1. Основные алгебраические системы, используемые в теории кодирования

1.1. Показать, что множество всех целых чисел (положительных, отрицательных и нуля) является группой по операциям:

а) обычного сложения G_+,

б) обычного умножения G_x.

В группе G_+ по операции сложения выделить подгруппу, состоящую из чисел:

а) кратных 3,

б) кратных 4,

в) кратных 5.

Построить смежные классы для каждой из этих подгрупп.

1.2. Проверить, обладают ли полученные в п. 1.1 смежные классы групповыми свойствами:

а) по операции сложения,

б) по операции умножения.

1.3. Являются ли образованные в п. 1.2 смежные классы кольцом? Почему?

1.4. Являются ли образованные в п. 1.2 смежные классы полем? Почему?

1.5. Построить все возможные двоичные последовательности длины 5.

Являются ли они группой по операции поразрядного сложения по mod 2? Доказать.

1.6. Образовать все возможные подгруппы в группе двоичных последовательностей длины 5 по операции, введенной в п. 1.5.

(Рассмотреть элементы группы как вектора и воспользоваться понятием базиса векторного пространства. Для каждой подгруппы указать ее порядок).

1.7. Для каждой найденной подгруппы в п. 1.6 найти подгруппу из этого же множества с ортогональными векторами. Ортогональности векторов соответствует равенство нулю их скалярного произведения.

1.8. Что нужно сделать, чтобы все последовательности длины 5 из п. 1.5 стали кольцом?

1.9. Является ли кольцо из п. 1.8 полем?

1.10. Какие подполя существуют в поле из всех двоичных последовательностей длины 5?

1.11. Проверить, что элементы поля $GF(2^2)$ α и $1+\alpha$ являются корнями многочлена $\pi(x)=1+x+x^2$ в двоичном поле.

Задачи.

1.1 Используя таблицы сложения и умножения для полей GF(2) и GF(3):

Поле GF(2) содержит 2 элемента 0 и 1; 0={0}, 1={1}.

Таблицы сложения и умножения:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

б) $p = 3$:

GF(3) – совокупность классов вычетов по mod 3:

…	–12	–9	–6	–3	{0}	3	6	9	12	…
…	–11	–8	–5	–2	{1}	4	7	10	13	…
…	–10	–7	–4	–1	{2}	5	8	11	14	…

определить, чему равны суммы и произведения пар чисел 1 и 2, 2 и 3, 3 и 4, 4 и 5, 5 и 6, 6 и 7 по mod 2 и по mod 3.

1.2 Показать, что пространство строк матрицы $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ содержит последовательности 000, 001, 010, 011

2. Кольца многочленов и поля Галуа

2.1. Над полем GF(2) заданы многочлены $p_1(x)=x^3+1$ и $p_2(x)=x^4+x^3+x+1$:

а) найти наибольший общий делитель этих многочленов НОД $[p_1(x), p_2(x)]$ (указание: использовать алгоритм Евклида);

б) найти многочлены A(x) и B(x), удовлетворяющие равенству:

$$\text{НОД}\,[p_1(x), p_2(x)] = A(x)\,p_1(x) + B(x)\,p_2(x).$$

2.2. Сколько различных многочленов второй степени вида x^2+ax+b, где a и b – элементы GF(2) имеется над полем GF(2)?

2.3. Сколько различных многочленов вида $(x–\alpha)(x–\beta)$, где α и β не равны 0, имеется над полем GF(2^4), сколько из них неприводимых над этим полем? Сколько из них неприводимо над полем GF(2)?

2.4. Используя алгоритм Евклида, найти НОД (1573,308) и целые числа A и B, удовлетворяющие равенству НОД (1573,308) = 1573A+308B.

2.5. Доказать, что в кольце целых чисел по модулю 15 многочлен $p(x)=x^2-1$ имеет более двух корней, а в поле GF(2^3) – один. Чему равно значение этих корней?

2.6. Сколько различных многочленов над GF(2) делят многочлен x^6-1?

2.7. Построить поле GF(5), выписав для него таблицы сложения и умножения. Определить порядок ненулевых элементов поля.

2.8. Определить возможные порядки ненулевых элементов GF(7). Сколько элементов каждого порядка имеется? Указать порядок каждого ненулевого элемента из этого поля.

2.9. Вычислить $3^{100} \pmod 5$.

2.10. Доказать, что многочлен x^2+x+1 неприводим над GF(2). В каком поле корни этого многочлена являются примитивными элементами? Построить это поле.

2.11. Доказать, что многочлен x^3+x+1 неприводим над GF(2). В каком поле корни этого многочлена являются примитивными элементами? Построить это поле.

2.12. Сколько примитивных элементов имеет поле GF(2^3)? Корнями каких многочле-

нов они являются?

2.13. Построить поле $GF(2^4)$:

а) по модулю многочлена $\pi(x)=1+x+x^4$;

б) по модулю многочлена $\pi(x)=1+x^3+x^4$;

в) каков порядок корней этих многочленов?

г) каков порядок остальных ненулевых элементов $GF(2^4)$?

д) каким многочленом (указать степень) принадлежат в качестве корней ненулевые элементы $GF(2^4)$ из п. б?

2.14. Показать, что поле $GF(2^2)$ является подполем $GF(2^4)$.

2.15. Какие подполя содержит $GF(2^8)$?

2.16. Сколько идеалов существует в кольце многочленов по модулю многочлена $f(x)$ над полем GF(2), если идеалы образуют все многочлены, кратные каждому неприводимому сомножителю многочлена $f(x)$? Какова размерность идеалов:

а) $f(x) = x^3+1$;

б) $f(x) = x^7+1$.

Задачи.

2.1. Построить поле $GF(2^4)$ на основе мультипликативной группы порядка 2^4-1. Проверить прямой подстановкой справедливость распределения элементов поля $GF(2^4)$ в качестве корней по неприводимым многочленам, входящим в разложение $x^{15}+1$.

2.2. Построить поле $GF(2^5)$ по модулю $\pi(\alpha)=1+\alpha^2+\alpha^5$.

3. Теорема Ферма и циклотомические классы

3.1. Перечислить все многочлены степени n над полем GF(2), представить их в виде неприводимых сомножителей и определить показатели, к которым эти многочлены принадлежат в следующих случаях:

а) n=2, б) n=3, в) n=4, г) n=5.

3.2. Определить показатели, которым принадлежат следующие многочлены над полем GF(2):

а) $x^8 + x^7 + x^5 + x^4 + x^3 + x+1$,

б) $x^7 + x^3 + x+1$,

в) $x^6 + x^5 + x^4 + x^3 + x^2 + x+1$

и указать их неприводимые сомножители.

3.3. Определить число и степени неприводимых сомножителей многочленов над полем GF(2):

x^8+1, x^9+1, $x^{10}+1$, $x^{11}+1$, $x^{12}+1$, $x^{13}+1$, $x^{14}+1$, $x^{15}+1$, $x^{16}+1$, $x^{17}+1$, $x^{18}+1$, $x^{19}+1$, $x^{20}+1$, $x^{21}+1$, $x^{22}+1$, $x^{23}+1$.

3.4. Определить все неприводимые сомножители следующих двучленов:

а) $x^{30}+1$,

б) $x^{31}+1$,

в) $x^{32}+1$.

3.5. Используя результат решения задачи 2.13, а, прямым умножением показать, что многочлены из примера п. 2.1 равны: $f_1(x)=x^4 + x +1= (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$ и $f_2(x) = x^4+x+1= (x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13})(x+\alpha^{14})$.

3.6. Найти двойственные многочлены для следующих многочленов:

x^2+x+1, x^3+x+1, x^5+x+1, x^6+x^3+1, x^9+x^4+1.

Задачи.

3.1. Проверить делимость многочлена $x^5 + x + 1$ на многочлен $x^3 + x^2 + 1$. Решить методом проверки общих корней.

3.2. Найти все неприводимые многочлены пятой степени над полем GF(2).

4. Разложение $x^n - 1$ на неприводимые сомножители

4.1. Найти все неприводимые сомножители двучленов следующих степеней: 23, 51, 73, 85, 127.

4.2. Указать, какие из найденных в п. 4.1 многочленов являются примитивными (см. [1] и приложение).

4.3. Определить максимальную степень неприводимых в двоичном поле многочленов в разложении двучленов степеней 255 и 511. Каким показателям принадлежат эти многочлены?

4.4. Написать в общепринятом виде многочлены, заданные в двоично-восьмеричном представлении: 7, 13, 23, 45, 103, 211, 435, 1021, 2011, 4005.

4.5. Написать в двоично-восьмеричном представлении многочлены, найденные в п. 4.1.

Задачи.

4.1. Определить степени, число и вид неприводимых над GF(2) многочленов, входящих в разложение двучленов $x^{127} + 1$ и $x^{255} + 1$. (*Есть решение, нужно найти вид многочленов 8-й степени, принадлежащих к показателям 85 и 255*)

4.2. Найти неприводимые многочлены степени 9, принадлежащие показателю, меньшему 511.

(*Из приложения находим, что им соответствуют следующие многочлены 9-й степени:*

7 1231 A и двойственный многочлен 1145,

21 1027 A и двойственный многочлен 1641,

35 1401 C и двойственный многочлен 1003,

77 1511 C и двойственный многочлен 1113.

Записать эти многочлены в обычном виде.)

5. Декодер Меггита

5.1. Нарисовать схему декодера Меггита для исправления однократных ошибок укороченными циклическими кодами Хемминга:

а) (10,5) с $g(x) = 1 + x^2 + x^5$;

б) (11,5) с $g(x) = 1 + x + x^6$;

в) (12,5) с $g(x) = 1 + x + x^7$.

5.2. Для каждого кода из предыдущей задачи определить комбинацию, на которую должен быть настроен дешифратор, и показать по тактам работу синдромного регистра при выводе информационных разрядов принятой комбинации из буферного регистра, начиная с того момента, когда в нем сформировался синдром, до момента исправления ошибки. Считать, что ошибка произошла в символе кодовой комбинации, соответствующем коэффициенту при x^7 .

Задачи.

5.1. Построить порождающую и проверочную матрицы укороченного циклического кода (10,5) с порождающим многочленом $g(x) = 1 + x^2 + x^5$.

Решение

Код (10,5) с порождающим многочленом $g(x)=1+x^2+x^5$ является укороченным кодом Хемминга, так как многочлен $1+x^2+x^5$ – примитивный многочлен, принадлежащий показателю 31.

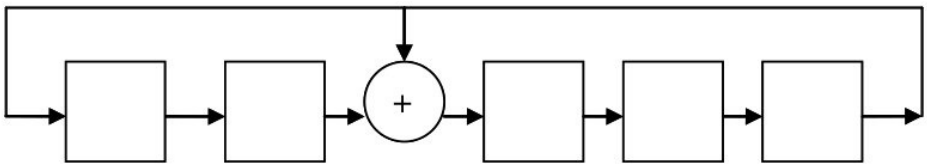
В таблице неприводимых многочленов он указан условной записью 1 45 Е.

Наиболее простое решение задачи состоит в построении генератора элементов поля $GF(2^5)$ и нахождении десяти первых значений степеней примитивного корня. Их двоичное представление даст столбцы проверочной матрицы в канонической форме:

$H_{(10,5)}=[\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9]$, где α^i – элемент поля $GF(2^5)$.

Затем по проверочной матрице и известным правилам найдем порождающую матрицу. Она также получится в канонической форме.

Генератор элементов поля $GF(2^5)$, построенный на основе примитивного многочлена $1+x^2+x^5$, содержимое ячеек памяти на 10 тактах работы и матрицы, характеризующие код, представлены на рис. 1.



$$H^T_{(10,5)}=\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

$$G_{(10,5)}=\begin{bmatrix}1&0&1&0&0&1&0&0&0&0\\0&1&0&1&0&0&1&0&0&0\\0&0&1&0&1&0&0&1&0&0\\1&0&1&1&0&0&0&0&1&0\\0&1&0&1&1&0&0&0&0&1\end{bmatrix}$$

Рис.1

5.4. Построить декодер Меггита для циклического кода (7,5) над полем $GF(2^3)$ с порождающим многочленом $g(x)=x^2+\alpha^4 x+\alpha^3$. Код гарантированно исправляет однократные ошибки.

Значения элементов поля $GF(2^3)$:

$0 = 000$

$\alpha^0 = 1 = 100$

$\alpha^1 = \alpha = 010$

$\alpha^2 = \alpha^2 = 001$

$\alpha^3 = 1+\alpha = 110$

$\alpha^4 = \alpha+\alpha^2 = 011$

$\alpha^5 = 1+\alpha+\alpha^2 = 111$

$\alpha^6 = 1+\alpha^2 = 101$

$\alpha^7 = 1 = 100$

6. Быстрое декодирование кодов БЧХ

6.1. Вычислить порождающий многочлен для кода Рида–Соломона (7,5).

6.2. Методом быстрого декодирования закодировать кодом Рида–Соломона (7,5) свой порядковый номер в журнале группы.

6.3. Для кода Рида–Соломона (7,5) построить кодер на основе регистра сдвига с обратными связями и закодировать комбинацию из предыдущей задачи. Сравнить результаты кодирования.

6.4. С помощью кодера предыдущей задачи построить порождающую и проверочную матрицы кода Рида–Соломона (7,5) в канонической форме.

6.5. Вычислить порождающий многочлен для кода Рида–Соломона (7,3).

Задачи.

6.1. Построить код Рида–Соломона (7,4) над полем GF(2).

Решение

Находим порождающий многочлен по теореме Безу:

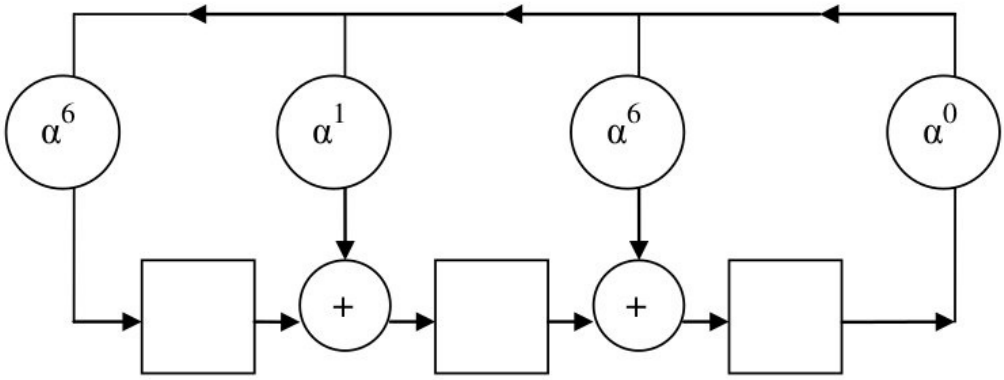
$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3) = (x^2 +\alpha^2 x+\alpha x+\alpha^3)(x+\alpha^3) =$$
$$=x^3 +\alpha^2 x^2 +\alpha x^2 +\alpha^3 x+\alpha^3 x^2 +\alpha^5 x+ \alpha^4 x +\alpha^6 =$$
$$= x^3 +(\alpha+\alpha^2 +\alpha^3)x+(\alpha^3 +\alpha^4 +\alpha^5)x +\alpha^6 =x^3 +\alpha^6 x^2 +\alpha x+\alpha^6$$

и по формуле Виета:

$g_3=1$, $g_2= \alpha+\alpha^2 +\alpha^3 = \alpha^6$, $g_1 = \alpha\alpha^2 + \alpha\alpha^3 +\alpha^2 \alpha^3 =\alpha^3 +\alpha^4 +\alpha^5 =\alpha$, $g_0=\alpha\alpha^2 \alpha^3 =\alpha^6$.

Итак, $g(x) = x^3 +\alpha^6 x^2 +\alpha x+\alpha^6$.

Для построения порождающей и проверочной матриц воспользуемся приемом, примененным в п. 5.3. Строим генератор элементов GF(2^3) по виду *g(x)* (рис. 2). Записав в крайнюю слева ячейку памяти «1», выполним 7 сдвигов до получения в ячейках регистра исходной последовательности 1 0 0. Содержимое ячеек памяти регистра на первых 7 тактах работы схемы соответствует строкам транспонированной проверочной матрицы кода. Последние четыре строки данной матрицы соответствуют столбцам порождающей матрицы этого кода, расположенных на местах избыточных элементов в канонической форме. Приписав к ним справа единичную матрицу размером 4×4, получаем всю порождающую матрицу кода (7,4) в канонической форме.



$$H^{T}_{(7,4)}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha^{6} & \alpha^{1} & \alpha^{6} \\ \alpha^{5} & \alpha^{2} & \alpha^{6} \\ \alpha^{5} & \alpha^{4} & \alpha^{3} \\ \alpha^{2} & \alpha^{0} & \alpha^{1} \end{bmatrix}$$

$$G_{(7,4)}=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{matrix} 1 & 0 & 0 \end{matrix}$$

Рис. 2

[1. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон / Пер. с англ. – М. : Мир, 1964. – 338 с.]