ıary self dual code of length 4 gener-

stance d, then the minimum distance

ance word c with

stance word c with

ion about codes over GF(p) for any

From:

Vermani

Elements of

Algebraic Coding

Theory

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 $(a_0, a_1, \dots, a_{n-1})$ is in $\mathscr{C}$ then so is $(a_{n-1}, a_0, \dots, a_{n-2})$.

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

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

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

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

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 $a = (a_0, a_1, \dots, a_{n-1}) \in \mathscr{C}$. Then $(a_{n-1}, a_0, \dots, a_{n-2}) \in \mathscr{C}$ iff

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

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 $(a_0, a_1, \dots, a_{n-1})$ in

$\mathscr{C}$ with the corresponding element

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + \langle X^n - 1 \rangle$$

or with the polynomial $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ 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 $g(X) = g_0 + g_1X + \cdots + g_rX^r$, then the $(n-r) \times n$ matrix

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

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 $\mathscr{C}$.

$+\langle X^n - 1\rangle$

X^{n-1} of degree at most $n-1$, we
an ideal of the quotient ring

er F.

) of minimal degree in $\mathscr{C}$ which

f $\mathscr{C}$ is $n-r$ and any $a(X)\in\mathscr{C}$
form $a(X)=b(X)g(X)$, where

$n-r) \times n$ matrix

$$\begin{matrix} 0 & \cdots & 0 \\ g_r & \cdots & 0 \\ & \ddots & \\ g_0 & \cdots & g_r \end{matrix}\Bigg)$$

X] generated by X^n-1. Let
negative integers being well or-
ynomial of minimal degree such
(X) to be a monic polynomial. If
l degree such that $g'(X)+I\in\mathscr{C}$,

leg $g(X)$

monic polynomial with $g(X)+I$
ng a field, $F[X]$ is a Euclidean
$X), r(X)$ in $F[X]$ such that

$r(X)$

$\neq 0$, then

$(X)+I\in\mathscr{C}$

$(X)+I)$

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

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

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

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

Thus it follows that

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

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:

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

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.

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

ength 15 and dimension 11.
ɔible over $\mathbb{B}$ and is a divisor of

$X^3 + 1\rangle$

ε minimal polynomial of

$\Upsilon^3 + 1\rangle$

. root of $X^{15} - 1$, α is also a root of
polynomial $X^4 + X^3 + 1$ divides

$\Upsilon^{15} - 1\rangle\rangle$

ıf length 15. The dimension of this

length 9.
f length 8.
length 5.
. is irreducible over the field $\mathbb{B}$ of
nary cyclic code of length 9 and

ı coprime to p. Does there always
ı)?
limension 2 over the field GF(5) of

$w^2\}$ with $1 + w + w^2 = 0$, $w^3 = 1$,
ts. Prove that the polynomials
rreducible over F. Use these to
nension (i) 3 and (ii) 2 over the field

$\Upsilon - 1$ over GF(3), construct a field
ɛ, a cyclic code of length 5 and

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

$$c(X) = c_0 + c_1X + \cdots + c_6X^6$$

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

$$(c_0 + c_1X + \cdots + c_6X^6)(1 + X + X^2 + X^4) = 0$$

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

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

In the matrix form, these may be rewritten as

$$(c_0 \quad c_1 \quad \cdots \quad c_6)\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = 0$$

or **cH** = 0, where **H** is the 7 × 7 matrix

$$\begin{pmatrix} 0 & 0 & h_4 & h_3 & h_2 & h_1 & h_0 \\ 0 & h_4 & h_3 & h_2 & h_1 & h_0 & 0 \\ h_4 & h_3 & h_2 & h_1 & h_0 & 0 & 0 \\ h_3 & h_2 & h_1 & h_0 & 0 & 0 & h_4 \\ h_2 & h_1 & h_0 & 0 & 0 & h_4 & h_3 \\ h_1 & h_0 & 0 & 0 & h_4 & h_3 & h_2 \\ h_0 & 0 & 0 & h_4 & h_3 & h_2 & h_1 \end{pmatrix}$$

Definition 6.1

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

$$h(X) = h_0 + h_1X + \cdots + h_{n-r}X^{n-r}$$

be its check polynomial. Then a word

$$c(X) + I = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + I$$

is in $\mathscr{C}$, iff $c(X)h(X) = 0$ in $F[X]/I$, where as before $I = \langle X^n - 1\rangle$. This is equivalent to saying that

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0 \quad j = 0, 1, 2, \ldots, n-1$$

where the subscripts are taken modulo n and where it is also understood that $h_j = 0$ if $j > n - r$. These are the n check equations and, in the matrix form, may be rewritten as

$$\mathbf{cH} = (c_0 \quad c_1 \quad \cdots \quad c_{n-1})\mathbf{H} = 0$$

where **H** is the $n \times n$ matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & h_1 & h_0 \\ 0 & & & h_{n-r} & h_{n-r-1} & \cdots & h_0 & 0 \\ \vdots & \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & \vdots \\ h_0 & 0 & \cdots & \cdots & \cdots & \cdots & h_2 & h_1 \end{pmatrix},$$

the rows of which are defined inductively as follows:

en as

$$\begin{matrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{matrix}\right) = 0$$

$$\begin{matrix} h_2 & h_1 & h_0 \\ h_1 & h_0 & 0 \\ h_0 & 0 & 0 \\ 0 & 0 & h_4 \\ 0 & h_4 & h_3 \\ h_4 & h_3 & h_2 \\ h_3 & h_2 & h_1 \end{matrix}\right)$$

r F with generator polynomial $g(X)$ of

$$\cdots + h_{n-r}X^{n-r}$$

$$\cdots + c_{n-1}X^{n-1} + I$$

nere as before $I = \langle X^n - 1\rangle$. This is

$$= 0, 1, 2, \ldots, n-1$$

n and where it is also understood that

quations and, in the matrix form, may

$$\cdots \quad c_{n-1})\mathbf{H} = 0$$

$$\begin{matrix} & \cdots & h_1 & h_0 \\ & \cdots & h_0 & 0 \\ & \cdot^{\cdot^{\cdot}} & & \vdots \\ & \cdots & h_2 & h_1 \end{matrix}\right)$$

ly as follows:

The first row is taken as

$$0 \ \cdots \ 0 \ \ h_{n-r} \ \cdots \ h_1 \ \ h_0$$

and once the ith row is defined, the $(i+1)$th row is obtained by giving a cyclic shift to the ith. The matrix $\mathbf{H}$ thus obtained is called the **parity check matrix** of the cyclic code $\mathscr{C}$ (mark the difference from the usual definition of a parity check matrix!)

Thus $c(X) + I$ is in $\mathscr{C}$ iff $\mathbf{cH} = 0$ or equivalently $\mathbf{H}^t\mathbf{c}^t = 0$. From this, it follows that the dual code $\mathscr{C}^\perp$ contains the linear code generated by the rows of $\mathbf{H}^t = \mathbf{H}$, as $\mathbf{H}$ is clearly a symmetric matrix. The dual code $\mathscr{C}^\perp$ is of dimension $n-(n-r) = r$ and clearly the first r rows of $\mathbf{H}$ are linearly independent. Therefore, the linear code generated by $\mathbf{H}$ must be of dimension r, and hence, it must equal $\mathscr{C}^\perp$. Also, we could as well have taken the $r \times n$ matrix

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 0 & 0 & h_{n-r} & \cdots & h_1 & h_0 \\ 0 & & h_{n-r} & h_{n-r-1} & \cdots & h_0 & 0 \\ \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \vdots & \vdots \\ h_{n-r} & \cdots & \cdots & \cdots & h_0 & 0 & 0 \end{pmatrix}$$

as the parity check matrix of $\mathscr{C}$. (Now we have the usual form of the parity check matrix!)

Since the rows of the matrix $\mathbf{H}$ are all the possible cyclic shifts of the vector

$$0 \ \cdots \ 0 \ \ h_{n-r} \ \cdots \ h_1 \ \ h_0$$

of length n, any linear combination over F of the rows of $\mathbf{H}$ will again be a linear combination of the rows of $\mathbf{H}$. Hence $\mathscr{C}^\perp$, the code generated by $\mathbf{H}$ (or $\mathbf{H}_1$) is again cyclic.

Reversing the order of the rows of $\mathbf{H}_1$, we may take the parity check matrix of $\mathscr{C}$ (and, so, also the generator matrix of $\mathscr{C}^\perp$) as

$$\mathbf{H}_2 = \begin{pmatrix} h_{n-r} & \cdots & h_1 & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & h_{n-r} & \cdots & h_2 & h_1 & h_0 & 0 & 0 \\ \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & h_{n-r} & \cdots & h_1 & h_0 \end{pmatrix}$$

Thus it follows (see Theorem 2.4) that code $\mathscr{C}^\perp$ is the polynomial code generated by

$$\begin{aligned} k(X) &= h_{n-r} + h_{n-r-1}X + \cdots + h_0X^{n-r} \\ &= X^{n-r}(h_0 + h_1X^{-1} + \cdots + h_{n-r}X^{-n+r}) \end{aligned}$$

Now

$$X^n - 1 = g(X)h(X) \Rightarrow X^{-n} - 1 = g(X^{-1})h(x^{-1})$$

or

$$1 - X^n = X^r g(X^{-1})k(X)$$

showing that $k(X) \mid X^n - 1$ as it should.

Theorem 6.2
Let $\mathscr{C}$ be a cyclic code of length n over F with generator polynomial $g(X)$ of degree r and $h(X)$ as its check polynomial. Then:

(i) the dual code $\mathscr{C}^{\perp}$ is also cyclic with $k(X) = X^{n-r}h(X^{-1})$ as a generator polynomial; and
(ii) the dual code $\mathscr{C}^{\perp}$ is equivalent to the code generated by $h(X)$.

Proof
We only have to prove (ii).

Consider the permutation matrix $\mathbf{P} = (p_{ij})$ where

$$p_{ij} = \begin{cases} 1 & \text{if } i+j=n+1 \\ 0 & \text{otherwise} \end{cases}$$

Let $\mathbf{c}_1, \ldots, \mathbf{c}_n$ denote the columns of the generator matrix $\mathbf{H}_1$ of $\mathscr{C}^{\perp}$. Then

$$\begin{aligned} \mathbf{H}_1\mathbf{P} &= (\mathbf{c}_1 \quad \cdots \quad \mathbf{c}_n)P \\ &= \left(\sum_i \mathbf{c}_i p_{i1} \quad \sum \mathbf{c}_i p_{i2} \quad \cdots \quad \sum \mathbf{c}_i p_{in}\right) \\ &= (\mathbf{c}_n \quad \mathbf{c}_{n-1} \quad \cdots \quad \mathbf{c}_1) \\ &= \begin{pmatrix} h_0 & h_1 & \cdots & h_{n-r} & 0 & \cdots & \cdots & 0 \\ 0 & h_0 & \cdots & h_{n-r-1} & h_{n-r} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-r} \end{pmatrix} \end{aligned}$$

The linear code generated by $\mathbf{H}_1\mathbf{P}$ is thus the code $\langle h(X) + I \rangle$ generated by $h(X)$. But the code generated by $\mathbf{H}_1\mathbf{P}$ is equivalent to $\mathscr{C}^{\perp}$. Hence the result.

Exercise 6.2

1. Is a code equivalent to a cyclic code cyclic?
2. Determine the check polynomials and also parity check matrices of the cyclic codes constructed in Exercise 6.1.
3. Determine the duals of the codes constructed in Exercise 6.1.

6.3 BCH AND HAMMING CODES AS CYCLIC CODES

Let $\mathscr{C}$ be a cyclic code of length n over F (i.e. an ideal in $F[X]/I, I = \langle X^n - 1 \rangle$) with generator matrix $g(X)$ of degree r. Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the roots of $g(X)$ in a suitable extension field of F. Then

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_r)$$

Observe that $g(X)$ divides a polynomial $a(X)$ iff $\alpha_1, \ldots, \alpha_r$ are among the roots of $a(X)$. Therefore $a(X) + I$ is in $\mathscr{C}$ iff $\alpha_1, \ldots, \alpha_r$ are among the roots of $a(X)$.

F with generator polynomial $g(X)$ of
al. Then:

ı $k(X) = X^{n-r}h(X^{-1})$ as a generator

: code generated by $h(X)$.

: (p_{ij}) where

$+ j = n + 1$

:rwise

generator matrix $\mathbf{H}_1$ of $\mathscr{C}^{\perp}$. Then

$\cdots \quad \sum \mathbf{c}_i p_{in} \Big)$

$$\begin{matrix} . & 0 & \cdots & \cdots & 0 \\ \cdot_{-1} & h_{n-r} & 0 & \cdots & 0 \\ & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \vdots \\ & h_0 & h_1 & \cdots & h_{n-r} \end{matrix}\Bigg)$$

us the code $\langle h(X) + I \rangle$ generated by
equivalent to $\mathscr{C}^{\perp}$. Hence the result.

cyclic?
nd also parity check matrices of the
5.1.
ıstructed in Exercise 6.1.

ΑS CYCLIC CODES

(i.e. an ideal in $F[X]/I, I = \langle X^n - 1 \rangle$)
.et $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the roots of $g(X)$ in

$.) \cdots (X - \alpha_r)$

$a(X)$ iff $\alpha_1, \ldots, \alpha_r$ are among the roots
$, \ldots, \alpha_r$ are among the roots of $a(X)$.

Given a positive integer m, we defined a binary $(2^m - m - 1, 2^m - 1)$ Hamming code by taking $\mathbf{H}^t$ as the parity check matrix where $\mathbf{H}$ is the $m \times (2^m - 1)$ matrix the ith row of which, $1 \leq i \leq 2^m - 1$, is the binary representation of the number i and by insisting that in a code word $b_1 b_2 \cdots b_n$ $(n = 2^m - 1)$, $b_1, b_2, b_{2^2}, \ldots, b_{2^{m-1}}$ are the check symbols. If we do not insist on the condition about the position of the check symbols, we may define the **binary Hamming code** as the code with parity check matrix $\mathbf{H}^t$.

With the parity check matrix given, it is not easy to find the code words. For finding these, we observe that $\mathbf{H}^t$ contains m columns, a suitable permutation of which forms the identity matrix $\mathbf{I}_m$ of order m. Let σ be a permutation of the columns of $\mathbf{H}^t$ which, when applied, transforms $\mathbf{H}^t$ into $(\mathbf{A} \quad \mathbf{I}_m) = \mathbf{H}_1$. The corresponding generating matrix then becomes

$$\mathbf{G}_1 = (\mathbf{I}_{n-m} \quad \mathbf{A}^t)$$

An application of the permutation σ^{-1} to the columns of $\mathbf{G}_1$ gives a generator matrix $\mathbf{G}$ of the Hamming code. The code words of the Hamming code are then given by $a\mathbf{G}$, $a \in V(n - m, 2)$.

We illustrate this procedure for the case $m = 3$. Here,

$$\mathbf{H}^t = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Applying the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 4 & 3 & 5 & 6 & 7 \\ 7 & 6 & 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

to the columns of $\mathbf{H}^t$ gives

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The corresponding generator matrix is

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Applying σ^{-1} to the columns of $\mathbf{G}_1$ gives the generator matrix of the code corresponding to $\mathbf{H}^t$ as

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

For a message word $a = a_1a_2a_3a_4$, we have

$$\mathbf{a}\mathbf{G} = (a_1 + a_2 + a_4 \quad a_1 + a_3 + a_4 \quad a_1 \quad a_2 + a_3 + a_4 \quad a_2 \quad a_3 \quad a_4)$$

Observe that the message symbols occupy the 3rd, 5th, 6th and 7th positions while the 1st, 2nd and 4th positions are occupied by check symbols as they do in the case of Hamming codes defined originally.

Going back to the case of arbitrary m, we may define

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 2^2 & \cdots & 2^{m-1} & 3 & 5 & 6 & 7 & 9\cdots \\ n & n-1 & n-2 & \cdots & n-m+1 & 1 & 2 & 3 & 4 & 5\cdots \end{pmatrix}$$

Applying $\boldsymbol{\sigma}$ to the columns of $\mathbf{H}^t$ gives

$$\mathbf{H}_1 = (\mathbf{A} \quad \mathbf{I}_m)$$

so that the corresponding generating matrix is

$$\mathbf{G}_1 = (\mathbf{I}_{n-m} \quad \mathbf{A}^t)$$

Now applying $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$ gives the generator matrix $\mathbf{G}$ of the code corresponding to the parity check matrix $\mathbf{H}^t$. With this generating matrix $\mathbf{G}$, we find that the code word in the Hamming code corresponding to the message word a is the same as the code word corresponding to a for the Hamming code originally defined. Thus, the two definitions of the Hamming code give the *same* code.

Let $\mathscr{C}$ be a Hamming code of length $n = 2^r - 1$ so that $\mathscr{C}$ is a code with a parity check matrix $\mathbf{H}$ of order $r \times n$ in which the columns are the binary representations of the numbers $1, 2, \ldots, n$. Then no two columns of $\mathbf{H}$ are identical and so the code is single error correcting (Theorem 1.5). But then the minimum distance of the code is at least 3 (Theorem 1.2). Thus we have an alternative proof of Theorem 3.1.

Examples 6.1

Case (i)

As a first illustration of the use of the above discussion we obtain all the code words of binary Hamming code of length $7 = 2^3 - 1$. A parity check matrix of this code is

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Applying the permutation

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 5 & 2 & 3 & 4 \end{pmatrix}$$

ave

$a_1 \quad a_2+a_3+a_4 \quad a_2 \quad a_3 \quad a_4)$

py the 3rd, 5th, 6th and 7th positions
occupied by check symbols as they do
riginally.
n, we may define

$$\begin{matrix} \iota-1 & 3 & 5 & 6 & 7 & 9\cdots \\ -m+1 & 1 & 2 & 3 & 4 & 5\cdots \end{matrix}\Bigg)$$

$I_m)$

atrix is

$_m \quad A^t)$

$_1$ gives the generator matrix G of the
natrix H^t. With this generating matrix
Hamming code corresponding to the
de word corresponding to a for the
, the two definitions of the Hamming

n $n=2^r-1$ so that $\mathscr{C}$ is a code with
in which the columns are the binary
.., n. Then no two columns of H are
correcting (Theorem 1.5). But then the
st 3 (Theorem 1.2). Thus we have an

ove discussion we obtain all the code
h $7=2^3-1$. A parity check matrix of

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

$$\begin{matrix} 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 4 \end{matrix}\Bigg)$$

to the columns of H gives a parity check matrix

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The corresponding generator matrix is

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Now apply the permutation σ^{-1} to the columns of $\mathbf{G}_1$ to obtain the generator **G** matrix corresponding to the parity check matrix **H**:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The code words of this Hamming code are:

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

Case (ii)

Our second illustration results in a generator matrix of binary Hamming code of length $15=2^4-1$. A parity check matrix of this code is

$$\mathbf{H} = \begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}$$

To obtain a canonical form of parity check matrix, we consider a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 15 & 14 & 1 & 13 & 2 & 3 & 4 & 12 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{pmatrix}$$

Then

$$\mathbf{H}_1 = \boldsymbol{\sigma}(\mathbf{H}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Corresponding to $\mathbf{H}_1$ the generator matrix is $\mathbf{G}_1 = (\mathbf{I}_{11} \quad \mathbf{A}^t)$, where

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Applying the permutation $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$, we obtain the generator matrix of the Hamming code as

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem 6.3

The binary cyclic code of length $n = 2^m - 1$ for which the generator is the minimal polynomial of a primitive element of $GF(2^m)$ is equivalent to the $(n - m, n)$ Hamming code.

Proof

Let α be a primitive element of $GF(2^m)$. Let $m(X)$ be the minimal polynomial of α over $\mathbb{B}$. Since for $\beta \in GF(2^m)$, β and β^2 have the same minimal polynomial, $\alpha, \alpha^2, \ldots, \alpha^{2^{m-1}}$ are distinct roots of $m(X)$. Since the degree $[GF(2^m) : \mathbb{B}] = m$, the degree of the minimal polynomial of any element of $GF(2^m)$ over $\mathbb{B}$ is at most m. Hence

$$m(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{2^{m-1}})$$

The elements $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ form a basis of $GF(2^m)$ over $\mathbb{B}$ and, therefore,

$$\begin{matrix} l & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ ) & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ l & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ ) & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{matrix}\Bigg)$$

atrix is $\mathbf{G}_1 = (\mathbf{I}_{11} \quad \mathbf{A}^t)$, where

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

:olumns of $\mathbf{G}_1$, we obtain the generator

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}\left.\vphantom{\begin{matrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{matrix}}\right)$$

$2^m - 1$ for which the generator is the lement of GF(2^m) is equivalent to the

Let $m(X)$ be the minimal polynomial of β^2 have the same minimal polynomial,). Since the degree $[\mathrm{GF}(2^m):\mathbb{B}] = m$, the ıy element of GF($2^m$) over $\mathbb{B}$ is at most m.

$$-\alpha^2)\cdots(X - \alpha^{2^{m-1}})$$

a basis of GF(2^m) over $\mathbb{B}$ and, therefore,

every element of GF(2^m) can be uniquely written as

$$\sum_{i=0}^{m-1} e_i\alpha^i \quad e_i \in \mathbb{B}$$

For $0 \le j \le 2^m - 2$, let

$$\alpha^j = \sum_{i=0}^{m-1} e_{ij}\alpha^i$$

and let $\mathbf{H}$ be the $m \times n$ matrix, the $(j+1)$th column of which is

$$(e_{0j} \quad e_{1j} \quad \cdots \quad e_{m-1,j})^t$$

Every row vector

$$(e_{0j} \quad e_{1j} \quad \cdots \quad e_{m-1,j})$$

gives the binary representation of one and only one positive integer at most n.

Now $a(X) + \langle X^n - 1\rangle$ belongs to the cyclic code generated by $m(X)$ iff $a(\alpha) = 0$. But this is so iff $\mathbf{H}\mathbf{a}^t = 0$, where $a = (a_0 a_1 \cdots a_{n-1})$ with

$$a(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$$

Therefore, the cyclic code generated by $m(X)$ is the same as the code given by the parity check matrix $\mathbf{H}$. But $\mathbf{H}$ is obtained by permutating the binary representations of the numbers $1, 2, \ldots, n$. This completes the proof.

Remark 6.1

Observe that, in the above proof, we have also shown that a binary Hamming code is a BCH code (up to equivalence).

We have seen earlier that every non-zero element of GF(2^m) is a root of the polynomial $X^n - 1$ with $n = 2^m - 1$. Therefore, the minimal polynomial of every element β of GF(2^m) divides $X^n - 1$. Also the minimal polynomials of two elements are either identical or relatively coprime. Hence, if α is a primitive element of GF(2^m) and $d \ge 2$ is a positive integer then

$$g(X) = \mathrm{LCM}\,\{m_1(X), \ldots, m_{d-1}(X)\}$$

where $m_i(X)$ denotes the minimal polynomial of α^i, divides $X^n - 1$. It then follows that the polynomial code of length n generated by $g(X)$ is the same as the cyclic code with generator $g(X)$. Thus, every binary BCH code is a cyclic code.

6.4 NON-BINARY HAMMING CODES

We have so far restricted ourselves only to binary Hamming codes. However, Hamming codes may be defined over any finite field GF(q).