) \cdot (11) = (3 \cdot 1)x^2 + (3 \cdot 1 + 3 \cdot 1)x + (3 \cdot 1) = 3x^2 + 6x + 3 \pmod{5} = \\ 3x^2 + 1x + 3 \pmod{4x^2 + 2x + 2} = 2x + 4 = (24).$$

$$\begin{array}{r}
 -\frac{3x^2+1x+3}{3x^2+4x+4} \mid \frac{4x^2+2x+2}{2} \\
 \hline
 2x+4
 \end{array}$$

$$(33) \cdot (12) = (3 \cdot 1)x^2 + (3 \cdot 2 + 3 \cdot 1)x + (3 \cdot 2) = 3x^2 + 9x + 6 \pmod{5} = \\ 3x^2 + 4x + 1 \pmod{4x^2 + 2x + 2} = 0x + 2 = (02).$$

$$\begin{array}{r}
 -\frac{3x^2+4x+1}{3x^2+4x+4} \mid \frac{4x^2+2x+2}{2} \\
 \hline
 2
 \end{array}$$

$$(33) \cdot (13) = (3 \cdot 1)x^2 + (3 \cdot 3 + 3 \cdot 1)x + (3 \cdot 3) = 3x^2 + 12x + 9 \pmod{5} = \\ 3x^2 + 2x + 4 \pmod{4x^2 + 2x + 2} = 3x + 0 = (30).$$

$$\begin{array}{r} - \frac{3x^2+2x+4}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 3x \end{array} \right. \end{array}$$

$$(33) \cdot (14) = (3 \cdot 1)x^2 + (3 \cdot 4 + 3 \cdot 1)x + (3 \cdot 4) = 3x^2 + 15x + 12 \pmod{5} = 3x^2 + 0x + 2 \pmod{4x^2 + 2x + 2} = 1x + 3 = (13).$$

$$\begin{array}{r} - \frac{3x^2+0x+2}{3x^2+4x+4} \left| \begin{array}{r} 4x^2+2x+2 \\ 2 \\ 1x+3 \end{array} \right. \end{array}$$

$$(33) \cdot (20) = (3 \cdot 2)x^2 + (3 \cdot 0 + 3 \cdot 2)x + (3 \cdot 0) = 6x^2 + 6x + 0 \pmod{5} = 1x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 3x + 2 = (32).$$

$$\begin{array}{r} - \frac{1x^2+1x+0}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 3x+2 \end{array} \right. \end{array}$$

$$(33) \cdot (21) = (3 \cdot 2)x^2 + (3 \cdot 1 + 3 \cdot 2)x + (3 \cdot 1) = 6x^2 + 9x + 3 \pmod{5} = 1x^2 + 4x + 3 \pmod{4x^2 + 2x + 2} = 1x + 0 = (10).$$

$$\begin{array}{r} - \frac{1x^2+4x+3}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 1x \end{array} \right. \end{array}$$

$$(33) \cdot (22) = (3 \cdot 2)x^2 + (3 \cdot 2 + 3 \cdot 2)x + (3 \cdot 2) = 6x^2 + 12x + 6 \pmod{5} = 1x^2 + 2x + 1 \pmod{4x^2 + 2x + 2} = 4x + 3 = (43)$$

$$\begin{array}{r} - \frac{1x^2+2x+1}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 4x+3 \end{array} \right. \end{array}$$

$$(33) \cdot (23) = (3 \cdot 2)x^2 + (3 \cdot 3 + 3 \cdot 2)x + (3 \cdot 3) = 6x^2 + 15x + 9 \pmod{5} = 1x^2 + 0x + 4 \pmod{4x^2 + 2x + 2} = 2x + 1 = (21).$$

$$\begin{array}{r} - \frac{1x^2+0x+4}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 2x+1 \end{array} \right. \end{array}$$

$$(33) \cdot (24) = (3 \cdot 2)x^2 + (3 \cdot 4 + 3 \cdot 2)x + (3 \cdot 4) = 6x^2 + 18x + 12 \pmod{5} = 1x^2 + 3x + 2 \pmod{4x^2 + 2x + 2} = 0x + 4 = (04).$$

$$\begin{array}{r} - \frac{1x^2+3x+2}{1x^2+3x+3} \left| \begin{array}{r} 4x^2+2x+2 \\ 4 \\ 4 \end{array} \right. \end{array}$$

$$(33) \cdot (30) = (3 \cdot 3)x^2 + (3 \cdot 0 + 3 \cdot 3)x + (3 \cdot 0) = 9x^2 + 9x + 0 \pmod{5} = 4x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 2x + 3 = (23).$$

$$\begin{array}{r} \underline{-\frac{4x^2+4x+0}{4x^2+2x+2}} \\ \underline{\underline{2x+3}} \end{array}$$

$$(33) \cdot (31) = (3 \cdot 3)x^2 + (3 \cdot 1 + 3 \cdot 3)x + (3 \cdot 1) = 9x^2 + 12x + 3 \pmod{5} = \\ 4x^2 + 2x + 3 \pmod{4x^2 + 2x + 2} = 0x + 1 = (01).$$

$$\begin{array}{r} \underline{-\frac{4x^2+2x+3}{4x^2+2x+2}} \\ \underline{\underline{1}} \end{array}$$

$$(33) \cdot (32) = (3 \cdot 3)x^2 + (3 \cdot 2 + 3 \cdot 3)x + (3 \cdot 2) = 9x^2 + 15x + 6 \pmod{5} = \\ 4x^2 + 0x + 1 \pmod{4x^2 + 2x + 2} = 3x + 4 = (34).$$

$$\begin{array}{r} \underline{-\frac{4x^2+0x+1}{4x^2+2x+2}} \\ \underline{\underline{3x+4}} \end{array}$$

$$(33) \cdot (33) = (3 \cdot 3)x^2 + (3 \cdot 3 + 3 \cdot 3)x + (3 \cdot 3) = 9x^2 + 18x + 9 \pmod{5} = \\ 4x^2 + 3x + 4 \pmod{4x^2 + 2x + 2} = 1x + 2 = (12).$$

$$\begin{array}{r} \underline{-\frac{4x^2+3x+4}{4x^2+2x+2}} \\ \underline{\underline{1x+2}} \end{array}$$

$$(33) \cdot (34) = (3 \cdot 3)x^2 + (3 \cdot 4 + 3 \cdot 3)x + (3 \cdot 4) = 9x^2 + 21x + 12 \pmod{5} = \\ 4x^2 + 1x + 2 \pmod{4x^2 + 2x + 2} = 4x + 0 = (40).$$

$$\begin{array}{r} \underline{-\frac{4x^2+1x+2}{4x^2+2x+2}} \\ \underline{\underline{4x}} \end{array}$$

$$(33) \cdot (40) = (3 \cdot 4)x^2 + (3 \cdot 0 + 3 \cdot 4)x + (3 \cdot 0) = 12x^2 + 12x + 0 \pmod{5} = \\ 2x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 1x + 4 = (14).$$

$$\begin{array}{r} \underline{-\frac{2x^2+2x+0}{2x^2+1x+1}} \\ \underline{\underline{1x+4}} \end{array}$$

$$(33) \cdot (41) = (3 \cdot 4)x^2 + (3 \cdot 1 + 3 \cdot 4)x + (3 \cdot 1) = 12x^2 + 15x + 3 \pmod{5} = \\ 2x^2 + 0x + 3 \pmod{4x^2 + 2x + 2} = 4x + 2 = (42).$$

$$\begin{array}{r} \underline{-\frac{2x^2+0x+3}{2x^2+1x+1}} \\ \underline{\underline{4x+2}} \end{array}$$

$$(33) \cdot (42) = (3 \cdot 4)x^2 + (3 \cdot 2 + 3 \cdot 4)x + (3 \cdot 2) = 12x^2 + 18x + 6 \pmod{5} = \\ 2x^2 + 3x + 1 \pmod{4x^2 + 2x + 2} = 2x + 0 = (20).$$

$$\begin{array}{r} - \frac{2x^2+3x+1}{2x^2+1x+1} \left| \begin{array}{r} 4x^2+2x+2 \\ 3 \\ 2x \end{array} \right. \end{array}$$

$$(33) \cdot (43) = (3 \cdot 4)x^2 + (3 \cdot 3 + 3 \cdot 4)x + (3 \cdot 3) = 12x^2 + 21x + 9 \pmod{5} = 2x^2 + 1x + 4 \pmod{4x^2 + 2x + 2} = 0x + 3 = (03).$$

$$\begin{array}{r} - \frac{2x^2+1x+4}{2x^2+1x+1} \left| \begin{array}{r} 4x^2+2x+2 \\ 3 \\ 3 \end{array} \right. \end{array}$$

$$(33) \cdot (44) = (3 \cdot 4)x^2 + (3 \cdot 4 + 3 \cdot 4)x + (3 \cdot 4) = 12x^2 + 24x + 12 \pmod{5} = 2x^2 + 4x + 2 \pmod{4x^2 + 2x + 2} = 3x + 1 = (31).$$

$$\begin{array}{r} - \frac{2x^2+4x+2}{2x^2+1x+1} \left| \begin{array}{r} 4x^2+2x+2 \\ 3 \\ 3x+1 \end{array} \right. \end{array}$$

**(34)**

$$(34) \cdot (00) = (3 \cdot 0)x^2 + (3 \cdot 0 + 4 \cdot 0)x + (4 \cdot 0) = 0x^2 + 0x + 0 \pmod{5} = 0x^2 + 0x + 0 \pmod{4x^2 + 2x + 2} = 0x + 0 = (00).$$

$$\begin{array}{r} - \frac{0x^2+0x+0}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 0 \end{array} \right. \end{array}$$

$$(34) \cdot (01) = (3 \cdot 0)x^2 + (3 \cdot 1 + 4 \cdot 0)x + (4 \cdot 1) = 0x^2 + 3x + 4 \pmod{5} = 0x^2 + 3x + 4 \pmod{4x^2 + 2x + 2} = 3x + 4 = (34).$$

$$\begin{array}{r} - \frac{0x^2+3x+4}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 3x+4 \end{array} \right. \end{array}$$

$$(34) \cdot (02) = (3 \cdot 0)x^2 + (3 \cdot 2 + 4 \cdot 0)x + (4 \cdot 2) = 0x^2 + 6x + 8 \pmod{5} = 0x^2 + 1x + 3 \pmod{4x^2 + 2x + 2} = 1x + 3 = (13).$$

$$\begin{array}{r} - \frac{0x^2+1x+3}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 1x+3 \end{array} \right. \end{array}$$

$$(34) \cdot (03) = (3 \cdot 0)x^2 + (3 \cdot 3 + 4 \cdot 0)x + (4 \cdot 3) = 0x^2 + 9x + 12 \pmod{5} = 0x^2 + 4x + 2 \pmod{4x^2 + 2x + 2} = 4x + 2 = (42).$$

$$\begin{array}{r} - \frac{0x^2+4x+2}{0x^2+0x+0} \left| \begin{array}{r} 4x^2+2x+2 \\ 0 \\ 4x+2 \end{array} \right. \end{array}$$

$$(34) \cdot (04) = (3 \cdot 0)x^2 + (3 \cdot 4 + 4 \cdot 0)x + (4 \cdot 4) = 0x^2 + 12x + 16 \pmod{5} = 0x^2 + 2x + 1 \pmod{4x^2 + 2x + 2} = 2x + 1 = (21)$$

$$\begin{array}{r} 0x^2+2x+1 \\ \hline 0x^2+0x+0 \\ \hline 2x+1 \end{array}$$

$$(34) \cdot (10) = (3 \cdot 1)x^2 + (3 \cdot 0 + 4 \cdot 1)x + (4 \cdot 0) = 3x^2 + 4x + 0 \pmod{5} = 3x^2 + 4x + 0 \pmod{4x^2 + 2x + 2} = 0x + 1 = (01).$$

$$\begin{array}{r} 3x^2+4x+0 \\ \hline 3x^2+4x+4 \\ \hline 1 \end{array}$$

$$(34) \cdot (11) = (3 \cdot 1)x^2 + (3 \cdot 1 + 4 \cdot 1)x + (4 \cdot 1) = 3x^2 + 7x + 4 \pmod{5} = 3x^2 + 2x + 4 \pmod{4x^2 + 2x + 2} = 3x + 0 = (30)$$

$$\begin{array}{r} 3x^2+2x+4 \\ \hline 3x^2+4x+4 \\ \hline 3x \end{array}$$

$$(34) \cdot (12) = (3 \cdot 1)x^2 + (3 \cdot 2 + 4 \cdot 1)x + (4 \cdot 2) = 3x^2 + 10x + 8 \pmod{5} = 3x^2 + 0x + 3 \pmod{4x^2 + 2x + 2} = 1x + 4 = (14).$$

$$\begin{array}{r} 3x^2+0x+3 \\ \hline 3x^2+4x+4 \\ \hline 1x+4 \end{array}$$

$$(34) \cdot (13) = (3 \cdot 1)x^2 + (3 \cdot 3 + 4 \cdot 1)x + (4 \cdot 3) = 3x^2 + 13x + 12 \pmod{5} = 3x^2 + 3x + 2 \pmod{4x^2 + 2x + 2} = 4x + 3 = (43).$$

$$\begin{array}{r} 3x^2+3x+2 \\ \hline 3x^2+4x+4 \\ \hline 4x+3 \end{array}$$

$$(34) \cdot (14) = (3 \cdot 1)x^2 + (3 \cdot 4 + 4 \cdot 1)x + (4 \cdot 4) = 3x^2 + 16x + 16 \pmod{5} = 3x^2 + 1x + 1 \pmod{4x^2 + 2x + 2} = 2x + 2 = (22).$$

$$\begin{array}{r} 3x^2+1x+1 \\ \hline 3x^2+4x+4 \\ \hline 2x+2 \end{array}$$

$$(34) \cdot (20) = (3 \cdot 2)x^2 + (3 \cdot 0 + 4 \cdot 2)x + (4 \cdot 0) = 6x^2 + 8x + 0 \pmod{5} = 1x^2 + 3x + 0 \pmod{4x^2 + 2x + 2} = 0x + 2 = (02).$$

$$\begin{array}{r} 1x^2+3x+0 \\ \hline 1x^2+3x+3 \\ \hline 2 \end{array}$$

$$(34) \cdot (21) = (3 \cdot 2)x^2 + (3 \cdot 1 + 4 \cdot 2)x + (4 \cdot 1) = 6x^2 + 11x + 4 \pmod{5} = 1x^2 + 1x + 4 \pmod{4x^2 + 2x + 2} = 3x + 1 = (31).$$

$$\begin{array}{r} \cancel{1x^2+1x+4} \mid \cancel{4x^2+2x+2} \\ \cancel{1x^2+3x+3} \mid 4 \\ 3x+1 \end{array}$$

$$(34) \cdot (22) = (3 \cdot 2)x^2 + (3 \cdot 2 + 4 \cdot 2)x + (4 \cdot 2) = 6x^2 + 14x + 8 \pmod{5} = \\ 1x^2 + 4x + 3 \pmod{4x^2 + 2x + 2} = 1x + 0 = (10).$$

$$\begin{array}{r} \cancel{1x^2+4x+3} \mid \cancel{4x^2+2x+2} \\ \cancel{1x^2+3x+3} \mid 4 \\ 1x \end{array}$$

$$(34) \cdot (23) = (3 \cdot 2)x^2 + (3 \cdot 3 + 4 \cdot 2)x + (4 \cdot 3) = 6x^2 + 17x + 12 \pmod{5} = \\ 1x^2 + 2x + 2 \pmod{4x^2 + 2x + 2} = 4x + 4 = (44).$$

$$\begin{array}{r} \cancel{1x^2+2x+2} \mid \cancel{4x^2+2x+2} \\ \cancel{1x^2+3x+3} \mid 4 \\ 4x+4 \end{array}$$

$$(34) \cdot (24) = (3 \cdot 2)x^2 + (3 \cdot 4 + 4 \cdot 2)x + (4 \cdot 4) = 6x^2 + 20x + 16 \pmod{5} = \\ 1x^2 + 0x + 1 \pmod{4x^2 + 2x + 2} = 2x + 3 = (23).$$

$$\begin{array}{r} \cancel{1x^2+0x+1} \mid \cancel{4x^2+2x+2} \\ \cancel{1x^2+3x+3} \mid 4 \\ 2x+3 \end{array}$$

$$(34) \cdot (30) = (3 \cdot 3)x^2 + (3 \cdot 0 + 4 \cdot 3)x + (4 \cdot 0) = 9x^2 + 12x + 0 \pmod{5} = \\ 4x^2 + 2x + 0 \pmod{4x^2 + 2x + 2} = 0x + 3 = (03).$$

$$\begin{array}{r} \cancel{4x^2+2x+0} \mid \cancel{4x^2+2x+2} \\ \cancel{4x^2+2x+2} \mid 1 \\ 3 \end{array}$$

$$(34) \cdot (31) = (3 \cdot 3)x^2 + (3 \cdot 1 + 4 \cdot 3)x + (4 \cdot 1) = 9x^2 + 15x + 4 \pmod{5} = \\ 4x^2 + 0x + 4 \pmod{4x^2 + 2x + 2} = 3x + 2 = (32).$$

$$\begin{array}{r} \cancel{4x^2+0x+4} \mid \cancel{4x^2+2x+2} \\ \cancel{4x^2+2x+2} \mid 1 \\ 3x+2 \end{array}$$

$$(34) \cdot (32) = (3 \cdot 3)x^2 + (3 \cdot 2 + 4 \cdot 3)x + (4 \cdot 2) = 9x^2 + 18x + 8 \pmod{5} = \\ 4x^2 + 3x + 3 \pmod{4x^2 + 2x + 2} = 1x + 1 = (11).$$

$$\begin{array}{r} \cancel{4x^2+3x+3} \mid \cancel{4x^2+2x+2} \\ \cancel{4x^2+2x+2} \mid 1 \\ 1x+1 \end{array}$$

$$(34) \cdot (33) = (3 \cdot 3)x^2 + (3 \cdot 3 + 4 \cdot 3)x + (4 \cdot 3) = 9x^2 + 21x + 12 \pmod{5} = \\ 4x^2 + 1x + 2 \pmod{4x^2 + 2x + 2} = 4x + 0 = (40).$$

$$\begin{array}{r} - \frac{4x^2+1x+2}{4x^2+2x+2} \mid \frac{4x^2+2x+2}{1} \\ \quad \quad \quad 4x \end{array}$$

$$(34) \cdot (34) = (3 \cdot 3)x^2 + (3 \cdot 4 + 4 \cdot 3)x + (4 \cdot 4) = 9x^2 + 24x + 16 \pmod{5} = \\ 4x^2 + 4x + 1 \pmod{4x^2 + 2x + 2} = 2x + 4 = (24).$$

$$\begin{array}{r} - \frac{4x^2+4x+1}{4x^2+2x+2} \mid \frac{4x^2+2x+2}{1} \\ \quad \quad \quad 2x+4 \end{array}$$

$$(34) \cdot (40) = (3 \cdot 4)x^2 + (3 \cdot 0 + 4 \cdot 4)x + (4 \cdot 0) = 12x^2 + 16x + 0 \pmod{5} = \\ 2x^2 + 1x + 0 \pmod{4x^2 + 2x + 2} = 0x + 4 = (04).$$

$$\begin{array}{r} - \frac{2x^2+1x+0}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \quad \quad \quad 4 \end{array}$$

$$(34) \cdot (41) = (3 \cdot 4)x^2 + (3 \cdot 1 + 4 \cdot 4)x + (4 \cdot 1) = 12x^2 + 19x + 4 \pmod{5} = \\ 2x^2 + 4x + 4 \pmod{4x^2 + 2x + 2} = 3x + 3 = (33).$$

$$\begin{array}{r} - \frac{2x^2+4x+4}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \quad \quad \quad 3x+3 \end{array}$$

$$(34) \cdot (42) = (3 \cdot 4)x^2 + (3 \cdot 2 + 4 \cdot 4)x + (4 \cdot 2) = 12x^2 + 22x + 8 \pmod{5} = \\ 2x^2 + 2x + 3 \pmod{4x^2 + 2x + 2} = 1x + 2 = (12).$$

$$\begin{array}{r} - \frac{2x^2+2x+3}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \quad \quad \quad 1x+2 \end{array}$$

$$(34) \cdot (43) = (3 \cdot 4)x^2 + (3 \cdot 3 + 4 \cdot 4)x + (4 \cdot 3) = 12x^2 + 25x + 12 \pmod{5} = \\ 2x^2 + 0x + 2 \pmod{4x^2 + 2x + 2} = 4x + 1 = (41).$$

$$\begin{array}{r} - \frac{2x^2+0x+2}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \quad \quad \quad 4x+1 \end{array}$$

$$(34) \cdot (44) = (3 \cdot 4)x^2 + (3 \cdot 4 + 4 \cdot 4)x + (4 \cdot 4) = 12x^2 + 28x + 16 \pmod{5} = \\ 2x^2 + 3x + 1 \pmod{4x^2 + 2x + 2} = 2x + 0 = (20).$$

$$\begin{array}{r} - \frac{2x^2+3x+1}{2x^2+1x+1} \mid \frac{4x^2+2x+2}{3} \\ \quad \quad \quad 2x \end{array}$$

$$f) (30)^{-1} = 13, (31)^{-1} = 33, (32)^{-1} = 41, (33)^{-1} = 31, (34)^{-1} = 10.$$

Таблица 7.16

$\times$	0	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	4

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

**Задача 22.** Полином  $f(x)$  задан как в задаче 21. Найти степень (по умножению) элемента поля  $GF(p^m)$  и указать, является ли заданный элемент генератором для  $GF(p^m)$ . Элемент поля  $a_1x + a_0$  задан как вектор  $a_1a_0$

Полином  $f(x) = 4x^2 + 3x + 2$ .

**22.1.** 10. **22.2.** 11. **22.3.** 12. **22.4.** 13. **22.5.** 14.

**22.6.** 20. **22.7.** 21. **22.8.** 22. **22.9.** 23. **22.10.** 24.

**22.11.** 30. **22.12.** 31. **22.13.** 32. **22.14.** 33. **22.15.** 34.

**22.16.** 40. **22.17.** 41. **22.18.** 42. **22.19.** 43. **22.20.** 44.

Полином  $f(x) = 4x^2 + 2x + 2$ .

**22.21.** 30. **22.22.** 31. **22.23.** 32. **22.24.** 33. **22.25.** 34.

**22.26.** 40. **22.27.** 41. **22.28.** 42. **22.29.** 43. **22.30.** 44.

**Пример.**  $p = 5$ ,  $m = 2$ . Найти степени (по умножению) элементов поля  $GF(p^m) = \mathbb{Z}_p[x]/(f(x))$  и указать, является ли заданный элемент генератором для  $GF(p^m)$ . Элемент поля  $a_1x + a_0$  задан как вектор  $a_1a_0 = 34 = 3x + 4$ .

Полином  $f(x) = 4x^2 + 2x + 1$ .

*Решение.*

$$(3x + 4)^1 = 3x + 4.$$

$$(3x + 4)^2 = 9x^2 + 24x + 16 = 4x^2 + 4x + 1 = 2x \pmod{f(x)}.$$

$$\begin{array}{r} 4x^2+4x+1 \\ - 4x^2+2x+1 \\ \hline 2x \end{array}$$

$$(3x + 4)^3 = 2x(3x + 4) = 6x^2 + 8x = 1 \pmod{f(x)}.$$

$$\begin{array}{r} 1x^2+3x+0 \\ - 1x^2+3x+4 \\ \hline 4 \\ 1 \end{array}$$

$$\text{ord}(3x + 4) = 3.$$

*Ответ.* Элемент  $3x + 4$  генератором не является.

$$(x + 1)^1 = x + 1.$$

$$(x+1)^2 = x^2 + 2x + 1 = 4x + 2.$$

$$\begin{array}{r} x^2+2x+1 \\ \hline x^2+3x+4 \\ \hline 4x+2 \end{array}$$

$$(x+1)^3 = (x+1)^2(x+1) = (4x+2)(x+1) = 4x^2 + x + 2 = 4x + 1.$$

$$\begin{array}{r} 4x^2+1x+2 \\ \hline 4x^2+2x+1 \\ \hline 4x+1 \end{array}$$

$$(x+1)^4 = (4x+1)(x+1) = 4x^2 + 0x + 1 = 3x.$$

$$\begin{array}{r} 4x^2+0x+1 \\ \hline 4x^2+2x+1 \\ \hline 3x \end{array}$$

$$(x+1)^5 = (3x)(x+1) = 3x^2 + 3x = 4x + 3.$$

$$\begin{array}{r} 3x^2+3x+0 \\ \hline 3x^2+4x+2 \\ \hline 4x+3 \end{array}$$

$$(x+1)^6 = (4x+3)(x+1) = 4x^2 + 2x + 3 = 2.$$

$$\begin{array}{r} 4x^2+2x+3 \\ \hline 4x^2+2x+1 \\ \hline 2 \end{array}$$

$$(x+1)^7 = (2)(x+1) = 2x + 2.$$

$$(x+1)^8 = (2x+2)(x+1) = 2x^2 + 4x + 2 = 3x + 4.$$

$$\begin{array}{r} 2x^2+4x+2 \\ \hline 2x^2+1x+3 \\ \hline 3x+4 \end{array}$$

$$(x+1)^9 = (3x+4)(x+1) = 3x^2 + 2x + 4 = 3x + 2.$$

$$\begin{array}{r} 3x^2+2x+4 \\ \hline 3x^2+4x+2 \\ \hline 3x+2 \end{array}$$

$$(x+1)^{10} = (3x+2)(x+1) = 3x^2 + 0x + 2 = x.$$

$$\begin{array}{r} 3x^2+0x+2 \\ \hline 3x^2+4x+2 \\ \hline 1x \end{array}$$

$$(x+1)^{11} = (x)(x+1) = 1x^2 + 1x = 3x + 1.$$

$$\begin{array}{r} - \ 1x^2+1x+0 \Big| 4x^2+2x+1 \\ \underline{- \ 1x^2+3x+4} \quad 4 \\ \phantom{-} \ 3x+1 \end{array}$$

$$(x + 1)^{12} = (3x + 1)(x + 1) = 3x^2 + 4x + 1 = 4.$$

$$\begin{array}{r} - \ 3x^2+4x+1 \Big| 4x^2+2x+1 \\ \underline{- \ 3x^2+4x+2} \quad 2 \\ \phantom{-} \ 4 \end{array}$$

$$(x + 1)^{13} = (4)(x + 1) = 4x + 4.$$

$$(x + 1)^{14} = (4x + 4)(x + 1) = 4x^2 + 3x + 4 = x + 3.$$

$$\begin{array}{r} - \ 4x^2+3x+4 \Big| 4x^2+2x+1 \\ \underline{- \ 4x^2+2x+1} \quad 1 \\ \phantom{-} \ x+3 \end{array}$$

$$(x + 1)^{15} = (x + 3)(x + 1) = 1x^2 + 4x + 3 = x + 4.$$

$$\begin{array}{r} - \ 1x^2+4x+3 \Big| 4x^2+2x+1 \\ \underline{- \ 1x^2+3x+4} \quad 4 \\ \phantom{-} \ x+4 \end{array}$$

$$(x + 1)^{16} = (x + 4)(x + 1) = x^2 + 5x + 4 = x^2 + 0x + 4 = 12x = 2x.$$

$$\begin{array}{r} - \ 1x^2+0x+4 \Big| 4x^2+2x+1 \\ \underline{- \ 1x^2+3x+4} \quad 4 \\ \phantom{-} \ 2x \end{array}$$

$$(x + 1)^{17} = (2x)(x + 1) = 2x^2 + 2x = x + 2.$$

$$\begin{array}{r} - \ 2x^2+2x+0 \Big| 4x^2+2x+1 \\ \underline{- \ 2x^2+1x+3} \quad 3 \\ \phantom{-} \ x+2 \end{array}$$

$$(x + 1)^{18} = (x + 2)(x + 1) = 1x^2 + 3x + 2 = 3.$$

$$\begin{array}{r} - \ 1x^2+3x+2 \Big| 4x^2+2x+1 \\ \underline{- \ 1x^2+3x+4} \quad 4 \\ \phantom{-} \ 3 \end{array}$$

$$(x + 1)^{19} = (3)(x + 1) = 3x + 3.$$

$$(x + 1)^{20} = (3x + 3)(x + 1) = 3x^2 + 6x + 3 = 2x + 1.$$

$$\begin{array}{r} - \ 3x^2+1x+3 \Big| 4x^2+2x+1 \\ \underline{- \ 3x^2+4x+2} \quad 2 \\ \phantom{-} \ 2x+1 \end{array}$$

$$(x + 1)^{21} = (2x + 1)(x + 1) = 2x^2 + 3x + 1 = 2x + 3.$$

$$\begin{array}{r} \underline{-} \ 2x^2+3x+1 \mid 4x^2+2x+1 \\ \underline{2x^2+1x+3} \\ 2x+3 \end{array}$$

$$(x+1)^{22} = (2x+3)(x+1) = 2x^2 + 5x + 3 = 4x.$$

$$\begin{array}{r} \underline{-} \ 2x^2+0x+3 \mid 4x^2+2x+1 \\ \underline{2x^2+1x+3} \\ 4x \end{array}$$

$$(x+1)^{23} = (4x)(x+1) = 4x^2 + 4x = 2x + 4.$$

$$\begin{array}{r} \underline{-} \ 4x^2+4x+0 \mid 4x^2+2x+1 \\ \underline{4x^2+2x+1} \\ 1 \end{array}$$

$$(x+1)^{24} = (2x+4)(x+1) = 2x^2 + 6x + 4 = 1.$$

$$\begin{array}{r} \underline{-} \ 2x^2+1x+4 \mid 4x^2+2x+1 \\ \underline{2x^2+1x+3} \\ 1 \end{array}$$

$\text{ord}(x+1) = 24.$

*Ответ.* Элемент  $x+1$  есть генератор поля  $GF(p^m)$ .

## КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

**Задача 23.** Шифросистема RSA (R. Rivest, A. Shamir, L. Adleman).

Вычислить ключи, зашифровать и дешифровать сообщение. Простые числа  $p$  и  $q$  определяются вариантом задания. В качестве исходного текста взять три первые латинские буквы своей фамилии.

- |                           |                           |                           |
|---------------------------|---------------------------|---------------------------|
| <b>23.1.</b> 5737, 5669.  | <b>23.2.</b> 5741, 5659   | <b>23.3.</b> 5743, 5657.  |
| <b>23.4.</b> 5749, 5653.  | <b>23.5.</b> 5779, 5651.  | <b>23.6.</b> 5783, 5647.  |
| <b>23.7.</b> 5791, 5641.  | <b>23.8.</b> 6801, 5639.  | <b>23.9.</b> 5807, 5623.  |
| <b>23.10.</b> 5813, 5591. | <b>23.11.</b> 5821, 5581. | <b>23.12.</b> 5827, 5573. |
| <b>23.13.</b> 5839, 5569. | <b>23.14.</b> 5843, 5563. | <b>23.15.</b> 5849, 5557. |
| <b>23.16.</b> 5851, 5531. | <b>23.17.</b> 5857, 5527. | <b>23.18.</b> 5861, 5521. |
| <b>23.19.</b> 5867, 5519. | <b>23.20.</b> 5869, 5507. | <b>23.21.</b> 5879, 5503. |
| <b>23.22.</b> 5881, 5501. | <b>23.23.</b> 5897, 5483. | <b>23.24.</b> 5903, 5479. |
| <b>23.25.</b> 5923, 5477. | <b>23.26.</b> 5927, 5471. | <b>23.27.</b> 5939, 5449. |
| <b>23.28.</b> 5953, 5443. | <b>23.29.</b> 5981, 5441. | <b>23.30.</b> 5987, 5437. |

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и соответствующий ему секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два различных простых числа  $p$  и  $q$  примерно одного размера.
2. Вычислить  $n = pq$  и функцию Эйлера  $\phi(n) = (p-1)(q-1)$ .
3. Выбрать случайное число  $e$ ,  $1 < e < \phi$ , такое, что НОД  $(e, \phi) = 1$ .
4. С помощью расширенного алгоритма Евклида найти такие целые  $a$ ,  $x$ , что  $ca + \phi x = 1$ . Тогда  $ea \equiv 1 \pmod{\phi}$ . Пусть произвольное  $k \in \mathbb{Z}$ . Сложив  $ea \equiv 1 \pmod{\phi}$  и  $ek\phi \equiv 0 \pmod{\phi}$ , получим  $e(a + k\phi) \equiv 1 \pmod{\phi}$ . Если  $a \notin (1, \phi)$ , то найти такое целое  $k$ , что  $(a + k\phi) \in (1, \phi)$ , и в качестве  $a$  взять  $a + k\phi$ .
5. Открытый ключ адресата  $A$  есть  $(n, e)$ . Секретный ключ для  $A$  есть  $a$ .

**Шифрование.** Адресат  $A$  пишет письмо  $t$  адресату  $B$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $(n, e)$  адресата  $B$ .
2. С помощью какого-либо метода  $M$ , который публикуется, адресат  $A$  представляет свое письмо  $t$  как сообщение в виде натурального числа  $m$  из сегмента  $[0, n-1]$ .
3. Вычислить шифротекст  $c = m^e \pmod{n}$ .
4. Отправить шифротекст  $c$  адресату  $B$ .

**Дешифрование.** Чтобы извлечь текст  $t$  из шифротекста  $c$ , адресат  $B$  должен выполнить следующее.

1. Взять свой секретный ключ  $a$  и вычислить сообщение  $m = c^a \pmod{n}$ .
2. Вычислить текст  $t$  адресата  $A$  с помощью метода  $M$ .

**Пример.** Адресат  $A$  пишет письмо  $t=НАВ$  адресату  $B$ .

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и соответствующий ему секретный ключ. Адресат  $B$  должен выполнить следующее.

1. Выбрать два различных простых числа  $p$  и  $q$  примерно одного размера  $p=499$ ,  $q=631$ .
2. Вычислить  $n = pq = 499 \cdot 631 = 314869$  и функцию Эйлера  $\varphi = \varphi(n) = (p-1)(q-1) = 313740$ .
3. Выбрать случайное число  $e = 305183 \in (1, \varphi)$  с нод  $(e, \varphi) = 1$ .
4. С помощью расширенного алгоритма Евклида найти  $a = 181967 \in (1, \varphi)$ , что  $ea = 1 \pmod{\varphi}$ .
5. Открытый ключ адресата  $B$  есть пара чисел  $(n=314869, e=305183)$ . Секретный ключ для  $B$  есть число  $a=181967$ .

**Шифрование.** Адресат  $A$  пишет письмо  $t=NAB$  адресату  $B$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $(n=314869, e=305183)$  адресата  $B$ .
2. Представить свой текст  $t=NAB$  в виде натурального числа  $m$  из  $[0, n-1]$  с помощью какого либо метода, например, с помощью 27-ричной системы счисления следующим образом. Нумеруются буквы алфавита:

пробел	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Текст  $t=NAB$  представляется в виде числа  $m = 14 \cdot 27^2 + 1 \cdot 27 + 2 = 10235$ .

3. Вычислить шифротекст

$$c = m^e \pmod{n} = 10235^{305183} \pmod{314869} = 301085.$$

4. Отправить шифротекст  $c$  адресату  $B$ .

**Дешифрование.** Чтобы извлечь текст  $t$  из шифротекста  $c$ , адресат  $B$  должен выполнить следующее.

1. Взять свой секретный ключ  $a=181967$  и вычислить сообщение  $m = c^a \pmod{n} = 301085^{181967} \pmod{314869} = 10235$ .
2. Вычислить текст  $t$  адресата  $A$  с помощью метода  $M$ , для чего представить число  $m$  в 27-ричной системе счисления:  $m = 10235_{10} = (14\ 1\ 2)_{27}$  и получить исходный текст  $t=NAB$ .

**Замечание.** 1. Текст  $t$  в компьютере представляется бинарным массивом, который рассматривается как бинарная запись некоторого числа  $m$ . Предложенный выше способ представления текста числом носит иллюстративный характер и выбран из желания оперировать с небольшими числами.

2. На практике для криптографической стойкости модуль  $n$  задается двоичным числом с 1024 и более двоичными разрядами.

**Задача 24.1.** Электронная цифровая подпись RSA с хеш-функцией. Вычислить ключи, цифровую подпись под текстом, проверить цифровую подпись. Простые числа  $p$  и  $q$  взять из задачи 23. В качестве исходного текста взять три первые латинские буквы своей фамилии.

**Замечание.** Хеш-функции  $w = h(x)$ , сопоставляет любому тексту  $x$  уникальное натуральное число  $w = h(x)$ .

Адресат  $A$  подписывает свое сообщение произвольной длины. Всякий адресат  $B$  может проверить подпись адресата  $A$  под его текстом  $t$ .

Цифровая подпись RSA, основана на использовании криптографической хэш-функции  $h: \{0,1\}^* \rightarrow \mathbb{Z}_n$ , где  $n$  есть число элементов в мультиплективной группе  $G$ . Значение хэш-функции  $h$  не больше  $n$ . Предполагается, что каждый элемент  $r$  из  $G$  может быть представлен в бинарной записи  $f(r)$  с тем, чтобы можно было вычислить значение хэш-функции  $h(f(r))$ .

Алгоритм вычисления значений хэш-функции публикуется.

Заметим, что содержимое любого файла есть некоторый текст  $t$ , представляемый в компьютере как последовательность нулей и единиц, которая есть некоторое бинарное слово  $m$  (в алфавите  $\{0,1\}$ ), являющееся бинарным набором  $m$ , составленным из кодов ASCII для последовательных символов текста  $t$ . Хеш-функция  $h$  сопоставляет бинарному набору  $m$  уникальный бинарный набор фиксированной длины (на практике это набор длины 128, 160 или 256 бит, в зависимости от выбранной хэш-функции), который может рассматриваться как двоичное число (в системе счисления по основанию 2) и которое затем, вообще говоря, можно представить числом в системе счисления по любому основанию  $h$ . В конечном итоге с помощью хэш-функции тексту  $t$  ставится в соответствие уникальное число в системе счисления по любому нужному основанию.

Значение хэш-функции есть большое число, выходящее за пределы величин целых чисел, допустимых в алгоритмических языках программирования. Mathcad, например, допускает целые (10-ричные) числа длины не более 15 цифр. Для работы с большими целыми числами с длиной десятеричной записи в 100 и более цифр приходится писать специальный программный процессор. Поэтому в последующих примерах значение хэш-функции задается искусственно, только для примера, небольшим числом.

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и соответствующий ему секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два различных простых числа  $p$  и  $q$  примерно одного размера.
2. Вычислить  $n = pq$  и функцию Эйлера  $\phi(n) = (p-1)(q-1)$ .
3. Выбрать случайное число  $e$ ,  $1 < e < \phi$ , такое, что  $\text{НОД}(e, \phi) = 1$ .
4. С помощью расширенного алгоритма Евклида найти целое  $a$ ,  $1 < a < \phi$ , для которого  $ea = 1 \pmod{\phi}$ .
5. Открытый ключ адресата  $A$  есть  $(n, e)$ . Секретный ключ для  $A$  есть  $a$ .

**Вычисление подписи.** Адресат  $A$  подписывает текст  $t$ , пользуясь своим секретным ключом. Адресат  $A$  должен выполнить следующее.

1. Представить свой текст  $t$  в виде натурального числа  $m$  с помощью какого-либо метода  $M$ .

2. Вычислить значение хеш-функции  $h = h(t)$ .

3. Вычислить подпись  $s = h^a \pmod{n}$ .

4. Отправить текст  $t$  с подписью  $s$  адресату  $B$ .

**Проверка подписи.** Чтобы проверить подпись  $s$  адресата  $A$  под его текстом  $t$ , адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(n, e)$  адресата  $A$ .

2. Способом  $M$  представить текст  $t$  в виде целого числа  $m$  из  $[0, n-1]$ .

3. Вычислить  $h = h(t) = h(m)$ . ( $h$  должно быть меньше  $n$ ).

4. Вычислить  $h_1 = s^e \pmod{n}$ .

5. Если  $h = h_1$ , то принять подпись. Если  $h \neq h_1$ , то отклонить подпись.

**Пример.** Адресат  $A$  подписывает свое сообщение  $t=DXN$ . Всякий адресат  $B$  может проверить подпись адресата  $A$  под его текстом  $t$ .

**Вычисление ключей.** Адресат  $A$  вычисляет свой открытый ключ и соответствующий ему секретный ключ. Адресат  $A$  должен выполнить следующее.

1. Выбрать два различных простых числа  $p$  и  $q$  примерно одного размера  $p=1019, q=2347$ .

2. Вычислить  $n = pq = 1019 \cdot 2347 = 2391593$  и функцию Эйлера  $\varphi = \varphi(n) = (p-1)(q-1) = 1018 \cdot 2346 = 2388228$ .

3. Выбрать случайное число  $e = 35 \in (1, \varphi)$  с НОД  $(e, \varphi) = 1$ .

4. С помощью расширенного алгоритма Евклида найти  $a = 1569407 \in (1, \varphi)$ , для которого  $ea = 1 \pmod{\varphi}$ .

5. Открытый ключ адресата  $B$  есть пара чисел  $(n=2391593, e=35)$ . Секретный ключ для  $B$  есть число  $a=1569407$ .

**Вычисление подписи.** Адресат  $A$  подписывает текст  $t=DXN$ , пользуясь своим секретным ключом. Адресат  $A$  должен выполнить следующее.

1. Представить свой текст  $t=DXN$  в виде натурального числа  $m$  из  $[0, n-1]$  с помощью какого либо метода, например, с помощью 27-ричной системы счисления:  $m = 4 \cdot 27^2 + 24 \cdot 27 + 14 = 3578$ .

2. Вычислить значение хеш-функции  $h = h(t) = h(m) = m = 3578$ .

3. Вычислить подпись  $s = h^a \pmod{n} = 3578^{1569407} \pmod{2391593} = 2146200$ .

4. Отправить текст  $t=DXN$  с подписью  $s=2146200$  адресату  $B$ .

**Проверка подписи.** Чтобы проверить подпись  $s=2146200$  адресата  $A$  под его текстом  $t=DXN$ , адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(n=2391593, e=35)$  адресата  $A$ .

2. Способом  $M$  представить текст  $t=DXN$  в виде целого числа  $m = 4 \cdot 27^2 + 24 \cdot 27 + 14 = 3578$ .

3. Вычислить  $h = h(t) = h(m) = h(3578) = 3578$ .

4. Вычислить  $h_1 = s^e \pmod{n} = 2146200^{35} \pmod{2391593} = 3578$ .

5. Принять подпись, если  $h = h_1$ , и отклонить в противном случае. Так как  $h = 3578 = h_1$ , то подпись принимается.

**Задача 24.2.** Электронная цифровая подпись RSA с возвратом сообщения. Вычислить ключи, цифровую подпись под текстом, проверить цифровую подпись и получить исходное сообщение. Простые числа  $p$  и  $q$  взять из задачи 23. В качестве исходного текста взять три первые латинские буквы своей фамилии.

Подписать сообщение с помощью электронной цифровой подписью RSA с извлечением сообщения.

Для схемы подписи RSA с извлечением сообщения требуется взаимно-однозначная функция  $R : \mathbb{N} \rightarrow \mathbb{N}$ , для которой множество  $R(\mathbb{N})$  значений  $R$  имеет характеристическое свойство, которое операция шифрования не сохраняет. В этом параграфе для этой цели возьмем, например, функцию  $R(m) = m|m$ , где  $m|m$  есть конкатенация (соединение) 10-ричных записей  $m$  и  $n$ . Например,  $12734|47590 = 127347590$ ,  $2354|2354 = 23542354$ .

Адресат  $A$  подписывает свое сообщение. Всякий адресат  $B$  может проверить подпись  $A$  и извлечь из нее сообщение от  $A$ .

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и соответствующий ему секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать два различных простых числа  $p$  и  $q$  примерно одного размера.
2. Вычислить  $n = pq$  и функцию Эйлера  $\varphi(n) = (p-1)(q-1)$ .
3. Выбрать случайное число  $e$ ,  $1 < e < \varphi$ , такое, что НОД  $(e, \varphi) = 1$ .
4. С помощью расширенного алгоритма Евклида найти целое  $a$ ,  $1 < a < \varphi$ , для которого  $ea = 1 \pmod{\varphi}$ .

5. Открытый ключ адресата  $A$  есть  $(n, e)$ . Секретный ключ для  $A$  есть  $a$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t$ . Любой адресат  $B$  может проверить подпись и извлечь из нее текст  $t$ . Адресат  $A$  должен выполнить следующее.

1. Каким-либо способом  $M$ , который публикуется, представить свой текст  $t$  в виде целого числа  $m$  из  $[0, n-1]$ .
2. Найти число  $w = R(m)$  с помощью открытой взаимно-однозначной функции  $R : [0, n-1] \rightarrow M_R$ , где есть некоторое числовое множество в  $[0, n-1]$ , например,  $R(m) = m|m$ , где  $a||b$  есть конкатенация слов  $a$  и  $b$ . Тогда  $M_R = \{w = m|m : m \in [0, n-1]\}$  есть множество всех целых десятеричных чисел из  $[0, n-1]$ , которые есть конкатенации  $m|m$  для некоторого  $m$  из  $[0, n-1]$ .
3. Найти число  $s = w^a \pmod{n}$ .
4. Отправить подписанный шифротекст  $s$  адресату  $B$ .

**Проверка подписи и вычисление сообщения.** Чтобы проверить подпись  $s$  адресата  $A$  и извлечь из нее текст  $t$ , адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(n, e)$  адресата  $A$ .
2. Найти число  $w = s^e \pmod{n}$ .
3. Проверить, что  $w \in M_R$ . Если нет, то отклонить подпись  $s$ .
4. Найти  $m = R^{-1}(w)$ .
5. С помощью метода  $M$  вычислить отправленный текст  $t$ .

**Пример.** Адресат  $A$  пишет письмо  $t=\text{НАВ}$  адресату  $B$ .

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и соответствующий ему секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать два различных простых числа  $p$  и  $q$  примерно одного размера  $p=1019, q=2347$ .
2. Вычислить  $n = pq = 1019 \cdot 2347 = 2391593$  и функцию Эйлера  $\varphi = \varphi(n) = (p-1)(q-1) = 1018 \cdot 2346 = 2388228$ .
3. Выбрать случайное число  $e = 35 \in (1, \varphi)$  с НОД  $(e, \varphi) = 1$ .
4. С помощью расширенного алгоритма Евклида найти  $a = 1569407 \in (1, \varphi)$ , что  $ea = 1 \pmod{\varphi}$ .
5. Открытый ключ адресата  $B$  есть пара чисел  $(n=2391593, e=35)$ . Секретный ключ для  $B$  есть число  $a=1569407$ .

**Вычисление подписи.** Адресат  $A$  пишет письмо  $t = \text{АВХ}$  адресату  $B$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $(n=314869, e=305183)$  адресата  $B$ .
2. Представить свой текст  $t=\text{НАВ}$  в виде натурального числа  $m$  из  $[0, n-1]$  с помощью какого либо метода, например, с помощью 27-ричной системы счисления:  $m = 1 \cdot 27^2 + 2 \cdot 27 + 24 = 807$ .
3. Вычислить  $w = R(m) = R(807) = 807||807 = 807 \cdot 1001 = 807807$ .
4. Вычислить подпись  $s = w^a \pmod{n} = 807807^{1569407} \pmod{2391593} = 794011$ .
5. Отправить шифротекст с подписью  $s$  адресату  $B$ .

**Проверка подписи и извлечение сообщения.** Чтобы извлечь текст  $t$  из шифротекста  $s$ , адресат  $B$  должен выполнить следующее.

1. Взять открытый ключ  $(n=2391593, e=35)$  адресата  $A$ .
2. Вычислить  $w = s^e \pmod{n} = 794011^{35} \pmod{2391593} = 807807$ .
3. Проверить, что  $w \in M_R$ . Так как  $w = 807807 = 807||807$  есть конкатенация двух равных слов, то подпись  $s$  принимается.
4. Найти  $m = R^{-1}(w) = R^{-1}(807807) = 807||807 = 807 \cdot 1001 = 807$ .
5. С помощью метода  $M$  вычислить  $m = (807)_{10} = (1\ 2\ 24)_{27}$  и получить исходный текст  $t=\text{АВХ}$ .

**Замечание.** 1. Есть другие более сложные функции  $R(m)$  с меньшей длиной записи значения  $R(m)$ , чем для здесь предложенной функции  $R(m)$ .

2. На практике для криптографической стойкости цифровой подписи RSA модуль  $n$  задается двоичным числом с 1024 и более двоичными разрядами.

**Задача 25.** Шифросистема ЭльГамала над числовым полем Галуа  $GF(p)$ . Вычислить ключи, зашифровать и дешифровать сообщение. В качестве простого числа взять большое число из задачи 29. В качестве исходного текста взять три первые латинские буквы своей фамилии.

**Вычисление ключей.** Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать простое  $p$  и найти генератор  $\alpha$  мультипликативной группы  $\mathbb{Z}_p^*$  целых чисел по модулю  $p$ , используя алгоритм Гаусса.

2. Выбрать случайное число  $a$  из  $[1, p-2]$ , и найти  $y = \alpha^a \pmod{p}$ .

3. Открытый ключ адресата есть тройка чисел  $(p, \alpha, y)$ . Секретный ключ адресата есть число  $a$ .

**Шифрование.** Адресат  $A$  шифрует свой текст  $t$  и отправляет его адресату  $B$ . Адресат  $B$  дешифрует сообщение от  $A$  и получает исходный текст  $t$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $(p, \alpha, y)$  адресата  $B$ .

2. С помощью какого-либо метода  $M$ , который публикуется, представить свой текст  $t$  как сообщение в виде натурального числа  $m$  из сегмента  $[0, p-1]$ .

3. Выбрать случайное число  $k$ ,  $1 \leq k \leq p-2$  (сесоновый ключ, только на один сеанс).

4. Вычислить  $\gamma = \alpha^k \pmod{p}$  и  $\delta = m \cdot (y^k) \pmod{p}$ .

5. Отправить шифротекст  $c = (\gamma, \delta)$  адресату  $B$ .

**Дешифрование.** Чтобы получить исходный текст  $t$  по  $c = (\gamma, \delta)$ , адресат  $B$  должен выполнить следующее.

1. Взять свой секретный ключ  $a$  и вычислить целое число  $\gamma^{p-1-a} \pmod{p}$ .

2. Вычислить  $m = (\gamma^{-a} \cdot \delta) \pmod{p}$ , где  $\gamma^{-a} = (\gamma^{-1})^a$ , а число  $\gamma^{-1}$  есть решение сравнения  $x \cdot \gamma \equiv 1 \pmod{p}$  и вычисляется с помощью расширенного алгоритма Евклида.

3. Вычислить исходный текст  $t$  от  $A$  с помощью метода  $M$ .

**Пример.** Адресат  $A$  шифрует свой  $t=BUJ$  и отправляет его адресату  $B$ .

**Вычисление ключей.** Адресат  $B$  должен выполнить следующее.

1. Выбрать простое  $p=2357$  и найти генератор  $\alpha=2$  для мультипликативной группы  $\mathbb{Z}_{2357}^*$ .

2. Выбрать случайное число  $a=1751$  из  $[1, p-2]$  и вычислить

$$y = \alpha^a \pmod{p} = 2^{1751} \pmod{2357} = 1185.$$

3. Открытый ключ адресата  $B$  есть тройка чисел  $(p=2357, \alpha=2, y=1185)$ . Секретный ключ адресата  $B$  есть число  $a=1751$ .

**Шифрование.** Адресат  $A$  шифрует свой текст  $t=BUJ$  и должен выполнить следующее.

1. Получить открытый ключ ( $p=2357$ ,  $\alpha=2$ ,  $y=1185$ ) для  $B$ .
  2. Представить свой текст  $t=BUJ$  в виде натурального числа  $m$  из  $[0, p-1]$ , с помощью 27-ричной системы счисления числом  $m = 2 \cdot 27^2 + 21 \cdot 27 + 10 = 2035$ .
  3. Выбрать случайное число  $k = 1520$ ,  $1 \leq k \leq p-2$  (сессионный ключ, только на один сеанс).
  4. Вычислить  $\gamma = \alpha^k \pmod{p} = 2^{1520} \pmod{2357} = 1430$ ,  
 $\delta = m \cdot \gamma^k \pmod{p} = m \cdot (\alpha^k)^k \pmod{p} = 2035 \cdot 1185^{1520} \pmod{2357} = 697$ .
  5. Послать шифротекст  $c = (\gamma=1430, \delta=697)$  адресату  $B$ .
- Дешифрование.** Чтобы дешифровать шифротекст  $c = (\gamma=1430, \delta=697)$  от  $A$ , адресат  $B$  должен выполнить следующее.
1. Вычислить  
 $\gamma^{p-1-a} \pmod{p} = 1430^{605} \pmod{2357} = 872$  и получает,  
 $m = ((\gamma^{p-1-a} \pmod{p}) \cdot \delta) \pmod{p} = 872 \cdot 697 \pmod{2357} = 2035$ .
  2. Представить число  $m$  в 27-ричной системе счисления  
 $m = 2035_{10} = (2\ 21\ 10)_{27}$  и получить исходный текст  $t=BUJ$ .

**Замечание.** Криптографическая стойкость крипtosистемы Эль-Гамаля основана на трудной практической осуществимостью проблемы нахождения дискретного логарифма в мультипликативной группе  $\mathbb{Z}_p^*$  при больших простых числах  $p$ . На практике для криптографической стойкости простое число  $p$  задается двоичным числом с 1024 и более бит (двоичными разрядами).

**Задача 26.** Электронная цифровая подпись ЭльГамаля над числовым полем Галуа  $GF(p)$ . Вычислить ключи, цифровую подпись под текстом, проверить цифровую подпись. В качестве простого числа  $p$  взять большее число из задачи 29. В качестве исходного текста взять три первые латинские буквы своей фамилии.

**Вычисление ключей.** Каждый адресат создаёт свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать случайное простое число  $p$  и найти генератор  $\alpha$  для мультипликативной группы  $\mathbb{Z}_p^*$ .
2. Выбрать произвольное число  $a$ ,  $1 \leq a \leq p-2$ .
3. Вычислить  $y = \alpha^a \pmod{p}$ .
4. Открытый ключ для адресата  $A$  есть тройка чисел  $(p, \alpha, y)$ . Секретный ключ адресата есть число  $a$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t$  (произвольной длины). Любой адресат  $B$  может проверить подпись адресата  $A$  под его текстом  $t$ . Адресат  $A$  должен выполнить следующее.

1. Вычислить значение хеш-функции  $h(t)$ .
2. Выбрать случайное секретное целое число  $k$  из  $[1, p-2]$  такое, что  $\text{nод}(k, p-1) = 1$  (сессионный ключ, только на один сеанс).

3. Вычислить  $k^{-1} \pmod{(p-1)}$ .
  4. Вычислить  $r = \alpha^k \pmod{p}$ .
  5. Вычислить  $s = k^{-1} \cdot (h(t) - a \cdot r) \pmod{(p-1)}$ . Если разность  $h(t) - a \cdot r < 0$ , то к этой разности прибавить модуль  $p-1$ .
  6. Подпись адресата  $A$  под его текстом  $t$  есть пара  $(r, s)$ .
- Проверка подписи.** Чтобы проверить подпись  $(r, s)$  адресата  $A$  под его текстом  $t$ , адресат  $B$  должен выполнить следующее.
1. Получить открытый ключ  $(p, \alpha, y)$  адресата  $A$ .
  2. Вычислить значение хеш-функции  $h(t)$ .
  3. Проверить, что  $r \in [1, p-1]$ ; если нет, отклонить подпись.
  4. Вычислить  $v_1 = y^r \cdot r^s \pmod{p}$ .
  5. Вычислить  $v_2 = \alpha^{h(m)} \pmod{p}$ .
  6. Принять подпись, если  $v_1 = v_2$ , и отклонить в противном случае.

**Пример.** Адресат  $A$  подписывает свой текст  $t=\text{FIL}$ . Любой адресат  $B$  может проверить подпись  $A$  под его текстом  $t$ .

**Вычисление ключей.** Адресат  $A$  должен выполнить следующее.

1. Выбрать простое число  $p=5903$  и найти генератор  $\alpha=2$  мультипликативной группы  $\mathbb{Z}_p^*$  целых чисел по модулю  $p$ .
2. Выбрать случайное целое  $a=1751$  из  $[1, p-2]$ .
3. Вычислить  $y = \alpha^a \pmod{p} = 2^{1751} \pmod{5903} = 5395$ .
4. Открытый ключ адресата  $A$  есть тройка  $(p=5903, \alpha=2, y=5395)$ . Секретный ключ адресата  $A$  есть число  $a=1751$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t=\text{FIL}$  и для этого должен выполнить следующее.

1. Представить свой текст  $t=\text{FIL}$  в виде натурального числа  $m$  из  $[0, p-1]$ , с помощью 27-ричной системы счисления числом  $m = 6 \cdot 27^2 + 9 \cdot 27 + 12 = 4629$ .
2. Вычислить значение хеш-функции  $h(t)$ . Пусть для примера  $h(t) = h(m) = m = 4629$ .
3. Выбрать случайное секретное число  $k=1529$  из  $[1, p-2]$ , для которого  $\text{нод}(k, p-1) = 1$  (сессийный ключ, только на один сеанс).
4. Вычислить  $k^{-1} \pmod{p-1} = 1529^{-1} \pmod{5902} = 1903$ .
5. Вычислить  $r = \alpha^k \pmod{p} = 2^{1529} \pmod{5903} = 2373$ .
6. Вычислить  $s = k^{-1} \cdot (h(t) - ar) \pmod{(p-1)} = 1529^{-1} \cdot (4629 - 1751 \cdot 2373) \pmod{5902} = 2732$ .
7. Подпись  $A$  под текстом  $t$  есть пара  $(r=2373, s=2732)$ .

**Проверка подписи.** Чтобы проверить подпись  $(r=2373, s=2732)$  адресата  $A$  под его текстом  $t=\text{FIL}$ , адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(p=5903, \alpha=2, y=5395)$  адресата  $A$ .
2. Представить присланный текст  $t=\text{FIL}$  в виде натурального числа  $m$  из  $[0, p-1]$  с помощью 27-ричной системы счисления числом  $m = 6 \cdot 27^2 + 9 \cdot 27 + 12 = 4629$ .
2. Вычислить значение хеш-функции  $h(t) = h(m) = m = 4629$ .

3. Проверить, что  $r = 2373 \in [1, p-1] = [1, 5902]$ . Если нет, то отклонить подпись.

4. Вычислить число  $v_1 = y^r r^s \pmod{p} = 5395^{2373} \cdot 2373^{2732} \pmod{5903} = 4197$ .

5. Вычислить число  $v_2 = \alpha^{h(t)} \pmod{p} = 2^{4629} \pmod{5903} = 4197$ .

6. Принять подпись, ибо  $v_1 = 4197 = v_2$ .

**Замечание.** Для криптографической стойкости рекомендуется брать  $p$  длиной 1024 и более бит.

**Задача 27.** Полиномиальная шифросистема ЭльГамаля над полиномиальном полем Галуа  $GF(p^m)$ . Вычислить ключи, зашифровать и дешифровать сообщение. В качестве исходного текста взять три первые латинские буквы своей фамилии. Взять простое число  $p=31$ , натуральное число  $m=3$ . Неприводимый (он же примитивный) полином над  $\mathbb{Z}_p$  определяется номером варианта. В качестве исходного текста взять три первые латинские буквы своей фамилии.

$$27.1. \quad x^3 + x + 14.$$

$$27.4. \quad x^3 + 2x + 7.$$

$$27.7. \quad x^3 + 3x + 20.$$

$$27.10. \quad x^3 + 4x + 28.$$

$$27.13. \quad x^3 + 5x + 28.$$

$$27.16. \quad x^3 + 6x + 28.$$

$$27.19. \quad x^3 + 7x + 28.$$

$$27.22. \quad x^3 + 9x + 14.$$

$$27.25. \quad x^3 + 10x + 14.$$

$$27.28. \quad x^3 + 11x + 18.$$

$$27.2. \quad x^3 + x + 19.$$

$$27.5. \quad x^3 + 2x + 14.$$

$$27.8. \quad x^3 + 4x + 7.$$

$$27.11. \quad x^3 + 5x + 14.$$

$$27.14. \quad x^3 + 6x + 9.$$

$$27.17. \quad x^3 + 7x + 7.$$

$$27.20. \quad x^3 + 8x + 14.$$

$$27.23. \quad x^3 + 9x + 19.$$

$$27.26. \quad x^3 + 11x + 7.$$

$$27.29. \quad x^3 + 12x + 14$$

$$27.3. \quad x^3 + x + 28.$$

$$27.6. \quad x^3 + 3x + 18.$$

$$27.9. \quad x^3 + 4x + 19.$$

$$27.12. \quad x^3 + 5x + 19.$$

$$27.15. \quad x^3 + 6x + 10.$$

$$27.18. \quad x^3 + 7x + 19.$$

$$27.21. \quad x^3 + 8x + 19.$$

$$27.24. \quad x^3 + 10x + 7.$$

$$27.27. \quad x^3 + 11x + 10.$$

$$27.30. \quad x^3 + 12x + 20.$$

Числовая схема шифрования ЭльГамаля может быть обобщена для работы в любой конечной циклической группе  $G$ . Криптографическая стойкость схемы ЭльГамаля в группе  $G$  основана на трудности решения проблемы дискретного логарифма в  $G$ . Группа  $G$  должна удовлетворять следующим условиям:

1. *Эффективность*, то есть групповые операции в  $G$  должны вычисляться относительно просто.

2. *Криптографическая стойкость*, то есть решение проблемы дискретного логарифма в  $G$  должно быть практически неосуществимой.

Ниже следуют удовлетворяющие этим двум условиям группы, первые три из которых наиболее употребительны.

1. Мультипликативная группа  $\mathbb{Z}_p^*$  целых чисел по модулю простого числа  $p$ .

2. Группа обратимых элементов  $\mathbb{Z}_n^*$ , где  $n$  есть составное целое число.

3. Мультипликативная группа  $\mathbb{Z}_q^*$  конечного поля  $\mathbb{F}_q$ , где  $q=p^s$ ,  $p$  есть простое число,  $s$  есть положительное целое число.

4. Группа точек эллиптической кривой над конечным полем.

5. Якобиан гиперэллиптической кривой над конечным полем.
6. Класс групп мнимого и вещественного квадратичных полей.
7. Группы кос.

Адресат  $A$  шифрует свой текст  $t$  и посыпает его адресату  $B$ .  $B$  дешифрует сообщение от  $A$  и получает исходный текст  $t$ .

**Вычисление ключей.** Каждый адресат создаёт свой открытый ключ и ему соответствующий секретный ключ. Адресат  $A$  должен выполнить следующее.

1. Выбрать подходящую (мультипликативную) циклическую группу  $G$  порядка  $n$ .

2. Вычислить какой либо генератор  $\alpha$  группы  $G$ .

3. Выбрать случайное целое число  $a$ ,  $1 \leq a \leq n-1$ .

4. Вычислить элемент  $y = \alpha^a$  группы  $G$ .

5. Открытый ключ адресата есть пара  $(\alpha, y)$  элементов группы  $G$ . Открыто также описание умножения элементов в  $G$ . Секретный ключ для  $A$  есть  $a$ .

**Шифрование.** Адресат  $A$  шифрует свой текст  $t$  и отправляет адресату  $B$ . Адресат  $A$  должен выполнить следующее.

1. Каким-либо методом  $M$  (который публикуется) представить свой текст  $t$  как элемент  $m$  группы  $G$ .

2. Получить открытый ключ  $(\alpha, y)$  адресата  $B$ .

3. Выбрать случайное целое число  $k$ ,  $1 \leq k \leq n-1$  (сеансовый ключ, только на один сеанс).

4. Вычислить  $\gamma = \alpha^k$  и  $\delta = m \cdot y^k$ .

5. Отправить шифротекст  $c = (\gamma, \delta)$  адресату  $B$ .

**Дешифрование.** Чтобы получить исходный текст  $t$  по  $c = (\gamma, \delta)$ , адресат  $B$  должен выполнить следующее:

1. Взять свой секретный ключ  $a$ , вычислить  $\gamma^{-a}$  и найти  $\gamma^a = (\gamma^a)^{-1}$ .

2. Вычислить  $m = (\gamma^{-a}) \cdot \delta$ .

3. Вычислить исходный текст  $t$  от  $A$  с помощью метода  $M$ .

**Замечание.** Все адресаты могут выбрать одну и ту же циклическую группу  $G$  и ее генератор  $\alpha$ .

**Пример.** Шифросистема Эль-Гамаля с мультипликативной группой  $G$  конечного полиномиального поля  $GF(p^s)$ .

**Вычисление ключей.** Адресат  $B$  должен выполнить следующее.

1. Выбрать мультипликативную группу  $G$  конечного полиномиального поля, например, поля  $GF(p^s)$ ,  $p=13$ ,  $s=4$ , элементы которого представляются полиномами из  $\mathbb{Z}_{13}[x]$  над  $\mathbb{Z}_{13}$  степени меньше 4, и умножение в котором выполняется по модулю неприводимого полинома  $f(x) = (a_4 a_3 a_2 a_1 a_0)_{13} = (1 0 1 0 2)_{13} = x^4 + x^2 + 2$ . Группа  $G$  имеет порядок (число элементов)  $n = p^s - 1 = 13^4 - 1 = 28560$ .

2. Найти генератор  $\alpha = x+5 = (0 0 1 5)$  группы  $G$ .

3. Выбрать случайное число  $a=2 \in [1, n-1]$ .

4. Вычислить  $y = \alpha^a = \alpha^2 = (x+5)^2 \pmod{f(x)} = x^2 + 10x + 12 = (0 1 10 12)_{13}$ .

5. Открытый ключ для  $B$  есть пара  $(\alpha^a = (0 \ 0 \ 1 \ 5)_{13}, y = (0 \ 1 \ 10 \ 12)_{13})$  элементов группы  $G$ . Секретный ключ для  $A$  есть число  $a=2$ .

**Шифрование.** Адресат  $A$  шифрует свой текст  $t=\text{ZAM}$  и должен выполнить следующее.

1. Представить свой текст  $t=\text{ZAM}$  числом каким-либо методом  $M$ , например, в 27-ричной системе счисления  $u=26 \cdot 27^2 + 1 \cdot 27 + 13 = 18994_{10}$ , а затем вычислить 13-ричное представление числа  $u$  в виде сообщения  $m=(8 \ 8 \ 5 \ 1)_{13}$ , рассматриваемом как полином  $8x^3+8x^2+5x+1$  из  $\mathbb{Z}_{13}[x]$ .

2. Получить открытый ключ  $(\alpha = (0 \ 0 \ 1 \ 5), y = (0 \ 1 \ 10 \ 12))$  адресата  $B$ .

3. Выбрать произвольное целое число  $k=2134$ ,  $1 \leq k \leq n-1$ , (сессионный ключ, только на один сеанс).

4. Вычислить следующие элементы из  $G$ .

$$\begin{aligned}\gamma &= \alpha^k = (0 \ 0 \ 1 \ 5)^{2134} = (x+5)^{2134} \pmod{f(x)} = 8x^3+9x^2+7x+5 = (8 \ 9 \ 7 \ 5)_{13}, \\ y^k &= (0 \ 1 \ 10 \ 12)^{2134} = (x^2+10x+12)^{2134} \pmod{f(x)} = 10x^3+12x^2+3x+1 = \\ &= (10 \ 12 \ 3 \ 1)_{13}, \\ \delta &= m \cdot y^k = (8 \ 8 \ 5 \ 1) \cdot (10 \ 12 \ 3 \ 1) = (8x^3+8x^2+5x+1) \cdot (10x^3+12x^2+3x+1) \pmod{f(x)} \\ &= 4x^3+6x^2+7x+1 = (4 \ 6 \ 7 \ 3)_{13}.\end{aligned}$$

5. Отправить шифротекст  $c = (\gamma = (8 \ 9 \ 7 \ 5), \delta = (4 \ 6 \ 7 \ 3))$  адресату  $B$ .

**Дешифрование.** Чтобы получить исходный текст  $t$  по  $c$  адресат  $B$  должен выполнить следующее.

1. Пользуясь своим секретным ключом  $a=2$ , вычислить следующие элементы группы  $G$ .

$$\begin{aligned}\gamma^a &= (8 \ 9 \ 7 \ 5)^2 = (8x^3+9x^2+7x+5)^2 \pmod{f(x)} = 10x^3+12x^2+3x+1 = (10 \ 12 \ 3 \ 1)_{13}, \\ \gamma^{-a} &= (\gamma^a)^{-1} = (10 \ 12 \ 3 \ 1)^{-1} = (10x^3+12x^2+3x+1)^{-1} \pmod{f(x)} = \\ &= 5x^3+7x^2+6x+11 = (5 \ 7 \ 6 \ 11)_{13}.\end{aligned}$$

2. Вычислить в группе  $G$  элемент

$$\begin{aligned}m &= \gamma^{-a} \cdot \delta = (5 \ 7 \ 6 \ 11) \cdot (4 \ 6 \ 7 \ 3) = \\ &= (5x^3+7x^2+6x+11) \cdot (4x^3+6x^2+7x+1) \pmod{f(x)} = 8x^3+8x^2+5x+1 = (8 \ 8 \ 5 \ 1)_{13}.\end{aligned}$$

3. Чтобы получить текст  $t$  по элементу  $m$ , произвести следующие вычисления.

$$m = (8 \ 8 \ 5 \ 1)_{13} = 8 \cdot 13^3 + 8 \cdot 13^2 + 5 \cdot 13 + 1 = 18994_{10} = (26 \ 1 \ 13)_{27}, \text{ откуда текст } t=\text{ZAM}.$$

**Задача 28.** Полиномиальная электронная цифровая подпись ЭльГамаля над полиномиальным полем Галуа  $GF(p^m)$ . Вычислить ключи, цифровую подпись под текстом, проверить цифровую подпись. Взять простое число  $p=31$ , натуральное число  $m=3$ . Неприводимый полином над  $\mathbb{Z}_p$  взять из задачи 27. В качестве исходного текста взять три первые латинские буквы своей фамилии.

Схема электронной цифровой подписи Эль-Гамаля, основанная на мультиплексивной группе  $\mathbb{Z}_p^*$ , может быть обобщена на любую конечную

абелеву группу  $G$ . Алгоритм подписи использует криптографическую хеш-функцию  $h: \{1,0\}^* \rightarrow \mathbb{Z}_n$ , где  $n$  есть число элементов в  $G$ . Предполагается, что каждый элемент  $r$  из  $G$  может быть представлен в бинарной записи  $f(r)$ , с тем, чтобы можно было вычислить значение хеш-функции  $h(f(r))$ .

Алгоритм вычисления хеш-функции публикуется.

Криптографическая стойкость подписи основана на трудной практической осуществимости проблемы нахождения дискретного логарифма в группе  $G$  большого порядка.

При использовании схемы цифровой подписи Эль-Гамаля по тексту  $t$  вычисляется значение хеш-функции  $h(t)$  которая затем используется при вычислении и проверке цифровой подписи под текстом сообщения.

**Вычисление ключей.** Каждый адресат создаёт свой открытый ключ и ему соответствующий секретный ключ. Адресат  $A$  должен выполнить следующее.

1. Выбрать подходящую (мультипликативную) циклическую группу  $G$  порядка  $n$ .

2. Вычислить какой либо генератор  $\alpha$  группы  $G$ .

3. Выбрать случайное целое число  $a$ ,  $1 \leq a \leq n-1$ .

4. Вычислить элемент  $y = \alpha^a$  группы  $G$ .

5. Открытый ключ адресата есть пара  $(\alpha, y)$  элементов группы  $G$ . Открыто также описание умножения элементов в  $G$ . Секретный ключ адресата есть  $a$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t$  (произвольной длины). Любой адресат  $B$  может проверить подпись адресата  $A$  под его текстом  $t$ . Адресат  $A$  должен выполнить следующее.

1. Каким-либо методом  $M$  (который публикуется) представить свой текст  $t$  как элемент  $m$  группы  $G$  и вычислить  $h(m)$ .

2. Выбрать случайное целое число  $k$  из  $[1, n-1]$ , для которого  $\text{nод}(k, n) = 1$  (сессийный ключ, только на один сеанс).

3. Вычислить целое число  $k^{-1}(\text{mod } n)$ .

4. Вычислить элемент  $r = \alpha^k$  группы  $G$ .

5. Вычислить значение хеш-функции  $h(r)$ .

6. Вычислить число  $s = k^{-1} \cdot (h(m) - a \cdot h(r)) \pmod{n}$ .

7. Подпись адресата  $A$  под его текстом  $t$  есть пара  $(r, s)$ .

**Проверка подписи.** Чтобы проверить подпись  $(r, s)$  адресата  $A$  под его текстом  $t$ , адресат  $B$  должен выполнить следующее:

1. Представить текст  $t$  с помощью метода  $M$  числом  $m$  группы  $G$  и вычислить  $h(m)$ .

2. Получить открытый ключ  $(\alpha, y)$  адресата  $A$ .

3. Вычислить значение хеш-функции  $h(r)$ .

4. Вычислить в группе  $G$  элементы  $v_1 = (\alpha^{a \cdot h(r)}) \cdot r^s$  и  $v_2 = \alpha^{h(m)} \cdot r^s$ .

5. Принять подпись, если  $v_1 = v_2$  и отклонить в противном случае.

**Пример.** Схема электронной цифровой подписи Эль-Гамаля с мультипликативной группой конечного поля  $GF(p^s)$ ,  $p=13$ ,  $s=4$ . Пусть для удобства элемент поля представляется  $p$ -ричным стрингом  $(a_4 a_3 a_2 a_1 a_0)$ .

Адресат  $A$  подписывает свой текст  $t$  (произвольной длины). Любой адресат  $B$  может проверить подпись  $A$ .

**Вычисление ключей.** Адресат  $A$  должен выполнить следующее.

1. Выбрать мультиликативную группу  $G$  конечного поля, например, поля  $GF(p^s)$ ,  $p=13$ ,  $s=4$ , элементы которого представляются полиномами из  $\mathbb{Z}_{13}[x]$  над  $\mathbb{Z}_{13}$  степени меньше 4, и умножение в котором выполняется по модулю неприводимого полинома  $f(x) = (a_4 \ a_3 \ a_2 \ a_1 \ a_0)_{13} = (1 \ 0 \ 1 \ 0 \ 2)_{13} = x^4 + x^2 + 2$ . Группа  $G$  имеет порядок (число элементов)  $n = p^s - 1 = 13^4 - 1 = 28560$ .

2. Найти генератор  $\alpha = x+5 = (0 \ 0 \ 1 \ 5)$  группы  $G$ .

3. Выбрать случайное число  $a=2 \in [1, n-1]$ .

4. Вычисляет  $y = \alpha^a = \alpha^2 = (x+5)^2 \pmod{f(x)} = x^2 + 10x + 12 = (0 \ 1 \ 10 \ 12)_{13}$ .

5. Открытый ключ для  $A$  есть пара  $(\alpha^a = (0 \ 0 \ 1 \ 5)_{13}, y = (0 \ 1 \ 10 \ 12)_{13})$  элементов группы  $G$ . Секретный ключ для  $A$  есть число  $a=2$ .

**Вычисление подписи.** Пользуясь своим секретным ключом  $a=2$ , адресат  $A$  подписывает свой текст  $t=RUS$  и должен выполнить следующее.

1. Представить текст  $t=RUS$  числом каким-либо методом  $M$ , например, в 27-ричной системе счисления следующим образом.

$$m = 18 \cdot 27^2 + 21 \cdot 27 + 19 = 13708_{10}.$$

2. Выбрать случайное целое число  $k = 2141$  из  $[1, n-1]$ , для которого  $\text{nод}(k, n) = 1$  (сессийный ключ, только на один сеанс).

3. Вычислить целое число  $k^{-1} \pmod{n} = 2141^{-1} \pmod{n} = 16421_{10}$ .

4. Вычислить в группе  $G$  элемент  $r = \alpha^k = (0 \ 0 \ 1 \ 5)^{2141} = (x+5)^{2141} \pmod{f(x)} = 3x^3 + 8x^2 + 4 = (3 \ 8 \ 0 \ 4)_{13}$ .

5. Вычислить значение хеш-функции  $h(r)$ , например, следующим образом. По  $r = (3 \ 8 \ 0 \ 4)$  вычислить 10-ричное число  $(3 \ 8 \ 0 \ 4)_{13} = 3 \cdot 13^3 + 8 \cdot 13^2 + 4 = 7947_{10}$ . Пусть  $h(r) = 7947_{10}$ .

6. Вычислить в  $\mathbb{Z}_n$  число  $s = k^{-1} \cdot (h(t) - a \cdot h(r)) \pmod{n} = 1642 \cdot (13708 - 2 \cdot 7947) \pmod{n} = 3614_{10}$ .

7. Подпись адресата  $A$  под его текстом  $t$  есть пара  $(r=(3 \ 8 \ 0 \ 4)_{13}, s=3614_{10})$ .

**Проверка подписи.** Чтобы проверить подпись  $(r, s)$  адресата  $A$  под его текстом  $t$ , адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(\alpha=(0 \ 0 \ 1 \ 5)_{13}, y=(0 \ 1 \ 10 \ 12)_{13})$  адресата  $A$ .

2. Представить текст  $t = RUS$  с помощью метода  $M$  числом

$$m = 18 \cdot 27^2 + 21 \cdot 27 + 19 = 13708_{10}.$$

3. Пусть, например, хеш-функция  $h(t) = h(m) = m$ . Тогда  $h(RUS) = h(13708) = 13708_{10}$ .

4. Вычислить значение хеш-функции  $h(r) = h((3 \ 8 \ 0 \ 4)_{13}) = 3 \cdot 13^3 + 8 \cdot 13^2 + 4 = 7947_{10}$ .

5. Вычислить в группе  $G$  элементы

$v_1 = y^{h(r)} \cdot r^s = (0 \ 1 \ 10 \ 12)^{7947} \cdot (3 \ 8 \ 0 \ 4)^{3614} = (x^2 + 10x + 12)^{7947} \cdot (3x^3 + 8x^2 + 4)^{3614} \pmod{f(x)} = 6x^3 + 2x^2 + 5x + 12 = (6 \ 2 \ 5 \ 12)_{13}$ ,

$v_2 = \alpha^{h(m)} = (0 \ 0 \ 1 \ 5)^{13708} = (x+5)^{13708} \pmod{f(x)} = 6x^3 + 2x^2 + 5x + 12 = (6 \ 2 \ 5 \ 12)_{13}$ ,

6. Так как  $v_1 = (6 \ 2 \ 5 \ 12) = v_2$ , то подпись принимается.

**Замечание.** При вычислении подписи используются вычисления в группе  $G$  и вычисления в  $\mathbb{Z}_n$ . При проверке подписи используются только вычисления в группе  $G$ .

**Задача 29.** Электронная цифровая подпись DSA (Digital Signature Algorithm) над числовым полем Галуа  $GF(p)$ . Простые числа  $p$  и  $q$  определяются вариантом задания.

- |                               |                              |                               |
|-------------------------------|------------------------------|-------------------------------|
| <b>29.1.</b> 1350551, 27011.  | <b>29.2.</b> 378239, 27017.  | <b>29.3.</b> 270311, 27031.   |
| <b>29.4.</b> 324517, 27043.   | <b>29.5.</b> 541181, 27059.  | <b>29.6.</b> 324733, 27061.   |
| <b>29.7.</b> 433073, 27067.   | <b>29.8.</b> 812191, 27073.  | <b>29.9.</b> 487387, 27077.   |
| <b>29.10.</b> 325093, 27091.  | <b>29.11.</b> 813091, 27103. | <b>29.12.</b> 379499, 27107.  |
| <b>29.13.</b> 325309, 27109.  | <b>29.14.</b> 488287, 27127. | <b>29.15.</b> 868577, 27143.  |
| <b>29.16.</b> 326149, 27179.  | <b>29.17.</b> 489439, 27191. | <b>29.18.</b> 979093, 27197.  |
| <b>29.19.</b> 489799, 27211.  | <b>29.20.</b> 326869, 27239. | <b>29.21.</b> 272411, 27241.  |
| <b>29.22.</b> 1635181, 27253. | <b>29.23.</b> 490663, 27259. | <b>29.24.</b> 1090841, 27271. |
| <b>29.25.</b> 272771, 27277.  | <b>29.26.</b> 491059, 27281. | <b>29.27.</b> 436529, 27283.  |
| <b>29.28.</b> 873569, 27299.  | <b>29.29.</b> 491923, 27329. | <b>29.30.</b> 492067, 27337.  |
| <b>29.31.</b> 328333, 27361.  |                              |                               |

**Вычисление ключей.** Каждый адресат создаёт свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать случайное простое число  $q$ ,  $2^{159} < q < 2^{160}$ .
2. Выбрать число  $t$ ,  $0 \leq t \leq 8$ , и случайное простое число  $p$ ,  $2^{511+64t} < p < 2^{512+64t}$  такое, что  $q$  делит  $p-1$ .
3. Найти генератор  $\alpha \in \mathbb{Z}_p^*$  для циклической подгруппы порядка  $q$  в группе  $\mathbb{Z}_p^*$ . Для этого  $A$  должен сделать следующее.
  - 3.1. Выбрать случайный элемент  $g \in \mathbb{Z}_p^*$  и найти  $\alpha = g^{(p-1)/q} \pmod{p}$ .
  - 3.2. Если  $\alpha = 1$ , то перейти к шагу 3.1 с другим  $g$ .
  4. Выбрать произвольное число  $a$ ,  $1 \leq a \leq q-1$ .
  5. Вычислить  $y = \alpha^a \pmod{p}$ .
  6. Открытый ключ адресата есть  $(p, q, \alpha, y)$ . Секретный ключ адресата есть число  $a$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t$  произвольной длины. Любой адресат  $B$  может проверить подпись  $A$  с помощью открытого ключа адресата  $A$ . Адресат  $A$  должен выполнить следующее.

1. Выбрать произвольное секретное число  $k$ ,  $0 < k < q$ , (сеансовый ключ, только на один сеанс).
2. Вычислить  $r = (\alpha^k \pmod{p})(\pmod{q})$ .
3. Вычислить  $k^{-1} \pmod{p}$ .

4. Вычислить  $s = k^{-1} \cdot (h(m) + a \cdot r) \pmod{q}$ , где  $h(m): (0,1)^* \rightarrow \mathbb{Z}_p$  есть некоторая хеш-функция (публикуется на сайте).

5. Подпись адресата  $A$  есть пара чисел  $(r, s)$ .

**Проверка подписи.** Чтобы проверить подпись  $(r, s)$  адресата  $A$  под его текстом  $t$ , адресат  $B$  должен выполнить следующее.

1. Взять открытый ключ  $(p, q, \alpha, y)$  адресата  $A$ .

2. Проверить, что  $0 < r < q$  и  $0 < s < q$ . Если нет, то отклонить подпись.

3. Вычислить  $w = s^{-1} \pmod{q}$  и  $h(m)$ .

4. Вычислить  $h(t)$ .

5. Вычислить  $u_1 = w \cdot h(t) \pmod{q}$  и  $u_2 = r \cdot w \pmod{q}$ .

6. Вычислить  $v = (\alpha^{u_1} \cdot y^{u_2}) \pmod{p}$ .

7. Принять подпись, если  $v = r$  и отклонить в противном случае.

**Пример.** Адресат  $A$  подписывает свой текст  $t$  и всякий адресат  $B$  может проверить подпись  $A$ .

**Вычисление ключей.** Адресат  $A$  создаёт свой открытый ключ и ему соответствующий секретный ключ. Адресат  $A$  должен сделать следующее.

1. Выбрать случайное простое число  $q = 27367$ .

2. Выбрать случайное простое число  $p = 656809$ , для которого  $q$  делит  $(p-1)$ . Тогда  $(p-1)/q = 24$ .

3. Выбрать случайный элемент  $g = 2732$  из  $\mathbb{Z}_p^*$  и вычислить  $\alpha = g^{(p-1)/q} \pmod{p} = 2732^{24} \pmod{656809} = 68909$ . Так как  $\alpha \neq 1$ , то  $\alpha$  есть генератор для единственной циклической подгруппы порядка  $q$  в группе  $\mathbb{Z}_p^*$ . (Если  $\alpha = 1$ , то следует выбрать другое  $g$ ).

4. Выбрать случайное число  $a = 80$  из  $[1, q-1]$ .

5. Вычислить  $y = \alpha^a \pmod{p} = 68909^{80} \pmod{656809} = 50951$ .

6. Открытый ключ адресата  $A$  есть  $(p=656809, q=27367, \alpha=68909, y=50951)$ . Секретный ключ адресата есть число  $a = 80$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t=\text{BAN}$ , пользуясь своим секретным ключом  $a=80$ . Адресат  $A$  должен выполнить следующее.

1. Представить текст  $t=\text{BAN}$  числом каким-либо методом  $M$ , например, в 27-ричной системе счисления следующим образом.

$$m = 2 \cdot 27^2 + 1 \cdot 27 + 14 = 1499_{10}.$$

2. Вычислить значение хеш-функции. Пусть, для примера,  $h(t) = h(m) = m$ . Тогда  $h(t) = h(\text{BAN}) = h(1499) = 1499$ .

3. Выбрать случайное целое число  $k = 74$  из  $[0, q]$ , для которого  $\text{нод}(k, q) = 1$  (сеансовый ключ, только на один сеанс).

4. Вычислить  $k^{-1} \pmod{p} = 74^{-1} \pmod{p} = 21080$ .

5. Вычислить  $r = (\alpha^k \pmod{p})(\pmod{q}) = (68909^{74} \pmod{656809})(\pmod{27367}) = 145325 \pmod{27367} = 8490$ .

5. Вычислить  $s = k^{-1} \cdot (h(t) + ar) \pmod{q} =$

$$21080 \cdot (1499 + 80 \cdot 8490) \pmod{27367} = 14746.$$

6. Подпись адресата  $A$  под текстом  $t$  есть пара чисел ( $r=8490, s=14746$ ).

**Проверка подписи.** Чтобы проверить подпись ( $r=8490, s=14746$ ) адресата  $A$  под текстом  $t=BAN$ , адресат  $B$  должен выполнить следующее.

1. Взять открытый ключ адресата  $A$  ( $p = 656809, q = 27367, \alpha = 68909, y = 50951$ ).

2. Представить текст  $t=BAN$  числом каким-либо методом  $M$ , например, в 27-ричной системе счисления следующим образом.

$$m = 2 \cdot 27^2 + 1 \cdot 27 + 14 = 1499_{10}.$$

3. Вычислить значение хеш-функции  $h(t) = h(m) = m$ . Тогда  $h(t) = h(BAN) = h(1499) = 1499$ .

4. Проверить, что  $r=8490 \in [0, q] = [0, 27367], s=14746 \in [0, q] = [0, 27367]$ .

Если проверка не проходит, то подпись отклонить.

5. Вычислить  $w = s^{-1} \pmod{q} = 14746^{-1} \pmod{27367} = 15699$ .

6. Вычислить

$$u_1 = w \cdot h(t) \pmod{q} = 15699 \cdot 1499 \pmod{27367} = 24548,$$

$$u_2 = r \cdot w \pmod{q} = 8490 \cdot 15699 \pmod{27367} = 7220.$$

5. Вычислить  $v = (\alpha^{u_1} \cdot y^{u_2} \pmod{p}) \pmod{q} = (68909^{24548} \cdot 50951^{7220} \pmod{656809}) \pmod{27367} = (280146 \cdot 334407 \pmod{656809}) \pmod{27367} = 145325 \pmod{27367} = 8490$ .

6. Принять подпись, так как  $v = 8490 = r$ .

Для криптографической стойкости рекомендуется брать  $q$  длиной 160 бит, размер  $p$  при любом кратном 64 лежит между 512 (лучше 768) и 1024 бит включительно.

**Задача 30.** Шифросистема Рабина. Простые числа  $p$  и  $q$  определяются вариантом задания задачи 23.

Желательное свойство схемы шифрования есть наличие доказательства, что взлом схемы так же труден, как и трудность решения какой-либо другой известной трудно вычислимой проблемы, например, проблемы факторизации целых чисел или проблемы вычисления дискретного алгоритма. Есть пока недоказанное предположение, что взлом схемы RSA так же труден, как трудность факторизации целых чисел. Схема Рабина была первой схемой с доказанной трудностью взлома, равной трудности факторизации.

**Вычисление ключей.** Каждый адресат создаёт (вычисляет) свой открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два различных случайных простых числа  $p$  и  $q$  примерно одного размера.

2. Вычислить  $n = pq$ .

3. Открытый ключ адресата есть  $n$ . Секретный ключ адресата есть  $(p, q)$ .

**Шифрование.** Пользуясь открытым ключом  $n$  адресата  $B$ , адресат  $A$  шифрует свой текст  $t$ . Адресат  $A$  должен выполнить следующее.

1. Взять открытый ключ  $n$  адресата  $B$ .

2. С помощью какого-либо метода  $M$ , который публикуется, адресат  $A$

представляет своё письмо  $t$  как сообщение в виде натурального числа  $m$  сегмента  $[0, n-1]$ .

3. Вычислить  $c = m^2 \pmod{n}$ .

4. Послать свой шифротекст  $c$  адресату  $B$ .

**Дешифрование.** Пользуясь своим секретным ключом  $(p, q)$ , адресат  $B$  дешифрует сообщение  $c$  от  $A$ . Адресат  $B$  должен выполнить следующее.

1. Решить уравнение  $c = m^2 \pmod{n}$  и найти четыре квадратных корня  $m_1, m_2, m_3, m_4$  по модулю  $n$ . (Число  $c$  имеет один или два корня из  $c$  по модулю  $n$ , если  $\text{нод}(m, n) \neq 1$ , что возможно с очень малой вероятностью).

2. Посланное адресатом  $A$  сообщение  $m$  есть одно из чисел  $m_1, m_2, m_3, m_4$ . Адресат  $B$  каким-либо способом распознаёт (позже мы покажем как), какое из чисел  $m_1, m_2, m_3, m_4$  есть посланное  $m$ .

**Замечание.** Если  $p$  и  $q$  выбраны сравнимыми с 3 по модулю 4, то алгоритм вычисления четырех квадратных корней из  $c$  по модулю  $n$  можно упростить следующим образом.

1. Используя расширенный алгоритм Евклида, найти такие целые  $a$  и  $b$ , что  $ap + bq = 1$ .

2. Вычислить  $r = c^{(p+1)/4} \pmod{p}$ .

3. Вычислить  $s = c^{(q+1)/4} \pmod{q}$ .

4. Вычислить  $x = (aps + bqr) \pmod{n}$ .

5. Вычислить  $y = (aps - bqr) \pmod{n}$ .

6. Четыре квадратных корня из  $c$  по модулю  $n$  есть  $x, -x, y, -y$ .

**Пример.** Адресат  $A$  посыпает текст  $t=RAB$  адресату  $B$ .

**Вычисление ключей.** Адресат  $B$  должен выполнить следующее.

1. Выбрать два различных простых числа  $p=2131, q=2437$ .

2. Вычислить  $n = pq = 5193247$ .

3. Открытый ключ адресата  $B$  есть число  $n=5193247$ . Секретный ключ адресата  $B$  есть пара чисел  $(p=2131, q=2437)$ .

**Шифрование.** Пользуясь открытым ключом для  $B$ , адресат  $A$  шифрует свой текст  $t=RAB$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $n=5193247$  адресата  $B$ .

2. Представить текст  $t=RAB$  числом каким-либо методом  $M$ , например, в 27-ричной системе счисления следующим образом.

$$m = 18 \cdot 27^2 + 1 \cdot 27 + 2 = 13151_{10}.$$

3. Удваивает в  $m=13151$  слово из двух последних цифр 51 и получает  $m1 = 1315151$ . Значение функции  $R(m)$  есть число  $m$  с приписанными к  $m$  двумя последними цифрами числа  $m$ . Можно взять и другую функцию  $R(m)$ .

4. Вычислить  $c = m1^2 \pmod{n} = 1315151^2 \pmod{5193247} = 852957$ .

5. Отправить шифротекст  $c=852957$  адресату  $B$ .

**Дешифрование.** Пользуясь своим секретным ключом  $(p=2131, q=2437)$ , адресат  $B$  дешифрует сообщение  $c=852957$  от  $A$ . Адресат  $B$  должен выполнить следующее.

1. Используя алгоритм вычисления дискретного квадратного корня по модулю  $n=p \cdot q$ , где  $p$  и  $q$  есть простые числа, решить сравнение  $c = m^2 \pmod{n}$

относительно  $m$ , то есть найти четыре квадратных корня из  $c$  по модулю  $n$ :

$$m_1 = 1315151, m_2 = -1315151, m_3 = 2050346, m_4 = -2050346.$$

2. Прибавить к отрицательным корням модуль  $n$ . Тогда

$$m_1 = 1315151, m_2 = 3878096, m_3 = 2050346, m_4 = 3142901.$$

Так как только  $m_1$  имеет справа два одинаковых двухбуквенных слова, то  $B$  дешифрует  $c$  как  $R^{-1}(m_1)$  и получает  $m = 13151_{10}$ .

3. Представить число  $m$  в 27-ричной системе счисления

$$m = 13151_{10} = (18\ 1\ 2)_{27} \text{ и получить исходный текст } t=RAB.$$

**Замечание.** Шифрование по схеме Рабина является довольно быстрой операцией, ибо используется только одна модульная операция возведения в квадрат. Дешифрование по Рабину медленнее чем шифрование, однако сопоставимо по скорости с дешифрованием по схеме RSA.

На практике для криптографической стойкости модуль  $n$  задается двоичным числом с 1024 и более бит.

**Задача 31.** Электронная цифровая подпись Рабина с извлечением сообщения. Простые числа  $p$  и  $q$  определяются вариантом задания задачи 23.

Цифровая подпись по схеме Рабина, подобна цифровой подписи по схеме RSA. Пространство подписей  $M_S$  есть  $Q_n$  (множество квадратичных вычетов по модулю  $n$ ) и подписи есть квадратные корни из них. Взаимно-однозначная функция  $R$  из пространства сообщений  $M$  в пространство подписей  $M_S$  публикуется.

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два различных случайных простых числа  $p$  и  $q$  примерно одного размера.

2. Вычислить  $n = pq$ .

3. Публикуемая функция  $R$  определяется следующим образом. Если число  $m$  есть подписываемое сообщение, то  $R(m)$  есть ближайшее к  $m$  число, для которого существуют четыре различных корня  $\sqrt{R(m)} \pmod{n}$ . (Такое число существует). При этом  $R(m) > m$ , если четыре корня  $\sqrt{R(m)} \pmod{n}$  для  $m < n$  существуют и  $R(m) < m$ , в противном случае.

4. Открытый ключ адресата есть  $n$ . Секретный ключ адресата есть  $(p, q)$ .

**Вычисление подписи.** Пользуясь своим секретным ключом  $(p, q)$ , адресат  $A$  подписывает свой текст  $t$ . Адресат  $A$  должен выполнить следующее.

1. Представить свой текст  $t$  в виде натурального числа  $m$  с помощью какого-либо метода  $M$ .

1. Вычислить  $w = R(m)$  и  $i = R(m) - m$ .

2. Вычислить  $s = \sqrt{w} \pmod{n}$ .

3. Подпись  $A$  (включающая текст  $t$ ) есть число  $s$ .

**Проверка подписи.** Пользуясь открытым ключом  $n$  для  $A$ , любой адресат  $B$  может проверить подпись  $s$  адресата  $A$  и извлечь из подписи  $s$  сообщение  $t$

от A. Адресат B должен выполнить следующее.

1. Получить открытый ключ n адресата A.
2. Вычислить  $w = s^2 \pmod{n}$ .
3. Проверить, что  $w \in M_R$ . Если нет, то отклонить подпись A.
4. Получить  $m = R^{-1}(w)$  и найти текст t.

**Пример. Вычисление ключей.** Адресат A должен выполнить следующее.

1. Выбрать два различных случайных простых числа  $p=1699$  и  $q=1597$  примерно одного размера.

2. Вычислить  $n = pq = 1699 \cdot 1597 = 2713303$ .

3. Открытый ключ для A есть число  $n=2713303$ . Секретный ключ для A есть пара чисел ( $p=1699$ ,  $q=1597$ ).

**Вычисление подписи.** Пользуясь своим секретным ключом ( $p=1699$ ,  $q=1597$ ), адресат A подписывает свой текст  $t=RAD$ . Адресат A должен выполнить следующее.

1. Представить свой текст  $t=RAD$  числом каким-либо методом M, например, в 27-ричной системе счисления следующим образом.

$$m1 = 18 \cdot 27^2 + 1 \cdot 27 + 4 = 13153_{10}.$$

2. Взять правое слово из двух букв в m1, приписать его к m1 справа и получить  $m = 1315353$ . (Можно взять какую-либо другую взаимно-однозначную функцию для преобразования числа m1).

3. Вычислить  $w = R(m)$  как ближайшее к  $m=1315353$  число, для которого существуют четыре различных корня  $\sqrt{R(m)} \pmod{n}$ , и получить  $w = R(m) = R(1315353) = 1315358$ ;  $i = R(m)-m = 1315358 - 1315353 = 5$ .

4. Вычислить  $s1 = \sqrt{w} \pmod{n} = \sqrt{1315358} \pmod{2713303} = (2264649, -2264649, 399147, -399147)$ .

5. К каждой отрицательной компоненте в s1 прибавить модуль n и получить  $s = (2264649, 4486546, 399147, 2314156)$ .

6. Подпись адресата A есть любое число в s и число i, например, ( $s=2314156$ ,  $i=5$ ).

**Проверка подписи.** Чтобы проверить подпись ( $s=2314156$ ,  $i=5$ ) адресата A и извлечь из s текст t, адресат B должен выполнить следующее.

1. Получить открытый ключ  $n=3185549$  адресата A.
2. Вычислить  $w = s^2 \pmod{n} = 2314156^2 \pmod{3185549} = 1315358$ ,  $m = w-i = 1315358-5 = 1315353$ .
3. Так как m справа имеет сдвоенное двухбуквенное слово 53, то подпись принимается.
4.  $m1 = 13153_{10} = (18 1 4)_{27}$  и потому текст  $t=RAD$ .

**Задача 32.** Модифицированная электронная цифровая подпись Рабина с извлечением сообщения. Простое число  $p = 1811$ ,  $\text{mod}(p, 4) = 3$ . Простые числа  $q$  с  $\text{mod}(q, 4) = 3$  определяются вариантом задания.

- 32.1.** 1823. **32.2.** 1831. **32.3.** 1847. **32.4.** 1871. **32.5.** 1879. **32.6.** 1951.  
**32.7.** 1999. **32.8.** 2039. **32.9.** 2063. **32.10.** 2087. **32.11.** 2111. **32.12.** 2143.

**32.13.** 2207. **32.14.** 2239. **32.15.** 2287. **32.16.** 2311. **32.17.** 2351. **32.18.** 2383.

**32.19.** 2399. **32.20.** 2423. **32.21.** 2447. **32.22.** 2503. **32.23.** 2543. **32.24.** 2551.

**32.25.** 2591. **32.26.** 2647. **32.27.** 2663. **32.28.** 2671. **32.29.** 2687. **32.30.** 2711.

Представленная здесь техника подобна технике в цифровой подписи ISO/IEC 9796. Последняя предлагает детерминированный метод для связи сообщения с элементами пространства подписей  $M_S$  с таким расчетом, чтобы вычисление квадратного корня (или чего-то близкого к корню) было всегда возможно.

**Утверждение.** Пусть  $p$  и  $q$  есть различные простые числа, каждое из которых сравнимо с 3 по модулю 4. Пусть  $n = pq$ .

1. Если  $\text{нод}(x, n) = 1$ , то  $x^{(p-1)(q-1)/2} \equiv 1 \pmod{n}$ .
2. Если  $x \in Q_n$  (множество квадратичных вычетов по модулю  $n$ ), то  $x^{(n-p-q+5)/8} \pmod{n}$  есть  $\sqrt{x} \pmod{n}$ .
3. Если  $x$  есть целое, для которого символ Якоби  $\left(\frac{x}{n}\right) = 1$ , и если  $d = (n-p-q+5)/8$ , то  $x^{2d} \pmod{n} = \begin{cases} x, & \text{если } x \in Q_n, \\ n-x, & \text{если } x \notin Q_n. \end{cases}$
4. Если  $p \not\equiv q \pmod{8}$ , то  $\left(\frac{2}{n}\right) = -1$  и потому умножение любого целого  $x$  на 2 или на  $2^{-1} \pmod{n}$  обращает символ Якоби для  $x$ . (Целые вида  $n = pq$ , где  $p \equiv q \equiv 3 \pmod{4}$  и  $p \not\equiv q \pmod{8}$  иногда называют целыми Вильямса.)

Пространство сообщений  $M = \{m \in \mathbb{Z}_n : m \leq \lfloor (n-6)/16 \rfloor\}$ .  
Подписываемое пространство  $M_S = \{m \in \mathbb{Z}_n : m \equiv 6 \pmod{16}\}$ .  
Пространство подписей  $S = \{s \in \mathbb{Z}_n : s^2 \pmod{n} \in M_S\}$ .

Функция  $R(m) = 16m + 6 \quad \forall m \in M$ .

$M_R = \{m \in \mathbb{Z}_n : m \equiv 6 \pmod{16}\}$  есть множество значений для  $R$ .

**Вычисление ключей.** Каждый адресат вычисляет свой открытый ключ и соответствующий секретный ключ. Каждый адресат должен сделать следующее.

1. Выбрать два различных случайных простых числа  $p \equiv 3 \pmod{8}$ ,  $q \equiv 7 \pmod{8}$  примерно одного размера.
2. Вычислить  $n = pq$ .
3. Вычислить  $d = (n-p-q+5)/8$ .
4. Открытый ключ адресата есть  $n$ . Секретный ключ адресата есть число  $d$ .

**Вычисление подписи.** Адресат  $A$  представляет свой текст  $t$  в виде сообщения (числа) и подписывает его. Любой адресат  $B$  может проверить подпись адресата  $A$  и извлечь из подписи текст  $t$ . Адресат  $A$  должен сделать следующее.

1. Представить свой текст  $t$  в виде натурального числа  $m \leq \lfloor (n-6)/16 \rfloor$  с помощью какого-либо метода  $M$ .
2. Вычислить  $w = R(m) = 16m + 6$ .

3. Вычислить символ Якоби  $J = \left(\frac{w}{n}\right)$ .

4. Если  $J = 1$ , то вычислить  $s = w^d \pmod{n}$ .

5. Если  $J = -1$ , то вычислить  $s = (w/2)^d \pmod{n}$ .

Если  $J \neq 1$  или  $-1$ , то  $J = 0$  и потому  $\text{нод}(w,n) \neq 1$ . Это потребует факторизации числа  $n$ . Вероятность факторизации большого  $n$  на практике ничтожно мала.

6. Подпись адресата  $A$  есть число  $s$ .

**Проверка подписи.** Чтобы проверить подпись  $s$  адресата  $A$  и извлечь из  $s$  текст  $t$ , адресат  $B$  должен сделать следующее.

1. Получить открытый ключ  $n$  адресата  $A$ .

2. Вычислить  $u = s^2 \pmod{n}$ .

3. Если  $u \equiv 6 \pmod{8}$ , то взять  $w = u$ .

4. Если  $u \equiv 3 \pmod{8}$ , то взять  $w = 2u$ .

5. Если  $u \equiv 7 \pmod{8}$ , то взять  $w = n-u$ .

6. Если  $u \equiv 2 \pmod{8}$ , то взять  $w = 2(n-u)$ .

7. Если  $w \in M_R$ , принять подпись. Если нет, отклонить подпись.

8. Получить  $m = R^{-1}(w) = (w-6)/16$ .

**Доказательство.** Подпись  $s$  зависит от знака символа Якоби для  $v = w$  и  $v = w/2$ . Только одно из  $w$ ,  $w/2$  имеет символ Якоби 1. Значение  $v$  таково, что  $v = 3$  или  $6 \pmod{8}$ . Число  $s \pmod{n}$  равно  $v$  или  $n-v$  в зависимости от принадлежности или непринадлежности  $v$  к  $Q_n$ . Последнее может быть установлено, ибо  $n \equiv 5 \pmod{8}$ .

**Пример (Модифицированная схема подписи Рабина).**

**Вычисление ключей.** Адресат  $A$  должен выполнить следующее.

1. Выбрать два различных случайных простых числа  $p=1811 \equiv 3 \pmod{8}$ ,  $q=1759 \equiv 7 \pmod{8}$  примерно одного размера.

2. Вычислить  $n = pq = 1811 \cdot 1759 = 3185549$ .

3. Вычислить  $d = (n-p-q+5)/8 = (3185549-1811-1759+5)/8 = 397748$ .

4. Открытый ключ для  $A$  есть  $n=3185549$ . Секретный ключ для  $A$  есть число  $d=397748$ .

**Вычисление подписи.** Адресат  $A$  подписывает свой текст  $t=RAB$  и делает следующее.

1. Представляет свой текст  $t=RAB$  в виде натурального числа  $m$  с помощью какого-либо метода, например, с помощью 27-ричной системы счисления:

$$m = 18 \cdot 27^2 + 1 \cdot 27 + 2 = 13151.$$

2. Вычислить  $w = R(m) = 16m+6 = 16 \cdot 13151+6 = 210422$ .

3. Вычислить символ Якоби  $J = \left(\frac{w}{n}\right) = \left(\frac{210422}{3185549}\right) = -1$ .

4. Так как  $J = -1$ , то найти  $s = (w/2)^d \pmod{n} = (210422/2)^{397748} \pmod{3185549} = 548579$ .

5. Подпись адресата  $A$  под сообщением  $m$  есть  $s=548579$ .

**Проверка подписи.** Чтобы проверить подпись  $s=548579$  адресата  $A$  и

извлечь из  $s$  текст  $t$ , адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $n=3185549$  адресата  $A$ .
2. Вычислить  $u = s^2 \pmod{n} = 548579^{3185549} \pmod{3185549} = 105211$ .
3. Так как  $u \equiv 3 \pmod{8}$ , то берет  $w = 2u = 2 \cdot 105211 = 210422$ .
4. Так как  $w \equiv 6 \pmod{16}$  и  $w \in M_R$ , то принять подпись.
5. Получить  $m = R^{-1}(w) = (w-6)/16 = (105211-6)/16 = 13151$ .
6. Получить  $m = 13151_{10} = (18\ 1\ 2)_{27}$  и текст  $t = RAB$ .

**Замечание.** (Образцы значений параметров для ISO/IEC 9796)

Следующая таблица приводит образцы значений параметров в процессе получения подписи для 150-битового сообщения и 1024-битовой подписи.

Параметр	$k$ (бит)	$d$ (бит)	$z$ (байт)	$r$ (бит)	$t$ (байт)
Значение	1024	150	19	3	64

**Задача 33.** Вероятностная схема шифрования Голдвассер–Микали.

Простые числа  $p$  и  $q$  определяются вариантом задания из задачи 23.

Минимальное требование криптографической стойкости схемы шифрования есть трудность несанкционированного дешифрования перехваченного шифротекста. Иногда желательны более сильные требования к криптографической стойкости схемы.

Схемы RSA, Рабина, рюкзачные схемы шифрования детерминированы в том смысле, что при фиксированном открытом ключе исходный текст  $m$  всегда шифруется в один и тот же шифротекст  $c$ . Детерминированная схема может иметь, например, следующие недостатки.

1. Схема не стойка для всех возможных исходных текстов. Например, схема RSA, сообщения 0 и 1 шифруются в 0 и 1 соответственно.

2. Иногда по шифротексту о шифровке можно получить частичную информацию. Например, если в RSA шифротекст  $c = m^e \pmod{n}$  соответствует исходному тексту  $m$ , то при нечетном  $n$  символ Яакби

$$\left(\frac{c}{n}\right) = \left(\frac{m}{n}\right)^e = \left(\frac{m}{n}\right) \text{ дает некоторую информацию о сообщении } m.$$

3. Два одинаковых шифротекста соответствуют двум одинаковым исходным текстам.

*Вероятностное шифрование* использует рандомизацию для получения очень высокой степени стойкости.

**Определение.** Схема шифрования с открытым ключом *полиномиально стойка*, если противник не может в полиномиальное время выбрать два текста  $m_1$  и  $m_2$  и затем правильно отличить шифротексты для  $m_1$  и  $m_2$  с вероятностью значительно больше  $1/2$ .

**Определение.** Схема шифрования с открытым ключом *семантически стойка*, если для всякого сообщения, если противник может в полиномиальное время получить частичную информацию об исходном тексте по шифротексту, то он может ее вычислить также в полиномиальное время без шифротекста.

Интуитивно, схема шифрования с открытым ключом семантически стойка,

если по шифротексту нельзя в полиномиальное время получить частичную информацию об исходном тексте.

**Утверждение.** Схема шифрования с открытым ключом семантически стойка, если и только если она полиномиально стойка.

### **Вероятностная схема шифрования Голдвассер–Микали**

Вероятностная схема шифрования Голдвассер–Микали семантически стойка в предположении трудности решения проблемы квадратичного вычета.

Криптографическая стойкость схемы основана на трудности вычисления (дискретного) квадратного корня.

**Вычисление ключей.** Каждый адресат вычисляет открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два различных случайных простых числа  $p$  и  $q$  примерно одного размера.

2. Вычислить  $n = pq$ .

3. Выбрать в  $\mathbb{Z}_n$  квадратичный невычет  $u$  по модулю  $n$ , для которого

символ Якоби  $\left(\frac{y}{n}\right) = 1$  (то есть  $y$  есть псевдоквадрат по модулю  $n$ ). Для этого сначала (случайным подбором с использованием символа Лежандра) находят квадратичный невычет  $a$  по модулю  $p$  и квадратичный невычет  $b$  по модулю  $q$ . Затем с помощью алгоритма Гаусса вычисляют такое целое  $y$ ,  $0 \leq y \leq n-1$ , что  $y \equiv a \pmod{p}$  и  $y \equiv b \pmod{q}$ . Так как  $y$  есть квадратичный невычет по модулю  $p$ , то  $y$  есть квадратичный невычет по модулю  $n$ . По свойствам

символов Лежандра и Якоби  $\left(\frac{y}{n}\right) = \left(\frac{y}{p}\right) \cdot \left(\frac{y}{q}\right) = (-1) \cdot (-1) = 1$ . То есть  $y$  есть псевдоквадрат по модулю  $n$ .

4. Открытый ключ адресата есть пара  $(n, y)$ . Секретный ключ адресата есть пара  $(p, q)$ .

**Шифрование.** Адресат  $A$  шифрует свой текст  $t$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $(n, y)$  адресата  $B$ .

2. Представить свой текст  $t$  каким-либо методом как бинарный стринг  $m = m_0 m_1 \dots m_t$  длины  $t$ .

3. Для  $i$  от 0 до  $t$  выполнить следующее.

3.1. Взять случайное число  $x \in \mathbb{Z}_n$ .

3.2. Если  $m_i = 1$ , то  $c_i := ux^2 \pmod{n}$ . Иначе  $c_i := x^2 \pmod{n}$ .

4. Послать шифротекст  $c = (c_1, c_2, \dots, c_t)$  адресату  $B$ .

**Дешифрование.** Адресат  $B$  дешифрует сообщение  $c = (c_1, c_2, \dots, c_t)$  от  $A$ , пользуясь открытым ключом для  $A$ . Адресат  $B$  должен выполнить следующее.

1. Для  $i$  от 0 до  $t$  выполнить следующее.

1.1. Вычислить символ Лежандра  $e_i = \left(\frac{c_i}{p}\right)$ .

1.2. Если  $e_i = 1$ , то  $m_i := 0$ . Иначе  $m_i := 1$ .

2. Положить  $m = m_1 m_2 \dots m_t$ .

3. Методом  $M$  восстановить текст  $t$ .

**Доказательство.** Если бит  $m_i = 0$ , то  $c_i := x^2 \pmod{n}$  есть квадратичный вычет по модулю  $n$ . Если бит  $m_i = 1$ , то так как  $y$  есть псевдоквадрат по модулю  $n$ , то  $c_i = yx^2 \pmod{n}$  есть тоже псевдоквадрат по модулю  $n$ . Число  $c_i$  есть квадратичный вычет по модулю  $n$ , если и только если  $c_i$  есть

квадратичный вычет по модулю  $p$ , то есть если символ Лежандра  $\left(\frac{c_i}{p}\right) = 1$ .

Так как  $B$  знает  $p$ , то он может вычислить этот символ Лежандра и получить бит  $m_i$ .

**Пример.** Адресат  $A$  пишет письмо адресату  $B$ .

**Вычисление ключей.** Адресат  $A$  должен выполнить следующее.

1. Выбрать два различных случайных простых числа  $p = 499$  и  $q = 631$  примерно одного размера.

2. Вычислить  $n = pq = 499 \cdot 631 = 314869$ .

3. Выбрать в  $\mathbb{Z}_n$  квадратичный невычет  $y$  по модулю  $n = 314869$ , для которого символ Якоби  $\left(\frac{y}{n}\right) = 1$ . Для этого сначала найти квадратичный невычет  $a = 7$  по модулю  $p = 499$  и квадратичный невычет  $b = 3$  по модулю  $q = 631$ . Затем с помощью алгоритма Гаусса вычислить целое  $y = 76354$ ,  $0 \leq y \leq n - 1$ , такое, что  $y \equiv a \pmod{p}$  и  $y \equiv b \pmod{q}$ .

4. Открытый ключ адресата  $A$  есть пара  $(n = 314869, y = 135460)$ . Секретный ключ адресата  $A$  есть пара  $(p = 499, q = 631)$ .

**Шифрование.** Пользуясь открытым ключом адресата  $B$ , адресат  $A$  шифрует свой текст  $t = \text{BLM}$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $(n = 314869, y = 135460)$  адресата  $B$ .

2. Представить свой текст  $t = \text{BLM}$  в виде натурального числа с помощью, например, 27-ричной системы счисления:  $m = 2 \cdot 27^2 + 12 \cdot 27 + 13 = 1795$ . Затем по основанию 2 представить  $m = 1795$  как бинарный стринг  $m = m_0 m_1 \dots m_t = 11100000011_2$  длины  $t = 10$ .

3. Для  $i$  от 0 до 10 взять случайные числа  $x_i$  из  $\mathbb{Z}_n$  и вычислить соответствующие  $c_i$ .

$$x_0 = 233486, c_0 = y \cdot x_0^2 \pmod{n} = 206861, \text{ ибо } m_0 = 1,$$

$$x_1 = 148997, c_1 = y \cdot x_1^2 \pmod{n} = 252056, \text{ ибо } m_1 = 1,$$

$$x_2 = 294740, c_2 = y \cdot x_2^2 \pmod{n} = 236339, \text{ ибо } m_2 = 1,$$

$$x_3 = 144311, c_3 = x_3^2 \pmod{n} = 229061, \text{ ибо } m_3 = 0,$$

$$x_4 = 150802, c_4 = x_4^2 \pmod{n} = 144548, \text{ ибо } m_4 = 0,$$

$x_5 = 178883$ ,  $c_5 = x_5^2 \pmod{n} = 250695$ , ибо  $m_5 = 0$ ,  
 $x_6 = 214657$ ,  $c_6 = x_6^2 \pmod{n} = 13058$ , ибо  $m_6 = 0$ ,  
 $x_7 = 25787$ ,  $c_7 = x_7^2 \pmod{n} = 280910$ , ибо  $m_7 = 0$ ,  
 $x_8 = 100889$ ,  $c_8 = x_8^2 \pmod{n} = 135027$ , ибо  $m_8 = 0$ ,  
 $x_9 = 109032$ ,  $c_9 = y \cdot x_9^2 \pmod{n} = 31370$ , ибо  $m_9 = 1$ ,  
 $x_{10} = 249721$ ,  $c_{10} = y \cdot x_{10}^2 \pmod{n} = 264850$ , ибо  $m_{10} = 1$ .

4. Послать шифротекст  $c = (c_0, c_1, \dots, c_t)$  адресату  $B$ .

**Дешифрование.** Адресат  $B$  дешифрует шифротекст  $c = (c_0, c_1, \dots, c_t)$ , пользуясь своим секретным ключом. Адресат  $B$  должен выполнить следующее.

1. Для  $i$  от 0 до  $t=10$  выполнить следующее.

1.1. Вычислить символ Лежандра  $e_i = \left(\frac{c_i}{p}\right)$ .

1.2. Если  $e_i = 1$ , то  $m_i := 0$ . Иначе  $m_i := 1$ .

$e_i = -1, -1, -1, 1, 1, 1, 1, 1, -1, -1$ .

$m_i = 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1$ .

2. Положить  $m = m_0 m_1 \dots m_{t=10} = 11100000011_2$ .

3. Методом  $M$  восстановить текст  $t$  следующим образом.

$$m = \sum_{i=0}^{t=10} m_{t-i} \cdot 2^i = 1795_{10} = (2\ 12\ 13)_{27}. \text{ Текст } t=\text{BLM}.$$

**Задача 34.** Вероятностная схема шифрования Блюма–Голдвассер. Простые числа  $p$  и  $q$  с  $\text{mod}(p, 4) = \text{mod}(q, 4) = 3$  определяются вариантом задания.

**34.01.** 503,523. **34.02.** 563,471. **34.03.** 547,587. **34.04.** 563,599. **34.05.** 571,607.  
**34.06.** 587,619. **34.07.** 599,631. **34.08.** 607,643. **34.09.** 619,647. **34.10.** 631,659.  
**34.11.** 643,683. **34.12.** 647,691. **34.13.** 659,719. **34.14.** 683,727. **34.15.** 691,739.  
**34.16.** 719,643. **34.17.** 727,751. **34.18.** 399,787. **34.19.** 743,811. **34.20.** 751,823.  
**34.21.** 787,827. **34.22.** 811,839. **34.23.** 823,859. **34.24.** 827,869. **34.25.** 839,883.  
**34.21.** 859,887. **34.22.** 863,907. **34.23.** 883,911. **34.24.** 887,919. **34.25.** 907,947.

Вероятностная схема шифрования Блюма–Голдвассер есть наиболее эффективная из известных вероятностных схем шифрования, по эффективности сравнимая со схемой шифрования RSA. Она семантически стойка в предположении трудности проблемы факторизации. Схема использует Блюм–Блюм–Шуб генератор для порождения псевдослучайной битовой последовательности, которая затем покоординатно XOR-суммируется с исходным текстом. Результирующая битовая последовательность вместе с шифрованием случайного "зерна" передается получателю, который использует свою информацию, чтобы вычислить "зерно", реконструировать псевдослучайную битовую последовательность и исходный текст.

Криптографическая стойкость схемы основана на трудности факторизации

натуральных чисел.

**Вычисление ключей.** Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать два больших случайных различных примерно одного размера простых числа  $p$  и  $q$ , сравнимых с 3 по модулю 4.
2. Вычислить  $n = pq$ .
3. Использовать расширенный алгоритм Евклида и вычислить целые  $a$  и  $b$ , для которых  $ap + bq = 1$ .
4. Открытый ключ адресата есть число  $n$ . Секретный ключ адресата есть набор  $(p, q, a, b)$ .

**Шифрование.** Пользуясь открытым ключом для  $B$ , адресат  $A$  шифрует свое сообщение  $m$  к  $B$ . Адресат  $A$  должен выполнить следующее.

1. Получить открытый ключ  $n$  адресата  $B$ .
2. При  $k = \lfloor \log_2 n \rfloor$  и  $h = \lfloor 3\log_2 k \rfloor$  представить свое сообщение  $m$  как стринг  $m = m_1m_2\dots m_t$  длины  $t$ , где каждое  $m_i$  есть бинарный стринг длины  $h$ .
3. Выбрать в качестве "зерна"  $x_0$  случайный квадратичный вычет по модулю  $n$ , взяв, например, случайное число  $r \in \mathbb{Z}_n$  и положив  $x_0 := r^2 \pmod{n}$ .
4. Для  $i$  от 1 до  $t$  выполнить следующее.
  - 4.1. Вычислить  $x_i = (x_{i-1} - 1) \pmod{n}$ .
  - 4.2. Пусть  $r_i$  есть  $h$  наименьших значащих бит в бинарном представлении числа  $x_i$ .
  - 4.3. Вычислить  $c_i = r_i \oplus m_i$ .
  5. Вычислить  $x_{t+1} = x_t^2 \pmod{n}$ .
  6. Послать шифротекст  $c = (c_1, c_2, \dots, c_t, x_{t+1})$  адресату  $B$ .

**Дешифрование.** Пользуясь своим секретным ключом, адресат  $B$  дешифрует шифротекст  $c$  от  $A$ . Адресат  $B$  должен выполнить следующее.

1. Вычислить  $d_1 = ((p+1)/4)^{t+1} \pmod{(p-1)}$ .
2. Вычислить  $d_2 = ((q+1)/4)^{t+1} \pmod{(q-1)}$ .
3. Вычислить  $u = x_{t+1}^{d_1} \pmod{p}$ .
4. Вычислить  $v = x_{t+1}^{d_2} \pmod{q}$ .
5. Вычислить  $x_0 = vap + ubq \pmod{n}$ .
6. Для  $i$  от 1 до  $t$  выполнить следующее.
  - 6.1.  $x_i := x_{i-1}^2 \pmod{n}$ .
  - 6.2. Пусть  $r_i$  есть  $h$  наименьших значащих бит в  $x_i$ .
  - 6.3.  $m_i := r_i \oplus c_i$  (ибо  $r_i \oplus c_i = r_i \oplus r_i \oplus m_i = m_i$ ).

**Доказательство.** Так как  $x_t$  есть квадратичный вычет по модулю  $n$ , то  $x_t$  есть квадратичный вычет по модулю  $p$ . Поэтому

$$x_t^{(p-1)/2} \equiv 1 \pmod{p}. \text{ Заметим, что}$$

$$x_{t+1}^{(p+1)/4} \equiv (x_t^2)^{(p+1)/4} \equiv x_t^{(p+1)/2} \equiv x_t^{(p-1)/2} \pmod{p}.$$

Аналогично получаем:  $x_t^{(p+1)/4} \equiv x_{t-1} \pmod{p}$ . Тогда  $x_{t+1}^{((p+1)/4)^2} \equiv x_{t-1} \pmod{p}$ .

Повторяя эти рассуждения, получаем следующее.

$u \equiv x_{t+1}^{d_1} \equiv x_{t+1}^{((p+1)/4)^{t+1}} \equiv x_0 \pmod{p}$ . Аналогично:  $v \equiv x_{t+1}^{d_2} \equiv x_0 \pmod{q}$ .

Так как  $ap + bq = 1$ , то  $vap + ubq \equiv x_0 \pmod{p}$  и  $vap + ubq \equiv x_0 \pmod{q}$ .

Поэтому  $x_0 \equiv vap + ubq \pmod{n}$  и адресат  $B$  вычисляет использованное адресатом  $A$  при шифровании случайное "зерно"  $x_0$ , по которому восстанавливается исходный текст.

### Пример.

**Вычисление ключей.** Адресат  $B$  выбирает простые числа  $p=499$ ,  $q=547$ , сравнимые с 3 по модулю 4, и вычисляет  $n = pq = 272953$ . Используя расширенный алгоритм Евклида,  $B$  вычисляет целые  $a=-57$ ,  $b=52$  такие, что  $ap + bq = 1$ . Открытый ключ адресата  $B$  есть  $n = 272953$ . Секретный ключ адресата  $B$  есть набор ( $p=499$ ,  $q=547$ ,  $a=-57$ ,  $b=52$ ).

**Шифрование.** Параметры  $k=18$ ,  $h=4$ . Адресат  $A$  представляет свое сообщение  $m$  как стринг  $m = m_1m_2m_3m_4m_5$  ( $t=5$ ), где  $m_1=1001$ ,  $m_2=1100$ ,  $m_3=0001$ ,  $m_4=0000$ ,  $m_5=1100$ . Адресат  $A$  выбирает случайный квадратичный вычет  $x_0 = 159201$  ( $= 399_2 \pmod{n}$ ) и вычисляет следующее.

$i$	$x_i = x_{i-1}^2 \pmod{n}$	$r_i$	$c_i = r_i \oplus m_i$
1	180539	1011	0010
2	193932	1100	0000
3	245613	1101	1100
4	130286	1110	1110
5	40632	1000	0100

и  $x_6 = x_5^2 \pmod{n} = 139680$ . Адресат  $A$  посыпает шифротекст  $c = (c_1=0010, c_2=0000, c_3=1100, c_4=1110, c_5=0100, x_0=139680)$  адресату  $B$ .

**Дешифрование.** Чтобы дешифровать  $c$ , адресат  $B$  вычисляет:

$$d_1 = ((p+1)/4)^{t+1} \pmod{(p-1)} = ((p+1)/4)^{5+1} \pmod{(p-1)} = 463.$$

$$d_2 = ((q+1)/4)^{t+1} \pmod{(q-1)} = ((q+1)/4)^{5+1} \pmod{(q-1)} = 337,$$

$$u = x_{t+1}^{d_1} \pmod{p} = x_{5+1}^{463} \pmod{499} = 20.$$

$$v = x_{t+1}^{d_2} \pmod{q} = x_{5+1}^{337} \pmod{547} = 24.$$

$$x_0 = vap + ubq \pmod{n} = 24 \cdot -57 \cdot 499 + 20 \cdot 52 \cdot 547 \pmod{272953} = 159201.$$

Адресат  $B$  использует  $x_0$  и получает все  $x_i$  и  $r_i$  так же, как это делал адресат  $A$  при шифровании. Затем  $B$  получает  $m_i$  XOR-суммированием  $r_i$  с блоками  $c_i$  шифротекста.

**Замечание.** Для криптографической стойкости модуль  $n$  следует брать длиной 1024 бит. Например, если  $n$  есть 1025-битовое число, то можно взять  $k=1024$  и  $h=10$ .

**Задача 35.** Электронная цифровая подпись Фейге–Фиат–Шамира с хешфункцией. Простые числа  $p$  и  $q$  определяются вариантом задания задачи 23.

Схема цифровой подписи Фейге–Фиата–Шамира есть некоторая модификация более ранней схемы Фиата–Шамира цифровой подписи. Схема требует хеш-функции  $h: \{0,1\}^* \rightarrow \{0,1\}^k$ . Здесь  $\{0,1\}^k$  есть множество всех битовых стрингов длины  $k$  и  $\{0,1\}^*$  есть множество всех битовых стрингов произвольной длины.

Криптографическая стойкость схемы основана на трудности вычисления дискретного квадратного корня.

**Вычисление ключей.** Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать случайные различные секретные простые числа  $p, q$  примерно одного размера и вычислить  $n = p \cdot q$ .
2. Выбрать положительное целое число  $k$  и случайные различные целые числа  $s_1, s_2, \dots, s_k \in \mathbb{Z}_n^*$ .
3. Вычислить  $v_j = s_j^{-2} \pmod{n}$ ,  $1 \leq j \leq k$ ,
4. Открытый ключ адресата есть набор  $((v_1, v_2, \dots, v_k), n)$ . Секретный ключ адресата есть  $k$ -набор  $(s_1, s_2, \dots, s_k)$ .

**Вычисление подписи.** Пользуясь своим секретным ключом, адресат  $A$  подписывает бинарное сообщение  $m$  произвольной длины. Адресат  $A$  должен выполнить следующее.

1. Выбрать случайное целое  $r$ ,  $1 \leq r \leq n-1$ .
2. Вычислить  $u = r^2 \pmod{n}$ .
3. Вычислить  $e = (e_1, e_2, \dots, e_k) = h(m||u)$ , где каждое  $e_i \in \{0,1\}$ . (Здесь  $m||u$  означает конкатенацию  $m$  и  $u$ , то есть приписывание  $u$  к  $m$  справа. Например,  $ab||aca = abaca$ ).
4. Вычислить  $s = r \cdot \prod_{j=1}^{j=k} s_j^{e_j} \pmod{n}$ .
5. Подпись адресата  $A$  под текстом  $m$  есть пара  $(e, s)$ .

**Проверка подписи.** Пользуясь открытым ключом адресата  $A$ , адресат  $B$  может проверить подпись адресата  $A$ . Адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $((v_1, v_2, \dots, v_k), n)$  адресата  $A$ .
2. Вычислить  $w = s^2 \cdot \prod_{j=1}^{j=k} v_j^{e_j} \pmod{n}$ .
3. Вычислить  $e' = h(m||w)$ .
4. Принять подпись, если  $e = e'$ . В противном случае подпись отклонить.

**Доказательство.**  $w \equiv s^2 \cdot \prod_{j=1}^{j=k} v_j^{e_j} \equiv r^2 \cdot \prod_{j=1}^{j=k} s_j^{2e_j} \cdot \prod_{j=1}^{j=k} v_j^{e_j} \equiv$

$r^2 \cdot \prod_{j=1}^{j=k} s_j^2 v_j \equiv r^2 \equiv u \pmod{n}$ . Следовательно,  $w = u$  и потому  $e = e'$ .

**Пример.**

**Вычисление ключей.** Адресат  $A$  берет простые числа  $p=3571$ ,  $q=4523$  и вычисляет  $n = pq = 16151633$ .  $A$  выбирает положительное целое число  $k=5$  и

случайные различные целые числа  $s_1=42, s_2=73, s_3=85, s_4=101, s_5=150$  из  $\mathbb{Z}_n^*$ .

Адресат  $A$  выполняет следующие вычисления.

$j$	1	2	3	4	5
$s_j$	42	73	85	101	150
$s_j^{-1} \pmod{n}$	4999315	885021	6270634	13113207	11090788
$v_j = s_j^{-2} \pmod{n}$	503594	4879739	7104483	1409171	6965302

Открытый ключ адресата  $A$  есть набор  $((v_1, v_2, \dots, v_k), n) = ((503594, 4879739, 7104483, 1409171, 6965302), 16151633)$ . Секретный ключ адресата  $A$  есть набор  $(s_1, s_2, \dots, s_k) = (42, 73, 85, 101, 150)$ .

**Вычисление подписи.** Пусть  $h: \{0,1\}^* \rightarrow \{0,1\}^5$  есть хеш-функция.

Адресат  $A$  выбирает случайное целое  $r = 23181 \in [1, n-1]$  и вычисляет  $u = r^2 \pmod{n} = 4354872$ .  $A$  вычисляет  $e = h(m||u) = s_1 s_2 s_3 s_4 s_5 = 10110$  (значение хеш-функции взято искусственно, это произвольный стринг из 0 и 1 длины 5).  $A$  вычисляет

$$s = r s_1^{e_1} s_2^{e_2} s_3^{e_3} s_4^{e_4} s_5^{e_5} \pmod{n} = r s_1^1 s_2^0 s_3^1 s_4^1 s_5^0 \pmod{n} = 23181 \cdot 42 \cdot 85 \cdot 101 \pmod{n} = 7978909.$$

Подпись  $A$  под текстом  $m$  есть  $(e=10110, s=7978909)$ .

**Проверка подписи.** Адресат  $B$  вычисляет  $s^2 \pmod{n} = 2926875$  и  $v_1 v_3 v_4 \pmod{n} = 503594 \cdot 7104483 \cdot 1409171 \pmod{n} = 15668174$ .  $B$  вычисляет  $w = s^2 v_1 v_3 v_4 \pmod{n} = 4354872$ . Так как  $w = u$ , то  $e' = h(m||w) = h(m||u) = e$ ,  $e' = e$ . Следовательно, адресат  $B$  принимает подпись адресата  $A$ .

**Замечание.** Для криптографической стойкости модуль  $n$  следует брать длиной 1024 и более бит.

Если  $n$  есть  $t$ -битовое число, то секретный ключ имеет размер  $kt$  бит. Его можно уменьшить выбором случайных чисел  $s_j$ ,  $1 \leq j \leq k$ , битовой длины  $t' < t$ . Однако число  $t'$  не может быть слишком малым во избежание возможности вычисления чисел  $s_j$ . Размер открытого ключа есть  $(k+1)t$  бит. Например, если  $t=768$  и  $k=128$ , то секретный и открытый ключи требуют 98304 и 99072 бит соответственно.

**Задача 36.** Электронная цифровая подпись GQ (Гилу-Куискуатера (Guillou-Quisquater, GQ)) с хеш-функцией. Простые число  $p = 503$ . Простое число  $q$  определяется вариантом задания.

**36.01.** 523. **36.02.** 563. **36.03.** 571. **36.04.** 547. **36.05.** 587. **36.06.** 563.

**36.07.** 599. **36.08.** 607. **36.09.** 619. **36.10.** 631. **36.11.** 643. **36.12.** 647.

**36.13.** 659. **36.14.** 691. **36.15.** 719. **36.16.** 683. **36.17.** 727. **36.18.** 739.

**36.19.** 751. **36.20.** 787. **36.21.** 743. **36.22.** 811. **36.23.** 823. **36.24.** 827.

**36.25.** 839. **36.26.** 859. **36.27.** 863. **36.28.** 883. **36.29.** 907. **36.30.** 911.

Схема Гилу-Куискуатера (Guillou-Quisquater, GQ) цифровой подписи требует хеш-функции  $h: \{0,1\}^* \rightarrow \mathbb{Z}_n$ , где  $n$  есть некоторое положительное целое число. Схема основана на трудности решения проблемы факторизации целых чисел.

**Вычисление ключей.** Каждый адресат создает свой открытый ключ и ему

соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать случайные различные секретные простые числа  $p, q$  примерно одного размера и вычислить  $n = pq$ .
2. Выбрать целое  $e \in [1, n-1]$ , для которого  $\text{нод}(e, (p-1) \cdot (q-1)) = 1$ .
3. Выбрать целое  $J_A$ ,  $1 \leq J_A \leq n$ , для которого  $\text{нод}(J_A, n) = 1$ . (Бинарное представление для  $J_A$  можно использовать для передачи информации об адресате, такой как имя, адрес, номер водительских прав и т.д.)
4. Найти такое целое  $a \in \mathbb{Z}_n$ , что  $J_A \cdot a^e \equiv 1 \pmod{n}$ , и выполнить это следующим образом.
  - 4.1. Вычислить  $J_A^{-1} \pmod{n}$ .
  - 4.2. Вычислить  $d_1 = e^{-1} \pmod{(p-1)}$  и  $d_2 = e^{-1} \pmod{(q-1)}$ .
  - 4.3. Вычислить  $a_1 = (J_A^{-1})^{d_1} \pmod{p}$  и  $a_2 = (J_A^{-1})^{d_2} \pmod{q}$ .
  - 4.4. Найти такое  $a$ , что одновременно  $a \equiv a_1 \pmod{p}$  и  $a \equiv a_2 \pmod{q}$ .
5. Открытый ключ адресата есть набор  $(n, e, J_A)$ . Секретный ключ адресата есть число  $a$ .

**Вычисление подписи.** Пользуясь своим секретным ключом, адресат  $A$  подписывает бинарное сообщение  $m$  произвольной длины. Адресат  $A$  делает следующее.

1. Выбрать случайное целое число  $k$  и вычислить  $r = k^e \pmod{n}$ .
2. Вычислить  $l = h(m||r)$ .
3. Вычислить  $s = ka^l \pmod{n}$ .
4. Подпись адресата  $A$  под текстом  $m$  есть пара  $(s, l)$ .

**Проверка подписи.** Пользуясь открытым ключом адресата  $A$ , адресат  $B$  может проверить подпись  $(s, l)$  адресата  $A$ . Адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(n, e, J_A)$  адресата  $A$ .
2. Вычислить  $u = k^e \cdot (J_A)^l \pmod{n}$  и  $l' = h(m||u)$ .
3. Принять подпись  $A$ , если  $l = l'$  и отклонить в противном случае.

**Доказательство.** Заметим, что  $u \equiv s^e \cdot (J_A)^l \equiv (ka^l)^e \cdot (a^e \cdot J_A)^l \equiv k^e \cdot (a^e \cdot J_A)^l \equiv k^e \equiv r \pmod{n}$ . Следовательно,  $u = r$  и потому  $l = l'$ .

**Пример. Вычисление ключей.** Адресат  $A$  выбирает простые числа  $p=20849, q=27457$  и вычисляет  $n = pq = 572450993$ .  $A$  выбирает целые  $e=47, J_A=1091522$ , решает сравнение  $J_A \cdot a^e \equiv 1 \pmod{n}$  и получает  $a=214611724$ . Открытый ключ адресата  $A$  есть набор  $(n=572450993, e=47, J_A=1091522)$ . Секретный ключ для  $A$  есть целое  $a=214611724$ .

**Вычисление подписи.** Чтобы подписать (бинарное) сообщение  $m=1101110001$ , адресат  $A$  выбирает случайное целое  $k=42134$  и вычисляет  $r = k^e \pmod{n} = 297543350$ . Затем  $A$  вычисляет  $l = h(m||r) = 2713833$  (значение хеш-функции взято искусственно) и  $s = ka^l \pmod{n} = 42134 \cdot (214611724^{2713833}) \pmod{n} = 252000854$ .

Подпись адресата  $A$  под текстом  $m$  есть пара  $(s=252000854, l=2713833)$ .

**Проверка подписи.** В вычисляет

$$s^e \pmod{n} = 252000854^{47} \pmod{n} = 398641962,$$

$$(J_A)^l \pmod{n} = 1091522^{2713833} \pmod{n} = 110523867,$$

$$u = s^e \cdot (J_A)^l \pmod{n} = 297543350.$$

Так как  $u = r$ ,  $l' = h(m||u) = h(m||r) = l$ , то  $l' = l$  и адресат  $B$  принимает подпись адресата  $A$ .

**Замечание.** Для криптографической стойкости модуль  $n$  следует брать модуль  $n$  длины  $\geq 768$  бит, число  $e$  длины  $\geq 128$  бит, значение хеш-функции от 128 до 160 бит. Тогда открытый ключ будет длины  $896+u$  бит, где  $u$  есть число бит для представления  $J_A$ . Секретный ключ  $a$  был бы 768 бит.

**Задача 37.** Электронная цифровая подпись Шнорра с хеш-функцией.

Простые числа  $p$  и  $q$  определяются вариантом задания задачи 29.

Схема Шнорра есть некоторая модификация схемы DSA без ограничений DSA на простые  $p$  и  $q$  при вычислении ключей. В схеме Шнорра, как и в схеме DSA, используется подгруппа порядка  $q$  группы  $\mathbb{Z}_p^*$ , где  $p$  есть некоторое большое простое число. Схема также требует хеш-функции  $h$ :  $\{0,1\}^* \rightarrow \mathbb{F}_q$ . Схема основана на трудности решения проблемы дискретного логарифма.

**Вычисление ключей.** Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать примерно одного размера простые числа  $p$  и  $q$ , для которых  $q$  делит  $p-1$ .

2. Выбрать генератор  $\alpha \in \mathbb{Z}_p^*$  для циклической подгруппы порядка  $q$  в группе  $\mathbb{Z}_p^*$ . Для этого адресат должен выполнить следующее.

2.1. Выбрать элемент  $g \in \mathbb{Z}_p^*$  и найти  $\alpha = g^{(p-1)/q} \pmod{p}$ .

2.2. Если  $\alpha = 1$ , то перейти к шагу 2.1 с другим  $g$ .

3. Выбрать произвольное число  $a$ ,  $1 \leq a \leq q-1$ .

4. Вычислить  $y = \alpha^a \pmod{p}$ .

5. Открытый ключ адресата есть  $(p, q, \alpha, y)$ . Секретный ключ адресата есть число  $a$ .

**Вычисление подписи.** Пользуясь своим секретным ключом, адресат  $A$  подписывает бинарное сообщение  $m$  произвольной длины. Адресат  $A$  должен выполнить следующее.

1. Выбрать случайное секретное целое  $k$ ,  $1 \leq k \leq q-1$ .

2. Вычислить  $r = \alpha^k \pmod{p}$ ,  $e = h(m||r)$ ,  $s = ae + k \pmod{q}$ .

3. Подпись адресата  $A$  под текстом  $m$  есть пара  $(s, e)$ .

**Проверка подписи.** Пользуясь открытым ключом адресата  $A$ , адресат  $B$  может проверить подпись  $(s, e)$  адресата  $A$ . Адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(p, q, \alpha, y)$  адресата  $A$ .

2. Вычислить  $v = \alpha^s \cdot y^{-e} \pmod{p}$ ,  $e' = h(m||v)$ .

3. Принять подпись  $A$  если  $e' = e$  и отклонить в противном случае.

**Доказательство.** В подписи адресата  $A$  число  $v \equiv \alpha^s \cdot y^{-e} \equiv \alpha^s \cdot \alpha^{-ae} \equiv \alpha^k \equiv r \pmod{p}$ , откуда  $h(m||v) = h(m||r)$  и  $e' = e$ .

**Пример. Вычисление ключей.** Адресат  $A$  выбирает простые числа  $p=129841$ ,  $q=541$ , для которых  $q|(p-1)$ . Число  $(p-1)/q = 240$ . Затем  $A$  выбирает случайное целое  $g = 26346 \in \mathbb{Z}_p^*$  и вычисляет  $\alpha = g^{(p-1)/q} \pmod{p} = 26346^{240} \pmod{p} = 26$ . Так как  $\alpha \neq 1$ , то  $\alpha$  порождает в  $\mathbb{Z}_p^*$  единственную циклическую подгруппу порядка 541. Адресат  $A$  выбирает произвольное число  $a = 423 \in [1, q-1]$  и вычисляет  $y = \alpha^a \pmod{p} = 26^{423} \pmod{p} = 115917$ . Открытый ключ адресата  $A$  есть набор  $(p=129841, q=541, \alpha=26, y=115917)$ . Секретный ключ для  $A$  есть число  $\alpha = 423$

**Вычисление подписи.** Чтобы подписать (бинарное) сообщение  $m=11101101$ , адресат  $A$  выбирает случайное число  $k = 327 \in [1, q-1]$  и вычисляет  $r = \alpha^k \pmod{p} = 26^{327} \pmod{p} = 49375$  и  $e = h(m||r) = 155$  (значение хеш-функции взято искусственно).  $A$  вычисляет  $s = ae + k \pmod{q} = 423 \cdot 155 + 327 \pmod{541} = 431$ . Подпись адресата  $A$  под текстом  $m$  есть пара  $(s=431, e=155)$ .

**Проверка подписи.**  $B$  вычисляет

$$v = \alpha^s \cdot y^{-e} \pmod{p} = 26^{431} \cdot 115917^{-155} \pmod{p} = 49375,$$

$$e' = h(m||v) = 155.$$

Так как  $e = e'$ , то  $B$  принимает подпись  $A$ .

**Замечание.** Для криптографической стойкости рекомендуется брать  $q$  длиной 160 бит, размер  $p$  лежит между 512 (лучше 768) и 1024 и более бит.

**Задача 38.** Электронная цифровая подпись Ниберга-Рюппеля с извлечением сообщения. Простые числа  $p$  и  $q$  определяются вариантом задания задачи 29.

Схема Ниберга-Рюппеля есть некоторая модификация схемы DSA без ограничений DSA на простые  $p$  и  $q$  при вычислении ключей. Схема основана на трудности решения проблемы дискретного логарифма.

**Вычисление ключей.** Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Каждый адресат должен выполнить следующее.

1. Выбрать простые числа  $p$  и  $q$ , для которых  $q$  делит  $p-1$ .

2. Выбрать генератор  $\alpha \in \mathbb{Z}_p^*$  для циклической подгруппы порядка  $q$  в группе  $\mathbb{Z}_p^*$ . Для этого адресат должен выполнить следующее.

2.1. Выбрать элемент  $g \in \mathbb{Z}_p^*$  и найти  $\alpha = g^{(p-1)/q} \pmod{p}$ .

2.2. Если  $\alpha=1$ , то перейти к шагу 2.1 с другим  $g$ .

3. Выбрать произвольное число  $a$ ,  $1 \leq a \leq q-1$ .

4. Вычислить  $y = \alpha^a \pmod{p}$ .

5. Открытый ключ адресата есть  $(p, q, \alpha, y)$ . Секретный ключ адресата есть число  $a$ .

**Вычисление подписи.** Пользуясь своим секретным ключом, адресат  $A$  подписывает бинарное сообщение  $m$ . Адресат  $A$  должен выполнить следующее.

1. Вычислить  $m' = R(m)$ .
2. Выбрать случайное секретное целое  $k$ ,  $1 \leq k \leq q-1$   
и вычислить  $r = \alpha^{-k} \pmod{p}$ .

3. Вычислить  $e = m'r \pmod{p}$ .

4. Вычислить  $s = ae + k \pmod{q}$ .

5. Подпись  $A$  под  $m$  есть пара  $(e, s)$ .

**Проверка подписи и вычисление сообщения.** Пользуясь открытым ключом адресата  $A$ , адресат  $B$  может проверить подпись  $(e, s)$  адресата  $A$  и извлечь из подписи сообщение от  $A$ . Адресат  $B$  должен выполнить следующее.

1. Получить открытый ключ  $(p, q, \alpha, y)$  адресата  $A$ .
2. Проверить, что  $e \in [1, p-1]$ . Если нет, то отклонить подпись.
3. Проверить, что  $s \in [1, q-1]$ . Если нет, то отклонить подпись.
4. Вычислить  $v = \alpha^s \cdot y^{-e} \pmod{p}$  и  $m' = ve \pmod{p}$ .
5. Проверить, что  $m' \in M_R$ . Если нет, то отклонить подпись.
6. Вычислить  $m = R^{-1}(m')$ .

**Доказательство.** Для подписи адресата  $A$  число  $v \equiv \alpha^s \cdot y^{-e} \equiv \alpha^{s-ae} \equiv a^k \pmod{p}$ . Следовательно,  $ve \equiv \alpha^k m' \alpha^{-k} \equiv m' \pmod{p}$ , что и требовалось.

**Пример. Вычисление ключей.** Адресат  $A$  выбирает простые числа  $p=1256993$ ,  $q=3571$ , где  $q$  делит  $(p-1)$ . Число  $(p-1)/q = 352$ .  $A$  выбирает случайное число  $g = 42077 \in \mathbb{Z}_p^*$  и вычисляет  $\alpha = g^{(p-1)/q} \pmod{p} = 42077^{352} \pmod{p} = 441238$ . Так как  $\alpha \neq 1$ , то  $\alpha$  порождает в  $\mathbb{Z}_p^*$  единственную циклическую подгруппу порядка 3571.  $A$  выбирает случайное целое  $a = 2774 \in [1, q-1]$  и вычисляет  $y = \alpha^a \pmod{p} = 1013657$ . Открытый ключ адресата  $A$  есть набор  $(p=1256993, q=3571, \alpha=441238, y=1013657)$ . Секретный ключ для  $A$  есть число  $a = 2774$ .

**Вычисление подписи.** Чтобы подписать сообщение  $m$ , адресат  $A$  вычисляет  $m' = R(m) = 1147892$  (значение  $R(m)$  взято искусственно).  $A$  выбирает случайное  $k = 1001 \in [1, q-1]$  и вычисляет  $r = \alpha^{-k} \pmod{p} = 441238^{-1001} \pmod{p} = 1188935$ ,  $e = m'r \pmod{p} = 138207$ ,  $s = ae + k \pmod{q} = 2774 \cdot 138207 + 1001 \pmod{q} = 1088$ . Подпись адресата  $A$  с сообщением  $m$  есть пара  $(e=138207, s=1088)$ .

**Проверка подписи и извлечение сообщения.**  $B$  вычисляет

$$v = 441238^{1088} \cdot 1013657^{-138207} \pmod{1256993} = 504308,$$

$$m' = v \cdot 138207 \pmod{1256993} = 1147892.$$

$B$  проверяет, что  $m' \in M_R$  и получает  $m = R^{-1}(m')$ .

**Замечание.** Для криптографической стойкости рекомендуется брать  $q$  длиной 160 бит, размер  $p$  лежит между 512 (лучше 768) и 1024 и более бит.

## ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

**Задача 39.** Взять три первых буквы своей фамилии, и для этого трехбуквенного слова найти его бинарный код ASCII длины 24. Поделить код на 6 бинарных слов  $a_1, a_2, a_3, a_4, a_5, a_6$  длины 4 каждое слово. С помощью бинарного систематического (7,4)-кода Хэмминга

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

найти соответствующие кодовые слова  $u_1, u_2, u_3, u_4, u_5, u_6$  длины 7. Исказить их в одном разряде по диагонали через один и получить кодовые слова  $v_1, v_2, v_3, v_4, v_5, v_6$ . Как это сделано в примере, проверить все их с помощью синдрома, восстановить искаженные и выделить в полученном результате информационные слова.

**16-ричные и бинарные коды ASCII букв латинского алфавита**

	20	0010 0000									
A	41	0100 0001	I	49	0100 1001	Q	51	0101 0001	Y	59	0101 0000
B	42	0100 0010	J	4a	0100 1010	R	52	0101 0010	Z	5a	0101 1001
C	43	0100 0011	K	4b	0100 1011	S	53	0101 0011			
D	44	0100 0100	L	4c	0100 1100	T	54	0101 0100			
E	45	0100 0101	M	4d	0100 1101	U	55	0101 0101			
F	46	0100 0110	N	4e	0100 1110	V	56	0101 0110			
G	47	0100 0111	O	4f	0100 1111	W	57	0101 0111			
H	48	0100 1000	P	50	0101 0000	X	58	0101 1000			

**Пример.** Пусть  $a_1=(1011)$ ,  $a_2=(0011)$ ,  $a_3=(1001)$ ,  $a_4=(1111)$ ,  $a_5=(1010)$ ,  $a_6=(0001)$ .

**Шаг 1.**

$$a_1=(1011), \quad u_1 = a_1 \cdot G = (1011000), \quad v_1=(0011000), \quad S(v_1) = H \cdot v_1^T = (101).$$

Синдром (локатор ошибки)  $S(v_1)=(101)$  есть 1-й столбец в  $H$ .

1-й столбец в  $v_1=(0011000)$  ошибочен,  $u_1=(1011000)$ .

Первые четыре символа в  $u_1$  есть  $a_1 = (1011)$ .

**Шаг 2.**

$$a_2=(0011), \quad u_2 = a_2 \cdot G = (0011101), \quad v_2=(0011101), \quad S(v_2) = H \cdot v_2^T = (000).$$

Синдром (локатор ошибки)  $S(v_2) = (000)$ .

Кодовый вектор  $u_2$  при передаче не искажен,  $v_2=u_2=(0011101)$ .

Первые четыре символа в  $v_2$  есть  $a_2 = (0011)$ .

**Шаг 3.**

$$a_3=(1001), \quad u_3 = a_3 \cdot G = (1001110), \quad v_3=(1011110), \quad S(v_3) = H \cdot v_3^T = (110).$$

Синдром (локатор ошибки)  $S(v_3)=(110)$  есть 3-й столбец в  $H$ .

3-й столбец в  $v_3=(1011110)$  ошибочен,  $u_3=(1001000)$ .

Первые четыре символа в  $\mathbf{u}3$  есть  $\mathbf{a}3 = (1001)$ .

**Шаг 4.**

$\mathbf{a}4 = (1111)$ ,  $\mathbf{u}4 = \mathbf{a}4 \cdot G = (1111111)$ ,  $\mathbf{v}4 = (1111111)$ ,  $S(\mathbf{v}4) = H \cdot \mathbf{v}4^T = (000)$ .

Синдром (локатор ошибки)  $S(\mathbf{v}4) = (000)$ .

Кодовый вектор  $\mathbf{u}4$  при передаче не искажен,  $\mathbf{v}4 = \mathbf{u}4 = (1111111)$ .

Первые четыре символа в  $\mathbf{v}4$  есть  $\mathbf{a}4 = (1111)$ .

**Шаг 5.**

$\mathbf{a}5 = (1010)$ ,  $\mathbf{u}5 = \mathbf{a}5 \cdot G = (1010011)$ ,  $\mathbf{v}5 = (1010111)$ ,  $S(\mathbf{v}5) = H \cdot \mathbf{v}5^T = (100)$ .

Синдром (локатор ошибки)  $S(\mathbf{v}5) = (100)$  есть 5-й столбец в  $H$ .

5-й столбец в  $\mathbf{v}5 = (1010111)$  ошибочен,  $\mathbf{u}5 = (1010011)$ .

Первые четыре символа в  $\mathbf{u}5$  есть  $\mathbf{a}5 = (1010)$ .

**Шаг 6.**

$\mathbf{a}6 = (0001)$ ,  $\mathbf{u}6 = \mathbf{a}6 \cdot G = (0001011)$ ,  $\mathbf{v}6 = (0001011)$ ,  $S(\mathbf{v}6) = H \cdot \mathbf{v}6^T = (000)$ .

Синдром (локатор ошибки)  $S(\mathbf{v}6) = (000)$ .

Кодовый вектор  $\mathbf{u}6$  при передаче не искажен,  $\mathbf{v}6 = \mathbf{u}6 = (0001011)$ .

Первые четыре символа в  $\mathbf{v}6$  есть  $\mathbf{a}6 = (0001)$ .

**Задача 40.** Найти минимальный полином для элемента поля

$$GF(q^m) = GF((p^n)^m), n = 1, p = 2, q = p^n = 2^1 = 2, m = 5.$$

Заданы следующие объекты.

**Шесть примитивных полиномов степени 5.**

$$p_1(x) = 100101 = 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1.$$

$$p_2(x) = 101001 = 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1.$$

$$p_3(x) = 101111 = 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1.$$

$$p_4(x) = 110111 = 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1.$$

$$p_5(x) = 111011 = 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1.$$

$$p_6(x) = 111101 = 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1.$$

Каждый примитивный полином порождает конечное поле.

**Пять элементов** (полиномов поля)

$$1. 1001 = 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1.$$

$$2. 1010 = 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0.$$

$$3. 1011 = 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1.$$

$$4. 1101 = 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1.$$

$$5. 1110 = 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0.$$

Они порождаются степенями полинома  $x$  следующим образом.

$$x^{29} = 1001, x^6 = 1010, x^{27} = 1011, x^8 = 1101, x^{12} = 1110 \pmod{p_1}.$$

$$x^5 = 1001, x^{29} = 1010, x^{26} = 1011, x^7 = 1101, x^{23} = 1110 \pmod{p_2}.$$

$$x^8 = 1001, x^{25} = 1010, x^{10} = 1011, x^{18} = 1101, x^{28} = 1110 \pmod{p_3}.$$

$$x^{11} = 1001, x^8 = 1010, x^{28} = 1011, x^{17} = 1101, x^{24} = 1110 \pmod{p_4}.$$

$$x^{23} = 1001, x^{27} = 1010, x^{17} = 1011, x^6 = 1101, x^{11} = 1110 \pmod{p_5}.$$

$$x^{26} = 1001, x^{10} = 1010, x^{16} = 1011, x^{24} = 1101, x^7 = 1110 \pmod{p_6}.$$

**Варианты.** Найти минимальный полином для данного конечного поля, порождаемого данным примитивным полиномом и данного элемента поля.

- 01.  $(p_1, 1001)$ . 02.  $(p_1, 1010)$ . 03.  $(p_1, 1011)$ . 04.  $(p_1, 1101)$ . 05.  $(p_1, 1110)$ .
- 06.  $(p_2, 1001)$ . 07.  $(p_2, 1010)$ . 08.  $(p_2, 1011)$ . 09.  $(p_2, 1101)$ . 10.  $(p_2, 1110)$ .
- 11.  $(p_3, 1001)$ . 12.  $(p_3, 1010)$ . 13.  $(p_3, 1011)$ . 14.  $(p_3, 1101)$ . 15.  $(p_3, 1110)$ .
- 16.  $(p_4, 1001)$ . 17.  $(p_4, 1010)$ . 18.  $(p_4, 1011)$ . 19.  $(p_4, 1101)$ . 20.  $(p_4, 1110)$ .
- 21.  $(p_5, 1001)$ . 22.  $(p_5, 1010)$ . 23.  $(p_5, 1011)$ . 24.  $(p_5, 1101)$ . 25.  $(p_5, 1110)$ .
- 26.  $(p_6, 1001)$ . 27.  $(p_6, 1010)$ . 28.  $(p_6, 1011)$ . 29.  $(p_6, 1101)$ . 30.  $(p_6, 1110)$ .

**Пример.** Пусть имеем поле  $GF(q^m) = GF((p^n)^m)$ ,  $n = 1$ ,  $p = 2$ ,  $q = p^n = 2^1 = 2$ ,  $m = 5$ , то есть  $GF(q^m)$ ,  $q = 2$ ,  $m = 5$ , примитивный полином  $p(x) = 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ .

Найти минимальный полином для элемента

$$\beta = \alpha^{24} = x^{24} = 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 = x^3 + x^2 + 1.$$

*Решение.* Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^{24}) = \text{ord}(x^3 + x^2 + 1) = 15$ ,  $\beta^{15} = 1$ . Так как

$$\beta^{2^1} = (\alpha^{24})^{2^1} = \alpha^{48} = \alpha^{\text{mod}(48,31)} = \alpha^{17} = 10110 \neq \beta = 1101,$$

$$\beta^{2^2} = (\alpha^{24})^{2^2} = \alpha^{96} = \alpha^{\text{mod}(96,31)} = \alpha^3 = 1000 \neq \beta = 1101,$$

$$\beta^{2^3} = (\alpha^{24})^{2^3} = \alpha^{192} = \alpha^{\text{mod}(192,31)} = \alpha^6 = 111 \neq \beta = 1101,$$

$$\beta^{2^4} = (\alpha^{24})^{2^4} = \alpha^{384} = \alpha^{\text{mod}(384,31)} = \alpha^{12} = 10101 \neq \beta = 1101, \beta^{2^5} = (\alpha^{24})^{2^5} =$$

$$\alpha^{768} = \alpha^{\text{mod}(768,31)} = \alpha^{24} = 1101 = \beta = 1101,$$

то  $r = 5$ ,  $r-1 = 4$ ,  $\beta = \alpha^{24}$  и потому минимальный полином

$$\begin{aligned} m_{24}(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3})(x - \beta^{2^4}) = \\ &= (x - (\alpha^{24})^{2^0})(x - (\alpha^{24})^{2^1})(x - (\alpha^{24})^{2^2})(x - (\alpha^{24})^{2^3})(x - (\alpha^{24})^{2^4}) = \\ &= (x - \alpha^{24})(x - \alpha^{48})(x - \alpha^{96})(x - \alpha^{192})(x - \alpha^{384}) = \\ &= (x - \alpha^{24})(x - \alpha^{17})(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12}) = \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{17})(x - \alpha^{24}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{17}, \alpha^{24}\}$ . Пусть  $C(M, k)$  есть сумма всех произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Так как  $-1 \equiv 1 \pmod{2}$  и  $\beta = \alpha^{24}$ , то получаем следующее.

$$\begin{aligned} m_{24}(x) &= C(M,0)x^5 + C(M,1)x^4 + C(M,2)x^3 + C(M,3)x^2 + C(M,4)x + C(M,5) = \\ &= x^5 + (\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{17} + \alpha^{24})x^4 + \\ &+ (\alpha^3\alpha^6 + \alpha^3\alpha^{12} + \alpha^3\alpha^{17} + \alpha^3\alpha^{24} + \alpha^6\alpha^{12} + \alpha^6\alpha^{17} + \alpha^6\alpha^{24} + \alpha^{12}\alpha^{17} + \alpha^{12}\alpha^{24} + \alpha^{17}\alpha^{24})x^3 + \\ &+ (\alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^6\alpha^{17} + \alpha^3\alpha^6\alpha^{24} + \alpha^3\alpha^{12}\alpha^{17} + \alpha^3\alpha^{12}\alpha^{24} + \alpha^3\alpha^{17}\alpha^{24} + \alpha^6\alpha^{12}\alpha^{17} + \\ &+ \alpha^6\alpha^{12}\alpha^{24} + \alpha^6\alpha^{17}\alpha^{24} + \alpha^{12}\alpha^{17}\alpha^{24})x^2 + \\ &+ (\alpha^3\alpha^6\alpha^{12}\alpha^{17} + \alpha^3\alpha^6\alpha^{12}\alpha^{24} + \alpha^3\alpha^6\alpha^{17}\alpha^{24} + \alpha^3\alpha^{12}\alpha^{17}\alpha^{24} + \alpha^6\alpha^{12}\alpha^{17}\alpha^{24})x + \\ &+ \alpha^3\alpha^6\alpha^{12}\alpha^{17}\alpha^{24} = \end{aligned}$$

$$\begin{aligned}
& x^5 + (01000+00111+10101+10110+01101)x^4 + \\
& (\alpha^9 + \alpha^{15} + \alpha^{20} + \alpha^{27} + \alpha^{18} + \alpha^{23} + \alpha^{30} + \alpha^{29} + \alpha^{36} + \alpha^{41})x^3 + \\
& (\alpha^{21} + \alpha^{26} + \alpha^{33} + \alpha^{32} + \alpha^{39} + \alpha^{44} + \alpha^{35} + \alpha^{42} + \alpha^{47} + \alpha^{53})x^2 + \\
& (\alpha^{38} + \alpha^{45} + \alpha^{50} + \alpha^{56} + \alpha^{59})x + \alpha^{62} = \\
& x^5 + 1x^4 + \\
& (\alpha^9 + \alpha^{15} + \alpha^{20} + \alpha^{27} + \alpha^{18} + \alpha^{23} + \alpha^{30} + \alpha^{29} + \alpha^5 + \alpha^{10})x^3 + \\
& (\alpha^{21} + \alpha^{26} + \alpha^2 + \alpha^1 + \alpha^8 + \alpha^{13} + \alpha^4 + \alpha^{11} + \alpha^{16} + \alpha^{22})x^2 + \\
& (\alpha^7 + \alpha^{14} + \alpha^{19} + \alpha^{25} + \alpha^{28})x + \alpha^{31} = \\
& x^5 + 1x^4 + \\
& (00101+11011+00011+10010+10001+11000+11110+01111+11101+01010)x^3 + \\
& (00110+01001+00100+00010+11100+10111+10000+10100+01011+01100)x^2 + \\
& (01110+10011+11111+11010+11001)x + 1 = \\
& x^5 + 1x^4 + 0x^3 + 1x^2 + 1x + 1.
\end{aligned}$$

Для  $\beta = \alpha^{24} = x^3 + x^2 + 1$  минимальный полином  $m_{24}(x) = x^5 + x^4 + x^2 + x + 1$ .  
Ответ. Для  $\beta = x^3 + x^2 + 1$  минимальный полином  $m(x) = x^5 + x^4 + x^2 + x + 1$ .

**Задача 41.** Построить ( $n=15$ ,  $k=5$ )-код БЧХ (кодер и декодер), исправляющий не более  $t=3$  ошибок. Обнаружить и исправить ошибки передачи информации с конкретными данными.

Заданы следующие объекты.

#### Два примитивных полинома степени 4.

$$p_1(x) = 11011 = 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1.$$

$$p_2(x) = 10111 = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1.$$

Генератор несистематического БЧХ-кода

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Для систематического бинарного (15,5)-кода БЧХ взять кодовый полином  $u(x) = x^{n-k} a(x) + (x^{n-k} a(x)) \pmod{g(x)} = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)}$ .

**Пятнадцать информационных слов  $a$  длины пять.**

1.  $10000 = 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 0$ .
2.  $10001 = 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1$ .
3.  $10010 = 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0$ .
4.  $10011 = 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1$ .
5.  $10100 = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 0$ .
6.  $10101 = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 0$ .
7.  $10110 = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1$ .
8.  $10111 = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0$ .
9.  $11000 = 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 0$ .
10.  $11001 = 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1$ .

$$11. \ 11010 = 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0.$$

$$12. \ 11011 = 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1.$$

$$13. \ 11100 = 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 0.$$

$$14. \ 11101 = 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1.$$

$$15. \ 11110 = 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0.$$

**Варианты  $p_i, a$ .**

$$01. p_1, 10000. \ 02. p_1, 10001. \ 03. p_1, 10010. \ 04. p_1, 10011. \ 05. p_1, 10100.$$

$$06. p_1, 10101. \ 07. p_1, 10110. \ 08. p_1, 10111. \ 09. p_1, 11000. \ 10. p_1, 11001.$$

$$11. p_1, 11010. \ 12. p_1, 11011. \ 13. p_1, 11100. \ 14. p_1, 11101. \ 15. p_1, 11110.$$

$$16. p_2, 10000. \ 17. p_2, 10001. \ 18. p_2, 10010. \ 19. p_2, 10011. \ 20. p_2, 10100.$$

$$21. p_2, 10101. \ 22. p_2, 10110. \ 23. p_2, 10111. \ 24. p_2, 11000. \ 25. p_2, 11001.$$

$$26. p_2, 11010. \ 27. p_2, 11011. \ 28. p_2, 11100. \ 29. p_2, 11101. \ 30. p_2, 11110.$$

### Алгоритм Питерсона-Горенстейна-Цирлера БЧХ-кода с исправлением $t$ и менее ошибок

Построить БЧХ-код, исправляющий  $t$  и менее ошибок.

1. Построить конечное поле  $GF(p^m)$  с  $p^m > 2t$ . Пусть  $p(x)$  и  $\alpha$  есть примитивный полином и примитивный элемент (генератор для  $GF^*(p^m)$ ) этого поля соответственно.

2. Найти степени  $\alpha^1, \alpha^2, \dots, \alpha^{2t}$  и их минимальные функции  $m_1(x), m_2(x), \dots, m_{2t}(x)$  соответственно.

3. Найти генератор  $g(x) = \text{нок}(m_1(x), m_2(x), \dots, m_{2t}(x))$  конструируемого БЧХ-кода. Пусть  $r$  есть степень полинома  $g(x)$ . Если  $r \leq 2t$ , то перейти к пункту 1 и увеличить степень  $m$  в  $GF(p^m)$  на единицу.

4. ( $n=p^m-1, k=p^m-r$ )-код БЧХ построен. Числа  $n=p^m-1$  и  $k=p^m-r$  есть длины кодового слова и информационного слова соответственно.

5. Пусть  $v(x)$  есть принятое слово (в виде полинома степени  $p^m-1$ ), в котором не более  $t$  ошибок.

6. Вычислить элементы (компоненты) синдрома  $S_j = v(\alpha^j), j=1,2,\dots,2t$ .

$$7. \ \text{Найти матрицу } M_t = \begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_t \\ S_2 & S_3 & S_4 & \cdots & S_{t+1} \\ S_3 & S_4 & S_5 & \cdots & S_{t+2} \\ & & & \ddots & \\ S_t & S_{t+1} & S_{t+2} & \cdots & S_{2t-1} \end{bmatrix}.$$

8. Если  $\det(M_t) = 0$ , то уменьшить  $M$  на единицу и перейти к пункту 7.

9. Если  $\det(M_j) = 0$  для всех  $j = t, t-1, t-2, \dots, 2, 1$ , то в принятом слове искажений нет.

10. Если  $\det(M_j) = 0$  для всех  $j = t, t-1, w-1$ , и  $\det(M_w) \neq 0$ , то решить

систему уравнений

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_w \\ S_2 & S_3 & \cdots & S_{w+1} \\ \cdots & \cdots & \cdots & S_{2w-1} \\ S_w & S_{w+1} & \cdots & S_{2w-1} \end{bmatrix} \cdot \begin{bmatrix} \lambda_w \\ \lambda_{w-1} \\ \cdots \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{w+1} \\ -S_{w+2} \\ \cdots \\ -S_{2w} \end{bmatrix}, \text{ откуда}$$

$$\begin{bmatrix} \lambda_w \\ \lambda_{w-1} \\ \cdots \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & \cdots & S_w \\ S_2 & S_3 & \cdots & S_{w+1} \\ \cdots & \cdots & \cdots & S_{2w-1} \\ S_w & S_{w+1} & \cdots & S_{2w-1} \end{bmatrix}^{-1} \cdot \begin{bmatrix} -S_{w+1} \\ -S_{w+2} \\ \cdots \\ -S_{2w} \end{bmatrix}.$$

11. Полином локаторов ошибок

$$\lambda(x) = \lambda_w x^w + \lambda_{w-1} x^{w-1} + \lambda_{w-2} x^{w-2} + \dots + \lambda_1 x + 1.$$

12. Найти  $w$  корней  $\beta_1, \beta_2, \dots, \beta_w$  полинома локаторов ошибок  $\lambda(x)$ , найти их обратные значения  $(\beta_j)^{-1}$  и представить их в виде  $\alpha^{i_j}$ ,  $j = 1, 2, \dots, w$ . Для вычисления корней полинома  $\lambda(x)$  можно использовать *процедуру Чена*, состоящую в последовательном вычислении  $\lambda(\alpha^j)$  для каждого  $j$  и проверки полученных значений на ноль.

Наиболее простым способом вычисления значения  $\lambda(x)$  в точке  $\beta$  является схема Горнера:  $\lambda(\beta) = (\dots(((\lambda_w \beta + \lambda_{w-1})\beta + \lambda_{w-2})\beta + \lambda_{w-3})\beta + \dots + \lambda_0)$ .

Для вычисления  $\lambda(\beta)$  по схеме Горнера требуется только  $v$  умножений и  $v$  сложений.

13. Вектор ошибок  $e(x)$  найден. Он имеет ненулевые значения лишь в позициях  $i_1, i_2, \dots, i_w$  (пункт 12). В принятом векторе  $v(x)$  позиции  $i_1, i_2, \dots, i_w$  искажены.

14. Переданный вектор  $c(x) = v(x) + e(x)$ .

15. При известных  $c(x), g(x)$  переданное информационное слово  $a(x)$  можно найти из равенства  $c(x) = a(x)g(x)$ , последовательно проверяя это равенство на информационных словах  $a(x)$  длины  $k=p^m-r$  (пункт 4).

## ПРИМЕРЫ РЕШЕНИЯ

**Пример 1а.** Несистематический ( $n=15, k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай трех ошибок.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое число такое, что  $\beta^{q^r} = \beta$ .

$$\beta = \alpha^1 = x. \text{ Степени } \alpha^t = \alpha^{\text{mod}(t, 15)}, \beta^t = \beta^{\text{mod}(t, 15)}.$$

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_1(x) = (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$m(x) = C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ (\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \\ x^4 + (0010 + 0100 + 0011 + 0101)x^3 + (\alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12})x^2 + \\ (\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14})x + \alpha^{15} = \\ x^4 + 0x^3 + (1000 + 0110 + 1010 + 1100 + 0111 + 1111)x^2 + \\ (1011 + 1110 + 1101 + 1001)x + 1 = \\ x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .

$\beta = \alpha^2 = x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_2(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ (x - (\alpha^2)^{2^0})(x - (\alpha^2)^{2^1})(x - (\alpha^2)^{2^2})(x - (\alpha^2)^{2^3}) = \\ (x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) =$

$$(x - (\alpha^3)^{2^0})(x - (\alpha^3)^{2^1})(x - (\alpha^3)^{2^2})(x - (\alpha^3)^{2^3}) = \\ (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = \\ (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned}
m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\
&x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^3\alpha^6 + \alpha^3\alpha^9 + \alpha^3\alpha^{12} + \alpha^6\alpha^9 + \alpha^6\alpha^{12} + \alpha^9\alpha^{12})x^2 + \\
&(\alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^9\alpha^{12} + \alpha^6\alpha^9\alpha^{12})x + \alpha^3\alpha^6\alpha^9\alpha^{12} = \\
&x^4 + (1000 + 1100 + 1010 + 1111)x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 + \\
&(\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} = \\
&x^4 + 1x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{15} + \alpha^3 + \alpha^6)x^2 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + \alpha^{15} = \\
&x^4 + 1x^3 + (1010 + 1111 + 0001 + 0001 + 1000 + 1100)x^2 + \\
&(1000 + 1100 + 1010 + 1111)x + 1 = \\
&x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{21} = (\alpha^4)^{21} = \alpha^8 = x^3 + x^2 \neq \beta$ ,  $\beta^{22} = (\alpha^4)^{22} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{23} = (\alpha^4)^{23} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$   $\beta^{24} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned}
m_4(x) &= (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) = \\
&(x - (\alpha^4)^{20})(x - (\alpha^4)^{21})(x - (\alpha^4)^{22})(x - (\alpha^4)^{23}) = \\
&(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\
&= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).
\end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2 + x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2 + x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{21} = (\alpha^5)^{21} = \alpha^{10} = x^2 + x + 1 \neq \beta$ ,  $\beta^{22} = (\alpha^5)^{22} = \alpha^{20} = \alpha^5 = x^2 + x = \beta$ , то  $r = 2$ ,  $r-1 = 1$ , и потому

$$\begin{aligned}
m_5(x) &= (x - \beta^{20})(x - \beta^{21}) = (x - (\alpha^5)^{20})(x - (\alpha^5)^{21}) = \\
&(x - \alpha^5)(x - \alpha^{10}). \text{ Положим множество } M = \{\alpha^5, \alpha^{10}\}.
\end{aligned}$$

Тогда получаем следующее.

$$\begin{aligned}
m_5(x) &= C(M,0)x^2 + C(M,1)x + C(M,2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5\alpha^{10})x^2 = \\
&x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1.
\end{aligned}$$

Для  $\beta = \alpha^5 = x^2 + x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3 + x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3 + x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{21} = (\alpha^6)^{21} = \alpha^{12} = x^3 + x^2 + x + 1 \neq \beta$ ,  $\beta^{22} = (\alpha^6)^{22} = \alpha^{24} = \alpha^9 = x^3 + x + 1 \neq \beta$ ,  $\beta^{23} = (\alpha^6)^{23} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{24} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3 + x^2$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned}
m_6(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\
&= (x - (\alpha^6)^{2^0})(x - (\alpha^6)^{2^1})(x - (\alpha^6)^{2^2})(x - (\alpha^6)^{2^3}) = \\
&= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = \\
&= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = \\
&= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).
\end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3 + x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического ( $n=15, k=5$ )-кода БЧХ есть полином

$$\begin{aligned}
g(x) &= \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) = \\
m_1(x) \cdot m_3(x) \cdot m_5(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\
(x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \\
g(x) &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.
\end{aligned}$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = \mathbf{a}$ .

5. Для несистематического (15,5)-кода БЧХ кодовое слово

$$\begin{aligned}
u(x) &= a(x) \cdot g(x) = (x^4 + x^3 + x)(x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1) = \\
x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^5 + x &= \mathbf{111000010100110}.
\end{aligned}$$

Принятое (искаженное) кодовое слово

$$v(x) = \mathbf{101100010101110} = x^{14} + x^{12} + x^{11} + x^7 + x^5 + x^3 + x^2 + x.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ . Умножения проводятся по модулю  $p(x) = x^4 + x + 1$ .

$$\begin{aligned}
S_1 &= v(\alpha^1) = \alpha^{14} + \alpha^{12} + \alpha^{11} + \alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha^1 = \\
1001 + 1111 + 1110 + 1011 + 0110 + 1000 + 0100 + 0010 &= 1011 = \alpha^7.
\end{aligned}$$

$$\begin{aligned}
S_2 &= v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{12} + (\alpha^2)^{11} + (\alpha^2)^7 + (\alpha^2)^5 + (\alpha^2)^3 + (\alpha^2)^2 + (\alpha^2)^1 = \\
\alpha^{28} + \alpha^{24} + \alpha^{22} + \alpha^{14} + \alpha^{10} + \alpha^6 + \alpha^4 + \alpha^2 &= \\
\alpha^{13} + \alpha^9 + \alpha^7 + \alpha^{14} + \alpha^{10} + \alpha^6 + \alpha^4 + \alpha^2 &=
\end{aligned}$$

$$1101 + 1010 + 1011 + 1001 + 0111 + 1100 + 0011 + 0100 = 1001 = \alpha^{14}.$$

$$\begin{aligned}
S_3 &= v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{12} + (\alpha^3)^{11} + (\alpha^3)^7 + (\alpha^3)^5 + (\alpha^3)^3 + (\alpha^3)^2 + (\alpha^3)^1 = \\
\alpha^{42} + \alpha^{36} + \alpha^{33} + \alpha^{21} + \alpha^{15} + \alpha^9 + \alpha^6 + \alpha^3 &= \\
\alpha^{12} + \alpha^6 + \alpha^3 + \alpha^6 + \alpha^0 + \alpha^9 + \alpha^6 + \alpha^3 &=
\end{aligned}$$

$$1111 + 1100 + 1000 + 1100 + 0001 + 1010 + 1100 + 1000 = 1000 = \alpha^3.$$

$$\begin{aligned}
S_4 &= v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{12} + (\alpha^4)^{11} + (\alpha^4)^7 + (\alpha^4)^5 + (\alpha^4)^3 + (\alpha^4)^2 + (\alpha^4)^1 = \\
\alpha^{56} + \alpha^{48} + \alpha^{44} + \alpha^{28} + \alpha^{20} + \alpha^{12} + \alpha^8 + \alpha^4 &= \\
\alpha^{11} + \alpha^3 + \alpha^{14} + \alpha^{13} + \alpha^5 + \alpha^{12} + \alpha^8 + \alpha^4 &=
\end{aligned}$$

$$1110 + 1000 + 1001 + 1101 + 0110 + 1111 + 0101 + 0011 = 1101 = \alpha^{13}.$$

$$\begin{aligned}
S_5 &= v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{12} + (\alpha^5)^{11} + (\alpha^5)^7 + (\alpha^5)^5 + (\alpha^5)^3 + (\alpha^5)^2 + (\alpha^5)^1 = \\
\alpha^{70} + \alpha^{60} + \alpha^{55} + \alpha^{35} + \alpha^{25} + \alpha^{15} + \alpha^{10} + \alpha^5 &= \\
\alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^5 + \alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^5 &=
\end{aligned}$$

$$0111 + 0001 + 0111 + 0110 + 0111 + 0001 + 0111 + 0110 = 0000 = 0.$$

$$\begin{aligned}
S_6 &= v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{12} + (\alpha^6)^{11} + (\alpha^6)^7 + (\alpha^6)^5 + (\alpha^6)^3 + (\alpha^6)^2 + (\alpha^6)^1 = \\
&\alpha^{84} + \alpha^{72} + \alpha^{66} + \alpha^{42} + \alpha^{30} + \alpha^{18} + \alpha^{12} + \alpha^6 = \\
&\alpha^9 + \alpha^{12} + \alpha^6 + \alpha^{12} + \alpha^0 + \alpha^3 + \alpha^{12} + \alpha^6 = \\
&1010 + 1111 + 1100 + 1111 + 0001 + 1000 + 1111 + 1100 = 1100 = \alpha^6. \\
S_1 &= \alpha^7 = 1011, S_2 = \alpha^{14} = 1001, S_3 = \alpha^3 = 1000, \\
S_4 &= \alpha^{13} = 1101, S_5 = 0, S_6 = \alpha^6 = 1100.
\end{aligned}$$

6. Матрица

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^7 & \alpha^{14} & \alpha^3 \\ \alpha^{14} & \alpha^3 & \alpha^{13} \\ \alpha^3 & \alpha^{13} & 0 \end{bmatrix}, \det(M) = 0 + \alpha^{30} + \alpha^{30} + \alpha^9 + \alpha^{33} + 0 = \\
0 + 1 + 1 + \alpha^9 + \alpha^3 + 0 = 1010 + 1000 = 0010 = \alpha \neq 0.$$

Следовательно, произошло  $w = 3$  ошибки.

$$\text{Решить систему } \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} \begin{bmatrix} \lambda_3 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ -S_{v+3} \end{bmatrix}.$$

$$\begin{bmatrix} \alpha^7 & \alpha^{14} & \alpha^3 \\ \alpha^{14} & \alpha^3 & \alpha^{13} \\ \alpha^3 & \alpha^{13} & 0 \end{bmatrix} \begin{bmatrix} \lambda_3 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_4 \\ -S_5 \\ -S_6 \end{bmatrix} = \begin{bmatrix} \alpha^{13} \\ 0 \\ \alpha^6 \end{bmatrix}, \text{ откуда } \begin{bmatrix} \lambda_3 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} \alpha^{12} \\ \alpha^0 \\ \alpha^7 \end{bmatrix}.$$

Решение  $\lambda_3 = \alpha^{12}$ ,  $\lambda_2 = \alpha^0$ ,  $\lambda_1 = \alpha^7$ .

Полином локатора ошибок

$$\lambda(x) = \lambda_3 x^3 + \lambda_2 x^2 + \lambda_1 x + 1 = \alpha^{12} x^3 + \alpha^0 x^2 + \alpha^7 x + 1.$$

Используя процедуру Ченя (перебор элементов поля), находим корни  $\alpha^2$ ,  $\alpha^4$ ,  $\alpha^{12}$  для  $\lambda(x)$ . Именно

$$\begin{aligned}
\lambda(\alpha^2) &= \alpha^{12} (\alpha^2)^3 + \alpha^0 (\alpha^2)^2 + \alpha^7 (\alpha^2)^1 + 1 = \alpha^{18} + \alpha^4 + \alpha^9 + 1 = \\
&\alpha^3 + \alpha^4 + \alpha^9 + 1 = 1000 + 0011 + 1010 + 0001 = 0000 = 0.
\end{aligned}$$

$$\begin{aligned}
\lambda(\alpha^4) &= \alpha^{12} (\alpha^4)^3 + \alpha^0 (\alpha^4)^2 + \alpha^7 (\alpha^4)^1 + 1 = \alpha^{24} + \alpha^8 + \alpha^{11} + 1 = \\
&\alpha^9 + \alpha^8 + \alpha^{11} + 1 = 1010 + 0101 + 1110 + 0001 = 0000 = 0.
\end{aligned}$$

$$\begin{aligned}
\lambda(\alpha^{12}) &= \alpha^{12} (\alpha^{12})^3 + \alpha^0 (\alpha^{12})^2 + \alpha^7 (\alpha^{12})^1 + 1 = \alpha^{48} + \alpha^{24} + \alpha^{19} + 1 = \\
&\alpha^3 + \alpha^9 + \alpha^4 + 1 = 1000 + 1010 + 0011 + 0001 = 0000 = 0.
\end{aligned}$$

Тогда  $(\alpha^2)^{-1} = \alpha^{15-2} = \alpha^{13}$ ,  $(\alpha^4)^{-1} = \alpha^{15-4} = \alpha^{11}$ ,  $(\alpha^{12})^{-1} = \alpha^{15-12} = \alpha^3$ ,

ошибки произошли в третьей, одиннадцатой, тринадцатой позициях.

Полином ошибок  $e(x) = x^{13} + x^{11} + x^3$  и посланный кодовый полином

$$\begin{aligned}
u(x) &= v(x) + e(x) = (x^{14} + x^{12} + x^{11} + x^7 + x^5 + x^3 + x^2 + x) + (x^{13} + x^{11} + x^3) = \\
&x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^1 = 111000010100110 = u.
\end{aligned}$$

Информационное слово вычисляем перебором бинарных слов  $a$  длины пять, для которых  $a(x)g(x) = u(x)$ . Слово  $a = 11010 = x^4 + x^3 + x$ .

**Пример 16.** Несистематический ( $n=15$ ,  $k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай двух ошибок.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое число такое, что  $\beta^{q^r} = \beta$ .

$\beta = \alpha^1 = x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_1(x) &= (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$\begin{aligned} m(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &= x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ &= (\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \\ &= x^4 + (0010 + 0100 + 0011 + 0101)x^3 + (\alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12})x^2 + \\ &= (\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14})x + \alpha^{15} = \\ &= x^4 + 0x^3 + (1000 + 0110 + 1010 + 1100 + 0111 + 1111)x^2 + \\ &= (1011 + 1110 + 1101 + 1001)x + 1 = \\ &= x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1. \end{aligned}$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .

$\beta = \alpha^2 = x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_2(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^2)^{2^0})(x - (\alpha^2)^{2^1})(x - (\alpha^2)^{2^2})(x - (\alpha^2)^{2^3}) = \\ &= (x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = (x - (\alpha^3)^{2^0})(x - (\alpha^3)^{2^1})(x - (\alpha^3)^{2^2})(x - (\alpha^3)^{2^3}) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12})$ .

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned} m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^3\alpha^6 + \alpha^3\alpha^9 + \alpha^3\alpha^{12} + \alpha^6\alpha^9 + \alpha^6\alpha^{12} + \alpha^9\alpha^{12})x^2 + \\ &(\alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^9\alpha^{12} + \alpha^6\alpha^9\alpha^{12})x + \alpha^3\alpha^6\alpha^9\alpha^{12} = \\ &x^4 + (1000 + 1100 + 1010 + 1111)x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 + \\ &(\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} = \\ &x^4 + 1x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^3 + \alpha^6)x^2 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + \alpha^{15} = \\ &x^4 + 1x^3 + (1010 + 1111 + 0001 + 0001 + 1000 + 1100)x^2 + \\ &(1000 + 1100 + 1010 + 1111)x + 1 = \\ &x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^4)^{2^1} = \alpha^8 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = (\alpha^4)^{2^2} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{2^3} = (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_4(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &(x - (\alpha^4)^{2^0})(x - (\alpha^4)^{2^1})(x - (\alpha^4)^{2^2})(x - (\alpha^4)^{2^3}) = \\ &(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2+x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2+x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{2^1} = (\alpha^5)^{2^1} = \alpha^{10} = x^2+x+1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^5)^{2^2} = \alpha^{20} = \alpha^5 = x^2+x = \beta$ , то  $r=2$ ,  $r-1 = 1$ , и потому

$$m_5(x) = (x - \beta^{2^0})(x - \beta^{2^1}) = (x - (\alpha^5)^{2^0})(x - (\alpha^5)^{2^1}) =$$

$(x - \alpha^5)(x - \alpha^{10})$ . Положим множество  $M = \{\alpha^5, \alpha^{10}\}$ .

Тогда получаем следующее.

$$m_5(x) = C(M,0)x^2 + C(M,1)x + C(M,2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5 \alpha^{10})x^2 = x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1.$$

Для  $\beta = \alpha^5 = x^2 + x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$$\beta = \alpha^6 = x^3 + x^2. \text{ Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3 + x^2) = 5, \beta^5 = 1.$$

Так как  $\beta^{2^1} = (\alpha^6)^{2^1} = \alpha^{12} = x^3 + x^2 + x + 1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^6)^{2^2} = \alpha^{24} = \alpha^9 = x^3 + x + 1 \neq \beta$ ,  $\beta^{2^3} = (\alpha^6)^{2^3} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3 + x^2$ , то  $r = 4$ ,  $r-1=3$ , и потому

$$\begin{aligned} m_6(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^6)^{2^0})(x - (\alpha^6)^{2^1})(x - (\alpha^6)^{2^2})(x - (\alpha^6)^{2^3}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3 + x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического ( $n=15, k=5$ )-кода БЧХ есть полином

$$\begin{aligned} g(x) &= \text{HOK}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) = \\ m_1(x) \cdot m_3(x) \cdot m_5(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \\ g(x) &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \end{aligned}$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = \mathbf{a}$ .

5. Для несистематического (15,5)-кода БЧХ кодовое слово

$$\begin{aligned} u(x) &= a(x) \cdot g(x) = (x^4 + x^3 + x)(x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1) = \\ x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^5 + x &= 111000010100110. \end{aligned}$$

Принятое (искаженное) кодовое слово

$$v(x) = 101100010100110 = x^{14} + x^{12} + x^{11} + x^7 + x^5 + x^2 + x.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ . Умножения проводятся по модулю  $p(x) = x^4 + x + 1$ .

$$S_1 = v(\alpha^1) = \alpha^{14} + \alpha^{12} + \alpha^{11} + \alpha^7 + \alpha^5 + \alpha^2 + \alpha^1 =$$

$$1001 + 1111 + 1110 + 1011 + 0110 + 0100 + 0010 = 0011 = \alpha^4.$$

$$S_2 = v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{12} + (\alpha^2)^{11} + (\alpha^2)^7 + (\alpha^2)^5 + (\alpha^2)^2 + (\alpha^2)^1 =$$

$$\alpha^{28} + \alpha^{24} + \alpha^{22} + \alpha^{14} + \alpha^{10} + \alpha^4 + \alpha^2 =$$

$$\alpha^{13} + \alpha^9 + \alpha^7 + \alpha^{14} + \alpha^{10} + \alpha^4 + \alpha^2 =$$

$$1101 + 1010 + 1011 + 1001 + 0111 + 0011 + 0100 = 0101 = \alpha^8.$$

$$S_3 = v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{12} + (\alpha^3)^{11} + (\alpha^3)^7 + (\alpha^3)^5 + (\alpha^3)^2 + (\alpha^3)^1 =$$

$$\begin{aligned}\alpha^{42} + \alpha^{36} + \alpha^{33} + \alpha^{21} + \alpha^{15} + \alpha^6 + \alpha^3 = \\ \alpha^{12} + \alpha^6 + \alpha^3 + \alpha^6 + \alpha^0 + \alpha^6 + \alpha^3 = \\ 1111+1100+1000+1100+0001+1100+1000 = 0010 = \alpha^1.\end{aligned}$$

$$\begin{aligned}S_4 = v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{12} + (\alpha^4)^{11} + (\alpha^4)^7 + (\alpha^4)^5 + (\alpha^4)^2 + (\alpha^4)^1 = \\ \alpha^{56} + \alpha^{48} + \alpha^{44} + \alpha^{28} + \alpha^{20} + \alpha^8 + \alpha^4 = \\ \alpha^{11} + \alpha^3 + \alpha^{14} + \alpha^{13} + \alpha^5 + \alpha^8 + \alpha^4 = \\ 1110+1000+1001+1101+0110+0101+0011 = 0010 = \alpha^1.\end{aligned}$$

$$\begin{aligned}S_5 = v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{12} + (\alpha^5)^{11} + (\alpha^5)^7 + (\alpha^5)^5 + (\alpha^5)^2 + (\alpha^5)^1 = \\ \alpha^{70} + \alpha^{60} + \alpha^{55} + \alpha^{35} + \alpha^{25} + \alpha^{10} + \alpha^5 = \\ \alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^5 + \alpha^{10} + \alpha^{10} + \alpha^5 = \\ 0111+0001+0111+0110+0111+0111+0110 = 0001 = 1.\end{aligned}$$

$$\begin{aligned}S_6 = v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{12} + (\alpha^6)^{11} + (\alpha^6)^7 + (\alpha^6)^5 + (\alpha^6)^2 + (\alpha^6)^1 = \\ \alpha^{84} + \alpha^{72} + \alpha^{66} + \alpha^{42} + \alpha^{30} + \alpha^{12} + \alpha^6 = \\ \alpha^9 + \alpha^{12} + \alpha^6 + \alpha^{12} + \alpha^0 + \alpha^{12} + \alpha^6 = \\ 1010+1111+1100+1111+0001+1111+1100 = 0100 = \alpha^2.\end{aligned}$$

$$\begin{aligned}S_1 = \alpha^4 = 0011, S_2 = \alpha^8 = 0101, S_3 = \alpha^1 = 0010, \\ S_4 = \alpha^1 = 0010, S_5 = \alpha^0 = 1, S_6 = \alpha^2 = 00100.\end{aligned}$$

6. Матрица

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^4 & \alpha^8 & \alpha^1 \\ \alpha^8 & \alpha^1 & \alpha^1 \\ \alpha^1 & \alpha^1 & \alpha^0 \end{bmatrix}, \det(M) = \alpha^5 + \alpha^{10} + \alpha^{10} + \alpha^3 + \alpha^{16} + \alpha^6 = \\ \alpha^5 + \alpha^3 + \alpha^1 + \alpha^6 = 0110 + 1000 + 0010 + 1100 = 0000 = 0.$$

7. Матрица

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha^1 \end{bmatrix}, \det(M) = \alpha^5 + \alpha^{16} = \alpha^5 + \alpha^1 =$$

$$0110 + 0010 = 0100 \neq 0.$$

Следовательно, произошло  $w = 2$  ошибки.

$$\text{Решить систему } \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_3 \\ -S_4 \end{bmatrix}.$$

$$\begin{bmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha^1 \end{bmatrix} \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} \alpha^1 \\ \alpha^1 \end{bmatrix}, \text{ откуда } \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} \alpha^9 \\ \alpha^4 \end{bmatrix}.$$

$$\text{Решение } \lambda_2 = \alpha^9, \lambda_1 = \alpha^4.$$

Полином локатора ошибок

$$\lambda(x) = \lambda_2 x^2 + \lambda_1 x + 1 = \alpha^9 x^2 + \alpha^4 x + 1.$$

Используя процедуру Ченя (перебор элементов поля), находим корни  $\alpha^2, \alpha^4$  для  $\lambda(x)$ .

$$\lambda(\alpha^2) = \alpha^9 (\alpha^2)^2 + \alpha^4 (\alpha^2)^1 + 1 = \alpha^{13} + \alpha^6 + 1 = 1101+1100+0001 = 0.$$

$$\lambda(\alpha^4) = \alpha^9(\alpha^4)^2 + \alpha^4(\alpha^4)^1 + 1 = \alpha^{17} + \alpha^8 + 1 = \alpha^2 + \alpha^8 + 1 = \\ 0100 + 0101 + 0001 = 0000 = 0.$$

Тогда  $(\alpha^2)^{-1} = \alpha^{15-2} = \alpha^{13}$ ,  $(\alpha^4)^{-1} = \alpha^{15-4} = \alpha^{11}$ . Ошибки произошли в тринадцатой и одиннадцатой позициях. Полином ошибок  $e(x) = x^{13} + x^{11}$  и посланный кодовый полином

$$u(x) = v(x) + e(x) = (x^{14} + x^{12} + x^{11} + x^7 + x^5 + x^2 + x) + (x^{13} + x^{11}) = \\ x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^1 = 111000010100110 = u.$$

Информационное слово вычисляем перебором бинарных слов  $a$  длины пять, для которых  $a(x)g(x) = u(x)$ . Слово  $a = 11010 = x^4 + x^3 + x$ .

**Пример 1в.** Несистематический ( $n=15$ ,  $k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай одной ошибки.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое число такое, что  $\beta^{q^r} = \beta$ .

$$\beta = \alpha^1 = x. \text{Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha) = 15, \beta^{15} = 1.$$

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_1(x) = (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$m(x) = C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ (\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \\ x^4 + (0010 + 0100 + 0011 + 0101)x^3 + (\alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12})x^2 + \\ (\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14})x + \alpha^{15} = \\ x^4 + 0x^3 + (1000 + 0110 + 1010 + 1100 + 0111 + 1111)x^2 + \\ (1011 + 1110 + 1101 + 1001)x + 1 = \\ x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .

$$\beta = \alpha^2 = x^2. \text{Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15, \beta^{15} = 1.$$

Так как  $\beta^{2^1} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_2(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^2)^{2^0})(x - (\alpha^2)^{2^1})(x - (\alpha^2)^{2^2})(x - (\alpha^2)^{2^3}) = \\ &= (x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) =$

$$\begin{aligned} &(x - (\alpha^3)^{2^0})(x - (\alpha^3)^{2^1})(x - (\alpha^3)^{2^2})(x - (\alpha^3)^{2^3}) = \\ &(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = \\ &(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned} m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^3 \alpha^6 + \alpha^3 \alpha^9 + \alpha^3 \alpha^{12} + \alpha^6 \alpha^9 + \alpha^6 \alpha^{12} + \alpha^9 \alpha^{12})x^2 + \\ &(\alpha^3 \alpha^6 \alpha^9 + \alpha^3 \alpha^6 \alpha^{12} + \alpha^3 \alpha^9 \alpha^{12} + \alpha^6 \alpha^9 \alpha^{12})x + \alpha^3 \alpha^6 \alpha^9 \alpha^{12} = \\ &x^4 + (1000 + 1100 + 1010 + 1111)x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 + \\ &(\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} = \\ &x^4 + 1x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^3 + \alpha^6)x^2 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + \alpha^{15} = \\ &x^4 + 1x^3 + (1010 + 1111 + 0001 + 0001 + 1000 + 1100)x^2 + \\ &(1000 + 1100 + 1010 + 1111)x + 1 = \\ &x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^4)^{2^1} = \alpha^8 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = (\alpha^4)^{2^2} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{2^3} = (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_4(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^4)^{2^0})(x - (\alpha^4)^{2^1})(x - (\alpha^4)^{2^2})(x - (\alpha^4)^{2^3}) = \\ &= (x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2+x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2+x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{21} = (\alpha^5)^{21} = \alpha^{10} = x^2+x+1 \neq \beta$ ,  $\beta^{22} = (\alpha^5)^{22} = \alpha^{20} = \alpha^5 = x^2+x = \beta$ , то  $r=2$ ,  $r-1=1$ , и потому

$$m_5(x) = (x - \beta^{20})(x - \beta^{21}) = (x - (\alpha^5)^{20})(x - (\alpha^5)^{21}) =$$

$$(x - \alpha^5)(x - \alpha^{10}). \text{ Положим множество } M = \{\alpha^5, \alpha^{10}\}.$$

Тогда получаем следующее.

$$m_5(x) = C(M,0)x^2 + C(M,1)x + C(M,2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5 \alpha^{10})x^2 = x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1.$$

Для  $\beta = \alpha^5 = x^2+x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3+x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3+x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{21} = (\alpha^6)^{21} = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{22} = (\alpha^6)^{22} = \alpha^{24} = \alpha^9 = x^3+x+1 \neq \beta$ ,  $\beta^{23} = (\alpha^6)^{23} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{24} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3+x^2$ , то  $r=4$ ,

$r-1=3$ , и потому

$$m_6(x) = (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) = (x - (\alpha^6)^{20})(x - (\alpha^6)^{21})(x - (\alpha^6)^{22})(x - (\alpha^6)^{23}) = (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3+x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического ( $n=15, k=5$ )-кода БЧХ есть полином

$$g(x) = \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) =$$

$$m_1(x) \cdot m_3(x) \cdot m_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) =$$

$$(x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = \mathbf{a}$ .

5. Для несистематического ( $15,5$ )-кода БЧХ кодовое слово

$$u(x) = a(x) \cdot g(x) = (x^4 + x^3 + x)(x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1) = x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^5 + x = \mathbf{111000010100110}.$$

Принятое (искаженное) кодовое слово

$$v(x) = \mathbf{101000010100110} = x^{14} + x^{12} + x^7 + x^5 + x^2 + x.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ . Умножения проводятся по модулю  $p(x) = x^4 + x + 1$ .

$$S_1 = v(\alpha^1) = \alpha^{14} + \alpha^{12} + \alpha^{11} + \alpha^7 + \alpha^5 + \alpha^2 + \alpha^1 =$$

$$1001 + 1111 + 1011 + 0110 + 0100 + 0010 = 1101 = \alpha^{13}.$$

$$S_2 = v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{12} + (\alpha^2)^7 + (\alpha^2)^5 + (\alpha^2)^2 + (\alpha^2)^1 =$$

$$\alpha^{28} + \alpha^{24} + \alpha^{14} + \alpha^{10} + \alpha^4 + \alpha^2 =$$

$$\alpha^{13} + \alpha^9 + \alpha^{14} + \alpha^{10} + \alpha^4 + \alpha^2 =$$

$$1101 + 1010 + 1011 + 1001 + 0111 + 0011 + 0100 = 1110 = \alpha^{11}.$$

$$S_3 = v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{12} + (\alpha^3)^7 + (\alpha^3)^5 + (\alpha^3)^2 + (\alpha^3)^1 =$$

$$\alpha^{42} + \alpha^{36} + \alpha^{21} + \alpha^{15} + \alpha^6 + \alpha^3 =$$

$$\alpha^{12} + \alpha^6 + \alpha^6 + \alpha^0 + \alpha^6 + \alpha^3 =$$

$$1111 + 1100 + 1100 + 0001 + 1100 + 1000 = 1010 = \alpha^9.$$

$$S_4 = v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{12} + (\alpha^4)^7 + (\alpha^4)^5 + (\alpha^4)^2 + (\alpha^4)^1 =$$

$$\alpha^{56} + \alpha^{48} + \alpha^{28} + \alpha^{20} + \alpha^8 + \alpha^4 =$$

$$\alpha^{11} + \alpha^3 + \alpha^{13} + \alpha^5 + \alpha^8 + \alpha^4 =$$

$$1110 + 1000 + 1001 + 1101 + 0110 + 0101 + 0011 = 1011 = \alpha^7.$$

$$S_5 = v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{12} + (\alpha^5)^7 + (\alpha^5)^5 + (\alpha^5)^2 + (\alpha^5)^1 =$$

$$\alpha^{70} + \alpha^{60} + \alpha^{35} + \alpha^{25} + \alpha^{10} + \alpha^5 =$$

$$\alpha^{10} + \alpha^0 + \alpha^5 + \alpha^{10} + \alpha^{10} + \alpha^5 =$$

$$0111 + 0001 + 0111 + 0110 + 0111 + 0111 + 0110 = 0110 = \alpha^5.$$

$$S_6 = v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{12} + (\alpha^6)^7 + (\alpha^6)^5 + (\alpha^6)^2 + (\alpha^6)^1 =$$

$$\alpha^{84} + \alpha^{72} + \alpha^{42} + \alpha^{30} + \alpha^{12} + \alpha^6 =$$

$$\alpha^9 + \alpha^{12} + \alpha^{12} + \alpha^0 + \alpha^{12} + \alpha^6 =$$

$$1010 + 1111 + 1100 + 1111 + 0001 + 1111 + 1100 = 1000 = \alpha^3.$$

$$S_1 = \alpha^{13} = 1101, S_2 = \alpha^{11} = 1110, S_3 = \alpha^9 = 1010,$$

$$S_4 = \alpha^7 = 1011, S_5 = \alpha^5 = 0110, S_6 = \alpha^3 = 1000.$$

## 6. Матрица

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^{13} & \alpha^{11} & \alpha^9 \\ \alpha^{11} & \alpha^9 & \alpha^7 \\ \alpha^9 & \alpha^7 & \alpha^5 \end{bmatrix}, \det(M) = \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^7 = 0.$$

$$7. \text{Матрица } M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{13} & \alpha^{11} \\ \alpha^{11} & \alpha^9 \end{bmatrix}, \det(M) = \alpha^{22} + \alpha^{22} = 0.$$

$$8. \text{Матрица } M = [S_1] = [\alpha^{13}], \det(M) = \alpha^{13} \neq 0.$$

Произошла  $w = 1$  ошибка.

Решить уравнение  $S_1 \cdot \lambda_1 = -S_2, \alpha^{13} \cdot \lambda_1 = \alpha^{11}, \lambda_1 = \alpha^{-2} = \alpha^{15-2} = \alpha^{13}$ .

Полином локатора ошибок

$$\lambda(x) = \lambda_1 x + 1 = \alpha^{13} x + 1.$$

Используя процедуру Ченя (перебор элементов поля), находим корень уравнения  $\alpha^{13}x + 1 = 0$ . Отсюда  $\alpha^{13}x = -1 = 1$ ,  $x = \alpha^2$ , ибо  $\alpha^{13} \cdot \alpha^2 = \alpha^{15} = 1$ .

Тогда  $(\alpha^2)^{-1} = \alpha^{15-2} = \alpha^{13}$ . Ошибка произошла в тринадцатой позиции. Полином ошибок  $e(x) = x^{13}$  и посланный кодовый полином

$$u(x) = v(x) + e(x) = (x^{14} + x^{12} + x^{11} + x^7 + x^5 + x^2 + x) + (x^{13}) = \\ x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^1 = 111000010100110 = u.$$

Информационное слово вычисляем перебором бинарных слов  $a$  длины пять, для которых  $a(x)g(x) = u(x)$ . Слово  $a = 11010 = x^4 + x^3 + x$ .

**Пример 1г.** Несистематический ( $n=15$ ,  $k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай отсутствия ошибок.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое такое, что  $\beta^{q^r} = \beta$ .

$\beta = \alpha^1 = x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_1(x) = (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$m(x) = C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ (\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \\ x^4 + (0010 + 0100 + 0011 + 0101)x^3 + (\alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12})x^2 + \\ (\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14})x + \alpha^{15} = \\ x^4 + 0x^3 + (1000 + 0110 + 1010 + 1100 + 0111 + 1111)x^2 + \\ (1011 + 1110 + 1101 + 1001)x + 1 = \\ x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .

$\beta = \alpha^2 = x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_2(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^2)^{2^0})(x - (\alpha^2)^{2^1})(x - (\alpha^2)^{2^2})(x - (\alpha^2)^{2^3}) = \\ &= (x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) =$

$$\begin{aligned} &(x - (\alpha^3)^{2^0})(x - (\alpha^3)^{2^1})(x - (\alpha^3)^{2^2})(x - (\alpha^3)^{2^3}) = \\ &(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = \\ &(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned} m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^3\alpha^6 + \alpha^3\alpha^9 + \alpha^3\alpha^{12} + \alpha^6\alpha^9 + \alpha^6\alpha^{12} + \alpha^9\alpha^{12})x^2 + \\ &(\alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^9\alpha^{12} + \alpha^6\alpha^9\alpha^{12})x + \alpha^3\alpha^6\alpha^9\alpha^{12} = \\ &x^4 + (1000 + 1100 + 1010 + 1111)x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 + \\ &(\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} = \\ &x^4 + 1x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^3 + \alpha^6)x^2 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + \alpha^{15} = \\ &x^4 + 1x^3 + (1010 + 1111 + 0001 + 0001 + 1000 + 1100)x^2 + \\ &(1000 + 1100 + 1010 + 1111)x + 1 = \\ &x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^4)^{2^1} = \alpha^8 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = (\alpha^4)^{2^2} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{2^3} = (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_4(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^4)^{2^0})(x - (\alpha^4)^{2^1})(x - (\alpha^4)^{2^2})(x - (\alpha^4)^{2^3}) = \\ &= (x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2+x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2+x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{21} = (\alpha^5)^{21} = \alpha^{10} = x^2+x+1 \neq \beta$ ,  $\beta^{22} = (\alpha^5)^{22} = \alpha^{20} = \alpha^5 = x^2+x = \beta$ , то  $r=2$ ,  $r-1=1$ , и потому

$$m_5(x) = (x - \beta^{20})(x - \beta^{21}) = (x - (\alpha^5)^{20})(x - (\alpha^5)^{21}) = \\ (x - \alpha^5)(x - \alpha^{10}). \text{ Положим множество } M = \{\alpha^5, \alpha^{10}\}.$$

Тогда получаем следующее.

$$m_5(x) = C(M,0)x^2 + C(M,1)x + C(M,2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5 \alpha^{10})x^2 = \\ x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1.$$

Для  $\beta = \alpha^5 = x^2+x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3+x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3+x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{21} = (\alpha^6)^{21} = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{22} = (\alpha^6)^{22} = \alpha^{24} = \alpha^9 = x^3+x+1 \neq \beta$ ,  $\beta^{23} = (\alpha^6)^{23} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{24} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3+x^2$ , то  $r=4$ ,  $r-1=3$ , и потому

$$m_6(x) = (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) = \\ (x - (\alpha^6)^{20})(x - (\alpha^6)^{21})(x - (\alpha^6)^{22})(x - (\alpha^6)^{23}) = \\ (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = \\ (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = \\ (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3+x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического ( $n=15, k=5$ )-кода БЧХ есть полином

$$g(x) = \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) = \\ m_1(x) \cdot m_3(x) \cdot m_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \\ g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = \mathbf{a}$ .

5. Для несистематического ( $15,5$ )-кода БЧХ кодовое слово

$$u(x) = a(x) \cdot g(x) = (x^4 + x^3 + x)(x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1) = \\ x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^5 + x = 111000010100110.$$

Принятое (не искаженное) кодовое слово

$$v(x) = 111000010100110 = x^{14} + x^{13} + x^{12} + x^7 + x^5 + x^2 + x^5 + x.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ . Умножения проводятся по модулю  $p(x) = x^4 + x + 1$ .

$$S_1 = v(\alpha^1) = \alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^{11} + \alpha^7 + \alpha^5 + \alpha^2 + \alpha^1 =$$

$$1001 + 1101 + 1111 + 1011 + 0110 + 0100 + 0010 = 0000 = 0.$$

$$S_2 = v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{13} + (\alpha^2)^{12} + (\alpha^2)^7 + (\alpha^2)^5 + (\alpha^2)^2 + (\alpha^2)^1 =$$

$$\alpha^{28} + \alpha^{26} + \alpha^{24} + \alpha^{14} + \alpha^{10} + \alpha^4 + \alpha^2 =$$

$$\alpha^{13} + \alpha^{11} + \alpha^9 + \alpha^{14} + \alpha^{10} + \alpha^4 + \alpha^2 =$$

$$1101 + 1110 + 1010 + 1011 + 1001 + 0111 + 0011 + 0100 = 0000 = 0.$$

$$S_3 = v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{13} + (\alpha^3)^{12} + (\alpha^3)^7 + (\alpha^3)^5 + (\alpha^3)^2 + (\alpha^3)^1 =$$

$$\alpha^{42} + \alpha^{39} + \alpha^{36} + \alpha^{21} + \alpha^{15} + \alpha^6 + \alpha^3 =$$

$$\alpha^{12} + \alpha^9 + \alpha^6 + \alpha^6 + \alpha^0 + \alpha^6 + \alpha^3 =$$

$$1111 + 1010 + 1100 + 1100 + 0001 + 1100 + 1000 = 0000 = 0.$$

$$S_4 = v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{13} + (\alpha^4)^{12} + (\alpha^4)^7 + (\alpha^4)^5 + (\alpha^4)^2 + (\alpha^4)^1 =$$

$$\alpha^{56} + \alpha^{52} + \alpha^{48} + \alpha^{28} + \alpha^{20} + \alpha^8 + \alpha^4 =$$

$$\alpha^{11} + \alpha^7 + \alpha^3 + \alpha^{13} + \alpha^5 + \alpha^8 + \alpha^4 =$$

$$1110 + 1011 + 1000 + 1001 + 1101 + 0110 + 0101 + 0011 = 0000 = 0.$$

$$S_5 = v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{13} + (\alpha^5)^{12} + (\alpha^5)^7 + (\alpha^5)^5 + (\alpha^5)^2 + (\alpha^5)^1 =$$

$$\alpha^{70} + \alpha^{65} + \alpha^{60} + \alpha^{35} + \alpha^{25} + \alpha^{10} + \alpha^5 =$$

$$\alpha^{10} + \alpha^5 + \alpha^0 + \alpha^5 + \alpha^{10} + \alpha^{10} + \alpha^5 =$$

$$0111 + 0110 + 0001 + 0111 + 0110 + 0111 + 0110 = 0000 = 0.$$

$$S_6 = v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{13} + (\alpha^6)^{12} + (\alpha^6)^7 + (\alpha^6)^5 + (\alpha^6)^2 + (\alpha^6)^1 =$$

$$\alpha^{84} + \alpha^{78} + \alpha^{72} + \alpha^{42} + \alpha^{30} + \alpha^{12} + \alpha^6 =$$

$$\alpha^9 + \alpha^3 + \alpha^{12} + \alpha^{12} + \alpha^0 + \alpha^{12} + \alpha^6 =$$

$$1010 + 1000 + 1111 + 1100 + 1111 + 0001 + 1111 + 1100 = 0000 = 0.$$

$$S_1 = 0, S_2 = 0, S_3 = 0, S_4 = 0, S_5 = 0, S_6 = 0.$$

## 6. Матрица

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \det(M) = 0.$$

При передаче ошибок нет. Поэтому  $v(x) = u(x) = 111000010100110$ .

Информационное слово вычисляем перебором бинарных слов  $a$  длины пять, для которых  $a(x)g(x) = u(x)$ . Слово  $a = 11010 = x^4 + x^3 + x$ .

**Пример 2а.** Систематический ( $n=15, k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай трех ошибок.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое число такое, что  $\beta^{q^r} = \beta$ .

$$\beta = \alpha^1 = x. \text{ Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha) = 15, \beta^{15} = 1.$$

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2, \beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1, \beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1, \beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4, r-1 = 3$ , и потому

$$m_1(x) = (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$m(x) = C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ (\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \\ x^4 + (0010 + 0100 + 0011 + 0101)x^3 + (\alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12})x^2 + \\ (\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14})x + \alpha^{15} = \\ x^4 + 0x^3 + (1000 + 0110 + 1010 + 1100 + 0111 + 1111)x^2 + \\ (1011 + 1110 + 1101 + 1001)x + 1 = \\ x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .

$$\beta = \alpha^2 = x^2. \text{ Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15, \beta^{15} = 1.$$

Так как  $\beta^{2^1} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta, \beta^{2^2} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta, \beta^{2^3} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta, \beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4, r-1 = 3$ , и потому

$$m_2(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ (x - (\alpha^2)^{2^0})(x - (\alpha^2)^{2^1})(x - (\alpha^2)^{2^2})(x - (\alpha^2)^{2^3}) = \\ (x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$$\beta = \alpha^3 = x^3. \text{ Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5, \beta^5 = (\alpha^3)^5 = \alpha^{15} = 1.$$

Так как  $\beta^{2^1} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta, \beta^{2^2} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta, \beta^{2^3} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta, \beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4, r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) =$

$$(x - (\alpha^3)^{2^0})(x - (\alpha^3)^{2^1})(x - (\alpha^3)^{2^2})(x - (\alpha^3)^{2^3}) =$$

$$(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) =$$

$$(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$m_3(x) = C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) =$$

$$x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^3\alpha^6 + \alpha^3\alpha^9 + \alpha^3\alpha^{12} + \alpha^6\alpha^9 + \alpha^6\alpha^{12} + \alpha^9\alpha^{12})x^2 +$$

$$(\alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^9\alpha^{12} + \alpha^6\alpha^9\alpha^{12})x + \alpha^3\alpha^6\alpha^9\alpha^{12} =$$

$$x^4 + (1000 + 1100 + 1010 + 1111)x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 +$$

$$(\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} =$$

$$x^4 + 1x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{15} + \alpha^3 + \alpha^6)x^2 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + \alpha^{15} =$$

$$x^4 + 1x^3 + (1010 + 1111 + 0001 + 0001 + 1000 + 1100)x^2 +$$

$$(1000 + 1100 + 1010 + 1111)x + 1 =$$

$$x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1.$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{21} = (\alpha^4)^{21} = \alpha^8 = x^3 + x^2 \neq \beta$ ,  $\beta^{22} = (\alpha^4)^{22} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{23} = (\alpha^4)^{23} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$   $\beta^{24} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_4(x) = (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) =$$

$$(x - (\alpha^4)^{20})(x - (\alpha^4)^{21})(x - (\alpha^4)^{22})(x - (\alpha^4)^{23}) =$$

$$(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2)$$

$$= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2 + x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2 + x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{21} = (\alpha^5)^{21} = \alpha^{10} = x^2 + x + 1 \neq \beta$ ,  $\beta^{22} = (\alpha^5)^{22} = \alpha^{20} = \alpha^5 = x^2 + x = \beta$ , то  $r = 2$ ,  $r-1 = 1$ , и потому

$$m_5(x) = (x - \beta^{20})(x - \beta^{21}) = (x - (\alpha^5)^{20})(x - (\alpha^5)^{21}) =$$

$$(x - \alpha^5)(x - \alpha^{10}).$$

Положим множество  $M = \{\alpha^5, \alpha^{10}\}$ .

Тогда получаем следующее.

$$m_5(x) = C(M,0)x^2 + C(M,1)x + C(M,2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5\alpha^{10})x^2 =$$

$$x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1.$$

Для  $\beta = \alpha^5 = x^2 + x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3 + x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3 + x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{2^1} = (\alpha^6)^{2^1} = \alpha^{12} = x^3 + x^2 + x + 1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^6)^{2^2} = \alpha^{24} = \alpha^9 = x^3 + x + 1 \neq \beta$ ,  $\beta^{2^3} = (\alpha^6)^{2^3} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3 + x^2$ , то  $r = 4$ ,  $r-1=3$ , и потому

$$\begin{aligned} m_6(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^6)^{2^0})(x - (\alpha^6)^{2^1})(x - (\alpha^6)^{2^2})(x - (\alpha^6)^{2^3}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3 + x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического и систематического ( $n=15, k=5$ )-кода БЧХ есть полином

$$\begin{aligned} g(x) &= \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) = \\ m_1(x) \cdot m_3(x) \cdot m_5(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \\ g(x) &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \end{aligned}$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = a$ .

Для систематического (15,5)-кода БЧХ кодовый полином

$$u(x) = x^{n-k} a(x) + (x^{n-k} a(x)) \pmod{g(x)} = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)},$$

5. Кодовое слово

$$\begin{aligned} u(x) &= x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)} = \\ x^{10}(x^4 + x^3 + x) + (x^{10} \cdot (x^4 + x^3 + x)) \pmod{g(x)} &= \\ (x^{14} + x^{13} + x^{11}) + (x^{14} + x^{13} + x^{11}) \pmod{g(x)} &= \\ (x^{14} + x^{13} + x^{11}) + (x^9 + x^8 + x^5 + x + 1) &= \\ x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x + 1 &= 110101100100011. \end{aligned}$$

Принятое (искаженное) кодовое слово

$$v(x) = 100001100101011 = x^{14} + x^9 + x^8 + x^5 + x^3 + x^1 + 1.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ . Умножения проводятся по модулю  $p(x) = x^4 + x + 1$ .

$$S_1 = v(\alpha^1) = \alpha^{14} + \alpha^9 + \alpha^8 + \alpha^5 + \alpha^3 + \alpha^1 + 1 =$$

$$1001 + 1010 + 0101 + 0110 + 1000 + 0010 + 0001 = 1011 = \alpha^7.$$

$$S_2 = v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^9 + (\alpha^2)^8 + (\alpha^2)^5 + (\alpha^2)^3 + (\alpha^2)^1 + 1 =$$

$$\alpha^{28} + \alpha^{18} + \alpha^{16} + \alpha^{10} + \alpha^6 + \alpha^2 + 1 =$$

$$\alpha^{13} + \alpha^3 + \alpha^1 + \alpha^{10} + \alpha^6 + \alpha^2 + 1 =$$

$$1101 + 1000 + 0010 + 0111 + 1100 + 0100 + 0001 = 1001 = \alpha^{14}.$$

$$S_3 = v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^9 + (\alpha^3)^8 + (\alpha^3)^5 + (\alpha^3)^3 + (\alpha^3)^1 + 1 =$$

$$\alpha^{42} + \alpha^{27} + \alpha^{24} + \alpha^{15} + \alpha^9 + \alpha^3 + 1 =$$

$$\alpha^{12} + \alpha^{12} + \alpha^9 + \alpha^0 + \alpha^9 + \alpha^3 + 1 =$$

$$\begin{aligned}
& 1111+1111+1010+0001+1010+1000+0001 = 1000 = \alpha^3. \\
& S_4 = v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^9 + (\alpha^4)^8 + (\alpha^4)^5 + (\alpha^4)^3 + (\alpha^4)^1 + 1 = \\
& \alpha^{56} + \alpha^{36} + \alpha^{32} + \alpha^{20} + \alpha^{12} + \alpha^4 + 1 = \\
& \alpha^{11} + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^{12} + \alpha^4 + 1 = \\
& 1110+1100+0100+0110+1111+0011+0001 = 1101 = \alpha^{13}. \\
& S_5 = v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^9 + (\alpha^5)^8 + (\alpha^5)^5 + (\alpha^5)^3 + (\alpha^5)^1 + 1 = \\
& \alpha^{70} + \alpha^{45} + \alpha^{40} + \alpha^{25} + \alpha^{15} + \alpha^5 + 1 = \\
& \alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^{10} + \alpha^0 + \alpha^5 + 1 = \\
& 0111+0001+0111+0111+0001+0110+0001 = 0000 = 0. \\
& S_6 = v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^9 + (\alpha^6)^8 + (\alpha^6)^5 + (\alpha^6)^3 + (\alpha^6)^1 + 1 = \\
& \alpha^{84} + \alpha^{54} + \alpha^{48} + \alpha^{30} + \alpha^{18} + \alpha^6 + 1 = \\
& \alpha^9 + \alpha^9 + \alpha^3 + \alpha^0 + \alpha^3 + \alpha^6 + 1 = \\
& 1010+1010+1000+0001+1000+1100+0001 = 1100 = \alpha^6. \\
& S_1 = \alpha^7 = 1011, S_2 = \alpha^{14} = 1001, S_3 = \alpha^3 = 1000, \\
& S_4 = \alpha^{13} = 1101, S_5 = 0, S_6 = \alpha^6 = 1100.
\end{aligned}$$

6. Пусть размерность матрицы  $M$  (число ошибок)  $v = 3$ .

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^7 & \alpha^{14} & \alpha^3 \\ \alpha^{14} & \alpha^3 & \alpha^{13} \\ \alpha^3 & \alpha^{13} & 0 \end{bmatrix}, \det(M) = 0 + \alpha^{30} + \alpha^{30} + \alpha^9 + \alpha^{33} + 0 = 0 + 1 + 1 + \alpha^9 + \alpha^3 + 0 = 1010 + 1000 = 0010 = \alpha \neq 0.$$

Следовательно, произошло  $w = 3$  ошибки.

$$\text{Решить систему } \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} \begin{bmatrix} \lambda_3 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ -S_{v+3} \end{bmatrix},$$

$$\begin{bmatrix} \alpha^7 & \alpha^{14} & \alpha^3 \\ \alpha^{14} & \alpha^3 & \alpha^{13} \\ \alpha^3 & \alpha^{13} & 0 \end{bmatrix} \begin{bmatrix} \lambda_3 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_4 \\ -S_5 \\ -S_6 \end{bmatrix} = \begin{bmatrix} \alpha^{13} \\ 0 \\ \alpha^6 \end{bmatrix}, \text{ откуда } \begin{bmatrix} \lambda_3 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} \alpha^{12} \\ \alpha^0 \\ \alpha^7 \end{bmatrix}.$$

$$\lambda_1 = \alpha^7, \lambda_2 = \alpha^0 = 1, \lambda_3 = \alpha^{12}.$$

Полином локатора ошибок

$$\lambda(x) = \lambda_3 x^3 + \lambda_2 x^2 + \lambda_1 x + 1 = \alpha^{12} x^3 + \alpha^0 x^2 + \alpha^7 x + 1.$$

Используя процедуру Ченя (перебор элементов поля), находим корни  $\alpha^2, \alpha^4, \alpha^{12}$  для  $\lambda(x)$ . Именно

$$\begin{aligned}
\lambda(\alpha^2) &= \alpha^{12}(\alpha^2)^3 + \alpha^0(\alpha^2)^2 + \alpha^7(\alpha^2)^1 + 1 = \alpha^{18} + \alpha^4 + \alpha^9 + 1 = \\
&\alpha^3 + \alpha^4 + \alpha^9 + 1 = 1000 + 0011 + 1010 + 0001 = 0000 = 0. \\
\lambda(\alpha^4) &= \alpha^{12}(\alpha^4)^3 + \alpha^0(\alpha^4)^2 + \alpha^7(\alpha^4)^1 + 1 = \alpha^{24} + \alpha^8 + \alpha^{11} + 1 = \\
&\alpha^9 + \alpha^8 + \alpha^{11} + 1 = 1010 + 0101 + 1110 + 0001 = 0000 = 0.
\end{aligned}$$

$$\begin{aligned}\lambda(\alpha^{12}) &= \alpha^{12}(\alpha^{12})^3 + \alpha^0(\alpha^{12})^2 + \alpha^7(\alpha^{12})^1 + 1 = \alpha^{48} + \alpha^{24} + \alpha^{19} + 1 = \\ &\alpha^3 + \alpha^9 + \alpha^4 + 1 = 1000 + 1010 + 0011 + 0001 = 0000 = 0.\end{aligned}$$

Тогда  $(\alpha^2)^{-1} = \alpha^{15-2} = \alpha^{13}$ ,  $(\alpha^4)^{-1} = \alpha^{15-4} = \alpha^{11}$ ,  $(\alpha^{12})^{-1} = \alpha^{15-12} = \alpha^3$ ,

Ошибки произошли в третьей, одиннадцатой, тринадцатой позициях.  
Полином ошибок  $e(x) = x^{13} + x^{11} + x^3$  и посланный кодовый полином

$$\begin{aligned}u(x) &= v(x) + e(x) = (x^{14} + x^9 + x^8 + x^5 + x^3 + x^1 + 1) + (x^{13} + x^{11} + x^3) = \\ &x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x^1 + 1 = 110101100100011 = \mathbf{u}.\end{aligned}$$

Первые пять позиций в  $\mathbf{u}$  есть информационное слово  $a = 11010$ .

**Пример 26.** Систематический ( $n=15$ ,  $k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай двух ошибок.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое число такое, что  $\beta^{q^r} = \beta$ .

$\beta = \alpha^1 = x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned}m_1(x) &= (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ &(x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).\end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$\begin{aligned}m(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ &(\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \\ &x^4 + (0010 + 0100 + 0011 + 0101)x^3 + (\alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12})x^2 + \\ &(\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14})x + \alpha^{15} = \\ &x^4 + 0x^3 + (1000 + 0110 + 1010 + 1100 + 0111 + 1111)x^2 + \\ &(1011 + 1110 + 1101 + 1001)x + 1 = \\ &x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.\end{aligned}$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .

$\beta = \alpha^2 = x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_2(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^2)^{2^0})(x - (\alpha^2)^{2^1})(x - (\alpha^2)^{2^2})(x - (\alpha^2)^{2^3}) = \\ &= (x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{2^3} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) =$

$$\begin{aligned} &(x - (\alpha^3)^{2^0})(x - (\alpha^3)^{2^1})(x - (\alpha^3)^{2^2})(x - (\alpha^3)^{2^3}) = \\ &(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = \\ &(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned} m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^3 \alpha^6 + \alpha^3 \alpha^9 + \alpha^3 \alpha^{12} + \alpha^6 \alpha^9 + \alpha^6 \alpha^{12} + \alpha^9 \alpha^{12})x^2 + \\ &(\alpha^3 \alpha^6 \alpha^9 + \alpha^3 \alpha^6 \alpha^{12} + \alpha^3 \alpha^9 \alpha^{12} + \alpha^6 \alpha^9 \alpha^{12})x + \alpha^3 \alpha^6 \alpha^9 \alpha^{12} = \\ &x^4 + (1000 + 1100 + 1010 + 1111)x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 + \\ &(\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} = \\ &x^4 + 1x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^3 + \alpha^6)x^2 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + \alpha^{15} = \\ &x^4 + 1x^3 + (1010 + 1111 + 0001 + 0001 + 1000 + 1100)x^2 + \\ &(1000 + 1100 + 1010 + 1111)x + 1 = \\ &x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^4)^{2^1} = \alpha^8 = x^3+x^2 \neq \beta$ ,  $\beta^{2^2} = (\alpha^4)^{2^2} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{2^3} = (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_4(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^4)^{2^0})(x - (\alpha^4)^{2^1})(x - (\alpha^4)^{2^2})(x - (\alpha^4)^{2^3}) = \\ &= (x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2+x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2+x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{21} = (\alpha^5)^{21} = \alpha^{10} = x^2+x+1 \neq \beta$ ,  $\beta^{22} = (\alpha^5)^{22} = \alpha^{20} = \alpha^5 = x^2+x = \beta$ , то  $r=2$ ,  $r-1=1$ , и потому

$$m_5(x) = (x - \beta^{20})(x - \beta^{21}) = (x - (\alpha^5)^{20})(x - (\alpha^5)^{21}) =$$

$$(x - \alpha^5)(x - \alpha^{10}). \text{ Положим множество } M = \{\alpha^5, \alpha^{10}\}.$$

Тогда получаем следующее.

$$m_5(x) = C(M,0)x^2 + C(M,1)x + C(M,2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5 \alpha^{10})x^2 = x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1.$$

Для  $\beta = \alpha^5 = x^2+x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3+x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3+x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{21} = (\alpha^6)^{21} = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{22} = (\alpha^6)^{22} = \alpha^{24} = \alpha^9 = x^3+x+1 \neq \beta$ ,  $\beta^{23} = (\alpha^6)^{23} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{24} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3+x^2$ , то  $r=4$ ,

$r-1=3$ , и потому

$$m_6(x) = (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) = (x - (\alpha^6)^{20})(x - (\alpha^6)^{21})(x - (\alpha^6)^{22})(x - (\alpha^6)^{23}) = (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3+x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического и систематического ( $n=15$ ,  $k=5$ )-кода БЧХ есть полином

$$g(x) = \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) = m_1(x) \cdot m_3(x) \cdot m_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = a$ .

Для систематического (15,5)-кода БЧХ кодовый полином

$$u(x) = x^{n-k} a(x) + (x^{n-k} a(x)) \pmod{g(x)} = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)},$$

5. Кодовое слово

$$u(x) = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)} =$$

$$\begin{aligned}
&x^{10}(x^4 + x^3 + x) + (x^{10} \cdot (x^4 + x^3 + x)) \pmod{g(x)} = \\
&(x^{14} + x^{13} + x^{11}) + (x^{14} + x^{13} + x^{11}) \pmod{g(x)} = \\
&(x^{14} + x^{13} + x^{11}) + (x^9 + x^8 + x^5 + x + 1) = \\
&x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x + 1 = \mathbf{110101100100011}.
\end{aligned}$$

Принятое кодовое слово

$$v(x) = \mathbf{100101100101011} = x^{14} + x^{11} + x^9 + x^8 + x^5 + x^3 + x^1 + 1.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ .

$$\begin{aligned}
S_1 &= v(\alpha^1) = \alpha^{14} + \alpha^{11} + \alpha^9 + \alpha^8 + \alpha^5 + \alpha^3 + \alpha^1 + 1 = \\
&1001 + 1110 + 0101 + 0110 + 1000 + 0010 + 0001 = 0101 = \alpha^8. \\
S_2 &= v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{11} + (\alpha^2)^9 + (\alpha^2)^8 + (\alpha^2)^5 + (\alpha^2)^3 + (\alpha^2)^1 + 1 = \\
&\alpha^{28} + \alpha^{22} + \alpha^{18} + \alpha^{16} + \alpha^{10} + \alpha^6 + \alpha^2 + 1 = \\
&\alpha^{13} + \alpha^7 + \alpha^3 + \alpha^1 + \alpha^{10} + \alpha^6 + \alpha^2 + 1 = \\
&1101 + 1011 + 1000 + 0010 + 0111 + 1100 + 0100 + 0001 = 0010 = \alpha^1. \\
S_3 &= v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{11} + (\alpha^3)^9 + (\alpha^3)^8 + (\alpha^3)^5 + (\alpha^3)^3 + (\alpha^3)^1 + 1 = \\
&\alpha^{42} + \alpha^{33} + \alpha^{27} + \alpha^{24} + \alpha^{15} + \alpha^9 + \alpha^3 + 1 = \\
&\alpha^{12} + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^0 + \alpha^9 + \alpha^3 + 1 = \\
&1111 + 1000 + 1111 + 1010 + 0001 + 1010 + 1000 + 0001 = 0000 = 0. \\
S_4 &= v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{11} + (\alpha^4)^9 + (\alpha^4)^8 + (\alpha^4)^5 + (\alpha^4)^3 + (\alpha^4)^1 + 1 = \\
&\alpha^{56} + \alpha^{44} + \alpha^{36} + \alpha^{32} + \alpha^{20} + \alpha^{12} + \alpha^4 + 1 = \\
&\alpha^{11} + \alpha^{14} + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^{12} + \alpha^4 + 1 = \\
&1110 + 1001 + 1100 + 0100 + 0110 + 1111 + 0011 + 0001 = 0100 = \alpha^2. \\
S_5 &= v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{11} + (\alpha^5)^9 + (\alpha^5)^8 + (\alpha^5)^5 + (\alpha^5)^3 + (\alpha^5)^1 + 1 = \\
&\alpha^{70} + \alpha^{55} + \alpha^{45} + \alpha^{40} + \alpha^{25} + \alpha^{15} + \alpha^5 + 1 = \\
&\alpha^{10} + \alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^{10} + \alpha^0 + \alpha^5 + 1 = \\
&0111 + 0111 + 0001 + 0111 + 0111 + 0001 + 0110 + 0001 = 0111 = \alpha^{10}. \\
S_6 &= v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{11} + (\alpha^6)^9 + (\alpha^6)^8 + (\alpha^6)^5 + (\alpha^6)^3 + (\alpha^6)^1 + 1 = \\
&\alpha^{84} + \alpha^{66} + \alpha^{54} + \alpha^{48} + \alpha^{30} + \alpha^{18} + \alpha^6 + 1 = \\
&\alpha^9 + \alpha^6 + \alpha^9 + \alpha^3 + \alpha^0 + \alpha^3 + \alpha^6 + 1 = \\
&1010 + 1100 + 1010 + 1000 + 0001 + 1000 + 1100 + 0001 = 0011 = \alpha^4.
\end{aligned}$$

$$S_1 = \alpha^8 = 0101, S_2 = \alpha^1 = 0010, S_3 = 0,$$

$$S_4 = \alpha^2 = 0100, S_5 = \alpha^{10} = 0111, S_6 = \alpha^4 = 0011.$$

6. Пусть (число ошибок)  $v = 3$ .

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^8 & \alpha^1 & 0 \\ \alpha^1 & 0 & \alpha^2 \\ 0 & \alpha^2 & \alpha^{10} \end{bmatrix}, \det(M) = 0 + 0 + 0 + 0 + \alpha^{12} + \alpha^{12} = 0.$$

$$7. \text{ Положить } v = 2. M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^8 & \alpha^1 \\ \alpha^1 & 0 \end{bmatrix}, \det(M) = \alpha^2 \neq 0.$$

Следовательно, произошло  $w = 2$  ошибки.

Решить систему  $\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{\nu+1} \\ -S_{\nu+2} \end{bmatrix}, \begin{bmatrix} \alpha^8 & \alpha^1 \\ \alpha^1 & 0 \end{bmatrix} \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_3 \\ -S_4 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha^2 \end{bmatrix}$ ,

откуда  $\begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} \alpha^1 \\ \alpha^8 \end{bmatrix}, \lambda_2 = \alpha^1, \lambda_1 = \alpha^8$ .

Полином локатора ошибок  $\lambda(x) = \lambda_2 x^2 + \lambda_1 x + 1 = \alpha^1 x^2 + \alpha^8 x + 1$ .

Используя процедуру Ченя (перебор элементов поля), находим корни  $\alpha^2$  и  $\alpha^{13}$  для  $\lambda(x)$ .

$$\lambda(\alpha^2) = \alpha^1 (\alpha^2)^2 + \alpha^8 \alpha^2 + 1 = \alpha^5 + \alpha^{10} + 1 = 0110 + 0111 + 0001 = 0000 = 0.$$

$$\lambda(\alpha^{13}) = \alpha^1 (\alpha^{13})^2 + \alpha^8 \alpha^{13} + 1 = \alpha^{25} + \alpha^{20} + 1 = \alpha^{10} + \alpha^5 + 1 =$$

$$0111 + 0110 + 0001 = 0000 = 0.$$

Тогда  $(\alpha^2)^{-1} = \alpha^{15-2} = \alpha^{13}$ ,  $(\alpha^{12})^{-1} = \alpha^{15-12} = \alpha^3$ . Ошибки произошли в третьей и тринадцатой позициях. Полином ошибок  $e(x) = x^{13} + x^3$ , и посланный кодовый полином  $u(x) = v(x) + e(x) = (x^{14} + x^{11} + x^9 + x^8 + x^5 + x^3 + x^1 + 1) + (x^{13} + x^3) = u(x) = x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x^1 + 1 = 110101100100011 = u$ . Первые пять позиций в  $u$  есть информационное слово  $a = 11010$ .

**Пример 2в.** Систематический ( $n=15$ ,  $k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай одной ошибки.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое число такое, что  $\beta^{q^r} = \beta$ .

$$\beta = \alpha^1 = x. \text{ Степени } \alpha^t = \alpha^{\text{mod}(t,15)}, \beta^t = \beta^{\text{mod}(t,15)}.$$

$$\text{Порядок } \text{ord}(\beta) = \text{ord}(\alpha) = 15, \beta^{15} = 1.$$

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_1(x) = (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = \\ (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$m(x) = C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1 \alpha^2 + \alpha^1 \alpha^4 + \alpha^1 \alpha^8 + \alpha^2 \alpha^4 + \alpha^2 \alpha^8 + \alpha^4 \alpha^8)x^2 + \\ (\alpha^1 \alpha^2 \alpha^4 \alpha^8 + \alpha^1 \alpha^4 \alpha^8 + \alpha^2 \alpha^4 \alpha^8)x + \alpha^1 \alpha^2 \alpha^4 \alpha^8 =$$

$$\begin{aligned}
&x^4 + (0010+0100+0011+0101)x^3 + (\alpha^3+\alpha^5+\alpha^9+\alpha^{10}+\alpha^{12})x^2 + \\
&(\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})x + \alpha^{15} = \\
&x^4 + 0x^3 + (1000+0110+1010+1100+0111+1111)x^2 + \\
&(1011+1110+1101+1001)x + 1 = \\
&x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.
\end{aligned}$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .  
 $\beta = \alpha^2 = x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{21} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{22} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{23} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{24} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned}
m_2(x) &= (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) = \\
&(x - (\alpha^2)^{20})(x - (\alpha^2)^{21})(x - (\alpha^2)^{22})(x - (\alpha^2)^{23}) = \\
&(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).
\end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{21} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{22} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{23} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{24} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) =$

$$\begin{aligned}
&(x - (\alpha^3)^{20})(x - (\alpha^3)^{21})(x - (\alpha^3)^{22})(x - (\alpha^3)^{23}) = \\
&(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = \\
&(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).
\end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned}
m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\
&x^4 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^3 + (\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12})x^2 + \\
&(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12})x + \alpha^3\alpha^6\alpha^9\alpha^{12} = \\
&x^4 + (1000+1100+1010+1111)x^3 + (\alpha^9+\alpha^{12}+\alpha^{15}+\alpha^{15}+\alpha^{18}+\alpha^{21})x^2 + \\
&(\alpha^{18}+\alpha^{21}+\alpha^{24}+\alpha^{27})x + \alpha^{30} = \\
&x^4 + 1x^3 + (\alpha^9+\alpha^{12}+\alpha^{15}+\alpha^{15}+\alpha^3+\alpha^6)x^2 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x + \alpha^{15} = \\
&x^4 + 1x^3 + (1010+1111+0001+0001+1000+1100)x^2 + \\
&(1000+1100+1010+1111)x + 1 = \\
&x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^4)^{2^1} = \alpha^8 = x^3 + x^2 \neq \beta$ ,  $\beta^{2^2} = (\alpha^4)^{2^2} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{2^3} = (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_4(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^4)^{2^0})(x - (\alpha^4)^{2^1})(x - (\alpha^4)^{2^2})(x - (\alpha^4)^{2^3}) = \\ &= (x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2 + x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ ,  $\beta^t = \beta^{\text{mod}(t, 15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2 + x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{2^1} = (\alpha^5)^{2^1} = \alpha^{10} = x^2 + x + 1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^5)^{2^2} = \alpha^{20} = \alpha^5 = x^2 + x = \beta$ , то  $r=2$ ,  $r-1 = 1$ , и потому

$$\begin{aligned} m_5(x) &= (x - \beta^{2^0})(x - \beta^{2^1}) = (x - (\alpha^5)^{2^0})(x - (\alpha^5)^{2^1}) = \\ &= (x - \alpha^5)(x - \alpha^{10}). \end{aligned}$$

Положим множество  $M = \{\alpha^5, \alpha^{10}\}$ .

Тогда получаем следующее.

$$\begin{aligned} m_5(x) &= C(M, 0)x^2 + C(M, 1)x + C(M, 2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5 \alpha^{10})x^2 = \\ &= x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1. \end{aligned}$$

Для  $\beta = \alpha^5 = x^2 + x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3 + x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ ,  $\beta^t = \beta^{\text{mod}(t, 15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3 + x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{2^1} = (\alpha^6)^{2^1} = \alpha^{12} = x^3 + x^2 + x + 1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^6)^{2^2} = \alpha^{24} = \alpha^9 = x^3 + x + 1 \neq \beta$ ,  $\beta^{2^3} = (\alpha^6)^{2^3} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3 + x^2$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_6(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^6)^{2^0})(x - (\alpha^6)^{2^1})(x - (\alpha^6)^{2^2})(x - (\alpha^6)^{2^3}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3 + x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического и систематического ( $n=15$ ,  $k=5$ )-кода БЧХ есть полином

$$g(x) = \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) =$$

$$m_1(x) \cdot m_3(x) \cdot m_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \\ g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = a$ .

Для систематического (15,5)-кода БЧХ кодовый полином

$$u(x) = x^{n-k} a(x) + (x^{n-k} a(x)) \pmod{g(x)} = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)},$$

5. Кодовое слово

$$u(x) = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)} = \\ x^{10}(x^4 + x^3 + x) + (x^{10} \cdot (x^4 + x^3 + x)) \pmod{g(x)} = \\ (x^{14} + x^{13} + x^{11}) + (x^{14} + x^{13} + x^{11}) \pmod{g(x)} = \\ (x^{14} + x^{13} + x^{11}) + (x^9 + x^8 + x^5 + x + 1) = \\ x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x + 1 = 110101100100011.$$

Принятое кодовое слово

$$v(x) = 100101100100011 = x^{14} + x^{11} + x^9 + x^8 + x^5 + x^1 + 1.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ .

$$S_1 = v(\alpha^1) = \alpha^{14} + \alpha^{11} + \alpha^9 + \alpha^8 + \alpha^5 + \alpha^1 + 1 =$$

$$1001 + 1110 + 1010 + 0101 + 0110 + 0010 + 0001 = 1101 = \alpha^{13}.$$

$$S_2 = v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{11} + (\alpha^2)^9 + (\alpha^2)^8 + (\alpha^2)^5 + (\alpha^2)^1 + 1 =$$

$$\alpha^{28} + \alpha^{22} + \alpha^{18} + \alpha^{16} + \alpha^{10} + \alpha^2 + 1 =$$

$$\alpha^{13} + \alpha^7 + \alpha^3 + \alpha^1 + \alpha^{10} + \alpha^2 + 1 =$$

$$1101 + 1011 + 1000 + 0010 + 0111 + 0100 + 0001 = 1110 = \alpha^{11}.$$

$$S_3 = v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{11} + (\alpha^3)^9 + (\alpha^3)^8 + (\alpha^3)^5 + (\alpha^3)^1 + 1 =$$

$$\alpha^{42} + \alpha^{33} + \alpha^{27} + \alpha^{24} + \alpha^{15} + \alpha^3 + 1 =$$

$$\alpha^{12} + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^0 + \alpha^3 + 1 =$$

$$1111 + 1000 + 1111 + 1010 + 0001 + 1000 + 0001 = 1010 = \alpha^9.$$

$$S_4 = v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{11} + (\alpha^4)^9 + (\alpha^4)^8 + (\alpha^4)^5 + (\alpha^4)^1 + 1 =$$

$$\alpha^{56} + \alpha^{44} + \alpha^{36} + \alpha^{32} + \alpha^{20} + \alpha^4 + 1 =$$

$$\alpha^{11} + \alpha^{14} + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^4 + 1 =$$

$$1110 + 1001 + 1100 + 0100 + 0110 + 0011 + 0001 = 1011 = \alpha^7.$$

$$S_5 = v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{11} + (\alpha^5)^9 + (\alpha^5)^8 + (\alpha^5)^5 + (\alpha^5)^1 + 1 =$$

$$\alpha^{70} + \alpha^{55} + \alpha^{45} + \alpha^{40} + \alpha^{25} + \alpha^5 + 1 =$$

$$\alpha^{10} + \alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^{10} + \alpha^5 + 1 =$$

$$0111 + 0111 + 0001 + 0111 + 0111 + 0110 + 0001 = 0110 = \alpha^5.$$

$$S_6 = v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{11} + (\alpha^6)^9 + (\alpha^6)^8 + (\alpha^6)^5 + (\alpha^6)^1 + 1 =$$

$$\alpha^{84} + \alpha^{66} + \alpha^{54} + \alpha^{48} + \alpha^{30} + \alpha^6 + 1 =$$

$$\alpha^9 + \alpha^6 + \alpha^9 + \alpha^3 + \alpha^0 + \alpha^6 + 1 =$$

$$1010 + 1100 + 1010 + 1000 + 0001 + 1100 + 0001 = 1011 = \alpha^7.$$

$$S_1 = \alpha^{13} = 1101, S_2 = \alpha^{11} = 1110, S_3 = \alpha^9 = 1010,$$

$$S_4 = \alpha^7 = 1011, S_5 = \alpha^5 = 0110, S_6 = \alpha^7 = 1011.$$

6. Положить (число ошибок)  $v = 3$ .

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^{13} & \alpha^{11} & \alpha^9 \\ \alpha^{11} & \alpha^9 & \alpha^7 \\ \alpha^9 & \alpha^7 & \alpha^5 \end{bmatrix}, \det(M) = \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} = 0$$

$$7. \text{ Положить } v = 2. M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{13} & \alpha^{11} \\ \alpha^{11} & \alpha^9 \end{bmatrix}, \det(M) = \alpha^{22} + \alpha^{22} = 0.$$

8. Положить  $v = 1$ .  $M = [S_1] = [\alpha^{13}]$ ,  $\det(M) = \alpha^{13} \neq 0$ . Произошла одна ошибка.

Решить уравнение  $S_1\lambda_1 + 1 = 0$ . Тогда  $\alpha^{13}\lambda_1 = 1$ ,  $\lambda_1 = \alpha^{-13} = \alpha^2$ .

Полином локатора ошибок  $\lambda(x) = \lambda_1 x + 1 = \alpha^2 x + 1$ . Для  $\lambda(x)$  корень  $x = \alpha^{-2} = \alpha^{15-2} = \alpha^{13}$ . Ошибка произошла в тринадцатой позиции. Полином ошибок  $e(x) = x^{13}$ , и посланный кодовый полином

$$u(x) = v(x) + e(x) = (x^{14} + x^{11} + x^9 + x^8 + x^5 + x^3 + x^1 + 1) + (x^{13}) = x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x^3 + x^1 + 1 = 110101100100011 = u.$$

Первые пять позиций в  $u$  есть информационное слово  $a = 11010$ .

**Пример 2г.** Систематический ( $n=15$ ,  $k=5$ )-код БЧХ, исправляющий не более  $t=3$  ошибок. Случай отсутствия ошибок.

1. Выбрать  $GF(q^m)$ ,  $q=2$ ,  $m=4$ , примитивный полином  $p(x) = x^4 + x + 1$ , генератор  $\alpha = x$  для  $GF^*(q^m)$ ,  $2t = 6$ .

2. Взять последовательность элементов

$$A = \{\alpha^1 = x, \alpha^2 = x^2, \alpha^3 = x^3, \alpha^4 = x+1, \alpha^5 = x^2+x, \alpha^6 = x^3+x^2\}.$$

3. Для каждого  $\beta$  из  $A$  найти минимальный полином

$$m(x) = (x - \beta^{q^0})(x - \beta^{q^1})(x - \beta^{q^2}) \dots (x - \beta^{q^{r-1}}),$$

где  $r$  есть наименьшее положительное целое чистое такое, что  $\beta^{q^r} = \beta$ .

$\beta = \alpha^1 = x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = \alpha^{2^1} = \alpha^2 = x^2$ ,  $\beta^{2^2} = \alpha^{2^2} = \alpha^4 = x^4 = x+1$ ,  $\beta^{2^3} = \alpha^{2^3} = \alpha^8 = x^8 = x^2+1$ ,  $\beta^{2^4} = \beta^{16} = \beta^{\text{mod}(16,15)} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$m_1(x) = (x - \alpha^{2^0})(x - \alpha^{2^1})(x - \alpha^{2^2})(x - \alpha^{2^3}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Пусть  $C(M,k)$  есть сумма произведений элементов всех сочетаний из  $M$  по  $k$  элементов в каждом сочетании. Тогда (ввиду  $-1=1(\text{mod } 2)$ ) получаем следующее.

$$\begin{aligned} m(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\ &= x^4 + (\alpha^1 + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^1\alpha^2 + \alpha^1\alpha^4 + \alpha^1\alpha^8 + \alpha^2\alpha^4 + \alpha^2\alpha^8 + \alpha^4\alpha^8)x^2 + \\ &\quad (\alpha^1\alpha^2\alpha^4\alpha^8 + \alpha^1\alpha^4\alpha^8 + \alpha^2\alpha^4\alpha^8)x + \alpha^1\alpha^2\alpha^4\alpha^8 = \end{aligned}$$

$$\begin{aligned}
&x^4 + (0010+0100+0011+0101)x^3 + (\alpha^3+\alpha^5+\alpha^9+\alpha^{10}+\alpha^{12})x^2 + \\
&(\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})x + \alpha^{15} = \\
&x^4 + 0x^3 + (1000+0110+1010+1100+0111+1111)x^2 + \\
&(1011+1110+1101+1001)x + 1 = \\
&x^4 + 0x^3 + 0x^2 + (0001)x + 1 = x^4 + x + 1.
\end{aligned}$$

Для  $\beta = \alpha^1 = x$  минимальный полином  $m_1(x) = x^4 + x + 1$ .  
 $\beta = \alpha^2 = x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^2) = \text{ord}(x^2) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{21} = (\alpha^2)^2 = \alpha^4 = x+1 \neq \beta$ ,  $\beta^{22} = \beta^4 = (\alpha^2)^4 = \alpha^8 = x^2+x \neq \beta$ ,  $\beta^{23} = \beta^8 = (\alpha^2)^8 = \alpha^{16} = \alpha^{\text{mod}(16,15)} = \alpha = x \neq \beta$ ,  $\beta^{24} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned}
m_2(x) &= (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) = \\
&(x - (\alpha^2)^{20})(x - (\alpha^2)^{21})(x - (\alpha^2)^{22})(x - (\alpha^2)^{23}) = \\
&(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).
\end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ .

Для  $\beta = \alpha^2 = x^2$  минимальный полином  $m_2(x) = x^4 + x + 1$ .

$\beta = \alpha^3 = x^3$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^3) = \text{ord}(x^3) = 5$ ,  $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ .

Так как  $\beta^{21} = (\alpha^3)^2 = \alpha^6 = x^3+x^2 \neq \beta$ ,  $\beta^{22} = \beta^4 = (\alpha^3)^4 = \alpha^{12} = x^3+x^2+x+1 \neq \beta$ ,  $\beta^{23} = \beta^8 = (\alpha^3)^8 = \alpha^{24} = \alpha^{\text{mod}(16,15)} = \alpha^9 = x^3+x^2 \neq \beta$ ,  $\beta^{24} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому  $m_3(x) = (x - \beta^{20})(x - \beta^{21})(x - \beta^{22})(x - \beta^{23}) =$

$$\begin{aligned}
&(x - (\alpha^3)^{20})(x - (\alpha^3)^{21})(x - (\alpha^3)^{22})(x - (\alpha^3)^{23}) = \\
&(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) = \\
&(x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).
\end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Тогда получаем следующее.

$$\begin{aligned}
m_3(x) &= C(M,0)x^4 + C(M,1)x^3 + C(M,2)x^2 + C(M,3)x + C(M,4) = \\
&x^4 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^3 + (\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12})x^2 + \\
&(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12})x + \alpha^3\alpha^6\alpha^9\alpha^{12} = \\
&x^4 + (1000+1100+1010+1111)x^3 + (\alpha^9+\alpha^{12}+\alpha^{15}+\alpha^{15}+\alpha^{18}+\alpha^{21})x^2 + \\
&(\alpha^{18}+\alpha^{21}+\alpha^{24}+\alpha^{27})x + \alpha^{30} = \\
&x^4 + 1x^3 + (\alpha^9+\alpha^{12}+\alpha^{15}+\alpha^{15}+\alpha^3+\alpha^6)x^2 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x + \alpha^{15} = \\
&x^4 + 1x^3 + (1010+1111+0001+0001+1000+1100)x^2 + \\
&(1000+1100+1010+1111)x + 1 = \\
&x^4 + 1x^3 + 1x^2 + 1x + 1 = x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Для  $\beta = \alpha^3$  минимальный полином  $m_3(x) = x^4 + x^3 + x^2 + x + 1$ .

$\beta = \alpha^4 = x+1$ . Степени  $\alpha^t = \alpha^{\text{mod}(t,15)}$ ,  $\beta^t = \beta^{\text{mod}(t,15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^4) = \text{ord}(x+1) = 15$ ,  $\beta^{15} = 1$ .

Так как  $\beta^{2^1} = (\alpha^4)^{2^1} = \alpha^8 = x^3 + x^2 \neq \beta$ ,  $\beta^{2^2} = (\alpha^4)^{2^2} = \alpha^{16} = \alpha^1 = x \neq \beta$ ,  $\beta^{2^3} = (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2 = x^2 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = \beta$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_4(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^4)^{2^0})(x - (\alpha^4)^{2^1})(x - (\alpha^4)^{2^2})(x - (\alpha^4)^{2^3}) = \\ &= (x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = (x - \alpha^4)(x - \alpha^8)(x - \alpha^1)(x - \alpha^2) \\ &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8). \end{aligned}$$

Положим множество  $M = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^1$ , и для  $\beta = \alpha^4 = x+1$  получаем минимальный полином  $m_4(x) = x^4 + x + 1$ .

Для  $\beta = \alpha^4 = x+1$  минимальный полином  $m_4(x) = x^4 + x + 1$ .

$\beta = \alpha^5 = x^2 + x$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ ,  $\beta^t = \beta^{\text{mod}(t, 15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^5) = \text{ord}(x^2 + x) = 3$ ,  $\beta^3 = 1$ .

Так как  $\beta^{2^1} = (\alpha^5)^{2^1} = \alpha^{10} = x^2 + x + 1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^5)^{2^2} = \alpha^{20} = \alpha^5 = x^2 + x = \beta$ , то  $r=2$ ,  $r-1 = 1$ , и потому

$$\begin{aligned} m_5(x) &= (x - \beta^{2^0})(x - \beta^{2^1}) = (x - (\alpha^5)^{2^0})(x - (\alpha^5)^{2^1}) = \\ &= (x - \alpha^5)(x - \alpha^{10}). \end{aligned}$$

Положим множество  $M = \{\alpha^5, \alpha^{10}\}$ .

Тогда получаем следующее.

$$\begin{aligned} m_5(x) &= C(M, 0)x^2 + C(M, 1)x + C(M, 2) = 1x^2 + (\alpha^5 + \alpha^{10})x^3 + (\alpha^5 \alpha^{10})x^2 = \\ &= x^2 + (0110 + 0111)x + \alpha^{15} = x^2 + 1x + 1. \end{aligned}$$

Для  $\beta = \alpha^5 = x^2 + x$  минимальный полином  $m_5(x) = x^2 + x + 1$ .

$\beta = \alpha^6 = x^3 + x^2$ . Степени  $\alpha^t = \alpha^{\text{mod}(t, 15)}$ ,  $\beta^t = \beta^{\text{mod}(t, 15)}$ .

Порядок  $\text{ord}(\beta) = \text{ord}(\alpha^6) = \text{ord}(x^3 + x^2) = 5$ ,  $\beta^5 = 1$ .

Так как  $\beta^{2^1} = (\alpha^6)^{2^1} = \alpha^{12} = x^3 + x^2 + x + 1 \neq \beta$ ,  $\beta^{2^2} = (\alpha^6)^{2^2} = \alpha^{24} = \alpha^9 = x^3 + x + 1 \neq \beta$ ,  $\beta^{2^3} = (\alpha^6)^{2^3} = \alpha^{48} = \alpha^3 = x^3 \neq \beta$ ,  $\beta^{2^4} = \beta^{16} = (\alpha^6)^{16} = \alpha^6 = \beta = x^3 + x^2$ , то  $r = 4$ ,  $r-1 = 3$ , и потому

$$\begin{aligned} m_6(x) &= (x - \beta^{2^0})(x - \beta^{2^1})(x - \beta^{2^2})(x - \beta^{2^3}) = \\ &= (x - (\alpha^6)^{2^0})(x - (\alpha^6)^{2^1})(x - (\alpha^6)^{2^2})(x - (\alpha^6)^{2^3}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48}) = \\ &= (x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)(x - \alpha^3) = \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}). \end{aligned}$$

Положим множество  $M = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ . Дальнейшие вычисления совпадают с вычислениями случая  $\beta = \alpha^3$ .

Для  $\beta = \alpha^6 = x^3 + x^2$  минимальный полином  $m_6(x) = x^4 + x^3 + x^2 + x + 1$ .

4. Генератор несистематического и систематического ( $n=15$ ,  $k=5$ )-кода БЧХ есть полином

$$g(x) = \text{НОК}(m_1(x), m_2(x), m_3(x), m_4(x), m_5(x), m_6(x)) =$$

$$m_1(x) \cdot m_3(x) \cdot m_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \\ g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Пусть информационное слово  $a(x) = x^4 + x^3 + x = 11010 = a$ .

Для систематического (15,5)-кода БЧХ кодовый полином

$$u(x) = x^{n-k} a(x) + (x^{n-k} a(x)) \pmod{g(x)} = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)},$$

5. Кодовое слово

$$u(x) = x^{10} \cdot a(x) + (x^{10} \cdot a(x)) \pmod{g(x)} = \\ x^{10}(x^4 + x^3 + x) + (x^{10} \cdot (x^4 + x^3 + x)) \pmod{g(x)} = \\ (x^{14} + x^{13} + x^{11}) + (x^{14} + x^{13} + x^{11}) \pmod{g(x)} = \\ (x^{14} + x^{13} + x^{11}) + (x^9 + x^8 + x^5 + x + 1) = \\ x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x + 1 = 110101100100011.$$

Принятое кодовое слово

$$v(x) = 110101100100011 = x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x^1 + 1.$$

Вычислить синдромы  $S_j, j = 1, 2, \dots, 2t=6$ .

$$S_1 = v(\alpha^1) = \alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^9 + \alpha^8 + \alpha^5 + \alpha^1 + 1 = \\ 1001 + 1101 + 1110 + 1010 + 0101 + 0110 + 0010 + 0001 = 0.$$

$$S_2 = v(\alpha^2) = (\alpha^2)^{14} + (\alpha^2)^{13} + (\alpha^2)^{11} + (\alpha^2)^9 + (\alpha^2)^8 + (\alpha^2)^5 + (\alpha^2)^1 + 1 = \\ \alpha^{28} + \alpha^{26} + \alpha^{22} + \alpha^{18} + \alpha^{16} + \alpha^{10} + \alpha^2 + 1 = \\ \alpha^{13} + \alpha^{11} + \alpha^7 + \alpha^3 + \alpha^1 + \alpha^{10} + \alpha^2 + 1 =$$

$$1101 + 1110 + 1011 + 1000 + 0010 + 0111 + 0100 + 0001 = 0.$$

$$S_3 = v(\alpha^3) = (\alpha^3)^{14} + (\alpha^3)^{13} + (\alpha^3)^{11} + (\alpha^3)^9 + (\alpha^3)^8 + (\alpha^3)^5 + (\alpha^3)^1 + 1 = \\ \alpha^{42} + \alpha^{39} + \alpha^{33} + \alpha^{27} + \alpha^{24} + \alpha^{15} + \alpha^3 + 1 = \\ \alpha^{12} + \alpha^9 + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^0 + \alpha^3 + 1 =$$

$$1111 + 1010 + 1000 + 1111 + 1010 + 0001 + 1000 + 0001 = 0.$$

$$S_4 = v(\alpha^4) = (\alpha^4)^{14} + (\alpha^4)^{13} + (\alpha^4)^{11} + (\alpha^4)^9 + (\alpha^4)^8 + (\alpha^4)^5 + (\alpha^4)^1 + 1 = \\ \alpha^{56} + \alpha^{52} + \alpha^{44} + \alpha^{36} + \alpha^{32} + \alpha^{20} + \alpha^4 + 1 = \\ \alpha^{11} + \alpha^7 + \alpha^{14} + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^4 + 1 =$$

$$1110 + 1011 + 1001 + 1100 + 0100 + 0110 + 0011 + 0001 = 0.$$

$$S_5 = v(\alpha^5) = (\alpha^5)^{14} + (\alpha^5)^{13} + (\alpha^5)^{11} + (\alpha^5)^9 + (\alpha^5)^8 + (\alpha^5)^5 + (\alpha^5)^1 + 1 = \\ \alpha^{70} + \alpha^{65} + \alpha^{55} + \alpha^{45} + \alpha^{40} + \alpha^{25} + \alpha^5 + 1 = \\ \alpha^{10} + \alpha^5 + \alpha^{10} + \alpha^0 + \alpha^{10} + \alpha^{10} + \alpha^5 + 1 =$$

$$0111 + 0110 + 0111 + 0001 + 0111 + 0111 + 0110 + 0001 = 0.$$

$$S_6 = v(\alpha^6) = (\alpha^6)^{14} + (\alpha^6)^{13} + (\alpha^6)^{11} + (\alpha^6)^9 + (\alpha^6)^8 + (\alpha^6)^5 + (\alpha^6)^1 + 1 = \\ \alpha^{84} + \alpha^{78} + \alpha^{66} + \alpha^{54} + \alpha^{48} + \alpha^{30} + \alpha^6 + 1 = \\ \alpha^9 + \alpha^3 + \alpha^6 + \alpha^9 + \alpha^3 + \alpha^0 + \alpha^6 + 1 =$$

$$1010 + 1000 + 1100 + 1010 + 1000 + 0001 + 1100 + 0001 = 0011 = \alpha^4.$$

$$S_1 = 0, S_2 = 0, S_3 = 0, S_4 = 0, S_5 = 0, S_6 = \alpha^4 = 0011.$$

6. Положить (число ошибок)  $v = 3$ .

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^{13} & \alpha^{11} & \alpha^9 \\ \alpha^{11} & \alpha^9 & \alpha^7 \\ \alpha^9 & \alpha^7 & \alpha^5 \end{bmatrix}, \det(M) = \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} + \alpha^{27} = 0.$$

Все последующие матрицы порядков 1, 2, 3 нулевые. Кодовое слово  $\mathbf{u} = 110101100100011$  передано без искажений. Первые пять позиций в  $\mathbf{u}$  есть информационное слово  $\mathbf{a} = 11010$ .

## СЖАТИЕ ИНФОРМАЦИИ (АРХИВАЦИЯ)

**Задача 41.** Написать свое полное имя (фамилия, имя, отчество, ФИО) и взять для исследования текст  $T$  из десяти первых букв ФИО. Если ФИО имеет меньше десяти букв, то дополнить ФИО любыми другими именами до получения слова с длиной больше десяти. Взять для исследования текст  $T$  из десяти первых букв нового ФИО. С точностью до сотых (две цифры после десятичной точки) найти в тексте  $T$  частоту появления букв. Сумма частот должна равняться единице.

### 1. Сжатие по Фано

1. Найти разделимую префиксную схему алфавитного кодирования Фано. Найти сжатый код Фано (архив) текста  $T$ . Декодировать код и проверить, совпадает ли результат декодирования с исходным текстом  $T$ .

#### Алгоритм Фано

**ВХОД.** Пусть буквам  $a_1, \dots, a_n$  соответствует последовательность  $P = (p_1, \dots, p_n)$  вероятностей их появления, упорядоченных по невозрастанию:

$$1 \geq p_1 \geq \dots \geq p_n > 0, \quad p_1 + \dots + p_n = 1.$$

**ВЫХОД.** Массив элементарных кодов, вычисляемых рекурсивным алгоритмом Фано (Fano).

1. Разбить последовательность  $P$  вероятностей на две последовательности  $P_0 = (p_1, \dots, p_k)$ ,  $P_1 = (p_k, p_{k+1}, \dots, p_n)$  с примерно равными суммами вероятностей. Каждой из последовательностей  $P_0$ ,  $P_1$  назначить коды  $c_0=0$ ,  $c_1=1$  соответственно. Перейти к пункту 2.

2. Пока существует последовательность  $Q$  длины больше 1, разбить  $Q$  на две последовательности  $Q_0$ ,  $Q_1$  как в пункте 1, и приписать справа к ранее полученному коду  $c$  для  $Q$  числа 0 и 1 для  $Q_0$ ,  $Q_1$  соответственно. Иначе перейти к пункту 3.

3. Вернуть последовательность элементарных кодов  $b_1, \dots, b_n$  для букв  $a_1, \dots, a_n$  соответственно, накопленных в пунктах 1 и 2 алгоритма.

**Замечание.** Работу алгоритма Фано можно изобразить в виде дерева, которое строится и обрабатывается от корня к листьям.

**Пример 1.** Пусть для последовательности букв  $(a_1, \dots, a_n)$  соответствует последовательность вероятностей  $P = (0.20, 0.20, 0.19, 0.12, 0.11, 0.09, 0.09)$  их появления. Использовать алгоритм Фано и найти разделимую префиксную схему алфавитного кодирования. Результаты вычислений сведены в табл.17.1.

Разделимая префиксная схема алфавитного кодирования, близкого к оптимальному

$$f = (a_1 \rightarrow 00, a_2 \rightarrow 010, a_3 \rightarrow 011, a_4 \rightarrow 100, a_5 \rightarrow 101, a_6 \rightarrow 110, a_7 \rightarrow 111).$$

$$\text{Цена Фано} = 0.20 \cdot 2 + 0.20 \cdot 3 + 0.19 \cdot 3 + 0.12 \cdot 3 + 0.11 \cdot 3 + 0.09 \cdot 3 + \\ 0.09 \cdot 3 = 2.8.$$

Таблица 17.1

$a_i$	$p_i$	$\Sigma$	$c$	$\Sigma$	$c$	$\Sigma$	$c$
$a_1$	0.20		0	0.20	<b>00</b>		
$a_2$	0.20	0.59	0	0.39	01	0.20	<b>010</b>
$a_3$	0.19		0		01	0.19	<b>011</b>
$a_4$	0.12		1	0.23	10	0.12	<b>100</b>
$a_5$	0.11	0.41	1		10	0.11	<b>101</b>
$a_6$	0.09		1	0.18	11	0.09	<b>110</b>
$a_7$	0.09		1		11	0.09	<b>111</b>

**Пример 2.** Пусть для последовательности букв  $(a_1, \dots, a_n)$  соответствует последовательность вероятностей  $P = (0.25, 0.15, 0.12, 0.11, 0.08, 0.06, 0.06, 0.06, 0.06, 0.05)$  их появления. Использовать алгоритм Фано и найти разделимую префиксную схему алфавитного кодирования. Результаты вычислений сведены в табл.17.2.

Таблица 17.2

$a_i$	$p_i$	$\Sigma$	$C$	$\Sigma$	$c$	$\Sigma$	$c$	$\Sigma$	$c$
$a_1$	0.25		0	0.25	<b>00</b>				<b>00</b>
$a_2$	0.15	0.52	0	0.27	01	0.15	<b>010</b>		<b>010</b>
$a_3$	0.12		0		01	0.12	<b>011</b>		<b>011</b>
$a_4$	0.11		1		10	0.11	<b>100</b>		<b>100</b>
$a_5$	0.08		1	0.25	10	0.14	101	0.08	<b>1010</b>
$a_6$	0.06		1		10		101	0.06	<b>1011</b>
$a_7$	0.06	0.48	1		11	0.12	110	0.06	<b>1100</b>
$a_8$	0.06		1	0.23	11		110	0.06	<b>1101</b>
$a_9$	0.06		1		11	0.11	111	0.06	<b>1110</b>
$a_{10}$	0.05		1		11		111	0.05	<b>1111</b>

Разделимая префиксная схема алфавитного кодирования, близкого к оптимальному

$$f = (a_1 \rightarrow 00, a_2 \rightarrow 010, a_3 \rightarrow 011, a_4 \rightarrow 100, a_5 \rightarrow 1010, a_6 \rightarrow 1011, \\ a_7 \rightarrow 1100, a_8 \rightarrow 1101, a_9 \rightarrow 1110, a_{10} \rightarrow , a_{11} \rightarrow 1111).$$

$$\text{Цена} = 0.25 \cdot 2 + 0.15 \cdot 3 + 0.12 \cdot 3 + 0.11 \cdot 3 + 0.08 \cdot 4 + 0.06 \cdot 4 + \\ 0.06 \cdot 4 + 0.06 \cdot 4 + 0.06 \cdot 4 + 0.05 \cdot 4 = 3.12.$$

## 2. Сжатие по Хаффману.

Найти разделимую префиксную схему алфавитного кодирования Хаффмана. Найти сжатый код Хаффмана (архив) текста  $T$ . Декодировать код и проверить, совпадает ли результат декодирования с исходным текстом  $T$ .

### Алгоритм Хаффмана.

**ВХОД.** Буквы (символы)  $a_1, \dots, a_n$ ,  $n \geq 2$ , и последовательность  $P = (p_1, \dots, p_n)$  вероятностей их появления, упорядоченных по не возрастанию:

$1 \geq p_1 \geq \dots \geq p_n > 0$ ,  $p_1 + \dots + p_n = 1$ .

**ВЫХОД.** Оптимальная разделимая префиксная схема алфавитного кодирования  $f = \{a_1 \rightarrow b_1, \dots, a_n \rightarrow b_n\}$ .

**Шаг 0.** Инициализация.

$a_1, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_{n-2}, b, c$  (для удобства  $b = a_{n-1}, c = a_n$ ),

$p_1, \dots, p_{j-1}, p_j, p_{j+1}, \dots, p_{n-2}, q, r$ , (для удобства  $q = p_{n-1}, r = p_n$ ).

Построить схему алфавитного кодирования.

$f = \{a_1 \rightarrow , \dots, a_{j-1} \rightarrow , a_j \rightarrow , a_{j+1} \rightarrow , \dots, a_{n-2} \rightarrow , b \rightarrow , c \rightarrow \}$ .

**Шаг 1.**  $qr = q + r$ . В ряду  $a_1, a_2, \dots, a_{n-2}$ , найти такое  $j$ , что  $p_j \geq qr > p_{j+1}$ . Возможно также, что  $qr > p_1$ .

Если  $p_j \geq qr > p_{j+1}$ , то построить ряды

$a_1, a_2, \dots, a_{j-1}, bc, a_{j+1}, \dots, a_{n-2}$ ,

$p_1, p_2, \dots, p_{j-1}, qr, p_{j+1}, \dots, p_{n-2}$ .

Если  $qr > p_1$ , то построить ряды

$bc, a_1, a_2, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_{n-2}$ ,

$qr, p_1, p_2, \dots, p_{j-1}, p_j, p_{j+1}, \dots, p_{n-2}$ .

Построить схему алфавитного кодирования.

$f = \{a_1 \rightarrow , \dots, a_{j-1} \rightarrow , a_j \rightarrow , a_{j+1} \rightarrow , \dots, a_{n-2} \rightarrow , a_{n-1} \rightarrow 0, a_n \rightarrow 1\}$ .

**Шаг k.** Пусть на шаге  $k$  получены следующие словарный и числовой ряды.

$w_1, \dots, w_{j-1}, w_j, w_{j+1}, \dots, w_{k-2}, w_{k-1} = a_{i_1} \dots a_{i_s}, w_k = a_{j_1} \dots a_{j_s},$

$q_1, \dots, q_{j-1}, q_j, q_{j+1}, \dots, q_{k-2}, q_{k-1}, \dots, q_k$ ,

и схема алфавитного кодирования

$f = \{a_1 \rightarrow w_1, \dots, a_{i_1} \rightarrow w_{i_1}, \dots, a_{i_s} \rightarrow w_{i_s}, \dots, a_{j_1} \rightarrow w_{j_1}, \dots, a_{j_t} \rightarrow w_{j_t}, \dots, a_k \rightarrow w_k\}$ .

**Шаг k+1.**  $q = q_{k-1} + q_k$ . В ряду  $w_1, w_2, \dots, w_{k-2}$ , найти такое  $j$ , что  $q_j \geq q > q_{j+1}$ .

Возможно также, что  $q > q_1$ .

Если  $q_j \geq q > p_{j+1}$ , то построить ряды

$w_1, w_2, \dots, w_{j-1}, a_{i_1} \dots a_{i_s} a_{j_1} \dots a_{j_s}, w_{j+1}, \dots, w_{k-2}$ ,

$q_1, q_2, \dots, q_{j-1}, \dots, q, \dots, q_{j+1}, \dots, q_{n-2}$ ,

Если  $qr > p_1$ , то построить ряды

$a_{i_1} \dots a_{i_s} a_{j_1} \dots a_{j_s}, w_1, w_2, \dots, w_{j-1}, w_j, w_{j+1}, \dots, w_{k-2}$ ,

$q, \dots, q_1, q_2, \dots, q_{j-1}, q_j, q_{j+1}, \dots, q_{k-2}$ .

Построить схему алфавитного кодирования.

$f = \{a_1 \rightarrow w_1, \dots, a_{i_1} \rightarrow 0 w_{i_1}, \dots, a_{i_s} \rightarrow 0 w_{i_s}, \dots, a_{j_1} \rightarrow 1 w_{j_1}, \dots, a_{j_t} \rightarrow 1 w_{j_t}, \dots, a_{k-1} \rightarrow w_{k-1}\}$ .

И так далее. С парой  $\frac{w}{c}$  закончить работу.

**Шаг n.** Вернуть последнюю полученную схему кодирования  $f$ .

**Замечание.** Работу алгоритма Хаффмана можно изобразить в виде дерева, которое строится и обрабатывается от листьев к корню.

**Пример 1.** Пусть для последовательности букв  $a, b, c, d, e, f, g$  соответствует последовательность вероятностей  $P = (0.20, 0.20, 0.19, 0.12, 0.11, 0.09, 0.09)$  их появления. Использовать алгоритм Хаффмана и найти разделимую префиксную схему алфавитного кодирования.

**Шаг 0.** Инициализация. Для удобства вычислений заменить вероятности появления букв их частотами и положить:  $a=20, b=20, c=19, d=12, e=11, f=9, g=9$ . Построить два следующих ряда.

$$\begin{array}{ccccccc} a & b & c & d & e & f & g, \\ 20, & 20, & 19, & 12, & 11, & 9, & 9. \end{array}$$

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow , e \rightarrow , f \rightarrow , g \rightarrow \}.$$

**Шаг 1.** Для двух последних элементов  $fg := f+g = 9+9 = 18$ . Поместить узел  $fg=18$  между узлами  $c=19$  и  $d=12$ . Удалить два последних элемента.

Построить два следующих ряда.

$$\begin{array}{cccccc} a & b & c & fg & d & e, \\ 20, & 20, & 19, & 18, & 12, & 11. \end{array}$$

Продолжить коды символами слева для  $f, g$ :  $\text{cod}(f):=0, \text{cod}(g):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow , e \rightarrow , f \rightarrow 0, g \rightarrow 1\}.$$

**Шаг 2.** Для двух последних элементов  $de := d+e = 12+11 = 23$ . Поместить узел  $de=23$  перед  $a=20$ . Удалить два последних элемента.

Построить два следующих ряда.

$$\begin{array}{ccccc} de & a & b & c & fg, \\ 23, & 20, & 20, & 19, & 18. \end{array}$$

Продолжить коды символами слева для  $d, e$ :  $\text{cod}(d):=0, \text{cod}(e):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow 0, e \rightarrow 1, f \rightarrow 0, g \rightarrow 1\}.$$

**Шаг 3.** Для двух последних элементов  $cfg := c+fg = 19+18 = 37$ . Поместить узел  $cfg=37$  перед  $de=23$ . Удалить два последних элемента.

Построить два следующих ряда.

$$\begin{array}{ccccc} cfg & de & a & b, \\ 37, & 23, & 20, & 20. \end{array}$$

Продолжить коды символами слева для  $c, fg$ :  $\text{cod}(c):=0, \text{cod}(fg):=1, \text{cod}(g):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow 0, d \rightarrow 0, e \rightarrow 1, f \rightarrow 10, g \rightarrow 11\}$$

**Шаг 4.** Для двух последних элементов  $ab := a+b = 20+20 = 40$ . Поместить узел  $ab=40$  перед  $cfg=37$ . Удалить два последних элемента.

Построить два следующих ряда.

$$\begin{array}{ccccc} ab & cfg & de, \\ 40, & 37, & 23. \end{array}$$

Продолжить коды символами слева для  $a, b$ :  $\text{cod}(a):=0, \text{cod}(b):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow 0, b \rightarrow 1, c \rightarrow 0, d \rightarrow 0, e \rightarrow 1, f \rightarrow 10, g \rightarrow 11\}.$$

**Шаг 5.** Для двух последних элементов  $cfgde := cfg+de = 37+23 = 60$ . Поместить узел  $cfgde=60$  перед  $ab=40$ . Удалить два последних элемента.

Построить два следующих ряда.

$$\begin{array}{ll} cfgde & ab, \\ 60 & 40. \end{array}$$

Продолжить коды символами слева для  $cfg de$ :  $\text{cod}(c):=0$ ,  $\text{cod}(f):=0$ ,  $\text{cod}(g):=0$ ,  $\text{cod}(d):=1$ ,  $\text{cod}(e):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow 0, b \rightarrow 1, c \rightarrow 00, d \rightarrow 10, e \rightarrow 11, f \rightarrow 010, g \rightarrow 011\}$$

**Шаг 6.** Для двух последних элементов  $cfgdeab := cfgde+ab = 60+40 = 100$ . Поместить  $cfgdeab=100$  перед  $cfgde=60$ . Удалить два последних элемента.

Построить два следующих ряда.

$$\begin{array}{l} cfgdeab, \\ 100. \end{array}$$

Продолжить коды символами слева для  $cfgde ab$ :  $\text{cod}(c):=0$ ,  $\text{cod}(f):=0$ ,  $\text{cod}(g):=0$ ,  $\text{cod}(d):=0$ ,  $\text{cod}(e):=0$ ,  $\text{cod}(a):=1$ ,  $\text{cod}(b):=1$ .

$$s = \{a \rightarrow 10, b \rightarrow 11, c \rightarrow 000, d \rightarrow 010, e \rightarrow 011, f \rightarrow 0010, g \rightarrow 0011\}.$$

**Шаг 7.** Вернуть разделимую префиксную схему алфавитного кодирования  
 $s = \{a \rightarrow 10, b \rightarrow 11, c \rightarrow 000, d \rightarrow 010, e \rightarrow 011, f \rightarrow 0010, g \rightarrow 0011\}$ .

**Замечание.** Цена схемы  $s$  есть число

$$\text{Cost}(s) = 0.20 \cdot 2 + 0.20 \cdot 2 + 0.19 \cdot 3 + 0.12 \cdot 3 + 0.11 \cdot 3 + 0.09 \cdot 4 + 0.09 \cdot 4 = 2.78.$$

По схеме Фано  $\text{Cost}(s) = 2.80$ .

**Пример 2.** Пусть для последовательности букв  $a, b, c, d, e, f, g, h, i, k$  соответствует последовательность вероятностей  $P = (0.25, 0.15, 0.12, 0.11, 0.08, 0.06, 0.06, 0.06, 0.06, 0.05)$  их появления. Использовать алгоритм Хаффмана и найти оптимальную разделимую префиксную схему алфавитного кодирования.

**Решение.**

**Шаг 0.** Инициализация. Для удобства вычислений заменим вероятности появления букв их частотами и положим:  $a=25$ ,  $b=15$ ,  $c=12$ ,  $d=11$ ,  $e=8$ ,  $f=6$ ,  $g=6$ ,  $h=6$ ,  $i=6$ ,  $k=5$ . Построить два следующих ряда.

$$\begin{array}{llllllllll} a & b & c & d & e & f & g & h & i & k, \\ 25 & 15 & 12 & 11 & 8 & 6 & 6 & 6 & 6 & 5. \end{array}$$

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow , e \rightarrow , f \rightarrow , g \rightarrow , h \rightarrow , i \rightarrow , k \rightarrow \}.$$

**Шаг 1.** Для двух последних элементов  $ik := i+k = 6+5 = 11$ . Поместить узел  $ik=11$  между узлами  $d=11$  и  $e=8$ . Удалить два последних элемента. Построить два следующих ряда.

$$\begin{array}{llllllllll} a & b & c & d & ik & e & f & g & h, \\ 25 & 15 & 12 & 11 & 11 & 8 & 6 & 6 & 6. \end{array}$$

Продолжить коды символами слева для  $i k$ :  $\text{cod}(i):=0$ ,  $\text{cod}(k):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow , e \rightarrow , f \rightarrow , g \rightarrow , h \rightarrow , i \rightarrow 0, k \rightarrow 1\}$$

**Шаг 2.** Для двух последних элементов  $gh := g+h = 6+6 = 12$ . Поместить узел  $gh=12$  между узлами  $c=12$  и  $d=11$ . Удалить два последних элемента. Построить два следующих ряда.

$$\begin{array}{ccccccccc} a & b & c & gh & d & ik & e & f, \\ 25 & 15 & 12 & 12 & 11 & 11 & 8 & 6. \end{array}$$

Продолжить коды символами слева для  $g h$ :  $\text{cod}(g):=0$ ,  $\text{cod}(h):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow , e \rightarrow , f \rightarrow , g \rightarrow 0, h \rightarrow 1, i \rightarrow 0, k \rightarrow 1\}$$

**Шаг 3.** Для двух последних элементов  $ef := e+f = 8+6 = 14$ . Поместить узел  $ef=14$  между узлами  $b=15$  и  $c=12$ . Удалить два последних элемента. Построить два следующих ряда.

$$\begin{array}{ccccccccc} a & b & ef & c & gh & d & ik, \\ 25 & 15 & 14 & 12 & 12 & 11 & 11. \end{array}$$

Продолжить коды символами слева для  $e f$ :  $\text{cod}(e):=0$ ,  $\text{cod}(f):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow , e \rightarrow 0, f \rightarrow 1, g \rightarrow 0, h \rightarrow 1, i \rightarrow 0, k \rightarrow 1\}$$

**Шаг 4.** Для двух последних элементов  $dik := di+k = 11+11 = 22$ . Поместить узел  $dik=12$  между узлами  $a=25$  и  $b=15$ . Удалить два последних элемента. Построить два следующих ряда.

$$\begin{array}{ccccccccc} a & dik & b & ef & c & gh, \\ 25 & 22 & 15 & 14 & 12 & 12. \end{array}$$

Продолжить коды символами слева для  $d ik$ :  $\text{cod}(d):=0$ ,  $\text{cod}(i):=1$ ,  $\text{cod}(k):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow , d \rightarrow 1, e \rightarrow 0, f \rightarrow 1, g \rightarrow 0, h \rightarrow 1, i \rightarrow 00, k \rightarrow 11\}$$

**Шаг 5.** Для двух последних элементов  $cgh := c+gh = 12+12 = 24$ . Поместить узел  $cgh=24$  между узлами  $a=25$  и  $dik=22$ . Удалить два последних элемента. Построить два следующих ряда.

$$\begin{array}{ccccccccc} a & cgh & dik & b & ef, \\ 25 & 24 & 22 & 15 & 14. \end{array}$$

Продолжить коды символами слева для  $c gh$ :  $\text{cod}(c):=0$ ,  $\text{cod}(g):=1$ ,  $\text{cod}(h):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow , c \rightarrow 0, d \rightarrow 1, e \rightarrow 0, f \rightarrow 1, g \rightarrow 10, h \rightarrow 11, i \rightarrow 00, k \rightarrow 11\}$$

**Шаг 6.** Для двух последних элементов  $bef := b+ef = 15+14 = 29$ . Поместить узел  $bef=29$  перед узлом  $a=25$ . Удалить два последних элемента. Построить два следующих ряда.

$$\begin{array}{ccccccccc} bef & a & cgh & dik, \\ 29 & 25 & 24 & 22. \end{array}$$

Продолжить коды символами слева для  $b ef$ :  $\text{cod}(b):=0$ ,  $\text{cod}(e):=1$ ,  $\text{cod}(f):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow 0, c \rightarrow 0, d \rightarrow 1, e \rightarrow 10, f \rightarrow 11, g \rightarrow 10, h \rightarrow 11, \\ i \rightarrow 00, k \rightarrow 11\}$$

**Шаг 7.** Для двух последних элементов  $cghdik := cgh+dik = 24+22 = 46$ . Поместить узел  $cghdik = 46$  перед узлом  $bef=29$ . Построить два следующих ряда.

$$\begin{array}{ccc} cghdik & bef & a, \\ 46 & 29 & 25. \end{array}$$

Продолжить коды символами слева для  $cgh$   $dik$ :  $\text{cod}(c):=0$ ,  $\text{cod}(g):=0$ ,  $\text{cod}(h):=0$ ,  $\text{cod}(d):=1$ ,  $\text{cod}(i):=1$ ,  $\text{cod}(k):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow , b \rightarrow 0, c \rightarrow 00, d \rightarrow 11, e \rightarrow 10, f \rightarrow 11, g \rightarrow 010, h \rightarrow 011, i \rightarrow 100, k \rightarrow 111\}$$

**Шаг 8.** Для двух последних элементов  $befa := bef+a = 29+25 = 54$ . Поместить узел  $befa=46$  перед узлом  $cghdik=46$ . Построить два следующих ряда.

$$\begin{array}{ccc} befa & cghdik, \\ 54 & 46. \end{array}$$

Продолжить коды символами слева для  $bef$   $a$ :  $\text{cod}(b):=0$ ,  $\text{cod}(e):=0$ ,  $\text{cod}(f):=0$ ,  $\text{cod}(a):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow 1, b \rightarrow 00, c \rightarrow 00, d \rightarrow 11, e \rightarrow 010, f \rightarrow 011, g \rightarrow 010, h \rightarrow 011, i \rightarrow 100, k \rightarrow 111\}$$

**Шаг 9.** Для двух последних элементов  $befacghdik := befa+cghdik = 54+46 = 100$ . Поместить узел  $befa=54$  перед узлом  $cghdik=46$ . Построить два следующих ряда.

$$\begin{array}{c} befacghdik, \\ 100. \end{array}$$

Продолжить коды символами слева для  $befa$   $cghdik$ :  $\text{cod}(b):=0$ ,  $\text{cod}(e):=0$ ,  $\text{cod}(f):=0$ ,  $\text{cod}(a):=0$ ,  $\text{cod}(c):=1$ ,  $\text{cod}(g):=1$ ,  $\text{cod}(h):=1$ ,  $\text{cod}(d):=1$ ,  $\text{cod}(i):=1$ ,  $\text{cod}(k):=1$ .

Построить следующую схему алфавитного кодирования.

$$s = \{a \rightarrow 01, b \rightarrow 000, c \rightarrow 100, d \rightarrow 110, e \rightarrow 0010, f \rightarrow 0011, g \rightarrow 1010, h \rightarrow 1011, i \rightarrow 1100, k \rightarrow 1111\}.$$

**Шаг 10.** Вернуть разделимую префиксную схему алфавитного кодирования  
 $s = \{a \rightarrow 01, b \rightarrow 000, c \rightarrow 100, d \rightarrow 110, e \rightarrow 0010, f \rightarrow 0011, g \rightarrow 1010, h \rightarrow 1011, i \rightarrow 1100, k \rightarrow 1111\}$ .

**Замечание.** Цена схемы  $s$  есть число

$$\begin{aligned} \text{Cost}(s) = & 0.25 \cdot 2 + 0.15 \cdot 3 + 0.12 \cdot 3 + 0.11 \cdot 3 + 0.08 \cdot 4 + 0.06 \cdot 4 + \\ & 0.06 \cdot 4 + 0.06 \cdot 4 + 0.06 \cdot 4 + 0.05 \cdot 4 = 3.12. \end{aligned}$$

По схеме Фано  $\text{Cost}(s) = 3.12$ .

## ИНФОРМАЦИЯ И ЭНТРОПИЯ

**Определение.** Информация есть любая конечная последовательность знаков, допустимых в компьютерах и компьютерных сетях.  $\square$

Пусть  $A = \{a_1, a_2, \dots, a_m\}$  есть  $m$ -элементный алфавит из  $m$  знаков при равновероятности всех знаков алфавита. *Сообщение* есть слово длины  $n$  в алфавите  $A$ . Количество всех сообщений длины  $n$  равно  $N = m^n$ . Информация обращается в компьютерах такими порциями длины  $n$ . Естественно определить количество информации как число  $N$ . Теоретически удобнее задать ее как логарифм числа  $N$ .

**Определение.** Количество информации  $I = \log N = \log m^n = n \log m$ .

**Определение.** Энтропия  $H = \frac{I}{n} = \frac{n \log m}{n} = \log m$  есть количество информации, приходящееся на один элемент сообщения (знак алфавита  $A$ ).

**Замечание.** Основание логарифма в определении количества информации и энтропии несущественно, ибо при переходе от одного основания логарифма к другому  $\log_a m = \frac{\log_b m}{\log_b a} = \frac{\log_b m}{(\log_a a)/(\log_a b)} = \log_a b \cdot \log_b m$  (в знаменателе перешли к основанию  $a$ ). В практике наиболее употребимо бинарное основание логарифма. Энтропия  $H_0 = \log_2 m$ . При  $m = 2$  число  $H_0 = \log_2 2 = 1$  есть один бит на один знак бинарного алфавита. (Bit от англ. binary digit – двоичная единица). Двоичное сообщение длины  $n$  содержит  $n$  бит информации.

*Байт* есть единица количества информации, равная 8 битам.

Если основание логарифма есть десять, то энтропия выражается в десятичных единицах на элемент алфавита – в дитах, причем 1 дит =  $\log_{10} 2$  бит = 3.32 бит.

### Разновероятность знаков алфавита. Формулы Шеннона

Пусть в сообщении длины  $n$  знак  $x_i$  появляется  $n_i$  раз. Тогда вероятность появления знака  $x_i$  равна  $P_i = \frac{n_i}{n}$ , ( $i = 1, 2, \dots, m$ ). Все знаки алфавита составляют полную систему случайных событий. Поэтому  $\sum_{i=1}^m P_i = 1$ .

Для количества информации  $I$  и энтропии  $H$  справедливы *формулы Шеннона*:  $I = -n \sum_{i=1}^m P_i \log P_i$ ;  $H = -\sum_{i=1}^m P_i \log P_i$ .

В выражениях для количества информации  $I$  и энтропии  $H$  обычно используются логарифмы с основанием 2.

**Замечание.** При равновероятности знаков алфавита вероятность  $P_i = 1/m$ , где  $m$  есть мощность алфавита, из формулы Шеннона энтропия

$$H = -\sum_{i=1}^m P_i \log P_i = -\sum_{i=1}^m \frac{1}{m} \log \frac{1}{m} = -(m \cdot \frac{1}{m})(-\log m) = \log m.$$

При равновероятности знаков алфавита энтропия зависит только от мощности  $m$  алфавита и является характеристикой только алфавита.

**Задача 42.** Написать свое полное имя (фамилия, имя, отчество, ФИО) и взять для исследования текст  $T$  из тридцати первых букв ФИО. Если ФИО имеет меньше тридцати букв, то дополнить ФИО любыми другими именами

до получения слова с длиной больше тридцати. Взять для исследования текст  $T$  из  $n = 30$  первых букв нового ФИО. С точностью до сотых (две цифры после десятичной точки) найти в тексте  $T$  частоту появления букв. Сумма частот должна равняться единице. Найти количество информации  $I$  в тексте  $T$  и энтропию  $H$  текста  $T$ .

**Пример.** Найти количество информации  $I$  и энтропию  $H$  в тексте длины  $n=30$  в алфавите  $\{x_1, x_2, x_3, x_4\}$  из  $m = 4$  букв с распределением вероятностей  $P(x_1) = 0.1, P(x_2) = 0.1, P(x_3) = 0.1, P(x_4) = 0.7$ .

*Решение.* Энтропия  $H = -\sum_{i=1}^{m=4} P_i \log P_i =$

$$\begin{aligned} & -P_1 \cdot \log P_1 - P_2 \cdot \log P_2 - P_3 \cdot \log P_3 - P_4 \cdot \log P_4 = \\ & -0.1 \cdot \log 0.1 - 0.1 \cdot \log 0.1 - 0.1 \cdot \log 0.1 - 0.7 \cdot \log 0.7 = \\ & -0.3 \cdot \log 0.1 - 0.7 \cdot \log 0.7 = 1.357. \end{aligned}$$

Количество информации  $I = -n \sum_{i=1}^m P_i \log P_i = -30 \cdot (-1.357) = 40.71$ .  $\square$

**Замечание.** При бинарном алфавите с вероятностями  $P$  и  $1-P$  его знаков энтропия  $H = -P \cdot \log P - (1-P) \cdot \log (1-P)$ .

**Задача 43.** Закон распределения вероятностей  $p_{ij} = P(x_i, y_j)$  системы двух зависимых источников информации  $X$  и  $Y$  задан в следующей таблице.

$\text{№}\backslash p_{ij}$	$p_{11}$	$p_{12}$	$p_{13}$	$p_{21}$	$p_{22}$	$p_{23}$	$p_{31}$	$p_{32}$	$p_{33}$
<b>43.1</b>	0.14	0.26	0	0	0.23	0.16	0	0	0.21
<b>43.2</b>	0.21	0.14	0.26	0	0	0.23	0.16	0	0
<b>43.3</b>	0	0.21	0.14	0.26	0	0	0.23	0.16	0
<b>43.4</b>	0	0	0.21	0.14	0.26	0	0	0.23	0.16
<b>43.5</b>	0.16	0	0	0.21	0.14	0.26	0	0	0.23
<b>43.6</b>	0.23	0.16	0	0	0.21	0.14	0.26	0	0
<b>43.7</b>	0	0.23	0.16	0	0	0.21	0.14	0.26	0
<b>43.8</b>	0	0	0.23	0.16	0	0	0.21	0.14	0.26
<b>43.9</b>	0.26	0	0	0.23	0.16	0	0	0.21	0.14
<b>43.10</b>	0.14	0	0.26	0	0.23	0	0.16	0	0.21
<b>43.11</b>	0.21	0.14	0	0.26	0	0.23	0	0.16	0
<b>43.12</b>	0	0.21	0.14	0	0.26	0	0.23	0	0.16
<b>43.13</b>	0.16	0	0.21	0.14	0	0.26	0	0.23	0
<b>43.14</b>	0	0.16	0	0.21	0.14	0	0.26	0	0.23
<b>43.15</b>	0.23	0	0.16	0	0.21	0.14	0	0.26	0
<b>43.16</b>	0	0.23	0	0.16	0	0.21	0.14	0	0.26
<b>43.17</b>	0.26	0	0.23	0	0.16	0	0.21	0.14	0
<b>43.18</b>	0	0.26	0	0.23	0	0.16	0	0.21	0.14
<b>43.19</b>	0.21	0	0	0.16	0.23	0	0	0.26	0.14
<b>43.20</b>	0.14	0.21	0	0	0.16	0.23	0	0	0.26
<b>43.21</b>	0.26	0.14	0.21	0	0	0.16	0.23	0	0
<b>43.22</b>	0	0.26	0.14	0.21	0	0	0.16	0.23	0

<b>43.23</b>	0	0	0.26	0.14	0.21	0	0	0.16	0.23
<b>43.24</b>	0.23	0	0	0.26	0.14	0.21	0	0	0.16
<b>43.25</b>	0.16	0.23	0	0	0.26	0.14	0.21	0	0
<b>43.26</b>	0	0.16	0.23	0	0	0.26	0.14	0.21	0
<b>43.27</b>	0	0	0.16	0.23	0	0	0.26	0.14	0.21
<b>43.28</b>	0.14	0	0.26	0	0	0.23	0.16	0.21	0
<b>43.29</b>	0	0.14	0	0.26	0	0	0.23	0.16	0.21
<b>43.30</b>	0.21	0	0.14	0	0.26	0	0	0.23	0.16

Найти энтропии  $H(X)$ ,  $H(Y)$ ,  $H_X(Y)$ ,  $H(X,Y)$ .

**Замечание.** Стока 43.30 задает следующую таблицу.

$X/Y$	$y_1$	$y_2$	$y_3$
$x_1$	$p_{11}=0.21$	$p_{12}=0$	$p_{13}=0.14$
$x_2$	$p_{21}=0$	$p_{22}=0.26$	$p_{23}=0$
$x_3$	$p_{31}=0$	$p_{32}=0.23$	$p_{33}=0.16$

**Пример.** Закон распределения вероятностей  $P(x_i, y_j)$  системы двух зависимых источников информации  $X$  и  $Y$ , задан в следующей таблице.

$X/Y$	$y_1$	$y_2$	$y_3$
$x_1$	0.3	0.2	0
$x_2$	0	0.1	0.2
$x_3$	0	0	0.2

Найти энтропии  $H(X)$ ,  $H(Y)$ ,  $H_X(Y)$ ,  $H(X,Y)$ .

*Решение.* 1. Найдем безусловные вероятности  $P(x_i)$  и  $P(y_j)$  системы.

а) сложим вероятности “по строкам” и получим вероятности возможных значений  $X$ :  $P(x_1) = \sum_{j=1}^s P(x_1, y_j) = 0.5$ ,  $P(x_2) = 0.3$ ,  $P(x_3) = 0.2$ .

б) сложим вероятности “по столбцам” и получим вероятности возможных значений  $Y$ :  $P(y_1) = \sum_{i=1}^r P(x_i, y_1) = 0.3$ ,  $P(y_2) = 0.3$ ,  $P(y_3) = 0.4$ .

2. Энтропия источника информации  $X$ .

$$H(X) = -\sum_{i=1}^r P(x_i) \log P(x_i) = -(0.5 \log 0.5 + 0.3 \log 0.3 + 0.2 \log 0.2) = 1.485 \text{ бит.}$$

3. Энтропия источника информации  $Y$ .

$$H(Y) = -\sum_{j=1}^s P(y_j) \log P(y_j) = -(0.3 \log 0.3 + 0.3 \log 0.3 + 0.4 \log 0.4) = 1.571 \text{ бит.}$$

4. Условная энтропия источника информации  $Y$  при условии, что сообщения источника  $X$  известны.

$$H_X(Y) = -\sum_{i=1}^r P(x_i) \sum_{j=1}^s P_{x_i}(y_j) \log P_{x_i}(y_j).$$

Условная вероятность события  $y_j$  при условии выполнения события  $x_i$  принимается по определению  $P_{x_i}(y_j) = \frac{P(x_i, y_j)}{P(x_i)}$ . Отсюда можно найти условные вероятности возможных значений  $Y$  при условии, что составляющая  $X$  приняла значение  $x_i$ .

Для  $x_1$ .

$$P_{x_1}(y_1) = \frac{P(x_1, y_1)}{P(x_1)} = \frac{0.3}{0.5} = 0.6.$$

$$P_{x_1}(y_2) = \frac{P(x_1, y_2)}{P(x_1)} = \frac{0.2}{0.5} = 0.4.$$

$$P_{x_1}(y_3) = \frac{P(x_1, y_3)}{P(x_1)} = \frac{0}{0.5} = 0.$$

Для  $x_2$ .

$$P_{x_2}(y_1) = \frac{P(x_2, y_1)}{P(x_2)} = \frac{0}{0.3} = 0.$$

$$P_{x_2}(y_2) = \frac{P(x_2, y_2)}{P(x_2)} = \frac{0.1}{0.3} = 0.33.$$

$$P_{x_2}(y_3) = \frac{P(x_2, y_3)}{P(x_2)} = \frac{0.2}{0.3} = 0.67.$$

Для  $x_3$ .

$$P_{x_3}(y_1) = \frac{P(x_3, y_1)}{P(x_3)} = \frac{0}{0.2} = 0.$$

$$P_{x_3}(y_2) = \frac{P(x_3, y_2)}{P(x_3)} = \frac{0}{0.2} = 0.$$

$$P_{x_3}(y_3) = \frac{P(x_3, y_3)}{P(x_3)} = \frac{0.2}{0.2} = 1.$$

Поэтому

$$\begin{aligned} H_X(Y) &= -\sum_{i=1}^r P(x_i) \sum_{j=1}^s P_{x_i}(y_j) \log P_{x_i}(y_j) = \\ &= -[0.5(0.6 \log 0.6 + 0.4 \log 0.4 + 0) + \\ &\quad 0.3(0 + 0.33 \log 0.33 + 0.67 \log 0.67) + \\ &\quad 0.2(0 + 0 + 1 \log 1)] = 0.76 \text{ бит.} \end{aligned}$$

5. Условная вероятность события  $x_i$  при условии выполнения события  $y_j$  принимается по определению  $P_{y_j}(x_i) = \frac{P(x_i, y_j)}{P(y_j)}$ . Отсюда можно найти условные вероятности возможных значений  $X$  при условии, что составляющая  $Y$  приняла значение  $y_j$ .

Для  $y_1$ .

$$P_{y_1}(x_1) = \frac{P(x_1, y_1)}{P(y_1)} = \frac{0.3}{0.3} = 1.$$

$$P_{y_1}(x_2) = \frac{P(x_2, y_1)}{P(y_1)} = \frac{0}{0.3} = 0.$$

$$P_{y_1}(x_3) = \frac{P(x_3, y_1)}{P(y_1)} = \frac{0}{0.3} = 0.$$

Для  $y_2$ .

$$P_{y_2}(x_1) = \frac{P(x_1, y_2)}{P(y_2)} = \frac{0.2}{0.3} = 0.67.$$

$$P_{y_2}(x_2) = \frac{P(x_2, y_2)}{P(y_2)} = \frac{0.1}{0.3} = 0.33.$$

$$P_{y_2}(x_3) = \frac{P(x_3, y_2)}{P(y_2)} = \frac{0}{0.3} = 0.$$

Для  $y_3$ .

$$P_{y_3}(x_1) = \frac{P(x_1, y_3)}{P(y_3)} = \frac{0}{0.4} = 0.$$

$$P_{y_3}(x_2) = \frac{P(x_2, y_3)}{P(y_3)} = \frac{0.2}{0.4} = 0.50.$$

$$P_{y_3}(x_3) = \frac{P(x_3, y_3)}{P(y_3)} = \frac{0.2}{0.4} = 0.50.$$

$$\begin{aligned} H_Y(X) &= -\sum_{j=1}^s P(y_j) \sum_{i=1}^r P_{y_j}(x_i) \log P_{y_j}(x_i) = \\ &= -[0.3 (\log 1 + 0 + 0) + 0.3 (0.67 \log 0.67 + 0.33 \log 0.33 + 0) + \\ &\quad 0.4 (0 + 0.50 \log 0.50 + 0.50 \log 0.50)] = 0.874 \text{ бит.} \end{aligned}$$

6. Общая энтропия зависимых источников информации  $X$  и  $Y$ .

$$\begin{aligned} H(X, Y) &= -\sum_{i=1}^r \sum_{j=1}^s P(x_i, y_j) \log P(x_i, y_j) = -((0.3 \log 0.3 + 0.2 \log 0.2 + 0) + \\ &\quad (0 + 0.1 \log 0.1 + 0.2 \log 0.2) + (0 + 0 + 0.2 \log 0.2)) = \\ &= (0.521 + 0.464 + 0) + (0 + 0.332 + 0.464) + (0 + 0 + 0.464) = 2.245 \text{ бит.} \end{aligned}$$

Проверка.

$$H(X, Y) = 2.245 \text{ бит.}$$

$$H(X, Y) = H(X) + H_Y(Y) = 1.485 + 0.760 = 2.245 \text{ бит.}$$

## 4. МАТЕМАТИЧЕСКАЯ ЛОГИКА

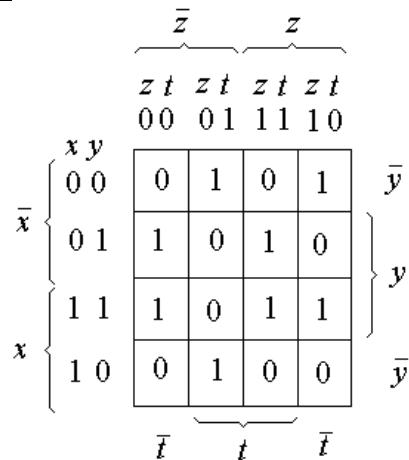
**Задача 1.** Заданную функцию  $f(x_1, x_2, x_3, x_4)$  представить: 1) таблицей своих значений, 2) множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых  $f$  принимает значение 1, 3) множеством  $M_0$  десятичных эквивалентов двоичных наборов, на которых  $f$  принимает значение 0, 4) картой Карно, 5) на двоичном единичном кубе.

- |                         |                         |
|-------------------------|-------------------------|
| 1.1. 0111001011110001.  | 1.2. 0001110000111011.  |
| 1.3. 1100111001110010.  | 1.4. 0101000111000101.  |
| 1.5. 1100010110100110.  | 1.6. 1001110100011010.  |
| 1.7. 0100110000011110.  | 1.8. 1111000100111011.  |
| 1.9. 0000110101110110.  | 1.10. 1011101011000101. |
| 1.11. 0011101100011110. | 1.12. 0111011001011010. |
| 1.13. 0001111010111010. | 1.14. 0101101010011101. |
| 1.15. 1011101011011100. | 1.16. 1011000101111100. |
| 1.17. 1001110101111100. | 1.18. 0011011101111100. |
| 1.19. 1101110001110111. | 1.20. 0111110010001101. |
| 1.21. 0111011111100010. | 1.22. 1000110101000101. |
| 1.23. 1110001010111001. | 1.24. 0100010101000111. |
| 1.25. 1011100110000110. | 1.26. 0100011101110011. |
| 1.27. 1000011001110011. | 1.28. 0101011001110011. |
| 1.29. 0111010001010110. | 1.30. 0101011001010110. |

**Пример.** Заданную функцию  $f(x_1, x_2, x_3, x_4)$  представить: 1) таблицей своих значений, 2) множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых  $f$  принимает значение 1, 3) множеством  $M_0$  десятичных эквивалентов двоичных наборов, на которых  $f$  принимает значение 0, 4) картой Карно.  $f = 0100100101001011$ .

*Решение.*  $M_1 = \{1, 2, 4, 7, 12, 14, 15\}$ ,  $M_0 = \{0, 3, 5, 6, 8, 10, 11, 13\}$ . Кarta Карно

$x$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$y$	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
$z$	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	1
$t$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$f$	0	1	1	0	1	0	0	1	0	1	0	0	1	0	1	1



**Задача 2.** Для данных формул построить таблицу истинностных значений и определить, является ли формула а) общезначимой, б) выполнимой, в) опровергимой, г) невыполнимой.

- 2.1.  $(x \rightarrow (y \rightarrow z)) \rightarrow ((x \rightarrow y) \rightarrow (x \rightarrow z)),$   
 $\neg(((x \rightarrow y) \rightarrow (\neg z \rightarrow u)) \rightarrow w) \rightarrow w \rightarrow (x \rightarrow (u \rightarrow x)),$   
 $(x \vee \neg x) \equiv \neg x, (x \& \neg x) \equiv x.$
- 2.2.  $(x \rightarrow y) \rightarrow ((x \rightarrow z) \rightarrow (x \rightarrow yz)),$   
 $\neg((x \rightarrow y) \rightarrow ((x \rightarrow (y \rightarrow z)) \rightarrow (x \rightarrow z))),$   
 $(x \rightarrow y) \rightarrow ((\neg(x \rightarrow z) \rightarrow (x \rightarrow yz)).$
- 2.3.  $(x \rightarrow z) \rightarrow ((y \rightarrow z) \rightarrow (x \equiv (y \rightarrow z))), \neg((xy \rightarrow z) \rightarrow (x \rightarrow (y \rightarrow z))),$   
 $(x \rightarrow (y \rightarrow z)) \rightarrow (\neg(x \rightarrow y) \rightarrow (x \rightarrow z)).$
- 2.4.  $(x \equiv x) \vee x, (x \& x) \equiv x, (x \vee x) \equiv x, \neg((x \rightarrow (y \rightarrow z)) \rightarrow (x \& y \rightarrow z)),$   
 $(x \vee \neg y) \equiv \neg(x \vee y), x \& y \equiv y \& x.$
- 2.5.  $x \vee y \equiv y \vee x, x \& y \equiv y \& x, ((\neg x \rightarrow \neg y) \rightarrow ((\neg y \rightarrow x) \rightarrow y)),$   
 $(xy \rightarrow z) \rightarrow (x \rightarrow (\neg(y \rightarrow z))).$
- 2.6.  $((x \rightarrow y) \rightarrow (\neg z \rightarrow u)) \rightarrow w \rightarrow ((w \rightarrow x) \rightarrow (u \rightarrow x)),$   
 $\neg((x \vee y) \equiv (y \vee x)), \neg((x \& y) \equiv (y \& x)), (\neg x \rightarrow \neg y) \rightarrow ((\neg y \rightarrow x) \rightarrow \neg y).$
- 2.7.  $(x \rightarrow y) \rightarrow ((x \rightarrow (y \rightarrow z)) \rightarrow (x \rightarrow z)),$   
 $\neg((x \rightarrow z) \rightarrow ((y \rightarrow z) \rightarrow (x \equiv (y \rightarrow z)))), (x \rightarrow (y \rightarrow z)) \rightarrow (\neg(xy \rightarrow z)).$
- 2.8.  $(x \rightarrow y) \rightarrow ((y \rightarrow z) \rightarrow (x \rightarrow z)), \neg((x \rightarrow y) \rightarrow ((x \rightarrow z) \rightarrow (x \rightarrow yz))),$   
 $((x \rightarrow y) \rightarrow (\neg z \rightarrow \neg u)) \rightarrow \neg w \rightarrow ((w \rightarrow x) \rightarrow (z \rightarrow x)).$
- 2.9.  $(\neg y \rightarrow x) \rightarrow ((y \rightarrow x) \rightarrow x),$   
 $\neg((x \rightarrow (y \rightarrow z)) \rightarrow ((x \rightarrow y) \rightarrow (x \rightarrow z))), x \vee yz \equiv (x \vee y) \& (\neg x \& \neg y).$
- 2.10.  $(xy \rightarrow z) \rightarrow (x \rightarrow (y \rightarrow z)), \neg((x \vee x) \equiv x), \neg(((x \& x) \equiv x),$   
 $x \& \neg(yz) \equiv (xy)z.$
- 2.11.  $(x \rightarrow (y \rightarrow z)) \rightarrow (xy \rightarrow z), \neg((\neg y \rightarrow x) \rightarrow ((y \rightarrow x) \rightarrow x)),$   
 $(x \rightarrow y) \rightarrow ((\neg y \rightarrow z) \rightarrow (\neg x \rightarrow z)).$
- 2.12.  $(\neg x \rightarrow \neg y) \rightarrow ((\neg y \rightarrow x) \rightarrow y), \neg((x \rightarrow y) \rightarrow ((y \rightarrow z) \rightarrow (x \rightarrow z))),$   
 $(x \vee z) \rightarrow (\neg(y \rightarrow z) \rightarrow ((x \vee y) \rightarrow z)).$
- 2.13.  $(x \vee yz) \equiv (x \vee y)(x \vee z), \neg((x \rightarrow y) \equiv (\neg y \rightarrow \neg x)),$   
 $(x \rightarrow y) \rightarrow ((x \rightarrow (\neg y \rightarrow z)) \rightarrow (x \rightarrow z)).$
- 2.14.  $(x \vee (y \vee z)) \equiv ((x \vee y) \vee z), \neg((x \rightarrow y) \equiv (\neg x \vee y)), x(\neg y \vee z) \equiv (xy \vee xz).$
- 2.15.  $x \rightarrow (y \rightarrow x), \neg(\neg x \rightarrow (\neg y \rightarrow \neg(x \vee y))), \neg(x \vee y) \equiv (x \& \neg y).$
- 2.16.  $xy \rightarrow x, \neg(x(y \vee z) \equiv (xy \vee xz)), (\neg y \rightarrow x) \rightarrow ((y \rightarrow x) \rightarrow \neg x).$
- 2.17.  $xy \rightarrow y, \neg((x(yz) \equiv (xy)z)). (x \rightarrow y) \equiv (y \rightarrow \neg x).$
- 2.18.  $x \rightarrow (x \vee y), \neg(x(x \vee y) \equiv x). \neg x \equiv \neg \neg \neg x.$
- 2.19.  $y \rightarrow (x \vee y), \neg(y \rightarrow (x \vee y)), (x \vee (y \vee \neg z)) \equiv ((x \vee y) \vee z).$
- 2.20.  $(x \rightarrow y) \equiv (\neg y \rightarrow \neg x), \neg(x \rightarrow (y \rightarrow x)), x \rightarrow (\neg y \rightarrow (x \vee y)).$
- 2.21.  $x \equiv \neg x, \neg(\neg(x \vee y) \equiv \neg x \& \neg y), ((x \vee \neg y) \equiv \neg(x \& y)).$
- 2.22.  $(x \& \neg y) \equiv (\neg x \vee y), \neg((x \vee xy) \equiv x), xy \rightarrow \neg y.$
- 2.23.  $x(yz) \equiv (xy)z, \neg(\neg(x \vee y) \equiv (\neg x \& \neg y)), x(x \vee \neg y) \equiv x.$
- 2.24.  $(x \vee xy) \equiv x, \neg(x \vee (y \vee z) \equiv (x \vee y) \vee z), xy \rightarrow x.$

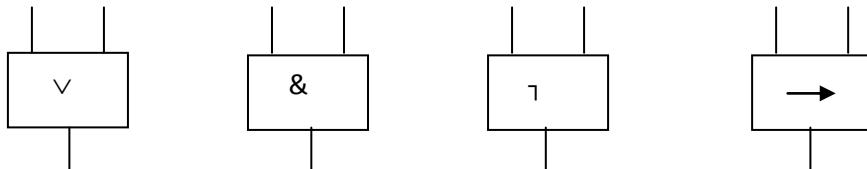
- 2.25.**  $x(x \vee y) \equiv x$ ,  $\neg(x \equiv \neg \neg x)$ ,  $\neg x \vee xy \equiv x$ .
- 2.26.**  $x(y \vee z) \equiv (xy \vee xz)$ ,  $\neg((x \& y) \rightarrow y)$ ,  $\neg x \rightarrow (y \rightarrow x)$ .
- 2.27.**  $x \vee \neg x \& y$ ,  $\neg(x \rightarrow (x \vee y))$ ,  $(x \rightarrow \neg y) \equiv (\neg x \vee y)$ .
- 2.28.**  $(x \vee y) \equiv (\neg x \& \neg y)$ ,  $\neg(x \vee \neg y)$ ,  $x \rightarrow (\neg x \vee y)$ .
- 2.29.**  $(x \& y) \equiv (\neg x \vee \neg y)$ ,  $\neg(x \& y \rightarrow x)$ ,  $\neg x \vee \neg x$ .
- 2.30.**  $\neg x \rightarrow (\neg y \rightarrow x \vee y)$ ,  $\neg((x \vee yz) \equiv (x \vee y)(x \vee z))$ ,  $y \rightarrow x \vee \neg y$ .

**Пример.** Для данной формулы построить таблицу истинностных значений и определить, является ли формула а) общезначимой, б) выполнимой, в) опровергимой, г) невыполнимой.  $f(x, y, z) = \overline{(x \vee yz) \equiv (x \vee y)(x \vee \bar{y} \cdot z)}$ .  
**Решение.**

	0	1	2	3	4	5	6	7
$x$	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
$f$	0	0	1	1	0	0	0	0

*Ответ.* Формула  $f$ : а) общезначимой не является, б) выполнима (столбцы 2,3), в) опровергима (столбцы 0,1,4 – 7), г) невыполнимой не является.

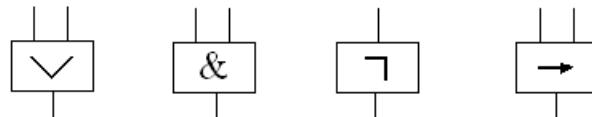
**Задача 3.** Для данных формул построить таблицу истинностных значений и определить, является ли формула а) общезначимой, б) выполнимой, в) опровергимой, г) невыполнимой, д) упростить формулу. Для обеих формул построить схемы из функциональных элементов для дизъюнкции, конъюнкции, отрицания, импликации.



- 3.1.**  $x \rightarrow \neg(\neg(x \& \neg y) \vee (x \rightarrow y))$ .    **3.2.**  $\neg x \vee (\neg y \rightarrow x) \vee \neg(x \rightarrow y)$ .
- 3.3.**  $\neg(x \rightarrow \neg(xy)) \vee \neg(y \rightarrow \neg x \& \neg y)$ .    **3.4.**  $\neg(xy) \rightarrow (y \rightarrow \neg(xy))$ .
- 3.5.**  $(x \rightarrow y) \rightarrow \neg(\neg y \rightarrow \neg(\neg(xy) \vee x))$ .
- 3.6.**  $\neg(x \rightarrow y) \rightarrow (\neg y \vee \neg(xy))$ .    **3.7.**  $\neg(\neg x \rightarrow y) \rightarrow \neg(\neg x \vee \neg(xy))$ .
- 3.8.**  $\neg(\neg(x \vee xy) \rightarrow x) \rightarrow y$ .    **3.9.**  $\neg((xy \vee x \& \neg y) \rightarrow x) \rightarrow y$ .
- 3.10.**  $\neg(\neg(x \vee y) \vee \neg(x \rightarrow y)) \rightarrow x$ .
- 3.11.**  $\neg(xy \vee \neg x \& y) \vee \neg(\neg(x \vee xy) \vee \neg x) \vee x$ .
- 3.12.**  $\neg(x \rightarrow y) \vee \neg(\neg x \rightarrow y) \vee \neg(x \rightarrow xy) \vee (y \rightarrow x)$ .
- 3.13.**  $\neg(x \vee y) \rightarrow \neg(x \rightarrow y) \vee y$ .
- 3.14.**  $(\neg(xy \vee y) \rightarrow \neg(xy \rightarrow x)) \rightarrow x$ .
- 3.15.**  $\neg(\neg x \& y \vee x) \vee \neg(xy \rightarrow y) \rightarrow (x \vee y)$ .
- 3.16.**  $(\neg(x \rightarrow y) \vee x) \rightarrow ((x \vee y) \rightarrow y)$ .
- 3.17.**  $(\neg(xy) \rightarrow y) \rightarrow ((xy \rightarrow \neg x \& y) \rightarrow x)$ .
- 3.18.**  $\neg(x \vee y) \vee \neg(y \rightarrow ((xy \rightarrow (x \vee y)))$ .

- 3.19.**  $\neg(xy \rightarrow y) \vee ((\neg(x \rightarrow y) \vee xy) \rightarrow x)$ .  
**3.20.**  $\neg(xy \rightarrow y \rightarrow \neg((x \rightarrow y) \rightarrow xy))$ .  
**3.21.**  $\neg(x \vee y) \vee \neg(y \rightarrow (xy \rightarrow \neg x \& y) \rightarrow y)$ .  
**3.22.**  $(\neg(xy \vee y) \rightarrow x) \rightarrow \neg x$ .  
**3.23.**  $((x \& \neg y \vee \neg(\neg x \vee y)) \rightarrow x) \rightarrow y$ .  
**3.24.**  $(\neg y \vee x) \rightarrow (x \& \neg y \vee y)$ .  
**3.25.**  $\neg(x \rightarrow \neg x \& y) \rightarrow \neg(y \rightarrow (x \rightarrow y))$ .  
**3.26.**  $\neg(x \& \neg y) \vee \neg(xy) \rightarrow x$ .  
**3.27.**  $\neg((\neg x \& \neg y \rightarrow x) \rightarrow (yx \vee \neg x))$ .  
**3.28.**  $\neg(\neg x \rightarrow y) \vee \neg(\neg x \& y \rightarrow x \& \neg y)$ .  
**3.29.**  $(x \vee \neg(xy)) \rightarrow \neg(y \rightarrow xy)$ .  
**3.30.**  $(\neg(xy) \vee x \& \neg y) \rightarrow \neg(x \vee y)$ .

**Пример.** Для данной формулы  $f(x,y) = (\overline{xy} \vee x \cdot \bar{y}) \rightarrow \overline{x \vee y}$  построить таблицу истинностных значений и определить, является ли формула а) общезначимой, б) выполнимой, в) опровергимой, г) невыполнимой, д) упростить формулу. Для обеих формул построить схемы из функциональных элементов для дизъюнкции, конъюнкции, отрицания, импликации.



**Решение.**  $f(x,y) = ((\overline{xy} \vee x \cdot \bar{y}) \rightarrow \overline{x \vee y}) = \overline{xy} \& \overline{xy} \vee \bar{x} \& \bar{y} = xy(\bar{x} \vee y) \vee \bar{x} \bar{y} = xy \vee \bar{x} \bar{y}$ . Подформулы формулы  $f$ :  $\overline{xy} \vee x \bar{y}$ ,  $\overline{x \vee y}$ ,  $xy$ ,  $x \bar{y}$ ,  $x \vee y$  (рис.10.1).

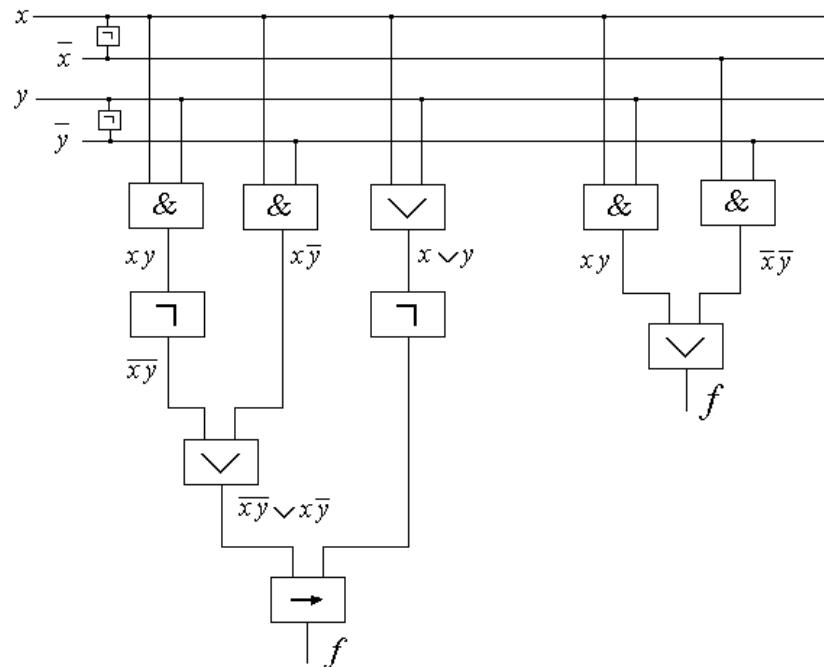


Рис.10.1

**Задача 4.** Построить СДНФ, СКНФ, полином Жегалкина для функции  $f(x_1, x_2, x_3)$ , заданной множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых  $f$  принимает значение 1.

- |                           |                           |                         |                           |
|---------------------------|---------------------------|-------------------------|---------------------------|
| <b>4.1.</b> {4,5,6,7}.    | <b>4.2.</b> {3,4,5,6}.    | <b>4.3.</b> {2,3,5,6}.  | <b>4.4.</b> {1,3,5,6}.    |
| <b>4.5.</b> {0,1,2,3}.    | <b>4.6.</b> {0,1,2,7}.    | <b>4.7.</b> {0,1,4,7}.  | <b>4.8.</b> {0,2,4,7}.    |
| <b>4.9.</b> {4,5,7}.      | <b>4.10.</b> {4,6,7}.     | <b>4.11.</b> {2,3,7}.   | <b>4.12.</b> {0,1,4,5,6}. |
| <b>4.13.</b> {1,3,7}.     | <b>4.14.</b> {0,1,2,3,6}. | <b>4.15.</b> {0,5,7}.   | <b>4.16.</b> {2,6,7}.     |
| <b>4.17.</b> {0,5,6}.     | <b>4.18.</b> {0,1,2,3,5}. | <b>4.19.</b> {0,3,6}.   | <b>4.20.</b> {0,3,5}.     |
| <b>4.21.</b> {1,2,3,4,6}. | <b>4.22.</b> {1,2,3}.     | <b>4.23.</b> {1,4,6}.   | <b>4.24.</b> {0,2,4,5,6}. |
| <b>4.25.</b> {0,6,7}.     | <b>4.26.</b> {0,1,5,6,7}. | <b>4.27.</b> {2,4,5,6}. | <b>4.28.</b> {3,4,5,7}.   |
| <b>4.29.</b> {1,4,6,7}.   | <b>4.30.</b> {4,5,7}.     |                         |                           |

**Пример.** Построить СДНФ, СКНФ, полином Жегалкина для функции  $f(x_1, x_2, x_3)$ , заданной множеством  $M_1 = \{0, 2, 4, 5, 7\}$  десятичных эквивалентов двоичных наборов, на которых  $f$  принимает значение 1.

*Решение.* Полином Жегалкина

$$f(x_1, x_2, \dots, x_n) = \sum_{(i_1, \dots, i_n) \in E_2^n} a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \text{ где } x^i = \begin{cases} x, & \text{если } i=1, \\ 1, & \text{если } i=0, \end{cases}$$

каждый коэффициент  $a_{i_1, i_2, \dots, i_n} \in \{0, 1\}$ .

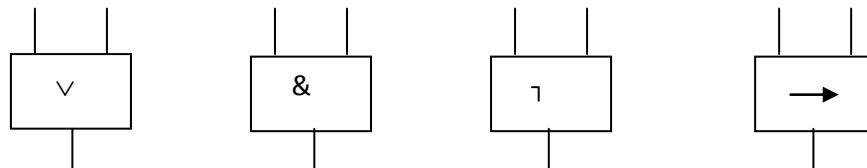
	0	1	2	3	4	5	8	7
x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
f	1	0	1	0	1	1	0	1

СДНФ.  $f(x, y, z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}y\bar{z} \vee x\bar{y}\bar{z} \vee x\bar{y}z \vee xyz$ .

СКНФ.  $f(x, y, z) = (x \vee y \vee \bar{z})(x \vee \bar{y} \vee \bar{z})(\bar{x} \vee \bar{y} \vee z)$ .

Полином Жегалкина.  $f(x, y, z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}y\bar{z} \vee x\bar{y}\bar{z} \vee x\bar{y}z \vee xyz = (x+1)(y+1)(z+1) + (x+1)y(z+1) + x(y+1)(z+1) + x(y+1)z + xyz = xyz + xy + xz + yz + x + y + 1 + xyz + xy + yz + y + xyz + xy + xz + x + xyz + xz + xyz = xy + xz + z + 1$ .

**Задача 5.** Найти все тупиковые и все минимальные ДНФ и КНФ для всюду определенной функции. Одну из минимальных форм реализовать схемой с элементами для  $\&$ ,  $\vee$ ,  $\neg$ .



- |                               |                               |
|-------------------------------|-------------------------------|
| <b>5.1.</b> 1001001110011011. | <b>5.2.</b> 0010100011011111. |
| <b>5.3.</b> 1101111100100010. | <b>5.4.</b> 1001100110111001. |
| <b>5.5.</b> 1110110011001100. | <b>5.6.</b> 1101110110001010. |
| <b>5.7.</b> 1010100011011101. | <b>5.8.</b> 1110110011001100. |

- |                                 |                                |
|---------------------------------|--------------------------------|
| <b>5.9.</b> 1101001000111011.   | <b>5.10.</b> 1010000011011111. |
| <b>5.11.</b> 1010100001110111.  | <b>5.12.</b> 1010101001011101. |
| <b>5.13.</b> 0110111011000110.  | <b>5.14.</b> 1110010011101100. |
| <b>5.15.</b> 0111110100101010.  | <b>5.16.</b> 0010100011111101. |
| <b>5.17.</b> 1100011011101100.  | <b>5.18.</b> 1111001000111011. |
| <b>5.19.</b> 0011011111001111.  | <b>5.20.</b> 1010001101110011. |
| <b>5.21.</b> 1110011111100001.  | <b>5.22.</b> 0010001001010111. |
| <b>5.23.</b> 11011101100001010. | <b>5.24.</b> 0111001001111010. |
| <b>5.25.</b> 1011011100001011.  | <b>5.26.</b> 1010001111011011. |
| <b>5.27.</b> 1101101011010010.  | <b>5.28.</b> 1010100001111111. |
| <b>5.29.</b> 0111110110001010.  | <b>5.30.</b> 0101100011110010. |

**Пример.** Найти все тупиковые и все минимальные ДНФ и КНФ для всюду определенной функции. Одну из минимальных форм реализовать схемой с элементами для  $\&$ ,  $\vee$ ,  $\neg$ .

#### *Алгоритм минимизации в классе нормальных форм*

Пусть  $f$  есть функция алгебры логики.

1. Строим все МДНФ функции  $f$ .
2. Строим все МКНФ функции  $f$ .
3. Из построенных минимальных форм выбираем минимальные по числу букв.

**Пример.** В классе нормальных форм минимизировать функцию  $f = 11011011$ .

1. СДНФ.  $f(x,y,z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee xy\bar{z} \vee xyz$ .
2. Сокращенная ДНФ.  $f(x,y,z) = (x \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z}) = xy \vee x\bar{z} \vee \bar{y}\bar{z} \vee \bar{x}z \vee yz \vee \bar{x}\bar{y}$ .

3. Строим матрицу покрытий (табл.10.3).

*Таблица 10.3*

N	ПИ	$\bar{x}\bar{y}\bar{z}$	$\bar{x}\bar{y}z$	$\bar{x}yz$	$x\bar{y}\bar{z}$	$xy\bar{z}$	$xyz$
1	$xy$					+	+
2	$x\bar{z}$				+	+	
3	$\bar{y}\bar{z}$	+			+		
4	$\bar{x}z$		+	+			
5	$yz$			+			+
6	$\bar{x}\bar{y}$	+	+				

Решеточный полином.  $E = (3 \vee 6)(4 \vee 6)(4 \vee 5)(2 \vee 3)(1 \vee 2)(1 \vee 5) = 1246 \vee 1356 \vee 134 \vee 256 \vee 2345$ .

4. Все тупиковые ДНФ функции  $f$ .

$$f(x,y,z) = xy \vee x\bar{z} \vee \bar{x}z \vee \bar{x}\bar{y}; f(x,y,z) = xy \vee \bar{y}\bar{z} \vee yz \vee \bar{x}\bar{y};$$

$$f(x,y,z) = xy \vee \bar{y}\bar{z} \vee \bar{x}z; f(x,y,z) = x\bar{z} \vee yz \vee \bar{x}\bar{y}; f(x,y,z) = x\bar{z} \vee \bar{y}\bar{z} \vee \bar{x}z \vee yz.$$

5. Все минимальные ДНФ функции  $f$ .

$$f(x,y,z) = xy \vee \bar{y}\bar{z} \vee \bar{x}z; f(x,y,z) = x\bar{z} \vee yz \vee \bar{x}\bar{y}.$$

6. Повторяем указанные выше этапы для функции  $\bar{f}$ .

$$\text{СДНФ. } \bar{f}(x,y,z) = \bar{x}y\bar{z} \vee x\bar{y}z.$$

$$\text{Сокращенная ДНФ. } \bar{f}(x,y,z) =$$

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

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

Построенная сокращенная ДНФ функции  $\bar{f}$  является для нее тупиковой и минимальной.

$$\text{Минимальная КНФ функции } f(x,y,z) = (x \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z}).$$

Построенные МДНФ и МКНФ имеют одно и то же число букв; все они составляют минимальные формы для  $f$ .

$$f(x,y,z) = xy \vee \bar{y}\bar{z} \vee \bar{x}z; f(x,y,z) = x\bar{z} \vee yz \vee \bar{x}\bar{y};$$

$$f(x,y,z) = (x \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z}).$$

**Задача 6.** Найти все тупиковые и все минимальные ДНФ и КНФ для всюду определенной функции. Одну из минимальных форм реализовать схемой с элементами для  $\&$ ,  $\vee$ ,  $\neg$ .

6.1.  $\{1,3,5,7,9,10,11,12,13\}.$

6.3.  $\{4,5,6,7,9,10,12,13,14\}.$

6.5.  $\{2,3,5,6,7,9,10,11,14\}.$

6.7.  $\{2,3,5,6,7,10,11,12,14\}.$

6.9.  $\{3,4,5,6,7,9,12,13,14\}.$

6.11.  $\{5,6,8,9,10,11,12,13,14\}.$

6.13.  $\{3,5,8,9,10,11,12,13,14\}.$

6.15.  $\{1,2,5,6,7,9,10,11,13,14\}.$

6.17.  $\{1,3,5,6,7,9,10,11,13,14\}.$

6.19.  $\{0,2,3,6,7,9,10,11,12,14\}.$

6.21.  $\{0,1,2,5,6,7,9,10,11,13\}.$

6.23.  $\{0,1,3,5,6,7,9,11,12,13\}.$

6.25.  $\{2,6,12,13,14,15\}.$

6.27.  $\{3,6,7,11,12,13,14,15\}.$

6.29.  $\{0,1,4,5,7,10,11,12,13,15\}.$

6.2.  $\{2,3,6,7,9,10,11,12,14\}.$

6.4.  $\{1,2,5,6,7,9,10,11,13\}.$

6.6.  $\{1,3,5,6,7,9,11,12,13\}.$

6.8.  $\{3,4,5,6,7,10,12,13,14\}.$

6.10.  $\{1,3,5,6,7,9,10,11,13\}.$

6.12.  $\{3,6,8,9,10,11,12,13,14\}.$

6.14.  $\{1,3,5,7,9,10,11,12,13,14\}.$

6.16.  $\{1,3,5,6,7,9,11,12,13,14\}.$

6.18.  $\{0,1,3,5,7,9,10,11,12,13\}.$

6.20.  $\{0,4,5,6,7,9,10,12,13,14\}.$

6.22.  $\{0,2,3,5,6,7,9,10,11,14\}.$

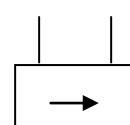
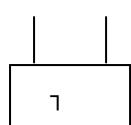
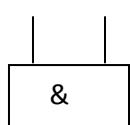
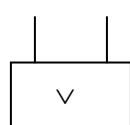
6.24.  $\{0,2,3,5,6,7,10,11,12,14\}.$

6.26.  $\{0,1,4,5,8,9,11,12,13,14,15\}.$

6.28.  $\{2,3,7,10,11,12,13,14,15\}.$

6.30.  $\{0,2,3,4,6,7,8,14,15\}.$

**Задача 7.** Найти все тупиковые и все минимальные ДНФ и КНФ для частично определенной функции. Одну из минимальных форм реализовать схемой с элементами  $\&$ ,  $\vee$ ,  $\neg$ .



<p>7.1. 1---010010--1--1.</p> <p>7.3. 1---011110--0--0.</p> <p>7.5. 1---110110--0--0.</p> <p>7.7. 0---111100--0--1.</p> <p>7.9. 0---011111--0--0.</p> <p>7.11. 1-1-0010-01--100.</p> <p>7.13. --1-01-0001-1-1-.</p> <p>7.15. 0-11011--1--0--0.</p> <p>7.17. -1--00001-1--1-1.</p> <p>7.19. --1-1-01010-01--.</p> <p>7.21. --1--1110-0-010-.</p> <p>7.23. 0-01010--1--1--1.</p> <p>7.25. 1-1-0-01--0-1--1.</p> <p>7.27. 1-1----0-010101.</p> <p>7.29. 1--0--101--010-1.</p>	<p>7.2. 1---111100--0--0.</p> <p>7.4. 1---101110--0--0.</p> <p>7.6. 1---111100--0--0.</p> <p>7.8. 0---11100--0--10.</p> <p>7.10. 0-1-1-010-`110---.</p> <p>7.12. -1-1010101--0---.</p> <p>7.14. -1-1-10-00110---.</p> <p>7.16. 1-010-0-01-1---1.</p> <p>7.18. 1-1-10-01010----.</p> <p>7.20. --1-1-010-010-1.</p> <p>7.22. 11-11-1-0-0-0-0-0.</p> <p>7.24. -10-010-0-0-1--1-.</p> <p>7.26. -1---1010-0-01-1.</p> <p>7.28. 010-1-01--01--1-.</p> <p>7.30. -01-10-10-0-1--1.</p>
--	--

**Задача 7.** Найти все тупиковые и все минимальные ДНФ и КНФ для частично определенной функции. Одну из минимальных форм реализовать схемой с элементами  $\&$ ,  $\vee$ ,  $\neg$ .

### *10.3. Алгоритм минимизации частично определенных функций в классе ДНФ*

1. Строим СДНФ функции  $f_1$ .
2. Строим сокращенную ДНФ функции  $f_1$ .
3. С помощью матрицы покрытий конституент единицы функции  $f_0$  простыми импликантами функции  $f_1$  и решеточного выражения строим все тупиковые ДНФ (для некоторых доопределений функции  $f$ ).
4. Среди полученных ТДНФ выбираем простейшие; они являются минимальными ДНФ (для некоторых доопределений функции  $f$ ).

### *10.4. Алгоритм минимизации частично определенных функций в классе КНФ*

Построение минимальных КНФ для частично определенной функции аналогично построению минимальных КНФ для всюду определенной функции.

Алгоритм минимизации частично определенных функций в классе нормальных форм аналогичен алгоритму минимизации в классе нормальных форм для всюду определенных функций.

**Пример.** В классе нормальных форм минимизировать частично определенную функцию  $f(x,y,z,t) = 1---010010-01--1$ .

*Решение.* Минимизация функции  $f$  в классе ДНФ.

1. Строим СДНФ для доопределения нулями  $f_0$  функции  $f$ .  

$$f_0(x,y,z,t) = \bar{x} \bar{y} \bar{z} \bar{t} \vee \bar{x} y \bar{z} t \vee x \bar{y} \bar{z} \bar{t} \vee x y \bar{z} \bar{t} \vee x y z t.$$
2. Строим сокращенную ДНФ для доопределения единицами  $f_1$  функции  $f$  (табл.10.10).

Таблица 10.10

N	$xyzt$	$f$	$f_0$	$f_1$	$\bar{f}$	$h_0$	$h_1$
0	0000	1	1	1	0	0	0
1	0001	-	0	1	-	0	1
2	0010	-	0	1	-	0	1
3	0011	-	0	1	-	0	1
4	0100	0	0	0	1	1	1
5	0101	1	1	1	0	0	0
6	0110	0	0	0	1	1	1
7	0111	0	0	0	1	1	1
8	1000	1	1	1	0	0	0
9	1001	0	0	0	1	1	1
10	1010	-	0	1	-	0	1
11	1011	0	0	0	1	1	1
12	1100	1	1	1	0	0	0
13	1101	-	0	1	-	0	1
14	1110	-	0	1	-	0	1
15	1111	1	1	1	0	0	0

$$\begin{aligned}
 f_1(x,y,z,t) &= (x \vee \bar{y} \vee z \vee t)(x \vee \bar{y} \vee \bar{z} \vee t)(x \vee \bar{y} \vee \bar{z} \vee \bar{t})(\bar{x} \vee y \vee z \vee \bar{t})(\bar{x} \vee \bar{y} \vee \bar{z} \vee \bar{t}) = \\
 &= (x \vee \bar{y} \vee t)(xy \vee \bar{x} \bar{y} \vee \bar{z} \vee \bar{t})(\bar{x} \vee y \vee z \vee \bar{t}) = \\
 &= (x \vee \bar{y} \vee t)(xy \vee \bar{x} \bar{y} \vee \bar{x} \bar{z} \vee y \bar{z} \vee \bar{z} \bar{t} \vee \bar{x} \bar{t} \vee y \bar{t} \vee z \bar{t} \vee \bar{t}) = \\
 &= (x \vee \bar{y} \vee t)(xy \vee \bar{x} \bar{y} \vee \bar{x} \bar{z} \vee y \bar{z} \vee \bar{t}) = \\
 &= xy \vee xy \bar{z} \vee x \bar{t} \vee \bar{x} \bar{y} \vee \bar{x} \bar{y} \bar{z} \vee \bar{y} \bar{t} \vee xyt \vee xy \bar{t} \vee \bar{x} \bar{z} t \vee y \bar{z} t = \\
 &= xy \vee x \bar{t} \vee \bar{y} \bar{t} \vee \bar{x} \bar{y} \vee \bar{x} \bar{z} t \vee y \bar{z} t.
 \end{aligned}$$

3. Строим матрицу покрытий конституент единицы в СДНФ для доопределения нулями  $f_0$  функции  $f$  с помощью построенной сокращенной ДНФ для  $f_1$  (табл.10.11).

4. По табл.10.11 строим решеточный многочлен

$$E = (2 \vee 4)(5 \vee 6)(3 \vee 4)(1 \vee 3)1 = 145 \vee 1235 \vee 146 \vee 1236.$$

Таблица 10.11

N	ПИ	$\bar{x} \bar{y} \bar{z} \bar{t}$	$\bar{x} y \bar{z} t$	$x \bar{y} \bar{z} \bar{t}$	$x y \bar{z} \bar{t}$	$x y \bar{z} t$	$xyzt$
1	$xy$					+	+
2	$\bar{x} \bar{y}$	+					
3	$x \bar{t}$				+	+	
4	$y \bar{t}$	+			+		
5	$\bar{x} \bar{z} t$		+				
6	$y \bar{z} t$		+				

5. Строим все тупиковые ДНФ.

$$g_1 = xy \vee \bar{y} \bar{t} \vee \bar{x} \bar{z} t; \quad g_2 = xy \vee \bar{x} \bar{y} \vee x \bar{t} \vee \bar{x} \bar{z} t;$$

$$g_3 = xy \vee \bar{y} \bar{t} \vee y \bar{z} t; \quad g_4 = xy \vee \bar{x} \bar{y} \vee x \bar{t} \vee y \bar{z} t.$$

6. Из построенных тупиковых ДНФ выбираем минимальные.

$$g_1 = xy \vee \bar{y} \bar{t} \vee \bar{x} \bar{z} t; \quad g_3 = xy \vee \bar{y} \bar{t} \vee y \bar{z} t.$$

Функции  $g_1$  и  $g_3$  есть минимальные доопределения функции  $f$  в классе ДНФ.

Минимизация функции  $f$  в классе КНФ. Для этого проведем минимизацию функции  $\bar{f}$  в классе ДНФ. Пусть  $h_0$  и  $h_1$  есть доопределения нулями и единицами соответственно функции  $\bar{f}$ .

1. Строим СДНФ для доопределения нулями  $h_0$  функции  $\bar{f}$ .

$$h_0(x,y,z,t) = \bar{x} y \bar{z} \bar{t} \vee \bar{x} y z \bar{t} \vee \bar{x} y z t \vee x \bar{y} \bar{z} t \vee x \bar{y} z t.$$

2. Сокращенная ДНФ для

$$\begin{aligned} h_1 &= (x \vee y \vee z \vee t)(x \vee \bar{y} \vee z \vee \bar{t})(\bar{x} \vee y \vee z \vee t)(\bar{x} \vee \bar{y} \vee z \vee t)(\bar{x} \vee \bar{y} \vee \bar{z} \vee \bar{t}) = \\ &= (x \vee z \vee y \bar{t} \vee \bar{y} t)(\bar{x} \vee z \vee t)(\bar{x} \vee \bar{y} \vee \bar{z} \vee \bar{t}) = \\ &= (x \vee z \vee y \bar{t} \vee \bar{y} t)(\bar{x} \vee \bar{y} z \vee z \bar{t} \vee \bar{y} t \vee \bar{z} t) = \\ &= \bar{y} t \vee x \bar{y} z \vee x z \bar{t} \vee x \bar{z} t \vee \bar{x} z \vee \bar{y} z \vee z \bar{t} \vee \bar{x} y \bar{t} \vee y z \bar{t} = \\ &= \bar{y} t \vee \bar{x} z \vee z \bar{t} \vee x \bar{z} t \vee \bar{x} y \bar{t} \vee \bar{y} z. \end{aligned}$$

3. Матрица покрытий конституент единицы в СДНФ для  $h_0$  с помощью простых импликант в сокращенной ДНФ для  $h_1$  приведена в табл.10.12.

Таблица 10.12

N	ПИ	$\bar{x} y \bar{z} \bar{t}$	$\bar{x} y z \bar{t}$	$\bar{x} y z t$	$x \bar{y} \bar{z} t$	$x \bar{y} z t$
1	$\bar{y} t$				+	+
2	$\bar{x} z$		+	+		
3	$z \bar{t}$		+			
4	$x z \bar{t}$				+	
5	$\bar{x} y \bar{t}$	+	+			
6	$\bar{y} z$					+

4. Решеточное выражение  $E = 5(2 \vee 3 \vee 5)2(1 \vee 4)(1 \vee 6) = 25(1 \vee 46) = 125 \vee 2456$ .

5. Строим две тупиковые ДНФ.

$$g_5 = \bar{y} t \vee \bar{x} z \vee \bar{x} y \bar{t}, \quad g_6 = \bar{x} z \vee x \bar{z} t \vee \bar{x} y \bar{t} \vee \bar{y} z.$$

Минимальная ДНФ  $g_5 = \bar{y} t \vee \bar{x} z \vee \bar{x} y \bar{t}$ .

6. Функция  $\bar{g}_5 = (y \vee \bar{t})(x \vee \bar{z})(x \vee \bar{y} \vee t)$  есть минимальное доопределение функции  $f$  в классе КНФ.

Найденные МДНФ  $g_1$ ,  $g_3$  и МКНФ  $\bar{g}_5$  являются минимальными доопределениями функции  $f$  в классе нормальных форм.

**Задача 8.** Минимизировать всюду определенную функцию алгебры логики из задачи 6 и частично определенную функцию из задачи 7 с помощью карт Карно.

**Задача 9.** Построить минимальную ДНФ системы функций  $f_1(x_1, x_2, x_3)$ ,  $f_2(x_1, x_2, x_3)$ ,  $f_3(x_1, x_2, x_3)$  и реализовать ее с помощью ПЛМ.

Каждая функция задана множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

- |   |   |
|---|---|
| <b>9.1.</b> {2,3,4,5,7}; {0,4,5}; {3,4,5,7}.    | <b>9.2.</b> {1,3,4,6,7}; {0,4,6}; {3,4,5,7}.  |
| <b>9.3.</b> {2,3,4,5,7}; {0,2,6}; {2,3,5,7}.    | <b>9.4.</b> {1,3,4,6,7}; {0,1,3}; {1,3,6,7}.  |
| <b>9.5.</b> {1,2,5,6,7}; {0,1,5}; {1,5,6,7}.    | <b>9.6.</b> {1,2,5,6,7}; {0,2,5}; {2,5,6,7}.  |
| <b>9.7.</b> {1,3,5,7}; {1,2,3}; {4,5,7}.        | <b>9.8.</b> {2,3,6,7}; {1,2,3}; {4,6,7}.      |
| <b>9.9.</b> {1,3,5,7}; {1,4,5}; {2,3,7}.        | <b>9.10.</b> {2,3,6,7}; {2,4,6}; {1,3,7}.     |
| <b>9.11.</b> {4,5,6,7}; {2,4,6}; {1,5,7}.       | <b>9.12.</b> {4,5,6,7}; {1,4,5}; {1,6,7}.     |
| <b>9.13.</b> {3,4,5,7}; {4,5,6}; {1,2,3}.       | <b>9.14.</b> {3,4,6,7}; {4,5,6}; {1,2,3}.     |
| <b>9.15.</b> {2,3,5,7}; {2,3,6}; {1,4,5}.       | <b>9.16.</b> {1,3,6,7}; {1,3,5}; {2,4,6}.     |
| <b>9.17.</b> {1,5,6,7}; {1,3,5}; {2,4,6}.       | <b>9.18.</b> {2,5,6,7}; {2,3,6}; {1,4,5}.     |
| <b>9.19.</b> {0,2,4}; {0,2,3}; {1,2,3}.         | <b>9.20.</b> {0,1,4}; {0,1,3}; {1,2,3}.       |
| <b>9.21.</b> {0,2,4}; {0,4,5}; {1,4,5}.         | <b>9.22.</b> {0,1,4}; {0,4,6}; {2,4,6}.       |
| <b>9.23.</b> {0,1,2}; {0,2,6}; {2,4,6}.         | <b>9.24.</b> {0,1,2}; {0,1,5}; {1,4,5}.       |
| <b>9.25.</b> {0,2,6,7}; {0,1,6}; {0,2,7}.       | <b>9.26.</b> {0,2,6,7}; {2,5,7}; {1,3,7}.     |
| <b>9.27.</b> {0,1,4,6,7}; {3,4,5,6,7}; {4,5,7}. | <b>9.28.</b> {0,1,2,3,5,7}; {4,5,7}; {0,1,3}. |
| <b>9.29.</b> {0,1,2}; {0,1,4,7}; {6,7}.         | <b>9.30.</b> {4,5,7}; {0,3,4,5,7}; {2,3,6}.   |

**Задача 9.** Построить минимальную ДНФ системы функций  $f_1(x_1, x_2, x_3)$ ,  $f_2(x_1, x_2, x_3)$ ,  $f_3(x_1, x_2, x_3)$  и реализовать ее с помощью программируемой логической матрицы (ПЛМ).

Каждая функция задана множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

### 10.5. Алгоритм совместной минимизации

1. Построить все возможные конъюнкции функций  $f_1, f_2, f_3$ , а именно,  $f_1 \& f_2$ ,  $f_1 \& f_3$ ,  $f_2 \& f_3$ ,  $f_1 \& f_2 \& f_3$ .
2. Для каждой  $f_i$  и для каждой из этих конъюнкций найти максимальные интервалы (сокращенную ДНФ).
3. Для каждой из функций  $f_1, f_2, f_3$  построить таблицу, в которой строкам сопоставляются те интервалы, полученные в пункте 2, которые принадлежат множеству  $M_1$  соответствующей функции, а столбцам наборы множества  $M_1$  этой функции.
4. Найти минимальное общее покрытие этих таблиц, т.е. при нахождении покрытия надо взять конъюнкцию логических выражений покрытия каждой отдельной таблицы.
5. Полученное покрытие дает минимальную ДНФ заданной системы функций.
6. Покрыть каждую функцию отдельно интервалами полученного минимального покрытия системы.

**Пример.** Провести совместную минимизацию функций

$$f_1 = 01110101, f_2 = 10100111, f_3 = 01101101.$$

*Решение.* 1. Строим все возможные конъюнкции:  $f_1 \& f_2 = 00100101$ ,  $f_1 \& f_3 = 01100101$ ,  $f_2 \& f_3 = 00100101$ ,  $f_1 \& f_2 \& f_3 = 0100101$  (табл.10.13).

Таблица 10.13

n	xyz	$f_1$	$f_2$	$f_3$	$f_1 \& f_2$	$f_1 \& f_3$	$f_2 \& f_3$	$f_1 \& f_2 \& f_3$
0	000	0	1	0	0	0	0	0
1	001	1	0	1	0	1	0	0
2	010	1	1	1	1	1	1	1
3	011	1	0	0	0	0	0	0
4	100	0	0	1	0	0	0	0
5	101	1	1	1	1	1	1	1
6	110	0	1	0	0	0	0	0
7	111	1	1	1	1	1	1	1

2. Заметим, что  $f_1 \& f_2 = f_2 \& f_3 = f_1 \& f_2 \& f_3 = 00100101$ .

Для функций  $f_1, f_2, f_3, f_1 \& f_2, f_1 \& f_3, f_2 \& f_3, f_1 \& f_2 \& f_3$  строим максимальные интервалы (сокращенные ДНФ) (табл.10.14).

Таблица 10.14

Функция	Сокращенная ДНФ	Простые импликанты
$f_1 =$	$z \vee \bar{x}y$	$n_1 = **1, n_2 = 01*$
$f_2 =$	$xz \vee xy \vee y\bar{z} \vee \bar{x}\bar{z}$	$n_3 = 1*1, n_4 = 11*, n_5 = *10, n_6 = 0*0$
$f_3 =$	$xz \vee \bar{y}z \vee x\bar{y} \vee \bar{x}y\bar{z}$	$n_3 = 1*1, n_7 = *01, n_8 = 10*, n_9 = 010$
$f_1 \& f_2 =$	$xz \vee \bar{x}y\bar{z}$	$n_3 = 1*1, n_9 = 010$
$f_1 \& f_3 =$	$xz \vee \bar{y}z \vee \bar{x}y\bar{z}$	$n_3 = 1*1, n_7 = *01, n_9 = 010$
$f_2 \& f_3 =$	$xz \vee \bar{x}y\bar{z}$	$n_3 = 1*1, n_9 = 010$
$f_1 \& f_2 \& f_3 =$	$xz \vee \bar{x}y\bar{z}$	$n_3 = 1*1, n_9 = 010$

$$n_1 = z, n_2 = \bar{x}y, n_3 = xz, n_4 = xy, n_5 = y\bar{z}, n_6 = \bar{x}\bar{z}, n_7 = \bar{y}z, n_8 = x\bar{y}, n_9 = \bar{x}y\bar{z}.$$

3. Составляем список всех максимальных интервалов, участвующих в построении функций. Например, для  $f_1$  собираем максимальные интервалы функций  $f_1, f_1 f_2, f_1 f_3, f_1 f_2 f_3$ .

$$f_1: n_1, n_2, n_3, n_7, n_9,$$

$$f_2: n_3, n_4, n_5, n_6, n_9,$$

$$f_3: n_3, n_7, n_8, n_9,$$

4. Таблица покрытий для  $f_1, f_2, f_3$  (табл.10.15, 10.16, 10.17).

Таблица 10.15

СДНФ для  $f_1$

$f_1$	001	010	011	101	111
$n_1=**1$	+	+	+	+	+
$n_2=01*$		+	+		
$n_3=1*1$				+	+
$n_7=*01$	+			+	
$n_9=010$		+			

Решеточное выражение

$$E_1 = (n_1 \vee n_7)(n_2 \vee n_9)(n_1 \vee n_2)(n_1 \vee n_3 \vee n_7)(n_1 \vee n_3) = n_1 n_2 \vee n_1 n_9 \vee n_2 n_3 n_7.$$

Максимальные интервалы и тупиковые ДНФ для  $f_1$ .

$$\begin{aligned} n_1 n_2, \quad f_1 &= z \vee \bar{x} y, \\ n_1 n_9, \quad f_1 &= z \vee \bar{x} y \bar{z}, \\ n_2 n_3 n_7, \quad f_1 &= \bar{x} y \vee x z \vee \bar{y} z. \end{aligned}$$

5. Таблица покрытий для  $f_2$  (табл.10.16).

Таблица 10.16  
СДНФ для  $f_2$

$f_2$	000	010	101	110	111
$n_3=1*1$		+	+		
$n_4=11*$			+	+	
$n_5=*10$	+		+		
$n_6=0*0$	+	+			
$n_9=010$		+			

Решеточное выражение

$$E_2 = n_6(n_5 \vee n_6 \vee n_9) n_3 (n_4 \vee n_5)(n_3 \vee n_4) = n_3 n_4 n_6 \vee n_3 n_5 n_6.$$

Максимальные интервалы и тупиковые ДНФ для  $f_2$ .

$$\begin{aligned} n_3 n_4 n_6, \quad f_2 &= x z \vee x y \vee \bar{x} \bar{z}, \\ n_3 n_5 n_6, \quad f_2 &= x z \vee y \bar{z} \vee \bar{x} \bar{z}. \end{aligned}$$

6. Таблица покрытий для  $f_3$  (табл.10.17).

Таблица 10.17  
СДНФ для  $f_3$

$f_3$	001	010	100	101	111
$n_3=1*1$			+	+	
$n_7=*01$	+		+		
$n_8=10*$			+	+	
$n_9=010$		+			

Решеточное выражение

$$E_3 = n_7 n_9 n_8 (n_3 \vee n_7 \vee n_8) n_3 = n_3 n_7 n_8 n_9.$$

Максимальные интервалы и тупиковые ДНФ для  $f_3$ .

$$n_3 n_7 n_8 n_9, \quad f_3 = x z \vee \bar{y} z \vee x \bar{y} \vee \bar{x} y \bar{z}.$$

7. Решеточное выражение  $E_1 \& E_2 \& E_3 =$

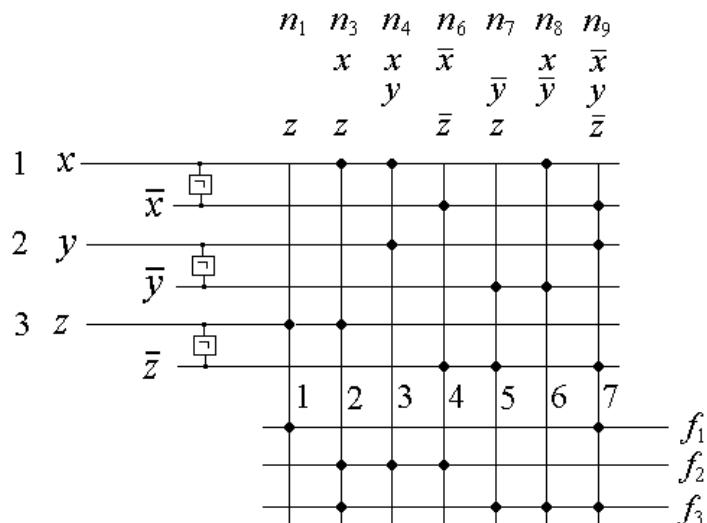
$$\begin{aligned}
 & [(n_1 \vee n_7)(n_2 \vee n_9)(n_1 \vee n_2)(n_1 \vee n_3 \vee n_7)(n_1 \vee n_3)] \text{ для } f_1 \\
 & [n_6(n_5 \vee n_6 \vee n_9)n_3(n_4 \vee n_5)(n_5 \vee n_4)] \text{ для } f_2 \\
 & [n_7n_9n_8(n_3 \vee n_7 \vee n_8)n_3] = \text{ для } f_3 \\
 & n_1\ n_3\ n_4\ n_6\ n_7\ n_8\ n_9 \vee n_1\ n_3\ n_5\ n_6\ n_7\ n_8\ n_9 \vee n_2\ n_3\ n_4\ n_6\ n_7\ n_8\ n_9 \vee \\
 & n_2\ n_3\ n_5\ n_6\ n_7\ n_8\ n_9.
 \end{aligned}$$

Все дизъюнктивные слагаемые содержат по 7 сомножителей. Для дальнейшего выбираем любое, например, первое:  $n_1 n_3 n_4 n_6 n_7 n_8 n_9$ .

8. Функции  $f_1, f_2, f_3$  реализуем следующими максимальными интервалами и соответствующими тупиковыми ДНФ. Максимальные интервалы должны содержаться среди  $n_1, n_3, n_4, n_6, n_7, n_8, n_9$ .

$$\begin{aligned} f_1 &: n_1 n_9, & f_1 &= z \vee \bar{x} y \bar{z}, \\ f_2 &: n_3 n_4 n_6, & f_2 &= xz \vee xy \vee \bar{x} \bar{z}, \\ f_3 &: n_3 n_7 n_8 n_9, & f_3 &= xz \vee \bar{y} z \vee x \bar{y} \vee \bar{x} y \bar{z}. \end{aligned}$$

9. ПЛМ (ширины 7), совместно реализующая функции  $f_1$ ,  $f_2$ ,  $f_3$  имеет следующий вид.



Построенная ПЛМ имеет тип  $(3,7,3)$ , т.е. 3 переменных, ширина 7, функций 3.

**Задача 10.** Провести приближенную совместную минимизацию трех функций алгебры логики. В качестве заданий взять из задачи 5 две последние функции и функцию своего варианта из задачи 6. Результат минимизации реализовать с помощью программируемых логических матриц (ПЛМ). Минимизацию проводить с помощью карт Карно. Минимизировать каждую функцию в отдельности (с помощью карт Карно) и результат из трех функций реализовать на ПЛМ. Сравнить две реализации и указать, какая из них экономнее.

## *Алгоритм совместной минимизации системы из k функций (жадный алгоритм приближенной минимизации)*

1. Найти все простые импликанты функции  $f_1 \& f_2 \& \dots \& f_k$ . Выбрать минимальное покрытие ее единиц простыми импликантами. Перевести

область общих единиц в область неопределенности для каждой из данных функций.

2. Применять пункт 1, пока это возможно, по всем возможным произведениям  $f_{i_1} \& f_{i_2} \& \dots \& f_{i_t}$ , где  $\{i_1, i_2, \dots, i_t\} \subseteq \{1, 2, \dots, k\}$ ,  $t = k-1, \dots, 3, 2, 1$ .

**Пример.**  $f_1 = 0011 0101 1111 0101$ ,  $f_2 = 0011 0111 0011 0011$ ,

$f_3 = 0000 0011 1100 0111$ .

*Решение.* Для функций  $f_1$ ,  $f_2$ ,  $f_3$  заполняем карты Карно (рис.10.3).

	$\bar{z} \quad z$ $\underbrace{\quad}_{\bar{x}} \quad \underbrace{\quad}_{x}$		
	$z \ t \ z \ t \ z \ t \ z \ t$ 00 01 11 10		
$\bar{x}$	$x \ y$ $\left\{ \begin{array}{l} 0 \ 0 \\ 0 \ 1 \\ 1 \ 1 \\ 1 \ 0 \end{array} \right.$	$\bar{y}$	$0 \ 0 \ 1 \ 1$ $0 \ 1 \ 1 \ 1$ $0 \ 0 \ 1 \ 1$ $0 \ 0 \ 1 \ 1$
$x$	$\boxed{\begin{array}{ c c c c } \hline x & y & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 & 1 & 1 \\ \hline \end{array}}$	$y$	$0 \ 0 \ 0 \ 0$ $0 \ 0 \ 1 \ 1$ $0 \ 1 \ 1 \ 1$ $1 \ 1 \ 0 \ 0$
	$\bar{t} \quad \underbrace{t}_{\bar{t}} \quad \bar{t}$		
	$f_1(x,y,z,t)$	$f_2(x,y,z,t)$	$f_3(x,y,z,t)$

Рис.10.3

Строим функцию  $f_1 \& f_2 \& f_3$  и находим ее карту Карно (рис.10.4).

	$\bar{z} \quad z$ $\underbrace{\quad}_{\bar{x}} \quad \underbrace{\quad}_{x}$		
	$z \ t \ z \ t \ z \ t \ z \ t$ 00 01 11 10		
$\bar{x}$	$x \ y$ $\left\{ \begin{array}{l} 0 \ 0 \\ 0 \ 1 \\ 1 \ 1 \\ 1 \ 0 \end{array} \right.$	$\bar{y}$	$0 \ 0 \ 0 \ 0$ $0 \ 0 \ 1 \ 0$ $0 \ 0 \ 1 \ 0$ $0 \ 0 \ 0 \ 0$
$x$	$\boxed{\begin{array}{ c c c c } \hline x & y & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}}$	$y$	$0 \ 0 \ 0 \ 0$ $0 \ 0 \ 1 \ 0$ $0 \ 0 \ 1 \ 0$ $0 \ 0 \ 0 \ 0$
	$\bar{t} \quad \underbrace{t}_{\bar{t}} \quad \bar{t}$		

Рис.10.4

Две единицы функции  $f_1 \& f_2 \& f_3$  покрывает ДНФ  $d_{f_1 f_2 f_3} = yzt$ .

Переводим единицы функции  $f_1 \& f_2 \& f_3$  в область неопределенности (она обозначается знаком «-») функций  $f_1$ ,  $f_2$ ,  $f_3$  и получаем функции  $f_1^{(1)}$ ,  $f_2^{(1)}$ ,  $f_3^{(1)}$ , задаваемыми следующими (рис.10.5) картами Карно.

	$\bar{z}$	$z$	
	$z t$	$z t$	$z t$
	00	01	11
	10		
$\bar{x}$	$x y$		
00	0 0 1 1	$\bar{y}$	0 0 1 1
01	0 1 — 0	$y$	0 1 — 1
11	0 1 — 0		0 0 — 1
10	1 1 1 1	$\bar{y}$	0 0 1 1
	$\bar{t}$	$t$	$\bar{t}$
		$f_1^{(1)}$	$f_2^{(1)}$
			$f_3^{(1)}$

Рис.10.5

Конъюнкция значений функций проводится в соответствии с операцией  $\&$ , определяемой следующей таблицей (рис.10.6а).

$\&$	0	1	—
0	0	0	0
1	0	1	1
—	0	1	—

Рис.10.6 а

Строим функцию  $f_1^{(1)} \& f_2^{(1)}$  и находим ее карту Карно (рис.10.6б)

Единицы функции  $f_1^{(1)} \& f_2^{(1)}$  покрывает ДНФ  $d_{f_1^{(1)} f_2^{(1)}} = \bar{y} z \vee \bar{x} yt$ .

Переводим единицы функции  $f_1^{(1)} \& f_2^{(1)}$  в область неопределенности функций  $f_1^{(1)}, f_2^{(1)}$  и получаем функции  $f_1^{(2)}, f_2^{(2)}, f_3^{(2)}$ , ( $f_3^{(2)} = f_3^{(1)}$ ), задаваемыми следующими (рис.10.7) картами Карно.

	$\bar{z}$	$z$	
	$z t$	$z t$	$z t$
	00	01	11
	10		
$\bar{x}$	$x y$		
00	0 0 — —	$\bar{y}$	0 0 — —
01	0 — — 0	$y$	0 — — 1
11	0 1 — 0		0 0 — 1
10	1 1 — —	$\bar{y}$	0 0 — —
	$\bar{t}$	$t$	$\bar{t}$

$f_1^{(2)}$  $f_2^{(2)}$  $f_3^{(2)}$ 

Рис.10.7

Строим функцию  $f_1^{(2)} \& f_3^{(2)}$  и находим ее карту Карно (рис.10.8).

		$\bar{z}$		$z$	
		$z t$	$z t$	$z t$	$z t$
		0 0	0 1	1 1	1 0
$\bar{x}$	0 0	0	0	0	0
	0 1	0	0	—	0
	1 1	0	1	—	0
	1 0	1	1	0	0

Рис.10.8

Единицы функции  $f_1^{(2)} \& f_3^{(2)}$  покрывают ДНФ  $d_{f_1^{(2)} f_3^{(2)}} = x \bar{z} t \vee x \bar{y} \bar{z}$ .

Переводим единицы функции  $f_1^{(2)} \& f_3^{(2)}$  в область неопределенности функций  $f_1^{(2)}, f_3^{(2)}$  и получаем функции  $f_1^{(3)}, f_2^{(3)}, f_3^{(3)}$ , ( $f_2^{(3)} = f_2^{(2)}$ ), задаваемыми следующими (рис.10.9) картами Карно.

		$\bar{z}$		$z$	
		$z t$	$z t$	$z t$	$z t$
		0 0	0 1	1 1	1 0
$\bar{x}$	0 0	0	0	—	—
	0 1	0	—	—	0
	1 1	0	—	—	0
	1 0	—	—	—	—

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

		$\bar{t}$		$t$		$\bar{t}$	
		$t$	$t$	$t$	$t$	$t$	$t$
		0	0	0	0	0	0
$\bar{y}$	0 0	0	0	—	—	—	—
	0 1	0	—	—	0	—	—
	1 1	0	—	—	0	—	—
	1 0	—	—	—	—	—	—

$f_1^{(3)}$

$f_2^{(3)}$

$f_3^{(3)}$

Рис.10.9

Строим функцию  $f_2^{(3)} \& f_3^{(3)}$  и находим ее карту Карно (рис.10.10).

		$\bar{z}$		$z$	
		$z t$	$z t$	$z t$	$z t$
		00	01	11	10
$\bar{x}$	$x$	$y$			
		0 0	0 0 0 0		$\bar{y}$
		0 1	0 0 — 1		$y$
		1 1	0 0 — 1		$y$
		1 0	0 0 0 0		$\bar{y}$
			$t$	$t$	$t$

Рис.10.10

Единицы функции  $f_2^{(3)}$  &  $f_3^{(3)}$  покрывает ДНФ  $d_{f_2^{(3)} f_3^{(3)}} = yz$ .

Переводим единицы функции  $f_2^{(3)}$  &  $f_3^{(3)}$  в область неопределенности функций  $f_2^{(3)}, f_3^{(3)}$  и получаем функции  $f_1^{(4)}, f_2^{(4)}, f_3^{(4)}$ , ( $f_1^{(4)} = f_1^{(3)}$ ), задаваемыми следующими (рис.10.11) картами Карно.

		$\bar{z}$		$z$	
		$z t$	$z t$	$z t$	$z t$
		00	01	11	10
$\bar{x}$	$x$	$y$			
		0 0	0 0 — —		$\bar{y}$
		0 1	0 — — 0		$y$
		1 1	0 — — 0		$y$
		1 0	— — — —		$\bar{y}$
			$t$	$t$	$t$

$f_1^{(4)}$	$f_2^{(4)}$	$f_3^{(4)}$

Рис.10.11

Единицы исчерпаны. Строим ДНФ-представления функций  $f_1, f_2, f_3$ .

$$d_{f_1 f_2 f_3} = yzt, d_{f_1^{(1)} f_2^{(1)}} = \bar{y}z \vee \bar{x}yt, d_{f_1^{(2)} f_3^{(2)}} = x\bar{z}t \vee x\bar{y}\bar{z}, d_{f_2^{(3)} f_3^{(3)}} = yz.$$

Для  $f_i$  собираем те  $d$ , в индексе которых есть  $f_i$  и  $f_i$  со штрихами,  $i = 1,2,3$ .

$$f_1(x,y,z,t) = d_{f_1 f_2 f_3} \vee d_{f_1^{(1)} f_2^{(1)}} \vee d_{f_1^{(2)} f_3^{(2)}},$$

$$f_2(x,y,z,t) = d_{f_1 f_2 f_3} \vee d_{f_1^{(1)} f_2^{(1)}} \vee d_{f_2^{(3)} f_3^{(3)}},$$

$$f_3(x,y,z,t) = d_{f_1 f_2 f_3} \vee d_{f_1^{(2)} f_3^{(2)}} \vee d_{f_2^{(3)} f_3^{(3)}},$$

откуда

$$f_1(x,y,z,t) = yzt \vee \bar{y}z \vee \bar{x}yt \vee x\bar{z}t \vee x\bar{y}\bar{z},$$

$$f_2(x,y,z,t) = yzt \vee \bar{y}z \vee \bar{x}yt \vee \dots yz.$$

$$f_3(x,y,z,t) = yzt \vee x\bar{z}t \vee x\bar{y}\bar{z} \vee yz.$$

Программируемая логическая матрица (ПЛМ), реализующая совместно функции  $f_1, f_2, f_3$  строится с использованием элементарных конъюнкций  $yzt, \bar{y}z, \bar{x}yt, x\bar{z}t, x\bar{y}\bar{z}, yz$  (рис.10.12).

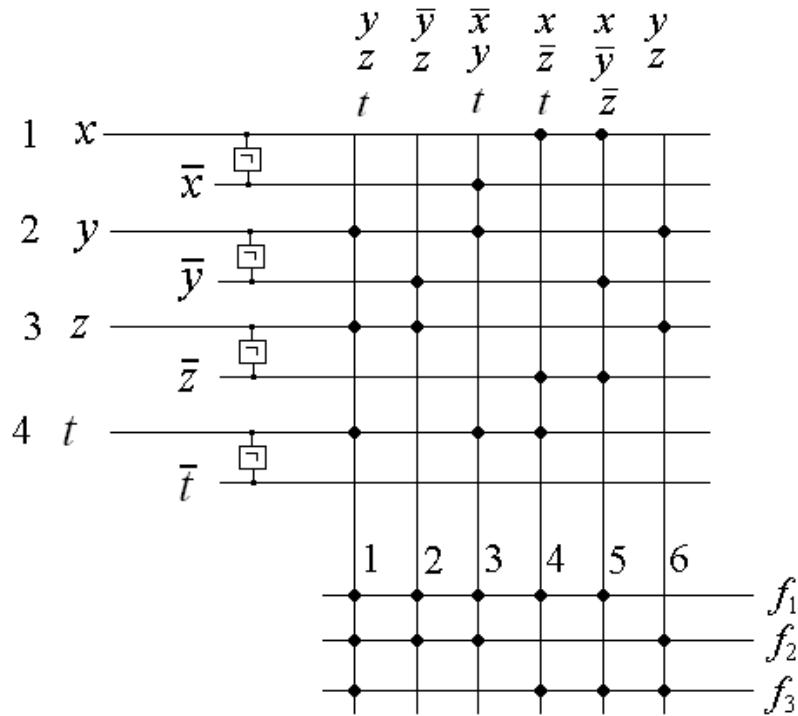


Рис.10.12

ПЛМ имеет размер  $(4,6,3)$ , где 4 есть местность функций, 6 есть ширина ПЛМ, 3 есть число реализуемых функций.

**Замечание.** Возможна совместная минимизация нескольких частично определенных функций. Конъюнкция значений функций проводится в соответствии с операцией  $\&$ , определяемой следующей таблицей.

$\&$	0	1	-
0	0	0	0
1	0	1	1
-	0	1	-

**Задача 11.** Заданную систему булевых функций исследовать на полноту с помощью теоремы Поста.

- |  |   |
|--|---|
| <b>11.1.</b> $(x \equiv y) + yz$ , $x \& \neg y$ .                                 | <b>11.2.</b> $(x \rightarrow y) + (x \vee z)$ , 0, 1.                           |
| <b>11.3.</b> $x \equiv (y + z)$ , $\neg(x \rightarrow y) \equiv z$ .               | <b>11.4.</b> $(x + yz) \& \neg x \rightarrow z$ , $xy$ .                        |
| <b>11.5.</b> $(x \equiv \neg y) \rightarrow (\neg x \equiv z)$ , $x \vee \neg y$ . | <b>11.6.</b> $(x \equiv \neg y) + xz$ , $xy$ .                                  |
| <b>11.7.</b> $x + \neg(y \equiv z)$ , $\neg x \equiv y$ .                          | <b>11.8.</b> $\neg x \equiv (y + z)$ , $xy$ .                                   |
| <b>11.9.</b> $(x \rightarrow z)   y$ , $\neg x \vee yz$ .                          | <b>11.10.</b> $(x \equiv y) \rightarrow (x \not\equiv z)$ , 0.                  |
| <b>11.11.</b> $(x \equiv y) \rightarrow \neg z$ , $x \vee \neg y$ .                | <b>11.12.</b> $(x z) + y$ , $x \equiv y \& \neg z$ .                            |
| <b>11.13.</b> $(x \rightarrow y) + (y \rightarrow z)$ , $\neg x \& y$ .            | <b>11.14.</b> $(x \rightarrow y)   (y \rightarrow z)$ , $x + y$ .               |
| <b>11.15.</b> $(x+y) + (y \equiv \neg z)$ , $\neg x \rightarrow y$ .               | <b>11.16.</b> $x \equiv (y + \neg z)$ , $x$ .                                   |
| <b>11.17.</b> $\neg x \rightarrow y$ , 00, 11.                                     | <b>11.18.</b> $(x \rightarrow y) + \neg z$ , $x \vee \neg y$ .                  |
| <b>11.19.</b> $(x \rightarrow y) \vee \neg z$ , $x \& \neg y$ .                    | <b>11.20.</b> $(\neg x \equiv \neg y)   z$ , $\neg x \equiv y$ .                |
| <b>11.21.</b> $(x \vee \neg y) \equiv z$ , $(x \rightarrow y) \rightarrow y$ .     | <b>11.22.</b> $x   z \rightarrow y$ , $x \equiv y$ , 00.                        |
| <b>11.23.</b> $(x   y) \equiv (y   z)$ , 00, 11.                                   | <b>11.24.</b> $(x \rightarrow \neg(yz)) \vee z$ , $\neg x \rightarrow \neg y$ . |
| <b>11.25.</b> $(x \equiv \neg y) \rightarrow z$ , $x \& \neg y$ .                  | <b>11.26.</b> $(\neg x \vee \neg yz) + z$ , $x \rightarrow y$ .                 |
| <b>11.27.</b> $(x + y \& \neg z) \rightarrow z$ , $\neg x \& y$ .                  | <b>11.28.</b> $x \vee \neg y \& z$ , $\neg x \rightarrow y$ .                   |
| <b>11.29.</b> $(x \rightarrow yz) \vee \neg z$ , $\neg x \vee yz$ .                | <b>11.30.</b> $(x \vee \neg y) \equiv z$ , $\neg x \rightarrow y$ .             |

**Задача 11.** Заданную систему булевых функций исследовать на полноту с помощью теоремы Поста.

**Теорема** (Е.Пост). Чтобы система функций из  $P_2$  была функционально полной (в  $P_2$ ), необходимо и достаточно, чтобы эта система содержала:

- 1) функцию, не сохраняющую 0;
- 2) функцию, не сохраняющую 1;
- 3) несамодвойственную функцию;
- 4) немонотонную функцию;
- 5) нелинейную функцию.

**Определение.** Двойственной для функции  $f(x_1, \dots, x_n)$  называется функция  $f^*(x_1, \dots, x_n) = \bar{f}(\bar{x}_1, \dots, \bar{x}_n)$ .

**Определение.** Функция, совпадающая со своей двойственной, называется самодвойственной.

**Критерий самодвойственности.** Функция самодвойственна, если и только если на всяких двух противоположных наборах она принимает различные значения.

Полином Жегалкина в поле  $F$  есть выражение

$$\sum_{(i_1, \dots, i_n) \in E_2^n} a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad \text{где } x^i = \begin{cases} x, & \text{если } i=1, \\ 1, & \text{если } i=0, \end{cases}$$

а каждый коэффициент  $a_{i_1, i_2, \dots, i_n}$  равен 0 или 1.

**Пример.** Многочлен Жегалкина для функции  $f(x, y, z) = (\bar{x} \vee \bar{y} \vee \bar{z})$ .

$$f(x, y, z) = \bar{x} \bar{y} z \vee \bar{x} yz \vee x \bar{y} z \vee xy \bar{z} \vee xyz = (x+1)(y+1)z + (x+1)yz + x(y+1)z + xy(z+1) + xyz = xyz + xz + yz + z + xyz + yz + xyz + xz + xyz + xy + xyz = xyz + xy + z.$$

Тогда  $g(x, y, z) = 1 + z + y + xz + xy + xyz$ .

**Определение.** Функция  $f(x_1, \dots, x_n)$  называется *линейной*, если многочлен Жегалкина для нее имеет линейный относительно переменных вид:

$$f(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n + a_{n+1}, \text{ где каждое } a_i \text{ равно } 0 \text{ или } 1.$$

**Определение.** Функция  $f(x_1, \dots, x_n)$  называется *монотонной*, если для всяких наборов  $a = (a_1, \dots, a_n)$ ,  $b = (b_1, \dots, b_n)$  условие  $a \leq b$  влечет  $f(a) \leq f(b)$ .

**Критерий монотонности.** Функция монотонна, если и только если ее сокращенная ДНФ не содержит отрицаний.

**Определение.** Функция  $f(x_1, \dots, x_n)$  сохраняет константу  $a \in \{0,1\}$ , если  $f(a, \dots, a) = a$ .

### Примеры.

1.  $F = \{1, x*y\}$ , где  $x*y = 0010$ .

Проверяем условия полноты.

1) константа 1 не сохраняет 0;

2)  $x * y$  не сохраняет 1;

3)  $x * y$  не самодвойственна, ибо  $0*0 = 1*1$ ;

4)  $x * y$  не монотонна, ибо  $(1,0) \leq (1,1)$ , но  $1*0 > 1*1$ ;

5)  $x * y$  не линейна, ибо  $x * y = \bar{x}y = xy + y$ .

Следовательно, система  $F$  по теореме Поста полна. Отрицание есть  $1*x$ . Конъюнкция  $x&y = \bar{x} * y$ .

2.  $F = \{0, 1, \bar{x}, m(x,y,z)\}$ , где функция  $m(x,y,z) = 00010111$  равна единице на тех и только тех наборах, в которых число единиц больше числа нулей.

Проверяем условия полноты:

1) 0 не сохраняет 1;

2) 1 не сохраняет 0;

3) константа 1 не самодвойственна;

4) отрицание не монотонно;

5) функция  $m(x,y,z) = xyz + xy + xz + yz$  не линейна.

По теореме Поста система  $F$  полна. Конъюнкция  $x&y = m(x,y,0)$ .

Заметим, что система  $F$  избыточно полна. Ее подсистемы  $\{1, \bar{x}, m(x,y,z)\}$  и  $\{0, \bar{x}, m(x,y,z)\}$  являются функционально полными системами.

**Задача 12.** Заданную систему булевых функций исследовать на полноту с помощью теоремы Поста.

**12.1.** 10110111, 01010100, 00100111.

**12.2.** 00110100, 11010101, 0111.

**12.3.** 01010101, 0111, 00, 01010001.

**12.4.** 11101110, 1100.

**12.5.** 11101000, 1010, 00.

**12.6.** 10110001, 0001, 0000.

**12.7.** 10110001, 0011, 00.

**12.8.** 10110001, 0010.

**12.9.** 01001100, 1001.

**12.10.** 00101011, 1100, 11.

**12.11.** 10101011, 1100, 11.

**12.12.** 10010010, 0010, 11.

**12.13.** 01011000, 0101, 11.

**12.14.** 01101110, 0000, 11.

**12.15.** 00011111, 1011, 00.

**12.16.** 01101101, 0001, 11, 00.

**12.17.** 10111000, 1011.

**12.18.** 00111101, 1111, 00.

- |                                       |                                     |
|---------------------------------------|-------------------------------------|
| <b>12.19.</b> 01101101, 1001, 00.     | <b>12.20.</b> 00110011, 0101, 0011. |
| <b>12.21.</b> 1011001, 1000, 00.      | <b>12.22.</b> 10110001, 1001, 01.   |
| <b>12.23.</b> 11000111, 00011111, 00. | <b>12.24.</b> 10100011, 0110.       |
| <b>12.25.</b> 10100011, 1001, 00.     | <b>12.26.</b> 01001101, 1001, 00.   |
| <b>12.27.</b> 00110111, 1111, 00.     | <b>12.28.</b> 00101001, 1101, 01.   |
| <b>12.29.</b> 01001011, 0001, 11.     | <b>12.30.</b> 00001010, 1010, 11.   |

**Задача 13.** Реализовать функции из задач 5 и 6 с помощью мультиплексора (в базисе  $\&$ ,  $\vee$ ,  $\neg$ , MUX(2)).

**Определение.** Мультиплексор MUX есть большая интегральная схема (БИС)  $M(n)$ , имеющая  $n$  управляющих входов,  $2^n$  информационных входов и один выход. Для поданного на управляющие входы набора  $(c_1, \dots, c_n)$  из 0 и 1 схема делает проходимым (отпирает) и пропускает сигнал единственного информационного входа, помеченного набором  $(c_1, \dots, c_n)$ ; остальные информационные входы заперты и к выходу не проходимы (рис.10.13).



Рис.10.13

**Пример.** Реализовать функцию трех переменных  $f(x,y,z) = 00101101$  с помощью мультиплексора  $M(2)$ .

В задаче используется разложение Шеннона функции по переменным  $x, y$ . Требуемая реализация приведена на рис.10.14.

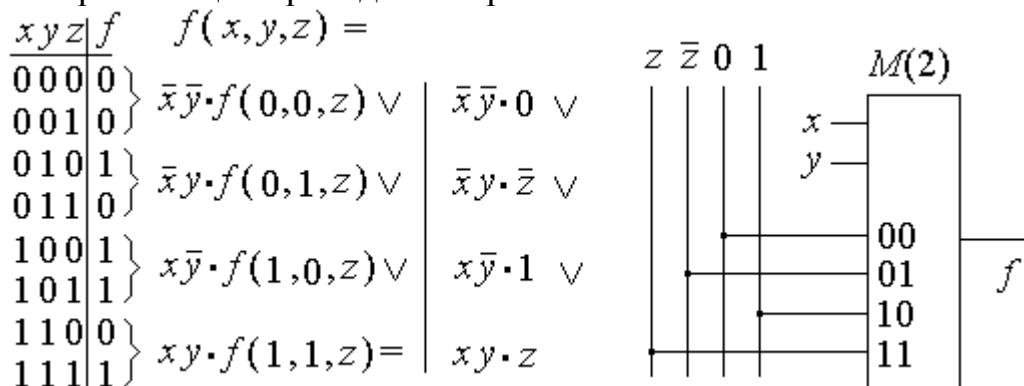


Рис.10.14

**Задача 14.** Построить простую непересекающуюся декомпозицию функции  $f(x_1, x_2, x_3, x_4, x_5) = f_1(x_1, x_2, x_3, f_2(x_4, x_5))$  и реализовать ее с помощью

мультиплексора. Каждая функция задана множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

- 14.1.**  $\{3,8,9,10,11,20,21,22,27\}.$
- 14.2.**  $\{4,5,6,11,19,24,25,26,27\}.$
- 14.3.**  $\{0,1,2,3,11,19,28,29,30\}.$
- 14.4.**  $\{7,12,13,14,15,16,17,18,31\}.$
- 14.5.**  $\{1,8,9,10,11,20,22,23,25\}.$
- 14.6.**  $\{2,8,9,10,11,20,21,23,26\}.$
- 14.7.**  $\{3,12,13,14,16,17,18,19,27\}.$
- 14.8.**  $\{0,1,2,15,23,28,29,30,31\}.$
- 14.9.**  $\{4,6,7,9,17,24,25,26,27\}.$
- 14.10.**  $\{4,9,10,11,20,21,22,23,28\}.$
- 14.11.**  $\{4,5,7,10,18,24,25,26,27\}.$
- 14.12.**  $\{4,5,6,7,15,23,24,25,26\}.$
- 14.13.**  $\{0,1,2,3,9,17,28,30,31\}.$
- 14.14.**  $\{0,1,2,3,10,18,28,29,31\}.$
- 14.15.**  $\{5,12,13,14,15,16,18,19,29\}.$
- 14.16.**  $\{6,12,13,14,15,16,17,19,30\}.$
- 14.17.**  $\{0,8,9,10,11,21,22,23,24\}.$
- 14.18.**  $\{7,8,9,10,20,21,22,23,31\}.$
- 14.19.**  $\{5,8,10,11,20,21,22,23,29\}.$
- 14.20.**  $\{2,12,13,15,16,17,18,19,26\}.$
- 14.21.**  $\{4,5,6,7,13,21,24,26,27\}.$
- 14.22.**  $\{4,5,6,7,14,22,24,25,27\}.$
- 14.23.**  $\{0,1,2,3,8,16,29,30,31\}.$
- 14.24.**  $\{4,12,13,14,15,17,18,19,28\}.$
- 14.25.**  $\{1,2,3,4,9,10,11,16,20,21,22,23\}.$
- 14.26.**  $\{1,2,9,10,12,14,20,21,22,23\}.$
- 14.27.**  $\{11,12,13,14,28,29,30,31\}.$
- 14.28.**  $\{12,13,14,15,20,25,26,27,28,29,30,31\}.$
- 14.29.**  $\{12,13,14,16,17,18,27,31\}.$
- 14.30.**  $\{8,9,10,11,17,18,20,23,25,26\}.$

**Задача 14.** Построить простую непересекающуюся декомпозицию функции  $f(x_1, x_2, x_3, x_4, x_5) = f_1(x_1, x_2, x_3, f_2(x_4, x_5))$  и реализовать ее с помощью мультиплексора. Каждая функция задана множеством  $M_1$  десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

### 10.7. Элементы функциональной декомпозиции

Разобьем множество  $X = \{x_1, \dots, x_n\}$  из  $n$  переменных на два непересекающихся подмножества  $Y = \{y_1, \dots, y_m\}$ ,  $Z = \{z_{m+1}, \dots, z_n\}$  в сумме (в объединении) дающих все множество  $X$ .

**Определение.** Простая непересекающаяся декомпозиция функции  $f(x_1, \dots, x_n)$  есть ее представление в виде  $f(X) = \phi(Y, \psi(Z))$  при некоторых функциях  $\phi$  и  $\psi$ .

**Замечание.** В случае декомпозиции функцию  $f(X)$  можно реализовать следующей схемой, построенной из более простых функций  $\varphi$  и  $\psi$  (рис.10.15).

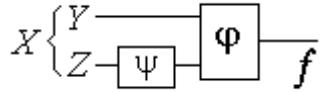


Рис.10.15

В последующем для простоты будем считать, что  $Y=\{x_1, \dots, x_m\}$ ,  $Z=x_{m+1}, \dots, x_n\}$ .

**Определение.**  $Y$ -компонентой функции  $f(Y, Z)$  есть совокупность функций  $\{f(c_1, \dots, c_m, x_{m+1}, \dots, x_n) : (c_1, \dots, c_m) \in E_2^m\}$ .  $Z$ -компонетой функции  $f(Y, Z)$  есть совокупность функций  $\{f(x_1, \dots, x_m, c_{m+1}, \dots, c_n) : (c_{m+1}, \dots, c_n) \in E_2^{n-m}\}$ .

**Пример.**  $f(x_1, x_2, x_3, x_4)$ ,  $Y=\{x_1, x_2\}$ ,  $Z=\{x_3, x_4\}$  (рис.10.17).

Столбцы таблицы на рис.10.17 составляют  $Z$ -компоненту  $\{f(0,0, x_3, x_4) = 1001, f(0,1, x_3, x_4) = 0110, f(1,1, x_3, x_4) = 1101, f(1,0, x_3, x_4) = 1011\}$  функции  $f$ .

	$x_3x_4$	$x_3x_4$	$x_3x_4$	$x_3x_4$	Функции $Y$ -компоненты
$x_1x_2$	0 0	0 1	1 1	1 0	
0 0	1	0	1	1	$f(0,0, x_3, x_4)$
0 1	0	1	1	0	$f(0,1, x_3, x_4)$
1 1	0	1	0	1	$f(1,1, x_3, x_4)$
1 0	1	1	1	1	$f(1,0, x_3, x_4)$

Рис.10.17

**Теорема 1.** Простая непересекающаяся декомпозиция  $f(X) = \varphi(Y, \psi(Z))$  для функции  $f(X)$  существует  $\Leftrightarrow$  всякая функция  $y$  ее  $Y$ -компоненты  $f(c_1, \dots, c_m, Z) \in \{0,1, \psi(Z), \neg\psi(Z)\}$ .

**Пример 1.** Найти простую непересекающуюся декомпозицию функции  $f(x_1, x_2, x_3, x_4)$ ,  $Y=\{x_1, x_2\}$ ,  $Z=\{x_3, x_4\}$  (рис.10.18).

	$x_3x_4$	$x_3x_4$	$x_3x_4$	$x_3x_4$	Функции $Y$ -компоненты
$x_1x_2$	0 0	0 1	1 1	1 0	
0 0	0	0	0	0	$f(0,0, x_3, x_4) = \psi(x_3, x_4)$
0 1	0	0	0	0	$f(0,1, x_3, x_4) = 0$
1 1	1	0	1	1	$f(1,1, x_3, x_4) = \psi(x_3, x_4)$
1 0	0	1	0	0	$f(1,0, x_3, x_4) = \neg\psi(x_3, x_4)$

Рис.10.18

Все функции  $Y$ -компоненты (по строкам) лежат в  $\{0,1, \psi(x_3, x_4), \neg\psi(x_3, x_4)\}$ .

Функция  $f$  допускает простую непересекающуюся декомпозицию

$$f(x_1, x_2, x_3, x_4) =$$

$$f(0,0, x_3, x_4) \cdot \bar{x}_1 \bar{x}_2 \vee f(0,1, x_3, x_4) \cdot \bar{x}_1 x_2 \vee$$

$$f(1,0, x_3, x_4) \cdot x_1 \bar{x}_2 \vee f(1,1, x_3, x_4) \cdot x_1 x_2 =$$

$$\bar{x}_1 \bar{x}_2 \cdot \psi(x_3, x_4) \vee \bar{x}_1 x_2 \cdot 0 \vee x_1 \bar{x}_2 \cdot \neg\psi(x_3, x_4) \vee x_1 x_2 \cdot \psi(x_3, x_4) =$$

$$(\bar{x}_1 \bar{x}_2 \cdot u \vee x_1 \bar{x}_2 \cdot \bar{u} \vee x_1 x_2 \cdot u)|_{u=\psi(x_3, x_4)} = \varphi(x_1, x_2, \psi(x_3, x_4)),$$

где  $\varphi(x_1, x_2, u) = \bar{x}_1 \bar{x}_2 \cdot u \vee x_1 \bar{x}_2 \cdot \bar{u} \vee x_1 x_2 \cdot u$ ,

$\psi(x_3, x_4) = 1011 = \bar{x}_3 \bar{x}_4 \vee x_3 \bar{x}_4 \vee x_3 x_4$ .

Реализация функции

$$f(x_1, x_2, x_3, x_4) = \bar{x}_1 \bar{x}_2 \cdot \psi(x_3, x_4) \vee \bar{x}_1 x_2 \cdot 0 \vee x_1 \bar{x}_2 \cdot \overline{\psi(x_3, x_4)} \vee x_1 x_2 \cdot \psi(x_3, x_4)$$

с помощью мультиплексора приведена на рис.10.19.

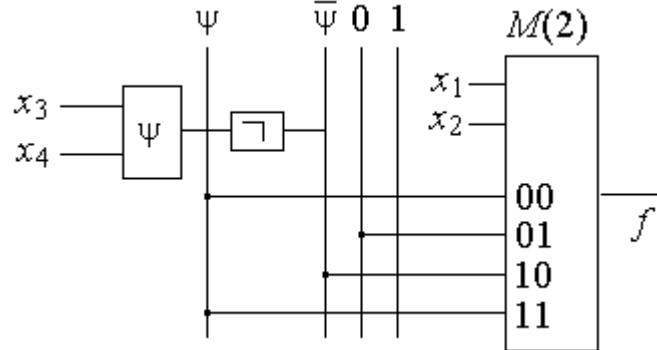


Рис.10.19

**Пример 2.** Найти простую непересекающуюся декомпозицию функции  $f(x_1, x_2, x_3, x_4)$  (рис.10.20.).

	$x_3x_4$	$x_3x_4$	$x_3x_4$	$x_3x_4$	Функции Y-компоненты
$x_1x_2$	0 0	0 1	1 1	1 0	
0 0	0	1	0	0	$f(0,0, x_3, x_4) = \psi(x_3, x_4)$
0 1	0	0	0	0	$f(0,1, x_3, x_4) = 0$
1 1	0	1	1	0	$f(1,1, x_3, x_4) = \psi(x_3, x_4)$
1 0	1	1	1	1	$f(1,0, x_3, x_4) = 1$

Рис.10.20

Функция  $f$  простую непересекающуюся декомпозицию не допускает, ибо функции ее Y-компонент не лежат в  $\{0,1, \psi(x_3, x_4), \neg\psi(x_3, x_4)\}$ .

**Теорема 2.** Функция  $f(X)$  допускает простую непересекающуюся декомпозицию  $f(Y,Z) = \varphi(Y, \psi(Z)) \leftrightarrow$  функция  $f$  имеет в Z-компоненте не более двух различных функций.

**Пример 1.** Найти простую непересекающуюся декомпозицию функции  $f(x_1, x_2, x_3, x_4)$ ,  $Y=\{x_1, x_2\}$ ,  $Z=\{x_3, x_4\}$  (рис.10.21).

	$x_3x_4$	$x_3x_4$	$x_3x_4$	$x_3x_4$	Функции Z-компоненты
$x_1x_2$	0 0	0 1	1 1	1 0	(по вертикали)
0 0	0	1	0	0	$f(x_1, x_2, 0, 0) = h_1(x_1, x_2)$
0 1	1	0	1	1	$f(x_1, x_2, 0, 1) = h_2(x_1, x_2)$
1 1	0	0	0	0	$f(x_1, x_2, 1, 1) = h_1(x_1, x_2)$
1 0	0	0	0	0	$f(x_1, x_2, 0, 1) = h_1(x_1, x_2)$

Рис.10.21

$$\begin{aligned} f(Y, Z) &= f(x_1, x_2, x_3, x_4) = \\ &= f(x_1, x_2, 0, 0) \cdot \bar{x}_3 \bar{x}_4 \vee f(x_1, x_2, 0, 1) \cdot \bar{x}_3 x_4 \vee f(x_1, x_2, 1, 0) \cdot x_3 \bar{x}_4 \vee f(x_1, x_2, 1, 1) \cdot x_3 x_4 = \\ &= h_1(x_1, x_2) \bar{x}_3 \bar{x}_4 \vee h_2(x_1, x_2) \bar{x}_3 x_4 \vee h_1(x_1, x_2) x_3 \bar{x}_4 \vee h_1(x_1, x_2) x_3 x_4 = \end{aligned}$$

$$\begin{aligned}
& h_1(x_1, x_2) \cdot \underbrace{(\bar{x}_3 \bar{x}_4 \vee \underbrace{x_3 \bar{x}_4 \vee x_3 x_4}_{\psi(x_3, x_4)})}_{\psi(x_3, x_4)} \vee h_2(x_1, x_2) \cdot \underbrace{\bar{x}_3 x_4}_{\neg \psi(x_3, x_4)} = \\
& (h_1(x_1, x_2) \cdot \psi(x_3, x_4) \vee h_2(x_1, x_2) \cdot \overline{\psi(x_3, x_4)}) = \\
& \underbrace{(h_1(x_1, x_2) \cdot u \vee h_2(x_1, x_2) \cdot \bar{u})}_{\varphi(Y, u)} \Big|_{u=\psi(x_3, x_4)} = \varphi(Y, \psi(x_3, x_4)).
\end{aligned}$$

Функция  $f$  допускает простую непересекающуюся декомпозицию  $f(Y, Z) = \varphi(Y, \psi(Z))$ . Реализация функции

$f(x_1, x_2, x_3, x_4) = h_1(x_1, x_2)\bar{x}_3\bar{x}_4 \vee h_2(x_1, x_2)\bar{x}_3x_4 \vee h_1(x_1, x_2)x_3\bar{x}_4 \vee h_1(x_1, x_2)x_3x_4$  с помощью мультиплексора приведена на рис.10.22.

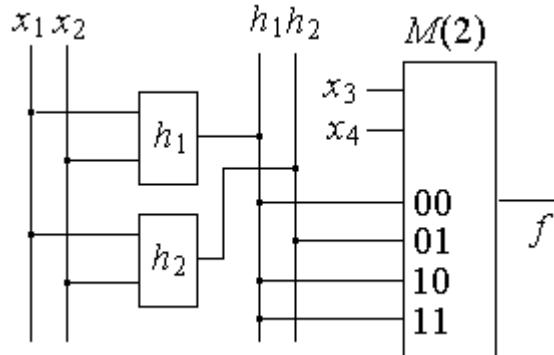


Рис.10.22

**Задача 15.** Для булевой функции из задачи 4 построить минимальные проверяющие и полные тесты для указанных классов ошибок ( $s_{ij}$  есть слипание каналов  $i$  и  $j$ ;  $0_i$  есть обрыв канала  $i$ ,  $1_i$  есть замыкание канала  $i$ ).

- |                                       |                                    |                                       |                                       |
|---------------------------------------|------------------------------------|---------------------------------------|---------------------------------------|
| <b>15.1.</b> $0_1, s_{24}$ .          | <b>15.2.</b> $0_3, s_{14}$ .       | <b>15.3.</b> $1_2, s_{34}$ .          | <b>15.4.</b> $s_{13}, s_{24}$ .       |
| <b>15.5.</b> $0_2, 1_3, s_{14}$ .     | <b>15.6.</b> $0_3, 1_1, s_{24}$ .  | <b>15.7.</b> $0_3, s_{14}$ .          | <b>15.8.</b> $1_3, s_{12}$ .          |
| <b>15.9.</b> $s_{13}, s_{24}$ .       | <b>15.10.</b> $0_1, 1_2, s_{34}$ . | <b>15.11.</b> $0_1, 1_3, s_{24}$ .    | <b>15.12.</b> $1_3, s_{14}$ .         |
| <b>15.13.</b> $0_2, s_{14}$ .         | <b>15.14.</b> $s_{23}, s_{24}$ .   | <b>15.15.</b> $0_3, 1_2, s_{13}$ .    | <b>15.16.</b> $0_2, 1_1, s_{24}$ .    |
| <b>15.17.</b> $0_4, s_{14}$ .         | <b>15.18.</b> $0_3, s_{12}$ .      | <b>15.19.</b> $0_3, s_{13}, s_{24}$ . | <b>15.20.</b> $0_1, 1_2, s_{14}$ .    |
| <b>15.21.</b> $0_3, 1_1, s_{24}$ .    | <b>15.22.</b> $1_1, s_{14}$ .      | <b>15.23.</b> $1_2, s_{14}$ .         | <b>15.24.</b> $0_1, s_{23}, s_{24}$ . |
| <b>15.25.</b> $0_2, 1_3, s_{13}$ .    | <b>15.26.</b> $0_4, 1_1, s_{23}$ . | <b>15.27.</b> $0_1, 1_3, s_{14}$ .    | <b>15.28.</b> $0_3, 1_2, s_{12}$ .    |
| <b>15.29.</b> $1_4, s_{13}, s_{24}$ . | <b>15.30.</b> $0_3, s_{24}$ .      |                                       |                                       |

#### Теоретическое пояснение

Пусть мы конструируем схему из функциональных элементов для данной функции. В результате брака схема может реализовать другую функцию. Задача контроля состоит в том, чтобы определить

- 1) исправна ли схема, то есть реализует ли схема данную функцию,
- 2) какую функцию реализует схема в случае неисправности.

Обнаружение неисправностей в схеме (тестирование схемы) есть важная и непростая задача. Для знакомства с ней мы рассмотрим следующий простой случай.

Пусть мы конструируем схему  $S$  из функциональных элементов для функции  $f_0(x_1, \dots, x_n)$ . В результате брака схема  $S$  может реализовать другую функцию из числа функций  $f_1, f_2, \dots, f_r$  от  $n$  переменных. Задача контроля состоит в том, чтобы определить 1) исправна ли схема, то есть реализует ли схема функцию  $f_0$ , 2) какую функцию из  $f_1, f_2, \dots, f_r$  реализует схема в случае неисправности (Табл.10.19).

Таблица 10.19

$x_1, \dots, x_{n-1}, x_n$	$f_0$	$f_1$	$f_2$	$\dots$	$f_r$
0 ... 0 0	$\alpha_0$	$\beta_0$	$\gamma_0$	$\dots$	$\delta_0$
0 ... 0 1	$\alpha_1$	$\beta_1$	$\gamma_1$	$\dots$	$\delta_1$
...					...
$a_1 \dots a_{n-1} a_n$	$\alpha_p$	$\beta_p$	$\gamma_p$	$\dots$	$\delta_p$
...					...
1 ... 1 1	$\alpha_z$	$\beta_z$	$\gamma_z$	$\dots$	$\delta_p$

где  $z = 2^n - 1$ .

**Определение.** Тест (тестовый набор) для таблично заданной функции  $f_0(x_1, \dots, x_n)$  есть совокупность наборов длины  $n$  из 0 и 1 (совокупность строк в таблице функции  $f$ ), которая высекает из столбцов значения функций  $f_0, f_1, f_2, \dots, f_r$  столбцы со следующими свойствами.

- 1) все высекаемые столбцы различны и тогда тест полный;
- 2) все высекаемые столбцы отличны от столбца для  $f_0$  и тогда тест проверяющий.

**Замечание.** 1. Полный тест есть проверяющий тест.

2. Множество всех наборов длины  $n$  есть полный тест.

**Определение.** Сложность теста есть число входящих в него наборов.

**Определение.** Тест минимальный (туниковый), если удаление из него любого набора приводит к совокупности наборов, которая тестом уже не является. Тест наименьший, если он имеет наименьшую сложность.

**Замечание.** Все наименьшие тесты находятся среди туниковых тестов.

#### Пример построения всех туниковых и наименьших тестов

Пусть строится схема для функции  $f(x_1, \dots, x_n)$ . Примем список следующих неисправностей.

$s_{ij}$ , слипание входов  $x_i$  и  $x_j$ . Тогда реализуется функция

$$g(\dots, x_i, \dots, x_j, \dots) = f(\dots, x_i \vee x_j, \dots, x_i \vee x_j, \dots).$$

$0_i$ , обрыв входа  $x_i$ . Тогда реализуется функция  $g(\dots, x_i, \dots) = f(\dots, 0, \dots)$ .

$1_i$ , замыкание входа  $x_i$ . Тогда реализуется функция  $g(\dots, x_i, \dots) = f(\dots, 1, \dots)$ .

Построим тесты для функции  $f_0=10110110$  для группы неисправностей  $\{0_3, s_{12}\}$ . Возможны только указанные неисправности, причем каждая схема может иметь только одну неисправность.

Для неисправности  $0_3$  функция  $f_1(x_1, x_2, x_3) = f_0(x_1, x_2, 0)$ .

Для неисправности  $s_{12}$  функция  $f_2(x_1, x_2, x_3) = f_0(x_1 \vee x_2, x_1 \vee x_2, x_3)$ .

Пусть  $y_0, \dots, y_7$  есть восемь наборов длины 3 из 0 и 1 (табл.10.20). Каждый тест имеет вид  $y_{i_1} \& y_{i_2} \& \dots \& y_{i_p}$ .

$f_0$  от  $f_1$  отличают строки  $y_1, y_5, y_7$ . Положим  $D_{f_0, f_1} = y_1 \vee y_5 \vee y_7$ .

$f_0$  от  $f_2$  отличают строки  $y_3, y_4, y_5$ . Положим  $D_{f_0, f_2} = y_3 \vee y_4 \vee y_5$ .

Построим все тупиковые проверяющие тесты.

$$D_{f_0, f_1} \& D_{f_0, f_2} = (y_1 \vee y_5 \vee y_7)(y_3 \vee y_4 \vee y_5) =$$

$$y_1y_3 \vee y_1y_4 \vee y_1y_5 \vee y_3y_5 \vee y_4y_5 \vee y_5 \vee y_3y_7 \vee y_4y_7 \vee y_5y_7 =$$

$$y_1y_3 \vee y_1y_4 \vee y_5 \vee y_3y_7 \vee y_4y_7.$$

Таблица 10.20

	$x_1$	$x_2$	$x_3$	$f_0$	$f_1$	$f_2$
$y_0$	0	0	0	1	1	1
$y_1$	0	0	1	0	1	0
$y_2$	0	1	0	1	1	1
$y_3$	0	1	1	1	1	0
$y_4$	1	0	0	0	0	1
$y_5$	1	0	1	1	0	0
$y_6$	1	1	0	1	1	1
$y_7$	1	1	1	0	1	0

Получили пять тупиковых проверяющих тестов. Наименьший проверяющий тест есть  $y_5$ :

$$\begin{array}{ccccccc} & x_1 & x_2 & x_3 & f_0 & f_1 & f_2 \\ y_5 & 1 & 0 & 1 & 1 & 0 & 0 \end{array}$$

Подаем на вход схемы набор 101. Если на выходе 1, то схема реализует функцию  $f_0$ . Если на выходе 0, то схема неисправна и функцию  $f_0$  не реализует.

Построим все полные тупиковые тесты.

$f_1$  от  $f_2$  отличают строки  $y_1, y_3, y_4, y_7$ .

Положим  $D_{f_1, f_2} = y_1 \vee y_3 \vee y_4 \vee y_7$ . Тогда  $D_{f_0, f_1} \& D_{f_0, f_2} \& D_{f_1, f_2} =$

$$(y_1 \vee y_5 \vee y_7)(y_3 \vee y_4 \vee y_5)(y_1 \vee y_3 \vee y_4 \vee y_7) =$$

$$(y_1y_3 \vee y_1y_4 \vee y_5 \vee y_3y_7 \vee y_4y_7)(y_1 \vee y_3 \vee y_4 \vee y_7) =$$

$$y_1y_3 \vee y_1y_3 \vee y_1y_5 \vee y_1y_3y_7 \vee y_1y_4y_7 \vee y_1y_3 \vee y_1y_3y_4 \vee y_3y_5 \vee y_3y_7 \vee$$

$$y_3y_4y_7 \vee y_1y_3y_4 \vee y_1y_4 \vee y_4y_5 \vee y_3y_4y_7 \vee y_4y_7 \vee y_1y_3y_7 \vee y_1y_4y_7 \vee y_5y_7 \vee y_3y_7 \vee y_4y_7 =$$

$$y_1y_3 \vee y_1y_4 \vee y_1y_5 \vee y_3y_5 \vee y_3y_7 \vee y_4y_5 \vee y_4y_7 \vee y_5y_7.$$

Получили 8 полных тупиковых тестов. Они все наименьшие.

Например,  $y_1y_3$ :

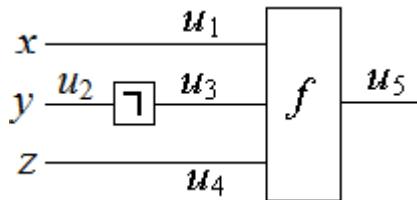
$$\begin{array}{ccccccc} & x_1 & x_2 & x_3 & f_0 & f_1 & f_2 \\ y_1 & 0 & 0 & 1 & 0 & 1 & 0 \\ y_3 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}$$

Подаем на вход схемы последовательно наборы  $y_1, y_3$ , то есть наборы  $\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}$ . Пара  $\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}$  на выходе укажет, что схема реализует функцию  $f_0$ , пара  $\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$  – функцию  $f_1$ , пара  $\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}$  – функцию  $f_2$ .

**Задача 16.** Для данной схемы из функциональных элементов (СФЭ) найти:  
 1)) наименьший проверяющий тест,  
 б) наименьший полный (диагностический) тест.

- 16.1.**  $f = x \& (y \rightarrow z)$ ,  $0_1, 0_2, \neg_3$ .
- 16.2.**  $f = (x \& y) \rightarrow z$ ,  $0_1, 0_2, 1_3$ .
- 16.3.**  $f = (x \& y) | z$ ,  $0_1, 0_2, 1_4$ .
- 16.4.**  $f = (x \& y) + z$ ,  $0_1, 0_2, 1_4$ .
- 16.5.**  $f = x \& y \& z$ ,  $0_1, \neg_2, 1_4$ .
- 16.6.**  $f = (x + y) \rightarrow z$ ,  $1_1, 0_3, 0_4$ .
- 16.7.**  $f = (x + y) | z$ ,  $1_1, \neg_3, 1_4$ .
- 16.8.**  $f = (x + y) \& z$ ,  $1_1, 1_3, 0_4$ .
- 16.9.**  $f = (x \rightarrow y) \& z$ ,  $1_1, 1_3, \neg_5$ .
- 16.10.**  $f = (x \rightarrow y) | z$ ,  $0_1, 0_3, 1_4$ .
- 16.11.**  $f = (x \rightarrow y) + z$ ,  $0_1, 0_2, \neg_3$ .
- 16.12.**  $f = (x | y) \& z$ ,  $0_1, 0_2, 0_4$ .
- 16.13.**  $f = (x | y) | z$ ,  $0_1, 1_2, 1_4$ .
- 16.14.**  $f = (x | y) + z$ ,  $0_1, 1_2, 1_4$ .
- 16.15.**  $f = x \& (y \rightarrow z)$ ,  $1_1, \neg_3, 0_4$ .
- 16.16.**  $f = (x \& y) \rightarrow z$ ,  $1_1, 0_3, 1_4$ .
- 16.17.**  $f = (x \& y) | z$ ,  $1_1, 1_3, 0_4$ .
- 16.18.**  $f = (x \& y) + z$ ,  $1_1, 1_3, 1_4$ .
- 16.19.**  $f = x \& y \& z$ ,  $0_1, 0_2, \neg_5$ .
- 16.20.**  $f = (x + y) \rightarrow z$ ,  $0_1, 1_3, \neg_4$ .
- 16.21.**  $f = (x + y) | z$ ,  $0_1, 0_2, 0_4$ .
- 16.22.**  $f = (x + y) \& z$ ,  $0_1, 0_2, 1_4$ .
- 16.23.**  $f = (x \rightarrow y) \& z$ ,  $0_1, 1_2, 1_4$ .
- 16.24.**  $f = (x \rightarrow y) | z$ ,  $1_1, 0_3, 0_4$ .
- 16.25.**  $f = x \vee (y \& z)$ ,  $1_1, 0_2, 3_4$ .
- 16.26.**  $f = x \vee (y | z)$ ,  $1_1, \neg_3, 0_4$ .
- 16.27.**  $f = x \vee (y \rightarrow z)$ ,  $0_1, \neg_2, 1_5$ .
- 16.28.**  $f = x \vee (y + z)$ ,  $0_1, \neg_3, 1_4$ .
- 16.29.**  $f = x \& (y \vee z)$ ,  $1_1, \neg_4, 0_5$ .
- 16.30.**  $f = x + (y \vee z)$ ,  $1_1, 1_3, \neg_5$ .

Расположение неисправностей показано на следующей схеме.



Для возможных однократных неисправностей  $u_i, i=1,2,3,4,5$ , принятые следующие обозначения:

$u_1, u_2, u_3, u_4, u_5$ , возможные однократные неисправности:

$0_i$ , обрыв контакта  $i$ ,  $u_i = 0$ ;

$1_i$ , замыкание контакта  $i$ ,  $u_i = 1$ ;

$\neg_i$ , вместо  $u_i$  реализуется  $\neg u_i$ ,  $u_i = \neg$ ;

$|$ , штрих Шеффера.

Для данных трех неисправностей остальных двух неисправностей нет.

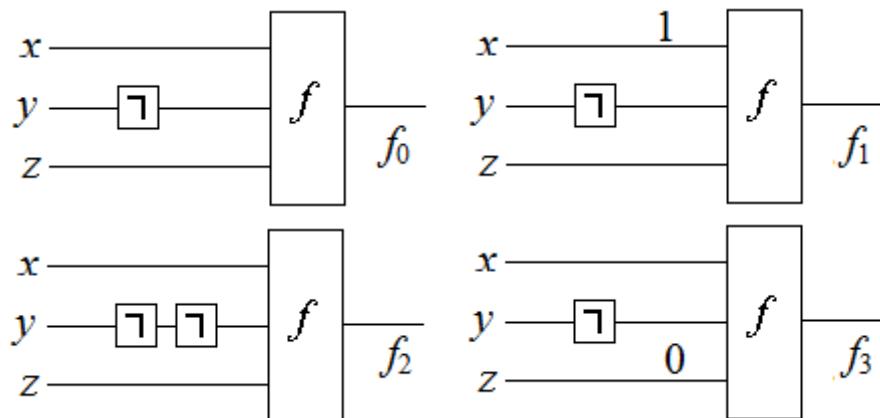
**Указание.**

Пусть  $f(x, y, z) = x \& (y \rightarrow z)$ .

Неисправности  $1_1, \neg_3, 0_4$ , то есть  $u_1 = 1, u_3 = \neg, u_4 = 0$ .

Следующие схемы реализуют функции

$f_0(x, y, z), f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)$ .



$$f_0(x, y, z) = f(x, \neg y, z) = x \& (\neg y \rightarrow z).$$

$$f_1(x, y, z) = f_0(1, y, z) = f(1, \neg y, z) = 1 \& (\neg y \rightarrow z).$$

$$f_2(x, y, z) = f_0(x, \neg y, z) = f(x, \neg \neg y, z) = f(x, y, z) = x \& (y \rightarrow z).$$

$$f_3(x, y, z) = f_0(x, y, 0) = f(x, \neg y, 0) = x \& (\neg y \rightarrow 0).$$

Далее решение как в задаче 15.

**16.1.**  $f = x \& (y \rightarrow z), 0_1, 0_2, \neg_3$ .

**16.2.**  $f = (x \& y) \rightarrow z, 0_1, 0_2, 1_3$ .

**16.3.**  $f = (x \& y) | z, 0_1, 0_2, 1_4$ .

**16.4.**  $f = (x \& y) + z, 0_1, 0_2, 1_4$ .

**16.5.**  $f = x \& y \& z, 0_1, \neg_2, 1_4$ .

**16.6.**  $f = (x + y) \rightarrow z, 1_1, 0_3, 0_4$ .

**16.7.**  $f = (x + y) | z, 1_1, \neg_3, 1_4$ .

**16.8.**  $f = (x + y) \& z, 1_1, 1_3, 0_4$ .

**16.9.**  $f = (x \rightarrow y) \& z, 1_1, 1_3, \neg_5$ .

- 16.10.**  $f = (x \rightarrow y) | z, 0_1, 0_3, 1_4$ .
- 16.11.**  $f = (x \rightarrow y) + z, 0_1, 0_2, \neg_3$ .
- 16.12.**  $f = (x | y) \& z, 0_1, 0_2, 0_4$ .
- 16.13.**  $f = (x | y) | z, 0_1, 1_2, 1_4$ .
- 16.14.**  $f = (x | y) + z, 0_1, 1_2, 1_4$ .
- 16.15.**  $f = x \& (y \rightarrow z), 1_1, \neg_3, 0_4$ .
- 16.16.**  $f = (x \& y) \rightarrow z, 1_1, 0_3, 1_4$ .
- 16.17.**  $f = (x \& y) | z, 1_1, 1_3, 0_4$ .
- 16.18.**  $f = (x \& y) + z, 1_1, 1_3, 1_4$ .
- 16.19.**  $f = x \& y \& z, 0_1, 0_2, \neg_5$ .
- 16.20.**  $f = (x + y) \rightarrow z, 0_1, 1_3, \neg_4$ .
- 16.21.**  $f = (x + y) | z, 0_1, 0_2, 0_4$ .
- 16.22.**  $f = (x + y) \& z, 0_1, 0_2, 1_4$ .
- 16.23.**  $f = (x \rightarrow y) \& z, 0_1, 1_2, 1_4$ .
- 16.24.**  $f = (x \rightarrow y) | z, 1_1, 0_3, 0_4$ .
- 16.25.**  $f = x \vee (y \& z), 1_1, 0_2, 3_4$ .
- 16.26.**  $f = x \vee (y | z), 1_1, \neg_3, 0_4$ .
- 16.27.**  $f = x \vee (y \rightarrow z), 0_1, \neg_2, 1_5$ .
- 16.28.**  $f = x \vee (y + z), 0_1, \neg_3, 1_4$ .
- 16.29.**  $f = x \& (y \vee z), 1_1, \neg_4, 0_5$ .
- 16.30.**  $f = x + (y \vee z), 1_1, 1_3, \neg_5$ .

**Задача 17.** Задана формула логики предикатов  $A$  и двухэлементное множество  $M = \{1,2\}$ . Привести формулу  $A$  к префиксной нормальной форме. Является ли формула  $A$  на множестве  $M$ : 1) выполнимой; 2) опровергимой; 3) общезначимой; 4) невыполнимой? Вычислить значение истинности формулы  $A$  на множестве  $M$  со следующими предикатами, определенными на  $M$ .

$x$	1	2
$P(x)$	1	0
$R(x)$	0	1

$Q(x,y)$	1	2
1	1	0
2	0	0

- 17.1.**  $(\forall x)(P(x) \& R(x) \rightarrow (\exists y)Q(x,y))$ .
- 17.2.**  $(\forall x)(P(x) \rightarrow (R(x) \rightarrow (\exists y)Q(x,y)))$ .
- 17.3.**  $(\forall x)(P(x) \& \neg R(x) \rightarrow (\exists y)Q(x,y))$ .
- 17.4.**  $(\forall x)(\neg P(x) \rightarrow (\neg R(x) \rightarrow (\exists y)\neg Q(x,y)))$ .
- 17.5.**  $(\forall x)(\neg P(x) \vee \neg R(x) \rightarrow (\exists y)Q(x,y))$ .
- 17.6.**  $(\exists x)(P(x) \& R(x) \rightarrow (\forall y)Q(x,y))$ .
- 17.7.**  $(\exists x)(P(x) \rightarrow (R(x) \rightarrow (\forall y)Q(x,y)))$ .
- 17.8.**  $(\exists x)(P(x) \vee \neg(R(x) \rightarrow (\forall y)Q(x,y)))$ .
- 17.9.**  $(\exists x)(\neg P(x) \rightarrow (\neg R(x) \rightarrow (\forall y)Q(x,y)))$ .
- 17.10.**  $(\exists x)(\neg P(x) \vee \neg R(x) \rightarrow (\exists y)\neg Q(x,y))$ .
- 17.11.**  $(\forall y)(P(y) \& R(y) \rightarrow (\exists x)Q(x,y))$ .

- 17.12.**  $(\forall y)(P(y) \rightarrow (R(y) \rightarrow (\exists x)Q(x,y))).$
- 17.13.**  $(\forall y)(P(y) \vee \neg R(y) \rightarrow (\exists x)Q(x,y))).$
- 17.14.**  $(\forall y)(\neg P(y) \rightarrow (\neg R(y) \rightarrow (\exists x)Q(x,y))).$
- 17.15.**  $(\forall y)(P(y) \rightarrow (\neg R(y) \rightarrow (\exists x)Q(x,y))).$
- 17.16.**  $(\forall x)(P(x) \& R(x) \rightarrow (\forall y)Q(x,y)).$
- 17.17.**  $(\forall x)(P(x) \rightarrow (R(x) \rightarrow (\forall y)Q(x,y))).$
- 17.18.**  $(\forall x)(P(x) \vee \neg P(x) \rightarrow (\forall y)Q(x,y)).$
- 17.19.**  $(\forall x)((P(x) \rightarrow R(x)) \rightarrow (\forall y)Q(x,y)).$
- 17.20.**  $(\forall x)(\neg P(x) \vee \neg R(x) \rightarrow (\forall y)Q(x,y)).$
- 17.21.**  $(\exists y)(\forall x)(Q(x,y) \& R(x) \rightarrow (\forall y)P(y)).$
- 17.22.**  $(\exists y)((\exists x)(Q(x,y) \rightarrow P(x) \vee Q(x,y))).$
- 17.23.**  $(\exists y)((\forall x)(Q(x,y) \rightarrow \neg P(x) \vee \neg Q(x,y))).$
- 17.24.**  $(\forall y)((\exists x)(Q(x,y) \rightarrow (P(x) \rightarrow Q(x,y)))).$
- 17.25.**  $(\forall x)((\exists y)Q(x,y) \rightarrow (R(x) \rightarrow P(x))).$
- 17.26.**  $(\forall x)(P(x) \rightarrow (\exists y)(Q(x,y) \rightarrow R(x))).$
- 17.27.**  $(\exists x)(P(x) \rightarrow (\exists y)(Q(x,y) \rightarrow \neg R(x))).$
- 17.28.**  $(\exists y)(P(y) \rightarrow (\forall x)Q(x,y) \rightarrow R(y))).$
- 17.29.**  $(\forall y)(P(y) \rightarrow (\forall x)(Q(y,x) \rightarrow \neg R(x))).$
- 17.30.**  $(\forall y)(P(y) \rightarrow (\forall x)(Q(x,y) \vee \neg R(x))).$

**Задача 17.** Задана формула логики предикатов

$$A = (\exists y)(P(y) \rightarrow (\forall x)(Q(x,y) \vee \neg R(x)))$$

и двухэлементное множество  $M = \{1,2\}$ . Привести формулу А к префиксной нормальной форме. Является ли формула А на множестве  $M$ : 1) выполнимой; 2) опровергимой; 3) общезначимой; 4) невыполнимой? Вычислить значение истинности формулы А на множестве  $M$  со следующими предикатами, определенными на  $M$ .

$x$	1	2
$P(x)$	1	0
$R(x)$	0	1

$Q(x,y)$	1	2
1	1	0
2	0	0

*Решение.* Интерпретация  $I = (M=\{1,2\}, P, Q, R)$ .

1. Префиксная нормальная форма.

$$A = (\exists y)(P(y) \rightarrow (\forall x)(Q(x,y) \vee \neg R(x))) = (\exists y)(\neg P(y) \vee (\forall x)(Q(x,y) \vee \neg R(x))) = (\exists y)(\forall x) (\neg P(y) \vee Q(x,y) \vee \neg R(x)).$$

кванторная бескванторная

приставка формула

На интерпретации  $I = (M=\{1,2\}, P, Q, R)$  формула

$$A = (\exists y)(\forall x) (\neg P(y) \vee Q(x,y) \vee \neg R(x)).$$

2. Элиминация кванторов на конечном множестве  $M = \{1,2\}$ .

$$A(I) = (\exists y)((\neg P(y) \vee Q(1,y) \vee \neg R(1)) \& (\neg P(y) \vee Q(2,y) \vee \neg R(2)) =$$

$$\begin{array}{cccc} x & x & x & x \\ (\neg P(1) \vee Q(1,1) \vee \neg R(1)) & \& (\neg P(1) \vee Q(2,1) \vee \neg R(2)) & \vee \end{array}$$

$$\begin{array}{ccccccc}
 & y & x & y & x & y & x \\
 (\neg P(2) \vee Q(1,2) \vee \neg R(1)) & \& (\neg P(2) \vee Q(2,2) \vee \neg R(2)). \\
 & y & x & y & x & y & x
 \end{array}$$

3. Вычисление значения формулы  $A$  на интерпретации  $I$ .

$$\begin{aligned}
 A(I) = & (\neg 1 \vee 1 \vee 1) \& (\neg 1 \vee 0 \vee 0) \vee (\neg 0 \vee 0 \vee 1) \& (\neg 0 \vee 0 \vee 0) = \\
 & (0 \vee 1 \vee 1) \& (0 \vee 0 \vee 0) \vee (1 \vee 0 \vee 1) \& (1 \vee 0 \vee 0) = 1 \& 0 \vee 1 \& 1 = 1.
 \end{aligned}$$

4. Пусть  $x_1 = P(1)$ ,  $x_2 = P(2)$ ,  $x_3 = R(1)$ ,  $x_4 = R(2)$ ,  $x_5 = Q(1,1)$ ,  $x_6 = Q(1,2)$ ,  $x_7 = Q(2,1)$ ,  $x_8 = Q(2,2)$ . Тогда

$$A = (\bar{x}_1 \vee x_5 \vee \bar{x}_3) \& (\bar{x}_1 \vee x_7 \vee \bar{x}_4) \vee (\bar{x}_2 \vee x_6 \vee \bar{x}_3) \& (\bar{x}_2 \vee x_8 \vee \bar{x}_4).$$

При  $x_1=0$ ,  $x_2=0$   $A=1$  при любых других значениях аргументов. Поэтому, например, при  $I = (0,0,0,1,1,0,1,0)$  значение  $A(I) = 1$ . В наших обозначениях  $x_1=P(1)=0$ ,  $x_2=P(2)=0$ ,  $x_3=R(1)=0$ ,  $x_4=R(1)=1$ ,  $x_5=Q(1,1)=1$ ,  $x_6=Q(1,2)=0$ ,  $x_7=Q(2,1)=1$ ,  $x_8=Q(2,2)=0$ .

На множестве  $M=\{0,1\}$  другая выполняющая интерпретация для  $A$ :

$x$	1	2
$P(x)$	0	0
$R(x)$	0	1

$Q(x,y)$	1	2
1	1	0
2	1	0

$$\begin{aligned}
 5. \bar{A} = & (x_1 \bar{x}_5 x_3 \vee x_1 \bar{x}_7 x_4) \& (x_2 \bar{x}_6 x_3 \vee x_2 \bar{x}_8 x_4) = \\
 & x_1 x_2 x_3 \bar{x}_5 \bar{x}_6 \vee x_1 x_2 x_3 x_4 \bar{x}_5 \bar{x}_6 \vee x_1 x_2 x_3 x_4 \bar{x}_6 \bar{x}_7 \vee x_1 x_2 x_4 \bar{x}_7 \bar{x}_8.
 \end{aligned}$$

Хотя бы одно слагаемое должно быть равно единице, например, третье:  $x_1=1$ ,  $x_2=1$ ,  $x_3=1$ ,  $x_4=1$ ,  $x_6=0$ ,  $x_7=0$ . Значения остальных переменных произвольно. Поэтому, например, при  $I = (1,1,1,1,1,0,0,1)$  значение  $\neg A(I) = 1$ . Тогда  $A(I) = 0$ .

В наших обозначениях:

$$\begin{aligned}
 x_1=P(1)=1, x_2=P(2)=1, x_3=R(1)=1, x_4=R(1)=1, \\
 x_5=Q(1,1)=1, x_6=Q(1,2)=0, x_7=Q(2,1)=0, x_8=Q(2,2)=1.
 \end{aligned}$$

На множестве  $M = \{0,1\}$  опровергающая интерпретация для формулы  $A$ :

$x$	1	2
$P(x)$	1	1
$R(x)$	1	1

$Q(x,y)$	1	2
1	1	0
2	0	1

**Задача.** Проверить, является ли логическими законами следующие логические формулы (Новикова помечены буквой N, Клини – буквой K).

1.  $p \rightarrow (q \rightarrow p)$ . NK.
2.  $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$ . N.
- 2a.  $(p \rightarrow q) \rightarrow ((p \rightarrow (q \rightarrow r)) \rightarrow (p \rightarrow r))$ . K.
3.  $p \& q \rightarrow p$ . NK.
4.  $p \& q \rightarrow q$ . NK.
5.  $(p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow q \& r))$ . NK.
6.  $p \rightarrow p \vee q$ . NK.
7.  $q \rightarrow p \vee q$ . NK.

8.  $(p \rightarrow r) \rightarrow ((q \rightarrow r) \rightarrow (p \vee q \rightarrow r)).$  NK.
9.  $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p).$  N.
- 9a.  $(p \rightarrow q) \rightarrow (p \rightarrow \neg q) \rightarrow \neg p.$  K
10.  $p \rightarrow \neg \neg p.$  N.
11.  $\neg \neg p \rightarrow p.$  NK.
- 11a.  $\neg p \rightarrow (p \rightarrow q).$  K.
12.  $((p \rightarrow q) \rightarrow (p \rightarrow r)) \rightarrow (p \rightarrow (q \rightarrow r)).$
13.  $\neg(p \vee q) \equiv \neg p \& \neg q.$
14.  $\neg(p \& q) \equiv \neg p \vee \neg q.$
15.  $(p \rightarrow (q \rightarrow r)) \equiv (q \rightarrow (p \rightarrow r)).$
16.  $(p \& q \rightarrow r) \equiv (p \rightarrow (q \rightarrow r)).$
17.  $p \vee q \equiv \neg(\neg p \& \neg q).$
18.  $p \& q \equiv \neg(\neg p \vee \neg q).$
19.  $(p \rightarrow q) \equiv \neg p \vee q.$

**Замечание.** Формулы 1,2,3,4,5,6,7,8,9,10,11, помеченные буквой N, составляют аксиоматику Новикова. Формулы 1,2a,3,4, 5,6,7,8,9a,11, помеченные буквой K, составляют аксиоматику Клини. Аксиомы Клини, в которой формула 11 заменена на формулу 11a, составляют аксиоматику интуиционистского (или конструктивистского) исчисления. Аксиомы Клини без аксиомы 11 составляют аксиоматику минимального исчисления Иогансона. Известно, что между интуиционистским и классическим исчислениями имеется континuum суперинтуиционистских (или суперконструктивистских) исчислений.

**Задача 17а.** Проверить, являются ли логическими законами следующие логические формулы (Новикова помечены буквой N, Клини – буквой K).

**Задача 17б.** Доказать или опровергнуть справедливость следующих правил вывода, установив общезначимость соответствующих формул.

1.  $\frac{A \rightarrow B, A}{B}.$  2.  $\frac{A \rightarrow B, \neg B}{\neg A}.$  3.  $\frac{A \rightarrow B, \neg A}{\neg B}.$
4.  $\frac{A \vee B, \neg A}{B}.$  5.  $\frac{A \vee B, \neg B}{A}.$  6.  $\frac{A \vee B, A}{\neg B}.$
7.  $\frac{A \rightarrow (B \rightarrow C)}{A \& B \rightarrow C}.$  8.  $\frac{\neg A \rightarrow (B \rightarrow C)}{A \& B \rightarrow \neg C}.$  9.  $\frac{A \& B \rightarrow C}{A \rightarrow (B \rightarrow C)}.$  10.  $\frac{A \vee \neg B \rightarrow C}{A \rightarrow B \& C}.$
11.  $\frac{C \rightarrow A, C \rightarrow B}{C \rightarrow A \& B}.$  12.  $\frac{C \rightarrow \neg A, C \rightarrow B}{C \rightarrow A \vee B}.$  13.  $\frac{A \rightarrow C, B \rightarrow C}{A \vee B \rightarrow C}.$  14.  $\frac{A \vee C, B \rightarrow \neg C}{A \vee B \rightarrow C}.$
15.  $\frac{A \rightarrow C, B \rightarrow C, A \vee B}{C}.$  16.  $\frac{A \rightarrow C, B \rightarrow D, A \vee B}{C \vee D}.$
17.  $\frac{C \rightarrow A, D \rightarrow B, \neg A \vee \neg B}{\neg C}.$  18.  $\frac{C \rightarrow A, D \rightarrow B, \neg A \vee \neg B}{\neg C \vee \neg D}.$

**Естественный вывод Гентцена (Исчисление секвенций)**

## Схемы аксиом

Если  $A$  есть формула СИВ, то секвенция вида  $\Gamma, A \models \Delta$ ;  $A$  есть единственная схема аксиом в СИВ.

## Пропозициональные правила (секвенциального) вывода

### Введение отрицания

$$\frac{\Gamma \Rightarrow \Delta; A}{\Gamma, \neg A \Rightarrow \Delta} (\neg \Rightarrow); \quad \frac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \Delta; \neg A} (\Rightarrow \neg);$$

### Введение конъюнкции

$$\frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \& B \Rightarrow \Delta} (\& \Rightarrow); \quad \frac{\Gamma \Rightarrow \Delta; A \quad \Gamma \Rightarrow \Delta; B}{\Gamma \Rightarrow \Delta; A \& B} (\Rightarrow \&)$$

### Введение дизъюнкции

$$\frac{\Gamma, A \Rightarrow \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta} (\vee \Rightarrow); \quad \frac{\Gamma \Rightarrow \Delta; A; B}{\Gamma \Rightarrow \Delta; A \vee B} (\Rightarrow \vee)$$

### Введение импликации

$$\frac{\Gamma, B \Rightarrow \Delta \quad \Gamma \Rightarrow \Delta; A}{\Gamma, A \rightarrow B \Rightarrow \Delta} (\rightarrow \Rightarrow); \quad \frac{\Gamma, A \Rightarrow \Delta; B}{\Gamma \Rightarrow \Delta; A \rightarrow B} (\Rightarrow \rightarrow)$$

## Предикатные правила (секвенциального) вывода

$$\frac{\Gamma \Rightarrow \Delta; A(y)}{\Gamma \Rightarrow \Delta; (\forall x)A(x)} (\Rightarrow \forall); \quad \frac{\Gamma, A(y) \Rightarrow \Delta}{\Gamma, (\exists x)A(x) \Rightarrow \Delta} (\exists \Rightarrow);$$

переменная  $y$  не входит в нижнюю секвенцию свободно;

$$\frac{\Gamma, A(t), (\forall x)A(x) \Rightarrow \Delta}{\Gamma, (\forall x)A(x) \Rightarrow \Delta} (\forall \Rightarrow); \quad \frac{\Gamma \Rightarrow \Delta; A(t); (\exists x)A(x)}{\Gamma \Rightarrow \Delta; (\exists x)A(x)} (\Rightarrow \exists);$$

переменная  $x$  не входит в верхнюю секвенцию свободно.

**Задача.** Доказать справедливость правил секвенциального вывода, установив общезначимость соответствующей формулы.

**Задача 18.** Установить правильность или неправильность правил вывода, установив общезначимость соответствующей формулы.

$$18.1. \frac{P \rightarrow \neg M, S \& M}{S \& \neg P}.$$

$$18.2. \frac{P \rightarrow \neg M, M \rightarrow S, M}{S \& \neg P}.$$

$$18.3. \frac{M \rightarrow P, S \& M}{S \& P}.$$

$$18.4. \frac{P \rightarrow M, M \rightarrow S, P}{S \& P}.$$

$$18.5. \frac{P \rightarrow \neg M, M \& S}{S \& \neg P}.$$

$$18.6. \frac{P \rightarrow M, M \rightarrow \neg S}{S \rightarrow \neg P}.$$

$$18.7. \frac{P \& M, M \rightarrow S}{S \& P}.$$

$$18.8. \frac{P \rightarrow M, M \rightarrow \neg S, P}{\neg S \& P}.$$

$$18.9. \frac{M \rightarrow \neg P, M \rightarrow S, M}{S \& \neg P}.$$

$$18.10. \frac{M \rightarrow P, M \rightarrow S, M}{P \& S}.$$

$$18.11. \frac{M \rightarrow \neg P, M \& S}{S \& \neg P}.$$

$$18.12. \frac{M \rightarrow P, M \& S}{S \rightarrow P}.$$

$$18.13. \frac{M \& P, M \rightarrow S}{S \& P}.$$

$$18.15. \frac{P \rightarrow \neg M, S \rightarrow M, S}{S \& \neg P}.$$

$$18.17. \frac{P \rightarrow \neg M, S \& M}{S \& \neg P}.$$

$$18.19. \frac{P \rightarrow \neg M, S \rightarrow M}{S \rightarrow \neg P}.$$

$$18.21. \frac{M \rightarrow \neg P, S \rightarrow M, S}{S \& \neg P}.$$

$$18.23. \frac{M \rightarrow P, S \& M}{S \& P}.$$

$$18.25. \frac{M \rightarrow P, S \rightarrow M}{S \rightarrow P}.$$

$$18.27. \frac{P \rightarrow \neg M, S \rightarrow M, S}{S \& \neg P}.$$

$$18.29. \frac{M \rightarrow \neg P, \neg M \rightarrow \neg S}{S \rightarrow \neg P}.$$

$$18.14. \frac{M \& \neg P, M \rightarrow S}{S \rightarrow \neg P}.$$

$$18.16. \frac{P \rightarrow M, S \rightarrow \neg M, S}{S \& \neg P}.$$

$$18.18. \frac{P \rightarrow M, S \rightarrow \neg M}{S \rightarrow \neg P}.$$

$$18.20. \frac{P \rightarrow M, S \& \neg M}{S \& \neg P}.$$

$$18.22. \frac{M \rightarrow P, S \rightarrow M, S}{S \& P}.$$

$$18.24. \frac{M \rightarrow \neg P, S \rightarrow M}{S \rightarrow \neg P}.$$

$$18.26. \frac{\neg M \rightarrow \neg P, M \rightarrow \neg S}{S \rightarrow \neg P}.$$

$$18.28. \frac{\neg P \rightarrow \neg M, S \rightarrow M, S}{S \& P}.$$

$$18.30. \frac{\neg M \rightarrow \neg P, S \& \neg M}{S \& \neg P}.$$

**Пример.** Проверить правильность или неправильность правила вывода  
 $\frac{\neg M \rightarrow \neg P, S \& \neg M}{S \& \neg P}$ , установив общезначимость соответствующей формулы.

*Решение.* Правило  $\frac{\neg M \rightarrow \neg P, S \& \neg M}{S \& \neg P}$  верно  $\leftrightarrow$  формула

$$F = (\neg M \rightarrow \neg P) \& (S \& \neg M) \rightarrow (S \& \neg P) \text{ тождественно истинна.}$$

$$F = F(M, P, S) = (\overline{M} \rightarrow \overline{P}) \& (S \& \overline{M}) \rightarrow (S \& \overline{P}) =$$

$$\overline{(\overline{M} \vee \overline{P})(S \& \overline{M})} \vee S \& \overline{P} = \overline{\overline{M} \vee \overline{P}} \vee \overline{S \& \overline{M}} \vee S \& \overline{P} =$$

$$\overline{\overline{M} \overline{P}} \vee \overline{S} \vee \overline{\overline{M}} \vee S \& \overline{P} = \overline{M} P \vee \overline{S} \vee M \vee S \& \overline{P} =$$

$$(\overline{M} \vee M)(P \vee \overline{M}) \vee (\overline{S} \vee S)(\overline{S} \vee \overline{P}) =$$

$$P \vee M \vee \overline{S} \vee \overline{P} \equiv 1. \text{ Правило вывода верно.}$$

2. Пусть  $F_1 = \neg M \rightarrow \neg P$ ,  $F_2 = S \& \neg M$ ,  $F_3 = F_1 \& F_2$ ,  $F_4 = S \& \neg P$ .

Вычисления занесем в табл. 10.15.

Таблица 10.15

	MPS	$F_1$	$F_2$	$F_3$	$F_4$	$F$
0	000	1	0	0	0	1
1	001	1	1	1	1	1
2	010	0	0	0	0	1
3	011	0	1	0	0	1
4	100	1	0	0	0	1
5	101	1	0	0	1	1

6	110	1	0	0	0	1
1	111	1	0	0	0	1

*Ответ.* Формула  $F \equiv 1$ . Следовательно, правило вывода верно.

**Задача 19.** Установить правильность или неправильность правил вывода, установив общезначимость соответствующей формулы.

$$19.1. \frac{P \rightarrow \neg M, \neg S \& M}{\neg S \& \neg P}.$$

$$19.3. \frac{M \rightarrow \neg P, \neg S \& M}{\neg S \& P}.$$

$$19.5. \frac{\neg P \rightarrow \neg M, \neg M \& S}{\neg S \& \neg P}.$$

$$19.7. \frac{\neg P \& M, \neg M \rightarrow S}{S \& \neg P}.$$

$$19.9. \frac{M \rightarrow \neg P, M \rightarrow S, M}{\neg S \& \neg P}.$$

$$19.11. \frac{M \rightarrow \neg P, \neg M \& S}{\neg S \& \neg P}.$$

$$19.13. \frac{M \& P, \neg M \rightarrow S}{S \& P}.$$

$$19.15. \frac{P \rightarrow \neg M, \neg S \rightarrow M, \neg S}{S \& \neg P}.$$

$$19.17. \frac{P \rightarrow \neg M, \neg S \rightarrow M}{\neg S \& \neg P}.$$

$$19.19. \frac{P \rightarrow \neg M, \neg S \rightarrow M}{\neg S \rightarrow \neg P}.$$

$$19.21. \frac{\neg M \rightarrow \neg P, \neg S \rightarrow M, S}{\neg S \& \neg P}.$$

$$19.23. \frac{\neg M \rightarrow \neg P, S \& M}{S \& \neg P}.$$

$$19.25. \frac{\neg M \rightarrow P, S \rightarrow \neg M}{\neg S \rightarrow \neg P}.$$

$$19.27. \frac{P \rightarrow \neg M, S \rightarrow M, \neg S}{S \& \neg P}.$$

$$19.29. \frac{\neg M \rightarrow \neg P, \neg M \rightarrow \neg S}{S \rightarrow \neg P}.$$

$$19.2. \frac{P \rightarrow \neg M, \neg M \rightarrow S, M}{\neg S \& \neg P}.$$

$$19.4. \frac{P \rightarrow M, \neg M \rightarrow S, \neg P}{\neg S \& P}.$$

$$19.6. \frac{\neg P \rightarrow M, M \rightarrow \neg S}{\neg S \rightarrow \neg P}.$$

$$19.8. \frac{\neg P \rightarrow M, \neg M \rightarrow \neg S, \neg P}{S \& P}.$$

$$19.10. \frac{\neg M \rightarrow P, M \rightarrow \neg S, \neg P}{\neg P \& S}.$$

$$19.12. \frac{M \rightarrow \neg P, \neg M \& S}{\neg S \rightarrow P}.$$

$$19.14. \frac{\neg M \& \neg P, \neg M \rightarrow S}{S \rightarrow \neg P}.$$

$$19.16. \frac{\neg P \rightarrow M, \neg S \rightarrow \neg M, S}{S \& \neg P}.$$

$$19.18. \frac{\neg P \rightarrow M, S \rightarrow \neg M}{\neg S \rightarrow \neg P}.$$

$$19.20. \frac{\neg P \rightarrow M, S \& \neg M}{\neg S \& \neg P}.$$

$$19.22. \frac{\neg M \rightarrow P, S \rightarrow \neg M, \neg S}{\neg S \& \neg P}.$$

$$19.24. \frac{\neg M \rightarrow \neg P, \neg S \rightarrow M}{\neg S \rightarrow \neg P}.$$

$$19.26. \frac{\neg M \rightarrow \neg P, M \rightarrow \neg S}{\neg S \rightarrow \neg P}.$$

$$19.28. \frac{\neg P \rightarrow \neg M, S \rightarrow \neg M, S}{S \& P}.$$

$$19.30. \frac{\neg M \rightarrow \neg P, \neg S \& \neg M}{S \& \neg P}.$$

**Пример.** Проверить правильность или неправильность правила вывода  
 $\frac{\neg M \rightarrow \neg P, \neg S \& \neg M}{S \& \neg P}$ , установив общезначимость соответствующей формулы.

*Решение.* Правило  $\frac{\neg M \rightarrow \neg P, \neg S \& \neg M}{S \& \neg P}$  верно  $\leftrightarrow$  формула

$F = (\neg M \rightarrow \neg P) \& (\neg S \& \neg M) \rightarrow (S \& \neg P)$  тождественно истинна.

$$1. F = F(M, P, S) = (\overline{M} \rightarrow \overline{P}) \& (\overline{S} \& \overline{M}) \rightarrow (S \& \overline{P}) =$$

$$(\overline{\overline{M}} \vee \overline{P})(\overline{S} \& \overline{M}) \vee S \& \overline{P} = \overline{M} \vee \overline{P} \vee \overline{S} \& \overline{M} \vee S \& \overline{P} = \overline{M} \overline{P} \vee \overline{S} \vee \overline{\overline{M}} \vee S \& \overline{P} =$$

$\overline{M} P \vee S \vee M \vee S \& \overline{P} = (\overline{M} \vee M)(P \vee M) \vee S = P \vee M \vee S \not\equiv 1$ . Правило вывода не верно.

2. Пусть  $F_1 = \neg M \rightarrow \neg P$ ,  $F_2 = \neg S \& \neg M$ ,  $F_3 = F_1 \& F_2$ ,  $F_4 = S \& \neg P$ .

Вычисления занесем в табл.10.16.

Таблица 10.16

	MPS	$F_1$	$F_2$	$F_3$	$F_4$	$F$
0	000	1	1	1	0	0
1	001	1	0	0	1	1
2	010	0	1	0	0	1
3	011	0	0	0	0	1
4	100	1	0	0	0	1
5	101	1	0	0	1	1
6	110	1	0	0	0	1
7	111	1	0	0	0	1

*Ответ.* Формула  $F$  тождественно истинной не является. Правило вывода не верно.

**Задача 20.** Установить правильность или неправильность правил вывода, используя естественный вывод Генцена. Задание взять из задачи 18.

**Пример.** Установить правильность или неправильность правило вывода

$$\text{ПВ} = \frac{x \rightarrow z}{(y \rightarrow z) \rightarrow (x \vee y \rightarrow z)}, \text{ используя естественный вывод Генцена.}$$

*Решение.* Правило вывода ПВ =  $\frac{x \rightarrow z}{(y \rightarrow z) \rightarrow (x \vee y \rightarrow z)}$  верно  $\leftrightarrow$

формула  $F = (x \rightarrow z) \rightarrow ((y \rightarrow z) \rightarrow (x \vee y \rightarrow z))$  тождественно истинна.

Построим для  $F$  дерево вывода (рис.10.7).

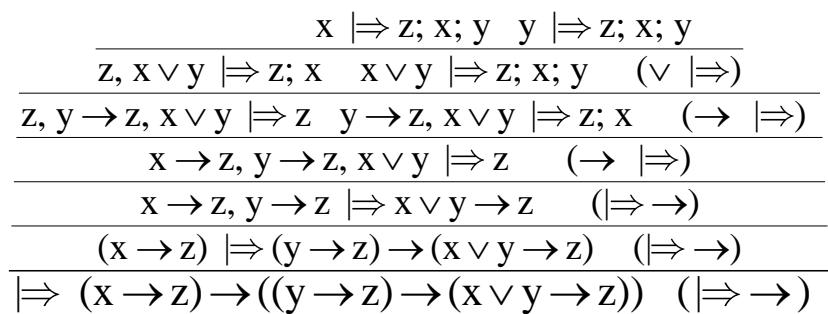


Рис.10.7

Все листья есть аксиомы. Правило вывода ПВ верно.

**Задача 21.** Установить правильность или неправильность правил вывода, используя естественный вывод Генцена. Задание взять из задачи 19.

**Задача 21.** Установить правильность или неправильность правил вывода  
 $\text{ПВ} = \frac{x \rightarrow y \vee z}{(y \rightarrow z) \rightarrow (x \vee y \rightarrow z)}$ , используя естественный вывод Генцена.

*Решение.* Правило вывода ПВ =  $\frac{x \rightarrow y \vee z}{(y \rightarrow z) \rightarrow (x \vee y \rightarrow z)}$  верно  $\leftrightarrow$  формула  $F$   
 $= (x \rightarrow y \vee z) \rightarrow ((y \rightarrow z) \rightarrow (x \vee y \rightarrow z))$  тождественно истинна. Построим для  $F$  дерево вывода (рис.10.8).

$$\begin{array}{c}
 \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{y, x \Rightarrow z; y \quad t, x \Rightarrow z; y}{y \vee t, x \Rightarrow z; y \quad x \Rightarrow z; y; x (\vee \Rightarrow)} \\ \dfrac{\dfrac{x \vee y, x \Rightarrow z; y \quad x \rightarrow y \vee t, y \Rightarrow z; y (\rightarrow \Rightarrow)}{y \rightarrow y \vee t, z, x \vee y \Rightarrow z \quad y \rightarrow y \vee t, x \vee y \Rightarrow z; y (\vee \Rightarrow)} \\ \dfrac{\dfrac{x \rightarrow y \vee t, y \rightarrow z, x \vee y \Rightarrow z}{x \rightarrow y \vee t, y \rightarrow z \Rightarrow x \vee y \rightarrow z (\Rightarrow \rightarrow)} \\ \dfrac{(x \rightarrow y \vee t) \Rightarrow (y \rightarrow z) \rightarrow (x \vee y \rightarrow z) (\Rightarrow \rightarrow)}{\Rightarrow (x \rightarrow y \vee t) \rightarrow ((y \rightarrow z) \rightarrow (x \vee y \rightarrow z)) (\Rightarrow \rightarrow)}}}}}}}}}
 \end{array}$$

Рис.10.8

Не все листья являются аксиомами. Правило вывода ПВ не верно.

**Задача 22.** Установить правильность или неправильность правил вывода, используя метод резолюций. Задание взять из задачи 18.

**Задача 23.** Установить правильность или неправильность правил вывода, используя метод резолюций. Задание взять из задачи 19.

**Задача 24.** Доказать или опровергнуть невыполнимость множества дизъюнктов  $S$  путем построения обрезанного семантического дерева и построить вывод пустого дизъюнкта из  $S$  в случае невыполнимости  $S$ .

- 24.1.  $p \vee q \vee r, p \vee q \vee r, \neg q \vee \neg r, q, r.$
- 24.2.  $p \vee q \vee r, p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.3.  $p \vee q \vee r, p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.4.  $p \vee q \vee r, \neg p \vee q \vee r, \neg q \vee \neg r, q, r.$
- 24.5.  $p \vee q \vee r, \neg p \vee q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.6.  $p \vee q \vee r, \neg p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.7.  $p \vee q \vee r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.8.  $p \vee q \vee \neg r, p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.9.  $p \vee q \vee \neg r, p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.10.  $p \vee q \vee \neg r, \neg p \vee q \vee r, \neg q \vee \neg r, q, r.$
- 24.11.  $p \vee q \vee \neg r, \neg p \vee q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.12.  $p \vee q \vee \neg r, \neg p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.13.  $p \vee q \vee \neg r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.14.  $p \vee \neg q \vee r, p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.15.  $\neg p \vee \neg q \vee \neg r, \neg p \vee q \vee r, \neg q \vee \neg r, q, r.$
- 24.16.  $\neg p \vee \neg q \vee \neg r, \neg p \vee q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.17.  $\neg p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.18.  $p \vee \neg q \vee r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$

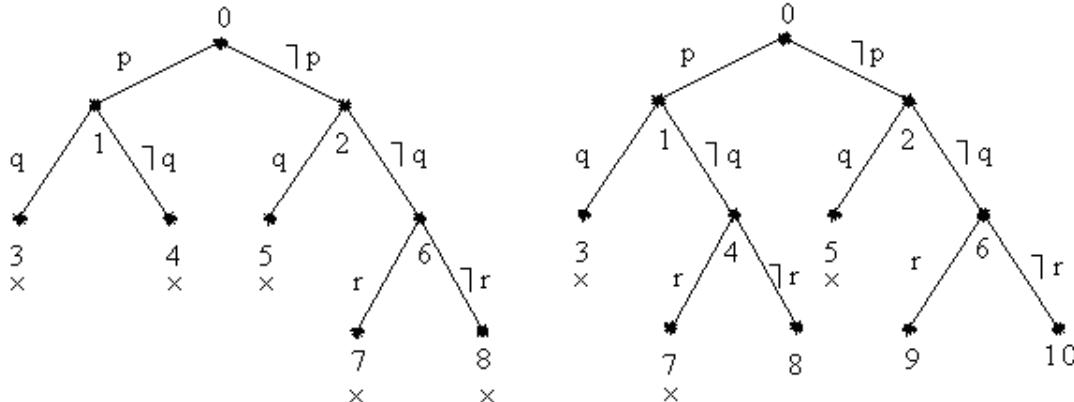
- 24.19.**  $p \vee \neg q \vee \neg r, \neg p \vee q \vee r, \neg q \vee \neg r, q, r.$
- 24.20.**  $p \vee \neg q \vee \neg r, \neg p \vee q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.21.**  $p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.22.**  $p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.23.**  $\neg p \vee q \vee r, \neg p \vee q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.24.**  $\neg p \vee q \vee r, \neg p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.25.**  $\neg p \vee q \vee r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.26.**  $\neg p \vee q \vee \neg r, \neg p \vee \neg q \vee r, \neg q \vee \neg r, q, r.$
- 24.27.**  $\neg p \vee q \vee \neg r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.28.**  $\neg p \vee \neg q \vee r, \neg p \vee \neg q \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.29.**  $p \vee q \vee r, \neg p \vee \neg r, \neg q \vee \neg r, q, r.$
- 24.30.**  $p \vee q \vee \neg r, \neg q \vee r, \neg q \vee \neg r, q, r.$

**Пример.** Доказать или опровергнуть невыполнимость множества дизъюнктов  $S$  путем построения замкнутого семантического дерева и построить вывод пустого дизъюнкта из  $S$  в случае невыполнимости  $S$ .

**Решение.** Множество дизъюнктов

$$S = \{p \vee q \vee r, p \vee q \vee \neg r, p \vee \neg q, \neg p \vee \neg q, \neg p \vee q\}.$$

Строим для  $S$  замкнутое семантическое дерево  $T$  (рис.10.9).



Все его концевые узлы опровергающие. Поэтому множество  $S$  невыполнимо. В узле 6 из дизъюнктов  $p \vee q \vee r, p \vee q \vee \neg r$  выводится  $p \vee q$ . В узле 2 из дизъюнктов  $p \vee \neg q, p \vee q$  выводится  $p$ . В узле 1 из  $\neg p \vee \neg q, \neg p \vee q$  выводится  $\neg p$ . В узле 0 из  $p$  и  $\neg p$  выводим  $p$ . Вывод пустого дизъюнкта из  $S$  имеет следующий вид:

- (1)  $p \vee q \vee r$ , из  $S$ ; (2)  $p \vee q \vee \neg r$ , из  $S$ ; (3)  $p \vee q$ , ПР(1,2);
- (4)  $p \vee \neg q$ , из  $S$ ; (5)  $p$ , ПР(3,4); (6)  $\neg p \vee \neg q$ , из  $S$ ;
- (7)  $\neg p \vee q$ , из  $S$ ; (8)  $\neg p$ , ПР(6,7); (9)  $p$ , ПР(5,8).

**Задача 25.** Доказать или опровергнуть невыполнимость множества дизъюнктов  $S$  путем построения обрезанного семантического дерева и построить вывод пустого дизъюнкта из  $S$  в случае невыполнимости  $S$ .

- 25.1.**  $\neg p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee r, \neg p \vee q \vee \neg r.$
- 25.2.**  $\neg p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee r, \neg p \vee q \vee r.$
- 25.3.**  $\neg p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee r, p \vee \neg q \vee \neg r.$
- 25.4.**  $\neg p \vee \neg q \vee \neg r, \neg p \vee \neg q \vee r, p \vee \neg q \vee r.$

- 25.5.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee \neg q \vee r$ ,  $p \vee q \vee \neg r$ .
- 25.6.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee \neg q \vee r$ ,  $p \vee q \vee r$ .
- 25.7.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee \neg r$ ,  $\neg p \vee q \vee r$ .
- 25.8.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee \neg r$ ,  $p \vee \neg q \vee \neg r$ .
- 25.9.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee \neg r$ ,  $p \vee \neg q \vee r$ .
- 25.10.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee \neg r$ ,  $\neg p \vee \neg q \vee r$ .
- 25.11.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee \neg r$ ,  $p \vee q \vee r$ .
- 25.12.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee r$ ,  $p \vee \neg q \vee \neg r$ .
- 25.13.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee r$ ,  $p \vee \neg q \vee r$ .
- 25.14.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee r$ ,  $p \vee q \vee \neg r$ .
- 25.15.**  $\neg p \vee \neg q \vee \neg r$ ,  $\neg p \vee q \vee r$ ,  $p \vee q \vee r$ .
- 25.16.**  $\neg p \vee \neg q \vee \neg r$ ,  $p \vee \neg q \vee \neg r$ ,  $p \vee \neg q \vee r$ .
- 25.17.**  $\neg p \vee \neg q \vee \neg r$ ,  $p \vee \neg q \vee \neg r$ ,  $p \vee q \vee \neg r$ .
- 25.18.**  $\neg p \vee \neg q \vee \neg r$ ,  $p \vee \neg q \vee \neg r$ ,  $p \vee q \vee r$ .
- 25.19.**  $\neg p \vee \neg q \vee \neg r$ ,  $p \vee \neg q \vee r$ ,  $p \vee q \vee \neg r$ .
- 25.20.**  $\neg p \vee \neg q \vee \neg r$ ,  $p \vee \neg q \vee r$ ,  $p \vee q \vee r$ .
- 25.21.**  $\neg p \vee \neg q \vee \neg r$ ,  $p \vee q \vee \neg r$ ,  $p \vee q \vee r$ .
- 25.22.**  $\neg p \vee \neg q \vee r$ ,  $\neg p \vee q \vee \neg r$ ,  $\neg p \vee q \vee r$ .
- 25.23.**  $\neg p \vee \neg q \vee r$ ,  $p \vee q \vee r$ ,  $p \vee \neg q \vee \neg r$ .
- 25.24.**  $\neg p \vee \neg q \vee r$ ,  $p \vee q \vee r$ ,  $p \vee \neg q \vee r$ .
- 25.25.**  $\neg p \vee \neg q \vee r$ ,  $p \vee q \vee r$ ,  $p \vee \neg q \vee \neg r$ .
- 25.26.**  $\neg p \vee \neg q \vee r$ ,  $\neg p \vee q \vee \neg r$ ,  $p \vee q \vee r$ .
- 25.27.**  $\neg p \vee \neg q \vee r$ ,  $\neg p \vee q \vee r$ ,  $p \vee \neg q \vee \neg r$ .
- 25.28.**  $\neg p \vee \neg q \vee r$ ,  $\neg p \vee q \vee r$ ,  $p \vee \neg q \vee r$ .
- 25.29.**  $\neg p \vee \neg q \vee r$ ,  $p \vee q \vee r$ ,  $p \vee q \vee \neg r$ .
- 25.30.**  $\neg p \vee \neg q \vee r$ ,  $\neg p \vee q \vee r$ ,  $p \vee q \vee r$ .

**Пример.** Доказать или опровергнуть невыполнимость множества дизъюнктов  $S$  путем построения замкнутого семантического дерева и построить вывод пустого дизъюнкта из  $S$  в случае невыполнимости  $S$ .

**Решение.** Множество дизъюнктов  $S = \{\neg p \vee \neg q, \neg p \vee q \vee \neg r, p \vee \neg q\}$ . Строим для  $S$  замкнутое семантическое дерево  $T$  (рис.10.10). Не все его концевые узлы опровергающие (узлы 8,9,10). Поэтому множество дизъюнктов  $S$  невыполнимым не является, и потому пустой дизъюнкт из  $S$  не выводится.

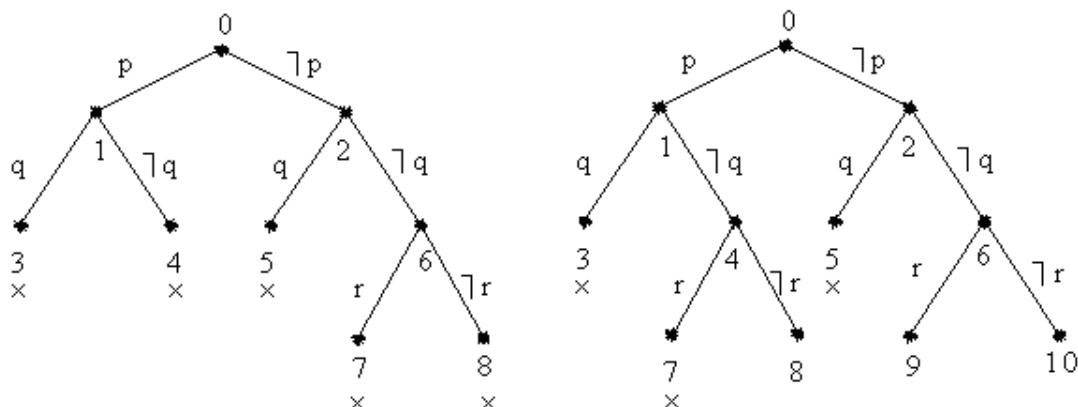


Рис.10.9

**Задача 26.** Доказать правильность правил вывода, установив общезначимость соответствующей формулы.

$$26.1. \frac{(\forall x)(P(x) \rightarrow \neg M(x)), (\exists x)(S(x) \& M(x))}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.2. \frac{(\forall x)(P(x) \rightarrow \neg M(x)), (\forall x)(M(x) \rightarrow S(x)), (\exists x)M(x)}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.3. \frac{(\forall x)(M(x) \rightarrow P(x)), (\exists x)(S(x) \& M(x))}{(\exists x)(S(x) \& P(x))}.$$

$$26.4. \frac{(\forall x)(P(x) \rightarrow M(x)), (\forall x)(M(x) \rightarrow S(x)), (\exists x)P(x)}{(\exists x)(S(x) \& P(x))}.$$

$$26.5. \frac{(\forall x)(P(x) \rightarrow \neg M(x)), (\exists x)(M(x) \& S(x))}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.6. \frac{(\forall x)(P(x) \rightarrow M(x)), (\forall x)(M(x) \rightarrow \neg S(x))}{(\forall x)(S(x) \rightarrow \neg P(x))}.$$

$$26.7. \frac{(\exists x)(P(x) \& M(x)), (\forall x)(M(x) \rightarrow S(x))}{(\exists x)(S(x) \& P(x))}.$$

$$26.8. \frac{(\forall x)(P(x) \rightarrow M(x)), (\forall x)(M(x) \rightarrow \neg S(x)), (\exists x)S(x)}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.9. \frac{(\forall x)(M(x) \rightarrow \neg P(x)), (\forall x)(M(x) \rightarrow S(x)), (\exists x)M(x)}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.10. \frac{(\forall x)(M(x) \rightarrow P(x)), (\forall x)(M(x) \rightarrow S(x)), (\exists x)M(x)}{(\exists x)(P(x) \& S(x))}.$$

$$26.11. \frac{(\forall x)(M(x) \rightarrow \neg P(x)), (\exists x)(M(x) \& S(x))}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.12. \frac{(\forall x)(M(x) \rightarrow P(x)), (\exists x)(M(x) \& S(x))}{(\exists x)(S(x) \rightarrow P(x))}.$$

$$26.13. \frac{(\exists x)(M(x) \& P(x)), (\forall x)(M(x) \rightarrow S(x))}{(\exists x)(S(x) \& P(x))}.$$

$$26.14. \frac{(\exists x)(M(x) \& \neg P(x)), (\forall x)(M(x) \rightarrow S(x))}{(\exists x)(S(x) \rightarrow \neg P(x))}.$$

$$26.15. \frac{(\forall x)(P(x) \rightarrow \neg M(x)), (\forall x)(S(x) \& M(x)), (\exists x)S(x)}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.16. \frac{(\forall x)(P(x) \rightarrow M(x)), (\forall x)(S(x) \rightarrow \neg M(x)), (\exists x)S(x)}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.17. \frac{(\forall x)(P(x) \rightarrow \neg M(x)), (\exists x)(S(x) \rightarrow M(x))}{(\exists x)(S(x) \& \neg P(x))}.$$

$$26.18. \frac{(\forall x)(P(x) \rightarrow M(x)), (\forall x)(S(x) \rightarrow \neg M(x))}{(\forall x)(S(x) \rightarrow \neg P(x))}.$$

Рис.10.10

- 26.19.**  $\frac{(\forall x)(P(x) \rightarrow \neg M(x)), (\forall x)(S(x) \rightarrow M(x))}{(\forall x)(S(x) \rightarrow \neg P(x))}.$
- 26.20.**  $\frac{(\forall x)(P(x) \rightarrow M(x)), (\exists x)(S(x) \& \neg M(x))}{(\exists x)(S(x) \& \neg P(x))}.$
- 26.21.**  $\frac{(\forall x)(M(x) \rightarrow \neg P(x)), (\forall x)(S(x) \rightarrow M(x)), (\exists x)S(x)}{(\exists x)(S(x) \& \neg P(x))}.$
- 26.22.**  $\frac{(\forall x)(M(x) \rightarrow P(x)), (\forall x)(S(x) \rightarrow M(x)), (\exists x)S(x)}{(\exists x)(S(x) \& P(x))}.$
- 26.23.**  $\frac{(\forall x)(M(x) \rightarrow P(x)), (\exists x)(S(x) \& M(x))}{(\exists x)(S(x) \& P(x))}.$
- 26.24.**  $\frac{(\forall x)(M(x) \rightarrow \neg P(x)), (\forall x)(S(x) \rightarrow M(x))}{(\forall x)(S(x) \rightarrow \neg P(x))}.$
- 26.25.**  $\frac{(\forall x)(M(x) \rightarrow P(x)), (\forall x)(S(x) \rightarrow M(x))}{(\forall x)(S(x) \rightarrow P(x))}.$
- 26.26.**  $\frac{(\forall x)(\neg M(x) \rightarrow \neg P(x)), (\forall x)(M(x) \rightarrow \neg S(x))}{(\forall x)(S(x) \rightarrow \neg P(x))}.$
- 26.27.**  $\frac{(\forall x)(\neg P(x) \rightarrow \neg M(x)), (\forall x)(S(x) \rightarrow M(x)), (\exists x)S(x)}{(\exists x)(S(x) \& P(x))}.$
- 26.28.**  $\frac{(\forall x)(\neg P(x) \rightarrow \neg M(x)), (\forall x)(S(x) \rightarrow M(x)), (\exists x)S(x)}{(\exists x)(S(x) \& P(x))}.$
- 26.29.**  $\frac{(\forall x)(M(x) \rightarrow \neg P(x)), (\forall x)(\neg M(x) \rightarrow \neg S(x))}{(\forall x)(S(x) \rightarrow \neg P(x))}.$
- 26.30.**  $\frac{(\forall x)(\neg M(x) \rightarrow \neg P(x)), (\exists x)(S(x) \& \neg M(x))}{(\exists x)(S(x) \& \neg P(x))}.$

**Задача 26.** Доказать правильность правил вывода, установив общезначимость соответствующей формулы.

*Решение.* а1.  $\frac{(\forall x)(S(x) \rightarrow \overline{\overline{P(x)}})}{(\exists x)(S(x) \& P(x))}. A = A(P,S) =$

$$\begin{aligned} & (\forall x)(S(x) \rightarrow \overline{\overline{P(x)}}) \rightarrow (\exists x)(S(x) \& P(x)) = \\ & \overline{(\forall x)(S(x) \rightarrow \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& P(x)) = \overline{(\forall x)(\overline{\overline{S(x)}} \vee \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& P(x)) = \\ & \overline{(\exists x)(\overline{\overline{S(x)}} \vee \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& P(x)) = \overline{(\exists x)(\overline{\overline{S(x)}} \& \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& P(x)) = \\ & \overline{(\exists x)(S(x) \& P(x))} \vee (\exists x)(S(x) \& P(x)) \equiv 1. \text{ Правило верно.} \end{aligned}$$

а2.  $\frac{(\forall x)(S(x) \rightarrow \overline{\overline{P(x)}})}{(\exists x)(S(x) \& \overline{\overline{P(x)}})}. A = A(P,S) = \overline{(\forall x)(S(x) \rightarrow \overline{\overline{P(x)}})} \rightarrow (\exists x)(S(x) \& \overline{\overline{P(x)}}) =$

$$\begin{aligned} & \overline{(\forall x)(\overline{\overline{S(x)}} \vee \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& \overline{\overline{P(x)}}) = \overline{(\exists x)(\overline{\overline{S(x)}} \& \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& \overline{\overline{P(x)}}) = \\ & \overline{(\exists x)(S(x) \& \overline{\overline{P(x)}})} \vee (\exists x)(S(x) \& \overline{\overline{P(x)}}) \equiv 1. \text{ Правило верно.} \end{aligned}$$

$$a3. \frac{(\forall x)(S(x) \rightarrow P(x))}{(\exists x)(S(x) \& \overline{P(x)})}. A = A(P, S) = (\forall x)(S(x) \rightarrow P(x)) \rightarrow \overline{(\exists x)(S(x) \& \overline{P(x)})} =$$

$$\overline{(\forall x)(S(x) \rightarrow P(x))} \vee \overline{(\exists x)(S(x) \& \overline{P(x)})} = (\exists x) \overline{\overline{S(x)} \vee P(x)} \vee \overline{(\exists x)(S(x) \& \overline{P(x)})} = \\ (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{(\exists x)(S(x) \& \overline{P(x)})} \equiv 1. \text{ Правило верно.}$$

$$a4. \frac{(\forall x)(S(x) \rightarrow \overline{P(x)})}{(\exists x)(S(x) \& P(x))}. A = A(P, S) = (\forall x)(S(x) \rightarrow \overline{P(x)}) \rightarrow \overline{(\exists x)(S(x) \& P(x))} =$$

$$\overline{(\forall x)(S(x) \rightarrow \overline{P(x)})} \vee \overline{(\exists x)(S(x) \& P(x))} = (\exists x) \overline{\overline{S(x)} \vee \overline{P(x)}} \vee \overline{(\exists x)(S(x) \& P(x))} = \\ (\exists x) \overline{\overline{S(x)} \& \overline{P(x)}} \vee \overline{(\exists x)(S(x) \& P(x))} = (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{(\exists x)(S(x) \& P(x))} \equiv 1.$$

Правило верно.

$$a5. \frac{(\forall x)(S(x) \rightarrow P(x)), (\exists x)S(x)}{(\exists x)(S(x) \& P(x))}. A = A(P, S) =$$

$$(\forall x)(S(x) \rightarrow P(x)) \& (\exists x)S(x) \rightarrow (\exists x)(S(x) \& P(x)) =$$

$$\overline{(\forall x)(\overline{S(x)} \vee P(x))} \& (\exists x)S(x) \vee (\exists x)(S(x) \& P(x)) =$$

$$(\exists x) \overline{(\overline{S(x)} \vee P(x))} \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& P(x)) =$$

$$(\exists x)(S(x) \& \overline{P(x)}) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& P(x)) =$$

$$(\exists x)(S(x) \& \overline{P(x)}) \vee (\exists x)(S(x) \& P(x)) \vee \overline{(\exists x)S(x)} =$$

$$(\exists x)(S(x) \& \overline{P(x)}) \vee (\exists x)(S(x) \& P(x)) \vee \overline{(\exists x)S(x)} =$$

$$(\exists x)(S(x) \& \overline{P(x)}) \vee (S(x) \& P(x)) \vee \overline{(\exists x)S(x)} =$$

$$(\exists x)(S(x) \& (\overline{P(x)} \vee P(x))) \vee \overline{(\exists x)S(x)} = (\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1.$$

Правило верно.

$$a6. \frac{(\forall x)(S(x) \rightarrow P(x)), (\exists x)S(x)}{(\forall x)(S(x) \rightarrow \overline{P(x)})}. A = A(P, S) =$$

$$(\forall x)(S(x) \rightarrow P(x)) \& (\exists x)S(x) \rightarrow \overline{(\forall x)(S(x) \rightarrow \overline{P(x)})} =$$

$$\overline{(\forall x)(\overline{S(x)} \vee P(x))} \& (\exists x)S(x) \vee \overline{(\forall x)(S(x) \rightarrow \overline{P(x)})} =$$

$$\overline{(\forall x)(\overline{S(x)} \vee P(x))} \vee \overline{(\exists x)S(x)} \vee (\exists x) \overline{\overline{S(x)} \vee \overline{P(x)}} =$$

$$(\exists x)(S(x) \& \overline{P(x)}) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& P(x)) =$$

$$(\exists x)(S(x) (\overline{P(x)} \vee P(x))) \vee \overline{(\exists x)S(x)} = (\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1.$$

Правило верно.

$$a7. \frac{(\exists x)(S(x) \& P(x)), (\exists x)S(x)}{(\exists x)(S(x) \& \overline{P(x)})}. A = A(P, S) =$$

$$\overline{(\exists x)(S(x) \& P(x))} \& (\exists x)S(x) \rightarrow (\exists x)(S(x) \& \overline{P(x)}) =$$

$$\overline{(\exists x)(S(x) \& P(x))} \& (\exists x) \overline{S(x)} \vee (\exists x)(S(x) \& \overline{P(x)}) =$$

$$\overline{(\exists x)(S(x) \& P(x))} \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& \overline{P(x)}) =$$

$$(\exists x)(S(x) \& P(x)) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& \overline{P(x)}) =$$

$$(\exists x)(S(x)(P(x) \vee \overline{P(x)})) \vee \overline{(\exists x)S(x)} = (\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1.$$

Правило верно.

$$\text{a8. } \frac{(\forall x)(S(x) \rightarrow \overline{P(x)}), (\exists x)S(x)}{(\exists x)(S(x) \& \overline{P(x)})}. A = A(P, S) =$$

$$\begin{aligned} & (\forall x)(S(x) \rightarrow \overline{P(x)}) \& (\exists x)S(x) \rightarrow (\exists x)(S(x) \& \overline{P(x)}) = \\ & \overline{(\forall x)(\overline{S(x)} \vee \overline{P(x)}) \& (\exists x)S(x)} \vee (\exists x)(S(x) \& \overline{P(x)}) = \\ & (\exists x)\overline{(\overline{S(x)} \vee \overline{P(x)})} \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& \overline{P(x)}) = \\ & (\exists x)(S(x) \& P(x)) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x) \& \overline{P(x)}) = \\ & (\exists x)(S(x)(P(x) \vee \overline{P(x)})) \vee \overline{(\exists x)S(x)} = (\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1. \end{aligned}$$

Правило верно.

$$\text{a9. } \frac{(\forall x)(M(x) \rightarrow \overline{P(x)}), (\forall x)(S(x) \rightarrow M(x))}{(\forall x)(S(x) \rightarrow \overline{P(x)})}. A = A(M, P, S) =$$

$$\begin{aligned} & (\forall x)(M(x) \rightarrow \overline{P(x)}) \& (\forall x)(S(x) \rightarrow M(x)) \rightarrow (\forall x)(S(x) \rightarrow \overline{P(x)}) = \\ & \frac{1 \quad \quad \quad 2 \quad \quad \quad 3}{1 \& 2 \rightarrow 3 = \overline{1 \& 2} \vee 3 = \overline{\overline{1} \vee \overline{2}} \vee 3 =} \\ & \overline{(\forall x)(M(x) \rightarrow \overline{P(x)}) \& (\forall x)(S(x) \rightarrow M(x))} \vee (\forall x)(\overline{S(x)} \vee \overline{P(x)}) = \\ & \overline{(\forall x)(\overline{M(x)} \vee \overline{P(x)})} \vee \overline{(\forall x)(\overline{S(x)} \vee M(x))} \vee \overline{(\exists x)S(x) \& P(x)} = \\ & \frac{4}{(\exists x)(\overline{\overline{M(x)}} \& \overline{\overline{P(x)}}) \vee (\exists x)(\overline{\overline{S(x)}} \vee M(x)) \vee (\exists x)S(x) \& P(x)} = \\ & (\exists x)(\overline{\overline{M(x)}} \& \overline{\overline{P(x)}}) \vee (\exists x)(\overline{\overline{S(x)}} \vee M(x)) \vee 4 = \\ & (\exists x)(M(x) \& P(x)) \vee (\exists x)(S(x) \& \overline{M(x)}) \vee 4 = (\exists x)(M(x) \& P(x) \vee S(x) \& \overline{M(x)}) \vee 4 = \\ & (\exists x)(M \& P \vee S \& \overline{M}) \vee 4 = (\exists x)((M \vee S) \& (M \vee \overline{M}) \& (P \vee S) \& (P \vee \overline{M})) \vee 4 = \\ & (\exists x)((M \vee S) \& (P \vee S) \& (P \vee \overline{M})) \vee 4 = \\ & (\exists x)((MP \vee MS \vee PS \vee S) \& (P \vee \overline{M})) \vee 4 = (\exists x)((MP \vee S) \& (P \vee \overline{M})) \vee 4 = \\ & (\exists x)((MP \vee MP\overline{M} \vee SP \vee S\overline{M})) \vee 4 = (\exists x)((MP \vee SP \vee S\overline{M})) \vee 4 = \\ & (\exists x)MP \vee (\exists x)SP \vee (\exists x)S\overline{M} \vee 4 = \\ & (\exists x)(M(x) \& P(x)) \vee (\exists x)(S(x) \& (P(x))) \vee (\exists x)(S(x) \& \overline{M(x)}) \vee (\exists x)S(x) \& P(x) \equiv 1. \end{aligned}$$

Правило верно.

$$\text{a10. } \frac{(\forall x)(M(x) \rightarrow \overline{P(x)}), (\exists x)(S(x) \& M(x))}{(\exists x)(S(x) \& \overline{P(x)})}. A = A(M, P, S) =$$

$$\begin{aligned} & (\forall x)(M(x) \rightarrow \overline{P(x)}) \& (\exists x)(S(x) \& M(x)) \rightarrow (\exists x)(S(x) \& \overline{P(x)}) = \\ & \frac{1 \quad \quad \quad 2 \quad \quad \quad 3}{1 \& 2 \rightarrow 3 = \overline{1 \& 2} \vee 3 = \overline{\overline{1} \vee \overline{2}} \vee 3 =} \end{aligned}$$

$$\begin{aligned} & \overline{(\forall x)(M(x) \rightarrow \overline{P(x)})} \vee \overline{(\exists x)(S(x) \& M(x))} \vee (\exists x)(S(x) \& \overline{P(x)}) = \\ & \frac{4}{(\forall x)(\overline{M(x)} \vee \overline{P(x)}) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee 4 =} \\ & (\exists x)(\overline{\overline{M(x)}} \vee \overline{\overline{P(x)}}) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee 4 = \\ & (\exists x)(\overline{\overline{M(x)}} \& \overline{\overline{P(x)}}) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee 4 = \end{aligned}$$

$$\begin{aligned}
& (\exists x)(M(x) \& P(x)) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee 4 = \\
& (\exists x)(M(x) \& P(x) \vee S(x) \& \overline{P(x)}) \vee 4 = (\exists x)(M \& P \vee S \& \overline{P}) \vee 4 = \\
& (\exists x)((M \vee S) \& (M \vee \overline{P}) \& (P \vee S) \& (P \vee \overline{P})) \vee 4 = \\
& (\exists x)((M \vee S) \& (M \vee \overline{P}) \& (P \vee S)) \vee 4 = \\
& (\exists x)((M \vee M\overline{P}) \vee MS \vee \overline{P}S) \& (P \vee S) \vee 4 = \\
& (\exists x)((M \vee \overline{P}S) \& (P \vee S)) \vee 4 = (\exists x)(MP \vee MS \vee \overline{P}SP \vee \overline{P}S) \vee 4 = \\
& (\exists x)(MP \vee MS \vee \overline{P}S) \vee 4 = (\exists x)MP \vee (\exists x)MS \vee (\exists x)\overline{P}S \vee 4 = \\
& (\exists x)(M(x) \& P(x)) \vee (\exists x)(S(x) \& M(x)) \vee (\exists x)(\overline{P(x)} \& S(x)) \vee \overline{(\exists x)(S(x) \& M(x))} \equiv 1.
\end{aligned}$$

Правило верно.

$$\text{a11. } \frac{(\forall x)(M(x) \rightarrow \overline{P(x)}), (\forall x)(M(x) \rightarrow S(x)), (\exists x)M(x)}{(\exists x)(S(x) \& \overline{P(x)})}. A = A(M, P, S) =$$

$$\begin{aligned}
& (\forall x)(M(x) \rightarrow \overline{P(x)}) \& (\forall x)(M(x) \rightarrow S(x)) \& (\exists x)M(x) \rightarrow (\exists x)(S(x) \& \overline{P(x)}) = \\
& 1 \quad \quad \quad 2 \quad \quad \quad 3 \quad \quad \quad 4 \\
& 1 \& 2 \& 3 \rightarrow 4 = \overline{1 \& 2 \& 3} \vee 4 = \overline{\overline{1}} \vee \overline{\overline{2}} \vee \overline{\overline{3}} \vee 4 = \overline{\overline{1}} \vee \overline{\overline{2}} \vee 4 \vee \overline{\overline{3}} =
\end{aligned}$$

$$\begin{aligned}
& \overline{(\forall x)(M(x) \rightarrow \overline{P(x)})} \vee \overline{(\forall x)(M(x) \rightarrow S(x))} \vee (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{(\exists x)M(x)} = \\
& \overline{\overline{1}} \quad \quad \quad \overline{\overline{2}} \quad \quad \quad 4 \quad \quad \quad \overline{\overline{3}} \\
& (\exists x)(\overline{\overline{M(x)}} \vee \overline{\overline{P(x)}}) \vee (\exists x)(\overline{\overline{M(x)}} \vee \overline{\overline{S(x)}}) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{\overline{3}} = \\
& (\exists x)(\overline{\overline{M(x)}} \& (\overline{\overline{P(x)}}) \vee (\exists x)(\overline{\overline{M(x)}} \& \overline{\overline{S(x)}}) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{\overline{3}} = \\
& (\exists x)(M(x) \& P(x) \vee (\exists x)(M(x) \& \overline{S(x)}) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{\overline{3}} = \\
& (\exists x)(M(x) \& P(x) \vee M(x) \& \overline{S(x)} \vee S(x) \& \overline{P(x)}) \vee \overline{\overline{3}} = (\exists x)(MP \vee M\overline{S} \vee S\overline{P}) \vee \overline{\overline{3}} = \\
& (\exists x)(MP \vee (M \vee S)(M \vee \overline{P})(\overline{S} \vee S)(\overline{S} \vee \overline{P})) \vee \overline{\overline{3}} = \\
& (\exists x)(MP \vee (M \vee S)(M \vee \overline{P})(\overline{S} \vee \overline{P})) \vee \overline{\overline{3}} = \\
& \text{умножить} \\
& (\exists x)(MP \vee (M \vee M\overline{P} \vee SM \vee S\overline{P})(\overline{S} \vee \overline{P})) \vee \overline{\overline{3}} = \\
& (\exists x)(MP \vee (M \vee S\overline{P})(\overline{S} \vee \overline{P})) \vee \overline{\overline{3}} = \\
& (\exists x)(MP \vee M\overline{S} \vee M\overline{P} \vee S\overline{P} \vee \overline{S}\overline{P}) \vee \overline{\overline{3}} = \\
& (\exists x)(M(P \vee \overline{P}) \vee M\overline{S} \vee S\overline{P}) \vee \overline{\overline{3}} = (\exists x)(M \vee M\overline{S} \vee S\overline{P}) \vee \overline{\overline{3}} = \\
& (\exists x)(M \vee S\overline{P}) \vee \overline{\overline{3}} = (\exists x)M \vee (\exists x)(S\overline{P}) \vee \overline{\overline{3}} = \\
& (\exists x)M(x) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee \overline{(\exists x)M(x)} \equiv 1. \text{ Правило верно.}
\end{aligned}$$

**Задача 27.** Доказать справедливость правил вывода, используя естественный вывод Генцена. Задание взять из задачи 26.

**Пример.** Доказать справедливость правил вывода, используя естественный вывод Генцена. Задание взять из задачи 26.

*Решение.* Правило вывода ПВ верно  $\leftrightarrow$  формула

$F = (\exists x)(P(a) \rightarrow Q(x)) \rightarrow (P(a) \rightarrow (\exists x)Q(x))$  общезначима.

Докажем в СИП формулу  $F$ .

Доказательство формулы  $F$  оформим в виде дерева, рассуждая при этом так же, как это делали в случае вывода формул в СИВ (рис.10.11):

$Q(b), P(a) \Rightarrow Q(b); (\exists x)Q(x)$
$Q(b), P(a) \Rightarrow (\exists x)Q(x) \quad P(a) \Rightarrow (\exists x)Q(x); P(a) \Rightarrow \exists$
$P(a) \rightarrow Q(b), P(a) \Rightarrow (\exists x)Q(x) \quad (\rightarrow \Rightarrow)$
$(\exists x)(P(a) \rightarrow Q(x)), P(a) \Rightarrow (\exists x)Q(x) \quad (\exists \Rightarrow)$
$(\exists x)(P(a) \rightarrow Q(x)) \Rightarrow P(a) \rightarrow (\exists x)Q(x) \quad (\Rightarrow \rightarrow)$
$\Rightarrow (\exists x)(P(a) \rightarrow Q(x)) \rightarrow (P(a) \rightarrow (\exists x)Q(x)) \quad (\Rightarrow \rightarrow)$

Рис.10.11

Прокомментируем этот вывод для правил, связанных с кванторами. В секвенции  $(\exists x)(P(a) \rightarrow Q(x))$ ,  $P(a) \Rightarrow (\exists x)Q(x)$  формула  $(\exists x)(P(a) \rightarrow Q(x))$  истинна, если существует  $x$ , например, равный предмету  $b$ , отличному от всех ранее встречавшихся предметов, для которого формула  $P(a) \rightarrow Q(b)$  истинна. Переходим к секвенции  $P(a) \rightarrow Q(b)$ ,  $P(a) \Rightarrow (\exists x)Q(x)$ . В секвенции  $Q(b), P(a) \Rightarrow (\exists x)Q(x)$  формула  $(\exists x)Q(x)$  ложна, если формула  $\neg(\exists x)Q(x)$  истинна, т.е. для всякого  $x$ , в том числе и для  $x$ , равного  $b$ , формула  $Q(b)$  ложна. От секвенции  $Q(b), P(a) \Rightarrow (\exists x)Q(x)$  переходим к секвенции  $Q(b), P(a) \Rightarrow Q(b); (\exists x)Q(x)$ , которая является аксиомой. В построенном дереве все листья есть аксиомы. Потому исходная формула (являясь общезначимой) доказуема в СИП, откуда следует ее общезначимость и верность правила вывода ПВ.

**Задача 28.** Доказать справедливость правил вывода путем построения обрезанного семантического дерева (указав сначала префиксную и скулемову формы соответствующей формулы, эрбранов универсум и эрбранов базис). Задание взять из задачи 26.

**Задача 29.** Доказать справедливость правил вывода путем нахождения опровергающего множества основных примеров (указав сначала префиксную и скулемову формы соответствующей формулы, эрбранов универсум и эрбранов базис). Задание взять из задачи 26.

**Задача 30.** Задание взять из задачи 26. Доказать справедливость правил вывода методом резолюций, для чего выполнить следующее.

- Построить формулу  $A$ , для которой правило вывода верно  $\leftrightarrow$  формула  $A$  общезначима  $\leftrightarrow$  формула  $\neg A$  невыполнима.
- Найти префиксную нормальную форму для формулы  $A$ .
- Найти префиксную нормальную форму для формулы  $\neg A$ .
- Найти стандартную форму Скулема для формулы  $\neg A$ .
- Указать множество дизъюнктов  $S$  для формулы  $\neg A$ .
- Написать эрбрановский универсум  $H$  для  $S$ .
- Написать эрбрановский базис  $B$  для  $S$ .
- Указать множество основных примеров дизъюнктов из  $S$ .
- Построить обрезанное семантическое дерево для  $S$  и сделать вывод о верности данного правила вывода.

к. Найти (конечное) множество основных примеров, опровергающих каждую  $H$ -интерпретацию, а потому и все интерпретации множества дизъюнктов  $S$ . Сделать вывод о верности данного правила вывода.

*Решение.* Правило вывода

$$\text{а. ПВ} = \frac{(\forall x)(\overline{P(x)} \rightarrow \overline{M(x)}), (\forall x)(\overline{M(x)} \rightarrow \overline{S(x)}), (\exists x)S(x)}{(\exists x)(S(x) \& P(x))} \text{ верно} \leftrightarrow$$

формула  $A = A(M, P, S) =$

$$(\forall x)(\overline{P(x)} \rightarrow \overline{M(x)}) \& (\forall x)(\overline{M(x)} \rightarrow \overline{S(x)}) \& (\exists x)S(x) \rightarrow (\exists x)(S(x) \& P(x))$$

общезначима  $\leftrightarrow$  формула  $\neg A = \neg A(M, P, S)$  невыполнима.

Формула  $A = A(M, P, S) =$

$$(\forall x)(\overline{P(x)} \rightarrow \overline{M(x)}) \& (\forall x)(\overline{M(x)} \rightarrow \overline{S(x)}) \& (\exists x)S(x) \rightarrow (\exists x)(S(x) \& P(x)) \equiv 1.$$

**б.** Приведем формулу  $A$  к префиксной нормальной форме. Формула  $A =$

$$(\forall x)(P(x) \vee \overline{M(x)}) \& (\forall x)(M(x) \vee \overline{S(x)}) \& (\exists x)S(x) \vee (\exists x)(S(x) \& P(x)) =$$

$$(\exists x)(\overline{P(x)} \& M(x)) \vee (\exists x)(\overline{M(x)} \& S(x)) \vee (\forall x)\overline{S(x)} \vee (\exists x)(S(x) \& P(x)) =$$

$$(\exists x)(\forall y)(\overline{P(x)} \& M(x) \vee \overline{M(x)} \& S(x) \vee \overline{S(y)} \vee S(x) \& P(x)).$$

**в.** Префиксная нормальная форма формулы  $\neg A =$

$$(\forall x)(\exists y)(\overline{P(x)} \& M(x) \vee \overline{M(x)} \& S(x) \vee \overline{S(y)} \vee S(x) \& P(x))$$

$$(\forall x)(\exists y)((\overline{\overline{P(x)}} \vee \overline{M(x)}) \& (\overline{M(x)} \vee \overline{S(x)}) \& \overline{S(y)} \& (\overline{S(x)} \vee \overline{P(x)})) =$$

$$(\forall x)(\exists y)((P(x) \vee \overline{M(x)}) \& (M(x) \vee \overline{S(x)}) \& S(y) \& (\overline{S(x)} \vee \overline{P(x)})).$$

**г.** Стандартная форма Сколема формулы  $\neg A =$

$$(\forall x)((P(x) \vee \overline{M(x)}) \& (M(x) \vee \overline{S(x)}) \& S(f(x)) \& (\overline{S(x)} \vee \overline{P(x)}))$$

**д.** Множество дизъюнктов формулы  $\neg A$  есть множество

$$D = \{C_1 = S(f(x)), C_2 = \overline{M(x)} \vee P(x), C_3 = M(x) \vee \overline{S(x)}, C_4 = \overline{P(x)} \vee \overline{S(x)}\}.$$

**е.** Множество  $\{a, f\}$  составит материал (множество символов) для построения эрбранова универсума. Эрбранов универсум множества дизъюнктов  $D$  есть множество

$$H = \{a, fa = f(a), ffa = f(f(a)), fffa = f(f(f(a))), \dots\}.$$

**ж.** Множество  $\{a, f, M, P, S\}$  составит материал (множество символов) для построения эрбранова базиса.

Эрбранов базис множества дизъюнктов  $S$  есть множество

$$B = \{M(t), P(t), S(t) : t \text{ пробегает элементы эрбранова универсума } H\} =$$

$$\{A_1 = S(fa), A_2 = M(a), A_3 = P(a), A_4 = S(a), A_5 = S(ffa), A_6 = M(fa),$$

$$A_7 = P(fa), A_8 = M(ffa), A_9 = P(ffa), \dots\}.$$

**з.** Множество основных примеров дизъюнктов из  $D$  состоит из следующих множеств.

$$\{S(f(t)) : t \text{ пробегает элементы эрбранова универсума } H\}.$$

$$\{\overline{M(t)} \vee P(t) : t \text{ пробегает элементы эрбранова универсума } H\}.$$

$$\{M(t) \vee \overline{S(t)} : t \text{ пробегает элементы эрбранова универсума } H\}.$$

$$\{\overline{P(t)} \vee \overline{S(t)} : t \text{ пробегает элементы эрбранова универсума } H\}.$$

и. Строим замкнутое семантическое дерево для  $D$  (рис.10.12).

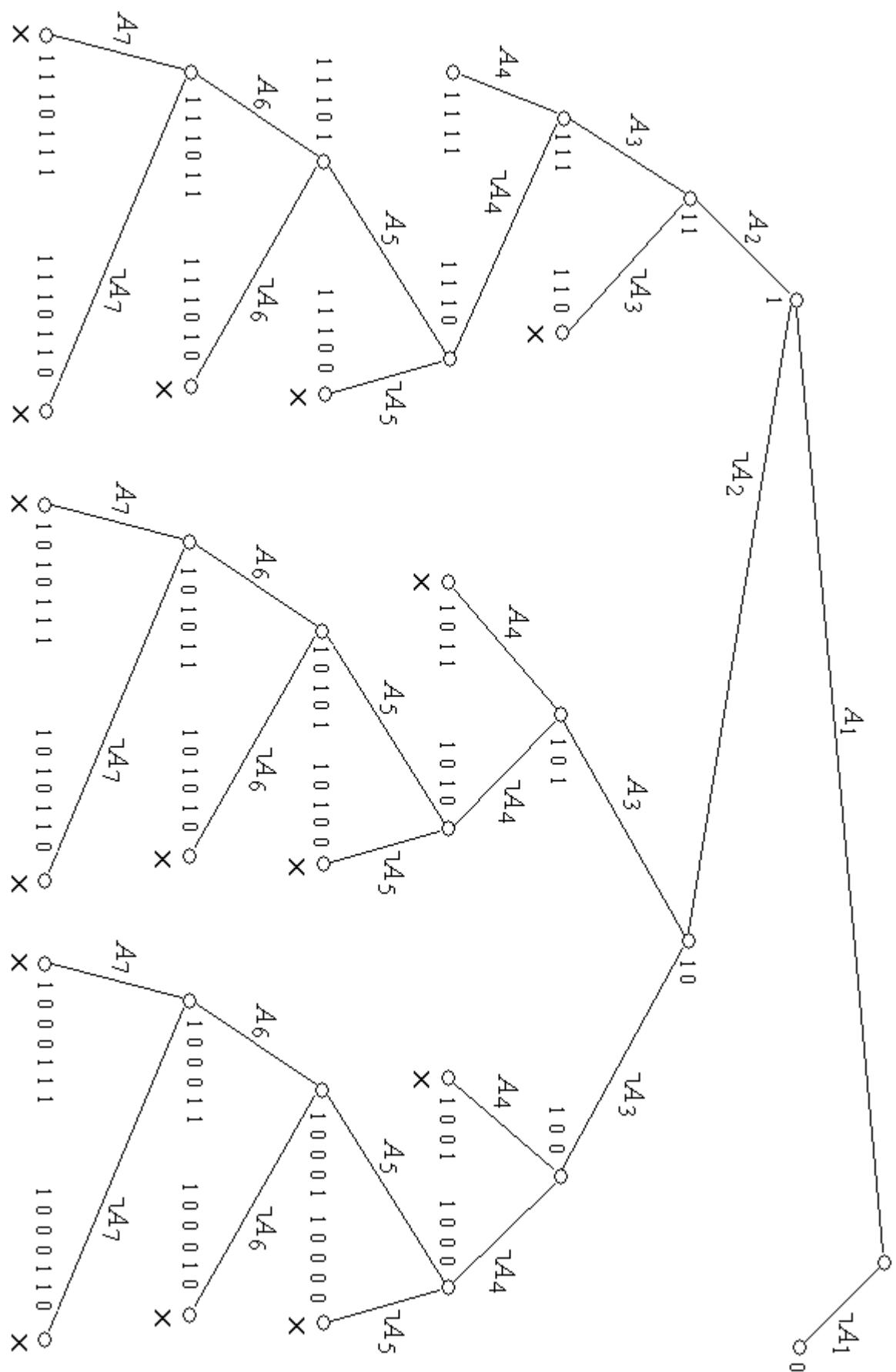


Рис.10.12

Множество дизъюнктов формулы  $\neg A$  есть множество  
 $D = S(f(x)) \& (\overline{M(x)} \vee P(x)) \& (M(x) \vee \overline{S(x)}) \& (\overline{P(x)} \vee \overline{S(x)})$ .

Эрбранов базис множества дизъюнктов  $D$  есть множество  
 $B = \{M(t), P(t), S(t) : t \text{ пробегает элементы эрбранова базиса } H\} =$   
 $\{A_1 = S(fa), A_2 = M(a), A_3 = P(a), A_4 = S(a), A_5 = \overline{Sffa}, A_6 = M(fa),$   
 $A_7 = P(fa), A_8 = \overline{Mffa}, A_9 = \overline{Pffa}, \dots\}$ .

**Узел 0.**  $A_1 = S(fa) = 0$ . Остальные  $A_i$  не определены (прочерки). Эрбранова интерпретация  $I = (0, -, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$   
 $0 \& (-\vee-) \& (-\vee-) \& - \& (-\vee-) = 0 \& - \& - \& - = 0$ . Узел 0 является опровергающим. В узле 0 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_1 = S(fa) = 0$ .

**Узел 1.**  $A_1 = S(fa) = 1$ . Остальные  $A_i$  не определены.

Эрбранова интерпретация  $I = (1, -, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$   
 $1 \& (-\vee-) \& (-\vee-) \& (-\vee-) = 1 \& - \& - \& - = -$ . Узел 1 опровергающим не является.

**Узел 10.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0$ .  $H$ -интерпретация  
 $I = (1, 0, -, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$   
 $1 \& (1 \vee -) \& (0 \vee -) \& (-\vee-) = 1 \& 1 \& - \& - = -$ . Узел 10 опровергающим не является.

**Узел 11.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1$ .  $H$ -интерпретация  
 $I = (1, 1, -, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$   
 $1 \& (0 \vee -) \& (1 \vee -) \& (-\vee-) = 1 \& - \& 1 \& - = -$ . Узел 11 опровергающим не является.

**Узел 100.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0$ .  
 $H$ -интерпретация  $I = (1, 0, 0, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$   
 $1 \& (1 \vee 0) \& (0 \vee -) \& (1 \vee -) = 1 \& 1 \& - \& 1 = -$ . Узел 100 опровергающим не является.

**Узел 101.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1$ .  
 $H$ -интерпретация  $I = (1, 0, 1, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$   
 $1 \& (1 \vee 1) \& (0 \vee -) \& (0 \vee -) = 1 \& 1 \& - \& - = -$ . Узел 101 опровергающим не является.

**Узел 110.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 0$ .  
 $H$ -интерпретация  $I = (1, 1, 0, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (0 \vee 0) \& (1 \vee -) \& (1 \vee -) = 1 \& 0 \& 1 \& 1 = 0.$  Узел 110 является

опровергающим. В узле 110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(a)} \vee P(a) = 0$ .

**Узел 111.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1.$   $H$ -интерпретация  $I = (1, 1, 1, -, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (0 \vee 1) \& (1 \vee -) \& (0 \vee -) = 1 \& 1 \& 1 \& - = -.$  Узел 111 опровергающим не является.

**Узел 1000.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0.$

$H$ -интерпретация  $I = (1, 0, 0, 0, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (1 \vee 0) \& (0 \vee 1) \& (1 \vee 1) = 1 \& 1 \& 1 \& 1 = 1.$  Узел 1000 опровергающим не является.

**Узел 1001.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 1.$

$H$ -интерпретация  $I = (1, 0, 0, 1, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (1 \vee 0) \& (0 \vee 0) \& (1 \vee 0) = 1 \& 1 \& 0 \& 1 = 0.$  Узел 1001 является

опровергающим. В узле 1001 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(a) \vee \overline{S(a)} = 0$ .

**Узел 1010.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0.$

$H$ -интерпретация  $I = (1, 0, 1, 0, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (1 \vee 1) \& (0 \vee 1) \& (0 \vee 1) = 1 \& 1 \& 1 \& 1 = 1.$  Узел 1010 опровергающим не является.

**Узел 1011.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 1.$

$H$ -интерпретация  $I = (1, 0, 1, 1, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (1 \vee 1) \& (0 \vee 0) \& (0 \vee 0) = 1 \& 1 \& 0 \& 0 = 0.$  Узел 1011 является

опровергающим. В узле 1011 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(a)} \vee \overline{S(a)} = 0$ .

**Узел 1110.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0.$

$H$ -интерпретация  $I = (1, 1, 1, 0, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (0 \vee 1) \& (1 \vee 1) \& (0 \vee 1) = 1 \& 1 \& 1 \& 1 = 1.$  Узел 1110 опровергающим не является.

**Узел 1111.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 1.$

$H$ -интерпретация  $I = (1, 1, 1, 1, -, \dots)$ .

$D(a) = S(f(a)) \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) =$

$1 \& (0 \vee 1) \& (1 \vee 0) \& (0 \vee 0) = 1 \& 1 \& 1 \& 0 = 0$ . Узел 1111 является опровергающим. В узле 1111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(a)} \vee \overline{S(a)} = 0$ .

**Узел 10000.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0, A_5 = Sffa = 0$ .  $H$ -интерпретация  $I = (1, 0, 0, 0, 0, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 0 \& (-\vee-) \& (-\vee 0) \& (-\vee 0) = 0 \& - \& - \& - = 0$ . Узел 10000 является опровергающим. В узле 10000 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_5 = Sffa = 0$ .

**Узел 10001.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0, A_5 = Sffa = 1$ .  $H$ -интерпретация  $I = (1, 0, 0, 0, 1, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (-\vee-) \& (-\vee 0) \& (-\vee 0) = 1 \& - \& - \& - = -$ . Узел 10001 опровергающим не является.

**Узел 10100.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0, A_5 = Sffa = 0$ .  $H$ -интерпретация  $I = (1, 0, 1, 0, 0, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(a)} \vee P(a)) \& (M(a) \vee \overline{S(a)}) \& (\overline{P(a)} \vee \overline{S(a)}) = 0 \& (-\vee-) \& (-\vee 0) \& (-\vee 0) = 0 \& - \& - \& - = 0$ . Узел 10100 является опровергающим. В узле 10100 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_5 = Sffa = 0$ .

**Узел 10101.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0, A_5 = Sffa = 1$ .  $H$ -интерпретация  $I = (1, 0, 1, 0, 1, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (-\vee-) \& (-\vee 0) \& (-\vee 0) = 1 \& - \& - \& - = -$ . Узел 10101 опровергающим не является.

**Узел 11100.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0, A_5 = Sffa = 0$ .  $H$ -интерпретация  $I = (1, 1, 1, 0, 0, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 0 \& (-\vee-) \& (-\vee 0) \& (-\vee 0) = 0 \& - \& - \& - = 0$ . Узел 11100 является опровергающим. В узле 11100 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_5 = Sffa = 0$ .

**Узел 11101.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0, A_5 = Sffa = 1$ .  $H$ -интерпретация  $I = (1, 1, 1, 0, 1, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (-\vee-) \& (-\vee 0) \& (-\vee 0) = 1 \& - \& - \& - = -$ . Узел 11101 опровергающим не является.

**Узел 100010.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0, A_5 = Sffa = 1, A_6 = M(fa) = 0$ .  $H$ -интерпретация  $I = (1, 0, 0, 0, 1, 0, -, \dots)$ .  
 $D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) =$

$1 \& (1 \vee -) \& (0 \vee 0) \& (- \vee 0) = 1 \& 1 \& 0 \& - = 0$ . Узел 100010 является опровергающим. В узле 100010 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(fa) \vee \overline{S(fa)} = 0$ .

**Узел 100011.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 1$ .  $H$ -интерпретация  $I = (1, 0, 0, 0, 1, 1, -, \dots)$ .

$D(fa) = S(ffa)) \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (0 \vee -) \& (1 \vee 0) \& (- \vee 0) = 1 \& - \& 1 \& - = -$ . Узел 100011 опровергающим не является.

**Узел 101010.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 0$ .  $H$ -интерпретация  $I = (1, 0, 1, 0, 1, 0, -, \dots)$ .

$D(fa) = S(ffa)) \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (1 \vee -) \& (0 \vee 0) \& (- \vee 0) = 1 \& 1 \& 0 \& - = 0$ . Узел 101010 является опровергающим. В узле 101010 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(fa) \vee \overline{S(fa)} = 0$ .

**Узел 101011.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 1$ .  $H$ -интерпретация  $I = (1, 0, 1, 0, 1, 1, -, \dots)$ .

$D(fa) = S(ffa)) \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (0 \vee -) \& (1 \vee 0) \& (- \vee 0) = 1 \& - \& 1 \& - = -$ . Узел 101011 опровергающим не является.

**Узел 111010.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 0$ .  $H$ -интерпретация  $I = (1, 1, 1, 0, 1, 0, -, \dots)$ .

$D(fa) = S(ffa)) \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (1 \vee -) \& (0 \vee 0) \& (- \vee 0) = 1 \& 1 \& 0 \& - = 0$ . Узел 111010 является опровергающим. В узле 111010 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(fa) \vee \overline{S(fa)} = 0$ .

**Узел 111011.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 1$ .  $H$ -интерпретация  $I = (1, 1, 1, 0, 1, 1, -, \dots)$ .

$D(fa) = S(ffa)) \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (0 \vee -) \& (1 \vee 0) \& (- \vee 0) = 1 \& - \& 1 \& - = -$ . Узел 111011 опровергающим не является.

**Узел 1000110.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 1, A_7 = P(fa) = 0$ .  $H$ -интерпретация

$I = (1, 0, 0, 0, 1, 1, 0, -, \dots)$ .

$D(fa) = S(ffa)) \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) = 1 \& (0 \vee 0) \& (1 \vee 0) \& (1 \vee 0) = 1 \& 0 \& 1 \& 1 = 0$ . Узел 1000110 является опровергающим. В узле 1000110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0$ .

**Узел 1000111.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 0, A_4 = S(a) = 0,$

$A_5 = S(ffa) = 1, A_6 = M(fa) = 1, A_7 = P(fa) = 1$ .  $H$ -интерпретация

$I = (1,0,0,0,1,1,1,-,...).$

$D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) =$

$1 \& (0 \vee 1) \& (1 \vee 0) \& (0 \vee 0) = 1 \& 1 \& 1 \& 0 = 0.$  В узле 1000111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(fa)} \vee \overline{S(fa)} = 0.$

**Узел 1010110.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = Sffa = 1, A_6 = M(fa) = 1, A_7 = P(fa) = 0.$   $H$ -интерпретация

$I = (1,0,1,0,1,1,0,-,...).$

$D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) =$

$1 \& (0 \vee 0) \& (1 \vee 0) \& (1 \vee 0) = 1 \& 0 \& 1 \& 1 = 0.$  В узле 1010110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0.$

**Узел 1010111.**  $A_1 = S(fa) = 1, A_2 = M(a) = 0, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = Sffa = 1, A_6 = M(fa) = 1, A_7 = P(fa) = 1.$   $H$ -интерпретация

$I = (1,0,1,0,1,1,1,-,...).$

$D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) =$

$1 \& (0 \vee 1) \& (1 \vee 0) \& (0 \vee 0) = 1 \& 1 \& 1 \& 0 = 0.$  В узле 1010111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(fa)} \vee \overline{S(fa)} = 0.$

**Узел 1110110.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = Sffa = 1, A_6 = M(fa) = 1, A_7 = P(fa) = 0.$   $H$ -интерпретация

$I = (1,1,1,0,1,1,1,-,...).$

$D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) =$

$1 \& (0 \vee 0) \& (1 \vee 0) \& (1 \vee 0) = 1 \& 0 \& 1 \& 1 = 0.$  В узле 1110110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0.$

**Узел 1110111.**  $A_1 = S(fa) = 1, A_2 = M(a) = 1, A_3 = P(a) = 1, A_4 = S(a) = 0,$

$A_5 = Sffa = 1, A_6 = M(fa) = 1, A_7 = P(fa) = 1.$   $H$ -интерпретация

$I = (1,1,1,0,1,1,1,-,...).$

$D(fa) = Sffa \& (\overline{M(fa)} \vee P(fa)) \& (M(fa) \vee \overline{S(fa)}) \& (\overline{P(fa)} \vee \overline{S(fa)}) =$

$1 \& (0 \vee 1) \& (1 \vee 1) \& (0 \vee 0) = 1 \& 1 \& 1 \& 0 = 0.$  В узле 1010111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(fa)} \vee \overline{S(fa)} = 0.$

Все концевые узлы построенного замкнутого семантического дерева опровергающие. Множество дизъюнктов  $S$  опровергимо на каждой  $H$ -интерпретации.

Справедлива следующая теорема.

**Теорема.** Следующие утверждения эквивалентны.

1. Множество дизъюнктов  $D$  невыполнимо (на всех  $H$ -интерпретациях).
2. Множество дизъюнктов  $D$  невыполнимо на всех интерпретациях.
3. Конъюнкция дизъюнктов  $D$  невыполнима.
4. Стандартная форма Скулема формулы  $\neg A$  невыполнима.
5. Формула  $\neg A$  невыполнима.
6. Формула  $A$  общезначима.
7. Правило вывода, описываемое формулой  $A$ , верно.

Отсюда сразу следует верность исходного правила вывода.

**к.** (Конечное) множество основных примеров, опровергающих каждую  $H$ -интерпретацию множества дизъюнктов  $D$ , выписывается из сведений в опровергающих узлах обрезанного семантического дерева для множества дизъюнктов  $D$ .

Множество опровергающих узлов обрезанного семантического дерева для множества дизъюнктов  $D$  есть множество

$$U = \{0,110,1001,1011,1111, \\ 10000,10100,11100, \\ 100010,101010,111010, \\ 1000110,1000111,1010110,1010111,1110110,1110111\}.$$

Множеству узлов  $U$  соответствует выписанное (без повторов) по узлам соответствующее конечное множество основных примеров  $BE$ , опровергающих каждую  $H$ -интерпретацию множества дизъюнктов  $D$ .

В узле 0 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1 = A_1 = S(fa) = 0$ .

В узле 110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(a)} \vee P(a) = 0$ .

В узле 1001 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(a) \vee \overline{S(a)} = 0$ .

В узле 1011 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(a)} \vee \overline{S(a)} = 0$ .

В узле 1111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(a)} \vee \overline{S(a)} = 0$ .

В узле 1000 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_5 = Sffa = 0$ .

В узле 10100 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_5 = Sffa = 0$ .

В узле 11100 опровергается дизъюнкт  $C_1 = S(f(x))$ , ибо его основной пример  $C_1' = A_5 = Sffa = 0$ .

В узле 100010 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(fa) \vee \overline{S(fa)} = 0$ .

В узле 101010 опровергается дизъюнкт  $C_3 = M(x) \vee \overline{S(x)}$ , ибо его основной пример  $C_3' = M(fa) \vee \overline{S(fa)} = 0$ .

В узле 111010 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0$ .

В узле 1000110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0$ .

В узле 1000111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(fa)} \vee \overline{S(fa)} = 0$ .

В узле 1010110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0$ .

В узле 1010111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(fa)} \vee \overline{S(fa)} = 0$ .

В узле 1110110 опровергается дизъюнкт  $C_2 = \overline{M(x)} \vee P(x)$ , ибо его основной пример  $C_2' = \overline{M(fa)} \vee P(fa) = 0$ .

В узле 1010111 опровергается дизъюнкт  $C_4 = \overline{P(x)} \vee \overline{S(x)}$ , ибо его основной пример  $C_4' = \overline{P(fa)} \vee \overline{S(fa)} = 0$ .

**Опровергающее множество основных примеров  $BE =$**   
 $\{S(fa), \overline{M(a)} \vee P(a), M(a) \vee \overline{S(a)}, \overline{P(a)} \vee \overline{S(a)}, Sffa, M(fa) \vee \overline{S(fa)},$   
 $\overline{M(fa)} \vee P(fa), \overline{P(fa)} \vee \overline{S(fa)}\}.$

**Теорема.** Следующие утверждения эквивалентны.

1. Множество дизъюнктов  $D$  невыполнимо.
2. Множество дизъюнктов  $D$  опровержимо на каждой  $H$ -интерпретации.
3. Замкнутое семантическое дерево  $T$  для  $D$  конечно (имеет конечное число узлов). Все концевые узлы в  $T$  опровергающие.
4. Множество  $BE$  основных примеров, опровергающих дизъюнкты из  $D$  в концевых узлах дерева  $T$ , невыполнимы на всякой  $H$ -интерпретации.
5. Множество  $BE$  основных примеров, опровергающих дизъюнкты из  $D$  в концевых узлах дерева  $T$ , невыполнимы на всякой интерпретации.

Отсюда сразу следует верность правила вывода.

**К.** Покажем, что  $D \vdash \square$ .

- (1)  $S(f(x))$ , условие,
- (2)  $\overline{M(x)} \vee P(x)$ , условие,
- (3)  $M(x) \vee \overline{S(x)}$ , условие,
- (4)  $\overline{P(x)} \vee \overline{S(x)}$ , условие,
- (5)  $P(x) \vee \overline{S(x)}$ , ПР(2,3),
- (6)  $\overline{S(f(x))} S(f(x))$ , ПР(4,5), подстановка  $\theta = \{f(x) \mid x\}$ ,
- (7)  $\square$ , ПР(1,6).

Так как  $D \vdash \square$ , то  $D \equiv 0$  и потому исходное правило вывода верно.

**Задача 31.** Написать протокол работы Пролог-программ для предикатов

```
member(X,Y), first(X,Y), last(X,Y), append(X,Y,Z), reverse(X,Y), add(X,Y),
delete(X,Y,Z), delall(X,Y,Z), substitute(X,Y,Z), sublist([X|L],[X|M]), subset(X,Y),
unionset(X,Y,Z), intersect(X,Y,Z), difset(X,Y,Z), go(S,G,T),
```

заданных следующими программами.

```
member(X,[X|Y]).
```

```

member(X,[Y|Z]) :- member(X,Z).
first(X,[X|Y]).  

last(X,[X]).  

last(X,[Z|Y]) :- last(X,Y).
append([],L,L).
append([X|L1],L2,[X|L3]) :- append(L1,L2,L3).
reverse([],[]).
reverse([H|T],L) :- reverse(T,Z),append(Z,[H],L).
reverse1(L1,L2) :- rev(L1,[],L2).
rev([],L,L).
rev([X|L],L2,L3) :- rev(L,[X|L2],L3).
add(X,L,[X|L]).  

delete(A,[A|B],B) :- !.
delete(A,[B|L],[B|M]) :- delete(A,L,M).
delall(_,[],[]).
delall(X,[X|L],M) :- !,delall(X,L,M).
delall(X,[Y|L1],[Y|L2]) :- delall(X,L1,L2).
substitute(_,[],_,[]).
substitute(X,[X|L],A,[A|M]) :- !,substitute(X,L,A,M).
substitute(X,[Y|L],A,[Y|M]) :- substitute(X,L,A,M).
sublist([X|L],[X|M]) :- coincide(L,M),!.
sublist(L,[_|M]) :- sublist(L,M).
coincide([],_).
coincide([X|L],[X|M]) :- coincide(L,M).
subset([],Y).
subset([A|X],Y) :- member(A,Y),subset(X,Y).
unionset([X|R],Y,Z) :- member(X,Y),!,unionset(R,Y,Z).
unionset([X|R],Y,[X|Z]) :- unionset(R,Y,Z).
unionset([],X,X).
intersect([],X,[]).
intersect([X|R],Y,[X|Z]) :- member(X,Y),!,intersect(R,Y,Z).
intersect([X|R],Y,Z) :- intersect(R,Y,Z).
difset(X,Y,T) :- dif1(X,Y,X,T).
dif1([R|X],Y,[R|Z],T) :- not(member(R,Y)),
    append(Z,[R],Z1),dif1(X,Y,Z1,T).
dif1([R|X],Y,[R|Z],T) :- member(R,Y),dif1(X,Y,Z,T).
dif1([],Y,Z,Z).
go(S,G,T) :- go1(S,G,[ ],T).
a(n,k). a(k,p). a(d,n). a(p,d). a(w,k). a(w,p).
go1(S,S,Tr,T) :- T=[S|Tr].
go1(S,N,Tr,T) :-
nextnode(N,Tr,N1),go1(S,N1,[N|Tr],T).
nextnode(N,Tr,N1) :-
    (a(N,N1) ; a(N1,N)),not(member(N1,Tr)).
member(X,[X|Y]).  

member(X,[Y|Z]) :- member(X,Z).

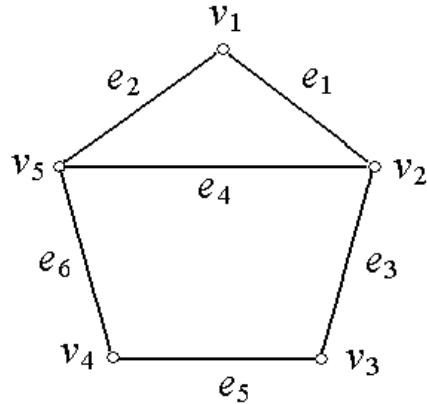
```

## 5. ГРАФЫ

**Задача 1.** Для данного неориентированного графа написать маршрут, цепь, простую цепь, цикл, простой цикл, матрицу смежностей (соседства вершин) и матрицу инциденций (принадлежности вершин и ребер). Преобразовать данный неориентированный граф в ориентированный и написать для него ормаршрут, путь, простой путь, контур, простой контур, матрицу смежностей и матрицу инциденций.

**Пример.** Для данного графа найти степени вершин, написать матрицу смежностей (соседства вершин) и матрицу инциденций (принадлежности вершин и ребер).  $G = (V, E)$ ,  $V = \{v_1, v_2, v_3, v_4, v_5\}$ ,

$$E = \{e_1=(v_1, v_2), e_2=(v_1, v_5), e_3=(v_2, v_3), e_4=(v_2, v_5), e_5=(v_3, v_4), e_6=(v_4, v_5)\}.$$



*Решение.* Степени вершин.  $\deg(v_1)=2$ ,  $\deg(v_2)=3$ ,  $\deg(v_3)=2$ ,  $\deg(v_4)=2$ ,  $\deg(v_5)=3$ . Матрица  $A$  смежностей и матрица  $B$  инциденций.

$$A = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 & v_5 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \left[ \begin{matrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{matrix} \right] \end{matrix}, \quad B = \begin{matrix} & \begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \left[ \begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{matrix} \right] \end{matrix},$$

### Варианты.

- 1.1.  $G = (V, E) = (V=\{1,2,3,4,5,6\}, E=\{(1,2),(1,3),(1,5),(1,6),(2,3),(2,4),(2,6), (3,4),(3,5),(4,5),(4,6),(5,6)\})$ .
- 1.2.  $G = (V, E) = (V=\{1,2,3,4,5,6,7\}, E=\{(1,4),(1,5), (1,6),(1,7),(2,4),(2,7),(3,4), (3,5),(3,6),(3,7),(4,7)\})$ .
- 1.3.  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,6),(1,8), (2,6),(2,7),(3,4),(3,5), (3,6),(3,8),(4,5),(4,6),(4,8),(7,8)\})$ .
- 1.4.  $G = (V, E) = (V=\{1,2,3,4,5,6\}, E=\{(1,2),(1,3),(1,4), (1,6),(2,3),(3,4),(3,6), (4,5),(4,6),(5,6)\})$ .
- 1.5.  $G = (V, E) = (V=\{1,2,3,4,5,6\}, E=\{(1,2),(1,3),(1,5), (1,6),(2,4),(3,4),(3,5), (3,6),(4,5),(4,6),(5,6)\})$ .
- 1.6.  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,2),(1,4), (1,5),(1,6),(2,3),(2,4), (2,8),(3,8),(5,6),(6,7),(6,8), (7,8)\})$ .

- 1.7.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9\}, E=\{(1,8),(1,9), (2,5),(2,9),(3,5),(3,6), (3,7),(3,9),(4,5),(4,9),(5,6), (7,9),(8,9)\})$ .
- 1.8.**  $G = (V, E) = (V=\{1,2,3,4,5,6\}, E=\{(1,4),(1,5),(1,6), (1,7),(2,4),(2,7),(3,4), (3,7),(4,5),(6,7)\})$ .
- 1.9.**  $G = (V, E) = (V=\{1,2,3,4,5,6\}, E=\{(1,2),(1,3),(1,5), (1,6),(2,3),(2,4),(2,6), (3,4),(3,5),(4,5),(4,6),(5,6)\})$ .
- 1.10.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7\}, E=\{(1,2),(1,3), (1,4),(1,5),(2,4),(2,6), (2,7),(3,4),(4,5),(5,6),(5,7)\})$ .
- 1.11.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9\}, E=\{(1,4),(1,9),(2,5),(2,9),(3,5),(3,7), (4,6),(4,7),(4,9),(6,7), (7,8),(8,9)\})$ .
- 1.12.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7\}, E=\{(1,2),(1,3), (1,6),(1,7),(2,3),(2,5), (2,6),(3,4),(3,7),(4,7),(5,6), (6,7)\})$ .
- 1.13.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7\}, E=\{(1,2),(1,3), (1,5),(1,6),(2,5),(2,6), (3,7),(4,6),(4,7),(6,7)\})$ .
- 1.14.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7\}, E=\{(1,2),(1,3), (1,5),(1,7),(2,6),(3,4), (3,6),(3,7),(4,5),(4,6),(4,7), (6,7)\})$ .
- 1.15.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,2),(1,8), (2,3),(2,5),(2,8),(3,4), (3,6),(3,7),(4,6),(5,6),(5,7), (5,8),(6,8)\})$ .
- 1.16.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,2),(1,3), (1,5),(1,8),(2,3),(2,4), (2,6),(2,7),(2,8),(3,4),(3,7), (4,5),(4,6)\})$ .
- 1.17.**  $G = (V, E) = (V=\{1,2,3,4,5\}, E=\{(1,2),(1,3),(1,4), (1,5),(2,3),(2,4),(2,5), (3,4),(3,5),(4,5)\})$ .
- 1.18.**  $G = (V, E) = (V=\{1,2,3,4,5\}, E=\{(1,2),(1,3),(1,4), (1,5),(2,3),(2,4),(2,5), (3,4),(3,5),(4,5)\})$ .
- 1.19.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,4),(1,5), (1,6),(1,7),(2,4),(2,5), (2,6),(2,7),(3,4),(3,5),(3,6), (3,7),(4,8),(5,8),(6,8),(7,8)\})$ .
- 1.20.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,2),(1,4), (1,6),(1,8),(2,3),(2,5), (2,7),(3,4),(3,6),(3,8),(4,5), (4,7),(5,6),(5,8),(6,7),(7,8)\})$ .
- 1.21.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9\}, E=\{(1,5), (1,6),(1,7),(1,9),(2,4), (2,5),(2,6),(2,7),(3,4),(3,5),(3,6), (3,9),(4,8),(4,9),(6,8),(7,8),(7,9)\})$ .
- 1.22.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,2),(1,4), (1,7),(1,8),(2,3),(2,4), (2,6),(3,5),(3,7),(3,8),(4,5), (4,8),(5,6),(7,8)\})$ .
- 1.23.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7\}, E=\{(1,2),(1,4), (1,5),(1,6),(2,3),(2,4), (2,7),(3,4),(3,5),(3,7), (4,5),(4,6),(4,7),(5,6),(6,7)\})$ .
- 1.24.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8\}, E=\{(1,2),(1,3), (1,6),(1,7),(2,3),(2,7), (2,8),(3,4),(3,8),(4,5),(4,7), (4,8),(5,6),(5,7),(5,8)\})$ .
- 1.25.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9\}, E=\{(1,7), (1,8),(2,4),(2,6),(2,8),(2,9), (3,6),(3,8),(4,8),(5,6), (5,7),(6,8),(6,9),(7,8)\})$ .
- 1.26.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9\}, E=\{(1,2),(1,3), (1,5),(1,9),(2,3),(2,6), (2,8),(3,4),(3,9),(4,5),(4,7),(4,8), (5,6),(5,7),(6,8),(6,9),(8,9)\})$ .
- 1.27.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9,10,11\}, E=\{(1,2), (1,6),(2,3),(2,4),(2,7), (3,6),(4,5),(4,9),(4,11),(5,7), (6,8),(6,10),(7,9),(7,11),(8,9),(9,10)\})$ .
- 1.28.**  $G = (V, E) = (V=\{1,2,3,4,5,6,7,8,9,10\}, E=\{(1,3), (1,5),(1,8),(1,10),(2,4), (2,7),(3,4),(3,6),(3,7),(4,7), (4,9),(5,10),(6,9),(7,10),(8,10)\})$ .

**1.29.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1,2), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5), (4,6), (4,7), (5,6), (5,7)\})$ .

**1.30.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7, 8\}, E=\{(1,2), (1,3), (1,5), (1,6), (2,3), (2,4), (2,6), (3,4), (3,5), (3,7), (3,8), (6,7), (6,8)\})$ .

**Задача 2.** Найти кратчайший путь между вершинами  $s=v_1$ ,  $t=v_4$  в нагруженном связном ориентированном графе

$G = (V, E) = (V=\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9\}, E=\{\{v_1, v_2\}, (v_1, v_7), \{v_1, v_8\}, \{v_1, v_9\}, \{v_2, v_3\}, \{v_2, v_7\}, \{v_2, v_9\}, \{v_3, v_4\}, \{v_3, v_6\}, \{v_3, v_9\}, (v_4, v_5), (v_4, v_6), \{v_4, v_7\}, \{v_5, v_6\}, \{v_6, v_7\}, \{v_6, v_8\}, \{v_6, v_9\}, \{v_7, v_9\}, \{v_8, v_9\}\})$ .

Вес  $w_{ji}$  ребра  $\{v_i, v_j\}$  или дуги  $(v_i, v_j)$  равен  $N(i^2 + j^2) + i^2 + j^2 + i + j$  по модулю 10 (остаток от деления  $w_{ij}$  на 10).  $N$  есть номер варианта.

Неориентированные ребра (проходящие в обоих направлениях) указаны в фигурных скобках. Ориентированные ребра указаны в круглых скобках. Третья координата ребра есть его вес.

**Пример.** Найти кратчайший путь между вершинами  $s$  и  $t$  в нагруженном связном ориентированном графе  $G = (V, E)$ , где

$V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ ,  $s = v_1$ ,  $t = v_6$ ,

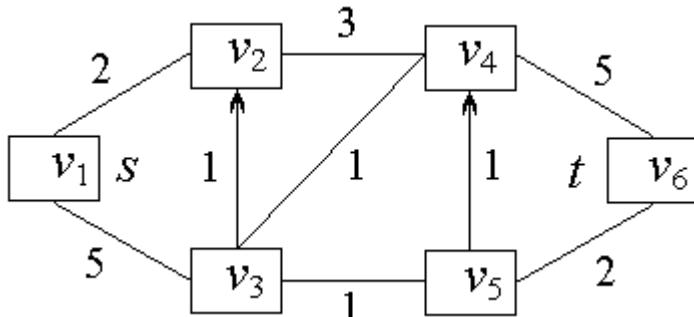
 $E = \{\{v_1, v_2, 2\}, \{v_1, v_3, 5\}, \{v_2, v_4, 3\}, (v_3, v_2, 1), \{v_3, v_4, 1\}, \{v_3, v_5, 1\}, \{v_4, v_6, 5\}, (v_5, v_4, 1), \{v_5, v_6, 2\}\}$  (рис. 11.1).


Рис. 11.1

### 11.1. Помечивающий алгоритм (Дейкстры) поиска кратчайшего (с наименьшим весом) пути между двумя вершинами $s$ и $t$ в связном нагруженном ориентированном графе

#### 11.1.1. Вычисление наименьшего веса пути от $s$ до $t$

**Шаг 1.** Присвоим вершине  $s$  постоянную (подчеркнутую) пометку 0. Вершину  $s$  объявляем активной и помечаем знаком плюс. Всем остальным вершинам присвоим временные пометки  $\infty$ . Переход к шагу 2.

**Шаг 2.** Если пометка вершины  $t$  постоянна (подчеркнута), то алгоритм заканчивает работу. Пометка вершины  $t$  равна весу кратчайшего пути от  $s$  к  $t$ . Постоянные пометки других вершин равны весам кратчайших путей от  $s$  до этих вершин. Если пометка вершины  $t$  временная, то переход к шагу 3.

**Шаг 3.** Изменим временные пометки вершин  $v$ , соседних (по дугам) с активной, следующим образом. Присваиваем вершине  $v$  временную пометку, равную сумме пометки активной вершины и веса дуги, идущей в вершину  $v$  из активной вершины, если эта сумма меньше, чем существующая временная

пометка вершины  $v$ . В противном случае оставим у вершины  $v$  прежнюю пометку. Переход к шагу 4.

**Шаг 4.** Среди всех вершин с временными пометками найдем вершину с наименьшей пометкой. Если таких вершин несколько, то возьмем любую из них, объявим ее постоянной, а эту вершину – новой активной вершиной, которую помечаем знаком плюс. Прежняя активная вершина свой плюс теряет. Переход к шагу 2.

#### 11.1.2. Построение наименьшего пути от $s$ до $t$

Кратчайший путь от  $s$  до  $t$  соответствует (в обратном порядке) начинающейся в  $t$  и заканчивающейся в  $s$  любой последовательности вершин, в которой каждая предыдущая вершина смежна (по дуге) с последующей, причем разность между пометками соседних вершин последовательности равна весу ребра, соединяющему эти вершины.

*Решение.* Постоянные пометки подчеркиваем. Активную вершину помечаем знаком плюс.

#### Вычисление наименьшего веса пути от $s$ до $t$

**Шаг 1.** Присвоим вершине  $s = v_1$  постоянную (подчеркнутую) пометку 0. Остальные вершины получают временные пометки  $\infty$ . Вершину  $s = v_1$  объявляем активной и помечаем знаком плюс (рис.11.2). Переход к шагу 2.

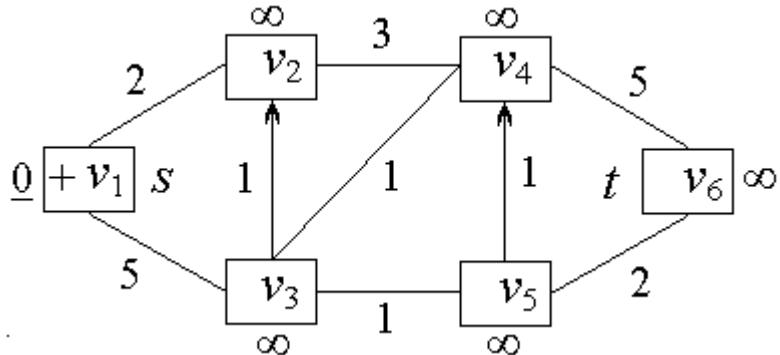


Рис. 11.2

**Шаг 2.** Вершина  $t$  постоянной пометки не имеет. Переход к шагу 3.

**Шаг 3.** Среди всех вершин с временными пометками соседние с активной вершиной  $s = v_1$  с пометкой 0 вершины  $v_2, v_3$  имеют временные пометки  $\infty$ . Для  $v_2$ :  $0+2 = 2 < \infty$ . Для  $v_3$ :  $0+5 = 5 < \infty$ . Присваиваем для  $v_2$  и  $v_3$  новые временные пометки 2 и 5 соответственно (рис.11.3). Переход к шагу 4.

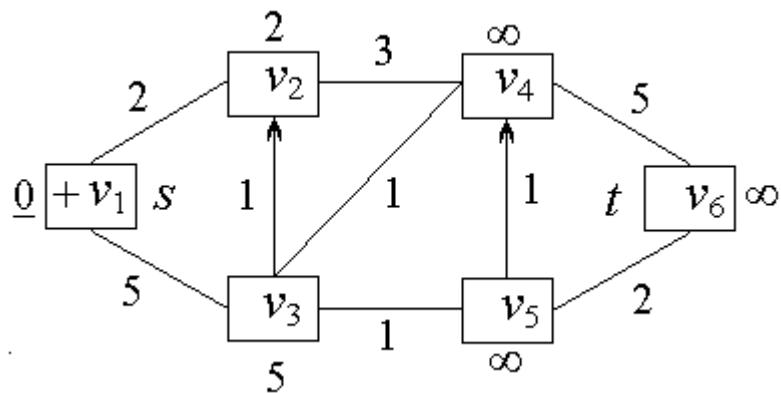


Рис. 11.3

**Шаг 4.** Из всех временных пометок пометка 2 для  $v_2$  наименьшая. Объявляем пометку 2 для  $v_2$  постоянной, вершину  $v_2$  объявляем активной и помечаем знаком плюс. Вершина  $v_1$  свой плюс теряет (рис.11.4). Переход к шагу 2.

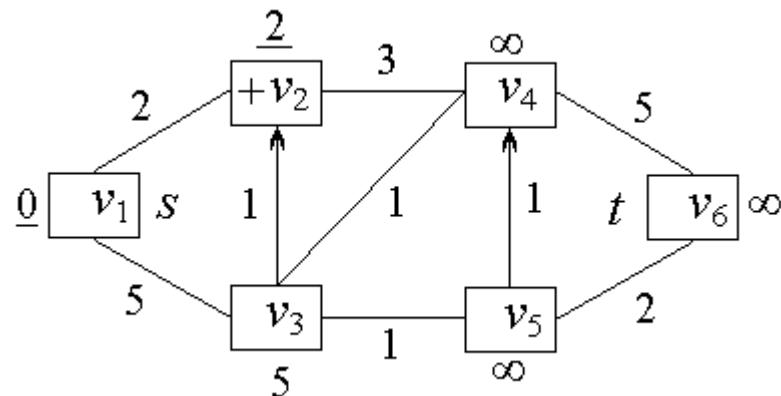


Рис. 11.4

**Шаг 2.** Вершина  $t$  постоянной пометки не имеет. Переход к шагу 3.

**Шаг 3.** Среди всех вершин с временными пометками соседняя с активной вершиной  $v_2$  с пометкой 2 вершина  $v_4$  имеет временную пометку  $\infty$ . Для  $v_4$ :  $2+3 = 5 < \infty$ . Присваиваем для  $v_4$  новую временную пометку 5 (рис.11.5). Переход к шагу 4.

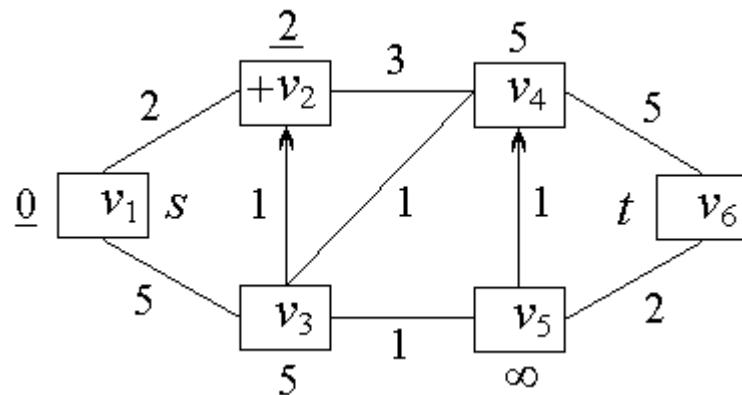


Рис.11.5

**Шаг 4.** Наименьшие временные пометки 5 у вершин  $v_3$ ,  $v_4$  одинаковы. Любую из них, например, 5 у  $v_4$ , объявляем постоянной, вершину  $v_4$

объявляем активной и помечаем знаком плюс. Вершина  $v_2$  свой плюс теряет (рис.11.6.). Переход к шагу 2.

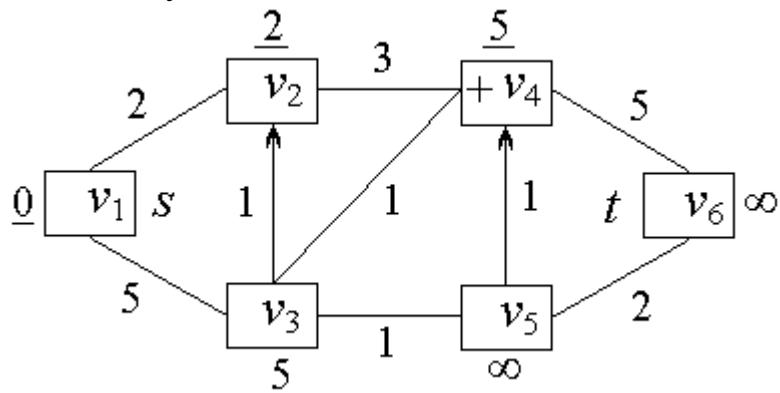


Рис.11.6

**Шаг 2.** Вершина  $t$  постоянной пометки не имеет. Переход к шагу 3.

**Шаг 3.** Среди всех вершин с временными пометками соседние с активной вершиной  $v_4$  с пометкой 5 вершины  $v_3, v_6$  имеют временные пометки 5 и  $\infty$  соответственно. Для  $v_3$ :  $5+1 = 6 \geq 5$ . Оставляем для  $v_3$  старую пометку 5. Для  $v_6$ :  $5+5 = 10 < \infty$ . Присваиваем для  $v_6$  новую временную пометку 10 (рис.11.7). Переход к шагу 4.

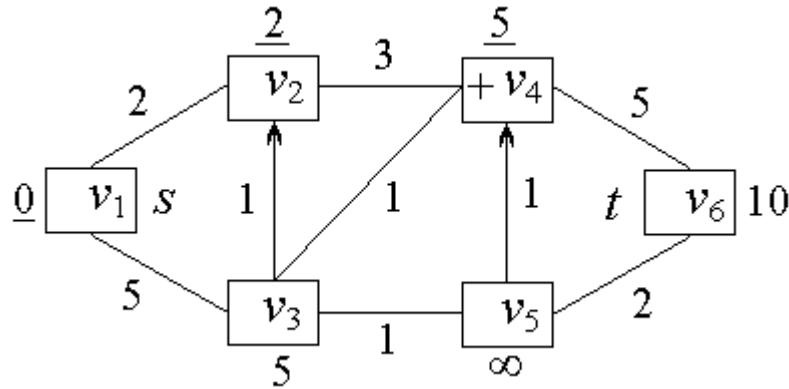


Рис. 11.7

**Шаг 4.** Из всех временных (не подчеркнутых) пометок пометка 5 для  $v_3$  наименьшая. Объявляем пометку 5 для  $v_3$  постоянной, вершину  $v_3$  объявляем активной и помечаем знаком плюс. Вершина  $v_4$  свой плюс теряет (рис.11.8). Переход к шагу 2.

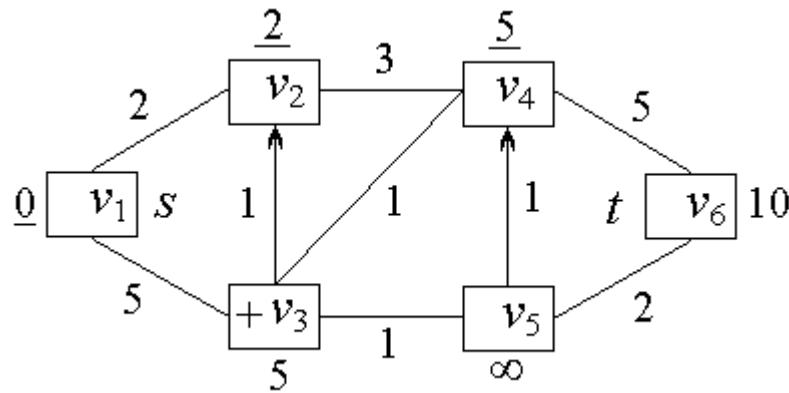


Рис. 11.8

**Шаг 2.** Вершина  $t$  постоянной пометки не имеет. Переход к шагу 3.

**Шаг 3.** Среди всех вершин с временными пометками соседняя с активной вершиной  $v_3$  вершина  $v_5$  имеет временную пометку  $\infty$ . Для  $v_5$ :  $5+1=6<\infty$ . Присваиваем для  $v_5$  новую временную пометку 6 (рис.11.9). Переход к шагу 4.

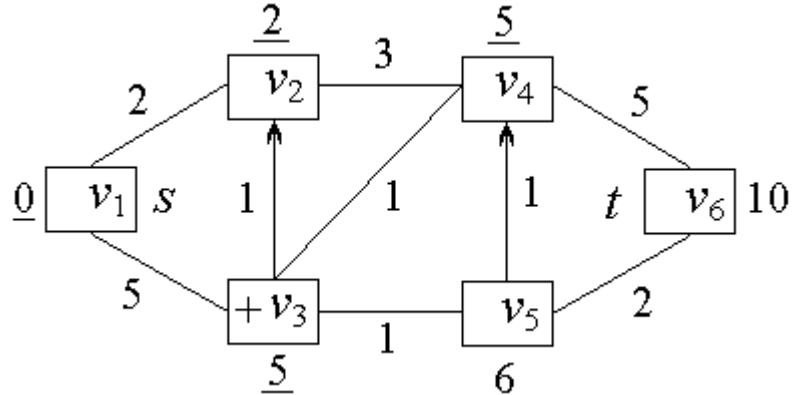


Рис.11.9

**Шаг 4.** Из всех временных пометок пометка 6 для  $v_5$  наименьшая. Объявляем пометку 6 для  $v_5$  постоянной, вершину  $v_5$  объявляем активной и помечаем знаком плюс. Вершина  $v_3$  свой плюс теряет (рис.11.10). Переход к шагу 2.

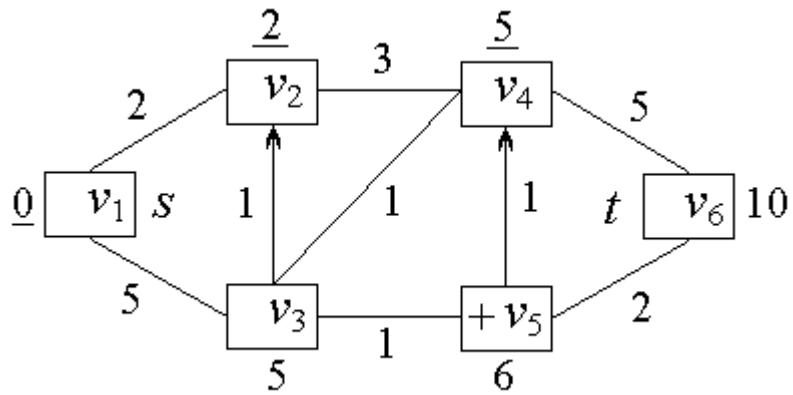


Рис.11.10

**Шаг 2.** Вершина  $t$  постоянной пометки не имеет. Переход к шагу 3.

**Шаг 3.** Среди всех вершин с временными пометками соседняя с активной вершиной  $v_5$  вершина  $v_6$  имеет временную пометку 10. Для  $v_6$ :  $6+2 = 8 < 10$ . Присваиваем для  $v_6$  новую временную пометку 8(рис.11.11).Переход к шагу 4

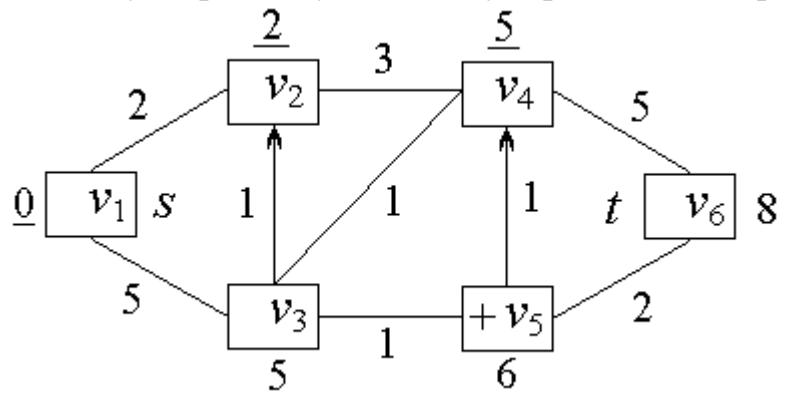


Рис.11.11

**Шаг 4.** Из всех временных пометок пометка 8 для  $v_6$  наименьшая. Объявляем пометку 8 для  $v_6$  постоянной, вершину  $v_6$  объявляем активной и помечаем знаком плюс. Вершина  $v_5$  свой плюс теряет (рис.11.12). Переход к шагу 2.

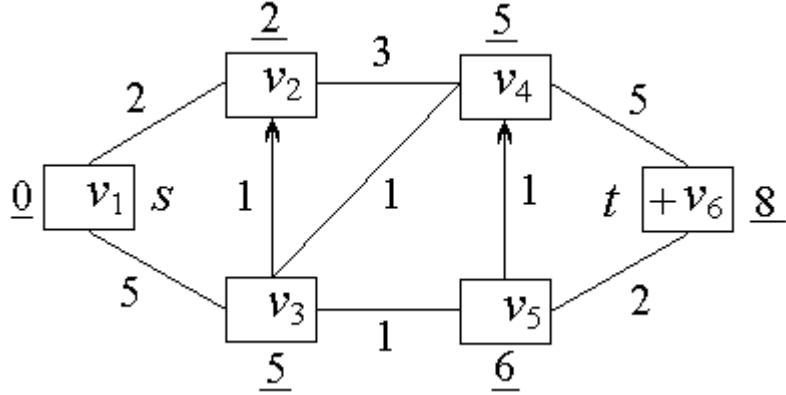


Рис.11.12

**Шаг 2.** Пометка 8 вершины  $t = v_6$  постоянна. Алгоритм заканчивает работу. Пометка 8 вершины  $t$  равна весу кратчайшего пути от  $s$  до  $t$ .

*Построение кратчайшего пути от  $s$  до  $t$*

Пусть  $f^{-1}(v)$  есть множество всех вершин  $v'$ , смежных с  $v$ ;  $d(v)$  есть пометка вершины  $v$ ;  $c(v_i, v_j)$  есть вес ребра  $(v_i, v_j)$ .

$$f^{-1}(t) = \{v_4, v_5\},$$

$$d(t) - d(v_4) = 8 - 5 = 3 \neq 5 = c(v_4, t); d(t) - d(v_5) = 8 - 6 = 2 = c(v_5, t) = 2.$$

$v_5, t$  есть подпоследовательность кратчайшего пути.

$$f^{-1}(v_5) = \{v_3\}; v_4 \notin f^{-1}(v_5), \text{ ибо ребро } (v_4, v_5) \text{ не направлено к } v_5;$$

$$d(v_5) - d(v_3) = 6 - 5 = 1 = c(v_3, v_5) = 1.$$

$v_3, v_5, t$  есть подпоследовательность кратчайшего пути.

$$f^{-1}(v_3) = \{v_1, v_4\},$$

$$d(v_3) - d(v_1) = 5 - 0 = 5 = c(v_1, v_3) = 5;$$

$$d(v_3) - d(v_4) = 5 - 5 = 0 \neq 1 = c(v_3, v_4).$$

$s, v_3, v_5, t$  есть кратчайший путь от  $s$  до  $t$ .

*Ответ.* Путь  $s = v_1 \rightarrow v_3 \rightarrow v_5 \rightarrow v_6 = t$  от  $s$  до  $t$  кратчайший. Его (наименьший) вес есть 8.

**Задача 3.** Проверить, является ли граф из задачи 1 эйлеровым (если граф не эйлеров, то достроить его до эйлерова графа) и найти в нем эйлеров цикл. Взять номер варианта, под которым стоит фамилия студента в аудиторном журнале.

**Пример.** Проверить, является ли граф  $G$  эйлеров (если граф не эйлеров, то достроить его до эйлерова графа) и найти в нем эйлеров цикл.

$$G = (V, E) =$$

$$(V = \{1, 2, 3, 4, 5, 6\}, E = \{(1, 2), (1, 6), (2, 3), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 5), (5, 6)\}).$$

*Решение.* Находим степени вершин в  $G$ .  $\deg(1)=2$ ,  $\deg(2)=4$ ,  $\deg(3)=4$ ,  $\deg(4)=2$ ,  $\deg(5)=4$ ,  $\deg(6)=4$ . Все вершины имеют четную степень. Граф  $G$  четен и потому эйлеров. Следовательно,  $G$  имеет эйлеров цикл. Найдем его.

*Алгоритм 1.*

Выбираем цикл в  $G$ .

$$C_1 = 2352; G_1 = G - C_1 = \{(1,2), (1,6), (2,6), (3,4), (3,6), (4,5), (5,6)\}.$$

Выбираем цикл в  $G_1$ .

$$C_2 = 63456; G_2 = G_1 - C_2 = \{(1,2), (1,6), (2,6)\}.$$

Выбираем цикл в  $G_2$ .

$$C_3 = 1261; G_3 = G_2 - C_3 = \emptyset.$$

Из циклов  $C_1$ ,  $C_2$ ,  $C_3$  компонуем эйлеров цикл. Выбираем два цикла  $C_1 = 2352$ ,  $C_2 = 34563$  с общей вершиной 3 и вставляем  $C_2$  в  $C_1$  на место вершины 3; получаем цикл  $C_4 = 23456352$ . Циклы  $C_4$ ,  $C_3$  объединяем по общей вершине 6; получаем  $C_5 = 23456126352$ . Цикл  $C_5$  является эйлеровым циклом.

*Алгоритм 2.*

Эйлеров цикл в четном графе можно построить, начав его любым ребром, а затем последовательно надстраивая его вправо смежными ребрами, одновременно удаляя выбранные ребра из графа и следя за тем, чтобы при очередном удалении ребра из графа он не распался на несвязные компоненты, или не очутились в изолированной вершине, не исчерпав при этом всех ребер графа.

Построим эйлеров цикл в эйлеровом графе  $G = (V, E)$  с множеством вершин  $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$  и со следующими ребрами:

$$\begin{aligned} e_1 &= (1,2), e_2 = (2,8), e_3 = (8,6), e_4 = (6,4), e_5 = (4,2), e_6 = (2,3), e_7 = (3,4), e_8 = (4,5), \\ e_9 &= (5,6), e_{10} = (6,7), e_{11} = (7,8), e_{12} = (8,1). \end{aligned}$$

Мы перечислили ребра в порядке их удаления из графа. Построенная последовательность ребер  $e_1, e_2, e_3, \dots, e_{12}$  составляет эйлеров цикл. Заметим, что после удаления ребра  $e_4$  нельзя убрать ребро  $e_8$ , ибо полученный тогда график распадется на два несвязных компонента. После удаления ребра  $e_2$  нельзя удалять ребро  $e_{12}$ , ибо тогда мы попадем в изолированную вершину 1, не исчерпав всех ребер графа.

**Задача 4.** В ненагруженном графе  $G$  из задачи 1 с помощью алгоритма удаления циклических ребер найти фундаментальную систему циклов и соответствующие множество хорд, каркас, все фундаментальные сечения (разрезы).

**Пример.** В ненагруженном графе  $G$  с помощью алгоритма удаления циклических ребер найти фундаментальную систему циклов, соответствующее множество хорд, каркас, все фундаментальные сечения (разрезы).

$G = (V, E) = (V = \{1, 2, 3, 4, 5, 6\}, E = \{(1,2), (1,4), (1,5), (1,6), (2,3), (2,5), (3,4), (3,6), (4,5), (5,6)\})$ . Найти число каркасов в заданном графике.

*Решение.* Фундаментальную систему циклов можно построить, последовательно выделяя в  $G$  простой цикл, удаляя затем из  $G$  произвольное

ребро (хорду) этого цикла, снова выделяя в получившемся графе цикл, и так далее, пока выделение циклов в последовательно получающихся графах возможно. Система получившихся циклов составит фундаментальную систему циклов графа  $G$ . Оставшийся после последовательного удаления из  $G$  хорд граф образует каркас графа  $G$ . Фундаментальный разрез составят хорды плюс одно произвольное ребро каркаса.

Граф	Цикл	Удаляемое ребро
$G$	$C_1 = 12341$	$e_1 = (2, 3)$
$G_1 = G - e_1$	$C_2 = 1451$	$e_2 = (1, 5)$
$G_2 = G_1 - e_2$	$C_3 = 34563$	$e_3 = (5, 6)$
$G_3 = G_2 - e_3$	$C_4 = 14361$	$e_4 = (3, 6)$
$G_4 = G_3 - e_4$	$C_5 = 12541$	$e_5 = (2, 5)$

Граф  $G_5 = G_4 - e_5$  циклов не имеет. Множество  $\{C_1, C_2, C_3, C_4, C_5\}$  составляет фундаментальную систему циклов графа  $G$ . Множество  $H = \{e_1, e_2, e_3, e_4, e_5\}$  содержит все хорды графа  $G$ . Граф  $G_5 = \{(1,2), (1,4), (1,6), (3,4), (4,5)\}$  есть каркас графа  $G$ . Всякий фундаментальный разрез составят хорды плюс одно произвольное ребро каркаса. Все фундаментальные разрезы:

$$H \cup \{(1,2)\}, H \cup \{(1,4)\}, H \cup \{(1,6)\}, H \cup \{(3,4)\}, H \cup \{(4,5)\}.$$

Найти число каркасов (стягивающих деревьев) графа  $G$ .

### Матричная теорема о деревьях (Кирхгоф).

Пусть граф  $G = (V, E)$  имеет множество вершин  $V = \{v_1, \dots, v_p\}$  и ребер  $E$ .

Пусть:

$A$  есть матрица смежности (соседства вершин) графа  $G$ ,

$M$  есть матрица, полученная из матрицы  $-A$  заменой элемента  $i$  главной диагонали на степень вершины  $v_i$ , то есть на число ребер, принадлежащих вершине  $v_i$ .

Стягивающее дерево (каркас) графа  $G$  есть наименьшее по числу ребер подграф-дерево графа  $G$ , соединяющее все вершины в  $G$ .

Все алгебраические дополнения матрицы  $M$  равны между собой и их общее значение равно числу стягивающих деревьев (каркасов) графа  $G$ .

Для графа  $G$  вычисления дают следующее.

$$A = v_3 \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}, M = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \\ v_1 & 4 & -1 & 0 & -1 & -1 & -1 \\ v_2 & -1 & 3 & -1 & 0 & -1 & 0 \\ v_3 & 0 & -1 & 3 & -1 & 0 & -1 \\ v_4 & -1 & 0 & -1 & 3 & -1 & 0 \\ v_5 & -1 & -1 & 0 & -1 & 4 & -1 \\ v_6 & -1 & 0 & -1 & 0 & -1 & 3 \end{bmatrix},$$

$$A_{42} = (-1)^{4+2} = \begin{vmatrix} 4 & 0 & -1 & -1 & -1 \\ -1 & -1 & 0 & -1 & 0 \\ 0 & 3 & -1 & 0 & -1 \\ -1 & 0 & -1 & 4 & -1 \\ -1 & -1 & 0 & -1 & 3 \end{vmatrix} = 135.$$

**Задача 5.** В ненагруженном графе  $G$  из задачи 1 с помощью алгоритма надстраивания ребер найти каркас и соответствующие множество хорд, фундаментальную систему циклов, все фундаментальные сечения (разрезы).

**Пример.** В ненагруженном графе  $G$  с помощью алгоритма надстраивания ребер найти каркас, соответствующее множество хорд, фундаментальную систему циклов, все фундаментальные сечения (разрезы).

$$G = (V, E) = (V = \{a, b, c, d, e, f, g\}, E = \{(a, b), (a, g), (b, c), (b, d), (b, f), (b, g), (c, d), (c, g), (d, e), (d, f), (d, g), (e, f), (e, g), (f, g)\}).$$

*Решение.* Каркас графа  $G$  можно получить, последовательно надстраивая ребрами из  $G$  произвольно взятое в  $G$  ребро до дерева, являющегося каркасом. При этом надстройку каждый раз следует выполнять, избегая появления циклов.

Исходим из ребра  $(a, b)$ . Последовательное его расширение ребрами (избегаем при этом появления циклов) приводит нас к каркасу (стягивающему дереву)

$$T = \{(a, b), (a, g), (d, g), (d, e), (c, d), (e, f)\}.$$

Множество хорд

$$H = E - T = \{(b, c), (b, d), (b, f), (b, g), (c, g), (d, f), (e, g), (f, g)\}.$$

Последовательно возвращаем в каркас по одной хорде и получаем фундаментальную систему из восьми циклов:

$$C_1 = abcdga, C_2 = abdga, C_3 = abfedga, C_4 = abga, C_5 = cdgc, C_6 = defd, C_7 = degd, C_8 = defgd.$$

Всякий фундаментальный разрез составят хорды плюс одно произвольное ребро каркаса. Все фундаментальные разрезы:

$$H \cup \{(a, b)\}, H \cup \{(a, g)\}, H \cup \{(d, g)\}, H \cup \{(d, e)\}, H \cup \{(c, d)\}, H \cup \{(e, f)\}.$$

**Задача 6.** В нагруженном графе  $G$  из задачи 1 найти кратчайший (наименьший по весу) каркас и соответствующие множество хорд, фундаментальную систему циклов, все фундаментальные сечения (разрезы). Вес  $w_{ij}$  неориентированного ребра  $(vi, vj)$  с  $i < j$  равен  $N(i^2 + j^2) + i^2 + j^2 + i + j$  по модулю 10 (остаток от деления  $w_{ij}$  на 10).  $N$  есть номер варианта.

**Пример.** В нагруженном графе  $G$  найти кратчайший каркас и соответствующие множество хорд, фундаментальную систему циклов, все фундаментальные сечения (разрезы).

$$G = (V, E) = (V = \{a, b, c, d, e, f, g\}, E = \{(a, b, 1), (a, g, 2), (b, c, 7), (b, d, 6), (b, f, 8), (b, g, 3), (c, d, 2), (c, g, 9), (d, e, 1), (d, f, 9), (d, g, 1), (e, f, 4), (e, g, 5), (f, g, 9)\}).$$

*Решение.* Если граф  $G$  является нагруженным (каждому ребру графа  $G$  приписано некоторое неотрицательное число – вес ребра, его стоимость, то

наименьший каркас (с наименьшей суммой весов ребер) можно получить, последовательно надстраивая ребрами из  $G$  произвольно взятое в  $G$  ребро с наименьшим весом до дерева, являющегося каркасом. При этом надстройку каждый раз следует выполнять ребром с наименьшим возможным весом, избегая появления циклов.

Исходим из ребра  $(a,b,1)$ . Последовательное его расширение ребрами с наименьшим весом (избегаем при этом появления циклов) приводит нас к каркасу (стягивающему дереву)

$$T = \{(a,b,1), (a,g,2), (d,g,1), (d,e,1), (c,d,2), (e,f,4)\}$$

с наименьшим весом 11. Множество хорд

$$H = E - T = \{(b,c,7), (b,d,6), (b,f,8), (b,g,3), (c,g,9), (d,f,9), (e,g,5), (f,g,9)\}.$$

Последовательно возвращаем в каркас по одной хорде и получаем фундаментальную систему из восьми циклов:

$$\begin{aligned} C_1 &= abcdga, C_2 = abdga, C_3 = abfedga, C_4 = abga, C_5 = cdgc, C_6 = defd, C_7 = degd, \\ C_8 &= defgd. \end{aligned}$$

Всякий фундаментальный разрез составят хорды плюс одно произвольное ребро каркаса. Все фундаментальные разрезы:

$$H \cup \{(a,b,1)\}, H \cup \{(a,g,2)\}, H \cup \{(d,g,1)\}, H \cup \{(d,e,1)\},$$

$$H \cup \{(c,d,2)\}, H \cup \{(e,f,4)\}.$$

**Задача 7.** В данном двудольном графе  $G = \{U, V, E\}$ ,

$$U = \{x_1, x_2, x_3, x_4, x_5, x_6\}, V = \{y_1, y_2, y_3, y_4, y_5, y_6\},$$

$$E = \{(x_1, y_1), (x_1, y_2), (x_1, y_5), (x_2, y_1), (x_2, y_3), (x_2, y_5), (x_3, y_1), (x_3, y_6),$$

$$(x_4, y_3), (x_4, y_4), (x_4, y_6), (x_4, y_7), (x_5, y_5), (x_5, y_7), (x_6, y_4), (x_6, y_6), (x_6, y_7)\}.$$

найти совершенное паросочетание. Если его нет, то указать получившееся максимальное паросочетание.

### **11.2. Алгоритм построения совершенного паросочетания для двудольного графа**

Пусть  $G = (U, V, E)$  есть двудольный граф. Выберем исходное паросочетание  $P_1$ , например, одно ребро графа  $G$ . Допустим, что паросочетание  $P_i = (U_i, V_i, E_i)$  для графа  $G$  построено.

Построим паросочетание  $P_{i+1}$  для  $G$  следующим образом.

1. Выбираем  $u$  из  $U$  не из  $P_i$ . Если такой вершины и нет, то  $P_i$  есть совершенное паросочетание. Если есть, то строим в  $G$  чередующуюся цепь  $\mu_i = [u_1, v_1, u_2, v_2, \dots, u_p, v_p]$  с  $u_1 = u$ , в которой всякое ребро  $(u_i, v_i)$  не принадлежит  $E_i$  а всякое ребро  $(v_i, u_{i+1})$  принадлежит  $E_i$ . Если такой цепи нет, то совершенного паросочетания граф  $G$  не имеет, а паросочетание  $P_i$  является для  $G$  максимальным (тупиковым). Цепь  $\mu_i$  есть  $P_i$ -увеличитель.

2. Удаляем из  $P_i$  все ребра  $(v_i, u_{i+1})$  и добавляем все ребра  $(u_i, v_i)$  цепи  $\mu_i$ .

Получившееся паросочетание  $P_{i+1}$  на одно ребро длиннее паросочетания  $P_i$ . Переходим к п. 1.

*Решение.* **Шаг 1.** Выбираем исходное паросочетание  $P_1 = \{(x_1, y_1)\}$ .  $P_1$ -увеличитель (чередующаяся цепь)

$$\mu_1 = [x_2, y_1, x_1, y_5].$$

0	1	0
1	0	1

Единственная единица в первой строке из нулей и единиц означает, что соответствующее этой единице ребро  $(y_1, x_1)$  лежит в  $P_1$ . Убираем это ребро из  $P_1$ , а вместо него добавляем два ребра  $(x_2, y_1), (x_1, y_5)$ , соответствующие двум единицам второй строки из нулей и единиц. В результате получим следующее паросочетание  $P_2$ , число ребер в котором на одно больше чем в  $P_1$ .

**Шаг 2.**  $P_2 = \{(x_1, y_5), (x_2, y_1)\}$ .

$$\mu_2 = [x_3, y_1, x_2, y_3].$$

0	1	0
1	0	1

Удаляем из  $P_2$  ребро  $(x_2, y_1)$  и добавляем вместо него ребра  $(x_3, y_1), (x_2, y_3)$ .

**Шаг 3.**  $P_3 = \{(x_1, y_5), (x_2, y_3), (x_3, y_1)\}$ .

$$\mu_3 = [x_4, y_4].$$

Добавляем в  $P_3$  ребро  $(x_4, y_4)$ .

**Шаг 4.**  $P_4 = \{(x_1, y_5), (x_2, y_3), (x_3, y_1), (x_4, y_4)\}$ .

$$\mu_4 = [x_5, y_5, x_1, y_1, x_3, y_6].$$

0	1	0	1	0
1	0	1	0	1

Удаляем из  $P_4$  ребра  $(x_1, y_5), (x_3, y_1)$  и добавляем вместо них ребра  $(x_5, y_5), (x_1, y_1), (x_3, y_6)$ .

**Шаг 5.**  $P_5 = \{(x_1, y_1), (x_2, y_3), (x_3, y_6), (x_4, y_4), (x_5, y_5)\}$ .

$$\mu_5 = [x_6, y_6, x_3, y_1, x_1, y_5, x_5, y_7].$$

0	1	0	1	0	1	0
1	0	1	0	1	0	1

Удаляем из  $P_5$  ребра  $(x_3, y_6), (x_1, y_1), (x_5, y_5)$  и добавляем вместо них ребра  $(x_6, y_6), (x_3, y_1), (x_1, y_5), (x_5, y_7)$ .

**Шаг 6.**  $P_6 = \{(x_1, y_5), (x_2, y_3), (x_3, y_1), (x_4, y_4), (x_5, y_7), (x_6, y_6)\}$ .  $P_6$  есть искомое совершенное паросочетание для исходного графа.

### Варианты.

**7.1.**  $E = \{(x_1, y_2), (x_1, y_5), (x_1, y_6), (x_2, y_3), (x_2, y_4), (x_2, y_6), (x_3, y_1), (x_3, y_2), (x_3, y_4), (x_3, y_5), (x_4, y_1), (x_4, y_2), (x_4, y_5), (x_5, y_2), (x_5, y_3), (x_5, y_6)\}$ .

**7.2.**  $E = \{(x_1, y_5), (x_1, y_6), (x_2, y_1), (x_2, y_3), (x_2, y_4), (x_3, y_1), (x_3, y_2), (x_3, y_5), (x_4, y_2), (x_4, y_5), (x_4, y_6), (x_5, y_2), (x_5, y_4), (x_5, y_6)\}$ .

**7.3.**  $E = \{(x_1, y_5), (x_1, y_6), (x_2, y_3), (x_2, y_4), (x_2, y_5), (x_3, y_1), (x_3, y_2), (x_3, y_4), (x_3, y_5), (x_4, y_2), (x_4, y_3), (x_4, y_5), (x_5, y_2), (x_5, y_6)\}$ .

**7.4.**  $E = \{(x_1, y_5), (x_1, y_5), (x_1, y_6), (x_2, y_3), (x_2, y_4), (x_3, y_2), (x_3, y_1), (x_3, y_2), (x_3, y_5), (x_4, y_2), (x_4, y_3), (x_4, y_5), (x_5, y_1), (x_5, y_2), (x_5, y_6)\}$ .

**7.5.**  $E = \{(x_1, y_5), (x_1, y_6), (x_2, y_3), (x_2, y_4), (x_3, y_1), (x_3, y_2), (x_3, y_5), (x_4, y_2), (x_4, y_5), (x_5, y_2), (x_5, y_5), (x_5, y_6)\}$ .



**7.28.**  $E = \{(x_1, y_3), (x_1, y_4), (x_1, y_1), (x_2, y_5), (x_2, y_6), (x_3, y_2), (x_3, y_6), (x_4, y_1), (x_4, y_2), (x_4, y_5), (x_5, y_4), (x_5, y_1), (x_5, y_2), (x_5, y_5)\}$ .

**7.29.**  $E = \{(x_1, y_3), (x_1, y_4), (x_1, y_1), (x_2, y_5), (x_2, y_6), (x_3, y_5), (x_3, y_2), (x_3, y_6), (x_4, y_2), (x_4, y_5), (x_5, y_4), (x_5, y_1), (x_5, y_2), (x_5, y_5)\}$ .

**7.30.**  $E = \{(x_1, y_5), (x_1, y_4), (x_1, y_1), (x_2, y_4), (x_2, y_5), (x_2, y_6), (x_3, y_2), (x_3, y_6), (x_4, y_2), (x_4, y_5), (x_5, y_3), (x_5, y_1), (x_5, y_2), (x_5, y_5)\}$ .

**Задача 8.** Для указанных множеств найти систему различных представителей.

$$A_1 = \{1, 2, 5\}, A_2 = \{1, 3, 5\}, A_3 = \{1, 6\}, A_4 = \{3, 4, 6, 7\}, A_5 = \{5, 7\}, A_6 = \{4, 6, 7\}.$$

*Решение.* Пусть множества вершин  $U = \{A_1, A_2, A_3, A_4, A_5\}; V = \{1, 2, 3, 4, 5, 6, 7\}$ ,

множество  $E$  ребер таково, что  $(A_i, j) \in E \leftrightarrow j \in A_i$ . Тогда

$$E = \{(A_1, 1), (A_1, 2), (A_1, 5), (A_2, 1), (A_2, 3), (A_2, 5), (A_3, 1), (A_3, 6), (A_4, 3), (A_4, 4), (A_4, 6), (A_4, 7), (A_5, 5), (A_5, 7), (A_6, 4), (A_6, 6), (A_6, 7)\}.$$

Двудольный граф  $G = (U, V, E)$  есть двудольный граф предыдущей задачи.

Его совершенное паросочетание

$$P = \{(A_1, 5), (A_2, 3), (A_3, 1), (A_4, 4), (A_5, 7), (A_6, 6)\}.$$

Система различных представителей:

$$5 \in A_1 = \{1, 2, 5\}, 3 \in A_2 = \{1, 3, 5\}, 1 \in A_3 = \{1, 6\},$$

$$4 \in A_4 = \{3, 4, 6, 7\}, 7 \in A_5 = \{5, 7\}, 6 \in A_6 = \{4, 6, 7\}.$$

### Варианты.

$$\textbf{8.1. } A_1 = \{1, 3\}, A_2 = \{2, 3, 4\}, A_3 = \{2, 3, 5\}, A_4 = \{1, 2\}, A_5 = \{3, 6\}.$$

$$\textbf{8.2. } A_1 = \{2, 3\}, A_2 = \{2, 4\}, A_3 = \{3, 4, 5\}, A_4 = \{1, 2, 3\}, A_5 = \{1, 6\}.$$

$$\textbf{8.3. } A_1 = \{5, 6\}, A_2 = \{1, 2, 3\}, A_3 = \{4, 5, 6\}, A_4 = \{3, 4\}, A_5 = \{1, 2\}.$$

$$\textbf{8.4. } A_1 = \{1, 2\}, A_2 = \{1, 4\}, A_3 = \{3, 4, 5\}, A_4 = \{1, 3, 4\}, A_5 = \{2, 3\}.$$

$$\textbf{8.5. } A_1 = \{3, 4, 5\}, A_2 = \{1, 5\}, A_3 = \{2, 3\}, A_4 = \{2, 4, 5\}, A_5 = \{1, 5\}.$$

$$\textbf{8.6. } A_1 = \{2, 3\}, A_2 = \{4, 5\}, A_3 = \{1, 3, 5\}, A_4 = \{3, 4, 5\}, A_5 = \{1, 6\}.$$

$$\textbf{8.7. } A_1 = \{2, 4, 5\}, A_2 = \{1, 2, 3\}, A_3 = \{1, 3, 4\}, A_4 = \{3, 5\}, A_5 = \{2, 6\}.$$

$$\textbf{8.8. } A_1 = \{3, 4\}, A_2 = \{1, 2, 3\}, A_3 = \{2, 5\}, A_4 = \{3, 4, 5\}, A_5 = \{3, 6\}.$$

$$\textbf{8.9. } A_1 = \{2, 6\}, A_2 = \{1, 3, 4, 6\}, A_3 = \{1, 2, 5\}, A_4 = \{1, 3, 5\}, A_5 = \{3, 4\}.$$

$$\textbf{8.10. } A_1 = \{1, 3, 5\}, A_2 = \{2, 4, 6\}, A_3 = \{1, 2, 3, 4\}, A_4 = \{3, 4, 5, 6\}, A_5 = \{5, 6\}.$$

$$\textbf{8.11. } A_1 = \{1, 3, 6\}, A_2 = \{4, 5, 6\}, A_3 = \{2, 3, 5, 6\}, A_4 = \{1, 2, 4\}, A_5 = \{5, 6\}.$$

$$\textbf{8.12. } A_1 = \{1, 2\}, A_2 = \{3, 5, 6\}, A_3 = \{1, 3, 6\}, A_4 = \{1, 2, 3, 4\}, A_5 = \{3, 4\}.$$

$$\textbf{8.13. } A_1 = \{2, 3, 5\}, A_2 = \{1, 2, 3, 5\}, A_3 = \{3, 4, 6\}, A_4 = \{3, 5, 6\}, A_5 = \{1, 2, 5, 6\}.$$

$$\textbf{8.14. } A_1 = \{1, 3, 4\}, A_2 = \{2, 4, 5\}, A_3 = \{1, 5, 6\}, A_4 = \{1, 2, 3\}, A_5 = \{2, 6\}.$$

$$\textbf{8.15. } A_1 = \{1, 2, 3\}, A_2 = \{1, 3, 5\}, A_3 = \{2, 3, 4\}, A_4 = \{1, 2, 3, 4\}, A_5 = \{1, 2, 3, 5\}.$$

$$\textbf{8.16. } A_1 = \{1, 2, 3, 4\}, A_2 = \{2, 3, 4, 5\}, A_3 = \{3, 4, 5, 6\}, A_4 = \{1, 3, 5\}, A_5 = \{2, 4, 6\}.$$

$$\textbf{8.17. } A_1 = \{1, 2, 3, 4\}, A_2 = \{1, 5, 6\}, A_3 = \{3, 5, 6\}, A_4 = \{1, 4, 5\}, A_5 = \{2, 3, 6\}.$$

$$\textbf{8.18. } A_1 = \{1, 2, 5\}, A_2 = \{1, 5, 6\}, A_3 = \{1, 2, 3, 4\}, A_4 = \{1, 4, 5\}, A_5 = \{1, 3, 6\}.$$

$$\textbf{8.19. } A_1 = \{1, 4, 5, 6\}, A_2 = \{1, 2, 5\}, A_3 = \{1, 2, 3, 6\}, A_4 = \{2, 3, 5\}, A_5 = \{1, 4, 5\}.$$

$$\textbf{8.20. } A_1 = \{2, 3, 5\}, A_2 = \{1, 3, 5, 6\}, A_3 = \{1, 2, 6\}, A_4 = \{2, 5, 6\}, A_5 = \{1, 4, 5, 6\}.$$

$$\textbf{8.21. } A_1 = \{1, 3, 6\}, A_2 = \{1, 2, 5\}, A_3 = \{1, 3, 5\}, A_4 = \{2, 4, 6\}, A_5 = \{1, 2, 3, 5\}.$$

$$\textbf{8.22. } A_1 = \{1, 4, 5\}, A_2 = \{2, 3, 5\}, A_3 = \{1, 2, 3\}, A_4 = \{1, 3, 5\}, A_5 = \{2, 4, 5\}.$$

**8.23.**  $A_1 = \{2,4,5\}$ ,  $A_2 = \{2,5,6\}$ ,  $A_3 = \{2,4,6\}$ ,  $A_4 = \{1,3,5\}$ ,  $A_5 = \{1,4,5\}$ .

**8.24.**  $A_1 = \{1,2,4,5\}$ ,  $A_2 = \{2,4,6\}$ ,  $A_3 = \{2,3,4\}$ ,  $A_4 = \{2,4,5\}$ ,  $A_5 = \{1,2,5,6\}$ .

**8.25.**  $A_1 = \{2,4,5\}$ ,  $A_2 = \{1,2,4,5\}$ ,  $A_3 = \{1,2,3,5\}$ ,  $A_4 = \{2,3,4\}$ ,  $A_5 = \{1,2,5\}$ .

**8.26.**  $A_1 = \{2,4,5\}$ ,  $A_2 = \{1,3,4\}$ ,  $A_3 = \{2,4,5,6\}$ ,  $A_4 = \{1,2,4,5\}$ ,  $A_5 = \{1,2,4,6\}$ .

**8.27.**  $A_1 = \{1,2,3,5\}$ ,  $A_2 = \{2,4,5,6\}$ ,  $A_3 = \{1,2,4,5\}$ ,  $A_4 = \{1,2,4,6\}$ ,  $A_5 = \{1,2,5\}$ .

**8.28.**  $A_1 = \{2,4,5,6\}$ ,  $A_2 = \{1,2,4,5\}$ ,  $A_3 = \{1,2,3,5\}$ ,  $A_4 = \{1,2,3,4\}$ ,  $A_5 = \{2,3,6\}$ .

**8.29.**  $A_1 = \{2,4,5\}$ ,  $A_2 = \{1,2,4,5\}$ ,  $A_3 = \{2,4,6\}$ ,  $A_4 = \{3,4,5,6\}$ ,  $A_5 = \{1,3,4,6\}$ .

**8.30.**  $A_1 = \{1,2,4,5\}$ ,  $A_2 = \{2,3,4,5\}$ ,  $A_3 = \{1,3,4,5\}$ ,  $A_4 = \{1,3,6\}$ ,  $A_5 = \{2,3,4,6\}$ .

**Задача 9.** Построить наибольшее по весу совершенное паросочетание в полном двудольном графе

$$G = (V_1, V_2, E), V_1 = \{x_1, x_2, x_3, x_4\}, V_2 = \{y_1, y_2, y_3, y_4\},$$

$$E = \{e_{ij} = (x_i, y_j) : i=1,2,3,4; j=1,2,3,4\}.$$

с весами ребер, заданными в  $4 \times 4$ -матрице  $W = [w_{ij}]$ , где вес  $w_{ij}$  ребра  $e_{ij} = (x_j, y_j)$  равен  $N(i^2 + j^2) + i^2 + j^2 + i + j$  по модулю 10 (остаток от деления  $w_{ij}$  на 10).  $N$  есть номер варианта.

**Пример.** Построить наибольшее по весу совершенное паросочетание в полном двудольном графе  $G = K_{4,4} = (V_1, V_2, E)$   $V_1 = \{x_1, x_2, x_3, x_4\}$ ,  $V_2 = \{y_1, y_2, y_3, y_4\}$ ,  $E = \{e_{ij} = (x_i, y_j) : i, j = 1, 2, 3, 4\}$ ; с весами ребер, заданными в матрице

$$A = [a_{ij}] = \begin{matrix} & v_1 & v_2 & v_3 & v_4 \\ v_1 & \left[ \begin{matrix} 5 & 3 & 4 & 2 \\ 3 & 1 & 2 & 1 \end{matrix} \right] \\ v_2 & \left[ \begin{matrix} 4 & 2 & 2 & 1 \\ 6 & 5 & 4 & 2 \end{matrix} \right] \\ v_3 & \\ v_4 & \end{matrix}.$$

### 11.3. Алгоритм построения наибольшего совершенного паросочетания в полном нагруженном двудольном графе

Пусть полный двудольный с нагруженными ребрами граф  $G = K_{n,n} = (X, Y, E)$ , где вершины  $X = \{x_1, \dots, x_n\}$ ,  $Y = \{y_1, \dots, y_n\}$ , ребра  $E = \{e_{ij} = (x_i, y_j) : i, j = 1, 2, \dots, n\}$ , веса ребер  $e_{ij}$  задаются  $n \times n$ -матрицей  $A = [a_{ij}]$ , в которой вес ребра  $e_{ij}$  равен  $a_{ij}$ . Полный двудольный граф  $G$  всегда имеет совершенное паросочетание (обозначим его через СПС). Далее выполнить следующее.

Пометить вершины из  $G$  числами по правилу:  $\forall x_i \in X \ u_i = \max a_{ij}$  (это максимумы чисел соответствующих строк матрицы  $A$ ) и  $\forall y \in Y \ v_j = 0$ . Для любого ребра  $a_{ij}$  выполняется  $a_{ij} \leq u_i + v_j$ . Взять в  $G$  исходное паросочетание  $P = \emptyset$ .

1. Построить подграф  $G'$  графа  $G$ , содержащий все вершины в  $G$  и все ребра из  $G$ , для которых  $u_i + v_j = a_{ij}$ . Перейти к пункту 2.

2. Взять вне  $P$  некоторую вершину. Методом чередующихся цепей (как это делалось в предыдущей задаче) найти  $P$ -увеличитель и построить новое паросочетание в  $G$ , у которого ребер больше чем в  $P$ . Далее построить в  $G'$

дерево  $T$  всех возможных чередующихся цепей (как в предыдущей задаче). Перейти к пункту 3.

3. Вычислить  $\Delta = \max (u_i + v_j - a_{ij})$  по всем  $x_i \in T, y_j \in T$ . Изменить пометки вершин по правилу:  $\forall x_i \in T \quad u_i := u_i - \Delta; \forall y_j \in T \quad v_j := v_j + \Delta$ . Перейти к пункту 4.

4. Если построенное  $P$  есть СПС для  $G$ , то алгоритм заканчивает работу. Если нет, то перейти к пункту 1.

*Решение.* На рис.11.13 приведены последовательные шаги построения совершенного паросочетания для  $G$ .

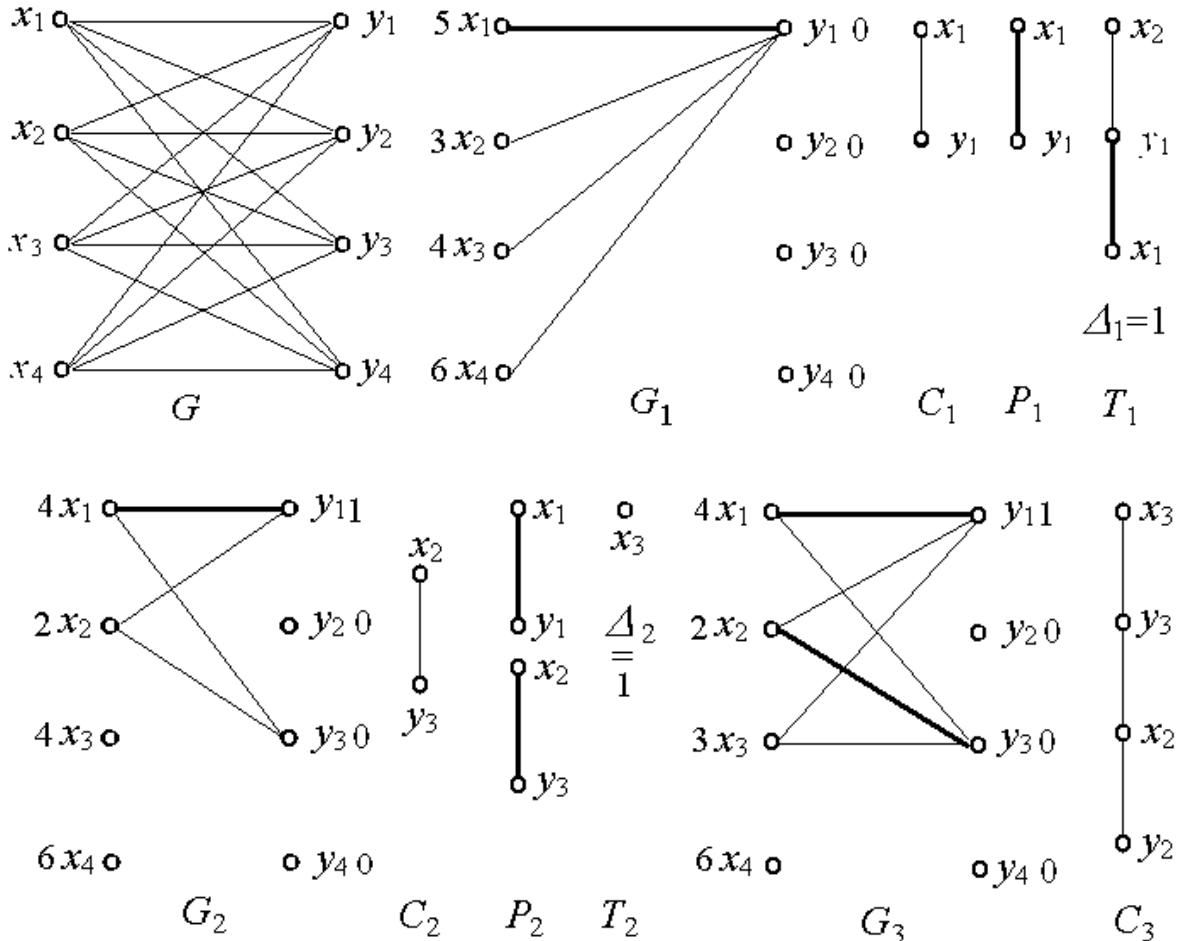


Рис.11.13 ( $T_1, T_2$ )

**Шаг 0.** Пометим вершины  $x_1, \dots, x_4, y_1, \dots, y_4$  соответственно числами  $u_1=0, u_2=8, u_3=4, u_4=8, v_1=v_2=v_3=v_4=0$ . Возьмем в  $G$  исходное паросочетание  $P_0=\emptyset$ .

**Шаг 1.** 1. Подграф  $G_1=\{e_{11}, e_{21}, e_{31}, e_{41}\}$ , ибо  $5=a_{11}=u_1+v_1=5+0=5, 3=a_{21}=u_2+v_1=3+0=3, 4=a_{31}=u_3+v_1=4+0=4, 6=a_{41}=u_4+v_1=6+0=6$ . Переход к пункту 2.

2. Вершина  $x_1 \notin P_3$ .  $C_1=[x_1, y_1]=\{e_{11}\}$  есть чередующаяся цепь в  $G$  с корнем в  $x_1$ . Для  $G$  паросочетание  $P_1=(P_0-C_1) \cup (C_1-P_0)=\{e_{11}\}$ . Вершина  $x_2 \notin P_1$ . Дерево  $T_1$  всех чередующийся цепей в  $G_1$  с корнем  $x_2$  на рис.11.13  $T_1$ . Переход к пункту 3.

3. По всем  $x_i \in T_1$ ,  $y_j \notin T_1$  число  $\Delta = \min(u_i + v_j - a_{ij}) = \min(u_1 + v_2 - a_{12}, u_1 + v_3 - a_{13}, u_1 + v_4 - a_{14}, u_2 + v_2 - a_{12}, u_2 + v_3 - a_{13}, u_2 + v_4 - a_{14}) = \min(5+0-3, 5+0-4, 5+0-2, 3+0-1, 3+0-2, 3+0-1) = \min(2, 1, 3, 2, 1, 2) = 1$ . Новые пометки вершин в  $G$  есть  $u_1 := u_1 - \Delta = 5 - 1 = 4$ ,  $u_2 := u_2 - \Delta = 3 - 1 = 2$ ,  $v_1 := v_1 + \Delta = 0 + 1 = 1$ . Переход к пункту 4.

4.  $P_1$  не есть СПС для  $G$ . Переход к пункту 1.

**Шаг 2.** 1. Подграф  $G_2 = \{e_{11}, e_{13}, e_{21}, e_{23}\}$ , ибо  $5 = a_{11} = u_1 + v_1 = 4 + 1 = 5$ ,  $4 = a_{13} = u_1 + v_3 = 4 + 0 = 4$ ,  $3 = a_{21} = u_2 + v_1 = 2 + 1 = 3$ ,  $2 = a_{23} = u_2 + v_3 = 2 + 0 = 2$ . Переход к пункту 2.

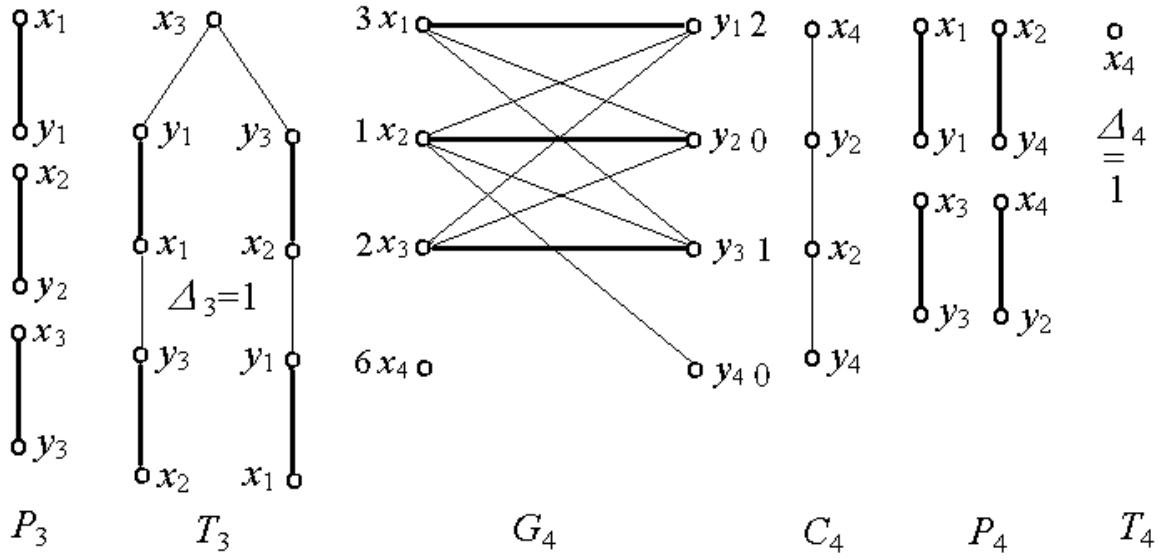


Рис.11.13 ( $T_3, T_4$ )

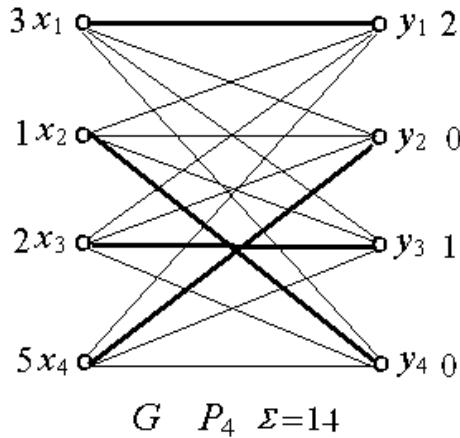


Рис.11.13 ( $G$ )

2. Вершина  $x_2 \notin P_1$ .  $C_2 = [x_2, y_3] = \{e_{23}\}$  есть чередующаяся цепь в  $G$  с корнем в  $x_2$ . Для  $G$  паросочетание  $P_2 = (P_1 - C_2) \cup (C_2 - P_1) = \{e_{11}, e_{23}\}$ . Вершина  $x_3 \notin P_2$ . Дерево  $T_2$  всех чередующихся цепей в  $G_2$  с корнем  $x_3$  есть лишь вершина  $x_3$ . Переход к пункту 3.

3. По всем  $x_i \in T_2$ ,  $y_j \notin T_2$  число  $\Delta = \min(u_i + v_j - a_{ij}) = \min(u_3 + v_1 - a_{31}, u_3 + v_2 - a_{32}, u_3 + v_3 - a_{33}, u_3 + v_4 - a_{34}) = \min(4+1-4, 4+0-2, 4+0-3, 4+0-1) = \min(1, 2, 1, 3) = 1$ . Новые пометки вершин в  $G$  есть  $u_3 := u_3 - \Delta = 4 - 1 = 3$ . Переход к пункту 4.

4.  $P_2$  не есть СПС для  $G$ . Переход к пункту 1.

**Шаг 3.** 1. Подграф  $G_3 = \{e_{11}, e_{13}, e_{21}, e_{23}, e_{31}, e_{33}\}$ , ибо  $5 = a_{11} = u_1 + v_1 = 4 + 1 = 5$ ,  $4 = a_{13} = u_1 + v_3 = 4 + 0 = 4$ ,  $3 = a_{21} = u_2 + v_1 = 2 + 1 = 3$ ,  $2 = a_{23} = u_2 + v_3 = 2 + 0 = 2$ ,  $4 = a_{31} = u_3 + v_1 = 3 + 1 = 4$ ,  $3 = a_{33} = u_3 + v_3 = 3 + 0 = 3$ . Переход к пункту 2.

2. Вершина  $x_3 \notin P_2$ .  $C_3 = [x_3, y_3, x_2, y_2] = \{e_{22}, e_{23}, e_{33}\}$  есть чередующаяся цепь в  $G$  с корнем в  $x_3$ . Для  $G$  паросочетание  $P_3 = (P_2 - C_3) \cup (C_3 - P_2) = \{e_{11}, e_{22}, e_{33}\}$ . Вершина  $x_3 \notin P_2$ . Дерево  $T_2$  всех чередующихся цепей в  $G_2$  с корнем  $x_3$  на рис.11.13  $T_3$ . Переход к пункту 3.

3. По всем  $x_i \in T_3$ ,  $y_j \notin T_3$  число  $\Delta = \min(u_i + v_j - a_{ij}) = \min(u_1 + v_4 - a_{14}, u_2 + v_4 - a_{24}, u_3 + v_4 - a_{34}) = \min(4 + 0 - 2, 2 + 0 - 1, 3 + 0 - 1) = \min(2, 1, 3) = 1$ . Новые пометки в  $G$  есть  $u_1 := u_1 - \Delta = 4 - 1 = 3$ ,  $u_2 := u_2 - \Delta = 2 - 1 = 1$ ,  $u_3 := u_3 - \Delta = 3 - 1 = 2$ ,  $v_1 := v_1 + \Delta = 1 + 1 = 2$ ,  $v_3 := v_3 + \Delta = 0 + 1 = 1$ . Переход к пункту 4.

4.  $P_3$  не есть СПС для  $G$ . Переход к пункту 1.

**Шаг 4.** 1. Подграф  $G_4 = \{e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}, e_{24}, e_{31}, e_{32}, e_{33}\}$ , ибо  $5 = a_{11} = u_1 + v_1 = 3 + 2 = 5$ ,  $3 = a_{12} = u_1 + v_2 = 3 + 0 = 3$ ,  $4 = a_{13} = u_1 + v_3 = 3 + 1 = 4$ ,  $3 = a_{21} = u_2 + v_1 = 1 + 2 = 3$ ,  $1 = a_{22} = u_2 + v_2 = 1 + 0 = 1$ ,  $2 = a_{23} = u_2 + v_3 = 1 + 1 = 2$ ,  $1 = a_{24} = u_2 + v_4 = 1 + 0 = 1$ ,  $4 = a_{31} = u_3 + v_1 = 2 + 2 = 4$ ,  $2 = a_{32} = u_3 + v_2 = 2 + 0 = 2$ ,  $3 = a_{33} = u_3 + v_3 = 2 + 1 = 3$ . Переход к пункту 2.

2. Вершина  $x_4 \notin P_2$ .  $C_4 = [x_4, y_2, x_2, y_4] = \{e_{42}, e_{22}, e_{24}\}$  есть чередующаяся цепь в  $G$  с корнем в  $x_4$ . Для  $G$  паросочетание  $P_4 = (P_3 - C_4) \cup (C_4 - P_3) = \{e_{11}, e_{24}, e_{33}, e_{42}\}$ .

3. По всем  $x_i \in T_4$ ,  $y_j \notin T_4$  число  $\Delta = \min(u_i + v_j - a_{ij}) = \min(u_4 + v_1 - a_{41}, u_4 + v_2 - a_{42}, u_4 + v_3 - a_{43}, u_4 + v_4 - a_{44}) = \min(6 + 2 - 6, 6 + 0 - 5, 6 + 1 - 3, 6 + 0 - 2) = \min(2, 1, 3, 4) = 1$ . Переход к пункту 4.

4.  $P_4$  есть СПС для  $G$ . Алгоритм заканчивает работу.  $P_4$  есть наибольшее СПС для  $G$  с суммой весов ребер  $\sum = a_{11} + a_{24} + a_{33} + a_{42} = 5 + 1 + 3 + 5 = 14$  (рис.11.13 ( $G$ )).

**Задача 10.** Построить плоское изображение графа, если это возможно.  $G = (V, E) = (V = \{1, 2, 3, 4, 5, 6\}, E = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 4), (2, 6), (3, 5), (3, 6), (4, 6), (5, 6)\})$ .

#### 11.4. Алгоритм построения плоского изображения графа

Изложим алгоритм построения плоского изображения графа. Пусть  $G = (V, E)$  есть исходный граф, плоское изображение которого нам требуется построить (если оно имеется). Будем предполагать, что граф  $G$  связен, не имеет висячих вершин и точек сочленения, т.е. вершин, удаление которых из  $G$  вместе с принадлежащими им ребрами приводит к несвязному графу.

Пусть  $G' = (V', E')$  есть некоторый плоский подграф графа  $G$ . Остаток графа  $G$  относительно  $G'$  есть граф  $R = (V'' - V', E'') = (V - V', E'')$  есть подграф графа  $G$ , порожденный подмножеством вершин  $V - V'$ , т.е.  $R$  состоит из всех тех ребер графа  $G$ , концы которых не лежат в  $V'$  (т.е. лежат вне  $V'$ ).

Кусок  $P$  графа  $G$  относительно его подграфа  $G'$  есть один из следующих объектов:

1) компонента связности остатка  $R$  относительно  $G'$ , дополненная теми ребрами графа  $G$ , которые соединяют вершины этой компоненты и вершины  $V'$  графа  $G'$ ;

2) одно ребро из  $E - E'$  с концами, лежащими в  $V'$ .

Контактные точки куска  $P$  есть вершины, общие для  $P$  и  $G'$ . Грань  $F$  в  $G'$  совместима с куском  $P$ , если все контактные точки куска  $P$  принадлежат грани  $F$ .

Пусть  $G_1$  есть некоторый простой цикл графа  $G$ . Поместим на плоскости его плоское изображение.

Допустим, что плоский граф  $G_i$  уже построен. Плоский граф  $G_{i+1}$  получим следующим образом.

1. Построим остаток  $R_i$  графа  $G$  относительно  $G_i$ .
2. Построим все куски графа  $G$  относительно  $G_i$ . Если ни одного такого куска построить не удается, то  $G_i$  есть плоское изображение графа  $G$ .
3. Для каждого куска выписать все грани, которые с ним совместимы. При этом возможны три случая:
  - а) существует кусок, не совместимый ни с одной гранью плоского графа  $G_i$ ; тогда граф  $G$  на плоскость не укладывается;
  - б) существует кусок, совместимый с единственной гранью графа  $G_i$ ; тогда выбираем этот кусок;
  - в) каждый из кусков совместим по крайней мере с двумя гранями графа  $G_i$ ; тогда выбираем любой из таких кусков.
4. В выбранном куске  $P$  находим такую цепь  $\mu$ , один или оба конца которой (и только они) принадлежат  $G_i$ . Построим граф  $G_{i+1}$ , дополнив граф  $G_i$  ребрами цепи  $\mu$ , проведя  $\mu$  внутри любой из совместимых с куском  $P$  граней. Плоский граф  $G_{i+1}$  построен. Переходим к пункту 1.

В случае неоднозначности проведения цепи  $\mu$  будем проводить ее во внутренней грани.

**Пример.** Построим плоское изображение графа

$$G = (\{1,2,3,4,5,6\}, \{(1,2), (2,6), (5,6), (1,3), (1,4), (1,5), (2,4), (3,5), (3,6), (4,6)\}).$$

**Шаг 1.** Выбираем в  $G$  плоский цикл  $G_1 = [1,2,6,5,1]$ .

Граф  $G_1$  определяет две грани:

$F_{10} = [1,2,6,5,1]$ , внешняя;

$F_{11} = [1,2,6,5,1]$ , внутренняя.

Остаток  $R_1$  графа  $G$  относительно  $G_1$  распадается в две компоненты связности:  $R_{11} = (\{3\}, \emptyset)$  и  $R_{12} = (\{4\}, \emptyset)$ .

Строим куски графа  $G$  относительно  $G_1$  и их контактные точки.

$$P_{11} = (\{1,3,5,6\}, \{(1,3), (3,5), (3,6)\}); \{1,5,6\};$$

$$P_{12} = (\{1,2,4,6\}, \{(1,4), (2,4), (4,6)\}); \{1,2,6\}.$$

Кусок  $P_{11}$  совместим с гранями  $F_{10}, F_{11}$ .

Кусок  $P_{12}$  совместим с гранями  $F_{10}, F_{11}$ .

Цепь  $\mu_1 = [1,4,2]$  в куске  $P_{12}$  помещаем в грани  $F_{11}$  графа  $G_1$ .

**Шаг 2.** Плоский граф

$$G_2 = (\{1,2,4,5,6\}, \{(1,5),(5,6),(2,6),(1,2),(2,4),(1,4)\}).$$

Граф  $G_2$  определяет грани:

$$F_{20} = [1,2,6,5,1]; F_{21} = [1,4,2,6,5,1]; F_{22} = [1,4,2,1].$$

Остаток  $R_2$  для  $G$  относительно  $G_2$  принимает вид:  $R_2 = (\{3\}, \emptyset)$ . Строим куски графа  $G$  относительно  $G_2$  и их контактные точки.

$$P_{21} = (\{1,3,5,6\}, \{(1,3),(3,5),(3,6)\}); \quad \{1,5,6\}; P_{22} = (\{4,6\}, \{(4,6)\}); \quad \{4,6\}.$$

Кусок  $P_{21}$  совместим с гранями  $F_{20}, F_{21}$ .

Кусок  $P_{22}$  совместим с гранью  $F_{21}$ .

Цепь  $\mu_2 = [4,6]$  в куске  $P_{22}$  помещаем в грани  $F_{21}$  графа  $G_2$ .

**Шаг 3.** Плоский граф

$$G_3 = (\{1,2,6,5,4\}, \{(1,5),(5,6),(2,6),(1,2),(2,4),(1,4),(4,6)\}).$$

Граф  $G_3$  определяет грани:

$$F_{30} = [1,2,6,5,1]; F_{31} = [1,4,6,5,1]; F_{32} = [1,4,2,1]; F_{33} = [4,6,2,4].$$

Остаток  $R_3$  для  $G$  относительно  $G_3$  принимает вид:  $R_3 = (\{3\}, \emptyset)$ . Строим куски графа  $G$  относительно  $G_3$  и их контактные точки.

$$P_{31} = (\{1,3,5,6\}, \{(1,3),(3,5),(3,6)\}); \quad \{1,5,6\};$$

Кусок  $P_{31}$  совместим с гранями  $F_{30}, F_{31}$ .

Цепь  $\mu_3 = [1,3,5]$  в куске  $P_{31}$  помещаем в грани  $F_{31}$  графа  $G_3$ .

**Шаг 4.** Плоский граф

$$G_4 = (\{1,2,6,5,4,3\}, \{(1,5),(5,6),(2,6),(1,2),(2,4),(1,4),(4,6),(3,5),(1,3)\}).$$

Граф  $G_4$  определяет грани:

$$F_{40} = [1,2,6,5,1]; F_{41} = [1,3,5,6,4,1]; F_{42} = [1,4,2,1];$$

$$F_{43} = [4,6,2,4]; F_{44} = [1,3,5,1].$$

Остаток  $R_4$  для  $G$  относительно  $G_4$  принимает вид:  $R_4 = \emptyset$ .

Строим куски графа  $G$  относительно  $G_4$  и их контактные точки.

$$P_{41} = (\{3,6\}, \{(3,6)\}); \quad \{3,6\};$$

Кусок  $P_{41}$  совместим с гранью  $F_{41}$ .

Цепь  $\mu_4 = [3,6]$  в куске  $P_{41}$  помещаем в грани  $F_{41}$  графа  $G_4$ .

**Шаг 5.** Плоский граф

$$G_5 = (\{1,2,6,5,4,3\}, \{(1,5),(5,6),(2,6),(1,2),(2,4),(1,4),(4,6),(3,5),(1,3),(3,6)\}).$$

Ни одного куска относительно графа  $G_5$  построить не удается.

Следовательно, граф  $G_5$  есть плоская укладка графа  $G$ .

Последовательные графы  $G_1, G_2, G_3, G_4, G_5$  приведены на рис.10.13.

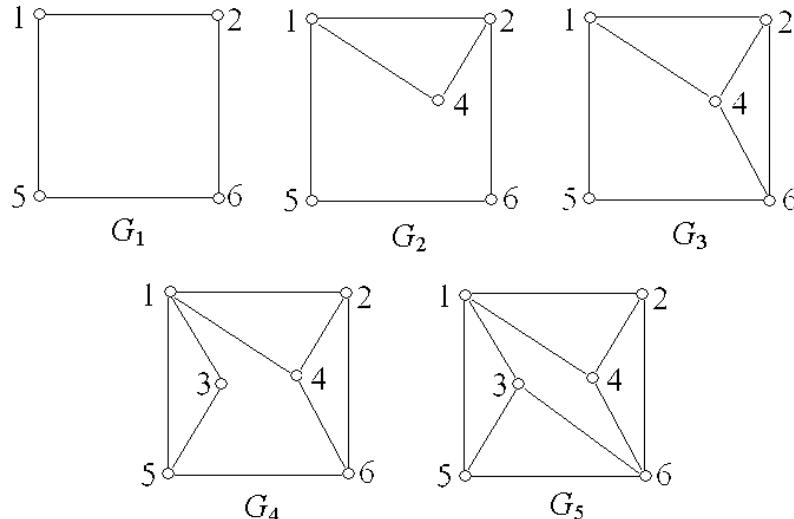


Рис.10.13

### Варианты.

Построить плоское изображение графа, если это возможно.

- 10.1.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 6), (2, 7), (3, 4), (3, 5), (3, 7), (5, 6), (6, 7)\})$ .
- 10.2.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 6), (1, 7), (2, 4), (2, 6), (3, 4), (3, 5), (3, 6), (3, 7), (4, 5), (5, 6), (6, 7)\})$ .
- 10.3.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (1, 7), (2, 3), (2, 4), (2, 6), (3, 4), (4, 5), (4, 6), (4, 7)\})$ .
- 10.4.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (4, 7), (6, 7)\})$ .
- 10.5.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (1, 6), (2, 3), (2, 6), (3, 4), (3, 6), (3, 7), (4, 5), (4, 7), (5, 6), ((6, 7)\})$ .
- 10.6.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (1, 6), (2, 3), (2, 5), (2, 6), (3, 4), (3, 5), (3, 7), (4, 5), (5, 6), (5, 7), (6, 7)\})$ .
- 10.7.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7, 8\}, E=\{(1, 3), (1, 4), (2, 4), (2, 6), (2, 7), (3, 4), (3, 5), (4, 7), (4, 8), (5, 6), (5, 7), (6, 7), (7, 8)\})$ .
- 10.8.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 3), (1, 5), (1, 6), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (3, 4), (3, 5), (4, 5), (5, 6), (6, 7)\})$ .
- 10.9.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 5), (1, 6), (1, 7), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 5), (4, 7), (6, 7)\})$ .
- 10.10.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 6), (1, 7), (2, 3), (2, 7), (3, 4), (3, 5), (4, 5), (4, 6), (5, 6), (5, 7)\})$ .
- 10.11.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (3, 7), (4, 5), (5, 6), (5, 7), (6, 7)\})$ .
- 10.12.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (1, 6), (2, 3), (2, 4), (2, 5), (3, 5), (3, 6), (4, 5), (5, 7), (6, 7)\})$ .
- 10.13.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (4, 6), (4, 7), (5, 6), (5, 7)\})$ .
- 10.14.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 5), (1, 7), (2, 3), (2, 5), (3, 4), (3, 6), (3, 7), (4, 5), (4, 6), (4, 7), (6, 7)\})$ .

- 10.15.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 7), (2, 3), (2, 5), (2, 7), (3, 4), (3, 6), (3, 7), (4, 6), (5, 6), (5, 7), (5, 7), (6, 7)\})$ .
- 10.16.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 5), (1, 7), (2, 3), (2, 4), (2, 6), (2, 7), (3, 4), (3, 5), (3, 7), (4, 5), (4, 6)\})$ .
- 10.17.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 7), (2, 3), (2, 6), (3, 4), (3, 5), (3, 6), (3, 7), (4, 5), (4, 6), (5, 7)\})$ .
- 10.18.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 4), (1, 7), (2, 3), (2, 6), (2, 7), (3, 4), (3, 6), (4, 5), (4, 7)\})$ .
- 10.19.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7, 8\}, E=\{(1, 4), (1, 5), (1, 6), (1, 7), (2, 4), (2, 5), (2, 6), (2, 7), (3, 4), (3, 5), (3, 6), (3, 7), (4, 5), (4, 8), (5, 8), (6, 8), (7, 8)\})$ .
- 10.20.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 5), (1, 6), (2, 3), (2, 6), (2, 7), (3, 4), (4, 6), (4, 7), (5, 6), (6, 7)\})$ .
- 10.21.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 5), (1, 6), (1, 7), (2, 3), (3, 4), (3, 5), (3, 6), (3, 7), (4, 5), (4, 6)\})$ .
- 10.22.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7, 8\}, E=\{(1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 3), (2, 8), (3, 5), (3, 7), (4, 5), (5, 6), (6, 7), (7, 8)\})$ .
- 10.23.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 5), (1, 7), (2, 5), (2, 7), (3, 4), (3, 5), (4, 6), (5, 7)\})$ .
- 10.24.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7, 8, 9\}, E=\{(1, 2), (1, 4), (1, 9), (2, 3), (2, 4), (2, 6), (2, 9), (3, 4), (3, 5), (3, 8), (5, 6), (6, 7), (6, 9), (7, 8), (5, 8)\})$ .
- 10.25.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 3), (1, 4), (1, 5), (2, 3), (2, 6), (2, 7), (3, 7), (4, 5), (5, 6), (5, 7), (6, 7)\})$ .
- 10.26.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 7), (2, 3), (2, 4), (2, 5), (2, 6), (3, 5), (4, 5), (4, 7), (5, 6), (5, 7)\})$ .
- 10.27.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7, 8\}, E=\{(1, 3), (1, 5), (1, 6), (1, 7), (2, 4), (2, 6), (2, 8), (3, 5), (3, 6), (4, 6), (5, 6), (5, 7)\})$ .
- 10.28.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 7), (2, 3), (2, 4), (2, 6), (3, 4), (3, 5), (4, 5), (4, 6), (5, 6), (5, 7)\})$ .
- 10.29.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 4), (1, 5), (1, 7), (2, 3), (2, 5), (2, 7), (3, 5), (4, 5), (4, 6), (5, 6), (6, 7)\})$ .
- 10.30.**  $G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 7), (2, 4), (2, 6), (2, 7), (3, 5), (4, 6), (4, 7), (6, 6), (6, 7)\})$ .

**Задача 11.** В заданном неориентированном графе  $G$  из задачи 10 найти все максимальные и все наибольшие внутренне устойчивые (независимые) множества вершин.

$$G = (V, E) = (V=\{1, 2, 3, 4, 5, 6, 7\}, E=\{(1, 2), (1, 3), (1, 5), (1, 6), (2, 3), (3, 4), (3, 6), (4, 5), (4, 7), (5, 6), (6, 7)\})$$

*Внутренне устойчивые (независимые) множества вершин графа*

**Определение.** Подмножество  $S$  вершин графа  $G = (V, E)$  внутренне устойчиво, если никакие две вершины из  $S$  не смежны в  $G$ . Число внутренней устойчивости графа  $G$

$$\alpha(G) = \max \{|S| : S \subseteq V \text{ и } S \text{ внутренне устойчиво в } G\}.$$

Внутренне устойчивое множество вершин  $S$  называется (*максимально тупиковым*, если всякое строгое надмножество множества  $S$  внутренне устойчивым уже не является. При этом  $S$  называется наибольшим, если среди всех внутренне устойчивых множеств вершин в  $G$  оно имеет наибольшую мощность.

Пусть  $S$  есть внутренне устойчивое множество вершин графа  $G = (V, E)$  и ребро  $e=(u,v) \in E$ . С каждой вершиной  $v \in V$  свяжем логическую переменную  $x_v$  и пусть  $x_v$  означает, что  $v \notin S$ .

### 11.5. Алгоритм вычисления всех наибольших внутренне устойчивых множеств вершин графа $G = (V, E)$

1. Построить формулу  $F = \bigwedge_{(u,v) \in E} (x_u \vee x_v)$ , условие внутренней устойчивости графа  $G$ .

2. Построить минимальную ДНФ  $D$  формулы  $F$ .

3. Для каждого дизъюнктивного слагаемого  $K = x_{u_1}x_{v_1}\dots x_{w_1}$  в  $D$  получить соответствующее ему максимальное внутренне устойчивое множество вершин  $S = V - \{u_1, v_1, \dots, w_1\}$ .

4. Из полученных максимальных внутренне устойчивых множеств вершин выбрать все наибольшие.

**Замечание.** Этот алгоритм пригоден и для ориентированных графов.

**Решение.** Условие внутренней устойчивости графа  $G$

$$F = \bigwedge_{(u,v) \in E} (x_u \vee x_v) = (1 \vee 2)(1 \vee 3)(1 \vee 5)(1 \vee 6)(2 \vee 3)(3 \vee 4)(3 \vee 6)(4 \vee 5)(4 \vee 7) \& (5 \vee 6)(6 \vee 7) = 1357 \vee 23456 \vee 23567 \vee 1246 \vee 1346.$$

Максимальными внутренне устойчивыми множествами вершин будут множества:

$$\begin{aligned} V - \{1, 3, 5, 7\} &= \{2, 4, 6\}; \\ V - \{2, 3, 4, 5, 6\} &= \{1, 7\}; \\ V - \{2, 3, 5, 6, 7\} &= \{1, 4\}; \\ V - \{1, 2, 4, 6\} &= \{3, 5, 7\}; \\ V - \{1, 3, 4, 6\} &= \{2, 5, 7\}. \end{aligned}$$

Выбираем из них наибольшие:  $\{2, 4, 6\}$ ;  $\{3, 5, 7\}$ ;  $\{2, 5, 7\}$ .

**Задача 12.** В заданном ориентированном графе  $G$  из задачи 11 найти все максимальные и все наибольшие внутренне устойчивые (независимые) множества вершин.

**Замечание.** Алгоритм для неориентированных графов пригоден и для ориентированных графов.

**Задача 13.** В заданном неориентированном графе из задачи 10 найти все минимальные и все наименьшие внешне устойчивые (доминирующие) множества вершин.

**Пример.** В заданном неориентированном графе  $G$  найти все минимальные и все наименьшие внешне устойчивые (доминирующие) множества вершин.

$$G = (V, E) = (\{1, 2, 3, 4, 5, 6, 7\}, \{(1, 2), (1, 3), (1, 5), (1, 6), (2, 3), (3, 4), (3, 6), (4, 5), (4, 7), (5, 6), (6, 7)\}).$$

*Внешне устойчивые (доминирующие) множества вершин графа*

**Определение.** Множество  $T$  вершин графа  $G = (V, E)$  называется *внешне устойчивым* (в  $G$ ), если  $\forall v \notin T \exists u \in T (e=(u,v) \in E)$ . Число внешней устойчивости графа  $G$

$$\beta(G) = \min \{|T| : T \subseteq V \text{ и } T \text{ есть внешне устойчивое множество в } G\}.$$

Внешне устойчивое множество вершин  $T$  называется (*минимально тупиковым*, если  $T$  не содержит в себе строго ни одного подмножества, являющегося внешне устойчивым. Внешне устойчивое множество вершин называется наименьшим, если среди всех внешне устойчивых множеств вершин в  $G$  оно имеет наименьшую мощность.

### 11.6. Алгоритм вычисления всех наименьших внешне устойчивых множеств вершин графа $G = (V, E)$

Пусть  $T$  есть внешне устойчивое множество вершин графа  $G = (V, E)$ . С каждой вершиной  $u \in V$  свяжем логическую переменную  $x_u$  и пусть  $x_u$  означает, что  $u \in T$ .

1. Построить формулу  $F = \&_{u \in V} (x_u \vee (\bigvee_{(u,v) \in E} x_v))$ , условие внешней устойчивости графа  $G$ .
2. Построить минимальную ДНФ  $D$  формулы  $F$ .
3. Для каждого дизъюнктивного слагаемого  $K = x_u x_v \dots x_w$  в  $D$  получить соответствующее ему минимальное внешне устойчивое множество вершин  $S = \{u, v, \dots, w\}$ .
4. Из полученных минимальных внешне устойчивых множеств вершин выбрать все наименьшие.

**Замечание.** Этот алгоритм пригоден и для ориентированных графов.

**Решение.** Условие внешней устойчивости для графа  $G$

$$F = \&_{u \in V} (u \vee (\bigvee_{(u,v) \in E} x_v)) = (1 \vee 2 \vee 3 \vee 5 \vee 6)(2 \vee 1 \vee 3)(3 \vee 1 \vee 2 \vee 4 \vee 6) \& (4 \vee 3 \vee 5 \vee 7)(5 \vee 1 \vee 4 \vee 6)(6 \vee 1 \vee 3 \vee 5 \vee 7)(7 \vee 4 \vee 6) = \\ 156 \vee 17 \vee 246 \vee 247 \vee 257 \vee 245 \vee 256 \vee 267 \vee 357 \vee 36 \vee 34 \vee 14.$$

Все минимальные внешне устойчивые множества:

$$\{1,5,6\}, \{1,7\}, \{2,4,6\}, \{2,4,7\}, \{2,5,7\}, \{2,4,5\}, \{2,5,6\}, \{2,6,7\}, \\ \{3,5,7\}, \{3,6\}, \{3,4\}, \{1,4\}.$$

Из полученных множеств выбираем наименьшие по мощности. Они и составят все наименьшие внешне устойчивые множества вершин:

$$\{1,7\}; \{3,6\}; \{3,4\}; \{1,4\}.$$

**Задача 14.** В заданном ориентированном графе  $G$  из задачи 11 найти все минимальные и все наименьшие внешне устойчивые (доминирующие) множества вершин.

**Пример.** Граф  $G = (V, E) = (V=\{1,2,3,4,5\}, E=\{(1,4), (1,5), (2,1), (2,3), (3,1), (3,4), (4,5), (5,2)\})$ .

**Замечание.** Алгоритм для неориентированных графов пригоден и для ориентированных графов.

*Решение.* Условие внешней устойчивости для графа  $G$

$$F = \&_{u \in V} (u \vee (\bigvee_{(u,v) \in E} x_v)) = (1 \vee 4 \vee 5)(2 \vee 1 \vee 3)(3 \vee 1 \vee 4 \vee 6)(4 \vee 5)(5 \vee 2 = \\ 35 \vee 24 \vee 15.$$

Все минимальные внешне устойчивые множества:  $\{3,5\}$ ,  $\{2,4\}$ ,  $\{1,5\}$ .

Из полученных множеств выбираем наименьшие по мощности. Они и составляют все наименьшие внешне устойчивые множества вершин:

$$\{3,5\}, \{2,4\}, \{1,5\}.$$

**Задача 15.** Найти хроматическое число графа и оптимальную раскраску графа  $G$  из задачи 1.

**Пример.**  $G = (V, E) = (V = \{1, 2, 3, 4, 5, 6, 7, 8\}, E = \{(1,2), (1,3), (1,5), (1,6), (2,3), (3,4), (3,6), (4,5), (4,7), (5,6), (6,7), (7,8)\})$ .

### Оптимальная раскраска вершин графа $G = (V, E)$

Пусть  $S_1, S_2, \dots, S_r$  есть все максимальные внутренне устойчивые множества вершин в  $G$ . С каждым  $S_i$  свяжем логическую переменную  $x_{S_i}$  и пусть  $x_{S_i}$  означает, что вершина  $v \in S_i$ .

#### 11.7. Алгоритм оптимальной раскраски $(p,q)$ -графа $G = (V, E)$

1. Построить все максимальные внутренне устойчивые множества вершин  $S_1, S_2, \dots, S_r$ .
2. Построить логическую формулу  $F$ , условие оптимальной раскраски графа  $G$ :  $F = \&_{u \in V} (\bigvee_{v \in S_i, i=1, \dots, r} x_{S_i})$ .
3. Построить минимальную ДНФ  $D$  для  $F$ .
4. Каждому дизъюнктивному слагаемому  $K_i = x_{S_a} x_{S_b} \dots x_{S_c}$  в  $D$

соответствует минимальное семейство  $L_i = \{S_a, S_b, \dots, S_c\}$  внутренне устойчивых множеств  $S_a, S_b, \dots, S_c$ . Из всех  $L_i$  выбираем наименьшее по длине  $k$  семейство  $\{S_{j_1}, S_{j_2}, \dots, S_{j_k}\}$ . Хроматическое число  $x(G) = k$ . Ему

соответствует следующая оптимальная раскраска вершин графа  $G$ . В цвета 1, 2, ...,  $k$  последовательно окрашиваем семейства вершин

$S_{j_1}, S_{j_2} - S_{j_1}, S_{j_3} - (S_{j_1} \cup S_{j_2}), \dots, S_{j_k} - (S_{j_1} \cup \dots \cup S_{j_{k-1}})$  соответственно.

*Решение.* Условие внутренней устойчивости графа  $G$

$$F = \&_{(u,v) \in E} (x_u \vee x_v) =$$

$$(1 \vee 2)(1 \vee 3)(1 \vee 5)(1 \vee 6)(2 \vee 3)(3 \vee 4)(3 \vee 6)(4 \vee 5)(4 \vee 7)(5 \vee 6)(6 \vee 7)(7 \vee 8) = \\ 23567 \vee 12467 \vee 12468 \vee 13467 \vee 13468 \vee 1357 \vee 234568.$$

Рассматривая полученные дизъюнктивные слагаемые как множества и дополняя их до множества вершин  $V$ , получим, что множество

$$S = \{S_1 = \{1, 4, 8\}, S_2 = \{3, 5, 8\}, S_3 = \{3, 5, 7\}, S_4 = \{2, 5, 8\}, \\ S_5 = \{2, 5, 7\}, S_6 = \{2, 4, 6, 8\}, S_7 = \{1, 7\}\} =$$

есть список всех максимальных (тупиковых) внутренне устойчивых множеств вершин графа  $G$ . Составляем решеточное выражение – условие оптимальной раскраски вершин графа

$$R = \& \left( \bigvee_{v \in V} \bigvee_{v \in S_i, i=1,\dots,r} i \right) = (1 \vee 7)(4 \vee 5 \vee 6)(2 \vee 3)(1 \vee 6)(2 \vee 3 \vee 4 \vee 5)6 \&$$

$$(3 \vee 5 \vee 7)(1 \vee 2 \vee 4 \vee 6) = 672 \vee 736 \vee 2651 \vee 631, \text{ где}$$

$(1 \vee 7)$  означает, что вершина 1 принадлежит  $S_1, S_7$ ;

$(4 \vee 5 \vee 6)$  означает, что вершина 2 принадлежит  $S_4, S_5, S_6$ ;

...

$(1 \vee 2 \vee 4 \vee 6)$  означает, что вершина 8 принадлежит  $S_1, S_2, S_4, S_6$ .

Из полученных дизъюнктивных слагаемых выбираем наименьшие по длине: 672, 736, 631. Построим оптимальные раскраски вершин графа по множествам  $\{S_6, S_7, S_2\}, \{S_7, S_3, S_6\}, \{S_6, S_3, S_1\}$ . Хроматическое число  $\chi(G)=3$ , т.е. для правильной раскраски вершин графа необходимо три краски.

Возможны следующие варианты оптимальной раскраски вершин.

1. Вершины  $L_1 = S_6 = \{2, 4, 6, 8\}$  окрасим цветом 1;

вершины  $L_2 = S_7 - S_6 = \{1, 7\}$  цветом 2;

вершины  $L_3 = S_2 - (S_6 \cup S_7) = \{3, 5\}$  цветом 3.

2.  $L_1 = S_7 = \{1, 7\}; L_2 = S_3 - S_7 = \{3, 5\}; L_3 = S_6 - (S_7 \cup S_3) = \{2, 4, 6, 8\}$ .

3.  $L_1 = S_6 = \{2, 4, 6, 8\}; L_2 = S_3 - S_6 = \{3, 5, 7\}; L_3 = S_1 - (S_6 \cup S_3) = \{1\}$ .

**Задача 16.** Найти максимальный поток и минимальный разрез между вершинами  $s$  и  $t$  в транспортной сети с ориентированным графом

$G = (V, E)$ , где

$V = \{s, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, t\}$ ,

$E = \{(s, 1), (s, 2), (s, 3), (1, 2), (1, 4), (1, 5), (2, 6), (2, 9), (3, 2), (3, 6), (3, 7), (4, 5), (4, 8), (4, 11), (5, 8), (5, 10), (6, 1), (7, 10), (7, t), (8, t), (8, 9), (8, 12), (9, 6), (9, 10), (9, t), (10, t), (11, 1), (11, 12), (12, 13), (13, 8), (13, t)\}$ .

Вес  $w_{ij}$  дуги  $(i, j)$  равен  $N(i^2 + j^2) + i^2 + j^2 + i + j$  по модулю 10 (остаток от деления  $w_{ij}$  на 10).  $N$  есть номер варианта.

**Задача 16.**

$S = (V, E, s, t, c)$  есть транспортная сеть, где

$V = \{s, 1, 2, 3, 4, 5, t\}$ ,

$E = \{e_1 = (s, 1, 5), e_2 = (s, 2, 7), e_3 = (s, 3, 9), e_4 = (1, 2, 1), e_5 = (1, 4, 4), e_6 = (2, 5, 4), e_7 = (3, 5, 1), e_8 = (3, t, 1), e_9 = (4, 5, 4), e_{10} = (4, t, 2), e_{11} = (5, t, 6)\}$ .

Пропускная способность дуги  $e = (i, j, c)$  есть ее третья координата  $c$ .

Построить в сети  $S$  максимальный поток  $f_{\max} : E \rightarrow \mathbb{N}$  и минимальное сечение (разрез).

### **11.8. Помечивающий алгоритм вычисления максимального потока в транспортной сети**

Пусть  $S = (V, E, s, t, c)$  есть транспортная сеть и  $v_1, v_2, \dots, v_n$  есть внутренние вершины сети.

1. Задать начальный поток  $f$ , например, нулевой.
2. Вершину  $s$  пометим знаком  $s$ .
3. Присвоим всем вершинам сети пометки: если  $v_i$  помеченная вершина, то помечаем
  - a) знаком  $+i$  все непомеченные вершины  $v_j$ , для которых в дуге  $e=(v_i, v_j)$ , исходящей из  $v_i$ , имеем  $f(e) < c(e)$ ;
  - b) знаком  $-i$  все непомеченные вершины  $v_j$ , для которых в дуге  $e=(v_j, v_i)$ , заходящей в  $v_i$ , имеем  $f(e) > 0$ .
4. Если полюс  $t$  получил пометку, то между  $s$  и  $t$  существует неориентированный путь (его следует строить от  $t$ ), вершины которого помечены номерами предыдущих вершин (со знаком плюс или минус) и который допускает увеличение потока до потока  $f$  по правилу построения потока для найденного пути. Стираем все пометки вершин и переходим к пункту 2 с новым потоком. Если полюс  $t$  пометки не получил, то последний построенный поток максимален.

*Решение.* Граф-схема транспортной сети  $S$  приведена на рис.11.15. В скобках приведены пропускные способности ребер.

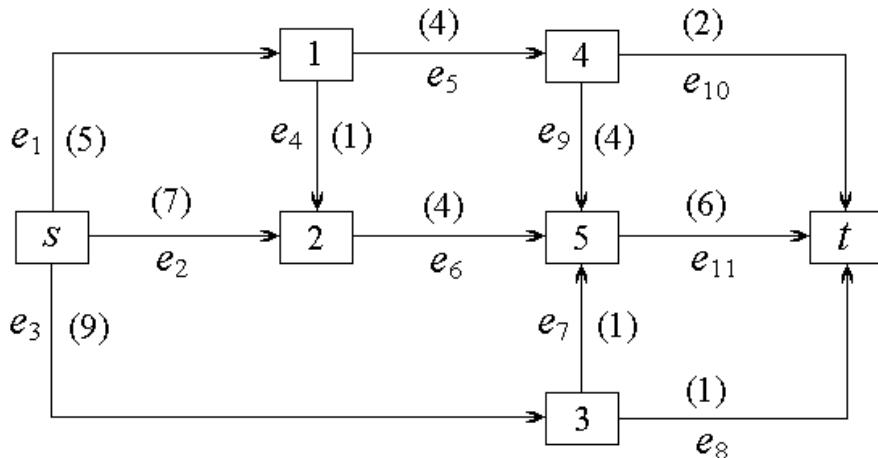


Рис.11.15

Положим начальный поток  $f_0$  нулевым. Пометим вершины сети рис.11.16). Ход от вершины  $t$  до вершины  $s$ :  $t, 5, 4, 1, s$ .

$s \rightarrow 1 \rightarrow 4 \rightarrow 5 \rightarrow t$	очередная цепь $\mu$ между $s$ и $t$
$\vec{e}_1 \quad \vec{e}_5 \quad \vec{e}_9 \quad \vec{e}_{11}$	направленность дуг в цепи $\mu$
5    4    4    6	пропускная способность $c(e)$ дуг
0    0    0    0	старый поток $f_0(e)$
5    4    4    6	$\delta = \min(c(e) - f_0(e)) = 4$
4    4    4    4	новый поток $f_1(e) = f_0(e) + \delta = f_0(e) + 4$ .

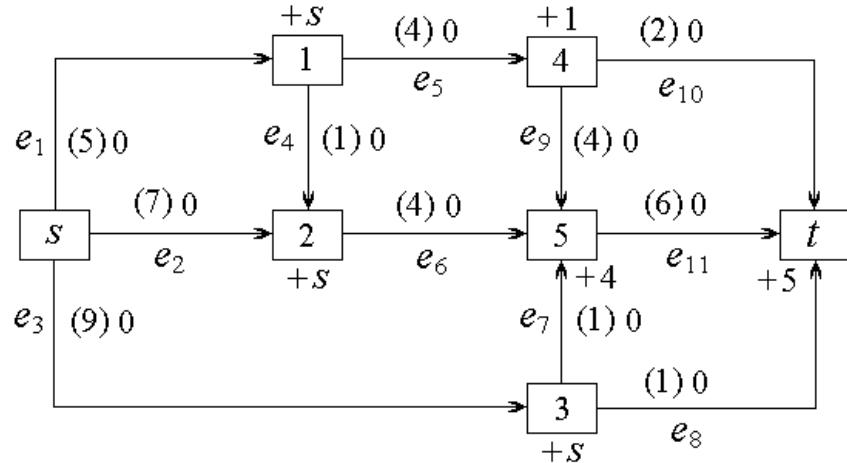
Новый поток  $f_1$  и новая разметка вершин сети приведена на рис.11.17. Ход от вершины  $t$  до вершины  $s$ :  $t, 5, 2, s$ .

$s \rightarrow 2 \rightarrow 5 \rightarrow t$	очередная цепь $\mu$ между $s$ и $t$
$\vec{e}_2 \quad \vec{e}_6 \quad \vec{e}_{11}$	направленность дуг в цепи $\mu$
7    4    6	пропускная способность $c(e)$ дуг

0	0	4	старый поток $f_1(e)$
7	4	2	$\delta = \min(c(e) - f_1(e)) = 2$
2	2	6	новый поток $f_2(e) = f_1(e) + \delta = f_1(e) + 2$ .

Новый поток  $f_2$  и новая разметка вершин сети приведена на рис.11.18.  
Ход от вершины  $t$  до вершины  $s$ :  $t, 3, s$ .

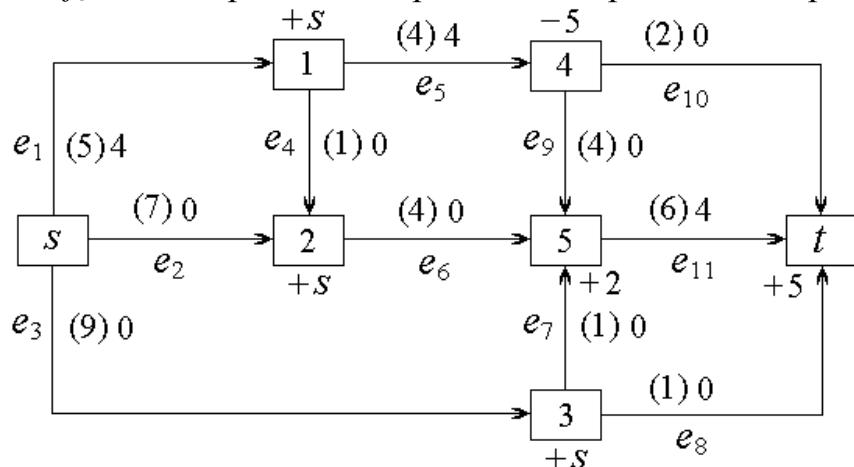
$s \rightarrow 3 \rightarrow t$	очередная цепь $\mu$ между $s$ и $t$
$\vec{e}_3$ $\vec{e}_8$	направленность дуг в цепи $\mu$
9    1	пропускная способность $c(e)$ дуг
0    0	старый поток $f_2(e)$
9    1	$\delta = \min(c(e) - f_2(e)) = 1$
1    1	новый поток $f_3(e) = f_2(e) + \delta = f_1(e) + 1$ .



Поток  $f_0$

Рис.11.16

Новый поток  $f_3$  и новая разметка вершин сети приведена на рис.11.19.



Поток  $f_1$

Рис.11.17

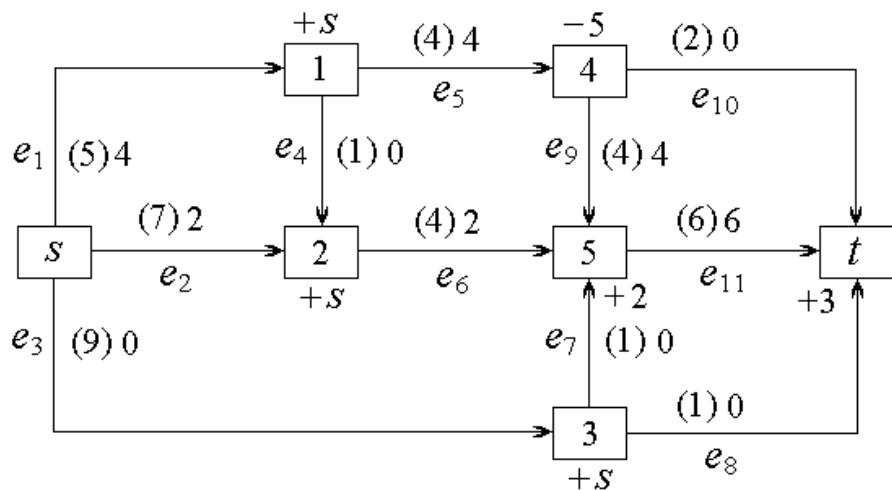
Поток  $f_2$ 

Рис.11.18

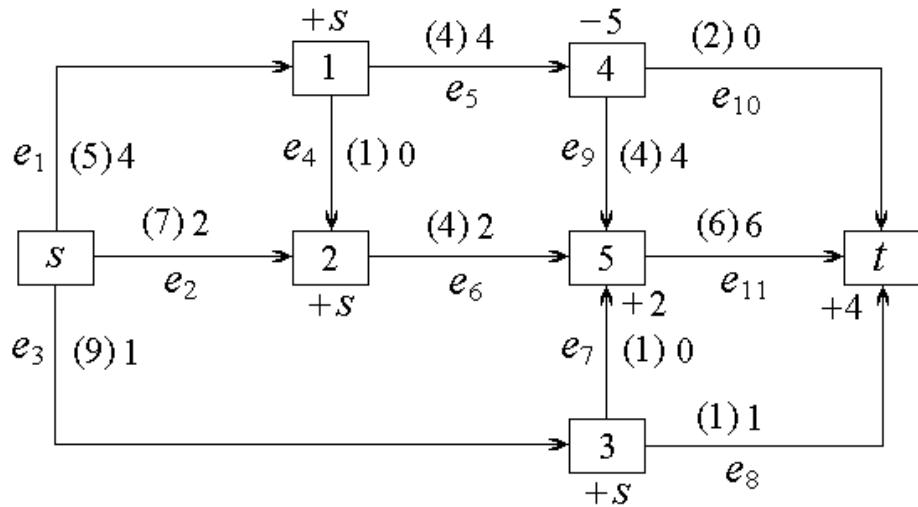
Поток  $f_3$ 

Рис.11.19

Ход от вершины  $t$  до вершины  $s$ :  $t, 4, 5, 2, s$ .

$s \rightarrow 2 \rightarrow 5 \leftarrow 4 \rightarrow t$  очередная цепь  $\mu$  между  $s$  и  $t$

$\vec{e}_2 \quad \vec{e}_6 \quad \bar{e}_9 \quad \bar{e}_{10}$  направленность дуг в цепи  $\mu$

7 4 4 2 пропускная способность  $c(e)$  дуг

2 2 4 0 старый поток  $f_3(e)$

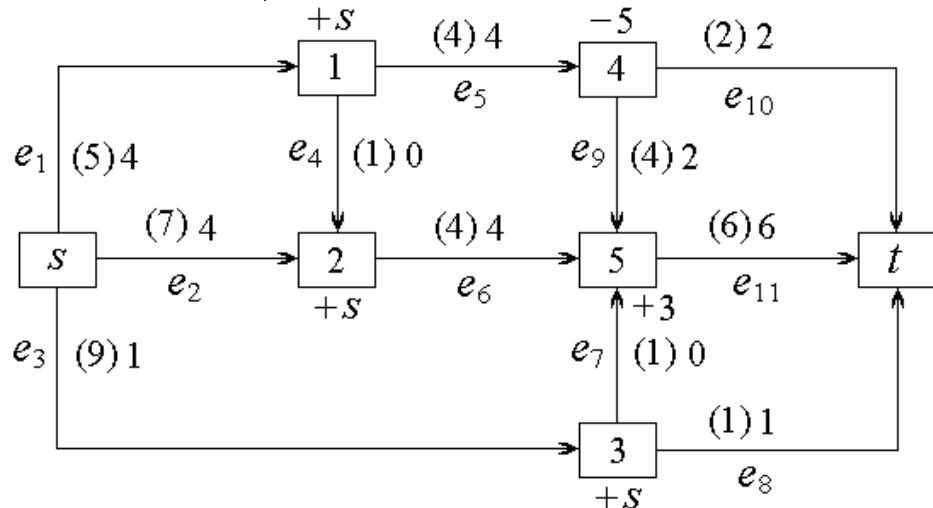
5 2 - 2  $\delta = \min(c(\vec{e}) - f_3(\vec{e})) = 2$

- - 4 -  $\eta = \min(f_3(\bar{e})) = 4; \varepsilon = \min(\delta, \eta) = 2$

4 4 2 2 новый поток  $f_4(e) = f_3(e) \begin{cases} +\varepsilon & \text{à } \vec{e}, \\ -\varepsilon & \text{à } \bar{e}. \end{cases}$

Новый поток  $f_4$  и новая разметка вершин сети приведена на рис.11.20. Вершина  $t$  пометки не получила. От  $s$  до  $t$  новой цепи построить не удается. Последний поток  $f_4$  есть максимальный и величина потока  $M_{f\max} = 9$ .

Максимально возможная величина потока (нагружающая дуги истока, равно как и дуги стока)  $M_{f\max} = 9$ .



Поток  $f_4$

Рис.11.20

Минимальный разрез  $MS$  есть множество дуг для  $f_4$  на рис.33.13, заходящих в непомеченные вершины из помеченных вершин.  $MS = \{e_8, e_{10}, e_{11}\} = \{(3,t,1),(4,t,2),(5,t,6)\}$ . Пропускная способность минимального разреза  $c_{\min} = M_{f\max} = f_4(e_8) + f_4(e_{11}) + f_4(e_{12}) = 1+2+6 = 9$ .

*Ответ.*  $MS = \{e_8, e_{10}, e_{11}\}$ ,  $M_{f\max} = f_4(e_1) + f_4(e_2) + f_4(e_3) = 4+4+1 = 9$ .

**Задача 17.** Найти число ожерелей, которые можно составить из семи бусин не более чем  $t$  цветов. Число цветов  $t$  равно числу букв в фамилии студента. Цвета бусины обозначить буквами фамилии студента. Недостающие буквы взять из алфавита. Не должно быть повторов букв.

**Пример.** Найти число ожерелей, которые можно составить из шести бусин не более чем  $t=2$  цветов, синего и красного.

**Решение.** Ожерелье типа  $(n, k)$  есть правильный  $n$ -угольник, вершины которого раскрашены в не более чем  $k$  цветов. Два ожерелья *неотличимы* (одинаковы), если одно можно получить из другого, поворачивая его относительно точки симметрии или симметрично отражая относительно одной из осей симметрии.

Для подсчета числа ожерелей типа  $(n, k)$  нужно найти группу  $G$  вращений и симметрий правильного  $n$ -угольника, которая есть некоторая группа подстановок на множестве  $X = \{1, 2, \dots, n\}$ , потом составить многочлен циклов, а затем применить теорему Пойа.

Подсчитаем число ожерелей, которые можно составить из шести бусин (рис.11.21) не более чем двух цветов, синего и красного.

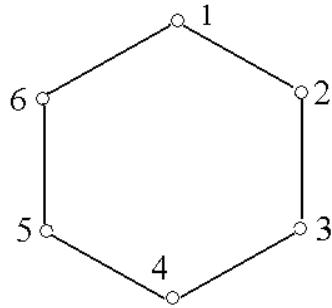


Рис.11.21

Для перечисленных операций соответствующая группа  $G$  состоит из 12 следующих подстановок, которые распределены по типам следующим образом.

Повороты.

$$p_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)(6), \langle 1,1,1,1,1,1 \rangle.$$

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (123456), \langle 6 \rangle.$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (135)(246), \langle 3,3 \rangle.$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (14)(25)(36), \langle 2,2,2 \rangle.$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (153)(264), \langle 3,3 \rangle.$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (165432), \langle 6 \rangle.$$

Симметрия относительно диагоналей.

$$p_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix} = (1)(26)(35)(4), \langle 1,1,2,2 \rangle.$$

$$p_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix} = (13)(2)(46)(5), \langle 1,1,2,2 \rangle.$$

$$p_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = (15)(24)(3)(6), \langle 1,1,2,2 \rangle.$$

Симметрия относительно прямых через середины сторон.

$$p_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = (12)(36)(45), \langle 2,2,2 \rangle.$$

$$p_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} = (14)(23)(56), \langle 2,2,2 \rangle$$

$$p_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (16)(25)(34), \langle 2,2,2 \rangle.$$

Мы получили следующее.

1 подстановка  $p_0$  типа  $<1,1,1,1,1,1>$  дает слагаемое  $s_1^6$  и  $m^6$  неподвижных точек.

2 подстановки  $p_1, p_5$  типа  $<6>$  дают слагаемое  $2s_6$  и  $2m$  неподвижных точек.

2 подстановки  $p_2, p_4$  типа  $<3,3>$  дают слагаемое  $2s_3^2$  и  $2m^2$  неподвижных точек.

4 подстановки  $p_3, p_9, p_{10}, p_{11}$  типа  $<2,2,2>$  дают слагаемое  $4s_2^3$  и  $4m^3$  неподвижных точек.

3 подстановки  $p_6, p_7, p_8$  типа  $<1,1,2,2>$  дают слагаемое  $3s_1^2 s_2^2$  и  $3m^2 m^2$  неподвижных точек.

По теореме Пойа число орбит  $N(G) = |G|^{-1} \sum_{p \in G} \prod_{k=1}^n s_k^{j_k(p)} \Big|_{s_k=m}$ .

Из 6 бусин не более чем двух цветов можно составить

$$\begin{aligned} N(G) &= |G|^{-1} \sum_{p \in G} \prod_{k=1}^n s_k^{j_k(p)} \Big|_{s_k=m=2} = \\ &(1/12) \cdot (s_1^6 + 2s_6 + 2s_3^2 + 4s_2^3 + 3s_1^2 s_2^2) \Big|_{s_1=\dots=s_6=m=2} = \\ &(1/12) \cdot (m^6 + 2 \cdot m + 2 \cdot m^2 + 4 \cdot m^3 + 3 \cdot m^2 \cdot m^2) = \\ &(1/12) \cdot (2^6 + 2 \cdot 2 + 2 \cdot 2^2 + 4 \cdot 2^3 + 3 \cdot 2^2 \cdot 2^2) = \\ &(1/12) \cdot (64 + 4 + 8 + 32 + 48) = 156/12 = 13 \text{ ожерелий.} \end{aligned}$$

**Замечание.** Если число бусин нечетно, то из движений будут лишь повороты и симметрии относительно прямых через вершины и середины противоположных сторон.

**Задача 18.** Найти число различных раскрасок вершин многогранника  $M$  в не более чем  $m$  цветов. Многогранник  $M$  составлен из двух одинаковых правильных четырехугольных пирамид с общим основанием и вершинами, расположенными по разные стороны от основания. Число цветов  $m$  равно числу букв в фамилии студента. Недостающие буквы взять из алфавита. Не должно быть повторов букв.

**Пример.** Найти число различных раскрасок вершин куба в не более, чем  $m=3$  цветов.

**Решение.** Две раскраски считаются одинаковыми, если вращением куба в пространстве их раскраски можно совместить. Восемь вершин куба не более чем тремя красками, например, синей, зеленой, красной (с,з,к) можно раскрасить  $3^8 = 6561$  способами. Многие раскраски окажутся одинаковыми.

Для вычисления числа раскрасок вершин куба нужно сделать следующее.

Вычислить группу вращений куба (рис.11.22), состоящую из подстановок, в которых укажем только вторую строку подстановки. Вращение по часовой стрелке. Циклы пишем в естественном порядке. Например, при вращении куба относительно оси, проходящей через середины граней 1584 и 2673 на 90, 180, 270 градусов, получим следующие подстановки.

$$(1,5,8,4)(2,6,7,3), (1,8)(5,4)(2,7)(6,3), (1,4,8,5)(5,4)(2,3,7,6).$$

Среднюю подстановку пишем в естественном порядке:  $(1,8)(2,7)(3,6)(4,5)$ . В угловых скобках пишем тип каждой подстановки.

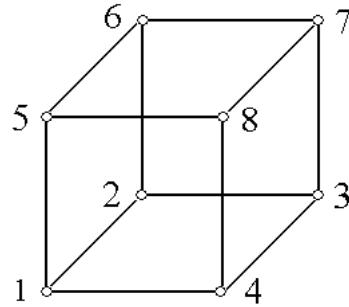


Рис.11.22

**Тождественная подстановка.**

$$p_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = (1)(2)(3)(4)(5)(6)(7)(8), \text{ тип } <1,1,1,1,1,1,1,1>.$$

8 циклов длины 1.

**1. Центры противоположных граней.**

**Середина грани 1584.**

Поворот на 90 градусов.

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 2 & 1 & 8 & 7 & 3 & 4 \end{pmatrix} = (1584)(2673), \text{ тип } <4,4>.$$

2 цикла длины 4.

Поворот на 180 градусов.

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (18)(27)(36)(45), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

Поворот на 270 градусов.

$$p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 2 & 6 & 5 \end{pmatrix} = (1562)(3487), \text{ тип } <4,4>.$$

**Середина грани 1562.**

Поворот на 90 градусов.

$$p_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 4 & 8 & 6 & 2 & 3 & 7 \end{pmatrix} = (1584)(2673), \text{ тип } <4,4>.$$

2 цикла длины 4.

Поворот на 180 градусов.

$$p_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \end{pmatrix} = (16)(25)(38)(47), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

Поворот на 270 градусов.

$$p_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 3 & 1 & 5 & 8 & 4 \end{pmatrix} = (1265)(3784), \text{ тип } <4,4>.$$

2 цикла длины 4.

**Середина грани 1234.**

Поворот на 90 градусов.

$$p_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix} = (1234)(5678), \text{ тип } <4,4>.$$

2 цикла длины 4.

Поворот на 180 градусов.

$$p_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix} = (13)(24)(57)(86), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

Поворот на 270 градусов.

$$p_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 3 & 8 & 5 & 6 & 7 \end{pmatrix} = (1432)(5876), \text{ тип } <4,4>.$$

2 цикла длины 4.

## **2. Четыре диагонали куба.**

### **Диагональ 17.**

Поворот на 120 градусов.

$$p_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 3 & 8 & 5 & 6 & 7 \end{pmatrix} = (1)(254)(368)(7), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

Поворот на 240 градусов.

$$p_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 8 & 5 & 2 & 3 & 7 & 6 \end{pmatrix} = (1)(245)(386)(7), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

### **Диагональ 28.**

Поворот на 120 градусов.

$$p_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 7 & 4 & 1 & 5 & 8 \end{pmatrix} = (2)(136)(475)(8), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

Поворот на 240 градусов.

$$p_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 1 & 5 & 7 & 3 & 4 & 8 \end{pmatrix} = (2)(163)(457)(8), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

### **Диагональ 35.**

Поворот на 120 градусов.

$$p_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 3 & 2 & 5 & 8 & 4 & 1 \end{pmatrix} = (3)(168)(274)(5), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

Поворот на 240 градусов.

$$p_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 3 & 7 & 5 & 1 & 2 & 6 \end{pmatrix} = (3)(186)(247)(5), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

### **Диагональ 46.**

Поворот на 120 градусов.

$$p_{16} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 4 & 2 & 6 & 5 & 1 \end{pmatrix} = (4)(638)(275)(6), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

Поворот на 240 градусов.

$$p_{17} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 1 & 4 & 7 & 6 & 2 & 3 \end{pmatrix} = (4)(183)(257)(6), \text{ тип } <1,1,3,3>.$$

2 цикла длины 1, 2 цикла длины 3.

### **3. Середины противоположных ребер.**

*Ребра 15, 37.*

Поворот на 180 градусов.

$$p_{18} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 & 1 & 4 & 3 & 2 \end{pmatrix} = (15)(28)(37)(46), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

*Ребра 26, 48.*

Поворот на 180 градусов.

$$p_{19} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 5 & 8 & 3 & 2 & 1 & 4 \end{pmatrix} = (17)(26)(35)(48), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

*Ребра 14, 67.*

Поворот на 180 градусов.

$$p_{20} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 5 & 1 & 3 & 7 & 6 & 2 \end{pmatrix} = (14)(28)(35)(67), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

*Ребра 23, 58.*

Поворот на 180 градусов.

$$p_{21} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 2 & 6 & 8 & 4 & 1 & 5 \end{pmatrix} = (17)(23)(46)(58), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

*Ребра 12, 78.*

Поворот на 180 градусов.

$$p_{22} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 6 & 3 & 4 & 8 & 7 \end{pmatrix} = (12)(35)(46)(78), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

*Ребра 34, 56.*

Поворот на 180 градусов.

$$p_{23} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} = (17)(28)(34)(56), \text{ тип } <2,2,2,2>.$$

4 цикла длины 2.

Это составляет 24 подстановки группы  $G$ .

В группе вращений  $G$  куба по типу каждой подстановки найти соответствующее слагаемое в многочлене циклов (в цикловом индексе). В группе вращений  $G$  куба они следующие.

1 подстановка типа  $<1,1,1,1,1,1,1,1>$  из 8 циклов дает  $3^8$  неподвижных точек и соответствует слагаемому  $s_1^8$  многочлена циклов;

6 подстановок типа  $<4,4>$  (это 2 цикла длины 4) дают  $6 \cdot 3^2$  неподвижных точек и соответствуют слагаемому  $6 s_4^2$  многочлена циклов;

9 подстановок типа  $<2,2,2,2>$  (это 4 цикла длины 2) дают  $9 \cdot 3^4$  неподвижных точек и соответствуют слагаемому  $9 s_2^4$  многочлена циклов;

8 подстановок типа  $<1,1,3,3>$  (это 4 цикла, из которых 2 длины 1 и других 2 длины 3) дают  $8 \cdot 3^4$  неподвижных точек и соответствуют слагаемому  $8 s_1^2 s_3^2$  многочлена циклов.

По теореме Пойа многочлен циклов  $N(G_M) = |G|^{-1} \sum_{p \in G} \prod_{k=1}^n s_k^{j_k(p)}$ .

Число различных раскрасок вершин куба в не более чем  $m=3$  цвета есть число

$$N(G_M) = |G|^{-1} \sum_{p \in G} \prod_{k=1}^n s_k^{j_k(p)} \Big|_{s_k=m=3} = |G|^{-1} (s_1^8 + 6s_4^2 + 9s_2^4 + 8s_1^2 s_3^2) \Big|_{s_1=\dots=s_8=3} = \\ (1/24) \cdot (m^8 + 6 \cdot m^2 + 9 \cdot m^4 + 8 \cdot m^2 m^2) = (1/24) \cdot (3^8 + 6 \cdot 3^2 + 9 \cdot 3^4 + 8 \cdot 3^4) = 333.$$

*Ответ.* 333 есть число различных раскрасок вершин куба не более чем тремя красками.

**Задача 19.** Кодер и декодер Прюфера для деревьев.

#### *Алгоритм кодирования (кодер)*

**ВХОД.** Дерево  $T$  с вершинами  $V = \{1, 2, \dots, p\}$ .

**ВЫХОД.** Упорядоченный набор  $C$  с повторами элементов из  $V$  длины  $p-2$  (код Прюфера).

1.  $C := ()$ , пустой набор.

2. Пока не останется одно ребро, выполнять следующее.

Найти в дереве лист с наименьшим номером, удалить его вместе с инцидентным с ним ребром и приписать в  $C$  справа смежную с удаленным листом вершину  $t$ .

3. Вернуть код Прюфера  $C$ .

**Замечание.** Выбор в дереве  $T$  очередного листа единственен. Поэтому каждому дереву соответствует единственный набор длины  $p-2$ . Число наборов с повторами из  $p$ -элементного множества  $V$  с  $p-2$  элементами равно  $p^{p-2}$ . Поэтому число помеченных деревьев  $t_p \leq p^{p-2}$ .

**Пример.** Дерево  $T = (V, E)$ , где  $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ,  $E = \{(1, 2), (1, 7), (1, 8), (2, 6), (3, 5), (4, 5), (5, 6), (5, 9)\}$ . На рис.17.1 изображены дерево  $T$  и последовательные шаги удаления листьев с принадлежащими им ребрами и формирования кода Прюфера.

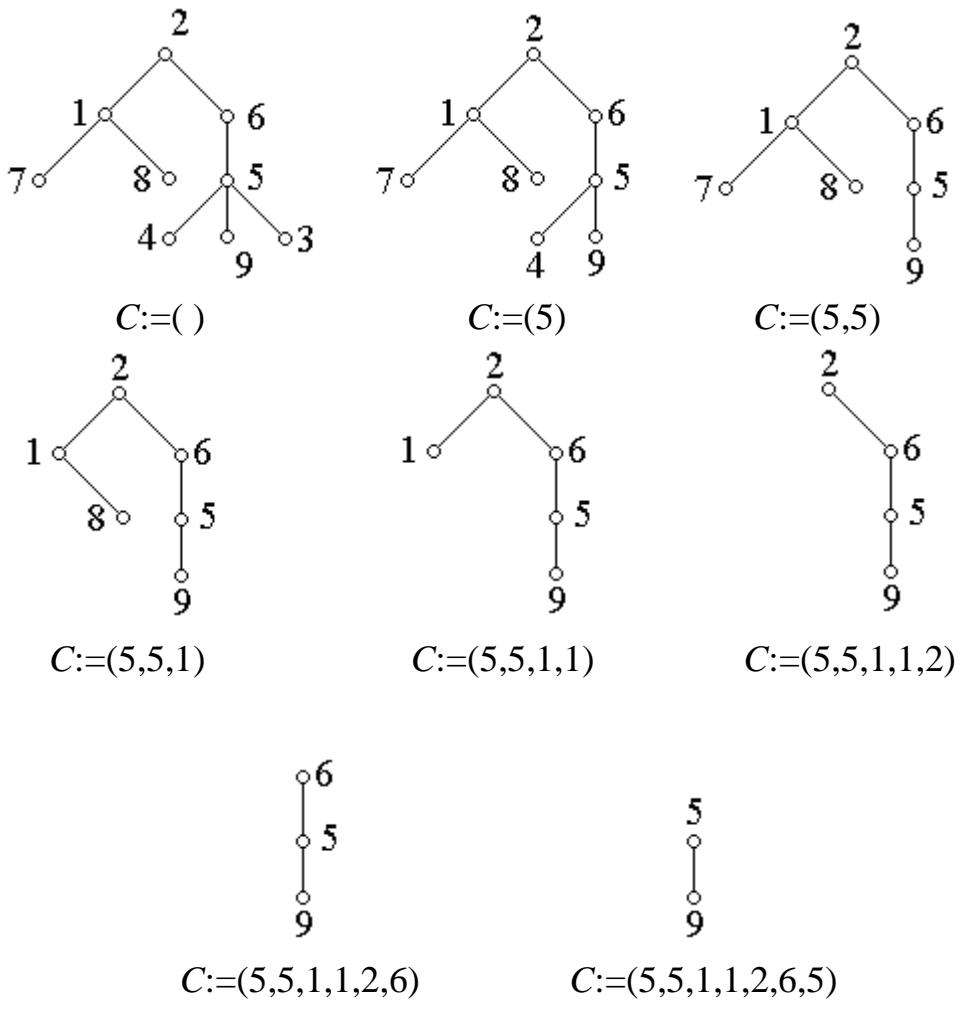


Рис.17.1

*Ответ.* Код Прюфера  $C=(5,5,1,1,2,6,5)$ .

### Алгоритм декодирования (декодер)

**ВХОД.** Код Прюфера  $C$  для дерева.

**ВЫХОД.** Дерево, соответствующее коду  $C$ .

1.  $n := |C|$ ;  $p := n+2$ . Множество вершин  $V := \{1, 2, \dots, p\}$ .

Множество ребер  $E = \emptyset$ .

2. Найти наименьший элемент  $m$  в множестве  $V$ , которого нет в  $C$ .

3. Взять первый элемент  $c$  в наборе  $C$ .

4. Множество ребер  $E := E \cup \{e = (m, c)\}$ .

5.  $V := V - \{m\}$ ,  $C := C - \{c\}$ .

7. Если  $V = \{u, v\}$  состоит из двух элементов, то  $E := E \cup \{(u, v)\}$ . Вернуть  $E$ .

8. Перейти к пункту 2.

**Замечание.** Выбор наименьшего элемента  $m$  в множестве  $V$  в пункте 2 единственен. Первый элемент  $c$  в множестве  $C$  в пункте 3 единственен. Поэтому для каждого кода Прюфера строится единственное ему соответствующее дерево. Число кодов Прюфера есть число наборов с

повторами из  $p$ -элементного множества с  $p-2$  элементами, равное  $p^{p-2}$ . Поэтому число деревьев  $t_p \geq p^{p-2}$ .

**Пример.** Код Прюфера  $C=(5,5,1,1,2,6,5)$ . Строим соответствующее дерево.  $|C| = n = 7$ . Число  $|V| = n+2 = 7+2 = 9$ . Множество вершин  $V = \{1,2,3,4,5,6,7,8,9\}$ . Множество ребер  $E=\emptyset$ . Вычисления сведены в табл.17.3.

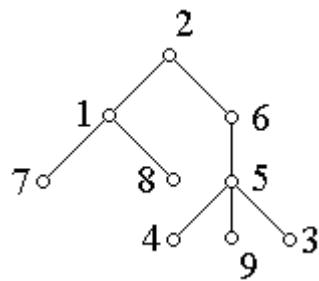
**Теорема.** (Кэли, Cayley). Число различных деревьев с  $p$  вершинами  $t_p = p^{p-2}$ . Доказательство следует из двух ранее полученных неравенств:  $t_p \leq p^{p-2}$ ,  $t_p \geq p^{p-2}$ .

Таблица 17.3

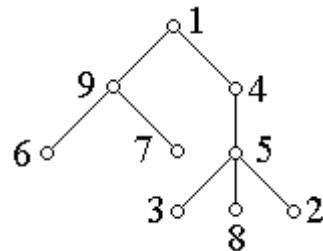
№	$V$ есть вершины в дереве $T$	$m$ есть наименьший элемент в $V$ , которого нет в $C$ . $c$ есть первый элемент в $C$ .	Ребро $(m,c)$ в дереве $T$	$V:=V-\{m\}$ $C:=C-\{c\}$
1	$V := (1,2,\mathbf{3},4,5,6,7,8,9)$ $C := (\mathbf{5},5,1,1,2,6,5)$	$m:=3$ $c:=5$	$e_1:=(3,5)$	$V:=V-\{3\}$ $C:=C-\{5\}$
2	$V =: \{1,2,\mathbf{4},5,6,7,8,9\}$ $C =: (\mathbf{5},1,1,2,6,5)$ .	$m:=4$ $c:=5$	$e_2:=(4,5)$	$V:=V-\{4\}$ $C:=C-\{5\}$
3	$V =: \{1,2,5,6,\mathbf{7},8,9\}.$ $C =: (\mathbf{1},1,2,6,5)$ .	$m:=7$ $c:=1$	$e_3:=(7,1)$	$V:=V-\{7\}$ $C:=C-\{1\}$
4	$V =: \{1,2,5,6,\mathbf{8},9\}.$ $C =: (\mathbf{1},2,6,5)$ .	$m:=8$ $c:=1$	$e_4:=(8,1)$	$V:=V-\{8\}$ $C:=C-\{1\}$
5	$V =: \{1,2,5,6,9\}.$ $C =: (\mathbf{2},6,5)$ .	$m:=1$ $c:=2$	$e_5:=(1,2)$	$V:=V-\{1\}$ $C:=C-\{2\}$
6	$V =: \{2,5,6,9\}.$ $C =: (\mathbf{6},5)$ .	$m:=2$ $c:=6$	$e_6:=(2,6)$	$V:=V-\{2\}$ $C:=C-\{6\}$
7	$V =: \{5,\mathbf{6},9\}.$ $C =: (\mathbf{5})$ .	$m:=6$ $c:=5$	$e_7:=(6,5)$	$V:=V-\{6\}$ $C:=C-\{5\}$
8	$V =: \{5,9\}.$ $C =: ()$ .		$e_8:=(5,9)$	

*Ответ.*  $E = \{(3,5),(4,5),(7,1),(8,1),(1,2),(2,6),(6,5),(5,9)\}$  есть множество ребер графа  $G$ .

**Варианты.** Взять ниже следующее дерево  $T$ .



Взять вариант с номером вашей фамилии в аудиторном журнале, например, 30. Перенумеровать вершины данного дерева в соответствии с заданием 33.30:  $1 \rightarrow 9$ ,  $2 \rightarrow 1$ ,  $3 \rightarrow 2$ ,  $4 \rightarrow 3$ ,  $5 \rightarrow 5$ ,  $6 \rightarrow 4$ ,  $7 \rightarrow 6$ ,  $8 \rightarrow 7$ ,  $9 \rightarrow 8$ . Получить следующее дерево  $T$ .



Для полученного дерева  $T$  найти его код Прюфера  $C$ .

Декодировать код  $C$  и получить дерево  $T$ .

- 19.1.** 234567891. **19.2.** 345678912. **19.3.** 456789123. **19.4.** 567891234.
- 19.5.** 678912345. **19.6.** 789123456. **19.7.** 891234567. **19.8.** 912345678.
- 19.9.** 198765432. **19.10.** 321987654. **19.11.** 543219876. **19.12.** 765432198.
- 19.13.** 987654321. **19.14.** 219876543. **19.15.** 432198765. **19.16.** 654321987.
- 19.17.** 876543219. **19.18.** 129876543. **19.19.** 423198765. **19.20.** 653421987.
- 19.21.** 876453219. **19.22.** 218756439. **19.23.** 132986721. **19.24.** 654321789.
- 19.25.** 763542189. **19.26.** 981246367. **19.27.** 987123456. **19.28.** 157689231.
- 19.29.** 934657812. **19.30.** 912354678.

## 6. КОНЕЧНЫЕ АВТОМАТЫ

**Задача 1.** Построить по автомату Мили  $A = (X, Y, Q, q_1, T, B)$  (рис.6.1) эквивалентный ему автомат Мура. Множества входных и выходных символов  $X = \{0, 1, 2\}$ ,  $Y = \{a, b, c\}$ . Вариант автомата получить, взяв указанный в варианте переход из одного состояния в другое при поступлении на вход автомата указанных в варианте входного и выходного символов. Например, в варианте 30 указан переход  $(q_2, 0a, q_2)$ . Это значит, что из граф-схемы автомата  $A$  надо удалить стрелку  $(q_2, 0a, q_4)$  и добавить стрелку  $(q_2, 0a, q_2)$ .

**Определение.** Автомат Мили есть система объектов  $A = (X, Y, Q, q_0, T, B)$ , где  $X$  есть входной алфавит;  $Y$  есть выходной алфавит;  $Q$  есть алфавит (внутренних) состояний;  $q_0 \in Q$  есть начальное состояние;  $T : X \times Q \rightarrow Q$  есть функция переходов;  $B : X \times Q \rightarrow Y$  есть функция выходов.

Автомат Мили можно задать каноническими уравнениями

$$\begin{aligned} q(0) &= q_0, \\ q(t+1) &= T(q(t), x(t)), \\ y(t) &= B(q(t), x(t)). \end{aligned}$$

**Определение.** Автомат Мура есть система объектов  $A = (X, Y, Q, q_0, T, B)$ , где  $X, Y, Q, q_0, T$  задаются как для автомата Мили, а  $B : Q \rightarrow Y$  есть функция выходов. Канонические уравнения автомата Мура имеют вид

$$\begin{aligned} q(0) &= q_0, \\ q(t+1) &= T(q(t), x(t)), \\ y(t) &= B(q(t)). \end{aligned}$$

**Замечание.** Автомат Мура есть частный случай автомата Мили. Автомат Мура проще и потому в некоторых случаях предпочтительнее автомата Мили.

**Определение.** Два автомата с выходом эквивалентны, если они реализуют один и тот же оператор  $\mathcal{O} : X^* \rightarrow Y^*$ .

**Теорема.** По любому автомату Мили можно построить эквивалентный ему автомат Мура.

**Доказательство.** Пусть  $A = (X, Y, Q, q_0, T, B)$  есть автомат Мили. Построим автомат Мура  $A' = (X, Y, Q', q', T', B')$ , положив

$$\begin{aligned} q' &= q_0; \\ Q' &= \{q_0\} \cup \{(q, a) : q \in Q, a \in X\}; \\ T'((q, a), b) &= (T(q, a), b), q \in Q, \{a, b\} \subseteq X; \\ B'((q, a)) &= B(q, a), q \in Q, a \in X. \end{aligned}$$

Построенный автомат Мура эквивалентен автомату Мили; однако для этого необходимо пренебречь выходом автомата Мура в начальный момент времени.

**Пример.** Для автомата Мили из табл.27.1 функции переходов и выходов эквивалентного ему автомата Мура приведены в табл.27.3. Выход  $B'(q_0)$  произволен.

Автомат Мили. Алфавиты  $X = \{0,1\}$ ;  $Y = \{0,1,2\}$ ; Множество состояний  $Q = \{q_0, q_1, q_2\}$ ; функции переходов и выходов задаются в табл.27.1 или граф-схемой (рис.27.1).

Table 27.1

	$q_1$	$q_2$	$q_3$
0	$q_3/1$	$q_3/0$	$q_1/1$
1	$q_2/2$	$q_3/2$	$q_2/2$

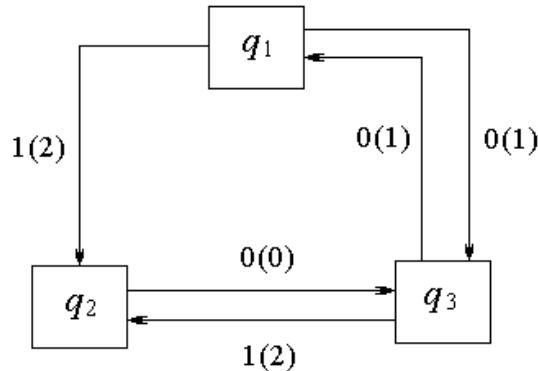


Рис.27.1

Table 27.3

	$q_0$	1 ( $q_0,0$ )	2 ( $q_0,1$ )	0 ( $q_1,0$ )	2 ( $q_1,1$ )	1 ( $q_2,0$ )	2 ( $q_2,1$ )
0	( $q_0,0$ )	( $q_2,0$ )	( $q_2,0$ )	( $q_2,0$ )	( $q_2,0$ )	( $q_1,0$ )	( $q_1,0$ )
1	( $q_0,1$ )	( $q_1,1$ )	( $q_1,1$ )	( $q_2,1$ )	( $q_2,1$ )	( $q_2,1$ )	( $q_2,1$ )

Общий для всех вариантов автомат Мили, рис.6.1.

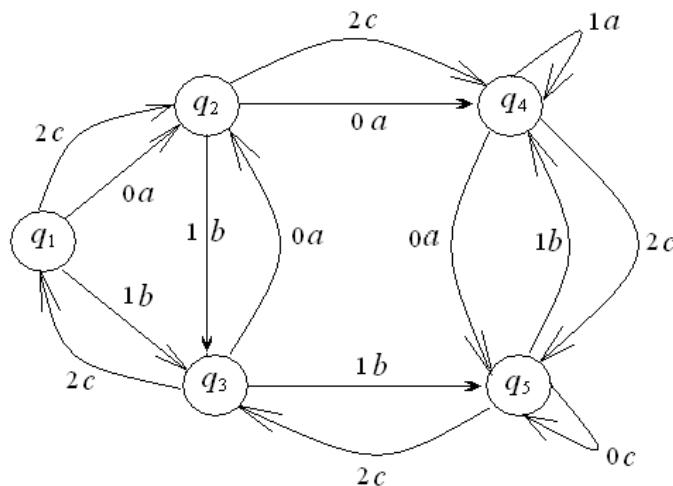


Рис.6.1

### Варианты.

- 1.1. ( $q_1, 2c, q_1$ ).    1.2. ( $q_1, 2c, q_3$ ).    1.3. ( $q_1, 2c, q_4$ ).    1.4. ( $q_1, 2c, q_5$ ).
- 1.5. ( $q_2, 2c, q_1$ ).    1.6. ( $q_2, 2c, q_2$ ).    1.7. ( $q_2, 2c, q_3$ ).    1.8. ( $q_2, 2c, q_5$ ).
- 1.9. ( $q_3, 2c, q_2$ ).    1.10. ( $q_3, 2c, q_3$ ).    1.11. ( $q_3, 2c, q_4$ ).    1.12. ( $q_3, 2c, q_5$ ).
- 1.13. ( $q_4, 2c, q_1$ ).    1.14. ( $q_4, 2c, q_2$ ).    1.15. ( $q_4, 2c, q_3$ ).    1.16. ( $q_4, 2c, q_4$ ).

- 1.17.** ( $q_5, 2c, q_1$ ). **1.18.** ( $q_5, 2c, q_2$ ). **1.19.** ( $q_5, 2c, q_4$ ). **1.20.** ( $q_5, 2c, q_5$ ).  
**1.21.** ( $q_1, 0a, q_1$ ). **1.22.** ( $q_1, 0a, q_3$ ). **1.23.** ( $q_1, 0a, q_4$ ). **1.24.** ( $q_1, 0a, q_5$ ).  
**1.25.** ( $q_1, 1b, q_1$ ). **1.26.** ( $q_1, 1b, q_2$ ). **1.27.** ( $q_1, 1b, q_4$ ). **1.28.** ( $q_1, 1b, q_5$ ).  
**1.29.** ( $q_2, 0a, q_1$ ). **1.30.** ( $q_2, 0a, q_2$ ). **1.31.** ( $q_2, 0a, q_3$ ). **1.32.** ( $q_2, 0a, q_5$ ).

**Задача 2.** Построить автоматы  $A = (X, Q, q_1, T, F)$  для объединения и для пересечения двух языков, представимых детерминированными автоматами  $A' = (X, Q', q_1', T', F')$ ,  $A'' = (X, Q'', q_1'', T'', F'')$  (рис.6.2) с множеством входных символов  $X = \{0, 1, 2\}$ , с начальными состояниями  $q_1'$  и  $q_1''$  и с выделенными состояниями  $F' = \{q_3', q_5'\}$ ,  $F'' = \{q_3''\}$ . Каждый вариант автомата получить, взяв указанный в варианте переход из одного состояния в другое при поступлении на вход автомата указанного в варианте входного символа. Например, в варианте 30 указан переход  $(q_3'', 1, q_2'')$ . Это значит, что из граф-схемы автомата  $A''$  надо убрать стрелку  $(q_3'', 1, q_3'')$  и добавить стрелку  $(q_3'', 1, q_2'')$ .

**Определение.** Автомат без выхода (акцептор) есть система объектов  $A = (X, Q, q_0, T, F)$ , где  $(X, Q, q_0, T)$  задаются как у автомата с выходом, а  $F \subseteq Q$  есть множество выделенных (отмеченных, заключительных, финальных) состояний. Так определенный автомат называется также *детерминированным конечным автоматом* (ДКА).

**Замечание.** Автомат без выхода можно рассматривать как автомат Мура с выходом, полагая его выход

$$y(t) = B(q(t)) = \begin{cases} 1, & \text{если } q(t) \in F, \\ 0, & \text{если } q(t) \notin F. \end{cases}$$

**Определение.** Слово  $x \in X^*$  допустимо (определимо) автоматом  $A = (X, Q, q_0, T, F)$ , если  $T(q_0, x) \in F$ . Если  $T(q_0, x) \notin F$ , то слово  $x$  не допускается (отвергается) автоматом  $A$ .

**Определение.** Поведение  $Beh(A)$  автомата  $A$  есть множество всех слов в алфавите  $X$ , допустимых автоматом  $A$ . Язык  $L \subseteq X^*$  (автоматно) определим (допустим, представим), если существует автомат  $A$  без выхода, для которого  $L = Beh(A)$ .

**Замечание.** Иногда автомат  $A = (X, Q, q_0, T)$  задается без выхода и без множества выделенных состояний, иногда и без указания начального состояния  $A = (X, Q, T)$ .

**Определение.** Два автомата без выхода эквивалентны, если они представляют один и тот же входной язык.

**Определение.** Прямое (декартово) произведение автоматов  $A' = (X, Q', q', T')$  и  $A'' = (X, Q'', q'', T'')$  есть автомат  $A' \times A'' = (X, Q' \times Q'', (q', q''), T)$ , где  $T((q', q''), a) = (T(q', a), T''(q'', a))$ ,  $q' \in Q'$ ,  $q'' \in Q''$ ,  $a \in X$ .

**Пример.** Пусть граф-схемы автоматов  $A'$  и  $A''$  (без выходов) приведены на рис.27.3 и 27.4. Граф-схема автомата  $A' \times A''$  изображена на рис.27.5.

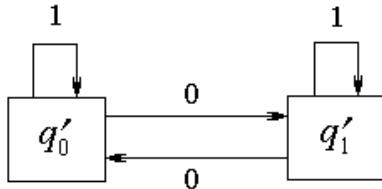


Fig.27.3

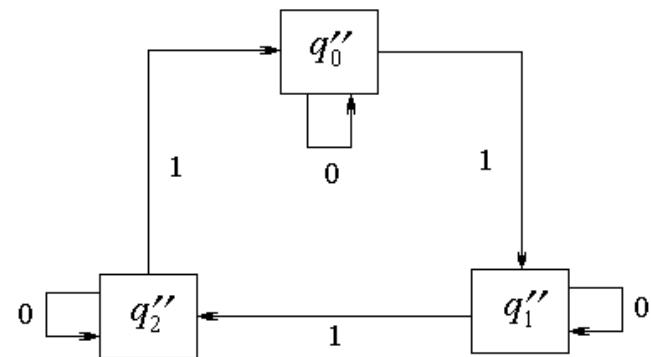


Fig.27.4

**Теорема.** Класс автоматно представимых языков замкнут относительно булевых операций (объединения, пересечения, дополнения).

**Доказательство.** Пусть автоматы  $A' = (X, Q', q', T, F')$  и  $A'' = (X, Q'', q'', T'', F'')$  определяют языки  $Beh(A')$  и  $Beh(A'')$  соответственно.

*Дополнение*  $CA' = X^* - Beh(A')$  определимо автоматом  $(X, Q', q', T, Q' - F')$ .

*Пересечение*  $Beh(A') \cap Beh(A'')$  определимо декартовым произведением  $A' \times A''$  с множеством выделенных состояний  $F' \cap F''$ .

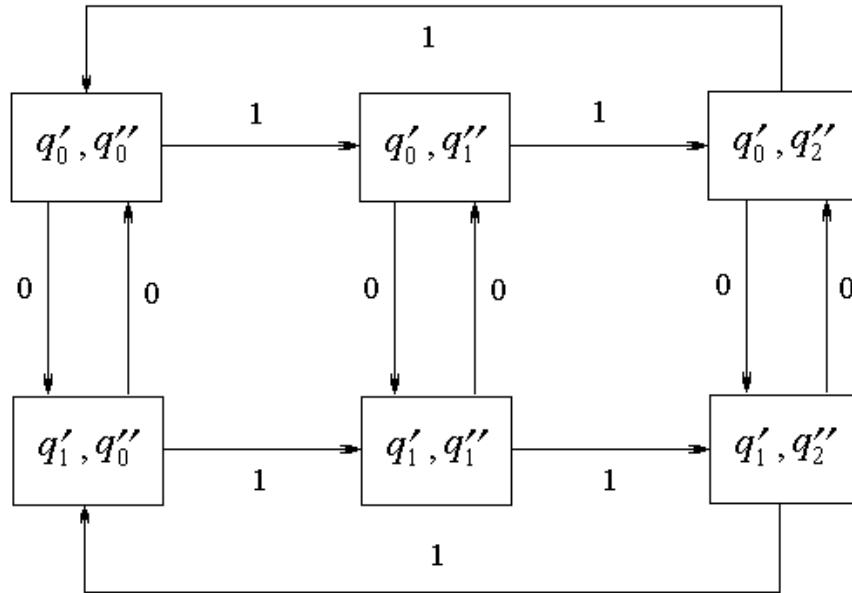


Fig.27.5

*Объединение*  $Beh(A') \cup Beh(A'')$  определимо декартовым произведением  $A' \times A''$  с множеством выделенных состояний  $F' \times Q'' \cup Q' \times F''$ .

**Следствие.** Класс автоматно представимых языков замкнут относительно разности, ибо разность множеств  $M - N = M \cap CN$ .

**Варианты.**

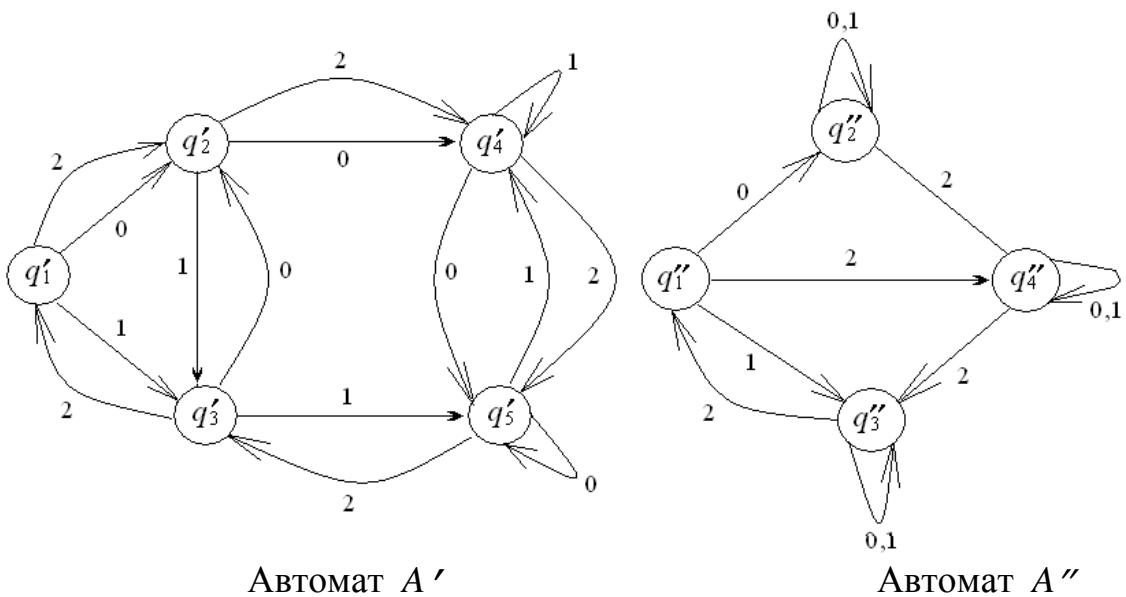


Рис.6.2

- 2.1.**  $(q_1', 2, q_2')$ . **2.2.**  $(q_1', 2, q_3')$ . **2.3.**  $(q_1', 2, q_4')$ . **2.4.**  $(q_1', 2, q_5')$ .  
**2.5.**  $(q_2', 2, q_3')$ . **2.6.**  $(q_2', 2, q_4')$ . **2.7.**  $(q_2', 2, q_5')$ . **2.8.**  $(q_3', 2, q_4')$ .  
**2.9.**  $(q_3', 2, q_5')$ . **2.10.**  $(q_4', 2, q_5')$ . **2.11.**  $(q_1'', 2, q_2'')$ . **2.12.**  $(q_1'', 2, q_3'')$ .  
**2.13.**  $(q_1'', 2, q_4'')$ . **2.14.**  $(q_2'', 2, q_3'')$ . **2.15.**  $(q_2'', 2, q_4'')$ . **2.16.**  $(q_3'', 2, q_4'')$ .  
**2.17.**  $(q_2', 2, q_2')$ . **2.18.**  $(q_3', 2, q_1')$ . **2.19.**  $(q_4', 2, q_1')$ . **2.20.**  $(q_5', 2, q_1')$ .  
**2.21.**  $(q_3', 2, q_2')$ . **2.22.**  $(q_4', 2, q_2')$ . **2.23.**  $(q_5', 2, q_2')$ . **2.24.**  $(q_4', 2, q_3')$ .  
**2.25.**  $(q_5', 2, q_3')$ . **2.26.**  $(q_5', 2, q_4')$ . **2.27.**  $(q_2'', 2, q_1'')$ . **2.28.**  $(q_3'', 2, q'')$ .  
**2.29.**  $(q_4'', 2, q_1'')$ . **2.30.**  $(q_3'', 1, q_2'')$ .

**Задача 3.** Построить автомат для дополнения языка, представленного детерминированным автоматом. Вариант автомата  $A'$  взять из задачи 2.

**Задача 4.** Детерминизировать источник, граф-схема которого изображена на рис.6.3. Множество входных символов  $X = \{0,1,2\}$ . Множество начальных состояний  $Q_0 = \{q_1, q_2\}$ . Множество выделенных состояний  $F = \{q_3, q_5\}$ . Вариант источника получить, добавив к граф-схеме на рис.6.3 стрелку варианта. Например, для варианта 30 к граф-схеме источника надо добавить стрелку  $(q_3, 2, q_2)$ .

**Определение.** Источник есть объект  $S = (X, Q, Q_0, D, F)$ , где  $X$  есть входной алфавит;  $Q$  есть алфавит состояний,  $Q_0 \subseteq Q$  есть множество начальных состояний,  $D \subseteq Q \times X \times Q$  есть (недетерминированная) таблица переходов (здесь в качестве входного сигнала допускается пустой символ, обозначаемый \*),  $F \subseteq Q$  есть множество выделенных состояний.

Тройка  $(q, a, q')$  из  $D$  называется *переходом* источника.

**Замечание.** 1. В случае источника некоторые дуги (стрелки) в его граф-схеме могут быть помечены пустым символом (т.е. дуги ничем не помечены).

2. Недетерминированный автомат есть частный случай источника, в котором нет дуг, помеченных пустым символом.

3. Детерминированный автомат есть частный случай недетерминированного автомата, а потому и частный случай источника.

**Определение.** Входное слово допустимо источником, если оно в движении по стрелкам граф-схемы источника из начального состояния приводит к выделенному состоянию. В противном случае входное слово отвергается (не принимается) источником.

**Определение.** Поведение  $Beh(S)$  источника  $S$  есть множество всех слов, допустимых источником  $S$ . Два источника эквивалентны, если они имеют одинаковые поведения. Язык  $L \subseteq X^*$  представим (допустим, определим) источником, если существует источник  $S$ , для которого  $L = Beh(S)$ . Множество  $Q' \subseteq Q$  состояний источника  $S = (X, Q, Q_0, D, F)$  замкнуто, если  $\forall q \in Q \ \forall q' \in Q' ((q, *, q) \in D \rightarrow q \in Q')$ .

**Замечание.** 1. Замыкание  $[Q']$  множества  $Q'$  есть наименьшее замкнутое множество состояний, содержащее  $Q'$ .

2. Всякий источник  $A$  эквивалентен некоторому двухполюсному источнику  $B$  с единственным начальным  $s$  и единственным финальным  $f$  состояниями. Источник  $B$  строится по источнику  $A$  следующим образом. В граф-схеме источника  $A$  начальное состояние  $s$  соединяется пустыми стрелками с начальными состояниями в  $A$ . Все финальные состояния в  $A$  соединяются пустыми стрелками с финальным состоянием  $f$ . Источник  $B$  построен.

**Теорема** (о детерминизации источника). Пусть язык  $L \subseteq X^*$ .

Следующие утверждения эквивалентны.

1. Язык  $L$  представим конечным автоматом.
2. Язык  $L$  представим источником.

### Алгоритм детерминизации источника

Пусть источник  $S = (X, Q, Q_0, D, F)$ . Возьмем  $Q' \subseteq Q$ ,  $a \in X$ . Пусть  $S(Q', a) = \{q \in Q : \exists q' \in Q' ((q', a, q) \in D)\}$  есть множество всех состояний, в которые источник  $S$  переходит из состояний множества  $Q'$  под воздействием входной непустой буквы  $a$  из  $X$ . Автомат  $A$  с тем же поведением, что и источник  $S$ , строим следующим образом.

1. Формируем замыкание множества начальных состояний источника и объявляем это замыкание начальным состоянием конструируемого автомата.

2. Если состояние  $s = Q' \subseteq Q$  автомата  $A$  уже построено, то  $T(s, a) = [S(Q', a)]$  есть замыкание  $[S(Q', a)]$  состояния  $s = S(Q', a)$ , в которое перейдет автомат  $A$  из состояния  $s$  под воздействием буквы  $a$ .

3. Применяем п.2 алгоритма до тех пор, пока его применение порождает новые состояния автомата  $A$ .

4. Объявляем выделенными те состояния  $s = Q' \subseteq Q$  автомата  $A$ , которые содержат в себе выделенные состояния источника  $S$ .

**Пример.**  $X = \{0, 1\}$ ;  $Q = \{q_0, q_1, q_2\}$ ;  $Q_0 = \{q_0\}$ ;  $F = \{q_0, q_2\}$ . Таблица переходов  $D$  источника  $S = (X, Q, Q_0, D, F)$  изображена на рис.27.8. Таблица переходов детерминированного автомата  $A$ , эквивалентного источнику  $S$ , приведена в табл.27.4. Выделенные состояния автомата  $A$  помечены звездами.

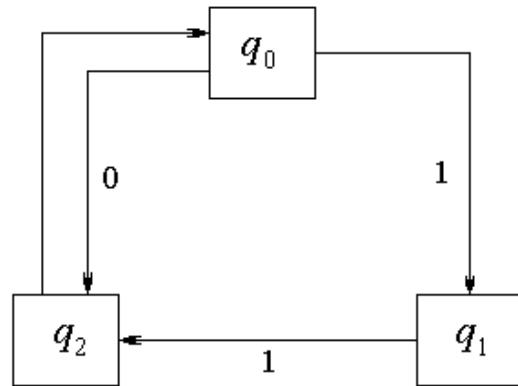


Рис.27.8

Table 27.4

	*	$\{q_0\}$	$\{q_1\}$	*	$\{q_0, q_2\}$	$\emptyset$
0	$\{q_0, q_2\}$			$\{q_0, q_2\}$		$\emptyset$
1	$\{q_1\}$		$\{q_0, q_2\}$	$\{q_1\}$		$\emptyset$

**Замечание.** 1. Недетерминированный конечный автомат (НКА) есть источник без переходов вида  $(q, *, q')$ . Граф-схема такого источника не содержит стрелок, помеченных пустым символом  $e$ .

2. Иногда источник называют недетерминированным конечным автоматом с  $e$ -переходами.

### Варианты.

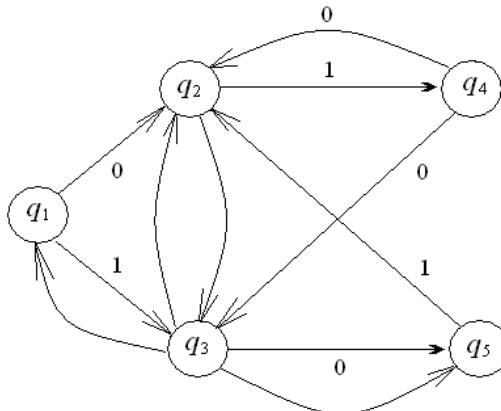


Рис.6.3

- |                                |                                |                                |                                |
|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| <b>4.1.</b> $(q_1, 2, q_2)$ .  | <b>4.2.</b> $(q_1, 2, q_3)$ .  | <b>4.3.</b> $(q_1, 2, q_4)$ .  | <b>4.4.</b> $(q_1, 2, q_5)$ .  |
| <b>4.5.</b> $(q_2, 2, q_3)$ .  | <b>4.6.</b> $(q_2, 2, q_4)$ .  | <b>4.7.</b> $(q_2, 2, q_5)$ .  | <b>4.8.</b> $(q_3, 2, q_4)$ .  |
| <b>4.9.</b> $(q_3, 2, q_5)$ .  | <b>4.10.</b> $(q_4, 2, q_5)$ . | <b>4.11.</b> $(q_1, 1, q_2)$ . | <b>4.12.</b> $(q_1, 0, q_3)$ . |
| <b>4.13.</b> $(q_1, 1, q_4)$ . | <b>4.14.</b> $(q_2, 2, q_3)$ . | <b>4.15.</b> $(q_2, 2, q_4)$ . | <b>4.16.</b> $(q_3, 2, q_4)$ . |
| <b>4.17.</b> $(q_2, 1, q_1)$ . | <b>4.18.</b> $(q_3, 2, q_1)$ . | <b>4.19.</b> $(q_4, 2, q_1)$ . | <b>4.20.</b> $(q_5, 2, q_1)$ . |
| <b>4.21.</b> $(q_3, 2, q_2)$ . | <b>4.22.</b> $(q_4, 2, q_2)$ . | <b>4.23.</b> $(q_5, 2, q_2)$ . | <b>4.24.</b> $(q_4, 2, q_3)$ . |
| <b>4.25.</b> $(q_5, 2, q_3)$ . | <b>4.26.</b> $(q_5, 2, q_4)$ . | <b>4.27.</b> $(q_2, 2, q_1)$ . | <b>4.28.</b> $(q_3, 0, q_1)$ . |
| <b>4.29.</b> $(q_4, 2, q_1)$ . | <b>4.30.</b> $(q_3, 2, q_2)$ . |                                |                                |

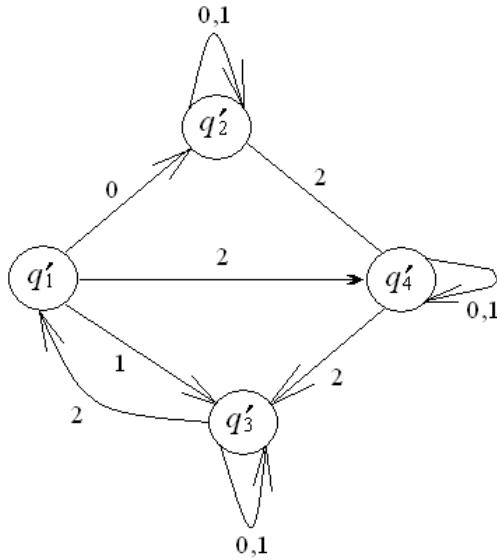
**Задача 5.** Найти источник  $S = (X, Q, Q_0, D, F)$  для объединения языков, представимых источниками  $S' = (X, Q', Q'_0, D', F')$ ,  $S'' = (X, Q'', Q''_0, D'', F'')$  (рис.6.4). Множество входных символов  $X = \{0, 1, 2\}$ . Множество начальных состояний  $Q'_0 = \{q'_1\}$ ,  $Q''_0 = \{q''_1\}$ . Множество выделенных состояний  $F' = \{q'_2\}$ ,  $F'' = \{q''_2\}$ . Детерминизировать полученный источник. Вариант источника получить, добавив к граф-схеме источника  $S''$  на рис.6.4 стрелку варианта. Например, для варианта 30 к граф-схеме источника  $S''$  надо добавить стрелку  $(q''_3, 2, q_2)$ .

**Указание.** Пусть языки  $L_1$  и  $L_2$  представимы источниками  $S_1 = (X, Q', Q'_0, D', F')$  и  $S_2 = (X, Q'', Q''_0, D'', F'')$  соответственно.

*Объединение*  $L_1 \cup L_2$  представимо источником  $S = (X, Q' \cup Q'', Q'_0 \cup Q''_0, D' \cup D'', F' \cup F'')$ .

Граф-схемы источников  $S_1$  и  $S_2$  объединяются. Начальные состояния для  $S_1$  и  $S_2$  становятся начальными состояниями для  $S$ . Выделенные состояния для  $S_1$  и  $S_2$  становятся выделенными состояниями для  $S$ .

### Варианты.



Источник  $S'$

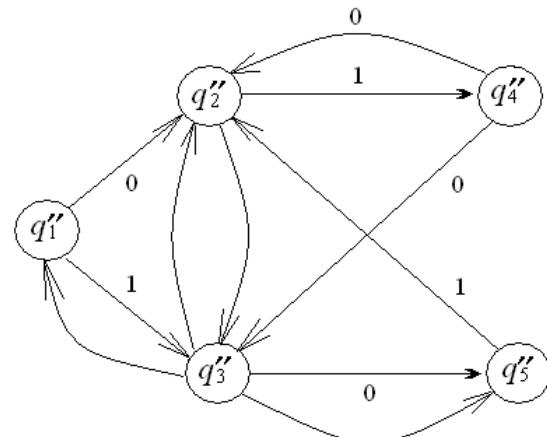


Рис.6.4

Источник  $S''$

- 5.1.  $(q''_1, 2, q''_2)$ . 5.2.  $(q''_1, 2, q''_3)$ . 5.3.  $(q''_1, 2, q''_4)$ . 5.4.  $(q''_1, 2, q''_5)$ .
- 5.5.  $(q''_2, 2, q''_3)$ . 5.6.  $(q''_2, 2, q''_4)$ . 5.7.  $(q''_2, 2, q''_5)$ . 5.8.  $(q''_3, 2, q''_4)$ .
- 5.9.  $(q''_3, 2, q''_5)$ . 5.10.  $(q''_4, 2, q''_5)$ . 5.11.  $(q''_1, 1, q''_2)$ . 5.12.  $(q''_1, 0, q''_3)$ .
- 5.13.  $(q''_1, 1, q''_4)$ . 5.14.  $(q''_2, 2, q''_3)$ . 5.15.  $(q''_2, 2, q''_4)$ . 5.16.  $(q''_3, 2, q''_4)$ .
- 5.17.  $(q''_2, 1, q''_1)$ . 5.18.  $(q''_3, 2, q''_1)$ . 5.19.  $(q''_4, 2, q''_1)$ . 5.20.  $(q''_5, 2, q''_1)$ .
- 5.21.  $(q''_3, 2, q''_2)$ . 5.22.  $(q''_4, 2, q''_2)$ . 5.23.  $(q''_5, 2, q''_2)$ . 5.24.  $(q''_4, 2, q''_3)$ .
- 5.25.  $(q''_5, 2, q''_3)$ . 5.26.  $(q''_5, 2, q''_4)$ . 5.27.  $(q''_2, 2, q''_1)$ . 5.28.  $(q''_3, 0, q''_1)$ .
- 5.29.  $(q''_4, 2, q''_1)$ . 5.30.  $(q''_3, 2, q''_2)$ .

**Задача 6.** Найти источник для конкатенации языков, представимых источниками из задачи 5. Детерминизировать полученный источник.

**Указание.** Пусть языки  $L_1$  и  $L_2$  представимы источниками  $S_1 = (X, Q', Q_0', D', F')$  и  $S_2 = (X, Q'', Q_0'', D'', F'')$  соответственно.

**Конкатенация**  $L_1 \cdot L_2$  представима источником  $S = (X, Q' \cup Q'', Q_0', D, F'')$ , где  $D = D' \cup D'' \cup \{(q', *, q'') : q' \in F', q'' \in Q_0''\}$ .

Граф-схемы источников  $S_1$  и  $S_2$  при конкатенации объединяются. Добавляются пустые (т.е. ничем не помеченные) стрелки, ведущие из выделенных состояний для  $S_1$  в начальные состояния для  $S_2$ . Начальные состояния для  $S_1$  являются начальными состояниями для  $S$ . Выделенные состояния для  $S_2$  являются выделенными состояниями для  $S$ .

**Задача 7.** Найти источник для итерации языка, представимого источником из задачи 4. Детерминизировать полученный источник.

**Указание.** Пусть язык  $L_1$  представим источником  $S_1 = (X, Q', Q_0', D', F')$ .

*Итерация*  $(L_1)^*$  представима источником  $S = (X, Q', Q_0', D, F)$ , где  $D = D' \cup \{(q, *, q') : q \in F', q' \in Q_0'\}$ .

При итерации в граф-схеме для  $S_1$  добавляются пустые стрелки из выделенных состояний для  $S_1$  в его начальные состояния.

**Задача 8.** Провести анализ и синтез конечного автомата по регулярному выражению.

#### Анализ конечных автоматов.

Задача анализа конечных автоматов состоит в построении регулярного выражения  $R$  по данному конечному automату  $A$ , такому, что представляемые ими множества слов (языки) одинаковы.

#### *Алгоритм МакНотона–Ямады анализа автомата (McNaughton–Yamada)*

Пусть автомат  $A = (X, Q, q_0, \delta, F)$  с множеством состояний  $Q = \{0, 1, \dots, n\}$  с одним финальным состоянием  $F = \{r\}$ .

Далее вычисление регулярных выражений выполняется индукция по числу  $n$  состояний  $0, 1, \dots, n$  автомата.

*Базис.* Шаг  $k = 0$ . Для  $i$  от 0 до  $n$ , для  $j$  от 0 до  $n$ , выполнить следующее.

$R_{ij}^0 = \{w \in X^* : \delta(q_i, w) = q_j\}; i, j = 0, 1, \dots, n$ , есть множество всех входных слов  $w$ , для которых  $\delta(q_i, w) = q_j; i, j = 0, 1, \dots, n$ ; причем промежуточные состояния не могут быть больше  $k$ .

*Предположение индукции.* Шаг  $k - 1$ . Предположим, что на шаге  $k - 1$  для  $i$  от 0 до  $n$ , для  $j$  от 0 до  $n$ , регулярные выражения  $R_{ij}^{k-1}$  построены.

*Шаг индукции.* Шаг  $k$ . На шаге  $k$  для  $i$  от 0 до  $n$ , для  $j$  от 0 до  $n$ , регулярные выражения

$$R_{ij}^k = R_{ij}^{k-1} + R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}. \quad (\text{Знак } + \text{ означает объединение множеств}).$$

При этом вычисления упрощаются если:

для  $i = k$ ,  $j = 0, 1, 2, 3$ , регулярное выражение  $R_{kj}^k = (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}$ ;  
 для  $j = k$ ,  $i = 0, 1, 2, 3$ , регулярное выражение  $R_{ik}^k = R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^*$ .  
 Регулярное выражение  $R = R_{0r}^n$ .

При множестве финальных состояний  $F = \{i_1, i_2, \dots, i_r\}$  из  $Q$  регулярное выражение  $R = E_{0,i_1}^n + E_{0,i_2}^n + \dots + E_{0,i_r}^n$ .

**Замечание.** Алгоритм применим и к источникам.

**Пример 1.** Алгоритм МакНотона–Ямады (McNaughton–Yamada) для автомата, заданного диаграммой. На рис П3.1 представлена диаграмма со состояниями  $0, 1, \dots, n$ .

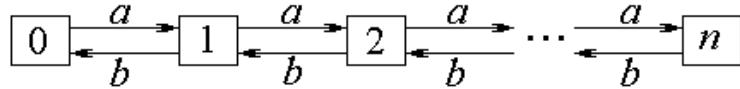


Рис. П3.1

В примере рассматривается случай задания автомата диаграммой при  $n=3$  (рис П3.2). Начальное состояние 0, финальное состояние  $n = 3$ .

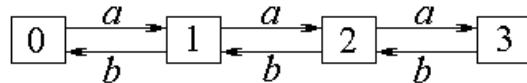


Рис. П3.2

**Шаг  $k = 0$ .** Промежуточные состояния не больше  $k = 0$ .

$$R_{ij}^0 = \{w \in X^*: \delta(q_i, w) = q_j, i, j = 0, 1, 2, 3\}.$$

$$R_{00}^0 = \emptyset, R_{01}^0 = a, R_{02}^0 = \emptyset, R_{03}^0 = \emptyset;$$

$$R_{10}^0 = b, R_{11}^0 = \emptyset, R_{12}^0 = a, R_{13}^0 = \emptyset;$$

$$R_{20}^0 = \emptyset, R_{21}^0 = b, R_{22}^0 = \emptyset, R_{23}^0 = a;$$

$$R_{30}^0 = \emptyset, R_{31}^0 = \emptyset, R_{32}^0 = b, R_{33}^0 = \emptyset.$$

$R_{ij}^0$	0	1	2	3
0	$\emptyset$	$a$	$\emptyset$	$\emptyset$
1	$b$	$\emptyset$	$a$	$\emptyset$
2	$\emptyset$	$b$	$\emptyset$	$a$
3	$\emptyset$	$\emptyset$	$b$	$\emptyset$

**Шаг  $k = 1$ .**

$$R_{ij}^k = R_{ij}^{k-1} + R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i, j = 0, 1, 2, 3; \quad i \neq k, j \neq k.$$

$$R_{kj}^k = (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i = k, \quad j = 0, 1, 2, 3.$$

$$R_{ik}^k = R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^*; \quad j = k, \quad i = 0, 1, 2, 3.$$

$$R_{ij}^1 = R_{ij}^0 + R_{i1}^0 \cdot (R_{11}^0)^* \cdot R_{1j}^0;$$

$$\begin{aligned}
& i=0, j=0; R_{00}^1 = R_{00}^0 + R_{01}^0 \cdot (R_{11}^0)^* \cdot R_{10}^0 = \emptyset + b \cdot (\emptyset)^* \cdot \emptyset = \emptyset. \\
& i=0, j=1; R_{01}^1 = (R_{11}^0)^* \cdot R_{11}^0 = (\emptyset)^* \cdot \emptyset = \emptyset. \\
& i=0, j=2; R_{02}^1 = R_{02}^0 + R_{01}^0 \cdot (R_{11}^0)^* \cdot R_{12}^0 = \emptyset + a \cdot (\emptyset)^* \cdot a = aa. \\
& i=0, j=3; R_{03}^1 = R_{03}^0 + R_{01}^0 \cdot (R_{11}^0)^* \cdot R_{13}^0 = \emptyset + a \cdot (\emptyset)^* \cdot \emptyset = \emptyset. \\
& i=1, j=0; R_{10}^1 = (R_{11}^0)^* \cdot R_{10}^0 = (\emptyset)^* \cdot b = b. \\
& i=1, j=1; R_{11}^1 = (R_{11}^0)^* \cdot R_{11}^0 = (\emptyset)^* \cdot \emptyset = \emptyset. \\
& i=1, j=2; R_{12}^1 = (R_{11}^0)^* \cdot R_{12}^0 = (\emptyset)^* \cdot a = a. \\
& i=1, j=3; R_{13}^1 = (R_{11}^0)^* \cdot R_{13}^0 = (\emptyset)^* \cdot \emptyset = \emptyset. \\
& i=2, j=0; R_{20}^1 = R_{20}^0 + R_{21}^0 \cdot (R_{11}^0)^* \cdot R_{10}^0 = \emptyset + b \cdot (\emptyset)^* \cdot b = bb. \\
& i=2, j=1; R_{21}^1 = E_{21}^0 \cdot (E_{11}^0)^* = b \cdot (\emptyset)^* = b. \\
& i=2, j=2; R_{22}^1 = R_{22}^0 + R_{21}^0 \cdot (R_{11}^0)^* \cdot R_{12}^0 = \emptyset + b \cdot (\emptyset)^* \cdot a = ba. \\
& i=2, j=3; R_{23}^1 = R_{23}^0 + R_{21}^0 \cdot (R_{11}^0)^* \cdot R_{13}^0 = a + b \cdot (\emptyset)^* \cdot \emptyset = a. \\
& i=3, j=0; R_{30}^1 = R_{30}^0 + R_{31}^0 \cdot (R_{11}^0)^* \cdot R_{10}^0 = \emptyset + \emptyset \cdot (\emptyset)^* \cdot b = \emptyset. \\
& i=3, j=1; R_{31}^1 = R_{31}^0 \cdot (R_{11}^0)^* = \emptyset \cdot (\emptyset)^* = \emptyset. \\
& i=3, j=2; R_{32}^1 = R_{32}^0 + R_{31}^0 \cdot (R_{11}^0)^* \cdot R_{12}^0 = b + \emptyset \cdot (\emptyset)^* \cdot a = b. \\
& i=3, j=3; R_{33}^1 = R_{33}^0 + R_{31}^0 \cdot (R_{11}^0)^* \cdot R_{13}^0 = \emptyset + \emptyset \cdot (\emptyset)^* \cdot \emptyset = \emptyset.
\end{aligned}$$

$R_{ij}^1$	0	1	2	3
0	$\emptyset$	$\emptyset$	$aa$	$\emptyset$
1	$b$	$\emptyset$	$a$	$\emptyset$
2	$b$	$b$	$ba$	$a$
3	$\emptyset$	$\emptyset$	$b$	$\emptyset$

$$R_{00}^1 = \emptyset, R_{01}^1 = \emptyset, R_{02}^1 = aa, R_{03}^1 = \emptyset;$$

$$R_{10}^1 = b, R_{11}^1 = \emptyset, R_{12}^1 = a, R_{13}^1 = \emptyset;$$

$$R_{20}^1 = bb, R_{21}^1 = b, R_{22}^1 = bb, R_{23}^1 = a;$$

$$R_{30}^1 = \emptyset, R_{31}^1 = b, R_{32}^1 = bb, R_{33}^1 = a;$$

**Шар  $k=2$ .**

$$R_{ij}^k = R_{ij}^{k-1} + R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i,j = 0,1,2,3; \quad i \neq k, j \neq k.$$

$$R_{kj}^k = (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i=k, j=0,1,2,3.$$

$$R_{ik}^k = R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^*; \quad j=k, \quad i=0,1,2,3.$$

$$R_{ij}^2 = R_{ij}^1 + R_{il}^1 \cdot (R_{22}^1)^* \cdot R_{1j}^1; \quad i,j = 0,1,2,3.$$

$$i=0, j=0; R_{00}^2 = R_{00}^1 + R_{02}^1 \cdot (R_{22}^1)^* \cdot R_{20}^1 = \emptyset + aa \cdot (ba)^* \cdot bb = aa \cdot (ba)^* \cdot bb.$$

$$\begin{aligned}
& i=0, j=1; R_{01}^2 = R_{01}^1 + R_{02}^1 \cdot (R_{22}^1)^* \cdot R_{21}^1 = \emptyset + aa \cdot (ba)^* \cdot b = aa \cdot (ba)^* \cdot b. \\
& i=0, j=2; R_{02}^2 = R_{02}^1 \cdot (R_{22}^1)^* = aa \cdot (ba)^*. \\
& i=0, j=3; R_{03}^2 = R_{03}^1 + R_{02}^1 \cdot (R_{22}^1)^* \cdot R_{23}^1 = \emptyset + aa \cdot (ba)^* \cdot a = aa \cdot (ba)^* \cdot a. \\
& i=1, j=0; R_{10}^2 = R_{10}^1 + R_{12}^1 \cdot (R_{22}^1)^* \cdot R_{20}^1 = b + a \cdot (ba)^* \cdot bb. \\
& i=1, j=1; R_{11}^2 = R_{11}^1 + R_{12}^1 \cdot (R_{22}^1)^* \cdot R_{21}^1 = \emptyset + a \cdot (ba)^* \cdot b = a \cdot (ba)^* \cdot b. \\
& i=1, j=2; R_{12}^2 = R_{12}^1 \cdot (R_{22}^1)^* = a \cdot (ba)^*. \\
& i=1, j=3; R_{13}^2 = R_{13}^1 + R_{12}^1 \cdot (R_{22}^1)^* \cdot R_{23}^1 = \emptyset + aa \cdot (ba)^* \cdot a = aa \cdot (ba)^* \cdot a. \\
& i=2, j=0; R_{20}^2 = (R_{22}^1)^* \cdot R_{20}^1 = (ba)^* \cdot bb. \\
& i=2, j=1; R_{21}^2 = (R_{22}^1)^* \cdot R_{21}^1 = (ba)^* \cdot b. \\
& i=2, j=2; R_{22}^2 = (R_{22}^1)^* \cdot R_{22}^1 = (ba)^* \cdot ba. \\
& i=2, j=3; R_{23}^2 = (R_{22}^1)^* \cdot R_{23}^1 = (ba)^* \cdot a. \\
& i=3, j=0; R_{30}^2 = R_{30}^1 + R_{32}^1 \cdot (R_{22}^1)^* \cdot R_{20}^1 = \emptyset + b \cdot (ba)^* \cdot bb = b \cdot (ba)^* \cdot bb. \\
& i=3, j=1; R_{31}^2 = R_{31}^1 + R_{32}^1 \cdot (R_{22}^1)^* \cdot R_{21}^1 = \emptyset + b \cdot (ba)^* \cdot b = b \cdot (ba)^* \cdot b. \\
& i=3, j=2; R_{32}^2 = (R_{22}^1)^* \cdot E_{22}^1 = (ba)^* \cdot ba. \\
& i=3, j=3; R_{33}^2 = R_{33}^1 + R_{32}^1 \cdot (R_{22}^1)^* \cdot R_{23}^1 = \emptyset + b \cdot (ba)^* \cdot a = b \cdot (ba)^* \cdot a.
\end{aligned}$$

$E_{ij}^2$	0	1	2	3
0	$aa \cdot (ba)^* \cdot bb$	$aa \cdot (ba)^* \cdot b$	$aa \cdot (ba)^*$	$aa \cdot (ba)^* \cdot a$
1	$b + a \cdot (ba)^* \cdot bb$	$a \cdot (ba)^* \cdot b$	$a \cdot (ba)^*$	$aa \cdot (ba)^* \cdot a$
2	$(ba)^* \cdot bb$	$(ba)^* \cdot b$	$(ba)^* \cdot ba$	$(ba)^* \cdot a$
3	$b \cdot (ba)^* \cdot bb$	$b \cdot (ba)^* \cdot b$	$(ba)^* \cdot ba$	$b \cdot (ba)^* \cdot a$

$$\begin{aligned}
R_{00}^2 &= aa \cdot (ba)^* \cdot bb, \quad R_{01}^2 = aa \cdot (ba)^* \cdot b, \quad R_{02}^2 = aa \cdot (ba)^*, \quad R_{03}^2 = aa \cdot (ba)^* \cdot a; \\
R_{10}^2 &= b + a \cdot (ba)^* \cdot bb, \quad R_{11}^2 = a \cdot (ba)^* \cdot b, \quad R_{12}^2 = a \cdot (ba)^*, \quad R_{13}^2 = aa \cdot (ba)^* \cdot a; \\
R_{20}^1 &= (ba)^* \cdot bb, \quad R_{21}^2 = (ba)^* \cdot b, \quad R_{22}^2 = (ba)^* \cdot ba, \quad R_{23}^2 = (ba)^* \cdot a; \\
R_{30}^2 &= b \cdot (ba)^* \cdot bb, \quad R_{31}^2 = b \cdot (ba)^* \cdot b, \quad R_{32}^2 = (ba)^* \cdot ba, \quad R_{33}^2 = b \cdot (ba)^* \cdot a.
\end{aligned}$$

**Шар  $k = 3$ .**

$$R_{ij}^k = R_{ij}^{k-1} + R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i,j = 0,1,2,3; \quad i \neq k, j \neq k.$$

$$R_{kj}^k = (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i = k, \quad j = 0,1,2,3.$$

$$R_{ik}^k = R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^*; \quad j = k, \quad i = 0,1,2,3.$$

$$R_{ij}^3 = R_{ij}^2 + R_{il}^2 \cdot (R_{22}^2)^* \cdot R_{lj}^2; \quad i,j = 0,1,2,3.$$

$$\begin{aligned}
i=0, j=0; \quad R_{00}^3 &= R_{00}^2 + R_{03}^2 \cdot (E_{33}^2)^* \cdot R_{30}^2 = \\
& (aa(ba)^*bb) + (aa(ba)^*a) \cdot (b(ba)^*a) \cdot (b(ba)^*bb).
\end{aligned}$$

$$\begin{aligned}
& i=0, j=1; R_{01}^3 = R_{01}^2 + R_{03}^2 \cdot (R_{33}^2)^* \cdot R_{31}^2 = \\
& \quad (aa(ba)^*b) + (aa(ba)^*a) \cdot (b(ba)^*a)^* \cdot (b(ba)^*b). \\
& i=0, j=2; R_{02}^3 = R_{02}^2 + R_{03}^2 \cdot (R_{33}^2)^* \cdot R_{32}^2 = \\
& \quad (aa(ba)^*) + (aa(ba)^*a) \cdot (b(ba)^*a)^* \cdot ((ba)^*ba). \\
& i=0, j=3; R_{03}^3 = R_{03}^2 \cdot (R_{33}^2)^* = (aa(ba)^*a) \cdot (b(ba)^*a)^*. \\
& i=1, j=0; R_{10}^3 = E_{10}^2 + R_{13}^2 \cdot (R_{33}^2)^* \cdot R_{30}^2 = \\
& \quad (b+a(ba)^*bb) + (ba(ba)^*a) \cdot (b \cdot (ba)^* \cdot a) \cdot (b(ba)^*bb). \\
& i=1, j=1; R_{11}^3 = R_{11}^2 + R_{13}^2 \cdot (R_{33}^2)^* \cdot R_{31}^2 = \\
& \quad (a(ba)^*b) + (aa(ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*b). \\
& i=1, j=2; R_{12}^3 = E_{12}^2 + R_{13}^2 \cdot (R_{33}^2)^* \cdot R_{32}^2 = \\
& \quad (a(ba)^*) + (aa(ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (ba(ba)^*). \\
& i=1, j=3; R_{13}^3 = R_{13}^2 \cdot (R_{33}^2)^* = (aa(ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^*. \\
& i=2, j=0; R_{20}^3 = R_{20}^2 + R_{23}^2 \cdot (R_{33}^2)^* \cdot R_{30}^2 = \\
& \quad ((ba)^*bb) + ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*bb). \\
& i=2, j=1; R_{21}^3 = R_{21}^2 + R_{23}^2 \cdot (R_{33}^2)^* \cdot R_{31}^2 = \\
& \quad ((ba)^*bb) + ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*b). \\
& i=2, j=2; R_{22}^3 = R_{22}^2 + R_{23}^2 \cdot (R_{33}^2)^* \cdot R_{32}^2 = \\
& \quad ((ba)^*ba) + ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot ((ba)^*ba). \\
& i=2, j=3; R_{23}^3 = R_{23}^2 \cdot (R_{33}^2)^* = ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^*. \\
& i=3, j=0; R_{30}^3 = (R_{33}^2)^* \cdot R_{30}^2 = (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*bb). \\
& i=3, j=1; R_{31}^3 = (R_{33}^2)^* \cdot R_{31}^2 = (b(ba)^* \cdot a)^* \cdot (b(ba)^*b). \\
& i=3, j=2; R_{32}^3 = (R_{33}^2)^* \cdot E_{32}^2 = (b \cdot (ba)^* \cdot a)^* \cdot ((ba)^*ba). \\
& i=3, j=3; R_{33}^3 = (R_{33}^2)^* \cdot E_{33}^2 = (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*a). \\
& R_{00}^3 = (aa(ba)^*bb) + (aa(ba)^*a) \cdot (b(ba)^*a) \cdot (b(ba)^*bb). \\
& R_{01}^3 = (aa(ba)^*b) + (aa(ba)^*a) \cdot (b(ba)^*a)^* \cdot (b(ba)^*b). \\
& R_{02}^3 = (aa(ba)^*) + (aa(ba)^*a) \cdot (b(ba)^*a)^* \cdot ((ba)^*ba). \\
& R_{03}^3 = (aa(ba)^*a) \cdot (b(ba)^*a)^*. \\
& R_{10}^3 = (b+a(ba)^*bb) + (ba(ba)^*a) \cdot (b \cdot (ba)^* \cdot a) \cdot (b(ba)^*bb). \\
& R_{11}^3 = (a(ba)^*b) + (aa(ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*b). \\
& R_{12}^3 = (a(ba)^*) + (aa(ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (ba(ba)^*). \\
& R_{13}^3 = (aa(ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^*. \\
& R_{20}^3 = ((ba)^*bb) + ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*bb). \\
& R_{21}^3 = ((ba)^*bb) + ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*b).
\end{aligned}$$

$$R_{22}^3 = ((ba)^*ba) + ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^* \cdot ((ba)^*ba).$$

$$R_{23}^3 = ((ba)^*a) \cdot (b \cdot (ba)^* \cdot a)^*.$$

$$R_{30}^3 = (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*bb).$$

$$R_{31}^3 = (b(ba)^* \cdot a)^* \cdot (b(ba)^*b).$$

$$R_{32}^3 = (b \cdot (ba)^* \cdot a)^* \cdot ((ba)^*ba).$$

$$R_{33}^3 = (b \cdot (ba)^* \cdot a)^* \cdot (b(ba)^*a).$$

Для начального состояния 0 и  $F = \{3\}$  регулярное выражение

$$R = E_{03}^3 = (aa(ba)^*a) \cdot (b(ba)^*a)^*.$$

Для начального состояния 0 и  $F = \{0\}$  регулярное выражение

$$R = (aa(ba)^*bb) + (aa(ba)^*a) \cdot (b(ba)^*a) \cdot (b(ba)^*bb).$$

Для начального состояния 3 и  $F = \{1,2\}$  регулярное выражение

$$R = R_{31}^3 + R_{32}^3 = (b(ba)^* \cdot a)^* \cdot (b(ba)^*b) + (b \cdot (ba)^* \cdot a)^* \cdot ((ba)^*ba)..$$

**Пример 2.** Пусть конечный автомат  $A = (X, Q, q_0, T, F)$ , где входной алфавит  $X = \{a, b\}$ , множество состояний  $Q = \{0, 1, 2\}$ , начальное состояние 0, множество финальных состояний  $F = \{0, 1\}$ . Функция переходов  $\delta$  задана на рис. П3.3.

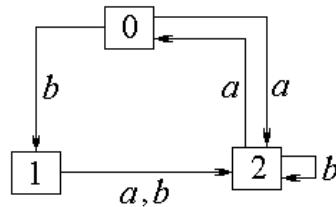


Рис. П3.3

**Шаг  $k = 0$ .** Промежуточные состояния не больше  $k = 0$ .

$$R_{ij}^0 = \{a \in X: \delta(q_i, a) = q_j, i, j = 0, 1, 2\}.$$

$$R_{00}^0 = \emptyset, \quad R_{01}^0 = b, \quad R_{02}^0 = a;$$

$$R_{10}^0 = \emptyset, \quad R_{11}^0 = \emptyset, \quad R_{12}^0 = a+b;$$

$$R_{20}^0 = a, \quad R_{21}^0 = ab, \quad R_{22}^0 = aa.$$

$E_{ij}^0$	0	1	2
0	$\emptyset$	$b$	$a$
1	$\emptyset$	$\emptyset$	$a+b$
2	$a$	$ab$	$aa$

**Шаг  $k = 1$ .**

$$R_{ij}^k = R_{ij}^{k-1} + R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i, j = 0, 1, 2; \quad i \neq k, j \neq k.$$

$$R_{kj}^k = (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i = k, \quad j = 0, 1, 2.$$

$$R_{ik}^k = R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^*; \quad j = k, \quad i = 0, 1, 2.$$

$$\begin{aligned}
R_{ij}^1 &= R_{ij}^0 + R_{i1}^0 \cdot (R_{11}^0)^* \cdot R_{1j}^0; \quad i,j = 0,1,2. \\
i=0, j=0; \quad R_{00}^1 &= R_{00}^0 + R_{01}^0 \cdot (R_{11}^0)^* \cdot E_{10}^0 = \emptyset + b \cdot (\emptyset)^* \cdot \emptyset = \emptyset. \\
i=0, j=1; \quad R_{01}^1 &= R_{01}^0 \cdot (R_{11}^0)^* = b \cdot (\emptyset)^* = b. \\
i=0, j=2; \quad R_{02}^1 &= R_{02}^0 + R_{01}^0 \cdot (R_{11}^0)^* \cdot R_{12}^0 = a + b \cdot (\emptyset)^* \cdot (a+b) = a + b(a+b). \\
i=1, j=0; \quad R_{10}^1 &= (R_{11}^0)^* \cdot R_{10}^0 = (\emptyset)^* \cdot \emptyset = \emptyset. \\
i=1, j=1; \quad R_{11}^1 &= (R_{11}^0)^* \cdot E_{11}^0 = (\emptyset)^* \cdot \emptyset = \emptyset. \\
i=1, j=2; \quad R_{12}^1 &= (R_{11}^0)^* \cdot R_{12}^0 = (\emptyset)^* \cdot (a+b) = a+b. \\
i=2, j=0; \quad R_{20}^1 &= R_{20}^0 + E_{21}^0 \cdot (R_{11}^0)^* \cdot R_{10}^0 = a + ab \cdot (\emptyset)^* \cdot \emptyset = a. \\
i=2, j=1; \quad R_{21}^1 &= R_{21}^0 \cdot (R_{11}^0)^* = ab \cdot (\emptyset)^* = ab. \\
i=2, j=2; \quad R_{22}^1 &= R_{22}^0 + R_{21}^0 \cdot (R_{11}^0)^* \cdot R_{12}^0 = b + ab \cdot (\emptyset)^* \cdot (a+b) = b+ab(a+b).
\end{aligned}$$

$R_{ij}^1$	0	1	2
0	$\emptyset$	$b$	$a+b(a+b)$
1	$\emptyset$	$\emptyset$	$a+b$
2	$a$	$ab$	$b+ab(a+b)$

$$\begin{aligned}
R_{00}^1 &= \emptyset, \quad R_{01}^1 = b, \quad R_{02}^1 = a+b(a+b); \\
R_{10}^1 &= \emptyset, \quad R_{11}^1 = \emptyset, \quad R_{12}^1 = a+b; \\
R_{20}^1 &= a, \quad R_{21}^1 = ab, \quad R_{22}^1 = b+ab(a+b).
\end{aligned}$$

**Шаг  $k = 2$ .**

$$\begin{aligned}
R_{ij}^k &= R_{ij}^{k-1} + R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i,j = 0,1,2; \quad i \neq k, j \neq k. \\
R_{kj}^k &= (R_{kk}^{k-1})^* \cdot R_{kj}^{k-1}; \quad i = k, \quad j = 0,1,2. \\
R_{ik}^k &= R_{ik}^{k-1} \cdot (R_{kk}^{k-1})^*; \quad j = k, \quad i = 0,1,2. \\
R_{ij}^2 &= R_{ij}^1 + R_{i1}^1 \cdot (R_{22}^1)^* \cdot R_{1j}^1; \quad i,j = 0,1,2. \\
i=0, j=0; \quad R_{00}^2 &= R_{00}^1 + R_{02}^1 \cdot (R_{22}^1)^* \cdot R_{20}^1 = \emptyset + (a+b(a+b)) \cdot (b+ab(a+b))^* \cdot a = \\
&\quad (a+b(a+b)) \cdot (b+ab(a+b))^* \cdot a. \\
i=0, j=1; \quad R_{01}^2 &= R_{01}^1 + R_{02}^1 \cdot (R_{22}^1)^* \cdot R_{21}^1 = b + (a+b(a+b)) \cdot (b+ab(a+b))^* \cdot ab. \\
i=0, j=2; \quad R_{02}^2 &= R_{02}^1 \cdot (R_{22}^1)^* = (a+b(a+b)) \cdot (b+ab(a+b))^*. \\
i=1, j=0; \quad R_{10}^2 &= R_{10}^1 + R_{12}^1 \cdot (R_{22}^1)^* \cdot R_{20}^1 = (a+b) \cdot (b+ab(a+b))^* \cdot a. \\
i=1, j=1; \quad R_{11}^2 &= R_{11}^1 + R_{12}^1 \cdot (R_{22}^1)^* \cdot R_{21}^1 = \emptyset + (a+b) \cdot (b+ab(a+b))^* \cdot ab. \\
i=1, j=2; \quad R_{12}^2 &= R_{12}^1 \cdot (R_{22}^1)^* = (a+b) \cdot (b+ab(a+b))^*. \\
i=2, j=0; \quad R_{20}^2 &= (R_{22}^1)^* \cdot R_{20}^1 = (b+ab(a+b))^* \cdot a. \\
i=2, j=1; \quad R_{21}^2 &= (R_{22}^1)^* \cdot R_{21}^1 = (b+ab(a+b))^* \cdot ab.
\end{aligned}$$

$$i = 2, j = 2; R_{22}^2 = (R_{22}^1)^* \cdot R_{22}^1 = (b+ab(a+b))^* \cdot (b+ab(a+b)).$$

$$R_{00}^2 = (a+b(a+b)) \cdot (b+ab(a+b))^* \cdot a.$$

$$R_{01}^2 = b+(a+b(a+b)) \cdot (b+ab(a+b))^* \cdot ab.$$

$$R_{02}^2 = (a+b(a+b)) \cdot (b+ab(a+b))^*.$$

$$R_{10}^2 = (a+b) \cdot (b+ab(a+b))^* \cdot a.$$

$$R_{11}^2 = (a+b) \cdot (b+ab(a+b))^* \cdot ab.$$

$$R_{12}^2 = (a+b) \cdot (b+ab(a+b))^*.$$

$$R_{20}^2 = (b+ab(a+b))^* \cdot a.$$

$$R_{21}^2 = (b+ab(a+b))^* \cdot ab.$$

$$R_{22}^2 = (b+ab(a+b))^* \cdot (b+ab(a+b)).$$

Для начального состояния 0 и  $F = \{0, 1\}$  регулярное выражение

$$R = R_{00}^2 + R_{01}^2 = (a+b(a+b)) \cdot (b+ab(a+b))^* \cdot a + b+(a+b(a+b)) \cdot (b+ab(a+b))^* \cdot ab.$$

**Замечание.** В двух предыдущих примерах вычислены регулярные выражения для любых начальных и финальных состояний данного конечного автомата. Для конкретных начального и конечного состояний число промежуточных вычислений можно сократить, выбрав только необходимы промежуточные регулярные выражения.

### *Алгоритм МакКласки анализа автомата методом удаления состояний* (Brzozowski J.A., McCluskey E.J.)

Пусть  $A = (X, Q, q_0, \delta, F)$  есть источник, с множеством состояний  $Q = \{0, 1, \dots, n\}$ , с единственным начальным состоянием 0, с единственным финальным состоянием  $f = n$ . Источник задан диаграммой  $D$ . Далее индукция по удаляемым состояниям.

**Базис.** Шаг 0. Каждую дугу диаграммы  $D_0$ , ведущую из состояния  $i$  в состояние  $j$  (дуга может быть петлей) и помеченную входными символами  $a_1, \dots, a_u$  (среди них может быть пустой символ  $e$ ), пометить регулярным выражением  $R = a_1 + \dots + a_u$ . Если некоторое состояние имеет петлю, помеченную регулярным выражением  $R$  без внешней звезды, то заменить  $R$  на  $R^*$ . Построена диаграмма  $D_0$ .

**Предположение индукции.** Допустим, что на шаге  $k - 1$  построена диаграмма  $D_{k-1}$ , в которой число состояний уменьшилось на  $k - 1$  состояний и в которой каждая дуга помечена некоторым регулярным выражением.

**Шаг индукции.** Шаг  $k$ . Выберем в  $D_{k-1}$  любое состояние  $s$  вне  $\{0, f\}$  для удаления из  $D_{k-1}$ .

Пусть в  $D_{k-1}$  в состояние  $s$  заходят дуги из состояний  $p_1, \dots, p_u$ , помеченные регулярными выражениями  $P_1, \dots, P_u$  соответственно.

Пусть в  $D_{k-1}$  из состояния  $s$  выходят дуги в состояния  $q_1, \dots, q_v$ , помеченные регулярными выражениями  $Q_1, \dots, Q_v$  соответственно (табл. П3.1).

Таблица П3.1

Состояния	$p_1$	$\dots$	$p_u$	$q_1$	$\dots$	$q_v$
Регулярные выражения	$P_1$	$\dots$	$P_u$	$Q_1$	$\dots$	$Q_v$

Пусть в  $D_{k-1}$  всякая дуга из  $p_i$  ( $i = 1, \dots, u$ ) в  $q_j$  ( $j = 1, \dots, v$ ) помечена регулярным выражением  $R_{ij}$ . Если дуги из  $p_i$  в  $q_j$  нет, то положим  $R_{ij} = \emptyset$ . Построим табл. П3.2 значений регулярных выражений  $R_{ij}$ .

Таблица П3.2

$p_i / q_j$	$q_1$	$\dots$	$q_v$
$p_1$	$R_{11}$	$\dots$	$R_{1v}$
$\dots$	$\dots$	$\dots$	$\dots$
$p_u$	$R_{u1}$	$\dots$	$R_{uv}$

Далее для простоты будем иногда состояния  $p_i, q_j$  обозначать индексами  $i, j$  соответственно. Состояние  $s$  из  $D_{k-1}$  удаляем следующим образом.

Для всех  $i = 1, \dots, u; j = 1, \dots, v$ , строим графы входящих из  $p_i$  в  $s$  ребер и исходящих из  $s$  в  $q_j$  ребер и их пометки  $P_l, Q_j$  соответственно, а также дуги от  $p_i$  до  $q_j$  (если они существуют) с пометками  $R_{ij}$  из табл. П3.1 и табл. П3.2 (рис. П3.4).

Удаляем состояние  $s$  и все инцидентные (принадлежащие)  $s$  дуги (рис. П3.5).

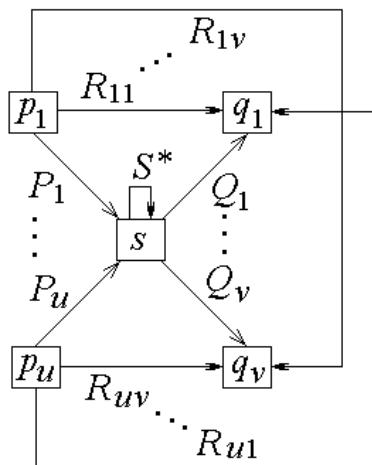


Рис. П3.4

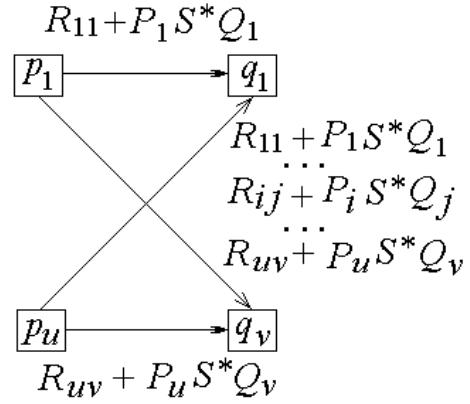


Рис. П3.5

Если удаляются две дуги из  $p_i$  в  $s$  и из  $s$  в  $q_j$ , то дуга из  $p_i$  в  $q_j$  помечается: регулярным выражением  $R_{ij} + P_i \cdot S^* \cdot Q_j$ , если петля на  $s$  помечена регулярным выражением  $S^*$  (рис. П3.6),  
регулярным выражением  $R_{ij} + P_i \cdot \emptyset^* \cdot Q_j$ , если  $s$  петли не имеет (рис. П3.7).

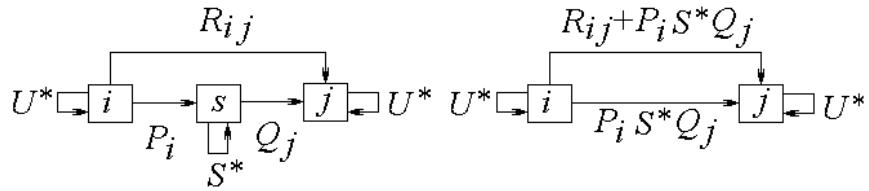


Рис. П3.6

Рис. П3.7

При удалении состояния  $s$  при  $q_i = p_i$  появляется петля (рис. П3.8, рис. П3.9).

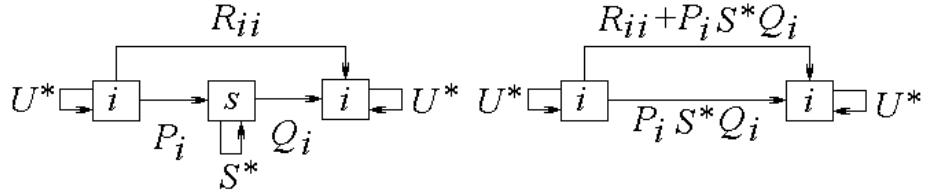


Рис. П3.8

Рис. П3.9

Петля на рис. П3.9 изображена на рис.П3.10 и после упрощений на рис. П3.11.

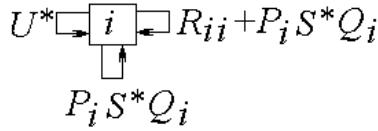


Рис. П3.10

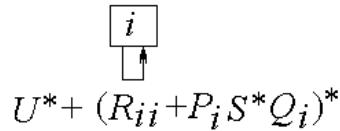


Рис. П3.11

В  $D_{k-1}$  удаляем состояние  $s$  и все его дуги. Достраиваем получившуюся диаграмму графами из рисунков П3.7, П3.11 и получаем диаграмму  $D_k$ .

Индукция заканчивается следующими двумя случаями.

*Случай 1.* Начальное состояние является допускающим. Поэтому индукция заканчивается диаграммой  $D_1$  с одним лишь начальным состояниями 0. Тогда состояние 0 имеет петлю, помеченную некоторым регулярным выражением  $R = T$  (рис. П3.12). Оно представляет язык, допустимый данным источником  $A$ .

*Случай 2.* Начальное состояние не является допускающим. Тогда индукция заканчивается диаграммой  $D_2$  с лишь начальным и финальным состояниями 0 и  $f$ , дуги которых помечены, например, следующим образом (рис. П3.12).

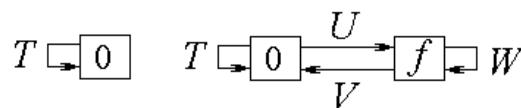


Рис. П3.12

Тогда регулярное выражение  $R = (T + UW^*V)^*UW^*$  представляет язык, допустимый источником  $A$ . Не следует дублировать звезду у  $W$ , если  $W$  звезду уже имеет.

Если отсутствуют петли у состояния 0 или у состояния  $f$ , то в  $R$  соответствующие  $T$  и  $W$  заменяются на  $\emptyset$ .

Если отсутствует дуга из  $f$  в 0, то  $R = (T + UW^*)UW^*$ .

**Замечание.** Вид (форма) регулярного выражения зависит от порядка удаления состояний конечного автомата.

**Пример 1.** Диаграмма  $D$  автомата  $A$  приведена на рис. П3.13. Начальное состояние  $0$ , финальное состояние  $f = 1$ . Найти регулярное выражение  $R$ , представляющее конечный автоматный язык  $L$ .

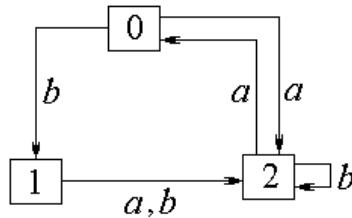


Рис. П3.13

### Начальное состояние $0$ , финальное состояние $1$

**Шаг  $k = 0$ .** Каждую дугу диаграммы  $D_0$ , ведущую из состояния  $i$  в состояние  $j$  (дуга может быть петлей) и помеченную входными символами  $a_1, \dots, a_u$  (среди них может быть пустой символ  $e$ ), пометить регулярным выражением  $R = a_1 + \dots + a_u$ . Состояние  $2$  в  $D_0$ , имеет петлю, помеченную регулярным выражением  $R = b$ . Заменяем  $R$  на  $b^*$  (рис. П3.14).

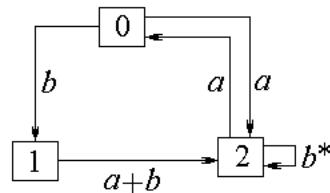


Рис. П3.14

**Шаг  $k = 1$ .** Состояние  $s = 2$  вне  $\{0, f\}$  есть единственное состояние для удаления.

В  $D_{k-1}$  в состояние  $s = 2$  заходит дуга:

из состояния  $1$  с регулярным выражением  $a + b$ ,

из состояния  $0$  с регулярным выражением  $a$ .

В  $D_{k-1}$  из состояния  $s = 2$  выходит дуга

в состояние  $0$  с регулярным выражением  $a$ . (Рис. П3.15).

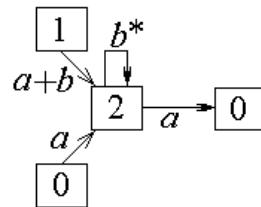


Рис.П3.15

Удаление состояния  $2$  на рис. П3.15 дает рис. П3.16 и рис. П3.17. Цикл на рис. П3.17 помещаем на рис. П3.16 и получаем рис. П3.18.

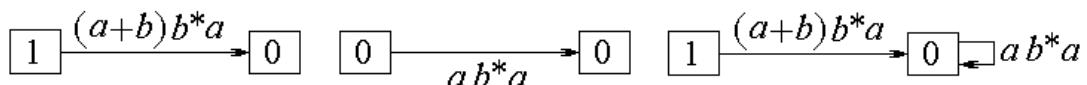


Рис. П3.16

Рис. П3.17

Рис. П3.18

Из диаграммы на рис. П3.12 удаляем состояние 2 и все инцидентные с 2 дуги. Получаем рис. П3.19. Достраиваем диаграмму на рис. П3.19 диаграммой на рис. П3.18 и получаем диаграмму  $D_1$  на рис. П3.20.

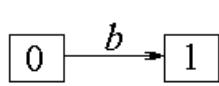


Рис. П3.19

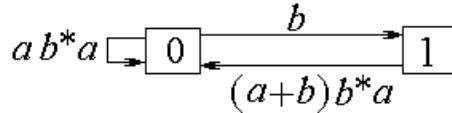


Рис. П3.20

В диаграмме  $D_{k=1}$  (рис. П3.20) регулярное выражение  $T = ab^*a$ ,  $U = b$ ,  $V = (a+b)b^*a$ ,  $W = \emptyset$ . Тогда

$$R = (T + UW^*V)^*UW^* = (ab^*a + b\emptyset^*(a+b)b^*a)^*b\emptyset^* = (ab^*a + b(a+b)b^*a)^*b.$$

Регулярное выражение  $R = (ab^*a + b(a+b)b^*a)^*b$  представляет язык  $L$ , допустимый источником  $A$ .

### **Начальное состояние 0, финальное состояние 2**

Удаляем состояние 1. Исходя из диаграммы на рис. П3.12, строим диаграмму входящих и выходящих для состояния 1 стрелок (рис. П3.21). Удаляем состояние 1 и получаем диаграмму на рис. П3.22.

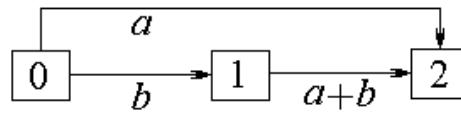


Рис. П3.21

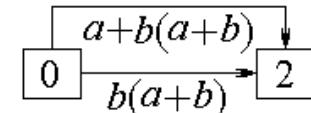


Рис. П3.22

Удаляем из диаграммы на рис. П3.12 состояние 1 и инцидентные с ним дуги (рис. П3.23), достраиваем диаграмму на рис.П3.23 диаграммой на рис. П3.22 и получаем диаграмму на рис. П3.24, эквивалентную диаграмме на рис. П3.25.

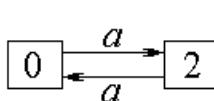


Рис. П3.23

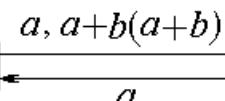


Рис. П3.24

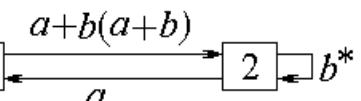


Рис. П3.25

В диаграмме  $D_{k=1}$  (рис. П3.25) регулярное выражение  $T = \emptyset$ ,  $U = a+b(a+b)$ ,  $V = a$ ,  $W = b^*$ . Тогда

$$R = (T + UW^*V)^*UW^* = (\emptyset + (a+b(a+b)) \cdot b^* \cdot a)^* \cdot (a+b(a+b)) \cdot b^* = ((a+b(a+b)) \cdot b^* \cdot a)^* \cdot (a+b(a+b)) \cdot b^*.$$

Регулярное выражение  $R = ((a+b(a+b)) \cdot b^* \cdot a)^* \cdot (a+b(a+b)) \cdot b^*$  представляет язык  $L$ , допустимый источником  $A$ .

### **Начальное состояние 0, финальное состояние 0**

После удаления состояния 2 из диаграммы на рис. П3.12 получаем следующую диаграмму (рис. П3.26).

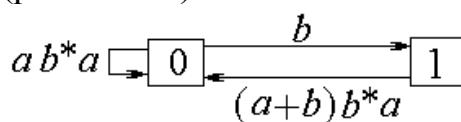


Рис. П3.26

Строим диаграмму входящих и исходящих для состояния 1 стрелок (рис. П3.27).

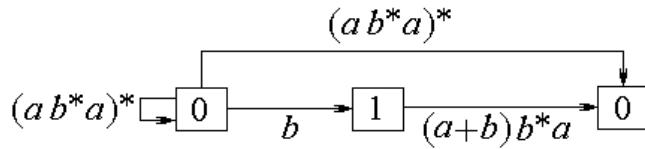


Рис. П3.27

Удаляем на рис. П3.12 состояние 1 и получаем рис. П3.28 и П3.29.

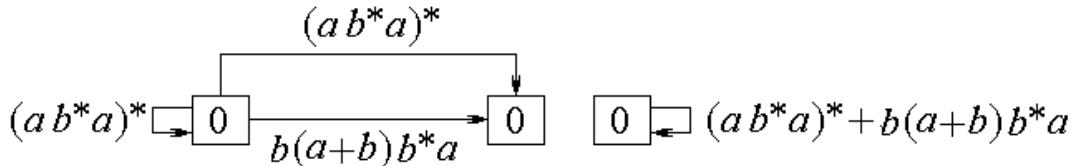


Рис. П3.28

Рис. П3.29

В диаграмме  $D_{k=1}$  (рис. П3.29) регулярное выражение  $T = (ab^*a)^* + b(a+b)b^*a$ . Тогда  $R = T = (ab^*a)^* + b(a+b)b^*a$ .

Регулярное выражение  $R = (ab^*a)^* + b(a+b)b^*a$  представляет язык, допустимый источником  $A$ .

**Пример 2.** Диаграмма  $D$  автомата  $A$  приведена на рис. П3.30. Начальное состояние 0, финальное состояние  $f = 3$ . Найти регулярное выражение  $R$ , представляющее конечно автоматный язык  $L$ .

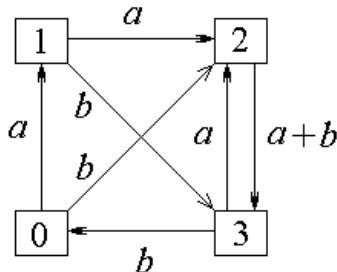


Рис. П3.30

Удаление состояния 2. Все входящие в состояние 2 и выходящие из состояния 2 дуги приведены на рис. П3.31. Цикл из состояния 3 в состояние 3 подсоединяется к состоянию 3 и снабжается пометкой дуги звездой. Получаем рис. П3.32.

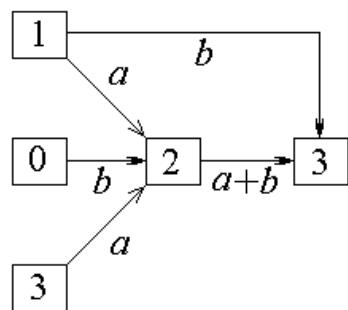


Рис. П3.31

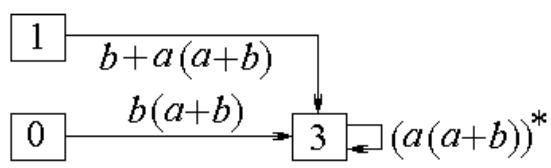


Рис. П3.32

Из диаграммы на рис. П3.30 удаляем состояние 2 и все его дуги. Результат достраиваем графом на рис. П3.32. Получаем новую диаграмму (рис. П3.33).

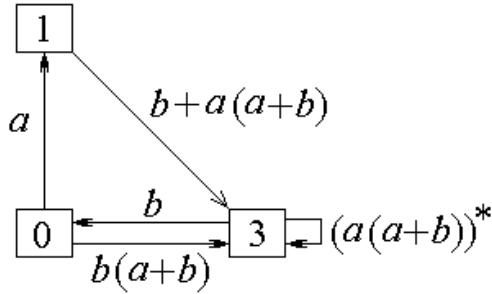


Рис. П3.33

Удаление состояния 1 в диаграмме на рис. П3.33. Для этого строим диаграмму входящих и исходящих ребер для состояния 1 (рис. П3.34). Удаляем в рис. П3.34 состояние 1 и получаем рис.П3.35.

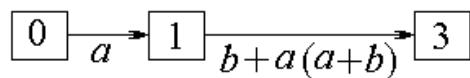


Рис. П3.34

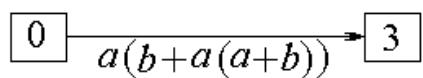


Рис. П3.35

Удаляем из рис. П3.33 состояние 1 с его дугами, получаем рис. П3.36.

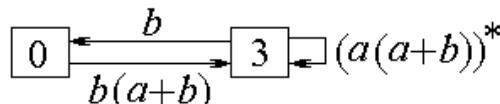


Рис. П3.36

Достраиваем рис. П3.36 с помощью рис. П3.35 и получаем граф на рис. П3.37.

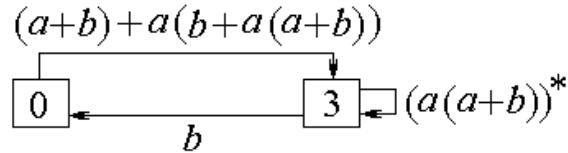


Рис. П3.37

В диаграмме на рис. П3.37 регулярное выражение  $T = \emptyset$ ,  $U=(a+b)+a(b+a(a+b))$ ,  $V=b$ ,  $W=(a(a+b))^*$ . Тогда

$$R = (T + UW^*V)^*UW^* =$$

$$(\emptyset + (a+b)+a(b+a(a+b))\cdot(a(a+b))^*\cdot b)^* \cdot (a+b)+a(b+a(a+b))\cdot(a(a+b))^*.$$

Регулярное выражение

$$R = ((a+b)+a(b+a(a+b))\cdot(a(a+b))^*\cdot b)^* \cdot (a+b)+a(b+a(a+b))\cdot(a(a+b))^*.$$

представляет язык, допустимый источником  $A$ .

**Пример 3.** Источник  $A$  задан диаграммой на рис.П3.38. Начальное состояние 0, финальное состояние  $f = 3$ . Найти регулярное выражение, представляющее язык, определимый источником  $A$ .

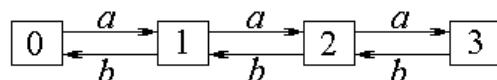


Рис. П3.38

1. Удаление состояния 2 в диаграмме на рис. П3.38. Строим все входящие в состояние 2 дуги, все дуги, выходящие из состояния 2 дуги, а также все дуги из левых состояний в правые состояния там, где они существуют (рис. П3.39). Строим все пути от левых состояний в правые состояния (рис. П3.40).

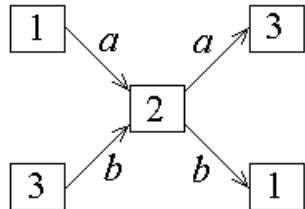


Рис. П3.39

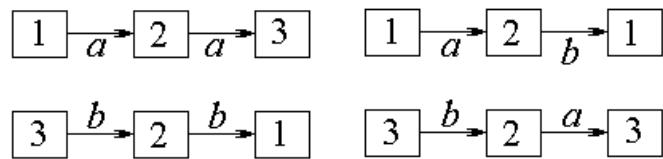


Рис. П3.40

В диаграмме на рис. П3.40 удаляем состояние 2, сохраняя пометки на принадлежащих состоянию 2 дугах (рис. П3.41). Снабжаем звездами пометки на появившихся петлях (рис. П3.42).

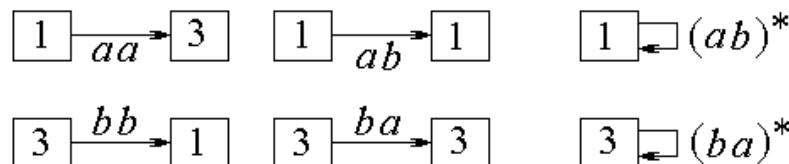


Рис. П3.41

Рис. П3.42

В диаграмме на рис. П3.38 удаляем состояние 2 и все его дуги вместе пометками (рис. П3.43). Достраиваем диаграмму на рис. П3.43 дугами с их пометками из диаграмм на рисунках П3.41 и П3.42 (рис.П3.44).

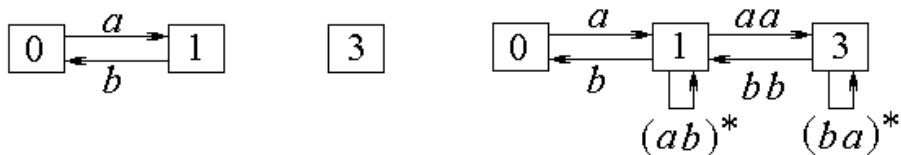


Рис. П3.43

Рис. П3.44

2. Удаление состояния 1 в диаграмме на рис. П3.44. Строим все входящие в состояние 1 дуги, все выходящие из состояния 1 дуги, а также все дуги из левых состояний в правые состояния там, где они существуют (рис. П3.45). Строим все пути от левых состояний в правые состояния (рис. П3.46).

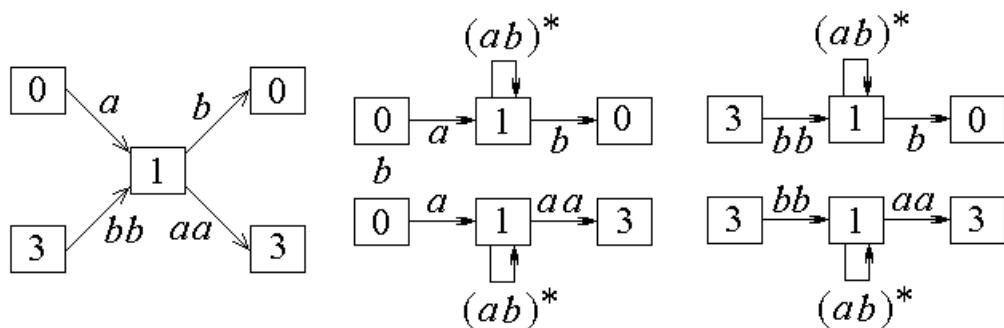


Рис. П3.45

Рис. П3.46

В двух диаграммах рис. ПЗ.46 удаляем состояние 1 и все его дуги, сохраняя пометки на принадлежащих состоянию 1 дугах. Снабжаем звездами пометки на появившихся петлях (рис. ПЗ.47, ПЗ.48).

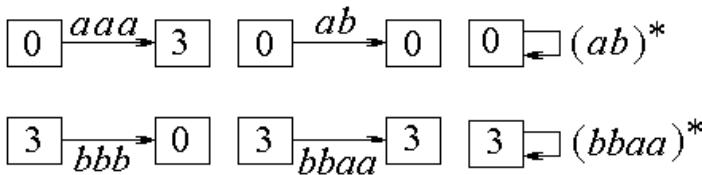


Рис. ПЗ.47

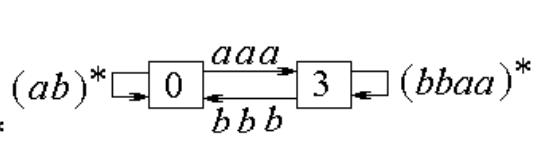


Рис. ПЗ.48

В диаграмме на рис. ПЗ.48 регулярное выражение

$T = (ab)^*$ ,  $U = aaa$ ,  $V = bbb$ ,  $W = (bbbaa)^*$ . Тогда  $R = (T + UW^*V)^*UW^* = ((ab)^* + (aaa) \cdot (bbbaa)^* \cdot bbb)^* \cdot aaa \cdot (bbbaa)^*$ .

Регулярное выражение  $R = ((ab)^* + (aaa) \cdot (bbbaa)^* \cdot bbb)^* \cdot aaa \cdot (bbbaa)^*$  представляет язык, допустимый источником  $A$ .

**Задача 1.** Диаграмма источника задана на рис. ПЗ.49. Методом МакНотона–Ямады найти регулярное выражение  $R$ , представляющее язык, допустимый данным источником. Начальные и финальные состояния источника указаны как пары  $(i, j)$ ;  $i, j = 0, 1, \dots, 5$ . Варианты после задачи 2.

**Задача 2.** Диаграмма источника задана на рис. ПЗ.49. Методом МакКласки найти регулярное выражение  $R$ , представляющее язык, допустимый данным источником. Начальные и финальные состояния источника указаны как пары  $(i, j)$ ;  $i, j = 0, 1, \dots, 5$ .

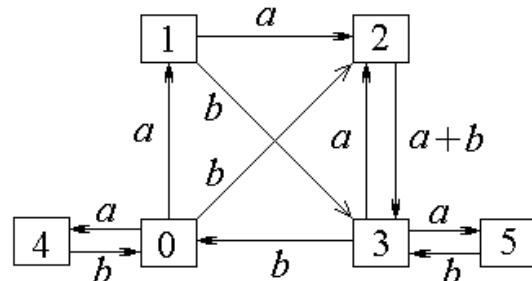


Рис. ПЗ.49

- 1.1.** (0, 0). **1.2.** (0, 1). **1.3.** (0, 2). **1.4.** (0, 3). **1.5.** (0, 4). **1.6.** (0, 5).
- 1.7.** (1, 0). **1.8.** (1, 1). **1.9.** (1, 2). **1.10.** (1, 3). **1.11.** (1, 4). **1.12.** (1, 5).
- 1.13.** (2, 0). **1.14.** (2, 1). **1.15.** (2, 2). **1.16.** (2, 3). **1.7.** (2, 4). **1.18.** (2, 5).
- 1.19.** (3, 0). **1.20.** (3, 1). **1.21.** (3, 2). **1.22.** (3, 3). **1.23.** (3, 24). **1.24.** (3, 5).
- 1.25.** (4, 0). **1.26.** (4, 1). **1.27.** (4, 2). **1.28.** (4, 3). **1.29.** (4, 4). **1.30.** (4, 5).
- 1.31.** (5, 0). **1.32.** (5, 1). **1.33.** (5, 2). **1.34.** (5, 3). **1.35.** (5, 4). **1.36.** (5, 5).

### Синтез конечных автоматов

Синтез конечного автомата по регулярному выражению  $R$  состоит в построении такого конечного автомата  $A$ , что языки представимые автоматом  $A$  и регулярным выражением  $R$  совпадают.

**Задача 1.** Найти источник для языка в алфавите  $\{0,1,2\}$ , представимого регулярным выражением. Детерминизировать полученный источник.

**Пример.** Найти источник для языка в алфавите  $\{a,b,c\}$ , представимого регулярным выражением  $R = a \cdot b^* \cdot (a \vee b \cdot c)^* \cdot c$ . Детерминизировать полученный источник.

1. Индукцией по построению формулы  $R$  выполнить парсинг (анализ) регулярного выражения  $R$ , то есть синтаксический разбор регулярного выражения  $R$ . Дерево разбора от корня к листьям показано на рис.П4.1.

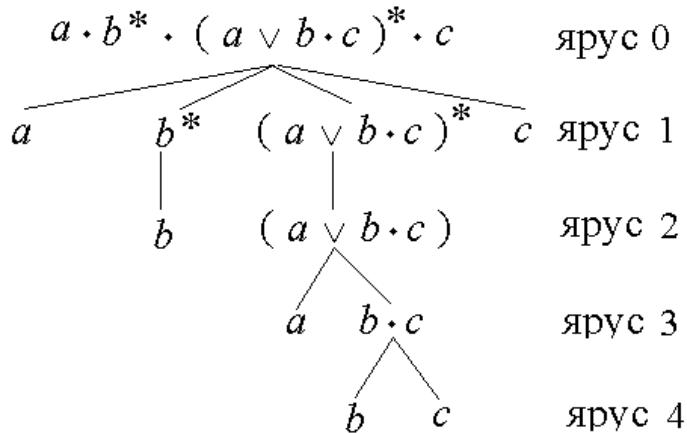


Рис. П4.1

Построение источника (синтез) для регулярного выражения  $R$  выполнять от листьев к корню дерева разбора. В следующих диаграммах строящихся источников знак  $i$  (initial) означает начальное состояние, а знак  $f$  (final) означает финальное состояние.

Для яруса 4 из рис. П4.1 построить диаграммы источников для языков регулярных выражений  $b$  и  $c$  (рис. П4.2).

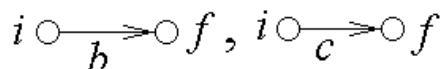


Рис. П4.2

Для яруса 3 из рис. П4.1 построить диаграммы источников для языков регулярных выражений  $a$  и  $b \cdot c$  (рис. П4.3).

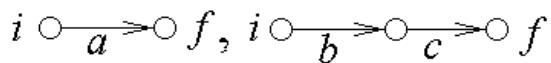


Рис. П4.3

Для яруса 2 из рис. П4.1 построить диаграммы источников для языков регулярных выражений  $b$  и  $a \vee b \cdot c$  (рис. П4.4).

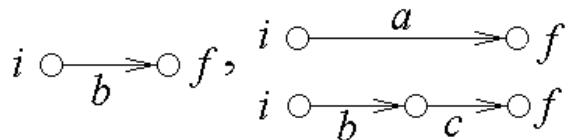


Рис. П4.4

Для яруса 1 из рис. П4.1 построить диаграммы источников для языков регулярных выражений  $a$ ,  $(a \vee b \cdot c)^*$ ,  $c$  (рис. П4.5).

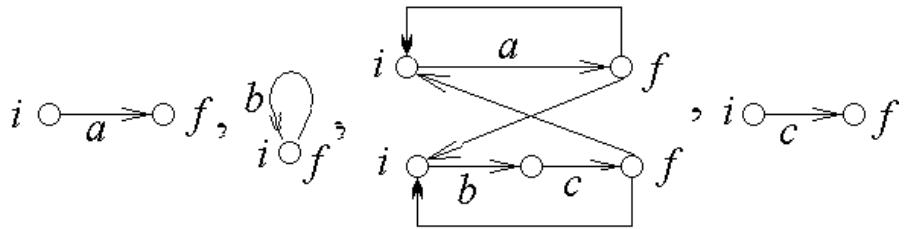


Рис. П4.5

Для яруса 0 из рис.1 построить диаграмму источника для языка регулярного выражения  $R = a \cdot (a \vee b \cdot c)^* \cdot c$  (рис. П4.6).

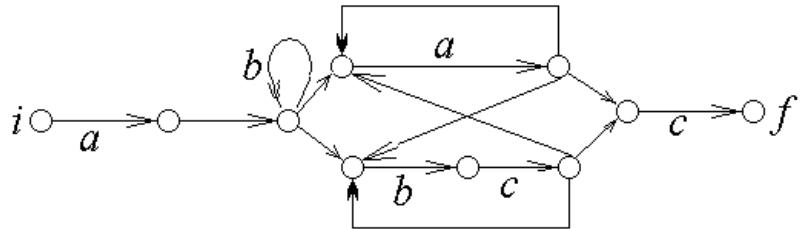


Рис. П4.6

Источник  $A$ , допускающий язык для регулярного выражения  $R$ , построен. Обозначим его состояния (рис.П4.7).

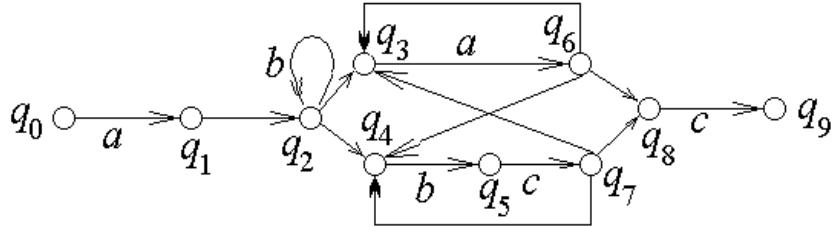


Рис. П4.7

Источник  $A = (X, Q, Q_0, T, F)$ , где

$$X = \{a, b, c\},$$

$$Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\},$$

$$Q_0 = \{q_0\},$$

$$T = \{(q_0, a, q_1), (q_1, *, q_2), (q_2, b, q_2), (q_2, *, q_3), (q_2, *, q_4), (q_3, a, q_6), (q_4, b, q_5), (q_5, c, q_7), (q_6, *, q_3), (q_6, *, q_4), (q_6, *, q_8), (q_7, *, q_4), (q_7, *, q_3), (q_7, *, q_8), (q_8, c, q_9)\},$$

$$F = \{q_9\}.$$

Таблица переходов состояний источника  $A$

	$q_0$	$q_1$	$q_2$	$q_3$	$q_4$	$q_5$	$q_6$	$q_7$	$q_8$	$q_9$
$a$	$q_1$			$q_6$						
$b$			$q_2$		$q_5$					
$c$						$q_7$				$q_9$
$*$		$q_2$	$q_3, q_4$				$q_3, q_4, q_8$	$q_3, q_4, q_8$		

Далее проводится детерминизация построенного источника.

Таблица детерминированного автомата

	$q_0$	$q_1, q_2,$ $q_3, q_4$	$q_2, q_3,$ $q_4, q_5$	$q_3, q_4,$ $q_6, q_8$	$q_3, q_4,$ $q_7, q_8$	$q_5$	$q_9$	$\square$
$a$	$q_1, q_2, q_3, q_4$	$q_3, q_4,$ $q_6, q_8$	$q_3, q_4,$ $q_6, q_8$	$q_3, q_4,$ $q_6, q_8$	$q_3, q_4,$ $q_6, q_8$	$\square$	$\square$	$\square$
$b$	$\square$	$q_2, q_3,$ $q_4, q_5$	$q_2, q_3,$ $q_4, q_5$	$q_5$	$q_5$	$\square$	$\square$	$\square$
$c$	$\square$	$\square$	$\square$	$q_3, q_4,$ $q_7, q_8$	$q_9$	$q_9$	$q_3, q_4,$ $q_7, q_8$	$\square$

Таблица переобозначеного детерминированного автомата

	$q_0$	$q_1$	$q_2$	$q_3$	$q_4$	$q_5$	$q_6$	$q_7$
$a$	$q_1$	$q_3$	$q_3$	$q_3$	$q_3$	$q_7$	$q_7$	$q_7$
$b$	$q_7$	$q_2$	$q_2$	$q_5$	$q_5$	$q_7$	$q_7$	$q_7$
$c$	$q_7$	$q_7$	$q_4$	$q_6$	$q_6$	$q_4$	$q_7$	$q_7$

Столбцы для  $q_3$  и  $q_4$  одинаковы. Поэтому в таблице столбец  $q_4$  можно удалить, а все состояния  $q_4$  в таблице заменить на  $q_3$ . Столбцы для  $q_6$  и  $q_7$  тоже одинаковы. Поэтому в таблице столбец  $q_7$  можно удалить, а все состояния  $q_7$  в таблице заменить на  $q_6$ . В результате получим следующую таблицу.

Таблица нового детерминированного автомата

	$q_0$	$q_1$	$q_2$	$q_3$	$q_5$	$q_6$
$a$	$q_1$	$q_3$	$q_3$	$q_3$	$q_6$	$q_6$
$b$	$q_6$	$q_2$	$q_2$	$q_5$	$q_6$	$q_6$
$c$	$q_6$	$q_6$	$q_3$	$q_6$	$q_3$	$q_6$

В результате получаем детерминированный конечный автомат

$A = (X, Q, Q_0, T, F)$ , где  $X = \{a, b, c\}$ ,  $Q = \{q_0, q_1, q_2, q_3, q_5, q_6\}$ ,  $Q_0 = \{q_0\}$ ,  $T = \{(q_0, a, q_1), (q_0, b, q_6), (q_0, c, q_6), (q_1, a, q_3), (q_1, b, q_2), (q_1, c, q_6), (q_2, a, q_3), (q_2, b, q_2), (q_2, c, q_3), (q_3, a, q_3), (q_3, b, q_5), (q_3, c, q_6), (q_5, a, q_6), (q_5, b, q_6), (q_5, c, q_3), (q_6, a, q_6), (q_6, b, q_6), (q_6, c, q_6)\}$ ,  $F = \{q_6\}$ .

**Варианты.**

- |   |   |
|---|---|
| <b>8.1.</b> $0 \cdot 1^* \cdot (0 \cdot 2 \cdot 1)^* \vee 2.$ | <b>8.2.</b> $0 \cdot 1^* \cdot (0 \cdot 2 \vee 1)^* \cdot 2.$ |
| <b>8.3.</b> $0 \cdot 1^* \cdot (0 \cdot 2 \vee 1)^* \vee 2.$  | <b>8.4.</b> $0 \cdot 1^* \cdot (0 \vee 2 \cdot 1)^* \cdot 2.$ |
| <b>8.5.</b> $0 \cdot 1^* \cdot (0 \vee 2 \cdot 1)^* \vee 2.$  | <b>8.6.</b> $0 \cdot 1^* \cdot (0 \vee 2 \vee 1)^* \cdot 2.$  |
| <b>8.7.</b> $0 \cdot 1^* \cdot (0 \vee 2 \vee 1)^* \vee 2.$   | <b>8.8.</b> $0 \cdot 1^* \vee (0 \cdot 2 \cdot 1)^* \cdot 2.$ |
| <b>8.9.</b> $0 \cdot 1^* \vee (0 \cdot 2 \cdot 1)^* \vee 2.$  | <b>8.10.</b> $0 \cdot 1^* \vee (0 \cdot 2 \vee 1)^* \cdot 2.$ |
| <b>8.11.</b> $0 \cdot 1^* \vee (0 \cdot 2 \vee 1)^* \vee 2.$  | <b>8.12.</b> $0 \cdot 1^* \vee (0 \vee 2 \cdot 1)^* \cdot 2.$ |
| <b>8.13.</b> $0 \cdot 1^* \vee (0 \vee 2 \cdot 1)^* \vee 2.$  | <b>8.14.</b> $0 \cdot 1^* \vee (0 \vee 2 \vee 1)^* \cdot 2.$  |

- 8.15.**  $0 \cdot 1^* \vee (0 \vee 2 \vee 1)^* \vee 2.$     **8.16.**  $0 \vee 1^* \cdot (0 \cdot 2 \cdot 1)^* \cdot 2.$   
**8.17.**  $0 \vee 1^* \cdot (0 \cdot 2 \cdot 1)^* \vee 2.$     **8.18.**  $0 \vee 1^* \cdot (0 \cdot 2 \vee 1)^* \cdot 2.$   
**8.19.**  $0 \vee 1^* \cdot (0 \cdot 2 \vee 1)^* \vee 2.$     **8.20.**  $0 \vee 1^* \cdot (0 \vee 2 \cdot 1)^* \cdot 2.$   
**8.21.**  $0 \vee 1^* \cdot (0 \vee 2 \cdot 1)^* \vee 2.$     **8.22.**  $0 \vee 1^* \cdot (0 \vee 2 \vee 1)^* \cdot 2.$   
**8.23.**  $0 \vee 1^* \cdot (0 \vee 2 \vee 1)^* \vee 2.$     **8.24.**  $0 \vee 1^* \vee (0 \cdot 2 \cdot 1)^* \cdot 2.$   
**8.25.**  $0 \vee 1^* \cdot \vee (0 \cdot 2 \cdot 1)^* \vee 2.$     **8.26.**  $0 \vee 1^* \vee (0 \cdot 2 \vee 1)^* \cdot 2.$   
**8.27.**  $0 \vee 1^* \vee (0 \cdot 2 \vee 1)^* \vee 2.$     **8.28.**  $0 \vee 1^* \vee (0 \vee 2 \cdot 1)^* \cdot 2.$   
**8.29.**  $0 \vee 1^* \vee (0 \vee 2 \cdot 1)^* \vee 2.$     **8.30.**  $0 \vee 1^* \vee (0 \vee 2 \vee 1)^* \cdot 2.$   
**8.31.**  $0 \vee 1^* \vee (0 \vee 2 \vee 1)^* \vee 2$     **8.32.**  $0 \cdot 1^* \cdot (0 \cdot 2 \cdot 1)^* \cdot 2.$

**Задача 9.** По заданному источнику  $S$ , представляющему язык  $L$ , построить источник, представляющий язык  $L^{-1}$ . Детерминизировать полученный источник. Вариант источника  $S$  взять из задачи 4.

**Указание.** Пусть  $X$  есть конечный алфавит. Обращение слова  $x = x(0)x(1)\dots x(k-1)x(k)$  из  $X^*$  есть слово  $x^{-1} = x(k)x(k-1)\dots x(1)x(0)$ . Если множество  $M \subseteq X^*$ , то  $M^{-1} = \{x^{-1} : x \in M\}$ .

Пусть язык  $M$  представим источником  $S = (X, Q, Q_0, D, F)$ . Тогда язык  $M^{-1}$  представим источником  $S' = (X, Q, F, D', Q_0)$ , где  $D' = \{(q', a, q) : (q, a, q') \in D\}$ , т.е. в граф-схеме источника  $S$  все стрелки меняют свое направление на противоположное. Начальные состояния в  $S$  становятся выделенными состояниями в  $S'$ . Выделенные состояния в  $S$  становятся начальными состояниями в  $S'$ .

**Задача 10.** По заданному источнику  $S$  (рис.6.6), представляющему язык  $L$  в входном алфавите  $X = \{0, 1, 2, 3, 4, 5\}$ , построить источник, представляющий проекцию языка  $L$  при отображении  $f: X \rightarrow Y$  с алфавита  $X$  на алфавит  $Y$ . Положить алфавит  $Y = \{a, b, c\}$ . Функция  $f$  определяется вариантом задания.

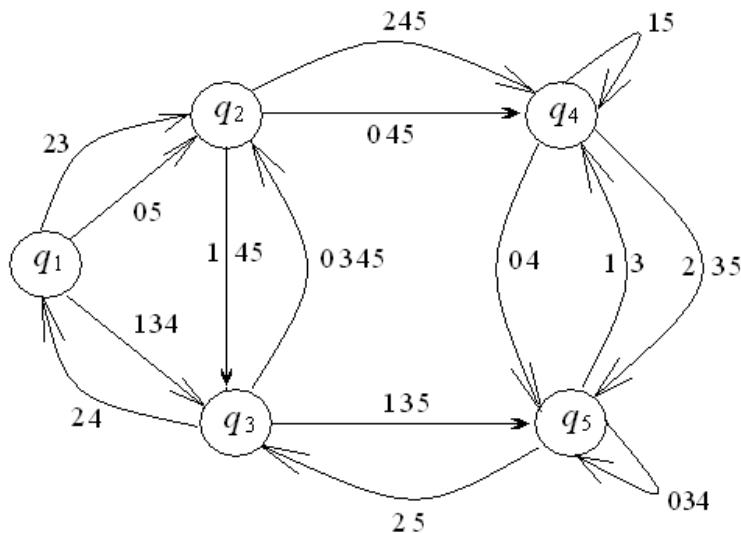


Рис.6.6

**Указание.** Пусть  $X = \{a_0, a_1, \dots, a_k\}$ ,  $Y = \{b_0, b_1, \dots, b_l\}$  есть два конечных алфавита, и пусть функция  $f: X \rightarrow Y$  осуществляет проекцию с одного алфавита на другой (т.е. с алфавита  $X$  на алфавит  $Y$ ). Пусть  $x = x(0)x(1)\dots x(r)$  есть слово в алфавите  $X$ . Тогда слово  $f(x) = f(x(0))f(x(1))\dots f(x(r))$  есть проекция слова  $x$  при отображении  $f$ . Если  $M \subseteq X^*$ , то  $f(M) = \{f(x) : x \in M\}$  есть проекция множества  $M$  при отображении  $f$ .

**Теорема.** Класс языков, представимых источниками, замкнут относительно проекции.

**Доказательство.** Пусть язык  $M$  представим источником  $S = (X, Q, Q_0, D, F)$ , и функция  $f: X \rightarrow Y$  осуществляет проекцию с алфавита  $X$  на алфавит  $Y$ . Тогда язык  $f(M)$  представим источником  $S' = (f(X), Q, Q_0, D', F)$ , где  $D' = \{(q, b, q') : \exists a \in X (f(a) = b \ \& \ (q, a, q') \in D)\}$ , т.е. в граф-схеме источника  $S$  всякая пометка  $a$  из  $X$  заменяется на пометку  $f(a)$  из  $Y$ .

### Варианты.

	$x$	0	1	2	3	4	5		$x$	0	1	2	3	4	5	
<b>10.1.</b>	$f(x)$	<i>a</i>	<i>a</i>	<i>b</i>	<i>b</i>	<i>c</i>	<i>c</i>		<b>10.17.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>c</i>
<b>10.2.</b>	$f(x)$	<i>a</i>	<i>b</i>	<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>		<b>10.18.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>a</i>
<b>10.3.</b>	$f(x)$	<i>a</i>	<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>c</i>		<b>10.19.</b>	$f(x)$	<i>a</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>b</i>	<i>c</i>
<b>10.4.</b>	$f(x)$	<i>a</i>	<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>a</i>		<b>10.20.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<b>10.5.</b>	$f(x)$	<i>a</i>	<i>b</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>c</i>		<b>10.21.</b>	$f(x)$	<i>b</i>	<i>c</i>	<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<b>10.6.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>b</i>	<i>b</i>	<i>c</i>	<i>c</i>		<b>10.22.</b>	$f(x)$	<i>b</i>	<i>c</i>	<i>a</i>	<i>b</i>	<i>a</i>	<i>c</i>
<b>10.7.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>		<b>10.23.</b>	$f(x)$	<i>b</i>	<i>c</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>a</i>
<b>10.8.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>c</i>		<b>10.24.</b>	$f(x)$	<i>c</i>	<i>a</i>	<i>b</i>	<i>b</i>	<i>b</i>	<i>c</i>
<b>10.9.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>a</i>		<b>10.25.</b>	$f(x)$	<i>c</i>	<i>a</i>	<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<b>10.10.</b>	$f(x)$	<i>b</i>	<i>b</i>	<i>a</i>	<i>a</i>	<i>c</i>	<i>c</i>		<b>10.26.</b>	$f(x)$	<i>c</i>	<i>a</i>	<i>a</i>	<i>b</i>	<i>a</i>	<i>c</i>
<b>10.11.</b>	$f(x)$	<i>b</i>	<i>b</i>	<i>a</i>	<i>c</i>	<i>a</i>	<i>c</i>		<b>10.26.</b>	$f(x)$	<i>c</i>	<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>a</i>
<b>10.12.</b>	$f(x)$	<i>b</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>c</i>	<i>a</i>		<b>10.28.</b>	$f(x)$	<i>c</i>	<i>b</i>	<i>b</i>	<i>a</i>	<i>b</i>	<i>c</i>
<b>10.13.</b>	$f(x)$	<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>a</i>	<i>c</i>		<b>10.29.</b>	$f(x)$	<i>c</i>	<i>b</i>	<i>a</i>	<i>b</i>	<i>a</i>	<i>c</i>
<b>10.14.</b>	$f(x)$	<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>c</i>	<i>a</i>		<b>10.30.</b>	$f(x)$	<i>c</i>	<i>b</i>	<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>
<b>10.15.</b>	$f(x)$	<i>b</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>a</i>	<i>a</i>		<b>10.31.</b>	$f(x)$	<i>c</i>	<i>b</i>	<i>b</i>	<i>a</i>	<i>c</i>	<i>a</i>
<b>10.16.</b>	$f(x)$	<i>b</i>	<i>a</i>	<i>c</i>	<i>a</i>	<i>b</i>	<i>c</i>		<b>10.32.</b>	$f(x)$	<i>c</i>	<i>c</i>	<i>b</i>	<i>b</i>	<i>a</i>	<i>b</i>

**Задача 11.** По заданному источнику  $S$  с множеством входных символов  $X = \{a, b, c\}$ , допускающему язык  $L$ , построить источник, допускающий язык  $\text{Trunc}(L, a)$ . Множество входных символов  $X = \{a, b, c\}$ . Множество начальных состояний  $Q_0 = \{q_1, q_2\}$ . Множество выделенных состояний  $F = \{q_3, q_5\}$ . Вариант источника получить, добавив к граф-схеме источника на рис.7 стрелку варианта. Например, для варианта 30 к граф-схеме источника надо добавить стрелку  $(q_3, c, q_2)$ .

**Указание.** Пусть  $x = x(0)x(1)\dots x(k)aa\dots a$  при  $x(k) \neq a$  есть слово в алфавите  $X$ , содержащем букву  $a$ . Тогда операция *усечения* слова  $x$  по букве  $a$  (обозначение:  $Trunc(x,a)$ ) определяется как  $Trunc(x,a) = x(0)x(1)\dots x(k)$ . Если  $M \subseteq X$ , то множество  $Trunc(M,a) = \{Trunc(x,a) : x \in M\}$ .

**Замечание.** Множество всех слов в алфавите  $X = \{a,b,c\}$ , не заканчивающихся на символ  $a$ , допустимо (детерминированным) автоматом  $A$ , приведенным на рис.8. Начальное состояние есть  $q_0$ . Множество выделенных состояний  $F = \{q_b, q_c\}$ .

**Теорема.** Класс языков, представимых источниками, замкнут относительно операции усечения.

**Доказательство.** Пусть язык  $M$  представим источником  $S = (X, Q, Q_0, D, F)$ . Пусть  $a \in X$  и  $a^k = aaa\dots a$ ,  $k$  раз. Построим источник  $S' = (X, Q, Q_0, D, G)$ , где  $G = Q_a \cup F$ , где  $Q_a = \{q \in Q : \exists k \exists q' \in F ((q, a, q') \in D)\}$ , т.е.  $G$  есть  $F$ , объединенное с множеством  $Q_a$  всех тех состояний  $q \in Q$ , для которых существует слово  $a^k$  при некотором натуральном  $k$ , переводящее источник  $S$  из состояния  $q$  в состояние  $q'$ , при этом  $q' \in F$ . Например, для источника  $S$  (рис.6.7) множество  $Q_a$  строится следующим образом (рис.6.7a). Состояние  $q_4$  добавляется к  $F$ , ибо  $a^k$  при  $k=1$  переводит  $q_4$  в  $q_3 \in F$ . То же самое относительно  $q_3$ . Поэтому  $G = \{q_3, q_4\} \cup \{q_3, q_5\} = \{q_3, q_4, q_5\}$ . Источник  $S'$  отличается от источника  $S$  лишь множеством выделенных состояний  $G$ . Источник  $S'$  с поведением  $M' = Beh(S')$  допускает все те слова, которые допускают продолжение буквами  $a$  до слова, допустимого источником  $S$ , а также все слова, допустимые источником  $S$ .

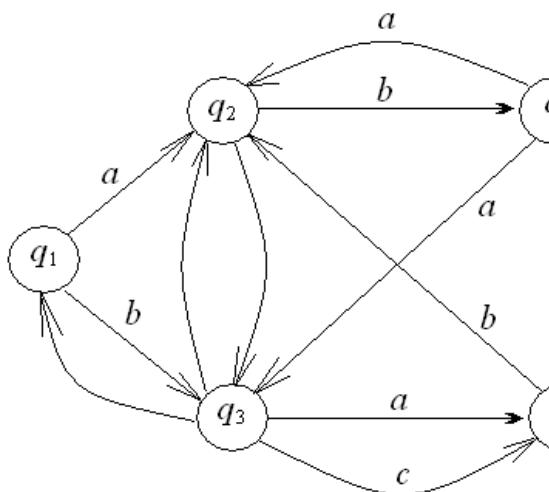


Рис.6.7

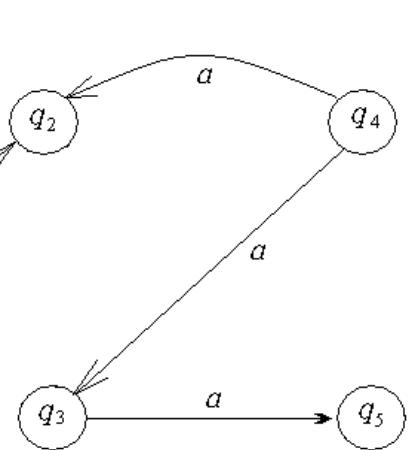


Рис.6.7a

Пусть  $S''$  есть источник, допускающий множество  $M''$  всех слов в алфавите  $X$ , не заканчивающихся на букву  $a$  (рис.6.8). Источник, допускающий множество  $M' \cap M''$  искомый.

**Замечание.** Множество всех слов в алфавите  $X = \{a,b,c\}$ , не заканчивающихся на символ  $a$ , допустимо (детерминированным) автоматом  $A$ , приведенным на рис.6.8. Начальное состояние есть  $q_0$ . Множество выделенных состояний  $F = \{q_b, q_c\}$ .

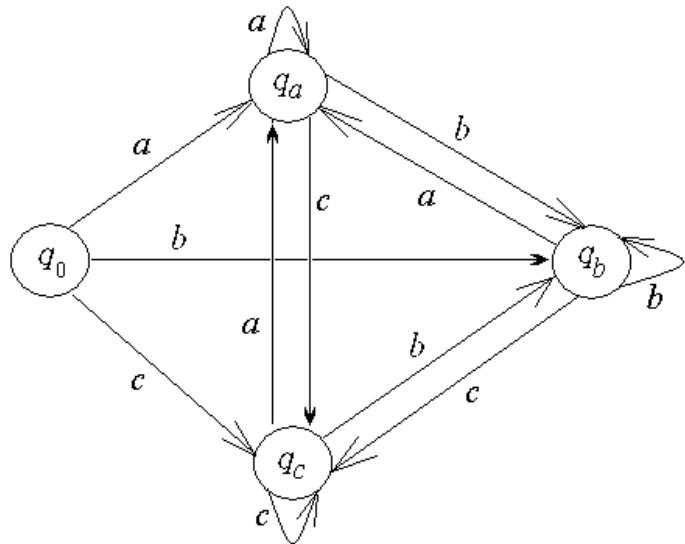


Рис.6.8

### Варианты.

- 11.1.**  $(q_1, c, q_2)$ .    **11.2.**  $(q_1, c, q_3)$ .    **11.3.**  $(q_1, c, q_4)$ .    **11.4.**  $(q_1, c, q_5)$ .  
**11.5.**  $(q_2, c, q_3)$ .    **11.6.**  $(q_2, c, q_4)$ .    **11.7.**  $(q_2, c, q_5)$ .    **11.8.**  $(q_3, c, q_4)$ .  
**11.9.**  $(q_3, c, q_5)$ .    **11.10.**  $(q_4, c, q_5)$ .    **11.11.**  $(q_1, b, q_2)$ .    **11.12.**  $(q_1, a, q_3)$ .  
**11.13.**  $(q_1, b, q_4)$ .    **11.14.**  $(q_2, c, q_3)$ .    **11.15.**  $(q_2, c, q_4)$ .    **11.16.**  $(q_3, c, q_4)$ .  
**11.17.**  $(q_2, b, q_1)$ .    **11.18.**  $(q_3, c, q_1)$ .    **11.19.**  $(q_4, c, q_1)$ .    **11.20.**  $(q_5, c, q_1)$ .  
**11.21.**  $(q_3, c, q_2)$ .    **11.22.**  $(q_4, c, q_2)$ .    **11.23.**  $(q_5, c, q_2)$ .    **11.24.**  $(q_4, c, q_3)$ .  
**11.25.**  $(q_5, c, q_3)$ .    **11.26.**  $(q_5, c, q_4)$ .    **11.27.**  $(q_2, c, q_1)$ .    **11.28.**  $(q_3, a, q_1)$ .  
**11.29.**  $(q_4, c, q_1)$ .    **11.30.**  $(q_3, c, q_2)$ .

**Задача 12.** Пусть  $x=x(0)x(1)\dots x(k)$  есть некоторое слово в алфавите  $X$ , причем слово  $x$  содержит букву  $a$ . Аннулирование буквы  $a$  в слове  $x$  есть удаление буквы  $a$  в слове  $x$  всюду, где она в  $x$  встречается. Обозначим эту операцию через  $An(x,a)$ . Пусть  $M \subseteq X^*$ . Тогда язык  $L_a = An(M,a) = \{An(x,a) : x \in M\}$ . По заданному источнику  $S$  из задачи 11 с множеством входных символов  $X=\{a,b,c\}$ , допускающему язык  $L$ , построить источник, допускающий язык  $L_a$ . Детерминизировать полученный источник.

**Указание.** Пусть  $x = x(0)x(1)\dots x(k)$  есть некоторое слово в алфавите  $X$ , причем слово  $x$  содержит букву  $a$ . Аннулирование буквы  $a$  в слове  $x$  есть удаление в слове  $x$  буквы  $a$  всюду, где она встречается. Обозначим эту операцию через  $An(x,a)$ . Пусть  $M \subseteq X^*$ . Пусть тогда  $An(M,a) = \{An(x,a) : x \in M\}$ .

**Теорема.** Класс языков, представимых источниками, замкнут относительно операции аннулирования.

**Доказательство.** Пусть язык  $M$  представим источником  $S = (X, Q, Q_0, D, F)$ . Тогда язык  $An(M,a)$  представим источником  $S' = (X, Q, Q_0, D', F)$ , где  $D' = \{(q,b,q') \in D : b \neq a\} \cup \{(q, *, q') : (q,a,q') \in D\}$ , т.е. в граф-схеме источника  $S$  удаляются буквы  $a$  всюду, где они встречаются, но сами стрелки, которые были помечены буквой  $a$ , остаются.

**Задача 13.** Провести анализ и синтез конечного автомата по регулярному выражению.

## ЛИТЕРАТУРА

- 1. Авдошин С. М., Набебин А. А.** Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.: ил.
- 2. Авдошин С. М., Набебин А. А.** Дискретная математика. Формально-логические системы и языки. – М.: ДМК Пресс, 2018. – 390 с.
- 3. Авдошин С. М., Набебин А. А.** Дискретная математика. Алгоритмы: теория и практика. – М.: ДМК Пресс, 2019. – 282 с.
- 4. Набебин А.А.** Логика и Пролог в дискретной математике. М.: МЭИ, 1996. 452с.
- 5. Набебин А.А., Кораблин Ю.П.** Математическая логика и теория алгоритмов. М.: Научный мир, 2008. 343с.
- 6. Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- 7. Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 509с.