**МИНОБРНАУКИ РОССИИ**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №7

Дисциплина: Теория информации

по теме «Помехоустойчивое кодирование. Коды БЧХ»

Выполнил: ст. группы ПВ-21  
Ковалев Павел

Проверил: Флоринский В.В.

Белгород 2020

Цель работы: научиться строить порождающий многочлен кода БЧХ с заданной корректирующей способностью.

1. Рассмотреть поле GF(24); положить m=4.

GF(24)

e0 = 1

e1 = e1

e2 = e2

e3 = e3

e4 = e3 + 1

e5 = e3 + e1 + 1

e6 = e3 + e2 + e1 + 1

e7 = e2 + e1 + 1

e8 = e3 + e2 + e1

e9 = e2 + 1

e10 = e3 + e1

e11 = e3 + e2 + 1

e12 = e1 + 1

e13 = e2 + e1

e14 = e3 + e2

e15 = 1

2. Разложить на неприводимые множители многочлен x15+1.

x15+1=(x+1)(x2+x+1)( x4+x+1)(x4+x3+1**)**

3. Выбрать в качестве примитивного многочлена многочлен x4+x+1. Убедиться в том, что его корень α–примитивный элемент поля GF(24).

P(x)= ( x4+x+1)

4. Выбрать t=2 и рассмотреть элементы α, α2, α3, α4.

Корнями первого множителя являются e*,* e*2,* e*4*, а второго - e*3.* При t=2 исправляются 2 ошибки.

5. Найти в разложении x15+1 минимальные многочлены fj(x) такие, что fj(aj)=0 для j=1,2,3,4.

Минимальный многочлен = (x+1)

6. Положить g(x)=НОК{f1(x),f2(x),f3(x),f4(x)}; определить его степень r.

*g(x) = x8+ x7 + x6 + x4 +1 = (*x4+x+1*)(*x4+x3+x2+x+1*)*

7. Так как n=15, то длина информационного слова k=n-r.

8. Взять произвольное ненулевое информационное слово длиной k. Получить кодовое слово длины n по формуле циклического кодирования.

(x)= 1010101

Длина сообщения:7

Кодирование:

Информационное слово i = 1010101

Информационный многочлен i(x) = 1+x2+x4+x6

xr \* i(x) = x^8 \* (1+x2+x4+x6) = x8 + x10 + x12 + x14

Остаток от деления Res(x) = 1 + x +x2+ x5 + x7

Кодовое слово c = 111001011010101

Кодовый многочлен c(x) = x14 + x12 + x10 + x8 + x7 +x5+ x2 + x+1

9. Внести в кодовое слово 2 произвольные ошибки (инвертировать любые 2 бита слова). Вычислить синдром. Локализовать ошибку и исправить еѐ. Получить информационное слово. Убедиться в идентичности полученного информационного и изначального слов.

Внесем 2 ошибки : в 3 и 8 бит

Кодовое слово с ошибками y = 111101010010101

Декодирование:

Принятое слово y = 111101010010101

Принятый многочлен y(x) = x14 + x12 + x10 + x7 +x5 + x3 + x2 + x+1

S1 = y(E) = e2 + e1

S3 = y(E3) = 0

S13 = e2+1

S1(-1) = (e2+1)(-1) = (e13)(-1) = e2

f: X^2 + (e2 + e1 ) \* X + e4 + e2

Корни уравнения:

f(e0) = e4 + e1 +1 = e3+e1

f(e1) = e4 + e3 + e2 = e2+1

f(e2) = e4+e3+e2= e2+1

f(e3) = e6+e5+e2 = 0

Ошибка в 3 бите.

f(e4) = e6 + e5 + e1 + 1 = e2 +e1+ 1

f(e5) = e6 + e5 + e3 + e1+1 = e3 +e2+ e1+1

f(e6) = e6 +e5+ e1 + 1 = e2+e1+1

f(e7) = e4+e1+1 = e3+e1

f(e8) = e6+e5+e2 = 0

Ошибка в 8 бите.

f(e9) = e4 + e3+e1+1 = e1

f(e10) = e6 + e5 + e3 + e2 = e3

f(e11) = e6 + e5+e3+e1+1 = e3+e2+e1+1

f(e12)= e4 + e3 + e1 + 1 = e1

f(e13) = e4 + e2 = e3 + e2 + 1

f(e14)= e6 + e5 + e3 + e2 = e3

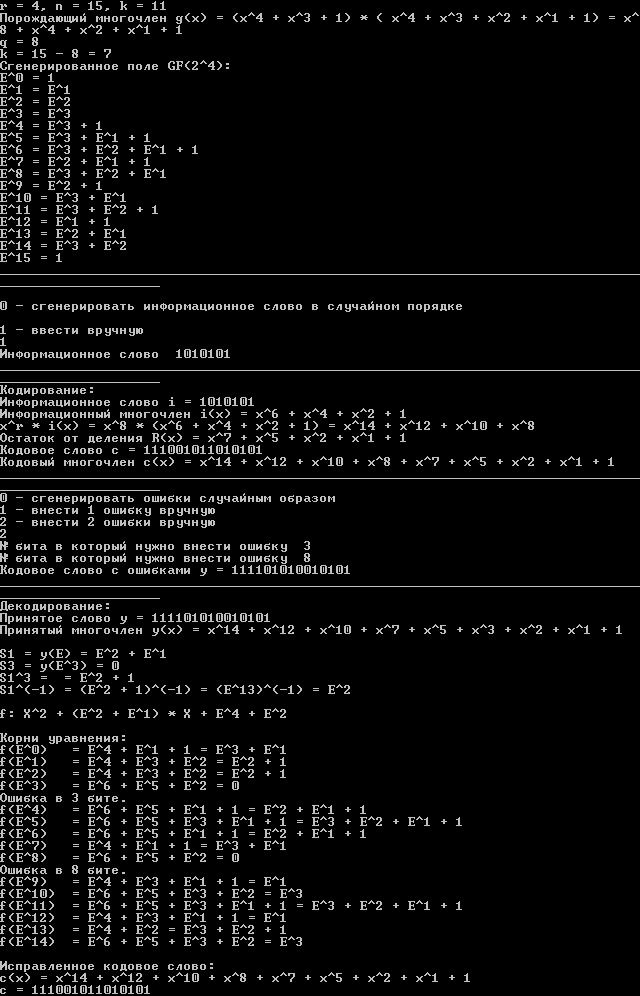
Исправленное кодовое слово:

c(x) = x^14 + x^12 + x^10 + x^8 + x^7 + x^5+x^2 + x + 1

c = 111001011010101

Информационное слово i = 1010101

Информационный многочлен i(x) = x^6 + x^4 + x^2 + 1



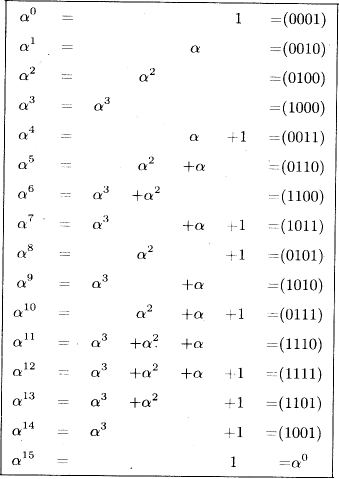
**Вопросы к защите**

*1. Представление элементов поля GF(2n); GF(24).*

На практике широко используются циклические коды с компонентами из расширенных полей Галуа GF(2n). Такими кодами являются коды Боуза-Чоудхури-Хоквингема (БЧХ). Проводя аналогию с полем GF(p), можно сказать, что роль эле­ментов GF(p) в поле GF(2n) играют двоичные слова или многочле­ны степени, меньшей n, а роль простого числа р - неприводимый многочлен степени n.

Для реализации операций в поле GF(2n) в качестве неприводимого многочлена степени n удобнее выбирать примитивный много­член. Для каждого поля Галуа существуют примитивные многочлены всех степеней.

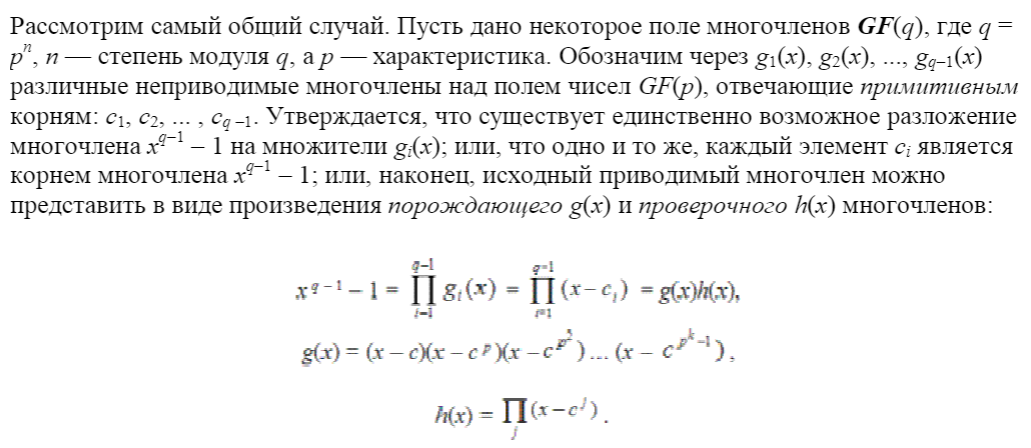
Представление поля GF(24):

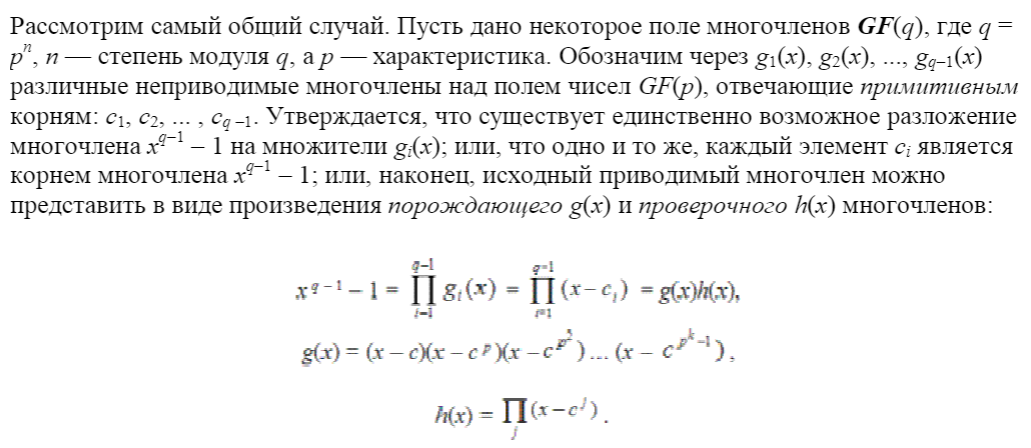


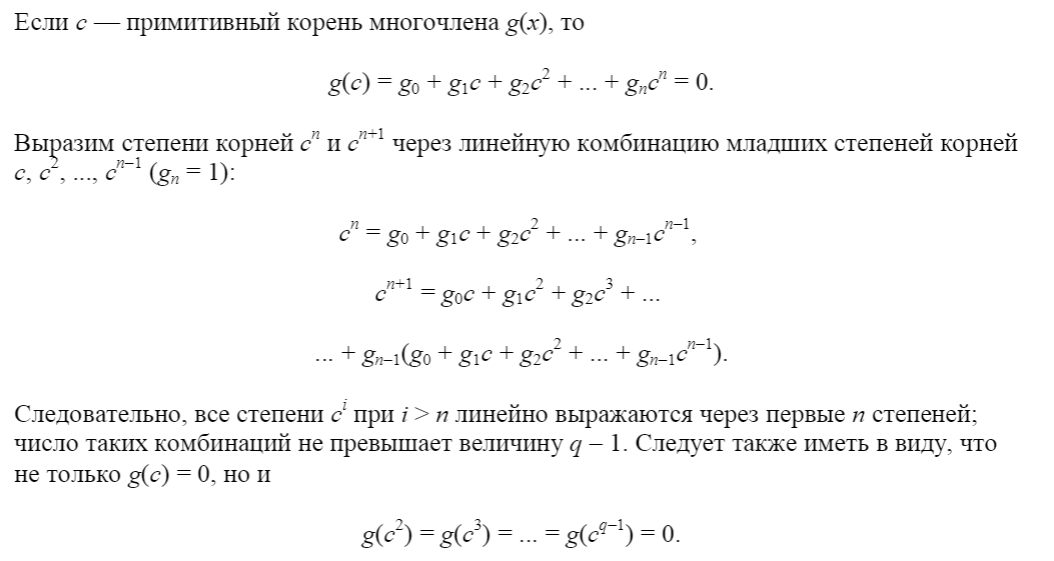
*2. Определение примитивного многочлена степени n (степени 4).*

Примитивным многочленом р(Х) над GF(2) называется непри­водимый многочлен степени n, такой, что в поле GF(2n), построен­ного по модулю р(Х), элемент поля X является примитивным. В качестве примера приведем поле Галуа GF(24), для построения которого был выбран примитивный многочлен четвертой степени Х4 + X + 1.

*3. Разложение многочлена степени 2m - 1 на неприводимые множители.*

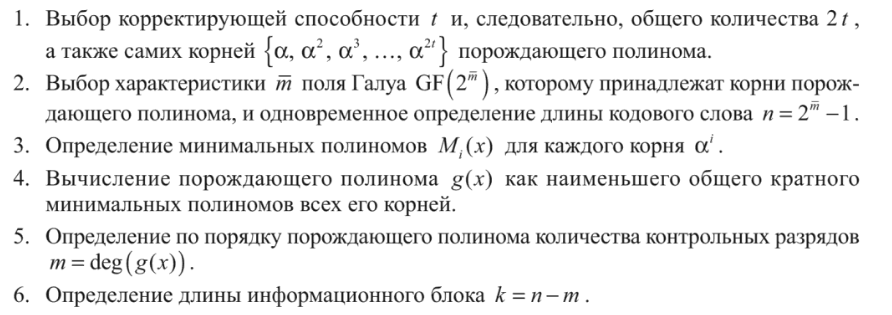


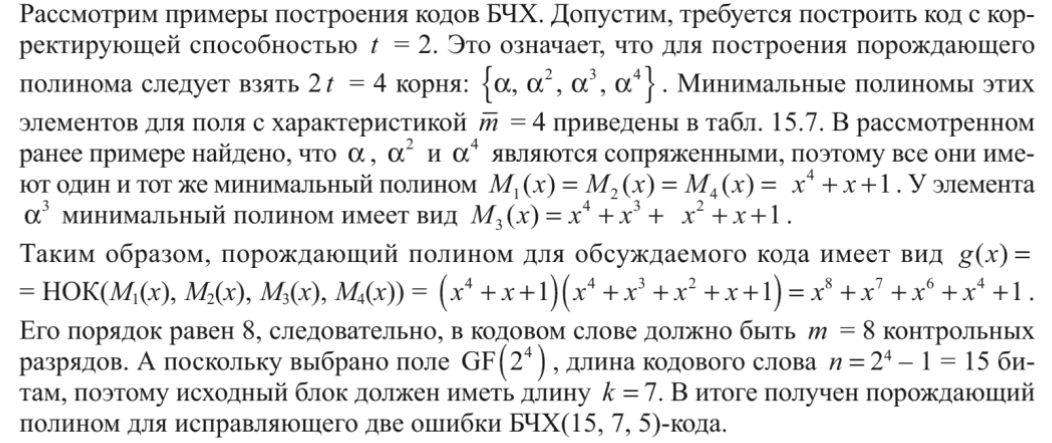


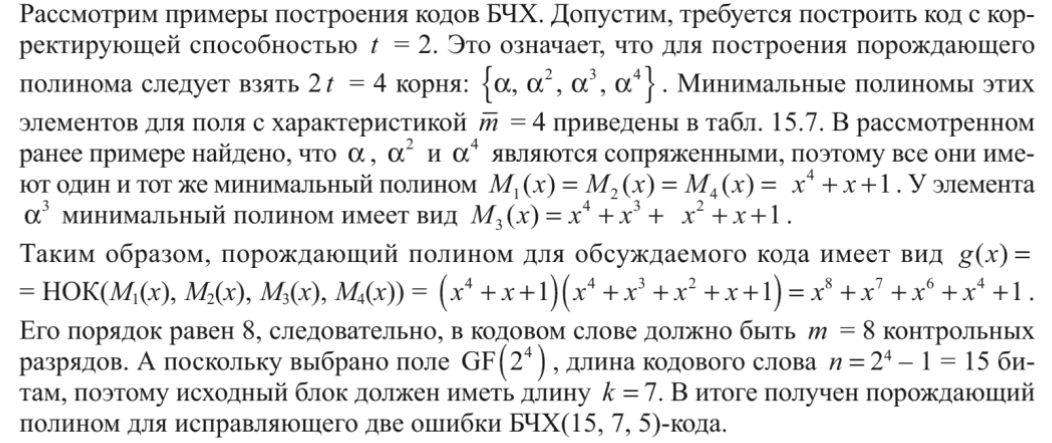


*4. Построение порождающего многочлена кода с корректирующей способностью t.*

Схема построения БЧХ-кода:







На основе поля GF(24) также можно построить коды с t = 3, 4, 5, 6, 7.

5.

**1. Определим количество контрольных m и информационных разрядов k:**

*m = h\*S .*

Параметр h определяется из формулы *n = 2h-1, h = log2(n+1)*

*k = n-m*

**2. Определим параметры образующего полинома:**

- количество минимальных многочленов, входящих в образующий

*L = S = 2;*

- порядок старшего (все минимальные - нечетные) минимального многочлена *r = 2S-1;*

- степень образующего многочлена *b = m = 8.*

**3. Выбор образующего многочлена.**

Из таблицы для минимальных многочленов для кодов БЧХ выбираем два минимальных многочлена

*M1(x)* *и* *M2(x)*

*При этом* *P(x) =M1(x)×M2(x)*

4**. Строим образующую матрицу.**

Записываем первую строку образующей матрицы, которая состоит из образующего полинома с предшествующими нулями, при этом общая длина кодовой комбинации равна *n*. Остальные строки матрицы получаем в результате k-кратного циклического сдвига справа налево первой строки матрицы. Строки образующей матрицы представляют собой k кодовых комбинаций кода БЧХ, а остальные могут быть получены путем суммирования по модулю 2 всевозможных сочетаний строк матрицы.

6.

1) Вычисляем y(e) это компонент синдрома S1, S3=y(e^3)

2) Найдем локаторы ошибок *х1, х2*как корни уравнения x^2 – S1\*x+

+ (s1^3-s3)/s1 = 0

3) Инвертируем полученные биты и получаем кодовое слово.