Министерство науки и высшего образования Российской Федерации
_____
САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ПЕТРА ВЕЛИКОГО

В.А.Варгаузин

СТАТИСТИЧЕСКАЯ ТЕОРИЯ РАДИОТЕХНИЧЕСКИХ СИСТЕМ

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

Практикум

Санкт-Петербург
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Лабораторные работы связаны с методами повышения энергетической и спектральной эффективности цифровых систем радиосвязи, включающие помехоустойчивое кодирование и охватывают следующие темы:

- Создание имитационной модели дискретного и непрерывного каналов.
- Исследование свойств помехоустойчивых линейных блоковых кодов.
- Циклические коды БЧХ, CRC и Рида-Соломона.
- Исследование свойств сверточных кодов и декодера Витерби.

Работы проводятся в программной среде MATLAB и среде моделирования SIMULINK.

Базовые сведения о «классических» методах помехоустойчивого блокового и сверточного кодирования и методах их декодирования представлены в [5, *глава 3*]. Сведения о комбинированных методах помехоустойчивого кодирования, сочетающих методы блокового и сверточного кодирования, в частности, о кодировании турбокодом (ТК), а также «классических» сигнально-кодовых конструкциях — изложены в [5, *глава 4*].

Потенциальные свойства помехоустойчивых линейных блоковых кодов, принципы построения линейных блоковых кодов, а также их подмножества — циклических кодов и циклических (двоичных) кодов БЧХ и (недвоичных) Рида-Соломона — изложены в [5, *глава 5*]. Там же рассмотрен принцип декодирования этих кодов, а также свойства циклических кодов CRC (*Cyclic Redundancy Code*), ориентированных на обнаружение ошибочно принятых комбинаций.

В излагаемые ниже методические указания не вошли ставшие «классическими» *итеративные* алгоритмы декодирования ТК и линейных блоковых кодов. Для линейных блоковых кодов такое декодирование является эффективным для их подмножества — так называемых кодов с малой плотностью проверок на четность (*англ LDPC — Low-Density Parity-Check*, в отечественной литературе также часто используется термин«низкоплотностные коды», НП). Алгоритмы итеративного декодирования кодов ТК и НП изложены в [5, *глава 5*].

Эффективность итеративных алгоритмов декодирования может быть исследована самостоятельно после освоения базовых вопросов, рассмотренных в данных методических указаниях.

1. СОЗДАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ ДИСКРЕТНОГО И НЕПРЕРЫВНОГО КАНАЛОВ

Задание 1. Модель дискретно-симметричного канала.

Создать модель, включающую двоичный источник сообщений без избыточности, двоичный дискретно-симметричного канал (*англ. BSC — Binary Symmetric Channel*) связи с вероятностью ошибки p и измеритель оценки $\hat{p}$ вероятности ошибки (относительной частоты ошибок, *англ. BER —Bit Error Rate*) на выходе канала. Продемонстрировать работоспособность модели путем соответствия величин $\hat{p}$ и p.

При неизвестной величине вероятности p определить необходимое число испытаний для нескольких величин доверительных вероятностей, для которых вычислить доверительные интервалы. Построить графики $\hat{p}$ от вероятности p для нескольких фиксированных доверительных вероятностей. Привести на графике границы доверительных интервалов (для этого удобно использовать функцию MATLAB построения графика **errorbar** с синтаксисом errorbar(X,Y,E), *см.* help errorbar).

Выполнить аналогичные вычисления и построение соответствующих графиков при неизвестной экспериментатору величине вероятности p.

Задание 2. Модель с модуляцией и непрерывным каналом.

Создать дискретную модель, включающую двоичный источник сообщений без избыточности, модулятор сигналов ФМ-2 (англ. *BPSK — BinaryPhase Shift Keying*), непрерывный канал с аддитивным шумом с независимыми отсчетами в дискретные моменты времени (*англ. AWGN — Additive White Gaussian Noise Channel*), демодулятор и измеритель оценки $\hat{p}$ вероятности ошибки p на выходе демодулятора.

Произвести оценки вероятности ошибки для различных показателей энергетической эффективности E_b/N_0, где E_b — энергия переданного сигнала, $N_0/2$ — спектральная плотность мощности в полосе частот радиосигнала (совпадающая с дисперсией отсчетов шума модели).

Построить график зависимости $\hat{p}$ от $E_b/N_0 = 0...10$ дБ. Привести теоретическую формулу вероятности ошибки p для сигналов ФМ-2. Сравнить полученную моделированием зависимость с теоретической зависимостью (для этого удобно использовать функцию MATLAB **qfunc)**.

Задание 3. Модель с кодированием.

Дополнить модель, созданную в Задании 1, кодером блокового кода и декодером. В качестве кода использовать код Хэмминга вида $(7,4)$ и соответствующий ему синдромный декодер [5, *глава 5*]. Произвести оценку $\hat{p}_b$ вероятности ошибки p_b на выходе декодера в зависимости от вероятности ошибки канала p.

Задание 4. Энергетическая эффективность кодирования в непрерывном канале.

Пусть в модели, рассмотренной в Задании 3, дискретно-симметричный канал включает в себя модулятор, непрерывный канал с аддитивным шумом с независимыми отсчетами и демодулятор с «жесткими» решениями.

Оценить энергетическую эффективность кода Хэмминга. Для этого, используя зависимости, полученные в Задании 2 и Задании 3, построить зависимости $\hat{p}_b$ от величин E_b/N_0.

Найти граничную величину $(E_b/N_0)_{гр}$, начиная с которой в непрерывном канале система с кодированием оказывается энергетически эффективней системы без кодирования. Оценить энергетический выигрыш от кодирования при вероятности $p_b \approx 10^{-5}$.

Задание 5. Сравнительная эффективность кодирования.

Рассмотренным выше методом оценить энергетическую эффективность кодов Хэмминга вида $(15,11)$ и $(31,26)$. Сделать вывод об энергетической эффективности кода Хэмминга.

Какова скорость кодов? Как связана скорость кода со спектральной эффективностью цифровой системы связи?

2. ИССЛЕДОВАНИЕ СВОЙСТВ ПОМЕХОУСТОЙЧИВЫХ ЛИНЕЙНЫХ БЛОКОВЫХ КОДОВ

Задание 6. Порождающая и проверочная матрицы линейных блоковых кодов [5, *п.3.3*].

Что такое линейный блоковый код ?

Используя функцию MATLAB **hammgen**, сформировать проверочную и порождающую матрицы кода Хэмминга с $M = N - K = 3$ проверками и найти параметры N (число кодовых символов) и K (число кодируемых информационных символов).

Каковы размеры этих матриц ?

Продемонстрировать свойство ортогональности проверочной и порождающей матриц.

Сколько кодовых слов имеет код ?

Используя порождающую матрицу, вычислить все кодовые слова.

Задание 7. Весовой спектр линейного блокового кода.

Что такое весовой спектр линейного блокового кода ?

Вычислить весовой спектр кода Хэмминга, рассмотренного в Задании 6.

Чему равно минимальное расстояние кода ?

Чему равна (гарантированная) корректирующая способность кода ?

Сколько кодовых слов имеют вес 2, 3, 4, 5, 6, 7 ?

Задание 8. Алгоритм синдромного декодирования [5, *п.5.3.1*].

Что такое синдром линейного блокового кода ?

Чему равен синдром кодового слова ?

Для кода Хэмминга, рассмотренного в Задании 6, составить таблицу корректирующих векторов для синдромного декодера (для этого удобно использовать функцию MATLAB **syndtable**). Каковы размеры этой таблицы ? Как связано значение синдрома с табличным вектором ?

Продемонстрировать алгоритм синдромного декодирования на примере декодирования переданного слова, искаженного одной ошибкой в дискретном канале.

Возможно ли правильное декодирование при двух ошибках в кодовом слове кода Хэмминга с $M=3$ и $M=10$ проверками ?

Задание 9. Циклический код [5, *п.3.3.5*].

Какой код называется циклическим ?

Используя функцию MATLAB **cyclpoly**, найти все полиномы, порождающие циклические коды вида $(7,4)$, $(16,11)$, $(23,12)$ и $(35,20)$.

Используя функцию MATLAB **gfweight**, вычислить минимальное расстояние циклического кода вида $(23,12)$. Как называется такой код ?

3. ЦИКЛИЧЕСКИЕ БЛОКОВЫЕ КОДЫ БЧХ, CRC И РИДА-СОЛОМОНА

Задание 10. Коды БЧХ.

Для каких N существует код БЧХ ?

Используя функцию MATLAB **bchgenpoly**, найти порождающие полиномы кодов БЧХ, параметры которых приведены в *Приложении 4*.

Продолжить таблицу *Приложения 4*, используя функцию MATLAB **bchnumerr**.

Задание 11. Энергетическая эффективность кодов БЧХ.

Разработать модель для оценки энергетической эффективности кода БЧХ. В качестве декодера использовать специально разработанный для кодов БЧХ неполный декодер [5, *глава 5*].

Продемонстрировать рост энергетической эффективности с ростом N при примерно одинаковой скорости кода $R \simeq 1/2$ (максимальное значение N выбрать 511).

Чему равна в этом случае спектральная эффективность при модуляции ФМ-2 ?

Задание 12. Коды CRC для обнаружения ошибок [5*, п.3.3.6., п.5.4.6, п.5.4.7*].

В чем сущность алгоритма синдромного обнаружения (детектора) для циклического кода ?

Что такое *пакет ошибок* и *циклический пакет ошибок* ?

Какова вероятность необнаруженного (циклического) пакета ошибок длины M синдромным детектором при использовании циклического кода с $M = N - K$ избыточными символами ?

Разработать модель с кодированием циклическим кодом CRC (порождающие полиномы *см. Приложение 2*) для оценки вероятности необнаруженной ошибки синдромным детектором.

Задание 13. Недвоичные линейные коды [5, *п.5.2.4*].

В основе создания линейных двоичных блоковых кодов лежит метод вычисления значений кодовых символов и сводится к тривиальной операции умножения и операции сложения по модулю два. Использование такого метода для недвоичных кодов, однако, предполагает не столь простые операции над недвоичными символами (которые можно интерпретировать как целые числа) в соответствии с правилами арифметики так называемых конечных полей Галуа (*см. Приложение 3*).

Используя функцию MATLAB **gf**, продемонстрировать операции сложения и умножения между недвоичными символами.

Задание 14. Циклические (недвоичные) коды Рида—Соломона.

По какой формуле вычисляется минимальное расстояние кода Рида—Соломона ?

Для каких N существует код Рида—Соломона ?

Чему равно минимальное расстояние кода Рида—Соломона вида $(7,3)$?

Сколько двоичных символов содержит (недвоичный) символ этого кода ?

Сколько двоичных символов в общей сложности кодирует этот код Рида—Соломона ?

Сколько слов имеет этот код ?

Написать порождающий полином циклического кода Рида-Соломона вида $(255,223)$, используя функцию MATLAB **rsgenpoly**.

Прокомментировать примеры, приведенные в help функций кодирования **rsenc** циклическим кодом Рида—Соломона и декодирования **rsdec** такого кода.

4. ИССЛЕДОВАНИЕ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ КОДИРОВАНИЯ СВЕРТОЧНЫМ КОДОМ

Задание 15. Кодирование [5, *п.3.4*].

В чем отличие кодирования сверточным кодом от кодирования блоковым кодом ?

Что называется *длиной кодового ограничения* сверточного кода ?

Нарисовать схему нерекурсивного сверточного кодера.

Задание 16. Декодер Витерби с «жестким» входом [5, *п.3.4.9*].

Что такое *свободное расстояние* сверточного кода ?

Какой критерий используется при декодировании по Витерби ?

Чему равно число состояний в декодере Витерби ?

Что такое *глубина декодирования* в декодере Витерби ?

Разработать модель для оценки энергетической эффективности сверточного кода при декодировании по алгоритму Витерби «жестких» решений демодулятора. В качестве кода использовать один из «хороших» кодов, полиномы которых приведены в *Приложении 2* для разных длин кодового ограничения.

Провести исследование по выбору минимальной величины глубины декодирования, начиная с которой помехоустойчивость почти не изменяется в области $p_b \approx 10^{-5}...10^{-6}$.

Задание 17. Декодер Витерби с «мягким» входом.

Модифицировать предыдущую модель для возможности декодирования тем же декодером Витерби «мягких» решений демодулятора. Оценить величину энергетического выигрыша при декодировании «мягких» решений.

Сравнить энергетическую эффективность метода передачи со сверточным кодированием и кодированием кодом БЧХ (Задание 11) при примерно одинаковой спектральной эффективности.

Задание 18. Прозрачные коды [5, *п.3.4.5*].

В *Приложении 2* строки, выделенные серым цветом, соответствуют так называемым *прозрачным* кодам. Продемонстрировать это свойство на модели.

ПРИЛОЖЕНИЕ 1. ТАБЛИЦА ПОРОЖДАЮЩИХ ПОЛИНОМОВ КОДОВ CRC

Код	Порождающий полином
CRC-4	$(1+x)(1+x+x^3)=1+x^2+x^3+x^4$
	$(1+x)(1+x^2+x^3)=1+x+x^4$
CRC-8	$(1+x)(1+x^3+x^7)=1+x+x^3+x^4+x^7+x^8$
	$(1+x)(1+x^2+x^3+x^4+x^5+x^6+x^7)=1+x+x^2+x^8$
	$(1+x)(1+x+x^2)(1+x^2+x^3+x^4+x^5)=$ $=1+x^2+x^4+x^6+x^7+x^8$
CRC-12	$(1+x)(1+x^2+x^{11})=1+x+x^2+x^3+x^{11}+x^{12}$
CRC-16	$(1+x)(1+x+x^{15})=1+x^2+x^{15}+x^{16}$
	$(1+x)(1+x^{14}+x^{15})=1+x+x^{14}+x^{16}$
	$(1+x)(1+x+x^2+x^3+x^4+x^{12}+x^{13}+x^{14}+x^{15})=$ $=1+x^5+x^{12}+x^{16}$
CRC-24	$(1+x)(1+x^5+x^{23})=1+x+x^5+x^6+x^{23}+x^{24}$
	$(1+x)(1+x^2+x^3)(1+x^4+x^6+x^9+x^{10})\times$ $\times(1+x+x^3+x^4+x^5+x^6+x^7+x^8+x^{10})=$ $=1+x^8+x^{12}+x^{14}+x^{23}+x^{24}$
CRC-32	$1+x+x^2+x^4+x^5+x^7+x^8+x^{10}+x^{11}+x^{12}+x^{16}+$ $+x^{22}+x^{23}+x^{26}+x^{32}$

ПРИЛОЖЕНИЕ 2. ТАБЛИЦА ПОРОЖДАЮЩИХ ПОЛИНОМОВ СВЕРТОЧНЫХ КОДОВ

Ниже представлена таблица полиномов, поражающих сверточные коды с максимальной величиной свободного расстояния $d_{св}$ при заданной величине кодового ограничения K'. Строки, выделенные серым цветом, соответствуют так называемым *прозрачным* кодам [5, *глава 3*].

K'	**Порождающие полиномы**	**Восьмеричное представление полинома**	$d_{св}$
2	$g_1(z)=1$ $g_2(z)=1+z^{-1}$	1 3	3
3	$g_1(z)=1+z^{-1}+z^{-2}$ $g_2(z)=1+z^{-2}$	7 5	5
4	$g_1(z)=1+z^{-1}+z^{-2}+z^{-3}$ $g_2(z)=1+z^{-1}+z^{-3}$	17 15	6
4	$g_1(z)=1+z^{-1}+z^{-3}$ $g_2(z)=1+z^{-2}+z^{-3}$	15 13	6
5	$g_1(z)=1+z^{-1}+z^{-2}+z^{-4}$ $g_2(z)=1+z^{-3}+z^{-4}$	35 23	7
6	$g_1(z)=1+z^{-1}+z^{-2}+z^{-3}+z^{-5}$ $g_2(z)=1+z^{-2}+z^{-4}+z^{-5}$	75 53	8
6	$g_1(z)=1+z^{-1}+z^{-2}+z^{-4}+z^{-5}$ $g_2(z)=1+z^{-1}+z^{-5}$	73 61	8
7	$g_1(z)=1+z^{-1}+z^{-2}+z^{-3}+z^{-6}$ $g_2(z)=1+z^{-2}+z^{-3}+z^{-5}+z^{-6}$	171 133	10
8	$g_1(z)=1+z^{-1}+z^{-2}+z^{-3}+z^{-4}+z^{-7}$ $g_2(z)=1+z^{-2}+z^{-5}+z^{-6}+z^{-7}$	371 247	10
9	$g_1(z)=1+z^{-1}+z^{-2}+z^{-3}+z^{-5}+z^{-7}+z^{-8}$ $g_2(z)=1+z^{-2}+z^{-3}+z^{-4}+z^{-8}$	753 561	12

ПРИЛОЖЕНИЕ 3. ПРАВИЛА ВЫЧИСЛЕНИЙ В КОНЕЧНЫХ ПОЛЯХ

Рассмотрим структуру конечного поля $GF\left(2^q\right)$ и математические операции между элементами поля. Все 2^q элементов поля образуют множество:

$$\left\{ \underbrace{0 \quad 1=\alpha^0}_{\text{ýëåì åò û GF(2)}} \quad \alpha^1 \quad \alpha^2 \quad \cdots \quad \alpha^{L-1} \right\},$$

где

$$L = 2^q - 1$$

равно числу ненулевых элементов поля. Первые два элемента представляет собой элементы исходного поля $GF\left(2\right)$. *Любой ненулевой элемент A поля представлен степенью элемента-генератора α*, которую обозначим как $\log_\alpha\left(A\right)$. Элемент α принято называть *примитивным элементом* поля или первообразующим элементом.

Элемент α во многом напоминает комплексную экспоненту вида

$$w = e^{j\frac{2\pi}{L}},$$

любая целая степень которой принадлежит конечному множеству ненулевых чисел:

$$\left\{ w^0 \quad w^1 \quad w^2 \quad \cdots \quad w^{L-1} \right\}.$$

Операция *умножения* между этими числами дает снова число из этого множества, поскольку

$$w^i \cdot w^k = w^{i+k \mod L}.$$

Аналогично и правило умножения между ненулевыми элементами конечного поля, согласно которому результатом операции вида

$$\alpha^i \cdot \alpha^k = \alpha^{i+k \mod L},$$

является ненулевой элемент из множества элементов поля $GF\left(2^q\right)$.

Пример представлений ненулевых элементов b, c, d, e, f, g, h поля $GF\left(2^3\right)$ в виде степени примитивного элемента приведен в колонке под названием «Элемент поля/в виде степени» таблицы П3.1.

Таблица П3.1

Элемент поля	**Элемент поля/в виде степени**	**Элемент поля/в виде полинома**	**Двоичное представление**	**Десятичное представление**
b	α^0	1	001	1
c	α^1	α	010	2
d	α^2	α^2	100	4
e	α^3	$\alpha + 1$	011	3
f	α^4	$\alpha^2 + \alpha$	110	6
g	α^5	$\alpha^2 + \alpha + 1$	111	7
h	α^6	$\alpha^2 + 1$	101	5

Рассмотрим пример. Пусть A — любой элемент поля, а $\left(A\right)_2$ и $\left(A\right)_{10}$ — его двоичное представление (приведенное в колонке под названием «Двоичное представление» таблицы П3.1) и десятичное представление (приведенное в последней колонке таблицы под названием «Десятичное представление») соответственно. Будем использовать знак «$\leftrightarrow$» для обозначения того, что $\left(A\right)_2$, $\left(A\right)_{10}$ и $\log_\alpha\left(A\right)$ соответствуют элементу A, а знак «$=$» — для операций в одном представлении. Тогда операция сложения между двумя элементами A и B выполняется по правилу

$$C = A + B \leftrightarrow \left(A\right)_2 \, xor \, \left(B\right)_2,$$

где xor обозначает операцию многоразрядного сложения по модулю два (операция исключающего ИЛИ) между двоичными представлениями элементов поля. Например, для $\left(A\right)_{10} = 3$ и $\left(B\right)_{10} = 5$ имеем:

$$C = A + B \leftrightarrow \left[011\right] xor \left[101\right] = \left[110\right] \leftrightarrow \left(6\right)_{10}.$$

Операция умножения между ненулевыми элементами поля выполняется как сложение между их логарифмами:

$$C = A \cdot B \leftrightarrow \log_\alpha\left(\alpha^{\log_\alpha(A)} \cdot \alpha^{\log_\alpha(B)}\right).$$

Например, для $(A)_{10} = 3$, $(B)_{10} = 5$ получаем

$$C = A \cdot B \leftrightarrow \log_\alpha\left(\alpha^3 \cdot \alpha^6\right) = \log_\alpha\left(\alpha^9\right) = \log_\alpha\left(\alpha^2\right) \leftrightarrow (4)_{10}.$$

Продолжим рассмотрение структуры поля. Во второй колонке таблицы П3.1 под названием «Элемент поля/в виде полинома» приведена запись рассмотренного выше двоичного представления элементов в виде полинома по степеням примитивного элемента α. Возможность такой записи вытекает из того, что для элемента $\alpha^q = \alpha^3$ рассматриваемого поля $GF\left(2^3\right)$ справедливо следующее соотношение:

$$\alpha^3 = \alpha + 1. \qquad (\text{П3.1})$$

При этом $L - q - 1 = 3$ элементов, степень которых больше q, могут быть получены с помощью следующих очевидных рекурсивных соотношений:

$$\alpha^4 = \alpha^1\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha$$
$$\alpha^5 = \alpha^1\alpha^4 = \alpha\left(\alpha^2 + \alpha\right) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$$
$$\alpha^6 = \alpha^1\alpha^5 = \alpha\left(\alpha^2 + \alpha + 1\right) = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1.$$

Важно, что при выбранном представлении элемента α^3 в виде (П3.1) все $2^q - 1$ полиномов, различны, что и требуется для представления всех ненулевых элементов поля.

В результате, например, трехразрядную двоичную комбинацию 110 можно интерпретировать элементом f, который может быть представлен как в виде степени примитивного элемента α^5, так и в виде полинома $1\alpha^2 + 1\alpha^1 + 0\alpha^0 = \alpha^2 + \alpha$ с коэффициентами из поля $GF(2)$.

На математическом языке соотношение (П3.1) означает, что *элемент* α *является корнем примитивного полинома степени* q, *коэффициенты которого являются элементами поля* $GF(2)$. Примитивный полином не может быть представлен в виде произведения полиномов с коэффициентами из поля $GF(2)$. Для рассматриваемого поля $GF(2^3)$ таким полиномом является полином вида

$$D^3 + D + 1, \qquad (\text{П3.2})$$

откуда и следует равенство (П3.1) при нахождении корня α этого полинома, т.е. решения уравнения

$$D^3 + D + 1 = 0$$

с учетом того, что в поле $GF(2)$ обратный элемент (обозначаемый как «-1») совпадает с единичным элементом, т.е. $-1 = 1$.

Смысл введения примитивного полинома в том, что *все математические операции между элементами поля* $GF(2^q)$ *могут интерпретироваться как операции между полиномами по модулю примитивного полинома*. Результатом таких операций являются полиномы (элементы поля), степень которых не превышает степени q примитивного полинома. (Заметим, что элементы исходного двоичного поля $GF(2)$ можно также рассматривать как полиномы с примитивным полиномом $D+1$.)

Например, для рассмотренного выше примера $(A)_{10} = 3$, $(B)_{10} = 5$ имеем $A(\alpha) = \alpha + 1$, $B(\alpha) = \alpha^2 + 1$. При этом:

$$A(\alpha)B(\alpha) = (\alpha+1)(\alpha^2+1) = \alpha^3 + \alpha^2 + \alpha + 1 =$$
$$\alpha^2 + (\alpha^3 + \alpha + 1) = \alpha^2 \mod \alpha^3 + \alpha + 1,$$

откуда $(C)_{10} = 4$.

В результате рассматриваемое поле $GF(2^q)$ оказывается подобным полю $GF(p)$, где p – простое число, а примитивный полином подобен простому числу. В

таком «простом» поле операции сложения и умножения можно рассматривать как обычные операции «по модулю p» между элементами, представленными целыми числами от нуля до $p-1$, т.е.

$$\{0 \quad 1 \quad 2 \quad \ldots \quad p-1\}.$$

Примерами таких полей являются поля $GF(3)$, $GF(5)$, $GF(7)$, $GF(11)$ и т.д.

Из изложенного ясно, что арифметика в поле $GF(2^q)$ однозначно определяется примитивным полиномом. В таблице П3.2 приведены некоторые возможные примитивные полиномы для $q=1,2,...,16$.

Как было отмечено выше, полином степени q является примитивным полиномом поля $GF(2^q)$, если он не может быть представлен в виде произведения полиномов с коэффициентами из поля $GF(2)$. В общем случае таких полиномов много. Например, для поля $GF(2^3)$ помимо полинома (П3.2), как видно из таблицы, можно использовать и второй полином вида:

$$D^3 + D^2 + 1. \qquad (\text{П3.3})$$

При этом, естественно, что вместо таблицы (П3.1), определяющей правила арифметических операций в поле, следует использовать другую таблицу представлений элементов.

Для поля $GF(2^5)$ существует 6 примитивных полиномов, для поля $GF(2^{10})$ — 60, а для поля $GF(2^{16})$ — 2048 (для этих полей в таблице приведен лишь один полином). В этом можно убедиться, используя функцию MATLAB **primpoly**. В соответствии с количеством возможных примитивных полиномов существует, и соответствующее количество правил для этих полей.

Таблица П3.2

q	**Примитивный полином**
1	$D+1$
2	D^2+D+1
3	D^3+D+1
	D^3+D^2+1
4	D^4+D+1
5	D^5+D^2+1
6	D^6+D+1
7	D^7+D^3+1
8	$D^8+D^4+D^3+D^2+1$
9	D^9+D^4+1
10	$D^{10}+D^3+1$
11	$D^{11}+D^2+1$
12	$D^{12}+D^6+D^4+D+1$
13	$D^{13}+D^4+D^3+1$
14	$D^{14}+D^{10}+D^6+D+1$
15	$D^{15}+D+1$
16	$D^{16}+D^{12}+D^3+D+1$
17	$D^{17}+D^3+1$
18	$D^{18}+D^7+1$
19	$D^{19}+D^5+D^2+D+1$
20	$D^{20}+D^3+1$
21	$D^{21}+D^2+1$
22	$D^{22}+D+1$
23	$D^{23}+D^5+1$

ПРИЛОЖЕНИЕ 4. ТАБЛИЦА ПАРАМЕТРОВ КОДОВ БЧХ

Ниже приведены параметры нескольких кодов семейства БЧХ. Здесь N — число кодовых символов, K — число информационных символов, t — так называема *конструктивная корректирующая способность*.

N	K	t
7	4	1

N	K	t
15	11	1
15	7	2
15	5	3

N	K	t
31	26	1
31	21	2
31	16	3
31	11	5
31	6	7

N	K	t
63	57	1
63	51	2
63	45	3
63	39	4
63	36	5
63	30	6
63	24	7
63	18	10
63	16	11
63	10	13
63	7	15

ЛИТЕРАТУРА И ИНТЕРНЕТ

1. **Волков Л. Н., Немировский М. С., Шинаков Ю. С.** Основы цифровой радиосвязи: базовые методы и характеристики: учебн. пособие. — М.: Эхо Трендз, 2005. — 392 с.
2. **Бабков В. Ю., Цикин И. А.** Сотовые системы мобильной радиосвязи: учебн. пособие для вузов. — СПб.:Изд-во Политехнического университета, 2011. — 426 с.
3. **Вернер М.** Основы кодирования: учебник для вузов; пер. с нем. / Под ред. Зинангирова Д. К. — М.: Техносфера, 2004. — 288 с.
4. **Варгаузин В.А., Иванов Д.И, Цикин И.А.** Сетевой доступ к среде моделирования MATLAB на базе служб терминала. Учебно-методическое пособие.: Учебно-методическое пособие. Изд-во Политехнического университета, 2008. — 28 с.
5. **Варгаузин В.А., Цикин И.А.** Методы повышения энергетической и спектральной эффективности в цифровой радиосвязи. — Учебное пособие. СПб., БХВ, 2013. — 400 с.

ВАРГАУЗИН Виктор Анатольевич

СТАТИСТИЧЕСКАЯ ТЕОРИЯ РАДИОТЕХНИЧЕСКИХ СИСТЕМ
Помехоустойчивое кодирование

Лицензия ЛР №020593 от 07.08.97

Налоговая льгота — Общероссийский классификатор продукции ОК 005-93, т.2; 95 3005 — учебная литература

Подписано в печать 25.04.2013. Формат 60x84/16. Печать цифровая.
Усл. печ.л. 1,44. Уч.-изд.л. 1,44. Тираж 50. Заказ

Отпечатано с готового оригинал-макета, предоставленного автором,
в типографии Издательства Политехнического университета
195251, Санкт-Петербург, Политехническая, 29.
Тел.:550-40-14
Тел./факс:297-57-76