

Министерство науки и высшего образования РФ  
ФГБОУ ВО «Ульяновский государственный университет»  
Факультет математики, информационных и авиационных технологий

Сутыркина Е.А.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ  
ПО ДИСЦИПЛИНЕ  
«Дополнительные главы дискретной математики»**

для студентов магистратуры 02.04.03  
«Математическое обеспечение и администрирование информационных систем»  
очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Дополнительные главы дискретной математики» для студентов магистратуры 02.04.03 «Математическое обеспечение и администрирование информационных систем» очной формы обучения / составитель: Е.А.Сутыркина. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов магистратуры по специальности 02.04.03 «Компьютерная безопасность» очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и задания для самостоятельной работы. Методические указания будут полезны при подготовке к лекциям, семинарам и к зачету по данной дисциплине.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИиАТ УлГУ (протокол 2/19 от 19 марта 2019г.)

## Содержание

<b>1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ</b> .....	4
<b>2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ</b> .....	5
<b>Раздел 1. Производящие функции, конечнозначные логики.</b> .....	5
<b>Тема.1</b> Отношения на множествах и комбинаторные отношения. ....	5
<b>Задания для самостоятельной работы по теме 1</b> .....	6
<b>Тема.2</b> Производящие функции. ....	6
<b>Задания для самостоятельной работы по теме 2</b> .....	9
<b>Тема.3</b> Элементы теории чисел.....	9
<b>Задания для самостоятельной работы по теме 3</b> .....	10
<b>Тема.4</b> Конечнозначные логики.....	11
<b>Задания для самостоятельной работы по теме 4</b> .....	11
<b>Контрольные вопросы по разделу 1</b> .....	12
<b>Раздел 2. Кодирование и конечные автоматы.</b> .....	12
<b>Тема.1</b> Кодирование и линейные коды. ....	12
<b>Задания для самостоятельной работы по теме 1</b> .....	17
<b>Тема.2</b> Конечные автоматы. ....	17
<b>Задания для самостоятельной работы по теме 2</b> .....	21
<b>Контрольные вопросы по разделу 2</b> .....	21

## 1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

### основная

1. Марченков С.С., Функциональные уравнения дискретной математики / Марченков С.С. - М. : ФИЗМАТЛИТ, 2013. - 60 с. - ISBN 978-5-9221-1486-8 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <http://www.studentlibrary.ru/book/ISBN9785922114868.html>
2. Гладков Л.А., Дискретная математика : учебник / Под ред. В.М. Курейчика. - М. : ФИЗМАТЛИТ, 2014. - 496 с. - ISBN 978-5-9221-1575-9 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <http://www.studentlibrary.ru/book/ISBN9785922115759.html>

### дополнительная

1. Гаврилов Г.П., Задачи и упражнения по дискретной математике : Учеб. пособие. / Гаврилов Г.П., Сапоженко А.А. - 3-е изд., перераб. - М. : ФИЗМАТЛИТ, 2009. - 416 с. - ISBN 978-5-9221-0477-7 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <http://www.studentlibrary.ru/book/ISBN9785922104777.html>
2. Пинус А.Г., Дискретные функции. Дополнительные главы дискретной математики : учеб. пособие / Пинус А.Г. - Новосибирск : Изд-во НГТУ, 2016. - 92 с. - ISBN 978-5-7782-2838-2 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <http://www.studentlibrary.ru/book/ISBN9785778228382.html>
3. Альметкина Л.А., Линейное программирование. Транспортная задача. Дискретная математика. Теория вероятностей и математическая статистика : учебное пособие / Альметкина Л.А., Громова Е.Ю., Шамилов Р.Р., Юсупова Р.И., Галяметдинов Ю.Г. - Казань : Издательство КНИТУ, 2017. - 84 с. - ISBN 978-5-7882-2189-2 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <http://www.studentlibrary.ru/book/ISBN9785788221892.html> библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/55106.html>

## 2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

### Раздел 1. Производящие функции, конечнозначные логики.

*Тема.1* Отношения на множествах и комбинаторные отношения.

**Пример 1.** Найдем произведение  $\tau\sigma$  двух перестановок из  $S_4$ .

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

В соответствии с нашей договоренностью о порядке, в котором берется композиция двух отображений, умножение начинаем со второй перестановки:

$$\begin{aligned} \tau\sigma(1) &= \tau(\sigma(1)) = \tau(2) = 3, \\ \tau\sigma(2) &= \tau(\sigma(2)) = \tau(3) = 1, \\ \tau\sigma(3) &= \tau(\sigma(3)) = \tau(1) = 4, \\ \tau\sigma(4) &= \tau(\sigma(4)) = \tau(4) = 2. \end{aligned}$$

Таким образом,

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

**Пример 2.** Разложение перестановки в произведение независимых циклов.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 4 & 2 & 5 & 8 & 10 & 9 & 6 & 7 \end{pmatrix} = (1342)(5)(689)(7, 10)$$

Заметим, что 5 осталось на месте. Числа, которые переходят сами в себя, принято опускать в такой записи перестановки, то есть писать просто  $(1342)(689)(7, 10)$ .

Заметим, что на самом деле описанный метод дает запись перестановки в виде **непересекающихся циклов** (то есть ни одно число не входит в два цикла сразу).

*Разложение перестановки в произведение непересекающихся циклов единственно с точностью до изменения порядка сомножителей.*

**Пример 3.** Возведение перестановки в степень.

Вычислим

$$\sigma = \begin{pmatrix} 4 & 3 & 7 & 9 & 2 & 5 & 1 & 6 & 8 & 10 \\ 2 & 8 & 9 & 6 & 1 & 5 & 10 & 3 & 7 & 4 \end{pmatrix}^{2017}.$$

Раскладывая в произведение независимых циклов, получаем

$$\begin{aligned} [(1, 10, 4, 2)(38796)]^{2017} &= (1, 10, 4, 2)^{2017} (38796)^{2017} = \{2017 = 4 \cdot 504 + 1 = 5 \cdot 403 + 2\} = \\ &= ((1, 10, 4, 2)^4)^{504} (1, 10, 4, 2) \cdot ((38796)^5)^{403} (38796)^2 = \\ &= (1, 10, 4, 2)(38796)^2 = (1, 10, 4, 2)(37689). \end{aligned}$$

Мы сразу получили запись результата в виде произведения независимых циклов. При необходимости можно перейти и к развернутой записи:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 1 & 7 & 2 & 5 & 8 & 6 & 9 & 3 & 4 \end{pmatrix}$$

### Задания для самостоятельной работы по теме 1

**Задание 1.** Перемножить перестановки в прямом и обратном порядке.

$$(1) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}.$$

**Задание 2.** Записать в виде произведения независимых циклов.

$$(1) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 5 & 1 & 2 & 4 \end{pmatrix}$$

**Задание 3.** Перемножить перестановки.

$$\begin{aligned} (1) & [(135)(2467)] \cdot [(147)(2356)]; \\ (2) & [(13)(57)(246)] \cdot [(135)(24)(67)]. \end{aligned}$$

**Задание 4.** Вычислить  $(\sigma\tau)^{100}$ ,  $(\sigma\tau)^{666}$ , если

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 8 & 1 & 2 & 4 & 7 & 5 & 3 & 6 & 10 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 6 & 10 & 2 & 4 & 9 & 7 & 3 & 8 \end{pmatrix}.$$

### Тема.2 Производящие функции.

**Пример 1.** Рассмотрим довольно произвольное рекуррентное соотношение:

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 2, \\ a_n &= 6a_{n-1} - 8a_{n-2} + n, n \geq 2 \end{aligned}$$

Запишем производящую функцию для этой последовательности и преобразуем правую часть:

$$G(z) = a_0 + a_1z + \sum_{n=2}^{\infty} (6a_{n-1} - 8a_{n-2} + n)z^n$$

$$G(z) = a_0 + a_1z + 6 \sum_{n=2}^{\infty} a_{n-1}z^n - 8 \sum_{n=2}^{\infty} a_{n-2}z^n + \sum_{n=2}^{\infty} nz^n$$

$$G(z) = a_0 + a_1z + 6z \sum_{n=1}^{\infty} a_n z^n - 8z^2 \sum_{n=0}^{\infty} a_n z^n + \sum_{n=2}^{\infty} nz^n$$

$$G(z) = a_0 + a_1z + 6z(G(z) - a_0) - 8z^2G(z) + \sum_{n=2}^{\infty} nz^n$$

$$G(z) = 1 - 4z + 6zG(z) - 8z^2G(z) + \sum_{n=2}^{\infty} nz^n$$

Для того, чтобы замкнуть последнюю сумму воспользуемся очень важным приемом, который используется при преобразовании производящих функций.

$$zB'(z) = z \left( \sum_{n=0}^{\infty} b_n z^n \right)' = z \sum_{n=1}^{\infty} n b_n z^{n-1} = \sum_{n=0}^{\infty} n b_n z^n$$

Тогда замкнем последнее слагаемое следующим образом:

$$\sum_{n=2}^{\infty} nz^n = z \sum_{n=2}^{\infty} nz^{n-1} = z \left( \sum_{n=2}^{\infty} z^n \right)'$$

$$\sum_{n=2}^{\infty} z^n = \sum_{n=0}^{\infty} z^n - 1 - z = \frac{1}{1-z} - 1 - z = \frac{z^2}{1-z}$$

$$z \left( \frac{z^2}{1-z} \right)' = \frac{z^2(2-z)}{(1-z)^2}$$

Таким образом, наше последнее слагаемое примет вид:

$$G(z) = 1 - 4z + 6zG(z) - 8z^2G(z) + \frac{z^2(2-z)}{(1-z)^2}$$

Это уравнение для производящей функции. Из него выражаем  $G(z)$

$$G(z) = \frac{1 - 6z + 11z^2 - 5z^3}{(1 - 6z + 8z^2)(1 - z)^2}$$

Разложим знаменатель на множители и разобьём дробь на сумму простых дробей

$$G(z) = \frac{1 - 6z + 11z^2 - 5z^3}{(1 - 6z + 8z^2)(1 - z)^2} = \frac{1 - 6z + 11z^2 - 5z^3}{(1 - 2z)(1 - 4z)(1 - z)^2} = \frac{1/3}{(1 - z)^2} + \frac{7/9}{1 - z} - \frac{1/2}{1 - 2z} + \frac{7/18}{1 - 4z}$$

Разложим первое слагаемое в ряд, используя расширенные биномиальные коэффициенты

$$\frac{1}{(1 - z)^2} = (1 - z)^{-2} = \sum_{n=0}^{\infty} \binom{-2}{n} (-z)^n = \sum_{n=0}^{\infty} (-1)^n \binom{n+1}{1} (-z)^n = \sum_{n=0}^{\infty} (n+1)z^n$$

$$G(z) = \frac{1/3}{(1 - z)^2} + \frac{7/9}{1 - z} - \frac{1/2}{1 - 2z} + \frac{7/18}{1 - 4z} = \frac{1}{3} \sum_{n=0}^{\infty} (n+1)z^n + \frac{7}{9} \sum_{n=0}^{\infty} z^n - \frac{1}{2} \sum_{n=0}^{\infty} 2^n z^n + \frac{7}{18} \sum_{n=0}^{\infty} 4^n z^n$$

$$a_n = \frac{n+1}{3} + \frac{7}{9} - \frac{2^n}{2} + \frac{7 \cdot 4^n}{18} = \frac{7 \cdot 4^n + 6n + 20}{18} - 2^{n-1}$$

**Пример 2.**

$$x_{n+2} + 4x_{n+1} - 5x_n = 0$$

$$\chi(\lambda) = \lambda^2 + 4\lambda - 5 = 0$$

Характеристическое уравнение имеет два действительных различных корня:  $\lambda_1 = 1, \lambda_2 = -5$ .

Поэтому общее решение исходного уравнения имеет вид:

$$x_n = C_1 1^n + C_2 (-5)^n = C_1 + C_2 (-5)^n$$

**Пример 3.**

$$x_{n+2} - 2x_{n+1} + 4x_n = 0$$

$$\chi(\lambda) = \lambda^2 - 2\lambda + 4 = 0$$

Характеристическое уравнение имеет два комплексно сопряженных корня:

$$\lambda_1 = 1 + \sqrt{3}i, \lambda_2 = 1 - \sqrt{3}i. r = \sqrt{1^2 + (\sqrt{3})^2} = 2, \varphi = \arctg\left(\frac{\sqrt{3}}{1}\right) = \frac{\pi}{3}$$

Поэтому общее решение исходного уравнения имеет вид:

$$x_n = 2^n \left( C_1 \cos\left(\frac{\pi n}{3}\right) + C_2 \sin\left(\frac{\pi n}{3}\right) \right)$$

**Пример 4.**

$$x_{n+2} + 6x_{n+1} + 9x_n = 0$$

$$\chi(\lambda) = \lambda^2 + 6\lambda + 9 = 0$$

Характеристическое уравнение имеет кратный корень кратности 2:  $\lambda_1 = \lambda_2 = -3$ .

Поэтому общее решение исходного уравнения имеет вид:

$$x_n = (C_1 + C_2 n) 3^n$$



### Задания для самостоятельной работы по теме 2

**Задание 1.** Пусть  $A(s) = a_0 + a_1s + a_2s^2 + \dots$  - производящая функция для последовательности  $a_0, a_1, a_2, \dots$ . Найдите производящие функции для последовательностей:

а)  $a_0 + a_1, a_1 + a_2, a_2 + a_3, \dots$ ;

б)  $a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots$ ;

**Задание 2.** Найдите производящие функции и явные выражения для элементов последовательностей, заданных рекуррентными формулами:

а)  $a_{n+2} = 4a_{n+1} - 4a_n, a_0 = a_1 = 1$ ;

б)  $a_{n+3} = -3a_{n+2} - 3a_{n+1} - a_n, a_0 = 1, a_1 = a_2 = 0$ ;

**Задание 3.** Пользуясь производящей функцией для чисел Фибоначчи, докажите, что:

а)  $f_0 + f_1 + \dots + f_n = f_{n+2} - 1$ ;

б)  $f_0 + f_2 + \dots + f_{2n} = f_{2n+1}$ ;

**Задание 4.** Решить рекуррентное соотношение

$$f(n+2) = -6f(n+1) + 7f(n) \text{ с начальными условиями } f(0) = 2 \text{ и } f(1) = 4.$$

**Задание 5.** Решить рекуррентное соотношение

$$f(n+2) = -2f(n+1) + 3f(n) \text{ с начальными условиями } f(0) = 1, f(1) = 3.$$

**Задание 6.** Решить рекуррентное соотношение

$$f(n+2) = -5f(n+1) - 4f(n) \text{ с начальными условиями } f(0) = 2, f(1) = 3.$$

### Тема.3 Элементы теории чисел

**Пример 1.** Используя доказательство китайской теоремы об остатках, постройте решение системы

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 1 \pmod{7}, \\ x \equiv 0 \pmod{2}. \end{cases}$$

Очевидно, что таким способом удастся решить далеко не всякую систему линейных сравнений.

В качестве универсального способа решения системы линейных сравнений можно указать один очень древний алгоритм. Он применялся еще в античности для решения проблем астрономии.

Суть этого метода раскрывается в решении следующей задачи.

Рассмотрим систему

$$\begin{cases} 3x \equiv 5 \pmod{7}, \\ 4x \equiv 6 \pmod{10}, \\ x \equiv 1 \pmod{2}. \end{cases}$$

Для первого сравнения имеем единственное решение

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

Вычеты этого класса следующие

$$x = 4 + 7t, t \in \mathbb{Z}.$$

Найдем решение первого сравнения, которое одновременно удовлетворяет и второму:

$$4(4 + 7t) \equiv 6 \pmod{10}.$$

Разделив на 2, получим

$$4t \equiv 0 \pmod{5},$$

$$t \equiv 0 \pmod{5},$$

то есть

$$t = 5s, s \in \mathbb{Z}.$$

Итак, первым двум сравнениям удовлетворяют вычеты вида

$$x = 4 + 7 \cdot 5 \cdot s.$$

Подставим это выражение для  $x$  в третье сравнение:

$$4 + 35s \equiv 1 \pmod{2}.$$

Откуда получаем, что

$$s \equiv 1 \pmod{2} \text{ и } s = 1 + 2v.$$

Окончательно

$$x = 4 + 35s = 39 + 70v \text{ или } x \equiv 39 \pmod{70}.$$

По модулю 140 система имеет два решения:

$$x \equiv 39 \pmod{140}, x \equiv 109 \pmod{140}.$$

### *Задания для самостоятельной работы по теме 3*

**Задание 1.** Решить системы сравнений

$$\begin{cases} x \equiv 7 \pmod{12}, \\ x \equiv 4 \pmod{15}, \\ x \equiv -2 \pmod{21}; \end{cases} \begin{cases} 7x \equiv 5 \pmod{11}, \\ 13x \equiv 12 \pmod{23}, \\ 15x \equiv 6 \pmod{21}; \end{cases} \begin{cases} 4x \equiv 1 \pmod{9}, \\ 5x \equiv 3 \pmod{7}, \\ 4x \equiv 16 \pmod{12}. \end{cases}$$

**Задание 2.** При каких значениях  $a$  следующая система сравнений совместна:

$$\begin{cases} x \equiv 5 \pmod{18}, \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}? \end{cases}$$

**Задание 3.** Найти наименьшее натуральное число, которое при делении на  $n$  дает остаток  $n-1$ , а при делении на  $n+1$  дает остаток  $n$ .

**Тема.4** Конечнзначные логики

**Пример 1.** Используя метод сведения к заведомо полным системам, доказать полноту в Pk следующей системы:

$$\{k-1, x-y+2, x^2 \dot{-} y\}$$

*Решение.* Очевидно, что  $x-y+2$  — существенная функция, принимающая все  $k$  значений. Далее,  $(k-1)^2 \dot{-} (k-1) = 0$ ,  $(k-1)^2 \dot{-} 0 = 1$ ,  $x-1+2 = x+1 = \bar{x}$ ,  $0+1 = 1$ ,  $1^2-x = j_0(x)$ . Также есть все константы и все  $j_i$ ,  $x-(y+2)+2 = x-y$ ,  $x-y-\dots-y = x+y \Rightarrow \underbrace{j_1(x) + \dots + j_1(x)}_{k-1} = J_1(x)$ ,  $h_{0,1}(x) = x + j_0(x) + J_1(x)$ , также имеется  $x + j_0(x)$ .

**Пример 2.** Используя метод сведения к заведомо полным системам, доказать полноту в Pk следующей системы:

$$\{(1 \dot{-} x) \cdot y + \bar{x} \cdot (1 \dot{-} y)\}$$

*Решение.* Обозначим  $f(x, y) = (1 \dot{-} x) \cdot y + \bar{x} \cdot (1 \dot{-} y)$ .

$$f(x, x) = j_0(x), f(x, j_0(x)) = \bar{x}, j_0(f(j_0(x), x)) = 0, \\ f(0, x) = x + j_0(x), f(j_1(x), x) = h_{0,1}(x),$$

**Пример 3.** Используя метод сведения к заведомо полным системам, доказать полноту в Pk следующей системы:

$$\{x \dot{-} y, (\sim x) - y\}$$

*Решение.* Усеченная разность является существенной функцией, принимающей все  $k$  значений. Далее,  $x \dot{-} x \equiv 0$ ,  $(\sim 0) - 0 = k-1$ ,  $(k-1) - y = \sim y$ ,  $(\sim(\sim x)) - y = x-y$ ,  $x-y-\dots-y = x+y$ ,  $(\dots(x \dot{-} 1) \dot{-} \dots) \dot{-} 1 = \underbrace{j_{k-1}(x)}_{k-2}$ ,  $0 - (k-1) = 1$ ,  $x+1 = \bar{x}$ , следовательно есть все  $j_i(x)$ , а, следовательно, есть и  $x + j_0(x)$ , и  $h_{0,1}(x) = x + j_0(x) + \underbrace{j_1(x) + \dots + j_1(x)}_{k-1}$ . Следовательно, исходная система содержит систему Софи Пикар 1 и является полной.

**Задания для самостоятельной работы по теме 4**

**Задание 1.** Исследовать полноту в Pk следующих систем:

- (a)  $\{\bar{x}, \min(x, y)\}$ ;
- (b)  $\{\min(x, y) - 1\}$ ;
- (c)  $\{J_0(x), x + y, x \cdot y^2\}$ ;
- (d)  $\{1, x^2 + y, x^2 \dot{-} y\}$ ;

## Контрольные вопросы по разделу 1

1. Бинарные отношения.
2. Фактор-множества.
3. Перестановки.
4. Характеристики перестановок.
5. Теорема Пойа.
6. Лемма Бернсайда.
7. Биномиальные коэффициенты.
8. Числа Стирлинга 2-го рода.
9. Числа Белла.
10. Числа Стирлинга 1-го рода.
11. Производящие функции.
12. Последовательность Фибоначчи.
13. Возвратные последовательности.
14. Общее решение возвратного уравнения: случай простых действительных и комплексно-сопряженных корней.
15. Общее решение возвратного уравнения: случай кратных корней.
16. Элементы теории чисел: делимость и делители. НОК, НОД.
17. Деление с остатком. Взаимно простые числа.
18. Сравнимые по модулю числа.
19. Классы вычетов. Операции сложения и умножения. Полнота системы вычетов.
20. Истинное сравнение.
21. Малая теорема Ферма.
22. Функция Эйлера.
23. Теорема Эйлера.
24. Функции конечной логики. Элементарные функции  $P_k$ .
25. Формулы над  $P_k$ . Понятие глубины. Первая и вторая формулы.
26. Понятие полноты. Примеры полных систем в  $P_k$ .
27. Доказательство полноты системы Поста и Вебба в  $P_k$ .
28. Операции замыкания. Свойства замыкания. Замкнутые классы в  $P_k$ .
29. Класс функций, сохраняющих множество  $\varepsilon$ . Предполный класс. Разбиение множества  $E_k$ . Свойства функций к разбиениям.

## Раздел 2. Кодирование и конечные автоматы.

### Тема.1 Кодирование и линейные коды.

**Пример 1.** Найти проверочную матрицу  $H$  линейного кода, если задана порождающая матрица

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

Из следствия нам известно, что вектора, образующие дуальную матрицу  $H$ , должны удовлетворять условию  $H \cdot G^T = 0$ . Т.е.

$$(h_1 h_2 h_3 h_4 h_5 h_6 h_7) \cdot \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = 0$$

Найдём общее решение данной системы уравнений. Чтобы привести её к известному виду ОСЛУ  $Ax = 0$ , транспонируем её справа и слева, тогда получим:

$$G \cdot h = \bar{0} \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} h_1 \\ h_2 \\ \dots \\ h_7 \end{pmatrix} = \bar{0}$$

Приведём матрицу  $G$  к ступенчатому виду:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \text{ то есть } \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} h_1 \\ h_2 \\ \dots \\ h_7 \end{pmatrix} = \bar{0}$$

Получили 4 главных члена и 3 свободных.

Запишем общее решение. Сначала подставляем свободные члены:  $(\bullet \bullet \bullet \bullet h_5 \ h_6 \ h_7)$ , а далее выражаем главные из ступенчатой матрицы, начиная снизу. Помните, что сложение происходит по mod 2.

Из последней строки получим  $0 \cdot h_1 + 0 \cdot h_2 + 0 \cdot h_3 + 1 \cdot h_4 + 1 \cdot h_5 + 1 \cdot h_6 + 1 \cdot h_7 = 0$ , следовательно,  $h_4 = h_5 + h_6 + h_7$ .

Из предпоследней получим  $0 \cdot h_1 + 0 \cdot h_2 + 1 \cdot h_3 + 0 \cdot h_4 + 1 \cdot h_5 + 1 \cdot h_6 + 0 \cdot h_7 = 0$ , следовательно,  $h_3 = h_5 + h_6$ . И т.д.

В итоге, получим общее решение:  $(h_6 + h_7 \ h_5 + h_7 \ h_5 + h_6 \ h_5 + h_6 + h_7 \ h_5 \ h_6 \ h_7)$ .

Теперь вместо свободных членов  $h_5, h_6, h_7$  подставим «1» и «0», чтобы получить разложение по базису дуального кода.

1.  $h_5 = 1, h_6 = 0, h_7 = 0 \Rightarrow (0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0)$
2.  $h_5 = 0, h_6 = 1, h_7 = 0 \Rightarrow (1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0)$
3.  $h_5 = 0, h_6 = 0, h_7 = 1 \Rightarrow (1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1)$

Получим, что проверочная матриц размерности  $n - k \times n = 7 - 4 \times 7$  имеет вид:

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

**Пример 2.** Алгоритм декодирования по синдрому

В общем виде алгоритм декодирования по синдрому выглядит следующим образом:

1. Разбиваем пространство  $V_n$  на смежные классы по коду.
2. В каждом смежном классе находим лидеров.
3. Вычисляем синдромы для лидеров.
4. Для принятого слова вычисляем синдром.
5. К принятому слову прибавляем лидера, соответствующего вычисленному синдрому.

✚ Рассмотрим  $(4,2)$ -код с порождающей матрицей  $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ .

✚ Вычислим проверочную матрицу  $H$ .

1. Воспользуемся равенством  $H \cdot G^T = 0$ , откуда получим ОСЛУ:

$$G \cdot h = \bar{0} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \end{pmatrix} = \bar{0}$$

2. Матрица  $G$  уже приведена к ступенчатому виду, из которого видно, что у нас имеется 2 главных и 2 свободных члена.

3. Запишем общее решение ОСЛУ:

- Подставим свободные члены:  $(\bullet \bullet h_3 h_4)$
- Выразим главные:
 
$$0 \cdot h_1 + 1 \cdot h_2 + 0 \cdot h_3 + 1 \cdot h_4 = 0 \Rightarrow h_2 = h_4$$

$$1 \cdot h_1 + 0 \cdot h_2 + 1 \cdot h_3 + 1 \cdot h_4 = 0 \Rightarrow h_1 = h_3 + h_4$$

В итоге, получим общее решение:  $(h_3 + h_4 \quad h_4 \quad h_3 \quad h_4)$ .

4. Теперь вместо свободных членов  $h_3, h_4$  подставим «1» и «0», чтобы получить разложение по базису дуального кода.

- a.  $h_3 = 1, h_4 = 0 \Rightarrow (1 \ 0 \ 1 \ 0)$
- b.  $h_3 = 0, h_4 = 1 \Rightarrow (1 \ 1 \ 0 \ 1)$

5. Получим, что проверочная матриц размерности  $n - k \times n = 4 - 2 \times 4$  имеет вид:

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

✚ Перейдём к алгоритму декодирования.

1. Так как в порождающей матрице 2 кодовых слова длины 4, то в коде всего  $2^2 = 4$  слова. Следовательно, мы можем закодировать всего 4 сообщения.

сообщение	00	01	10	11
-----------	----	----	----	----

Далее разобьём пространство  $V_4$  на 4 смежных класса.

сообщение	00	01	10	11
1й см.класс (код)				
2й см.класс				
3й см.класс				
4й см.класс				

Столбец для сообщения «00» заполняется первым, начиная с «0000», двигая 1-ку с первого до предпоследнего бита: «1000», «0100», «0010»:

сообщение	00	01	10	11
1й см.класс (код)	0000			
2й см.класс	1000			
3й см.класс	0100			
4й см.класс	0010			

Теперь заполним строку для 1го смежного класса. Элементы 1го смежного класса – это элементы кода, они находятся умножением текущего сообщения  $A$  на порождающую матрицу  $G$ .  
Для сообщения  $A=«01»$  получим соответствующий элемент:

$$A \cdot G = (0 \ 1) \cdot \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 0101.$$

Соответственно, для сообщения «10» получим:  $A \cdot G = (1 \ 0) \cdot \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 1011.$

И, последний элемент 1го смежного класса найдём как:  $A \cdot G = (1 \ 1) \cdot \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 1110.$

Помните, что сложение происходит по mod 2, т.е.  $1 + 1 = 0 \text{ mod } 2$

В итоге, получим таблицу с 1м смежным классом:

сообщение	00	01	10	11
1й см.класс (код)	0000	0101	1011	1110
2й см.класс	1000			
3й см.класс	0100			
4й см.класс	0010			

Элементы оставшихся смежных классов находятся сложением.

Найдём элементы 2го, 3го и 4го см.классов для сообщения «01». Для этого сложим «0101» соответствующими элементами первого столбца:

$$0101 + 1000 = 1101; \quad 0101 + 0100 = 0001; \quad 0101 + 0010 = 0111;$$

Запишем их в таблицу:

сообщение	00	01	10	11
1й см.класс (код)	0000	0101	1011	1110
2й см.класс	1000	1101		
3й см.класс	0100	0001		
4й см.класс	0010	0111		

Аналогично заполним оставшиеся ячейки. В итоге получим таблицу:

сообщение	00	01	10	11
1й см.класс (код)	0000	0101	1011	1110
2й см.класс	1000	1101	0011	0110
3й см.класс	0100	0001	1111	1010
4й см.класс	0010	0111	1001	1100

2. Перейдём ко второму пункту алгоритма. Здесь необходимо найти лидеров смежных классов. Лидер смежного класса – это вектор, имеющий наименьший вес, т.е. вектор, содержащий наименьшее количество «1».

Для каждого из смежных классов лидер находится в первом столбце. Исключение составляет 3й смежный класс, но об этом чуть позже.

сообщение	00	01	10	11
1й см.класс (код)	0000	0101	1011	1110
2й см.класс	1000	1101	0011	0110
3й см.класс	0100	0001	1111	1010
4й см.класс	0010	0111	1001	1100
	Лидеры смежных классов			

3. Для выбранных лидеров  $L$  вычислим синдромы  $S_L = HL^T$ .

Например для лидера 3го смежного класса  $L_3$ , получим:

$$S_{L_3} = HL_3^T = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} (0100)^T = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Соответственно, таблица примет вид:

сообщение	00	01	10	11	S
1й см.класс (код)	0000	0101	1011	1110	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
2й см.класс	1000	1101	0011	0110	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
3й см.класс	0100	0001	1111	1010	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
4й см.класс	0010	0111	1001	1100	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
	Лидеры смежных классов				

4. Перейдём к декодированию. Пусть, принято слово  $y = (1 \ 1 \ 1 \ 1)$ . Вычислим синдром для этого слова по формуле  $S_y = Hy^T$ .





**Пример 2.** Рассмотрим автомат, диаграмма Мура которого имеет вид:

	<p>Здесь          Входной алфавит <math>A = \{a_1, a_2\}</math>,          Множество состояний <math>Q = \{q_1, q_2\}</math></p> <p>Если положить <math>F = \{q_1\}</math>, то автомат допускает множество <math>\{\lambda\}</math>, состоящее только из пустого слова.          Если положить <math>F = \{q_2\}</math>, то автомат допускает множество <math>A^* \setminus \{\lambda\}</math> состоящее из слов алфавита, за исключением пустого слова.</p>
--	---

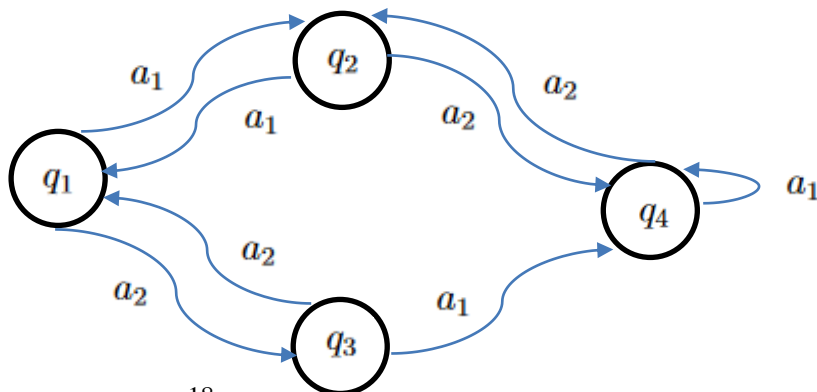
**Пример 3.** Рассмотрим автомат, диаграмма Мура которого имеет вид:

	<p>Здесь          Входной алфавит <math>A = \{a_1, a_2\}</math>,          Множество состояний <math>Q = \{q_1, q_2, q_3\}</math></p> <p>Если положить <math>F = \{q_1\}</math>, то автомат допускает множество <math>\{\lambda, a_2\}</math>.</p> <p>Если положить <math>F = \{q_2\}</math>, то автомат допускает множество слов вида <math>\{\lambda, a_2^n a_1\}</math>.</p> <p>Если положить <math>F = \{q_3\}</math>, то автомат допускает множество слов вида <math>\{\lambda, a_2^n a_1^k, a_2^n a_1^k a_2^l, a_2^n a_1 a_2^l, a_2^n a_1 a_2 a_1^k\}</math>, иначе можно записать <math>\{\lambda, a_2^n a_1 \bar{a}, \bar{a} \neq \lambda\}</math></p>
--	---

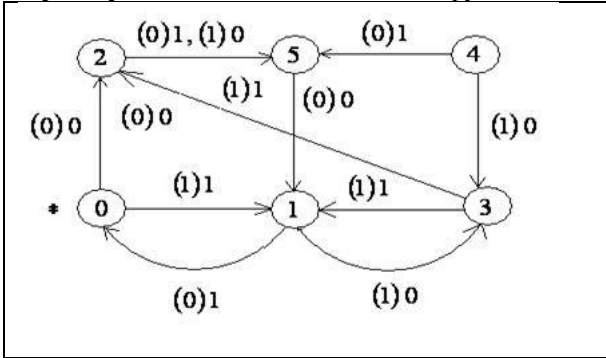
**Пример 4.** Построить диаграмму Мура инициального автомата  $\mathfrak{A} = (A, Q, f, q_1)$ , где входной алфавит  $A = \{a_1, a_2\}$ , множество состояний  $Q = \{q_1, q_2, q_3, q_4\}$ , а функция переходов задаётся таблицей

	$q_1$	$q_2$	$q_3$	$q_4$
$a_1$	$q_2$	$q_1$	$q_4$	$q_4$
$a_2$	$q_3$	$q_4$	$q_1$	$q_2$

Диаграмма Мура имеет вид:



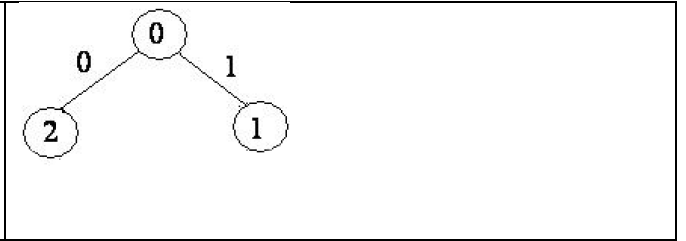
**Пример 5.** Найти вес автоматной функции, заданной диаграммой Мура



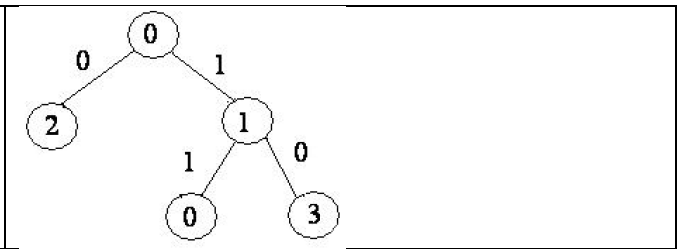
Здесь в скобках указан порядковый номер состояния, выходные состояния опущены.  
 В приведённой диаграмме состояние 4 является недостижимым (в него не входит ни одна дуга), поэтому его сразу можно исключить.

Построим дерево состояний.

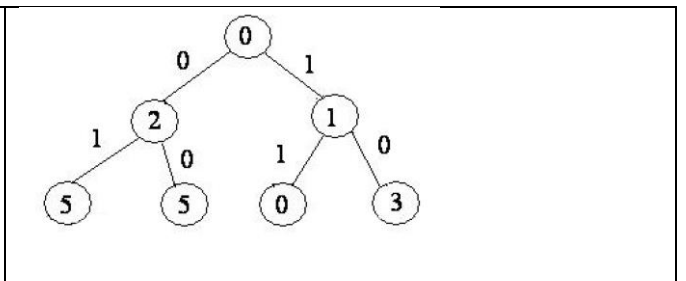
Рассмотрим состояние 0.  
 Из него выходят две дуги:  
 Первая (0) под действием 0 идёт в 2,  
 Вторая (1) под действием 1 идёт в 1.  
 Изобразим это на дереве.



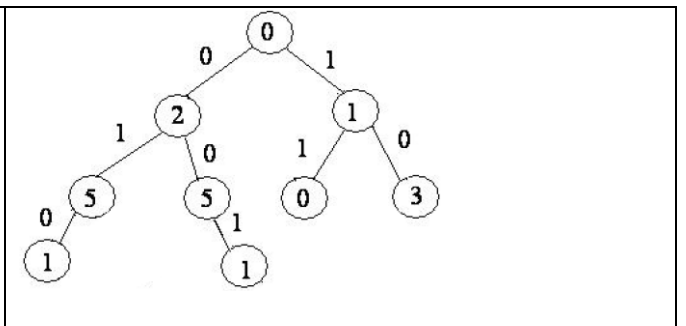
Рассмотрим состояние 1.  
 Из него выходят две дуги:  
 Первая (0) под действием 1 идёт в 0,  
 Вторая (1) под действием 0 идёт в 3.  
 Изобразим это на дереве.



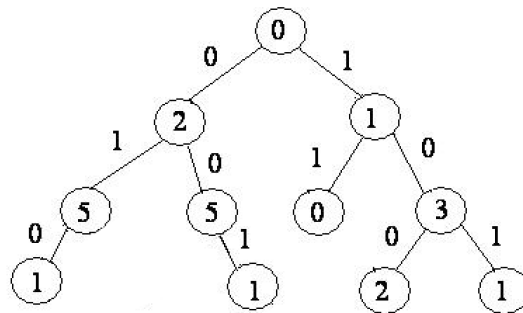
Далее обратимся к состоянию 2.  
 Из него также выходят 2 дуги, которые под действием 1 и 0 соответственно, заходят в состояние 5.  
 Изобразим это на дереве.



Продолжим с состояния 5.  
 Из состояния 5 идут в состояние 1:  
 Первая (0) дуга с входным значением 0  
 Вторая (1) дуга с входным значением 1

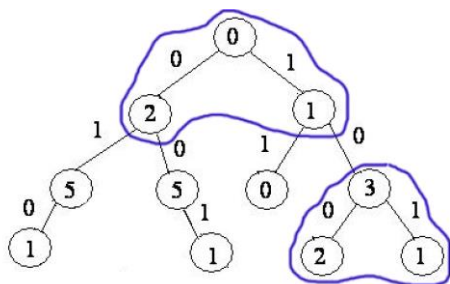


Осталось последнее состояние 3.  
 Первая дуга идет в состояние 2,  
 Вторая – в состояние 1.  
 В итоге получим дерево

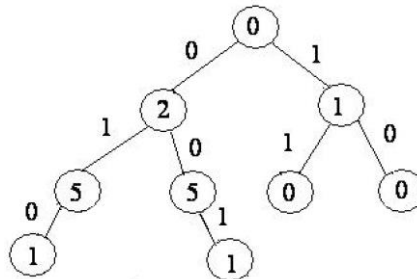


Найдём эквивалентные состояния в полученном дереве.

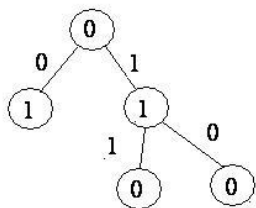
Первой парой эквивалентных состояний являются 0 и 3



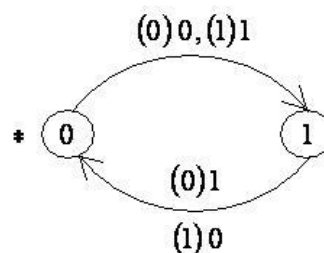
Что позволяет преобразовать дерево к виду



Далее выделяя эквивалентные состояния 1~2 и 0~3~5,  
 получим усечённое дерево



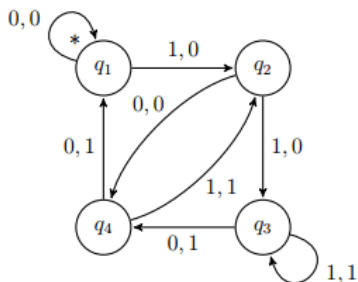
И соответствующую приведённую диаграмму Мура



Так как мы получили два класса эквивалентности, вес дерева равен 2, соответственно, вес автоматной функции тоже равен 2.

## Задания для самостоятельной работы по теме 2

**Задание 1.** Найти вес автоматной функции  $\varphi$ , заданной следующей диаграммой Мура:



### Контрольные вопросы по разделу 2

1. Блочные коды: основные определения, расстояние Хэмминга, вес слова.
2. Код, обнаруживающий ошибки и код, исправляющий ошибки. Пример кодирования сообщения.
3. Максимум правдоподобия. Критерий исправимости. Теорема об исправлении ошибки веса  $t$ .
4. Минимальное расстояние линейного кода. Критерии обнаруживающего и управляющего ошибки кодов.
5. Способы задания линейных кодов. Порождающая матрица, базис линейного кода. Дуальный код. Проверочная матрица.
6. Декодирование линейного кода. Смежные классы: определение, свойства.
7. Лидер смежного класса, синдром вектора. Алгоритм декодирования по синдрому.
8. Конечные автоматы-распознаватели. Определение алфавита, слова, функции переходов, операция конкатенации и её свойства.
9. Понятие простейшего автомата. Инициальный автомат. Канонические уравнения автомата.
10. Диаграмма Мура: алгоритм построения. Множество допустимых слов. Понятие автомата без выходов.
11. Понятие регулярного выражения над алфавитом. Теорема Клини: ход доказательства.