МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ, ИНФОРМАЦИОННЫХ
И АВИАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕОРИИ УПРАВЛЕНИЯ

Рацеев С.М.

Методические указания для самостоятельной работы студентов по дисциплине «Теория кодирования, сжатия и восстановления информации»

для студентов специальностей
10.05.01 «Компьютерная безопасность» и
10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск
2022

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Теория кодирования, сжатия и восстановления информации» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2022.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 3/22 от 19.04.2022 г.).

Тема 1. Основные понятия теории кодирования.

Основные вопросы темы:

Основные понятия теории кодирования. Блочные коды. Основные параметры блочного кода. Метрика Хемминга. Минимальное расстояние кода. Коды с обнаружением и исправлением ошибок, связь с минимальным расстоянием.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 12.1-12.3 учебного пособия [4].

Контрольные вопросы:

1. Основные параметры линейного кода. Метрика Хемминга. 2. Минимальное расстояние кода. Вес кодового вектора, связь с минимальным расстоянием. 3. Критерии обнаружения и исправления ошибок, связь с минимальным расстоянием.

Тема 2. Линейные коды.

Основные вопросы темы:

Код Хемминга, кодирование и декодирование, параметры кода. Оценка Хемминга, совершенный код. Двойственный код. Порождающая и проверочная матрица. Каноническая форма порождающей и проверочной матриц. Вес кодового вектора, связь с минимальным расстоянием. Границы объемов кодов. Граница Хэмминга. Связь проверочной матрицы и минимального расстояния кода. Граница Синглтона. Граница Варшамова-Гильберта.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 12.4-12.8 учебного пособия [4].

Контрольные вопросы:

1. Линейные коды. Двойственный код. Порождающая и проверочная матрица. Число порождающих матриц. 2. Каноническая форма порождающей и проверочной матриц. Теорема о связи порождающей и проверочной матриц. Систематический код. 3. Границы объемов кодов. Граница Хэмминга. Понятие совершенного кода. 4. Связь проверочной матрицы и минимального расстояния кода. Граница Синглтона. 5. Границы объемов кодов. Граница Варшамова-Гильберта. 6. Код Хемминга, кодирование и декодирование, параметры кода. Совершенность кода.

Задачи для самостоятельной работы:

1. Пусть порождающая матрица двоичного $[5, 2]$-кода равна $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$. Найти проверочную матрицу H. Найти кодовое расстояние.

2. Порождающую матрицу двоичного $[5, 2]$-кода $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$. привести к каноническому виду. После этого найти H. Найти кодовое расстояние.

Тема 3. Декодирование линейных кодов.

Основные вопросы темы:

Декодирование линейного кода. Синдромы, свойства синдромов, синдромное декодирование. Систематическое кодирование. Операции над кодами. Мажоритарное декодирование линейного кода. Коды Рида-Маллера. Границы для линейных кодов, исправляющих и обнаруживающих пакеты ошибок.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 12.9-12.14 учебного пособия [4].

Контрольные вопросы:

1. Декодирование линейного кода. Синдромы, свойства синдромов, синдромное декодирование. 2. Критерии линейного кода, исправляющего t ошибок и менее. Таблица стандартного расположения для кода. 3. Операции над кодами: метод комбинирования, расширение двоичного кода, выкалывание. 4. Операции над кодами: выбрасывание, пополнение, удлинение, укорочение. 5. Операции над кодами: конструкция Плоткина. 6. Мажоритарное декодирование линейного кода. 7. Коды Рида-Маллера. Вид порождающей матрицы. Минимальное кодовое расстояние. 8. Декодирование кодов Рида-Маллера, алгоритм Рида. 9. Границы для линейных кодов, исправляющих и обнаруживающих пакеты ошибок.

Задачи для самостоятельной работы:

1. Порождающая матрица линейного [5,2,3]-кода с параметрами $n = 5$, $k = 2$ имеет вид $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$. Найти проверочную матрицу H, кодовое расстояние d. Составить таблицу стандартного расположения. С помощью данной таблицы декодировать вектор $v = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \end{pmatrix}$, т.е. найти информационный вектор i.

2. Мажоритарное декодирование. Проверочная матрица [10,6,3]-кода имеет вид

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

На приемном конце принят вектор $v = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$. Декодировать данный вектор. Найти исходный информационный вектор.

3. Определим $[8, 4]$-код Рида-Маллера порядка 1: $m = 3, n = 8, r = 1$,

$$M_3^1 = \left(\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right) = \begin{pmatrix} G_0 \\ G_1 \end{pmatrix}.$$

Декодировать с помощью данного кода вектор $v = (1, 1, 0, 0, 1, 0, 0, 0)$, в котором не более одной ошибки.

Тема 4. Циклические коды.

Основные вопросы темы:

Описание циклического кода, как идеала фактор-кольца многочленов. Порождающий многочлен, определение и критерий. Проверочный многочлен, критерий принадлежности многочлена коду. Несистематическое и систематическое кодирование. Порождающая матрица циклического кода. Проверочная матрица циклического кода. Каноническая форма базисных матриц циклического кода. Циклический код Хэмминга.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 13.1-13.4 учебного пособия [4].

Контрольные вопросы:

1. Циклические коды. Описание циклического кода как идеала фактор-кольца многочленов. 2. Порождающий многочлен циклического кода, определение и свойства. 3. Порождающая матрица циклического кода. 4. Проверочная матрица циклического кода. Порождающий многочлен дуального кода. 5. Каноническая форма порождающей и проверочной матриц циклического кода.

Задачи для самостоятельной работы:

1. Пусть $F = GF(2)$, $n = 7$, $k = 4$. Построить циклический $[7, 4]$-код с помощью порождающего многочлена $g(x) = 1+x^2+x^3$. Найти порождающую и проверочную матрицы. Найти кодовое расстояние.

2. Для предыдущего примера найти канонический вид порождающей и проверочной матриц.

Тема 5. Декодирование циклических кодов.

Основные вопросы темы:

Пример циклического кода, исправляющего две ошибки, кодирование и декодирование. Порождающий многочлен с заданными свойствами. Свойства порождающего многочлена в примитивном случае: сопряженные корни и вид неприводимого многочлена. Критерий принадлежности многочлена циклическому коду с использованием корней порождающего многочлена, матричная запись. Свойства порождающего многочлена в непримитивном случае. Циклические коды, исправляющие пакеты ошибок. Декодер с вылавливанием пакетов ошибок. Получение кодов методом перемежения. Коды Файра. Циклические коды CRC.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 13.5-13.11 учебного пособия [4].

Контрольные вопросы:

1. Декодирование циклических кодов. Декодер Меггита. 2. Декодирование циклических кодов. Декодер с вылавливанием ошибок (декодер Касами). 3. Порождающий многочлен с заданными свойствами. 4. Свойства порождающего многочлена в примитивном случае: сопряженные корни и вид неприводимого многочлена. 5. Критерий принадлежности многочлена циклическому коду с использованием корней порождающего многочлена (нули кода), матричная запись. 6. Циклический код Хэмминга. 7. Циклический код, исправляющий две ошибки. Алгоритм поиска ошибок. 8. Циклические коды, исправляющие пакеты ошибок. Декодер с вылавливанием пакетов ошибок. 9. Циклические коды, исправляющие пакеты ошибок. Получение кодов методом перемежения. 10. Циклические коды, исправляющие пакеты ошибок. Коды Файра. 11. Циклические коды CRC.

Задачи для самостоятельной работы:

1. Рассмотрим $[15, 9]$-циклический код с порождающим многочленом $g(x) = x^6 + x^5 + x^4 + 1$, который исправляет пакеты ошибок длины не более трех. Пусть на приемном конце принят многочлен $v(x) = x^2 + x^4 + x^7 + x^8 + x^{10}$, в котором пакет ошибок длины не более трех. Декодировать данный многочлен.

2. Циклический код, исправляющий две ошибки. Поле $GF(2^4)$ строится с помощью примитивного многочлена $x^4 + x + 1$, α — примитивный элемент. Двоичный код (БЧХ) с параметрами $n = 15$, $k = 7$ порождается многочленом $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, $\alpha, \alpha^2, \alpha^3, \alpha^4$ — его подряд идущие корни. На приемном конце получен вектор

$$v = \big(\ 1,\ \ 0,\ \ 0,\ \ 1,\ \ 1,\ \ 0,\ \ 0,\ \ 1,\ \ 0,\ \ 0,\ \ 0,\ \ 0,\ \ 0,\ \ 0,\ \ 1\ \big),$$

в котором не более двух ошибок. Найти соответствующий кодовый вектор u и информационный вектор i.

Тема 6. БЧХ коды.

Основные вопросы темы:

Коды БЧХ. Конструктивное расстояние кода. Алгоритм построения кода БЧХ по максимально возможному числу исправляемых ошибок t и длине кода n.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 14.1-14.2 учебного пособия [4].

Контрольные вопросы:

1. Коды БЧХ. Конструктивное расстояние кода. 2. Алгоритм построения кода БЧХ по максимально возможному числу исправляемых ошибок t и длине кода n.

Задачи для самостоятельной работы:

Поле $GF(2^4)$ строится на основе примитивного многочлена $x^4 + x + 1$ с

примитивным элементом α. Построить для данного случая код БЧХ длины $n = 15$, который исправляет до t ошибок: а) $t = 2$, б) $t = 3$, в) $t = 4$.

Тема 7. Декодирование кодов БЧХ.

Основные вопросы темы:

Декодер Питерсона-Горенстейна-Цирлера для двоичного случая. Декодер Питерсона-Горенстейна-Цирлера для общего случая. Алгоритм Форни нахождения значений ошибок для кода БЧХ. Алгоритм Берлекэмпа-Месси. Декодирование кодов БЧХ с использованием алгоритма Берлекэмпа-Месси.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 14.3-14.6, 15.1-15.5 учебного пособия [4].

Контрольные вопросы:

1. Декодер Питерсона-Горенстейна-Цирлера для двоичного случая. 2. Декодер Питерсона-Горенстейна-Цирлера для общего случая. 3. Алгоритм Форни нахождения значений ошибок для кода БЧХ. 4. Алгоритм Берлекэмпа-Месси. 5. Декодирование кодов БЧХ с использованием алгоритма Берлекэмпа-Месси.

Задачи для самостоятельной работы:

1. Декодер Питерсона-Горенстейна-Цирлера (двоичный случай). Пусть поле $GF(2^4)$ порождается примитивным многочленом $p(x) = x^4 + x + 1$, циклический код длины 15 порождается многочленом

$$g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$

На приемном конце получен вектор v, в котором не более трех ошибок. Найти соответствующий кодовый вектор u и информационный вектор i:

$$\text{а) } v = \begin{pmatrix} 1, & 0, & 1, & 1, & 1, & 0, & 0, & 0, & 0, & 1, & 0, & 1, & 1, & 1, & 0 \end{pmatrix},$$

$$\text{б) } v = \begin{pmatrix} 1, & 1, & 1, & 0, & 0, & 0, & 1, & 1, & 0, & 0, & 1, & 0, & 0, & 1, & 0 \end{pmatrix},$$

$$\text{в) } v = \begin{pmatrix} 1, & 0, & 0, & 1, & 0, & 1, & 0, & 0, & 0, & 1, & 1, & 1, & 1, & 0, & 1 \end{pmatrix}.$$

2. Декодер Питерсона-Горенстейна-Цирлера (общий случай). Поле $GF(3^2)$ строится с помощью примитивного многочлена x^2+2x+2, α — примитивный элемент. Код БЧХ над $GF(3)$ с параметрами $n = 8$, $k = 3$ порождается многочленом $g(x) = 2 + x + 2x^2 + 2x^3 + x^5$, $\alpha, \alpha^2, \alpha^3, \alpha^4$ — его подряд идущие корни. На приемном конце получен вектор v, в котором не более двух ошибок. Найти соответствующий кодовый вектор u и информационный вектор i:

$$\text{а) } v = \begin{pmatrix} 1, & 1, & 1, & 2, & 0, & 2, & 2, & 0 \end{pmatrix},$$

$$\text{б) } v = \begin{pmatrix} 0, & 0, & 1, & 0, & 1, & 1, & 0, & 2 \end{pmatrix}.$$

Тема 8. МДР коды.

Основные вопросы темы:

Код Рида-Соломона. Эквивалентные определения кода Рида-Соломона. Кодирование информационных векторов кода Рида-Соломона на основе дискретного преобразования Фурье. Удлинение кодов Рида-Соломона.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 16.1-16.4 учебного пособия [4].

Контрольные вопросы:

1. МДР коды. Эквивалентные условия МДР кода. 2. Код Рида-Соломона. Код Рида-Соломона как МДР код. 3. Кодирование информационных векторов кода Рида-Соломона на основе дискретного преобразования Фурье.

Задачи для самостоятельной работы:

Поле $GF(2^3)$ строится с помощью примитивного многочлена x^3+x+1, α — примитивный элемент. Код Рида-Соломона с параметрами $n=7$, $k=3$, $d=5$ исправляет до двух ошибок. Закодировать информационный вектор i с помощью дискретного преобразования Фурье: $i=\left(\ \alpha^2,\ \ \alpha^6,\ \ \alpha\ \right)$.

Тема 9. Декодирование кодов Рида-Соломона.

Основные вопросы темы:

Декодирование кодов Рида-Соломона на основе метода Питерсона-Горенстейна-Цирлера. Декодирование кодов Рида-Соломона с помощью алгоритма Сугиямы. Эффективный метод декодирования кодов Рида-Соломона. Декодирование кодов Рида-Соломона на основе алгоритма Сугиямы на случай ошибок и стираний. Коды Рида-Соломона и построение каскадных кодов. Обобщенные коды Рида-Соломона. Декодирование обобщенных кодов Рида-Соломона.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 16.5-16.8, 17.1-17.2 учебного пособия [4].

Контрольные вопросы:

1. Декодирование кодов Рида-Соломона на основе декодера Питерсона-Горенстейна-Цирлера. 2. Декодирование кодов Рида-Соломона с помощью алгоритма Сугиямы. 3. Эффективный метод декодирования кодов Рида-Соломона. 4. Декодирование кодов Рида-Соломона на основе алгоритма Сугиямы на случай ошибок и стираний. 5. Удлинение кодов Рида-Соломона. 6. Построение каскадных кодов на основе кодов Рида-Соломона. 7. Обобщенные коды Рида-Соломона. 8. Декодирование обобщенных кодов Рида-Соломона.

Задачи для самостоятельной работы:

1. Поле $GF(2^3)$ строится с помощью примитивного многочлена x^3+x+1, α — примитивный элемент. Код Рида-Соломона с параметрами $n=7$, $k=3$, $d=5$ исправляет до двух ошибок. На приемном конце получен вектор v, в котором не более двух ошибок. Найти соответствующий кодовый вектор u

с помощью алгоритма Питерсона-Горенстейна-Цирлера и информационный вектор i. Получить вектор i с помощью дискретного преобразования Фурье, если:

$$\text{а) } v = \left(\alpha^2,\ 1,\ \alpha,\ \alpha^4,\ \alpha^2,\ \alpha^6,\ 1 \right),$$

$$\text{б) } v = \left(\alpha^6,\ \alpha^4,\ \alpha^6,\ 1,\ \alpha^5,\ \alpha^4,\ \alpha \right).$$

2. Поле $GF(2^3)$ строится с помощью примитивного многочлена $x^3 + x + 1$, α — примитивный элемент. Код Рида-Соломона с параметрами $n = 7$, $k = 3$, $d = 5$ исправляет до двух ошибок. На приемном конце получен вектор v, в котором не более двух ошибок. Найти соответствующий кодовый вектор u (с помощью алгоритма Сугиямы и метода Форни) и информационный вектор i, если:

$$\text{а) } v = \left(1,\ \alpha^4,\ \alpha^5,\ \alpha,\ 1,\ \alpha^4,\ \alpha^3 \right),$$

$$\text{б) } v = \left(\alpha^6,\ \alpha^2,\ \alpha,\ \alpha^3,\ \alpha^4,\ \alpha^3,\ \alpha^6 \right).$$

Тема 10. Альтернативные коды.

Основные вопросы темы:

Альтернативные коды. Декодирование альтернативных кодов. Коды Гоппы. Двоичные коды Гоппы. Примеры кодов Гоппы и варианты их декодирования.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 18.1-18.5 учебного пособия [4].

Контрольные вопросы:

1. Альтернативные коды. 2. Коды Гоппы. 3. Декодирование кодов Гоппы.

Задачи для самостоятельной работы:

Пусть $F = GF(2^3)$ — поле, построенное на основе многочлена $1 + x + x^3$ с примитивным элементом $\alpha \in GF(2^3)$. Код Гоппы $\Gamma(L, G)$ над полем $GF(2)$ задается множеством $L = GF(2^3) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$ и многочленом Гоппы $G(x) = 1 + x + x^2$.

а) Доказать, что код $\Gamma(L, G)$ является сепарабельным.

б) Найти проверочную и порождающую матрицу кода $\Gamma(L, G)$.

в) Найти кодовое расстояние данного кода.

г) Пусть на приемном конце получен вектор $v = \left(1,\ 0,\ 1,\ 1,\ 1,\ 1,\ 0,\ 1 \right)$, в котором не более двух ошибок. Декодировать этот вектор.

Тема 11. Кодовые криптосистемы.

Основные вопросы темы:

Кодовые криптосистемы Мак-Элиса и Нидеррайтера.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 18.6 учебного пособия [4].

Контрольные вопросы:

1. Кодовая криптосистема Мак-Элиса 2. Кодовая криптосистема Нидеррайтера.

Тема 12. Сжатие и восстановление данных.

Основные вопросы темы:

Алфавитное кодирование. Однозначно декодируемые, префиксные и суффиксные коды. Кодовые деревья. Теорема о соответствии между префиксными кодами и кодовыми деревьями. Необходимое и достаточное условие существования префиксного кода с заданными длинами кодовых слов – неравенство Крафта. Необходимое и достаточное условие однозначного декодирования – неравенство Мак-Миллана. Задача оптимального кодирования. Теорема об оценке средней длины оптимального префиксного кода. Теорема о пределе средней длины кодового слова при кодировании длинных блоков. Алгоритмы Фано и Хаффмана. Леммы о строении оптимального кода. Теорема об оптимальности кода Хаффмана.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 11.1-11.4 учебного пособия [4].

Контрольные вопросы:

1. Алфавитное кодирование. Однозначно декодируемые, префиксные и суффиксные коды. 2. Кодовые деревья. Теорема о соответствии между префиксными кодами и кодовыми деревьями. 3. Необходимое и достаточное условие существования префиксного кода с заданными длинами кодовых слов – неравенство Крафта. 4. Необходимое и достаточное условие однозначного декодирования – неравенство Мак-Миллана. 5. Задача оптимального кодирования. Теорема об оценке средней длины оптимального префиксного кода. 6. Теорема о пределе средней длины кодового слова при кодировании длинных блоков. 7. Алгоритмы Фано и Хаффмана. 8. Леммы о строении оптимального кода. Теорема об оптимальности кода Хаффмана.

Литература

[1] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: пер. с англ. – М: Связь, 1979. – 744 с.

[2] Сагалович Ю.Л. Введение в алгебраические коды. Учебное пособие. – 2-е изд., перераб. и доп. – М.: ИППИ РАН, 2010. – 302 с.

[3] Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 596 с.

[4] Рацеев С. М. Элементы высшей алгебры и теории кодирования : учебное пособие для вузов. – СПб. : Лань, 2022. 656 с.

[5] Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.