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, в борьбе за счастье людей труда, посвящаю

СБОРНИК ЗАДАНИЙ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ

Москва
Научный мир
2009

УДК 519.1 + 510.6
ББК 22.176 + 22.12 Н 134
Н 13

Набебин А.А.
Н13 **Сборник заданий по дискретной математике.** – М.: Научный мир, 2009. – 280 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 (007) (495) 691-2847.
E-mail: naumir@benran.ru Internet http://bookish.iring.ru

Подписано к печати 12.01.2009
Формат 60×90/16
Гарнитура Таймс. Печать офсетная. Печ. л. 17.5
Тираж 1000 экз. Заказ 113

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

ISBN 978-5-91522-072-9

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 процессе преподавания курсов "Дискретная математика" и "Математическая логика и теория алгоритмов" в Московском энергетическом институте (МЭИ) и Российском государственном социальном 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 одинадцатую) 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.Исаков (дискретный логарифм, хэш-функция MASH), 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 из не более чем 15 цифр. Для работы с большими целыми числами с длиной десятиричной 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 Набебин А.А. "Логика и Пролог в дискретной математике" приведены Пролог-программы для некоторых алгоритмов из теории графов, комбинаторики и конечных автоматов.

В составлении задач принимали участие А.А.Болотов, А.А. Жданова, К.В.Коляда, Ю.П.Кораблин, Л.И.Ляшенко, Д.Г.Мещанинов, А.Б.Фролов.

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

Часть 1. УСЛОВИЯ ЗАДАЧ

1. МНОЖЕСТВА, ФУНКЦИИ, ОТНОШЕНИЯ

Задача 1. Пусть A, B, C – произвольные подмножества некоторого множества U (универсума). Пусть $\bar{A} = U-A$, $A \dot{-} B = (A-B) \cup (B-A)$. Доказать соотношения.

1.1. $A-(A-B) = A \cap B$. **1.2.** $A-(B-C) = (A-B)-C$.
1.3. $A \dot{-} B = B \dot{-} A$. **1.4.** $A \dot{-} (A \dot{-} B) = B$.
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. $A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$. **1.14.** $A \cap (B-C) = (A \cap B) - (A \cap C)$.
1.15. $A \cup B = A \dot{-} (B-(A \cap B))$. **1.16.** $A \cup B = (A \dot{-} B) \cup (A \cap B))$.
1.17. $A \cup B \subseteq C \leftrightarrow A \subseteq C$ и $B \subseteq C$. **1.18.** $A \subseteq B \cap C \leftrightarrow A \subseteq B$ и $A \subseteq C$.
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. $A = \neg B \leftrightarrow A \cap B = \varnothing$ и $A \cup B = U$. **1.26.** $A \subseteq B \rightarrow \neg B \subseteq \neg A$.
1.27. $A = B = A \dot{-} (A \cap B)$. **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 $(A, \leqslant)$, $A=\{0,1,2,3,\ldots,20\}$, задано диаграммой (рис.1.1). Множество $B \subseteq A$.

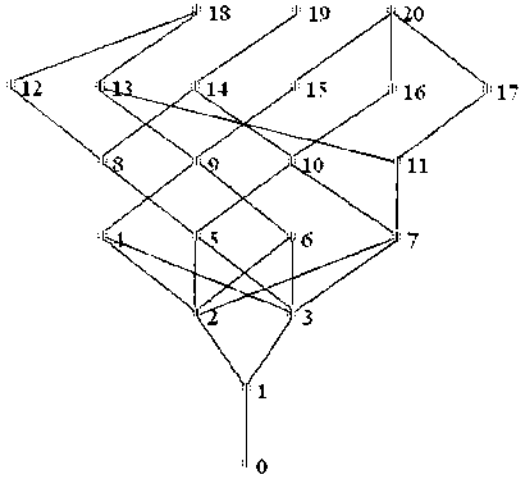


Рис.1.1

1. Начертить диаграмму для B.

2. Найти универсальные границы в A (наименьший элемент и наибольший элемент).

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.

Варианты множества B.

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

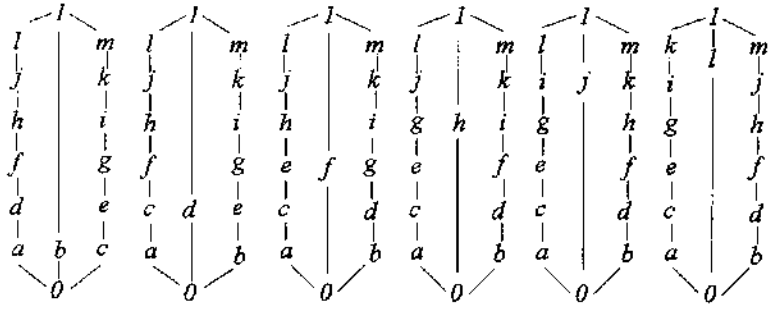
Задача 3. Пусть $A=\{0,1,2,\ldots,14\}$, $B=\{0,1,2,3,4,5\}$. Дана функция $f(x): A \to B$. Начертить ее график и найти для нее область определения, область значений, прообраз каждого ее значения, ядерную эквивалентность и каноническое разложение.

3.1. 310344501110451. **3.2.** 231434002301230.
3.3. 220330511113242. **3.4.** 321213141122123.
3.5. 121231234121231. **3.6.** 210311023230443.
3.7. 5454355544333453. **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.

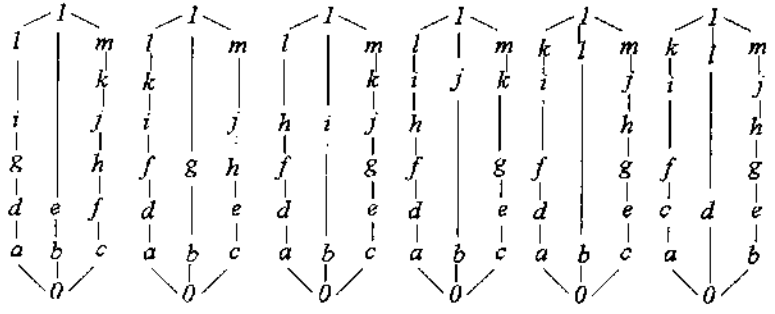
3.17. 104203201204321. **3.18.** 323213213232310.
3.19. 110023245013245. **3.20.** 312323123231223.
3.21. 240204040204040. **3.22.** 531335153531555.
3.23. 051212205005210. **3.24.** 450003205403231.
3.25. 023454320102030. **3.26.** 234143244312121.
3.27. 010101000203431. **3.28.** 054005545434502.
3.29. 324132433151230. **3.30.** 023415233143200.

Задача 4. Решетка задана своей диаграммой. Является ли она модулярной. Найти дополнения (если они есть) для элементов a, c, f, i.

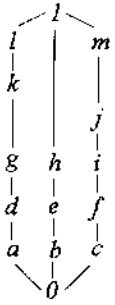
4.1 4.2 4.3 4.4 4.5 4.6



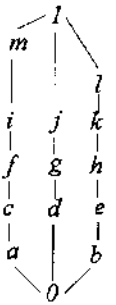
4.7 4.8 4.9 4.10 4.11 4.12



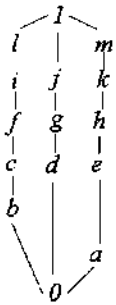
4.13



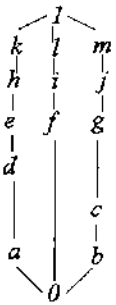
4.14



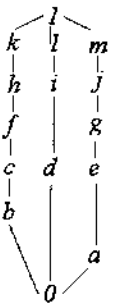
4.15



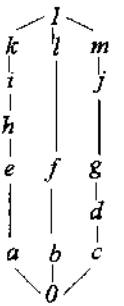
4.16



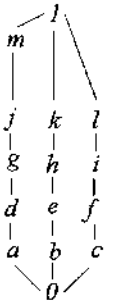
4.17



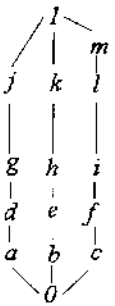
4.18



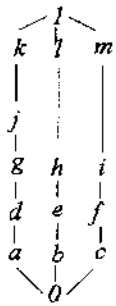
4.19



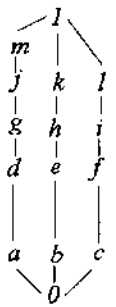
4.20



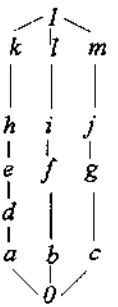
4.21



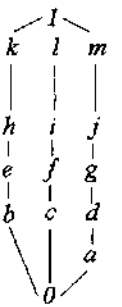
4.22



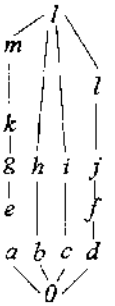
4.23



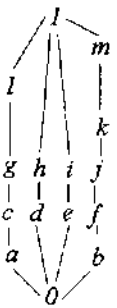
4.24



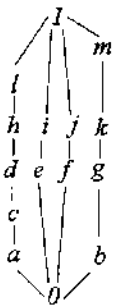
4.25



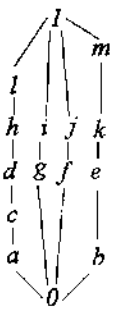
4.26



4.27



4.28



4.29

4.30

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

5.1.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

5.2.
$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

5.3.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.4.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.5.
$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

5.6.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.7.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

5.8.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.9.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.10.
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.11.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.12.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.13.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.14.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.15.
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

5.16.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.17.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.18.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.19.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.20.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.21.

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

5.22.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.23.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

5.24.

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.25.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.26.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.27.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

5.28.

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.29.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

5.30.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Задача 6. В булевой алгебре $(A,\leqslant)$ 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 $f: 2^A \to \{0,1\}$ и получить представление множества $Z=\{0,2,3\}$ из $A=\{0,1,2,3\}$ булевым многочленом относительно независимых множеств.

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. 0011011111100111. **6.20.** 1010001101110011.
6.21. 1110011111100001. **6.22.** 0010001001010111.
6.23. 1101110110001010. **4.24.** 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.

7.1. $r \subseteq (0,1)\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(0,+\infty)$,
$r = \{(x,y):\ y=x+3\}$, $s = \{(x,y):\ y \geqslant \sin x\}$.
7.2. $r \subseteq (0,1)\times\mathbb{R}$, $s \subseteq \mathbb{R}\times\mathbb{R}$,
$r = \{(x,y):\ y=x+3\}$, $s = \{(x,y):\ x^2+y^2 \leqslant 25\}$.
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. $r \subseteq (-1,1)\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(0,0.5)$,
$r = \{(x,y):\ y=x^2\}$, $s = \{(x,y):\ y=3x\}$.
7.5. $r \subseteq \mathbb{R}\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(0,1)$,
$r = \{(x,y):\ x \leqslant y^2\}$, $s = \{(x,y):\ x^2+y^2=4\}$.
7.6. $r \subseteq \mathbb{R}\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(0,1)$,
$r = \{(x,y):\ x=5y+3\}$, $s = \{(x,y):\ x^2+y^2 \leqslant 4\}$.
7.7. $r \subseteq (0,1)\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(2,4)$,
$r = \{(x,y):\ y=2x+3\}$, $s = \{(x,y):\ y=\cos x\}$,
7.8. $r \subseteq \mathbb{R}\times\mathbb{R}$, $s \subseteq \mathbb{R}\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2 \leqslant 4\}$, $s = \{(x,y):\ y=x^2+2\}$.
7.9. $r \subseteq (-2,2)\times(-2,2)$, $s \subseteq (-2,2)\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2=3\}$| $s = \{(x,y):\ x=5y+1\}$.
7.10. $r \subseteq (-2,2)\times(-2,2)$, $s \subseteq (-2,2)\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2 \geqslant 3\}$| $s = \{(x,y):\ y=5x^2-1\}$.
7.11. $r \subseteq (0,1)\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(0,+\infty)$,
$r = \{(x,y):\ y=x+3\}$, $s = \{(x,y):\ y \leqslant \sin x\}$.
7.12. $r \subseteq (-1,1)\times\mathbb{R}$, $s \subseteq \mathbb{R}\times(0,5)$,

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

7.13. $r \subseteq (0,2)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(-1,1)$,
$r = \{(x,y):\ y=x^3\},\ s = \{(x,y):\ y=x^2\}$.

7.14. $r \subseteq (-1,1)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,0.5)$,
$r = \{(x,y):\ y=x^2\},\ s = \{(x,y):\ y=3/x\}$.

7.15. $r \subseteq \mathbb{R}\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,1)$,
$r = \{(x,y):\ 2x \leqslant y^2\},\ s = \{(x,y):\ x^2+y^2=4\}$.

7.16. $r \subseteq \mathbb{R}\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,1)$,
$r = \{(x,y):\ x=y+3\},\ s = \{(x,y):\ x^2+y^2 \leqslant 4\}$.

7.17. $r \subseteq (0,1)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(2,4)$,
$r = \{(x,y):\ y=2x\},\ s = \{(x,y):\ y=\cos x\}$.

7.18. $r \subseteq \mathbb{R}\times\mathbb{R},\ s \subseteq \mathbb{R}\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2 \leqslant 4\},\ s = \{(x,y):\ y=x^2-2\}$.

7.19. $r \subseteq (-2,2)\times(-2,2),\ s \subseteq (-2,2)\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2=1\},\ s = \{(x,y):\ x=5y+1\}$.

7.20. $r \subseteq (-2,2)\times(-2,2),\ s \subseteq (-2,2)\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2 \geqslant 1\},\ s = \{(x,y):\ y=5x^2-1\}$.

7.21. $r \subseteq (0,1)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,+\infty)$,
$r = \{(x,y):\ y=2x\},\ s = \{(x,y):\ y \geqslant \sin x\}$.

7.22. $r \subseteq (0,1)\times\mathbb{R},\ s \subseteq \mathbb{R}\times\mathbb{R}$,
$r = \{(x,y):\ y=x+3\},\ s = \{(x,y):\ x^2+y^2 \leqslant 16\}$.

7.23. $r \subseteq (0,2)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(-1,1)$,
$r = \{(x,y):\ y=1/x-3x\},\ s = \{(x,y):\ y=x^2\}$.

7.24. $r \subseteq (-1,1)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,0.5)$,
$r = \{(x,y):\ y=x^2-x\},\ s = \{(x,y):\ y=3/x\}$.

7.25. $r \subseteq \mathbb{R}\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,1)$,
$r = \{(x,y):\ 2x \leqslant y^2\},\ s = \{(x,y):\ 2x^2+y^2=4\}$.

7.26. $r \subseteq \mathbb{R}\times\mathbb{R},\ s \subseteq \mathbb{R}\times(0,1)$,
$r = \{(x,y):\ x=y+3\},\ s = \{(x,y):\ 2x^2+y^2 \leqslant 4\}$.

7.27. $r \subseteq (0,1)\times\mathbb{R},\ s \subseteq \mathbb{R}\times(2,4)$,
$r = \{(x,y):\ y=1/x+2x\},\ s = \{(x,y):\ y=\cos x\}$.

7.28. $r \subseteq \mathbb{R}\times\mathbb{R},\ s \subseteq \mathbb{R}\times\mathbb{R}$,
$r = \{(x,y):\ 2x^2+y^2 \leqslant 4\},\ s = \{(x,y):\ y=x^2-2\}$.

7.29. $r \subseteq (-2,2)\times(-2,2),\ s \subseteq (-2,2)\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2=1\},\ s = \{(x,y):\ x^2=5y+1\}$.

7.30. $r \subseteq (-2,2)\times(-2,2),\ s \subseteq (-2,2)\times\mathbb{R}$,
$r = \{(x,y):\ x^2+y^2 \geqslant 1\},\ s = \{(x,y):\ y=5x^2-1/y\}$.

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.

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. 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. МОДУЛЯРНАЯ АРИФМЕТИКА

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, $0 \leqslant r_1, r_2 < b$, для которых $a=bq_1+r_1$, $-a=bq_2+r_2$.

Задача 2. Записать числа в восьмеричной, шестнадцатиричной, десятичной системах счисления.

2.1. $(1111001011110001)_2$.
2.2. $(1001110000111011)_2$.
2.3. $(1100111001110010)_2$.
2.4. $(1101000111000101)_2$.
2.5. $(1100010110100110)_2$.
2.6. $(1001110100011010)_2$.
2.7. $(1100110000011110)_2$.
2.8. $(1111000100111011)_2$.
2.9. $(1000110101110110)_2$.
2.10. $(1011101011000101)_2$.
2.11. $(1011101100011110)_2$.
2.12. $(1111011001011010)_2$.
2.13. $(1001111010111010)_2$.
2.14. $(1101101010011101)_2$.
2.15. $(1011101011011100)_2$.
2.16. $(1011000101111100)_2$.
2.17. $(1001110101111100)_2$.
2.18. $(1011011101111100)_2$.
2.19. $(1101110001110111)_2$.
2.20. $(1111110010001101)_2$.
2.21. $(1111011111100010)_2$.
2.22. $(1000110101000101)_2$.
2.23. $(1110001010111001)_2$.
2.24. $(1100010101000111)_2$.
2.25. $(1011100110000110)_2$.
2.26. $(1100011101110011)_2$.
2.27. $(1000011001110011)_2$.
2.28. $(1101011001110011)_2$.
2.29. $(1111010001010110)_2$.
2.30. $(1101011001010110)_2$.

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

Задача 4. Перемножить числа из задачи 3 в системе счисления по основанию семь.

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

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.

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.

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 $d = ua+vb$.

Задача 9. Найти непрерывную и подходящие дроби для числа a/b, $a>b$. Числа a и b взять из задачи 8.

Задача 10. Написать полную $\mathbb{Z}_n$, наименьшую по модулю, приведенную системы вычетов по данному модулю n. Для полной и приведенной системы вычетов написать таблицы сложения, умножения. Написать каноническое разложение числа n и вычислить для него функцию Эйлера $\varphi(n)$. 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.

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.

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

Задача 12. Решить (подбором) сравнения.

12.1. $x^4+2x^2+3x+4\equiv 0 \pmod 5$. **12.2.** $x^4+2x^3+3x+4\equiv 0 \pmod 5$.
12.3. $x^4+2x^3+3x^2+4\equiv 0 \pmod 5$. **12.4.** $x^4+x^2+3x+4\equiv 0 \pmod 5$.
12.5. $2x^4+x^3+3x+4\equiv 0 \pmod 5$. **12.6.** $2x^4+x^3+3x^2+4\equiv 0 \pmod 5$.
12.7. $2x^4+3x^2+x+4\equiv 0 \pmod 5$. **12.8.** $2x^4+3x^3+x+4\equiv 0 \pmod 5$.
12.9. $2x^4+3x^3+x^2+4\equiv 0 \pmod 5$. **12.10.** $2x^4+3x^3+x^2+4x\equiv 0 \pmod 5$.
12.11. $2x^4+3x^2+4x+1\equiv 0 \pmod 5$. **12.12.** $2x^4+3x^3+4x+1\equiv 0 \pmod 5$.
12.13. $2x^4+3x^3+4x^2+1\equiv 0 \pmod 5$. **12.14.** $x^4+3x^2+2x+4\equiv 0 \pmod 5$.
12.15. $x^4+3x^3+2x+4\equiv 0 \pmod 5$. **12.16.** $x^4+3x^3+2x^2+4\equiv 0 \pmod 5$.
12.17. $3x^4+x^2+2x+4\equiv 0 \pmod 5$. **12.18.** $3x^4+x^3+2x+4\equiv 0 \pmod 5$.
12.19. $3x^4+x^3+2x^2+4\equiv 0 \pmod 5$. **12.20.** $3x^4+2x^2+x+4\equiv 0 \pmod 5$.
12.21. $3x^4+2x^3+x+4\equiv 0 \pmod 5$. **12.22.** $3x^4+2x^3+x+4\equiv 0 \pmod 5$.
12.23. $3x^4+2x^2+4x+1\equiv 0 \pmod 5$. **12.24.** $3x^4+2x^3+4x+1\equiv 0 \pmod 5$.
12.25. $3x^4+2x^3+4x^2+1\equiv 0 \pmod 5$. **12.26.** $3x^4+2x^3+4x^2+x\equiv 0 \pmod 5$.
12.27. $x^4+3x^2+4x+2\equiv 0 \pmod 5$. **12.28.** $x^4+3x^3+4x+2\equiv 0 \pmod 5$.
12.29. $x^4+3x^3+4x^2+2\equiv 0 \pmod 5$. **12.30.** $x^4+3x^3+4x^2+2x\equiv 0 \pmod 5$.

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

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 15. Решить систему из трех сравнений.

5.1.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 1 \pmod{11}, \\ x\equiv 3 \pmod{13}. \end{cases}$$

15.2.
$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 1 \pmod{11}, \\ x\equiv 2 \pmod{13}. \end{cases}$$

15.3.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 5 \pmod{11}, \\ x\equiv 1 \pmod{13}. \end{cases}$$

15.4.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 1 \pmod{11}, \\ x\equiv 6 \pmod{13}. \end{cases}$$

15.5.
$$\begin{cases} x\equiv 1 \pmod 7, \\ x\equiv 2 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.6.
$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 1 \pmod{11}, \\ x\equiv 3 \pmod{13}. \end{cases}$$

15.7.
$$\begin{cases} x\equiv 3 \pmod 7, \\ x\equiv 1 \pmod{11}, \\ x\equiv 5 \pmod{13}. \end{cases}$$

15.8.
$$\begin{cases} x\equiv 6 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 1 \pmod{13}. \end{cases}$$

15.9.
$$\begin{cases} x\equiv 1 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.10.
$$\begin{cases} x\equiv 5 \pmod 7, \\ x\equiv 4 \pmod{11}, \\ x\equiv 1 \pmod{13}. \end{cases}$$

15.11.
$$\begin{cases} x\equiv 6 \pmod 7, \\ x\equiv 4 \pmod{11}, \\ x\equiv 1 \pmod{13}. \end{cases}$$

15.12.
$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 7 \pmod{11}, \\ x\equiv 1 \pmod{13}. \end{cases}$$

15.13.
$$\begin{cases} x\equiv 1 \pmod 7, \\ x\equiv 5 \pmod{11}, \\ x\equiv 6 \pmod{13}. \end{cases}$$

15.14.
$$\begin{cases} x\equiv 5 \pmod 7, \\ x\equiv 7 \pmod{11}, \\ x\equiv 1 \pmod{13}. \end{cases}$$

15.15.
$$\begin{cases} x\equiv 1 \pmod 7, \\ x\equiv 6 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.16.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 4 \pmod{13}. \end{cases}$$

15.17.
$$\begin{cases} x\equiv 3 \pmod 7, \\ x\equiv 2 \pmod{11}, \\ x\equiv 5 \pmod{13}. \end{cases}$$

15.18.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 6 \pmod{13}. \end{cases}$$

15.19.
$$\begin{cases} x\equiv 3 \pmod 7, \\ x\equiv 2 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.20.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 4 \pmod{11}, \\ x\equiv 5 \pmod{13}. \end{cases}$$

15.21.
$$\begin{cases} x\equiv 6 \pmod 7, \\ x\equiv 2 \pmod{11}, \\ x\equiv 4 \pmod{13}. \end{cases}$$

15.22.
$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 7 \pmod{11}, \\ x\equiv 2 \pmod{13}. \end{cases}$$

15.23.
$$\begin{cases} x\equiv 6 \pmod 7, \\ x\equiv 5 \pmod{11}, \\ x\equiv 2 \pmod{13}. \end{cases}$$

15.24.
$$\begin{cases} x\equiv 5 \pmod 7, \\ x\equiv 2 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.25.
$$\begin{cases} x\equiv 2 \pmod 7, \\ x\equiv 7 \pmod{11}, \\ x\equiv 6 \pmod{13}. \end{cases}$$

15.26.
$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 5 \pmod{13}. \end{cases}$$

15.27.
$$\begin{cases} x\equiv 3 \pmod 7, \\ x\equiv 4 \pmod{11}, \\ x\equiv 6 \pmod{13}. \end{cases}$$

15.28.
$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.29.
$$\begin{cases} x\equiv 5 \pmod 7, \\ x\equiv 3 \pmod{11}, \\ x\equiv 6 \pmod{13}. \end{cases}$$

15.30.
$$\begin{cases} x\equiv 3 \pmod 7, \\ x\equiv 5 \pmod{11}, \\ x\equiv 7 \pmod{13}. \end{cases}$$

15.31.
$$\begin{cases} x\equiv 6 \pmod 7, \\ x\equiv 7 \pmod{11}, \\ x\equiv 3 \pmod{13}. \end{cases}$$

Задача 16. Решить систему из трех сравнений.

16.1. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 1 \pmod 9, \\ x \equiv 4 \pmod{15}. \end{cases}$

16.2. $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv -1 \pmod 9, \\ x \equiv 2 \pmod{15}. \end{cases}$

16.3. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 5 \pmod 9, \\ x \equiv 2 \pmod{15}. \end{cases}$

16.4. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 1 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.5. $\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv 1 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.6. $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv -3 \pmod 9, \\ x \equiv 3 \pmod{15}. \end{cases}$

16.7. $\begin{cases} x \equiv 3 \pmod 7, \\ x \equiv -1 \pmod 9, \\ x \equiv 5 \pmod{15}. \end{cases}$

16.8. $\begin{cases} x \equiv 6 \pmod 7, \\ x \equiv 3 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.9. $\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv -2 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.10. $\begin{cases} x \equiv 5 \pmod 7, \\ x \equiv 4 \pmod 9, \\ x \equiv 1 \pmod{15}. \end{cases}$

16.11. $\begin{cases} x \equiv 6 \pmod 7, \\ x \equiv 4 \pmod 9, \\ x \equiv 1 \pmod{15}. \end{cases}$

16.12. $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv 7 \pmod 9, \\ x \equiv 1 \pmod{15}. \end{cases}$

16.13. $\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv -5 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.14. $\begin{cases} x \equiv 5 \pmod 7, \\ x \equiv 7 \pmod 9, \\ x \equiv 1 \pmod{15}. \end{cases}$

16.15. $\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv 8 \pmod 9, \\ x \equiv 2 \pmod{15}. \end{cases}$

16.16. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 8 \pmod 9, \\ x \equiv 2 \pmod{15}. \end{cases}$

16.17. $\begin{cases} x \equiv 3 \pmod 7, \\ x \equiv 2 \pmod 9, \\ x \equiv 5 \pmod{15}. \end{cases}$

16.18. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 3 \pmod 9, \\ x \equiv 6 \pmod{15}. \end{cases}$

16.19. $\begin{cases} x \equiv 3 \pmod 7, \\ x \equiv 1 \pmod 9, \\ x \equiv 8 \pmod{15}. \end{cases}$

16.20. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv -4 \pmod 9, \\ x \equiv 5 \pmod{15}. \end{cases}$

16.21. $\begin{cases} x \equiv 6 \pmod 7, \\ x \equiv -2 \pmod 9, \\ x \equiv 4 \pmod{15}. \end{cases}$

16.22. $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv -7 \pmod 9, \\ x \equiv 2 \pmod{15}. \end{cases}$

16.23. $\begin{cases} x \equiv 6 \pmod 7, \\ x \equiv -5 \pmod 9, \\ x \equiv 2 \pmod{15}. \end{cases}$

16.24. $\begin{cases} x \equiv 5 \pmod 7, \\ x \equiv -2 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.25. $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv -7 \pmod 9, \\ x \equiv 8 \pmod{15}. \end{cases}$

16.26. $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv -5 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.27. $\begin{cases} x \equiv 3 \pmod 7, \\ x \equiv -5 \pmod 9, \\ x \equiv 7 \pmod{15}. \end{cases}$

16.28. $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv -4 \pmod 9, \\ x \equiv 8 \pmod{15}. \end{cases}$

16.29.
$$\begin{cases} x\equiv 5 \pmod 7, \\ x\equiv -7 \pmod 9, \\ x\equiv 2 \pmod{15}. \end{cases}$$

16.30.
$$\begin{cases} x\equiv 3 \pmod 7, \\ x\equiv -5 \pmod 9, \\ x\equiv 1 \pmod{15}. \end{cases}$$

16.31.
$$\begin{cases} x\equiv 6 \pmod 7, \\ x\equiv 7 \pmod 9, \\ x\equiv 3 \pmod{15}. \end{cases}$$

Задача 17. Решить систему из трех сравнений.

17.1.
$$\begin{cases} 3x\equiv 2 \pmod 7, \\ 4x\equiv 1 \pmod 9, \\ 3x\equiv 4 \pmod{13}. \end{cases}$$

17.2.
$$\begin{cases} 4x\equiv 4 \pmod 7, \\ 2x\equiv -1 \pmod 9, \\ 5x\equiv 2 \pmod{13}. \end{cases}$$

17.3.
$$\begin{cases} 5x\equiv 2 \pmod 7, \\ 7x\equiv 5 \pmod 9, \\ 6x\equiv 2 \pmod{13}. \end{cases}$$

17.4.
$$\begin{cases} 6x\equiv 2 \pmod 7, \\ 5x\equiv 1 \pmod 9, \\ 4x\equiv 7 \pmod{13}. \end{cases}$$

17.5.
$$\begin{cases} 4x\equiv 1 \pmod 7, \\ 4x\equiv 1 \pmod 9, \\ 5x\equiv 7 \pmod{13}. \end{cases}$$

17.6.
$$\begin{cases} 3x\equiv 4 \pmod 7, \\ 5x\equiv -3 \pmod 9, \\ 3x\equiv 3 \pmod{13}. \end{cases}$$

17.7.
$$\begin{cases} 5x\equiv 3 \pmod 7, \\ 7x\equiv -1 \pmod 9, \\ 4x\equiv 5 \pmod{13}. \end{cases}$$

17.8.
$$\begin{cases} 6x\equiv 6 \pmod 7, \\ 2x\equiv 3 \pmod 9, \\ 6x\equiv 7 \pmod{13}. \end{cases}$$

17.9.
$$\begin{cases} 5x\equiv 1 \pmod 7, \\ 5x\equiv -2 \pmod 9, \\ 5x\equiv 7 \pmod{13}. \end{cases}$$

17.10.
$$\begin{cases} 4x\equiv 5 \pmod 7, \\ 2x\equiv 4 \pmod 9, \\ 7x\equiv 1 \pmod{13}. \end{cases}$$

17.11.
$$\begin{cases} 3x\equiv 6 \pmod 7, \\ 4x\equiv 4 \pmod 9, \\ 4x\equiv 1 \pmod{13}. \end{cases}$$

17.12.
$$\begin{cases} 6x\equiv 4 \pmod 7, \\ 7x\equiv 7 \pmod 9, \\ 3x\equiv 1 \pmod{13}. \end{cases}$$

17.13.
$$\begin{cases} 5x\equiv 1 \pmod 7, \\ 2x\equiv -5 \pmod 9, \\ 2x\equiv 7 \pmod{13}. \end{cases}$$

17.14.
$$\begin{cases} 4x\equiv 5 \pmod 7, \\ 4x\equiv 7 \pmod 9, \\ 3x\equiv 1 \pmod{13}. \end{cases}$$

17.15.
$$\begin{cases} 6x\equiv 1 \pmod 7, \\ 5x\equiv 8 \pmod 9, \\ 4x\equiv 2 \pmod{13}. \end{cases}$$

17.16.
$$\begin{cases} 3x\equiv 2 \pmod 7, \\ 7x\equiv 8 \pmod 9, \\ 5x\equiv 2 \pmod{13}. \end{cases}$$

17.17.
$$\begin{cases} 4x\equiv 3 \pmod 7, \\ 5x\equiv 2 \pmod 9, \\ 4x\equiv 5 \pmod{13}. \end{cases}$$

17.18.
$$\begin{cases} 3x\equiv 2 \pmod 7, \\ 4x\equiv 3 \pmod 9, \\ 3x\equiv 6 \pmod{13}. \end{cases}$$

17.19.
$$\begin{cases} 6x\equiv 3 \pmod 7, \\ 2x\equiv 1 \pmod 9, \\ 6x\equiv 8 \pmod{13}. \end{cases}$$

17.20.
$$\begin{cases} 5x\equiv 2 \pmod 7, \\ 7x\equiv -4 \pmod 9, \\ 5x\equiv 5 \pmod{13}. \end{cases}$$

17.21.
$$\begin{cases} 3x\equiv 6 \pmod 7, \\ 2x\equiv -2 \pmod 9, \\ 6x\equiv 4 \pmod{13}. \end{cases}$$

17.22.
$$\begin{cases} 6x\equiv 4 \pmod 7, \\ 5x\equiv -7 \pmod 9, \\ 7x\equiv 2 \pmod{13}. \end{cases}$$

17.23.
$$\begin{cases} 4x\equiv 6 \pmod 7, \\ 7x\equiv -5 \pmod 9, \\ 3x\equiv 2 \pmod{13}. \end{cases}$$

17.24.
$$\begin{cases} 5x\equiv 5 \pmod 7, \\ 4x\equiv -2 \pmod 9, \\ 5x\equiv 7 \pmod{13}. \end{cases}$$

17.25.
$$\begin{cases} 6x\equiv 2 \pmod 7, \\ 2x\equiv -7 \pmod 9, \\ 6x\equiv 8 \pmod{13}. \end{cases}$$

17.26.
$$\begin{cases} 3x\equiv 4 \pmod 7, \\ 2x\equiv -5 \pmod 9, \\ 4x\equiv 7 \pmod{13}. \end{cases}$$

17.27.
$$\begin{cases} 4x\equiv 3 \pmod 7, \\ 7x\equiv -5 \pmod 9, \\ 5x\equiv 7 \pmod{13}. \end{cases}$$

17.28.
$$\begin{cases} 5x\equiv 4 \pmod 7, \\ 4x\equiv -4 \pmod 9, \\ 3x\equiv 8 \pmod{13}. \end{cases}$$

17.29.
$$\begin{cases} 6x\equiv 5 \pmod 7, \\ 5x\equiv -7 \pmod 9, \\ 5x\equiv 2 \pmod{13}. \end{cases}$$

17.30.
$$\begin{cases} 4x\equiv 3 \pmod 7, \\ 7x\equiv -5 \pmod 9, \\ 5x\equiv 1 \pmod{13}. \end{cases}$$

17.31.
$$\begin{cases} 5x\equiv 6 \pmod 7, \\ 2x\equiv 7 \pmod 9, \\ 7x\equiv 3 \pmod{13}. \end{cases}$$

Задача 18. Определить с помощью символа Лежандра, имеет ли решение сравнение $x^2\equiv a \pmod p$. Взять 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.

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. Взять 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.

Задача 20. Полиномы $f(x), g(x) \in \mathbb{Z}_5[x]$. Найти их наибольший общий 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. $x^8+2x^7+2x^6+2x^4+x^3+x^2+3x+4$, $x^5+x^4+2x^3+2x^2+2x+1$.

20.3. $x^8+2x^7+4x^6+2x^5+4x^3+x+3x^4+x^2+1$, $x^5+x^4+2x^2+3x^3+3x+2$.
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. $x^8+4x^7+x^6+2x^5+4x+3x^4+2x^2+4$, $x^5+2x^4+3x^2+x+4$.
20.6. $x^8+x^7+4x^6+2x^5+x^3+2x+3x^4+x^2+1$, $x^5+3x^4+4x^2+4x^3+x+3$.
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. $x^8+3x^7+2x^6+4x^3+2x+2x^4+x^2+4$, $x^5+4x^4+2x^3+1$.
20.9. $x^8+3x^7+4x^6+3^5+x^3+4x+3x^4+x^2+1$, $x^5+4x^4+3x^3+x+2$.
20.10. $4x^8+3x^4+4$, $2x^5+2x^2+3x^3+x+1$.
20.11. $4x^8+2x^6+x^4+3x^2+4$, $2x^5+2x^2+x^3+4x+4$.
20.12. $4x^8+4x^7+x^6+3x^5+4x^3+3x+2x^4+4x^2+4$, $2x^5+x^4+3x^2+3+x^3+2x+1$.
20.13. $4x^8+4x^7+4x^6+2x^5+4x+2x^4+3x^2+1$, $2x^5+x^4+3x^2+4x+3$.
20.14. $4x^8+3x^7+3x^6+4x^3+2x+3x^4+4x^2+1$, $2x^5+2x^4+4x^2+4x^3+4x+2$.
20.15. $4x^8+3x^7+6x^6+3x^5+x^3+4x+2x^4+4x^2+4$, $2x^5+2x^4+4x^2+x^3+x+4$.
20.16. $4x^8+2x^7+3x^6+x^3+3x+3x^4+4x^2+1$, $2x^5+3x^4+4x^3+2$.
20.17. $4x^8+2x^7+x^6+2x^5+4x^3+x+2x^4+4x^2+4$, $2x^5+3x^4+x^3+2x+4$.
20.18. $4x^8+x^7+x^6+2x^5+x^3+2x+2x^4+4x^2+4$, $2x^5+4x^4+x^2+3x^3+1$.
20.19. $4x^8+x^7+4x^6+3x^5+x+2x^4+3x^2+1$, $2x^5+4x^4+x^2+2x+3$.
20.20. $4x^8+2x^6+x^4+3x^2+4$, $3x^5+3x^2+4x^3+x+1$.
20.21. $4x^8+3x^4+4$, $2x^5+2x^2+x^3+4x+4$.
20.22. $4x^8+x^7+4x^6+3x^5+x+2x^4+3x^2+1$, $3x^5+x^4+4x^2+3x+2$.
20.23. $4x^8+x^7+x^6+2x^5+x^3+2x+2x^4+4x^2+4$, $3x^5+x^4+4x^2, 2x^3+4$.
20.24. $4x^8+2x^7+x^6+2x^5+4x^3+x+2x^4+4x^2+4$, $3x^5+2x^4+4x^3+3x+1$.
20.25. $4x^8+2x^7+3x^6+x^3+3x+3x^4+4x^2+1$, $3x^5+2x^4+4x+2$.
20.26. $4x^8+3x^7+x^6+3x^5+x^3+4x+2x^4+4x^2+4$, $3x^5+3x^4+6x^2+4x^3+4x+1$.
20.27. $4x^8+3x^7+3x^6+4x^3+2x+3x^4+4x^2+1$, $3x^5+3x^4+x^2+x^3+x+3$.
20.28. $4x^8+4x^7+4x^6+2x^5+4x+2x^4+3x^2+1$, $3x^5+4x^4+2x^2+x+2$.
20.29. $4x^8+4x^7+x^6+3x^5+4x^3+3x+2x^4+4x^2+4$, $3x^5+4x^4+2x^2+2x^3+3x+4$.
20.30. $x^8+2x^7+2x^6+x^3+3x+2x^4+x^2+4$, $x^5+x^2+3x^3+2x+2$.

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 задания 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 $\mathrm{GF}(p^m) = \mathbb{Z}_p[x]/(f(x))$ из $q=p^m$ остатков от деления полиномов из $\mathbb{Z}_p[x]$ на $f(x)$ с операциями сложения и умножения полиномов по модулю $f(x)$.

d) для поля $GF(p^m)$ построить таблицы для сложения и умножения элементов a_1x+a_0, a_1=3, $a_0\in\mathbb{Z}_5$, на все элементы поля $GF(p^m)$.

е) 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.

Задача 22. $p=5$, $m=2$. Найти степень (по умножению) элемента 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 и определяется вариантом задания.

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.

Задача 23. Зашифровать и расшифровать сообщение с помощью криптосистемы RSA (R.Rivest, A.Shamir, L.Adleman). Простые числа p и q определяются вариантом задания. В качестве исходного текста взять три первых латинских буквы своей фамилии.

23.1. 5737,5669. **23.2.** 5741,5659. **23.3.** 5743,5657.
23.4. 5749,5653. **23.5.** 5779,5651. **23.6.** 5783,5647.
23.7. 5791,5641. **23.8.** 5801,5639. **23.9.** 5807,5623.
23.10. 5813,5591. **23.11.** 5821,5581. **23.12.** 5827,5573.
23.13. 5839,5569. **23.14.** 5843,5563. **23.15.** 5849,5557.
23.16. 5851,5531. **23.17.** 5857,5527. **23.18.** 5861,5521.
23.19. 5867,5519. **23.20.** 5869,5507. **23.21.** 5879,5503.
23.22. 5881,5501. **23.23.** 5897,5483. **23.24.** 5903,5479.
23.25. 5923,5477. **23.26.** 5927,5471. **23.27.** 5939,5449.
23.28. 5953,5443. **23.29.** 5981,5441. **23.30.** 5987,5437.

Задача 24. Зашифровать и расшифровать сообщение с помощью криптосистемы RSA с электронной подписью. Простые числа p и q взять из задачи 29. В качестве исходного текста взять три первые латинские буквы своей фамилии.

Задача 25. Зашифровать и расшифровать сообщение с помощью криптосистемы ЭльГамаля. В качестве простого числа p взять большее число варианта из задачи 29. В качестве исходного текста взять три первые латинские буквы своей фамилии.

Задача 26. Вычислить и проверить подпись под сообщением с помощью криптосистемы ElGamal для электронной подписи. В качестве простого числа p взять большее число варианта из задачи 23. В качестве исходного текста взять слова своего полного имени: фамилия, имя, отчество.

Задача 27. Зашифровать и расшифровать сообщение с помощью (обобщенной) криптосистемы ЭльГамаля над (конечным) полем Галуа $GF(p^m)$. Взять простое число p=31, натуральное m=3. Неприводимый полином над $\mathbb{Z}_p$ определяется номером варианта. В качестве исходного текста взять три первые латинские буквы своей фамилии.

27.1. $29x^3+3$. **27.2.** $29x^3+5$. **27.3.** $29x^3+6$.
27.4. $29x^3+7$. **27.5.** $29x^3+9$. **27.6.** $29x^3+10$.
27.7. $29x^3+11$. **27.8.** $29x^3+12$. **27.9.** $29x^3+13$.
27.10. $29x^3+14$. **27.11.** $29x^3+17$. **27.12.** $29x^3+18$.
27.13. $29x^3+19$. **27.14.** $29x^3+20$. **27.15.** $29x^3+21$.
27.16. $29x^3+22$. **27.17.** $29x^3+24$. **27.18.** $29x^3+25$.
27.19. $29x^3+26$. **27.20.** $29x^3+28$. **27.21.** $23x^3+3$.
27.22. $23x^3+5$. **27.23.** $23x^3+6$. **27.24.** $23x^3+7$.
27.25. $23x^3+9$. **27.26.** $23x^3+10$. **27.27.** $23x^3+11$.
27.28. $23x^3+12$. **27.29.** $23x^3+13$. **27.30.** $23x^3+14$.

Задача 28. Вычислить и проверить подпись под сообщением с помощью (обобщенной) криптосистемы ЭльГамаля для электронной подписи над (конечным) полем Галуа $GF(p^m)$. Взять простое число p=31, натуральное m=3. Неприводимый полином над $\mathbb{Z}_p$ взять из задачи 27. В качестве исходного текста взять слова своего полного имени: фамилия, имя, отчество.

Задача 29. Вычислить и проверить подпись под сообщением с помощью криптосистемы DSA (Digital Signature Algorithm) для электронной подписи. Простые числа p и q определяются вариантом задания. В качестве исходного текста взять слова своего полного имени: фамилия, имя, отчество.

29.1.1350551, 27011. **29.2.**378239,27017. **29.3.**270311,27031.
29.4.324517, 27043. **29.5.**541181,27059. **29.6.**324733, 27061.
29.7.433073, 27067. **29.8.**812191,27073. **29.9.**487387, 27077.

29.10.325093, 27091. 29.11.813091,27103. 29.12.379499,27107.
29.13.325309, 27109. 29.14.488287,27127. 29.15.868577,27143.
29.16.326149, 27179. 29.17.489439,27191. 29.18.979093,27197.
29.19.489799, 27211. 29.20.326869,27239. 29.21.272411,27241.
29.22.1635181,27253. 29.23.490663,27259.29.24.1090841,27271.
29.25.272771, 27277. 29.26.491059,27281. 29.27.436529,27283.
29.28.873569, 27299. 29.29.491923,27329. 29.30.492067,27337.

3. КОМБИНАТОРИКА

Формулы для размещений, перестановок, сочетаний

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.

Задача 2. В каталоге библиотеки приведены наименования N+100 различных журналов. Найти число способов выбора пяти попарно различных журналов.

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, считаются различными.

Задача 4. Сколькими способами можно выбрать 7 делегатов на конференцию от коллектива в N+200 человек?

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

Задача 6. В районе имеется N+10 памятников. Время позволяет осмотреть только 3 из них. Укажите число возможных маршрутов. Порядок прохождения маршрутов существенен.

Задача 7. Студентам предложено на выбор N+5 гуманитарных курсов. Сколькими способами студент может выбрать 3 из них?

Задача 8. Сколькими способами можно рассадить N+20 студентов (по одному за каждый компьютер) в дисплейном классе, оснащенном 20 компьютерами? Номера компьютеров существенны.

Задача 9. В соревновании участвуют N+15 спортсменов. Укажите число вариантов очередности их выступления.

Задача 10. В отделе работает N+12 сотрудников, которые могут уходить в отпуск только по одному в месяц. Сколько вариантов распределения отпусков в году возможно?

Задача 11. В киоске имеется N+10 сортов мороженого одинаковой стоимости. Сколькими способами можно купить 3 порции мороженого попарно различных сортов?

Задача 12. Группа из N+23 человека должна выполнить лабораторную работу. Сколькими способами можно разбить группу на бригады по 3 человека в бригаде?

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?

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?

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?

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?

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?

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

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. Сколькими способами можно выделитиь такой наряд, имея в распоряжении $n=N+20$ человек?

Задача 20. Сколькими способами можно распределить 6 именных стипендий между N+100 отличниками, если имеется 1 стипендия имени М1, 2 стипендии имени М2, 3 стипендии имени М3?

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,

$1 \leqslant l \leqslant n$. Сколько различных имен переменных возможно в этом языке?

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

а) все мальчики должны сидеть на самых левых местах;

б) никакие два мальчика не должны сидеть рядом;

в) Маша и Петя должны сидеть вместе.

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

а) в линию? б) в круг?

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

Задача 25.

а) Сколькими способами могут быть упорядочены буквы в слове parallelogram с приписанной к нему вашей фамилией, записанной в латинице?

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

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.

Задача 26–1. Пусть повторения цифр не запрещены. Сколько $N+24$–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 10-ричной записи N двоек, не имеющие пятерок и восьмерок и делящиеся на 3.

Задача 27. В анкете предлагается $N+15$ вопросов, на кото-

рые можно ответить "да", "нет", "затрудняюсь ответить". Сколькими способами можно ответить на вопросы анкеты?

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?

Задача 29. Сколько шестисимвольных слов можно сформировать из N+26 букв и цифр, если:

а) первые два символа есть буквы, а следующие четыре – цифры;

б) в слове может быть только две буквы, которые не должны стоять в слове рядом.

Задача 30. Найти число положительных натуральных чисел, не больших $1000+2 \cdot N+1$ и

1) не делящихся ни на одно из чисел 3,5,7,11,13;

2) делящихся в точности на два числа;

3) делящихся на не менее чем два числа.

N есть номер фамилии студента в аудиторном журнале. Использовать формулу включений и исключений.

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.

Задача 2. Для данных формул построить таблицу истинностных значений и определить, является ли формула
а) общезначимой, б) выполнимой,
в) опровержимой, г) невыполнимой.

2.1. $(x\to(y\to z))\to((x\to y)\to(x\to z))$,
$\neg((((x\to y)\to(\neg z\to u))\to w)\to w)\to(x\to(u\to x))$,
$(x\vee\neg x)\equiv\neg x$, $(x\cdot\neg x)\equiv x$.

2.2. $(x\to y)\to((x\to z)\to(x\to yz))$,
$\neg((x\to y)\to((x\to(y\to z))\to(x\to z)))$,
$(x\to y)\to((\neg(x\to z)\to(x\to yz))$.

2.3. $(x\to z)\to((y\to z)\to(x\equiv(y\to z)))$,
$\neg((xy\to z)\to(x\to(y\to z)))$,
$(x\to(y\to z))\to(\neg(x\to y)\to(x\to z))$.

2.4. $(x\equiv x)\vee x$, $(x\cdot x)\equiv x$, $(x\vee x)\equiv x$,
$\neg((x\to(y\to z))\to(x\cdot y\to z))$,
$(x\vee\neg y)\equiv\neg(x\vee y)$, $x\cdot y\equiv y\cdot x$.

2.5. $x\vee y\equiv y\vee x$, $x\cdot y\equiv y\cdot x$,
$\neg((\neg x\to\neg y)\to((\neg y\to x)\to y))$,
$(xy\to z)\to(x\to(\neg(y\to z)))$.

2.6. $(((x\to y)\to(\neg z\to u))\to w)\to((w\to x)\to(u\to x))$,
$\neg((x\vee y)\equiv(y\vee x))$, $\neg((x\cdot y)\equiv(y\cdot x))$,
$(\neg x\to\neg y)\to((\neg y\to x)\to\neg y)$.

2.7. $(x\to y)\to((x\to(y\to z)\to(x\to z))$,
$\neg((x\to z)\to((y\to z)\to(x\equiv(y\to z))))$,
$(x\to(y\to z))\to(\neg(xy\to z))$.

2.8. $(x\to y)\to((y\to z)\to(x\to z))$,
$\neg((x\to y)\to((x\to z)\to(x\to yz)))$,
$(((x\to y)\to(\neg z\to\neg u))\to\neg w)\to((w\to x)\to(z\to x))$.

2.9. $(\neg y\to x)\to((y\to x)\to x)$,
$\neg((x\to(y\to z))\to((x\to y)\to(x\to z)))$,
$x\vee yz\equiv(x\vee y)\cdot(\neg x\cdot\neg y)$.

2.10. $(xy\to z)\to(x\to(y\to z))$,
$\neg((x\vee x)\equiv x)$, $\neg((x\cdot x)\equiv x)$,
$x\cdot\neg(yz)\equiv(xy)z$.

2.11. $(x\to(y\to z))\to(xy\to z))$,
$\neg((\neg y\to x)\to((y\to x)\to x))$,
$(x\to y)\to((\neg y\to z)\to(\neg x\to z)$.

2.12. $(\neg x \to \neg y) \to ((\neg y \to x) \to y)$,
$\neg((x \to y) \to ((y \to z) \to (x \to z)))$,
$(x \vee z) \to (\neg(y \to z) \to ((x \vee y) \to z))$.

2.13. $(x \vee yz) \equiv (x \vee y)(x \vee z)$,
$\neg((x \to y) \equiv (\neg y \to \neg x))$,
$(x \to y) \to ((x \to (\neg y \to z)) \to (x \to z))$.

2.14. $(x \vee (y \vee z)) \equiv ((x \vee y) \vee z)$,
$\neg((x \to y) \equiv (\neg x \vee y))$,
$x(\neg y \vee z) \equiv (xy \vee xz)$.

2.15. $x \to (y \to x)$,
$\neg(\neg x \to (\neg y \to \neg(x \vee y))$,
$\neg(x \vee y) \equiv (x \cdot \neg y)$.

2.16. $xy \to x$,
$\neg(x(y \vee z) \equiv (xy \vee xz))$,
$(\neg y \to x) \to ((y \to x) \to \neg x)$.

2.17. $xy \to y$,
$\neg((\ x(yz) \equiv (xy)z))$.
$(x \to\ \ y) \equiv (y \to \neg x)$.

2.18. $x \to (x \vee y)$,
$\neg(x(x \vee y) \equiv x)$.
$\neg x \equiv \neg\neg\neg x$.

2.19. $y \to (x \vee y)$,
$\neg(y \to (x \vee y))$,
$(x \vee (y \vee \neg z)) \equiv ((x \vee y) \vee z)$.

2.20. $(x \to y) \equiv (\neg y \to \neg x)$,
$\neg(x \to (y \to x))$,
$x \to (\neg y \to (x \vee y))$.

2.21. $x \equiv \neg x$.
$\neg(\neg(x \vee y) \equiv \neg x \cdot \neg y)$,
$((x \vee \neg y) \equiv \neg(x \cdot y))$.

2.22. $(x \cdot \neg y) \equiv (\neg x \vee y)$,
$\neg((x \vee xy) \equiv x)$,
$xy \to \neg y$.

2.23. $x(yz) \equiv (xy)z$,
$\neg(\neg(x \vee y) \equiv (\neg x \cdot \neg y))$,
$x(x \vee \neg y) \equiv x$.

2.24. $(x \vee xy) \equiv x$,
$\neg(x \vee (y \vee z) \equiv (x \vee y) \vee z)$,
$xy \to x$.

2.25. $x(x \vee y) \equiv x$,
$\neg(x \equiv \neg\neg x)$,
$\neg x \vee xy \equiv x$.

2.26. $x(y \vee z) \equiv (xy \vee xz)$,
$\neg((x \cdot y) \to y)$,
$\neg x \to (y \to x)$.

2.27. $x \vee \neg x \cdot y$,
$\neg(x \to (x \vee y))$,
$(x \to \neg y) \equiv (\neg x \vee y)$.

2.28. $(x \vee y) \equiv (\neg x \cdot \neg y)$.
$\neg(x \vee \neg y)$,
$x \to (\neg x \vee y)$.

2.29. $(x \cdot y) \equiv (\neg x \vee \neg y)$,
$\neg(x \cdot y \to x)$,
$\neg x \vee \neg x$.

2.30. $\neg x \to (\neg y \to x \vee y)$,
$\neg((x \vee yz) \equiv (x \vee y)(x \vee z))$,
$y \to x \vee \neg y$.

Задача 3. Для данных формул построить таблицу истинностных значений, упростить формулы и построить для обеих схемы из фукнциональных элементов для дизъюнкции, конъюнкции, отрицания, импликации.

3.1. $x \to \neg(\neg(x \cdot \neg y) \vee (x \to y))$.

3.2. $\neg x \vee (\neg y \to x) \vee \neg(x \to y)$.

3.3. $\neg(x \to \neg(xy)) \vee \neg(y \to \neg x \cdot \neg y)$.

3.4. $\neg(xy) \to (y \to \neg(xy))$.

3.5. $(x \to y) \to \neg(\neg y \to \neg(\neg(xy) \vee x))$.

3.6. $\neg(x \to y) \to (\neg y \vee \neg(xy))$.

3.7. $\neg(\neg x \to x) \to \neg(\neg x \vee \neg(xy))$.

3.8. $\neg(\neg(x \vee xy) \to x) \to y$.

3.9. $\neg((xy \vee x \cdot \neg y) \to x) \to y$.

3.10. $\neg(\neg(x \vee y) \vee \neg(x \to y)) \to x$.

3.11. $\neg(xy \vee \neg x \cdot y) \vee \neg(\neg(x \vee xy) \vee \neg x) \vee x$.

3.12. $\neg(x \to y) \vee \neg(\neg x \to y) \vee \neg(x \to xy) \vee (y \to x)$.

3.13. $\neg(x \vee y) \to \neg(x \to y) \vee y$.

3.14. $(\neg(xy \vee y) \to \neg(xy \to x)) \to x$.

3.15. $\neg(\neg x \cdot y \vee x) \vee \neg(xy \to y)) \to (x \vee y)$.

3.16. $(\neg(x \to y) \vee x) \to ((x \vee y) \to y)$.

3.17. $(\neg(xy) \to y) \to ((xy \to \neg x \cdot y) \to x)$.

3.18. $\neg(x \vee y) \vee \neg(y \to ((xy \to (x \vee y)))$.
3.19. $\neg(xy \to y) \vee ((\neg(x \to y) \vee xy) \to x)$.
3.20. $\neg(xy \to y) \to \neg((x \to y) \to xy)$.
3.21. $\neg(x \vee y) \vee \neg(y \to ((xy \to \neg x \cdot y) \to y))$.
3.22. $(\neg(xy \vee y) \to x) \to \neg x$.
3.23. $((x \cdot \neg y \vee \neg(\neg x \vee y)) \to x) \to y$.
3.24. $(\neg y \vee x) \to (x \cdot \neg y \vee y)$.
3.25. $\neg(x \to \neg x \cdot y) \to \neg(y \to (x \to y))$.
3.26. $\neg(x \cdot \neg y) \vee \neg(xy) \to x$.
3.27. $\neg((\neg x \cdot \neg y \to x) \to (yx \vee x))$.
3.28. $\neg(\neg x \to y) \vee \neg(\neg x \cdot y \to x \cdot \neg y)$.
3.29. $(x \vee \neg(xy)) \to \neg(y \to xy)$.
3.30. $(\neg(xy) \vee x \cdot \neg y) \to \neg(x \vee y)$.

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.

4.1. {4,5,6,7}. **4.2.** {3,4,5,6}. **4.3.** {2,3,5,6}.
4.4. {1,3,5,6}. **4.5.** {0,1,2,3}. **4.6.** {0,1,2,7}.
4.7. {0,1,4,7}. **4.8.** {0,2,4,7}. **4.9.** {4,5,7}.
4.10. {4,6,7}. **4.11.** {2,3,7}. **4.12.** {0,1,4,5,6}.
4.13. {1,3,7}. **4.14.** {0,1,2,3,6}. **4.15.** {0,5,7}.
4.16. {2,6,7}. **4.17.** {0,5,6}. **4.18.** {0,1,2,3,5}.
4.19. {0,3,6}. **4.20.** {0,3,5}. **4.21.** {1,2,3,4,6}.
4.22. {1,2,3}. **4.23.** {1,4,6}. **4.24.** {0,2,4,5,6}.
4.25. {0,6,7}. **4.26.** {0,1,5,6,7}. **4.27.** {2,4,5,6}.
4.28. {3,4,5,7}. **4.29.** {1,4,6,7}. **4.30.** {4,5,7}.

Задача 5. Найти все тупиковые и все минимальные ДНФ и КНФ для всюду определенной функции. Одну из минимальных форм реализовать схемой с элементами для $\&, \vee, \neg$.

5.1. 1001001110011011. **5.2.** 0010100011011111.
5.3. 1101111100100010. **5.4.** 1001100110111001.
5.5. 1110110011001100. **5.6.** 1101110110001010.
5.7. 1010100011011101. **5.8.** 1110110011001100.
5.9. 1101001000111011. **5.10.** 1010000011011111.
5.11. 1010100001110111. **5.12.** 1010101001011101.
5.13. 0110111011000110. **5.14.** 1110010011101100.
5.15. 0111110100101010. **5.16.** 0010100011111101.
5.17. 1100011011101100. **5.18.** 1111001000111011.

5.19. 0011011111100111. **5.20.** 1010001101110011.
5.21. 1110011111100001. **5.22.** 0010001001010111.
5.23. 1101110110001010. **5.24.** 0111001001111010.
5.25. 1011011100001011. **5.26.** 1010001111011011.
5.27. 1101101011010010. **5.28.** 1010100001111111.
5.29. 0111110110001010. **5.30.** 0101100011110010.

Задача 6. Для заданной всюду определенной функции $f(x_1, x_2, x_3, x_4)$ построить минимальную ДНФ методом Квайна– Мак-Класски. Каждая функция задана множеством M_1 десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

6.1. {1,3,5,7,9,10,11,12,13}.
6.2. {2,3,6,7,9,10,11,12,14}.
6.3. {4,5,6,7,9,10,12,13,14}.
6.4. {1,2,5,6,7,9,10,11,13}.
6.5. {2,3,5,6,7,9,10,11,14}.
6.6. {1,3,5,6,7,9,11,12,13}.
6.7. {2,3,5,6,7,10,11,12,14}.
6.8. {3,4,5,6,7,10,12,13,14}.
6.9. {3,4,5,6,7,9,12,13,14}.
6.10. {1,3,5,6,7,9,10,11,13}.
6.11. {5,6,8,9,10,11,12,13,14}.
6.12. {3,6,8,9,10,11,12,13,14}.
6.13. {3,5,8,9,10,11,12,13,14}.
6.14. {1,3,5,7,9,10,11,12,13,14}.
6.15. {1,2,5,6,7,9,10,11,13,14}.
6.16. {1,3,5,6,7,9,11,12,13,14}.
6.17. {1,3,5,6,7,9,10,11,13,14}.
6.18. {0,1,3,5,7,9,10,11,12,13}.
6.19. {0,2,3,6,7,9,10,11,12,14}.
6.20. {0,4,5,6,7,9,10,12,13,14}.
6.21. {0,1,2,5,6,7,9,10,11,13}.
6.22. {0,2,3,5,6,7,9,10,11,14}.
6.23. {0,1,3,5,6,7,9,11,12,13}.
6.24. {0,2,3,5,6,7,10,11,12,14}.
6.25. {2,6,12,13,14,15}.
6.26. {0,1,4,5,8,9,11,12,13,14,15}.
6.27. {3,6,7,11,12,13,14,15}.
6.28. {2,3,7,10,11,12,13,14,15}.
6.29. {0,1,4,5,7,10,11,12,13,15}.

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 &, ∨, ¬.

7.1. 1---010010--1--1. **7.2.** 1---111100--0--0.
7.3. 1---011110--0--0. **7.4.** 1---101110--0--0.
7.5. 1---110110--0--0. **7.6.** 1---111100--0--0.
7.7. 0---111100--0--1. **7.8.** 0---11100--0--10.
7.9. 0---011111--0--0. **7.10.** 0-1-1-010-110---.
7.11. 1-1-0010-01--100. **7.12.** -1-1010101--0---.
7.13. --1-01-0001-1-1-. **7.14.** -1-1-10-00110---.
7.15. 0-11011--1--0--0. **7.16.** 1-010-0-01-1---1.
7.17. -1--00001-1--1-1. **7.18.** 1-1-10-01010----.
7.19. --1-1-01010-01--. **7.20.** ---1-1-010-010-1.
7.21. --1--1110-0-010-. **7.22.** 11-11--1-0-0-0-0.
7.23. 0-01010--1--1--1. **7.24.** -10-010-0--1--1-.
7.25. 1-1-0-01--0-1--1. **7.26.** -1---1010-0-01-1.
7.27. 1-1-----0-010101. **7.28.** 010-1-01--01--1-.
7.29. 1--0--101--010-1. **7.30.** -01-10-10-0-1--1.

Задача 8. Минимизировать всюду определенную функцию алгебры логики из задачи 4 и частично определенную функцию из задачи 6 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. Совместную минимизацию функций проводить с помощью карт Карно.

Каждая функция задана множеством M_1 десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

9.1. {2,3,4,5,7}; {0,4,5}; {3,4,5,7}.
9.2. {1,3,4,6,7}; {0,4,6}; {3,4,5,7}.
9.3. {2,3,4,5,7}; {0,2,6}; {2,3,5,7}.
9.4. {1,3,4,6,7}; {0,1,3}; {1,3,6,7}.
9.5. {1,2,5,6,7}; {0,1,5}; {1,5,6,7}.
9.6. {1,2,5,6,7}; {0,2,5}; {2,5,6,7}.
9.7. {1,3,5,7}; {1,2,3}; {4,5,7}.
9.8. {2,3,6,7}; {1,2,3}; {4,6,7}.
9.9. {1,3,5,7}; {1,4,5}; {2,3,7}.

9.10. {2,3,6,7}; {2,4,6}; {1,3,7}.
9.11. {4,5,6,7}; {2,4,6}; {1,5,7}.
9.12. {4,5,6,7}; {1,4,5}; {1,6,7}.
9.13. {3,4,5,7}; {4,5,6}; {1,2,3}.
9.14. {3,4,6,7}; {4,5,6}; {1,2,3}.
9.15. {2,3,5,7}; {2,3,6}; {1,4,5}.
9.16. {1,3,6,7}; {1,3,5}; {2,4,6}.
9.17. {1,5,6,7}; {1,3,5}; {2,4,6}.
9.18. {2,5,6,7}; {2,3,6}; {1,4,5}.
9.19. {0,2,4}; {0,2,3}; {1,2,3}.
9.20. {0,1,4}; {0,1,3}; {1,2,3}.
9.21. {0,2,4}; {0,4,5}; {1,4,5}.
9.22. {0,1,4}; {0,4,6}; {2,4,6}.
9.23. {0,1,2}; {0,2,6}; {2,4,6}.
9.24. {0,1,2}; {0,1,5}; {1,4,5}.
9.25. {0,2,6,7}; {0,1,6}; {0,2,7}.
9.26. {0,2,6,7}; {2.5.7}; {1,3,7}.
9.27. {0,1,4,6,7}; {3,4,5,6,7}; {4,5,7}.
9.28. {0,1,2,3,5,7}; {4,5,7}; {0,1,3}.
9.39. {0,1,2}; {0,1,4,7}; {6,7}.
9.30. {4,5,7}; {0,3,4,5,7}; {2,3,6}.

Задача 10. Провести приближенную совместную минимизацию четырех функций алгебры логики. В качестве заданий взять из задачи 4 три последние функции и функцию своего варианта. 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 четырех функций реализовать на ПЛМ. Сравнить две реализации и указать, какая из них экономнее.

Задача 11. Заданную систему булевых функций исследовать на полноту с помощью теоремы Поста.

11.1. $(x\equiv y)+yz,\ x\cdot\neg y.$ **11.2.** $(x\to y)+(x\vee z),\ 0,1.$
11.3. $x\equiv(y+z),\ \neg(x\to y)\equiv z.$ **11.4.** $(x+yz)\cdot\neg x\to z,\ xy.$
11.5. $(x\equiv\neg y)\to(\neg x\equiv z),\ x\vee\neg y.$ **11.6.** $(x\equiv\neg y)+xz,\ xy.$
11.7. $x+\neg(y\equiv z),\ \neg x\equiv y.$ **11.8.** $\neg x\equiv(y+z),\ xy.$
11.9. $(x\to z)\,|\,y,\ \neg x\vee yz.$ **11.10.** $(x\equiv y)\to(x\not\equiv z),\ 0.$
11.11. $(x\equiv y)\to\neg z,\ x\vee\neg y.$ **11.12.** $(x\,|\,z)+y,\ x\equiv y\cdot\neg z.$
11.13. $(x\to y)+(y\to z),\ \neg x\cdot y.$ **11.14.** $(x\to y)\,|\,(y\to z),\ x+y.$

11.15. $(x+y)+(y\equiv\neg z)$, $\neg x\to y$. **11.16.** $x\equiv(y+\neg z)$, x.
11.17. $\neg x\to y$, 00, 11. **11.18.** $(x\to y)+\neg z$, $x\vee\neg y$.
11.19. $(x\to y)\vee\neg z$, $x\cdot\neg y$. **11.20.** $(\neg x\equiv\neg y)\,|\,z$, $\neg x\equiv y$.
11.21. $(x\vee\neg y)\equiv z$, $(x\to y)\to y$. **11.22.** $x\,|\,z\to y$, $x\equiv y$, 00.
11.23. $(x\,|\,y)\equiv(y\,|\,z)$, 00, 11. **11.24.** $(x\to\neg(yz)\vee z$, $\neg x\to\neg y$.
11.25. $(x\equiv\neg y)\to z$, $x\cdot\neg y$. **11.26.** $(\neg x\vee\neg yz)+z$, $x\to y$.
11.27. $(x+y\cdot\neg z)\to z$, $\neg x\cdot y$. **11.28.** $x\vee\neg y\cdot z$, $\neg x\to y$.
11.29. $(x\to yz)\vee\neg z$, $\neg x\vee yz$. **11.30.** $(x\vee\neg y)\equiv z$, $\neg x\to y$.

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. **11.4.**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.
12.19. 01101101, 1001, 00. **12.20.** 00110011, 0101, 0011.
12.21. 1011001, 1000, 00. **12.22.** 10110001, 1001, 01.
12.23. 11000111, 00011111, 00. **12.24.** 10100011, 0110.
12.25. 10100011, 1001, 00. **12.26.** 01001101, 1001, 00.
12.27. 00110111, 1111, 00. **12.28.** 00101001, 1101, 01.
12.29. 01001011, 0001, 11. **12.30.** 00001010, 1010, 11.

Задача 13. Реализовать функции из задач 4 и 5 с помощью мультиплексора (в базисе &, $\vee$, $\neg$, MUX(2)).

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 15. Для булевой функции из задачи 5 построить минимальные проверяющие и полные тесты относительно указанных классов ошибок (s_{ij} – слипание каналов i и j; 0_i – обрыв канала i, 1_i – замыкание канала i).

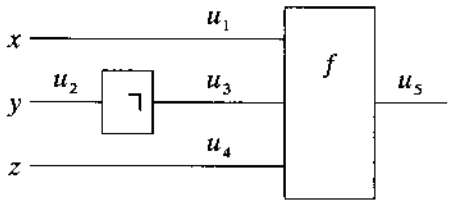
15.1. $\{0_1, s_{24}\}$. **15.2.** $\{0_3, s_{14}\}$.
15.3. $\{1_2, s_{34}\}$. **15.4.** $\{s_{13}, s_{24}\}$.
15.5. $\{0_2, 1_3, s_{14}\}$. **15.6.** $\{0_3, 1_1, s_{24}\}$.
15.7. $\{0_3, s_{14}\}$. **15.8.** $\{1_3, s_{12}\}$.
15.9. $\{s_{13}, s_{24}\}$. **15.10.** $\{0_1, 1_2, s_{34}\}$.
15.11. $\{0_1, 1_3, s_{24}\}$. **15.12.** $\{1_3, s_{14}\}$.
15.13. $\{0_2, s_{14}\}$. **15.14.** $\{s_{23}, s_{24}\}$.
15.15. $\{0_3, 1_2, s_{13}\}$. **15.16.** $\{0_2, 1_1, s_{24}\}$.
15.17. $\{0_4, s_{14}\}$. **15.18.** $\{0_3, s_{12}\}$.
15.19. $\{0_3, s_{13}, s_{24}\}$. **15.20.** $\{0_1, 1_2, s_{14}\}$.
15.21. $\{0_3, 1_1, s_{24}\}$. **15.22.** $\{1_1, s_{14}\}$.

15.23. $\{1_2,\ s_{14}\}$. **15.24.** $\{0_1,\ s_{23},\ s_{24}\}$.
15.25. $\{0_2,\ 1_3,\ s_{13}\}$. **15.26.** $\{0_4,\ 1_1,\ s_{23}\}$.
15.27. $\{0_1,\ 1_3,\ s_{14}\}$. **15.28.** $\{0_3,\ 1_2,\ s_{12}\}$.
15.29. $\{1_4, s_{13},\ s_{24}\}$. **15.30.** $\{0_3,\ s_{24}\}$.

Задача 16. Для данной схемы из функциональных элементов (СФЭ) найти:

а) минимальный проверяющий тест,

б) минимальный диагностический (полный) тест.



Обозначения: для возможных однократныч неисправностей u_i, i=1,2,3,4,5, приняты следующие обозначения:

0_i, вместо u_i реализуется 0 (обрыв),

1_i, вместо u_i реализуется 1 (замыкание),

$\neg_i$, отрицание u_i (вместо u_i реализуется $\neg u_i$),

$|$, штрих Шеффера.

Для данных трех неисправностей остальных двух нет.

16.1. $f = x\&(y\to z)$, 0_1, 0_2, $\neg_3$.
16.2. $f = (x\&y)\to z$, 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. $f = (x+y)\to z$, 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. $f = (x\to y)\&z$, 1_1, 1_3, $\neg_5$.
16.10. $f = (x\to y)\,|\,z$, 0_1, 0_3, 1_4.
16.11. $f = (x\to y)+z$, 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. $f = x\&(y\to z)$, 1_1, $\neg_3$, 0_4.
16.16. $f = (x\&y)\to z$, 1_1, 0_3, 1_4.

16.17. $f = (x\&y)\,|\,z, \quad 1_1, \quad 1_3, \quad 0_4.$
16.18. $f = (x\&y)+z, \quad 1_1, \quad 1_3, \quad 1_4.$
16.19. $f = x\&y\&z, \quad 0_1, \quad 0_2, \quad \neg_5.$
16.20. $f = (x+y)\to z, \quad 0_1, \quad 1_3, \quad \neg_4.$
16.21. $f = (x+y)\,|\,z, \quad 0_1, \quad 0_2, \quad 0_4.$
16.22. $f = (x+y)\&z, \quad 0_1, \quad 0_2, \quad 1_4.$
16.23. $f = (x\to y)\&z, \quad 0_1, \quad 1_2, \quad 1_4.$
16.24. $f = (x\to y)\,|\,z, \quad 1_1, \quad 0_3, \quad 0_4.$
16.25. $f = x\vee(y\&z), \quad 1_1, \quad 0_2, \quad \neg_4.$
16.26. $f = x\vee(y\,|\,z), \quad 1_1, \quad \neg_3, \quad 0_4.$
16.27. $f = x\vee(y\to z), \quad 0_1, \quad \neg_2, \quad 1_5.$
16.28. $f = x\vee(y+z), \quad 0_1, \quad \neg_3, \quad 1_4.$
16.29. $f = x\&(y\vee z), \quad 1_1, \quad \neg_4, \quad 0_5.$
16.30. $f = x+(y\vee z), \quad 1_1, \quad 1_3, \quad \neg_5.$

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) опровержимой; 3) общезначимой; 4) невыполнимой? Вычислить значение истинности формулы A на множестве M со следующими предикатами, определеными 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. $(\forall x)(P(x)\ \&\ R(x) \to (\exists y)Q(x,y))$.
17.2. $(\forall x)(P(x) \to (R(x) \to (\exists y)Q(x,y)))$.
17.3. $(\forall x)(P(x)\ \&\ \neg R(x) \to (\exists y)Q(x,y))$.
17.4. $(\forall x)(\neg P(x) \to (\neg R(x) \to (\exists y)\neg Q(x,y)))$.
17.5. $(\forall x)(\neg P(x) \vee \neg R(x) \to (\exists y)Q(x,y))$.
17.6. $(\exists x)(P(x)\ \&\ R(x) \to (\forall y)Q(x,y))$.
17.7. $(\exists x)(P(x) \to (R(x) \to (\forall y)Q(x,y)))$.
17.8. $(\exists x)(P(x) \vee \neg(R(x) \to (\forall y)Q(x,y))$.
17.9. $(\exists x)(\neg P(x) \to (\neg R(x) \to (\forall y)Q(x,y)))$.
17.10. $(\exists x)(\neg P(x) \vee \neg R(x) \to (\exists y)\neg Q(x,y))$.
17.11. $(\forall y)(P(y)\ \&\ R(y) \to (\exists x)Q(x,y))$.
17.12. $(\forall y)(P(y) \to (R(y) \to (\exists x)Q(x,y)))$.
17.13. $(\forall y)(P(y) \vee \neg R(y) \to (\exists x)Q(x,y))$.
17.14. $(\forall y)(\neg P(y) \to (\neg R(y) \to (\exists x)Q(x,y)))$.
17.15. $(\forall y)(P(x) \to (\neg P(x) \to (\exists x)Q(x,y)))$.
17.16. $(\forall x)(P(x)\ \&\ R(x) \to (\forall y)Q(x,y))$.
17.17. $(\forall x)(P(x) \to (R(x) \to (\forall y)Q(x,y)))$.

17.18. $(\forall x)(P(x) \vee \neg P(x) \to (\forall y)Q(x,y))$.
17.19. $(\forall x)((P(x) \to R(x)) \to (\forall y)Q(x,y))$.
17.20. $(\forall x)(\neg P(x) \vee \neg R(x) \to (\forall y)Q(x,y))$.
17.21. $(\forall x)(Q(x,y) \,\&\, R(x) \to (\forall y)P(y))$.
17.22. $(\exists y)((\exists x)(Q(x,y) \to P(x)) \vee Q(x,y))$.
17.23. $(\exists y)((\forall x)(Q(x,y) \to \neg P(x)) \vee \neg Q(x,y))$.
17.24. $(\forall y)((\exists x)Q(x,y) \to (P(x) \to Q(x,y)))$.
17.25. $(\forall x)((\exists y)Q(x,y) \to (R(x) \to P(x)))$.
17.26. $(\forall x)(P(x) \to (\exists y)(Q(x,y) \to R(x)))$.
17.27. $(\exists x)(P(x) \to (\exists y)(Q(x,y) \to \neg R(x)))$.
17.28. $(\exists y)(P(y) \to (\forall x)(Q(x,y) \to R(y)))$.
17.29. $(\forall y)(P(y) \to (\forall x)(Q(y,x) \to \neg R(x)))$.
17.30. $(\forall y)(P(y) \to (\forall x)(Q(x,y) \vee \neg R(x)))$.

Задача. Проверить, является ли логическими законами следующие логические формулы (Новикова помечены буквой N, Клини – буквой K).

1. $p \to (q \to p)$, NK.
2. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$, N.
2a. $(p \to q) \to ((p \to (q \to r)) \to (p \to r))$, K.
3. $p \,\&\, q \to p$, NK.
4. $p \,\&\, q \to q$, NK.
5. $(p \to q) \to ((p \to r) \to (p \to q \,\&\, r))$, NK.
6. $p \to p \vee q$, NK.
7. $q \to p \vee q$, NK.
8. $(p \to r) \to ((q \to r) \to (p \vee q \to r))$, NK.
9. $(p \to q) \to (\neg q \to \neg p)$, N.
9a. $(p \to q) \to ((p \to \neg q) \to \neg p))$, K.
10. $p \to \neg\neg p$, N.
11. $\neg\neg p \to p$, NK.
11a. $\neg p \to (p \to q))$, K.
12. $((p \to q) \to (p \to r)) \to (p \to (q \to r))$.
13. $\neg(p \vee q) \equiv \neg p \,\&\, \neg q$.
14. $\neg(p \,\&\, q) \equiv \neg p \vee \neg q$.
15. $(p \to (q \to r)) \equiv (q \to (p \to r))$.
16. $(p\&q \to r) \equiv (p \to (q \to r))$.
17. $p \vee q \equiv \neg(\neg p \,\&\, \neg q)$.
18. $p \,\&\, q \equiv \neg(\neg p \vee \neg q)$.
19. $(p \to q) \equiv \neg p \vee q$.

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 континуум суперинтуиционистских (или суперконструктивистских) исчислений.

Задача. Доказать или опровергнуть справедливость следующих правил вывода, установив общезначимость соответствующих формул.

1. $\dfrac{A \to B,\ A}{B}$. 2. $\dfrac{A \to B,\ \neg B}{\neg A}$. 3. $\dfrac{A \to B,\ \neg A}{\neg B}$.

4. $\dfrac{A \vee B,\ \neg A}{B}$. 5. $\dfrac{A \vee B,\ \neg B}{A}$. 6. $\dfrac{A \vee B,\ A}{\neg B}$.

7. $\dfrac{A \to (B \to C)}{A \,\&\, B \to C}$. 8. $\dfrac{\neg A \to (B \to C)}{A \,\&\, B \to \neg C}$.

9. $\dfrac{A \,\&\, B \to C}{A \to (B \to C)}$, 10. $\dfrac{A \vee \neg B \to C}{A \to B \,\&\, C}$.

11. $\dfrac{C \to A,\ C \to B}{C \to A \,\&\, B}$. 12. $\dfrac{C \to \neg A,\ C \to B}{C \to A \vee B}$.

13. $\dfrac{A \to C,\ B \to C}{A \vee B \to C}$. 14. $\dfrac{A \vee C,\ B \to \neg C}{A \vee B \to C}$.

15. $\dfrac{A \to C,\ B \to C,\ A \vee B}{C}$. 16. $\dfrac{A \to C,\ B \to D,\ A \vee B}{C \vee D}$.

17. $\dfrac{C \to A,\ D \to B,\ \neg A \vee \neg B}{\neg C}$. 18. $\dfrac{C \to A,\ D \to B,\ \neg A \vee \neg B}{\neg C \vee \neg D}$.

Естественный вывод Гентцена (Исчисление секвенций)

Схемы аксиом.

Если A – формула СИВ, то секвенция вида $\Gamma, A \vDash \Delta; A$ есть единственная схема аксиом в СИВ.

Замечание. Так как $A \vDash A \longleftrightarrow \vdash A \to A \longleftrightarrow \vdash A \vee \neg A$ (последняя формула есть закон исключенного третьего), то в качестве схемы аксиом в СИВ, в сущности, берем закон исключен-

ного третьего.

Пропозициональные правила (секвенциального) вывода

Введение отрицания.

$$\frac{\Gamma \Rightarrow \Delta;A}{\Gamma,\neg A \Rightarrow \Delta}\ (\neg \Rightarrow); \qquad \frac{\Gamma,A \Rightarrow \Delta}{\Gamma \Rightarrow \Delta;\neg A}\ (\Rightarrow \neg).$$

Введение конъюнкции.

$$\frac{\Gamma,A,B \Rightarrow \Delta}{\Gamma,A\&B \Rightarrow \Delta}\ (\& \Rightarrow); \qquad \frac{\Gamma \Rightarrow \Delta;A \quad \Gamma \Rightarrow \Delta;B}{\Gamma \Rightarrow \Delta;A\&B}\ (\Rightarrow \&).$$

Введение дизъюнкции.

$$\frac{\Gamma,A \Rightarrow \Delta \quad \Gamma,B \Rightarrow \Delta}{\Gamma,A\vee B \Rightarrow \Delta}\ (\vee \Rightarrow); \qquad \frac{\Gamma \Rightarrow \Delta;A;B}{\Gamma \Rightarrow \Delta;A\vee B}\ (\Rightarrow \vee).$$

Введение импликации.

$$\frac{\Gamma,B \Rightarrow \Delta \quad \Gamma \Rightarrow \Delta;A}{\Gamma,A\to B \Rightarrow \Delta}\ (\to \Rightarrow); \qquad \frac{\Gamma,A \Rightarrow \Delta;B}{\Gamma \Rightarrow \Delta;A\to B}\ (\Rightarrow \to).$$

Предикатные правила (секвенциального) вывода

$$\frac{\Gamma \Rightarrow \Delta;A(y)}{\Gamma \Rightarrow \Delta;(\forall x)A(x)}\ (\Rightarrow \forall); \qquad \frac{\Gamma,A(y) \Rightarrow \Delta}{\Gamma,(\exists x)A(x) \Rightarrow \Delta}\ (\exists \Rightarrow);$$

переменная y не входит в нижнюю секвенцию свободно;

$$\frac{\Gamma,A(t),(\forall x)A(x) \Rightarrow \Delta}{\Gamma,(\forall x)A(x) \Rightarrow \Delta}\ (\forall \Rightarrow); \qquad \frac{\Gamma \Rightarrow \Delta;A(t);(\exists x)A(x)}{\Gamma \Rightarrow \Delta;(\exists x)A(x)}\ (\Rightarrow \exists);$$

переменная x не входит в верхнюю секвенцию свободно.

Задача. Доказать справедливость правил секвенциального вывода, установив общезначимость соответствующей формулы.

Задача 18. Проверить правильность или неправильность правил вывода, установив общезначимость соответствующей формулы.

18.1. $\dfrac{P \to \neg M \quad S \;\&\; M}{S \;\&\; \neg P}$ **18.2.** $\dfrac{P \to \neg M \quad M \to S \quad M}{S \;\&\; \neg P}$ **18.3.** $\dfrac{M \to P \quad S \;\&\; M}{S \;\&\; P}$ **18.4.** $\dfrac{P \to M \quad M \to S \quad P}{S \;\&\; P}$

18.5. $\dfrac{P \to \neg M \quad M \;\&\; S}{S \;\&\; \neg P}$ **18.6.** $\dfrac{P \to M \quad M \to \neg S}{S \to \neg P}$ **18.7.** $\dfrac{P \;\&\; M \quad M \to S}{S \;\&\; P}$ **18.8.** $\dfrac{P \to M \quad M \to \neg S \quad P}{\neg S \;\&\; P}$

18.9. $\dfrac{M \to \neg P \quad M \to S \quad M}{S \;\&\; \neg P}$ **18.10.** $\dfrac{M \to P \quad M \to S \quad M}{P \;\&\; S}$ **18.11.** $\dfrac{M \to \neg P \quad M \;\&\; S}{S \;\&\; \neg P}$ **18.12.** $\dfrac{M \to P \quad M \;\&\; S}{S \to P}$

18.13. $\dfrac{M \;\&\; P \quad M \to S}{S \;\&\; P}$ **18.14.** $\dfrac{M \;\&\; \neg P \quad M \to S}{S \to \neg P}$ **18.15.** $\dfrac{P \to \neg M \quad S \to M \quad S}{S \;\&\; \neg P}$ **18.16.** $\dfrac{P \to M \quad S \to \neg M \quad S}{S \;\&\; \neg P}$

18.17. $\dfrac{P \to \neg M \quad S \;\&\; M}{S \;\&\; \neg P}$ **18.18.** $\dfrac{P \to M \quad S \to \neg M}{S \to \neg P}$ **18.19.** $\dfrac{P \to \neg M \quad S \to M}{S \to \neg P}$ **18.20.** $\dfrac{P \to M \quad S \;\&\; \neg M}{S \;\&\; \neg P}$

18.21. $\dfrac{M \to \neg P \quad S \to M \quad S}{S \;\&\; \neg P}$ **18.22.** $\dfrac{M \to P \quad S \to M \quad S}{S \;\&\; P}$ **18.23.** $\dfrac{M \to P \quad S \;\&\; M}{S \;\&\; P}$ **18.24.** $\dfrac{M \to \neg P \quad S \to M}{S \to \neg P}$

18.25. $\dfrac{M \to P \quad S \to M}{S \to P}$ **18.26.** $\dfrac{\neg M \to \neg P \quad M \to \neg S}{S \to \neg P}$ **18.27.** $\dfrac{P \to \neg M \quad S \to M \quad S}{S \;\&\; \neg P}$ **18.28.** $\dfrac{\neg P \to \neg M \quad S \to M \quad S}{S \;\&\; P}$

18.29. $\dfrac{M \to \neg P \quad \neg M \to \neg S}{S \to \neg P}$ **18.30.** $\dfrac{\neg M \to \neg P \quad S \;\&\; \neg M}{S \;\&\; \neg P}$

Задача 19. Проверить правильность или неправильность правил вывода, установив общезначимость соответствующей формулы.

19.1. $\dfrac{P \to \neg M \quad \neg S \,\&\, M}{\neg S \,\&\, \neg P}$ **19.2.** $\dfrac{P \to \neg M \quad \neg M \to S \quad M}{\neg S \,\&\, \neg P}$ **19.3.** $\dfrac{M \to \neg P \quad \neg S \,\&\, M}{\neg S \,\&\, P}$ **19.4.** $\dfrac{P \to M \quad \neg M \to S \quad \neg P}{\neg S \,\&\, P}$

19.5. $\dfrac{\neg P \to \neg M \quad \neg M \,\&\, S}{\neg S \,\&\, \neg P}$ **19.6.** $\dfrac{\neg P \to M \quad M \to \neg S}{\neg S \to \neg P}$ **19.7.** $\dfrac{\neg P \,\&\, M \quad \neg M \to S}{S \,\&\, \neg P}$ **19.8.** $\dfrac{\neg P \to M \quad \neg M \to \neg S \quad \neg P}{S \,\&\, P}$

19.9. $\dfrac{M \to \neg P \quad M \to S \quad M}{\neg S \,\&\, \neg P}$ **19.10.** $\dfrac{\neg M \to P \quad M \to \neg S \quad \neg P}{\neg P \,\&\, S}$ **19.11.** $\dfrac{M \to \neg P \quad \neg M \,\&\, S}{\neg S \,\&\, \neg P}$ **19.12.** $\dfrac{M \to \neg P \quad \neg M \,\&\, S}{\neg S \to P}$

19.13. $\dfrac{M \,\&\, P \quad \neg M \to S}{S \,\&\, P}$ **19.14.** $\dfrac{\neg M \,\&\, \neg P \quad \neg M \to S}{S \to \neg P}$ **19.15.** $\dfrac{P \to \neg M \quad \neg S \to M \quad \neg S}{S \,\&\, \neg P}$ **19.16.** $\dfrac{\neg P \to M \quad \neg S \to \neg M \quad S}{S \,\&\, \neg P}$

19.17. $\dfrac{P \to \neg M \quad \neg S \to M}{\neg S \,\&\, \neg P}$ **19.18.** $\dfrac{\neg P \to M \quad S \to \neg M}{\neg S \to \neg P}$ **19.19.** $\dfrac{P \to \neg M \quad \neg S \to M}{\neg S \to \neg P}$ **19.20.** $\dfrac{\neg P \to M \quad S \,\&\, \neg M}{\neg S \,\&\, \neg P}$

19.21. $\dfrac{\neg M \to \neg P \quad \neg S \to M \quad S}{\neg S \,\&\, \neg P}$ **19.22.** $\dfrac{\neg M \to P \quad S \to \neg M \quad \neg S}{\neg S \,\&\, \neg P}$ **19.23.** $\dfrac{\neg M \to \neg P \quad S \,\&\, M}{S \,\&\, \neg P}$ **19.24.** $\dfrac{\neg M \to \neg P \quad \neg S \to M}{\neg S \to \neg P}$

19.25. $\dfrac{\neg M \to P \quad S \to \neg M}{\neg S \to \neg P}$ **19.26.** $\dfrac{\neg M \to \neg P \quad M \to \neg S}{\neg S \to \neg P}$ **19.27.** $\dfrac{P \to \neg M \quad S \to M \quad \neg S}{S \,\&\, \neg P}$ **19.28.** $\dfrac{\neg P \to \neg M \quad S \to \neg M \quad S}{S \,\&\, P}$

19.29. $\dfrac{\neg M \to \neg P \quad \neg M \to \neg S}{S \to \neg P}$ **19.30.** $\dfrac{\neg M \to \neg P \quad \neg S \,\&\, \neg M}{S \,\&\, \neg P}$

Задача 20. Установить правильность или неправильность правил вывода, используя естественный вывод Генцена. Задание взять из задачи 18.

Задача 21. Установить правильность или неправильность правил вывода, используя естественный вывод Генцена. Задание взять из задачи 19.

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. $p \vee q \vee r$, $p \vee q \vee \neg r$, $\neg q \vee \neg r$, 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.

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. $\neg p \vee \neg q \vee r$, $\neg p \vee q \vee r$, $p \vee q \vee \neg r$.
25.30. $\neg p \vee \neg q \vee r$, $\neg p \vee q \vee r$, $p \vee q \vee r$.

Задача 26. Показать справедливость правил вывода, установив общезначимость соответствующей формулы.

26.1. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow \neg M(x)) \\ (\exists x)(S(x) \ \& \ M(x))\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.2. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow \neg M(x)) \\ (\forall x)(M(x) \rightarrow S(x)) \\ (\exists x)M(x)\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.3. $\dfrac{\begin{array}{l}(\forall x)(M(x) \rightarrow P(x)) \\ (\exists x)(S(x) \ \& \ M(x))\end{array}}{(\exists x)(S(x) \ \& \ P(x))}$

26.4. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow M(x)) \\ (\forall x)(M(x) \rightarrow S(x)) \\ (\exists x)P(x)\end{array}}{(\exists x)(S(x) \ \& \ P(x))}$

26.5. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow \neg M(x)) \\ (\exists x)(M(x) \ \& \ S(x))\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.6. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow M(x)) \\ (\forall x)(M(x) \rightarrow \neg S(x))\end{array}}{(\exists x)(S(x) \rightarrow \neg P(x))}$

26.7. $\dfrac{\begin{array}{l}(\exists x)(P(x) \ \& \ M(x)) \\ (\forall x)(M(x) \rightarrow S(x))\end{array}}{(\exists x)(S(x) \ \& \ P(x))}$

26.8. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow M(x)) \\ (\forall x)(M(x) \rightarrow \neg S(x)) \\ (\exists x)S(x)\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.9. $\dfrac{\begin{array}{l}(\exists x)(M(x) \rightarrow \neg P(x)) \\ (\forall x)(M(x) \rightarrow S(x)) \\ (\exists x)M(x)\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.10. $\dfrac{\begin{array}{l}(\forall x)(M(x) \rightarrow P(x)) \\ (\forall x)(M(x) \rightarrow S(x)) \\ (\exists x)P(x)\end{array}}{(\exists x)(P(x) \ \& \ S(x))}$

26.11. $\dfrac{\begin{array}{l}(\forall x)(M(x) \rightarrow \neg P(x)) \\ (\exists x)(M(x) \ \& \ S(x))\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.12. $\dfrac{\begin{array}{l}(\forall x)(M(x) \rightarrow P(x)) \\ (\exists x)(M(x) \ \& \ S(x))\end{array}}{(\exists x)(S(x) \rightarrow P(x))}$

26.13. $\dfrac{\begin{array}{l}(\exists x)(M(x) \ \& \ P(x)) \\ (\forall x)(M(x) \rightarrow S(x))\end{array}}{(\exists x)(S(x) \ \& \ P(x))}$

26.14. $\dfrac{\begin{array}{l}(\exists x)(M(x) \ \& \ \neg P(x)) \\ (\forall x)(M(x) \rightarrow S(x))\end{array}}{(\exists x)(S(x) \rightarrow \neg P(x))}$

26.15. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow \neg M(x)) \\ (\forall x)(S(x) \ \& \ M(x)) \\ (\exists x)S(x)\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.16. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow M(x)) \\ (\forall x)(S(x) \rightarrow \neg M(x)) \\ (\exists x)S(x)\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.17. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow \neg M(x)) \\ (\exists x)(S(x) \ \& \ M(x))\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.18. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow M(x)) \\ (\forall x)(S(x) \rightarrow \neg M(x))\end{array}}{(\forall x)(S(x) \rightarrow \neg P(x))}$

26.19. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow \neg M(x)) \\ (\forall x)(S(x) \rightarrow M(x))\end{array}}{(\forall x)(S(x) \rightarrow \neg P(x))}$

26.20. $\dfrac{\begin{array}{l}(\forall x)(P(x) \rightarrow M(x)) \\ (\exists x)(S(x) \ \& \ \neg M(x))\end{array}}{(\exists x)(S(x) \ \& \ \neg P(x))}$

26.21. $\dfrac{(\forall x)(M(x) \to \neg P(x)),\ (\forall x)(S(x) \to M(x)),\ (\exists x)S(x)}{(\exists x)(S(x)\ \&\ \neg P(x))}$

26.22. $\dfrac{(\forall x)(M(x) \to P(x)),\ (\forall x)(S(x) \to M(x)),\ (\exists x)S(x)}{(\exists x)(S(x)\ \&\ P(x))}$

26.23. $\dfrac{(\forall x)(M(x) \to P(x)),\ (\exists x)(S(x)\ \&\ M(x))}{(\exists x)(S(x)\ \&\ P(x))}$

26.24. $\dfrac{(\forall x)(M(x) \to \neg P(x)),\ (\forall x)(S(x) \to M(x))}{(\forall x)(S(x) \to \neg P(x))}$

26.25. $\dfrac{(\forall x)(M(x) \to P(x)),\ (\forall x)(S(x) \to M(x))}{(\forall x)(S(x) \to P(x))}$

26.26. $\dfrac{(\forall x)(\neg M(x) \to \neg P(x)),\ (\forall x)(M(x) \to \neg S(x))}{(\forall x)(S(x) \to \neg P(x))}$

26.27. $\dfrac{(\forall x)(P(x) \to \neg M(x)),\ (\forall x)(S(x) \to M(x)),\ (\exists x)S(x)}{(\exists x)(S(x)\ \&\ \neg P(x))}$

26.28. $\dfrac{(\forall x)(\neg P(x) \to \neg M(x)),\ (\forall x)(S(x) \to M(x)),\ (\exists x)S(x)}{(\exists x)(S(x)\ \&\ P(x))}$

26.29. $\dfrac{(\forall x)(M(x) \to \neg P(x)),\ (\forall x)(\neg M(x) \to \neg S(x))}{(\forall x)(S(x) \to \neg P(x))}$

26.30. $\dfrac{(\forall x)(\neg M(x) \to \neg P(x)),\ (\exists x)(S(x)\ \&\ \neg M(x))}{(\exists x)(S(x)\ \&\ \neg P(x))}$

Задача 27. Доказать справедливость правил вывода, используя естественный вывод Генцена. Задание взять из задачи 26.

Задача 28. Доказать справедливость правил вывода путем построения обрезанного семантического дерева (указав сначала префиксную и скулемову формы соответствующей формулы, эрбрановский универсум и эрбрановский 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, эрбрановский универсум и эрбрановский базис). Задание взять из задачи 26.

Задача 30. Задание взять из задачи 26. Доказать справедливость правил вывода методом резолюций, для чего выполнить следующее.

а. Построить формулу A, для которой правило вывода верно $\leftrightarrow$ формула A общезначима $\leftrightarrow$ формула $\neg A$ невыполнима.

б. Найти префиксную нормальную форму для формулы A.

в. Найти префиксную нормальную форму для формулы $\neg A$.

г. Найти стандартную форму Скулема для формулы $\neg A$.

д. Указать множество дизъюнктов S для формулы $\neg A$.

е. Написать эрбрановский универсум H для S.

ж. Написать эрбрановский базис B для S.

з. Указать множество основных примеров дизъюнктов из S.

и. 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.

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 (соседста 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 .

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_{ij} 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 (проходимые в обоих направлениях) указаны в фигурных скобках. Ориентированные ребра указаны в круглых скобках. Третья координата ребра есть его вес.

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.

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). По теореме Кирхгофа найти число каркасов данного графа.

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).

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 (v_i,v_j) 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.

Задача 7. В данном двудольном графе
$G=(V_1,V_2,E)$, $V_1=\{x_1,x_2,x_3,x_4,x_5\}$, $V_2=\{y_1,y_2,y_3,y_4,y_5,y_6\}$,

найти совершенное паросочетание. Если его нет, то указать получившееся максимальное паросочетание.

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. $E=\{(x_1,y_5),(x_1,y_6),(x_2,y_3),(x_2,y_4),$
$(x_3,y_1),(x_3,y_2),(x_3,y_5),(x_4,y_2),$
$(x_4,y_5),(x_5,y_2),(x_5,y_5),(x_5,y_6)\}$.

7.6. $E=\{(x_1,y_5),(x_1,y_6),(x_2,y_3),(x_2,y_4),(x_3,y_1),$
$(x_3,y_2),(x_3,y_5),(x_4,y_2),(x_4,y_5),$
$(x_4,y_6),(x_5,y_2),(x_5,y_4),(x_5,y_6)\}$.

7.7. $E=\{(x_1,y_3),(x_1,y_5),(x_1,y_6),(x_2,y_3),(x_2,y_4),(x_2,y_6),$
$(x_3,y_1),(x_3,y_2),(x_3,y_5),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_2),(x_5,y_4),(x_5,y_6)\}$.

7.8. $E=\{(x_1,y_3),(x_1,y_5),(x_1,y_6),(x_2,y_3),(x_2,y_4),(x_2,y_5),$
$(x_3,y_1),(x_3,y_2),(x_3,y_5),(x_3,y_6),(x_4,y_1),$
$(x_4,y_2),(x_4,y_5),(x_5,y_2),(x_5,y_4),(x_5,y_6)\}$.

7.9. $E=\{(x_1,y_3),(x_1,y_5),(x_1,y_6),(x_2,y_3),(x_2,y_4),(x_2,y_6),$
$(x_3,y_1),(x_3,y_2),(x_3,y_5),(x_4,y_2),$
$(x_4,y_5),(x_5,y_2),(x_5,y_4),(x_5,y_6)\}$.

7.10. $E=\{(x_1,y_5),(x_1,y_6),(x_2,y_3),(x_2,y_4),(x_3,y_1),$
$(x_3,y_2),(x_3,y_5),(x_3,y_6),(x_4,y_2),(x_4,y_2),$
$(x_4,y_5),(x_5,y_2),(x_5,y_3),(x_5,y_6)\}$.

7.11. $E=\{(x_1,y_2),(x_1,y_3),(x_1,y_4),(x_2,y_5),(x_2,y_6),$
$(x_3,y_2),(x_3,y_4),(x_3,y_5),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_2),(x_5,y_3),(x_5,y_6)\}$.

7.12. $E=\{(x_1,y_3),(x_1,y_4),(x_1,y_5),(x_2,y_1),(x_2,y_5),(x_2,y_6),$
$(x_3,y_2),(x_3,y_5),(x_4,y_1),(x_4,y_2),(x_4,y_5),$
$(x_4,y_6),(x_5,y_2),(x_5,y_4),(x_5,y_6)\}$.

7.13. $E=\{(x_1,y_3),(x_1,y_4),(x_1,y_6),(x_2,y_5),(x_2,y_6),$
$(x_3,y_4),(x_3,y_2),(x_3,y_5),(x_4,y_3),(x_4,y_1),$
$(x_4,y_2),(x_4,y_5),(x_5,y_2),(x_5,y_6)\}$.

7.14. $E=\{(x_1,y_5),(x_1,y_3),(x_1,y_4),(x_2,y_4),(x_2,y_5),(x_2,y_6),$
$(x_3,y_2),(x_3,y_5),(x_4,y_3),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_1),(x_5,y_2),(x_5,y_6)\}$.

7.15. $E=\{(x_1,y_6),(x_1,y_3),(x_1,y_4),(x_2,y_3),(x_2,y_5),(x_2,y_6),$
$(x_3,y_1),(x_3,y_2),(x_3,y_5),(x_4,y_2),(x_4,y_1),$
$(x_4,y_5),(x_5,y_5),(x_5,y_2),(x_5,y_6)\}$.

7.16. $E=\{(x_1,y_5),(x_1,y_3),(x_1,y_4),(x_2,y_3),(x_2,y_5),(x_2,y_6),$
$(x_3,y_1),(x_3,y_2),(x_3,y_5),(x_4,y_6),(x_4,y_1),$
$(x_4,y_2),(x_4,y_5),(x_5,y_4),(x_5,y_2),(x_5,y_6)\}$.

7.17. $E=\{(x_1,y_3),(x_1,y_4),(x_2,y_6),(x_2,y_5),(x_2,y_6),$
$(x_3,y_5),(x_3,y_2),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_4),(x_5,y_2),(x_5,y_6)\}$.

7.18. $E=\{(x_1,y_3),(x_1,y_4),(x_2,y_5),(x_2,y_6),(x_3,y_6),$
$(x_3,y_2),(x_3,y_5),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_4),(x_5,y_2),(x_5,y_6)\}$.

7.19. $E=\{(x_1,y_3),(x_1,y_4),(x_2,y_5),(x_2,y_6),(x_3,y_5),$
$(x_3,y_2),(x_4,y_1),(x_4,y_2),(x_4,y_5),$
$(x_5,y_4),(x_5,y_2),(x_5,y_6)\}$.

7.20. $E=\{(x_1,y_5),(x_1,y_3),(x_1,y_4),(x_2,y_4),(x_2,y_5),(x_2,y_6),$
$(x_3,y_6),(x_3,y_2),(x_3,y_5),(x_4,y_2),(x_4,y_1),$
$(x_4,y_5),(x_5,y_3),(x_5,y_2),(x_5,y_6)\}$.

7.21. $=\{(x_1,y_2),(x_1,y_4),(x_1,y_1),(x_2,y_2),(x_2,y_6),$
$(x_3,y_4),(x_3,y_5),(x_3,y_6),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_3),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

7.22. $E=\{(x_1,y_5),(x_1,y_4),(x_1,y_1),(x_2,y_1),(x_2,y_5),(x_2,y_6),$
$(x_3,y_2),(x_3,y_6)(x_4,y_6),(x_4,y_2),(x_4,y_5),$
$(x_5,y_4),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

7.23. $E=\{(x_1,y_6),(x_1,y_4),(x_1,y_1),(x_2,y_5),(x_2,y_6),$
$(x_3,y_4),(x_3,y_2),(x_3,y_6),(x_4,y_3),(x_4,y_2),$
$(x_4,y_5),(x_5,y_2),(x_5,y_1),(x_5,y_5)\}$.

7.24. $E=\{(x_1,y_5),(x_1,y_4),(x_1,y_1),(x_2,y_4),(x_2,y_5),(x_2,y_6),$
$(x_3,y_2),(x_3,y_6),(x_4,y_3),(x_4,y_2),$
$(x_4,y_5),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

7.25. $E=\{(x_1,y_6),(x_1,y_4),(x_1,y_1),(x_2,y_3),(x_2,y_5),$
$(x_2,y_6),(x_3,y_1),(x_3,y_2),(x_3,y_6),(x_4,y_2),$
$(x_4,y_5),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

7.26. $E=\{(x_1,y_5),(x_1,y_4),(x_1,y_1),(x_2,y_3),(x_2,y_5),(x_2,y_6),$
$(x_3,y_1),(x_3,y_2),(x_3,y_6),(x_4,y_6),(x_4,y_2),$
$(x_4,y_5),(x_5,y_4),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

7.27. $E=\{(x_1,y_3),(x_1,y_4),(x_1,y_1),(x_2,y_5),(x_2,y_6),$
$(x_3,y_5),(x_3,y_2),(x_3,y_6),(x_4,y_1),(x_4,y_2),$
$(x_4,y_5),(x_5,y_4),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

7.28. $E=\{(x_1,y_3),(x_1,y_4),(x_1,y_1),(x_2,y_5),(x_2,y_6),$
$(x_3,y_2),(x_3,y_6),(x_4,y_1),(x_4,y_2),(x_4,y_5),$
$(x_5,y_4),(x_5,y_1),(x_5,y_2),(x_5,y_5)\}$.

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.

8.1. $A_1=\{1,3\}$, $A_2=\{2,3,4\}$, $A_3=\{2,3,5\}$, $A_4=\{1,2\}$, $A_5=\{3,6\}$.

8.2. $A_1=\{2,3\}$, $A_2=\{2,4\}$, $A_3=\{3,4,5\}$, $A_4=\{1,2,3\}$, $A_5=\{1,6\}$.

8.3. $A_1=\{5,6\}$, $A_2=\{1,2,3\}$, $A_3=\{4,5,6\}$, $A_4=\{3,4\}$, $A_5=\{1,2\}$.

8.4. $A_1=\{1,2\}$, $A_2=\{1,4\}$, $A_3=\{3,4,5\}$, $A_4=\{1,3,4\}$, $A_5=\{2,3\}$.

8.5. $A_1=\{3,4,5\}$, $A_2=\{1,5\}$, $A_3=\{2,3\}$, $A_4=\{2,4,5\}$, $A_5=\{1,5\}$.

8.6. $A_1=\{2,3\}$, $A_2=\{4,5\}$, $A_3=\{1,3,5\}$, $A_4=\{3,4,5\}$, $A_5=\{1,6\}$.

8.7. $A_1=\{2,4,5\}$, $A_2=\{1,2,3\}$, $A_3=\{1,3,4\}$, $A_4=\{3,5\}$, $A_5=\{2,6\}$.

8.8. $A_1=\{3,4\}$, $A_2=\{1,2,3\}$, $A_3=\{2,5\}$, $A_4=\{3,4,5\}$, $A_5=\{3,6\}$.

8.9. $A_1=\{2,6\}$, $A_2=\{1,3,4,6\}$, $A_3=\{1,2,5\}$, $A_4=\{1,3,5\}$, $A_5=\{3,4\}$.

8.10. $A_1=\{1,3,5\}$, $A_2=\{2,4,6\}$, $A_3=\{1,2,3,4\}$, $A_4=\{3,4,5,6\}$, $A_5=\{5,6\}$.

8.11. $A_1=\{1,3,6\}$, $A_2=\{4,5,6\}$, $A_3=\{2,3,5,6\}$, $A_4=\{1,2,4\}$, $A_5=\{5,6\}$.

8.12. $A_1=\{1,2\}$, $A_2=\{3,5,6\}$, $A_3=\{1,3,6\}$, $A_4=\{1,2,3,4\}$, $A_5=\{3,4\}$.

8.13. $A_1=\{2,3,5\}$, $A_2=\{1,2,3,5\}$, $A_3=\{3,4,6\}$, $A_4=\{3,5,6\}$, $A_5=\{1,2,5,6\}$.

8.14. $A_1=\{1,3,4\}$, $A_2=\{2,4,5\}$, $A_3=\{1,5,6\}$, $A_4=\{1,2,3\}$, $A_5=\{2,6\}$.

8.15. $A_1=\{1,2,3\}$, $A_2=\{1,3,5\}$, $A_3=\{2,3,4\}$, $A_4=\{1,2,3,4\}$,

$A_5=\{1,2,3,5\}$.

8.16. $A_1=\{1,2,3,4\}$, $A_2=\{2,3,4,5\}$, $A_3=\{3,4,5,6\}$, $A_4=\{1,3,5\}$, $A_5=\{2,4,6\}$.

8.17. $A_1=\{1,2,3,4\}$, $A_2=\{1,5,6\}$, $A_3=\{3,5,6\}$, $A_4=\{1,4,5\}$, $A_5=\{2,3,6\}$.

8.18. $A_1=\{1,2,5\}$, $A_2=\{1,5,6\}$, $A_3=\{1,2,3,4\}$, $A_4=\{1,4,5\}$, $A_5=\{1,3,6\}$.

8.19. $A_1=\{1,4,5,6\}$, $A_2=\{1,2,5\}$, $A_3=\{1,2,3,6\}$, $A_4=\{2,3,5\}$, $A_5=\{1,4,5\}$.

8.20. $A_1=\{2,3,5\}$, $A_2=\{1,3,5,6\}$, $A_3=\{1,2,6\}$, $A_4=\{2,5,6\}$, $A_5=\{1,4,5,6\}$.

8.21. $A_1=\{1,3,6\}$, $A_2=\{1,2,5\}$, $A_3=\{1,3,5\}$, $A_4=\{2,4,6\}$, $A_5=\{1,2,3,5\}$.

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 4×4-матрице $W=[w_{ij}]$, где вес w_{ij} ребра $e_{ij}=(x_i,y_j)$ 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.

Задача 10. 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.

Задача 12. В заданном ориентированном графе из задачи 10 найти все максимальные и все наибольшие внутренне устойчивые (независимые) множества вершин.

Задача 13. В заданном неориентированном графе из задачи 10 найти все минимальные и все наименьшие внешне устойчивые (доминирующие) множества вершин.

Задача 14. В заданном ориентированном графе из задачи 10 найти все минимальные и все наименьшие внешне устойчивые (доминирующие) множества вершин.

Задача 15. Найти хроматическое число графа и оптимальную раскраску графа из задачи 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 17. Найти число ожерелий, которые можно составить из семи бусин не более чем m цветов. Число цветов m равно числу букв в фамилии студента. Бусины обозначить буквами фамилии студента. Недостающие буквы взять из алфавита.

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. Вершины многогранника M обозначить буквами фамилии студента. Недостающие буквы взять из алфавита.

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 переход из одного состояния в другое при поступлении на вход автомата указанных 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 $(q_2,0a,q_2)$.

Пример. Пусть автомат Мили задается функциями переходов и выходов (табл.6.1), где X={0,1}; Y={0,1,2} множества входных символов; Q={q_0,q_1,q_2} множество состояний. Для автомата Мили из табл.6.1 функции переходов и выходов эквивалентного ему автомата Мура приведены в табл.6.3; выход в состоянии q_0 произволен.

Таблица 6.1

		состояния		
		q_0	q_1	q_2
вход	0	$q_2,1$	$q_2,0$	$q_1,1$
	1	$q_1,2$	$q_2,2$	$q_2,2$

Таблица 6.2

	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	$(q_0,1)$	$(q_1,1)$	$(q_1,1)$	$(q_2,1)$	$(q_2,1)$	$(q_2,1)$	$(q_2,1)$

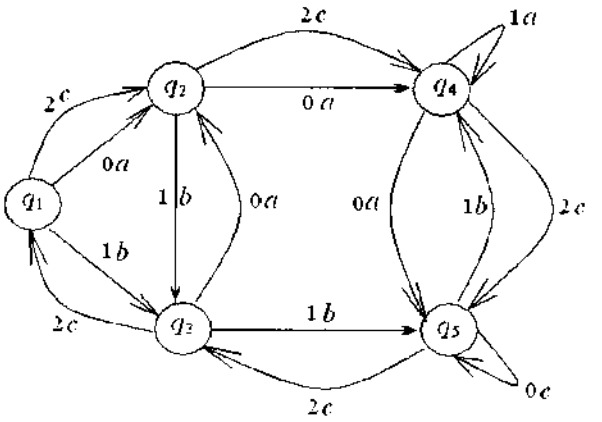


Рис.6.1

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.** $(q_2,0a,q_5)$.	

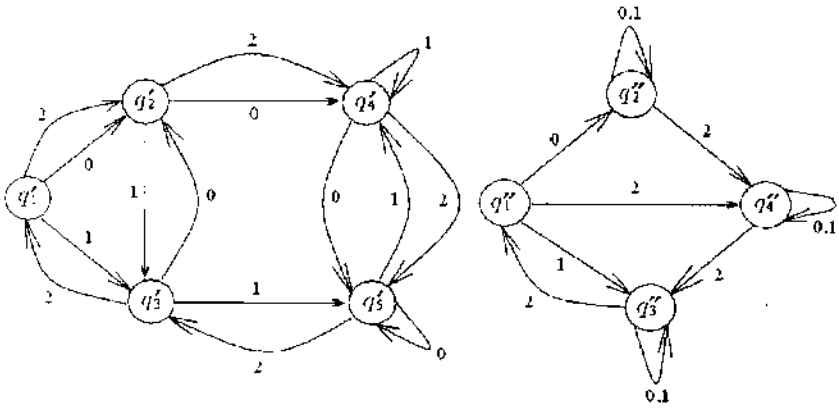
Задача 2. Построить автомат $A = (X,Q,q_1,T,F)$ для объединения двух языков, представимых детерминированными автоматами $A' = (X,Q',q_1',T',F')$, $A'' = (X,Q'',q_1'',T'',F'')$ (рис.6.2) с множеством входных символов $X = \{0,1,2\}$, с начальными состояниями q_1' и q_1'' и с выделенными состояниями $F' = \{q_3',q_5'\}$, $F'' = \{q_3''\}$. Вариант автомата получить, взяв указанный переход из одного состояния в другое при поступлении на вход автомата указанного 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 $(q_3'',1,q_2'')$.

Указание. *Прямое (декартово) произведение автоматов* $A' = (X,Q',q_0',T')$ и $A''=(X,Q'',q_0'',T'')$ есть автомат $A'\times A''=(X,Q'\times Q'',$

$(q_0,q''_0),T)$, где $T((q',q''),a)=(T'(q',a),T''(q'',a))$, $q'\in Q'$, $q''\in Q''$, $a\in X$.

Класс автоматно представимых языков замкнут относительно булевых операций (объединения, пересечения, дополнения).

В самом деле, пусть автоматы $A'=(X,Q',q'_0,T',F')$ и $A''=(X,Q'',q''_0,T'',F'')$ определяют языки $Beh(A')$ и $Beh(A'')$ соответственно. *Дополнение* $X^*-Beh(A')$ определимо автоматом $(X,Q',q'_0,T',Q'-F')$. *Пересечение* $Beh(A')\cap Beh(A'')$ определимо декартовым произведением $A'\times A''$ с множеством выделенных состояний $F'\times F''$. Объединение $Beh(A')\cup Beh(A'')$ определимо декартовым произведением $A'\times A''$ с множеством выделенных состояний $F'\times Q''\cup Q'\times F''$.



Автомат A' Автомат A''

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. $(q''_3,1,q''_1)$.	**2.29.** $(q''_4,2,q''_1)$.	**2.30.** $(q''_3,2,q''_2)$.

Задача 3. Построить автомат для пересечения двух языков, представимых детерминированными автоматами A', A'' (рис.6.2).

Вариант автомата и указание к решению 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 $(q_3, 2, q_2)$.

Указание. *Источник* есть объект $S = (X, Q, Q_0, D, F)$, где X – входной алфавит; Q – алфавит состояний, $Q_0 \subseteq Q$ – множество начальных состояний, $D \subseteq Q \times X \times Q$ – (недетерминированная) таблица переходов (здесь в качестве входного сигнала допускается пустой символ, обозначаемый $*$), $F \subseteq Q$ – множество выделенных состояний. Тройка (q, a, q') из D называется переходом 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 состояние, 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, котоые 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 слева от табл.6.3. Таблица переходов детерминированного автомата A, эквивалентного источнику S, приведена в табл.6.3. Выделенные состояния автомата A помечены звездочками.

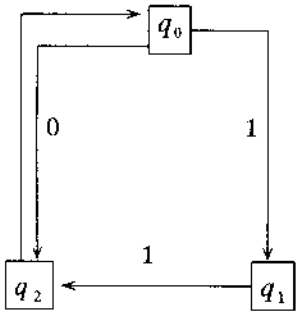


Таблица 6.3

	* $\{q_0\}$	$\{q_1\}$	* $\{q_0, q_2\}$	ø
0	$\{q_0, q_2\}$	ø	$\{q_0, q_2\}$	ø
1	$\{q_1\}$	$\{q_0, q_2\}$	$\{q_1\}$	ø

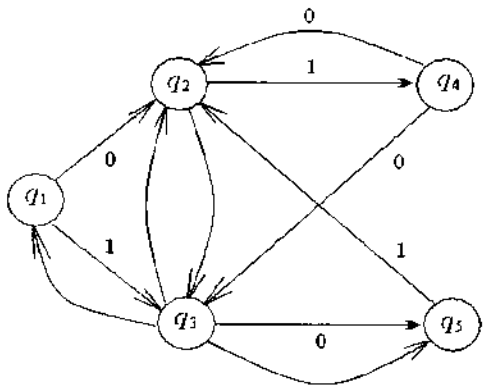


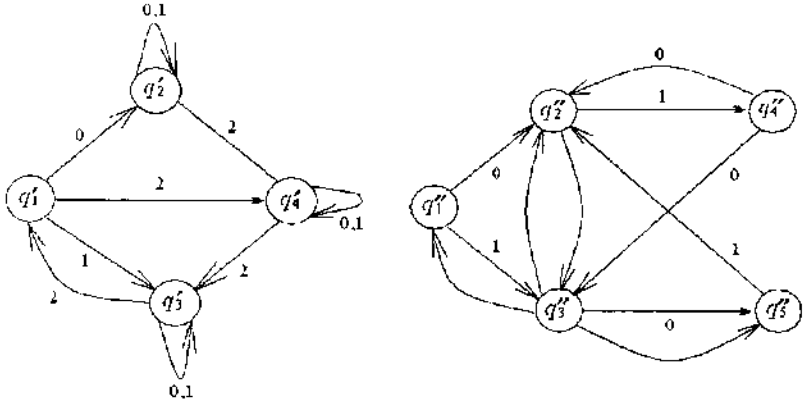
Рис.6.3

4.1. $(q_1,2,q_2)$. **4.2.** $(q_1,2,q_3)$. **4.3.** $(q_1,2,q_4)$.
4.4. $(q_1,2,q_5)$. **4.5.** $(q_2,2,q_3)$. **4.6.** $(q_2,2,q_4)$.
4.7. $(q_2,2,q_5)$. **4.8.** $(q_3,2,q_4)$. **4.9.** $(q_3,2,q_5)$.
4.10. $(q_4,2,q_5)$. **4.11.** $(q_1,1,q_2)$. **4.12.** $(q_1,0,q_3)$.
4.13. $(q_1,1,q_4)$. **4.14.** $(q_2,2,q_3)$. **4.15.** $(q_2,2,q_4)$.
4.16. $(q_3,2,q_4)$. **4.17.** $(q_2,1,q_1)$. **4.18.** $(q_3,2,q_1)$.
4.19. $(q_4,2,q_1)$. **4.20.** $(q_5,2,q_1)$. **4.21.** $(q_3,2,q_2)$.
4.22. $(q_4,2,q_2)$. **4.23.** $(q_5,2,q_2)$. **4.24.** $(q_4,2,q_3)$.
4.25. $(q_5,2,q_3)$. **4.26.** $(q_5,2,q_4)$. **4.27.** $(q_2,2,q_1)$.
4.28. $(q_3,0,q_1)$. **4.29.** $(q_4,2,q_1)$. **4.30.** $(q_3,2,q_2)$.

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

$X = \{0,1,2\}$. Множества начальных состояний $Q'_0 = \{q'_1\}$, $Q''_0 = \{q''_1, q''_2\}$. Множества выделенных состояний $F' = \{q'_3\}$, $F'' = \{q''_3, q''_5\}$. 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. Граф-схемы источников S_1 и S_2 при объединении объединяются. Начальные состояния для S_1 и S_2 становятся начальными состояниями для S, а выделенные состояния для S_1 и S_2 – выделенными состояниями для S.



Источник S' Источник S''

Рис.6.4

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. 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.

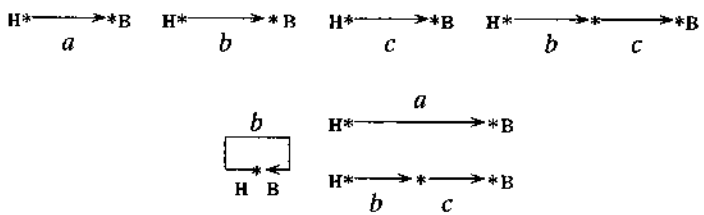
Указание. При итерации в граф-схеме для S_1 добавляются пустые стрелки из выделенных состояний для S_1 в его начальные состояния.

Задача 8. 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.

Источник строится индукцией по построению формулы R.

Для подформул a, b, c, $b \cdot c$, b^*, $a \vee b \cdot c$ будут соответственно следующие источники.



Соединяем их в порядке построения формулы и получаем искомый источник (рис.5) $A = (X,Q,Q_0T,F)$, $X = \{a,b,c\}$, $Q = \{q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7,q_8,q_9\}$, $Q_0 = \{q_0\}$, $T = \{(q_0,a,q_1), (q_1,*,q_2), (q_2,b,q_2), (q_2,*,q_3), (q_2,*,q_4), (q_3,a,q_6), (q_4,b,q_5), (q_5,c,q_7), (q_6,*,q_3), (q_6,*,q_4), (q_6,*,q_8), (q_7,*,q_4), (q_7,*,q_3), (q_7,*,q_8), (q_8,c,q_9)\}$, $F = \{q_9\}$, который детерминизируем, и полученный конечный автомат минимизируем по числу состояний.

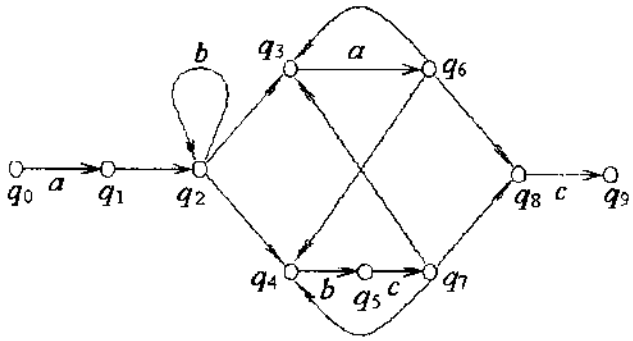


Рис.6.5

8.1. $0\cdot 1^*\cdot(0\cdot 2\cdot 1)^*\cdot 2$. **8.2.** $0\cdot 1^*\cdot(0\cdot 2\cdot 1)^*\vee 2$.
8.3. $0\cdot 1^*\cdot(0\cdot 2\vee 1)^*\cdot 2$. **8.4.** $0\cdot 1^*\cdot(0\cdot 2\vee 1)^*\vee 2$.
8.5. $0\cdot 1^*\cdot(0\vee 2\cdot 1)^*\cdot 2$. **8.6.** $0\cdot 1^*\cdot(0\vee 2\cdot 1)^*\vee 2$.
8.7. $0\cdot 1^*\cdot(0\vee 2\vee 1)^*\cdot 2$. **8.8.** $0\cdot 1^*\cdot(0\vee 2\vee 1)^*\vee 2$.
8.9. $0\cdot 1^*\vee(0\cdot 2\cdot 1)^*\cdot 2$. **8.10.** $0\cdot 1^*\vee(0\cdot 2\cdot 1)^*\vee 2$.
8.11. $0\cdot 1^*\vee(0\cdot 2\vee 1)^*\cdot 2$. **8.12.** $0\cdot 1^*\vee(0\cdot 2\vee 1)^*\vee 2$.
8.13. $0\cdot 1^*\vee(0\vee 2\cdot 1)^*\cdot 2$. **8.14.** $0\cdot 1^*\vee(0\vee 2\cdot 1)^*\vee 2$.
8.15. $0\cdot 1^*\vee(0\vee 2\vee 1)^*\cdot 2$. **8.16.** $0\cdot 1^*\vee(0\vee 2\vee 1)^*\vee 2$.
8.17. $0\vee 1^*\cdot(0\cdot 2\cdot 1)^*\cdot 2$. **8.18.** $0\vee 1^*\cdot(0\cdot 2\cdot 1)^*\vee 2$.
8.19. $0\vee 1^*\cdot(0\cdot 2\vee 1)^*\cdot 2$. **8.20.** $0\vee 1^*\cdot(0\cdot 2\vee 1)^*\vee 2$.
8.21. $0\vee 1^*\cdot(0\vee 2\cdot 1)^*\cdot 2$. **8.22.** $0\vee 1^*\cdot(0\vee 2\cdot 1)^*\vee 2$.
8.23. $0\vee 1^*\cdot(0\vee 2\vee 1)^*\cdot 2$. **8.24.** $0\vee 1^*\cdot(0\vee 2\vee 1)^*\vee 2$.
8.25. $0\vee 1^*\vee(0\cdot 2\cdot 1)^*\cdot 2$. **8.26.** $0\vee 1^*\vee(0\cdot 2\cdot 1)^*\vee 2$.
8.27. $0\vee 1^*\vee(0\cdot 2\vee 1)^*\cdot 2$. **8.28.** $0\vee 1^*\vee(0\cdot 2\vee 1)^*\vee 2$.
8.29. $0\vee 1^*\vee(0\vee 2\cdot 1)^*\cdot 2$. **8.30.** $0\vee 1^*\vee(0\vee 2\cdot 1)^*\vee 2$.
8.31. $0\vee 1^*\vee(0\vee 2\vee 1)^*\cdot 2$. **8.32.** $0\vee 1^*\vee(0\vee 2\vee 1)^*\vee 2$.

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 – конечный алфавит. *Обращение* слова $x = x(0)x(1)\ldots x(k-1)x(k)$ из X^* есть слово $x^{-1}=x(k)\ldots x(0)$. Если множество $M \subseteq X^*$, то $M^{-1} = \{x^{-1}: x \in M\}$.

Теорема. Класс языков, представимых источниками, замкнут отноительно операции обращения.

Доказательство. 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.

Задача 10. По данному источнику $S=(A,Q,Q_0,D,F)$, $Q_0=\{q_1\}$, $F=\{q_2,q_5\}$ (рис.6.6), представляющему язык L в входном алфавите $X = \{0,1,2,3,4,5\}$, построить источник, представляющий проекцию языка L при отображении $f: X \to Y$ с алфавита X на алфавит Y. Положить алфавит $Y = \{a,b,c\}$. Функция f определяется вариантом задания. Детерминизировать полученный источник.

Указание. Пусть $X = \{a_0,a_1,\ldots a_k\}$, $Y = \{b_0,b_1,\ldots,b_l\}$ – два конечных алфавита, и пусть функция $f: X \to Y$ осуществляет *проекцию* с одного алфавита на другой (т.е. с алфавита X на алфавит Y). Пусть $x = x(0)x(1)\ldots x(r)$ – слово в алфавите X. Тогда слово $f(x) = f(x(0))f(x(1))\ldots f(x(r))$ 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 отноительно проекции.

Доказательство. Пусть язык M представим источником $S = (X,Q,Q_0,D,F)$, и функция $f: X \to Y$ 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.

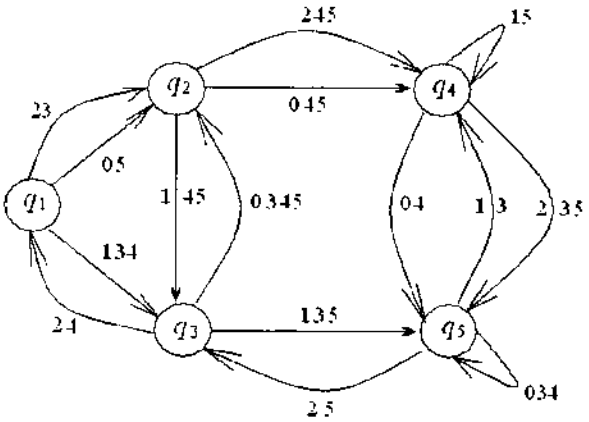


Рис.6.6

	x	0	1	2	3	4	5
10.1.	$f(x)$	a	b	b	c	c	a
10.2.	$f(x)$	b	b	a	c	c	a
10.3.	$f(x)$	b	b	c	a	c	a
10.4.	$f(x)$	b	a	c	c	a	a
10.5.	$f(x)$	b	a	b	c	c	a
10.6.	$f(x)$	a	b	b	c	c	b
10.7.	$f(x)$	a	b	a	c	c	b
10.8.	$f(x)$	a	b	c	a	c	b
10.9.	$f(x)$	a	a	c	c	a	b
10.10.	$f(x)$	b	a	a	c	c	b
10.11.	$f(x)$	b	a	c	a	c	b
10.12.	$f(x)$	b	c	c	c	a	b
10.13.	$f(x)$	b	c	a	a	c	b
10.14.	$f(x)$	b	c	a	c	a	b
10.15.	$f(x)$	b	c	c	a	a	b
10.16.	$f(x)$	a	c	a	b	c	b
10.17.	$f(x)$	a	c	b	a	c	b
10.18.	$f(x)$	a	c	b	c	a	b
10.19.	$f(x)$	b	c	a	b	c	a
10.20.	$f(x)$	a	a	a	b	c	b
10.21.	$f(x)$	c	a	a	b	c	b
10.22.	$f(x)$	c	a	b	a	c	b
10.23.	$f(x)$	c	a	b	c	a	b
10.24.	$f(x)$	a	b	b	b	c	c
10.25.	$f(x)$	a	a	a	b	c	c
10.26.	$f(x)$	a	a	b	a	c	c
10.27.	$f(x)$	a	a	b	c	a	c
10.28.	$f(x)$	b	b	a	b	c	c
10.29.	$f(x)$	b	a	b	a	c	c
10.30.	$f(x)$	b	b	b	c	a	c
10.31.	$f(x)$	b	b	a	c	a	c
10.32.	$f(x)$	c	b	b	a	b	c

Задача 11. По заданному источнику S с множеством входных символов $X = \{a,b,c\}$, допускающему язык L, построить источник, допускающий язык $Tranc(L,a)$. Множество начальных состояний $Q_0 = \{q_1,q_2\}$. Множество выделенных состояний $F = \{q_3, q_5\}$. Чтобы получить вариант источника, следует добавить к граф–схеме источника, изображенного на рис.6.7, стрелку варианта. Например, в варианте 30 к граф–схеме источника надо добавить стрелку (q_3,c,q_2). Детерминизировать полученный источник.

Указание. Пусть $x = x(0)x(1)\ldots x(k)aa\ldots a$ при $x(k) \neq a$ есть слово в алфавите X, содержащем букву a. Тогда операция *усечения* слова x по букве a (обозначение: $Tranc(x,a)$) определяется как $Tranc(x,a) = x(0)x(1)\ldots x(k)$. Если $M \subseteq X^*$, то множество $Tranc(M,a) = \{Tranc(x,a) : x \in M\}$.

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 $a^k = aaa\ldots a$, k раз. Построим источник $S'=(X,Q,Q_0,D,G)$, где $G=Q_a \cup F$, где $Q_a=\{q \in Q : \exists k\, \exists q' \in F\ ((q,a^k,q') \in D\}$, 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 так (рис.6.7*а*). 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 $G=Q_a \cup F=\{q_3,q_4\} \cup \{q_3,q_5\} = \{q_3,q_4,q_5\}$. 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.

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 $F = \{q_b,q_c\}$.

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 $x = x(0)x(1)\ldots x(k)$ – некоторое слово в алфавите X, причем слово x содержит букву a. *Аннулирование* буквы a в слове x есть стирание в слове x буквы a всюду, где

она встречается. Обозначим эту операцию через $An(x,a)$. Пусть $M \subseteq X^*$. Тогда $An(M,a) = \{An(x,a) : x \in M\}$.

По заданному источнику S из задачи 11 с множеством входных символов $X = \{a,b,c\}$, допускающему язык L, построить источник, допускающий язык $An(L,a)$. Детерминизировать полученный источник.

Теорема. Класс языков, представимых источниками, замкнут отосительно 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 стираются буквы a всюду, где они встречаются, но сами стрелки, которые помечены буквой a, остаются.

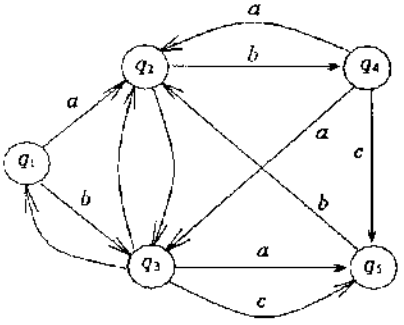


Рис.6.7

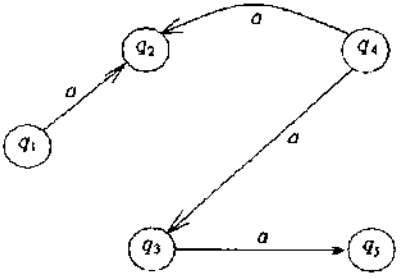


Рис.6.7*a*

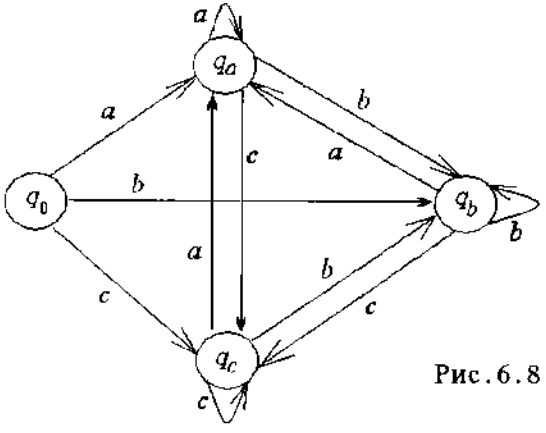


Рис.6.8

6. МНОЖЕСТВА, ФУНКЦИИ, ОТНОШЕНИЯ (Примеры решения)

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

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

Задача 2. Частично упорядоченное множество $(A, \leqslant)$, $A=\{0,1,2,3,\ldots,20\}$, задано диаграммой (рис.6.1). Множество $B = \{5,6,9,10\} \subseteq A$.

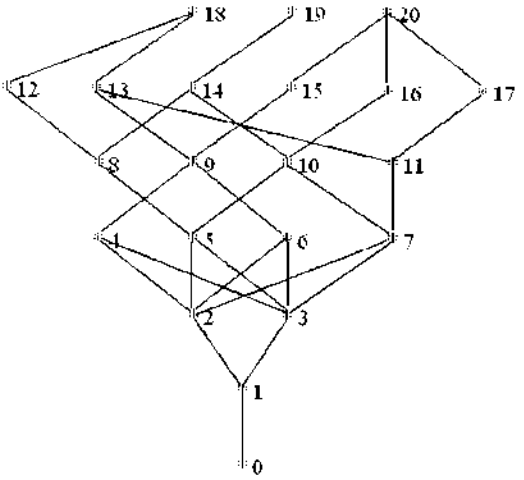


Рис.6.1

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.

Решение. M есть наибольший элемент в A (верхняя универсальная граница), если $a \leqslant M \ \forall a \in A$. m есть наименьший элемент в A (нижняя универсальная граница), если $m \leqslant a \ \forall a \in A$.

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

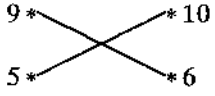
Элемент a минимален в A, если $\neg \exists x \in A \ x < a$.

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

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

Верхний конус B^{Δ} для B есть совокуность всех верхних граней для B. Нижний конус B^{∇} для B есть совокуность всех нижних граней для B. Точная верхняя грань для B есть наименьший элемент b^{Δ} в B^{Δ}. Точная нижняя грань для B есть наибольший элемент b^{∇} в B^{∇}.

1. Диаграмма для B имеет вид:

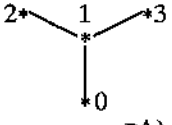


2. Наибольший элемент (верхняя универсальная граница в A) не существует. Наименьший элемент (нижняя универсальная граница в A) есть 0.

3. $\{18,19,20\}$ есть множество максимальных элементов. $\{0\}$ есть множество минимальных элементов.

4. Верхний конус для B есть $B^{\Delta}=\{20\}$.

5. Нижний конус для B есть $B^{\nabla}=\{0,1,2,3\}$. Это



6. Точная верхняя грань для B (наименьший элемент в B^{Δ}) есть 20.

7. Точная верхняя грань для B (наибольший элемент в B^{∇}) не существует.

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

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

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

$f^{-1}(0) = K_0 = [0]_\sigma = \{0,5\},\ q(K_0) = 0,$
$f^{-1}(1) = K_1 = [1]_\sigma = \{1,2,4\},\ q(K_1) = 1,$
$f^{-1}(2) = K_2 = [2]_\sigma = \{3\},\ q(K_2) = 2,$
$f^{-1}(3) = K_3 = [3]_\sigma = \{8,9\},\ q(K_3) = 3,$
$f^{-1}(5) = K_5 = [5]_\sigma = \{6,7\},\ q(K_5) = 5.$

Функции p,q задаются следующим образом.

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

$D(p) = A,\ \mathrm{Im}(p) = \{K_0,K_1,K_2,K_3,K_5\};$

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

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

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

$b_1b_2b_3b_4b_5b_6b_7$=2355131 в алфавите $\mathrm{Im}(f)$={0,1,2,3,5},

посылаем шифротекст $a_1a_2a_3a_4a_5a_6a_7$, где всякое $a_i \in K_i$, например, $a_1a_2a_3a_4a_5a_6a_7$ = 3967284, что дешифруется как

$f(a_1)f(a_2)f(a_3)f(a_4)f(a_5)f(a_6)f(a_7)$ = 2355131.

Задача 4. Решетка задана своей диаграммой в задаче 4.30. Является ли она модулярной. Найти дополнения (если они есть) для элементов a,d,h,l.

Решение. Аксиомы решетки.

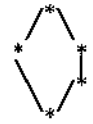
1. $a\wedge a=a,\ \ a\vee a=a.$
2. $a\wedge b=b\wedge a,\ a\vee b=b\vee a.$
3. $a\wedge(b\wedge c)=(a\wedge b)\wedge c,\ a\vee(b\vee c)=(a\vee b)\vee c.$
4. $a\wedge(a\vee b)=a,\ a\vee(a\wedge b)=a.$

Дистрибутивность.

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

Модулярность.

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

Решетка модулярна $\longleftrightarrow$ решетка  не является ее подрешеткой.

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

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

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

Задача 5. Найти все тупиковые и все наименьшие покрытия строк двоичной матрицы $A =$

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

Решение. Пусть $A=(a_{ij})$, $i=1,2,\ldots,m$, $j=1,2,\ldots,n$, 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)

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

В решеточном выражении n скобок. Первая скобка $(x_{1j_1} \vee \ldots x_{1j_k})$ означает, что строка 1 имеет единицы на местах $j_1, \ldots, j_k$ и потому покрыта столбцами $x_{j_1}, \ldots, x_{j_k}$. Аналогично для покрытия строк $2,3,\ldots,m$.

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 $x_{j_1} \ldots x_{j_k}$ дает тупиковое покрытие множеством столбцов $\{j_1, \ldots, j_k\}$.

7. Выбираем из них все наименьшие.

В данном примере вычисления дают следующее.

1. Решеточное выражение

$L = (x_1 \vee x_2 \vee x_6)(x_1 \vee x_4 \vee x_5 \vee x_6)(x_3 \vee x_4)(x_3 \vee x_4 \vee x_5)(x_5 \vee x_6) =$
$x_1x_3x_5 \vee x_2x_3x_5 \vee x_2x_4x_5 \vee x_3x_6 \vee x_4x_6 \vee x_1x_4x_5$.

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 $\{x_3, x_6\}, \{x_4, x_6\}$.

Задача 6. В булевой алгебре $(A, \leqslant)$ 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 $f: 2^A \to \{0,1\}$ и получить представление множества $Z = \{0,2,3\}$ из $A = \{0,1,2,3\}$ булевым многочленом относительно независимых множеств.

$f(z) = 0101100101011001 =$

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	0	0	0	1

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

A		2^U	0 1 2 3 $x_1x_2x_3x_4$	$f(z)$	Z
0	0000	$\varnothing$	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
			$A_1A_2A_3A_4$		

Порождающие множества.

$A_1=\{8,9,10,11,12,13,14,15\}$,
$A_2=\{4,5,6,7,12,13,14,15\}$,
$A_3=\{2,3,6,7,10,11,14,15\}$,
$A_4=\{1,3,5,7,9,11,13,15\}$.

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

Обозначение:

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

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

Функция алгебры логики

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

$$\bar{x}_1\bar{x}_2\bar{x}_3x_4 \vee \bar{x}_1\bar{x}_2x_3x_4 \vee \bar{x}_1x_2\bar{x}_3\bar{x}_4 \vee \bar{x}_1x_2x_3x_4 \vee$$
$$x_1\bar{x}_2\bar{x}_3x_4 \vee x_1\bar{x}_2x_3x_4 \vee x_1x_2x_3x_4.$$

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.

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

$$\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4 \cup \bar{A}_1 \cap \bar{A}_2 \cap A_3 \cap \bar{A}_4 \cup \bar{A}_1 \cap \bar{A}_2 \cap A_3 \cap A_4 \cup \bar{A}_1 \cap A_2 \cap A_3 \cap A_4 \cup$$
$$A_1 \cap \bar{A}_2 \cap A_3 \cap \bar{A}_4 \cup A_1 \cap A_2 \cap A_3 \cap \bar{A}_4.$$

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

$$r = \begin{bmatrix} 0 & 2 & 0 \\ 1 & 2 & 1 \\ 0 & 3 & 2 \\ 1 & 1 & 3 \end{bmatrix}, \quad s = \begin{bmatrix} 0 & 1 \\ 0 & 2 \\ 1 & 3 \\ 2 & 0 \end{bmatrix}, \quad r \circ s = \begin{bmatrix} 0 & 2 & 1 \\ 0 & 2 & 2 \\ 1 & 2 & 3 \\ 1 & 1 & 0 \end{bmatrix}.$$

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. $A = \mathbb{N}$, n=15.

Решение. $(x,y) \sim (x_1,y_1) \leftrightarrow y \equiv y_1 \pmod{15}$.

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

Определение. Соотношения R_0 и R_1

$L(x(k)) = x(k+n) + a_1 x(k+n-1) + \ldots + a_n x(k) = 0$,

$L(x(k)) = x(k+n) + a_1 x(k+n-1) + \ldots + a_n x(k) = f(k)$,

где $a_i \in \mathbb{R}$, $i = 1,2,\ldots,n$; $f(k) \not\equiv 0$ – известная функция, $x(k)$ – неизвестная функция, называются линейными рекуррентными уравнениями (ЛРУ) однородным и неоднородным соответственно с

постоянными коэффициентами.

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

Определение. Выражение $L(\lambda)=\lambda^n+a_1\lambda^{n-1}+a_2\lambda^{n-2}+\ldots+a_{n-1}\lambda+a_0$ 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

$\lambda_1,\ldots,\lambda_p$ –вещественные корни характеристического уравнения,

$l_1,\ldots,l_p$ – их кратности,

$\mu_1,\ldots,\mu_s$ – группа комплексных корней $\mu_j=\alpha_j+i\beta_j, j=1,2,\ldots,s$,

$\bar{\mu}_1,\ldots,\bar{\mu}_s$ – группа комплексных корней $\bar{\mu}_j=\alpha_j-i\beta_j, j=1,2,\ldots,s$,

$r_1,\ldots,r_s$ – их кратности,

ρ_j,φ_j – модуль и аргумент комплексного числа $\mu_j, j=1,\ldots,s$,

то функции

$$x_j(k) = k^{m_j}(\lambda_j)^k,\ j=1,\ldots,p;\ m_j=0,\ldots,l_j-1,$$

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

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

составляют ФСР однородного СЛРУ R_0.

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

$$x_{oo} = C_1x_1(k)+\ldots+C_nx_n(k),$$

где произвольные постоянные $C_1,\ldots,C_n$ пробегают $\mathbb{R}$ независимо друг от друга. Если $x_{чн}$ есть какое-либо частное решение неоднородного СЛРУ R_1, то его общее решение

$$x_{он} = x_{чн} + C_1x_1(k)+\ldots+C_nx_n(k).$$

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

3. Уравнение

$$a_nx(k+n) + a_{n-1}x(k+n-1) +\ldots+ a_{n-r}x(k+n-r) = f(k),$$

$k=0,1,2,\ldots$

допускает понижение порядка. Это уравнение имеет характеристическое уравнение

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

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

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

$k=n-r, n-r+1, \ldots$

порядка r с характеристическим уравнением

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

без нулевых корней.

В самом деле, из первого уравнения

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

Из второго уравнения

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

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

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

и тогда $y(k+3)=z(k)$, $k=0,1,2,\ldots$

Пример. 1. $x(k+2)-4x(k+1)+3x(k)=0$, $\lambda^2-4\lambda+3=0$, $\lambda_1=1, \lambda_2=3$,

$x_{oo} = C_1(\lambda_1)^k+C_2(\lambda_2)^k = C_1 1^k+C_2 3^k=C_1+C_2 3^k$, $C_1, C_2\in\mathbb{R}$.

2. $x(k+2)-3x(k)=0$, $\lambda^2-3=0$, $\lambda_1=\sqrt{3}, \lambda_2=-\sqrt{3}$,

$x_{oo}=C_1(\lambda_1)^k+C_2(\lambda_2)^k = C_1(\sqrt{3})^k+C_2(-\sqrt{3})^k$, $C_1, C_2\in\mathbb{R}$.

3. $x(k+2)-x(k+1)-x(k)=0$, $\lambda^2-\lambda-1=0$, $\lambda_1=\frac{1+\sqrt{5}}{2}$, $\lambda_2=\frac{1-\sqrt{5}}{2}$,

$$x_{oo} = C_1\left(\frac{1+\sqrt{5}}{2}\right)^k + C_2\left(\frac{1-\sqrt{5}}{2}\right)^k, \quad C_1, C_2\in\mathbb{R}.$$

4. $x(k+2)+2x(k+1)+x(k)=0$, $\lambda^2+2\lambda+1=0$, $\lambda=-1$ кратность 2,

$x_{oo} = C_1(-\lambda)^k+C_2k(-\lambda)^k = C_1(-1)^k+C_2k(-1)^k=(-1)^k(C_1+C_2k)$, $C_1, C_2\in\mathbb{R}$.

5. $x(k+3)+10x(k+2)+32x(k+1)+32x(k)=0$, $\lambda^3+10\lambda^2+32\lambda+32=0$, $(\lambda+4)^2(\lambda+2)=0$, $\lambda_1=-4$ кратности 2, $\lambda_2=-2$,

$x_{oo} = C_1(\lambda_1)^k + C_2k(\lambda_1)^k + C_3(\lambda_3)^k = C_1(-2)^k + C_2k(-2)^k + C_3(-2)^k$, $C_1, C_2, C_3 \in \mathbb{R}$.

6. $x(k+3)+3x(k+2)+3x(k+1)+x(k)=0$, $\lambda^3+3\lambda^2+3\lambda+1=0$, $(\lambda+1)^3=0$, $\lambda_1=-1$ кратности 3,
$x_{oo} = C_1(\lambda)^k + C_2k(\lambda)^k + C_3k^2(\lambda)^k = C_1(-1)^k + C_2k(-1)^k + C_3k^2(-1)^k = (-1)^k(C_1+kC_2+k^2C_3)$, $C_1, C_2, C_3 \in \mathbb{R}$.

7. $x(k+2)-4x(k+1)+3x(k)=0$, $x(0)=10$, $x(1)=16$.

$\lambda^2-4\lambda+3=0$, $\lambda_1=1$, $\lambda_2=3$, $x_{oo} = C_1 \cdot 1^k + C_2 \cdot 3^k = C_1 + C_2 3^k$,

$$\begin{cases} x(0)=C_1+C_2=10, \\ x(1)=C_1+C_2 3=16, \end{cases} \quad \begin{cases} C_1=7, \\ C_2=3, \end{cases} \quad x(k) = 7+3 \cdot 3^k = 7+3^{k+1}.$$

8. $64x(k+8)+48x(k+6)+12x(k+4)+x(k+2)=0$,

$64\lambda^8+48\lambda^6+12\lambda^4+\lambda^2=0$, $\lambda^2((2\lambda)^2+1)^2(4\lambda^2+2\lambda+1)=0$,

$\lambda=0$, кратность 2,

$\lambda=\frac{1}{2}i=\frac{1}{2}e^{(\pi/2)i}=\frac{1}{2}\left(\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}\right)$, кратность 2, $\rho=\frac{1}{2}$, $\varphi=\frac{\pi}{2}$,

$\bar{\lambda}=-\frac{1}{2}i$, комплексно сопряженный корень, кратность 2,

$\lambda = -\frac{1}{4} + i\frac{\sqrt{3}}{4}$, кратность 1, $\rho = \sqrt{\frac{1}{16}+\frac{3}{16}} = \frac{1}{2}$,

$$\operatorname{tg}\varphi = \frac{y}{x} = \frac{\sqrt{3}/4}{-1/4} = -\sqrt{3}, \quad \varphi = \frac{\pi}{2} + \frac{\pi}{6} = \frac{2\pi}{3},$$

$\lambda=-\frac{1}{4}-i\frac{\sqrt{3}}{4}$, комплексно сопряженный корень, кратность 1,

$$x_{oo}=C_1 \cdot 0^k + C_2k \cdot 0^k + C_3\left(\frac{1}{2}\right)^k \cos\left(\frac{\pi}{2}k\right) + C_4\left(\frac{1}{2}\right)^k \sin\left(\frac{\pi}{2}k\right) + C_5k\left(\frac{1}{2}\right)^k \cos\left(\frac{\pi}{2}k\right) + C_6k\left(\frac{1}{2}\right)^k \sin\left(\frac{\pi}{2}k\right) + C_7\left(\frac{1}{2}\right)^k \cos\left(\frac{2\pi}{3}k\right) + C_8\left(\frac{1}{2}\right)^k \sin\left(\frac{2\pi}{3}k\right).$$

9. $x(k+1)-x(k)=k+1$, $x(0)=1$; $\lambda-1=0$, $\lambda=1$, $x_{oo}=C \cdot 1^k = C$,
$x_{он} = x_{чн} + x_{oo} = x_{чн} + C$, $f(k)=k+1=1^k(k+1)$,
$x_{чн}(k)=k(ak+b) \cdot 1^k$, $x_{чн}(k+1)=(k+1)(a(k+1)+b)$.

Подставляем $x_{чн}(k)$, $x_{чн}(k+1)$ в исходное уравнение:

$(k+1)(a(k+1)+b) - k(ak+b) = k+1,\ 2ak+(a+b)=k+1.$

Приравниваем коэффициенты при одинаковых степенях k:

$2a=1,\ a+b=1;\ a=1/2,\ b=1/2;\ x_{чн}(k)=\frac{k(k+1)}{2};\ x_{он}(k) =$

$x_{чн}(k)+C=\frac{k(k+1)}{2}+C,\ 1=x(0)=\frac{0(0+1)}{2}+C=C,\ C=1;\ x(k)=\frac{k(k+1)}{2}+1.$

Ответ. $x(k)=\frac{k(k+1)}{2}+1.$

10. $x(k+5)-6x(k+4)+9x(k+3) = 3k-1,\quad k=0,1,2,\ldots$
$x(0)=1, x(1)=0, x(2)=1,\ x(3)=3,\ x(4)=0.$

Характеристическое уравнение $\lambda^5-6\lambda^4+9\lambda^3=0,\ \lambda^3(\lambda^2-6\lambda+9)=0.$
Корни: $\lambda=0$ кратности 3, $\lambda=3$ кратности 2.
Переходим к эквивалентному уравнению

$y(k+2)-6y(k+1)+9y(k)=3(k-3)-1=3k-10,\ k=3,4,\ldots,$
$y(0)=1, y(1)=0, y(2)=1,\ y(3)=3, y(4)=0.$

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

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

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

Характеристическое уравнение $\lambda^2-6\lambda+9=0.$

Корень $\lambda=3$ кратности 2.

$z_{он}(k) = z_{чн}(k)+z_{оо}(k) = z_{чн}(k) + C_1\cdot 3^k+C_2k\cdot 3^k.$

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

$z(k+2)=a(k+2)+b=ak+2a+b.$ Подставляем $z(k), z(k+1), z(k+2)$

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

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

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

$z_{он}(k) = \frac{3k+2}{4} + C_1\cdot 3^k+C_2k\cdot 3^k.$ Находим $C_1,\ C_2.$

$$\begin{cases} z_{\text{он}}(0) = \dfrac{3\cdot 0+2}{4} + C_1\cdot 3^0+C_2\cdot 0\cdot 3^0 = \dfrac{2}{4} + C_1+C_2\cdot 0\cdot 3^0 = 3, \\ z_{\text{он}}(1) = \dfrac{3\cdot 1+2}{4} + C_1\cdot 3^1+C_2\cdot 1\cdot 3^1 = \dfrac{5}{4} + 3C_1+ 3C_2 = 0, \end{cases}$$

$$\begin{cases} C_1 = \dfrac{10}{4}, \\ 3C_1+3C_2 = -\dfrac{5}{4}, \end{cases} \qquad 3C_2 = -\frac{5}{4} - 3C_1 = -\frac{5}{4} - \frac{30}{4} = -\frac{35}{4},$$

$$C_1 = \frac{10}{4},\ C_2 = -\frac{35}{4\cdot 3},$$

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

Ответ. $x(0)=1, x(1)=0, x(2)=1,$

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

8. МОДУЛЯРНАЯ АРИФМЕТИКА

(Примеры решения)

Задача 1. Даны целые числа a=321 и b=11. Найти целые q_1, q_2, r_1, r_2, $0 \leqslant r_1, r_2 < b$, для которых $a=bq_1+r_1$, $-a=bq_2+r_2$.

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

Задача 2. Записать числа в восьмеричной, шестнадцатеричной, десятиричной системах счисления.

Решение. $n=11\,101\,110\,010\,101_2 = 35625_8$.
$n=11\,1111\,1101\,0101_2 = 3FD5_{16}$.
$n=(d_{k-1}d_{k-2}\ldots d_1d_0)_b=d_{k-1}b^{k-1}+d_{k-2}b^{k-2}+\ldots+d_1b+d_0$.
$n = 11001001_2 =$
$1 \cdot 2^7+1 \cdot 2^6+0 \cdot 2^5+0 \cdot 2^4+1 \cdot 2^3+0 \cdot 2^2+0 \cdot 2+1 = 201_{10}$.

Задача 3. Записать десятиричные числа 160 и 199 в семиричной и двоичной системах счисления.

8.1. Алгоритм вычисления h-ричной записи десятеричного числа a

ВХОД. Натуральные числа $a>0$ и $h \geqslant 2$.
ВЫХОД. h-ричная запись числа $a=(a_ta_{t-1}\ldots a_1a_0)_h$.
1. $i := 0$.
2. Пока $q \neq 0$, выполнять следующее.
   2.1. $r := \mathrm{mod}(a,h)$, $q := (a-r)/h$.
   2.2. $a := q$, $a_i := r$.
   2.3. $i := i+1$.
3. Вернуть a.

Решение. По основанию h число $a_{10} = (a_ta_{t-1}\ldots a_1a_0)_h$.
$i := 0$, $a := 160$,
$r:=\mathrm{mod}(a,h)=\mathrm{mod}(160,7) = 6$, $q:=(a-r)/h=(160-6)/7 = 22$,
$a := q = 22$, $a_0 := r = 6$, $i := i+1 = 0+1 = 1$;
$r := \mathrm{mod}(a,h)=\mathrm{mod}(22,7)=1$, $q := (a-r)/h=(22-1)/7=3$,
$a := q = 3$, $a_1 := r = 1$, $i := i+1 = 1+1 = 2$.
$r := \mathrm{mod}(a,h)=\mathrm{mod}(3,7)=3$; $q := (a-r)/h=(3-3)/7=0$.
$a := q = 0$, $a_2 := r = 3$, $i := i+1 = 2+1 = 3$.

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

Таблица 7.1

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

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

Таблица 7.2

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

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

Таблица 7.3

h=7, $a = 160_{10} = 10100000_2$

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

Таблица 7.4

h=7, $a = 160_{10} = 10100000_2$

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. Написать таблицы сложения и умножения и перемножить числа $(160)_{10}$ и $(199)_{10}$ в системе счисления по основанию семь. (Таблицы 7.5 и 7.6).

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

$$\begin{array}{r} 316 \\ \times\ 403 \\ \hline 1254 \\ 1603 \\ \hline 161554 \end{array}$$

Таблица 7.5

$+_7$	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

Таблица 7.6

$\times_7$	0	1	2	3	4	5	6
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

Задача 5. В двоичной системе счисления разделить число $n=11001001_2$ на число $m=100111_2$.

Решение.

$$\begin{array}{l} 11001001 \;\big|\, 100111 \\ \underline{100111} \quad\;\; 101 \\ 101101 \\ \underline{100111} \\ 110 \end{array} \qquad 101\,\frac{110}{100111}$$

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

Задача 6. Найти число цифр в числе 8735284215_{10} по основаниям 2,3,5,7,8,12,16.

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

b	2	3	5	7	8	12	16
k	34	21	15	12	12	10	9

Задача 7. Разложить число $n=1728720$ на простые множители и найти число делителей $f(n)$ числа n.

Решение. 1728720 = 2*864360, 864360 = 2*432180, 432180 = 2*216090, 216090 = 2*108045, 108045 = 3*36015, 36015 = 3*12005, 12005 = 5*2401, 2401 = 7*343, 343 = 7*49, 49 = 7*7, 7 = 7*1, $n = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^4$.

Число $p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ имеет $(a_1+1)(a_2+1)\ldots(a_r+1)$ различных делителей.

$f(n) = 5 \cdot 3 \cdot 2 \cdot 5 = 150$.

8.2. Тест Соловэя–Штрассена для простоты числа

ВХОД. Нечетное целое $n \geqslant 3$ и параметр безопасности $t \geqslant 1$.

ВЫХОД. Ответ "простое" или "составное" на вопрос: "Является ли n простым числом?"

1. Для i от 1 до t выполнить следующее.
   1.1. Выбрать случайное целое a, $2 \leqslant a \leqslant n-2$.
   1.2. Вычислить $r = a^{(n-1)/2} \pmod{n}$.
   1.3. Если $r \neq 1$ и $r \neq n-1$, то вернуть "составное".
   1.4. Вычислить символ Якоби $s = \left(\frac{a}{n}\right)$.
   1.5. Если $r \not\equiv s \pmod{n}$, то вернуть "составное".
2. Вернуть "простое".

Замечание. Вероятность получить неверный ответ для целого положительного n меньше $(1/2)^t$.

8.3. Тест Миллера–Рабина для простоты числа

ВХОД. Нечетное целое $n \geqslant 3$ и параметр безопасности $t \geqslant 1$.

ВЫХОД. Ответ "простое" или "составное" на вопрос: "Является ли n простым числом?"

1. Найти s и нечетное r, для которых $n-1 = 2^s r$.
2. Для i от 1 до t выполнить следующее.
   2.1. Выбрать случайное целое a, $2 \leqslant a \leqslant n-1$.
   2.2. Вычислить $y = a^r \pmod{n}$.
   2.3. Если $y \neq 1$ и $y \neq n-1$, то выполнить следующее.
   $j := 1$.
   Пока $j \leqslant s-1$ и $y \neq n-1$, выполнить следующее.
   Вычислить $y := y^2 \pmod{n}$.
   Если $y = 1$, то вернуть "составное".
   $j := j+1$.
   Если $y \neq n-1$, то вернуть "составное".
3. Вернуть "простое".

Замечание. Вероятность получить неверный ответ для целого положительного n меньше $(1/4)^t$.

Задача 8. Найти наибольший общий делитель d и наименьшее общее кратное чисел a=1547 и b=560. Найти такие целые u и v, для которых $d = au+bv$.

Решение. Для поиска d,u,v алгоритм Евклида можно расширить следующим образом.

$1547 = 560\cdot 2 + 427$, остаток $r=427$,
$560 = 427\cdot 1 + 133$, остаток $r=133$,
$427 = 133\cdot 3 + 28$, остаток $r=28$,
$133 = 28\cdot 4 + 21$, остаток $r=21$,
$28 = 21\cdot 1 + 7$, остаток $r=7$,
$21 = 7\cdot 3 + 0$, остаток $r=0$.
$d = (1547,560) = 7$.

Отсюда последовательно находим:

$$427 = 1547-560\cdot 2;$$

$$133 = 560-427\cdot 1 = 560-\underbrace{(1547-560\cdot 2)}_{427}\cdot 1 = -1547 + 560\cdot 3;$$

$$28 = 427-133\cdot 3 = \underbrace{(1547-560\cdot 2)}_{427} - \underbrace{(-1547+560\cdot 3)}_{133}\cdot 3 =$$

$$1547\cdot 4 - 560\cdot 11;$$

$$21 = 133-28\cdot 4 = \underbrace{(-1547+560\cdot 3)}_{133} - \underbrace{(1547\cdot 4-560\cdot 11)}_{28}\cdot 4 =$$

$$-1547\cdot 17 + 560\cdot 47,$$

$$d = 7 = 28-21\cdot 1 = \underbrace{(1547\cdot 4-560\cdot 11)}_{28} - \underbrace{(-1547\cdot 17+560\cdot 47)}_{21}\cdot 1 =$$

$1547\cdot 21 + 560\cdot(-58)$. Найдено: $d=7$, $u=21$, $v=-58$.

$$M = [a,b] = \frac{a\cdot b}{(a,b)} = \frac{1547\cdot 560}{(1547,560)} = \frac{1547\cdot 560}{7} = 123760.$$

Ответ. $d=7$, $u=21$, $v=-58$, $M=123760$.

В общем виде расширенный алгоритм Евклида можно описать следующим образом.

$a = bq_1 + r_2$, $0<r_2<b$, $q_1=\lfloor a/b\rfloor$, $r_2=a-bq_1$,
$b = r_2q_2 + r_3$, $0<r_3<r_2$, $q_2=\lfloor b/r_2\rfloor$, $r_3=b-r_2q_2$,
$r_2 = r_3q_3 + r_4$, $0<r_4<r_3$, $q_3=\lfloor r_2/r_3\rfloor$, $r_4=r_2-r_3q_3$,
$r_3 = r_4q_4 + r_5$, $0<r_5<r_3$, $q_4=\lfloor r_3/r_4\rfloor$, $r_5=r_3-r_4q_4$,
...
$r_{n-2}=r_{n-1}q_{n-1}+r_n$, $q_{n-1}=\lfloor r_{n-2}/r_{n-1}\rfloor$, $r_n=r_{n-2}-r_{n-1}q_{n-1}$,
$r_{n-1} = r_nq_n$ (here $r_{n+1}=0$), $d=r_n$.

Тогда

$r_2=a-bq_1=a\cdot 1+b(-q_1)=au_1+bv_1$, $u_1=1$, $v_1=-q_1$,
$r_3=b-r_2q_2=b-(au_1+bv_1)=b(1-v_1)+a(-u_1)=au_2+bv_2$,
$u_2=1-v_1$, $v_2=-u_1$,

$r_4=r_2-r_3q_3=(au_1+bv_1)-(au_2+bv_2)q_3=a(u_1-u_2q_3)+b(v_1-v_2q_3)=$
au_3+bv_3, $u_3=u_1-u_2q_3$, $v_3=v_1-v_2q_3$,
$r_5=r_3-r_4q_4=(au_2+bv_2)-(au_3+bv_3)q_3=a(u_2-u_3q_4)+b(v_2-v_3q_4)=$
au_4+bv_4, $u_4=u_2-u_3q_4$, $v_4=v_2-v_3q_4$,
...
$d=r_n=r_{n-2}-r_{n-1}q_{n-1}=(au_{n-3}+bv_{n-3})-(au_{n-2}+bv_{n-2})q_{n-1}=$
$a(u_{n-3}-u_{n-2}q_{n-1})+b(v_{n-3}-v_{n-2}q_{n-1})=$
$au_{n-1}+bv_{n-1}$, $u_{n-1}=u_{n-3}-u_{n-2}q_{n-1}$, $v_{n-1}=v_{n-3}-v_{n-2}q_{n-1}$,
Получили: $d=r_n$, $u=u_{n-1}$, $v=v_{n-1}$.

8.4. Алгоритм Евклида нахождения нод(a,b), $a\geq b$

ВХОД. Натуральные числа a и b, $a\geq b$.
ВЫХОД. нод(a,b).

1. Пока $b\neq 0$, выполнять следующее.
   $q:=\lfloor a/b\rfloor$, $r:=a-qb$, $a:=b$, $b:=r$.
2. Вернуть a.

*8.5. Расширенный алгоритм Евклида нахождения d=*нод(a,b) *и тех целых чисел u,v, для которых $d=au+bv$*

ВХОД. Натуральные числа a и b, $a\geq b$.
ВЫХОД. d=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. $q:=\lfloor a/b\rfloor$, $r:=a-qb$, $u:=u_2-q\cdot u_1$, $v:=v_2-q\cdot v_1$.
   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).

Пример. Найти d=нод(a,b) и те u,v, для которых $d=au+bv$. Числа a=4864, b=3458.

Решение. Результаты вычислений заносим в табл.7.7, откуда d=нод(a,b)=нод(4864,3458)=38, u=32, v=−45

Задача 9. Найти непрерывную и подходящие дроби для числа a/b, $a>b$; a=105, b=38.

Решение. $105 = 38\cdot 2 + 29$, $q_1=2$,
$38 = 29\cdot 1 + 9$, $q_2=1$,
$29 = 9\cdot 3 + 2$, $q_3=3$,
$9 = 2\cdot 4 + 1$, $q_4=4$,
$2 = 1\cdot 2$, $q_5=2$.

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

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	38	0	32	−91	−45	128

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 δ_s:

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

8.6. Алгоритм вычисления подходящих дробей

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

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

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

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

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

$$\begin{cases} P_3=q_3P_2+P_1=3\cdot 3+2=11, \\ Q_3=q_3Q_2+Q_1=3\cdot 1+1=4, \end{cases} \qquad \delta_3 = \frac{P_3}{Q_3} = \frac{11}{4},$$

$$\begin{cases} P_4=q_4P_3+P_2=4\cdot 11+3=47, \\ Q_4=q_4Q_3+Q_2=4\cdot 4+1=17, \end{cases} \qquad \delta_4 = \frac{P_4}{Q_4} = \frac{47}{17},$$

$$\begin{cases} P_5=q_5P_4+P_3=2\cdot 47+11=105, \\ Q_5=q_5Q_4+Q_3=2\cdot 17+4=38, \end{cases} \qquad \delta_5 = \frac{P_5}{Q_5} = \frac{105}{38}.$$

Задача 10. Написать неотрицательную наименьшую полную, наименьшую по модулю, неотрицательную наименьшую 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 $\varphi(n)$. 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, если он существует.

Решение. Полная система вычетов:

$\mathbb{Z}_{15}=\{0,1,2,3,4,5,\ldots,14\}$.

Наименьшая по модулю система вычетов:

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

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

Сложение по модулю 15 для полной системы вычетов $\mathbb{Z}_{15}$ приведено в табл.7.9.

Умножение по модулю 15 для полной системы вычетов $\mathbb{Z}_{15}$ приведено в табл.7.10.

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

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

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

n=15=$3^1\cdot 5^1$. Функция Эйлера для числа $n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ есть $\varphi(n) = (p_1^{a_1}-p_1^{a_1-1})(p_2^{a_2}-p_2^{a_2-1})\ldots(p_k^{a_k}-p_k^{a_k-1})$.

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

Ниже указаны Обратные элементы по модулю 15 для системы вычетов $\mathbb{Z}_{15}-\{0\}$. (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

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

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

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

1. Найти d=нод(a,n) и те целые x и y, для которых $ax+ny=d$ (то есть $ax \equiv d \pmod n$).
2. Если $d>1$, то $a^{-1} \pmod n$ не существует. Иначе $a^{-1}=x$.

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

1. $b := a$, $k := 1$.
3. Пока $b>1$ и $k \leqslant p-1$ выполнить следующее.
   3.1. $b := b \cdot a \pmod p$, (остаток от деления $b \cdot a$ на p).
   3.2. $k := k+1$.
4. Если $b>1$ то порядок $\mathrm{ord}(a)$ 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. Случайным образом выбрать в $\mathbb{Z}_p^*$ элемент a.
2. $b := a$, $k := 1$.
3. Пока $b \neq 1$ и $k \leqslant p$ выполнить следующее.
   3.1. $b := b \cdot a \pmod p$, (остаток от деления $b \cdot a$ на p).
   3.2. $k := k+1$.
4. Если $b=1$ и $k=p-1$, то вернуть a. Иначе перейти к пункту 1.

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

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

Таблица 7.11

Сложение

$+_{15}$	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

Умножение

$\times_{15}$	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

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	1	
5			3		5	6			9	10		12		
6			9		10	6			6	10		9		
7			12		5	6			9	10		3		
8			6		10	6			6	10		6		
ord(a)	1	4	–	2	–	–	4	4	–	–	2	–	4	2

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

Задача 11. Найти степень $5^{596} \pmod{1234}$.

Решение. Если $k = k_t k_{t-1} \ldots k_1 k_0 = \sum_{i=0}^{t} k_i 2^i$ есть двоичное представление числа k, то $a^k = a^{\sum_{i=0}^{t} k_i 2^i} =$

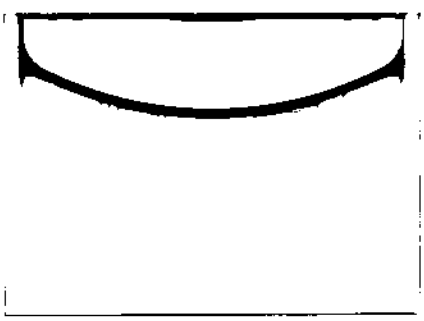
$a^{k_0 2^0 + k_1 2^1 + \ldots + k_t 2^t} = a^{k_0 2^0} \cdot a^{k_1 2^1} \cdot \ldots \cdot a^{k_t 2^t} =$

$= (a^{2^0})^{k_0} (a^{2^1})^{k_1} \ldots (a^{2^t})^{k_t} = \prod_{i=0}^{t} a^{k_i 2^i}$.

8.10. Алгоритм модулярной степени натурального числа

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 $a^k = 5^{596} \pmod{1234}$,
$a=5$, $k = 596_{10} = (k_9k_8\ldots k_1k_0)_2 = 1001010100_2$.
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) 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 $0,1,\ldots,6$ 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 $0,1,\ldots,10$ 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	6	1	6	5

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

Задача 13. Решить (подбором) систему из двух сравнений с одним неизвестным.

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

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 $0,1,\ldots,8$ по модулю 9 обоим сравнениям удовлетворяют числа $x=4$, $x=7$. Система имеет два решения: $x \equiv 4 \pmod 9$, $x \equiv 7 \pmod 9$.

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

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
$g(x) \pmod 4$	2	1	0	3	2	1	0	3	2	1	0	3

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

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

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

$f(x,y)$

$x\backslash y$	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

$g(x,y)$

$x\backslash y$	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

$f(x,y) \pmod 6$

$x\backslash y$	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

$g(x,y) \pmod 3$

$x\backslash y$	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), $0 \leqslant a,b \leqslant 5$, 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 систему сравнений (методом Гаусса).

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

$c_1=1$, $c_2=3$, $c_3=2$.

$m_1=4$, $m_2=5$, $m_3=7$ попарно взаимно просты. Система совместна.

Решение. $M=m_1m_2m_3=4 \cdot 5 \cdot 7=140$,
$M_1=m_2m_3=5 \cdot 7=35$, $M_2=m_1m_3=4 \cdot 7=28$, $M_3=m_1m_2=4 \cdot 5=20$. Сравнения $M_1N_1 \equiv 1 \pmod{m_1}$, $M_2N_2 \equiv 1 \pmod{m_2}$, $M_3N_3 \equiv 1 \pmod{m_3}$ есть $35N_1 \equiv 1 \pmod 4$, $28N_2 \equiv 1 \pmod 5$, $20N_3 \equiv 1 \pmod 7$ и им удовлетворяют числа $N_1=3$, $N_2=2$, $N_3=6$. Тогда $x_0=M_1N_1c_1+M_2N_2c_2+M_3N_3c_3=35 \cdot 3 \cdot 1+28 \cdot 2 \cdot 3+20 \cdot 6 \cdot 2=513$.
Решение $x \equiv 513 \pmod{140}$ or $x \equiv 93 \pmod{140}$.

Ответ. $x \equiv 93 \pmod{140}$.

8.11. Алгоритм Гаусса для системы сравнений $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots \\ x \equiv c_k \pmod{m_k} \end{cases}$

с попарно взаимно простыми модулями

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

где $M=m_1 m_2 \dots m_k$, $M_i=M/m_i$, $N_i \equiv M_i^{-1} \pmod{m_i}$, $i=1,2,\dots,k$.

Задача 16. Решить систему сравнений $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 5 \pmod 9, \\ x \equiv 11 \pmod{15}. \end{cases}$

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

$x=5+9t \equiv 2 \pmod 7$, $9t \equiv -3 \pmod 7$, $9t-7t \equiv -3 \pmod 7$, $2t \equiv -3 \pmod 7$, $2t \equiv -3+7 \pmod 7$, $2t \equiv 4 \pmod 7$, $t \equiv 2 \pmod 7$, $t=2+7y$, $x=5+9t=5+9(2+7y)=23+63y \equiv 23 \pmod{63}$. Исходная система эквивалентна системе $\begin{cases} x \equiv 23 \pmod{63}, \\ x \equiv 11 \pmod{15}. \end{cases}$ Здесь $d=(63,15)=3$ и $3 \mid (23-11)$, поэтому система совместна. Тогда $x=23+63y \equiv 11 \pmod{15}$, $63y-15y \cdot 4 \equiv -12 \pmod{15}$, $3y \equiv 3 \pmod{15}$, $y \equiv 1 \pmod 5$, $y=1+5z$, $x=23+63(1+5z)=86+315z$. *Ответ.* $x \equiv 86 \pmod{315}$.

Задача 17. Решить систему сравнений $\begin{cases} 7x \equiv 3 \pmod{11}, \\ 15x \equiv 5 \pmod{35}, \\ 3x \equiv 2 \pmod 5. \end{cases}$

Решение. Сравнение $15x \equiv 5 \pmod{35}$ эквивалентно сравнению $3x \equiv 1 \pmod 7$.

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

$c_1=2$, $c_2=5$, $c_3=4$, $m_1=11$, $m_2=7$, $m_3=5$, $M=m_1 m_2 m_3=11 \cdot 7 \cdot 5=385$, $M_1=7 \cdot 5=35$, $M_2=11 \cdot 5=55$, $M_3=11 \cdot 7=77$. Сравнения $M_1 N_1 \equiv 1 \pmod{m_1}$, $M_2 N_2 \equiv 1 \pmod{m_2}$, $M_3 N_3 \equiv 1 \pmod{m_3}$ are $35N_1 \equiv 1 \pmod{11}$, $55N_2 \equiv 1 \pmod 7$, $77N_3 \equiv 1 \pmod 5$ or $2N_1 \equiv 1 \pmod{11}$, $6N_2 \equiv 1 \pmod 7$, $7N_3 \equiv 1 \pmod 5$, которым

удовлетворяют $N_1=6$, $N_2=-1$, $N_3=3$. Тогда

$x_0=M_1N_1c_1+M_2N_2c_2+M_3N_3c_3=35\cdot 6\cdot 2-55\cdot 1\cdot 5+77\cdot 3\cdot 4=1069.$

Решение $x\equiv 1069 \pmod{385}$ или $x\equiv 299 \pmod{385}$.

Ответ. $x\equiv 299 \pmod{385}$.

Задача 18. Определить, имеет ли решение сравнение $x^2\equiv a \pmod p$.

Пусть p есть нечетное простое число и a есть некоторое целое число. Символ Лежандра

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } p\mid a,\\ 1, & \text{если } a \text{ есть квадратичный вычет по mod } p,\\ -1, & \text{если } a \text{ есть квадратичный невычет по mod } p,\end{cases}$$

$$= \begin{cases} 0, & \text{если } p\mid a,\\ 1, & \text{если сравнение } x^2\equiv a \pmod p \text{ имеет (два)решения},\\ -1, & \text{если сравнение } x^2\equiv a \pmod p \text{ не имеет решений},\end{cases}$$

$$= \begin{cases} 0, & \text{если } p\mid a,\\ 1, & \text{если существует } x=\sqrt{a} \pmod p,\\ -1, & \text{если не существует } x=\sqrt{a} \pmod p.\end{cases}$$

Свойства символа Лежандра.

(1) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.

$\left(\frac{1}{p}\right)=1$, ибо $x^2\equiv 1 \pmod p$ имеет решения $x=1$, $x=-1$.

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

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$. Если $a\in\mathbb{Z}_p^*$, то $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$.

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

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

(5) Если q есть нечетное простое число и $q\neq p$, то справед-

лив закон взаимности $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{(p-1)(q-1)/4}$.

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

$$\left(\frac{68}{113}\right) = \left(\frac{2^2 \cdot 17}{113}\right) \underset{(2)}{=} \left(\frac{2^2}{113}\right)\left(\frac{17}{113}\right) \underset{(2,5)}{=}$$

$$1 \cdot \left(\frac{113}{17}\right)(-1)^{(17-1)(113-1)/4} = \left(\frac{113}{17}\right) \underset{(3)}{=} \left[113 \equiv 11 \pmod{17}\right] =$$

$$\left(\frac{11}{17}\right) \underset{(5)}{=} \left(\frac{17}{11}\right)(-1)^{(11-1)(17-1)/4} = \left(\frac{17}{11}\right) = \left[17 \equiv 6 \pmod{11}\right] \underset{(3)}{=}$$

$$\left(\frac{6}{11}\right) = \left(\frac{2 \cdot 3}{11}\right) \underset{(2)}{=} \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \underset{(4)}{=} (-1)^{(11^2-1)/8} \cdot \left(\frac{3}{11}\right) \underset{(5)}{=}$$

$$-1 \cdot \left(\frac{11}{3}\right)(-1)^{(3-1)(11-1)/4} = \left(\frac{11}{3}\right) = \left[11 \equiv 2 \pmod{3}\right] \underset{(3)}{=}$$

$$\left(\frac{2}{3}\right) \underset{(4)}{=} (-1)^{(3^2-1)/8} = -1.$$

Ответ. Сравнение не имеет решений.

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

$$\left(\frac{310}{521}\right) = \left(\frac{2 \cdot 5 \cdot 31}{521}\right) \underset{(2)}{=} \left(\frac{2}{521}\right)\left(\frac{5}{521}\right)\left(\frac{31}{521}\right) \underset{(4)}{=}$$

$$(-1)^{(521^2-1)/8} \cdot \left(\frac{5}{521}\right)\left(\frac{31}{521}\right) \underset{(5)}{=}$$

$$\left(\frac{521}{5}\right)(-1)^{(5-1)(521-1)/4} \cdot \left(\frac{521}{31}\right)(-1)^{(31-1)(521-1)/4} =$$

$$\left(\frac{521}{5}\right)\left(\frac{521}{31}\right) = \left[\begin{matrix}521 \equiv 1 \pmod 5 \\ 521 \equiv 25 \pmod{31}\end{matrix}\right] \underset{(3)}{=} \left(\frac{1}{5}\right)\left(\frac{25}{31}\right) \underset{(1)}{=} \left(\frac{5^2}{31}\right) \underset{(2)}{=} 1.$$

Ответ. Сравнение имеет два решения.

3. $x^2 \equiv -174 \pmod{619}$. *Решение*. Символ Лежандра

$$\left(\frac{-174}{619}\right) = \left(\frac{-1}{619}\right)\left(\frac{2}{619}\right)\left(\frac{3}{619}\right)\left(\frac{29}{619}\right) \underset{(1,2)}{=}$$

$$-\left(\frac{2}{619}\right)\left(\frac{3}{619}\right)\left(\frac{29}{619}\right) \underset{(4,5)}{=} -(-1)^{(619^2-1)/8} \cdot$$

$$\left(\frac{619}{3}\right)(-1)^{(3-1)(619-1)/4} \cdot \left(\frac{619}{29}\right)(-1)^{(29-1)(619-1)/4} =$$

$$-(-1)(-1)\cdot 1\cdot \left(\frac{619}{3}\right)\left(\frac{619}{29}\right) \underset{(3)}{=} \left[\begin{matrix}619\equiv 1 \pmod 3\\ 619\equiv 10 \pmod{29}\end{matrix}\right] =$$

$$-\left(\frac{1}{3}\right)\left(\frac{10}{29}\right) \underset{(1)}{=} -\left(\frac{2\cdot 5}{29}\right) \underset{(3)}{=} -\left(\frac{2}{29}\right)\left(\frac{5}{29}\right) \underset{(4,5)}{=}$$

$$-(-1)^{(29^2-1)/8}\cdot \left(\frac{29}{5}\right)(-1)^{(5-1)(29-1)/4} =$$

$$\left(\frac{29}{5}\right) = \left[29\equiv 4 \pmod 5\right] \underset{(3)}{=} \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) \underset{(2)}{=} 1.$$

Ответ. Сравнение имеет два решения.

Задача 19. Определить, имеет ли решение сравнение $x^2\equiv a \pmod p$. Вычислять символ Лежандра $\left(\frac{a}{p}\right)$, рассматривая его как символ Якоби.

Пусть $n=p_1^{e_1}p_2^{e_2}\dots p_s^{e_s}\geqslant 3$, где p_i есть простые числа, среди которых могут быть одинаковые. Символ Якоби $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\dots\left(\frac{a}{p_s}\right)^{e_s}$, где $\left(\frac{a}{p_i}\right)$, $i=1,2,\dots,s$, есть символы Лежандра. (Символ Якоби вычисляется быстрее символа Лежандра.)

Свойства символа Якоби. Пусть $m\geqslant 3$, $n\geqslant 3$ и $a,b\in\mathbb{Z}$.

(1) $\left(\frac{a}{n}\right) = 0,1$ или -1. $\left(\frac{a}{n}\right)=0 \longleftrightarrow$ нод$(a,n)\neq 1$.

(2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. Если $a\in\mathbb{Z}_n^*$, то $\left(\frac{a^2}{n}\right)=1$.

(3) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

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

(5) $\left(\frac{1}{n}\right) = 1$.

(6) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$. $\left(\frac{-1}{n}\right) = \begin{cases}1, & \text{если } n\equiv 1 \pmod 4,\\ -1, & \text{если } n\equiv 3 \pmod 4.\end{cases}$

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

(8) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$.

(9) Если $a = 2^e b$, где b нечетно, то

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{n \pmod b}{b}\right)(-1)^{(b-1)(n-1)/4}.$$

1. $x^2 \equiv 506 \pmod{1103}$. *Решение.* Символ Якоби

$$\left(\frac{506}{1103}\right) = \left(\frac{2 \cdot 253}{1103}\right) \underset{(2)}{=} \left(\frac{2}{1103}\right)\left(\frac{253}{1103}\right) \underset{(7,8)}{=}$$

$$(-1)^{(1103^2-1)/8} \cdot \left(\frac{1103}{253}\right)(-1)^{(253-1)(1103-1)/4} =$$

$$1 \cdot 1 \cdot \left(\frac{1103}{253}\right) = \lceil 1103 \equiv 91 \pmod{253} \rceil \underset{(4)}{=} \left(\frac{91}{253}\right) \underset{(8)}{=}$$

$$\left(\frac{253}{91}\right)(-1)^{(91-1)(253-1)/4} = \left(\frac{253}{91}\right) \underset{(4)}{=} \lceil 253 \equiv -20 \pmod{91} \rceil =$$

$$\left(\frac{-20}{91}\right) = \left(\frac{-1}{91}\right)\left(\frac{20}{91}\right) \underset{(2,6)}{=} (-1)^{(91-1)/2} \cdot \left(\frac{2^2}{91}\right)\left(\frac{5}{91}\right) \underset{(2,8)}{=}$$

$$(-1) \cdot 1 \cdot \left(\frac{91}{5}\right)(-1)^{(5-1)(91-1)/4} = -\left(\frac{91}{5}\right) \underset{(4)}{=} \lceil 91 \equiv 1 \pmod 5 \rceil =$$

$$-\left(\frac{1}{5}\right) = -1. \quad \textit{Ответ.}$$ Сравнение не имеет решений.

2. $x^2 \equiv 903 \pmod{2111}$. *Решение.* Символ Якоби

$$\left(\frac{903}{2111}\right) \underset{(8)}{=} \left(\frac{2111}{903}\right)(-1)^{(903-1)(2111-1)/4} =$$

$$-\left(\frac{2111}{903}\right) = \lceil 2111 \equiv 305 \pmod{903} \rceil \underset{(4)}{=} -\left(\frac{305}{903}\right) \underset{(8)}{=}$$

$$-\left(\frac{903}{305}\right)(-1)^{(305-1)(903-1)/4} = -\left(\frac{903}{305}\right) \underset{(4)}{=} \lceil 903 \equiv -12 \pmod{305} \rceil =$$

$$-\left(\frac{-12}{305}\right) = -\left(\frac{-1}{305}\right)\left(\frac{12}{305}\right) \underset{(6)}{=} -(-1)^{(305-1)/2}\left(\frac{2^2 \cdot 3}{305}\right) \underset{(2)}{=}$$

$$-\left(\frac{2^2}{305}\right)\left(\frac{3}{305}\right) \underset{(2)}{=} -\left(\frac{3}{305}\right) \underset{(8)}{=} -\left(\frac{305}{3}\right)(-1)^{(3-1)(305-1)/4} =$$

$$-\left(\frac{305}{3}\right) \underset{(4)}{=} \lceil 305 \equiv 2 \pmod 3 \rceil = -\left(\frac{2}{3}\right) = -(-1)^{(3^2-1)/8} = 1.$$

Ответ. Сравнение имеет два решения.

8.12. Алгоритм вычисления символа Якоби (и Лежандра)

JACOBI(a,n)

ВХОД. Нечетное целое число $n \geqslant 3$ и число a, $0 \leqslant a < n$.

ВЫХОД. Символ Якоби $\left(\frac{a}{n}\right)$ (и следовательно символ Лежандра если число n просто).

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 $s := 1$, если $n \equiv 1$ или $7 \pmod 8$, или $s := -1$, если $n \equiv 3$ 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 $s \cdot$ JACOBI(n_1, a_1).

Задача 20. Полиномы $f(x), h(x) \in \mathbb{Z}_p[x]$, $p=5$. Найти их наибольший общий делитель $d(x) = \text{нод}(f(x), h(x))$ и два полинома $u(x), v(x) \in \mathbb{Z}_p[x]$, для которых $d(x) = u(x)f(x) + v(x)h(x)$.

8.13. Алгоритм Евклида для $\mathbb{Z}_p[x]$

ВХОД. Два полинома $f(x), h(x) \in \mathbb{Z}_p[x]$.
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 $f(x)$.

8.14. Расширенный алгоритм Евклида для $\mathbb{Z}_p[x]$

ВХОД. Два полинома $f(x), h(x) \in \mathbb{Z}_p[x]$.
ВЫХОД. $d(x) = \text{нод}(f(x), h(x))$ и два полинома $u(x), v(x) \in$

$\mathbb{Z}_p[x]$, для которых $d(x) = f(x)u(x) + h(x)v(x)$.

1. Если $h = 0$, то $d:=f$, $u:=1$, $v:=0$, вернуть (d,u,v).
2. $u_2:=1$, $u_1:=0$, $v_2:=0$, $v_1:=1$.
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 $d(x)$, 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 $\mathbb{Z}_2[x]$). 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 $d(x)$=нод$(f(x), h(x))$ и полиномы $u(x),v(x) \in \mathbb{Z}_2[x]$, для которых

$d(x) = f(x)u(x) + h(x)v(x)$.

Решение.

Исходное присваивание.

$u_2(x) := 1$, $u_1(x) := 0$, $v_2(x) := 0$, $v_1(x) := 1$.

Итерация 1.

$q(x) := \lfloor f(x)/h(x) \rfloor = x+1$,
$r(x) := f(x)-h(x)q(x) = x^8+x^7+x^6+x^2+x$,
$u(x) := u_2(x)-q(x)u_1(x)=1$, $v(x) := v_2(x)-q(x)v_1(x)=x+1$,
$f(x) := h(x)=x^9+x^6+x^5+x^3+x^2+1$, $h(x) := r(x)=x^8+x^7+x^6+x^2+1$,
$u_2(x) := u_1(x)=0$, $u_1(x) := u(x)=1$,
$v_2(x) := v_1(x)=1$, $v_1(x) := v(x)=x+1$.

Итерация 2.

$q(x) := \lfloor f(x)/h(x) \rfloor = x+1$,
$r(x) := f(x)-h(x)q(x) = x^5+x^2+x+1$,
$u(x) := x+1$, $v(x) := x^2$,
$f(x) := h(x) = x^8+x^7+x^6+x^2+1$, $h(x) := r(x) = x^5+x^2+x+1$,
$u_2(x) := u_1(x) = 1$, $u_1(x) := u(x) = x+1$,
$v_2(x) := v_1(x) = x+1$, $v_1(x) := v(x) = x^2$.

Итерация 3.

$q(x) := \lfloor f(x)/h(x) \rfloor = x^3+x^2+x+1$,
$r(x) := f(x)-h(x)q(x) = x^3+x+1$,
$u(x) := x^4$, $v(x) := x^5+x^4+x^3+x^2+x+1$,
$f(x) := h(x) = x^5+x^2+x+1$, $h(x) := r(x) = x^3+x+1$,

$u_2(x) := u_1(x) = x+1,\ u_1(x) := u(x) = x^4,$
$v_2(x) := v_1(x) = x^2,\ v_1(x) := v(x) = x^5+x^4+x^3+x^2+x+1.$

Итерация 4.

$q(x) := \lfloor f(x)/h(x) \rfloor = x^2+1,\ r(x) := f(x)-h(x)q(x) = 0,$
$u(x) := x^6+x^4+x+1,\ v(x) := x^7+x^6+x^2+x+1,$
$f(x) := h(x) = x^3+x+1,\ h(x) := r(x) = 0,$
$u_2(x) := u_1(x) = x^4,\ u_1(x) := u(x) = x^6+x^4+x+1,$
$v_2(x) := v_1(x) = x^5+x^4+x^3+x^2+x+1,\ v_1(x) := v(x) = x^7+x^6+x^2+x+1.$
Ответ. $d(x) = \gcd(f(x),h(x)) = x^3+x+1,$
$u(x)=x^4,\ v(x)=x^5+x^4+x^3+x^2+x+1.$

Пример 2. (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 $d(x)=$нод$(f(x), h(x))$ и полиномы $u(x),v(x) \in \mathbb{Z}_5[x]$, для которых
$d(x) = f(x)u(x) + h(x)v(x).$

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.

$q(x):=\lfloor f(x)/h(x) \rfloor = \lfloor (4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4)/$
$(3x^7+x^6+4x^4+3x^3+x^2+4x+4) \rfloor = 3x,$
$r(x):=f(x)-h(x)q(x)=4x^6+4x^3+2x^2+x+4,$
$u(x):=u_2(x)-q(x)u_1(x)=1,\ v(x):=v_2(x)-q(x)v_1(x)=-3x=2x,$
$f(x):=h(x)=3x^7+x^6+4x^4+3x^3+x^2+4x+4,$
$h(x):=r(x)=4x^6+4x^3+2x^2+x+4,$
$u_2(x):=u_1(x)=0,\ u_1(x):=u(x)=1,$
$v_2(x):=v_1(x)=1,\ v_1(x):=v(x)=-3x=2x.$

Итерация 2.

$q(x):=\lfloor f(x)/h(x) \rfloor = \lfloor (3x^7+x^6+4x^4+3x^3+x^2+4x+4)/$
$(4x^6+4x^3+2x^2+x+4) \rfloor = 2x+4,$
$r(x):=f(x)-h(x)q(x)=x^4+3x^3+x^2+2x+3,$
$u(x):=u_2(x)-q(x)u_1(x)=3x+1, v(x):=v_2(x)-q(x)v_1(x)=x^2+2x+1,$
$f(x):=h(x)=4x^6+4x^3+2x^2+x+4,\ h(x):=r(x)=x^4+3x^3+x^2+2x+3,$
$u_2(x):=u_1(x)=1,\ u_1(x):=u(x)=3x+1,$
$v_2(x):=v_1(x)=2x,\ v_1(x):=v(x)=x^2+2x+1.$

Итерация 3.

$q(x):=\lfloor f(x)/h(x)\rfloor=\lfloor(4x^4+4x^3+2x^2+x+4)/(x^4+3x^3+x^2+2x+3)\rfloor=$
$4x^2+3x+2,$
$r(x):=f(x)-h(x)q(x)=2x^3+2x^2+3x+3,$
$u(x):=u_2(x)-q(x)u_1(x)=3x^3+2x^2+x+4,$
$v(x):=v_2(x)-q(x)v_1(x)=x^4+4x^3+3x^2+3,$
$f(x):=h(x)=x^4+3x^3+x^2+2x+3,\ h(x):=r(x)=2x^3+2x^2+3x+3,$
$u_2(x):=u_1(x)=3x+1,\ u_1(x):=u(x)=3x^3+2x^2+x+4,$
$v_2(x):=v_1(x)=x^2+2x+1,\ v_1(x):=v(x)=x^4+4x^3+3x^2+3.$

Итерация 4.

$q(x):=\lfloor f(x)/h(x)\rfloor=\lfloor(x^4+3x^3+x^2+2x+3)/(2x^3+2x^2+3x+3)\rfloor=$
$3x+1,$
$r(x):=0,$
$u(x):=u_2(x)-q(x)u_1(x)=x^4+x^2+2,$
$v(x):=v_2(x)-q(x)v_1(x)=2x^5+2x^4+2x^3+3x^2+3x+3,$
$f(x):=h(x)=2x^3+2x^2+3x+3,\ h(x):=r(x)=0,$
$u_2(x):=u_1(x)=3x^3+2x^2+x+4,\ u_1(x):=u(x)=x^4+x^2+2,$
$v_2(x):=v_1(x)=x^4+4x^3+3x^2+3,$
$v_1(x):=v(x)=2x^5+2x^4+2x^3+3x^2+3x+3.$

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

$d(x) := d(x)\cdot 2^{-1}(\mathrm{mod}\ p) = d(x)\cdot 3\ (\mathrm{mod}\ p) = x^3+x^2+4x+4,$
$u(x) := u(x)\cdot 2^{-1}(\mathrm{mod}\ p) = u(x)\cdot 3\ (\mathrm{mod}\ p) = 4x^3+x^2+3x+2,$
$v(x) := v(x)\cdot 2^{-1}(\mathrm{mod}\ p) = v(x)\cdot 3\ (\mathrm{mod}\ p) = 3x^4+2x^3+4x^2+4.$

Ответ. $d(x)=x^3+x^2+4x+4$, $u(x)=4x^3+x^2+3x+2$,
$v(x)=3x^4+2x^3+4x^2+4.$

Задача 21. 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 от деления 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) $f(0)=2$, $f(1) = 4\cdot 1^2+2\cdot 1+2 = 8 = 3 \pmod 5$,
$f(2) = 4\cdot 2^2+2\cdot 2+2 = 22 = 2 \pmod 5$,
$f(3) = 4\cdot 3^2+2\cdot 3+2 = 44 = 4 \pmod 5$,
$f(4) = 4\cdot 4^2+2\cdot 4+2 = 74 = 4 \pmod 5$.

Таблица значений $f(x)$.

x	0	1	2	3	4
$f(x)$	2	3	2	4	4

$f(x)\neq 0 \ \forall x\in\mathbb{Z}_5$.

Полином $f(x)$ над полем $\mathbb{Z}_p$ неприводим.

c) множество F всех элементов поля $GF(q)$ определяется множеством всех остатков от деления 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_1a_0), где $a_1,a_0 \in \mathbb{Z}_5$.

0. $(00) = 0\cdot x+0 = 0$.
1. $(01) = 0\cdot x+1 = 1$.
2. $(02) = 0\cdot x+2 = 2$.
3. $(03) = 0\cdot x+3 = 3$.
4. $(04) = 0\cdot x+4 = 4$.
5. $(10) = 1\cdot x+0 = x$.
6. $(11) = 1\cdot x+1 = x+1$.
7. $(12) = 1\cdot x+2 = x+2$.
8. $(13) = 1\cdot x+3 = x+3$.
9. $(14) = 1\cdot x+4 = x+4$.
10. $(20) = 2\cdot x+0 = 2x$.
11. $(21) = 2\cdot x+1 = 2x+1$.
12. $(22) = 2\cdot x+2 = 2x+2$.
13. $(23) = 2\cdot x+3 = 2x+3$.
14. $(24) = 2\cdot x+4 = 2x+4$.
15. $(30) = 3\cdot x+0 = 3x$.
16. $(31) = 3\cdot x+1 = 3x+1$.
17. $(32) = 3\cdot x+2 = 3x+2$.
18. $(33) = 3\cdot x+3 = 3x+3$.
19. $(34) = 3\cdot x+4 = 3x+4$.
20. $(40) = 4\cdot x+0 = 4x$.
21. $(41) = 4\cdot x+1 = 4x+1$.
22. $(42) = 4\cdot x+2 = 4x+2$.
23. $(43) = 4\cdot x+3 = 4x+3$.
24. $(44) = 4\cdot x+4 = 4x+4$.

Табл.7.14 для сложения и умножения в $\mathbb{Z}_p$.

d) табл.7.15 для сложения в поле $GF(q)$, $q=p^m=5^2=25$.
$a+b = a_1a_0 + b_1b_0 = a_1x+a_0 + b_1x+b_0 = (a_1+b_1)x+(a_0+b_0)$.
Табл.7.16 для умножения в поле $GF(q)$, $q=p^m=5^2=25$.
$a\cdot b = a_1a_0 \cdot b_1b_0 = (a_1x+a_0)\cdot(b_1x+b_0) =$
$(a_1b_1)x^2+(a_1b_0+a_0b_1)x +(a_0b_0) \pmod{f(x)}$.

e) $(30)^{-1}=13$, $(31)^{-1}=33$, $(32)^{-1}=41$, $(33)^{-1}=31$, $(34)^{-1}=10$.

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	1	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

Таблица 7.15

+	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2	3	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	2	3	4
30	3	3	3	3	3	4	4	4	4	4	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2
	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
31	3	3	3	3	3	4	4	4	4	4	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2
	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
32	3	3	3	3	3	4	4	4	4	4	0	0	0	0	0	1	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	4	0	1
33	3	3	3	3	3	4	4	4	4	4	0	0	0	0	0	1	1	1	1	1	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	4	0	1	2
34	3	3	3	3	3	4	4	4	4	4	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2
	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3

Таблица 7.16

×	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2	3	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	2	3	4
30	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	1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4
31	0	3	1	4	2	2	0	3	1	4	4	2	0	3	1	1	4	2	0	3	3	1	4	2	0
	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
32	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
	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
33	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
	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
34	0	3	1	4	2	0	3	1	4	2	0	3	1	4	2	0	3	1	4	1	0	3	1	4	2
	0	4	3	2	1	1	0	4	3	2	2	1	0	4	3	3	2	1	0	3	4	3	2	1	0

8.15. Мультипликативный обратный элемент в $\mathbb{F}_{p^m}$

ВХОД. Ненулевой полином $g(x) \in \mathbb{F}_{p^m}$. (Элементы поля $\mathbb{F}_{p^m}$ 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. $g(x)^{-1} \in \mathbb{F}_{p^m}$.

1. С помощью расширенного алгоритма Евклида для полиномов найти два полинома $u(x)$ и $v(x) \in \mathbb{Z}_p[x]$, для которых $u(x)g(x) + v(x)f(x) = 1$.
2. Вернуть $u(x)$.

8.16. Модулярня степень в $\mathbb{F}_{p^m}$

ВХОД. $g(x) \in \mathbb{F}_{p^m}$ и целое $0 \leqslant k < p^m-1$ с бинарным представлением $k = \sum_{i=0}^{t} k_i 2^i$. (Поле $\mathbb{F}_{p^m}$ есть $\mathbb{Z}_p[x]/(f(x))$, где $f(x) \in \mathbb{Z}_p[x]$ есть неприводимый полином степень 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 нод$(f(x), x^{p^i}-x) = 1$ для каждого i, $1 \leqslant i \leqslant \lfloor m/2 \rfloor$.

8.17. 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. $d(x) :=$ нод$(f(x), u(x)-x)$.
   2.3. Если $d(x) \neq 1$, то вернуть "приводимый").

3. Вернуть "неприводимый".

8.18. Порождение случайного неприводимого полинома из $\mathbb{Z}_p[x]$

ВХОД. Простое число p и положительное целое m.

ВЫХОД. Неприводимый полином $f(x)$ степени m в $\mathbb{Z}_p[x]$.

1. Случайно выбираем целые $a_0, a_1, \ldots a_{m-1}$ между 0 и $p-1$ с $a_0 \neq 0$. Пусть $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_2x^2 + a_1x + a_0$.
2. Тестируем полином $f(x)$ на неприводимость.
   Если полином $f(x)$ приводим над $\mathbb{Z}_p$, перейти к 1.
3. Вернуть $f(x)$.

8.19. Тестирование неприводимого полинома из $\mathbb{Z}_p[x]$ *на примитивность*

ВХОД. Простое число p; целое $m \geqslant 1$; различные простые делители $r_1, r_2, \ldots, r_t$ 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".

8.20. Порождение случайного нормированного примитивного полинома из $\mathbb{Z}_p[x]$

ВХОД. Простое число p; целое $m \geqslant 1$; различные простые делители $r_1, r_2, \ldots, r_t$ 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 $f(x)$.

8.21. Вычисление порядка элемента конечной мультипликативной группы (алгоритм Гаусса)

ВХОД. Мультипликативная конечная группа G порядка n, элемент $a \in G$, факторизация $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

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. $a_1 := a^t$.

2.3. Пока $a_1 \neq 1$, выполнить: $a_1 := a_1^{p_i}$, $t := t \cdot p_i$.
3. Вернуть t.

8.22. Вычисление генератора конечной мультипликативной циклической группы (алгоритм Гаусса)

ВХОД. Конечная мультипликативная циклическая группа G порядка n, факторизация $n=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$.

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.

Задача 22. $p=5$, $m=2$. 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. $a_1x+a_0 = a_1a_0 = 34 = 3x+4$, полином $f(x) = 4x^2+2x+1$.

$(3x+4)^0 = 1$.
$(3x+4)^1 = 3x+4$.
$(3x+4)^2 = 9x^2+24x+16=4x^2+4x+1 = 2x$.
$(3x+4)^3 = 2x(3x+4)=6x^2+8x=x^2+3x = 1$.
$\mathrm{ord}(3x+4) = 3$. Элемент $3x+4$ генератором не является.

$(x+1)^0=1$.
$(x+1)^1=x+1$.
$(x+1)^2=x^2+2x+1=4x+2$.
$(x+1)^3=(4x+2)(x+1)=4x^2+x+2=4x+1$.
$(x+1)^4=(4x+1)(x+1)=4x^2+1=3x$.
$(x+1)^5=3x(x+1)=3x^2+3x=4x+3$.
$(x+1)^6=(4x+3)(x+1)=4x^2+2x+3=2$.
$(x+1)^7=2(x+1)=2x+2$.
$(x+1)^8=(2x+2)(x+1)=2x^2+4x+2=3x+4$.
$(x+1)^9=(3x+4)(x+1)=3x^2+2x+4=3x+2$.
$(x+1)^{10}=(3x+2)(x+1)=3x^2+0x+2=x$.
$(x+1)^{11}=x(x+1)=x^2+x=3x+1$.
$(x+1)^{12}=(3x+1)(x+1)=3x^2+4x+1=4$.

$(x+1)^{13}=4(x+1)=4x+4$.
$(x+1)^{14}=(4x+4)(x+1)=4x^2+3x+4=x+3$.
$(x+1)^{15}=(x+3)(x+1)=x^2+4x+3=x+4$.
$(x+1)^{16}=((x+3)^6)^2(x+1)^4=4\cdot 3x=12x=2x$.
$(x+1)^{17}=((x+3)^6)^2(x+1)^5=4(4x+3)=16x+12=x+2$.
$(x+1)^{18}=((x+3)^6)^3=2^3=8=3$.
$(x+1)^{19}=((x+3)^6)^3(x+1)=2^3(x+1)=8x+8=3x+3$.
$(x+1)^{20}=((x+3)^6)^3(x+1)^2=2^3(x+1)^2=8(4x+2)=32x+16=2x+1$.
$(x+1)^{21}=((x+3)^6)^3(x+1)^3=2^3(x+1)^3=8(4x+1)=32x+8=2x+3$.
$(x+1)^{22}=((x+3)^6)^3(x+1)^4=2^3(x+1)^4=8\cdot 3x=24x=4x$.
$(x+1)^{23}=((x+3)^6)^3(x+1)^5=2^3(x+1)^5=8(4x+3)=32x+24=2x+4$.
$(x+1)^{24}=((x+3)^6)^4=2^4=16=1$.
$\mathrm{ord}(x+1) = 24$. Элемент $x+1$ есть генератор поля $GF(p^m)$.

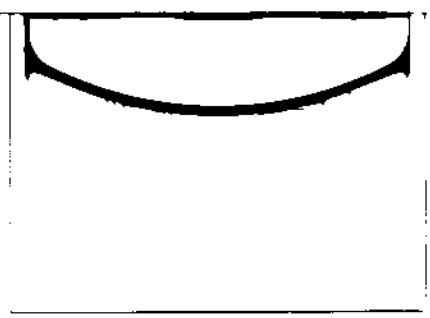
Задача 23. Зашифровать и расшифровать сообщение с помощью криптосистемы RSA (R.Rivest, A.Shamir, L.Adleman).

Вычисление ключей. Каждый адресат вычисляет свой открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два больших различных случайных простых числа p и q примерно одного размера.
2. Найти $n = pq$ и функцию Эйлера $\varphi=\varphi(n)=(p-1)(q-1)$.
3. Взять случайное число e, $1<e<\varphi$, такое, что $\mathrm{нод}(e,\varphi)=1$.
4. Найти такое целое $a \in (1,\varphi)$, что $ea \equiv 1 \pmod{\varphi}$. Для этого с помощью расширенного алгоритма Евклида найти такие целые a,x, что $ea + \varphi x = 1$. Тогда $ea \equiv 1 \pmod{\varphi}$. Пусть произвольное $k \in \mathbb{Z}$. Сложив $ea \equiv 1 \pmod{\varphi}$ и $ek\varphi \equiv 0 \pmod{\varphi}$, получим $e(a+k\varphi) \equiv 1 \pmod{\varphi}$. Если $a \notin (1,\varphi)$, то найти такое целое k, что $a+k\varphi \in (1,\varphi)$, и в качестве a взять $a+k\varphi$.
5. Открытый ключ адресата есть пара чисел (n,e). Секретный ключ адресата есть число a.

Шифрование. Адресат A шифрует свой текст t и отправляет шифротекст адресату B. B дешифрует сообщение от A и получает исходный текст t. Адресат A должен выполнить следующее.

1. Получить открытый ключ (n,e) адресата B.
2. С помощью какого-либо метода M, который публикуется, представить 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 свой 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=NAB адресату B.

Вычисление ключей. Адресат B выполняет следующее.

1. Выбирает два разных простых числа p=499, q=631.

2. Вычисляет $n=pq$=314869 и функцию Эйлера $\varphi=(p-1)(q-1)$ = 313740.

3. Выбирает случайное число e=305183$\in(1,\varphi)$ с нод(e,φ)=1.

4. С помощью расширенного алгоритма Евклида находит такое a = 181967 $\in (1,\varphi)$, что $ea \equiv 1 \pmod\varphi$.

5. Открытый ключ адресата B есть пара чисел (n=314869, e=305183). Секретный ключ адресата B есть число a = 181967.

Шифрование. Адресат A выполняет следующее.

1. Получает открытый ключ (n=314869,e=305183) адресата B.

2. Представляет 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	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	P	Q	R	S	T	U	V	W	X	Y	Z				
	16	17	18	19	20	21	22	23	24	25	26				

Текст NAB представляется в виде числа $m = 14\cdot 27^2 + 1\cdot 27 + 2$ = 10235.

3. Шифрует свое сообщение m=10235 числом $c = m^e \pmod n$ = $10235^{305183} \pmod{314869}$ = 301085.

4. Посылает свой шифротекст c адресату B.

Дешифрование. Чтобы дешифровать шифротекст c от A, адресат B выполняет следующее.

1. Находит (с помощью своего секретного ключа a) число
$m = c^a \pmod n = 301085^{181967} \pmod{314869} = 10235$.

2. Представляет число m в 27-ричной системе счисления: $m = (14\,1\,2)_{27}$ и получает исходный текст NAB.

Замечание. Криптографическая стойкость криптосистемы RSA основана на трудной практической осуществимости проблемы

факторизации больших чисел. На практике для криптографической стойкости модуль n задается двоичным числом с 1024 и более двоичными разрядами.

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 небольшими числами.

Задача 24. Электронная цифровая подпись RSA (R.Rivest, A.Shamir, L.Adleman) с извлечением сообщения и с хэш-функцией.

Вычисление ключей. Каждый адресат создает открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать два больших различных случайных простых числа p и q приблизительно одного размера.
2. Найти числа $n = pq$ и $\varphi = (p-1)(q-1)$.
3. Найти такое целое число e, $1<e<\varphi$, что нод$(e,\varphi)=1$.
4. С помощью расширенного алгоритма Евклида найти то единственное целое a, $1<a<\varphi$, для которого $ea \equiv 1 \pmod{\varphi}$.
5. Открытый ключ адресата есть пара (n,e). Секретный ключ адресата есть a.

Вычисление подписи. Адресат A подписывает свой текст t. Любой адресат B может проверить подпись A и извлечь из нее текст t. Адресат A должен выполнить следующее.

1. Каким-либо методом M (который публикуется) представить свой текст t в виде целого числа m, $1 < m < n-1$.
2. Найти число $w=R(m)$ с помощью открытой функции $R:[0, n-1] \to M_R$, где M_R есть некоторое числовое множество, например, $R(m) = m*m$, где $a*b$ есть результат приписывания слова b к слову a. Тогда $M_R = \{w=m*m : m \in [0,n-1]\}$.
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 сообщение m, 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, отвергнуть подпись s.

4. Найти число $m = R^{-1}(w)$.

5. С помощью метода M найти отправленный текст t.

Пример. Адресат A подписывает свой текст t. Любой адресат B может проверить подпись A.

Вычисление ключей. Адресат A выполняет следующее.

1. Выбирает разные простые числа p=1019, q=2347.

2. Находит $n=pq$ = 2391593 и функцию Эйлера $\varphi = (p-1)(q-1) = 1018 \cdot 2346 = 2388228$.

3. Выбирает случайное число e=35, $1<e<\varphi$, с нод(e,φ)=1.

4. С помощью расширенного алгоритма Евклида находит то единственное целое a=1569407$\in(1,\varphi)$, которое удовлетворяет сравнению $ea \equiv 1 \pmod{\varphi}$, это сравнение $35d \equiv 1 \pmod{2388228}$.

5. Открытый ключ для A есть пара (n=2391593, e=35). Секретный ключ для A есть число a=1569407.

Вычисление подписи. Адресат A подписывает свой текст t = ABX и выполняет следующее.

1. Представляет свой текст t=ABX числом каким-либо методом M, например, в 27-ричной системе счисления числом $m = 1 \cdot 27^2 + 2 \cdot 27 + 24 = 807$.

2. Вычисляет $w = R(m) = R(807) = 807*807 = 807807$.

3. Вычисляет подпись

$s = w^a \pmod{n} = 807807^{1569407} \pmod{2391593} = 794011$.

4. Отправляет подписанный шифротекст s адресату B.

Проверка подписи и вычисление сообщения. Адресат B получает от A подписанный шифротекст s и делает следующее.

1. Получает открытый ключ (n=2391593, e=35) адресата A.

2. С помощью открытого ключа (n,e) адресата A вычисляет:

$w = s^e \pmod{n} = 794011^{35} \pmod{2391593} = 807807$.

3. Так как w = 807807 = 807*807 и $w \in R(\mathbb{N})$, то B принимает подпись A.

4. Вычисляет $m = R^{-1}(w) = 807$.

5. Представляет число $m=(807)_{10}$ в 27-ричной системе счисления $m = (1\ 2\ 24)_{27}$ и получает исходный текст t = ABX.

Замечание. Допустима цифровая подпись RSA, основанная на использовании криптографической хэш-функции $h: \{0,1\}^* \to \mathbb{Z}_n$, где n есть число элементов в мультипликативной группе G. Предполагается, что каждый элемент r из G может быть пред-

ставлен 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 битовым набором m, составленным из кодов ASCII для последовательных символов текста t. Хэш-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 18 цифр. Для работы с большими целыми числами с длиной десятиричной записи в 100 и более цифр приходится писать специальный программный процессор. Поэтому в последующих примерах значение хэш-функции задается искусственно, для примера, небольшим числом.

Вычисление ключей. Пусть по-прежнему: пара (n=2391593, e = 35) есть открытый ключ для A и число a=1569407 есть секретный ключ для A.

Вычисление подписи. Адресат A подписывает свой текст t произвольной длины. Любой адресат B может проверить подпись A под его текстом t. Адресат A должен выполнить следующее.

1. Вычислить значение хэш-функции $h = h(t)$. Пусть для примера текст t=DXN, $m=4\cdot 27^2+24\cdot 27+14=3578$, $h=h(m)=m=3578$.

2. Вычислить $s = h^a \pmod n = 3578^{1569407} \pmod{2391593} = 2146200$. Число s есть подпись A под его текстом t.

Проверка подписи. Чтобы проверить подпись s адресата A, адресат B должен выполнить следующее.

1. Получить открытый ключ (n,e) адресата A.

2. Вычислить значение хэш-функции $h = h(t)$. Если текст t не изменялся, то h=3578.

3. Вычислить $h1 = s^e \pmod n = 2146200^{35} \pmod{2391593} =$

3578.

4. Принять подпись, если $h = h1$, и отвергнуть в противном случае. Так как $h = h1 = 3578$, то подпись принимается.

Задача 25. Зашифровать и расшифровать сообщение с помощью криптосистемы ЭльГамаля.

Вычисление ключей. Каждый адресат создает свой открытый ключ и ему соответствующмй секретный ключ. Адресат должен выполнить следующее.

1. Выбрать случайное простое число p и найти генератор α мультипликативной группы $\mathbb{Z}_p^*$ целых чисел по модулю p, используя в главе 7 алгоритмы задач 10 или 21 (алгоритм Гаусса).

2. Выбрать случайное число $a \in [1, p-2]$ и найти $y = \alpha^a \pmod p$.

3. Открытый ключ адресата есть тройка чисел (p, α, y). Секретный ключ адресата есть число a.

Шифрование. Адресат A шифрует свой текст t и отправляет шифротекст адресату B. B дешифрует сообщение от A и получает исходный текст t. Адресат A должен выполнить следующее.

1. Получить открытый ключ (p, α, y) адресата B.

2. С помощью какого-либо метода M, который публикуется, представить свое письмо t как сообщение в виде натурального числа m из сегмента $[0, p-1]$.

3. Выбрать случайное число k, $1 \leqslant k \leqslant p-2$.

4. Вычислить $\gamma = \alpha^k \pmod p$ и $\delta = m \cdot y^k \pmod p$.

5. Отправить свой 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 γ^{-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 текст t=BUJ и отправляет шифротекст адресату B.

Вычисление ключей. Адресат B выполняет следующее.

1. Выбирает простое число p=2357 и находит генератор α=2 для мультипликативной группы $\mathbb{Z}_{2357}^*$.

2. Выбирает случайное число a=1751, $1 \leqslant a \leqslant p-2$, и вычисляет $y = \alpha^a \pmod p = 2^{1751} \pmod{2357} = 1185$.

3. Открытый ключ адресата B есть тройка (p=2357, α=2, y = 1185). Секретный ключ адресата B есть число a=1751.

Шифрование. Адресат A шифрует свой текст t=BUJ и выполняет следующее.

1. Получает открытый ключ (p=2357, α=2, y=1185) для B.
2. Представляет свой текст t=BUJ в виде натурального числа m из $[0, p-1]$, с помощью какого-либо метода, например, с помощью 27–ричной системы счисления числом $m = 2 \cdot 27^2 + 21 \cdot 27 + 10 = 2035$.
3. Выбирает случайное число k=1520, $1 \leqslant k \leqslant p-2$.
4. Вычисляет

$$\gamma = \alpha^k \pmod p = 2^{1520} \pmod{2357} = 1430,$$

$$\delta = m \cdot y^k \pmod p = 2035 \cdot 1185^{1520} \pmod{2357} = 697.$$

5. Посылает шифротекст c = (γ=1430, δ=697) адресату B.

Дешифрование. Чтобы дешифровать шифротекст c = (γ=1430, δ=697) от A, адресат B выполняет следующее.

1. Вычисляет

$\gamma^{p-1-a} = 1430^{605} \pmod{2357} = 872$ и получает

$m = ((\gamma^{p-1-a} \pmod p) \cdot \delta) \pmod p =$

$872 \cdot 697 \pmod{2357} = 2035.$

2. Представляет число m в 27–ричной системе счисления: $m = (2\,21\,10)_{27}$ и получает исходный текст BUJ.

Замечание. Криптографическая стойкость криптосистемы ЭльГамаля основана на трудной практической осуществимости проблемы нахождения дискретного логарифма в группе $\mathbb{Z}_p^*$ при больших простых числах p. На практике для криптографической стойкости простое число p задается двоичным числом с 1024 и более двоичными разрядами.

Задача 26. Вычислить и проверить подпись под сообщением с помощью электронной цифровой подписи ЭльГамаля.

При использовании схемы цифровой подписи ЭльГамаля по тексту письма t вычисляется значение хэш-функции $h(t)$, которое затем используется при вычислении и проверке цифровой подписи под текстом сообщения.

Вычисление ключей. Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Далее адресат должен выполнить следующее.

1. Выбрать случайное простое число p и найти генератор α для мультипликативной группы $\mathbb{Z}_p^*$.

2. Выбрать произвольное число a, $1 \leqslant a \leqslant p-2$.

3. Вычислить $y=\alpha^a \pmod p$.

4. Открытый ключ адресата есть тройка чисел (p,α,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 хэш-функции $h(t)$.

2. Выбрать случайное секретное целое число k из $[1,p-2]$ такое, что $\text{нод}(k,p-1) = 1$.

3. Вычислить $k^{-1} \pmod{(p-1)}$.

4. Вычислить $r = \alpha^k \pmod p$.

6. Вычислить $s = k^{-1}(h(t)-ar) \pmod{(p-1)}$.

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. Вычислить значение хэш-функции $h(t)$.

2. Получить открытый ключ (p,α,y) адресата A.

3. Проверить, что $r \in [1,p-1]$; если нет, то отвергнуть подпись.

4. Вычислить $v_1 = y^r r^s \pmod p$.

5. Вычислить $v_2 = \alpha^{h(m)} \pmod p$.

6. Принять подпись, если $v_1=v_2$ и отвергнуть в противном случае.

Пример. Адресат A подписывает свой текст t. Любой адресат B может проверить подпись A.

Вычисление ключей. Адресат A выполняет следующее.

1. Выбирает простое число p=2357 и находит генератор α=2 мультипликативной группы $\mathbb{Z}_p^*$ целых чисел по модулю p.

2. Выбирает случайное целое a=1751 из $[1,p-2]$.

3. Вычисляет $y = \alpha^a \pmod p = 2^{1751} \pmod{2357} = 1185$.

4. Открытый ключ адресата A есть тройка (p=2357, α=2, y = 1185). Секретный ключ адресата A есть a=1751.

Вычисление подписи. Адресат A подписывает свой текст t и для этого выполняет следующее.

1. Вычисляет значение хэш-функции $h(t)$. Пусть для примера

$h(t) = 1490$.

2. Выбирает случайное секретное число k=1529 из $[1,p-2]$ такое, что нод$(k,p-1) = 1$.

3. Вычисляет $k^{-1} \pmod{p-1} = 1529^{-1} \pmod{2356} = 245$.

4. Вычисляет $r = \alpha^k \pmod{p} = 2^{1529} \pmod{2357} = 1490$.

5. Вычисляет $s = k^{-1}(h(t)-ar) \pmod{(p-1)} =$
$245 \cdot (1490-1751 \cdot 1490) \pmod{2356} = 1324$.

6. Подпись A есть пара (r=1490, s=1324).

Проверка подписи. Чтобы проверить подпись (r=1490,s=1324) адресата A под его текстом t, адресат B делает следующее.

1. Вычисляет значение хэш-функции $h(t)$. Если текст t не изменялся, то $h(t) = 1490$.

2. Получает открытый ключ (p=2357,α=2,y=1185) адресата A.

3. Проверяет, что r=1490 $\in [1,p-1] = [1,2356]$.

4. Вычисляет число
$v_1 = y^r r^s \pmod{p}$ =$1185^{1490} \cdot 1490^{1324} \pmod{2357} = 1101$.

5. Вычисляет число
$v_2 = \alpha^{h(t)} \pmod{p} = 2^{1490} \pmod{2357} = 1101$.

6. Принимает подпись, ибо v_1=v_2.

Для криптографической стойкости рекомендуется брать p длиной между 512 бит (лучше 768) и 1024 бит включительно.

Задача 27. Зашифровать и расшифровать сообщение с помощью (обобщенной) криптосистемы ЭльГамаля с мультипликативной группой G (конечнго) поля Галуа $GF(p^m)$.

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, из которых первые три наиболее употребительны.

1. Мультипликативная группа $\mathbb{Z}_p^*$ целых чисел по модулю простого числа p.

2. Мультипликативная группа $\mathbb{Z}_2^*s$ конечного поля $\mathbb{Z}_2s$ харак-

теристики два.

3. Группа точек эллиптической кривой над конечным полем.

4. Мультипликативная группа $\mathbb{Z}_q^*$ конечного поля $\mathbb{F}_q$, где $q = p^s$, p есть простое число, s есть положительное целое число.

5. Группа обратимых элементов $\mathbb{Z}_n^*$, где n есть составное целое число.

6. Якобиан гиперэллиптической кривой над конечным полем.

7. Класс групп мнимого квадратичного числового поля (imaginary quadratic number field).

Адресат A шифрует текст t и отсылает шифротекст адресату B. B дешифрует сообщение от A и получает исходный текст t.

Вычисление ключей. Каждый адресат создает свой открытый ключ и ему соответствующмй секретный ключ. Адресат должен выполнить следующее.

1. Выбрать подходящую (мультипликативную) циклическую группу G порядка n.

2. Найти генератор α группы G.

3. Выбрать случайное целое число a, $1 \leqslant a \leqslant n-1$.

4. Вычислить элемент $y = \alpha^a$ группы G.

5. Открытый ключ адресата есть пара (α, y) элементов группы G. Открыто также описание умножения элементов в G. Секретный ключ адресата есть число a.

Шифрование. Адресат A шифрует текст t и отправляет шифротекст адресату B. Адресат A должен выполнить следующее.

1. С помощью какого-либо метода M, который публикуется, представить свой текст t как элемент m группы G.

2. Получить открытый ключ (α, y) адресата B.

3. Выбрать случайное целое число k, $1 \leqslant k \leqslant n-1$.

4. Вычислить $\gamma = \alpha^k$ и $\delta = m \cdot y^k$.

5. Отправить свой 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 γ^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 α.

Пример 1. Криптосистема ЭльГамаля с мультипликативной

группой конечного поля $GF(p^m)$, p=13, m=4. Пусть для удобства элемент поля $a_3x^3+a_2x^2+a_1x+a_0$ представляется p–ричным стрингом $(a_3a_2a_1a_0)$.

Адресат A шифрует свой текст t=ZAM и отправляет шифротекст адресату B. B дешифрует сообщение от A и получает исходный текст t.

Вычисление ключей. Адресат B выполняет следующее.

1. Выбирает мультипликативную группу G конечного поля $GF(p^m)$, p=13, m=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 $f(x)$ = (1 0 1 0 2) = x^4+x^2+2 из $\mathbb{Z}_{13}[x]$. Группа G имеет порядок $n = p^m-1 = 13^4 - 1 = 28560$.
2. Находит генератор $\alpha = x+5 = (0\ 0\ 1\ 5)$.
3. Выбирает случайное число $a = 2 \in [1,n-1]$.
4. Вычисляет $y = \alpha^a = \alpha^2 = (x+5)^2 (\mathrm{mod}\ f(x)) = x^2+10x+12 =$ (0 1 10 12).
5. Открытый ключ для B есть пара (α=(0 0 1 5), y=(0 1 10 12) вместе с полиномом $f(x)$, который определяет умножение в G, если $f(x)$ и α не есть параметры, общие всем адресатам. Секретный ключ для B есть число a=2.

Шифрование. Адресат A шифрует текст t=ZAM и отправляет шифротекст адресату B. Адресат A выполняет следующее.

1. Представляет свой текст t=ZAM как элемент m группы G. Чтобы зашифровать письмо t, адресат A кодирует текст t каким-либо способом, например, в 27–ричной системе счисления 10-ричным числом $u=26\cdot 27^2+1\cdot 27+13=18994_{10}$, а затем вычисляет 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. Получает открытый ключ (α=(0 0 1 5), y=(0 1 10 12)) адресата B.
3. Выбирает произвольное целое число k=2134, $1 \leqslant k \leqslant n-1$.
4. Вычисляет следующие элементы из G.

$\gamma = \alpha^k = (0\ 0\ 1\ 5)^{2134} = (x+5)^{2134}\ (\mathrm{mod}\ f(x)) =$
$8x^3+9x^2+7x+5 = (8\ 9\ 7\ 5)$, $y^k = (0\ 1\ 10\ 12)^{2134} =$
$(x^2+10x+12)^{2134}\ (\mathrm{mod}\ f(x)) = 10x^3+12x^2+3x+1 =$
(10 12 3 1),

$\delta = m\cdot y^k = (8\ 8\ 5\ 1)\cdot(10\ 12\ 3\ 1) = (8x^3+8x^2+5x+1)\cdot$
$(10x^3+12x^2+3x+1)\ (\mathrm{mod}\ f(x)) = 4x^3+6x^2+7x+3 = (4\ 6\ 7\ 3)$.

5. Отправляет шифротекст c = (γ=(8 9 7 5), δ=(4 6 7 3))

адресату B.

Дешифрование. Чтобы получить исходный текст t по c, адресат B выполняет следующее.

1. Пользуясь своим секретным ключом a, адресат B вычисляет следующие элементы группы G.

$\gamma^a = (8\ 9\ 7\ 5)^2 = (8x^3+9x^2+7x+5)^2 \pmod{f(x)} =$
$10x^3+12x^2+3x+1 = (10\ 12\ 3\ 1)$,

$\gamma^{-a} = (\gamma^a)^{-1} = (10\ 12\ 3\ 1)^{-1} =$
$(10x^3+12x^2+3x+1)^{-1} \pmod{f(x)} =$
$5x^3+7x^2+6x+11 = (5\ 7\ 6\ 11)$.

2. Вычисляет в группе G элемент

$m = (\gamma^{-a})\cdot\delta = (5\ 7\ 6\ 11)\cdot(4\ 6\ 7\ 3) = (5x^3+7x^2+6x+11)\cdot$
$(4x^3+6x^2+7x+3) \pmod{f(x)} = 8x^3+8x^2+5x+1 = (8\ 8\ 5\ 1)$.

3. Чтобы получить текст t по элементу m, адресат B производит следующие вычисления.

$m = (8\ 8\ 5\ 1)_{13} = 8\cdot 13^3 + 8\cdot 13^2 + 5\cdot 13 + 1 = 18994_{10} =$
$(26\ 1\ 13)_{27}$, откуда текст t = ZAM.

Пример 2. Криптосистема ЭльГамаля с мультипликативной группой конечного поля $\mathbb{F}_{p^s}$, p=2, s=4. Пусть для удобства элемент поля $a_3x^3+a_2x^2+a_1x+a_0$ представляется бинарным стрингом $(a_3a_2a_1a_0)$.

Вычисление ключей. Адресат B выполняет следующее.

1. Выбирает мультипликативную группу $G=\mathbb{Z}_{24}^*$ конечного поля $(E_2^4,\{+,\cdot\})$, элементы которого представляются полиномами из $\mathbb{Z}_2[x]$ над $\mathbb{Z}_2$ степени меньше 4 и умножение в котором выполняется по модулю неприводимого полинома $f(x) = x^4+x+1$ из $\mathbb{Z}_2[x]$. Группа G имеет порядок n=15.

2. Находит генератор $\alpha=(0010) = 0\cdot x^3+0\cdot x^2+1\cdot x+0 = x$.

3. Выбирает случайное число $a = 7 \in [1,n-1]$.

4. Вычисляет $y = \alpha^a = \alpha^7 = x^7 \pmod{f(x)} =$
$1\cdot x^3+0\cdot x^2+1\cdot x+1 = (1011)$.

5. Открытый ключ для B есть пара $(\alpha=(0010), y=(1011))$ вместе с полиномом $f(x)$, который определяет умножение в G, если $f(x)$ и α не есть параметры, общие всем адресатам). Секретный ключ для B есть число a=7.

Шифрование. Чтобы зашифровать свое сообщение m=(1100), A получает открытый ключ $(\alpha=(0010), y=(1011))$ адресата B, выбирает случайное целое число k=11 и вычисляет

$\gamma = \alpha^k = (0010)^{11} = x^{11} \pmod{f(x)} =$

$x^3+x^2+x = (1110)$, $y^k = (1100)^{11} = (0100)$ и
$\delta = m \cdot (\alpha^a)^{11} = (x^3+x^2)(x^3+x+1) \pmod{f(x)} = x^2+1 = (0101)$.

A посылает шифротекст $c = (\gamma=(1110), \delta=(0101)$ адресату B.

Дешифрование. Чтобы дешифровать шифротекст c, B вычисляет
$\gamma^a = (1110)^7 = (x^3+x^2+x)^7 \pmod{f(x)} = x^3 = (0100)$,
$(\gamma^a)^{-1} = (0100)^{-1} = (x^3)^{-1} \pmod{f(x)} = x^3+x^2+1 = (1101)$,
$m = (\gamma^{-a}) \cdot \delta = (1101) \cdot (0101) = (x^3+x^2+1)(x^2+1) \pmod{f(x)} = x^3+x^2 = (1100)$.

Задача 28. Вычислить и проверить подпись под сообщением с помощью (обобщенной) электронной цифровой подписи ЭльГамаля над (конечным) полем Галуа $GF(p^m)$.

Схема электронной цифровой подписи ЭльГамаля, основанная на мультипликативной группе $\mathbb{Z}_p^*$, может быть обобщена на любую конечную абелеву группу G. Алгоритм подписи использует криптографическую хэш-функцию $h: \{0,1\}^* \to \mathbb{Z}_n$, 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 хэш-функции $h(f(r))$.

Алгоритм вычисления хэш-функции публикуется.

Криптографическая стойкость подписи основана на трудной осуществимости проблемы нахождения дискретного логарифма в группе G большого порядка.

При использовании схемы цифровой подписи ЭльГамаля по тексту письма t вычисляется значение хэш-функции $h(t)$, которое затем используется при вычислении и проверке цифровой подписи под текстом письма.

Вычисление ключей. Каждый адресат создает открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать подходящую (мультипликативную) циклическую группу G порядка n.
2. Найти генератор α группы G.
3. Выбрать случайное число a, $1 \leqslant a \leqslant n-1$.
4. Вычислить элемент $y = \alpha^a$ группы G.
5. Открытый ключ адресата есть пара (α, y) элементов группы G. Открыто также описание умножения элементов в G. 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 хэш-функции $h(t)$.
2. Выбрать случайное секретное целое число k из $[1, n-1]$, для которого нод$(k,n) = 1$.
3. Вычислить целое число $k^{-1} \pmod n$.
4. Вычислить элемент $r = \alpha^k$ группы G.
5. Вычислить значение хэш-функции $h(r)$.
6. Вычислить число $s = k^{-1}(h(t) - ah(r)) \pmod n$.
7. Подпись адресата A под его письмом t есть пара (r,s).

Проверка подписи. Чтобы проверить подпись (r,s) адресата A под его текстом t, адресат B должен выполнить следующее.

1. Вычислить значение хэш-функции $h(t)$.
2. Получить открытый ключ (α,y) для A.
3. Вычислить значение хэш-функции $h(r)$.
4. Вычислить в группе G элементы $v_1 = y^{h(r)} \cdot r^s$ и $v_2 = \alpha^{h(t)}$.
5. Принять подпись, если $v_1=v_2$ и отвергнуть в противном случае.

Пример 1. Схема электронной (цифровой) подписи ЭльГамаля с мультипликативной группой конечного поля $\mathbb{F}_{p^s}$, p=13, s=4. Пусть для удобства элемент поля $a_3x^3+a_2x^2+a_1x+a_0$ представляется p-ричным стрингом $(a_3a_2a_1a_0)$.

Адресат A подписывает свой текст t (произвольной длины). Любой адресат B может проверить подпись A.

Вычисление ключей. Адресат A выполняет следующее.

1. Выбирает мультипликативную группу $G=\mathbb{Z}_{13^4}-\{0\}$ конечного поля $(\mathbb{Z}_{13^4},\{+,\cdot\})$, 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 $f(x)$ = (1 0 1 0 2) = x^4+x^2+2 из $\mathbb{Z}_{13}[x]$. Группа G имеет порядок $n = p^s-1 = 13^4-1 = 28560$.
2. Находит генератор $\alpha = x+5$ = (0 0 1 5).
3. Выбирает 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).
5. Открытый ключ для A есть пара (α=(0 0 1 5), y=(0 1 10 12)) вместе с полиномом $f(x)$, который определяет умножение в

G, если $f(x)$ и α не есть параметры, общие всем адресатам). Секретный ключ для A есть число a=2.

Вычисление подписи. Адресат A подписывает свой текст t (произвольной длины). Адресат A выполняет следующее.

1. Вычисляет значение хэш-функции $h(t)$. Пусть для примера t = RUS, $m = 18\cdot 27^2+21\cdot 27+19=13708$, $h(t) = h(m) = 13708$.

2. Выбирает случайное секретное целое число k=2141, $1 \leqslant k \leqslant n-1$, такое, что нод$(k,n) = 1$.

3. Вычисляет в группе G элемент $r = \alpha^k = (0\ 0\ 1\ 5)^{2141} = (x+5)^{2141} \pmod{f(x)} = (3\ 8\ 0\ 4)$.

4. Вычисляет целое число
$k^{-1} \pmod n = 2141^{-1} \pmod n = 16421$.

5. Вычисляет значение хэш-функции $h(r)$, например, следующим образом. По $r = (3\ 8\ 0\ 4)$ вычисляет в $\mathbb{Z}_n$ 10-ричное число $(3\ 8\ 0\ 4)_{13} = 3p^3+8p^2+4 = 3\cdot 13^3 + 8\cdot 13^2 + 4 = 7947_{10}$. Пусть для примера $h(r) = 7947_{10}$.

6. Вычисляет в $\mathbb{Z}_n$ число $s = k^{-1}(h(t) - ah(r)) \pmod n = 16421\cdot(13708 - 2\cdot 7947) \pmod n = 3614$.

7. Подпись адресата A под его текстом t есть пара (r=(3 8 0 4), s=3614_{10}).

Проверка подписи. Чтобы проверить подпись (r,s) адресата A под его письмом t, адресат B выполняет следующее.

1. Вычисляет значение хэш-функции $h(t)$. Если текст t не изменялся, то $h(t) = 13708_{10}$.

2. Получает открытый ключ (α=(0 0 1 5), y=(0 1 10 12)) адресата A.

3. Вычисляет значение хэш-функции $h(r)$. Если вектор r не изменялся, то $h(r) = 7947_{10}$.

4. Вычисляет в группе G элементы
$v_1 = y^{h(r)}\cdot r^s = (0\ 1\ 10\ 12)^{7947}\cdot(3\ 8\ 0\ 4)^{3614} = (x^2+10x+12)^{7947}\cdot(3x^3+8x^2+4)^{3614} \pmod{f(x)} = (6\ 2\ 5\ 12)$,
$v_2 = \alpha^{h(t)} = (0\ 0\ 1\ 5)^{13708} = (x+5)^{13708} \pmod{f(x)} = (6\ 2\ 5\ 12)$.

5. Так как $v_1 = v_2$, то B принимает подпись адресата A.

Пример 2.Вычисление ключей. Рассмотрим конечное поле $\mathbb{F}_{2^5}$, построенное с помощью неприводимого полинома $f(x) = x^6+x^2+1$ над $\mathbb{Z}_2$. Элементы этого поля есть 32 набора из 0 и 1 длины 5 с нулем 00000. Элемент α = (00010) есть генератор мультипликативной циклической группы $G = \mathbb{F}^*_{2^5}$ поля. Порядок группы G есть n=31. Элементы группы приведены в табл.8.2 как степени

генератора α. Пусть h: $\{0,1\}^* \to \mathbb{Z}_{31}$ есть хэш-функция. Адресат A выбирает число $a = 19$ и вычисляет $y = \alpha^a = (00010)^{19} = (00110)$. Открытый ключ адресата A есть пара наборов из 0 и 1 длины пять (α=(00010), y=(00110)). Секретный ключ для A есть число $a = 19$.

Вычисление подписи. Чтобы подписать текст $m = 10110101$, адресат A выбирает случайное число $k = 24$ и вычисляет $r = \alpha^{24} = (11110)$ и $k^{-1} \pmod{31} = 22$. Потом адресат A вычисляет $h(m) = 16$, $h(r) = 7$ (значения хэш-функции не связано с сообщением m и вектором r и взято в качестве примера) и $s = 22 \cdot (16 - 19 \cdot 7) \pmod{31} = 30$. Подпись адресата A под сообщением m есть пара (r=(11110), s=30).

Проверка подписи. Адресат B вычисляет

$h(m) = 16$, $h(r) = 7$,
$v_1 = y^{h(r)} r^s = (00110)^7 \cdot (11110)^{30} = (11011)$,
$v_2 = \alpha^{h(m)} = \alpha^{16} = (11011)$.

Так как $v_1 = v_2$, то B принимает подпись адресата A.

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. Вычислить и проверить подпись под сообщением с помощью электронной цифровой подписи DSA (Digital Signature Algorithm).

Вычисление ключей. Каждый адресат создает свой открытый ключ и ему соответствующий секретный ключ. Адресат должен выполнить следующее.

1. Выбрать простое число q, $2^{159} < q < 2^{160}$.
2. Выбрать число t, $0 \leqslant t \leqslant 8$, и 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 адресат должен выполнить следующее.
   3.1. Выбрать элемент $g \in \mathbb{Z}_p^*$ и найти $\alpha = g^{(p-1)/q} \pmod{p}$.
   3.2. Если α=1, то перейти к шагу 3.1 с другим g.
4. Выбрать произвольное число a, $1 \leqslant a \leqslant q-1$.
5. Вычислить $y = \alpha^a \pmod{p}$.
6. Открытый ключ адресата есть (p,q,α,y); секретный ключ адресата есть число a.

Вычисление подписи. Адресат A подписывает свой текст t (произвольной длины). Любой адресат B может проверить подпись A под текстом t с помощью открытого ключа адресата A. Адресат A должен выполнить следующее.

1. Вычислить значение хэш-функции $h(t)$.
2. Выбрать произвольное секретное число k, $0<k<q$.
3. Вычислить $k^{-1} \pmod q$.
4. Вычислить $r=(\alpha^k \pmod p) \pmod q$.
5. Вычислить $s=k^{-1}(h(t)+ar) \pmod q$.
6. 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. Вычислить значение хэш-функции $h(t)$.
2. Взять открытый ключ (p,q,α,y) адресата A.
3. Проверить, что $0 < r < q$ и $0 < s < q$. Если нет, то отвергнуть подпись.
4. Вычислить $w = s^{-1} \pmod q$ и $h(w)$.
5. Вычислить $u_1 = w \cdot h(w) \pmod q$ и $u_2 = rw \pmod q$.
6. Вычислить $v = (\alpha^{u_1} y^{u_2} \pmod p) \pmod q$.
7. Принять подпись, если $v = r$ и отвергнуть в противном случае.

Пример. Адресат A подписывает свой текст t и всякий адресат B может проверить подпись A.

Вычисление ключей. Адресат A делает следующее.

1. Выбирает простое число q=27367.
2. Выбирает простое число p=656809, для которого q делит $(p-1)$. Пусть $(p-1)/q = 24$.
3. Выбирает случайное число $g = 2732 \in \mathbb{Z}_p^*$ и вычисляет $\alpha = g^{(p-1)/q} \pmod p = 2732^{24} \pmod{656809} = 68909$. Так как $\alpha \neq 1$, то α есть генератор для единственной циклической подгруппы порядка q в группе $\mathbb{Z}_p^*$. (Если α=1, то следует выбрать другое g).
4. Выбирает случайное число $a = 80 \in [1,q-1]$.
5. Вычисляет $y = \alpha^a \pmod p =$
$68909^{80} \pmod{656809} = 50951$.
6. Открытый ключ адресата A есть (p=656809, q=27367, α=68909, y=50951). Секретный ключ адресата A есть a=80.

Вычисление подписи. Чтобы подписать свой текст t (произвольной длины), адресат A делает следующее.

1. Вычисляет значение хэш-функции $h(t)$. Пусть для примера

t=BAN, $m=2\cdot 27^2+1\cdot 27+14=1499$, $h(t) = h(m) = 1499$.

2. Выбирает случайное секретное число $k = 74 \in [0,q]$.

3. Вычисляет $k^{-1} \pmod q = 21080$.

4. A вычисляет $r = (\alpha^k \pmod p) \pmod q =$
$(68909^{74} \pmod{656809}) \pmod{27367} =$
$145325 \pmod{27367} = 8490$.

5. A вычисляет $s = k^{-1}\cdot(h(t)+ar) \pmod q =$
$21080\cdot(1499 + 80\cdot 8490) \pmod{27367} = 14746$.

6. Подпись A под его текстом t есть пара чисел (r = 8490, s=14746).

Проверка подписи. Чтобы проверить подпись (r = 8490, s = 14746) адресата A под его текстом t, адресат B выполняет следующее.

1. Вычисляет значение хэш-функции $h(t)$. Если текст t не изменялся, то $h(t) = 1499$.

2. Берет открытый ключ адресата A:
(p=656809, q=27367, α=68909, y=50951).

3. Проверяет, что $r = 8490 \in [0,q] = [0,27367]$,
$s = 14746 \in [0,q] = [0,27367]$. Если проверка не проходит, то подпись отвергнуть.

4. Вычисляет $w = s^{-1} \pmod q = 15699$.

5. Вычисляет
$u_1 = w\cdot h(t) \pmod q =$
$15699\cdot 1499 \pmod{27367} = 24548$,
$u_2 = rw \pmod q = 8490\cdot 15699 \pmod{27367} = 7220$.

6. Вычисляет $v = (\alpha^{u_1} y^{u_2} \pmod p) \pmod q =$
$(68909^{24548}\cdot 50951^{7220} \pmod{656809}) \pmod{27367} =$
$(280146\cdot 334407 \pmod{656809}) \pmod{27367} =$
$145325 \pmod{27367} = 8490$.

7. Так как $v = 8490 = r$, то B принимает подпись A.

Для криптографической стойкости рекомендуется брать q длиной 160 бит, размер p при любом кратном 64 лежит между 512 (лучше 768) и 1024 бит включительно.

9. КОМБИНАТОРИКА (Примеры решения)

1. $P(N+10)$. **2.** $C(N+10,5)$. **3.** $A(N+300,3)$. **4.** $C(N+200,7)$.
5. $5!$. **6.** $A(N+10,3)$. **7.** $A(N+20,20)$. **8.** $A(N+20,20)$.
9. $P(N+15)$. **10.** $A(N+12,12)$. **11.** $C(N+10,3)$. **12.** $C(N+23,3)$.
13. $C(n,r)\cdot C(n-r,s)\cdot C(n-r-s,t)$. Число способов составления графика не зависит от порядка месяцев, ибо справедлива следующая последовательность равенств.

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

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

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

14. $C(n,r)\cdot C(n-r,s)\cdot C(n-r-s,t)$. (См. зад.13).
15. $C(n,r)\cdot C(n-r,s)\cdot C(n-r-s,t)$. (См. зад.13).
16. $C(n,r)\cdot C(n-r,s)\cdot C(n-r-s,t)$. (См. зад.13).
17. $C(n,r)\cdot C(n-r,s)\cdot C(n-r-s,t)$. (См. зад.13).
18. $C(n,r)\cdot C(n-r,s)\cdot C(n-r-s,t)$. (См. зад.13).
19. $A(n,r)\cdot A(n-r,s)\cdot A(n-r-s,t)$. Число способов составления наряда не зависит от порядка объектов охраны, ибо справедлива следующая последовательность раенств.

$$A(n,r)\cdot A(n-r,s) = A(n,s)\cdot A(n-s,r) \leftrightarrow$$

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

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

20. $A(n,r)\cdot A(n-r,s)\cdot A(n-r-s,t)$. (См. зад.19).
21. $n^1+n^2+n^3+\ldots+n^n$. **22.** 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.

1 2 ... $2N+8$
0 1 2 ... $2N+8$

23. а) $P(N+10)\cdot A((N+10)+2,N+5)$; б) $P(N+10)\cdot A(N+10,N+5)$.
24. Числа множества $\{1,2,\ldots,N+30\}-\{N,N+1\}$ 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 $N+23$ во-

зможностей 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.

1 2 3 4 5 ... N+23 N+24 N+25 N+26 N+27 N+28

0 1 2 3 4 5 6 ... N+22

6 ... N+23 N+24 N+25 N+26 N+27 N+28

25. 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

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

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

Три буквы l должны быть разделены в слове paraeogram хотя бы одной буквой. Ниже указыны 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 a r a e o g r a m буквы слова parallelogram без l

1 2 3 4 5 6 7 8 9 10 их позиции

0 1 2 3 4 5 6 7 8 9 10 позиции между ними

26. а) $n_a = {}_6A_4$.

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

в) числа четные заканчиваются на 2,6,8. $n_в = 3\cdot {}_5A_3$.

г) числа нечетные заканчиваются на 3,5,9. $n_г = 3\cdot {}_5A_3$.

д) пусть знак $\vdots$ означает "делится на". Число $\vdots 3$, если сумма его цифр делится на 3. Это любая перестановка чисел 2,5,8,a, где $a\in\{3,6,9\}$. $n_д = 3\cdot P_4$.

з) пусть знак $c(\vdots m)$ означает число (cardinality) чисел, которые $\vdots m$. Пусть знаки & и V означают "и" и "или" соответственно. Числа, которые $\vdots 3$ & $\vdots 2$ получатся, если из чисел, которые $\vdots 3$, 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 $n_з = c(\vdots 3 \,\&\, \vdots 2) = 5P_3$.

ж) $n_ж = c(\vdots 3 \vee \vdots 2) = c(\vdots 3) + c(\vdots 2) - c(\vdots 3 \,\&\, \vdots 2) = 3 \cdot P_4 + 3 \cdot {}_5A_3 - 5 \cdot P_3$.

е) пусть знак $\oplus$ означает "исключающее или". Тогда $n_е = c(\vdots 3 \oplus \vdots 2) = c(\vdots 3) + c(\vdots 2) - 2 \cdot c(\vdots 3 \,\&\, \vdots 2) = 3 \cdot P_4 + 3 \cdot {}_5A_3 - 2 \cdot 5 \cdot P_3 = 3 \cdot P_4 + 3 \cdot {}_5A_3 - 10 \cdot P_3$.

26–1. а) ${}_{N+24}\hat{A}_6 = 6^{N+4}$. б) это числа, начинающиеся с 2 и 3. Их число есть $2 \cdot 6^{N+23}$.

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 $x \vdots 3$, если сумма его цифр $\vdots 3$. 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. $S_2 \vdots 3$. 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 $P_{N+24}(N,i_1,i_2.i_3) = \dfrac{(N+24)!}{N!i_1!i_2!i_3!}$.

Ответ. Если сумма $2N$ всех двоек в x не кратна 3, то число обсуждаемых чисел равно нулю. Если $2N \vdots 3$, то число обсуждаемых чисел равно $\sum\limits_{i_1+i_2+i_3=24} P_{N+24} = \sum\limits_{i_1+i_2+i_3=24} \dfrac{(N+24)!}{N!i_1!i_2!i_3!}$.

27. 3^{N+15}. **28**. $26^{(N+7)/2}$, если $N+7$ четно; $26^{(N+7)/2} \cdot 26$, если $N+7$ нечетно. **29**. а) ${}_{26}A_2 \cdot 10^4$; б) $10^{N+24} \cdot {}_{N+25}C_2 \cdot 26^2$.

30. Найти число положительных натуральных чисел не больших N=1000 и

1) не делящихся ни на одно из чисел 3,5,7,
2) делящихся в точности на два числа из {3,5,7},
3) 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.

$$N(0) = \sum_{r=0}^{n} (-1)^r \sum_{1 \leqslant i_1 < i_2 < \ldots < i_r \leqslant n} N(i_1,i_2,\ldots,i_r);$$

$$N_{=k} = \sum_{j=0}^{n-k} (-1)^j \; C_{k+j}^{\,j} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{k+j} \leqslant n} N(i_1, i_2, \ldots, i_{k+j});$$

$$N_{\geqslant k} = \sum_{j=0}^{n-k} (-1)^j \; C_{k-1+j}^{\,k-1} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{k+j} \leqslant n} N(i_1, i_2, \ldots, i_{k+j}).$$

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 (табл.8.1).

Таблица 8.1

Свойство	Множество M чисел	Число чисел в M
1	$\{3k : k = 1,2,\ldots,333\}$	$N(1) = 333$
2	$\{5k : k = 1,2,\ldots,200\}$	$N(2) = 200$
3	$\{7k : k = 1,2,\ldots,142\}$	$N(3) = 142$
1,2	$\{15k : k = 1,2,\ldots,66\}$	$N(1,2) = 66$
1,3	$\{21k : k = 1,2,\ldots,47\}$	$N(1,3) = 47$
2,3	$\{35k : k = 1,2,\ldots,28\}$	$N(2,3) = 28$
1,2,3	$\{105k : k = 1,2,\ldots,9\}$	$N(1,2,3) = 9$

$$N(0) = 1000 - \sum_{1 \leqslant i \leqslant 3} N(i) + \sum_{1 \leqslant i < j \leqslant 3} N(i,j) - N(1,2,3) =$$

$1000 - (333 + 200 + 142) + (66 + 47 + 28) - 9 = 457.$

$$N_{=2} = \sum_{j=0}^{3-2} (-1)^j \; C_{2+j}^{\,j} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{2+j} \leqslant 3} N(i_1, i_2, \ldots, i_{2+j}) =$$

$$(-1)^0 C_2^0 \sum_{1 \leqslant i < j \leqslant 3} N(i,j) + (-1)^1 C_3^1 N(1,2,3) =$$

$1 \cdot (66+47+28) - 3 \cdot 9 = 104;$

$$N_{\geqslant 2} = \sum_{j=0}^{3-2} (-1)^j \; C_{2-1+j}^{\,j} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{2+j} \leqslant 3} N(i_1, i_2, \ldots, i_{2+j}) =$$

$$(-1)^0 C_1^1 \sum_{1 \leqslant i < j \leqslant 3} N(i,j) + (-1)^1 C_2^1 N(1,2,3) =$$

$1 \cdot (66+47+28) - 2 \cdot 9 = 113.$

10. МАТЕМАТИЧЕСКАЯ ЛОГИКА (Примеры решения)

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.

Решение. f = 0110100101001011.

	x	y	z	t	f
0	0	0	0	0	0
1	0	0	0	1	1
2	0	0	1	0	1
3	0	0	1	1	0
4	0	1	0	0	1
5	0	1	0	1	0
6	0	1	1	0	0
7	0	1	1	1	1
8	1	0	0	0	0
9	1	0	0	1	1
10	1	0	1	0	0
11	1	0	1	1	0
12	1	1	0	0	1
13	1	1	0	1	0
14	1	1	1	0	1
15	1	1	1	1	1

M_1 = {1,2,4,7,12,14,15}
M_0 = {0,3,4,6,8,10,11,13}

Карта Карно

xy \ zt	00	01	11	10	
$\bar{x}$ 00	0	1	0	1	$\bar{y}$
$\bar{x}$ 01	1	0	1	0	y
x 11	1	0	1	1	y
x 10	0	1	0	0	$\bar{y}$
	$\bar{t}$	t	$\bar{t}$		

($\bar{z}$: 00, 01; z: 11, 10)

Задача 2. Для данных формул построить таблицу истинностных значений и определить, является ли формула а) общезначимой, б) выполнимой, в) опровержимой, г) невыполнимой.

$$f(x,y,z) = \overline{(x \vee yz)} \equiv (x \vee y)(x \vee \bar{y} \cdot z).$$

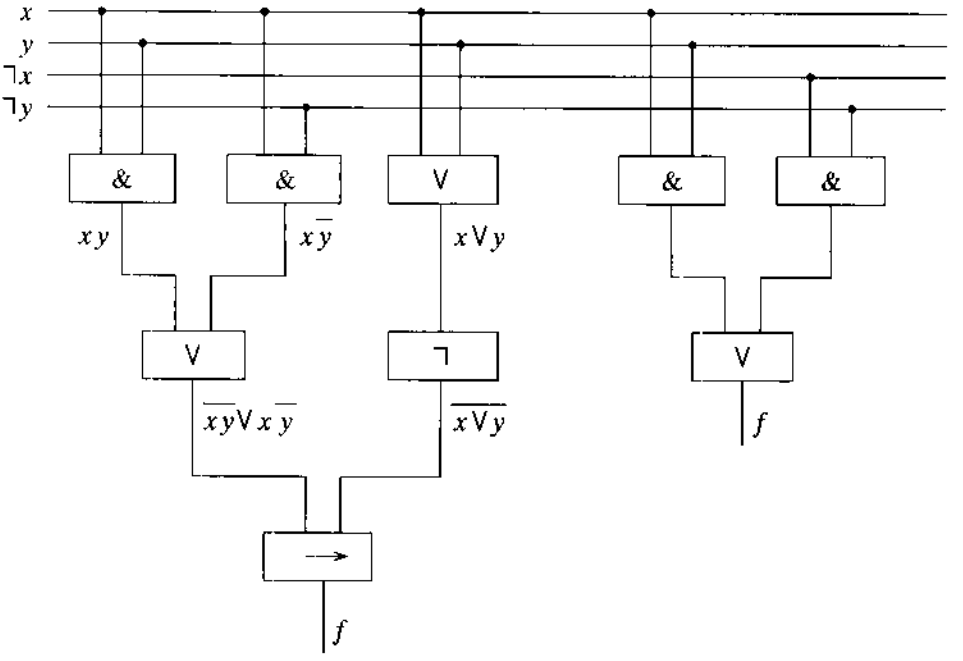
Решение.

	x	y	z	f
0	0	0	0	0
1	0	0	1	0
2	0	1	0	1
3	0	1	1	1
4	1	0	0	0
5	1	0	1	0
6	1	1	0	0
7	1	1	1	0

Формула f:
а) общезначимой не является,
б) выполнима (строки 2,3),
в) опровержима (строки 0,1,4–7),
г) невыполнимой не является.

Задача 3. Для данной формулы $f(x,y) = (\overline{xy} \vee x\overline{y}) \to \overline{x \vee y}$ построить таблицу истинностных значений, упростить формулы и построить для обеих схемы из фукнциональных элементов для дизъюнкции, конъюнкции, отрицания, импликации.

Решение. $f(x,y) = (\overline{xy} \vee x\overline{y}) \to \overline{x \vee y} = \overline{\overline{xy}} \,\&\, \overline{x\overline{y}} \vee \overline{x} \& \overline{y} =$
$xy(\overline{x} \vee y) \vee \overline{x}\,\overline{y} = xy \vee \overline{x}\,\overline{y}.$
Подформулы формулы f.
$\overline{xy} \vee x\overline{y}, \quad \overline{x \vee y}$
$xy, \quad x\overline{y}, \quad x \vee y.$



Задача 4. 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. Многочлен Жегалкина

$$f(x_1,x_2,\ldots,x_n) = \sum_{(i_1 i_2 \ldots i_n)\in E_2^n} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

где $a_{i_1 i_2 \ldots i_n} \in \{0,1\}$; $x^0=1$, $x^1=x$.

	x	y	z	f
0	0	0	0	1
1	0	0	1	0
2	0	1	0	1
3	0	1	1	0
4	1	0	0	1
5	1	0	1	1
6	1	1	0	0
7	1	1	1	1

СДНФ. $f=\bar{x}\bar{y}\bar{z}\vee\bar{x}y\bar{z}\vee x\bar{y}\bar{z}\vee x\bar{y}z\vee xyz$

СКНФ. $f=(x\vee y\vee\bar{z})(x\vee\bar{y}\vee\bar{z})(\bar{x}\vee\bar{y}\vee z)$

Многочлен (полином) Жегалкина

$$f=\bar{x}\bar{y}\bar{z}\vee\bar{x}y\bar{z}\vee x\bar{y}\bar{z}\vee x\bar{y}z\vee xyz =$$
$$(x+1)(y+1)(z+1)+(x+1)y(z+1)+$$
$$x(y+1)(z+1)+x(y+1)z+xyz =$$
$$xyz+xy+xz+yz+x+y+z+1 +$$
$$xyz+xy+yz+y + xyz+xy+xz+x +$$
$$xyz+xz + xyz = xyz+xy+xz+z+1.$$

Задача 5. Найти все тупиковые и все минимальные ДНФ и КНФ для всюду определенной функции. Одну из минимальных форм реализовать схемой с элементами для $\&, \vee, \neg$.

10.1. Алгоритм минимизации функций в классе нормальных форм

Пусть f – функция алгебры логики.

1. Строим все МДНФ функции f.
2. Строим все МКНФ функции f.
3. Из построенных минимальных форм выбираем простейшие (по числу букв).

Пример. В классе нормальных форм минимизировать функцию f = 01011110.

1. Строим СДНФ для функции f:

$$f(x,y,z) = \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee x\bar{y}z \vee xy\bar{z}.$$

2. Строим сокращенную ДНФ функции f:

$$f(x,y,z) = (x\vee y\vee z)(x\vee\bar{y}\vee z)(\bar{x}\vee\bar{y}\vee\bar{z}) =$$
$$(x\vee x\bar{y}\vee x\bar{z}\vee xy\vee y\bar{y}\vee yz\vee xz\vee\bar{y}z\vee zz)(\bar{x}\vee\bar{y}\vee\bar{z}) = (x\vee z)(\bar{x}\vee\bar{y}\vee\bar{z}) =$$
$$x\bar{x} \vee x\bar{y} \vee x\bar{z} \vee \bar{x}z \vee \bar{y}z \vee z\bar{z} = \bar{x}z \vee \bar{y}z \vee x\bar{y} \vee x\bar{z}.$$

3. Строим матрицу покрытий (табл.9.1).

Таблица 9.1

N	ПИ	$\bar{x}\bar{y}z$	$\bar{x}yz$	$x\bar{y}\bar{z}$	$x\bar{y}z$	$xy\bar{z}$
1	$\bar{x}z$	+	+			
2	$\bar{y}z$	+			+	
3	$x\bar{y}$			+	+	
4	$x\bar{z}$			+		+

Решеточное выражение $E = (1 \vee 2)1(3 \vee 4)4 = 134 \vee 124$.

4. Строим все тупиковые ДНФ функции f:

$f(x,y,z) = \bar{x}z \vee x\bar{y} \vee x\bar{z}$; $f(x,y,z) = \bar{x}z \vee \bar{y}z \vee x\bar{z}$.

5. Обе построенные ТДНФ являются минимальными.

6. Повторяем эти этапы для функции $\bar{f}$.

СДНФ: $\bar{f}(x,y,z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}y\bar{z} \vee xyz$.
Сокращенная ДНФ.

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

$(x \vee \bar{z})(\bar{x} \vee y)(\bar{x} \vee \bar{y} \vee z) = (x \vee \bar{z})(\bar{x} \vee yz) = xyz \vee \bar{x}\bar{z}$.

Строим матрицу покрытий (табл.9.2).

Решеточный многочлен $E = 112 = 12$. Единственная тупиковая ДНФ (она же минимальная) для функции $\bar{f}(x,y,z) = \bar{x}\bar{z} \vee xyz$. Минимальная КНФ функции $f(x,y,z) = (x \vee z)(\bar{x} \vee \bar{y} \vee \bar{z})$. Из построенных МДНФ и МКНФ выбираем простейшую:

$f(x,y,z) = (x \vee z)(\bar{x} \vee \bar{y} \vee \bar{z})$.

Пример. В классе нормальных форм минимизировать функцию $f = 11011011$.

Таблица 9.2

N	ПИ	$\bar{x}\bar{y}\bar{z}$	$\bar{x}y\bar{z}$	xyz
1	$\bar{x}\bar{z}$	+	+	
2	xyz			+

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.9.3).

Таблица 9.3

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	$\bar{x}\bar{y}$	+	+				

$E = (3 \vee 6)(4 \vee 6)(4 \vee 5)(2 \vee 3)(1 \vee 2)(1 \vee 5) = 1246 \vee 1356 \vee 134 \vee 256 \vee 2345$.

4. 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. Минимальные ДНФ функции f:

$f(x,y,z) = xy \vee \bar{y}\bar{z} \vee \bar{x}z$; $f(x,y,z) = x\bar{z} \vee yz \vee \bar{x}\bar{z}$.

6. Повторяем указанные выше этапы для функции $\bar{f}$.

СДНФ: $\bar{f}(x,y,z) = \bar{x}y\bar{z} \vee x\bar{y}z$.

Сокращенная ДНФ: $\bar{f}(x,y,z) = (x \vee y \vee z)(x \vee y \vee \bar{z})$ & $(x \vee \bar{y} \vee \bar{z})(\bar{x} \vee y \vee z)(\bar{x} \vee \bar{y} \vee z)(\bar{x} \vee \bar{y} \vee \bar{z}) = (x \vee y)(x \vee \bar{y} \vee \bar{z})(\bar{x} \vee y \vee z)(\bar{x} \vee \bar{y}) = (x \vee y\bar{z})(\bar{x} \vee \bar{y}z) = \bar{x}y\bar{z} \vee x\bar{y}z$.

Построенная сокращенная ДНФ функции $\bar{f}$ является для нее

тупиковой и минимальной.

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:

$f(x,y,z) = xy \vee \bar{y}\bar{z} \vee \bar{x}z;$

$f(x,y,z) = x\bar{z} \vee yz \vee \bar{x}\bar{z};$

$f(x,y,z) = (x \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z}).$

Задача 6. Для заданной всюду определенной функции $f(x_1, x_2, x_3, x_4)$ построить минимальную ДНФ методом Квайна–МакКласски. Каждая функция задана множеством M_1 десятичных эквивалентов двоичных наборов, на которых функция принимает значение 1.

10.2. Алгоритм Квайна–Мак–Класски построения минимальной ДНФ функции f

I. Найти все максимальные интервалы.

1. Разбить множество наборов из $M_1(f)$ на группы по количеству единиц.

2. Произвести всевозможные "склейки" наборов соседних групп, отметив знаком + наборы, участвовавшие в склейке.

3. Разбить полученное множество интервалов на группы, в которых компонента * стоит на одном и том же месте, а внутри групп – на подгруппы по количеству единиц. Если среди полученных интервалов есть одинаковые, то повторы удалить.

4. Произвести в каждой группе всевозможные "склейки" наборов соседних подгрупп, отметив знаком + интервалы, участвовавшие в склейке.

5. Выполнять пункты 3,4 до тех пор, пока это возможно.

6. Множество всех непомеченных интервалов есть множество всех максимальных интервалов.

II. Найти минимальное покрытие множества $M_1(f)$ максимальными интервалами (покрыть двоичную матрицу, в которой строке соответствуют интервалы, а столбцам – наборы из M_1).

Пример. Для функции $f(x,y,z,t) = \{0,3,4,7,8,9,10,11,12, 13,14,15\}$ построить минимальную ДНФ методом Квайна-МакКласски. Для функции f построить карту Карно и по ней найти все

простые импликанты и все максимальные интервалы.

I. Нахождение всех максимальных интервалов.

1. Разобъем множество наборов из M_1 на группы по количеству единиц.

Группа 1	Группа 2	Группа 3	Группа 4	Группа 5
0000 (0)+	0100 (4)+	0011 (3) +	0111 (7) +	1111 (15)+
	1000 (8)+	1001 (9) +	1011 (11)+	
		1010 (10)+	1101 (13)+	
		1100 (12)+	1110 (14)+	

2. Произведем всевозможные "склейки" наборов соседних групп, отметим знаком "+" наборы, участвовавшие в склейке (в предыдущем пункте). Получим следующие группы интервалов.

Группа 1	Группа 2	Группа 3	Группа 4
0*00 (0,4)	*100 (4,12)	0*11 (3,7)	*111 (7,15)
*000 (0,8)	100* (8,9)	*011 (3,11)	1*11 (11,15)
	10*0 (8,10)	10*1 (9,11)	11*1 (13,15)
	1*00 (8,12)	1*01 (9,13)	111* (14,15)
		101* (10,11)	
		1*10 (10,14)	
		110* (12,13)	
		11*0 (12,14)	

3. Разобьем полученное множество интервалов на группы, в которых компонента * стоит на одном и том же месте, а внутри групп – на подгруппы по количеству единиц. Если среди полученных интервыалов есть одинаковые, оставим по одному экземпляру (в нашем примере таких нет). Плюсы поставлены по пункту 4.

Группа 1	Группа 2	Группа 3	Группа 4
*000 (0,8) +	0*00 (0,4) +	10*0 (8,10) +	100* (8,9) +
*100 (4,12)+	1*00 (8,12) +	10*1 (9,11) +	101* (10,11)+
		11*0 (12,14)+	110* (12,13)+
*011 (3,11)+	0*11 (3,7) +		
	1*01 (9,13) +	11*1 (13,15)+	111* (14,15)+
*111 (7,15)+	1*10 (10,14)+		
	1*11 (11,15)+		

4. Произведем всевозможные "склейки" в каждой группе между наборами соседних подгрупп. Пометим знаком + интервалы, участвовавшие в склейке (в пункте 3).

Группа 1	Группа 2
**00 ((0,8),(4,12))	**00 ((0,4),(8,12)) повтор
**11 ((3,11),(7,15))	1*0* ((8,12),(9,13))
	1**0 ((8,12),(10,14)) повтор
	**11 ((3,7),(11,15)) повтор
	1**1 ((9,13),(11,15)) повтор
	1*1* ((10,14),(11,15))
Группа 3	Группа 4
10** ((8,10),(9,11))	10** ((8,9),(10,11)) повтор
1**0 ((8,10),(12,14))	1*0* ((8,9),(12,13)) повтор
1**1 ((9,11),(13,15))	1*1* ((10,11),(14,15)) повтор
11** ((12,14)(13,15))	11** ((12,13),(14,15)) повтор

Удалим повторы и получим интервалы:

**00 ((0,8),(4,12)) **11 ((3,11),(7,15))
1*0* ((8,12),(9,13)) 1*1* ((10,14),(11,15))
10** ((8,10),(9,11)) 1**0 ((8,10),(12,14))
1**1 ((9,11),(13,15)) 11** ((12,14)(13,15))

5. Разобъем полученное множество интервалов (без повто-

ров) на группы, в которых компоненты * стоят на одном и том же месте, а внутри групп – на подгруппы по количеству единиц. Если среди полученных интервалов есть одинаковые, то оставим по одному экземпляру.

Группа 1	Группа 2
**00 ((0,8),(4,12))	1**0 ((8,10),(12,14))+
**11 ((3,11),(7,15))	1**1 ((9,11),(13,15))+
Группа 3	Группа 4
1*0* ((8,12),(9,13)) +	10** ((8,10),(9,11)) +
1*1* ((10,14),(11,15))+	11** ((12,14)(13,15))+

6. Произведем всевозможные "склейки" в каждой группе между наборами соседних подгрупп. Пометим знаком + интервалы, участвовавшие в склейке (в пункте 5).

Группа 1 без изменений: склеек нет.

**00 ((0,8),(4,12))
**11 ((3,11),(7,15))

Группа 2
1*** (((8,10),(12,14)),((9,11),(13,15)))

Группа 3
1*** (((8,12),(9,13)),((10,14),(11,15))) повтор

Группа 4
1*** (((8,10),(9,11)),((12,14),(13,15))) повтор

7. Дальнейшие склейки в группах невозможны. Получили максимальные интервалы: **00, **11, 1*** (собраны интервалы непомеченные плюсами).

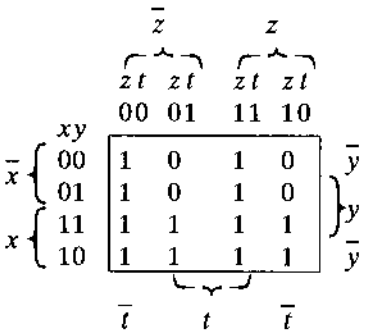
II. Нахождение минимального покрытия множества M_1 максимальными интервалами (для этого находим минимальное покрытие столбцов нижеуказанной матрицы строками).

		0	0	0	0	1	1	1	1	1	1	1	1
		0	0	1	1	0	0	0	0	1	1	1	1
		0	1	0	1	0	0	1	1	0	0	1	1
		0	1	0	1	0	1	0	1	0	1	0	1
1	**00 +		+		+					+			
2	**11	+		+					+				+
3	1***					+	+	+	+	+	+	+	+

Решеточное выражение E=1212(1V3)33(2V3)(1V3)33(2V3)=123.

Единственному слагаемому 123 соответствует минимальная ДНФ $f = \overline{z}\,\overline{t} \vee zt \vee x$.

III. Построим карту Карно и найдем по ней все простые импликанты и все максимальные интервалы.



Простые импликанты: $\overline{z}\,\overline{t}$, zt, x. Соответствующие максимальные интервалы: **00, **11, 1***.

Задача 7. Найти все тупиковые и все минимальные ДНФ и КНФ для частично определенной функции. Одну из минимальных форм реализовать схемой с элементами &, V, ¬.

10.3. Алгоритм минимизации частично определенных функций в классе ДНФ

1. Строим СДНФ функции f_0.
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 нормаьных форм для всюду определенных функций.

Пример. В классе нормальных форм минимизировать частично определенную функцию $f(x,y,z,t) = 1{-}{-}{-}010010{-}01{-}{-}1$.

Решение. Минимизируем функцию f в классе ДНФ.

1. Строим сокращенную ДНФ для доопределения единицами f_1 функции f (табл.9.4).

$$f_1(x,y,z,t) =$$
$$(x\vee\bar{y}\vee z\vee t)(x\vee\bar{y}\vee\bar{z}\vee t)(x\vee\bar{y}\vee\bar{z}\vee\bar{t})(\bar{x}\vee y\vee z\vee\bar{t})(\bar{x}\vee y\vee\bar{z}\vee\bar{t}) =$$
$$(x\vee\bar{y}\vee t)(xy\vee\bar{x}\bar{y}\vee\bar{z}\vee\bar{t})(\bar{x}\vee y\vee z\vee\bar{t}) =$$
$$(x\vee\bar{y}\vee t)(xy\vee\bar{x}\bar{y}\vee\bar{x}\bar{z}\vee yz\vee\bar{z}\bar{t}\vee\bar{x}\bar{t}\vee y\bar{t}\vee z\bar{t}\vee t) =$$
$$x\vee\bar{y}\vee t)(xy\vee\bar{x}\bar{y}\vee\bar{x}\bar{z}\vee y\bar{z}\vee\bar{t}) =$$
$$y\vee xyz\vee x\bar{t}\vee\bar{x}\bar{y}\vee\bar{x}\bar{y}z\vee\bar{y}\bar{t}\vee xyt\vee\bar{x}\bar{y}\bar{t}\vee\bar{x}\bar{z}t\vee y\bar{z}t =$$
$$xy \vee x\bar{t} \vee \bar{y}\bar{t} \vee \bar{x}\bar{y} \vee \bar{x}\bar{z}t \vee y\bar{z}t.$$

2. Строим матрицу покрытий конституент единицы в СДНФ для доопределения нулями f_0 функции f с помощью построенной сокращенной ДНФ для f_1 (табл.9.5).

3. По табл.1.14 строим решеточный многочлен

$$E = (2\vee4)(5\vee6)(3\vee4)(1\vee3)1 = 145 \vee 1235 \vee 146 \vee 1236.$$

4. Строим все тупиковые ДНФ:

$g_1 = xy \vee \bar{y}\bar{t} \vee \bar{x}\bar{z}t$; $\quad g_3 = xy \vee \bar{y}\bar{t} \vee y\bar{z}t$;

$g_2 = xy \vee \bar{x}\bar{y} \vee x\bar{t} \vee \bar{x}\bar{z}t$; $\quad g_4 = xy \vee \bar{x}\bar{y} \vee x\bar{t} \vee y\bar{z}t$.

Таблица 9.4

$xyzt$	f	f_0	f_1	$\bar{f}$	h_0	h_1
0000	1	1	1	0	0	0
0001	–	0	1	–	0	1
0010	–	0	1	–	0	1
0011	–	0	1	–	0	1
0100	0	0	0	1	1	1
0101	1	1	1	0	0	0
0110	0	0	0	1	1	1
0111	0	0	0	1	1	1
1000	1	1	1	0	0	0
1001	0	0	0	1	1	1
1010	–	0	1	–	0	1
1011	0	0	0	1	1	1
1100	1	1	1	0	0	0
1101	–	0	1	–	0	1
1110	–	0	1	–	0	1
1111	1	1	1	0	0	0

Таблица 9.5

N	ПИ	$\bar{x}\bar{y}\bar{z}\bar{t}$	$\bar{x}y\bar{z}t$	$x\bar{y}\bar{z}\bar{t}$	$xy\bar{z}\bar{t}$	$xyzt$
1	xy				+	+
2	$\bar{x}\bar{y}$	+				
3	$x\bar{t}$			+	+	
4	$\bar{y}\bar{t}$	+		+		
5	$\bar{x}\bar{z}t$		+			
6	$y\bar{z}t$		+			

5. 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.

Минимизируем теперь функцию 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. Сокращенная ДНФ для

$$h_1 = (x \vee y \vee z \vee t)(x \vee \bar{y} \vee z \vee \bar{t})(\bar{x} \vee y \vee z \vee t)(\bar{x} \vee \bar{y} \vee z \vee t)(\bar{x} \vee \bar{y} \vee \bar{z} \vee \bar{t}) =$$

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

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

$$\bar{y}t \vee x\bar{y}z \vee xz\bar{t} \vee x\bar{z}t \vee \bar{x}z \vee \bar{y}z \vee z\bar{t} \vee \bar{x}y\bar{t} \vee yz\bar{t} = \bar{y}t \vee \bar{x}z \vee z\bar{t} \vee x\bar{z}t \vee \bar{x}y\bar{t} \vee \bar{y}z.$$

2. Матрица покрытий конституент единицы в СДНФ для h_0 с помощью простых импликант в сокращенной ДНФ для h_1 приведена в табл.9.6.

Таблица 9.6

N	ПИ	$\bar{x}y\bar{z}\bar{t}$	$\bar{x}yz\bar{t}$	$\bar{x}yzt$	$x\bar{y}\bar{z}t$	$x\bar{y}zt$
1	$\bar{y}t$				+	+
2	$\bar{x}z$		+	+		
3	$z\bar{t}$		+			
4	$x\bar{z}t$				+	
5	$\bar{x}y\bar{t}$	+	+			
6	$\bar{y}z$					+

3. Решеточное выражение
$E = 5(2\vee3\vee5)2(1\vee4)(1\vee6) = 25(1\vee46) = 125 \vee 2456.$

4. Строим две тупиковые ДНФ:

$$g_5 = \bar{y}t \vee \bar{x}z \vee \bar{x}y\bar{t} \text{ и } g_6 = \bar{x}z \vee x\bar{z}t \vee \bar{x}y\bar{t} \vee \bar{y}z.$$

Минимальная ДНФ $g_5 = \bar{y}t \vee \bar{x}z \vee \bar{x}y\bar{t}$.

5. 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 доопреелениями функции f в классе нормальных форм.

Задача 8. Минимизировать всюду определенную функцию алгебры логики из задачи 4 и частично определенную функцию из задачи 6 с помощью карт Карно.

Решение. Минимизация с помощью карт Карно показана в примере задачи 9.

Задача 9. Построить минимальные ДНФ системы функций $f_1(x, y, z)$, $f_2(x, y, z)$, $f_3(x, y, z)$ и реализовать их 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. Строим все возможные конъюнкции: $f_1\&f_2$=00100101, $f_1\&f_3$=01100101, $f_2\&f_3$=00100101, $f_1\&f_2\&f_3$=00100101.

	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

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).

Функция	Сокращенная ДНФ	Максимальные интервалы
$f_1 =$	$z \vee \bar{x}y$	$n_1=**1, n_2=01*$
$f_2 =$	$xz \vee xy \vee y\bar{z} \vee \bar{x}\bar{z}$	$n_3=1*1, n_4=11*, n_5=*10, n_6=0*0$
$f_3 =$	$xz \vee \bar{y}z \vee x\bar{y} \vee \bar{x}y\bar{z}$	$n_3=1*1, n_7=*01, n_8=10*, n_9=010$
$f_1 \& f_2 =$	$xz \vee \bar{x}y\bar{z}$	$n_3=1*1, n_9=010$
$f_1 \& f_3 =$	$xz \vee \bar{y}z \vee \bar{x}y\bar{z}$	$n_3=1*1, n_7=*01, n_9=010$
$f_2 \& f_3 =$	$xz \vee \bar{x}y\bar{z}$	$n_3=1*1, n_9=010$
$f_1 \& f_2 \& f_3 =$	$xz \vee \bar{x}y\bar{z}$	$n_3=1*1, n_9=010$

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: 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,

где $n_1=**1, n_2=01*, n_3=1*1, n_4=11*, n_5=*10, n_6=0*0, n_7=*01, n_8=10*$, $n_9=010$. Строим таблицы покрытий для f_1, f_2, f_3.

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.

$n_1 n_2$, $f_1=z \vee \bar{x}y$,

$n_1 n_9$, $f_1=z \vee \bar{x}y\bar{z}$,

$n_2 n_3 n_7$, $f_1=\bar{x}y \vee xz \vee \bar{y}z$.

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 $E_2=n_6(n_5 \vee n_6 \vee n_9)n_3 \& (n_4 \vee n_5)(n_3 \vee n_4) = n_3n_4n_6 \vee n_3n_5n_6$.

Максимальные интервалы и тупиковые ДНФ для f_2.

$n_3n_4n_6$, $f_2=xz \vee xy \vee \bar{x}\bar{z}$,

$n_3n_5n_6$, $f_2=xz \vee y\bar{z} \vee \bar{x}\bar{z}$.

f_3	001	010	100	101	111
n_3=1*1				+	+
n_7=*01	+			+	
n_8=10*			+	+	
n_9=010		+			

Решеточное выражение $E_3=n_7n_9n_8(n_3 \vee n_7 \vee n_8)n_3 = n_3n_7n_8n_9$.

Максимальные интервалы и тупиковые ДНФ для f_3.

$n_3n_7n_8n_9$, $f_3=xz \vee \bar{x}y \vee x\bar{y} \vee \bar{x}\bar{z}$.

Решеточное выражение $E_1 \& E_2 \& E_3$ =

$[(n_1 \vee n_7)(n_2 \vee n_9)(n_1 \vee n_2)(n_1 \vee n_3 \vee n_7)(n_1 \vee n_3)]$ & для f_1
$[n_6(n_5 \vee n_6 \vee n_9)n_3(n_4 \vee n_5)(n_3 \vee n_4)]$ & для f_2
$[n_7n_9n_8(n_3 \vee n_7 \vee n_8)n_3]$ = для f_3

$n_1n_3n_4n_6n_7n_8n_9 \vee n_1n_3n_5n_6n_7n_8n_9 \vee n_2n_3n_4n_6n_7n_8n_9 \vee n_2n_3n_5n_6n_7n_8n_9$.

Все дизъюнктивные слагаемые содержат по 7 сомножителей. Для дальнейшего выбираем любое, например, первое:

$n_1n_3n_4n_6n_7n_8n_9$.

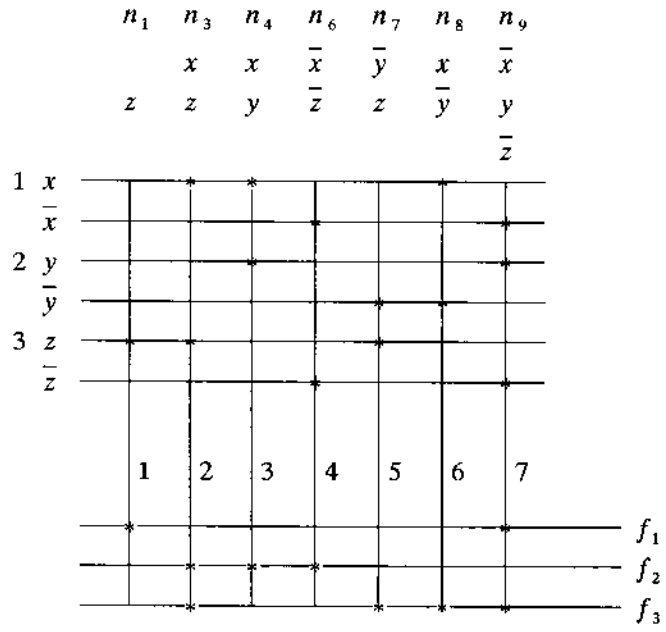
Функции f_1, f_2, f_3 реализуем следующими максимальными интервалами и соответствующими тупиковыми ДНФ. Максимальные интервалы содержатся среди $n_1, n_3, n_4, n_6, n_7, n_8, n_9$.

f_1: n_1n_9, $f_1 = z \vee \bar{x}y\bar{z}$,

f_2: $n_3n_4n_6$, $f_2 = xz \vee xy \vee \bar{x}\bar{z}$,

f_3: $n_3n_7n_8n_9$, $f_3 = xz \vee \bar{y}z \vee x\bar{y} \vee \bar{x}y\bar{z}$.

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 4 две последние функции и функцию своего варианта. 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 четырех функций реализовать на ПЛМ. Сравнить две реализации и указать, какая из них экономнее.

10.6. Алгоритм совместной минимизации системы из k функций (жадный алгоритм приближенной минимизации)

1. Найти все простые импликанты функции $f_1 \& f_2 \& \ldots \& f_k$. Выбрать минимальное покрытие ее единиц ппростыми импликантами.

Перевести область общих единиц в область неопределенности для каждой из данных функций.

2. Применять пункт 1, пока это возможно, по всем возможным произведениям $f_{i_1}\&f_{i_2}\&\ldots\&f_{i_t}$, где

$\{i_1,i_2,\ldots,i_t\} \subseteq \{1,2,\ldots,k\}$, $t=k-1,k-2,\ldots,3,2,1$.

Пример. f_1=0011 0101 0101 1111, f_2=0011 0111 0011 0011, f_3=0000 0011 0111 1100.

Решение. Для функций f_1,f_2,f_3 заполняем карты Карно.

xy \ zt	00	01	11	10
00	0	0	1	1
01	0	1	1	0
11	0	1	1	0
10	1	1	1	1

$f_1(x,y,z,t)$

xy \ zt	00	01	11	10
00	0	0	1	1
01	0	1	1	0
11	0	1	1	0
10	1	1	1	1

$f_2(x,y,z,t)$

xy \ zt	00	01	11	10
00	0	0	1	1
01	0	1	1	0
11	0	1	1	0
10	1	1	1	1

$f_3(x,y,z,t)$

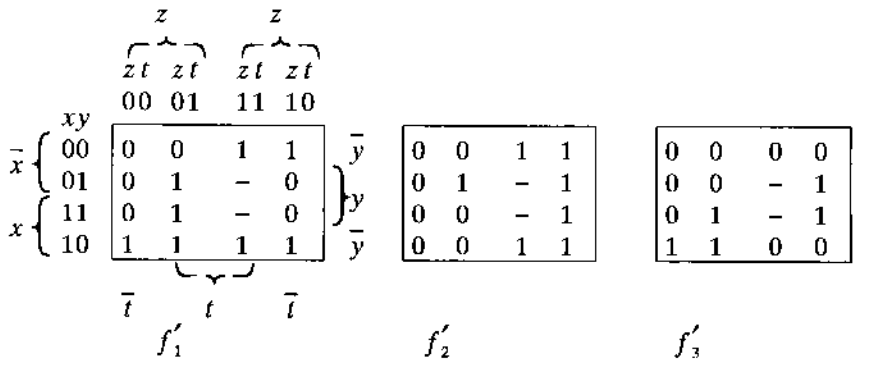
Строим функцию $f_1\&f_2\&f_3$ и находим ее карту Карно.

xy \ zt	00	01	11	10
00	0	0	0	0
01	0	0	1	0
11	0	0	1	0
10	0	0	0	0

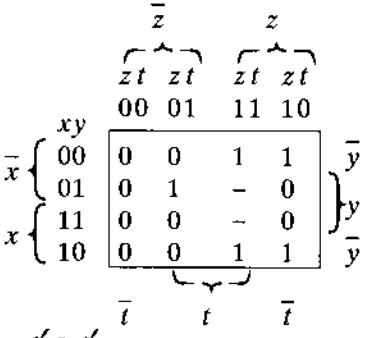
Две единицы функции $f_1\&f_2\&f_3$ покрывает ДНФ

$$d_{f_1f_2f_3} = yzt.$$

Переводим единицы функции единицы функции $f_1\&f_2\&f_3$ в область неопределенности функций f_1,f_2,f_3 и получаем функции f_1',f_2',f_3', задаваемыми следующими картами Карно.



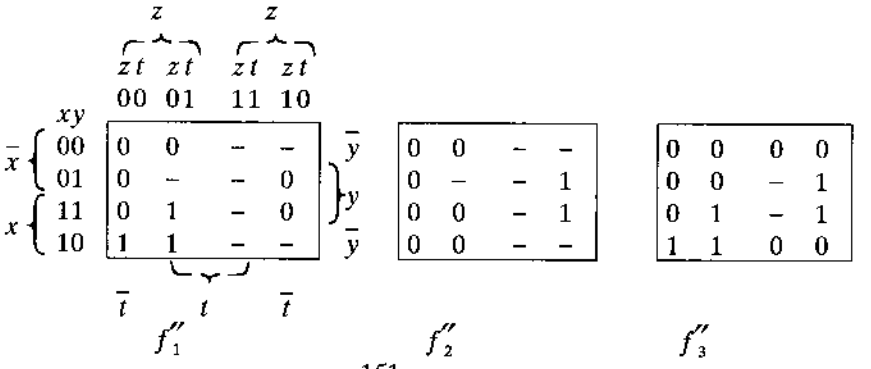
Строим функцию $f'_1 \& f'_2$ и находим ее карту Карно.



Единицы функции $f'_1 \& f'_2$ покрывает ДНФ

$$d_{f'_1 f'_2} = \bar{y}z \vee \bar{x}yt.$$

Переводим единицы функции $f'_1 \& f'_2$ в область неопределенности функций f'_1, f'_2 и получаем функции f''_1, f''_2, f''_3 ($f''_3 = f'_3$), задаваемыми следующими картами Карно.



Строим функцию $f_1''\&f_3''$ и находим ее карту Карно.

xy \ zt	$\bar{z}\bar{t}$	$\bar{z}t$	$z\bar{t}$	zt	
$\bar{x}\bar{y}$	0	0	0	0	$\bar{y}$
$\bar{x}y$	0	0	–	0	y
$x\bar{y}$	0	1	–	0	y
xy	1	1	0	0	$\bar{y}$
	$\bar{t}$	t		$\bar{t}$	

Единицы функции $f_1''\&f_3''$ покрывает ДНФ

$$d_{f_1''f_3''} = x\bar{z}t \vee x\bar{y}\bar{z}.$$

Переводим единицы функции $f_1''\&f_3''$ в область неопределенности функций f_1'', f_3'' и получаем функции f_1''', f_2''', f_3''', $(f_2''' = f_2'')$ задаваемыми следующими картами Карно.

xy \ zt	$\bar{z}\bar{t}$	$\bar{z}t$	$z\bar{t}$	zt	
$\bar{x}\bar{y}$	0	0	–	–	$\bar{y}$
$\bar{x}y$	0	–	–	0	y
$x\bar{y}$	0	1	–	0	y
xy	1	1	–	–	$\bar{y}$
	$\bar{t}$	t		$\bar{t}$	

f_1'''

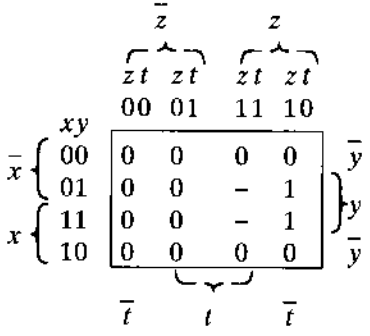
0	0	–	–
0	–	–	1
0	0	–	1
0	0	–	–

f_2'''

0	0	0	0
0	0	–	1
0	1	–	1
1	1	0	0

f_3'''

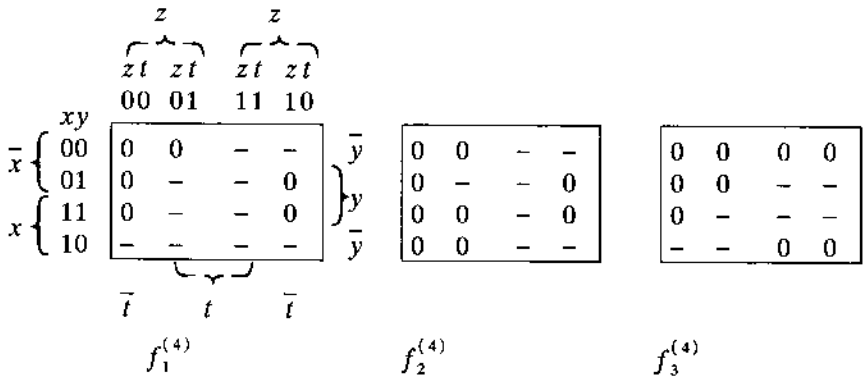
Строим функцию $f_2'''\&f_3'''$ и находим ее карту Карно.



Единицы функции $f_2'''\&f_3'''$ покрывает ДНФ

$$d_{f_2'''f_3'''} = yz.$$

Переводим единицы функции $f_2'''\&f_3'''$ в область неопределености функций f_2''', f_3''' и получаем функции $f_1^{(4)}, f_2^{(4)}, f_3^{(4)}$ ($f_1^{(4)}=f_1^{(3)}$), задаваемыми следующими картами Карно.



Единицы исчерпаны. Строим ДНФ-представления функций.

$$f_1(x,y,z) = d_{f_1f_2f_3} \vee d_{f_1'f_2'} \vee d_{f_1''f_3''},$$

$$f_2(x,y,z) = d_{f_1f_2f_3} \vee d_{f_1'f_2'} \vee d_{f_2'''f_3'''},$$

$$f_3(x,y,z) = d_{f_1f_2f_3} \vee d_{f_1''f_3''} \vee d_{f_2'''f_3'''},$$

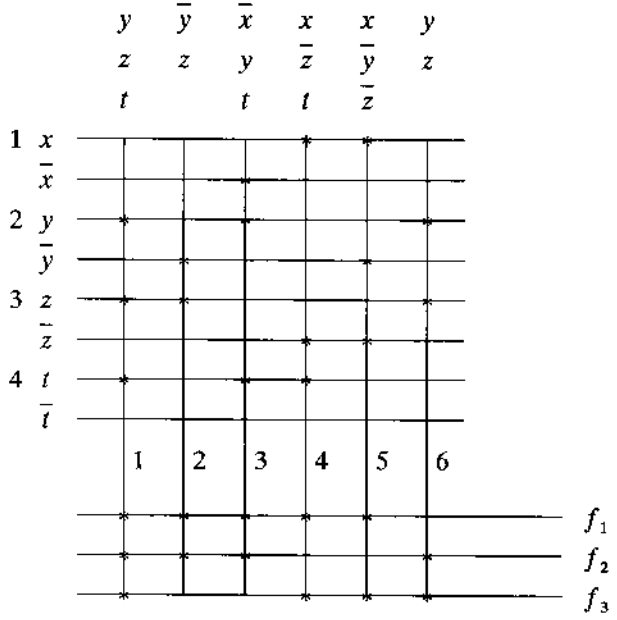
То есть

$$f_1(x,y,z) = yzt \vee \bar{y}z \vee \bar{x}yt \vee x\bar{z}t \vee x\bar{y}\bar{z},$$

$$f_2(x,y,z) = yzt \vee \bar{y}z \vee \bar{x}yt \vee yz,$$

$$f_3(x,y,z) = yzt \vee x\bar{z}t \vee x\bar{y}\bar{z} \vee yz.$$

Программируемая логическая матрица (ПЛМ), реализующая функции f_1, f_2, f_3 одновременно.



ПЛМ имеет размер (4,6,3), где 4 – местность функций, 6 – ширина ПЛМ, 3 – число реализуемых функций.

Замечание. Возможна совместная минимизаация нескольких частично определенных функций. Конъюнкция значений функций проводится в соответствии с операцией &, определяемой 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.

Теорема (Поста). 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.

Двойственной для функции $f(x_1,\ldots,x_n)$ называется функция $f^*(x_1,\ldots,x_n) = \overline{f}(\overline{x}_1,\ldots,\overline{x}_n)$.

Функция, совпадающая со своей двойственной, называется *самодвойственной*.

Теорема. Чтобы функция была самодвойственной, необходимо и достаточно, чтобы на всяких двух противоположных наборах она принимала разные значения.

Многочлен Жегалкина в поле F есть выражение

$$\sum_{(i_1,\ldots,i_n)\in E_2^n} a_{i_1,i_2,\ldots,i_n}\ x_1^{i_1}\ x_2^{i_2}\ \ldots\ x_n^{i_n},\ \text{где}$$

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

а каждый коэффициент $a_{i_1,i_2,\ldots,i_n}$ равен 0 или 1.

Пример. Многочлен Жегалкина для функции

$$f(x,y,z) = \overline{x}\,\overline{y}z \vee \overline{x}yz \vee x\overline{y}z \vee xy\overline{z} \vee xyz =$$
$$(x+1)(y+1)z + (x+1)yz + x(y+1)z + xy(z+1)+xyz =$$
$$xyz+xz+yz+z + xyz+yz + xyz+xz + xyz+xy + xyz =$$
$$xyz + xy + z.$$

Многочлен Жегалкина можно получить с помощью треугольника Паскаля (табл.9.7). Многочлен записывается по левой стороне треугольника.

Тогда $g(x,y,z) = 1 + z + y + xz + xy + xyz$.

Функция $f(x_1,\ldots,x_n)$ называется *линейной*, если многочлен Жегалкина для нее имеет линейный относительно переменных вид: $f(x_1,\ldots,x_n) = a_1x_1 + \ldots + a_nx_n + a_{n+1}$, где каждое a_i равно 0 или 1.

Таблица 9.7

N	xyz	f g	Треугольник Паскаля
1	000	0 1	g = 1 0 0 1 1 1 1 0
z	001	1 0	1 0 1 0 0 0 1
y	010	0 0	1 1 1 0 0 1
yz	011	1 1	0 0 1 0 1
x	100	0 1	0 1 1 1
xz	101	1 1	1 0 0
xy	110	1 1	1 0
xyz	111	1 0	1

Функция $f(x_1,\ldots,x_n)$ *сохраняет константу* $a \in \{0,1\}$, если $f(a,\ldots,a) = a$.

Функция $f(x_1,\ldots,x_n)$ называется *монотонной*, если для всяких наборов $\mathbf{a} = (a_1,\ldots,a_n)$, $\mathbf{b} = (b_1,\ldots,b_n)$ условие $\mathbf{a} \leqslant \mathbf{b}$ влечет $f(\mathbf{a}) \leqslant f(\mathbf{b})$.

Лемма. Функция монотонна тогда и только тогда, когда ее сокраенная ДНФ не содержит отрицаний..

Следствие. Функция монотонна тогда и только тогда, когда ее минимальная ДНФ не содержит отрицаний.

Пример.

1. $F = \{1, x*y\}$, где $x*y = 0010$.

xy	$x*y$
00	0
01	0
10	1
11	0

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 $(1,0) \leqslant (1,1)$, но $1*0 > 1*1$.

Можно построить сокращенную ДНФ по СКНФ. Именно, $x*y = (x \vee y)(x \vee \bar{y})(\bar{x} \vee \bar{y}) = x(\bar{x} \vee \bar{y}) = x\bar{y}$. Сокращенная ДНФ $x*y = x\bar{y}$ имеет отрицания, и потому функция $x*y$ не монотонна.

5) $x*y$ не линейна, ибо $x*y = \bar{x}y = (x+1)y = xy+y$.

Следовательно, система F по теореме Поста полна. Отрицание есть $1*x$.

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.

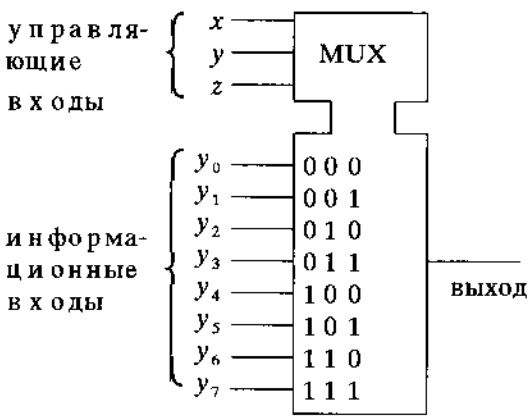
По теореме Поста система F полна.

Задача 12. Заданную систему булевых функций исследовать на полноту с помощью теоремы Поста.

Решение. Аналогично решению задачи 10.

Задача 13. Реализовать функции из задач 4 и 5 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 $(c_1,\ldots,c_n)$ из 0 и 1 схема делает проходимым (отпирает) и пропускает сигнал единственного информационного входа, помеченного набором $(c_1,\ldots,c_n)$; остальные информационные входы заперты и к выходу не проходимы.



Пример. Реализовать функцию трех переменных $f(x,y,z) = 00101101$ с помощью мультиплексора $M(2)$.

В задаче используется разложение функции по переменным x,y. Требуемая реализация приведена на рис.9.1.

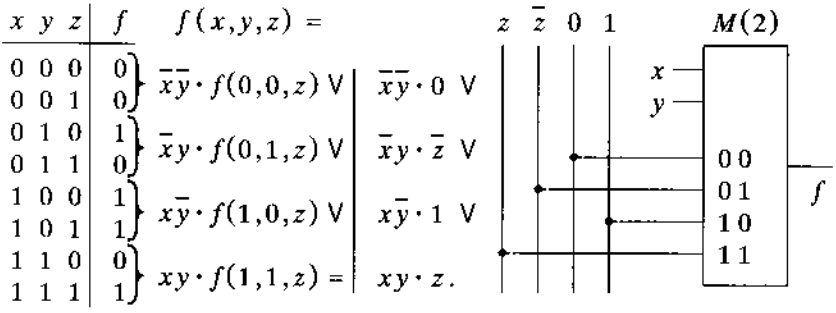


Рис.9.1

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 n переменных $X=\{x_1,\ldots,x_n\}$ на два непересекающихся подмножества $Y=\{y_1,\ldots,y_m\}$, $Z=\{z_{m+1},\ldots,z_n\}$ в сумме (в объединении) дающих все множество X.

Определение. *Простая непересекающаяся декомпозиция* функции $f(x_1,\ldots,x_n)$ есть ее представление в виде $f(X) = \varphi(Y,\psi(Z))$ при некоторых функциях φ и ψ.

Замечание. В случае декомпозиции функция $f(X)$ может быть реализована схемой, построенной из более простых функций φ и ψ (рис.9.2).

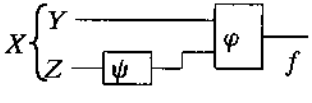


Рис.9.2

В последующем для простоты будем считать, что $Y=\{x_1,\ldots,$

$x_m\}$, $Z=\{x_{m+1},\ldots,x_n\}$.

Определение. Y-компонента функции $f(Y,Z)$ есть совокупность функций $\{f(c_1,\ldots,c_m,x_{m+1},\ldots,x_n)\colon (c_1,\ldots,c_m)\in E_2^m\}$. Z-компонента функции $f(Y,Z)$ есть совокупность функций $\{f(x_1,\ldots,x_m,c_{m+1},\ldots,c_n)\colon (c_{m+1},\ldots,c_n)\in E_2^{n-m}\}$.

Пример. $f(x_1,x_2,x_3,x_4)$, $Y=\{x_1,x_2\}$, $Z=\{x_3,x_4\}$ (рис.9.3).

x_1x_2	x_3x_4 0 0	x_3x_4 0 1	x_3x_4 1 0	x_3x_4 1 1	
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 0	0	1	0	1	$f(1,0,x_3,x_4)$
1 1	1	1	1	1	$f(1,1,x_3,x_4)$

Y-компонента

Рис.9.3

Столбцы таблицы рис.2.14 составляют Z-компоненту $\{f(x_1,x_2,0,0)=1001,\ f(x_1,x_2,0,1)=0111,\ f(x_1,x_2,1,0)=1101,\ f(x_1,x_2,1,1)=1011\}$ функции f.

Теорема 1. Простая непересекающаяся декомпозиция $f(X)=\varphi(Y,\psi(Z))$ для функции $f(X)$ существует $\leftrightarrow$ всякая функция у нее Y-компоненты $f(c_1,\ldots,c_m,Z)\in\{0,1,\psi(Z),\neg\psi(Z)\}$.

Пример. 1. Найти простую непересекающуюся декомпозицию следующей функции $f(x,x_2,x_3,x_4)$, $Y=\{x_1,x_2\}$, $Z=\{x_3,x_4\}$.

x_1x_2	x_3x_4 0 0	x_3x_4 0 1	x_3x_4 1 0	x_3x_4 1 1	Функции Y-компоненты
0 0	0	0	0	0	$f(0,0,x_3,x_4)=0$
0 1	1	0	1	1	$f(0,1,x_3,x_4)=\psi$
1 0	0	1	0	0	$f(1,0,x_3,x_4)=\neg\psi(x_3,x_4)$
1 1	1	0	1	1	$f(1,1,x_3,x_4)=\psi(x_3,x_4)$

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 $f(x_1,x_2,x_3,x_4)=$

$f(0,0,x_3,x_4)\cdot\bar{x}_1\bar{x}_2\ \vee\ f(0,1,x_3,x_4)\cdot\bar{x}_1x_2\ \vee$

$f(1,0,x_3,x_4)\cdot x_1\bar{x}_2 \vee f(1,1,x_3,x_4)\cdot x_1x_2 =$

$\bar{x}_1\bar{x}_2\cdot 0 \vee \bar{x}_1x_2\cdot\psi(x_3,x_4) \vee x_1\bar{x}_2\cdot\overline{\psi(x_3,x_4)} \vee x_1x_2\cdot\psi(x_3,x_4) =$

$(\bar{x}_1x_2\cdot u \vee x_1\bar{x}_2\cdot\bar{u} \vee x_1x_2\cdot u)\big|_{u=\psi(x_3,x_4)} =$

$\varphi(x_1,x_2,\psi(x_3,x_4))$, где $\varphi(x_1,x_2,u) = \bar{x}_1x_2u \vee x_1\bar{x}_2\bar{u} \vee x_1x_2u$,

$\psi(x_3,x_4) = 1011 = \bar{x}_3\bar{x}_4 \vee x_3\bar{x}_4 \vee x_3x_4$.

Реализация функции

$f = \bar{x}_1\bar{x}_2\cdot 0 \vee \bar{x}_1x_2\cdot\psi(x_3,x_4) \vee x_1\bar{x}_2\cdot\overline{\psi(x_3,x_4)} \vee x_1x_2\cdot\psi(x_3,x_4)$ с помощью мультиплексора приведена на рис.9.4.

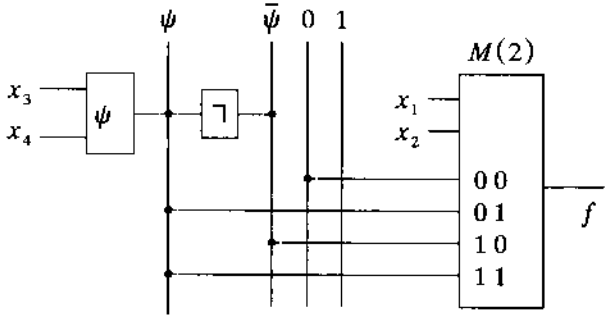


Рис.9.4

Пример 2. Найти простую непересекающуюся декомпозицию следующей функции $f(x_1,x_2,x_3,x_4)$.

	x_3x_4	x_3x_4	x_3x_4	x_3x_4	Функции Y-компоненты
x_1x_2	0 0	0 1	1 0	1 1	
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 0	1	1	1	1	$f(1,0,x_3,x_4)=1$
1 1	0	1	0	1	$f(1,1,x_3,x_4)=\psi_1(x_3,x_4)$

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 $f(Y,Z)=\varphi(X,\psi(Z)) \leftrightarrow$ функция f имеет в Z-компоненте не более двух различных функций.

Пример. 1. Найти простую непересекающуюся декомпозицию следующей функции $f(x,x_2,x_3,x_4)$, $Y=\{x_1,x_2\}$, $Z=\{x_3,x_4\}$.

x_1x_2	x_3x_4 0 0	x_3x_4 0 1	x_3x_4 1 0	x_3x_4 1 1	Функции Z-компоненты (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 0	0	0	0	0	$f(x_1,x_2,1,1)=h_1(x_1,x_2)$
1 1	0	0	0	0	$f(x_1,x_2,1,0)=h_1(x_1,x_2)$

$$f(Y,Z) = f(x_1,x_2,x_3,x_4) =$$

$$f(x_1,x_2,0,0)\cdot\bar{x}_3\bar{x}_4 \vee f(x_1,x_2,0,1)\cdot\bar{x}_3x_4 \vee$$

$$f(x_1,x_2,1,0)\cdot x_3\bar{x}_4 \vee f(x_1,x_2,1,1)\cdot x_3x_4 =$$

$$h_1(x_1,x_2)\bar{x}_3\bar{x}_4 \vee h_2(x_1,x_2)\bar{x}_3x_4 \vee h_1(x_1,x_2)x_3\bar{x}_4 \vee h_1(x_1,x_2)x_3x_4 =$$

$$h_1(x_1,x_2)\cdot(\underbrace{\bar{x}_3\bar{x}_4 \vee x_3\bar{x}_4 \vee x_3x_4}_{g(x_3,x_4)}) \vee h_2(x_1,x_2)\cdot\underbrace{\bar{x}_3x_4}_{\neg g(x_3,x_4)} =$$

$$h_1(x_1,x_2)\cdot g(x_3,x_4) \vee h_2(x_1,x_2)\cdot\overline{g(x_3,x_4)} =$$

$$\underbrace{(h_1(x_1,x_2)\cdot u \vee h_2(x_1,x_2)\cdot\bar{u})}_{\varphi(Y,u)}\Big|_{u=g(x_3,x_4)} = \varphi(Y,\underbrace{g(x_3,x_4)}_{\psi(x_3,x_4}) =$$

$\varphi(Y,\psi(Z))$. Функция f допускает простую непересекающуюся декомпозицию $f(Y,Z) = \varphi(Y,\psi(Z))$. Реализация функции

$$f = h_1(x_1,x_2)\bar{x}_3\bar{x}_4 \vee h_2(x_1,x_2)\bar{x}_3x_4 \vee h_1(x_1,x_2)x_3\bar{x}_4 \vee h_1(x_1,x_2)x_3x_4$$

с помощью мультиплексора приведена на рис.9.5.

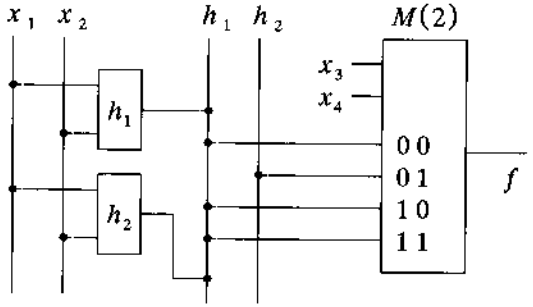


Рис.9.5.

Задача 15. Для булевой функции из задачи 4 построить минимальные проверяющие и полные тесты относительно указанных классов ошибок (s_{ij} – слипание каналов i и j; 0_i – обрыв канала i, 1_i – замыкание канала i).

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 $f_0(x_1,\ldots,x_n)$. В результате брака схема S может реализовать другую функцию из числа функций $f_1,f_2,\ldots,f_r$ 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 $f_1,f_2,\ldots,f_r$ реализует схема в случае неисправности (Табл.9.8).

Таблица 9.8

$x_1,\ldots,x_{n-1},x_n$	f_0	f_1	f_2	$\ldots$	f_r
0 $\ldots$ 0 0	α_0	β_0	γ_0	$\ldots$	δ_0
0 $\ldots$ 0 1	α_1	β_1	γ_1	$\ldots$	δ_1
$\ldots$				$\ldots$	
a_1 $\ldots$ $a_{n-1}a_n$	α_p	β_p	γ_p	$\ldots$	δ_p
$\ldots$				$\ldots$	
1 $\ldots$ 1 1	α_z	β_z	γ_z	$\ldots$	δ_z

$z=2^n-1$.

Определение. *Тест* (тестовый набор) для таблично заданной функции $f_0(x_1,\ldots,x_n)$ есть совокупность наборов длины n из 0 и 1 (совокупность строк в таблице функции f), которая высекает из столбцов значения функций $f_0,f_1,\ldots,f_r$ 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* (*тупиковый*), 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 тупиковых тестов.

Пример построения всех тупиковых и наименьших тестов

Пусть строится схема для функции $f(x_1,\ldots,x_n)$. Примем список следующих неисправностей.

s_{ij} – слипание входов x_i и x_j.

Тогда реализуется функция

$g(\ldots,x_i,\ldots,x_j,\ldots) = f(\ldots,x_i \vee x_j,\ldots,x_i \vee x_j,\ldots)$.

0_i – обрыв входа x_i.

Тогда реализуется функция $g(\ldots,x_i,\ldots) = f(\ldots,0,\ldots)$.

1_i – замыкание входа x_i.

Тогда реализуется функция $g(\ldots,x_i,\ldots) = f(\ldots,1,\ldots)$.

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 $y_0,\ldots,y_7$ есть восемь наборов длины 3 из 0 и 1 (табл.9.9). Каждый тест имеет вид $y_{i_1} \& y_{i_2} \& \ldots \& y_{i_p}$. Построим все тупиковые проверяющие тесты.

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 9.9

	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:

	x_1	x_2	x_3	f_0	f_1	f_2
y_5	1	0	1	1	0	0

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:

	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

Подаем на вход схемы последовательно наборы y_1, y_3, то есть наборы $\begin{matrix}0&0&1\\0&1&1\end{matrix}$. Пара $\begin{matrix}0\\1\end{matrix}$ на выходе укажет, что схема реализу-

ет функцию f_0, пара $\begin{matrix}1\\1\end{matrix}$ – функцию f_1, пара $\begin{matrix}0\\0\end{matrix}$ – функцию f_2.

Задача 16. Для данной схемы из функциональных элементов (СФЭ) найти:

а) минимальный проверяющий тест,

б) минимальный диагностический (полный) тест.

10.8. Алгоритм нахождения проверяющего и диагностического тестов для однократных неисправностей

Минимальный проверяющий тест

1. Построить таблицу значений функции f, реализуемой схемой без неисправностей и функций, реализуемых схемами с каждой однократной неисправностью.

2. Построить таблицу значений суммы по модулю 2 каждой из функций неисправности с функцией f.

3. Минимальное покрытие таблицы из п.2 дает миинимальный проверяющий тест.

Минимальный диагностический (полный) тест для однократных неисправностей

1. Построить таблицу значений функции f, реализуемой схемой без неисправностей и функций, реализуемых схемами с каждой однокатной неисправностью.

2. Построить таблицу значений суммы по модулю 2 каждой из ункций неисправности с функцией f, а также попарных сумм по модулю 2 функций неисправностей.

3. Минимальное покрытие таблицы из п.2 дает минимальный диагностический тест.

Пример. Найти минимальный проверяющий и минимальный диагностический (полный) тесты для однократных неисправностей в следующей схеме из функциональных элементов (СФЭ) (рис.9.6).

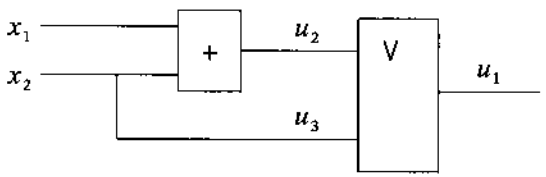


Рис.9.6

Обозначения:

u_1, u_2, u_3 – возможные однократные неисправности:
u_1, u_3 – тождественный 0,
u_2 – отрицание (т.е. вместо 'u_2' реализуется '$\neg u_2$'),
$+$ – сложение по модулю 2,
f – функция, реализуемая схемой без неисправностей,
f/u_1 – функция, реализуемая схемой с неисправностью u_1,
f/u_2 – функция, реализуемая схемой с неисправностью u_2,
f/u_3 – функция, реализуемая схемой с неисправностью u_3.

Построим табл.9.10 для функций f, f/u_1, f/u_2, f/u_3

Таблица 9.10

	x_1x_2	f	f/u_1	f/u_2	f/u_3
0	0 0	0	0	1	0
1	0 1	1	0	1	1
2	1 0	1	0	0	1
3	1 1	1	0	1	0

Построим минимальный проверяющий тест (табл.9.11).

Таблица 9.11

	x_1x_2	$f+f/u_1$	$f+f/u_2$	$f+f/u_3$
0	0 0	0	1	0
1	0 1	1	0	0
2	1 0	1	1	0
3	1 1	1	0	1

Функция $(f + f/u_i)$ равна 1 на тех наборах, на которых f и f/u_i имеют разные значения, т.е. на наборах, на которых проявляется неисправность u_i.

Найдем покрытие столбцов Табл.2 строками.

$(1 \vee 2 \vee 3)(0 \vee 2)3 = (0 \vee 2)3 = 03 \vee 23$.

Получаем два минимальных проверяющих теста: (0,3) и (2,3). Построим табл.9.12 для одного из них, например, для (0,3).

Как видно из табл.9.12 тест (0,3) действительно проверяющий, т.к. при подаче на вход схемы последовательно сначала набора x_1x_2=00, затем x_1x_2=11, на выходе схемы в случае отсутствия неисправности имеем сначала 0, потом 1, а в случае присутствия неисправности – либо 00 (для u_1 и u_3) либо 11

(для u_2).

Таблица 9.12

	x_1x_2	f	f/u_1	f/u_2	f/u_3
0	0 0	0	0	1	0
3	1 1	1	0	1	0

Минимальный диагностический тест (табл.9.13).

Таблица 9.13

	x_1x_2	$f+f/u_1$	$f+f/u_2$	$f+f/u_3$	$f/u_1+f/u_2$	$f/u_1+f/u_3$	$f/u_2+f/u_3$
0	0 0	0	1	0	1	0	1
1	0 1	1	0	0	1	1	0
2	1 0	1	1	0	0	1	1
3	1 1	1	0	1	1	0	1

Функция $(f/u_j + f/u_i)$ равна 1 на тех наборах, на которых неисправности u_i и u_j проявляются по-разному.

Найдем покрытие столбцов Табл.4 строками.

$[(1\vee2\vee3)(0\vee2)3][(0\vee1\vee3)(1\vee2)(0\vee2\vee3)] =$

$(0\vee2)(1\vee2)3 = 012 \vee 23$

Минимальный диагностический тест: (2,3).

Как видно из табл.9.14 тест (2,3) действительно диагностический, т.к. при подаче на вход схемы последовательно сначала набора x_1x_2=10, затем x_1x_2=11, на выходе схемы в случае отсутствия неисправности имеем сначала 0, потом 1, а в случае присутствия неисправности u_1 это 00, неисправности u_2 это 01, неисправности u_3 это 10.

Таблица 9.14

	x_1x_2	f	f/u_1	f/u_2	f/u_3
2	1 0	1	0	0	1
3	1 1	1	0	1	0

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 A к префиксной нормальной форме. Является ли формула A на множе-

стве M: 1) выполнимой; 2) опровержимой; 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

Решение. Интерпретация $I = (M=\{1,2\},P,Q,R)$.

1. Префиксная нормальная форма.

$$A = (\exists y)(P(y) \to (\forall x)(Q(x,y) \vee \neg R(x))) =$$
$$(\exists y)(\neg P(y) \vee (\forall x)(Q(x,y) \vee \neg R(x))) =$$
$$\underbrace{(\exists y)(\forall x)}_{\text{кванторная приставка}} \underbrace{(\neg P(y) \vee Q(x,y) \vee \neg R(x))}_{\text{бескванторная формула}}.$$

2. Элиминация кванторов на конечном множестве $M=\{1,2\}$.

$$A(I) = (\exists y)((\neg P(y) \vee \underset{x}{Q(1,y)} \vee \underset{x}{\neg R(1)}) \,\&\, (\neg P(y) \vee \underset{x}{Q(2,y)} \vee \underset{x}{\neg R(2)}) =$$
$$(\underset{y}{\neg P(1)} \vee \underset{x\,y}{Q(1,1)} \vee \underset{x}{\neg R(1)}) \,\&\, (\underset{y}{\neg P(1)} \vee \underset{x\,y}{Q(2,1)} \vee \underset{x}{\neg R(2)}) \vee$$
$$(\underset{y}{\neg P(2)} \vee \underset{x\,y}{Q(1,2)} \vee \underset{x}{\neg R(1)}) \,\&\, (\underset{y}{\neg P(2)} \vee \underset{x\,y}{Q(2,2)} \vee \underset{x}{\neg R(2)}).$$

3. Вычисление значения формулы A на интерпретации I.

$$A(I) = (\neg 1 \vee 1 \vee 1) \,\&\, (\neg 1 \vee 0 \vee 0) \vee (\neg 0 \vee 0 \vee 1) \,\&\, (\neg 0 \vee 0 \vee 0) =$$
$$(0 \vee 1 \vee 1) \,\&\, (0 \vee 0 \vee 0) \vee (1 \vee 0 \vee 1) \,\&\, (1 \vee 0 \vee 0) =$$
$$1 \,\&\, 0 \vee 1 \,\&\, 1 = 1.$$

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 формулы A:

x	1	2
$P(x)$	0	0
$R(x)$	0	1

$Q(x,y)$	x/y	1	2
	1	1	0
	2	1	0

5. $\bar{A} = (x_1\bar{x}_5x_3 \vee x_1\bar{x}_7x_4)\ \&\ (x_2\bar{x}_6x_3 \vee x_2\bar{x}_8x_4) =$

$x_1x_2x_3\bar{x}_5\bar{x}_6 \vee x_1x_2x_3x_4\bar{x}_5\bar{x}_8 \vee x_1x_2x_3x_4\bar{x}_6\bar{x}_7 \vee x_1x_2x_4\bar{x}_7\bar{x}_8.$

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

$x_1=P(1)=1,\ x_2=P(2)=1,\ x_3=R(1)=1,\ x_4=R(1)=1,$
$x_5=Q(1,1)=1,\ x_6=Q(1,2)=0,\ x_7=Q(2,1)=0,\ x_8=Q(2,2)=1.$

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 18. Проверить правильность или неправильность правила вывода $\dfrac{\neg M \to \neg P,\ S\ \&\ \neg M}{S\ \&\ \neg P}$, установив общезначимость соответствующей формулы.

Решение. Правило $\dfrac{\neg M \to \neg P,\ S\ \&\ \neg M}{S\ \&\ \neg P}$ верно $\leftrightarrow$ формула

$F = (\neg M \to \neg P)\&(S\ \&\ \neg M) \to S\ \&\ \neg P$ тождественно истинна.

Пусть $F_1=\neg M \to \neg P$, $F_2=S\ \&\ \neg M$, $F_3=F_1\&F_2$, $F_4=S\ \&\ \neg P$. Вычисления занесем в табл.9.15.

Ответ. Формула $F\equiv 1$. Следовательно, правило вывода верно.

Задача 19. Проверить правильность или неправильность правила вывода $\dfrac{\neg M \to \neg P,\ \neg S\ \&\ \neg M}{S\ \&\ \neg P}$, установив общезначимость соответствующей формулы.

Решение. Правило $\dfrac{\neg M \to \neg P,\ \neg S\ \&\ \neg M}{S\ \&\ \neg P}$ верно $\leftrightarrow$ формула

$F = (\neg M \to \neg P)\&(\neg S\ \&\ \neg M) \to S\ \&\ \neg P$ тождественно истинна.

Пусть $F_1=\neg M \to \neg P$, $F_2=\neg S\&\neg M$, $F_3=F_1\&F_2$, $F_4=S\&\neg P$. Вычисления занесем в табл.9.16.

Таблица 9.15

	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
7	111	1	0	0	0	1

Таблица 9.16

	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

Формула F тождественно истинной не является. Правило вывода неверно.

Задача 20. Установить правильность или неправильность правило вывода ПВ = $\dfrac{x \to z}{(y \to z) \to (x \vee y \to z)}$, используя естественный вывод Генцена.

Решение. Правило вывода ПВ = $\dfrac{x \to z}{(y \to z) \to (x \vee y \to z)}$ верно $\longleftrightarrow$ формула $F = (x \to z) \to ((y \to z) \to (x \vee y \to z))$ тождественно истинна. Построим для F дерево вывода (рис.9.7).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x \Vdash z;x;y \quad y \Vdash z;x;y}{x \vee y \Vdash z;x;y}(\vee \Vdash)}{z, x \vee y \Vdash z;x \qquad x \vee y \Vdash z;x;y}(\to \Vdash)}{z, y \to z, x \vee y \Vdash z \qquad y \to z, x \vee y \Vdash z;x}(\to \Vdash)}{x \to z, y \to z, x \vee y \Vdash z}(\Vdash \to)}{x \to z, y \to z \Vdash x \vee y \to z}(\Vdash \to)}{x \to z \Vdash (y \to z) \to (x \vee y \to z)}(\Vdash \to)}{\Vdash (x \to z) \to ((y \to z) \to (x \vee y \to z))}(\Vdash \to)$$

Рис.9.7

Все листья – аксиомы. Правило вывода ПВ верно.

Задача 21. Установить правильность или неправильность

правил вывода ПВ = $\frac{x \to y \vee t}{(y \to z) \to (x \vee y \to z)}$, используя естественный вывод Генцена.

Решение. Правило вывода ПВ = $\frac{x \to y \vee t}{(y \to z) \to (x \vee y \to z)}$ верно $\leftrightarrow$ формула $F = (x \to y \vee z) \to ((y \to z) \to (x \vee y \to z))$ тождественно истинна. Построим для F дерево вывода (рис.9.8).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{y, x \Rightarrow z; y \quad t, x \Rightarrow z; y}{y \vee t, x \Rightarrow z; y \quad x \Rightarrow z; y; x}\,(\vee \Rightarrow)}{x \to y \vee t, x \Rightarrow z; y \quad x \to y \vee t, y \Rightarrow z; y}\,(\to \Rightarrow)}{x \to y \vee t, z, x \vee y \Rightarrow z \quad x \to y \vee t, x \vee y \Rightarrow z; y}\,(\vee \Rightarrow)}{x \to y \vee t, y \to z, x \vee y \Rightarrow z}\,(\to \Rightarrow)}{x \to y \vee t, y \to z \Rightarrow x \vee y \to z}\,(\Rightarrow \to)}{x \to y \vee t \Rightarrow (y \to z) \to (x \vee y \to z)}\,(\Rightarrow \to)}{\Rightarrow (x \to y \vee t) \to ((y \to z) \to (x \vee y \to z))}\,(\Rightarrow \to)$$

Рис.9.8

Не все листья являются аксиомами. Правило вывода ПВ не верно.

Задача 24. 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.9.9). 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 $\square$. 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 ∨ q, ПР(1,2);
(4) p ∨ ¬q, из S;
(5) p, ПР(3,4);
(6) ¬p ∨ ¬q, из S;
(7) ¬p ∨ q, из S;
(8) ¬p, ПР(6,7);
(9) □, ПР(5,8).

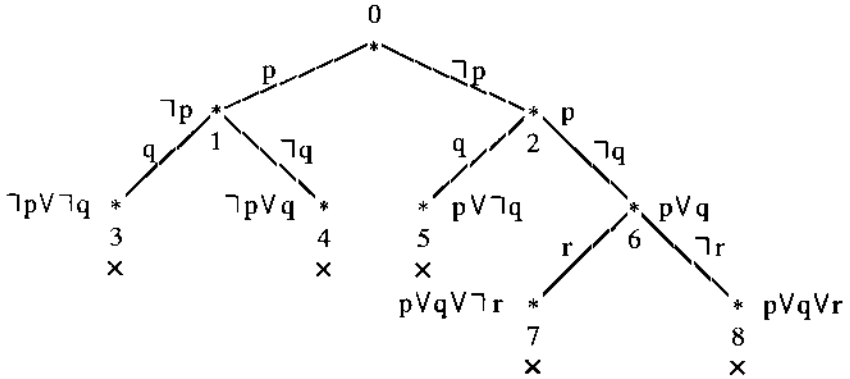


Рис.9.9

Задача 25. 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 ∨ ¬q, ¬p ∨ q ∨ ¬r, p ∨ ¬q}. Строим для S замкнутое семантическое дерево T (рис.9.10). 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.

Задача 26. Доказать правильность правил вывода, установив общезначимость соответствующей формулы.

Решение. **а1.** $\dfrac{\overline{(\forall x)(S(x)\to\overline{P(x)})}}{(\exists x)(S(x)\&P(x))}$. $A = A(P,S) =$

$$\overline{(\forall x)(S(x)\to\overline{P(x)})} \to (\exists x)(S(x)\&P(x)) =$$

$$\overline{\overline{(\forall x)(\overline{S(x)}\vee\overline{P(x)})}} \vee (\exists x)(S(x)\&P(x)) =$$

$$\overline{(\exists x)(\overline{\overline{S(x)}}\vee\overline{P(x)})} \vee (\exists x)(S(x)\&P(x)) =$$

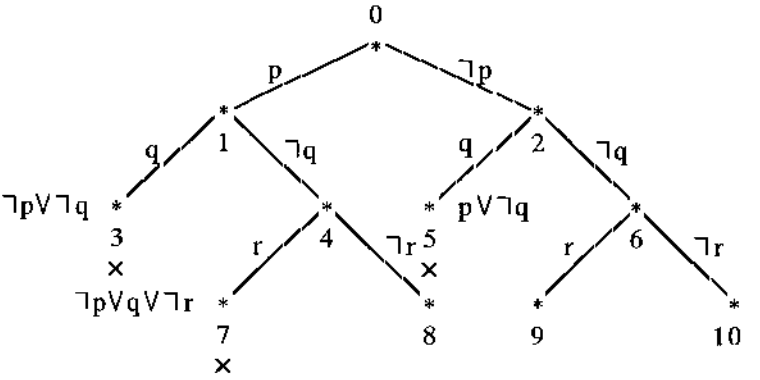


Рис. 9.10

$$\overline{\overline{(\exists x)(\overline{S(x)\&P(x)})} \vee (\exists x)(S(x)\&P(x))} =$$

$$\overline{(\exists x)(S(x)\&\overline{P(x)})} \vee (\exists x)(S(x)\&P(x)) \equiv 1.$$ Правило верно.

а2. $\dfrac{\overline{(\forall x)(S(x)\to P(x))}}{(\exists x)(S(x)\&\overline{P(x)})}$. $A = A(P,S) =$

$$\overline{(\forall x)(S(x)\to P(x))} \to (\exists x)(S(x)\&\overline{P(x)}) =$$

$$\overline{\overline{(\forall x)(\overline{S(x)}\vee P(x))}} \vee (\exists x)(S(x)\&\overline{P(x)}) =$$

$$\overline{(\exists x)(S(x)\&\overline{P(x)})} \vee (\exists x)(S(x)\&\overline{P(x)}) \equiv 1.$$ Правило верно.

а3. $\dfrac{(\forall x)(S(x)\to P(x))}{(\exists x)(S(x)\&\overline{P(x)})}$. $A = A(P,S) =$

$$(\forall x)(S(x)\to P(x)) \to \overline{(\exists x)(S(x)\&\overline{P(x)})} =$$

$$\overline{(\forall x)(S(x)\to P(x))} \vee \overline{(\exists x)(S(x)\&\overline{P(x)})} =$$

$$\overline{(\forall x)(\overline{S(x)}\vee P(x))} \vee \overline{(\exists x)(S(x)\&\overline{P(x)})} =$$

$$(\exists x)(S(x)\&\overline{P(x)}) \vee \overline{(\exists x)(S(x)\&\overline{P(x)})} \equiv 1.$$ Правило верно.

а4. $\dfrac{(\forall x)(S(x)\to\overline{P(x)})}{(\exists x)(S(x)\&P(x))}$. $A = A(P,S) =$

$(\forall x)(S(x)\to\overline{P(x)}) \to \overline{(\exists x)(S(x)\&P(x))} =$

$\overline{(\forall x)(S(x)\to\overline{P(x)})} \vee \overline{(\exists x)(S(x)\&P(x))} =$

$(\exists x)(\overline{S(x)}\vee\overline{P(x)}) \vee \overline{(\exists x)(S(x)\&P(x))} =$

$(\exists x)(\overline{\overline{S(x)}\&\overline{P(x)}}) \vee \overline{(\exists x)(S(x)\&P(x))} =$

$(\exists x)(S(x)\&P(x)) \vee \overline{(\exists x)(S(x)\&P(x))} \equiv 1$. Правило верно.

а5. $\dfrac{(\forall x)(S(x)\to P(x)),\ (\exists x)S(x)}{(\exists x)(S(x)\&P(x))}$. $A = A(P,S) =$

$(\forall x)(S(x)\to P(x)) \ \&\ (\exists x)S(x) \to (\exists x)(S(x)\&P(x)) =$

$\overline{(\forall x)(\overline{S(x)}\vee P(x)) \ \&\ (\exists x)S(x)} \vee (\exists x)(S(x)\&P(x)) =$

$(\exists x)(\overline{S(x)}\vee P(x)) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&P(x)) =$

$(\exists x)(\overline{S(x)}\vee P(x)) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&P(x)) =$

$(\exists x)(S(x)\&\overline{P(x)}) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&P(x)) =$

$(\exists x)(S(x)\&\overline{P(x)}) \vee S(x)\&P(x)) \vee \overline{(\exists x)S(x)} =$

$(\exists x)(S(x)\&(\overline{P(x)} \vee P(x))) \vee \overline{(\exists x)S(x)} =$

$(\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1$. Правило верно.

а6. $\dfrac{(\forall x)(S(x)\to P(x)),\ (\exists x)S(x)}{\overline{(\forall x)(S(x)\to\overline{P(x)})}}$. $A = A(P,S) =$

$(\forall x)(S(x)\to P(x)) \ \&\ (\exists x)S(x) \to \overline{(\forall x)(S(x)\to\overline{P(x)})} =$

$\overline{(\forall x)(\overline{S(x)}\vee P(x)) \ \&\ (\exists x)S(x)} \vee \overline{(\forall x)(S(x)\to\overline{P(x)})} =$

$\overline{(\forall x)(\overline{S(x)}\vee P(x))} \vee \overline{(\exists x)S(x)} \vee (\exists x)\overline{(\overline{S(x)}\vee\overline{P(x)})} =$

$(\exists x)(S(x)\&\overline{P(x)}) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&P(x)) =$

$(\exists x)(S(x)\&\overline{P(x)}\vee S(x)\&P(x)) \vee \overline{(\exists x)S(x)} =$

$(\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1$. Правило верно.

а7. $\dfrac{\overline{(\exists x)(S(x)\&P(x))},\ (\exists x)S(x)}{(\exists x)(S(x)\&\overline{P(x)})}$. $A = A(P,S) =$

$\overline{(\exists x)(S(x)\&P(x))}\&(\exists x)S(x) \to (\exists x)(S(x)\&\overline{P(x)}) =$

$\overline{\overline{(\exists x)(S(x)\&P(x))}\&(\exists x)S(x)} \vee (\exists x)(S(x)\&\overline{P(x)}) =$

$\overline{\overline{(\exists x)(S(x)\&P(x))}\vee\overline{(\exists x)S(x)}} \vee (\exists x)(S(x)\&\overline{P(x)}) =$

$(\exists x)(S(x)\&P(x))\vee\overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&\overline{P(x)}) =$

$(\exists x)(S(x)\&P(x) \vee S(x)\&\overline{P(x)}) \vee \overline{(\exists x)S(x)} =$

$(\exists x)(S(x)\&(P(x)\vee\overline{P(x)})) \vee \overline{(\exists x)S(x)} =$

$(\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1$. Правило верно.

а8. $\dfrac{(\forall x)(S(x)\to\overline{P(x)}) \ \&\ (\exists x)S(x)}{(\exists x)(S(x)\&\overline{P(x)})}$. $A = A(P,S) =$

$(\forall x)(S(x)\to\overline{P(x)}) \ \&\ (\exists x)S(x) \to (\exists x)(S(x)\&\overline{P(x)}) =$

$\overline{(\forall x)(\overline{S(x)}\vee\overline{P(x)}) \ \&\ (\exists x)S(x)} \vee (\exists x)(S(x)\&\overline{P(x)}) =$

$(\exists x)(\overline{\overline{S(x)}\vee\overline{P(x)}}) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&\overline{P(x)}) =$

$(\exists x)(S(x)\&P(x)) \vee \overline{(\exists x)S(x)} \vee (\exists x)(S(x)\&\overline{P(x)}) =$

$(\exists x)(S(x)\&P(x)\vee S(x)\&\overline{P(x)})) \vee \overline{(\exists x)S(x)} =$

$(\exists x)(S(x)\&(P(x)\vee\overline{P(x)})) \vee \overline{(\exists x)S(x)} =$

$(\exists x)S(x) \vee \overline{(\exists x)S(x)} \equiv 1$. Правило верно.

а9. $\dfrac{(\forall x)(M(x)\to\overline{P(x)}),\ (\forall x)(S(x)\to M(x))}{(\forall x)(S(x)\to\overline{P(x)})}$.

$A = A(M,P,S) =$

$\underbrace{(\forall x)(M(x)\to\overline{P(x)})}_{1} \ \&\ \underbrace{(\forall x)(S(x)\to M(x))}_{2} \to \underbrace{(\forall x)(S(x)\to\overline{P(x)})}_{3} =$

$1 \;\&\; 2 \to 3 = \overline{1 \;\&\; 2} \vee 3 = \bar{1} \vee \bar{2} \vee 3 =$

$\overline{(\forall x)(M(x) \to \overline{P(x)}) \;\&\; (\forall x)(S(x) \to M(x))} \vee (\forall x)(\overline{S(x)} \vee \overline{P(x)}) =$

$\overline{(\forall x)(\overline{M(x)} \vee \overline{P(x)})} \vee \overline{(\forall x)(\overline{S(x)} \vee M(x))} \vee \underbrace{(\exists x)(S(x) \& P(x))}_{4} =$

$(\exists x)(\overline{\overline{M(x)} \& \overline{P(x)}}) \vee (\exists x)(\overline{\overline{S(x)} \vee M(x)}) \vee 4 =$

$(\exists x)(M(x) \& P(x)) \vee (\exists x)(S(x) \& \overline{M(x)}) \vee 4 =$

$(\exists x)(M(x) \& P(x) \vee S(x) \& \overline{M(x)}) \vee 4 =$

$(\exists x)((M(x) \& P(x) \vee S(x)) \& (M(x) \& P(x) \vee \overline{M(x)})) \vee 4 =$

$(\exists x)((M(x) \vee S(x)) \& (P(x) \vee S(x)) \& (M(x) \vee \overline{M(x)}) \& (P(x) \vee \overline{M(x)})) \vee 4 =$

$(\exists x)((M(x) \vee S(x)) \& (P(x) \vee S(x)) \& (P(x) \vee \overline{M(x)})) \vee 4 =$

$(\exists x)((M(x)P(x) \vee M(x)S(x) \vee S(x)P(x) \vee S(x)) \& (P(x) \vee \overline{M(x)})) \vee 4 =$

$(\exists x)((M(x)P(x) \vee S(x)) \& (P(x) \vee \overline{M(x)})) \vee 4 =$

$(\exists x)((M(x)P(x) \vee S(x)P(x) \vee S(x)\overline{M(x)})) \vee 4 =$

$(\exists x)(M(x)P(x)) \vee (\exists x)(S(x)P(x)) \vee$

$(\exists x)(S(x)\overline{M(x)}) \vee \overline{(\exists x)(S(x) \& P(x))} \equiv 1$. Правило верно.

a10. $\dfrac{(\forall x)(M(x) \to \overline{P(x)}),\ (\exists x)(S(x) \& M(x))}{(\exists x)(S(x) \& \overline{P(x)})}$.

$A = A = A(M,P,S) =$

$\underbrace{(\forall x)(M(x) \to \overline{P(x)})}_{1} \;\&\; \underbrace{(\exists x)(S(x) \& M(x))}_{2} \to \underbrace{(\exists x)(S(x) \& \overline{P(x)})}_{3} =$

$1 \;\&\; 2 \to 3 = \overline{1 \;\&\; 2} \vee 3 = \bar{1} \vee \bar{2} \vee 3 =$

$\overline{(\forall x)(M(x) \to \overline{P(x)})} \vee \overline{\underbrace{(\exists x)(S(x) \& M(x))}_{4}} \vee (\exists x)(S(x) \& \overline{P(x)}) =$

$\overline{(\forall x)(M(x) \to \overline{P(x)})} \vee (\exists x)(S(x) \& \overline{P(x)}) \vee 4 =$

$(\exists x)(M(x) \& P(x)) \vee (\exists x)(S(x) \& \overline{P(x)}) \vee 4 =$

$(\exists x)(M(x) \& P(x) \vee S(x) \& \overline{P(x)}) \vee 4 =$

$(\exists x)((M(x)\&P(x)\vee S(x))\&(M(x)\&P(x)\vee\overline{P(x)}))\ \vee\ 4\ =$

$(\exists x)((M(x)\vee S(x))\&(P(x)\vee S(x))\&(M(x)\vee\overline{P(x)})\&(P(x)\vee\overline{P(x)}))\ \vee\ 4\ =$

$(\exists x)((M(x)\vee S(x))\&(P(x)\vee S(x))\&(M(x)\vee\overline{P(x)}))\ \vee\ 4\ =$

$(\exists x)((M(x)P(x)\vee M(x)S(x)\vee S(x)P(x)\vee S(x))\&(M(x)\vee\overline{P(x)}))\ \vee\ 4\ =$

$(\exists x)((M(x)P(x)\vee S(x))\&(M(x)\vee\overline{P(x)}))\ \vee\ 4\ =$

$(\exists x)((M(x)P(x)\vee S(x)M(x)\vee S(x)\overline{P(x)}))\ \vee\ 4\ =$
$(\exists x)(M(x)P(x))\vee(\exists x)(S(x)M(x))\vee$

$(\exists x)(S(x)\overline{P(x)})\vee\overline{(\exists x)(S(x)\&M(x))}\ \equiv\ 1$. Правило верно.

a11. $\dfrac{(\forall x)(M(x)\to\overline{P(x)}),\ (\forall x)(M(x)\to S(x)),(\exists x)M(x)}{(\exists x)(S(x)\&\overline{P(x)})}$.

$A\ =\ A(M,P,S)\ =$

$\underbrace{(\forall x)(M(x)\to\overline{P(x)})}_{1}\&\underbrace{(\forall x)(M(x)\to S(x))}_{2}\&\underbrace{(\exists x)M(x)}_{3}\to\underbrace{(\exists x)(S(x)\&\overline{P(x)})}_{4}\ =$

$1\&2\&3\to 4\ =\ \overline{1\&2\&3}\ \vee\ 4\ =\ \overline{1}\ \vee\ \overline{2}\ \vee\ \overline{3}\ \vee\ 4\ =$

$\overline{(\forall x)(M(x)\to\overline{P(x)})}\ \vee\ \overline{(\forall x)(M(x)\to S(x))}\ \vee\ (\exists x)(S(x)\&\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(\overline{M(x)\vee\overline{P(x)}})\ \vee\ (\exists x)(\overline{M(x)\vee S(x)})\ \vee\ (\exists x)(S(x)\&\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(\overline{M(x)}\&\overline{\overline{P(x)}})\ \vee\ (\exists x)(\overline{M(x)}\&\overline{S(x)})\ \vee\ (\exists x)(S(x)\&\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)\&P(x))\ \vee\ (\exists x)(M(x)\&\overline{S(x)})\ \vee\ (\exists x)(S(x)\&\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)\&P(x)\ \vee\ M(x)\&\overline{S(x)}\ \vee\ S(x)\&\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)P(x)\ \vee\ (M(x)\vee S(x))\&(M(x)\vee\overline{P(x)})\&(\overline{S(x)}\vee\overline{P(x)}))\ \vee\ \overline{3}\ =$
$(\exists x)(M(x)P(x)\ \vee$

$(M(x)\vee S(x))(M(x)\overline{S(x)}\vee\overline{P(x)}\overline{S(x)}\vee\overline{P(x)}\ \vee\ M(x)\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)P(x)\ \vee\ (M(x)\vee S(x))(M(x)\overline{S(x)}\vee\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)P(x)\vee M(x)\overline{P(x)}\ \vee\ M(x)\overline{S(x)}\vee S(x)\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)\ \vee\ M(x)\overline{S(x)}\ \vee\ S(x)\overline{P(x)})\ \vee\ \overline{3}\ =$

$(\exists x)(M(x)\ \vee\ S(x)\overline{P(x)}\ \vee\ \overline{3}\ =$

$(\exists x)M(x)\ \vee\ (\exists x)(S(x)\overline{P(x)})\ \vee\ \overline{(\exists x)M(x)}\ \equiv\ 1$. Правило верно.

Задача 27. Доказать справедливость правила вывода ПВ = $\frac{(\exists x)(P(a)\to Q(x))}{P(a)\to(\exists x)Q(x)}$, используя естественный вывод Генцена.

Решение. Правило вывода ПВ верно $\longleftrightarrow$ формула F = $(\exists x)(P(a) \to Q(x)) \to (P(a)\to(\exists x)Q(x))$ общезначима. Докажем F в СИП. Доказательство формулы F оформим в виде дерева, рассуждая при этом так же, как это делали в случае вывода формул в СИВ (рис.9.11).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{Q(b),P(a) \Vdash Q(b);(\exists x)Q(x)}{Q(b),P(a) \Vdash (\exists x)Q(x)} \quad P(a) \Vdash (\exists x)Q(x);P(a)}{P(a)\to Q(b),P(a) \Vdash (\exists x)Q(x)}}{(\exists x)(P(a)\to Q(x)),P(a) \Vdash (\exists x)Q(x)}}{(\exists x)(P(a)\to Q(x)) \Vdash P(a)\to(\exists x)Q(x)}}{\Vdash (\exists x)(P(a)\to Q(x)) \to (P(a)\to(\exists x)Q(x))}$$

(⊩ ∃) (→ ⊩) (∃ ⊩) (⊩ →) (⊩ →)

Рис.9.11

Прокомментируем этот вывод для правил, связанных с кванторами. В секвенции $(\exists x)(P(a)\to Q(x)),P(a)\Vdash(\exists x)Q(x)$ формула $(\exists x)(P(a)\to Q(x))$ истинна, если существует x, например, равный предмету b, отличному от всех ранее встречавшихся предметов, для которого формула $P(a)\to Q(b)$ истинна. Переходим к секвенции $P(a)\to Q(b),P(a)\Vdash(\exists x)Q(x)$. В секвенции $Q(b),P(a)\Vdash(\exists x)Q(x)$ 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 $P(a) \to Q(b)$, $P(a) \Vdash (\exists x)Q(x)$ переходим к секвенции $Q(b)$, $P(a) \Vdash Q(b)$; $(\exists x)Q(x)$, которая является аксиомой. В построенном дереве все листья – аксиомы, потому формула F доказуема в СИП, откуда следует ее общезначимость и верность правила вывода ПВ.

Задача 30. Задание взять из задачи 26. Доказать справедливость правил вывода методом резолюций, для чего выполнить следующее.

а. Построить формулу A, для которой правило вывода верно $\longleftrightarrow$ формула A общезначима $\longleftrightarrow$ формула $\neg A$ невыполнима.

б. Найти префиксную нормальную форму для формулы A.

в. Найти префиксную нормальную форму для формулы $\neg A$.

г. Найти стандартную форму Скулема для формулы $\neg A$.

д. Указать множество дизъюнктов S для формулы $\neg A$.

е. Написать эрбрановский универсум H для S.

ж. Написать эрбрановский базис B для S.

з. Указать множество основных примеров дизъюнктов из S.

и. 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.

$$\frac{\begin{array}{l}(\forall x)(\neg P(x) \to \neg M(x))\\ (\forall x)(\neg M(x) \to \neg S(x))\\ (\exists x)S(x)\end{array}}{(\exists x)(S(x)\ \&\ P(x))}$$

Решение.

а. Правило вывода $\dfrac{\begin{array}{l}(\forall x)(\neg P(x) \to \neg M(x))\\ (\forall x)(\neg M(x) \to \neg S(x))\\ (\exists x)S(x)\end{array}}{(\exists x)(S(x)\ \&\ P(x))}$ верно $\leftrightarrow$

формула $A = A(M,P,S) =$

$$(\forall x)(\overline{P(x)}\to\overline{M(x)})\&(\forall x)(\overline{M(x)}\to\overline{S(x)})\&(\exists x)S(x)\to(\exists x)(S(x)\&P(x))$$

общезначима $\leftrightarrow$ формула $\neg A = \neg A(M,P,S)$ невыполнима.

$A = A(M,P,S) =$

$$(\forall x)(\overline{P(x)}\to\overline{M(x)})\&(\forall x)(\overline{M(x)}\to\overline{S(x)})\&(\exists x)S(x)\to(\exists x)(S(x)\&P(x))\equiv 1.$$

б. Приведем формулу A к префиксной нормальной форме. $A =$

$$(\forall x)(P(x)\vee\overline{M(x)})\&(\forall x)(M(x)\vee\overline{S(x)})\&(\exists x)S(x)\vee(\exists x)(S(x)\&P(x)) =$$

$$(\exists x)(\overline{P(x)}\&M(x))\vee(\exists x)(\overline{M(x)}\&S(x))\vee(\forall x)\overline{S(x)}\vee(\exists x)(S(x)\&P(x)) =$$

$$(\exists x)(\overline{P(x)}\&M(x)\vee\overline{M(x)}\&S(x)\vee(\forall x)\overline{S(x)}\vee S(x)\&P(x)) =$$

$$(\exists x)(\overline{P(x)}\&M(x)\vee\overline{M(x)}\&S(x)\vee(\forall y)\overline{S(y)}\vee S(x)\&P(x)) =$$

$$(\exists x)(\forall y)(\overline{P(x)}\&M(x)\vee\overline{M(x)}\&S(x)\vee\overline{S(y)}\vee S(x)\&P(x)).$$

в. Префиксная нормальная форма формулы $\neg A$ =

$$(\forall x)(\exists y)(P(x)\&M(x) \vee \overline{M(x)}\&S(x) \vee \overline{S(y)} \vee S(x)\&P(x)) =$$

$$(\forall x)(\exists y)((P(x)\vee\overline{M(x)}) \ \&\ (M(x)\vee\overline{S(x)}) \ \&\ \overline{\overline{S(y)}} \ \&\ (\overline{S(x)}\vee\overline{P(x)})) =$$

$$(\forall x)(\exists y)((P(x)\vee\overline{M(x)}) \ \&\ (M(x)\vee\overline{S(x)}) \ \&\ S(y) \ \&\ (\overline{S(x)}\vee\overline{P(x)}))$$

г. Стандартная форма Скулема 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 эрбрановского универсума. Эрбрановский универсум множества дизъюнктов D есть множество

$H = \{a, fa=f(a), ffa=f(f(a)), fffa=f(f(f(a))),,,\}$.

ж. Множество $\{a,f,M,P,S\}$ составит материал (множество символов) для построения эрбрановского базиса. Эрбрановский базис множества дизъюнктов S есть множество $B=\{M(t), P(t), S(t) : t$ пробегает элементы эрбранова универсума $H\}$ = $\{A_1=S(fa), A_2=M(a), A_3=P(a), A_4=S(a), A_5=S(ffa), A_6=M(fa), A_7=P(fa), A_8=M(ffa), A_9=P(ffa), \ldots\}$.

з. Множество основных примеров дизъюнктов из D состоит из следующих множеств.

$\{S(f(t)) : t$ пробегает элементы эрбранова универсума $H\}$.

$\{\overline{M(t)}\vee P(t) : t$ пробегает элементы эрбранова универсума $H\}$.

$\{M(t)\vee\overline{S(t)} : t$ пробегает элементы эрбранова универсума $H\}$.

$\{\overline{P(t)}\vee\overline{S(t)} : t$ пробегает элементы эрбранова универсума $H\}$.

и. Строим замкнутое семантическое дерево для S (рис.9.12, 9.13).

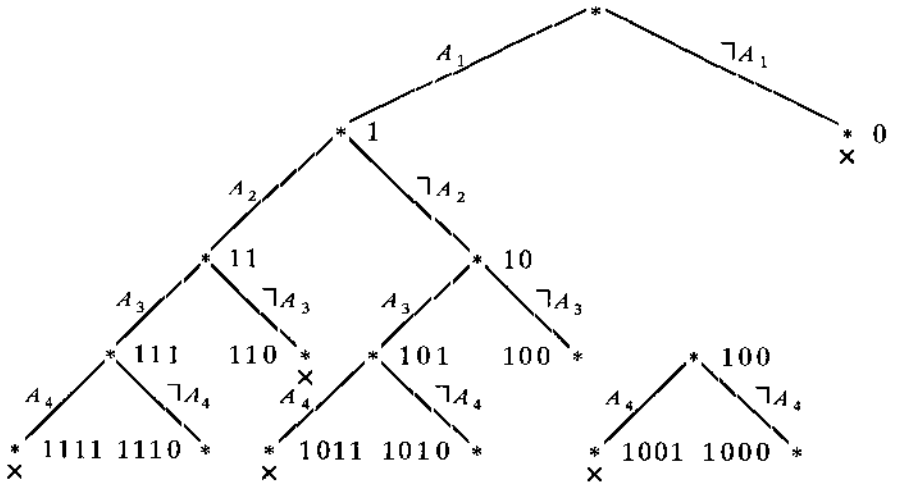
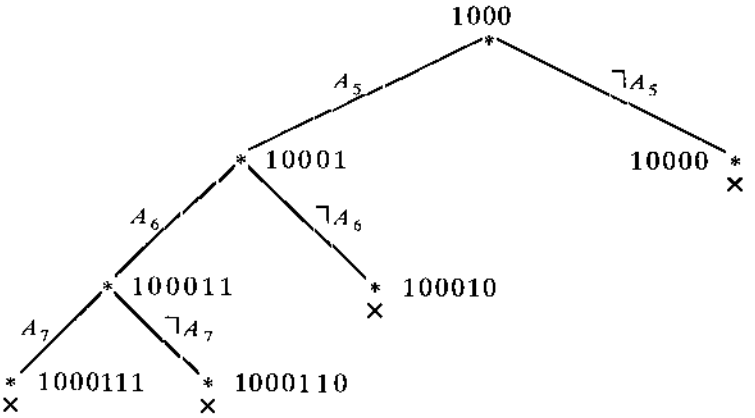

A_1
$\neg A_1$
1
0
A_2
$\neg A_2$
11
10
A_3
$\neg A_3$
A_3
$\neg A_3$
111
110
101
100
100
A_4
$\neg A_4$
A_4
$\neg A_4$
A_4
$\neg A_4$
1111
1110
1011
1010
1001
1000

Рис.9.12


1000
A_5
$\neg A_5$
10001
10000
A_6
$\neg A_6$
100011
100010
A_7
$\neg A_7$
1000111
1000110

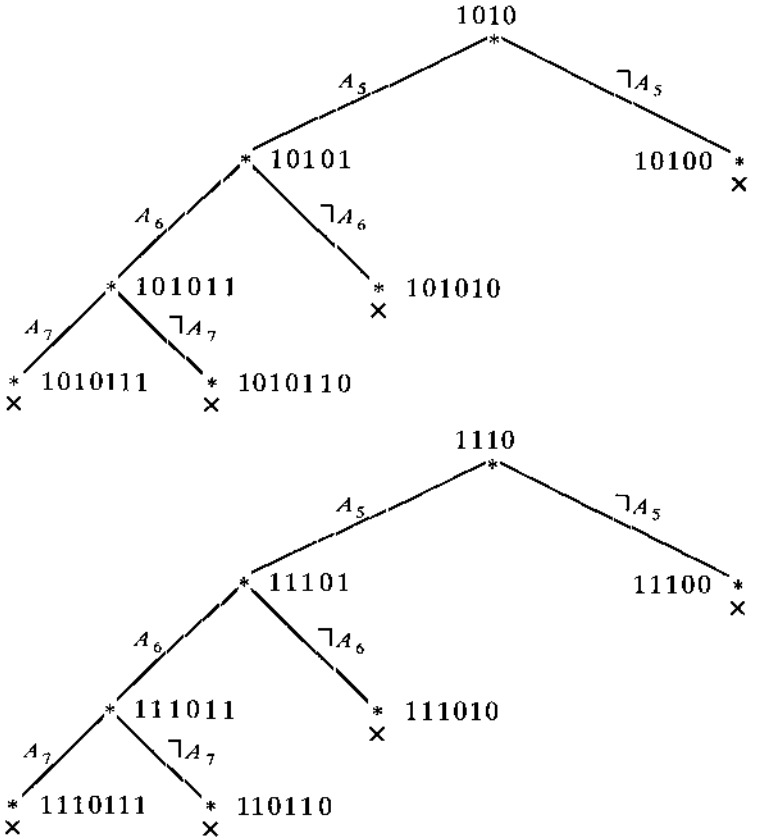


Рис.9.13

Множество дизъюнктов формулы $\neg A$ есть множество

$D = S(f(x))\&(\overline{M(x)}\vee P(x))\&(M(x)\vee\overline{S(x)})\&(\overline{P(x)}\vee\overline{S(x)})$.

Эрбрановский базис множества дизъюнктов S есть множество $B=\{M(t),P(t),S(t):t$ пробегает элементы эрбранова базиса $H\}$ $=\{A_1=S(fa),A_2=M(a),A_3=P(a),A_4=S(a),A_5=S(ffa),A_6=M(fa),$ $A_7=P(fa),A_8=M(ffa),A_9=P(ffa),\ldots\}$.

Узел 0. $A_1=S(fa)=0$. Остальные A_i не определены (прочерки). Эрбрановская интерпретация $I=(0,-,-,\ldots)$.

$D(a)=S(f(a))\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $0\&(-\vee-)\&(-\vee-)\&-\&(-\vee-)=0\&-\&-\&-=0$. 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. Эрбрановская интерпретация $I=(1,-,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $1\&(-\vee-)\&(-\vee-)\&(-\vee-)$ = $1\&-\&-\&-$ = $-$. Узел 1 опровергающим не является.

Узел 10. $A_1=S(fa)=1, A_2=M(a)=0$. H–интерпретация $I=(1,0,-,-,\ldots)$.

$D(a)=S(f(a))\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $1\&(1\vee-)\&(0\vee-)\&(-\vee-)=1\&1\&-\&-$ = $-$. Узел 10 опровергающим не является.

Узел 11. $A_1=S(fa)=1, A_2=M(a)=1$. H–интерпретация $I=(1,1,-,-,\ldots)$.

$D(a)=S(f(a))\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $1\&(0\vee-)\&(1\vee-)\&(-\vee-)$ = $1\&-\&1\&-$ = $-$. Узел 11 опровергающим не является.

Узел 100. $A_1=S(f(a)=1, A_2=M(a)=0, A_3=P(a)=0$. H–интерпретация $I=(1,0,0,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $1\&(1\vee0)\&(0\vee-)\&(1\vee-)$ = $1\&1\&-\&1$ = $-$. Узел 100 опровергающим не является.

Узел 101. $A_1=S(f(a)=1, A_2=M(a)=0, A_3=P(a)=1$. H–интерпретация $I=(1,0,1,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(x)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $1\&(1\vee1)\&(0\vee-)\&(0\vee-)$ = $1\&1\&-\&-$ = $-$. Узел 101 опровергающим не является.

Узел 110. $A_1=S(f(a)=1, A_2=M(a)=1, A_3=P(a)=0$. H–интерпретация $I=(1,1,0,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)})$ = $1\&(0\vee0)\&(1\vee-)\&(1\vee-)$ = $1\&0\&1\&1$ = 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 $I=(1,1,1,-,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(x)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(0\vee 1)\&(1\vee -)\&(0\vee -) = 1\&1\&1\&- = -$. 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 $I=(1,0,0,0,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(1\vee 0)\&(0\vee 1)\&(1\vee 1) = 1\&1\&1\&1 = 1$. 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 $I=(1,0,0,1,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(1\vee 0)\&(0\vee 0)\&(1\vee 0) = 1\&1\&0\&1 = 0$. 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 $I=(1,0,1,0,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(1\vee 1)\&(0\vee 1)\&(0\vee 1) = 1\&1\&1\&1 = 1$. 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 $I=(1,0,1,1,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(1\vee 1)\&(0\vee 0)\&(0\vee 0) = 1\&1\&0\&0 = 0$. 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 $I=(1,1,1,0,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(0\vee 1)\&(1\vee 1)\&(0\vee 1) = 1\&1\&1\&1 = 1$. 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 $I=(1,1,1,1,-,\ldots)$.

$D(a)=S(fa)\&(\overline{M(a)}\vee P(a))\&(M(a)\vee\overline{S(a)})\&(\overline{P(a)}\vee\overline{S(a)}) = 1\&(0\vee 1)\&(1\vee 0)\&(0\vee 0) = 1\&1\&1\&0 = 0$. Узел 1111 является опровергающим. В узле 1111 опровергается дизъюнкт $\overline{C_4}=\overline{P(x)}\vee\overline{S(x)}$, ибо его основной пример $C'_4=\overline{P(a)}\vee\overline{S(a)}=0$.

Узел 10000. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=0, A_4=S(a)=0, A_5=S(ffa)=0$. H–интерпретация $I=(1,0,0,0,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 0\&(-\vee -)\&(-\vee 0)\&(-\vee 0) = 0\&-\&-\&- = 0$. Узел 10000 является опровергающим. В узле 10000 опровергается дизъюнкт $C_1=S(f(x))$, ибо его основной пример $C'_1=A_5=S(ffa)=0$.

Узел 10001. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=0, A_4=S(a)=0, A_5=S(ffa)=1$. H–интерпретация $I=(1,0,0,0,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(-\vee -)\&(-\vee 0)\&(-\vee 0) = 1\&-\&-\&- = -$. Узел 10001 опровергающим не является.

Узел 10100. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=1, A_4=S(a)=0, A_5=S(ffa)=0$. H–интерпретация $I=(1,0,1,0,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 0\&(-\vee -)\&(-\vee 0)\&(-\vee 0) = 0\&-\&-\&- = 0$. Узел 10100 является опровергающим. В узле 10100 опровергается дизъюнкт $C_1=S(f(x))$, ибо его основной пример $C'_1=A_5=S(ffa)=0$.

Узел 10101. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=1, A_4=S(a)=0, A_5=S(ffa)=1$. H–интерпретация $I=(1,0,1,0,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(-\vee -)\&(-\vee 0)\&(-\vee 0) = 1\&-\&-\&- = -$. Узел 10101 опровергающим

не является.

Узел 11100. $A_1=S(fa)=1, A_2=M(a)=1, A_3=P(a)=1, A_4=S(a)=0$, $A_5=S(ffa)=0$. H–интерпретация $I=(1,1,1,0,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 0\&(-\vee-)\&(-\vee0)\&(-\vee0) = 0\&-\&-\&- = 0$. Узел 11100 является опровергающим. В узле 11100 опровергается дизъюнкт $C_1=S(f(x))$, ибо его основной пример $C_1'=A_5=S(ffa)=0$.

Узел 11101. $A_1=S(fa)=1, A_2=M(a)=1, A_3=P(a)=1, A_4=S(a)=0$, $A_5=S(ffa)=1$. H–интерпретация $I=(1,1,1,0,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(-\vee-)\&(-\vee0)\&(-\vee0) = 1\&-\&-\&- = -$. Узел 11101 опровергающим не является.

Узел 100010. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=0, A_4=S(a)=0$, $A_5=S(ffa)=1, A_6=M(fa)=0$. H–интерпретация $I=(1,0,0,0,1,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(1\vee-)\&(0\vee0)\&(-\vee0) = 1\&1\&0\&- = 0$. Узел 100010 является опровергающим. В узле 100010 опровергается дизъюнкт $C_3 = \overline{M(x)\vee S(x)}$, ибо его основной пример $C_3'=\overline{M(fa)\vee S(fa)}=0$.

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 $I=(1,0,0,0,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee-)\&(1\vee0)\&(-\vee0) = 1\&-\&1\&- = -$. 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 $I=(1,0,1,0,1,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(1\vee-)\&(0\vee0)\&(-\vee0) = 1\&1\&0\&- = 0$. Узел 101010 является опровергающим. В узле 101010 опровергается дизъюнкт $C_3 = M(x)\vee\overline{S(x)}$, ибо его основной пример $C_3'=\overline{M(fa)\vee S(fa)}=0$.

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 $I=(1,0,1,0,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee-)\&(1\vee0)\&(-\vee0) = 1\&-\&1\&- = -$. 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 $I=(1,1,1,0,1,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(1\vee-)\&(0\vee0)\&(-\vee0) = 1\&1\&0\&- = 0$. 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 $I=(1,1,1,0,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee-)\&(1\vee0)\&(-\vee0) = 1\&-\&1\&- = -$. 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 $I=(1,0,0,0,1,1,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee0)\&(1\vee0)\&(1\vee0) = 1\&0\&1\&1 = 0$. 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 $I=(1,0,0,0,1,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee1)\&(1\vee0)\&(0\vee0) = 1\&1\&1\&0 = 0$. В узле 1000111 опроверга-

ется 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. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=1, A_4=S(a)=0, A_5=S(ffa)=1, A_6=M(fa)=1, A_7=P(fa)=0$. H–интерпретация $I=(1,0,1,0,1,1,0,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee 0)\&(1\vee 0)\&(1\vee 0) = 1\&0\&1\&1 = 0$. 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. $A_1=S(fa)=1, A_2=M(a)=0, A_3=P(a)=1, A_4=S(a)=0, A_5=S(ffa)=1, A_6=M(fa)=1, A_7=P(fa)=1$. H–интерпретация $I=(1,0,1,0,1,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee 1)\&(1\vee 0)\&(0\vee 0) = 1\&1\&1\&0 = 0$. 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. $A_1=S(fa)=1, A_2=M(a)=1, A_3=P(a)=1, A_4=S(a)=0, A_5=S(ffa)=1, A_6=M(fa)=1, A_7=P(fa)=0$. H–интерпретация $I=(1,1,1,0,1,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee 0)\&(1\vee 0)\&(1\vee 0) = 1\&0\&1\&1 = 0$. 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. $A_1=S(fa)=1, A_2=M(a)=1, A_3=P(a)=1, A_4=S(a)=0, A_5=S(ffa)=1, A_6=M(fa)=1, A_7=P(fa)=1$. H–интерпретация $I=(1,1,1,0,1,1,1,-,\ldots)$.

$D(fa)=S(ffa)\&(\overline{M(fa)}\vee P(fa))\&(M(fa)\vee\overline{S(fa)})\&(\overline{P(fa)}\vee\overline{S(fa)}) = 1\&(0\vee 1)\&(1\vee 1)\&(0\vee 0) = 1\&1\&1\&0 = 0$. В узле 1010111 опроверга-

ется 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 опровержимо 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 10000 опровергается дизъюнкт $C_1=S(f(x))$, ибо его основной пример $C_1'=A_5=S(ffa)=0$.

В узле 10100 опровергается дизъюнкт $C_1=S(f(x))$, ибо его основной пример $C_1'=A_5=S(ffa)=0$.

В узле 11100 опровергается дизъюнкт $C_1=S(f(x))$, ибо его основной пример $C_1'=A_5=S(ffa)=0$.

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 $C_3=M(x)\vee\overline{S(x)}$, ибо его основной пример $C_3'=M(fa)\vee\overline{S(fa)}=0$.

В узле 1000110 опровергается дизъюнкт $C_2=M(x)\vee\overline{S(x)}$, 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 $C_2'=\overline{\overline{M(fa)}}\vee P(fa)=0$.

В узле 1010111 опровергается дизъюнкт $C_4=\overline{P(x)}\vee\overline{\overline{S(x)}}$, ибо его основной пример $C_4'=\overline{P(fa)}\vee\overline{\overline{S(fa)}}=0$.

Опровергающее множество основных примеров BE =

$\{S(fa),\ \overline{\overline{M(a)}}\vee P(a),\ M(a)\vee\overline{S(a)},\ \overline{\overline{P(a)}}\vee\overline{S(a)},\ S(ffa),$

$M(fa)\vee\overline{S(fa)},\ \overline{\overline{M(fa)}}\vee P(fa),\ \overline{P(fa)}\vee\overline{\overline{S(fa)}}\}$.

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 последует верность правила вывода.

к. Покажем, что $D\vdash\square$.

(1) $S(f(x))$, условие,

(2) $\overline{\overline{M(x)}}\vee P(x)$, условие,

(3) $M(x)\vee\overline{\overline{S(x)}}$, условие,

(4) $\overline{P(x)}\vee\overline{\overline{S(x)}}$, условие,

(5) $P(x)\vee\overline{S(x)}$, ПР(2,3),

(6) $\overline{\overline{S(f(x))}}$, ПР(4,5), подстановка $\theta=\{f(x)\,|\,x\}$,

(7) $\square$, ПР(1,6).

Так как $D\vdash\square$, то $D\equiv 0$ и потому исходное правило вывода верно.

11. ГРАФЫ (Примеры решений)

Задача 1. Для данного графа найти степени вершин, написать матрицу смежностей (соседста 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 есть:

$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array}, \qquad B = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array} \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array}$$

Задача 2. 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).

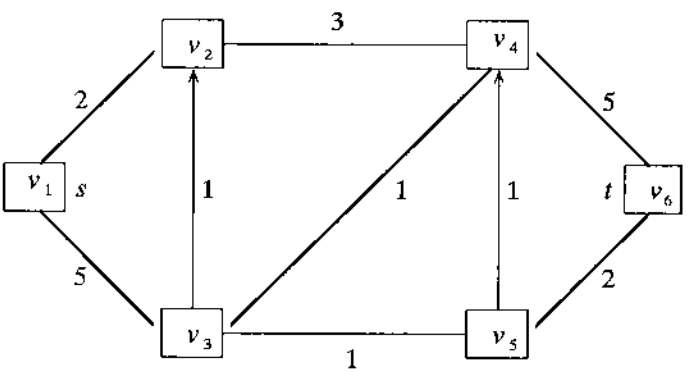


Рис.11.1

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 $\underline{0}$. Вершину s объявляем активной и помечаем знаком плюс. Всем остальным вершинам присвоим временные (неподчеркнутые) пометки ∞. 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 к 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. Присваиваем вершине $s=v_1$ постоянную пометку $\underline{0}$. Остальные вершины получают временные пометки ∞. Вершину $s=v_1$ объявляем активной и помечаем знаком плюс (рис.11.2). Переход к шагу 2.

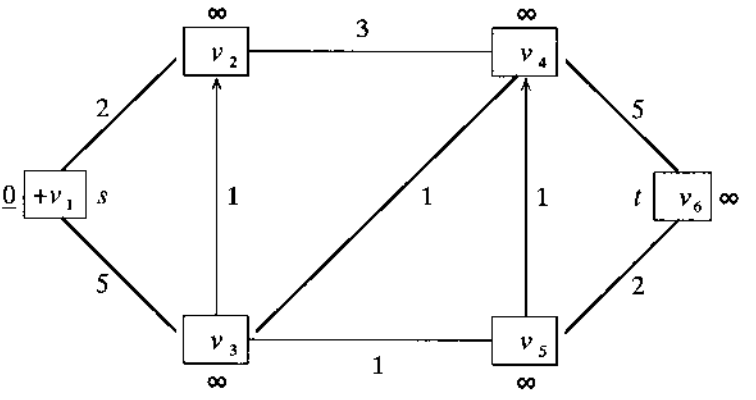


Рис.11.2

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 ∞. 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.

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.

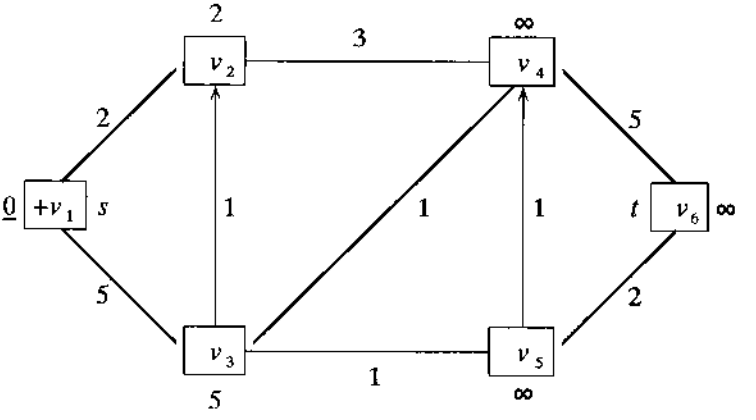


Рис.11.3

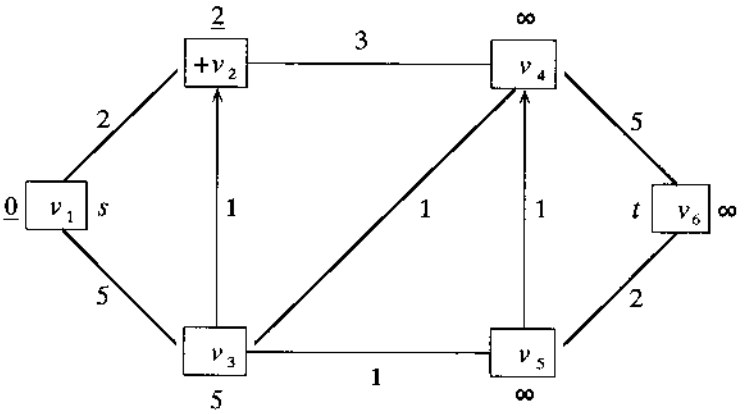


Рис.11.4

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 ∞. Для v_4: $2+3=5<\infty$. Присваиваем для v_4 новую временную пометку 5 (рис.11.5). Переход к шагу 4.

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.

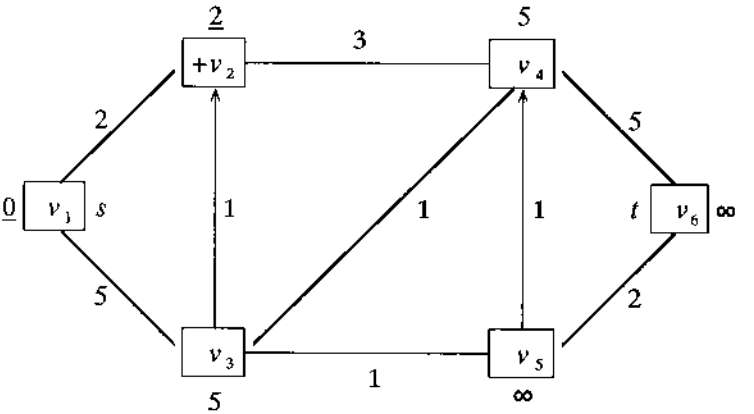


Рис.11.5

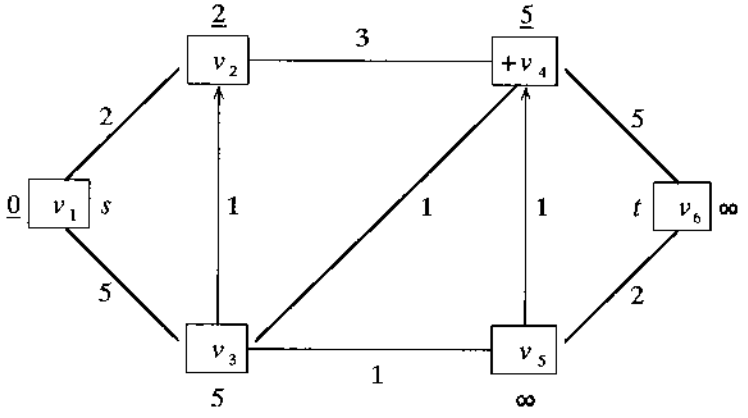


Рис.11.6

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 ∞ соответственно. Для v_3: $5+1=6 \geqslant 5$. 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.

Шаг 4. Из всех временных (не подчеркнутых) пометок пометка 5 для v_3 наименьшая. Объявляем пометку 5 для v_3 постоянной, вершину v_3 объявлем активной и помечаем знаком плюс. Вершина v_4 свой плюс теряет (рис.11.8). Переход к шагу 2.

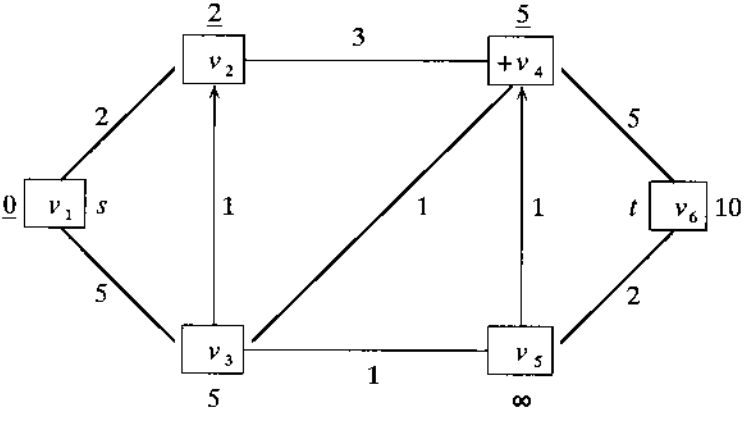


Рис.11.7

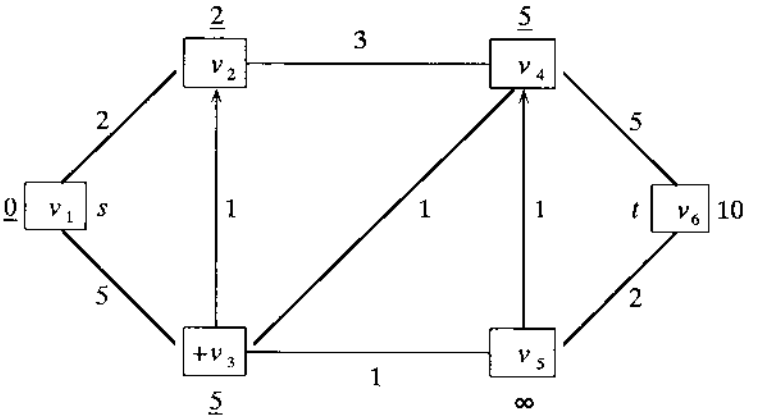


Рис.11.8

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 ∞. Для v_5: 5+1=6<∞. Присваиваем для v_5 новую временную пометку 6 (рис.11.9). Переход к шагу 4.

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.

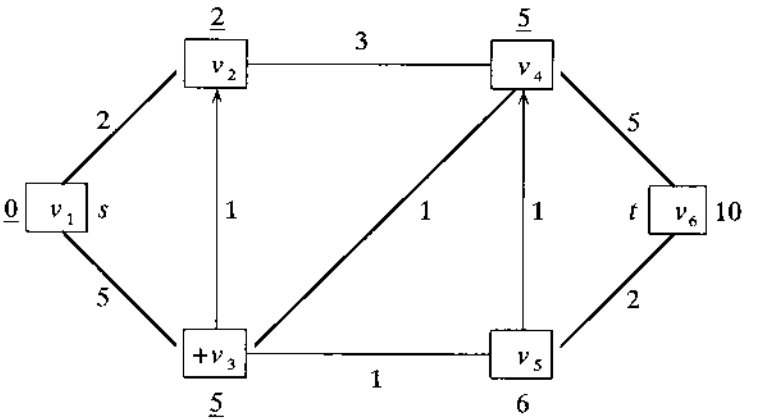


Рис.11.9

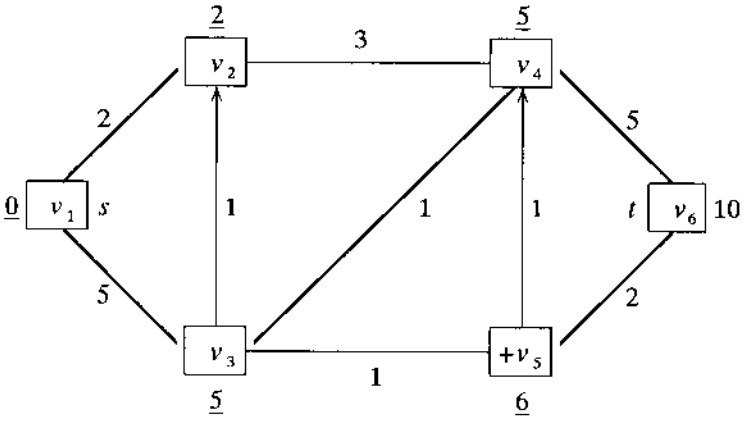


Рис.11.10

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.

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.

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).

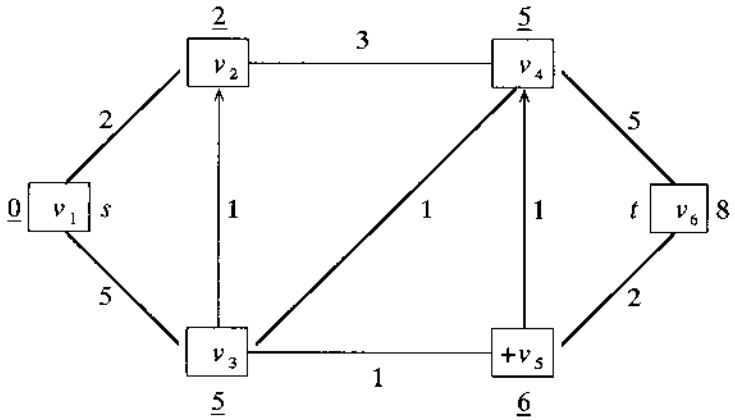


Рис.11.11

$f^{-1}(t) = \{v_4, v_5\}$,
$d(t)-d(v_4)=8-5=3\neq 5=c(v_4,t)$, $d(t)-d(v_5)=8-6=2=c(v_5,t)=2$.
v_5, t есть подпоследовательность кратчайшего пути.

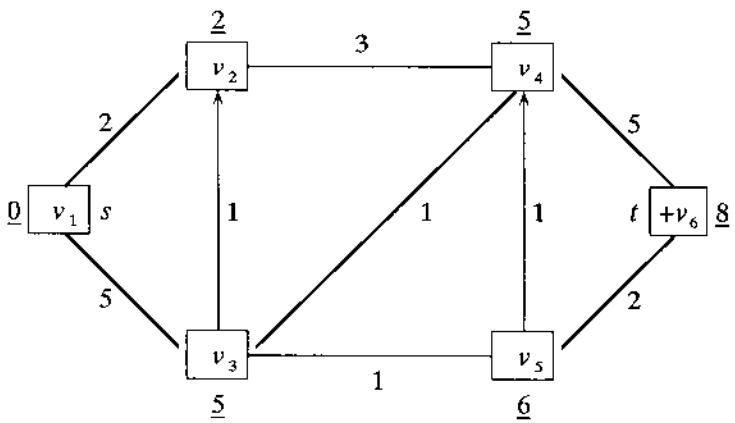


Рис.11.12

$f^{-1}(v_5) = \{v_3\}$; $v_4 \notin f^{-1}(v_5)$, ибо ребро (v_4, v_5) 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 $s=v_1 \to v_3 \to v_5 \to v_6=t$ 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.

$G = (V,E) = (V=\{1,2,3,4,5,6\}, E=\{(1,2),(1,6),(2,3),(2,5),(2,6),(3,4),(3,5),(3,6),(4,5),(5,6)\})$.

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:

$C_3=1261$; $G_3=G_2-C_3=\varnothing$.

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:

$e_1=(1,2), e_2=(2,8), e_3=(8,6), e_4=(6,4), e_5=(4,2), e_6=(2,3),$

$e_7=(3,4), e_8=(4,5), e_9=(5,6), e_{10}=(6,7), e_{11}=(7,8), e_{12}=(8,1)$.

Мы перечислили ребра в порядке их удаления из графа. Построеная последовательность ребер $e_1,e_2,e_3,\ldots,e_{12}$ составляет эйлеров цикл. Заметим, что после удаления ребра e_4 не-

льзя убрать ребро e_8, ибо полученный тогда граф распадется на две несвязные компонент. 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 с помощью алгоритма удаления циклических ребер найти фундаментальную систему циклов, соответствующее множество хорд, каркас, все фундаментальные сечения (разрезы).

$$G = (V,E)=(\{1,2,3,4,5,6\},\{(1,2),(1,4),(1,5),(1,6),(2,3),(2,5),(3,4),(3,6),(4,5),(5,6)\}).$$

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. Фундаметальный 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 фундаметальный разрез составят хорды плюс одно произвольное ребро каркаса. Все фундаментальные разрезы:

$H\cup\{(1,2)\}$, $H\cup\{(1,4)\}$, $H\cup\{(1,6\}$, $H\cup\{(3,4)\}$, $H\cup\{(4,5)\}$.

Матричная теорема о деревьях (Кирхгоф).

Пусть граф $G = (V,E)$ имеет множество вершин $V=\{v_1,\ldots,v_p\}$ 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 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.

$$A = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{matrix}\begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}, \quad M = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{matrix}\begin{bmatrix} 4 & -1 & 0 & -1 & -1 & -1 \\ -1 & 3 & -1 & 0 & -1 & 0 \\ 0 & -1 & 3 & -1 & 0 & -1 \\ -1 & 0 & -1 & 3 & -1 & 0 \\ -1 & -1 & 0 & -1 & 4 & -1 \\ -1 & 0 & -1 & 0 & -1 & 3 \end{bmatrix},$$

$$A_{42} = (-1)^{4+2} \begin{vmatrix} 4 & 0 & -1 & -1 & -1 \\ -1 & -1 & 0 & -1 & 0 \\ 0 & 3 & -1 & 0 & -1 \\ -1 & 0 & -1 & 4 & -1 \\ -1 & -1 & 0 & -1 & 3 \end{vmatrix} = 135.$$

Задача 5. В ненагруженном графе G с помощью алгоритма надстраивания ребер найти каркас, соответствующее множество хорд, фундаментальную систему циклов, все фундаментальные сечения (разрезы).

$G=(V,E)=(\{a,b,c,d,e,f,g\},\{(a,b),(a,g),(b,c),$
$(b,d),(b,f),(b,g),(c,d),(c,g),(d,e),(d,f),$
$(d,g),(e,f),(e,g),(f,g)\})$.

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 фундаметальный 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 найти кратчайший каркас и соответствующие множество хорд, фундаментальную систему циклов, все фундаментальные сечения (разрезы).

$G=(V,E)=(\{a,b,c,d,e,f,g\},\{(a,b,1),(a,g,2),(b,c,7),$
$(b,d,6),(b,f,8),(b,g,3),(c,d,2),(c,g,9),(d,e,1),(d,f,9),$
$(d,g,1),(e,f,4),(e,g,5),(f,g,9)\})$.

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:

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 фундаметальный 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 $G=(U,V,E)$,
$U=\{x_1,x_2,x_3,x_4,x_5,x_6\}$, $V=\{y_1,y_2,y_3,y_4,y_5,y_6,y_7\}$,
$E=\{(x_1,y_1),(x_1,y_2),(x_1,y_5),(x_2,y_1),(x_2,y_3),(x_2,y_5),$
$(x_3,y_1),(x_3,y_6),(x_4,y_3),(x_4,y_4),(x_4,y_6),(x_4,y_7),(x_5,y_5),$

$(x_5,y_7),(x_6,y_4),(x_6,y_6),(x_6,y_7)\}$).
найти совершенное паросочетание. Если его нет, то указать получившееся максимальное паросочетание.

11.2. Алгоритм построения совершенного паросочетания для двудольного графа

Пусть $G = (U,V,E)$ – 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 u нет, то P_i есть совершенное паросочетание. Если есть, то строим в G чередующуюся цепь $\mu_i = [u_1,v_1,u_2,v_2,\ldots,u_p,v_p]$ 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 μ_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 μ_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)

$$\mu_1 = [x_2,y_1,x_1,y_5].$$
$$\begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{matrix}$$

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. $P_2 = \{(x_1,y_5),(x_2,y_1)\}$.

$$\mu_2 = [x_3,y_1,x_2,y_3].$$
$$\begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{matrix}$$

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. $P_4 = \{(x_1,y_5),(x_2,y_3),(x_3,y_1),(x_4,y_4)\}$.

$$\mu_4 = \begin{matrix}[x_5, & y_5, & x_1, & y_1, & x_3, & y_6]. \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1\end{matrix}$$

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. $P_5 = \{(x_1,y_1),(x_2,y_3),(x_3,y_6),(x_4,y_4),(x_5,y_5\}$.

$$\mu_5 = \begin{matrix}[x_6, & y_6, & x_3, & y_1, & x_1, & y_5, & x_5, & y_7]. \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1\end{matrix}$$

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.

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

$U = \{A_1,A_2,A_3,A_4,A_5,A_6\}$,

$V = \bigcup_{i=1}^{6} A_i = \{1,2,3,4,5,6,7\}$,

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}.

Задача 9. Построить наибольшее по весу совершенное паросочетание в полном двудольном графе $G=K_{4,4}=(V_1,V_2,E)$ с весами ребер, заданными в матрице $A=[a_{ij}]$ (рис.11.13 *а*).

$V_1=\{x_1,x_2,x_3,x_4\}$, $V_2=\{y_1,y_2,y_3,y_4\}$, $E=\{e_{ij}=(x_i,y_j):$

$$i,j=1,2,3,4\};\quad A=\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}\begin{array}{c} \begin{array}{cccc} y_1 & y_2 & y_3 & y_4 \end{array} \\ \begin{bmatrix} 5 & 3 & 4 & 2 \\ 3 & 1 & 2 & 1 \\ 4 & 2 & 3 & 1 \\ 6 & 5 & 3 & 2 \end{bmatrix} \end{array}.$$

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 $X=\{x_1,\ldots,x_n\}$, $Y=\{y_1,\ldots,y_n\}$, ребра $E=\{e_{ij}=(x_i,y_j): i,j=1,2,\ldots,n\}$, 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 $\forall y_j\in Y\ v_j=0$. Для любого ребра a_{ij} выполняется $a_{ij}\leqslant u_i+v_j$. Взять в G исходное паросочетание $P=\varnothing$.

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 п.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 п.3.

3. Вычислить $\Delta=\max(u_i+v_j-a_{ij})$ по всем $x_i\in T$, $y_j\notin T$. Изменить пометки вершин по правилу: $\forall x_i\in T\ \ u_i:=u_i-\Delta$; $\forall y_j\in T\ \ v_j:=v_j+\Delta$. 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.

Шаг 0. Пометим вершины $x_1,\ldots,x_4,y_1,\ldots,y_4$ соответственно числами $u_1=5$, $u_2=3$, $u_3=4,u_4=6$, $v_1=v_2=v_3=v_4=0$. Возьмем в G исходное паросочетание $P_0=\varnothing$.

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 $x_1\notin P_0$. $C_1=[x_1,y_1]=\{e_{11}\}$ 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 чередующихся цепей в G_1 с корнем x_2 на рис.11.13T_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.

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_3 всех чередующихся цепей в G_3 с корнем x_3 на рис.11.13T_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 вершин 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 $x_4 \notin P_3$. $C_4=[x_4,y_2,x_2,y_4]=\{e_{42},e_{22},e_{24}\}$ есть чередующаяся цепь в G с корнем в x_4. Для G паросочетание $P_4=(P_3-C_4)\cup(C_4-P_3)=\{e_{11},e_{24},e_{33},e_{42}\}$. Вершина $x_4 \notin P_3$. Дерево T_4 всех чередующихся цепей в G_4 с корнем x_4 есть лишь вершина x_4. Переход к пункту 3.

3. По всем $x_i \in T_4$, $y_j \notin T_4$ число $\Delta = \min(u_i+v_j-a_{ij}) = \min(u_4+v_1-a_{41},\ u_4+v_2-a_{42},\ u_4+v_3-a_{43},\ u_4+v_4-a_{44}) = \min(6+2-6,\ 6+0-5,\ 6+1-3,\ 6+0-2) = \min(2,1,3,4) = 1$. Новые пометки вершин в G есть $u_4:=u_4-\Delta=6-1=5$. 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 $\Sigma = a_{11}+a_{24}+a_{33}+a_{42} = 5+1+3+5 = 14$.

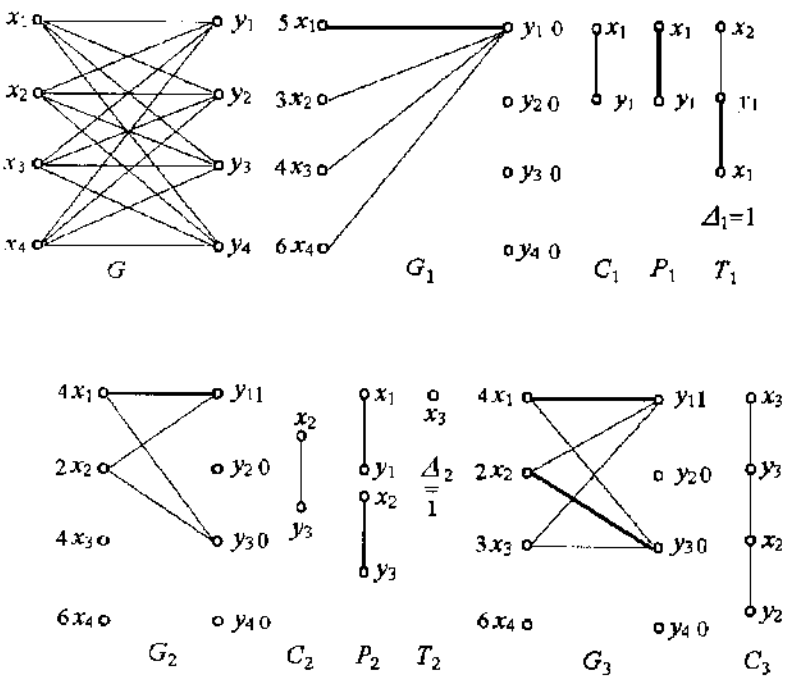
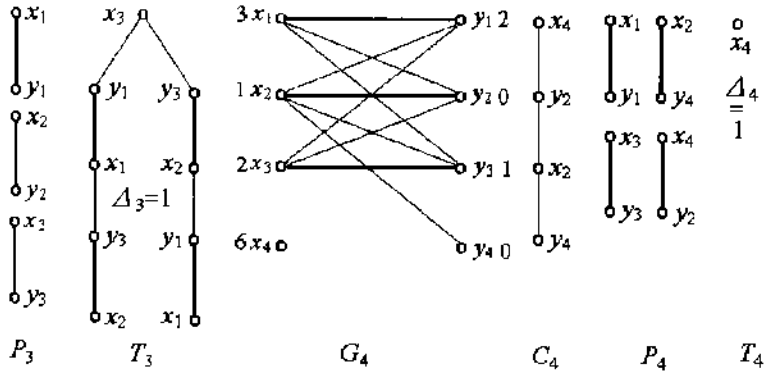
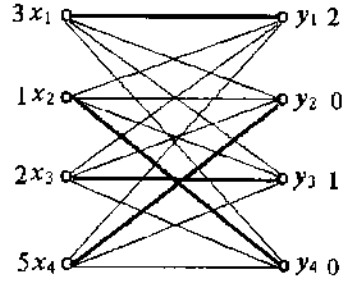


Рис.11.13





G P_4 Σ=14

Рис.11.13 *g*

Задача 10. Построить плоское изображение графа, если это возможно. G = ({1,2,3,4,5,6},{(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 $G=(V,E)$ – 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 $G' = (V',E')$ – некоторый плоский подграф графа G.

Остаток графа G относительно G' есть граф $R = (V'',E'') = (V-V',E'')$ – 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 слеующих 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 – некоторый простой цикл графа G. Поместим на плоскоти 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, несовместимый 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 μ, один или оба конца которой (и только они) принадлежат G_i. Построим граф G_{i+1}, дополнив граф G_i ребрами цепи μ, проведя μ внутри любой из совместимых с куском P граней. Плоский граф G_{i+1} построен. Переходим к пункту 1.

В случае неоднозначности проведения цепи μ будем проводить ее во внутренней грани.

Решение. **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: $R_{11} = (\{3\},\varnothing)$ и $R_{12} = (\{4\},\varnothing)$.

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: $R_2 = (\{3\}, \varnothing)$.

Строим куски графа G относительно G_2 и их контактные точки.

$P_{21} = (\{1,3,5,6\},\{(1,3),(3,5),(3,6)\})$; $\{1,5,6\}$;
$P_{22} = (\{4,6\},\{(4,6)\})$; $\{4,6\}$.

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: $R_3 = (\{3\},\varnothing)$.

Строим куски графа G относительно G_3 и их контактные точки.

$P_{31} = (\{1,3,5,6\},\{(1,3),(3,5),(3,6)\})$; $\{1,5,6\}$.

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:

$F_{40} = [1,2,6,5,1]$; $F_{41} = [1,3,5,6,4,1]$; $F_{42} = [1,4,2,1]$;
$F_{43} = [4,6,2,4]$; $F_{44} = [1,3,5,1]$.

$F_{43} = [4,6,2,4]$; $F_{44} = [1,3,5,1]$.

Остаток R_4 для G относительно G_4 принимает вид: $R_4 = \varnothing$.

Строим куски графа G относительно G_4 и их контактные точки.

$P_{41} = (\{3,6\},\{(3,6)\})$; $\{3,6\}$.

Кусок P_{41} совместим с гранью F_{41}.

Цепь μ_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.

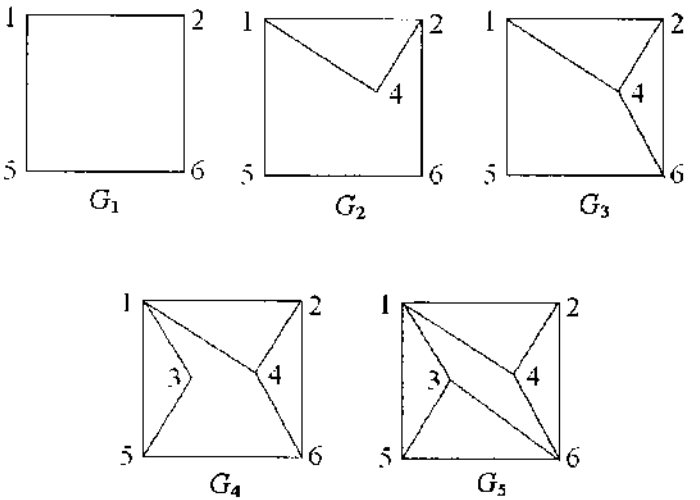


Рис.10.13

Задача 11. В заданном неориентированном графе G найти все максимальные и все наибольшие внутренне устойчивые (независимые) множества вершин.

$G = (V,E) = (\{1,2,3,4,5,6,7\},\{(1,2),(1,3),(1,5),$
$(1,6),(2,3),(3,4),(3,6),(4,5),(4,7),(5,6),(6,7)\})$.

Внутренне устойчивые 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

$\alpha(G) = \max\{|S| : S \subseteq V$ и S внутренне устойчиво в $G\}$.

Внутренне устойчивое множество вершин S называется максимальным (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 – 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

$$F = \mathop{\&}_{(u,v)\in E} (x_u \vee x_v) -$$

условие внутренней устойчивости графа G.

2. Построить минимальную ДНФ D формулы F.

3. Для каждого дизъюнктивного слагаемого $K = x_u x_v \ldots x_w$ в D получить соответствующее ему максимальное внутренне устойчивое множество вершин $S = V - \{u,v,\ldots,w\}$.

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

$$F = \mathop{\&}_{(u,v)\in E} (u \vee v) = (1\vee2)(1\vee3)(1\vee5)(1\vee6)(2\vee3)(3\vee4)\&$$

$$(3\vee6)(4\vee5)(4\vee7)(5\vee6)(6\vee7) = 1357\vee23456\vee23567\vee1246\vee1346.$$

Максимальными внутренне устойчивыми множествами вершин будут множества:

$V-\{1,3,5,7\}=\{2,4,6\}$; $V-\{2,3,4,5,6\}=\{1,7\}$;
$V-\{2,3,5,6,7\}=\{1,4\}$; $V-\{1,2,4,6\}=\{3,5,7\}$;
$V-\{1,3,4,6\}=\{2,5,7\}$.

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 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 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

$$\beta(G) = \min \{ |T| : T \subseteq V \text{ и } T \text{ есть внешне устойчивое множество вершин в } G\}.$$

Внешне устойчивое множество вершин T называется минимальным (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 – 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

$$F = \mathop{\&}_{u \in V} (x_u \vee (\mathop{\vee}_{(u,v) \in E} x_v)) \quad -$$

условие внешней устойчивости графа G.

2. Построить минимальную ДНФ D формулы F.

3. Для каждого дизъюнктивного слагаемого $K = x_u x_v \ldots x_w$ в D получить соответствующее ему минимальное внешне устойчивое множество вершин $S = \{u,v,\ldots,w\}$.

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

$$F = \&_{u \in V} (u \vee (\vee_{(u,v) \in E} v)) = (1V2V3V5V6)(2V1V3)(3V1V2V4V6)\&$$
$$(4V3V5V7)(5V1V4V6)(6V1V3V5V7)(7V4V6) = 156 \vee 17 \vee 246 \vee$$
$$247 \vee 257 \vee 245 \vee 256 \vee 267 \vee 357 \vee 36 \vee 34 \vee 14.$$

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 найти все минимальные и все наименьшие внешне устойчивые (доминирующие) множества вершин.

$$G = (V,E) = (\{1,2,3,4,5\},\{(1,4),(1,5),(2,1),$$
$$(2,3),(3,1),(3,4),(4,5),(5,2)\}).$$

Замечание. Алгоритм для неориентированных графов пригоден и для ориентированных графов.

Решение. Условие внешней устойчивости для графа G

$$F = \&_{u \in V} (u \vee (\vee_{(u,v) \in E} v)) = (1V4V5)(2V1V3)(3V1V4)\&$$
$$(4V5)(5V2) = 35 \vee 24 \vee 15.$$

Все минимальные внешне устойчивые множества: {3,5}, {2, 4}, {1,5}. Из полученных множеств выбираем наименьшие по мощности. Они и составят все наименьшие внешне устойчивые множества вершин: {3,5}; {2,4}; {1,5}.

Задача 15. Найти хроматическое число графа G и его оптимальную раскраску.

$$G=(V,E) = (\{1,2,3,4,5,6,7,8\}, \{(1,2),(1,3),(1,5),(1,6),$$
$$(2,3),(3,4),(3,6),(4,5),(4,7),(5,6),(6,7),(7,8)\}).$$

Оптимальная раскраска вершин графа $G = (V,E)$

Пусть $S_1,S_2,\ldots,S_r$ – 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 $S_1, S_2, \ldots, S_r$.

2. Построить логическую формулу F – условие оптимальной раскраски графа G:

$$F = \underset{v \in V}{\&} \left(\bigvee_{v \in S_i, i=1,\ldots,r} x_{S_i} \right).$$

3. Построить минимальную ДНФ D для F.

4. Каждому дизъюнктивному слагаемому $K_i = x_{S_a} x_{S_b} \ldots x_{S_c}$ в D соответствует минимальное семейство $L_i = \{S_a, S_b, \ldots, S_c\}$ внутренне устойчивых множеств $S_a, S_b, \ldots, S_c$. Из всех L_i выбираем наименьшее по длине k семейство $\{S_{j_1}, S_{j_2}, \ldots, S_{j_k}\}$. Хроматическое число $\chi(G) = k$. Ему соответствует следующая оптимальная раскраска вершин графа G. В цвета $1,2,\ldots,k$ последовательно окрашиваем семейства вершин S_{j_1}, $S_{j_2} - S_{j_1}$, $S_{j_3} - (S_{j_1} \cup S_{j_2}), \ldots, S_{j_k} - (S_{j_1} \cup \ldots \cup S_{j_{k-1}})$ соответственно.

Решение. Условие внутренней устойчивости графа G

$$F = \underset{(u,v) \in E}{\&} (u \vee v) = (1 \vee 2)(1 \vee 3)(1 \vee 5)(1 \vee 6)(2 \vee 3)(3 \vee 4) \&$$

$$(3 \vee 6)(4 \vee 5)(4 \vee 7)(5 \vee 6)(6 \vee 7)(7 \vee 8) =$$

$$23567 \vee 12467 \vee 12468 \vee 13467 \vee 13468 \vee 1357 \vee 234568.$$

Рассматривая полученные дизъюнктивные слагаемые как множества и дополняя их до множества вершин V, получим, что множество $S = \{S_1, S_2, S_3, S_4, S_5, S_6, S_7\} =$

$$\{\{1,4,8\},\{3,5,8\},\{3,5,7\},\{2,5,8\},\{2,5,7\},\{2,4,6,8\},\{1,7\}\}$$

есть список всех максимальных (тупиковых) внутренне устойчивых множеств вершин графа G.

Условие оптимальной раскраски вершин графа

$$R = \underset{v \in V}{\&} \left(\bigvee_{v \in S_i} i \right) = (1 \vee 7)(4 \vee 5 \vee 6)(2 \vee 3)(1 \vee 6)(2 \vee 3 \vee 4 \vee 5)6 \&$$

$$(3 \vee 5 \vee 7)(1 \vee 2 \vee 4 \vee 6) = 672 \vee 736 \vee 2651 \vee 631.$$

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.

$S = (V,E,s,t,c)$ – 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 $f_{max} : E \to \mathbb{N}$ и минимальное сечение (разрез).

II.8. Помечивающий алгоритм вычисления максимального потока в транспортной сети

Пусть $S = (V,E,s,t,c)$ – транспортная сеть и $v_1,v_2,\ldots,v_n$ – внутренние вершины сети.

1. Задать начальный поток f, например, нулевой.
2. Пометим исток пометкой 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 сток t получил пометку (t может получить лишь положительную 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.

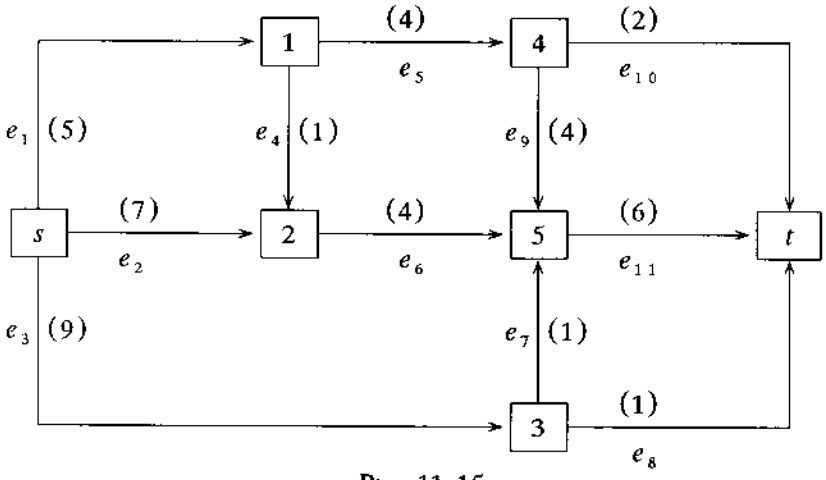
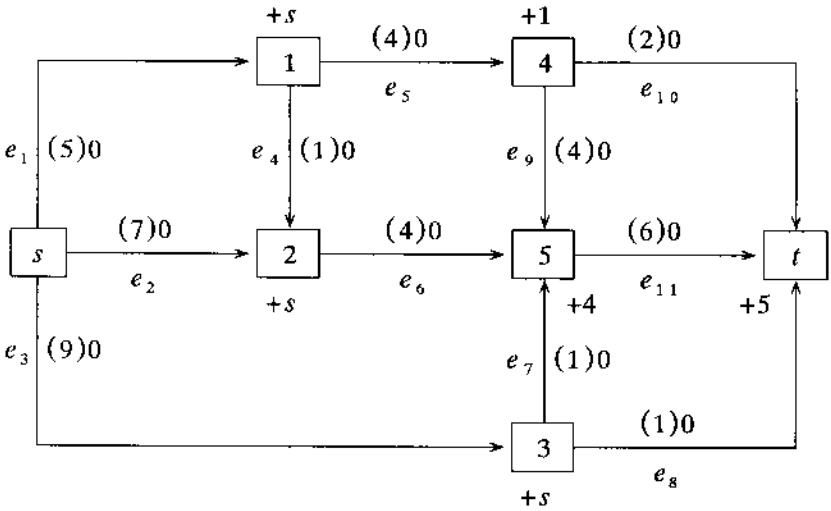


Рис.11.15

Положим начальный поток f_0 нулевым. Пометим вершины сети (рис.11.16).



Поток f_0

Рис.11.16

Ход от вершины t до вершины s: $t,5,4,1,s$.

$s \to 1 \to 4 \to 5 \to t$ – очередная цепь μ между s и t;

$\vec{e}_1$ $\vec{e}_5$ $\vec{e}_9$ $\vec{e}_{11}$ – направленность дуг в цепи μ;

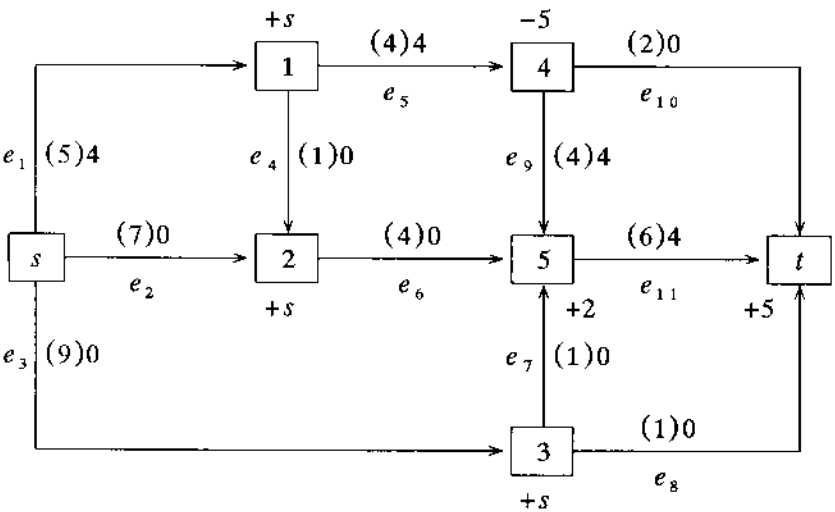
5 4 4 6 – пропускная способность $c(e)$ дуг;

0 0 0 0 – старый поток $f_0(e)$;

5 4 4 6 – $\delta = \min\limits_{e \in \mu} (c(\vec{e}) - f_0(\vec{e})) = 4$;

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 приведены на рис.11.17.



Поток f_1

Рис.11.17

Ход от вершины t до вершины s: $t,5,2,s$.

$s \to 2 \to 5 \to t$ – очередная цепь μ между s и t;

$\vec{e}_2$ $\vec{e}_6$ $\vec{e}_{11}$ – направленность дуг в цепи μ;

7 4 6 – пропускная способность $c(e)$ дуг;

0 0 4 – старый поток $f_1(e)$;

7 4 2 – $\delta = \min\limits_{e \in \mu} (c(e) - f_1(e)) = 2$;

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 приведены на рис.11.18.

Ход от вершины t до вершины s: $t,3,s$.

$s \to 3 \to t$ – очередная цепь μ между s и t;

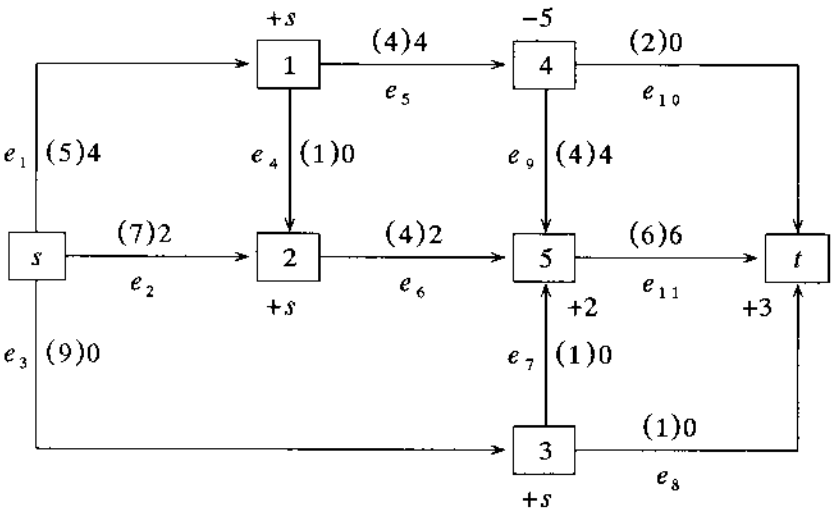
$\vec{e}_3$ $\vec{e}_8$ – направленность дуг в цепи μ;

9 1 – пропускная способность $c(e)$ дуг;

0 0 – старый поток $f_2(e)$;

9 1 – $\delta = \min\limits_{e \in \mu} (c(e) - f_2(e)) = 1$;

1 1 – новый поток $f_3(e) = f_2(e)+\delta = f_2(e)+1$.



Поток f_2

Рис.11.18

Новый поток f_3 и новая разметка вершин сети приведены на рис.11.19.

Ход от вершины t до вершины s: $t,4,5,2,s$.

$s \to 2 \to 5 \leftarrow 4 \to t$ – очередная цепь μ между s и t;

$\vec{e}_2$ $\vec{e}_6$ $\overleftarrow{e}_9$ $\vec{e}_{10}$ – направленность дуг в цепи μ;

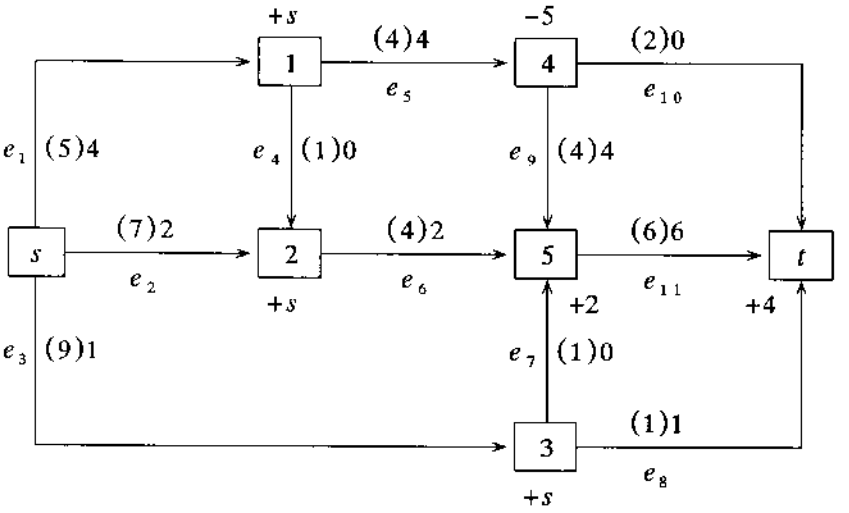
7 4 4 2 – пропускная способность $c(e)$ дуг;

2 2 4 0 – старый поток $f_3(e)$;

5 2 – 2 – $\delta = \min\limits_{e \in \mu} (c(\vec{e}) - f_3(\vec{e})) = 2$;

– – 4 – – $\eta = \min\limits_{e \in \mu} (f_3(\overleftarrow{e})) = 4$; $\varepsilon = \min(\delta, \eta) = 2$;

4 4 2 2 – новый поток $f_4(e) = f_3(e)\begin{cases} +\varepsilon \text{ на } \vec{e} \\ -\varepsilon \text{ на } \overleftarrow{e} \end{cases}$.



Поток f_3

Рис.11.19

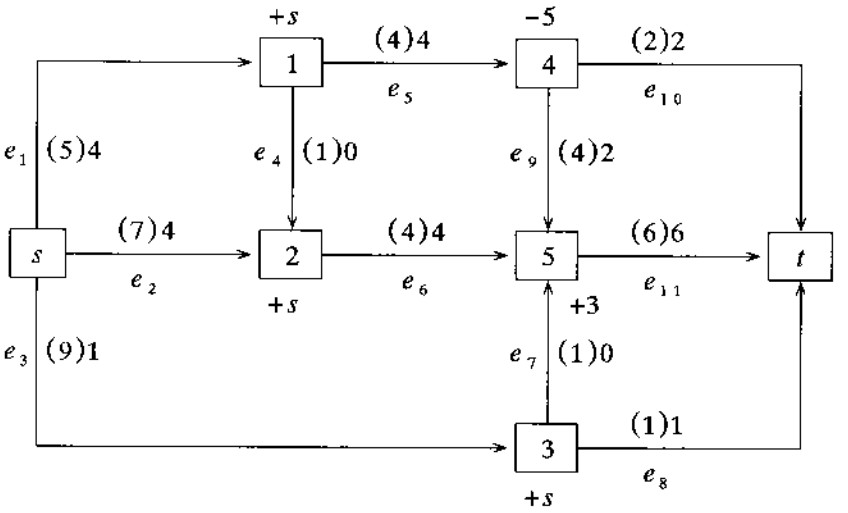
Новый поток f_4 и новая разметка вершин сети приведены на рис.11.20.

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_4}=9.

Максимально возможная величина потока (нагружающая дуги истока, равно как и дуги стока) $M_{f_{max}} = 9$.

Минимальный разрез MS есть множество дуг в потоке f_4 на рис.11.20, заходящих в непомеченные вершины из помеченных вершин.

$MS = \{e_8, e_{10}, e_{11}\} = \{(3,t,1),(4,t,2),(5,t,6)\}$.



Поток f_4

Рис.11.20

Пропускная способность минимального разреза
$c_{\min} = M_{f_{max}} = f_4(e_8)+f_4(e_{10})+f_4(e_{11}) = 1+2+6 = 9.$

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 ожерелий, которые можно составить из шести бусин не более чем m=2 цветов, синего и красного.

Решение. Ожерелье типа (n,k) есть правильный n-угольник, вершины которого раскрашены в не более чем k цветов.

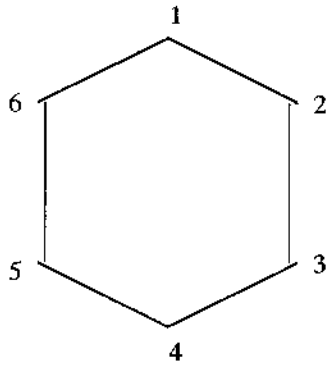
Два ожерелья неотличимы (одинаковы), если одно можно получить из другого, поворачивая его относительно точки симметрии или симметрично отражая относительно одной из осей симметрии.

Для подсчета числа ожерелий типа (n,k) нужно найти группу G вращений и симметрий правильного n–угольника, которая есть некоторая группа подстановок на множестве $X=\{1,2,\ldots,n\}$, потом составить многочлен циклов, а затем применить теорему Пойа.

Подсчитаем число ожерелий, которые можно составить из шести бусин не более чем двух цветов, синего и красного.

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 $(1,1,1,1,1,1>$ соответствует слагаемому s_1^6 многочлена циклов.

2 подстановки p_1, p_5 типа <6> соответствуют слагаемому $2s_6$ многочлена циклов.

2 подстановки p_2, p_4 типа <3,3> соответствуют слагаемому $2s_3^2$ многочлена циклов.

4 подстановки p_3, p_9, p_{10}, p_{11} типа <2,2,2> соответствуют слагаемому $4s_2^3$ многочлена циклов.

3 подстановки p_6, p_7, p_8 типа <1,1,2,2> соответствуют слагаемому $3s_1^2 s_2^2$ многочлена циклов.

По теореме Пойа многочлен циклов

$$N(G) = |G|^{-1} \sum_{p \in G} \prod_{k=1}^{n} s_k^{j_k(p)}.$$

Из 6 бусин не более чем двух цветов можно составить

$$N(G) = |G|^{-1} \sum_{p \in G} \prod_{k=1}^{n} s_k^{j_k(p)} \Big|_{s_k = m = 2} =$$

$$\frac{1}{12}(s_1^6 + 2s_6 + 2s_3^2 + 4s_2^3 + 3s_1^2 s_2^2) \Big|_{s_1 = \ldots = s_6 = m = 2} =$$

$$(m^6 + 2 \cdot m + 2 \cdot m^2 + 4 \cdot m^3 + 3 \cdot m^2 \cdot m^2)/12 =$$

$$(2^6 + 2 \cdot 2 + 2 \cdot 2^2 + 4 \cdot 2^3 + 3 \cdot 2^2 \cdot 2^2)/12 =$$

$$(64 + 4 + 8 + 32 + 48)/12 = 156/12 = 13 \text{ ожерелий.}$$

Задача 18. 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 G вращений куба, состоящую из следующих подстановок (укажем только вторую строку подстановки).

Вокруг каждой из трех осей, соединяющей центры противоположных граней.

(1,5,8,4)(2,6,7,3), (1,4,3,2)(5,8,7,6),
(1,8)(2,7)(3,6)(4,5), (1,3),(2,4)(5,7)(6,8),
(1,4,8,5)(2,3,7,6), (1,2,3,4)(5,6,7,8),
(1,5,6,2)(3,4,8,7), (1,6)(2,5)(3,8)(4,7),
(1,2,6,5)(3,7,8,4).

Вокруг каждой из четырех диагоналей куба.

(1)(2,5,4)(3,6,8)(7), (2)(1,3,6)(4,7,5)(8),
(3)(1,6,8)(2,7,4)(5), (4)(1,3,8)(2,7,5)(6),
(1)(2,4,5)(3,8,6)(7), (2)(1,6,3)(4,5,7)(8),
(3)(1,8,6)(2,4,7)(5), (4)(1,8,3)(2,5,7)(6).

Вокруг каждой из шести осей, соединяющих середины противоположных ребер.

(1,5)(2,8)(3,7)(4,6), (1,2)(3,5)(4,6)(7,8),
(1,7)(2,3)(4,6)(5,8), (1,7)(2,6)(3,5)(4,8),
(1,7)(2,8)(3,4)(5,6), (1,4)(2,8)(3,5)(6,7).

Вместе с тождественной (1)(2)(3)(4)(5)(6)(7)(8) это составляет 24 подстановки группы G.

В группе подстановок вращений G куба найти тип каждой подстановки и соответствующее слагаемое в многочлене циклов (в цикловом индексе). В группе подстановок вращений G куба:

1 подстановка типа <1,1,1,1,1,1,1,1> из 8 циклов соответствует слагаемому s_1^8 многочлена циклов;

6 подстановок типа <4,4> (это 2 цикла длины 4) соответствуют слагаемому $6s_4^2$ многочлена циклов;

9 подстановок типа <2,2,2,2> (это 4 цикла длины 2) соответствуют слагаемому $9s_2^4$ многочлена циклов;

8 подстановок типа <1,1,3,3> (это 4 цикла, из которых 2 длины 1 и других 2 длины 3), соответствуют слагаемому $8s_1^2s_3^2$ 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

$$N(G_M) = |G|^{-1} \sum_{p \in G} \prod_{k=1}^{n} s_k^{j_k(p)} \Bigg|_{s_k = m = 3} =$$

$$|G|^{-1}(s_1^8 + 6s_4^2 + 9s_2^4 + 8s_1^2s_3^2)\Big|_{s_1=\ldots=s_8=m=3} =$$
$$(1/24)(m^8 + 6m^2 + 9m^4 + 8m^2m^2) =$$
$$(1/24)(3^8 + 6\cdot 3^2 + 9\cdot 3^4 + 8\cdot 3^4) = 333.$$

Ответ. 333 есть число различных раскрасок вершин куба не более чем тремя красками.

12. ПАКЕТ MATHCAD–ПРОГРАММ ДЛЯ РАБОТЫ В ПОЛЯХ ГАЛУА

Полиномы задаются как векторы в порядке убывания степеней. Например, если знак T означает транспонирование, то полином $P(x) = 4x^5+2x^3+9$ задается вектором $P = (4\ 0\ 2\ 0\ 0\ 9)^T$.

12.1. Факторизация натурального числа n (перебор)

```
factoring(n) :=
  k ← 2
  s ← 1
  f_s ← 1
  while k ≤ n
    if mod(n,k) = 0
      s ← s+1
      f_s ← k
      n ← n/k
      k ← f_s
    k ← k+1 if mod(n,k) ≠ 0
  f
```

Например, factoring(3946)=$(1\ 2\ 1973)^T$, factoring(3832)=$(1\ 2\ 2\ 2\ 479)^T$, factoring(3930)=$(1\ 2\ 3\ 5\ 131)^T$, factoring(58104200)=$(1\ 2\ 2\ 2\ 5\ 5\ 7\ 7\ 7\ 7\ 11\ 11)^T$.

12.2. Вычисление в факторизации $n=r_0^{e_0}r_1^{e_1}\ldots r_k^{ek}$ векторов $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$

```
factoring_re(n) :=
  x ← factoring(n)
  i ← 2
  r_0 ← x_1
  e_0 ← 1
  k ← 0
  while i ≤ last(x)
    if x_i ≠ x_{i-1}
      k ← k+1
      r_k ← x_i
      e_k ← 1
    otherwise
      e_k ← e_k+1
```

```
factoring2(n) :=
  x ← factoring(n)
  i ← 2
  j_{0,0} ← x_1
  j_{0,1} ← 1
  k ← 0
  while i ≤ last(x)
    if x_i ≠ x_{i-1}
      k ← k+1
      j_{k,0} ← x_i
      j_{k,1} ← 1
    otherwise
      j_{k,1} ← j_{k,1}+1
```

```
|  |  |i←i                    |  |  |i←i
|  |i←i+1                     |  |i←i+1
|re←(r)                       |j
|   (e)
|re
```

Если n=58104200, то r=factoring_re(n)$_0$=(2 5 7 11)^T,
e=factoring_re(n)$_1$=(3 2 4 2)^T.
Если n=58104200, то r=factoring2(n)$^{<0>}$=(2 5 7 11)^T,
e=factoring2(n)$^{<1>}$=(3 2 4 2)^T.

12.3. Выделение всех множителей k в n (представление числа n в виде $n=k^e \cdot s$, где k не делит s)

```
factor_k_in_integer(n,k) :=
|s←0
|f_s←1
|while mod(n,k)=0
|  |s←s+1
|  |f_s←k
|  |n←n/k
|  |k←f_s
|fen_0←f
|fen_1←last(f)
|fen_2←n
|fen
```

Если n=26353800, k=2, то e:=factor_k_in_integer(n,k)$_1$=3,
s:=factor_k_in_integer(n,k)$_2$=3294225 и $n=2^e \cdot s = 2^3 \cdot 3294225$.

12.4. Конкатенация чисел

```
numconcat(m,r) :=
|ms←num2str(m)
|rs←num2str(r)
|mrs←concat(ms,rs)
|mr←str2num(mrs)
|mr
```

Если m=4379, r=795, то mr:=numconcat(m,r)=4379795.

```
inverse_vect(F) :=
  n ← last(F)
  for i ∈ 0..n
    Q_{n-i} ← F_i
  Q
```

Например, inverse_vect$((1\ -2\ 3)^T) = (3\ -2\ 1)^T$.

12.6. h-ричная запись десятеричного числа n

```
h_based_rep(n,h) :=
  q ← n
  i ← 0
  while q ≠ 0
    r ← mod(n,h)
    q ← (n-r)/h
    a_i ← r
    n ← q
    i ← i+1
  a ← inverse_vect(a)
  a
```

Например, h_based_rep$(4,2) = (1\ 0\ 0)^T$,
h_based_rep$(3945,21) = (8\ 19\ 18)^T$.

12.7. Модулярная степень $m^e \pmod n$ в $\mathbb{Z}_n$

```
modexpon(m,e,n) :=
  c ← 1 if e = 0
  c
  break if e = 0
  c ← mod(m,n) if e = 1
  c
  break if e = 1
  e2 ← h_based_rep(e,2)
  e1 ← inverse_vect(e2)
  t ← last(e1)
  c ← 1
  A ← m
```

```
c ← m  if  e1_0 = 1
for i ∈ 1..t
    A ← mod(A^2, n)
    c ← mod(A · c, n)  if  e1_i = 1
c
```

Например, $7^{593} \pmod{1325}$ = modexpon(7,593,1325) = 857.

*12.8. Алгоритм Евклида нахождения d=*нод(*a*,*b*)

gcd(a,b) :=

```
return a  if  b=0
break  if  b=0
while  b ≠ 0
    r ← mod(a,b)
    q ← (a−r)/b
    a ← b
    b ← r
    d ← a
d
```

Например, нод(3438,2466) = gcd(3438,2466) = 18.

*12.9. Расширенный алгоритм Евклида нахождения d=*нод(*a*,*b*) *и тех целых чисел u,v, для которых d=au+bv*

gcdxy(a,b) :=

$$dxy \leftarrow \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$$

```
dxy
break  if  b=0
b=0  otherwise
q ← 0
r ← 1
u ← 0
v ← 0
u2 ← 1
u1 ← 0
```

```
v2 ← 0
v1 ← 1
i ← 1
while b>0
    r ← mod(a,b)
    q ← (a−r)/b
    u ← u2−q·u1
    v ← v2−q·v1
    a ← b
    b ← r
    u2 ← u1
    u1 ← u
    v2 ← v1
    v1 ← v
    i ← i+1
    dxy ← (a, u2, v2)
dxy
```

Например, нод(3438,2466) = gcdxy(3438,2466) = $(18\ \ 33\ \ -46)^T$, d=18, u=33, v=−46.

12.10. Остаток от деления a на p в $\mathbb{Z}$ $(a \bmod p)$

```
nmod(a,p) :=
c ← mod(a,p)
c ← c+p if c<0 ∧ p≥0
c ← −c−p if c>0 ∧ p≤0
c ← −c if c<0 ∧ p≤0
c
```

12.11. Сумма чисел a,b из $\mathbb{Z}$ *по* $\bmod p$

```
nsum(a,b,p) :=
c ← a+b
c ← nmod(c,p)
c
```

12.12. Разность чисел a,b из $\mathbb{Z}$ *по* $\bmod p$

```
ndif(a,b,p) :=
|c ← a−b
|c ← nmod(c,p)
|c
```

12.13. Умножение чисел a,b из $\mathbb{Z}$ по $\bmod p$

```
nmul(a,b,p) :=
|c ← a · b
|c ← nmod(c,p)
|c
```

12.14. Мультипликативный обратный элемент $a^{-1} \pmod p$ в $\mathbb{Z}_p^*$ с простым p

```
rev(a,p) :=
|if gcdxy(a,p)_0 > 1
|  |return "no inverse"
|  |break
|c ← gcdxy(a,p)_1
|while c<0
|c ← c+p
|c ← mod(c,p)
|c
```

Например, $14^{-1} \pmod{31} = \text{rev}(14,31) = 20$.

12.15. Деление a на b из $\mathbb{Z}_p^*$ по $\bmod p$

```
ndiv(a,b,p) := mod(a · rev(b,p),p)
```

12.16. Тест Миллера–Рабина для простоты числа

```
MillerRabin(n,t) :=
|if n ≤ 1
|  |return "Take n > 1
|  |break
|if n = 2 ∨ n = 3 ∨ n = 5
|  |return "Prime"
|  |break
|if mod(n,2) = 0
|  |return "Composite"
|  |break
|n1 ← n−1
```

```
    if mod(n-1,2)=0
    s1←0
    n2←0
    while (n2=0)
      n2←mod(n1,2)
      if n2=0
        n1←n1/2
        s1←s1+1
    s←s1
    r←r1
  for i ∈ 1..t
    x←1
    while x<2
      x←rnd(n-2)
    a←round(x)
    y←modexpon(a,r,n)
    if (y≠1) ∧ (y≠n-1)
      j←1
      while (j≤s-1) ∧ (y≠n-1)
        y←mod(y^2,n)
        if y=1
          return "Composite"
          break
        j←j+1
      if y≠n-1
        return "Composite"
        break
    z←"Prime" if (y=1) ∧ (y=n-1)
  return z
```

Если n=2597, параметр безопасности t=1000, то MillerRabin(n, t) = "Composite". При n=2609 MillerRabin(n,t) = "Prime". Вероятность получить неверный ответ меньше $(1/4)^t$.

12.17. Метод Гаусса решения системы сравнений $x \equiv c_i \pmod{m_i}$ с попарно простыми m_i, i=1,2,...,r

```
Gauss_syst_congr(c,m) :=
  r←last(c)
```

```
M ← ∏_{i=0}^{r} m_i
for i ∈ 0..r
    R_i ← M / m_i
    N_i ← rev(R_i, m_i)
x ← mod(∑_{i=0}^{r} c_i · R_i · N_i, M)
x
```

Если $c = (1\ 3\ 2)^T$, $m = (4\ 5\ 7)^T$, то решение
x = Gauss_syst_congr(c,m) = 93.

12.18. Удаление всех первых нулей в полиноме $P(x)$ из $\mathbb{Z}_p[x]$

removepolzeroes(P) :=

```
R_0 ← 0 if P · P = 0
R
break if P · P = 0
mP ← last(P)
d ← 0
j ← 0
while P_j = 0 ∧ j ≤ mP
    d ← d+1
    j ← j+1
for i ∈ 0..mP−d
  R_i ← P_{i+d}
R
```

Например, removepolzeroes$((0\ 0\ 0\ -1\ 0\ 5)^T) = (-1\ 0\ 5)^T$.

12.19. Вычисление символа Якоби $\left(\frac{n}{a}\right)$

JACOBI(n,a) :=

```
JAC ← 0 if a ≠ 0
JAC ← 1 if a ≠ 1
JAC
break if a = 0 ∨ a = 1
e ← factor_k_in_integer(a,2)_1
a1 ← factor_k_in_integer(a,2)_2
s ← 1 if mod(e,2)=0
```

```
|s←1 if mod(e,2)≠0 ∧ (mod(e,8)=1 ∨ mod(e,2)=7)
|s←−1 if mod(e,2)≠0 ∧ (mod(e,8)=3 ∨ mod(e,2)=5)
|n1←mod(n,a1)
|JAC←s if a1=1
|JAC
|break if a1=1
|a←n1
|n←a1
|JAC←s·JACOBI(a,n) if a1≠1
```

Если n=24961, p_1=23, p_2=37, то JACOBI(n,p_1)=1, JACOBI(n,p_2)=−1.

12.20. Сумма полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$

sumpoloverZp(P,Q,p) :=

```
|mP←last(P)
|mQ←last(Q)
|mPQ←mP−mQ
|mQP←mQ−mP
|for i ∈ 0..mP
| R_i←nsum(P_i,Q_i,p) if mPQ=0
|for i ∈ 0..mP
| |R_i←P_i if mPQ>0 ∧ i<mPQ
| |R_i←nsum(P_i,Q_{i−mPQ},p) if mPQ>0 ∧ i≥mPQ
|for i ∈ 0..mQ
| |R_i←Q_i if mQP>0 ∧ i<mQP
| |R_i←nsum(P_i,Q_{i−mQP},p) if mQP>0 ∧ i≥mQP
|R←removepolzeroes(R)
|R
```

Если p=5, $P(x)=2x^4+3x^3+4x^2+x+1$, $Q(x)=3x^4+2x^3+3x^2+2x+1$, то $P(x)+Q(x)$ = sumpoloverZp(P,Q,p) = $(2\ 3\ 2)^T$ = $2x^2+3x+2$.

12.21. Разность полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$

difpoloverZp(P,Q,p) :=

```
|mP←last(P)
|mQ←last(Q)
|mPQ←mP−mQ
|mQP←mQ−mP
|for i ∈ 0..mP
```

```
  R_i ← ndif(P_i,Q_i,p) if mPQ=0
for i ∈ 0..mP
  |R_i ← P_i if mPQ>0 ∧ i<mPQ
  |R_i ← ndif(P_i,Q_{i-mPQ},p) if mPQ>0 ∧ i≥mPQ
for i ∈ 0..mQ
  |R_i ← ndif(0,Q_i,p) if mQP>0 ∧ i<mQP
  |R_i ← ndif(P_i,Q_{i-mPQ},p) if mQP>0 ∧ i≥mQP
R ← removepolzeroes(R)
R
```

Если p=5, $P(x)=3x^4+2x^3+4x^2+x+1$, $Q(x)=3x^4+2x^3+5x^2+2x+1$, то $P(x)-Q(x)$ = difpoloverZp(P,Q,p) = $(1\ 4\ 0)^T = x^2+4x$.

12.22. Произведение полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$

```
mulpol(P,Q,p) :=
|mP ← last(P)
|mQ ← last(Q)
|for i ∈ 0..mP+mQ
| mul_i ← 0
|for i ∈ 0..mP
| for j ∈ 0..mQ
|  mul_{i+j} ← nsum(mul_{i+j},mod(P_i·Q_i,p),p)
|mul ← removepolzeroes(mul)
|mul
```

Если p=6, $P(x)=3x^4+2x^3+4x^2+x+1$, $Q(x)=2x^4+3x^3+3x^2+2x+1$, то $P(x)\cdot Q(x)$ = mulpol(P,Q,p) = $(1\ 5\ 2\ 0\ 4\ 3\ 3\ 1)^T = x^7+5x^6+2x^5+4x^3+3x^2+3x+1$.

12.23. Частное и остаток от деления полинома $P(x)$ из $\mathbb{Z}_p[x]$ на полином $Q(x)$ из $\mathbb{Z}_p[x]$

```
divpolqoutrestZp(P,Q,p) :=
|mP ← last(P)
|mQ ← last(Q)
|QUOTIENT_0 ← 0 if if mP<mQ
|REST ← P if mP<mQ
|QR_0 ← QUOTIENT
|QR_1 ← REST
|QR
|break if mP<mQ
|RES ← P
```

```
for i ∈ 0..mP-mQ
  l ← RES_i
  QUOTIENT_i ← ndiv(l,Q_0,p)
  for j ∈ 0..mQ
    RES_{i+j} ← ndif(RES_{i+j},nmul(ndiv(l,Q_0,p),Q_j,p),p)
for i ∈ 0..mQ-1 if mQ > 0
  REST_{mQ-i-1} ← RES_{mP-i}
for i ∈ 0..mQ if mQ = 0
  REST_{mQ-i} ← RES_{mP-i}
REST ← removepolzeroes(REST)
QUOTIENT ← removepolzeroes(QUOTIENT)
QR_0 ← QUOTIENT
QR_1 ← REST
QR
```

Частное

divpolqoutZp(P,Q,p) := divpolqoutrestZp(P,Q,p)$_0$

Остаток

divpolrestZp(P,Q,p) := divpolqoutrestZp(P,Q,p)$_1$

Если p=5, $P(x)=3x^5+2x^4+0x^3+x^2+2x+4$, $Q(x)=4x^3+3x^2+3x+2$, то частное divpolqoutZp(P,Q,p) = $(2\ 0\ 1)^T = 2x^2+1$ и остаток divpolrestZp(P,Q,p) = $(1\ 4\ 2)^T = x^2+4x+2$.

12.24. Частное и остаток от деления произведения полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$ по модулю неприводимого полинома $F(x)$ из $\mathbb{Z}_p[x]$

```
divpolqoutrestGF(P,Q,F,p) :=
  RES ← mulpol(P,Q,p)
  mRES ← last(RES)
  mF ← last(F)
  QUOTIENT_0 ← 0 if mRES < mF
  REST ← RES if mRES < mF
  QR_0 ← QUOTIENT
  QR_1 ← REST
  QR
  break if mRES < mF
  mP ← last(P)
  mQ ← last(Q)
  mPQ ← mP+mQ
  mF ← last(F)
  for i ∈ 0..mPQ-mF
```

```
    l ← RES_i
    QUOTIENT_i ← ndiv(l,F_0,p)
    for j ∈ 0..mF
      RES_{i+j} ← ndif(RES_{i+j},nmul(ndiv(l,F_0,p),F_j,p),p)
  for i ∈ 0..mF−1
    REST_{mF−1−i} ← RES_{mP+mQ−i}
  QUOTIENT ← removepolzeroes(QUOTIENT)
  REST ← removepolzeroes(REST)
  QR_0 ← QUOTIENT
  QR_1 ← REST
  QR
```

Частное

$\mathrm{divpolqoutGF}(P,Q,F,p) := \mathrm{divpolqoutrestGF}(P,Q,F,p)_0$

Остаток

$\mathrm{divpolrestGF}(P,Q,F,p) := \mathrm{divpolqoutrestGF}(P,Q,F,p)_1$

Если p=5, $P(x)$=$3x^3+4x^2+2$, $Q(x)$=$4x^2+x+3$, неприводимый полином $F(x)$=x^4+2, то частное $\mathrm{divpolqoutGF}(P,Q,F,p) = (2\ 4)^T = 2x + 4$, остаток = $\mathrm{divpolrestGF}(P,Q,F,p) = (3\ 0\ 3\ 3)^T = 3x^3+3x+3$.

12.25. Умножение в поле Галуа $GF(p^m)$ полиномов $P(x),Q(x)$ по модулю неприводимого из $\mathbb{Z}_p[x]$ полинома $F(x)$

```
polmulinGF(P,Q,F,p) := divpolrestGF(P,Q,F,p)
```

Если p=5, $P(x)$=$3x^3+4x^2+2$, $Q(x)$=x^3+2x^2+4x+3, неприводимый полином $F(x)$=x^4+2, то $P(x)\cdot Q(x) \pmod{F(x)}$ = $\mathrm{polmulinGF}(P,Q,F,p) = (2\ 0\ 3\ 1)^T = 2x^3+3x+1$.

12.26. Алгоритм Евклида нахождения $d(x)$=нод$(P(x),Q(x))$ для полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$

12.26.1. Нахождение общего делителя $d(x)$=од$(P(x),Q(x))$ наибольшей степени

```
cdmaxdegpolZp(P,Q,p) :=
  a ← P
  b ← Q
  while b·b > 0
    q ← divpolqoutZp(a,b,p)
    r ← divpolrestZp(a,b,p)
    a ← b
    b ← r
```

```
d ← a
d
```

Если p=5, $P(x)=4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4$, $Q(x)=3x^7+x^6+4x^4+3x^3+1x^2+4x+4$, то $d(x)$ = од(P,Q) = cdmaxdegpolZp(P,Q,p)$_0$ = $(2\ 2\ 3\ 3)^T$ = $2x^3+2x^2+3x+3$; Заметим, что $d(x)=2x^3+2x^2+3x+3$ не есть наибольший общий делитель, ибо старший коэффициент в $d(x)$ не есть 1.

12.26.2. Нахождение $d(x)$=нод$(P(x),Q(x))$

```
gcdpolZp(P,Q,p) :=
d ← cdmaxdegpolZp(P,Q,p)
lc ← d_0
d
break if lc = 1
rlc_0 ← rev(lc,p)
d ← mulpol(d,rlc,p)
d
```

Если p=5, $P(x)=4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4$, $Q(x)=3x^7+x^6+4x^4+3x^3+1x^2+4x+4$, то $d(x)$ = нод(P,Q) = gcdpolZp(P,Q,p)$_0$ = $(1\ 1\ 4\ 4)^T$ = x^3+x^2+4x+4.

12.27. Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$ нахождения $d(x)$=нод$(P(x),Q(x))$ и таких $u(x),v(x)$, что $d(x)=P(x)u(x)+Q(x)v(x)$

12.27.1. Нахождение общего делителя $d(x)$=од$(P(x),Q(x))$ наибольшей степени и таких $u(x),v(x)$, что $d(x)=P(x)u(x)+Q(x)v(x)$

```
cdmaxdegDUVpolZp(P,Q,p) :=
a ← P
b ← Q
sp ← b · b
d ← a if sp = 0
x_0 ← 1 if sp = 0
y_0 ← 0 if sp = 0
sp = 0 otherwise
x2_0 ← 1
x1_0 ← 0
y2_0 ← 0
```

```
y1_0 ← 1
while b · b > 0
    q ← divpolqoutZp(a,b,p)
    r ← divpolrestZp(a,b,p)
    mpx ← mulpol(q,x1,p)
    mpy ← mulpol(q,y1,p)
    x ← removepolzeroes(difpoloverZp(x2,mpx,p))
    y ← removepolzeroes(difpoloverZp(y2,mpy,p))
    a ← b
    b ← r
    x2 ← x1
    x1 ← x
    y2 ← y1
    y1 ← y
d ← a
x ← x2
y ← y2
u_0 ← d
u_1 ← x
u_2 ← y
u
```

Если p=5, $P(x)=4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4$, $Q(x)=3x^7+x^6+4x^4+3x^3+1x^2+4x+4$, то $d(x)$ = од(P,Q) = cdmaxdegDUVpolZp(P,Q,p)$_0$ = $(2\ 2\ 3\ 3)^T$ = $2x^3+2x^2+3x+3$; $u(x)$ = cdmaxdegDUVpolZp(P,Q,p)$_1$ = $(3\ 2\ 1\ 4)^T$ = $3x^3+2x^2+1x+4$, $v(x)$ = cdmaxdegDUVpolZp(P,Q,p)$_2$ = $(1\ 4\ 3\ 0\ 3)^T$ = $x^4+4x^3+3x^2+3$. Заметим, что $d(x)=2x^3+2x^2+3x+3$ не есть наибольший общий делитель, ибо старший коэффициент не есть 1.

12.27.2. Нахождение $d(x)$=нод$(P(x),Q(x))$ и таких $u(x),v(x)$ из $\mathbb{Z}_p[x]$, что $d(x)=P(x)u(x)+Q(x)v(x)$

```
gcdDUVpolZp(P,Q,p) :=
    u ← cdmaxdegDUVpolZp(P,Q,p)
    d ← u_0
    lc ← d_0
    u
    break if lc = 1
    rlc_0 ← rev(lc,p)
    x ← u_1
    y ← u_2
```

```
d ← mulpol(d,rlc,p)
x ← mulpol(x,rlc,p)
y ← mulpol(y,rlc,p)
u_0 ← d
u_1 ← x
u_2 ← y
u
```

Если p=5, $P(x)$=$4x^8+3x^7+4x^6+2x^5+4x^4+2x^3+4x^2+3x+4$, $Q(x)$=$3x^7+x^6+4x^4+3x^3+1x^2+4x+4$, то $d(x)$ = нод(P,Q) = gcdDUVpolZp(P,Q,p)$_0$ = $(1\ 1\ 4\ 4)^T$ = x^3+x^2+4x+4;
$u(x)$ = gcdDUVpolZp(P,Q,p)$_1$ = $(4\ 1\ 3\ 2)^T$ = $4x^3+x^2+3x+2$,
$v(x)$ = gcdDUVpolZp(P,Q,p)$_2$ = $(3\ 2\ 4\ 0\ 4)^T$ = $3x^4+2x^3+4x^2+4$.

12.28. Мультипликативный обратный полином для полинома $P(x)$ в поле Галуа $GF(p^m)$ с неприводимым полиномом $F(x)$

inverseGF(P,F,p) := gcdDUVpolZp(P,F,p)$_1$

Если p=5, $P(x)$=$3x^3+4x^2+2$=$(3\ 4\ 0\ 2)^T$, $F(x)$=x^4+2 = $(1\ 0\ 0\ 0\ 2)^T$, то $P(x)^{-1}\ (\mathrm{mod}\ F(x))$ = inverseGF(P,F,p) = $(4\ 0\ 1\ 1)$ = $4x^3+x+1$.

12.29. Модулярня степень е полинома $P(x)$ в поле Галуа $GF(p^m)$ с неприводимым полиномом $F(x)$

modpolpowerZp(P,F,e,p) :=

```
c_0 ← 1 if e = 0
c
break if e = 0
c ← P if e = 1
c
break if e = 1
c_0 ← 1
e2 ← h_based_rep(e,2)
e1 ← inverse_vect(e2)
t ← last(e1)
A ← P
c ← polmulinGF(A,c,F,p) if e1_0 = 1
for i ∈ 1..t
    A ← divpolrestGF(A,A,F,p)
    c ← divpolrestGF(A,c,F,p) if e1_i = 1
```

```
c
```

Если $p=5$, $P(x)=3x^2+x+4=(3\ 1\ 4)^T$, $e=2367$, $F(x)=x^4+2=(1\ 0\ 0\ 0\ 2)^T$, то $P(x)^e \pmod{F(x)}$ = modpolpowerZp(P,F,e,p) = $(4\ 3\ 4\ 2)^T = 4x^3+3x^2+4x+2$.

12.30. Тестирование полинома $F(x)$ из $\mathbb{Z}_p[x]$ на неприводимость

```
irreduciblepolZp(F,p) :=
  m ← last(F)
  m1 ← floor(m/2)
  u ← (1)
      (0)
  for i ∈ 1..m1
    u ← modpolpowerZp(u,F,p,p)
  DUV ← gcdDUVpolZp(F,difpoloverZp(u,(1)
                                    (0),p),p)
  d ← DUV_0
  c_0 ← 1
  r ← "reducible"
  r
  break if d ≠ c
  r ← "irreducible"
  r
```

Если $p=5$, $F1(x)=3x^4+4x^2+x+2=(3\ 0\ 4\ 1\ 2)^T$, $F2(x)=3x^4+x^3+2=(3\ 1\ 0\ 0\ 2)^T$, то irreduciblepolZp(F1,p) = "reducible", irreduciblepolZp(F2,p) = "irreducible".

12.31. Тестирование полинома $F(x)$ степени m из $\mathbb{Z}_p[x]$ на примитивность, факторизация $p^m-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{ek}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$

```
primitive_pol(p,F,r) :=
  irred ← irreduciblepolZp(F,p)
  prim ← "not primitive"
  prim
  break if irred = "reducible"
```

```
m ← last(F)
c_0 ← 1
lr ← last(r)
pm ← p^m
x ← (1 0)^T
for i ∈ 0..lr
    e ← (pm−1)/r_i
    Fpi ← modpolpowerZp(x,F,e,p)
    prim ← "not primitive"
    prim
    break if Fpi = c
    prim ← "primitive"
    prim
prim
```

Если p=19, неприводимый полином $F(x)=17x^3+3x^2+13x+1$ = $(17\ 3\ 13\ 1)^T$ из $\mathbb{Z}_p[x]$, m=3 есть степень полинома F, $n=p^m-1$ = 6858, факторизация $n=2^1\cdot 3^3\cdot 127^1$, $r=(2\ 3\ 127)^T$, $e=(1\ 3\ 1)^T$, то primitive_pol(p,F,r) = "primitive". Если при тех же условиях неприводимый полином $F(x)=3x^3+3x^2+18x+3$ = $(3\ 3\ 18\ 3)^T$, то primitive_pol(p,F,r) = "not primitive".

12.32. Порядок элемента a мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p (перебор)

```
order_elemZp(a,p) :=
    ord ← "no order" if a = 0 ∨ p = 0
    ord
    break if a = 0 ∨ p = 0
    b ← a
    k ← 1
    while b ≠ 1 ∧ k ≤ p−1
        b ← mod(b · a, p)
        k ← k+1
    ord ← "no order" if b > 1
    ord
    break if b > 1
    ord ← k
    ord
```

Если p=3911, то order_elemZp(2,p)=1955, order_elemZp(23,p) = 3910, order_elemZp(1973,p)=115.

12.33. Порядок элемента a мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p, факторизация $p-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{ek}$, *векторы* $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ *(алгоритм Гаусса)*

```
ordGaussZp(a,p,r,e) :=
| ord ← "no order" if a = 0 ∨ p = 0
| ord
| break if a = 0 ∨ p = 0
| t ← p-1
| k ← last(r)
| for i ∈ 0..k
|   | t ← t / (r_i)^e_i
|   | a1 ← modexpon(a,t,p)
|   | while a1 ≠ 1
|   |   | a1 ← modexpon(a1,r_i,p)
|   |   | t ← t · r_i
| t
```

Если простое p=10808621, факторизация $p-1=2^2\cdot 5^1\cdot 23^1\cdot 23497^1$, $r=(2\ 5\ 23\ 23497)^T$, $e=(2\ 1\ 1\ 1)^T$, то ordGaussZp(2,p,r,e) = 10808620, ordGaussZp(4,p,r,e)=5404310, ordGaussZp(6,p,r,e) = 2702155, ordGaussZp(23,p,r,e)=234970.

12.34. Порядок элемента $P(x)$ мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого из $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m (перебор)

```
ordpolGF(P,F,p) :=
| ord ← "no order" if P·P = 0 ∨ p = 0 ∨ F·F = 0
| ord
| break if P·P = 0 ∨ p = 0 ∨ F·F = 0
| b ← P
| n ← p^(last(F)-1)
| u_0 ← 1
| k ← 1
```

```
while b ≠ u ∧ k ≤ n
  b ← molmulinGF(b,P,F,p)
  k ← k+1
ord ← "no order" if b ≠ u
ord
break if b ≠ u
ord ← k
ord
```

Если p=19, неприводимый из $\mathbb{Z}_p[x]$ полином $F(x)=17x^3+3x^2+13x+1$ = $(17\ 3\ 13\ 1)^T$, m=3, $n=p^m-1$=6858, то порядок для $P(x)=x+4$ = $(1\ 4)^T$ есть ordpolGF(P,F,p)=6858; порядок для $P(x)=x+7$= $(1\ 7)^T$ есть ordpolGF(P,F,p)=381.

12.35. Порядок элемента $P(x)$ мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого из $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m, факторизация $p^m-1=r_0^{e_0}r_1^{e_1}\dots r_k^{ek}$, векторы $r=(r_0,r_1,\dots,r_k)$, $e=(e_0,e_1,\dots,e_k)$ (алгоритм Гаусса)

ordGaussGF(P,F,p,r,e) :=

```
ord ← "no order" if P·P=0 ∨ p=0 ∨ F·F=0
ord
break if P·P=0 ∨ p=0 ∨ F·F=0
u0 ← 1
t ← p^last(F)−1
k ← last(r)
for i ∈ 0..k
  t ← t / (r_i)^e_i
  P1 ← modpolpowerGF(P,F,t,p)
  while P1 ≠ u
    P1 ← modpolpowerGF(P1,F,r_i,p)
    t ← t·r_i
t
```

Если p=19, неприводимый из $\mathbb{Z}_p[x]$ полином $F(x)=17x^3+3x^2+13x+1$ = $(17\ 3\ 13\ 1)^T$, m=3, $n=p^m-1$=6858=$2^1\cdot3^3\cdot127^1$, r=$(2\ 3\ 127)^T$, e=$(1\ 3\ 1)^T$, то порядок для $P(x)=x+4$ = $(1\ 4)^T$ есть ordpolGF(P,F,p)=6858; порядок для $P(x)=x+7$=$(1\ 7)^T$

есть ordpolGF(P,F,p)=381.

12.36. Тест для $a\in\mathbb{Z}_p^*$ быть генератором мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p (перебор)

```
genZp(a,p) :=
  gen ← "not generator" if a=0 ∨ p=0
  gen
  break if a=0 ∨ p=0
  b ← a
  k ← 1
  while b≠1 ∧ k≤p-1
    b ← mod(b·a,p)
    k ← k+1
  gen ← "not generator" if b>1 ∨ b=1 ∧ k<p-1
  gen
  break if b>1
  gen ← "generator" if b=1 ∧ k=p-1
  gen
```

Если p=2357, то для $\mathbb{Z}_p^*$ a=2 есть genZp(a,p) = "generator"; a=4 есть genZp(a,p) = "not generator".

12.37. Тест для $a\in\mathbb{Z}_p^*$ быть генератором мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p, факторизация $p-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ (алгоритм Гаусса)

```
genGaussZp(a,p,r,e) :=
  gen ← "not generator" if a=0 ∨ p=0
  gen
  break if a=0 ∨ p=0
  n ← p-1
  k ← last(r)
  for i ∈ 0..k
    b ← modexpon(a, n/r_i, p)
    gen ← "not generator" if b=1
    gen
    break if b=1
  break if b=1
```

```
gen ← "generator"
gen
```

Если простое p=10808621, факторизация $p-1=2^2\cdot 5^1\cdot 23^1\cdot 23497^1$, $r=(2\ 5\ 23\ 23497)^T$, $e=(2\ 1\ 1\ 1)^T$, то genGaussZp(2,p,r,e) = "generator", genGaussZp(4,p,r,e)="not generator".

12.38. Тест для $P(x)\in GF(p^m)$ быть генератором мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого из $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m (перебор)

```
genpolGF(P,F,n,p) :=
  gen ← "not generator" if P·P=0 ∨ p=0 ∨ F·F=0
  gen
  break if P·P=0 ∨ p=0 ∨ F·F=0
  b ← P
  n ← p^last(F)-1
  u_0 ← 1
  k ← 1
  while b≠u ∧ k≤n
    b ← molmulinGF(b,P,F,p)
    k ← k+1
  gen ← "not generator" if b≠u ∨ b=u ∧ k<n
  gen
  break if b≠u ∨ b=u ∧ k<n
  gen ← "generator" if b=r ∧ k=n
  gen
```

Если p=19, неприводимый из $\mathbb{Z}_p[x]$ полином $F(x)=17x^3+3x^2+13x+1$ = $(17\ 3\ 13\ 1)^T$, m=3, $n=p^m-1$=6858, то для $P(x)=x+4$ = $(1\ 4)^T$ genpolGF(P,F,n,p)="generator"; для $P(x)=x+7$ = $(1\ 7)^T$ genpolGF(P,F,n,p)="not generator".

12.39. Тест для $P(x)\in\mathbb{Z}_p[x]$ быть генератором мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого из $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m, факторизация $p^m-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ (алгоритм Гаусса)

```
genGaussGF(P,F,p,r,e) :=
  gen ← "not generator" if P·P=0 ∨ p=0 ∨ F·F=0
  gen
  break if P·P=0 ∨ p=0 ∨ F·F=0
  u_0 ← 1
  n ← p^last(F)−1
  k ← last(r)
  for i ∈ 0..k
    b ← modpolpower(P,F,n/r_i,p)
    gen ← "not generator" if b=u
    break if b=u
  gen
  break if b=u
  gen ← "generator"
  gen
```

Если p=19, неприводимый из $\mathbb{Z}_p[x]$ полином $F(x)=17x^3+3x^2+13x+1$ = $(17\ 3\ 13\ 1)^T$, m=3, $n=p^m-1=6858=2^1\cdot 3^3\cdot 127^1$, $r=(2\ 3\ 127)^T$, $e=(1\ 3\ 1)^T$, то для $P(x)=x=(1\ 0)^T$ genGaussGF(P,F,p) = "generator"; для $P(x)=x+7=(1\ 7)^T$ genGaussGF(P,F,p) = "not generator".

12.40. Квадратный корень из натурального числа a по простому модулю p≥2, 1≤a<p

```
square_root_p(a,p) :=
  JS ← JACOBI(a,p)
  root ← "no root" if JS=−1
  root
  break if JS=−1
  b ← 1
  while ← JACOBi(b,p)=1 ∧ b≤p−1
    b ← b+1
  s ← factor_k_in_integer(p−1,p)_1
  t ← factor_k_in_integer(p−1,p)_2
  a1 ← rev(a,p)
  c ← modexpon(b,t,p)
  r ← modexpon(a,(t+1)/2,p)
  for i∈1..s−1  if s≥2
```

```
    |   |d ← modexpon(r^2 · a1, 2^(s−i−1), p)
    |   |r ← nmul(r,c,p) if nmod(d,p) = p−1
    |   |c ← mod(c · c,p)
    |root ← ( r )
    |        (−r)
    |root
```

Если a_1=84, a_2=63, p=89, то square_root_p(a_1,p) = $(66\ -66)^T$, square_root_p(a_2,p)="no root".

12.41. Квадратный корень из натурального числа a по простому модулю p, p≡3 (mod 4)

```
square_root_p34(a,p) :=
    |JS ← JACOBI(a,p)
    |root ← "no root" if JS=−1
    |root
    |break if JS=−1
    |root ← "mod(p,4) is not 3" if mod(p,4)≠3
    |root
    |break if mod(p,4)≠3
    |e ← (p+1)/4
    |r ← modexpon(a,e,p)
    |root ← ( r )
    |        (−r)
    |root
```

Если a_1=7, a_2=200, p=4003, то square_root_p34(a_1,p)= $(155\ -155)^T$, square_root_p34(a_2,p)="no root".

12.42. Квадратный корень из натурального числа a по простому модулю p, p≡5 (mod 8)

```
square_root_p58(a,p) :=
    |JS ← JACOBI(a,p)
    |root ← "no root" if JS=−1
    |root
    |break if JS=−1
    |root ← "mod(p,8) is not 5" if mod(p,8)≠5
    |root
    |break if mod(p,8) ≠ 5
```

```
e ← (p−1)/4
d ← modexpon(a,e,p)
e1 ← (p+3)/8
r ← modexpon(a,e1,p) if d=1
e2 ← (p−5)/8
a4e2 ← modexpon(4·a,e2,p)
a2a4e2 ← nmul(2·a,a4e2,p)
r ← a2a4e2 if d=p−1
root ← (r, −r)^T
root
```

Если a_1=13, a_2=101, p=4003, то square_root_p58(a_1,p)= $(1439\ -1439)^T$, square_root_p58(a_2,p)="no root".

12.43. Квадратный корень из натурального числа a по простому модулю p>2, 1≤a<p, при больших s в представлении p−1=2^s·t, 2 не делит t (s есть число двоек в факторизации p−1)

```
square_root_p_large_s(a,p) :=
JS ← JACOBI(a,p)
root ← "no root" if JS=−1
root
break if JS=−1
b ← 1
while JACOBI(b^2−4·a,p)=1 ∧ b ≤ p−1
  b ← b+1
f ← (1, −b)^T
x ← (1, 0)^T
r ← modpolpowerGF(x,f,(p+1)/2,p)
root ← (r, −r)^T
root
```

Если a_1=47, a_2=54, p=89, то square_root_p_large_s(a_1,p)= $(88\ -88)^T$, square_root_p_large_s(a_2,p)="no root".

12.44. Квадратный корень из натурального числа a по модулю n, если факторизация n=p·q при простых p и q и если a есть квадратичный вычет по модулям p и q

```
square_root_npq(a,n,p,q) :=
| JS ← JACOBI(a,n)
| JSp ← JACOBI(a,p)
| JSq ← JACOBI(a,q)
| root ← "no root" if JS=-1 ∨ JSp=-1 ∨ JSq=-1
| root
| break if JS=-1 ∨ JSp=-1 ∨ JSq=-1
| root_p ← square_root_p(a,p)
| r ← root_p_0
| root_q ← square_root_p(a,q)
| s ← root_q_0
| cd ← gcdxy(p,q)
| c ← cd_1
| d ← cd_2
| rd ← mod(r · d,n)
| sc ← mod(s · c,n)
| rdq ← mod(rd · q,n)
| scp ← mod(sc · p,n)
| x ← nmod(rdq+scp,n)
| y ← nmod(rdq-scp,n)
|
| root ← ⎛  x⎞
|        ⎜ -x⎟
|        ⎜  y⎟
|        ⎝ -y⎠
| root
```

Если a=7, p=131, q=167, n=$p\cdot q$=21877, то square_root_npq(a,n,p,q) = $(19277\ -19277\ 19801\ -19801)^T$.

12.45. Вычисление дискретного логарифма $\log_a b$ методом "малый шаг – большой шаг" в подгруппе G порядка n мультипликативной группы $\mathbb{Z}_p^*$ с простым p

```
is_here(t,m,x) :=
```

```
|i ← 0
|0
|while j ≤ m
|   |t_{0,j}
|   |break if t_{1,j} = x
|   |j ← j+1
|-1 if j > m
```

Если p=251, n=125, m=12, α=12, x=144=12^2, степени элемента 12 в порядке возрастания степеней рамещены в таблице

$t =$

0	1	7	6	5	8	2	4	9	3	11	10
1	12	52	88	91	122	144	154	209	222	227	249

,

то is_here(t,m−1,x) = 2.

```
baby_giant_step(p,α,n,β) :=

|m ← ceil(√n)
|for j ∈ 0..m−1
|   |t1_{1,j} ← modexpon(α,j,p)
|   |t1_{0,j} ← j
|t1 ← rsort(t1,1)
|αm1 ← modexpon(rev(α,p),m,p)
|γ ← mod(β,p)
|i ← 0
|j ← is_here(t1,m−1,j2)
|while j < 0
|   |t2_{0,i} ← i
|   |t2_{1,i} ← γ
|   |i ← i+1
|   |j ← is_here(t1,m−1,γ)
|   |γ ← nmul(γ,αm1,p)
|m·(i−1)+j if i > 0
|j otherwise
```

Пусть в программе baby_giant_step(p,α,n,β) G есть подгруппа порядка n мультипликативной группы $\mathbb{Z}_p^*$ с простым p, α есть генератор для G, $\beta \in G$. Дискретные логарифмы $\log_\alpha \beta$ в группе G:
$\log_2 228$ = baby_giant_step(383,2,382,228) = 110,
$\log_3 57$ = baby_giant_step(113,3,112,57) = 100,
$\log_5 97$ = baby_giant_step(97,5,96,35) = 32.

12.46. Алгоритм Полларда rho вычисления дискретного логарифма $\log_\alpha\beta$ в подгруппе G простого порядка n мультипликативной группы $\mathbb{Z}_p^*$ с простым p

```
nextX(x,α,β,n) :=

|t ← mod(x,3)
|mod(β · x,p) if t=1
|mod(x^2,p) if t=0
|mod(α · x,p) otherwise

nextA(x,α,n) :=

|t ← mod(x,3)
|α if t=1
|mod(2 · α,n) if t=0
|mod(α+1,n) otherwise

nextB(x,β,n) :=

|t ← mod(x,3)
|β+1 if t=1
|mod(2 · β,n) if t=0
|β otherwise

Pollard_rho_log(p,α,n,β) :=

|x_0 ← 1
|aa_0 ← 0
|bb_0 ← 0
|j ← 1
|while j > 0
|  |for i ∈ j..2 · j
|  |  |x_i ← nextX(x_{i-1},α,β,p)
|  |  |aa_i ← nextA(x_{i-1},aa_{i-1},n)
|  |  |bb_i ← nextB(x_{i-1},bb_{i-1},n)
|  |if x_j = x_{2 · j}
|  |  |r ← ndif(bb_j,bb_{2 · j},n)
|  |  |if r = 0
|  |  |  |return 1
|  |  |  |break
|  |  |  otherwise
|  |  |  |x1 ← rev(r,n)
```

```
|  |  |  |  |x1 ← nmul(x1,ndif(aa_{2·j},aa_j,n),n)
|  |  |  |  |return x1
|  |  |j ← j+1
```

Пусть в программе Pollard_rho_log(p,α,n,β), элемент α есть генератор подгруппы G простого порядка n в мультипликативной группе $\mathbb{Z}_p^*$ с простым p, элемент $\beta \in G$. Дискретные логарифмы $\log_\alpha\beta$ в группе G:
$\log_2 72$ = Pollard_rho_log(383,2,191,72) = 180,
$\log_2 128$ = Pollard_rho_log(383,2,191,128) = 7,
$\log_2 288$ = Pollard_rho_log(383,2,191,288) = 182,
$\log_3 84$ = Pollard_rho_log(383,3,191,84) = 152,
$\log_3 232$ = Pollard_rho_log(383,3,191,232) = 86,
$\log_3 243$ = Pollard_rho_log(383,3,191,243) = 5.

12.47. Алгоритм Полига–Неллмана вычисления дискретного логарифма $\log_\alpha\beta$ в мультипликативной подгруппе G порядка n группы $\mathbb{Z}_p^*$ с простым p

```
Pohlig_Hellman(p,α,n,β) :=
|h ← factoring2(n)
|r ← rows(h)
|for i ∈ 1..r
|  |q ← h_{i-1,0}
|  |e ← h_{i-1,1}
|  |aa ← 1
|  |l_0 ← 0
|  |
|  |a1 ← modexpon(α, n/q, p)
|  |for j ∈ 1..e
|  |  |break if j<1
|  |  |otherwise
|  |  |  |lqp ← nmul(l_{j-1}, q^{j-2}, p)
|  |  |  |aa ← nmul(aa, modexpon(α, lqp, p), p)
|  |  |  |
|  |  |  |b1 ← modexpon(β · rev(aa,p), n/q^j, p)
|  |  |  |
|  |  |  |ord_a1 ← order_elemZp(a1,p)
|  |  |  |l_j ← baby_giant_step(p,a1,ord_a1,b1)
|  |xx_i ← 0
|  |for j ∈ 1..e
```

```
|  |  |qjp ← modexpon(q, j−1, p)
|  |  |xx_i ← nsum(xx_i, nmul(l_j, qjp, p), p)
|for i ∈ 1..r
|  |m_i ← modexpon(h_{i−1,0}, h_{i−1,1}, p)
|  |
|  |M_i ← n / m_i
|  |
|  |MM_i ← rev(M_i, m_i)
|
|x ← Σ_{i=1}^{r} xx_i · M_i · MM_i
|x ← nmod(x, n)
|x
```

Пусть в программе Pohlig_Hellman(p,α,n,β): p есть простое число, элемент α есть генератор подгруппы G порядка n в мультипликативной группе $\mathbb{Z}_p^*$ с простым p, элемент $\beta \in G$. Дискретные логарифмы $\log_\alpha \beta$ в группе G:

$\log_2 228$ = Pohlig_Hellman(383,2,191,91) = 36,
$\log_{12} 119$ = Pohlig_Hellman(251,12,125,119) = 102,
$\log_{20} 113$ = Pohlig_Hellman(251,20,5,113) = 4,
$\log_{20} 228$ = Pohlig_Hellman(383,20,382,228) = 140,
$\log_{71} 2$ = Pohlig_Hellman(251,71,250,2) = 105.

12.48. Алгоритм Полларда rho вычисления собственного делителя в n (n не есть степень простого числа)

```
NonTrivFactor(n) :=

|a ← 2
|b ← 2
|d ← 1
|while ¬((d>1 ∧ d<n) ∨ d=n)
|  |a ← mod(a^2+1, n)
|  |b ← mod(b^2+1, n)
|  |b ← mod(b^2+1, n)
|  |d ← gcd(a−b, n)
|  |if d=n
|  |  |return "Question remains open"
|  |  |break
```

```
return (d, d/n)
```

Например, NonTrivFactor(455459) = $\begin{pmatrix}743\\613\end{pmatrix}$.

12.49. Алгоритм Полларда p−1 вычисления собственного делителя в n (n не есть степень простого числа)

```
to_be_prime(k) :=
  if k ≠ 2
    i ← 2
    while i ≤ ceil(k/2)
      return 0 if mod(k,i)=0
      i ← i+1
  return 1

nontrivial_factor(n,B) :=
  a ← floor(2+rnd()n−1)−2)
  d ← gcd(a,n)
  if d ≥ 2
    return d
    break
  for q ∈ 2..B
    if q=2 ∨ to_be_prime(q)
      L ← floor(ln(n)/lg(q))
      a ← modexpo(a,q^L,n)
  d ← gcd(a−1,n)
  if d=1 ∨ d=n
    return "Take a new B"
    break
  return (d, d/n)
```

Если n:=19048567, то
nontrivial_factor(n,9) = "Take a new B",

nontrivial_factor(n,10) = "Take a new B",

nontrivial_factor(n,11) = $\begin{pmatrix}5281\\3607\end{pmatrix}$.

12.50. Хэш-функция MASH–1 (*Modular Arithmetic Secure Hash*)

```
f_or(a,b) :=
|for i∈0..last(a)
|  a1_i ← a_last(a)−i
|a ← a_1
|for i∈0..last(b)
|  b1_i ← b_last(b)−i
|b ← b1
|if last(b) > last(a)
|  |a1 ← a
|  |a ← b
|  |b ← a1
|i ← last(a)−last(b)
|i1 ← last(b)
|for j∈i if i > 0
|  b_j+i1 ← 0
|for i∈0..last(a)
|  b1_i ← |1 if a_i=1 ∨ b_i=1
|         |0 otherwise
|for i∈0..last(b1)
|  b_i ← b1_last(b1)−i
|removepolzeros(b)
```

Программа f_or(a,b) по двум бинарным векторам a,b выдает их покомпонентную дизъюнкцию. Если $a:=(1\ 0\ 1\ 0)^T$, $b:=(1\ 0\ 1\ 0\ 1\ 1)^T$, то $f\_or(a,b)=(1\ 0\ 1\ 0\ 1\ 1)^T$. Счет идет справа налево.

```
f_xor(a,b) :=
|for i∈0..last(a)
|  a1_i ← a_last(a)−i
|a ← a_1
|for i∈0..last(b)
|  b1_i ← b_last(b)−i
|b ← b1
|if last(b) > last(a)
|  |a1 ← a
```

```
|  |a ← b
|  |b ← a1
|i ← last(a)−last(b)
|i1 ← last(b)
|for j ∈ i if i > 0
|  b_{j+i1} ← 0
|for i ∈ 0..last(a)
|  b1_i ← |1 if a_i=1 ⊕ b_i=1
|         |0 otherwise
|for i ∈ 0..last(b1)
|  b_i ← b1_{last(b1)−i}
|removepolzeros(b)
```

Программа f_xor(a,b) по двум бинарным векторам a,b выдает их покомпонентное сложение по модулю 2. Если a:=(1 0 0 1 1 1 0)^T, b:=(1 0 1 0 0 1)^T, то f_or(a,b)=(1 1 0 0 1 1 1)^T. Счет идет справа налево.

```
dec2bin(n) := h_based_rep(n,2)
```

Программа dec2bin(n) по десятиричному натуральному числу n выдает его бинарное представление в виде вектора. Например, dec2bin(4)=(1 0 0)^T.

```
bin2dec(a) :=
|n ← 0
|for i ∈ 0..last(a)
|  n ← n + a_i · 2^{last(a)−i}
|n
```

Программа bin2dec(a) по бинарному представлению числа в виде вектора выдает его 10-ричное представление. Например, если a:=(1 0 1 0 0 1)^T, то bin2dec(a)=41.

```
t_vect_const(n) :=
|v ← h_based_rep(n,2)
|t ← last(v)
|m ← mod(t+1,4)
|s ← 0 if m=0
|s ← 4−m if m ≠ 0
|v ← inverse_vect(v)
|for i ∈ 1..s if m ≠ 0
```

```
| v_{t+i} ← 0
|v ← inverse_vect(v)
|vc ← " "
|for i ∈ 0 .. t+s
|  | c_i ← num2str(v_i)
|  | vc ← concat(vc,c_i)
|vc
```

Программа t_vect_const(n) по натуральному числу n выдает его бинарное представление в виде текстовой константы, дополненной слева нулями до слова длины, кратной четырем. Например, t_vect_const(351)="000101011111".

```
transfer(a,n) :=
|for i ∈ last(a)-n+1 .. last(a)
|  aa_{i-last(a)+n-1} ← a_i
|aa
```

Программа transfer(a,n) по бинарному вектору n выдает вектор из n правых компонент в a. Например, transfer$((0\ 0\ 0\ 1\ 1)^T$, 4) = $(0\ 0\ 1\ 1)^T$.

```
VFM(h,i) :=
|for j ∈ 0 .. cols(h)-1
|  hh_j ← h_{i,j}
|hh
```

Программа VFM(h,i) по матрице h выдает ее строку i в виде вектора. Например, $\mathrm{VFM}\left(\begin{bmatrix}1&1&1&0\\0&1&1&0\\1&1&0&0\end{bmatrix},1\right) = \begin{bmatrix}0\\1\\1\\0\end{bmatrix}$.

```
V2M(h,i,Hq) :=
|for j ∈ 0 .. last(h)
|  Hq_{i,j} ← h_j
|Hq
```

Программа V2M(h,i,Hq) по матрице Hq, вектору h, номеру i строки в Hq выдает матрицу, в которой строка i заменена на

матрицу-строку h. Например, $V2M\left(\left\langle \begin{bmatrix}0\\1\\1\\1\end{bmatrix}, 1, \begin{bmatrix}1&1&1&0\\0&1&1&0\\1&1&0&0\end{bmatrix}\right\rangle\right) = \begin{bmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\end{bmatrix}$.

MASH1(x) :=

M ← 5011427

m ← last(dec2bin(M))+1

$n \leftarrow \text{trunc}\left(\frac{m}{16}\right) \cdot 16$

x16 ←
- t ← last(x)
- for i ∈ 0..t
- $x16_i \leftarrow h\_based\_rep(x_i, 16)$
- x16

text_binstr ←
- a ← last(x)
- const ← " "
- for i ∈ 0..la
  - $nv_i \leftarrow t\_vec\_const(x_i)$
- cons ← concat(cons, nv_i)
- cons

x1 ← str2vect(text_binstr)

x2 ← inverse_vect(x1)

b ← last(x2)+1

for i ∈ 0..b−1

$x2_i \leftarrow x2_i - 48$

b_bit ← dec2bin(b)

$t \leftarrow \text{ceil}\left(\frac{2 \cdot b}{n}\right)$

return 2 if t < 2

t

x3 ←
- x3 ← x2
- for $i \in last(x2)+1 \ldots t \cdot \frac{n}{2}$
- x3

x4 ←
- $n2 \leftarrow \frac{n}{2}$
- for i ∈ 0..t−1

```
        | for j∈n2-1
        |   xx4_{i,j} ← xx3_{n2,i+j}
        |for i∈0..last(b_bit)
        | xx4_{t,i} ← b_bit_i
        |xx4
y1 ←    |n8 ← n/8
        |for i∈t
        | for j∈1..n8
        |   for ij∈0..3
        |     |ij8 ← 8·(j-i)+ij
        |     |xx_{i,ij8} ← 1
        |if j=n8
        | |xx_{i,n-5} ← 0
        | |xx_{i,n-7} ← 0
        |for ij∈4..7
        | |ij8 ← 8·(j-i)+ij
        | |ij4 ← 4·(j-i)+ij-4
        | |xx_{i,ij8} ← x4_{i,ij4}
        |xx
A ←     |for i∈0..3
        | A_i ← 1
        |for i∈4..n-1
        | A_i ← 0
        |A
H ←     |for i∈0..n-1
        | H_{0,i} ← 0
        |H
MASH1 ← |for i∈1..t-1
        |   |Hl ← f_xor(VFM(H,i-1),VFM(y1,i-1))
        |   |Hl ← f_or(Hl,A)
        |   |Hld ← modexpon(bin2dec(Hl),2,M)
        |   |Hl ← dec2bin(Hld)
        |   |Hl ← f_xor(transfer(Hl,n),VFM(H,i-1))
        |   |H ← V2M(Hl,i,H)
        |VMH ← VFM(H,t+1)
        |MASH ← bin2dec(VMH)
|MASH1
h(x) := MASH1(x)
```

Программа x16 по вектору x 10–ричных кодов ASCII некоторых символов строит вектор 16–ричных кодов тех же символов. Например, для вектора $x:=(57\ 48\ 53\ 50\ 56)^T$ вектор $(39\ 30\ 35\ 32\ 38)^T$ будет результатом.

Программа text_binstr по вектору 10–ричных кодов ASCII с помощью программы x16 строит вектор 16–ричных кодов тех же символов, в котором затем каждая 16–ричная цифра заменяется на соответствующий бинарный байт. Результат есть текстовая константа, составленная из полученных байтов. Например, если $x:=(57\ 48\ 53\ 50\ 56)^T$, то следующим будет вектор (39 30 35 32 38), а затем текстовая константа "0011 1001 0011 0000 0011 0101 0011 0010 0011 1000" в качестве результата.

Другие программы, составляющие MASH1, осуществляют преобразования бинарного текста (в виде бинарного вектора) в соответствии с алгоритмом MASH–1 и доводят его до хэш-значения для исходного текста.

12.50.1. Хэш-значение для текстовой константы

Получим хэш-значение для MS DOS текста из файла x1.txt файловой системы. Пусть Send 1000$ to Belyanin, number 2343 есть текст из файла x1.txt. Текст можно задать сразу в среде MATHCAD в виде текстовой константы. Вычисление хэш-значения для текста из файла можно задать следующей программой.

```
x := READBIN("x1.txt","byte")
h(x) = 50718
```

Если текст задан текстовой константой в среде MATHCAD, то вычисление хэш-значения можно задать следующей программой.

```
textconst := "Send 1000$ to Belyanin, number 2343"
x := str2vec(textconst)
h(x) = 50718
```

12.50.2. Хэш-значение для элемента поля Галуа $GF(p^m)$

Если элемент поля Галуа $GF(p^m)$ задан полиномом степени m (в порядке убывания степеней) с коэффициентами из $\mathbb{Z}_p$, а полином представлен вектором $s = (s_0, s_1, \ldots, s_m)$, то вычисление хэш-значения для s можно задать следующей программой.

```
hgf(p,s) :=
```

```
                last(s)
sn ← ∑ s_{last(s)−i} · p^i
                i=0
str_s ← num2str(sn)
x ← str2vec(str_s)
hash ← MASH1(x)
hash
```

13. НЕКОТОРЫЕ MATHCAD-ПРОГРАММЫ ДЛЯ РАБОТЫ С БОЛЬШИМИ ЧИСЛАМИ

Приведенные в этой главе маткад-программы используют маткад-программы предыдущего параграфа.

Пусть $a = (a_n a_{n-1} \ldots a_1 a_0)_h$ есть h-ричное представление числа a. Пусть *h-ричное полином-число a* (или *h-ричное полином-представление числа a*) есть представление числа a в виде полинома $a_n h^n + a_{n-1} h^{n-1} + \ldots + a_1 h + a_0$. Будем представлять его в Mathcad в виде вектора $(a_n \; a_{n-1} \; \ldots \; a_1 \; a_0)^T$.

13.1. Умножение h-ричных полином-чисел

Пусть $a = (a_n a_{n-1} \ldots a_1 a_0)_h = a_0 + a_1 h + \ldots + a_{n-1} h^{n-1} + a_n h^n$,

$b = (b_m b_{m-1} \ldots b_1 b_0)_h = b_0 + b_1 h + \ldots + b_{m-1} h^{m-1} + b_m h^m$ есть h-ричные представления чисел a и b. Их произведение $c = ab =$

$(a_0 + a_1 h + \ldots + a_{n-1} h^{n-1} + a_n h^n) \cdot (b_0 + b_1 h + \ldots + b_{m-1} h^{m-1} + b_m h^m) =$

$c_0 + c_1 h + \ldots + c_{s-1} h^{s-1} + c_s h^s$, где $s = n+m$,

при некоторых 10-ричных числах c_i, $0 \leqslant i \leqslant s$.

На примере последнего многочлена покажем, что всякий многочлен от h с целыми неотрицательными коэффициентами можно представить равным ему многочленом от h с целыми коэффициентами между 0 и $h-1$ следующим образом.

Частное q_0 и остаток r_0 от деления c_0 на h есть:

$r_0 = \mathrm{mod}(c_0, h)$, $q_0 = (c_0 - r_0)/h$, $c_0 = q_0 h + r_0$, $q_0 \in \mathbb{N}$, $0 \leqslant r_0 < h$.

Тогда $c = \sum_{k=0}^{s} c_k t^k = c_0 + \sum_{k=1}^{s} c_k t^k = r_0 + q_0 h + \sum_{k=1}^{s} c_k t^k =$

$r_0 + q_0 h + c_1 h + \sum_{k=1}^{s} c_k t^k = r_0 + (c_1 + q_0) h + \sum_{k=1}^{s} c_k t^k$.

Частное q_1 и остаток r_1 от деления $c_1 + q_0$ на h есть:

$r_1=\mathrm{mod}(c_1+q_0,h)$, $q_1=(c_1+q_0-r_1)/h$, $c_1+q_0=q_1h+r_1$. Тогда

$$c=\sum_{k=0}^{s}c_kt^k=r_0+r_1h+q_1h^2+c_2h^2+\sum_{k=3}^{s}c_kt^k=$$

$$\sum_{k=0}^{1}c_kt^k+(c_2+q_1)h^2+\sum_{k=3}^{s}c_kt^k.$$

И так далее. На шаге $t-1$ аналогично получаем:

$$c=\sum_{k=0}^{s}c_kt^k=\sum_{k=0}^{s}r_kt^k+q_sh^{s+1}.$$

Далее продолжаем:

$q_sh^{s+1}=(q_{s+1}h+r_{s+1})h^{s+1}=r_{s+1}h^{s+1}+q_{s+1}h^{s+2}$,
$0\leqslant r_{s+1}<h$, $q_{s+1}<q_s$;

$q_{s+1}h^{s+2}=(q_{s+2}h+r_{s+2})h^{s+2}=r_{s+2}h^{s+2}+q_{s+2}h^{s+3}$,
$0\leqslant r_{s+2}<h$, $q_{s+2}<q_{s+1}$;

$q_{s+2}h^{s+3}=(q_{s+3}h+r_{s+3})h^{s+3}=r_{s+3}h^{s+3}+q_{s+3}h^{s+4}$,
$0\leqslant r_{s+2}<h$, $q_{s+2}<q_{s+1}$.

И так далее. Так как последовательность $q_s>q_{s+1}>q_{s+2}>\ldots$, уменьшается, то при некотором t получим $q_t=0$. Тогда

$q_{t-1}h^t=(q_th+r_t)h^t=r_th^t+q_th^{t+1}$,
$0\leqslant r_t<h$, $q_t<q_{t-1}$. В результате получим

$$c=\sum_{k=0}^{s}c_kt^k=\sum_{k=0}^{s}r_kt^k+\sum_{k=s+1}^{t}r_kt^k=\sum_{k=0}^{t}r_kt^k=$$
$$r_th^t+r_{t-1}h^{t-1}+\ldots r_1h+r_0=(r_tr_{t-1}\ldots r_1r_0)_h.$$

Алгоритм умножения h-ричных полином-чисел

ВХОД. Два неотрицательных h-ричных полином-числа
$a=(a_na_{n-1}\ldots a_1a_0)_h=a_nh^n+a_{n-1}h^{n-1}+\ldots+a_1h+a_0$,
$b=(b_mb_{m-1}\ldots b_1b_0)_h=b_mh^m+b_{m-1}h^{m-1}\ldots+b_1h+b_0$.

ВЫХОД. Произведение
$c=a\cdot b=r_th^t+r_{t-1}h^{t-1}+\ldots+r_1h+r_0=(r_t,r_{t-1},\ldots r_1,r_0)_h$.

1. $c:=(a_nh^n+a_{n-1}h^{n-1}+\ldots+a_1h+a_0)\cdot(b_mh^m+b_{m-1}h^{m-1}+\ldots+b_1h+b_0)=c_sh^s+c_{s-1}h^{s-1}+\ldots+c_1h+c_0$, где $s=n+m$ и все c_i есть некоторые 10-ричные числа.
2. $k:=0$, $r_k:=\mathrm{mod}(c_k,h)$, $q=(c_k-r_k)/h$.
3. Пока $k<s$ выполнять следующее.
   3.1. $k:=k+1$, $r_k:=\mathrm{mod}(c_k+q,h)$, $q:=(c_k+q-r_k)/h$.

4. $k:=s+1$.
5. Пока $q>0$ выполнять слудующее.
   5.1. $r_k:=\mathrm{mod}(q,h)$, $q:=(q-r_k)/h$, $k:=k+1$.
6. Вернуть r.

```
mul_pol_num_h(P,Q,h) :=
|C ← mul_pol(P,Q)
|s ← last(C)
|C ← inverse_vect(C)
|k ← 0
|r_k ← mod(C_k,h)
|
|q ← (C_k − r_k)/h
|while k < s
|   |k ← k+1
|   |r_k ← mod(C_k+q,h)
|   |
|   |q ← (C_k+q−r_k)/h
|k ← s+1
|while q > 0
|   |r_k ← mod(q,h)
|   |
|   |q ← (q−r_k)/h
|   |k ← k+1
|r ← inverse_vect(r)
|r
```

```
mul_pol_num10(P,Q) := mul_pol_num_h(P,Q,10)
```

Пусть $P1:=(9\ 6\ 9\ 8\ 1)^T$, $Q1:=(8\ 9\ 1\ 2)^T$, $P2:=(15\ 14\ 7\ 13\ 12)^T$, $Q2:=(13\ 15\ 5\ 11P^T$. Тогда mul_pol_num_h(P1,Q1,10) = mul_pol_num10(P,Q) = $(8\ 6\ 4\ 2\ 9\ 4\ 6\ 7\ 2)^T$, mul_pol_num_h(P2,Q2,16)=$(13\ 14\ 0\ 10\ 0\ 0\ 15\ 3\ 4)^T$.

13.2. Умножение полинома на число

```
mul_pol_int(P,c) :=
|mP ← last(P)
|for i ∈ 0..mP
|  mul_i ← P_i · c
```

```
|mul
```

Если P:=(5 7 0 9)^T, c:=9, то mul_pol_int(P,c)=(45 63 0 81)^T.

13.3. Умножение 10-ричного полином-числа на 10-ричное положительное число

```
mul_pol_int10(P,c) :=
|Q0 ← c
|Pc ← mul_pol_num10(P,Q)
|Pc
```

При P:=(5 7 0 9)^T,c:=15 mul_pol_int10(P,c)=(8 5 6 3 5)^T.

13.4. Вычитание 10-ричных полином-чисел P и Q, P ⩾ Q

```
subtract10(P,Q) :=
|mP ← last(P)
|mQ ← last(Q)
|P ← inverse_vect(P)
|Q ← inverse_vect(Q)
|for i ∈ 0..mQ
| |Ri ← Pi−Qi if Pi ⩾ Qi
| |continue if Pi ⩾ Qi
| |Pi ⩾ Qi otherwise
| |k ← 1
| |while Pi+k = 0
| | k ← k+1
| |Pi+k ← Pi+k − 1
| |for j ∈ 1..k−1 if k > 1
| | Pi+j ← 9
| |Ri ← Pi+10−Qi
|for i ∈ mQ+1 .. mP if mP > mQ
| Ri ← Pi
|R ← inverse_vect(R)
|R ← removepolzeros(R)
|R
```

Если P:=(9 8 7 5 6 2 0 0 0 1 0 8 0 9 9)^T, Q:=(9 9 9 3 8 1 9 3 9 8 7 6 1 7)^T, то subtract10(P,Q)=(8 8 7 6 2 3 8 0 6 1 2 0 4 8 2)^T.

```
sum_pol_sum10(P,Q) :=
|p ← 10
|sumPQ ← sum_pol(P,Q)
|sumPQ ← inverse_vect(sumPQ)
|mPQ ← last(sumPQ)
|t ← 0
|for i ∈ 0..mPQ
|  |sumPQ_i ← sumPQ_i + t
|  |PQ_i ← sumPQ_i
|  |r ← mod(PQ_i,p)
|  |PQ_i ← r
|  |t ← (sumPQ_i − r)/p
|k ← 1
|while t > 0
|  |r ← mod(t,p)
|  |PQ_(mPQ+k) ← r
|  |t ← (t − r)/p
|  |k ← k+1
|PQ ← inverse_vect(PQ)
|PQ
```

Если P:=(9 8 7 5 6 2 0 0 0 1 0 8 0 9 9)^T, Q:=(9 9 9 3 8 1 9 3 9 8 7 6 1 7)^T, то sum_pol_sum10(P,Q)=(1 0 8 7 5 0 0 1 9 4 0 9 5 7 1 6)^T.

13.6. Отношения "больше", "больше или равно", "меньше", "меньше или равно", для 10-ричных полином-чисел

```
larger10(P,Q) :=
|P ← removepolzeroes(P)
|Q ← removepolzeroes(Q)
|mP ← last(P)
|mQ ← last(Q)
|lar ← 0 if P=Q
|lar
|break if P=Q
```

```
|lar←1 if mP>mQ
|lar←0 if mP<mQ
|lar
|break if mP>mQ ∨ mP<mQ
|i←0
|while i≤mP
|  |lar←1 if P_i>Q_i
|  |lar←0 if P_i<Q_i
|  |lar
|  |break if P_i>Q_i ∨ P_i<Q_i
|  |i←i+1
|lar
```

```
larger_eq10(P,Q) := larger10(P,Q) ∨ P=Q
```

```
less10(P,Q) :=
|less←1 if larger_eq10(P,Q)=0
|less←0 if larger_eq10(P,Q)=1
|less
```

```
less_eq10(P,Q) :=
|less_eq←1 if larger10(P,Q)=0
|less_eq←0 if larger10(P,Q)=1
|less_eq
```

13.7. Частное и остаток при делении двух 10-ричных полином-чисел

```
qoutrest_pol_num10(P,Q) :=
|mP←last(P)
|mQ←last(Q)
|QOUT_0←0 if less10(P,Q)
|REST←P if less10(P,Q)
|QR_0←QOUT if less10(P,Q)
|QR_1←REST if less10(P,Q)
|QR
|break if less10(P,Q)
|for i ∈ 0..mQ
|  PseqQ_i←P_i
|PseqQ_mQ+1←P_mQ+1 if less10(PsegQ,Q)
|c←1
```

```
|Qc ← Q
|while less_eq10(Qc,PsegQ)
|  |c ← c+1
|  |Qc1 ← Qc
|  |Qc ← mul_pol_int10(Q,c)
|Qc ← Qc1
|QOUT_0 ← c-1
|REST ← subtract10(PsegQ,Qc)
|Pseg ← PsegQ
|while last(Pseg) < mP
|  |REST_{last(REST)+1} ← P_{last(Pseg)+1}
|  |REST ← removepolzeroes(REST)
|  |Pseg_{last(Pseg)+1} ← P_{last(Pseg)+1}
|  |while less10(REST,Q) ∧ last(Pseg) < mP
|  |  |QOUT_{last(QOUT)+1} ← 0
|  |  |REST_{last(REST)+1} ← P_{last(Pseg)+1}
|  |  |REST ← removepolzeroes(REST)
|  |  |Pseg_{last(Pseg)+1} ← P_{last(Pseg)+1}
|  |c ← 1
|  |Qc ← Q
|  |while less_eq10(Qc,REST)
|  |  |c ← c+1
|  |  |Qc1 ← Qc
|  |  |Qc ← mul_pol_int10(Q,c)
|  |Qc ← Qc1
|  |QOUT_{last(QOUT)+1} ← c-1
|  |REST ← subtract10(REST,Qc) if larger_eq10(REST,Qc)
|  |REST ← removepolzeroes(REST)
|QR_0 ← QOUT
|QR_1 ← REST
|QR
```

qout_pol_num10(P,Q) := qoutrest_pol_num10(P,Q)$_0$

rest_pol_num10(P,Q) := qoutrest_pol_num10(P,Q)$_1$

mod_large_num10(P,Q) := rest_pol_num10(P,Q)

Пусть P:=(1 3 2 1 0 0 0 0 7)^T, Q:=(8 0 7 5)^T. Тогда
qout_pol_num10(P,Q)=(1 6 3 5 9)^T,
rest_pol_num10(P,Q)=(1 0 8 2)^T,
mod_large_num10(P,Q)=(1 0 8 2)^T.

13.8. Модулярное умножение двух 10-ричных полином-чисел

```
mod_mult_large_num10(P,Q,M) :=
|PQ ← mul_pol_num10(P,Q)
|PQmodM ← rest_pol_num10(PQ,M)
|PQmodM
```

Если P:=(1 0 0 0 4 3 5 6 0 0 0 6 1), Q:=(1 1 9 7 6), M:= (5 0 5 0 5), то mod_mult_large_num10(M,Q,M)=(4 6 2 5 2)^T.

13.9. Модулярная степень $P^e \pmod M$ 10-ричных полином-чисел P и M при малых экспонентах e

```
mod_exp_largeP_small_e10(P,e,M) :=
|C ← 1 if e=0
|C ← P if e=1
|C
|break if e=0 ∨ e=1
|e2 ← h_based_rep(e,2)
|t ← last(e2)
|e1 ← inverse_vect(e2)
|C0 ← 1
|A ← P
|C ← P if e1_0 = 1
|for i ∈ 1..t
| |A ← mod_mult_large_num10(A,A,M)
| |C ← mod_mult_large_num10(A,C,M) if e1_i = 1
|C
```

Если P:=(2 3 5)^T, e:=129979979, M:=(2 3 7 5)^T, то mod_exp_largeP_small_e10(P,e,M)=(1 2 5)^T.

13.10. Бинарное полином-представление 10-ричных полином-чисел

```
bin_rep_large10_num(N) :=
|H ← (2)
|Q ← N
|S0 ← 0
|i ← 0
|while Q ≠ S
| |R ← mod_large_num10(N,H)
| |NminR ← subtract10(N,R)
```

```
    |   |NminR ← removepolzeroes(NminR)
    |   |Q ← qout_pol_num10(NminR,H)
    |   |a_i ← R_0
    |   |N ← Q
    |   |i ← i+1
    |a ← inverse_vect(a)
    |a
```

Если $N:=(2\ 3\ 5)^T$, то bin_rep_large_num(N)=(1 1 1 0 1 0 1 1)^T.

13.11. h-ричное полином-представление 10-ричных полином-чисел

```
h_rep_large10_num(N,H) :=
|Q ← N
|S_0 ← 0
|i ← 0
|while Q ≠ S
|   |R ← mod_large_num10(N,H)
|   |NminR ← subtract10(N,R)
|   |NminR ← removepolzeroes(NminR)
|   |Q ← qout_pol_num10(NminR,H)
|   |a_i ← R
|   |N ← Q
|   |i ← i+1
|for i ∈ 0..last(a)
|   |a_i ← inverse_vect(a_i)
|   |a_i ← Σ_{k=0}^{last(a_i)} (a_i)_k · 10^k
|a ← inverse_vect(a)
|a
```

Если $N:=(1\ 2\ 0\ 9\ 7\ 8\ 9\ 3\ 9)^T$, H:=16, то h_rep_large10_num(N,H)=(7 3 5 15 13 15 11).

13.12. Модулярная степень $P^E \pmod M$ 10-ричных полином-чисел P,E,M

```
mod_exp_large_num10(P,E,M) :=
|C ← 1 if E=(0)
```

```
|C←P if E=(1)
|C
|break if E=(0) ∨ E=(1)
|E2←bin_rep_large10_num(E)
|t←last(E2)
|E1←inverse_vect(E2)
|C_0←1
|A←P
|C←P if E1_0=1
|for i ∈ 1..t
|  |A←mod_mult_large_num10(A,A,M)
|  |C←mod_mult_large_num10(A,C,M) if E1_i=1
|C
```

Если $P:=(9\ 2\ 3\ 0\ 0\ 0\ 7\ 3\ 0\ 7\ 1\ 8\ 4\ 8\ 4\ 5\ 0\ 0\ 2\ 1)^T$,
$E:=(8\ 4\ 3\ 5\ 6\ 7\ 2\ 3\ 0\ 9\ 0\ 0\ 0\ 9\ 7\ 0\ 0\ 3\ 0\ 4\ 4)^T$,
$M:=(1\ 1\ 0\ 7\ 0\ 1\ 0\ 0\ 4\ 9\ 0\ 9\ 0\ 8\ 0\ 2\ 3\ 9\ 5)^T$, то
mod_exp_large_num10(P,E,M) =
$(6\ 8\ 1\ 7\ 1\ 2\ 8\ 7\ 5\ 4\ 3\ 1\ 6\ 6\ 6\ 8\ 1\ 1)^T$.

ЛИТЕРАТУРА

Болотов А.А., Гашков С.Б., Фролов А.Б. Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: КомКнига, 2006. 328с.

Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. 280с.

Бухштаб А.А. Теория чисел. М.: Просвещение, 1966. 384 р.

Виноградов И.М. Основы теории чисел. М.: Высшая школа, 1965. 172 с.

Диффи У., Хеллман М. Защищенность и имитостойкость. Введение в криптографию. //ТИИЭР. 1979. Т.67. N3. С.71–109.

Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820с.

Набебин А.А. Логика и Пролог в дискретной математике. М.: Моск.энерг.институт, 1996. 452 с.

Нечаев В.И. Элементы криптографии. М.: Высшая школа. 1999. 109 с.

Смарт Н. Криптография. М.: Техносфера, 2006. 525 с.

Фролов А.Б., Андреев А.Е., Болотов А.А., Коляда К.В. Прикладные задачи дискретной математики и сложность алгоритмов. М.: Издат–во МЭИ, 1997. 312 с.

Шнайер Б., Фергюсон Н. Практическая криптография. М.: Вильямс, 2005. 424 с.

Albert A.A. Fundamental concept of higher algebra. 1956.

Fillmore J.P., Marks M.L. Linear recursive sequences. SIAM Rev., 10, 1968. P.342–353.

Garey M.R., Johnson D.S. Computers and intractability. A guide to the theory of NP–completeness. W.H.Freeman, San Francisco, 1979. 338 p.

Kahn D. The codebreakers. N.Y., 1967.

Koblitz N. A course in number theory and cryptography. Springer–Verlag, 1994. 238p.

Koblitz N. Algebraic aspects of cryptography. Springer–Verlag, 1997. 206p.

McEliece R.J. Finite fields для computer scientists and engineers. 1987. 207p.

Menezes A., van Oorschot P., Vanstone S. Handbook of applied cryptography. CRC Press. 1996. 780 p.

Интернет-адрес: www.cacr.math.uwaterloo.ca/hac

О Г Л А В Л Е Н И Е