Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Московский государственный институт электронной техники
(технический университет)

А.В. Клюшин, И.Б. Кожухов, Т.А. Олейник

Сборник задач по дискретной математике

Утверждено редакционно-издательским советом института
в качестве методических указаний

Москва 2008

УДК 512.8

Рецензент канд. физ.-мат. наук, доц. *А.М. Ревякин*

Клюшин А.В., Кожухов И.Б., Олейник Т.А.

Сборник задач по дискретной математике. - М.: МИЭТ, 2008. - 120 с.

В сборник включены упражнения по таким разделам дискретной математики, как «Алгебраические структуры», «Теория булевых функций», «Теория графов» и «Автоматы».

Сборник содержит задачи разного уровня сложности, предназначенные как для первоначального знакомства с основными понятиями, утверждениями и алгоритмами дискретной математики, так и для более глубокого изучения предмета. К части задач приведены указания и решения.

Сборник может быть использован в учебном процессе при проведении семинарских занятий, подготовке к экзамену, а также будет полезен студентам, самостоятельно изучающим предмет.

Выполнено в рамках инновационной образовательной программы МИЭТ "Современное профессиональное образование для российской инновационной системы в области электроники".

1. Алгебраические структуры

1.1. Множества и действия над ними

Мы будем использовать общепринятые обозначения для следующих числовых множеств: $\mathbb{N}$ – множество всех натуральных чисел; $\mathbb{Z}$ – множество всех целых чисел; $\mathbb{Q}$ – множество всех рациональных чисел; $\mathbb{R}$ – множество всех действительных чисел; $\mathbb{C}$ – множество всех комплексных чисел.

Если каждый элемент множества A принадлежит множеству B, то будем говорить, что множество A вложено в множество B и обозначать: $A \subset B$.

Если $A \subset B$, но $A \neq B$, будем говорить, что A – строгое подмножество множества B.

Пусть имеются два множества A и B. Их объединением будем называть множество, элементами которого являются все элементы множества A и множества B. Объединение множеств A и B обозначается символом $A \cup B$.

Пересечением множеств A и B будем называть множество, элементами которого являются все элементы, принадлежащие A и B одновременно. Пересечение множеств обозначается символом $A \cap B$.

Разностью множеств A и B будем называть множество, состоящее из всех тех элементов множества A, которые не принадлежат B. Разность множеств обозначается символом $A \setminus B$.

Множество, в котором нет элементов будем называть пустым и обозначать символом $\varnothing$. Считается, что пустое множество является подмножеством любого множества.

В случае, если множество A конечно, число его элементов будем обозначать символом $|A|$. В случае, когда множество A бесконечно, будем писать $|A| = \infty$.

Пусть все рассматриваемые множества содержатся в некотором одном множестве X, которое мы будем называть универсальным, и $A \subset X$ – одно из них. Тогда множество $X \setminus A$ будем называть дополнением множества A и обозначать символом $\overline{A}$. Например, если мы рассматриваем множества на плоскости, то роль X будет играть вся плоскость, а множество $\overline{A}$ будет состоять из всех точек плоскости, не принадлежащих A.

Пусть имеются два множества A и B. Их декартовым произведением будем называть множество $A \times B$, элементами которого являются пары (a,b), где $a \in A, b \in B$. Если имеется n множеств $A_1, A_2, \ldots, A_n$, то аналогично можно образовать их декартово произведение $A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \,|\, a_i \in A_i; i = 1, \ldots, n\}$.

Если все множества A_i совпадают, то декартово произведение $\underbrace{A \times A \times \ldots \times A}_{n}$ называют декартовой степенью множества A и обозначают A^n.

Если множества A и B конечны, то $|A \times B| = |A| \cdot |B|$. Аналогично, если множества $A_1, \ldots, A_n$ конечны, то $|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n|$. В частности, $|\underbrace{A \times A \times \ldots \times A}_{n}| = |A|^n$.

Например, если множество $A = \{x, y\}$, а множество $B = \{1, 2, 3\}$, то множество $A \times B$ состоит из шести элементов: $(x;1)$, $(x;2)$, $(x;3)$, $(y;1)$, $(y;2)$, $(y;3)$.

Число элементов множества $A \cup B$ можно выразить через $|A|$, $|B|$, $|A \cap B|$ следующим образом: $|A \cup B| = |A| + |B| - |A \cap B|$.

Эту формулу иногда называют теоремой о сумме. Для трех множеств эта формула примет вид: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Аналогичная формула существует и для n множеств. Часто ее называют формулой включения и исключения.

Упражнения

(1.1 – 1.4) Для следующих множеств A и B и универсального множества X найдите множества $A \cup B, A \cap B, A \setminus B, B \setminus A, \bar{A}, \bar{B}$.

1.1. $A = \{2,4,6,8\}$, $B = \{3,4,5,6,7\}$, $X = \{1,2,3,4,5,6,7,8,9\}$.

1.2. $A = \{1,3,5,7,9\}$, $B = \{2,3,4,6\}$, $X = \{1,2,3,4,5,6,7,8,9\}$.

1.3. $A = (-\infty;1] \cup [3;4] \cup [5;+\infty), B = (-1,2) \cup [4;5] \cup (6;+\infty), X = \mathbf{R}$.

1.4. $A = (-\infty;2] \cup \{4\} \cup (6;9]$, $B = [1,4) \cup \{7\} \cup (8;+\infty)$, $X = \mathbf{R}$.

1.5. Имеется два свитера, четверо брюк и три пары туфель. Каким числом способов можно одеться?

1.6. Сколько существует упорядоченных последовательностей из 0 и 1 длины 5?

1.7. Пусть $A = \{a,b,c,d,e\}$. Сколько подмножеств (включая пустое и само A) содержится в множестве A?

1.8. Пусть $A = \{a,b,c,d,e\}$. Сколько подмножеств из 3–х элементов содержится в множестве A?

1.9. В научно–исследовательском институте работают 67 человек. Из них 47 знают английский язык, 35 – немецкий язык и 23 – оба языка. Сколько человек в институте не знают ни английского, ни немецкого языка?

1.10. В научно-исследовательском институте работают 67 человек. Из них 47 знают английский язык, 35 – немецкий язык и 20 – французский язык. Далее, 23 человека знают английский и немецкий языки, 12 человек – английский и французский и 11 человек знают немецкий и французский языки. Наконец, 5 человек знают все три языка. Сколько человек в институте не знают ни одного из этих языков?

1.2. Отображения множеств. Взаимно однозначное отображение

Пусть имеются два множества A и B. Если каждому элементу $a \in A$ поставлен в соответствие какой–то элемент $b \in B$, то говорят, что задано отображение f из множества A в множество B. Этот факт обозначается следующим образом: $f: A \to B$.

Если элементу $a \in A$ поставлен в соответствие элемент $b \in B$, то b называют образом элемента a и обозначают символом $f(a)$. Элемент a при этом называют прообразом элемента b. Каждый элемент $a \in A$ при отображении f имеет ровно один образ. В то же время для элемента $b \in B$ число прообразов может быть любым (в том числе и равным 0).

Пусть множество A конечно и состоит из элементов $\{a_1, a_2, \ldots, a_n\}$. Тогда отображение $f: A \to B$ можно задать с помощью следующей таблицы $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$. В этой таблице внизу под каждым элементом a_i указывается его образ – элемент $b_i \in B$.

Отображение $f: A \to B$ называется инъективным, если $\forall a_1, a_2 \in A\, (a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2))$. Отображение $f: A \to B$ называется сюръективным, если $\forall b \in B \exists a \in A: f(a) = b.$ Отображение $f: A \to B$ называется взаимно однозначным, если оно инъективно и сюръективно.

Отображение $f: A \to A$ такое, что $\forall x \in A \quad f(x) = x$ называется тождественным (или единичным) и обозначается 1_A или е.

Пусть $f: A \to B$, а $g: B \to C$. Тогда можно образовать "сквозное" отображение $gf: A \to C$, определенное формулой $\forall a \in A \quad gf(a) = g(f(a))$. Это отображение называется суперпозицией отображений f и g. Отметим, что суперпозиция действует справа налево, т.е. в записи $gf(a)$ на элемент a сначала действует отображение f (правое), а потом g. Если $f = g$, то вместо ff будем писать f^2. Аналогично, $\underbrace{ff \ldots f}_{n}$ записываем как f^n.

Пусть $f: A \to B$. Отображение $g: B \to A$ называется обратным к f, если $gf = 1_A$ и $fg = 1_B$. Обратное отображение обозначается f^{-1}.

Пусть $A = \{1,\ldots,n\}$. Отображение $f: A \to A$, для которого $f(k) = i_k, k = 1,\ldots,n$, будем обозначать следующей таблицей

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Взаимно однозначное отображение $f: A \to A$ будем называть подстановкой. Множество всех подстановок на множестве A будем обозначать S_nТождественную подстановку будем обозначать буквой e. Порядком подстановки f будем называть наименьшее натуральное число n такое, что $f^n = e$. Порядок подстановки обозначается $o(f)$.

Упражнения

(1.11 – 1.15) Пусть $A = \{a,b,c\}$, $B = \{x,y,z\}$.

1.11. Приведите пример отображения $f: A \to B$.

1.12. Сколько существует отображений $f: A \to B$?

1.13. Приведите пример взаимно однозначного отображения $f: A \to B$.

1.14. Приведите пример отображения $f: A \to B$, не являющегося взаимно однозначным.

1.15. Сколько существует взаимно однозначных отображений $f: A \to B$?

1.16. Пусть $A = \{a,b,c,d\}$, $B = \{\alpha,\beta,\gamma\}$. Приведите пример сюръективного отображения $f: A \to B$.

(1.17 – 1.18) Для подстановок f и g найдите fg, gf, f^{-1}, g^{-1}. Найдите порядки подстановок f и g.

1.17. $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

1.18. $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

1.19. Докажите, что отображение $f: A \to B$ является взаимно однозначным тогда и только тогда, когда оно имеет обратное отображение $f^{-1}: B \to A$.

1.20. Пусть A и B – конечные множества. Докажите, что взаимно однозначное отображение $f: A \to B$ существует тогда и только тогда, когда $|A| = |B|$.

1.3. Бинарные отношения. Их свойства

Бинарным отношением на множестве A называется любое подмножество $\rho \subset A \times A$. Условимся писать $a\rho b$, если $(a,b) \in \rho$.

Бинарное отношение ρ на множестве A называется рефлексивным, если каждый элемент множества A состоит сам с собой в бинарном отношении ρ.

Бинарное отношение ρ на множестве A называется симметричным, если $(a,b) \in \rho$ тогда и только тогда, когда $(b,a) \in \rho$.

Бинарное отношение ρ на множестве A называется антисимметричным, если $(a,b) \in \rho$ и $(b,a) \in \rho$ может быть только в том случае, когда $a = b$.

Бинарное отношение ρ на множестве A называется транзитивным, если всегда, когда $(a,b) \in \rho$ и $(b,c) \in \rho$, пара (a,c) также принадлежит ρ.

Бинарное отношение ρ, обладающее свойствами рефлексивности, симметричности и транзитивности, называется отношением эквивалентности. Для элемента $a \in A$ множество $S(a) = \{x \in A \,|\, x\rho a\}$ называется смежным классом отношения ρ, содержащим a.

Бинарное отношение ρ, обладающее свойствами рефлексивности, антисимметричности и транзитивности, называется отношением порядка. Множество с заданным на нем отношением порядка называется частично упорядоченным. Два элемента, состоящие в отношении ρ, называются сравнимыми.

Частично упорядоченное множество A, в котором любые два элемента сравнимы, называется линейно упорядоченным.

Пусть имеется множество A на котором задано отношение эквивалентности ρ. Тогда можно образовать новое множество, элементами которого будут являться классы эквивалентности отношения ρ. Это множество будет называться фактор-множеством множества A по отношению ρ и обозначаться A/ρ.

Бинарное отношение на множестве $A = \{a, b, c\}$ из трех элементов будем задавать с помощью матрицы 3×3 из нулей и единиц, первая строчка и столбец которой соответствуют элементу a, вторая – элементу b, третья – c. Если на пересечении, например, 1-ой строки и второго столбца в этой матрице стоит 1, то это означает, что пара $(a,b) \in \rho$, если же 0, то данная пара ρ не принадлежит. Например, запись $\rho = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ означает, что $\rho = \{(a,b), (a,c), (b,a), (b,c), (c,b)\}$.

Упражнения

1.21. Сколько существует бинарных отношений на множестве из 3-х элементов?

1.22. Сколько существует рефлексивных бинарных отношений на множестве из 3-х элементов?

1.23. Сколько существует симметричных бинарных отношений на множестве из 3-х элементов?

1.24. Сколько существует антисимметричных бинарных отношений на множестве из 3-х элементов?

1.25. Приведите пример рефлексивного, симметричного, но не транзитивного бинарного отношения на множестве из 3-х элементов.

1.26. Приведите пример рефлексивного, транзитивного, но не симметричного бинарного отношения на множестве из 3-х элементов.

1.27. Приведите пример симметричного, транзитивного, но не рефлексивного бинарного отношения на множестве из 3-х элементов.

(1.28 – 1.30) Выясните, является ли следующее бинарное отношение ρ на множестве $\mathbb{N}$ натуральных чисел 1) рефлексивным; 2) симметричным; 3) антисимметричным; 4) транзитивным. Будет ли ρ отношением эквивалентности или порядка?

1.28. $m\rho n \Leftrightarrow m+n$ – четно.

1.29. $m\rho n \Leftrightarrow m+n$ – нечетно.

1.30. $m\rho n \Leftrightarrow m\cdot n$ – четно.

1.4. Понятие группы. Примеры групп

Пусть G – некоторое множество. Бинарной операцией на G называется произвольное отображение $G\times G \to G$. Если $(g_1, g_2) \in G_1 \times G_2$, то результат бинарной операции можно обозначать $g_1 \cdot g_2$, $g_1 * g_2$, $g_1 + g_2$, где $(\cdot), (*), (+)$ – различные обозначения для знака бинарной операции.

Множество G с бинарной операцией $(\cdot)$ называется группой, если

1) $\forall g_1, g_2, g_3 \in G \quad (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$;

2) $\exists e \in G: \quad e \cdot g = g \cdot e = g$. Этот элемент e будем называть единицей группы G;

3) $\forall g \in G \quad \exists g^{-1} \in G: \quad g \cdot g^{-1} = g^{-1} \cdot g = e$. Элемент g^{-1} для элемента g будем называть обратным к g.

Если к условиям 1) – 3) добавить условие

4) $\forall g_1, g_2 \in G \quad g_1 \cdot g_2 = g_2 \cdot g_1$,

то группа G называется абелевой или коммутативной. В этом случае знак бинарной операции чаще обозначают $(+)$.

Упражнения

(1.31 – 1.32) Пусть $G=\mathbb{R}$, а $(\cdot)$, $(+)$ – обычные операции умножения и сложения на множестве действительных чисел $\mathbb{R}$. В каких из следующих случаев бинарная операция (*), определенная на множестве $\mathbb{R}$, будет ассоциативной?

1.31. $x * y = 2x + y.$

1.32. $x * y = x + y + 2.$

1.33. $x * y = 2x \cdot y.$

1.34. $x * y = \sqrt{x^2 + y^2}.$

1.35. Пусть $G = \{0,1\}$. Тогда существует 16 отображений $G \times G \to G$. Какие из них будут представлять ассоциативную бинарную операцию?

(1.36 – 1.40) Какие из указанных множеств с заданной на них бинарной операцией являются группами?

1.36. $(A,+)$, где A – одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, а операция $(+)$ – обычное сложение.

1.37. $(A,\cdot)$, где A – одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, а операция $(\cdot)$ – обычное умножение.

1.38. $(A_0,\cdot)$, где A – одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $A_0 = A \setminus \{0\}$, а операция $(\cdot)$ – обычное умножение.

1.39. $(n\mathbb{Z},+)$, где n – некоторое фиксированное натуральное число, а операция $(+)$ – обычное сложение.

1.40. $(\{-1,1\},\cdot)$, а операция $(\cdot)$ – обычное умножение.

1.5. Гомоморфизмы и изоморфизмы групп

Пусть G_1 и G_2 – группы. Отображение $f: G_1 \to G_2$ называется гомоморфизмом, если для любых $g, h \in G_1$ $f(g \cdot h) = f(g) \cdot f(h).$

Изоморфизмом групп $f: G_1 \to G_2$ называется гомоморфизм, который является взаимно однозначным отображением. Если группы G_1 и G_2 изоморфны, то принято обозначать $G_1 \cong G_2$.

Пусть G – группа с единицей e, $g \in G$. Наименьшее натуральное n, для которого $g^n = e$ называется порядком элемента g и обозначается $o(g)$. Если такого n не существует, то считается, что $o(g) = \infty$.

Гомоморфизм $f: \mathbb{Z}_n \to \mathbb{Z}_m$, для которого $f(\bar{1}) = \bar{k}$, где $0 \le k < m$, будем обозначать f_k.

Упражнения

1.41. Пусть T – группа окружности. T состоит из всех комплексных чисел с модулем равным 1 и с операцией умножения. Рассмотрим отображение $f: \mathbb{R} \to T$, определенное формулой $f(x) = e^{2\pi x i}$. Определите, является ли f:

а) гомоморфизмом;

б) изоморфизмом.

1.42. Пусть на множестве всех действительных чисел из интервала $[0,1)$ задана операция $\oplus$, где $a \oplus b$ – дробная часть числа $a+b$. Докажите, что множество $[0,1)$ с операцией $(\oplus)$ является группой, изоморфной группе окружности T.

(**1.43 – 1.45**) Докажите, что следующие группы изоморфны группе движений треугольника D_3.

1.43. Группа S_3 подстановок на множестве $A = \{1,2,3\}$ (см. стр. 6).

1.44. Множество матриц

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

с операцией умножения матриц, причем сложение осуществляется по модулю 2 ($1+1=0$).

1.45. Функции $y_1 = x$, $y_2 = \frac{1}{x}$, $y_3 = \frac{1}{1-x}$, $y_4 = \frac{x-1}{x}$, $y_5 = 1-x$, $y_6 = \frac{x}{x-1}$ с операцией суперпозиции функций.

(**1.46 – 1.50**) Найдите группу автоморфизмов $Aut\,G$ для следующих групп.

1.46. $\mathbb{Z}_2$. **1.47.** $\mathbb{Z}_3$. **1.48.** $\mathbb{Z}_4$. **1.49.** $\mathbb{Z}_5$. **1.50.** S_3.

1.6. Подгруппы. Смежные классы. Теорема Лагранжа

Подмножество H группы G называется подгруппой, если выполнены следующие условия

1) $e \in H$;

2) $\forall h_1, h_2 \in H \quad h_1 \cdot h_2 \in H$;

3) $\forall h \in H \quad h^{-1} \in H$.

Во всякой группе имеется подгруппа, состоящая из одной единицы, а также совпадающая со всей группой. Эти подгруппы называются тривиальными. Остальные подгруппы группы G называются нетривиальными.

Если H – подгруппа группы G и $g \in G$, то множество $gH = \{gh \mid h \in H\}$ называется левым смежным классом группы G по подгруппе H. Соответственно, множество Hg называется правым смежным классом.

Число элементов конечной группы или, соответственно, подгруппы будем называть ее порядком.

Пусть $a_1, \ldots, a_n \in G$. Через $< a_1, \ldots, a_n >$ будем обозначать наименьшую подгруппу в G, содержащую элементы $a_1, \ldots, a_n$. Если $< a_1, \ldots, a_n > = G$, то элементы $\{a_1, \ldots, a_n\}$ будем называть системой образующих группы G. Систему $\{a_1, \ldots, a_n\}$ будем называть минимальной системой образующих группы G, если после удаления любого элемента оставшееся множество уже не будет являться системой образующих для G. Группу G будем называть циклической, если найдется элемент $g \in G$ такой, что $< g > = G$. Такой элемент g называется образующим данной циклической группы.

Упражнения

1.51. Найдите все нетривиальные подгруппы группы $\mathbb{Z}_{12}$. Найдите порядки всех элементов этой группы.

1.52. Найдите все нетривиальные подгруппы группы D_4 движений квадрата. Найдите порядки всех элементов этой группы.

1.53. Найдите все нетривиальные подгруппы группы движений прямоугольника, не являющегося квадратом. Найдите порядки всех элементов этой группы.

1.54. Найдите все нетривиальные подгруппы группы движений ромба, не являющегося квадратом. Найдите порядки всех элементов этой группы.

1.55. Найдите все подгруппы группы движений правильного пятиугольника. Найдите порядки всех элементов этой группы.

1.56. Найдите все подгруппы группы кватернионов Q_8. Найдите порядки всех элементов этой группы.

1.57. Найдите все образующие группы $\mathbb{Z}_{10}$.

1.58. Найдите все образующие группы $\mathbb{Z}_{12}$.

1.59.. Найдите все минимальные системы образующих группы движений треугольника D_3.

1.60. Найдите все минимальные системы образующих группы движений квадрата D_4.

1.7. Нормальные подгруппы. Фактор–группы

Подгруппа H группы G называется нормальной, если левые и правые смежные классы по этой подгруппе совпадают, то есть, если $\forall g \in G \quad gH = Hg$.

Тот факт, что H – нормальная подгруппа в G обозначается так: $H \lhd G$. Условие нормальности равносильно тому, что $\forall g \in G,\ gHg^{-1} \subset H$.

Пусть H – нормальная подгруппа в G. Смежный класс $gH = Hg$ будем обозначать $\overline{g}$. Рассмотрим множество $\overline{G}$ всех смежных классов с бинарной операцией $\overline{g} \cdot \overline{h} = \overline{gh}$.

Это множество образует группу, которую мы будем называть фактор-группой и обозначать $G/H = \overline{G}$.

Гомоморфизм $f : G \to G/H$, определенный формулой $f(g) = \overline{g}$, будем называть каноническим.

Все элементы группы G, перестановочные с любым элементом из G, образуют подгруппу, которая называется центром группы G.

Упражнения

1.61. Пусть $G = GL(n,\mathbb{R})$ – группа всех обратимых $n \times n$-матриц с действительными коэффициентами, H – подгруппа матриц с определителем, равным 1. Докажите, что $H \lhd G$.

1.62. Докажите, что центр группы G является нормальной подгруппой в G.

1.63. Пусть H – подгруппа конечной группы G. Число $k = \frac{|G|}{|H|}$ называется индексом подгруппы H. Докажите, что всякая подгруппа индекса 2 нормальна.

1.64. Докажите, что в группе кватернионов Q_8 любая подгруппа является нормальной.

(1.65 – 1.70) Выясните, что из себя представляет фактор–группа G/H.

1.65. $G = \mathbb{Z}_{12}, H = 3\mathbb{Z}_{12}$.

1.66. $G = Q_8, H = \{-1, 1\}$.

1.67. $G = 4\mathbb{Z}, H = 12\mathbb{Z}$.

1.68. $G = (\mathbb{R} \setminus \{0\}, \cdot)$ – группа всех ненулевых действительных чисел с операцией умножения, $H = (\mathbb{R}_+, \cdot)$ – группа всех положительных действительных чисел с операцией умножения.

1.69. $G = D_4, H = \{e, \varphi^2\}$.

1.70. Подгруппа Клейна V_4 группы S_4 состоит из 4–х элементов:

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

и единицы. Верно ли, что $V_4 < S_4$?

1.8. Циклические группы. Строение конечных абелевых групп

Циклические группы имеют достаточно простое строение. Всякая бесконечная циклическая группа изоморфна $(\mathbb{Z},+)$. Всякая конечная циклическая группа изоморфна $\mathbb{Z}_n$ для подходящего натурального n.

Перед тем как сформулировать основные результаты о строении конечных абелевых групп, напомним следующее определение. Пусть имеются две группы – G_1 и G_2. На декартовом произведении $G_1 \times G_2$ множеств G_1 и G_2 введем структуру группы, задав умножение формулой $(g_1, g_2) * (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$, $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$.

Легко проверить, что множество $G_1 \times G_2$ с введенной таким образом операцией образует группу. Эту группу будем называть прямым произведением групп G_1 и G_2. В случае, когда группы G_1 и G_2 – абелевы, будем использовать аддитивную запись: $G_1 \oplus G_2$. В этом случае полученную группу будем называть прямой суммой групп G_1 и G_2.

Пусть A – абелева группа, и p – простое число. Множество элементов группы A, порядки которых равны степени числа p, образуют подгруппу группы A, которую мы будем называть p-примарной компонентой или просто примарной компонентой и обозначать символом $A(p)$. Группу A, совпадающую со своей p-примарной компонентой будем называть p-группой. Циклическую p-группу будем называть примарной циклической группой.

Всякая конечная абелева группа A порядка $n = p_1^{n_1} \cdot p_2^{n_2} \cdot\ldots\cdot p_k^{n_k}$ допускает разложение $A = A(p_1) \oplus A(p_2) \oplus \ldots A(p_k)$ в прямую сумму своих примарных компонент.

Каждая конечная абелева p-группа изоморфна прямой сумме примарных циклических групп. Это разложение однозначно с точностью до перестановки сомножителей.

Если $n = p_1^{\alpha_1} \cdot\ldots\cdot p_k^{\alpha_k}$, то группа вычетов по модулю n раскладывается в прямую сумму примарных p-компонент следующим образом: $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus\ldots\oplus \mathbb{Z}_{p_k^{\alpha_k}}$.

Для того, чтобы разложить абелеву группу $\mathbb{Z}_{n_1} \oplus\ldots\oplus \mathbb{Z}_{n_m}$ в прямую сумму примарных циклических групп, нужно разложить каждое слагаемое этой группы.

Число неизоморфных абелевых групп порядка p^n равно числу $s(n)$ разбиений числа n в сумму нескольких (возможно, одного) натуральных чисел $n = n_1 + n_2 + \ldots + n_r$, где $1 \le n_1 \le n_2 \le \ldots \le n_r$, $1 \le r \le n$. Например, существует две неизоморфные абелевы группы порядка p^2: $\mathbb{Z}_{p^2}$ и $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

$s(3) = 3$, так как $3 = 1+2 = 1+1+1$;

$s(4) = 5$, так как $4 = 1+3 = 2+2 = 1+1+2 = 1+1+1+1$;

$s(5) = 7$, так как

$$5 = 1+4 = 2+3 = 1+1+3 = 1+2+2 = 1+1+1+2 = 1+1+1+1+1.$$

Упражнения

1.71. Пусть $A = \mathbb{Z}_{15}$. Найдите примарные компоненты группы A. Задайте явным образом изоморфизм $A(p_1) \oplus A(p_2) \oplus\ldots\oplus A(p_k) \to A$.

(**1.72 – 1.76**) Разложите в прямую сумму примарных циклических групп следующие группы.

1.72. $\mathbb{Z}_6$. **1.73.** $\mathbb{Z}_{12}$. **1.74.** $\mathbb{Z}_{60}$.

1.75. $\mathbb{Z}_{360}$. **1.76.** $\mathbb{Z}_{756} \oplus \mathbb{Z}_{2250} \oplus \mathbb{Z}_{25725}$.

(**1.77 – 1.81**) Выясните, изоморфны ли следующие группы.

1.77. $\mathbb{Z}_{15} \oplus \mathbb{Z}_{225}$ и $\mathbb{Z}_{75} \oplus \mathbb{Z}_{45}$.

1.78. $\mathbb{Z}_9 \oplus \mathbb{Z}_{225}$ и $\mathbb{Z}_{15} \oplus \mathbb{Z}_{135}$.

1.79. $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$.

1.80. $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_9 \oplus \mathbb{Z}_{24}$.

1.81. $\mathbb{Z}_6 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$ и $\mathbb{Z}_{60} \oplus \mathbb{Z}_{10}$.

(**1.82 – 1.85**) Найдите число неизоморфных абелевых групп следующих порядков.

1.82. 64. **1.83.** 36. **1.84.** 100. **1.85.** 864.

1.9. Конечные группы до 10-го порядка

В этом параграфе мы перечислим все конечные группы до 10-го порядка включительно с точностью до изоморфизма.

$|G| = 1$. Существует одна группа порядка 1, состоящая из одной единицы {e}. Естественно, она абелева.

$|G| = 2$. Существует одна абелева группа порядка 2 – это $\mathbb{Z}_2$.

$|G| = 3$. Существует одна абелева группа порядка 3 – это $\mathbb{Z}_3$.

$|G| = 4$. Здесь существуют две группы – это $\mathbb{Z}_4$ и $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Обе они абелевы.

$|G| = 5$. Существует одна абелева группа порядка 5 – это $\mathbb{Z}_5$.

$|G| = 6$. Здесь существуют две группы. Одна из них абелева – это $\mathbb{Z}_6$. Другая – неабелева. Это D_3 – группа движений треугольника.

$|G| = 7$. Существует одна абелева группа порядка 7. Это $\mathbb{Z}_7$.

$|G| = 8$. Существуют 5 групп порядка 8. Три из них абелевы. Это $\mathbb{Z}_8$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ и $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Кроме них существуют две неабелевы группы. Это D_4 – группа движений квадрата и $\mathbf{Q}_8$ – группа кватернионов.

$|G| = 9$. Существуют две абелевы группы порядка 9. Это $\mathbb{Z}_9$ и $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

$|G| = 10$. Существуют две группы порядка 10. Одна из них абелева. Это $\mathbb{Z}_{10}$. Другая – неабелева. Это D_5 – группа движений правильного пятиугольника.

Упражнения

1.86. Докажите, что всякая циклическая группа является абелевой.

1.87. Докажите, что любая конечная группа простого порядка p изоморфна $\mathbb{Z}_p$ – группе вычетов по модулю p.

1.88. Докажите, что если в группе каждый элемент кроме единицы имеет порядок два, то эта группа абелева.

1.89. Докажите, что любая группа порядка четыре изоморфна либо $\mathbb{Z}_4$, либо $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

1.90. Докажите, что в неабелевой группе порядка шесть должен существовать элемент порядка три.

1.91. Пусть G – неабелева группа порядка шесть, x – элемент порядка три и $y \in G \setminus \{e, x, x^2\}$. Докажите, что тогда все элементы e, x, x^2, xy, x^2y, y – разные и y имеет порядок два.

1.92. Докажите, что в обозначениях предыдущей задачи $yx = x^2 y$.

1.93. Докажите, что всякая неабелева группа порядка шесть изоморфна группе движений правильного треугольника D_3.

1.94. Пусть G – неабелева группа 8-го порядка. Докажите, что в G содержится элемент 4-го порядка x и некоммутирующий с ним элемент y такие, что $G=\{e,x,x^2,x^3,y,xy,x^2y,x^3y\}$, причем $yx=x^3y.$

1.95. В обозначениях задачи 1.94 докажите, что либо $y^2=e,$ либо $y^2=x^2$. В первом случае $G\cong D_4$, а во втором – $G\cong Q_8$.

1.10. Линейные коды

Напомним основные определения для блочных линейных кодов. Пусть имеется канал связи по которому передается двоичная информация. Если двоичная последовательность разбивается на блоки длины k, которые, в соответствии с процедурой кодирования, преобразуются в блоки длины $n\geq k$, то такое кодирование называется блочным.

Линейным (n,k)–кодом будем называть линейное подпространство C размерности k в линейном пространстве $\mathbb{Z}_2^n$.

Если $v\in\mathbb{Z}_2^n$, то весом Хэмминга $w(v)$ вектора v будем называть число его ненулевых координат. Если $u,v\in\mathbb{Z}_2^n$, то число $d(u,v)=w(u-v)$ будем называть расстоянием между векторами u и v.

Число $d=\min\limits_{u,v\in C} d(u,v)=\min\limits_{v\in C,v\neq 0} w(v)$ будем называть весом кода C и обозначать $w(C)$.

Матрицу G размера $k\times n$, строки которой составлены из координат векторов $g_1,\dots,g_n$ некоторого базиса кода C, будем называть порождающей матрицей кода C.

Пусть $u=(u_1,\dots,u_n), v=(v_1,\dots,v_n)$ – элементы пространства $\mathbb{Z}_2^n$. Величину $(u,v)=u_1\cdot v_1+\dots+u_n\cdot v_n \quad (mod\ 2)$ назовем их псевдоскалярным произведением. В случае $(u,v)=0$ элементы u и v будем называть ортогональными. Если C – линейное подпространство в $\mathbb{Z}_2^n$, то $C^\perp=\{u\in\mathbb{Z}_2^n \mid \forall v\in \mathbb{Z}_2^n (u,v)=0\}$ будем называть ортогональным дополнением для C.

Очевидно, $C^\perp$ само является линейным подпространством. Из курса линейной алгебры следует, что сумма размерностей подпространств $C^\perp$ и C равна n.

Заметим, что $(u,u)=0$ возможно для $u\neq 0$, т.е. не выполнена одна из аксиом скалярного произведения. Поэтому произведение (u,v) мы называем псевдоскалярным.

Пусть $C^\perp$ – ортогональное дополнение кода C в пространстве $\mathbb{Z}_2^n$. Код $C^\perp$ называется двойственным к C, а его порождающая матрица H размера $(n-k)\times n$ называется проверочной матрицей кода C. Очевидно, $v\in C \Leftrightarrow Hv^T=0$.

Путем переименования переменных $x_1,\dots,x_n$ и линейных преобразований над строками матрицы H всегда можно добиться, чтобы проверочная матрица имела бы вид $H_0=[P,I_{n-k}]$, где I_{n-k} – единичная подматрица. Такой вид будем называть каноническим. Порождающая матрица может быть задана в виде $G_0=[I_k,P]$. Если $H_0=[P,I_{n-k}]$ – проверочная матрица (n,k)- кода C над полем $\mathbb{Z}_2$, то $G_0=[I_k,P^T]$ – его порождающая матрица. Наоборот, если $G_0=[I_k,P]$ – порождающая матрица кода, то $H_0=[P^T,I_{n-k}]$ – его проверочная матрица.

Важной характеристикой кода является его вес. От веса кода зависит сколько ошибок обнаруживает и сколько исправляет этот код. Вес кода можно определить по проверочной матрице. А именно, вес линейного $(n.k)$-кода C равен $d \Leftrightarrow$ любые $(d-1)$ столбцов проверочной матрицы линейно независимы, но некоторые d столбцов линейно зависимы.

Числа n,k и d связаны неравенством $d\leq n-k+1$.

Число ошибок, которые обнаруживает и исправляет данный код, определяется следующим образом. Линейный код C обнаруживает t ошибок $\Leftrightarrow$ вес кода $\geq t+1$.

Линейный код C исправляет t ошибок $\Leftrightarrow$ вес кода $\geq 2t+1$.

Общая процедура декодирования линейного кода C состоит в следующем. Если имеется линейный (n,k)-код, то абелеву группу $\mathbb{Z}_2^n$ мы раскладываем в смежные классы по подгруппе C. В каждом смежном классе выбираем слово наименьшего веса e_i. Если в данном смежном классе несколько слов наименьшего веса, выбираем любое из них. Выбранное слово называется лидером. Если на прием поступило слово v, и это слово содержится в i–том смежном классе, то мы декодируем его как $u = v + e_i$. Таким образом, данный код будет исправлять в точности те ошибки, которые совпадают с лидерами смежных классов.

Упражнения

1.96. Пусть процедура кодирования состоит в том, что двоичной последовательности (x_1, x_2, x_3) длины 3 сопоставляется двоичная последовательность $(x_1, x_2, x_3, x_4, x_5)$ длины 5 по формулам $x_4 = x_1 + x_2$, $x_5 = x_2 + x_3$. Найдите порождающую матрицу этого кода *C*.

1.97. Выпишите все кодовые слова кода *C* из задачи 1.96.

1.98. Найдите проверочную матрицу кода *C* из задачи 1.96.

1.99. Задана порождающая матрица кода в каноническом виде

$$G_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Найдите канонический вид его проверочной матрицы.

1.100 Задана проверочная матрица кода в каноническом виде

$$H_0 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Найдите канонический вид его порождающей матрицы.

1.101. Дана проверочная матрица линейного кода. Определите его вес:

а) $H = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$; **б)** $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$.

1.102. Допустим, что код *C* имеет вес 9. Сколько ошибок обнаруживает и сколько исправляет такой код?

1.103. Для кода *C* из задачи 1.96 разложите абелеву группу $\mathbb{Z}_2^n$ в смежные классы по подгруппе *C*. Выберите лидеры смежных классов.

1.104. Рассматриваем код *C* из задачи 1.96. Закодируйте слово $u = (101)$ с помощью порождающей матрицы. Сделайте в нем одну ошибку. Декодируйте полученное слово с помощью общей процедуры декодирования для линейных кодов, используя разложение, полученной в задаче 1.103. Получилось ли исходное слово?

(**1.105 – 1.108**) Линейный код задан порождающей матрицей G. Найдите проверочную матрицу. Определите вес кода. Сколько ошибок обнаруживает и сколько ошибок исправляет такой код?

1.105. $G = \begin{pmatrix} 10011 \\ 01100 \end{pmatrix}$. **1.106.** $G = \begin{pmatrix} 10011 \\ 01101 \end{pmatrix}$.

1.107. $G = \begin{pmatrix} 10110 \\ 01111 \end{pmatrix}$. **1.108.** $G = \begin{pmatrix} 100011 \\ 010101 \\ 001110 \end{pmatrix}$.

1.11. Коды Хэмминга

Одним из известных видов линейных кодов являются коды Хэмминга. Введем следующее обозначение. Максимальное число точек пространства $\mathbf{Z}_2^n$, расстояние между которыми не меньше *s*, обозначим $A(n,s)$. Эта величина является важной для всей теории кодирования.

Справедливо неравенство Хэмминга $A(n,2t+1) \le \dfrac{2^n}{1+C_n^1+\ldots+C_n^t}$.

Коды, для которых неравенство Хэмминга превращается в равенство, называются совершенными.

Код Хэмминга, исправляющий одну ошибку, это линейный (n,k)-код, где $n=2^m-1, k=2^m-m-1$ (m – некоторое натуральное число).

Проверочная матрица H этого кода имеет размеры $m\times(2^m-1)$ и представляет собой двоичную запись натуральных чисел $1,2,3,\ldots,2^m-1$, расположенных по столбцам. Например, для $m=3$ получим следующую проверочную матрицу для (7,4) кода Хэмминга

$$H=\begin{pmatrix} 0001111 \\ 0110011 \\ 1010101 \end{pmatrix}.$$

Если была допущена одна ошибка, и на прием поступило слово u, то вектор Hu^T будет представлять двоичную запись разряда, в котором эта ошибка была допущена.

Отношение $R=\frac{k}{n}$ для блочного (n,k)–кода называется скоростью передачи.

Для кода Хэмминга $R=\frac{2^m-m-1}{2^m-1}=1-\frac{m}{2^m-1}\to 1$ при $m\to\infty$. Код Хэмминга является совершенным (при $t=1$), т.к. $\dfrac{2^n}{1+C_n^1}=\dfrac{2^{2^m-1}}{2^m}=2^{2^m-m-1}$, а $2^m-m-1=k$ – размерность пространства кодовых слов.

Вес кода Хэмминга $d=3$, т.к. в проверочной матрице нет одинаковых столбцов, т.е. любые два столбца линейно независимы, и существуют три столбца, которые линейно зависимы.

Упражнения

1.109. Докажите, что $A(n,1)=2^n$, $A(n,n)=2$.

1.110. Найдите $A(3,2)$.

1.111. Найдите порождающую матрицу для (7,4)-кода Хэмминга.

1.112. Рассматривается (7,4)-код Хэмминга. Известно, что в принятом слове *u* допущена одна ошибка. Исправьте ее:

а) $u=(1110010)$; **б)** $u=(1101110)$; **в)** $u=(1111100)$.

1.113. Запишите проверочную матрицу для (15,11)-кода Хэмминга.

1.114. Рассматривается (15,11)-код Хэмминга. Известно, что в принятом слове *u* допущена одна ошибка. Исправьте ее:

а) $u=(000111000111000)$; **б)** $u=(100100100100100)$;

в) $u=(000000001111111)$.

2. Теория булевых функций

2.1. Булевы функции и способы их задания

1. Понятие булевой функции. Упорядоченный набор $\tilde{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$, где $\alpha_i \in \{0,1\}$, называется *булевым вектором*. Числа α_i называются *координатами* вектора, число n – его *длиной*.

Множество всех булевых векторов длины n называется *единичным* n*-мерным кубом* и обозначается B^n. Сами векторы называются вершинами куба B^n. *Весом* вектора называется число его координат, равных 1. *Расстоянием* между вершинами $\tilde{\alpha}$ и $\tilde{\beta}$ куба B^n называется число $\rho(\tilde{\alpha}, \tilde{\beta}) = \sum_{i=1}^{n} |\alpha_i - \beta_i|$, равное числу координат, в которых они различаются. Вектора $\tilde{\alpha}$ и $\tilde{\beta}$ называются *соседними*, если $\rho(\tilde{\alpha}, \tilde{\beta}) = 1$, и *противоположными*, если $\rho(\tilde{\alpha}, \tilde{\beta}) = n$.

Функция, определенная на B^n и принимающая значения из множества $\{0,1\}$, называется *булевой функцией* от n переменных.

Множество всех булевых функций от n переменных обозначается $P_2(n)$; множество всех булевых функций - P_2.

Чтобы задать булеву функцию достаточно указать ее значение (0 или 1) для каждого набора $(\alpha_1, \alpha_2, ..., \alpha_n)$ значений аргументов $(x_1, x_2, ..., x_n)$. Удобно делать это с помощью таблицы (Табл. 1), которую называют *таблицей истинности функции*

Таблица 1.

x_1	x_2	…	x_{n-1}	x_n	$f(x_1, x_2, ..., x_{n-1}, x_n)$
0	0	…	0	0	$f(0, 0, ..., 0, 0)$
0	0	…	0	1	$f(0, 0, ..., 0, 1)$
…	…	…	…	…	…
1	1	…	1	1	$f(1, 1, ..., 1, 1)$

Приведем примеры булевых функций одной (Табл. 2) и двух (Табл. 3) переменных:

Таблица 2

x	0	x	$\neg x$	1
0	0	0	1	1
1	0	1	0	1

Таблица 3

x	y	$x \wedge y$	$x \oplus y$	$x \vee y$	$x \downarrow y$	$x \leftrightarrow y$	$x \to y$	$x \mid y$
0	0	0	0	0	1	1	1	1
0	1	0	1	1	0	0	1	1
1	0	0	1	1	0	0	0	1
1	1	1	0	1	0	1	1	0

Булевы функции, заданные таблицами 2 и 3, называются элементарными. Приведем их названия: 0 – тождественный ноль, x - тождественная функция; $\neg x$ ($\bar{x}$) – отрицание x; 1 – тождественная единица; $x \wedge y$ ($x \cdot y$, xy) – конъюнкция x и y; $x \vee y$ – дизъюнкция x и y; $x \oplus y$ – сумма по модулю два x и y; $x \leftrightarrow y$ – эквивалентность x и y; $x \to y$ – импликация x и y; $x \mid y$ – штрих Шеффера x и y; $x \downarrow y$ – стрелка Пирса x и y.

Переменная x_i называется *фиктивной* переменной функции $f(x_1,...,x_n)$, если для всех значений $\alpha_1,...,\alpha_{i-1},\alpha_{i+1},...,\alpha_n$ переменных $x_1,...,x_{i-1},x_{i+1},...,x_n$ выполняются равенства $f(\alpha_1,...,\alpha_{i-1},0,\alpha_{i+1},...\alpha_n)=f(\alpha_1,...,\alpha_{i-1},1,\alpha_{i+1},...\alpha_n)$. В противном случае переменная x_i называется *существенной*.

Пусть для функции $f(x_1,x_2,...,x_n)$ переменная x_i является фиктивной. Возьмем таблицу истинности функции f. Вычеркнем из нее все строки, в которых $x_i=1$, а также вычеркнем столбец переменной x_i. Полученная таким образом таблица будет задавать некоторую функцию $g(x_1,...,x_{i-1},x_{i+1},...,x_n)$, причем на любом наборе $\alpha_1,...,\alpha_{i-1},\alpha_i,\alpha_{i+1},...,\alpha_n$ значений переменных $x_1,...,x_{i-1},x_i,x_{i+1},...,x_n$ для функций f и g выполнено равенство $f(\alpha_1,...,\alpha_{i-1},\alpha_i,\alpha_{i+1},...,\alpha_n)=g(\alpha_1,...,\alpha_{i-1},\alpha_{i+1},...,\alpha_n)$. Про функцию g говорят, что она получена из функции f путем удаления фиктивной переменной, а про функцию f говорят, что она получена из g путем введения фиктивной переменной.

Функции f и g называются *равными*, если функцию g можно получить из функции f путем введения или удаления фиктивных переменных.

2. Реализация булевых функций формулами. Пусть В – некоторое подмножество функций из P_2; F – множество символов, используемых для обозначения функций из множества В; X – множество символов, используемых для обозначения переменных; $x_{èìä}\in X$, $f_{èìä}\in F$. *Формулой над* В называется:

1) каждое выражение вида $(f_0(x_1,x_2,...,x_n))$;

2) выражение вида $(f_0(A_1,A_2,...,A_n))$, где A_i - либо символ переменной $(A_i\in X)$, либо формула над В.

Для обозначения формулы над В используют запись $\Phi[\mathrm{B}]$.

Каждой формуле сопоставляется функция (при этом говорят, что формула реализует функцию и пишут $\Phi[\mathrm{B}]=f$). Функция, которая реализуется формулой над множеством В, называется *суперпозицией* над множеством В.

Если две формулы Φ_1 и Φ_2 реализуют равные функции, то их называют *равносильными* и пишут $\Phi_1=\Phi_2$.

Функция f^*, реализуемая формулой $\overline{f}(\overline{x_1},...,\overline{x_n})$, называется *двойственной* к функции $f(x_1,x_2,...,x_n)$.

Справедливо следующее утверждение (принцип двойственности): если формула $\Phi[f_1,f_2,...,f_n]$ реализует функцию g, то формула, полученная из нее заменой символов функций $f_1,f_2,...,f_n$ на символы двойственных к ним функций $f_1^*,f_2^*,...,f_n^*$, реализует функцию g^*, двойственную к функции g (эту формулу называют *двойственной к* $\Phi[f_1,f_2,...,f_n]$).

3. Реализация булевых функций в виде дизъюнктивных и конъюнктивных нормальных форм.

Если $f\not\equiv 0$, то она может быть реализована формулой $f(x_1,x_2,...,x_n)=\bigvee\limits_{\substack{(\sigma_1,...,\sigma_n)\in B^n:\\ f(\sigma_1,...,\sigma_n)=1}}\left(x_1^{\sigma_1}\wedge...\wedge x_n^{\sigma_n}\right)$ **(здесь** $x^\sigma=\overline{x}$, если $\sigma=0$, и $x^\sigma=x$, если $\sigma=1$), которую называют *совершенной дизъюнктивной нормальной формой* или, сокращенно, СДНФ.

обозначены элементарные конъюнкции над множеством X, называют *дизъюнктивной нормальной формой (ДНФ) над множеством* X. Сумма рангов конъюнкций, входящих в ДНФ, называется *сложностью* ДНФ.

Дизъюнктивная нормальная форма, имеющая по сравнению с другими ДНФ, реализующими данную функцию, наименьшую сложность, называется *минимальной дизъюнктивной нормальной формой* данной функции.

Элементарная конъюнкция называется *импликантой* функции $f(x_1, x_2, ..., x_n)$, если на любом наборе $(\alpha_1, \alpha_2, ..., \alpha_n)$, на котором эта элементарная конъюнкция равна 1, функция f также обращается в 1.

Импликанту функции f называют *простой*, если элементарная конъюнкция, получающаяся из нее удалением любой буквы, уже не является импликантой f.

Сокращенной ДНФ функции называется дизъюнкция всех ее простых импликант. Сокращенная ДНФ f реализует функцию f.

Тупиковой ДНФ функции называется такая реализующая ее дизъюнкция простых импликант, из которой нельзя удалить ни одну простую импликанту так, чтобы полученная после удаления ДНФ все еще реализовала функцию. Если $f \not\equiv 1$, то она может быть реализована формулой

$f(x_1, x_2, ..., x_n) = \bigwedge\limits_{\substack{(\tau_1,...,\tau_n)\in B^n: \\ f(\tau_1,...,\tau_n)=0}} \left(x_1^{\bar{\tau}_1} \vee ... \vee x_n^{\bar{\tau}_n} \right)$, которую называют *совершенной конъюнктивной нормальной формой* или, сокращенно, СКНФ.

Пусть задан алфавит переменных $X = \{x_1, x_2, ..., x_n\}$. Формулу вида $K = x_{i_1}^{\sigma_1} \cdot x_{i_2}^{\sigma_2} \cdot ... \cdot x_{i_r}^{\sigma_r}$ ($i_\nu < i_\mu$ при $\nu < \mu$, $\sigma_i \in \{0,1\}$) называют *элементарной конъюнкцией ранга* r *над множеством* X. Константа 1 рассматривается как элементарная конъюнкция ранга 0.

Формулу вида $D = K_1 \vee K_2 \vee ... \vee K_s$ ($K_i \neq K_j$ при $i \neq j$), где через K_i $(i = 1, 2, ..., s)$

Упражнения

2.1. а) Перечислить вершины булева куба B^4, соседние с вершиной $(0,1,0,0)$.

б) Определить число вершин булева куба B^n, соседних с данной вершиной.

в) Определить число неупорядоченных пар соседних вершин булева куба B^n.

2.2. а) Перечислить вершины булева куба B^4, удаленные от вершины $(0,1,1,0)$ на расстояние 2.

б) Найти число вершин булева куба B^n, удаленных от данной вершины на расстояние k ($0 \le k \le n$).

в) Найти число неупорядоченных пар вершин булева куба B^n, удаленных друг от друга на расстояние k ($0 \le k \le n$).

2.3. Определить, сколько булевых векторов длины n одинаково читаются слева направо и справа налево.

2.2. Найти номер булева вектора:

а) $(1,0,0,1,1)$; **б)** $(1,1,0,0,1,0)$;

в) $(1,1,1,1,1)$; **г)** $(1,0,0,1,1,0,1)$.

2.5. а) Перечислить векторы значений булевых функций двух переменных, принимающих на противоположных наборах значений переменных одинаковые значения?

б) Найти число булевых функций от n переменных, принимающих на противоположных наборах значений переменных одинаковые значения.

2.6. а) Перечислить векторы значений булевых функций двух переменных, принимающих на наборах веса 1 значение 0.

б) Найти число булевых функций от n переменных, принимающих на наборах веса k значение 1.

2.7. Каково число булевых функций от n переменных, которые на любой паре соседних наборов принимают одинаковые значения?

2.8. Указать существенные и фиктивные переменные функции:

а) $f=(1100)$; **б)** $f=(1001\ 1001)$;

в) $f=(1100\ 0011)$; **г)** $f=(1010\ 0000\ 1010\ 0000)$.

2.9. Задать вектором значений функцию, равную данной и существенно зависящую от всех своих аргументов:

а) $f=(1110\ 1110\ 1010\ 1010)$; **б)** $f=(1100\,1100)$;

в) $f=(1010\ 0101\ 1010\ 0101)$; **г)** $f=(0000\ 1111\ 0000\ 1111)$.

2.10. Задать вектором значений функцию, реализуемую формулой:

а) $\left(\left(x_1 \oplus \left(x_1 \vee x_2\right)\right) \to \overline{x_1}\right)$; **б)** $\left(\left(x_1 x_2\right) \leftrightarrow \left(\overline{x_2} \,|\, x_3\right)\right)$;

в) $\left(x_3 \downarrow \left(x_1 x_2\right)\right) \vee \left(1 \to x_3\right)$; **г)** $x_1 x_2 \oplus \left(x_3 \,|\, x_4\right)$.

2.11. Пусть $\mathbf{B}=\{f,g,h\}$ - множество булевых функций, причем $f \in P_2(1)$, $g \in P_2(2)$, $h \in P_2(3)$, $X=\{x,y,z\}$ - алфавит переменных. Определить, является ли выражение формулой над множеством $\mathbf{B}$ независимо от вида функций f,g,h:

а) $A=h(0,x,f(x))$; **б)** $A=g\left(f(z),\overline{x}\right)$;

в) $A=h(g(x,x),f(x),y)$; **г)** $A=f(h(x,y,z))$;

д) $A=g(f(1),g(y,z))$; **е)** $A=h(f(x,x),y,z)$.

2.12. По функциям $f(x_1,x_2)$ и $g(x_3,x_4)$, заданным векторами значений, построить векторы значений функции h:

а) $f=(1101)$, $g=(0110)$, $h(x_2,x_3,x_4)=f\left(g(x_3,x_4),x_2\right)$;

б) $f=(0100)$, $g=(0010)$,

$$h(x_1,x_2,x_3,x_4)=g\left(g(x_3,x_4),f(x_1,x_2)\right).$$

2.13. Учитывая соглашения о порядке выполнения операций, опустить «лишние» скобки и знак «$\wedge$» в формуле:

а) $x \wedge \left(y \wedge \left(\overline{x} \vee y\right)\right)$;

б) $\left(\left(x \vee y\right) \vee \left(x \wedge \left(y \wedge z\right)\right)\right) \to \left(\left(\overline{x} \wedge \overline{y}\right) \to z\right)$.

2.14. Учитывая соглашения о порядке выполнения операций, восстановить скобки и связку «$\wedge$» в формуле:

а) $xy \vee x\overline{yz} \vee z$; **б)** $(x \vee z)\,y \to xy$.

2.15. Применяя таблицы истинности, доказать равносильность формул:

1. $x \vee y = y \vee x$; 2. $x \wedge y = y \wedge x$;

3. $x \vee (y \vee z) = (x \vee y) \vee z$; 4. $x \wedge (y \wedge z) = (x \wedge y) \wedge z$;

5. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$;

6. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$;

7. $x \vee x = x$; 8. $x \wedge x = x$;

9. $\overline{x \vee y} = \overline{x} \wedge \overline{y}$; 10. $\overline{x \wedge y} = \overline{x} \vee \overline{y}$;

11. $x \vee 0 = x$; 12. $x \wedge 0 = 0$;

13. $x \vee 1 = 1$; 14. $x \wedge 1 = x$;

15. $x \vee (x \wedge y) = x$; 16. $x \wedge (x \vee y) = x$;

17. $x \wedge \overline{x} = 0$; 18. $x \vee \overline{x} = 1$;

19. $\bar{\bar{x}} = x$;   20. $x \vee \bar{x}y = x \vee y$.

2.16. Применяя таблицы истинности, доказать равносильность формул:

а) $x \to y = \bar{x} \vee y$;   **б)** $x \leftrightarrow y = \bar{x}\bar{y} \vee xy$;

в) $x | y = \bar{x} \vee \bar{y}$;   **г)** $x \downarrow y = \bar{x}\bar{y}$;

д) $x \oplus y = \bar{x}y \vee x\bar{y}$;   **е)** $x \vee y = x \oplus y \oplus xy$.

2.17. Применяя таблицы истинности, доказать равносильность формул:

а) $(x \to y) \wedge (y \to x) = x \leftrightarrow y$;   **б)** $x \to y = \bar{y} \to \bar{x}$.

2.18. Применяя таблицы истинности, доказать равносильность формул:

а) $x \oplus y = y \oplus x$;   **б)** $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;

в) $x \oplus 1 = \bar{x}$;   **г)** $x \oplus 0 = x$;

д) $x \oplus x = 0$;   **е)** $(x \oplus y)z = xz \oplus yz$.

2.19. Пусть $*$ - одна из связок $\{\to, \leftrightarrow\}$. Выяснить, обладает ли соответствующая элементарная операция алгебры логики свойством:

а) коммутативности $x * y = y * x$;

б) ассоциативности $x * (y * z) = (x * y) * z$.

2.20. Применяя равносильные преобразования, преобразовать формулу так, чтобы она содержала только «$\wedge$» и «$\neg$»:

а) $x \vee y \vee z$;   **б)** $x \to y$;   **в)** $x \leftrightarrow y$;   **г)** $x \vee (\bar{z} \to y)$.

2.21. Применяя равносильные преобразования, преобразовать формулу так, чтобы она содержала только «$\vee$» и «$\neg$»:

а) xyz;   **б)** $xy \to yz$;   **в)** $x \leftrightarrow y$;   **г)** $x \oplus y$.

2.22. Применяя равносильные преобразования, доказать тождественную истинность формул:

а) $(x \to y) \vee (y \to x)$;   **б)** $\bar{x}y\bar{z} \vee \bar{x}yz \vee x \vee \bar{y}$;

в) $\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}y\bar{z} \vee \bar{x}yz \vee x$;   **г)** $(x \leftrightarrow y)\bar{y} \to \bar{x}$.

2.23. С помощью равносильных преобразований упростить формулу:

а) $xyz \vee x\bar{y}z \vee \bar{z}$;   **б)** $(x \to \bar{y}) \vee \overline{x \vee y} \vee xy$;

в) $(\bar{x} \vee x\bar{y}) \leftrightarrow ((x \vee y) \leftrightarrow \bar{x}\bar{y})$;   **г)** $(\bar{x} \vee y)\overline{xy} \vee \overline{\bar{x} \vee y \vee z \vee \overline{xy}}$;

д) $\bar{y}x \vee \bar{\bar{x}}yz \vee \bar{z}$;   **е)** $(y \to \bar{x})(x \leftrightarrow y)$.

2.24. Упростив формулу, выявить существенные и фиктивные переменные функции:

а) $f(x_1, ..., x_6) = ((x_1 \to (x_2 \to x_1)) \to x_3)((x_4 \to (x_5 \to x_4)) \to x_6)$;

б) $f(x_1, x_2, x_3) = (x_1 \vee \overline{x_2} \vee \overline{x_3})(x_1 \vee \overline{x_2} \vee x_3)(\overline{x_1} \vee \overline{x_2} \vee x_3)(\overline{x_1} \vee \overline{x_2} \vee \overline{x_3})$.

2.25. а) Перечислить функции $f(x_1, x_2)$, у которых x_1 - фиктивная переменная.

б) Подсчитать число функций $f(x_1, ..., x_n)$, у которых x_n - фиктивная переменная.

в) Подсчитать число функций от n переменных, у которых одна из переменных фиктивная.

2.26. Выяснить, на скольких наборах значений переменных обращается в ноль функция:

а) $f(x_1, x_2, ..., x_6) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$;

б) $f(x_1, x_2, ..., x_6) = x_1x_2x_3 \vee x_4x_5x_6$;

в) $f(x_1, x_2, ..., x_{2n}) = x_1x_2 \vee x_3x_4 \vee ... \vee x_{2n-1}x_{2n}$;

г) $f(x_1, x_2, ..., x_{2n}) = (x_1 \vee x_2)(x_3 \vee x_4)...(x_{2n-1} \vee x_{2n})$.

2.27. Используя определение, найти элементарные функции, двойственные тождественному 0, тождественной 1, x, $\bar{x}$, $x \vee y$, $x \wedge y$, $x \downarrow y$, $x | y$, $x \leftrightarrow y$, $x \oplus y$.

2.28. **а)** Пусть $f(x_1, x_2)$ задана вектором $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$. Используя определение двойственной функции, выписать вектор значений функции $f^*(x_1, x_2)$.

б) Пусть $f(x_1, x_2, ..., x_n)$ задана вектором $(\alpha_1, \alpha_2, ..., \alpha_{2^n})$. Показать, что $f^*(x_1, x_2, ..., x_n)$ задается вектором $\left(\overline{\alpha_{2^n}}, ..., \overline{\alpha_2}, \overline{\alpha_1}\right)$.

2.29. Задать вектором значений функцию, двойственную данной:

а) $f = (1011)$; **б)** $f = (1011\ \ 0110)$;

в) $f = (1101\ \ 0100)$; **г)** $f = (1111\ \ 0011\ \ 1101\ \ 0010)$.

2.30. Задать вектором значений функцию, двойственную данной:

а) $f = (x_1 \downarrow x_3) \vee (\overline{x_1} \to x_2 x_3)$; **б)** $g = (x_1 \oplus x_2) \to x_2 x_3$.

2.31. Записать формулу, двойственную данной:

а) $xyz \vee x\bar{y}z \vee \bar{z} \vee 0$; **б)** $(x \oplus \bar{y})\, yz \vee 0$.

2.32. Применить принцип двойственности к равносильности:

а) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$; **б)** $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;

в) $(x \oplus y)\, z = xz \oplus yz$; **г)** $x \vee y = x \oplus y \oplus xy$.

2.33. Используя принцип двойственности, реализовать формулой функцию, двойственную данной (исходную формулу не упрощать):

а) $f = \overline{x \vee y} \cdot (x \vee \overline{yz})$; **б)** $f = (x \vee \bar{y}z \vee 0) \cdot \overline{zy}$;

в) $f = (\bar{x} \vee y)\, \overline{xy} \vee \overline{\bar{x} \vee y \vee z \vee \overline{xy}}$; **г)** $f = (x_1 \oplus x_2) \leftrightarrow (x_2 | x_3)$;

д) $f = xy\left(\overline{yx} \vee yz \cdot \overline{x \vee yz}\right) \vee 0$; **е)** $f = (x_1 \leftrightarrow x_3) \downarrow (x_2 | 0)$.

2.34. Показать, что если функция $f(x_1, x_2, ..., x_n)$ существенно зависит от переменной x_i $(i = 1, ..., n)$, то двойственная ей функция $f^*(x_1, x_2, ..., x_n)$ также существенно зависит от переменной x_i.

2.35. Реализовать функцию в виде СДНФ:

а) $x_1 \vee x_2$; **б)** $x_1 | x_2$;

в) $x_1 \downarrow x_2$; **г)** $x_1 \oplus x_2$;

д) $f = (1100\ \ 0101)$; **е)** $f = (0101\ \ 1110)$.

2.36. Реализовать функцию в виде СКНФ:

а) $x_1 x_2$; **б)** $x_1 | x_2$;

в) $x_1 \downarrow x_2$; **г)** $x_1 \oplus x_2$;

д) $f = (1100\ \ 0101)$; **е)** $f = (0101\ \ 1110)$.

2.37. Реализовать в виде СДНФ и СКНФ функцию:

а) $g(x_1, x_2, x_3) = (x_1 \oplus x_2) \to x_2 x_3$;

б) $f(x_1, x_2, x_3) = x_1 \cdot \bar{x}_2 \leftrightarrow (x_1 \vee x_2)\, x_3$;

в) $g(x_1, x_2, x_3) = f_1(x_1, x_2, x_3) \,|\, f_2(x_1, x_2, x_3)$,

где $f_1 = (00111011)$, $f_2 = (01100111)$;

г) $h(x_1, x_2) = g(x_1, x_2, x_2)$, где $g = (1101\ \ 0111)$.

2.38. **а)** Перечислить все элементарные конъюнкции над множеством $\{x_1, x_2\}$.

б) Найти число элементарных конъюнкций над множеством $\{x_1, x_2, ..., x_n\}$.

2.39. а) Перечислить все элементарные конъюнкции ранга 2 над множеством $\{x_1, x_2, x_3\}$.

б) Определить число элементарных конъюнкций ранга *r* над множеством $\{x_1, x_2, ..., x_n\}$ ($0 \le r \le n$).

2.40. а) Перечислить все элементарные конъюнкции ранга 3 над множеством $\{x_1, x_2, x_3, x_4\}$, обращающиеся в единицу на наборе $(1, 0, 0, 0)$.

б) Найти число элементарных конъюнкций ранга *r* над множеством $\{x_1, x_2, ..., x_n\}$, обращающихся в единицу на наборе $\{\alpha_1, \alpha_2, ..., \alpha_n\}$.

2.41. а) Перечислить все элементарные конъюнкции над множеством $\{x_1, x_2, x_3\}$, обращающиеся в единицу на наборе $(0, 1, 0)$.

б) Найти число элементарных конъюнкций над множеством $\{x_1, x_2, ..., x_n\}$, обращающихся в единицу на наборе $\{\alpha_1, \alpha_2, ..., \alpha_n\}$.

2.42. а) Подсчитать число функций от 3-х переменных, для которых элементарная конъюнкция $x_1 x_2$ является импликантой.

б) Подсчитать число функций от *n* переменных, для которых некоторая элементарная конъюнкция ранга *r* является импликантой.

2.43. Перечислить все простые импликанты функции:

а) $f = x \vee y$; **б)** $f = x | y$;

в) $f = (1100\ \ 0001)$; **г)** $f = (1111\ \ 0010)$.

2.44. С помощью равносильных преобразований привести к ДНФ формулу:

а) $F = (x_1 x_3 \vee x_1 x_2 x_3)(x_2 \overline{x_3} \vee x_1 \overline{x_2} x_3)$;

б) $F = (\overline{x_1 x_3} \vee x_1 x_3)(\overline{x_2}\,\overline{x_3} \vee x_1 \overline{x_2} x_3)$.

2.45. Построить сокращенную, тупиковые и минимальные ДНФ функции:

а) $f = (1101\ \ 0011)$; **б)** $f = (1100\ \ 1011)$;

в) $g = (1010\ \ 1011\ \ 1000\ \ 0001)$; **г)** $g = (1010\ \ 0000\ \ 1000\ \ 1111)$;

д) $g = (1111\ \ 0011\ \ 1010\ \ 1011)$; **е)** $g = (1111\ \ 0001\ \ 1001\ \ 1001)$.

2.46. Используя метод неопределенных коэффициентов, найти полином Жегалкина, реализующий функцию:

а) $f(x_1, x_2) = x_1 \downarrow x_2$; **б)** $f(x_1, x_2) = (0100)$;

в) $f(x_1, x_2, x_3) = (11001101)$; **г)** $f(x_1, x_2, x_3) = (10001101)$.

2.47. Используя метод равносильных преобразований, найти полином Жегалкина, реализующий функцию:

а) $f(x, y, z) = x(\overline{y} \vee z)$; **б)** $f(x, y, z) = x \to (\overline{y} \vee x\overline{z})$.

2.48. Используя метод равносильных преобразований, найти полином Жегалкина, реализующий функцию:

а) $f(x_1, x_2) = (0010)$; **б)** $f(x_1, x_2, x_3) = (0111\ \ 1011)$;

в) $f(x_1, x_2, x_3, x_4) = (0000\ \ 0000\ \ 0000\ \ 1011)$;

г) $f(x_1, x_2, x_3, x_4) = (1111\ \ 1111\ \ 1111\ \ 1010)$.

2.49. Используя принцип двойственности, построить формулу, реализующую функцию, двойственную функции f. Полученное выражение преобразовать, записав в виде полинома Жегалкина:

а) $f = xy \vee yz \vee xt \vee zt$; **б)** $f = \bar{x}y \vee xz\bar{t}$.

2.50. Показать, что если переменная x_i является существенной переменной функции, то она явно входит в ее полином Жегалкина.

2.2. Функционально замкнутые классы и полнота

1. Понятие полного множества. Множество булевых функций $\mathrm{B} = \{f_1, f_2, ..., f_m, ...\}$ называется *полной* системой, если любая булева функция из P_2 может быть реализована формулой над B.

Справедливо следующее утверждение (теорема о полноте двух систем): если система B_1 - полная и каждая ее функция может быть реализована формулой над B_2, то система B_2 тоже полная.

2. Понятие замыкания. Пусть B - некоторое подмножество P_2. Множество всех булевых функций, реализуемых формулой над B, называется *замыканием* B и обозначается $[\mathrm{B}]$.

Замыкание обладает следующими свойствами:

1. $\mathrm{B} \subset [\mathrm{B}]$; 2. $[[\mathrm{B}]] = [\mathrm{B}]$;

3. $(\mathrm{B}_1 \subset \mathrm{B}_2) \Rightarrow ([\mathrm{B}_1] \subset [\mathrm{B}_2])$; 4. $([\mathrm{B}_1] \cup [\mathrm{B}_2]) \subset ([\mathrm{B}_1 \cup \mathrm{B}_2])$.

3. Представление функции в виде полинома Жегалкина. Пусть M – произвольное подмножество булевого куба B^n, $\tilde{\sigma} = (\sigma_1, \sigma_2, ..., \sigma_n) \in M$, $\nu(\tilde{\sigma})$ – номер вектора $\tilde{\sigma}$, $\|\tilde{\sigma}\| = \sum_{i=1}^{n} \sigma_i$ - его вес, $i_1, i_2, ..., i_{\|\tilde{\sigma}\|}$ – номера отличных от нуля координат вектора $\tilde{\sigma}$. Формула вида $\sum_{\tilde{\sigma} \in M} a_{\nu(\tilde{\sigma})} \cdot x_{i_1} \cdot x_{i_2} \cdot ... \cdot x_{i_{\|\tilde{\sigma}\|}}$, где суммирование ведется по модулю два, а коэффициенты $a_{\nu(\tilde{\sigma})}$ равны либо 0, либо 1, называется *полиномом Жегалкина* от n переменных. Если суммирование в формуле, ведется по всем булевым векторам длины n, слагаемые идут в порядке возрастания номеров булевых векторов и $i_1 < i_2 < ... < i_{\|\tilde{\sigma}\|}$, то говорят, что полином Жегалкина записан в *канонической форме*.

Наибольший из рангов элементарных конъюнкций, входящих в полином с единичными коэффициентами, называется *степенью полинома*.

Справедливо следующее утверждение: каждая булева функция от n переменных может быть реализована в виде канонического полинома Жегалкина от n переменных, причем единственным образом.

4. Классы Поста. Говорят, что булева функция *сохраняет 0*, если $f(0, 0, ..., 0) = 0$. Множество булевых функций от n переменных, сохраняющих 0, обозначают $\mathbf{T_0}(n)$, множество всех булевых функций, сохраняющих 0 – $\mathbf{T_0}$.

Говорят, что булева функция *сохраняет* 1, если $f(1, 1, ..., 1) = 1$. Множество булевых функций от n переменных, сохраняющих 1, обозначают $\mathbf{T_1}(n)$, множество всех булевых функций, сохраняющих 1 - $\mathbf{T_1}$.

Булева функция называется *самодвойственной*, если $f = f^*$, т.е. на любом наборе $(\alpha_1, ..., \alpha_n)$ значений переменных $(x_1, ..., x_n)$ выполняется равенство $f(\alpha_1, ..., \alpha_n) = \overline{f}(\overline{\alpha_1}, ..., \overline{\alpha_n})$. Множество самодвойственных функций от n переменных обозначают $\mathbf{S}(n)$ множество, множество всех самодвойственных функций - $\mathbf{S}$.

Если для любого i $\alpha_i \le \beta_i$ $(i = 1, 2, ..., n)$, то говорят, что вектор $\tilde{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$ *предшествует вектору* $\tilde{\beta} = (\beta_1, \beta_2, ..., \beta_n)$ и пишут $\tilde{\alpha} \le \tilde{\beta}$.

Булева функция f называется *монотонной*, если для любых наборов $\tilde{\alpha}$ и $\tilde{\beta}$ значений переменных, таких что $\tilde{\alpha} \le \tilde{\beta}$, выполняется неравенство $f(\tilde{\alpha}) \le f(\tilde{\beta})$. Множество монотонных функций от n переменных обозначают $\mathbf{M}(n)$, множество всех монотонных функций - $\mathbf{M}$.

Булева функция называется *линейной*, если степень ее канонического полинома Жегалкина меньше либо равна 1. Множество линейных функций от n переменных обозначают $\mathbf{L}(n)$ множество, множество всех линейных булевых функций - $\mathbf{L}$.

Множества $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{S}$, $\mathbf{M}$, $\mathbf{L}$ называют классами Поста.

Классы Поста – замкнуты, попарно различны и неполны.

5. Критерий полноты. Справедливо следующее утверждение (теорема Поста): для того чтобы система функций В была полна, необходимо и достаточно, чтобы множество В не являлось подмножеством ни одного из классов Поста.

Система функций В называется *базисом*, если В - полна, а любое собственное подмножество В неполно.

Класс D называется *предполным* классом, если он неполон и добавление к нему любой функции, ему не принадлежащей, приводит к образованию полного множества.

Упражнения

2.51. Выяснить, сколько функций от n переменных содержится во множестве:

а) $\mathbf{T}_0$; **б)** $\mathbf{T}_1$;

в) $\mathbf{T}_0 \cap \mathbf{T}_1$; **г)** $\mathbf{T}_0 \cup \mathbf{T}_1$.

2.52. а) Выписать векторы значений всех самодвойственных функций двух переменных.

б) Найти число самодвойственных функций от n переменных.

2.53. а) Сколько функций содержит множество $\mathbf{T}_0(n) \cap \mathbf{S}(n)$?

б) Сколько функций содержит множество $\mathbf{T}_0(n) \cap \mathbf{T}_1(n) \cap \mathbf{S}(n)$?

в) Сколько функций содержит множество $\mathbf{T}_0(n) \cup \mathbf{S}(n)$?

г) Сколько функций содержит множество $\mathbf{T}_0(n) \cup \mathbf{T}_1(n) \cup \mathbf{S}(n)$?

2.54. Показать, что если $f(x_1, x_2, ..., x_n)$ самодвойственная функция, то число наборов, на которых она обращается в единицу, равно 2^{n-1}.

2.55. Убедившись в том, что функция f - несамодвойственная, реализовать формулой над множеством $\{f, \bar{x}\}$ константы 0 и 1:

а) $f = \bar{x}\bar{z} \vee \bar{x}y$; **б)** $f = \bar{y} \vee xz$;

в) $f = (1001\ \ 0111)$; **г)** $f = (1100\ \ 1000)$.

2.56. а) Перечислить булевы векторы, предшествующие вектору $(1, 0, 1, 1)$.

б) Найти число булевых векторов длины n, предшествующих некоторому вектору веса k?

2.57. а) Перечислить булевы векторы, которым предшествует вектор $(0, 1, 0, 1, 1, 1)$.

б) Найти число булевых векторов длины n, которым предшествует некоторый вектор веса k?

2.58. Рассмотрим на множестве булевых векторов бинарное отношение предшествования ($\le$): $\tilde{\alpha} \le \tilde{\beta} \Leftrightarrow \forall i (\alpha_i \le \beta_i)$. Показать, что это отношение является отношением частичного порядка на B^n.

2.59. Какие из основных элементарных функций являются монотонными?

2.60. Доказать, что монотонная функция, не сохраняющая ноль (единицу), равна тождественно единице (нулю).

2.61. Выяснить, монотонна или нет функция:

а) $f = (00011011)$; **б)** $f = (00000101)$;

в) $f = x \to \left(\overline{x} \leftrightarrow yz\right)$; **г)** $f = \left(x \leftrightarrow y\right) \vee \left(x \oplus z\right)$.

2.62. Показать, что если функция $f\left(x_1,...,x_n\right)$ немонотонная, то найдется пара соседних векторов $\tilde{\alpha}$, $\tilde{\beta}$ из B^n таких, что $\tilde{\alpha} \le \tilde{\beta}$, но $f\left(\tilde{\alpha}\right) > f\left(\tilde{\beta}\right)$.

2.63. а) Найти число монотонных функций от 2-х переменных.
б) Найти число монотонных функций от 3-х переменных.

2.64. Показать, что для проверки на монотонность функции $f\left(x_1,...,x_n\right)$, заданной своим вектором значений $\tilde{\alpha}_f$, можно придерживаться такого алгоритма. Делим вектор значений $\tilde{\alpha}_f$ на две равные части $\tilde{\alpha}_{f_1} = \left(\alpha_0,...,\alpha_{2^{n-1}-1}\right)$ и $\tilde{\alpha}_{f_2} = \left(\alpha_{2^{n-1}},...,\alpha_{2^n-1}\right)$. Если соотношение $\tilde{\alpha}_{f_1} \le \tilde{\beta}_{f_2}$ не выполнено, то функция f - немонотонная. В противном случае разделим каждый из векторов $\tilde{\alpha}_{f_1}$ и $\tilde{\alpha}_{f_2}$ также пополам на $\tilde{\alpha}_{f_{1,1}}$, $\tilde{\alpha}_{f_{1,2}}$ и $\tilde{\alpha}_{f_{2,1}}$, $\tilde{\alpha}_{f_{2,2}}$. Проверим сначала первую пару на выполнение соотношения $\tilde{\alpha}_{f_{1,1}} \le \tilde{\beta}_{f_{1,2}}$ и, в случае положительного результата, вторую. Если хотя бы для одной пары соотношение не выполняется, то функция немонотонна. В противном случае вновь делим пополам каждый из полученных векторов и т.д.

2.65. Выяснить, монотонна или нет функция:

а) $f = (0101\,1101\,1111\,0011)$; **б)** $f = (0001\,0101\,0000\,1111)$;

в) $f = \left(x \downarrow z\right)\left(y \oplus x\right)$; **г)** $f = 1 \oplus x \oplus yz \oplus xyz$.

2.66. Задать вектором значений функцию четырех переменных, являющуюся монотонной самодвойственной функцией и удовлетворяющую условию:

а) $f\left(0,1,1,1\right) = 0$;

б) $f(1,0,0,1) = f(1,0,1,0)$.

2.67. Доказать, что функция, двойственная монотонной функции, монотонна.

2.68. Показать, что если функция не сохраняет константу 0, то она либо немонотонная, либо несамодвойственная.

2.69. Убедившись в том, что функция f - немонотонная, реализовать формулой над множеством $\left\{f,0,1\right\}$ отрицание:

а) $f = \overline{x}\overline{z} \vee \overline{x}\overline{y}$; **б)** $f = 1 \oplus x \oplus y \oplus z$;
в) $f = \left(11000100\right)$; **г)** $f = \left(01111001\right)$.

2.70. Какие из основных элементарных функций являются линейными?

2.71. Определить число функций от n переменных, принадлежащих множеству:

а) $\mathbf{L}$; **б)** $\mathbf{T}_0 \cap \mathbf{L}$;

в) $\mathbf{T}_1 \cap \mathbf{L}$; **г)** $\mathbf{T}_0 \cap \mathbf{T}_1 \cap \mathbf{L}$;

д) $\mathbf{S} \cap \mathbf{L} \cap \mathbf{T}_0$; **е)** $\mathbf{M} \cap \mathbf{L}$.

2.72. а) Определить число линейных функций от n переменных, которые сохраняют константу 0 и не сохраняют константу 1.
б) Определить число функций от n переменных, принадлежащих множеству $\mathbf{L} \setminus \left(\mathbf{T}_0 \cap \mathbf{T}_1\right)$.

2.73. Доказать, что функция, двойственная линейной функции, также линейна.

2.74. Найти число линейных функций от n переменных, существенно зависящих ровно от k переменных.

2.75. Доказать, что если $f\left(x_1,...,x_n\right)$ - линейная функция, отличная от константы, то она обращается в единицу ровно на 2^{n-1} булевых векторах.

2.76. Убедившись в том, что функция f - нелинейная, реализовать формулой над множеством $\left\{f,0,1,\overline{x}\right\}$ конъюнкцию:

а) $f = 1 \oplus x \oplus y \oplus zx \oplus xy \oplus xyz$; **б)** $f = \overline{x}y \vee z\overline{t}$;

в) $f=(10111111)$; **г)** $f=\overline{xyt}\to z$.

2.77. Заполнить таблицу (поставить в ячейке «+», если функция принадлежит классу, и «–», если не принадлежит).

Функции		Классы функций				
		$\mathbf{T}_0$	$\mathbf{T}_1$	$\mathbf{S}$	$\mathbf{M}$	$\mathbf{L}$
1	0					
2	x					
3	$\overline{x}$					
4	1					
5	$x\wedge y$					
6	$x\vee y$					
7	$x\to y$					
8	$x\leftrightarrow y$					
9	$x\mid y$					
10	$x\downarrow y$					
11	$x\oplus y$					

2.78. Выяснить, каким из классов $\mathbf{T}_0,\mathbf{T}_1,\mathbf{S},\mathbf{M},\mathbf{L}$ принадлежит функция:

а) $f_1(x,y,z)=(0011\ 1101)$;

б) $f_2(x,y,z)=(x\vee z)(x\oplus y)$;

в) $f_3(x_1,x_2,x_3)=(x_1|x_2)\to(x_1\oplus x_3)$;

г) $f_4(x,y,z)=(x\oplus y)(x\to z)$;

д) $f_5(x_1,x_2,x_3)=\left(\overline{x_1}\downarrow x_2\right)\oplus x_3$;

е) $f_6(x_1,x_2,x_3,x_4)=x_1x_3\leftrightarrow x_2x_4$.

2.79. а) Показать, что класс $\mathbf{T}_0$ не содержится ни в одном из классов $\mathbf{T}_1$, $\mathbf{S}$, $\mathbf{M}$, $\mathbf{L}$.

б) Показать, что класс $\mathbf{T}_1$ не содержится ни в одном из классов $\mathbf{T}_0$, $\mathbf{S}$, $\mathbf{M}$, $\mathbf{L}$.

в) Показать, что класс $\mathbf{S}$ не содержится ни в одном из классов $\mathbf{T}_0,\mathbf{T}_1,\mathbf{M},\mathbf{L}$.

г) Показать, что класс $\mathbf{M}$ не содержится ни в одном из классов $\mathbf{T}_0,\mathbf{T}_1,\mathbf{S},\mathbf{L}$.

д) Показать, что класс $\mathbf{L}$ не содержится ни в одном из классов $\mathbf{T}_0,\mathbf{T}_1,\mathbf{S},\mathbf{M}$.

2.80. Пусть $f(x_1,x_2,...,x_n)$ - произвольная булева функция, $\varphi(x)$ получена из $f(x_1,x_2,...,x_n)$ путем отождествления всех переменных: $\varphi(x)=f(x,x,...,x)$. Определить $\varphi(x)$, если

а) $f\in\mathbf{T}_1\setminus\mathbf{T}_0$; **б)** $f\in\mathbf{T}_0\setminus\mathbf{T}_1$;

в) $f\in\mathbf{S}$; **г)** $f\in\mathbf{T}_1\cup\mathbf{S}$.

2.81. Какие из указанных ниже систем функций являются замкнутыми классами:
а) функции от одной переменной;
б) функции от двух переменных;
в) линейные функции;
г) самодвойственные функции;
д) монотонные функции;
е) функции, сохраняющие ноль;
ж) функции, сохраняющие единицу;
з) функции, сохраняющие и ноль, и единицу;
и) функции, сохраняющие ноль, но не сохраняющие единицу?

2.82. Является ли объединение функционально замкнутых классов функционально замкнутым классом?

2.83. Доказать, что функцию f нельзя реализовать формулой над множеством связок S, если:

а) $f=x|y$, $S=\{\vee,\to\}$;

б) $f = x \vee y$, $S = \{\leftrightarrow, \oplus\}$;

в) $f = (10100011)$, $S = \{\wedge, \vee\}$;

г) $f = x \to y$, $S = \{\leftrightarrow, \neg\}$;

д) $f = (10000101)$, $S = \{\neg, \oplus\}$;

е) $f = 1 \oplus x \oplus y \oplus z$, $S = \{\wedge, \vee\}$.

2.84. Доказать, что:

а) $\mathbf{T}_0 = [x \vee y, x \oplus y]$; **б)** $\mathbf{T}_0 \cap \mathbf{L} = [x \oplus y]$.

2.85. Используя теорему о полноте двух систем, доказать полноту системы булевых функций:

а) $\{\overline{x},\ x \to y\}$; **б)** $\{1, xy, x \oplus y\}$;

в) $\{1, x \vee y, x \oplus y\}$; **г)** $\{1 \oplus x \oplus y \oplus yz\}$.

2.86. С помощью теоремы Поста проверить на полноту систему булевых функций:

а) $\{xy, x \vee y, x \to y\}$; **б)** $\{x \to y, x \to \overline{y}z\}$;

в) $\{xy \vee xz \vee yz, 0, 1\}$; **г)** $\{x \leftrightarrow y, \overline{x}, \overline{x} \to \overline{y}\}$;

д) $\{xy, x \vee y,\ x \oplus y \oplus z \oplus 1\}$; **е)** $\{0, \left(x \middle| (xy)\right) \to z\}$;

ж) $\{x \to y, xy \oplus z\}$; **з)** $\{x \leftrightarrow y, (x \to z) \to xy, 0\}$.

2.87. Определить, является ли базисом система булевых функций:

а) $\{(0010), (10110011), (00101011)\}$;

б) $\{x \leftrightarrow y, (x \vee y) \oplus xy, x \vee y\}$.

2.88. Перечислить все базисы, которые можно выделить из системы функций $\{0,\ x,\ \overline{x},\ x \wedge y,\ x \vee y,\ x \to y,\ x \leftrightarrow y,\ x | y,\ x \downarrow y,\ x \oplus y,\ 1\}$.

2.89. Привести пример базиса из четырех функций.

2.90. Доказать, что базис не может содержать более четырех функций.

3. Теория графов

1. Основные понятия. ***Граф*** G (*неориентированный*) – это пара множеств $G=(V,E)$, где $V=V(G)$ – множество вершин, $E=E(G)$ – множество рёбер, причём ребро $e\in E(G)$ представляет собой неупорядоченную пару вершин: $e=(x,y)$, где $x,y\in V(G)$ и $x\neq y$. Множество V предполагается конечным, а значит, и множество E конечно. Граф изображают на плоскости так: вершины изображаются точками плоскости, а рёбра $e=(x,y)$ – линиями, соединяющими вершины x и y. Две вершины v и v' графа G называются *смежными*, если $(v,v')\in E(G)$. Рёбра называются *смежными*, если они имеют общую вершину. Вершина v *инцидентна* ребру e, если $e=(v,x)$ для некоторого x. ***Подграф*** H графа G – это пара $H=(V(H),E(H))$, где $V(H)\subseteq V(G)$ и $E(H)\subseteq E(G)$.

Некоторые обобщения понятия графа: а) *обобщённый граф – это множество вершин* V и рёбер E, причём допускаются *петли*, т.е. рёбра вида (a,a), и *кратные рёбра*, т.е. две вершины a и b могут соединяться не одним, а несколькими рёбрами; б) *бесконечный граф* (т.е. $V(G)$ – бесконечное множество).

Ориентированный граф $G=(V,E)$ определяется аналогично обычному, но его рёбра $e=(x,y)$ являются *упорядоченными* парами вершин.

Два графа G и G' называются ***изоморфными***, если существует взаимно однозначное отображение $j:V(G)\to V(G')$ такое, что $\forall x,y\in V(G)\ \ (x,y)\in E(G)\Leftrightarrow (j(x),j(y))\in E(G')$. Отображение j называется *изоморфизмом.*

Пусть G – граф, $V(G)=\{v_1,\mathbf{K},v_n\}$, $E(G)=\{e_1,\mathbf{K},e_m\}$. ***Матрица смежности*** графа G – это матрица $A=\|a_{ij}\|$ размера $n\times n$, причём $a_{ij}\in\{0,1\}$ и $a_{ij}=1\Leftrightarrow(v_i,v_j)\in E(G)$. ***Матрица инцидентности*** – это матрица $\|b_{ij}\|$ размера $n\times m$, причём $b_{ij}\in\{0,1\}$ и $b_{ij}=1$ в том и только том случае, если вершина v_i инцидентна ребру e_j. Для обобщённых графов, а также ориентированных графов матрицы смежности и инцидентности определяются похожим образом.

Граф называется ***двудольным***, если множество V его вершин можно разбить на два непересекающиеся подмножества V_1 и V_2 такие, что $(V_1\times V_1)\cap E(G)=\varnothing$ и $(V_2\times V_2)\cap E(G)=\varnothing$.

Стандартные обозначения некоторых графов:

K_n или F_n (***полный граф***) – граф с n вершинами, в котором любые две вершины смежны;

C_n (***цепь***) – граф с вершинами $1,2,,\mathbf{K},n$ и рёбрами (1,2), (2,3), …, $(n-1,n)$;

Z_n (***цикл***) – граф с вершинами $1,2,,\mathbf{K},n$ и рёбрами (1,2), (2,3), …, $(n-1,n)$, $(n,1)$;

$K_{m,n}$ (***полный двудольный граф***) – граф, в котором $V(G)=V_1\cup V_2$, причём $V_1\cap V_2=\varnothing$ и $E(G)=V_1\times V_2$;

B_n (*n-мерный куб*) – граф, вершинами которого являются строчки $(e_1,\mathbf{K},e_n)$ из 0 и 1, причём две вершины смежны в том и только том случае, если строчки отличаются ровно одним элементом.

Прямое произведение $G\times H$ графов G и H – это граф, у которого $V(G\times H)=V(G)\times V(H)$, причём вершины (x,y) и (x',y') смежны в том и только том случае, если либо $x=x'$ и $(y,y')\in E(H)$, либо $y=y'$ и $(x,x')\in E(G)$.

Степень вершины графа (обозначается: $\deg v$, где $v\in V(G)$) – количество рёбер, инцидентных данной вершине. Известно, что $\sum\limits_{v\in V(G)}\deg v=2\text{P}$, где Р – количество рёбер графа. Вершина степени 0 называется ***изолированной***, а вершина степени 1 – ***висячей***.

Дополнением $\bar{G}$ графа G называется граф с тем же множеством вершин, что и G, причём две вершины смежны в $\bar{G}$ тогда и только тогда, когда они не смежны в G.

Упражнения

3.1. Изобразить граф с заданным множеством вершин и рёбер:

а) вершины – числа 1,2,3,4,5,6, рёбра – пары (i,j) такие, что Í Î Ä$(i,j)=1$;

б) вершины – грани куба, рёбра соединяют вершины графа, соответствующие смежным граням куба;

в) вершины – грани куба, рёбра соединяют вершины графа, соответствующие противоположным граням куба;

г) вершины – рёбра тетраэдра, рёбра соединяют вершины графа, соответствующие смежным рёбрам тетраэдра;

д) вершины – булевы функции от двух переменных, рёбра соединяют функции $f(x,y)$ и $g(x,y)$, если выполнено тождество $f(x,y)+g(x,y)=x$;

е) вершины – подмножества множества $\{a,b,c\}$, рёбра соединяют подмножества, имеющие пустое пересечение.

3.2. Какие из графов предыдущей задачи изоморфны друг другу?

3.3. Построить граф по его матрице смежности:

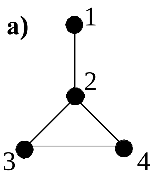
а) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$; **б)** $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$;

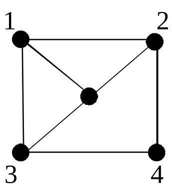
в) $\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$; **г)** $\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$.

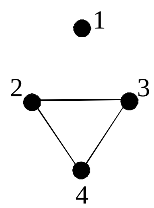
3.4. Построить граф по его матрице инцидентности:

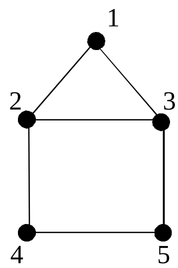
а) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$; **б)** $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$; **в)** $\begin{pmatrix}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

3.5. Построить матрицу смежности графа:

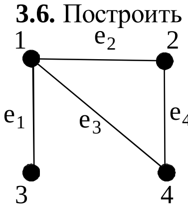
а)


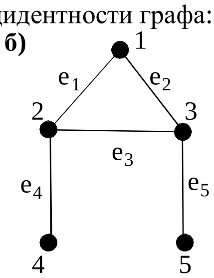
б)


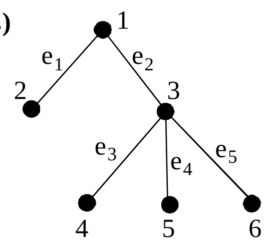
в)


г)


3.6. Построить матрицу инцидентности графа:

а)


б)


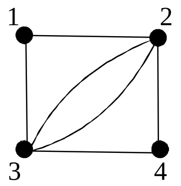
в)


3.7. Построить обобщённый граф по его матрице смежности:

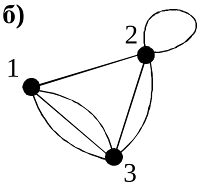
а) $\begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 1 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 3 & 1 & 0 \end{pmatrix}$; **б)** $\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$.

3.8. Построить матрицу смежности обобщённого графа:

а)



б)

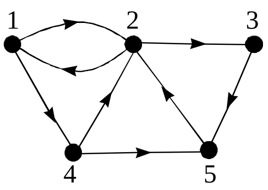


3.9. Построить ориентированный граф по его матрице смежности:

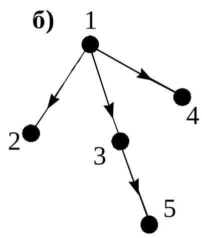
а) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$; **б)** $\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

3.10. Построить матрицу смежности ориентированного графа:

а)



б)



3.11. Изобразить графы:

а) $C_3 \times C_3$; **б)** $F_4 \times C_2$; **в)** $K_{3,4}$; **г)** $Z_3 \times Z_3$.

3.12. При каких a и b матрица $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ a & 1 & 0 & 1 \\ 0 & b & 1 & 0 \end{pmatrix}$ является матрицей смежности некоторого графа?

3.13. При каких a и b матрица $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ a & 0 & b & 1 & 0 \end{pmatrix}$ является матрицей инцидентности некоторого графа?

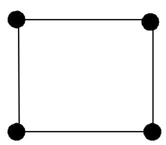
3.14. Дана матрица смежности $\|a_{ij}\|$ некоторого обобщённого графа. Найти количество петель в этом графе.

3.15. Сколько компонент связности имеет граф, заданный своей матрицей смежности:

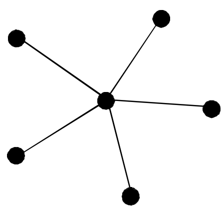
а) $\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$; **б)** $\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$; **в)** $\begin{pmatrix}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

3.16. Изобразить граф, являющийся дополнением к данному графу:

а)



б)



2. Пути и циклы. Связные графы. Компоненты связности. ***Путь*** в графе G – это последовательность рёбер вида (x_1, x_2), $(x_2, x_3), \ldots$, (x_{m-1}, x_m). *Простой путь* – путь, в котором вершины $x_1, x_2, \mathbf{K}, x_n$ различны. ***Цикл*** – путь, в котором начальная и конечная вершины совпадают. *Простой цикл* – цикл, в котором вершины $x_1, x_2, \mathbf{K}, x_{n-1}$ различны. Граф G называется ***связным***, если для любых двух вершин существует путь, их соединяющий. Любой граф G разбивается на связные подграфы $G_1, \mathbf{K}, G_k$, обладающие свойством: не существует рёбер, соединяющих вершины из различных подграфов G_i. Подграфы $G_1, \mathbf{K}, G_k$ называются ***компонентами связности*** графа G.

Эйлеров путь (***цикл***) – это путь (цикл), проходящий через все рёбра графа, причём каждое ребро проходится ровно один раз. Эйлеров путь в связном графе существует в том и только том случае, если ровно две вершины имеют нечётные степени, а остальные – чётные; эйлеров цикл существует тогда и только тогда, когда все вершины имеют чётные степени. ***Гамильтонов путь*** (***цикл***) – это путь (цикл), обходящий все вершины графа, причём каждая вершина проходится ровно один раз.

Расстоянием $d(a,b)$ между вершинами a и b графа G называется длина кратчайшего пути, соединяющего вершины a и b (напомним, что длина пути – это количество рёбер). Если не существует пути между a и b, то $d(a,b)=\infty$.

Диаметром $d(G)$ связного графа G называется наибольшее расстояние между вершинами этого графа: $d(G)=\max\{d(x,y)\,|\,x,y\in V(G)\}$. ***Радиусом*** $r(G)$ графа G назовём число $r(G)=\min\limits_x \max\limits_y d(x,y)$. Вершина a, для которой $r(G)=\max\limits_y d(y,a)$, называется ***центром*** графа G.

Упражнения

3.17. Каких графов на заданном множестве вершин V больше: связных или несвязных, если $|V|\geq 3$?

3.18. Сколько компонент связности имеет граф G, у которого $V(G)=\{1,2,\mathbf{K},100\}$, $E(G)=\{(i,j):|i-j|=3\}$?

3.19. Сколько всего неизоморфных графов, у которых:
а) 10 вершин и 3 ребра; **б)** 11 вершин и 53 ребра;
в) 13 вершин и 77 рёбер?

3.20. Доказать, что любой граф можно изобразить в трёхмерном пространстве так, чтобы рёбра являлись отрезками прямых и эти отрезки не имели общих внутренних точек.

3.21. Назовём ориентированный граф *бесконтурным*, если в нём нет замкнутых ориентированных путей (контуров). Доказать, что в бесконтурном графе можно так занумеровать вершины, что матрица смежности будет верхней треугольной.

3.22. Назовём ориентированный граф *сильно связным*, если для любых двух вершин a и b существует ориентированный путь из a в b. Верно ли, что в сильно связном графе существует простой ориентированный путь, обходящий все вершины?

3.23. В произвольном ориентированном графе G для вершин a и b положим $a\sim b$, если существуют пути из a в b и из b в a. Доказать, что $\sim$ – отношение эквивалентности (на множестве вершин), а подграфы, соответствующие классам эквивалентности, сильно связные (определение см. в предыдущей задаче). Они называются сильно связными компонентами графа. Обозначим через $\bar{G}$ граф, вершинами которого являются сильно связные компоненты графа G и из вершины $\bar{a}$ в вершину $\bar{b}$ ($\bar{a},\bar{b}\in V(\bar{G})$) идёт ребро в том и только том случае, если существуют вершины x,y графа G такие, что $x\in\bar{a}$, $y\in\bar{b}$ и $(x,y)\in E(G)$. Доказать, что граф $\bar{G}$ бесконтурный.

3.24. Доказать, что любые две цепи максимальной длины в связном неориентированном графе имеют хотя бы одну общую вершину.

3.25. Назовём *расстоянием* $d(a,b)$ между вершинами a и b графа G длину кратчайшего пути, соединяющего вершины a и b (напомним, что длина пути – это количество рёбер). Если не существует пути между a и b, то $d(a,b)=\infty$. Доказать, что расстояние $d(a,b)$ удовлетворяет аксиомам метрики, т.е.: (1) $d(a,b)\geq 0$, $d(a,b)=0 \Leftrightarrow a=b$. (2) $d(a,c)\leq d(a,b)+d(b,c)$, (3) $d(b,a)=d(a,b)$.

3.26. Найти расстояние (в смысле предыдущей задачи) между вершинами $(1,0,0,1,1)$ и $(0,1,0,1,0)$ 5-мерного куба B_5.

3.27. Написать формулу расстояния (в смысле теории графов) между вершинами $(\varepsilon_1,\varepsilon_2,\mathbf{K},\varepsilon_n)$ и $(\eta_1,\eta_2,\mathbf{K},\eta_n)$ n-мерного куба B_n (оно называется *расстоянием Хэмминга*).

3.28. Какие значения принимает расстояние (в смысле теории графов) между вершинами:
а) куба B_4; **б)** икосаэдра; **в)** додекаэдра;
г) графа $B_3\times B_4$; **д)** $C_5\times C_6$?

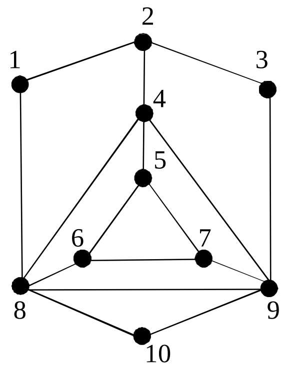
3.29. Назовём ***диаметром*** $d(G)$ связного графа G наибольшее расстояние между вершинами этого графа: $d(G)=\max\{d(x,y)\,|\,x,y\in V(G)\}$. Вычислить диаметры следующих графов:

а) K_n ; **б)** $K_{m,n}$ $(m,n \ge 2)$; **в)** $C_m \times C_n$; **г)** B_n ; **д)** G – октаэдр.

3.30. Верно ли, что диаметры графов обладают свойством $d(G \times H) = d(G) + d(H)$?

3.31. Найти диаметр графа G, заданного множеством вершин $V(G) = \{1, 2, 3, 4, 5, 6, 7, 8\}$ и множеством рёбер $E(G) = \{ (1,2), (1,4), (2,4), (2,5), (3,6), (4,7), (4,8), (5,6), (5,8) \}$.

3.32. ***Радиусом*** $r(G)$ графа G назовём число $r(G) = \min\limits_{x} \max\limits_{y} d(x, y)$. Вершину a, для которой $r(G) = \max\limits_{y} d(y, a)$, назовём ***центром*** графа G. Для графа, изображённого на рисунке, найти диаметр, радиус и все центры.



3.33. Найти радиусы следующих графов:

а) B_n ; **б)** K_n ; **в)** $K_{m,n}$ ($m \le n$).

3.34. Найти радиус и все центры графа: **а)** C_n ; **б)** Z_n .

3.35. Найти количество вершин и количество рёбер графа:

а) $B_3 \times B_3$; **б)** икосаэдра; **в)** $C_m \times Z_n$; **г)** $Z_m \times Z_n$.

3.36. Доказать, что $B_m \times B_n \cong B_{m+n}$.

3.37. Найти эйлеров путь в графе с вершинами $1, 2, 3, 4, 5$ и рёбрами $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(2,3)$, $(3,4)$, $(3,5)$, $(4,5)$.

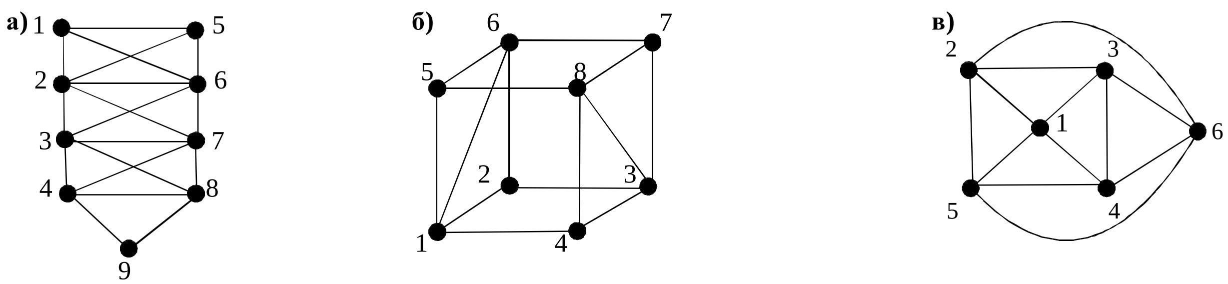
3.38. Существует ли эйлеров путь или эйлеров цикл в графе:

а) $K_{4,6}$; **б)** B_3 ; **в)** B_4 ; **г)** $C_m \times C_n$; **д)** додекаэдре?

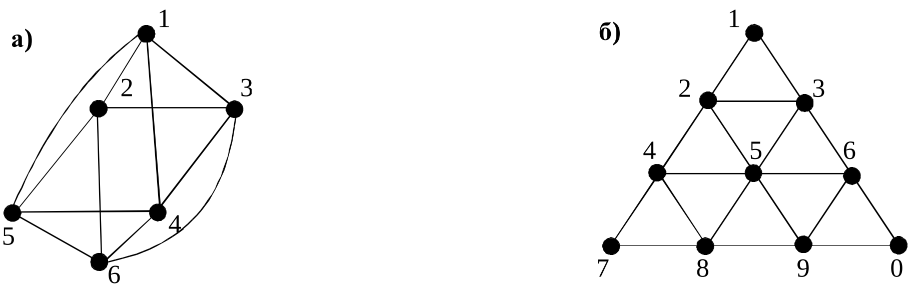
3.39. В каких графах вида $K_{m,n}$ существует:

а) эйлеров путь, **б)** эйлеров цикл?

3.40. Найти эйлеров путь в графе, изображённом на рисунке:



3.41. Найти эйлеров цикл графа, изображённого на рисунке:



3.42. Граф G задан множеством вершин и рёбер. Выяснить, имеет ли G гамильтонов путь или цикл:

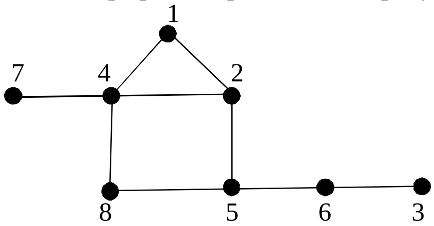
а) $V(G) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $E(G) = \{(1,3), (1,4), (2,3), (2,6), (3,4), (3,5), (4,8), (5,7), (6,7), (7,8), (8,9)\}$;

б) $V(G) = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $E(G) = \{(1,2), (1,7), (2,3), (2,4), (2,5), (3,6), (4,7), (5,6), (6,7), (6,8), (7,8)\}$.

3.43. В каких графах вида $K_{m,n}$ существует:

а) гамильтонов путь, **б)** гамильтонов цикл?

3.44. Доказать, что в графе, изображённом на рисунке, нет гамильтонова пути.



Какие рёбра следует добавить, чтобы в графе появился гамильтонов путь? Каково наименьшее число рёбер, добавление которых приведёт к существованию гамильтонова цикла?

3.45. Доказать, что если в графе есть вершина, после удаления которой граф распадается на 3 или более компонент связности, то у него не может быть гамильтонова пути или цикла.

3. Деревья. Кодирование деревьев. ***Деревом*** называется связный граф без циклов. Количество вершин В и количество рёбер Р любого дерева связаны соотношением $\text{Р} = \text{В} - 1$.

Каждому дереву, имеющему n рёбер, можно поставить в соответствие последовательность из 0 и 1 (***двоичный***, или ***бинарный код дерева***). В бинарном коде будет ровно m нулей и m единиц, где m – количество рёбер дерева. Построение бинарного кода осуществляется следующим образом: производится обход рёбер графа так, чтобы граф оставался всё время справа; при прохождении “нового” ребра (ребра, которое ещё не проходилось) пишем 0, при прохождении старого ребра пишем 1.

Ещё одним методом кодирования дерева является построение ***кода Прюфера*** (кода из натуральных чисел). Пронумеруем вершины дерева произвольным образом. Возьмём висячую вершину с наименьшим номером и запишем в код номер смежной с ней вершины; затем удалим висячую вершину вместе с ребром. Будем повторять этот процесс. В результате получим код Прюфера.

Упражнения

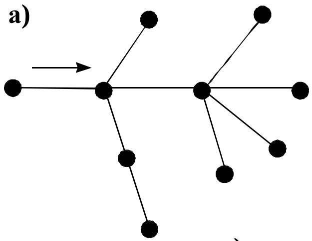
3.46. Сколько всего неизоморфных деревьев с 7 вершинами, из которых 3 висячие?

3.47. а) На окружности даны 4 точки. Эти точки соединяются отрезками прямых так, чтобы получилось дерево, но при этом никакие два отрезка не имеют общих внутренних точек. Сколько всего таких деревьев? Сколько из них неизоморфных?

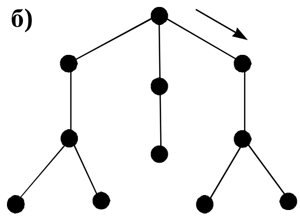
б) Решить аналогичную задачу для 5 точек.

3.48. Построить бинарный код дерева (направление обхода показано на рисунке):

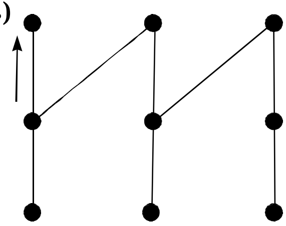
а)



б)



в)



3.49. Какие из следующих комбинаций цифр являются кодами дерева:

а) 00011010110111; **б)** 0000100111100111;

в) 00010111100110101; **г)** 000111001101001011?

3.50. Построить дерево по его бинарному коду:

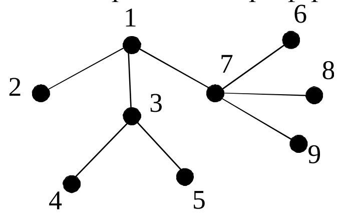
а) 00100101011011; **б)** 000110100000011011011111;

в) 001001010101011011.

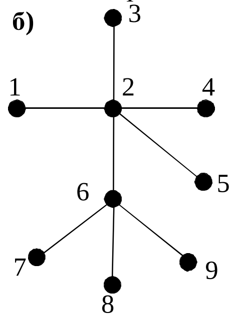
3.51. Доказать, что количество неизоморфных деревьев с n рёбрами не превосходит 4^n.

3.52. Построить код Прюфера дерева для заданной нумерации его вершин:

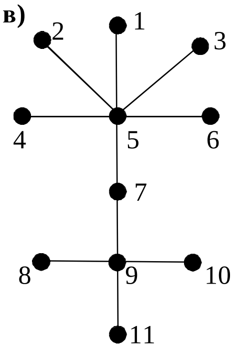
а)



б)



в)



3.53. Построить дерево по его коду Прюфера:

а) 1 4 1 4 7 4; **б)** 5 6 7 5 7 6 8 5 6 9;

в) 6 6 7 7 6 7 9 6 7 1 0.

4. Цикломатическое число графа. Пространство *циклов. Цикломатическим числом* графа G называется число $n(G) = \text{Р} - \text{В} + \text{К}$, где Р – количество рёбер, В – количество вершин, К – количество компонент связности. *Циклом* (в широком смысле) мы будем называть обычный цикл или объединение непересекающихся обычных циклов. Сложение циклов осуществляется путём удаления общих рёбер циклов и объединения оставшихся рёбер. При так определённом сложении все циклы будут образовывать линейное пространство над полем из двух элементов – *пространство циклов*. Оказывается, что размерность пространства циклов равна цикломатическому числу. Кроме того, если цикломатическое число графа равно k, то из графа можно удалить k рёбер (специальным образом подобранных) так, что циклов в нём не останется, а количество компонент связности останется прежним.

Лес – граф без циклов. Необходимое и достаточное условие того, чтобы граф G был лесом, – это равенство $n(G) = 0$.

Упражнения

3.54. Найти цикломатическое число графа:

а) B_4; **б)** $K_{m,n}$; **в)** $Z_m \times Z_n$.

3.55. Выяснить, существует ли граф со следующим набором степеней вершин:

а) 1, 1, 1, 1, 2, 2, 3, 3, 3; **б)** 1, 1, 1, 2, 2, 2, 3, 3, 3;

в) 1, 1, 2, 3, 3, 4, 4.

3.56. Найти цикломатическое число $\nu(G)$ графа G, если:

а) $G = K_5$; **б)** $G = K_{m,n}$; **в)** $G = B_4$;

г) $G = C_m \times C_n$; **д)** G – октаэдр; **е)** G – икосааэдр.

3.57. Пусть G_1, G_2, … , G_k – компоненты связности графа G. Доказать, что $\nu(G) = \sum_{i=1}^{k} \nu(G_i)$.

3.58. Дан связный граф G. Чему равно наименьшее натуральное число k такое, что удаление любых k рёбер делает граф несвязным?

3.59. Чему равно наименьшее натуральное число k такое, что в графе $K_{m,n}$ найдутся k рёбер, удаление которых сделает делает граф несвязным?

3.60. Сколько рёбер может быть у графа, имеющего 15 вершин и состоящего из 3 компонент связности?

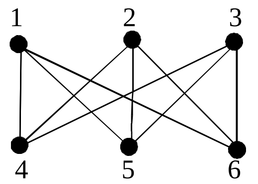
3.61. Сколько компонент связности может иметь граф, у которого 10 вершин и 30 рёбер?

3.62. Найти наибольшее количество рёбер, которое может иметь несвязный граф с n вершинами.

3.63. Доказать, что удаление ребра графа увеличивает количество компонент связности в том и только том случае, если это ребро не входит ни в один цикл.

3.64. Построить какой-нибудь базис пространства циклов графа, изображённого на рисунке

3.65. В графе $K_{3,3}$ взят цикл $C_1 = (1436)$.



Дополнить его до базиса пространства циклов.

3.66. Сколько циклов входит в базис пространства циклов графа G, у которого 15 вершин, 25 рёбер, 4 компоненты связности?

3.67. Чему равна размерность пространства циклов графа G и сколько в графе G всего обобщённых циклов, если:

а) $G = K_5$; **б)** $G = K_{10}$; **в)** $G = B_4$?

3.68. Найти количество компонент связности леса, имеющего:

а) 20 вершин и 10 рёбер; **б)** 25 вершин и 11 рёбер.

3.69. Сколько вершин может иметь лес, у которого 20 рёбер?

3.70. Доказать, что любое неодноэлементное дерево имеет не менее двух висячих вершин.

3.71. Сколько рёбер следует удалить из графа G, чтобы получилось дерево, если:

а) $G = K_8$; **б)** $G = K_{5,6}$; **в)** $G = Z_4 \times Z_4$?

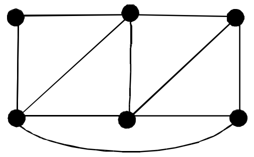
5. Раскрашивание графов. ***Хроматическим числом*** $c(G)$ графа G называется наименьшее число красок, необходимых для правильного раскрашивания вершин графа (при правильном раскрашивании смежные вершины должны быть окрашены в разные цвета). Граф G называется ***бихроматическим***, если $c(G) \le 2$. Оказывается, что для любого графа G эквивалентны условия: (1) G бихромаптический, (2) G двудольный, (3) G не имеет циклов нечётной длины.

Рёберным хроматическим числом $c_р(G)$ графа G называется наименьшее количество красок для правильного раскрашивания рёбер графа (при правильном раскрашивании смежные рёбра должны быть окрашены в разные цвета). Пусть $\Delta(G)=\max\limits_{v\in V(G)}\deg v$. Имеет место *теорема Визинга*: $\Delta(G)\le c_{\text{р}}(G)\le\Delta(G)+1$.

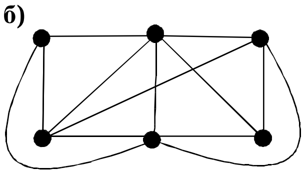
Упражнения

3.72. Найти хроматическое число $\chi(G)$ графа G, изображённого на рисунке

а)



б)



3.73. Найти хроматическое число $\chi(G)$ графа G:

а) $G=B_n$; **б)** $G=Z_n$; **в)** $G=K_{m,n}$; **г)** G – дерево.

3.74. Найти хроматическое число и привести пример правильной раскраски графа:
а) октаэдра; **б)** $K_4\times C_2$; **в)** $Z_3\times Z_3$.

3.75. Верно ли, что $\chi(G\times H)=\max(\chi(G),\chi(H))$?

3.76. Найти рёберное хроматическое число $\chi_{\text{Р}}(G)$ и указать какую-нибудь правильную раскраску рёбер графа: **а)** куба B_3; **б)** октаэдра, в котором проведена диагональ основания; **в)** додекаэдра.

3.77. Привести пример какого-нибудь графа G, у которого $\Delta(G)=3$, а $\chi_{\text{Р}}(G)=4$.

6. Планарность. Граф называется ***планарным***, если его можно изобразить на плоскости так, что рёбра не будут пересекаться во внутренних точках. Такое изображение называется ***плоской укладкой*** графа. Для связного планарного графа справедлива *теорема Эйлера*: $\text{В}+\Gamma=\text{Р}+2$, где В – число вершин графа, Р – число рёбер, Г – число ***граней***, т.е. областей, на которые граф разбивает плоскость. Связный планарный граф без висячих рёбер называется ***картой***. Карта имеет несколько ограниченных областей и одну неограниченную (называемую *океаном*). Каждой карте G можно поставить в соответствие ***сопряжённый граф*** G^* (вообще говоря, он может оказаться обобщённым графом, так как может иметь кратные рёбра). Сопряжённый граф строится следующим образом. В каждой грани карты выбираем по одной точке – это будут вершины графа G^*; две вершины будем соединять таким количеством рёбер, сколько общих рёбер имеют соответствующие грани. Количества вершин, рёбер и граней графов G и G^* связаны соотношениями $\text{В}^*=\Gamma$, $\text{Р}^*=\text{Р}$, $\Gamma^*=\text{В}$.

Операция разделения ребра для данного графа состоит в том, что внутри ребра берётся любая точка, объявляется новой вершиной графа, а данное ребро заменяется двумя другими. Графы G_1 и G_2 называются ***гомеоморфными***, если из них с помощью применения конечного числа раз операции разделения ребра можно получить изоморфные графы. Необходимое и достаточное условие планарности графа даёт *теорема Понтрягина – Куратовского*: граф планарен тогда и только тогда, когда у него нет подграфов, гомеоморфных графу K_5 или $K_{3,3}$.

Упражнения

3.78. Найти количество граней в плоской укладке связного планарного графа G, если:

а) G имеет 13 вершин и 34 ребра; **б)** $\nu(G)=5$?

3.79. Пусть G – связный связный планарный граф без висячих рёбер (такой граф называется *картой*). Пусть i – количество i-угольных граней в плоской укладке графа G. Доказать, что $\sum n_i = Ã,\ \sum i n_i = 2Ð \geq 2Â.$

3.80. Доказать, что если G – карта, то $\sum i n_i \geq (\min\limits_{v \in V(G)} \deg v) \cdot Â.$ В частности, если $\deg v \geq 3$ для всех $v \in V(G)$, то $\sum i n_i \geq 3Â.$

3.81. Пусть G – карта, в которой $\deg v \geq 3$ для всех $v \in V(G)$. Доказать, что $Ã \leq 2Â - 4.$

3.82. Сколько граней может быть в плоской укладке связного планарного графа с 10 вершинами, не являющегося деревом?

3.83. Каково минимальное число рёбер, которое может иметь непланарный граф?

3.84. Выяснить, является ли планарным граф: **а)** октаэдр; **б)** октаэдр, в котором добавлено ребро, соединяющее две противоположные вершины; **в)** граф K_5, из которого удалено ребро; **г)** $Z_3 \times C_3$; д) $Z_3 \times Z_3$; **е)** B_4; ж) граф K_6, из которого удалены три попарно смежных ребра.

3.85. При каких m, n граф $K_{m,n}$ является планарным?

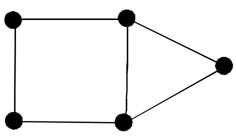
3.86. Связный планарный граф без петель, висячих вершин и кратных рёбер имеет 6 вершин. Сколько рёбер может иметь этот граф? Изобразить какой-нибудь граф с максимальным количеством рёбер.

3.87. Связный планарный обобщённый граф (т.е. допускаются кратные рёбра) без петель и висячих вершин имеет 16 рёбер. Сколько граней может быть в плоской укладке этого графа?

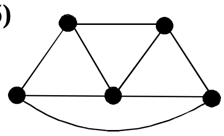
3.88. Связный планарный обычный граф без висячих вершин имеет 16 рёбер. Сколько граней может быть в плоской укладке этого графа? (Напомним, что обычный граф не имеет петель и кратных рёбер). Изобразить граф, удовлетворяющий условиям задачи и имеющий максимальное число граней.

3.89. Для графа, изображённого на рисунке, изобразить сопряжённый (обобщённый) граф:

а)



б)



7. Потоки в сетях. ***Сеть*** – это связный ориентированный граф, каждое ребро (x, y) которого помечено неотрицательным числом $c(x, y)$, называемым *пропускной способностью* ребра; кроме того, выделены две вершины: s (***источник***) и t (***сток***). ***Поток в сети*** – это совокупность действительных чисел $f(x, y)$, поставленных в соответствие рёбрам (x, y) сети, и числа v (***величины потока***), если выполнены условия:

(1) $0 \leq f(x, y) \leq c(x, y);$

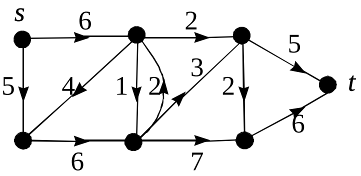
(2) $\sum\limits_x f(a, x) - \sum\limits_y f(y, a) = \begin{cases} v, & \text{если } a = s, \\ 0, & \text{если } a \neq s, t, \\ -v, & \text{если } a = t. \end{cases}$ Требуется найти поток, имеющий максимальную величину v.

Разрезом называется разбиение множества всех вершин N на два подмножества: $N = X \cup \bar{X}$ таких, что $s \in X$, $t \in \bar{X}$. Пропускной способностью разреза называется число $c(X, \bar{X}) = \sum\limits_{\substack{x \in X, \\ y \in \bar{X}}} c(x, y).$ Для любого разреза $(X, \bar{X})$ и любого потока имеет место неравенство $v \leq c(X, \bar{X})$. Таким образом, если мы найдём такой разрез $(X, \bar{X})$ и такой поток $\{f(x, y) \mid (x, y) \in E\}$, величина которого удовлетворяет условию $v = c(X, \bar{X})$, то поток будет максимальным. *Теорема Форда – Фалкерсона* утверждает, что такие поток и разрез существуют, *алгоритм Форда – Фалкерсона* позволяет построить максимальный поток. Доказательство максимальности потока обычно осуществляют с помощью разреза.

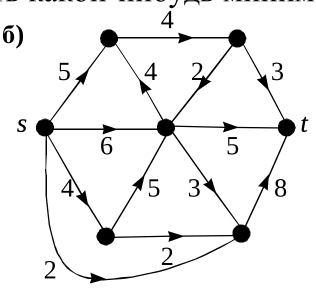
Упражнения

3.90. Найти максимальный поток сети, указать какой-нибудь минимальный разрез:

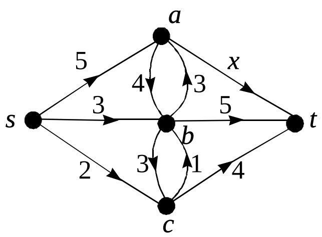
а)



б)



3.91. Какому условию должна удовлетворять пропускная способность ребра (a,t), чтобы величина максимального потока приняла наибольшее значение? Чему равно это значение?



4. Автоматы

1. Понятие конечного автомата. *Конечным автоматом* называется пятёрка $V=(A,Q,B,\varphi,\psi)$, где A,Q,B – конечные множества, а $\varphi:Q\times A\to Q$ и $\psi:Q\times A\to B$ – отображения. Отображение φ называется *функцией переходов*, а отображение ψ – *функцией выходов*. При этом равенство $\varphi(q,a)=q'$ означает, что если автомат V находится в данный момент времени в состоянии q и на его вход пришёл символ a, то к следующему моменту времени он перейдёт в состояние q'. Далее, равенство $\psi(q,a)=b$ означает, что если текущее состояние автомата есть q, а на вход поступил символ a, то на выход будет послан символ b.

Работа автомата описывается системой *канонических уравнений*:

$$\begin{cases} q(t+1)=\varphi\big(q(t),a(t)\big), \\ b(t)=\psi\big(q(t),a(t)\big), \end{cases}$$

которая должна быть дополнена начальным условием $q(0)=q_0$. Здесь $q(0)=q_0\in Q$ – *начальное*, или *инициальное* состояние.

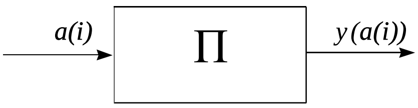
Замечания. 1. Автомат $V=(A,Q,B,\varphi,\psi)$, в котором выделено начальное состояние $q_0\in Q$, называют *инициальным автоматом*.

Иногда у автомата V выделяют одно или несколько состояний (скажем, $q_*\in Q$), называемых *конечными*, или *финальными* состояниями. Смысл их состоит в том, что если автомат «попадёт» в состояние q_*, то он прекращает свою работу.

Можно рассматривать *вероятностные*, или *стохастические* автоматы, т.е. такие, в которых переход из одного состояния в другое и формирование выходного символа осуществляются не по жёстко заданному правилу, а с некоторой вероятностью, закон распределения которой должен быть указан. В отличие от вероятностных автоматов обычные автоматы называют *детерминированными*.

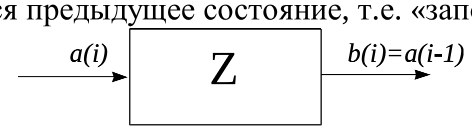
Многие утверждения, касающиеся автоматов, справедливы и без предположения о том, что A,B,Q – конечные множества. Назовём *абстрактным автоматом* пятёрку $V=(A,Q,B,\varphi,\psi)$, где функции φ и ψ определяются так же, как и раньше, т.е. $\varphi:Q\times A\to Q$, $\psi:Q\times A\to B$, но множества A,B,Q могут быть бесконечными.

Пример 1. *Автомат без памяти*. Таким автоматом называется автомат, в котором множество состояний состоит в точности из одного элемента. В этом случае функцию φ можно не рассматривать, а функция ψ зависит только от пришедшей на вход автомата буквы входного алфавита. Канонические уравнения автомата выглядят здесь так: $b(t)=\psi(a(t))$.



Так, в частности, работает автомат, который осуществляет перекодировку символов одного алфавита в другой (если при этом одна буква заменяется на одну).

Пример 2. *Элемент задержки*. Здесь входной и выходной алфавиты совпадают: $\grave{A}=\mathring{a}$, а выходной символ представляет собой задержанный на 1 такт входной символ: $b(t+1)=a(t)$ при всех $t\geq 0$. Пусть $Q=\{a_1,\dots a_n\}$. Тогда полагаем: $\varphi(q,a)=a\in Q$, $\psi(q,a)=q\in B$. Текущее состояние “запоминает” поступившую букву входного алфавита, а выходной буквой является предыдущее состояние, т.е. «запомненная» буква.



Автоматы $V=(A,Q,B,\varphi,\psi)$ называются *автоматами Мили*.

Автоматом Мура (автоматом без выхода) называется тройка $V=(A,Q,\varphi)$, где A,Q – множества, а $\varphi: Q\times A\to Q$ – отображение.

Множества A и Q называются соответственно входным алфавитом и множеством состояний. Функция φ называется функцией переходов. Равенство $\varphi(q,a)=q'$ означает, что если автомат находится в состоянии q и принимает символ a, то должен осуществиться его переход в состояние q'. В автомате Мили можно «избавиться» от выходного алфавита B, увеличив соответствующим образом множество состояний Q. Пусть дан автомат Мили $V=(A,Q,B,\varphi,\psi)$. Построим автомат Мура $V'=(A',Q',\varphi')$. В качестве множества состояний нового автомата возьмём $Q'=Q\times B$, входной алфавит сохраним прежним: $A'=A$, а функцию φ' определим следующим образом:

$$\varphi'(q',a)=\varphi'((q,b),a)=(\varphi(q,a),\psi(q,a)).$$

Автомат Мура $V'=(A',Q',\varphi')$ эквивалентен автомату Мили $V=(A,Q,B,\varphi,\psi)$ в том смысле, что V' «работает» так же, как V, но реакцией на входной сигнал является не выходной символ b, а изменённое более сложным образом состояние, в котором фактически “зашифрован” выходной символ b.

Диаграммой Мура автомата $V=(A,Q,B,\varphi,\psi)$ называется ориентированный граф, вершинами которого являются состояния $q\in Q$ и для каждого равенства вида $\varphi(a,q)=q'$ граф имеет ребро, идущее из q в q', на котором стоит метка a,b, где $b=\psi(q,a)$.

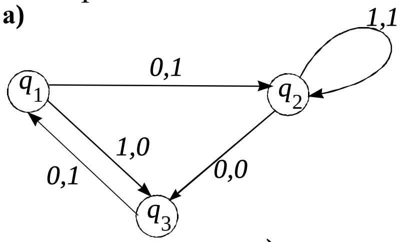
Из определения конечного автомата и диаграммы Мура следует, что ориентированный граф, рёбра которого помечены символами a,b $(a\in A, b\in B)$, является диаграммой Мура некоторого конечного автомата в том и только том случае, если из каждого состояния q_i выходило по одной стрелке для каждого символа $a\in A$.

Таблицей автомата $V=(A,Q,B,\varphi,\psi)$ называется прямоугольная таблица с $n=|Q|$ строками и $m=|A|$ столбцами, причём в клетке, стоящей на пересечении i-й строчки и j-го столбца написаны символы $\varphi(q_i,a_j)$ и $\psi(q_i,a_j)$.

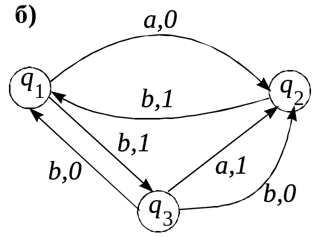
Упражнения

4.1. Выяснить, являются ли графы, изображённые на рисунке, диаграммами Мура некоторого автомата:

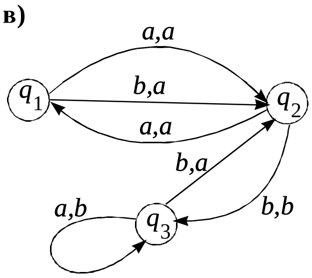
а)



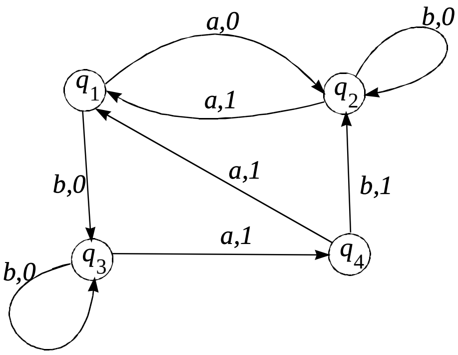
б)



в)



4.2. Построить таблицу автомата, заданного диаграммой Мура, изображённого на рисунке.



4.3. Автомат задан таблицей

	0	1	2
q_1	q_3 / 2	q_1 / 1	q_2 / 2
q_2	q_2 / 0	q_2 / 0	q_3 / 1
q_3	q_3 / 1	q_3 / 2	q_1 / 0

Построить диаграмму Мура этого автомата.

4.4. Автомат, у которого $Q=\{0,1,2\}$, $A=B=\{0,1\}$, задан каноническими уравнениями

$$\begin{cases} \varphi(q,a)=q+a \pmod 3, \\ \psi(q,a)=\begin{cases} a\,, & \text{åñëè } q<2, \\ 1-a, & \text{åñëè } q=2. \end{cases} \end{cases}$$

Построить диаграмму Мура этого автомата.

2. Продолжение функций переходов и выходов на слова. Пусть $A=\{a_1,a_2,\dots a_n\}$ – конечный алфавит. Через A^* будем обозначать множество всех слов $w=a_{i_1}a_{i_2}\dots a_{i_k}$. Число k называется *длиной* слова w и обозначается $|w|$. Например, если $A=\{a,b,c\}$, то $a, ab, babc\in A^*$, $|aba|=3$, $|c|=1$. Слово, в котором нет ни одной буквы, будем называть *пустым словом* и обозначать символом λ. Очевидно, $|\lambda|=0$. Пусть A^m – множество слов длины m, а A^+ – множество непустых слов. Тогда $A^+=A^*\setminus\{\lambda\}$, $A^*=\bigcup_{m=0}^{\infty}A^m$, $A^+=\bigcup_{m=1}^{\infty}A^m$.

Произведением слов $w,w'\in A^*$ называется слово, полученное приписыванием к слову w справа слова w'. Например, если $w=a_{i_1}a_{i_2}\dots a_{i_s}$, $w'=a_{j_1}a_{j_2}\dots a_{j_t}$, то $ww'=a_{i_1}a_{i_2}\dots a_{i_s}a_{j_1}a_{j_2}\dots a_{j_t}$. Произведение слов ассоциативно, т.е. $(w_1w_2)w_3=w_1(w_2w_3)$ для любых $w_1,w_2,w_3\in A^*$. Произведение слов *некоммутативно*, так как в общем случае $w_1w_2=w_2w_1$.

Множества A^* и A^+ являются полугруппами. Кроме того, A^* – моноид (т.е. полугруппа с единицей), пустое слово λ является единицей. Полугруппа A^+ моноидом не является.

Функции $\varphi: Q\times A\to Q$ и $\psi: Q\times A\to B$ продолжаются до функций $\overline{\varphi}: Q\times A^*\to Q$ и $\overline{\psi}: Q\times A^*\to B^*$ следующим образом: $\overline{\varphi}(q,a)=\varphi(q,a)$ при $a\in A$, $\overline{\varphi}(q,aw)=\overline{\varphi}(\varphi(q,a),w)$ при $a\in A$, $w\in A^+$; $\overline{\psi}(q,a)=\psi(q,a)$ при $a\in A$, $\overline{\psi}(q,aw)=\psi(q,a)\overline{\psi}(\varphi(q,a),w)$ при $a\in A$, $w\in A^+$; $\overline{\varphi}(q,\lambda)=q$, $\overline{\psi}(q,\lambda)=\lambda$.

Упражнения

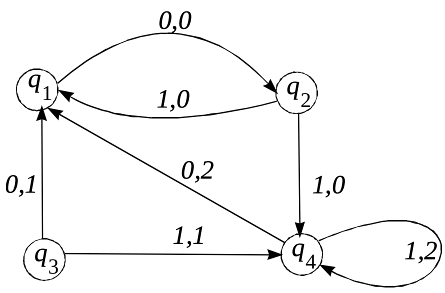
4.5. Автомат задан таблицей

	a	b	c
q_1	q_1 / 0	q_2 / 0	q_2

			1
q_2	q_1 0	q_1 1	q_2 1

Определить: $\overline{\varphi}(q_1, ab)$, $\overline{\varphi}(q_2, abc)$, $\overline{\varphi}(q_1, abca)$, $\overline{\psi}(q_1, ba)$, $\overline{\psi}(q_2, a^3b^2)$.

4.6. Автомат задан диаграммой Мура, изображённой на рисунке. Найти $\overline{\varphi}(q_1, 001)$, $\overline{\psi}(q_3, 110)$.



3. Приведенный автомат. Назовём состояния q и q' автомата $V = (A, Q, B, \varphi, \psi)$ *неотличимыми*, если $\overline{\psi}(q, w) = \overline{\psi}(q', w)$ для всех $w \in A^+$. Состояния q и q' *отличимы*, если $\overline{\psi}(q, w) \neq \overline{\psi}(q', w)$ при некотором $w \in A^+$. Положим $q \sim q'$, если q и q' неотличимы. Отношение неотличимости $\sim$ на множестве Q состояний автомата V является отношением эквивалентности. Это отношение вызывает разбиение множества Q на непересекающиеся классы эквивалентности: $Q = Q_1 \cup Q_2 \cup \ldots \cup Q_k$. Множество классов отношения ~ (фактор-множество $Q/\sim$) обозначим через $\hat{Q}$. Построим новый автомат $\hat{V}$. В качестве входного и выходного алфавитов автомата $\hat{V}$ возьмём те же множества A и B, которые были у автомата V, а в качестве множества состояний возьмём множество $\hat{Q}$. Определим функции $\hat{\varphi}: \hat{Q} \times A \to \hat{Q}$ и $\hat{\psi}: \hat{Q} \times A \to B$. Пусть $\hat{q} \in \hat{Q}$, $a \in A$. Возьмём какой-нибудь элемент q, принадлежащий классу $\hat{q}$, и положим $\hat{\varphi}(\hat{q}, a) = \widehat{\varphi(q, a)}$. Это определение *корректно*, т.е. не зависимо от выбора представителя в классе эквивалентности. Другими словами, если $q \sim q'$, то $\varphi(q, a) \sim \varphi(q', a)$. Функцию $\hat{\psi}$ определим на $\hat{Q}$ по формуле $\hat{\psi}(\hat{q}, a) = \psi(q, a)$. Это определение также корректно. Автомат $\hat{V} = (A, \hat{Q}, B, \hat{\varphi}, \hat{\psi})$ называется *приведённым автоматом*, соответствующим автомату $V = (A, Q, B, \varphi, \psi)$.

У приведённого автомата любые два различных состояния отличимы друг от друга.

Автомат $V = (A, Q, B, \varphi, \psi)$ и приведённый автомат $\hat{V} = (A, \hat{Q}, B, \hat{\varphi}, \hat{\psi})$ работают одинаково: для любой входной последовательности $a(1)a(2)a(3)\ldots$ последовательность $b(1)b(2)b(3)\ldots$ на выходе автомата V и автомата $\hat{V}$ одна и та же: $b(1) = \psi(q, a(1)) = \hat{\psi}(\hat{q}, a(1))$, $b(2) = \psi(q, a(1)a(2)) = \hat{\psi}(\hat{q}, a(1)a(2))$ и т.д. (здесь q – начальное состояние).

Теорема. Если входная последовательность конечного автомата является периодической, то выходная последовательность также периодическая, период которой не превышает $n\tau$, где τ – период выходной последовательности, а $n = |Q|$ – количество состояний автомата.

Отличимость состояний конечного автомата устанавливают обычно с помощью *тестирования*. А именно, если автомат, находясь в состоянии q и находясь в состоянии q', будет по-разному реагировать на одну и ту же входную последовательность, то состояния q и q' отличимы. Естественно возникает вопрос: сколько тестовых последовательностей и каких достаточно для установления неотличимости двух состояний? Ответ даёт ***первая теорема Мура***: если n – количество состояний автомата, то для установления отличимости или неотличимости его состояний достаточно подавать на вход последовательности длины $n-1$. Для двух автоматов V и V', имеющих одинаковые входные и одинаковые выходные алфавиты, справедлива ***вторая теорема Мура***: для отличимости или неотличимости состояний q и q' этих автоматов достаточно ограничиться входными последовательностями длины $n+n'-1$, где n и n' – количества состояний автоматов V и V'.

Приведём теперь пример, показывающий, что для установления отличимости состояний автомата $V=(A,Q,B,\varphi,\psi)$ с $|Q|=n$ может оказаться недостаточно брать последовательности длины $n-2$, т.е. число $n-1$ в формулировке первой теоремы Мура не может быть уменьшено.

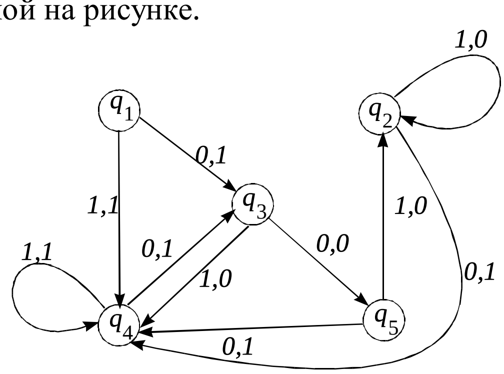
Пример 3. Рассмотрим автомат, представленный следующей таблицей:

	q_1	q_2	q_3	…	q_{n-1}	q_n
0	q_2 / 1	q_3 / 0	q_4 / 0	…	q_n / 0	q_n / 0
1	q_2 / 1	q_1 / 0	q_2 / 0	…	q_{n-2} / 0	q_{n-1} / 0

Состояния q_n и q_{n-1} отличимы словом $\underbrace{11\ldots1}_{n-1}$. Действительно, $\overline{\psi}(q_n,\underbrace{11\ldots1}_{n-1})=\underbrace{00\ldots0}_{n-1}$, а $\overline{\psi}(q_{n-1},\underbrace{11\ldots1}_{n-1})=\underbrace{0\ldots0}_{n-1}1$. В то же время слова длины $n-2$ эти состояния не отличают, так как если $\varepsilon_1,\ldots,\varepsilon_{n-2}\in\{0,1\}$, то $\overline{\psi}(q_n,\varepsilon_1\ldots\varepsilon_{n-2})=\overline{\psi}(q_{n-1},\varepsilon_1\ldots\varepsilon_{n-2})=\underbrace{00\ldots0}_{n-2}$.

Упражнения

4.7. Построить приведённый автомат для автомата, заданного диаграммой Мура, изображённой на рисунке.



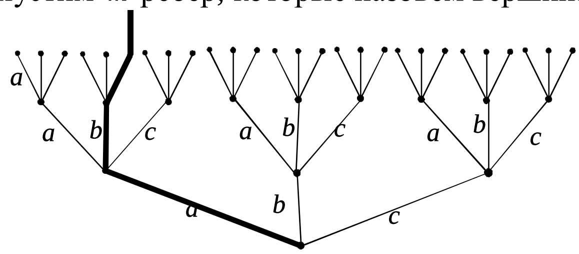
4.8. Построить приведённый автомат для автомата V, заданного следующей таблицей:

	q_1	q_2	q_3	q_4	q_5
0	q_3 / 1	q_1 / 1	q_4 / 0	q_1 / 1	q_1 / 1
1	q_4 / 1	q_5 / 0	q_3 / 1	q_4 / 0	q_4 / 0

4. Детерминированные и ограниченно-детерминированные функции. Пусть A – множество. Каждую бесконечную последовательность $a(1)a(2)a(3)\ldots$, где $a(i)\in A$, будем называть *сверхсловом*. Обозначим через A^∞ множество всех таких сверхслов. Пусть A, B – два конечных множества, их мы будем называть алфавитами. Рассмотрим отображение $f: A^\infty\to B^\infty$. Это отображение можно интерпретировать как воображаемое устройство, перерабатывающее сверхслова в алфавите A в сверхслова в алфавите B.

Функция $f: A^{\infty} \to B^{\infty}$ называется *детерминированной*, если выполнено условие: для любого i и для любых сверхслов $w = a(1)a(2)a(3)\ldots$, $w' = a'(1)a'(2)a'(3)\ldots$, если $f(w) = b(1)b(2)b(3)\ldots$, $f(w') = b'(1)b'(2)b'(3)\ldots$ и $a(1) = a'(1), \ldots, a(i) = a'(i)$, то $b(i) = b'(i)$.

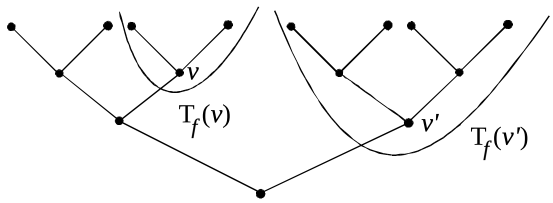
С множеством A^{∞} можно связать некоторое бесконечное дерево T. Пусть $A = \{a_1, a_2, \ldots, a_m\}$. Возьмём любую точку и назовём её *корнем* дерева. Из корня выпустим m рёбер, концы которых назовём вершинами первого яруса. Из каждой вершины первого яруса выпустим m рёбер, которые назовём вершинами второго яруса.



Ветви дерева T (бесконечные) соответствуют сверхсловам $a(1)a(2)a(3)\ldots \in A^{\infty}$, причём это соответствие взаимно однозначное. Будем считать, что рёбра, соответствующие буквам алфавита $A = \{a_1, a_2, \ldots, a_m\}$, идут слева направо (т.е. крайнее левое ребро соответствует букве a_1, следующее – букве a_2, крайнее правое – букве a_m). На рисунке изображено дерево, построенное для трёхбуквенного алфавита $A = \{a, b, c\}$. Ветвь дерева, отмеченная жирной линией, соответствует сверхслову $abcb\ldots$, а ветвь, отмеченная пунктирной линией, – сверхслову $bcbb\ldots$

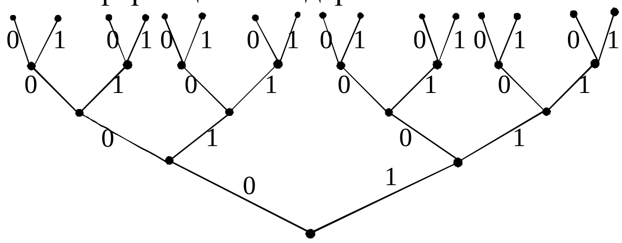
Пусть дана детерминированная функция $f: A^{\infty} \to B^{\infty}$. Построим дерево T, соответствующее множеству A^{∞}, и пометим его рёбра буквами алфавита B, как будет показано ниже. Рассмотрим произвольное сверхслово $w = a(1)a(2)a(3)\ldots \in A^{\infty}$. Пусть $f(w) = b(1)b(2)b(3)\ldots$ Рассмотрим ветвь дерева T, соответствующую сверхслову w, и пометим рёбра этой ветви символами $b(1), b(2), b(3), \ldots$ Так поступим с каждой ветвью. Если у двух сверхслов $w = a(1)a(2)a(3)\ldots$ и $w' = a'(1)a'(2)a'(3)\ldots$ совпадут первые k букв: $a(1) = a'(1)$, $\ldots, a(k) = a'(k)$, то ввиду детерминированности функции f у сверхслов $f(w)$ и $f(w')$ также будут совпадать первые k букв. Следовательно, в процессе расстановки пометок на рёбрах мы не получим противоречия (т.е. каждое ребро дерева T получит ровно одну пометку). Дерево T, рёбра которого помечены вышеописанным способом, назовём *информационным деревом*, соответствующим функции f, и обозначим его T_f. Наоборот, если дано дерево T для A^{∞}, то, пометив его рёбра буквами из B произвольным образом, мы получим информационное дерево, соответствующее некоторой функции f. Это соответствие между информационными деревьями и детерминированными функциями является взаимно однозначным. Детерминированность функции $f: A^{\infty} \to B^{\infty}$ является необходимым условием реализуемости функции f некоторым автоматическим устройством. Но она не является достаточным условием. Причина в том, что всякое механическое устройство имеет конечную память (т.е. может хранить лишь ограниченное количество единиц информации).

Пусть дано информационное дерево T_f, соответствующее детерминированной функции f. Для любой вершины v этого дерева пусть $T_f(v)$ обозначает поддерево, корнем которого является вершина v (оно состоит из вершины v и всех вершин и рёбер, идущих «после» v, вместе с пометками на этих рёбрах).



Введём отношение эквивалентности ~ на множестве вершин дерева T_f, полагая $v \sim v'$, если у деревьев $T_f(v)$ и $T_f(v')$ соответствующие друг другу рёбра имеют одинаковые пометки. Детерминированная функция $f: A^\infty \to B^\infty$ называется *ограниченно детерминированной* (или *о.д.-функцией*), если множество вершин информационного дерева T_f разбивается на конечное число ~-классов.

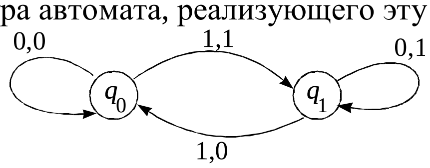
Пример 4. Пусть функция $f: \{0,1\}^\infty \to \{0,1\}^\infty$ определяется правилом $f(a(1)a(2)a(3)\ldots) = a(1),\, a(1)+a(2),\, a(1)+a(2)+a(3), \ldots$ (здесь + обозначает сложение по модулю 2). Изобразим информационное дерево.



Функция f является ограниченно детерминированной, так как всего два класса эквивалентности.

Теорема. Ограниченно детерминированные функции $f: A^\infty \to B^\infty$ и только они являются *автоматными*, т.е. реализуются некоторым конечным автоматом. При этом A является входным алфавитом автомата, а B – выходным.

Пример 5. Пусть $A = B = \{0,1\}$ и $f: A^\infty \to B^\infty$ – функция, определяемая равенством $b(i) = a(1) + a(2) + \ldots + a(i)$ (эта функция была рассмотрена перед теоремой). Ранее мы видели, что функция f в этом примере является ограниченно детерминированной, так как дерево T_f имеет два класса эквивалентности. Обозначив эти классы через q_0 и q_1, получим диаграмму Мура автомата, реализующего эту функцию.



Упражнения

4.9. Выяснить, какие из следующих функций $f: A^\infty \to B^\infty$ являются детерминированными:

а) $A = B = \{0,1\}$, $a(1)a(2)a(3)\ldots \xrightarrow{f} a(1)a(1)a(2)a(3)a(4)\ldots$;

б) $A = B = \{0,1\}$, $a(1)a(2)a(3)\ldots \xrightarrow{f} a(2)a(3)a(4)\ldots$;

в) $A = B = \{0,1\}$, $a(1)a(2)a(3)\ldots \xrightarrow{f} 0a(2)0a(4)0a(6)\ldots$;

г) $A = B = \{0,1\}$,

$$f(a(1)a(2)a(3)\ldots) = \begin{cases} 1\ 1\ 1\ldots, \text{åñëè } a(i) = 0 \text{ äëÿ âñåõ } i, \\ a(1)a(2)a(3)\ldots \text{ â ïðîòèâíîì ñëó÷àå.} \end{cases}$$

4.10. Выяснить, какие из следующих функций $f: A^\infty \to B^\infty$ являются ограниченно детерминированными:

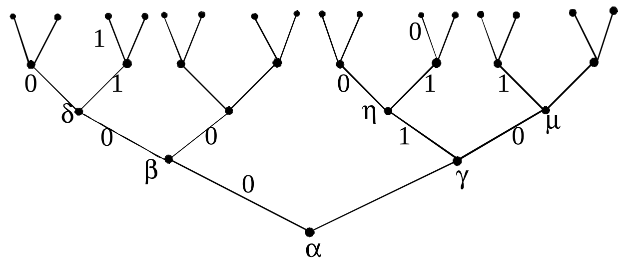
а) $A = B = \{0,1\},\quad a(1)a(2)a(3)\ldots \xrightarrow{f} 0\,a(1)a(2)a(3)\ldots;$

б) $A = B = \{a,b,c\},$

$$b(1) = a(1),\quad b(i) = \begin{cases} a(i), & \text{åñëè } a(i-1) = a, \\ b, & \text{åñëè } a(i) = c, \\ c, & \text{åñëè } a(i) = a \end{cases} \qquad (i \ge 2);$$

в) $A = B = \{0,1\},\quad f : a(1)a(2)a(3)\ldots \to a(1)a(1)a(2)a(2)a(3)a(3)\ldots$

4.11. На рисунке изображён фрагмент информационного дерева некоторой о.д.-функции. Каково наименьшее возможное число классов эквивалентности вершин этого дерева?



4.12. Выяснить, какие из следующих функций $f : A^{\infty} \to B^{\infty}$ являются детерминированными:

а) $A = \{0,1\},\quad B = \{a,b,c\},$

$$b(1) = a,\quad b(i) = \begin{cases} a, \text{ åñëè } a(i) = a(i-1) = 0, \\ b, \text{ åñëè } a(i) = a(i-1) = 1, \\ c, \text{ åñëè } a(i) \ne a(i-1); \end{cases}$$

б) $A = B = \{0,1\},\quad f(a(1)a(2)a(3)\ldots) = 0\,a(1)\,0\,a(2)\,0\,a(3)\ldots;$

в) $A = B = \{0,1\},$

$$f(a(1)a(2)a(3)\ldots) = \begin{cases} a(1)a(2)a(3)\ldots, \text{ åñëè } a(i) = 0 \text{ ïðè âñåõ ÷,òíûõ } i, \\ 0\,a(2)\,0\,a(4)\,0\ldots \text{ â ïðîòèâíîì ñëó÷àå.} \end{cases}$$

4.13. Выяснить, какие из следующих функций $f : A^{\infty} \to B^{\infty}$ являются ограниченно детерминированными:

а) $A = B = \{a,b,c\},\quad f(a(1)a(2)a(3)\ldots) = a\,b\,c\,a(1)a(2)a(3)\ldots;$

б) $A = B = \{0,1\},\quad a(1)a(2)a(3)\ldots \xrightarrow{f} 0\,a(1)\,0\,a(2)\,0\,a(3)\ldots;$

в) $A = B = \{a,b,c\},\quad b(i) = \begin{cases} a(i), \text{ åñëè } \forall j \le i \;\; a(j) \ne c, \\ c, \quad \text{åñëè } \exists j \le i \;\; a(j) = c. \end{cases}$

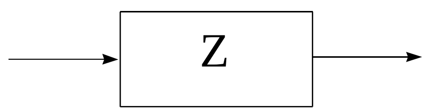
Определить количество классов эквивалентности множества вершин дерева T_f следующих функций:

а) $A = \{0,1\},\quad B = \{0,1,2\},\quad b(i) = a(1) + a(2) + \ldots + a(i) \pmod 3;$

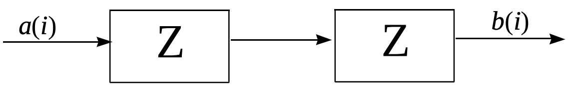
б) $A = B = \{0,1\},\quad f(a(1)a(2)a(3)\ldots) = 0\,0\,a(1)a(2)a(3)\ldots;$

в) $A = \{a,b,c\},\quad B = \{0,1\},\quad b(i) = \begin{cases} 0, \text{ åñëè } i = 1 \text{ èëè } a(i) \ne a(i-1), \\ 1 \text{ â ïðîòèâíîì ñëó÷àå.} \end{cases}$

5. Синтез автоматов. Под *синтезом автоматов* понимают построение автоматов, удовлетворяющих заданному свойству или выполняющих заданные функции. Ранее был построен элемент задержки, который сдвигает входную последовательность на один такт: $b(i) = a(i-1)$ при $i \ge 2$.

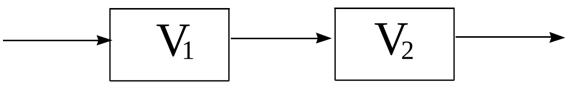


Соединяя последовательно два элемента задержки,



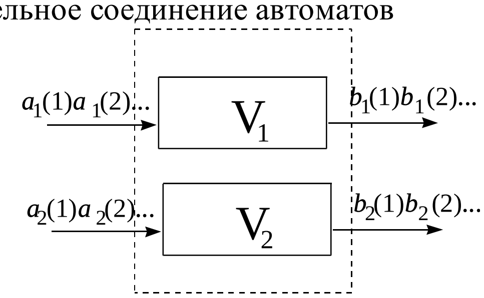
мы получим сдвиг на два такта: $b(i) = a(i-2)$ при $i \geq 3$.

Автоматы $V_1 = (A_1, Q_1, B_1, \varphi_1, \psi_1)$ и $V_2 = (A_2, Q_2, B_2, \varphi_2, \psi_2)$ можно соединять последовательно.



в случае, если $B_1 \subseteq A_2$. При этом получается автомат $V = (A, Q, B, \varphi, \psi)$, у которого $A = A_1$, $B = B_2$, $Q = Q_1 \times Q_2$, $\varphi((q_1, q_2), a) = (\varphi_1(a, q_1), \varphi_2(\psi_1(a, q_1), q_2))$, $\psi((q_1, q_2), a) = \psi_2(\varphi_1(a, q_1), q_2)$.

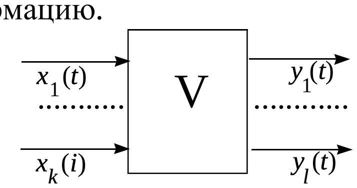
Параллельное соединение автоматов



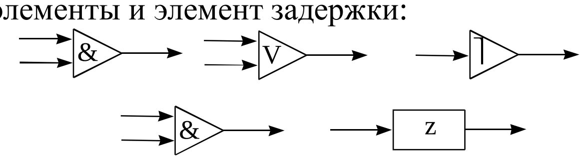
приводит к появлению автомата $V = (A_1 \times A_2, Q_1 \times Q_2, B_1 \times B_2, \varphi, \psi)$, где

$$\varphi((q_1, q_2), (a_1, a_2)) = (\varphi_1(q_1, a_1), \varphi_2(q_2, a_2)), \quad \psi((q_1, q_2), (a_1, a_2)) = (\psi_1(q_1, a_1), \psi_2(q_2, a_2)).$$

Пусть $V = (A, Q, B, \varphi, \psi)$ – конечный автомат. Если $A = \{a_1, a_2, \ldots, a_m\}$ и $m \leq 2^k$, то входной символ a можно закодировать двоичной последовательностью длины k, а именно: $a_1 \to \underbrace{00\ldots0}_{k}$, $a_2 \to \underbrace{00\ldots1}_{k}$, $a_3 \to \underbrace{00\ldots10}_{k}$ и т.д. Аналогично, если $B = \{b_1, \ldots, b_n\}$ и $n \leq 2^l$, то выходные символы $b \in B$ могут быть представлены двоичными последовательностями длины l. Автомат V, таким образом, становится устройством, перерабатывающим двоичную информацию.



Выходы $y_j(t)$ представляют собой булевы функции от входов $x_1(i), \ldots, x_k(i)$, где $i = t, t-1, \ldots$ Эти функции можно реализовать с помощью схем, содержащих стандартные булевы элементы и элемент задержки:



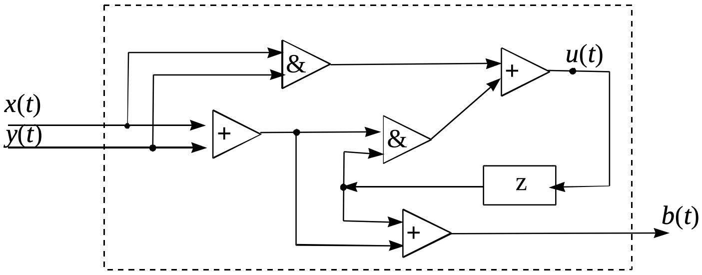
Пример 4. Рассмотрим устройство, осуществляющее сложение двух двоичных последовательностей с переносом разряда. Например,

$x(t)$	0	1	0	0	1	0	1	1	0	1	0	...
$y(t)$	1	0	1	1	1	0	1	0	1	1	0	...
$b(t)$	1	1	1	1	0	1	1	0	0	1	1	...

Таким образом, $b(t)=\begin{cases} x(t)+y(t), & \text{åñëè í å áûëî ï åðåï îëí åí èÿ,} \\ x(t)+y(t)+1 & \text{â ï ðî òèâí îì ñëó÷àå.} \end{cases}$

Положим $u(t)=\begin{cases} 1, \text{ åñëè åñòü ï åðåï îëí åí èå,} \\ 0, \text{ åñëè åñòü.} \end{cases}$

Тогда $b(t)=x(t)+y(t)+u(t-1)$, $u(t)=0$, если среди чисел $x(t)$, $y(t)$, $u(t-1)$ не более одного равны 1, $u(t)=1$ в противном случае. Нетрудно видеть, что $u(t)=x(t)y(t)+(x(t)+y(t))u(t-1)$. Теперь мы можем изобразить схему устройства.



Упражнения

4.15. Дан алфавит $A=\{a,b,c\}$. Построить автомат, отыскивающий во входной последовательности подслово abc и заменяющий после этого все символы символом $*$. Например, $ababbcacbabcabba... \to ababbcacbabc****...$

4.16. Выяснить, существует ли конечный автомат V с алфавитами $A=B=\{0,1\}$ такой, что:

а) $\psi(q_0,011)=101$, $\psi(q_0,110)=000$, $\psi(q_0,010)=111$?

б) $\psi(q_0,011)=101$, $\psi(q_0,110)=000$, $\psi(q_0,010)=100$?

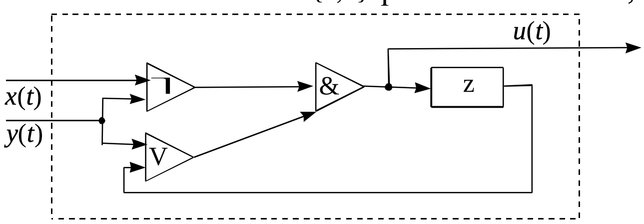
4.17. Построить автомат с наименьшим числом состояний, для которого $A=B=\{0,1\}$, $\psi(q_0,010)=110$, $\psi(q_0,0111)=1110$, $\psi(q_0,11)=00$.

4.18. Построить автомат с входным и выходным алфавитами $A=\{a,b,c\}$ и $B=\{\_,a,b,c,*\}$, который отыскивает во входной последовательности идущие подряд более одного раза буквы a и заменяет последнюю из них символом $*$. Символ _ зарезервирован здесь для начала последовательности. Пример: $abbcaabcacaaabc... \to \_\,abbca*bcacaa*bc...$

4.19. Построить диаграмму Мура автомата с $A=B=\{0,1\}$, который во входной последовательности заменяет символы, стоящие на чётных местах, на противоположные. Например, $01100101001110... \to 00110000011011...$

4.20. Построить таблицу автомата с наименьшим числом состояний, удовлетворяющий условиям: $\psi(q_0,011)=111$, $\psi(q_0,1011)=1101$, $\psi(q_0,11)=10$.

4.21. Автомат V с $A=B=\{0,1\}$ работает по схеме, показанной на рисунке.



При этом считается, что $u(0)=0$.

а) Выразить $u(t)$ через $x(t)$, $y(t)$, $u(t-1)$.

б) Найти первые 3 символа в выходной последовательности, если $x(1)x(2)x(3)\ldots = 100\ldots$, $y(1)y(2)y(3)\ldots = 011\ldots$

6. Алгебраический подход к теории автоматов. Алгебраический подход к теории автоматов предполагает рассмотрение автоматов без выхода, т.е. троек $V=(A,Q,\varphi)$, где $\varphi: Q\times A\to Q$ – функция переходов. В упрощённой записи пишем qw вместо $\varphi(q,w)$ для $w\in A^*$. При этом $q\lambda = q$, если λ – пустое слово. Произведение элемента из Q на элемент из A^* лежит в Q, поэтому мы можем говорить о *действии полугруппы* A^* *на множестве* Q. А именно, если $q'=qx$, где $x\in A^*$, то считаем, что элемент x переводит q в q'.

Автоматы $V=(A,Q,\varphi)$ и $V'=(A',Q',\varphi')$ называются *изоморфными* (записывается: $V\cong V'$), если существует взаимно однозначное отображение $\sigma: Q\to Q'$ такое, что $\sigma(qa)=\sigma(q)a$ для всех $q\in Q$, $a\in A$. *Гомоморфизм* автоматов $V=(A,Q,\varphi)$ и $V'=(A,Q',\varphi')$ над одним алфавитом A – это отображение $\sigma: Q\to Q'$ (не обязательно взаимно однозначное) такое, что $\sigma(qa)=\sigma(q)a$ для всех $q\in Q$, $a\in A$. Понятие *подавтомата* автомата $V=(A,Q,\varphi)$ обычно определяется одним из следующих способов: а) подавтоматом является непустое подмножество $X\subseteq Q$ такое, что $XA\subseteq A$; б) подавтомат – это тройка (A_1,Q_1,φ_1), где A_1 – непустое подмножество множества A, а Q_1 – непустое подмножество множества Q такие, что $Q_1A_1\subseteq Q_1$. Определение б) является более общим, а при $A=A_1$ они совпадают.

Отношение эквивалентности ρ на множестве Q называется *конгруэнцией* автомата $V=(A,Q,\varphi)$, если $q\,\rho\, q' \Rightarrow (qa)\,\rho\,(q'a)$ для всех $q,q'\in Q$. Класс эквивалентности конгруэнции ρ, в котором лежит элемент $q\in Q$, обозначим $[q]$. Множество всех классов эквивалентности (фактор-множество) обозначим Q/ρ. Определим действие букв из A на элементы множества Q/ρ, полагая $[q]a=[qa]$ для $q\in Q$, $a\in A$. Несложно проверяется *корректность* этого определения)т.е. независимость от выбора представителя в классе эквивалентности) и определяется отображение $\Phi: Q/\rho\times A\to Q/\rho$ (очевидно, $\Phi([q],a)=[qa]$). Автомат $W=(A,Q/\rho,\Phi)$ называется *фактор-автоматом* автомата V по конгруэнции ρ и обозначается $W=V/\rho$. В частности, приведённый автомат $\tilde{V}$, рассмотренный ранее, является фактор-автоматом автомата V.

Понятие автомата тесно связано с понятием *полигона над полугруппой*. Пусть S – полугруппа и X – множество. Будем говорить, что X – полигон над S, если определено отображение $X\times S\to X$, удовлетворяющее условию $(xs)t=x(st)$ при всех $x\in X$, $s,t\in S$. Всякий автомат $V=(A,Q,\varphi)$ можно рассматривать как полигон (а именно, полигон над полугруппой A^*). Наоборот, если X – полигон над полугруппой S, то X можно рассматривать как автомат, причём превращение X в автомат далеко не единственно. Один из способов (вообще говоря, неэкономный) состоит в том, что S рассматривается как входной алфавит, а $\varphi(x,s)=xs$ – функция переходов.

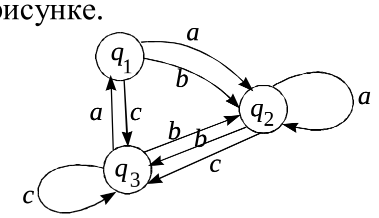
Пусть $V=(A,Q,\varphi)$ – абстрактный автомат (не обязательно конечный). Для каждого $w\in A^*$ рассмотрим отображение $f_w: Q\to Q$, определяемое по формуле $f_w(q)=qw$. Множество всех отображений f_w, где $w\in A^*$, образуют полугруппу. Действительно, $(f_w\circ f_{w'})(q)=f_{w'}(f_w(q))=(qw)w'=q(ww')=f_{ww'}(q)$, поэтому $f_w\circ f_{w'}=f_{ww'}$. Полугруппа всех таких отображений f_w, $w\in A^*$, называется *полугруппой переходов* автомата V и обозначается $S(V)$. Очевидно, множество состояний Q является полигоном над полугруппой $S(V)$.

Упражнения

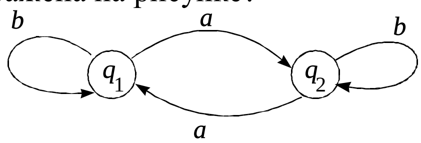
4.22. Доказать, что всякая полугруппа S является полигоном над собой.

4.23. Пусть G – группа и X – полигон над G, причём $xe = x$, если $x \in X$, а ε – единица группы G. *Орбитой* элемента $x \in X$ называется множество $xG = \{xg \mid g \in G\}$. Доказать, что X является объединением непересекающихся орбит.

4.24. Описать полугруппу переходов $S(V)$ автомата, диаграмма Мура которого изображена на рисунке.



4.25. Что из себя представляет полугруппа переходов автомата, диаграмма Мура которого изображена на рисунке?



4.26. Пусть G – группа, H – её подгруппа, $G/H = \{Hg \mid g \in G\}$ – множество всех правых смежных классов. Доказать, что G/H является G-полигоном относительно операции $Hg \cdot g' = Hgg'$.

4.27. Полигон X над полугруппой S называется *циклическим*, если существует такое $x_0 \in X$, что $X = x_0 S$. Доказать, что если X – циклический полигон над группой G с единицей e и $xe = x$ для всех $x \in X$, то $X \cong G/H$ для некоторой подгруппы H группы G.

4.28. Пусть X – полигон над полугруппой S, являющейся коммутативной полугруппой идемпотентов (т.е. $st = ts$ и $s^2 = s$ для всех $s, t \in S$). Доказать, что X будет являться частично упорядоченным множеством, если положить $x \le y \Leftrightarrow x = y$ èëè $x \in yS$.

4.29. Назовём полугруппу S *полугруппой правых нулей*, если $st = t$ для всех $s, t \in S$. Пусть X – полигон над полугруппой S правых нулей. Для $s \in S$ пусть $\sigma_s = \{(x, y) \in X \times X \mid xs = ys\}$. а) Доказать, что σ_s – отношение эквивалентности. б) Доказать, что $\sigma_s = \sigma_t$ при любых $s, t \in S$. в) Доказать, что для любого $x \in X$ множество xS пересекается с каждым σ_s-классом ровно по одному элементу. г) Доказать, что σ_s – конгруэнция полигона X.

$S(V) \cong \square_2$.

Ответы, указания, решения

1. Алгебраические структуры

1.1. $A\cup B=\{2,3,4,5,6,7,8\}$, $A\cap B=\{4,6\}$, $A\setminus B=\{2,8\}$, $B\setminus A=\{3,5,7\}$, $\overline{A}=\{1,3,5,7,9\}$, $\overline{B}=\{1,2,8,9\}$. **1.2.** $A\cap B=\{3\}$, $A\cup B=\{1,2,3,4,5,6,7,9\}$, , $A\setminus B=\{1,5,7,9\}$, $B\setminus A=\{2,4,6\}$, $\overline{A}=\{2,4,6,8\}$, $\overline{B}=\{1,5,7,8,9\}$. **1.3.** $A\cup B=(-\infty;2)\cup[3;+\infty)$, $A\cap B=(-1;1]\cup\{4\}\cup\{5\}\cup(6;+\infty)$, $A\setminus B=(-\infty;-1]\cup[3;4)\cup(5;6]$, $B\setminus A=(1;2)\cup(4;5)$, $\overline{A}=(1;3)\cup(4;5)$, $\overline{B}=(-\infty;-1]\cup[2;4)\cup(5;6]$. **1.4.** $A\cup B=(-\infty;4]\cup(6;+\infty)$, $A\cap B=[1;2]\cup\{7\}\cup(8;9]$, $A\setminus B=(-\infty;1)\cup\{4\}\cup(6;7)\cup(7;8]$, $B\setminus A=(2;4)\cup(9;+\infty)$, $\overline{A}=(2;4)\cup(4;6]\cup(9;+\infty)$, $\overline{B}=(-\infty;1)\cup[4;7)\cup(7;8]$. **1.5.** 24-мя способами. **1.6.** 32. **1.7.** 32. **1.8.** $C_5^3=10$. **1.9.** 8. **1.10.** 6. **1.11.** Например, такое: $\begin{pmatrix} a & b & c \\ y & y & x \end{pmatrix}$. **1.12.** 27. **1.13.** Например, такое: $\begin{pmatrix} a & b & c \\ z & y & x \end{pmatrix}$. **1.14.** См. 1.11 **1.15.** 6. **1.16.** Например, такое: $\begin{pmatrix} a & b & c & d \\ \alpha & \beta & \gamma & \alpha \end{pmatrix}$. **1.17.** $fg=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $gf=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $f^{-1}=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g^{-1}=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $o(f)=3$, $o(g)=2$. **1.18.** $fg=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, $gf=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, $f^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, $g^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, $o(f)=4$, $o(g)=3$.
1.19. Решение. Пусть отображение $f:A\to B$ является взаимно однозначным. Тогда каждый элемент $b\in B$ имеет ровно один прообраз $a\in A$. Положим $g(b)=a$. Таким образом определенное отображение $g:B\to A$ будет обратным к f. Далее, если отображение $f:A\to B$ имеет обратное отображение $f^{-1}:B\to A$ и $a_1,a_2\in A$, $a_1\neq a_2$, то $f(a_1)\neq f(a_2)$. Действительно, если бы $f(a_1)=f(a_2)$, то $a_1=f^{-1}(f(a_1))=f^{-1}(f(a_2))=a_2$, что противоречит условию. Теперь проверим второе условие в определении взаимно однозначного отображения. Пусть $b\in B$. Тогда $f(f^{-1}(b))=b$. Значит элемент $a=f^{-1}(b)$ является прообразом элемента b. Таким образом, отображение $f:A\to B$ будет взаимно однозначным. **1.20.** Решение. Поскольку разные элементы множества A должны переходить в разные, то $|A|\leq|B|$. А так как любой элемент множества B должен иметь прообраз, а прообразы для разных элементов множества B не могут совпадать, то $|B|\leq|A|$. Значит, $|A|=|B|$. **1.21.** 512. **1.22.** 64. **1.23.** 64. **1.24.** 216. **1.25.** Например, такое $\rho=\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.
1.26. Например, такое $\rho=\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. **1.27.** Например, такое $\rho=\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. **1.28.** Отношение ρ будет рефлексивным, симметричным и транзитивным, но не будет антисимметричным. Таким образом, ρ будет являться отношением эквивалентности, но не будет отношением порядка. **1.29.** Отношение ρ будет симметричным, но не будет рефлексивным, антисимметричным, транзитивным, отношением эквивалентности или порядка. **1.30.** Отношение ρ будет симметричным, но не будет рефлексивным, антисимметричным, транзитивным, отношением эквивалентности или порядка. **1.31.** Неассоциативна. **1.32.** Ассоциативна. **1.33.** Ассоциативна. **1.34.** Ассоциативна. **1.35.** Обозначим эти бинарные операции символами ψ_0 – ψ_{15} в соответствии с таблицей:

x	y	ψ_0	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	ψ_6	ψ_7	ψ_8
0	0	0	0	0	0	0	0	0	0	1
0	1	0	0	0	0	1	1	1	1	0
1	0	0	0	1	1	0	0	1	1	0

1	1	0	1	0	1	0	1	0	1	0

x	y	ψ_9	ψ_{10}	ψ_{11}	ψ_{12}	ψ_{13}	ψ_{14}	ψ_{15}
0	0	1	1	1	1	1	1	1
0	1	0	0	0	1	1	1	1
1	0	0	1	1	0	0	1	1
1	1	1	0	1	0	1	0	1

Тогда ассоциативными будут операции $\psi_0, \psi_1, \psi_3, \psi_5, \psi_6, \psi_7, \psi_9, \psi_{15}$.

1.36. $(\mathbb{N},+)$ – группу не образует, т.к. в ней нет единицы. Остальные множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ с операцией сложения образуют группу. **1.37.** $\mathbb{N}$ не является, т.к. элементы $2,3,4,\ldots$ не имеют обратных. $\mathbb{Z}$ не является, т.к. элементы $0,\pm2,\pm3,\pm4,\ldots$ не имеют обратных. $\mathbb{Q}$, $\mathbb{R}$ также не являются, т.к. 0 не имеет обратного. **1.38.** $\mathbb{N}$ не является, т.к. элементы $2,3,4,\ldots$ не имеют обратных. $\mathbb{Z}\setminus 0$ не является, т.к. элементы $\pm2,\pm3,\pm4,\ldots$ не имеют обратных. $\mathbb{Q}$, $\mathbb{R}$ являются. **1.39**. Да. Роль единицы играет 0. Обратным для kn является элемент $-kn$. **1.40**. Да.

1.41. Отображение f является гомоморфизмом, но не является изоморфизмом. Решение. Если $x, y \in \mathbb{R}$, то $f(x+y) = e^{2\pi i(x+y)} = e^{2\pi ix} \cdot e^{2\pi iy} = f(x)\cdot f(y)$, поэтому f – гомоморфизм, однако $f(0) = f(1) = 1$, поэтому f не является взаимно однозначным отображением, а значит, не является изоморфизмом. **1.42**. Отображение $f:[0,1) \to T$, определенное формулой $f(x) = e^{2\pi ix}$ является изоморфизмом. **1.43**. Решение. Пусть O – центр правильного треугольника ABC. В группе движений D_3 обозначим φ – поворот на 120° вокруг центра против часовой стрелки; φ^2 – поворот на 240°; a – симметрия относительно прямой, проходящей через точки A и O; b – симметрия относительно прямой BO; c – симметрия относительно прямой CO; e – тождественное преобразование. Тогда элементы a,b,c имеют 2-ой порядок, а φ и φ^2 – 3-ий. Элементы $\{a,\varphi\}$ можно взять за систему образующих группы D_3. Тогда $ñ = a\cdot\varphi, b = \varphi\cdot a$. В группе S_3 подстановки $x = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, y = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, z = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$ имеют 2-ой порядок, а $u = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, u^2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ 3-ий. Зададим отображение $f_1 : D_3 \to S_3$ на образующих следующим образом: $f(a) = x, f(\varphi) = u$. Тогда $f(\varphi^2) = u^2, f(b) = f(\varphi\cdot a) = u\cdot x = y, f(c) = f(a\cdot\varphi) = x\cdot u = z$ и отображение f_1 будет изоморфизмом. **1.44.** Матрицы $A = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, B = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, C = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ имеют 2-ой порядок, а $U = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} U^2 = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$ третий. Указание. Зададим отображение f_2 на образующих следующим образом: $f_2(a) = A, f_2(\varphi) = U$. Тогда $f_2(b) = B, f_2(c) = C, f_2(\varphi^2) = U^2$ и f_2 – изоморфизм. **1.45.** Решение. Определим порядки функций в последней группе. Например, $y_3^2 = y_3(y_3(x)) = \frac{1}{1-\frac{1}{1-x}} = \frac{1-x}{-x} = \frac{x-1}{x} = y_4$. Далее, $y_3^3 = y_3(y_4(x)) = \frac{1}{1-\frac{x-1}{x}} = x = y_1$. Значит, порядок функции y_3 (а, значит, и y_4) равен 3, поскольку y_1 – является единицей этой группы. Порядки функций y_2, y_5, y_6 равны 2-м. Положим $f_3(a) = y_2, f_3(\varphi) = y_3$. Тогда $f_3(b) = y_6, f_3(c) = y_5, f_3(\varphi^2) = y_4$ и f_3 – изоморфизм. **1.46.** $Aut\mathbb{Z}_2 \cong \{e\}$. **1.47.** $Aut\mathbb{Z}_3 = \{f_1, f_2\} \cong \mathbb{Z}_2$. **1.48.** $Aut\mathbb{Z}_4 = \{f_1, f_3\} \cong \mathbb{Z}_2$. **1.49.** $Aut\mathbb{Z}_5 = \{f_1, f_2, f_3, f_4\} \cong \mathbb{Z}_4$. **1.50.** $AutS_3 \cong S_3$. **1.51.** В группе $\mathbb{Z}_{12}$ имеются следующие нетривиальные подгруппы: $H_1 = \{\bar0, \bar2, \bar4, \bar6, \bar8, \overline{10}\}, H_2\{\bar0, \bar3, \bar6, \bar9\}, H_3\{\bar0, \bar4, \bar8\}, H_4 = \{\bar0, \bar6\}$. Элемент $\bar0$ является единицей группы, а единица всегда имеет первый порядок, элемент $\bar6$ имеет порядок 2, элементы $\bar4, \bar8$ – порядок 3, элементы $\bar3$ и $\bar9$ имеют порядок 4, элементы $\bar2, \overline{10}$ имеют порядок 6. Остальные элементы $\bar1, \bar5, \bar7, \overline{11}$ имеют порядок 12. **1.52.** Решение.Пусть $ABCD$ – квадрат, φ – поворот около центра квадрата на 90° против часовой стрелки, φ^2 и φ^3 – повороты на 180° и 270° соответственно, *e* – тождественное отображение, *a* – симметрия относительно прямой *AC*, *b* – относительно прямой *BD*, *f* – симметрия относительно прямой проходящей через середины сторон *AB* и *CD*, *g* – симметрия относительно прямой, проходящей через середины сторон *BC* и *AD*. Тогда нетривиальными подгруппами будут следующие: $H_1=\{e,\varphi^2\}$, $H_2=\{e,a\}$, $H_3=\{e,b\}$, $H_4=\{e,f\}$, $H_5=\{e,g\}$, $H_6=\{e,\varphi,\varphi^2,\varphi^3\}$, $H_7=\{e,\varphi^2,a,b\}$, $H_8=\{e,\varphi^2,f,g\}$. Единица группы *e* всегда имеет первый порядок, элементы φ^2,a,b,f,g имеют второй порядок, и элементы φ и φ^3 имеют четвертый порядок. **1.53.** Решение. Пусть *ABCD* – прямоугольник, $|AB|\neq|BC|$, φ – поворот около центра на 180°, *e* – тождественное отображение, *a* – симметрия относительно прямой проходящей через середины сторон *AB* и *CD*, *b* – симметрия относительно прямой, проходящей через середины сторон *BC* и *AD*. Тогда нетривиальными подгруппами будут следующие: $H_1=\{e,\varphi\}$, $H_2=\{e,a\}$, $H_3=\{e,b\}$. Единица группы *e* имеет первый порядок, элементы φ,a,b имеют второй порядок. **1.54.** Решение. Пусть *ABCD* – ромб, φ – поворот около центра на 180°, *e* – тождественное отображение, *a* – симметрия относительно прямой *AC*, *b* – относительно прямой *BD*. Тогда нетривиальными подгруппами будут следующие: $H_1=\{e,\varphi\}$, $H_2=\{e,a\}$, $H_3=\{e,b\}$. Единица группы *e* имеет первый порядок, элементы φ,a,b имеют второй порядок. **1.55.** Решение. Пусть *ABCDF* – правильный пятиугольник, точка *O* – его центр, φ – поворот около центра на 72° против часовой стрелки, φ^2, φ^3, φ^4 – повороты на 144°, 216° и 288° соответственно, *e* – тождественное отображение, ***a*, *b*, *c*, *d*, *f*** – симметрии относительно прямых *AO, BO, CO, DO и FO* соответственно. Тогда нетривиальными подгруппами будут следующие: $H_1=\{e,a\}$, $H_2=\{e,b\}$, $H_3=\{e,c\}$, $H_4=\{e,d\}$, $H_5=\{e,f\}$, $H_6=\{e,\varphi,\varphi^2,\varphi^3,\varphi^4\}$. Единица группы *e* имеет первый порядок, элементы a,b,c,d,f имеют второй порядок, и элементы $\varphi,\varphi^2,\varphi^3,\varphi^4$ имеют пятый порядок. **1.56.** Решение. Группа кватернионов состоит из элементов $Q_8=\{\pm1,\pm i,\pm j,\pm k\}$. Нетривиальными подгруппами будут следующие: $H_1=\{\pm1\}$, $H_2=\{\pm1,\pm i\}$, $H_3=\{\pm1,\pm j\}$, $H_4=\{\pm1,\pm k\}$. Единица группы 1 всегда имеет первый порядок, элемент (–1) – второй порядок, остальные элементы $\pm i,\pm j,\pm k$ имеют четвертый порядок. **1.57.** $\overline{1},\overline{3},\overline{7},\overline{9}$. **1.58.** $\overline{1},\overline{5},\overline{7},\overline{9}$. **1.59.** Решение. Пусть *ABC* – правильный треугольник, точка *O* – его центр, φ – поворот около центра на 120° против часовой стрелки, φ^2 – поворот на 240°, *e* – тождественное отображение, ***a*, *b*, *c*,** – симметрии относительно прямых *AO, BO, CO* соответственно. Тогда минимальными системами образующих будут следующие: $\{a,b\}$, $\{a,c\}$, $\{a,\varphi\}$, $\{a,\varphi^2\}$, $\{b,c\}$, $\{b,\varphi\}$, $\{b,\varphi^2\}$, $\{c,\varphi\}$, $\{c,\varphi^2\}$. **1.60.** $\{a,f\}$, $\{a,g\}$, $\{a,\varphi\}$, $\{a,\varphi^3\}$, $\{b,f\}$, $\{b,g\}$, $\{b,\varphi\}$, $\{b,\varphi^3\}$, $\{f,\varphi\}$, $\{f,\varphi^2\}$, $\{g,\varphi\}$, $\{g,\varphi^2\}$. **1.61.** Решение. Если $g\in G,\ h\in H$, то определитель матрицы ghg^{-1} равен единице, поэтому $gHg^{-1}\subset H$ и, следовательно, подгруппа *H* нормальна в *G*. **1.62.** Если *H* – центр группы G, то $gH=Hg$, поскольку элементы из *H* коммутируют со всеми элементами группы *G*. **1.63.** Решение. Если *H* – подгруппа индекса 2 группы *G*, то группа *G* является объединением двух левых, а также двух правых смежных классов по подгруппе *H*. Но одним из этих левых (правых) смежных классов является сама подгруппа *H*. Следовательно, оставшиеся левый и правый смежные классы совпадают, поскольку они совпадают с $G\setminus H$. **1.64.** Подгруппы $H_1=\{\pm1,\pm i\}, H_2=\{\pm1,\pm j\}, H_3=\{\pm1,\pm k\}$ являются нормальными, поскольку они имеют индекс 2. Подгруппа $H_4=\{\pm1\}$ нормальна, поскольку она является центром группы Q_8. **1.65.** $G/H\cong\mathbb{Z}_4$. **1.66.** G/H изоморфна группе движений прямоугольника, не являющегося квадратом. **1.67.** $G/H\cong\mathbb{Z}_3$. **1.68.** $G/H\cong\{\pm1\}$. **1.69.** G/H изоморфна группе движений прямоугольника, не являющегося квадратом. **1.70.** Да. **1.71.** Поскольку $n=15=3\cdot 5$, $A(3)=\{\bar{0},\bar{5},\overline{10}\}$, $A(5)=\{\bar{0},\bar{3},\bar{6},\bar{9},\overline{12}\}$. Изоморфизм $A(3)\oplus A(5)\to \mathbf{Z}_{15}$ можно задать следующим образом $(\bar{a},\bar{b})\to\overline{a+b}$. **1.72.** $\mathbb{Z}_6\cong\mathbb{Z}_2\oplus\mathbb{Z}_3$. **1.73.** $\mathbb{Z}_{12}\cong\mathbb{Z}_4\oplus\mathbb{Z}_3$. **1.74.** $\mathbb{Z}_{60}\cong\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5$. **1.75.** Поскольку $360=2^3\cdot 3^2\cdot 5$, то $\mathbb{Z}_{360}\cong\mathbb{Z}_8\oplus\mathbb{Z}_9\oplus\mathbb{Z}_5$. **1.76.** Решение. Поскольку $756=2^2\cdot 3^3\cdot 7, 2250=2\cdot 3^2\cdot 5^3, 25725=3\cdot 5^2\cdot 7^3$, то $\mathbb{Z}_{756}=\mathbb{Z}_4\oplus\mathbb{Z}_{27}\oplus\mathbb{Z}_7$, $\mathbb{Z}_{2250}=\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{125}$, $\mathbb{Z}_{25725}=\mathbb{Z}_3\oplus\mathbb{Z}_{25}\oplus\mathbb{Z}_{343}$. Поэтому $\mathbb{Z}_{756}\oplus\mathbb{Z}_{2250}\oplus\mathbb{Z}_{25725}\cong\mathbb{Z}_2\oplus\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{27}\oplus\mathbb{Z}_{25}\oplus\mathbb{Z}_{125}\oplus\mathbb{Z}_7\oplus\mathbb{Z}_{343}$. **1.77.** Решение. Поскольку $15=3\cdot 5, 225=9\cdot 25$, то $\mathbb{Z}_{15}\oplus\mathbb{Z}_{225}\cong\mathbb{Z}_3\oplus\mathbb{Z}_5\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{25}$. Далее, $75=3\cdot 25, 45=5\cdot 9$. Поэтому $\mathbb{Z}_{75}\oplus\mathbb{Z}_{45}\cong\mathbb{Z}_3\oplus\mathbb{Z}_{25}\oplus\mathbb{Z}_5\oplus\mathbb{Z}_9$. Так как разложения совпадают с точностью до перестановки слагаемых, группы изоморфны. **1.78.** Решение. Находим разложение каждой группы в прямую сумму примарных циклических групп: $\mathbb{Z}_9\oplus\mathbb{Z}_{225}\cong\mathbb{Z}_9\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{25}$, $\mathbb{Z}_{15}\oplus\mathbb{Z}_{135}\cong\mathbb{Z}_3\oplus\mathbb{Z}_5\oplus\mathbb{Z}_5\oplus\mathbb{Z}_{27}$. Примарные циклические слагаемые не совпадают. Группы не изоморфны. **1.79.** $\mathbb{Z}_6\oplus\mathbb{Z}_{36}\cong\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4\oplus\mathbb{Z}_9$. $\mathbb{Z}_{12}\oplus\mathbb{Z}_{18}\cong\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_2\oplus\mathbb{Z}_9$. Группы изоморфны. **1.80.** $\mathbb{Z}_6\oplus\mathbb{Z}_{36}\cong\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4\oplus\mathbb{Z}_9$. $\mathbb{Z}_9\oplus\mathbb{Z}_{24}\cong\mathbb{Z}_9\oplus\mathbb{Z}_3\oplus\mathbb{Z}_8$. Группы не изоморфны.

1.81. $\mathbb{Z}_6\oplus\mathbb{Z}_{10}\oplus\mathbb{Z}_{10}\cong\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_2\oplus\mathbb{Z}_5\oplus\mathbb{Z}_2\oplus\mathbb{Z}_5$. $\mathbb{Z}_{60}\oplus\mathbb{Z}_{10}\cong\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5\oplus\mathbb{Z}_2\oplus\mathbb{Z}_5$. Группы не изоморфны. **1.82.** Решение. Поскольку $64=2^6$ и 6=1+5=2+4=3+3=1+1+4=1+2+3=2+2+2=1+1+1+3=1+1+2+2=1+1+1+1++2=1+1+1+1+1+1, то $s(6)=11$. Поэтому существует 11 неизоморфных абелевых групп порядка 64. **1.83.** 4. **1.84.** 4. **1.85.** $864=3^3\cdot 2^5$. Решение. Так как $s(3)=3, s(5)=7$, то абелевых групп порядка 864 существует 21. **1.86.** Решение. Пусть G – циклическая группа с образующим g. Если $x,y\in G$, то $\exists n,m\in\mathbb{Z}$ такие, что $x=g^n, y=g^m$. Тогда $xy=yx=g^{n+m}$. **1.87.** Решение. Пусть G – группа простого порядка p и $g\in G, g\neq e$. Тогда $o(g)\neq 1$ и $o(g)\,|\,p$. Значит, $o(g)=p$. Таким образом, элемент g является образующим группы G, и $G\cong\mathbb{Z}_p$. **1.88.** Решение. Пусть $x,y\in G$. Тогда $xyxy=e$. Умножая это равенство справа на yx и учитывая, что $x^2=y^2=e$, получим $xy=yx$. **1.89.** Решение. Пусть G – группа порядка 4. Если в ней есть элемент порядка 4, то она изоморфна $\mathbb{Z}_4$. Если нет, то порядки ее элементов не превышают 2, следовательно, она абелева, но тогда она изоморфна $\mathbb{Z}_2\oplus\mathbb{Z}_2$ в силу теорем о строении конечных абелевых групп. **1.90.** Решение. В G не может быть элемента порядка 6, так как в противном случае G была бы абелевой. Если бы в G не существовал элемент порядка 3, то порядки элементов были бы не более 2, но тогда G была бы абелевой в силу задачи 3. Следовательно, в G имеется элемент порядка 3. **1.91.** Решение. Элементы e,x,x^2,y разные по условию. Элемент $xy\notin\{e,x,x^2\}$, т.к. иначе $y\in\{e,x,x^2\}$. Также $xy\neq y$. Значит элемент xy отличен от e,x,x^2,y. Аналогично, x^2y отличен от элементов e,x,x^2,y,xy. Если бы порядок элемента y равнялся бы 3, то y^2 равнялся бы одному из элементов x,x^2,y,xy,x^2y. Но отсюда следовало бы, что $y\in\{e,x,x^2\}$, а это невозможно. Значит, $o(y)=2$. **1.92.** Решение. Действительно, $yx\in\{e,x,x^2,y,xy,x^2y\}$. Но если $yx\in\{e,x,x^2\}$, то $y\in\{e,x,x^2\}$, что является противоречием. Если $yx=y$, то $x=e$, что невозможно. В случае $yx=xy$, группа $C^{\perp}$ была бы коммутативной. Остается только одна возможность: $yx=x^2y$. **1.93.** Решение. Полученные в задачах 1.90 – 1.92 соотношения полностью определяют группу G. Изоморфизм $F:G\to D_3$ можно задать формулами $F(x)=\varphi, F(y)=a$. Тогда $F(e)=e$, $F(x^2)=\varphi^2$, $F(xy)=c$, $F(x^2y)=b$. **1.94.** Решение. Если бы в G был бы элемент 8-го порядка или порядки всех элементов не превосходили бы 2-х, то G была бы абелевой. Значит, G содержит элемент 4-го порядка x. Обозначим $H=\{e,x,x^2,x^3\}$. Пусть $y\in G\setminus H$. Тогда $<x,y>=G$, поэтому элементы x и y не могут коммутировать, т.е. $xy\neq yx$. Элементы y,xy,x^2y,x^3y – разные и $y,xy,x^2y,x^3y\notin H$, т.к. иначе $y\in H$. Следовательно,

$G=\{e,x,x^2,x^3,y,xy,x^2y,x^3y\}$. Наконец, $yx\notin H, yx\neq y, yx\neq xy$. Если бы $yx=x^2y$, то $yx^2=x^2yx=y$, откуда следовало бы, что $x^2=e$, что невозможно. Значит, $yx=x^3y$. **1.95.** Решение. Пусть $y^2\neq e$. Тогда $o(y)=4$, следовательно, $o(y^2)=2$. Поэтому $y^2\neq x, y^2\neq x^3$. Кроме того $y^2\notin\{y,xy,x^2y,x^3y\}$, поскольку иначе $y\in H$. Следовательно, $y^2=x^2$. Рассмотрим первый случай $y^2=e$. В этом случае группа G полностью определена и отображение $F:G\to D_4$, при котором $F(x)=\varphi, F(y)=a$, задает изоморфизм групп $G\cong D_4$. Во втором случае $y^2=x^2$ изоморфизм $F:G\to Q_8$ можно задать на образующих так: $F(x)=i, F(y)=j$. **1.96.** Решение. Код C есть множество решений этой системы линейных однородных уравнений ранга 2 с пятью неизвестными. Следовательно, код C имеет размерность 3. Фундаментальную систему решений можно выбрать из векторов $\begin{matrix}(10010)\\(01011)\\(00101).\end{matrix}$ Порождающая матрица кода C, таким образом, имеет вид $C=\begin{pmatrix}10010\\01011\\00101\end{pmatrix}$. **1.97.** Кодовые слова представляют собой всевозможные линейные комбинации строк порождающей матрицы

0 0 0 0 0
1 0 0 1 0
0 1 0 1 1
0 0 1 0 1
1 1 0 0 1
1 0 1 1 1
0 1 1 1 0
1 1 1 0 0.

1.98. Ортогональным кодом $C^{\perp}$ будет множество решений системы уравнений $\begin{matrix}x_1+x_4=0\\x_2+x_4+x_5=0\\x_3+x_5=0.\end{matrix}$ Фундаментальная система решений имеет вид $\begin{matrix}(11010)\\(01101).\end{matrix}$ Таким образом, проверочная матрица кода C есть $H=\begin{pmatrix}11010\\01101\end{pmatrix}$. Код C есть линейный $(5,3)$-код. **1.99.** $H_0=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\0&1&1&0&0&0&1\end{pmatrix}$. **1.100.** $G_0=\begin{pmatrix}1&0&0&0&1&0\\0&1&0&0&0&1\\0&0&1&0&1&1\\0&0&0&1&0&1\end{pmatrix}$. **1.101.** Решение. **а)** В матрице есть два одинаковых столбца. Система из этих двух столбцов линейно зависима, значит, вес $d\le 2$. С другой стороны в матрице нет ненулевых столбцов. Это означает, что система из одного столбца всегда линейно независима, т.е. $d-1\ge 1$. Отсюда $d=2$. **б).** Сумма первого, третьего и пятого столбцов равна нулю, откуда $d\le 3$. А поскольку в матрице нет одинаковых столбцов, то $d-1\ge 2$. Значит, $d=3$. **1.102.** Код C обнаруживает 8 и исправляет 4 ошибки. **1.103.** Разложение абелевой группы $\mathbf{Z}_2^n$ по подгруппе C имеет следующий вид

00000	00001	00010	01000
10010	10011	10000	11010
01011	01010	01001	00011
00101	00100	00111	01101
11001	11000	11011	10001
10111	10110	10101	11111
01110	01111	01100	00110
11100	11101	11110	10100

В первой строке расположены лидеры смежных классов.

1.104. Решение. Слово $u=(101)$ кодируется как $v=u\cdot G=(10111)$. Предположим, что при передаче по каналу связи во втором разряде была допущена ошибка, и на приеме получено слово $v'=(11111)$. Это слово содержится в четвертом смежном классе, поэтому при декодировании к нему прибавляется лидер этого смежного класса: (01000). В результате мы получаем слово $v''=(10111)$, которое после отсечения последних двух разрядов будет равно $u'=(101)$. Таким образом, ошибка исправлена. Для того, чтобы исправить одну ошибку можно действовать и по другому. Если умножить проверочную матрицу H на вектор v', то получится слово (11). Оно называется синдромом и равно тому столбцу проверочной матрицы, в котором допущена ошибка. В данном случае слово (11) совпадает со вторым столбцом матрицы H, поэтому в слове v' нужно исправить второй разряд.

Заметим, что если бы ошибка произошла в первом или третьем разрядах, то слово было бы декодировано неправильно. Это свидетельствует о том, что данный код еще очень мало эффективен в плане исправления ошибок.

1.105. $H=\begin{pmatrix}0&1&1&0&0\\1&0&0&1&0\\1&0&0&0&1\end{pmatrix}$. Вес кода равен 2. Код обнаруживает одну ошибку, но не исправляет ни одной.

1.106. $H=\begin{pmatrix}0&1&1&0&0\\1&0&0&1&0\\1&1&0&0&1\end{pmatrix}$. Вес кода равен 3. Код обнаруживает две и исправляет одну ошибку.

1.107. $H=\begin{pmatrix}1&1&1&0&0\\1&1&0&1&0\\0&1&0&0&1\end{pmatrix}$. Вес кода равен 3. Код обнаруживает две и исправляет одну ошибку.

1.108. $H=\begin{pmatrix}0&1&1&1&0&0\\1&0&1&0&1&0\\1&1&0&0&0&1\end{pmatrix}$. Вес кода равен 3. Код обнаруживает две и исправляет одну ошибку.

1.109. Решение. Расстояние между любыми несовпадающими точками пространства $\mathbb{Z}_2^n$ не меньше 1, а число точек в $\mathbb{Z}_2^n$ равно 2^n, поэтому $A(n,1)=2^n$. Пусть $M(n,s)$ – максимальное множество точек в $\mathbb{Z}_2^n$, расстояние между любыми двумя из которых не меньше, чем *s*. Можно считать, что $\underbrace{00\ldots0}_{n}\in M(n,s)$, т.к. иначе все точки из $M(n,s)$ можно сдвинуть на один и тот же вектор. Существует только одно слово, расстояние от которого до точки $00\ldots0$ равно *n*, это $11\ldots1$. Поэтому $A(n,n)=2$. **1.110.** Решение. Можно считать, что $(000)\in M(3,2)$. Множество точек $M(3,2)=\{(000),(011),(101),(110)\}$ в $\mathbb{Z}_2^n$ будет максимальным множеством точек, расстояние между любыми двумя из которых не меньше 2. Поэтому $A(3,2)=4$.

1.111. $G=\begin{pmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{pmatrix}$. **1.112.** **а)** Ошибка в 6-м разряде. Исправленное слово $\tilde{v}=(1110000)$; **б)** Ошибка в 5-м разряде. Исправленное слово $\tilde{v}=(1101010)$; **в)** Ошибка в 1-м разряде. Исправленное слово $\tilde{v}=(0111100)$.

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

1.114. а) Ошибка в 10-м разряде. Исправленное слово $\tilde{a}=(000111000011000)$. **б)** Ошибка в 5-м разряде. Исправленное слово $\tilde{a}=(100110100100100)$. **в)** Ошибка в 8-м разряде. Исправленное слово $\tilde{a}=(000000011111111)$.

2. Теория булевых функций

2.1. а) $(1,1,0,0)$, $(0,0,0,0)$, $(0,1,1,0)$, $(0,1,0,1)$; **б)** n; **в)** $n\cdot 2^{n-1}$.

2.2. а) $(1,0,1,0)$, $(1,1,0,0)$, $(1,1,1,1)$, $(0,0,0,0)$, $(0,0,1,1)$, $(0,1,0,1)$; **б)** C_n^k; **в)** $C_n^k\cdot 2^{n-1}$. **2.3.** $2^{2^{\frac{n}{2}}}$, если n - четное число и $2^{2^{\frac{n+1}{2}}}$, если n - нечетное число. **2.2. а)** 19; **б)** 50; **в)** 31; **г)** 77. **2.5. а)** (0000), (0110), (1001), (1111); **б)** $2^{2^{n-1}}$. **2.6. а)** (0000), (0001), (1000), (1001); **б)** $2^{2^n-C_n^k}$. Указание к б). Вес k имеют C_n^k булевых векторов от n переменных. Следовательно, C_n^k определенных координат функции равны 1, а остальные $\left(2^n-C_n^k\right)$ координаты могут принимать любые значения (0 или 1). **2.7.** Указание. Пусть $f(0,0,\ldots,0)=0$. Тогда на всех наборах веса 1 значение функции также будет равно 0. Для каждого набора веса 2 найдется соседний с ним набор веса 1, следовательно, на всех наборах веса 2 значение функции также равно 0. Для каждого набора веса 3 найдется соседний с ним набор веса 2, следовательно, на всех наборах веса 3 значение функции также равно 0. И так далее вплоть до векторов веса n. Случай $f(0,0,\ldots,0)=1$ рассматривается аналогично. **2.8. а)** x_1 - существенная, x_2 - фиктивная; **б)** x_1 - фиктивная; x_2, x_3 - существенные; **в)** x_3 - фиктивная; x_1, x_2 - существенные; **г)** x_1, x_3 - фиктивные; x_2, x_4 - существенные. **2.9.а)** $(1110\,1010)$; **б)** (10); **в)** (1001); **г)** (01). **2.10. а)** (1111); **б)** $(0100\,0111)$; **в)** (11111101); **г)** $(1110\ \ 1110\ \ 1110\ \ 0001)$. **2.11. в)**, **г)** является; **а)**, **б)**, **д)**, **е)** не является. **2.12. а)** (10011111); **б)** $(0010\ \ 0000\ \ 0010\ \ 0010)$. **2.13. а)** $xy\left(\overline{x}\vee y\right)$;

б) $\left(x\vee y\vee xyz\right)\to\left(\overline{x}\,\overline{y}\to z\right)$. **2.12. а)** $\left(\left(\left(x\wedge y\right)\vee\left(x\wedge\left(\neg\left(y\wedge z\right)\right)\right)\right)\vee z\right)$; **б)** $\left(\left(\left(x\vee z\right)\wedge y\right)\to\left(x\wedge y\right)\right)$. **2.19. а)** коммутативна только $\{\leftrightarrow\}$; **б)** ассоциативна только $\{\leftrightarrow\}$. **2.20. а)** $\overline{\overline{x}\,\overline{y}\,\overline{z}}$; **б)** $\overline{x\overline{y}}$; **в)** $\overline{x\overline{y}}\cdot\overline{\overline{x}y}$; **г)** $\overline{\overline{x}\,\overline{y}\,\overline{z}}$. **2.21. а)** $\overline{\overline{x}\vee\overline{y}\vee\overline{z}}$; **б)** $\overline{x}\vee\overline{y}\vee\overline{\overline{y}\vee\overline{z}}$; **в)** $\overline{\overline{\overline{x}\vee y}\vee\overline{\overline{y}\vee x}}$; **г)** $\overline{\overline{x}\vee y}\vee\overline{\overline{y}\vee x}$. **2.23. а)** $\overline{z}\vee x$; **б)** 1; **в)** xy; **г)** $\overline{x}\vee\overline{y}$; **д)** $x\vee\overline{z}$; **е)** $\overline{x}\,\overline{y}$. **2.22. а)** x_1, x_2, x_4, x_5 - фиктивные; x_3, x_6 - существенная; **б)** x_2 - существенная, x_1, x_3 - фиктивные. **2.25. а)** (0000), (0101), (1010), (1111); **б)** $2^{2^{n-1}}$. Указание к б). Если x_n - фиктивная переменная, то для любого набора $\alpha_1,\alpha_2\ldots,\alpha_{n-1}$ выполняется равенство $f\left(\alpha_1,\alpha_2\ldots,\alpha_{n-1},0\right)=f\left(\alpha_1,\alpha_2\ldots,\alpha_{n-1},1\right)$, следовательно, чтобы задать функцию f необходимо и достаточно определить ее значения на 2^{n-1} булевом векторе; **в)** $n\cdot 2^{2^{n-1}}$. **2.26. а)** 36; **б)** 49; **в)** 3^n; **г)** $2^{2n}-3^n$. Указание к г). Можно от числа всех наборов длины $2n$ отнять число наборов, на которых функция обращается в единицу.

2.27. $(0)^*=1$, $(1)^*=0$; $(x)^*=x$; $\left(\overline{x}\right)^*=\overline{x}$; $\left(x\vee y\right)^*=x\wedge y$; $\left(x\wedge y\right)^*=x\vee y$; $\left(x\downarrow y\right)^*=x|y$; $\left(x|y\right)^*=x\downarrow y$; $\left(x\leftrightarrow y\right)^*=x\oplus y$; $\left(x\oplus y\right)^*=x\leftrightarrow y$. **2.28. а)** $\left(\overline{\sigma_4},\overline{\sigma_3},\overline{\sigma_2},\overline{\sigma_1}\right)$. **2.29. а)** (0010);

б) $(1001\ \ 0010)$; **в)** $(1101\ \ 0100)$; **г)** $(1011\ \ 0100\ \ 0011\ \ 0000)$.

2.30. а) $(0000\ \ 0010)$; **б)** $(0011\ \ 0100)$.

2.31. а) $\left(x\vee y\vee z\right)\wedge\left(x\vee\overline{y}\vee z\right)\wedge\overline{z}\wedge 1$; **б)** $\left(\left(x\leftrightarrow\overline{y}\right)\vee y\vee z\right)\wedge 1$.

2.32. а) $x\wedge\left(y\vee z\right)=\left(x\wedge y\right)\vee\left(x\wedge z\right)$; **б)** $\left(x\leftrightarrow y\right)\leftrightarrow z=x\leftrightarrow\left(y\leftrightarrow z\right)$; **в)** $\left(x\leftrightarrow y\right)\vee z=\left(x\vee z\right)\leftrightarrow\left(y\vee z\right)$; **г)** $xy=x\leftrightarrow y\leftrightarrow\left(x\vee y\right)$.

2.33. а) $\overline{xy}\vee x\cdot\overline{y\vee z}$; **б)** $x\left(\bar{y}\vee z\right)\cdot 1\vee\overline{z\vee y}$; **в)** $\left(\bar{x}y\vee\overline{x\vee y}\right)\cdot\overline{\overline{\bar{x}yz\cdot\overline{x\vee y}}}$; **г)** $\left(x_1\leftrightarrow x_2\right)\oplus\left(x_2\downarrow x_3\right)$; **д)** $\left(x\vee y\vee\overline{y\vee x}\cdot\left(y\vee z\vee\overline{x\left(y\vee z\right)}\right)\right)\cdot 1$; **е)** $\left(x_1\oplus x_3\right)\big|\left(x_2\downarrow 1\right)$. **2.32.** Пусть для определенности речь идет о переменной x_1. Тогда существует такой набор $\alpha_2\ldots,\alpha_n$ значений переменных $\left(x_2,\ldots,x_n\right)$, что $f\left(0,\alpha_2\ldots,\alpha_n\right)\neq f\left(1,\alpha_2\ldots,\alpha_n\right)$, т.е. $f\left(0,\alpha_2\ldots,\alpha_n\right)=\overline{f\left(1,\alpha_2\ldots,\alpha_n\right)}$. Согласно определению двойственной функции верны равенства $f^*\left(\bar{0},\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)=\overline{f\left(0,\alpha_2\ldots,\alpha_n\right)}$ и $f^*\left(\bar{1},\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)=\overline{f\left(1,\alpha_2\ldots,\alpha_n\right)}$, которые можно переписать в виде $\overline{f^*\left(1,\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)}=f\left(0,\alpha_2\ldots,\alpha_n\right)$ и $f^*\left(0,\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)=\overline{f\left(1,\alpha_2\ldots,\alpha_n\right)}$. Следовательно, равенство $f\left(0,\alpha_2\ldots,\alpha_n\right)=\overline{f\left(1,\alpha_2\ldots,\alpha_n\right)}$ можно также записать в виде $\overline{f^*\left(1,\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)}=f^*\left(0,\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)$. Таким образом, существует набор $\overline{\alpha_2}\ldots,\overline{\alpha_n}$ такой, что $f^*\left(0,\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)\neq f^*\left(1,\overline{\alpha_2}\ldots,\overline{\alpha_n}\right)$. Это означает, что $f^*\left(x_1,x_2,\ldots,x_n\right)$ существенно зависит от переменной x_1.

2.35. а) $x_1\vee x_2=\bar{x}_1x_2\vee x_1\bar{x}_2\vee x_1x_2$; **б)** $x_1\,|\,x_2=\bar{x}_1\bar{x}_2\vee\bar{x}_1x_2\vee x_1\bar{x}_2$;

в) $x_1\downarrow x_2=\bar{x}_1\bar{x}_2$; **г)** $x_1\oplus x_2=\bar{x}_1x_2\vee x_1\bar{x}_2$;

д) $\bar{x}_1\bar{x}_2\bar{x}_3\vee\bar{x}_1\bar{x}_2x_3\vee x_1\bar{x}_2x_3\vee x_1x_2x_3$; **е)** $\bar{x}_1\bar{x}_2x_3\vee\bar{x}_1x_2x_3\vee x_1\bar{x}_2\bar{x}_3\vee x_1\bar{x}_2x_3\vee x_1x_2\bar{x}_3$.

2.36. а) $\left(x_1\vee x_2\right)\left(x_1\vee\bar{x}_2\right)\left(\bar{x}_1\vee x_2\right)$; **б)** $\bar{x}_1\vee\bar{x}_2$;

в) $\left(x_1\vee\bar{x}_2\right)\left(\bar{x}_1\vee x_2\right)\left(\bar{x}_1\vee\bar{x}_2\right)$; **г)** $\left(x_1\vee x_2\right)\left(\bar{x}_1\vee\bar{x}_2\right)$;

д) $\left(x_1\vee\bar{x}_2\vee x_3\right)\left(x_1\vee\bar{x}_2\vee\bar{x}_3\right)\left(\bar{x}_1\vee x_2\vee x_3\right)\left(\bar{x}_1\vee\bar{x}_2\vee x_3\right)$;

е) $\left(x_1\vee x_2\vee x_3\right)\left(x_1\vee\bar{x}_2\vee x_3\right)\left(\bar{x}_1\vee\bar{x}_2\vee\bar{x}_3\right)$.

2.37. а) СДНФ: $\bar{x}_1\bar{x}_2\bar{x}_3\vee\bar{x}_1\bar{x}_2x_3\vee\bar{x}_1x_2x_3\vee x_1x_2\bar{x}_3\vee x_1x_2x_3$;

СКНФ: $\left(x_1\vee\bar{x}_2\vee x_3\right)\left(\bar{x}_1\vee x_2\vee x_3\right)\left(\bar{x}_1\vee x_2\vee\bar{x}_3\right)$;

б) СДНФ: $\bar{x}_1\bar{x}_2\bar{x}_3\vee\bar{x}_1\bar{x}_2x_3\vee\bar{x}_1x_2\bar{x}_3\vee x_1\bar{x}_2x_3\vee x_1x_2\bar{x}_3$;

СКНФ: $\left(x_1\vee\bar{x}_2\vee\bar{x}_3\right)\left(\bar{x}_1\vee x_2\vee x_3\right)\left(\bar{x}_1\vee\bar{x}_2\vee\bar{x}_3\right)$;

в) СДНФ: $\bar{x}_1\bar{x}_2\bar{x}_3\vee\bar{x}_1\bar{x}_2x_3\vee\bar{x}_1x_2x_3\vee x_1\bar{x}_2\bar{x}_3\vee x_1\bar{x}_2x_3$;

СКНФ: $\left(x_1\vee\bar{x}_2\vee x_3\right)\left(\bar{x}_1\vee\bar{x}_2\vee x_3\right)\left(\bar{x}_1\vee\bar{x}_2\vee\bar{x}_3\right)$;

г) СДНФ: $\bar{x}_1\bar{x}_2\vee\bar{x}_1x_2\vee x_1x_2$; СКНФ: $\bar{x}_1\vee x_2$.

2.38. а) $1,\ \bar{x}_1,\ \bar{x}_2,\ x_1,\ x_2,\ x_1x_2,\ x_1\bar{x}_2,\ \bar{x}_1x_2,\ \bar{x}_1\bar{x}_2$; **б)** 3^n.

Указание к б). Каждая переменная может не входить в элементарную конъюнкцию, входить с отрицанием, входить без отрицания.

2.39. а) $x_1x_2,\ x_1\bar{x}_2,\ \bar{x}_1x_2,\ \bar{x}_1\bar{x}_2,\ x_1x_3,\ x_1\bar{x}_3,\ \bar{x}_1x_3,\ \bar{x}_1\bar{x}_3,\ x_2x_3,\ x_2\bar{x}_3,\ \bar{x}_2x_3,\ \bar{x}_2\bar{x}_3$;

б) $C_n^k\cdot 2^k$. **2.40. а)** $\bar{x}_2\bar{x}_3\bar{x}_4$, $x_1\bar{x}_3\bar{x}_4$, $x_1\bar{x}_2\bar{x}_4$, $x_1\bar{x}_2\bar{x}_3$; **б)** C_n^r. Указание. Искомое число элементарных конъюнкций равно числу подмножеств мощности r множества $\left\{x_1^{\alpha_1},x_2^{\alpha_2},\ldots,x_n^{\alpha_n}\right\}$.

2.41. а) $1,\ \bar{x}_1,\ x_2,\ \bar{x}_3,\ x_2\bar{x}_3,\ \bar{x}_1\bar{x}_3,\ \bar{x}_1x_2,\ \bar{x}_1x_2\bar{x}_3$ **б)** 2^n. Указание к б). Число элементарных конъюнкций равно числу подмножеств множества $\left\{x_1^{\alpha_1},x_2^{\alpha_2},\ldots,x_n^{\alpha_n}\right\}$. **2.42. а)** 64; **б)** $2^{2^n-2^{n-r}}$. Указание к а). x_1x_2 является импликантой для тех и только тех функций, которые на наборах $(1,1,0)$ и $(1,1,1)$ равны 1. На остальных шести наборах функций может принимать любые значения, следовательно, число таких функций равно $2^6=64$. **2.43. а)** x,y; **б)** $\bar{x},\bar{y}$; **в)** $\bar{x}\bar{y},xyz$; г) $\bar{x},y\bar{z}$.

2.42. а) например, $x_1\overline{x}_2x_3$; **б)** например, $\overline{x}_2\overline{x}_3 \vee x_1\overline{x}_2$.

2.45. а) $\overline{x}_1\overline{x}_2 \vee \overline{x}_1x_3 \vee x_2x_3 \vee x_1x_2$ - сокращенная, $\overline{x}_1\overline{x}_2 \vee x_2x_3 \vee x_1x_2$, $\overline{x}_1\overline{x}_2 \vee \overline{x}_1x_3 \vee x_1x_2$ - тупиковые, они же минимальные ДНФ;

б) $\overline{x}_1\overline{x}_2 \vee x_1\overline{x}_3 \vee \overline{x}_2\overline{x}_3 \vee x_1x_2$ - сокращенная, $\overline{x}_1\overline{x}_2 \vee x_1\overline{x}_3 \vee x_1x_2$, $\overline{x}_1\overline{x}_2 \vee \overline{x}_2\overline{x}_3 \vee x_1x_2$ - тупиковые, они же минимальные ДНФ;

в) $\overline{x}_2\overline{x}_3\overline{x}_4 \vee x_2x_3x_4 \vee \overline{x}_1x_2x_3 \vee \overline{x}_1\overline{x}_4$ - сокращенная ДНФ,

$\overline{x}_2\overline{x}_3\overline{x}_4 \vee x_2x_3x_4 \vee \overline{x}_1\overline{x}_4$ - тупиковая, она же минимальная;

г) $\overline{x}_2\overline{x}_3\overline{x}_4 \vee x_1\overline{x}_3\overline{x}_4 \vee \overline{x}_1\overline{x}_2\overline{x}_4 \vee x_1x_2$ - сокращенная ДНФ,

$\overline{x}_2\overline{x}_3\overline{x}_4 \vee \overline{x}_1\overline{x}_2\overline{x}_4 \vee x_1x_2$, $x_1\overline{x}_3\overline{x}_4 \vee \overline{x}_1\overline{x}_2\overline{x}_4 \vee x_1x_2$ - тупиковые, они же минимальные ДНФ; **д)** $\overline{x}_2\overline{x}_4 \vee \overline{x}_1\overline{x}_2 \vee x_1\overline{x}_4 \vee x_3\overline{x}_4 \vee \overline{x}_1x_3 \vee x_2x_3$ - сокращенная ДНФ; $\overline{x}_1\overline{x}_2 \vee x_1\overline{x}_4 \vee x_2x_3$ - тупиковая и минимальная ДНФ;

е) $x_3x_4 \vee \overline{x}_1\overline{x}_2 \vee \overline{x}_2\overline{x}_3\overline{x}_4 \vee x_1\overline{x}_3\overline{x}_4$ - сокращенная ДНФ;

$x_3x_4 \vee \overline{x}_1\overline{x}_2 \vee x_1\overline{x}_3\overline{x}_4$ - тупиковая и минимальная ДНФ.

2.46. а) $1 \oplus x_2 \oplus x_1 \oplus x_1x_2$; **б)** $x_2 \oplus x_1x_2$; **в)** $1 \oplus x_2 \oplus x_1x_2x_3$; **г)** $1 \oplus x_3 \oplus x_2 \oplus x_2x_3 \oplus x_1x_3$. **2.47. а)** $x \oplus xy \oplus xyz$; **б)** $xyz \oplus 1$.

2.48. а) $x \oplus xy$; **б)** $x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_2x_3$; **в)** $x_1x_2 \oplus x_1x_2x_4 \oplus x_1x_2x_3x_4$; **г)** $1 \oplus x_1x_2x_4$.

2.49. а) $f = yt \oplus zx \oplus xyzt$; **б)** $f = 1 \oplus x \oplus t \oplus xy \oplus xt \oplus zt \oplus xzt$.

2.51. а) 2^{2^n-1}; **б)** 2^{2^n-1}; **в)** 2^{2^n-2}; **г)** $3 \cdot 2^{2^n-2}$. **2.52. а)** Выписать векторы значений всех самодвойственных функций двух переменных.

б) Сколько имеется самодвойственных функций от n переменных?

2.52. а) (0011), (0101), (1010), (1100); **б)** $2^{2^{n-1}}$. **2.53. а)** $2^{2^{n-1}-1}$; **б)** $2^{2^{n-1}-1}$; **в)** $2^{2^n-1} + 2^{2^{n-1}-1}$; **г)** $3 \cdot 2^{2^n-2} + 2^{2^{n-1}-1}$.

2.52. Указание. Если f - самодвойственная функция, то на любых двух противоположных наборах значений переменных она принимает противоположные значения. Следовательно, число наборов, на которых f принимает значение 1, равно числу пар противоположных наборов длины *n*, т.е. 2^{n-1}. **2.56. а)** $(0,0,0,0)$, $(0,0,0,1)$, $(0,0,1,1)$, $(1,0,0,1)$, $(1,0,1,0)$, $(1,0,1,1)$; **б)** 2^k **2.57. а)** $(0,1,0,1,1,1)$, $(0,1,1,1,1,1)$, $(1,1,0,1,1,1)$, $(1,1,1,1,1,1)$; **б)** 2^{n-k}. 2.59. $0, 1, x, xy, x \vee y$. **2.60.** Указание. Пусть монотонная функция не сохраняет 0. Поскольку нулевой набор предшествует остальным, монотонная функция на остальных наборах не может быть меньше, чем на нулевом наборе. Значит, из равенства монотонной функции единице на нулевом наборе следует ее тождественное равенство единице. Аналогично рассматривается случай монотонной функции, не сохраняющей единицу. **2.61. а)** немонотонна; **б)** монотонна; **в)** немонотонна; **г)** немонотонна. **2.62.** Решение. Если $f(x_1,\dots,x_n)$ немонотонная функция, то согласно определению найдутся два такие вектора $\vec{\alpha}_0$, $\vec{\beta}_0$ (необязательно соседние) из B^n, что $\vec{\alpha}_0 \le \vec{\beta}_0$, но $f(\vec{\alpha}_0) > f(\vec{\beta}_0)$. Пусть эти наборы различаются в k $1 \le k \le n$ координатах. Тогда, меняя по одной координате, можно выстроить последовательность из $k-1$ наборов $\vec{\alpha}_1,\dots,\vec{\alpha}_{k-1}$ таких, что $\vec{\alpha}_0 \le \vec{\alpha}_1 \le \dots \le \vec{\alpha}_{k-1} \le \vec{\beta}_0$ и каждый следующий набор отличается от предыдущего ровно в одной координате. Так как $f(\vec{\alpha}_0) > f(\vec{\beta}_0)$, то в этой последовательности найдутся два соседних набора такие, что $\vec{\alpha} \le \vec{\beta}$, но $f(\vec{\alpha}) > f(\vec{\beta})$. Это и есть искомые наборы. **2.63. а)** 6; **б)** 20.

2.65. а) немонотонная; **б)** монотонная; **в)** немонотонная; **г)** немонотонная. **2.66. а)** $(0000\ 0000\ 1111\ 1111)$; **б)** $(0000\ 0111\ 0001\ 1111)$, $(0000\ 1111\ 0000\ 1111)$, $(0001\ 0111\ 0001\ 0111)$,

$(0001\ 1111\ 0000\ 0111)$, $(0000\ 0000\ 1111\ 1111)$,

$(0000\ 0001\ 0111\ 1111)$, $(0001\ 0001\ 0111\ 0111)$.

2.68. Указание. Рассмотреть два случая: $f(1,1,\dots,1) = 0$ и $f(1,1,\dots,1) = 1$. **2.70.** $0, 1, x, \overline{x}, x \oplus y, x \leftrightarrow y$. **2.71. а)** 2^{n+1}; **б)** 2^n; **в)** 2^n; **г)** 2^{n-1}; **д)** 2^{n-1}; **е)** $n+2$. Решение е). Пусть свободный член полинома Жегалкина равен 1. Поскольку в явном виде (т.е. с ненулевыми коэффициентами) присутствуют только существенные переменные см. 2.50), то из сопоставления значений функции на нулевом наборе и наборе, содержащем ровно одну единицу на месте, соответствующем существенной переменной, следует немонотонность функции. Следовательно, если свободный член равен 1, то функция тождественно равна единице. Пусть теперь свободный член полинома Жегалкина равен 0 и линейная функция имеет, по крайней мере, два существенных аргумента. Тогда на наборе, содержащем ровно две единицы на местах, соответствующих этим существенным аргументам, значение функции равно 0, а на предшествующем ему наборе, содержащим ровно одну единицу на месте, соответствующем одному из этих аргументов, равно 1. Следовательно, функция немонотонна. Остаются два случая. В первом свободный член полинома Жегалкина равен 0 и линейная функция не имеет существенных аргументов, т.е. речь идет о тождественном нуле. Во втором случае, свободный член полинома Жегалкина равен 0 и линейная функция имеет один существенный аргумент, т.е. речь идет о функции $x_i, 1 \le i \le n$. **2.72. а)** 2^{n-1}; **б)** $3 \cdot 2^{n-1}$. **2.72.** $2 \cdot C_n^k$. **2.75.** 2^{n-1}. Указание. Если $f(x_1, \ldots, x_n)$ линейна, то ее полином Жегалкина можно записать в виде $f = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n$. Так как f отлична от константы, то среди коэффициентов $a_1, a_2, \ldots, a_n$ есть равные единице. Обозначим через k число таких коэффициентов. Пусть для определенности это $a_1, a_2, \ldots, a_k$ ($1 \le k \le n$). Рассмотрим два случая: $a_0 = 0$ и $a_0 = 1$. В первом случае $f(x_1, \ldots, x_n)$ реализуется формулой $x_1 \oplus x_2 \oplus \ldots \oplus x_k$ и, значит, обращается в единицу на векторах $(\beta_1, \ldots, \beta_k, \beta_{k+1}, \ldots, \beta_n)$, у которых некоторое нечетное число координат $\beta_1, \ldots, \beta_k$ равны 1, остальные координаты $\beta_1, \ldots, \beta_k$ равны 0, координаты же $\beta_{k+1}, \ldots, \beta_n$ могут принимать любые значения (0 или 1). Каждый набор $\beta_1, \ldots, \beta_k$ однозначно задается набором номеров единичных координат, поэтому таких наборов столько же, сколько подмножеств нечетной мощности у множества из k элементов, т.е. 2^{k-1}. Таким образом, первые k координат вектора $(\beta_1, \ldots, \beta_k, \beta_{k+1}, \ldots, \beta_n)$ можно выбрать 2^{k-1} способами, а оставшиеся $n-k$ координат 2^{n-k} способами. Следовательно, число таких векторов равно $2^{k-1} \cdot 2^{n-k} = 2^{n-1}$. Аналогично рассматривается случай $a_0 = 1$. **2.77.**

Функции		Классы функций				
		T_0	T_1	S	M	L
1	0	+	–	–	+	+
2	x	+	+	+	+	+
3	$\bar{x}$	–	–	+	–	+
4	1	–	+	–	+	+
5	$x \wedge y$	+	+	–	+	–
6	$x \vee y$	+	+	–	+	–
7	$x \to y$	–	+	–	–	–
8	$x \leftrightarrow y$	–	+	–	–	+
9	$x \mid y$	–	–	–	–	–
10	$x \downarrow y$	–	–	–	–	–
11	$x \oplus y$	+	–	–	–	+

2.78.

Функции	Классы функций				
	T_0	T_1	S	M	L
f_1	+	+	–	–	–
f_2	+	–	–	–	–
f_3	+	+	–	–	–
f_4	+	–	–	–	–
f_5	+	+	–	–	–
f_6	–	+	–	–	–

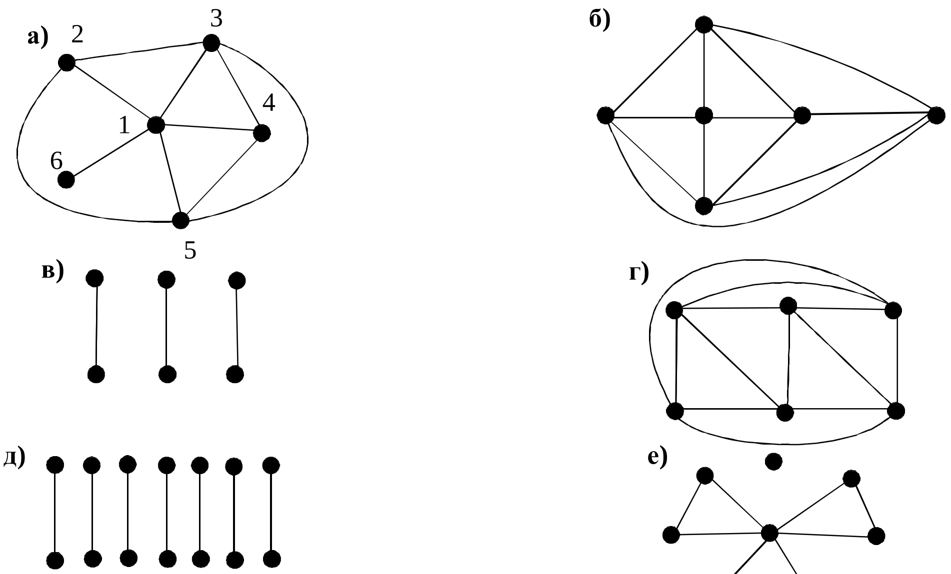
2.80. а) 1; **б)** 0; **в)** $x, \bar{x}$; **г)** $1, x, \bar{x}$. **2.81.** а), в), г), д), е), ж), з).

2.82. Нет. Р е ш е н и е. Возьмем классы функций $\mathbf{T}_0$ и $\mathbf{T}_1$. Их объединение сохраняет ноль или единицу. В частности, ему принадлежат $\bar{x}y$ (сохраняющая 0) и 1 (сохраняющая 1). Подставляя 1 в $\bar{x}y$ вместо y, мы получаем $\bar{x}$, которая не сохраняет ни нуля, ни единицы. **2.83.** У к а з а н и е к **а)**. Функции, соответствующие связкам $\wedge, \to$, принадлежат классу $\mathbf{T}_1$. Класс $\mathbf{T}_1$ функционально замкнут, следовательно, любая функция, реализованная над множеством связок $S=\{\vee,\to\}$, также будет принадлежать классу $\mathbf{T}_1$, а $x|y\notin\mathbf{T}_1$.

2.82. Р е ш е н и е **а)**. $\{x\vee y, x\oplus y\}\subset\mathbf{T}_0$, следовательно, $[x\vee y, x\oplus y]\subset[\mathbf{T}_0]$. Осталось доказать, что $\mathbf{T}_0\subset[x\vee y, x\oplus y]$. Действительно, если $f\in\mathbf{T}_0$, то свободный член в полиноме Жегалкина этой функции равен 0, значит, f можно выразить формулой через $\{xy, x\oplus y\}$. Но $x\vee y = x\oplus y\oplus xy$ и, значит, $xy = x\oplus y\oplus x\vee y$, следовательно, f можно выразить формулой над $\{x\vee y, x\oplus y\}$. **2.85.** У к а з а н и е. В качестве полной системы используйте $\{x\vee y,\ \bar{x}\}$ или $\{x\wedge y,\ \bar{x}\}$. **2.86. а)** неполная; **б)** полная; **в)** неполная; **г)** полная; **д)** полная; **е)** неполная; **ж)** полная; **з)** полная. **2.87. а)** нет; **б)** да. **2.88.** $\{x|y\}$, $\{x\downarrow y\}$, $\{x\to y, 0\}$, $\{x\to y, 0\}$, $\{x\to y, 0\}$, $\{x\vee y, \bar{x}\}$, $\{x\wedge y, \bar{x}\}$, $\{x\leftrightarrow y, x\wedge y, 0\}$, $\{x\leftrightarrow y, x\vee y, 0\}$, $\{x\oplus y, x\wedge y, x\leftrightarrow y\}$, $\{x\oplus y, x\vee y, x\leftrightarrow y\}$, $\{x\oplus y, x\wedge y, 1\}$, $\{x\oplus y, x\vee y, 1\}$. **2.89.** Например, $\{0, 1, x\oplus y\oplus z, xy\}$ или $\{0, 1, x\oplus y\oplus z, x\vee y\}$. **2.90.** У к а з а н и е. Будем рассуждать от противного. Предположим, найдется базис $\mathbf{B}$, состоящий не менее чем из 4-х функций. Поскольку базис представляет собой полную систему, то в $\mathbf{B}$ найдутся функции f_0, f_1, f_S, f_M, f_L такие, что $f_0\notin\mathbf{T}_0$, $f_1\notin\mathbf{T}_1$, $f_S\notin\mathbf{S}$, $f_M\notin\mathbf{M}$, $f_L\notin\mathbf{L}$. Ранее было показано (2.68), что функция f_0 либо немонотонная, либо несамодвойственная. Следовательно, одна из двух подсистем $\{f_0, f_1, f_S, f_L\}$, $\{f_0, f_1, f_M, f_L\}$ обязательно полна. Значит в $\mathbf{B}$ есть полная подсистема. Получили противоречие с определением базиса.

3. Теория графов

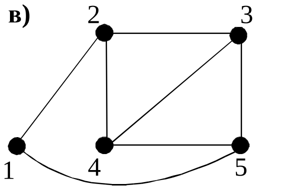
3.1.



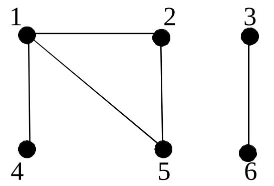
3.2. б) и г).

3.3.

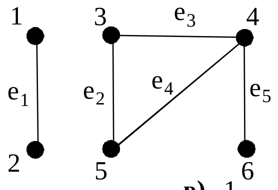
в)



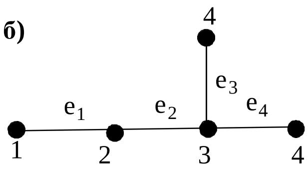
г)



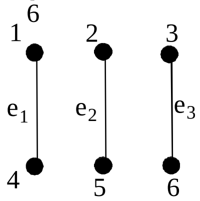
3.4. **а)**



б)



в)

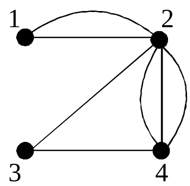


3.5. а) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$; б) $\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$; в) $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 &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

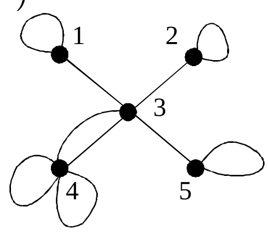
г) $\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$.

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

3.7. **а)**

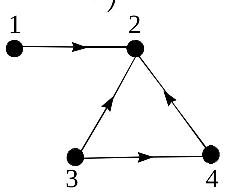


б)

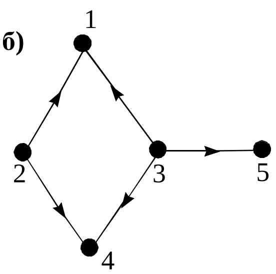


3.8. а) $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$; б) $\begin{pmatrix} 0 & 1 & 3 \\ 1 & 1 & 2 \\ 3 & 2 & 0 \end{pmatrix}$.

3.9. **а)**

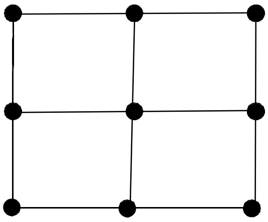


б)

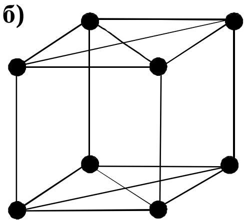


3.10. а) $\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$; б) $\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

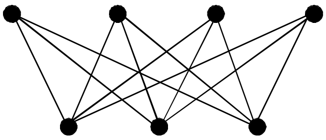
3.11. **а)**



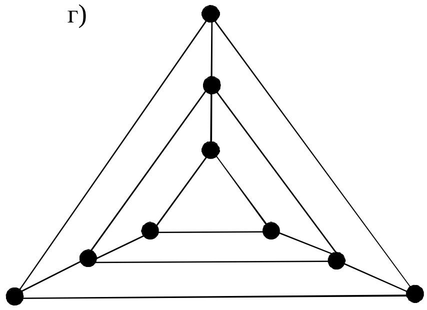
б)



в)

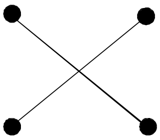


г)

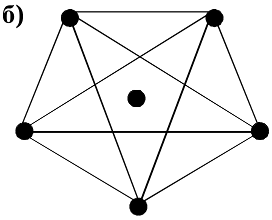


3.12. $a=0,\ b=1$. **3.13.** $a=1,\ b=0$. **3.14.** $\sum_i a_{ii}$. **3.15.** а) 2; б) 3; в) 1.

3.16. **а)**

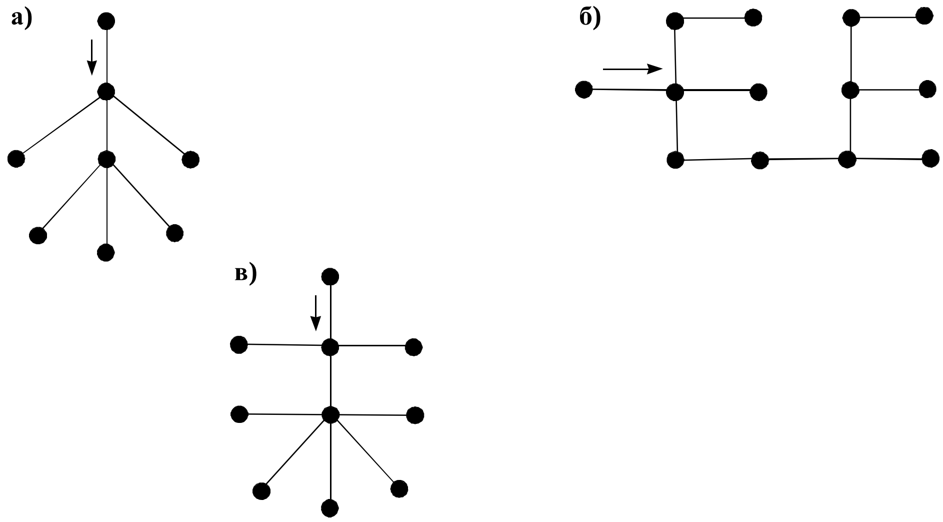


б)



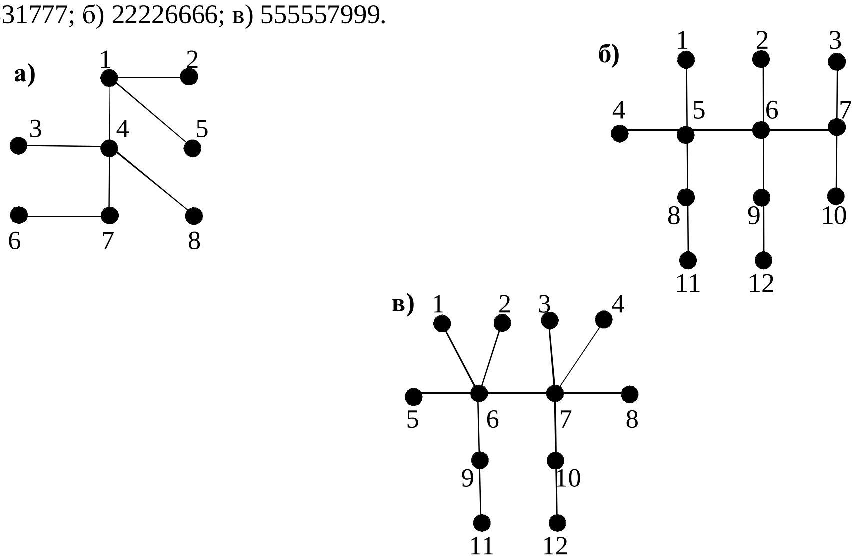
3.17. Связных, так как у каждого несвязного графа дополнение связно. **3.18.** 3. **3.19.** а) 5; б) 2; в) 1. **3.20.** Указание: Пусть n – количество вершин графа. Взять в $\mathbb{R}^3$ n попарно скрещивающихся прямых и расположить вершины графа на этих прямых по одной на каждой прямой. **3.21.** Указание: Начать нумерацию с вершины, не имеющей входящих в неё рёбер. **3.22.** Неверно. **3.26.** 3. **3.27.** $\sum_{i=1}^{n} |\varepsilon_i - \eta_i|$. **3.28.** а) 0,1,2,3,4; б) 0,1,2,3; в) 0,1,…,5; г) 0,1,2,…,6; д) 0, 1, … , 9. **3.29.** а) 1; б) 2; в) $m+n-2$; г) n; д) 2. **3.30.** Да. **3.31.** 5. **3.32.** $d(G)=3$, $r(G)=2$, вершины 8 и 9 – центры. **3.33.** а) n; б) 1; в) $r(G)=1$ при $m=1$, $r(G)=2$ при $m \geq 2$. **3.34.** а) $r(C_n)=[n/2]$; центром является вершина с номером $\frac{n+1}{2}$, если n – нечётное число, и вершины с номерами $\frac{n}{2}$, $\frac{n+1}{2}$, если n чётное. **3.35. а)** $Â = 2^6 = 64$, $Ð = 6 \cdot 2^5 = 192$; б) $Â = 12$, $Ð = 30$; в) $Â = mn$, $Ð = 2mn - n$; г) $Â = mn$, $Ð = 2mn$. **3.37.** 4-1-2-3-1-5-3-4-5. **3.38.** а) Существует эйлеров цикл; б) не существуют; в) существует эйлеров цикл; г) существует эйлеров цикл; д) не существуют. **3.39.** а) $K_{2,2k-1}$; б) $K_{2m,2k}$. **3.40.** а) 15678943216384725; б) 2162376578514834. **3.41.** а) 1325126543641; б) 12352478458956906З1. **3.42.** а) Есть гамильтонов путь: 532679841, но нет гамильтонова цикла; б) нет гамильтонова пути. **3.43.** а) $|m-n| \leq 1$: б) $m=n$. **3.44.** Например, (8,6), или (2,8), или (1,6)… Добавление одного ребра не приводит к наличию гамильтонова цикла, а добавление двух, например, (3,7) и (8,6), может привести. **3.46.** 3. **3.47.** а) Всего 12, неизоморфных 2; всего 55, неизоморфных 4. **3.48.** а) 001001010101100111; б)00010111001100010111; в) 0100000111011101. **3.49.** а) Не является (единиц больше, чем нулей); б) является; в) не является (среди первых 9 элементов единиц больше, чем нулей); г) является.

3.50.

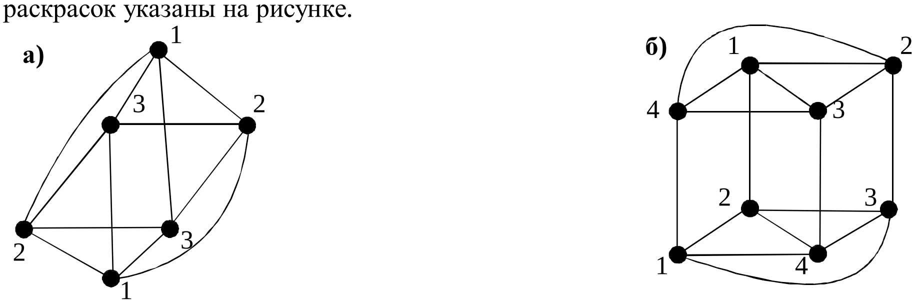


3.52. а) 2331777; б) 22226666; в) 555557999.

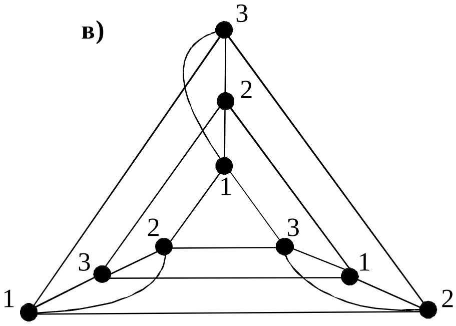
3.53.



3.54. а) 17; б) $(m-1)(n-1)$; в) $mn+1$. **3.55.** а) Нет; б) да; в) да. **3.56.** а) 6; б) $(m-1)(n-1)$; в) 17; г) $(m-1)(n-1)$; д) 7; е) 19. **3.58.** $\nu(G)+1$. **3.59.** $\min(m,n)$. **3.60.** Любое число от 12 до 78. **3.61.** 1 или 2. **3.62.** $\frac{(n-1)(n-2)}{2}$. **3.64.** а) $C_1=(346)$, $C_2=(367)$, $C_3=(4678)$, $C_4=(458)$; б) $C_1=(1234)$, $C_2=(2486)$, $C_3=(5687)$, $C_4=(1375)$, $C_5=(3487)$, $C_6=(1265)$, $C_7=(1378)$. **3.65.** Например, так: $C_2=(1425)$, $C_3=(1526)$, $C_4=(2536)$. **3.66.** $25-15+4=14$. **3.67.** а) 6 и 64; б) 36 и 2^{36}; в) 17 и 2^{17}. **3.68.** а) 10; б) 14. **3.70.** $\hat{A}\geq 21$. **3.71.** а) 11; б) 20; в) 17. **3.72.** а) 3; б) 4. **3.73.** а) 2; б) 2 при чётном n и 3 при нечётном; в) 2; г) 2, если количество вершин не менее двух и 1, если вершина одна. **3.74.** а) $\chi=3$; б) $\chi=4$; в) $\chi=3$; примеры раскрасок указаны на рисунке.

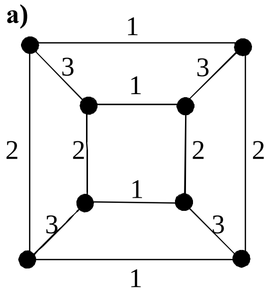


в)

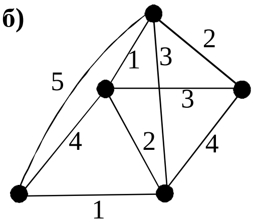


3.75. Да. **3.76.** а) $\chi_P(B_3) = 3$; б) $\chi_P(G) = 5$; в) $\chi_P(G) = 3$. Примеры раскрасок указаны на рисунке.

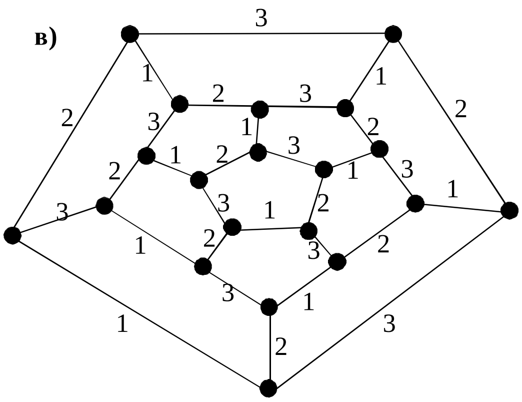
а)



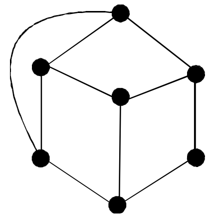
б)



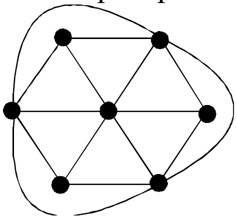
в)



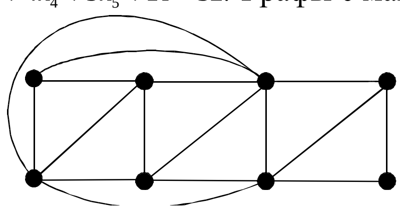
3.77.

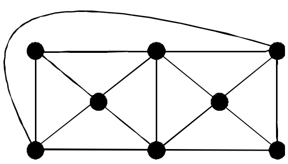


3.78. а) 23; б) 6. **3.82.** $2 \le \tilde{A} \le 16$. **3.83.** 9. **3.84.** а) Да: любой многогранник – это планарный граф; б) нет; в) да; г) да; д) нет; е) нет; ж) нет. **3.85.** $\min(m, n) \le 2$. **3.86.** 15. Граф с максимальным количеством рёбер изображён на рисунке.

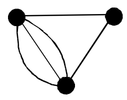


3.87. $2 \le \tilde{A} \le 16$. **3.88.** $2 \le \tilde{A} \le 10$. Указание: надо найти $\max(n_3 + n_4 + n_5 + \mathbf{K})$ при условии $3n_3 + 4n_4 + 5n_5 + \mathbf{K} = 32$. Графы с максимальным числом граней показаны на рисунке.

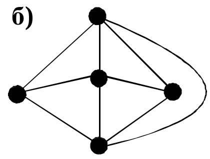




3.89. а)

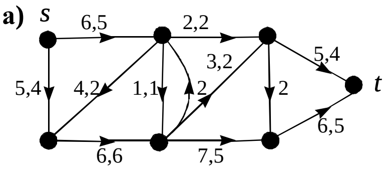


б)



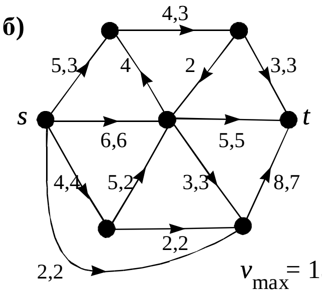
3.90.

а)



$v_{\max} = 9$

б)



$v_{\max} = 15$

3.91. $c(a,t) \geq 1$. При этом условии $v_{\max} = 10$.

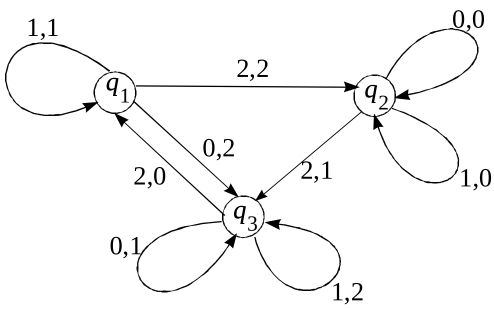
4. Автоматы

4.1. Граф (а) не является диаграммой Мура никакого автомата, так как на диаграмме не указано, в какое состояние должен переходить автомат, если он находится в состоянии q_3 и получает на входе символ 1. Граф (б) также не является диаграммой Мура, так как переход из состояния q_2 при получении символа b определён неоднозначно. Граф (в) является диаграммой Мура конечного автомата.

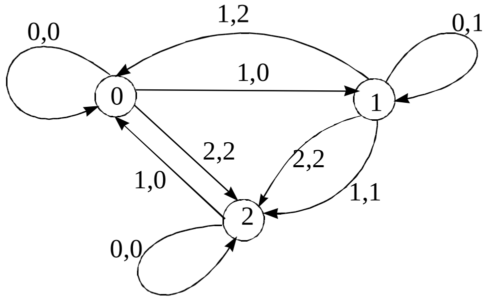
4.2.

	a	b
q_1	q_2 / 0	q_3 / 0
q_2	q_1 / 1	q_2 / 0
q_3	q_4 / 1	q_3 / 0
q_4	q_1 / 1	q_2 / 1

4.3.



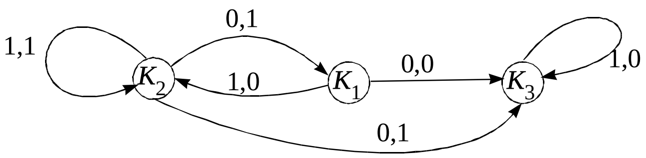
4.4.



4.5. $\overline{\varphi}(q_1, ab) = \varphi(\varphi(q_1, a), b) = \varphi(q_1, b) = q_2$;

$\overline{\varphi}(q_2, abc) = \overline{\varphi}(\varphi(q_2, a), bc) = \overline{\varphi}(q_1, bc) = \varphi(\varphi(q_1, b), c) = \varphi(q_2, c) = q_2$;

$q_1 \xrightarrow{a} q_1 \xrightarrow{b} q_2 \xrightarrow{c} q_2 \xrightarrow{a} q_1$, поэтому $\overline{\varphi}(q_1, abca) = q_1$; $\overline{\psi}(q_1, ba) = \psi(q_1, b)\psi(\varphi(q_1, b), a) = 0\psi(q_2, a) = 00$;
$\underset{0}{q_2 \xrightarrow{a} q_1} \underset{0}{\xrightarrow{a} q_1} \underset{0}{\xrightarrow{a} q_1} \underset{0}{\xrightarrow{b} q_2} \underset{1}{\xrightarrow{b} q_1}$, поэтому $\overline{\psi}(q_2, a^3b^2) = 00001$. **4.6.** $q_1 \xrightarrow{0} q_2 \xrightarrow{0} q_1 \xrightarrow{1} q_2$, поэтому $\overline{\varphi}(q_1, 001) = q_2$; $\overline{\psi}(q_3, 110) = \psi(q_3, 1)\psi(\phi(q_3, 1), 1)\psi(\phi(\phi(q_3, 1), 1), 0) = 1\psi(q_4, 1)\psi(\phi(q_4, 1), 0) = 12\psi(q_4, 0) = 121$. **4.7.** *Решение.* $\psi(q_1, 0) = 1$, $\psi(q_2, 0) = 1$, $\psi(q_3, 0) = 0$, $\psi(q_4, 0) = 1$, $\psi(q_5, 0) = 1$. Следовательно, состояние q_3 отличимо от всех остальных. Мы получаем (пока) следующее разбиение множества $Q = \{q_1, q_2, q_3, q_4, q_5\}$ на классы, т.е. непересекающиеся подмножества: $Q = \{q_3\} \cup \{q_1, q_2, q_4, q_5\}$ (далее это разбиение будет измельчаться). Далее вычисляем: $\psi(q_1, 1) = 1$, $\psi(q_2, 1) = 0$, $\psi(q_4, 1) = 1$, $\psi(q_5, 1) = 0$. Отсюда следует, что q_1 не может лежать в одном классе с q_2 или q_5, q_2 с q_1 или q_4 и т.д. Разбиение, полученное ранее, измельчается до следующего: $Q = \{q_3\} \cup \{q_1, q_4\} \cup \{q_2, q_5\}$. Положим $K_1 = \{q_3\}$, $K_2 = \{q_1, q_4\}$, $K_3 = \{q_2, q_5\}$. Покажем, что это окончательное разбиение. Имеем: $\varphi(q_1, 0) = q_3$, $\varphi(q_4, 0) = q_3$, поэтому $\varphi(K_2, 0) \subseteq K_1$. Аналогично получаем $\varphi(K_2, 1) \subseteq K_2$ и т.д. Следовательно, классы K_1, K_2, K_3 можно считать состояниями нового автомата. Это и есть приведённый автомат, его диаграмма Мура изображена на рисунке.

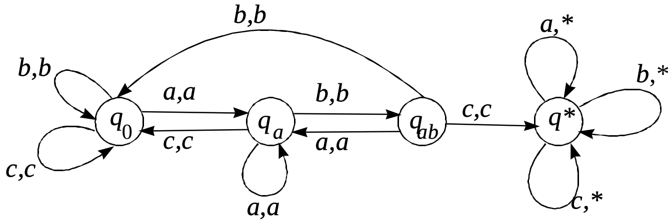


4.8. **В**ерхняя строка таблицы 11011 определяет разбиение $\sigma : Q = \{q_3\} \cup \{q_1, q_2, q_4, q_5\}$, нижняя строка – разбиение $\tau : Q = \{q_1, q_3\} \cup \{q_2, q_4, q_5\}$. Их пересечение $\sigma \cap \tau$ – это разбиение $Q = \{q_1\} \cup \{q_3\} \cup \{q_2, q_4, q_5\}$. Можно проверить, что состояния q_2, q_4, q_5 неотличимы друг от друга. Из таблицы автомата V получается таблица приведённого автомата $\hat{V}$: возьмём по одному представителю в каждом классе разбиения $\sigma \cap \tau$. Таким образом, мы получаем:

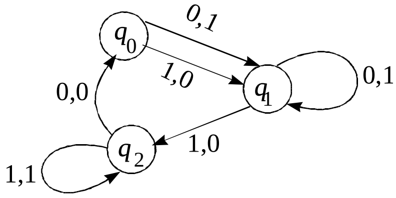
	$\hat{q}_1$	$\hat{q}_2$	$\hat{q}_3$
0	$\hat{q}_3$ 1	$\hat{q}_1$ 1	$\hat{q}_1$ 0
1	$\hat{q}_1$ 1	$\hat{q}_2$ 0	$\hat{q}_3$ 1

4.9. а) Функция f является детерминированной, так как $b(i) = a(i-1)$ при $i \geq 2$ – не зависит от $a(i+1), a(i+2), \ldots$ б) Функция f не является детерминированной, так как $b(1)$ зависит от $a(2)$, которое неизвестно в момент времени $t = 1$. в) Функция f детерминированная, так как $b(i) = \begin{cases} 0, & \text{åñëè } i \text{ í å÷¸òí î}, \\ a(i), & \text{åñëè } i \text{ ÷¸òí î} \end{cases}$ – не зависит от $a(i+1), a(i+2), \ldots$ г) Функция f детерминированной не является, так как выходная последовательность $b(1)b(2)b(3)\ldots$ определится только тогда, когда будут известны $a(i)$ для всех i. Другое объяснение: $0\,0\,0111\ldots1\ldots \xrightarrow{f} 0\,0\,0111\ldots$, $0\,0\,0\,0\,0\,0\ldots0\ldots \xrightarrow{f} 111111\ldots$, а это противоречит определению детерминированности. **4.10.** а) Функция f ограниченно детерминированная (множество вершин информационного дерева имеет два класса эквивалентности). б) Функция f ограниченно детерминированная (4 класса эквивалентности). в) f не является ограниченно детерминированной. **4.11.** **Н**аименьшее число классов эквивалентности равно 4. Один из вариантов разбиения на классы эквивалентности следующий: $\{\alpha, \delta, \ldots\}$, $\{\beta, \kappa, \ldots\}$,

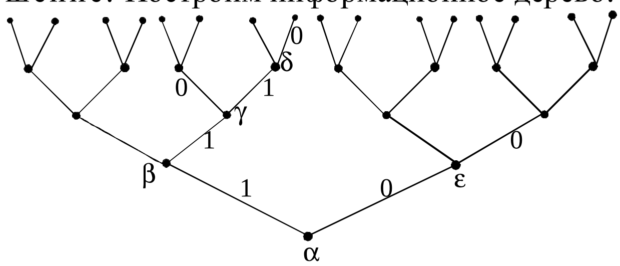
$\{\eta, \ldots\}$, $\{\gamma, \ldots\}$. **4.12.** а) Детерминированная; б) детерминированная; в) недетерминированная. **4.13.** а) Является; б) не является; в) является. **4.14.** а) 3; б) 4; в) 4. **4.15.** Пусть q_0 обозначает начальное состояние, q_a – состояние, в которое автомат перейдёт, получив на входе символ a, q_{ab} – символ b после a, q_* – финальное состояние.



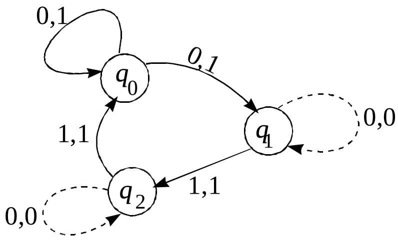
4.16. а) Такого автомата не существует: действительно, у входных слов 011 и 010 совпадают первые две буквы, а выходные слова 101 и 111 этим свойством не обладают. Другими словами, функцию $\overline{\psi}(q_0, x)$ нельзя продолжить до детерминированной функции $f : A^\infty \to B^\infty$. б) Условие детерминированности здесь выполнено. Построим диаграмму Мура автомата:



4.17. Р е ш е н и е. Построим информационное дерево:

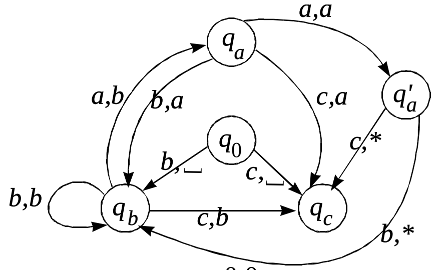


Очевидно, $\alpha \not\sim \beta$, $\beta \not\sim \gamma$, $\alpha \not\sim \gamma$. Значит, количество классов эквивалентности информационного дерева (т.е. количество состояний автомата) не меньше 3. Полагаем $q_0 = \{\alpha, \varepsilon, \delta, \ldots\}$, $q_1 = \{\beta, \ldots\}$, $q_2 = \{\gamma, \ldots\}$ и получаем диаграмму Мура искомого автомата:

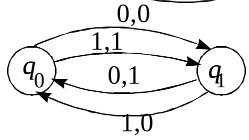


Пунктиром обозначены стрелки, добавленные для обеспечения полноты диаграммы. Эти стрелки можно направить и в другие кружочки.

4.18.



4.19.



4.20. Например,

	q_0	q_1	q_2	q_3
0	q_1 / 1	q_3 / 1	q_3 / 0	q_0 / 1
1	q_2 / 1	q_0 / 0	q_0 / 1	q_1 / 0

4.21. а) $u(t) = y(t) \vee \overline{x}(t)u(t-1)$; **б)** $u(1)u(2)u(3)\ldots = 011\ldots$

4.22. Р е ш е н и е. Умножение в полугруппе S – это отображение $S \times S \to S$. Так как $(st)u = s(tu)$ для всех $s, t, u \in S$, то S – полигон над S.

4.24. $$S(V) = \left\{ \begin{matrix} \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 221 \end{pmatrix}, \begin{pmatrix} 123 \\ 232 \end{pmatrix}, \begin{pmatrix} 123 \\ 332 \end{pmatrix}, \begin{pmatrix} 123 \\ 212 \end{pmatrix}, \begin{pmatrix} 123 \\ 323 \end{pmatrix}, \\ \begin{pmatrix} 123 \\ 121 \end{pmatrix}, \begin{pmatrix} 123 \\ 223 \end{pmatrix}, \begin{pmatrix} 123 \\ 112 \end{pmatrix}, \begin{pmatrix} 123 \\ 111 \end{pmatrix}, \begin{pmatrix} 123 \\ 222 \end{pmatrix}, \begin{pmatrix} 123 \\ 333 \end{pmatrix} \end{matrix} \right\}.$$

4.25. $S(V) \cong \mathbb{Z}_2$.

Содержание

Методические указания

***Клюшин** Александр Викторович*
***Кожухов** Игорь Борисович*
***Олейник** Татьяна Анатольевна*

Сборник задач по дискретной математике.

Текст печатается в авторской редакции. Верстка авторов.

Подписано в печать с оригинал-макета 25.09.08. Формат 60x84 1/16. Печать офсетная. Бумага офсетная. Гарнитура Times New Roman. Усл. печ. л. 6,96. Уч.-изд. л. 6,0. Тираж 600 экз. Заказ 90.

Отпечатано в типографии ИПК МИЭТ.
124498, Москва, Зеленоград, проезд 4806, д. 5, МИЭТ.