

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ.....	9
I. ВВЕДЕНИЕ. ОСНОВНЫЕ ПОНЯТИЯ И ТЕРМИНЫ ТЕОРИИ КОДИРОВАНИЯ.....	12
1.1. Начальные сведения о блоковых корректирующих кодах.....	13
1.2. Корректирующие коды и их основные виды.....	22
1.3. Блоковые корректирующие коды с многократной передачей символов.....	29
1.4. Блоковые корректирующие коды с одной проверкой на чётность.....	31
1.5. Блоковые корректирующие коды с разбиением множества запрещённых комбинаций на попарно не пересекающиеся подмножества.....	33
Таблица декодирования.....	37
Сложность кодера.....	40
Сложность декодера, реализующего универсальный алгоритм декодирования.....	41
1.6. Блоковые корректирующие коды с декодированием по методу максимального правдоподобия. Корректирующая способность кода и кодовое расстояние.....	44
1.7. Блоковые корректирующие коды со стиранием символов.....	51
1.8. Блоковые корректирующие коды с проверкой на чётность.....	53
1.9. Понятие свёрточного (непрерывного) корректирующего кода.....	58
1.10. Некоторые уточнения определений основных понятий теории кодирования.....	65

1.11. Приложение. Метрические пространства. Энергия сигнала.....	68
Понятия и соотношения для n -мерного евклидова пространства.....	68
Обобщения.....	73
Применения к описанию сигналов.....	75
1.12. Приложение. Обозначения числовых множеств и элементы комбинаторики.....	78
Обозначения числовые множеств.....	78
Элементы комбинаторики.....	79
1.13. Задачи.....	82
1.14. Выводы.....	87
1.15. Литература.....	88
II. ГРУППОВЫЕ КОДЫ.....	90
2.1. Некоторые сведения из алгебры. Группы, кольца, поля.....	90
Группы. Подгруппы.....	91
Разложение группы по подгруппе.....	102
Фактор-группа.....	107
Циклическая группа.....	108
Кольца.....	109
Поля.....	111
2.2. Описание групповых (n, k) -кодов с помощью порождающих матриц. Преобразование порождающих матриц. О числе различных базисов $N_{(n)}$ в B^n . Кодирование сообщений.....	113
Описание групповых (n, k) -кодов с помощью порождающих матриц.....	113
Преобразование порождающих матриц.....	114
О числе различных базисов $N_{(n)}$ в B^n	128
Кодирование сообщений.....	131

2.3. О числе различных (n, k) -кодов в B^n . Групповой (n, k) -код и его корректирующие свойства. Описание групповых (n, k) -кодов с помощью проверочных матриц.....	133
О числе различных (n, k) -кодов в B^n	133
Групповой (n, k) -код и его корректирующие свойства.....	136
Описание групповых (n, k) -кодов с помощью проверочных матриц.....	137
2.4. Некоторые оценки d_{\min} группового (n, k) -кода. Элементарные оценки сверху и снизу максимальной мощности $m(n, 2t+1)$ $\langle n, 2t+1 \rangle$ -кода. Некоторые совершенные коды.....	146
Верхняя граница Плоткина для d_{\min}	146
Верхняя граница Хэмминга для d_{\min}	146
Нижняя граница Варшамова-Гилберта для d_{\min}	147
Всевозможные систематические $(5, 2)$ -коды.....	151
Элементарные оценки сверху и снизу максимальной мощности $m(n, 2t+1)$ $\langle n, 2t+1 \rangle$ -кода.....	153
Примеры некоторых совершенных кодов.....	156
Двоичный код с многократной передачей символов или двоичный код с повторением нечётной длины $n = 2t+1$	156
Код Хэмминга.....	156
2.5. Принципы подсчёта различных однородных объектов, описываемых с помощью матриц. Основные результаты подсчётов.....	157
Принципы подсчёта различных однородных объектов.....	157
Основные результаты подсчётов.....	159
2.6. Декодирование принятых сообщений в случае группового (n, k) -кода применительно к ДСК.....	162
Стандартное расположение и синдромное декодирование.....	162

Обобщённый ДСК.....	163
Декодирование с помощью стандартного расположения.....	170
Средняя вероятность правильного декодирования.....	179
2.7. Укороченные групповые коды.....	183
2.8. Разновидности порождающих и проверочных матриц групповых (n, k) -кодов.....	184
2.9. Приложение. Линейные векторные пространства и линейные алгебры.....	191
Линейные векторные пространства.....	191
Линейные алгебры.....	192
2.10. Задачи.....	193
2.11. Выводы.....	198
2.12. Литература.....	199
 III. ЦИКЛИЧЕСКИЕ КОДЫ.....	 201
3.1. Кольцо классов вычетов Z_m и его свойства.....	202
3.2. Идеал и некоторые его свойства.....	207
3.3. Идеалы и классы вычетов целых чисел.....	209
3.4. Многочлены.....	215
3.5. Идеалы многочленов и классы вычетов.....	219
3.6. Алгебра многочленов.....	238
3.7. Поля Гауа.....	240
3.8. Циклические коды.....	245
3.9. Матричное описание циклических кодов на основе задания порождающего многочлена $g(X)$ или проверочного многочлена $h(X)$	255
3.10. Способ построения порождающей и проверочной матриц, имеющих каноническую форму, по порождающему многочлену.....	257
3.11. Способ построения порождающей и проверочной матриц по корням порождающего многочлена.....	263

3.12. Числовые циклы и их соответствие минимальным многочленам.....	266
3.13. Корректирующие свойства циклических (n, k) -кодов и выбор их порождающих многочленов.....	272
3.14. Некоторые виды БЧХ-кодов.....	282
БЧХ-коды.....	283
Примитивные БЧХ-коды или БЧХ-коды в узком смысле.....	283
Коды Хэмминга.....	283
Коды Рида-Соломона.....	284
Циклический $(23, 12)$ -код Голея.....	285
3.15. Кодирование и декодирование циклических (n, k) -кодов.....	285
3.16. Приложение. Элементы линейных переключаемых схем и некоторые стандартные схемы.....	289
Ячейка сдвигового регистра.....	289
Сумматор по модулю два.....	292
Умножитель на константу.....	293
Некоторые стандартные схемы.....	294
Сдвиговый регистр.....	294
Умножители многочленов.....	296
Делители многочленов.....	300
3.17. Приложение. Временные функции-оригиналы отдельных символов и их последовательностей. Преобразование Лапласа этих функций.....	301
Линейные эквиваленты ячейки памяти и сдвигового регистра и их передаточные функции.....	306
Умножители многочленов.....	306
Делитель многочленов.....	309
3.18. Приложение. Некоторые сведения из теории чисел. Сравнения и классы вычетов.....	315
Натуральные числа. Простые и составные числа.....	315
Целые числа.....	321

Сравнения.....	325
3.19. Задачи.....	329
3.20. Выводы.....	333
3.21. Литература.....	334
IV. ОТВЕТЫ И РЕШЕНИЯ ЗАДАЧ.....	336
4.1. Ответы и решения задач к разделу I.....	336
4.2. Ответы и решения задач к разделу II.....	359
4.3. Ответы и решения задач к разделу III.....	377
4.4. Литература.....	391
V. ПРИЛОЖЕНИЯ.....	392
5.1. Приложение. Всевозможные систематические (5, 2)-коды с их порождающими и проверочными матрицами.....	392
5.2. Приложение. Разложение бинома X^n+1 , $1 \leq n \leq 31$, на неприводимые сомножители над полем $GF(2)$	401
5.3. Приложение. Некоторые функции ядра и основной библиотеки математической системы Maple V R5.....	403
5.4. Приложение. Таблица разложения бинома X^n+1 на неприводимые сомножители над $GF(2)$	405
5.5. Приложение. Таблица циклических (n, k) -кодов.....	425
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ.....	436

ПРЕДИСЛОВИЕ

Теория кодирования – раздел теории информации, в котором изучаются *корректирующие коды* – коды обнаруживающие и исправляющие ошибки, возникающие вследствие действия шума при хранении и передаче информации. Основной проблемой здесь является экономное использование избыточности для достижения требуемой помехоустойчивости передачи данных по каналу с шумом или их хранения на некотором носителе. Знание этого раздела теории информации необходимо для разработчиков современных электронных цифровых информационных систем.

Ранее, в разделах 6.6 и 6.7 [1.8], были рассмотрены исходные соображения и допущения, положенные в основу реализации процедур блочного кодирования и декодирования; в частности там были изложены *Основная теорема о кодировании и декодировании для СБПК при передаче по нему сообщений* и *Обращение основной теоремы кодирования*. Профессиональная подготовка специалистов по теории кодирования предполагает знание основных положений классической теории информации и, в частности, знание двух вышеупомянутых теорем.

При отборе материала для пособия с целью более детального изложения отобранного материала автор существенно ограничил круг рассматриваемых вопросов теории кодирования. В частности, в данной книге излагаются вопросы построения лишь основных типов корректирующих кодов, свойства которых хорошо изучены и поняты в настоящее время в теории кодирования и понимание основ теории которых позволит продолжить изучение теории кодирования *на профессиональном уровне* [1.1 – 1.4]. Именно поэтому учебное пособие получило название «*Введение в теорию кодирования*».

В частности, в учебном пособии акцент сделан на изложении свойств двоичных блоковых кодов, образующих обширный класс двоичных *групповых* или *линейных* (n, k) -кодов (первый, второй и четвёртый разделы книги), и кодов из подкласса этого класса – так называемых *циклических кодов* (третий, четвёртый и пятый разделы книги). В первом разделе книги в меньшем объёме рассматриваются также *некоторые другие виды корректирующих кодов*.

В первом разделе пособия, выполняющем в нём роль «введения», рассмотрены основные простейшие понятия теории кодирования и основные подходы к созданию корректирующих кодов.

Второй раздел, в котором достаточно глубоко и обстоятельно рассмотрена теория групповых (n, k) -кодов, является прологом к третьему разделу.

Третий раздел пособия содержит наиболее сложный материал теории кодирования – теории циклических (n, k) -кодов. Читатель, освоивший материал этого раздела, сможет успешно конструировать циклические коды с требуемыми свойствами.

Четвёртый раздел пособия содержит формулировки задач, решения или советы по решению этих задач, а также – ответы к задачам.

Пятый раздел – «V. Приложения» содержит инструментарий для практических занятий теорией кодирования. Здесь приведены необходимые сведения для создания конкретных циклических кодов с требуемыми характеристиками.

При написании книги для решения различных задач теории кодирования широко использовались компьютерные пакеты Mathcad 2000, MATLAB 6.0 R12 и Maple V R5.

В большом числе примеров, рассматриваемых в книге, приведен обширный иллюстрационный материал по изучаемым кодам. Этот материал получен с помощью упомянутых выше компьютерных математических пакетов. Для успешно-

го освоения материала учебного пособия и решения ряда задач, приведенных в пособии, применение пакета Maple V R5 является *необходимым*.

Предполагается наличие математической подготовки читателя в объёме программы по высшей математике современного технического вуза.

В качестве справочного материала в книге приведены необходимые сведения из высшей алгебры, теории чисел и другие данные. Естественно, что этот справочный материал не предназначен для первоначального изучения соответствующих разделов математики.

Активное овладение теоретическим материалом, изложенным в книге, невозможно без *самостоятельного* решения многочисленных задач, содержащихся в ней.

Настоящая книга в качестве учебного пособия предназначена в первую очередь для студентов, специализирующихся в области разработки и эксплуатации электронных измерительных систем.

Структура книги и условные обозначения, принятые в книге, такие же, как и в [1.8]. В тех случаях, когда упоминается ещё не определённое понятие с пометкой «(см. ниже)», может оказаться полезным *предметный указатель*.

Предполагается, что материал книги в целом может быть изложен в течение одного семестра при 4-часовой еженедельной аудиторной нагрузке (3 часа лекций и 1 час семинарских занятий).

В.В. Панин