3. Obtain the augmented code of the ternary self dual code of length 4 generated by 1201 and 1012.
4. If $\mathscr{C}$ is a ternary code with minimum distance d, then the minimum distance $\hat{d}$ of the extended code $\hat{\mathscr{C}}$ is given by

$$d = \begin{cases} d & \text{if } \mathscr{C} \text{ has a minimum distance word } c \text{ with} \\ & \text{wt}(c) \equiv 0 (\text{mod } 3) \\ d+1 & \text{if } \mathscr{C} \text{ has no minimum distance word } c \text{ with} \\ & \text{wt}(c) \equiv 0 (\text{mod } 3). \end{cases}$$

Can we have this or a similar observation about codes over GF(p) for any prime p?

6

Cyclic codes

6.1 CYCLIC CODES

Let $F = \mathrm{GF}(q)$ be a field of q elements and $F^{(n)} = V(n, q)$, as before, be the vector space of all vectors (or sequences) of length n over F. Then $V(n, q)$ is of dimension n over F. **We suppose that** $(n, q) = 1$.

Definition 6.1
A linear code $\mathscr{C}$ of length n over F is called **cyclic** if any cyclic shift of a code word is again a code word, i.e. if $(a_0, a_1, \ldots, a_{n-1})$ is in $\mathscr{C}$ then so is $(a_{n-1}, a_0, \ldots, a_{n-2})$.

Algebraic description of cyclic codes
There is a beautiful algebraic description of cyclic codes. To obtain this we define a map

$$\theta: V(n, q) \to F[X]/\langle X^n - 1 \rangle$$

where $\langle X^n - 1 \rangle$ denotes the ideal of the polynomial ring $F[X]$ generated by $X^n - 1$, by

$$\theta(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + \langle X^n - 1 \rangle$$
$$\forall a_i \in F, 0 \leq i \leq n-1$$

Observe that $F[X]/\langle X^n - 1 \rangle$ is also a vector space over F and θ is a vector space isomorphism. Let $\mathscr{C}$ be a linear code of length n over F, i.e. $\mathscr{C}$ is a subspace of $V(n, q)$. Then $\theta(\mathscr{C})$ is a subspace of $F[X]/\langle X^n - 1 \rangle$. Let $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathscr{C}$. Then $(a_{n-1}, a_0, \ldots, a_{n-2}) \in \mathscr{C}$ iff

$$a_{n-1} + a_0 X + \cdots + a_{n-2} X^{n-1} + \langle X^n - 1 \rangle$$
$$= X(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}) + \langle X^n - 1 \rangle$$

is in $\theta(\mathscr{C})$. From this it follows that $\mathscr{C}$ is a cyclic code iff $\theta(\mathscr{C})$ is an ideal in the quotient ring $F[X]/\langle X^n - 1 \rangle$. Identifying the element $(a_0, a_1, \ldots, a_{n-1})$ in

$\mathscr{C}$ with the corresponding element

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + \langle X^n - 1 \rangle$$

or with the polynomial $a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$ of degree at most $n-1$, we may regard a cyclic code $\mathscr{C}$ of length n as an ideal of the quotient ring $F[X]/\langle X^n - 1 \rangle$.

Theorem 6.1
Let $\mathscr{C}$ be a non-zero cyclic code of length n over F.

(a) There is a unique monic polynomial $g(X)$ of minimal degree in $\mathscr{C}$ which generates it.
(b) $g(X)$ is a factor of $X^n - 1$.
(c) Let $\deg g(X) = r$. Then the dimension of $\mathscr{C}$ is $n-r$ and any $a(X) \in \mathscr{C}$ has a unique representation of the form $a(X) = b(X)g(X)$, where $\deg b(X) < n-r$.
(d) If $g(X) = g_0 + g_1 X + \cdots + g_r X^r$, then the $(n-r) \times n$ matrix

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & & g_{r-1} & g_r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \ddots & \\ 0 & 0 & & \cdots & g_0 & \cdots & g_r \end{pmatrix}$$

is a generator matrix of $\mathscr{C}$.

Proof
Let I denote the ideal $\langle X^n - 1 \rangle$ of $F[X]$ generated by $X^n - 1$. Let $N = \{\deg a(X) / a(X) + I \in \mathscr{C}\}$. The set of non-negative integers being well ordered, N has a least element. Let $g(X)$ be a polynomial of minimal degree such that $g(X) + I \in \mathscr{C}$. F being a field, we can take $g(X)$ to be a monic polynomial. If $g'(X)$ is another monic polynomial of minimal degree such that $g'(X) + I \in \mathscr{C}$, then $g(X) - g'(X) + I \in \mathscr{C}$ and

$$\deg(g(X) - g'(X)) < \deg g(X)$$

Hence $g'(X) - g(X) = 0$ and $g(X)$ is the unique monic polynomial with $g(X) + I$ in $\mathscr{C}$. Let $a(X) + I$ be any element in $\mathscr{C}$. F being a field, $F[X]$ is a Euclidean domain. Therefore, there exist polynomials $b(X), r(X)$ in $F[X]$ such that

$$a(X) = b(X)g(X) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < \deg g(X)$. If $r(X) \neq 0$, then

$$r(X) + I = a(X) - b(X)g(X) + I \in \mathscr{C}$$

giving a contradiction. Hence $r(X) = 0$ and

$$a(X) + I = (b(X) + I)(g(X) + I)$$

i.e. $g(X)$ generates $\mathscr{C}$.

Again, let

$$X^n - 1 = a(X)g(X) + r(X)$$

such that $\deg r(X) < \deg g(X)$ if $r(X) \neq 0$. This shows that

$$r(X) + I = -a(X)g(X) + I \in \mathscr{C}$$

and this gives a contradiction to the choice of $g(X)$. This proves part (b).

Observe that every element of $F[X]/I$ can be uniquely written as $a(X) + I$, where $a(X)$ is a polynomial of degree at most $n-1$ and, so, that is in particular true for every element of $\mathscr{C}$. As such, the elements

$$g(X) + I, Xg(X) + I, \ldots, X^{n-r-1}g(X) + I$$

of $\mathscr{C}$ are linearly independent over F. Let $a(X)$ be a polynomial of degree at most $n-1$ such that $a(X) + I \in \mathscr{C}$. Then

$$a(X) + I = b(X)g(X) + I$$

so that

$$a(X) = b(X)g(X) + (X^n - 1)c(X)$$

But $g(X) | X^n - 1$. Let $X^n - 1 = g(X)p(X)$. Then

$$a(X) = (b(X) + c(X)p(X))g(X) = d(X)g(X) \tag{6.1}$$

where $d(X) = b(X) + c(X)p(X)$. Also it follows from (6.1) and the degree considerations that $\deg d(X) < n - r$. Hence $a(X) + I$ is a linear combination of

$$g(X) + I, Xg(X) + I, \ldots, X^{n-r-1}g(X) + I$$

Thus it follows that

$$g(X) + I, Xg(X) + I, \ldots, X^{n-r-1}g(X) + I$$

is a basis of $\mathscr{C}$ over F, $\mathscr{C}$ is of dimension $n - r$, and every element of $\mathscr{C}$ can be uniquely written as $a(X)g(X) + I$, where $\deg a(X) < n - r$. Now $\mathscr{C}$ becomes a polynomial code and part (d) follows from Theorem 2.4.

Examples 6.1

Case (i)

We have seen earlier that over $\mathbb{B}$,

$$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

Therefore the (4, 7) polynomial codes generated by $X^3 + X + 1$ and $X^3 + X^2 + 1$ are binary cyclic codes of length 7. (Refer to Examples 2.1 for the sets of code words.)

Case (ii)

We show that every polynomial code need not be a cyclic code. Consider the binary cyclic code of length 5 generated by $1 + X + X^3$. The code words of this

code are:

$$\begin{aligned} 1(1+X+X^3) &\longrightarrow 1\ 1\ 0\ 1\ 0 \\ X(1+X+X^3) &\longrightarrow 0\ 1\ 1\ 0\ 1 \\ (1+X)(1+X+X^3) &\longrightarrow 1\ 0\ 1\ 1\ 1 \\ 0(1+X+X^3) &\longrightarrow 0\ 0\ 0\ 0\ 0 \end{aligned}$$

which is not a cyclic code.

Case (iii)

We next construct a binary cyclic code of length 15 and dimension 11.

The polynomial X^4+X^3+1 is irreducible over $\mathbb{B}$ and is a divisor of $X^{15}-1$. From this, we observe that

$$K = \mathbb{B}[X]/\langle X^4+X^3+1\rangle$$

is a field of order 16 and X^4+X^3+1 is the minimal polynomial of

$$\alpha = X + \langle X^4+X^3+1\rangle$$

As every non-zero element of the field K is a root of $X^{15}-1$, α is also a root of this polynomial and hence its minimal polynomial X^4+X^3+1 divides $X^{15}-1$. Therefore, the ideal

$$\langle X^4+X^3+1+\langle X^{15}-1\rangle\rangle$$

generated by X^4+X^3+1 is a cyclic code of length 15. The dimension of this code is $(15-4=)11$.

Exercise 6.1

1. Determine all the binary cyclic codes of length 9.
2. Determine all the ternary cyclic codes of length 8.
3. Determine all the binary cyclic codes of length 5.
4. Prove that the polynomial X^6+X^3+1 is irreducible over the field $\mathbb{B}$ of 2 elements. Use this to construct a binary cyclic code of length 9 and dimension 3.
5. Given a prime p and a positive integer n coprime to p. Does there always exist a cyclic code of length n over GF(p)?
6. Construct a cyclic code of length 4 and dimension 2 over the field GF(5) of 5 elements.
7. Let $F = \mathbb{B}[X]/\langle X^2+X+1\rangle = \{0, 1, w, w^2\}$ with $1+w+w^2=0$, $w^3=1$, $2w=0$, be the field of four elements. Prove that the polynomials $1+wX+X^2$ and $1+w^2X+X^2$ are irreducible over F. Use these to construct a cyclic code of length 5 and dimension (i) 3 and (ii) 2 over the field F of 4 elements.
8. Using the irreducible polynomial X^2+X-1 over GF(3), construct a field F of 9 elements. Construct, if possible, a cyclic code of length 5 and dimension (i) 2 and (ii) 3 over F.

6.2 CHECK POLYNOMIAL

Let $\mathscr{C}$ be a cyclic code of length n over F with generator polynomial $g(X)$ of degree r. Let $h(X)$ be the polynomial of degree $n-r$ with

$$X^n - 1 = g(X)h(X)$$

Any code word $c(X) + I$ is of the form

$$c(X) + I = a(X)g(X) + I$$

where $I = \langle X^n - 1 \rangle$ and, therefore, $c(X)h(X) = 0$, i.e. $c(X)h(X)$ is zero in $F[X]/I$. For this reason $h(X)$ is called the **check polynomial** of the code $\mathscr{C}$. We have seen that $\mathscr{C}$ is a matrix code and so $\mathscr{C}$ must have some sort of a parity check matrix. Before we define this in the general case we consider an example.

Example 6.1
Let $\mathscr{C}$ be a binary cyclic code of length 7 defined by the polynomial

$$g(X) = X^3 + X + 1$$

Then

$$h(X) = (X+1)(X^3 + X^2 + 1) = X^4 + X^2 + X + 1$$

Let

$$c(X) = c_0 + c_1 X + \cdots + c_6 X^6$$

be a code word in $\mathscr{C}$. Then $c(X)h(X) = 0$ in $\mathbb{B}[X]/\langle X^7 - 1 \rangle$, i.e.

$$(c_0 + c_1 X + \cdots + c_6 X^6)(1 + X + X^2 + X^4) = 0$$

in $\mathbb{B}[X]/\langle X^7 - 1 \rangle$. This means that

$$\begin{aligned}(c_0 + c_6 + c_5 + c_3) + (c_1 + c_0 + c_6 + c_4)X + (c_2 + c_1 + c_0 + c_5)X^2 \\ + (c_3 + c_2 + c_1 + c_6)X^3 + (c_4 + c_3 + c_2 + c_0)X^4 + (c_5 + c_4 + c_3 + c_1)X^5 \\ + (c_6 + c_5 + c_4 + c_2)X^6 = 0\end{aligned}$$

So the parity check equations are

$$\begin{aligned}c_0 + c_6 + c_5 + c_3 &= 0 \\ c_1 + c_0 + c_6 + c_4 &= 0 \\ c_2 + c_1 + c_0 + c_5 &= 0 \\ c_3 + c_2 + c_1 + c_6 &= 0 \\ c_4 + c_3 + c_2 + c_0 &= 0 \\ c_5 + c_4 + c_3 + c_1 &= 0 \\ c_6 + c_5 + c_4 + c_2 &= 0\end{aligned}$$