

(c)

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

Determine all the code words of the three codes. Does each of these codes correct all single errors?

### Definition 1.15 – dual codes

Let  $C$  be the  $(m, n)$  code with generator matrix  $\mathbf{G} = (\mathbf{I}_m \ A)$ . Then  $(n - m, n)$  matrix code defined by the parity check matrix  $\mathbf{H} = (A^T \ \mathbf{I}_m)$  is called the **dual code** of  $C$  and it is denoted by  $C^\perp$ .

For example, if  $C$  is the code defined by the matrix

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

all the code words of this code are

$$0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1$$

The minimum distance of the code is 3 and so it is a double error detecting, single error correcting code. Writing  $\mathbf{G} = (\mathbf{I} \ A)$  we find that  $\mathbf{H} = (A^T \ \mathbf{I})$ . The code words of the code with  $\mathbf{H}$  as the parity check matrix are the same as the code words of the code with generator matrix

$$\mathbf{G}_1 = (\mathbf{I}_3 \ A^T) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Hence all the code words are

$$\begin{aligned} 0\ 0\ 0 &\longrightarrow 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \longrightarrow 0\ 1\ 1\ 1\ 1 \\ 0\ 0\ 1 &\longrightarrow 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \longrightarrow 1\ 0\ 1\ 1\ 0 \\ 0\ 1\ 0 &\longrightarrow 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \longrightarrow 1\ 1\ 0\ 0\ 1 \\ 1\ 0\ 0 &\longrightarrow 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0 \longrightarrow 1\ 1\ 1\ 0\ 0 \end{aligned}$$

The minimum distance of the code is 2 and so it is single error detecting. It is not a single error correcting code; for example, for the received word 1 1 1 0 1 we have

$$1\ 1\ 1\ 0\ 0 + 0\ 0\ 0\ 0\ 1 = 1\ 1\ 0\ 0\ 1 + 0\ 0\ 1\ 0\ 0$$

it is at equal distance from two code words and so we are unable to decide about the code word transmitted.

Incidentally, the above also shows that the dual of a single error correcting code need not be single error correcting.

## 22 Group codes

### Exercise 1.3

1. Find generator and parity check matrices for dual codes to the codes in questions 2 and 3 of Exercise 1.2.
2. Find a code  $E: \mathbb{B}^2 \rightarrow \mathbb{B}^6$  with minimum distance 4.
3. Describe the generator matrices  $\mathbf{G}$  whose associated parity check matrices  $\mathbf{H}$  will correctly decode all single errors. (We answer this question in the following theorem.)

### Theorem 1.7

An  $(m, n)$ -code with generator matrix  $\mathbf{G} = (\mathbf{I}_m \quad \mathbf{A})$  will decode all single errors correctly iff all the rows of  $\mathbf{A}$  are distinct and the weight of each one of them is at least 2.

#### *Proof*

The parity check matrix of this code is  $\mathbf{H} = (\mathbf{A}^t \quad \mathbf{I}_{n-m})$ . But the parity check matrix  $\mathbf{H}$  decodes all single errors correctly iff all the columns of  $\mathbf{H}$  are non-zero and distinct. But this is so iff all the columns of  $\mathbf{A}^t$  are distinct and each one of them is of weight at least 2. This is so iff the rows of  $\mathbf{A}$  are all distinct and each one of them is of weight at least 2.

This theorem may be restated as follows:

### Theorem 1.8

An  $(m, n)$ -code with generator matrix  $\mathbf{G}$  will decode all single errors correctly iff the distance between any two rows of  $\mathbf{G}$  is at least 3 and each one of them is of weight at least 3.

Let  $\mathbf{H}$  be a parity check matrix and  $\mathbf{C}$  be the  $(m, n)$ -code defined by  $\mathbf{H}$ . Then, we know that  $\mathbf{C}$  is a group code.  $\mathbf{C}$  is in fact a subgroup of  $\mathbb{B}^n$ . We then have the following proposition.

### Proposition 1.3

Words  $x, y \in \mathbb{B}^n$  are in the same coset of  $\mathbf{C}$  iff they have the same syndrome.

#### *Proof*

$x, y$  are in the same coset iff  $y = x + c$  for some code word  $c \in \mathbf{C}$ . But this is so iff  $x + y = c \in \mathbf{C}$ . Now

$$\begin{aligned} x + y \in \mathbf{C} &\text{ iff } \mathbf{H}(x + y)^t = 0 \\ &\Leftrightarrow \mathbf{H}(x^t + y^t) = 0 \\ &\Leftrightarrow \mathbf{H}x^t + \mathbf{H}y^t = 0 \\ &\Leftrightarrow \mathbf{H}x^t = \mathbf{H}y^t \end{aligned}$$

**Remark**

Throughout this chapter, we restricted ourselves to the field  $\mathbb{B}$  of two elements. This was done to keep the presentation simple and for having a concrete picture. However, most of the material could equally well have been developed over any finite field.

Let  $F$  be a finite field and  $F^{(n)}$  be the set of all sequences of length  $n$  with entries in the field  $F$ . By the weight (or **Hamming weight**)  $\text{wt}(a)$  of a word  $a$  we mean the number of non-zero entries in  $a$ . Also for  $a = a_1a_2\cdots a_n$ ,  $b = b_1b_2\cdots b_n$  in  $F^{(n)}$ , we define the distance  $d(a, b)$  between  $a$  and  $b$  to be the number of  $i$ 's for which  $a_i \neq b_i$ . Lemma 1.1 then becomes  $d(a, b) = \text{wt}(a - b) \forall a, b \in F^{(n)}$  while its Corollary, Lemma 1.2, Theorems 1.1, 1.2, 1.3 remain valid without change (of course, slight changes in the proofs are needed). We could have, similarly, defined and studied matrix codes and group codes over  $F$  and almost all the results of section 1.2 and section 1.3 (up to Theorem 1.5) are valid in the general case. Statement of Theorem 1.6 needs slight change.

**Exercise 1.4**

Prove all the results stated in the above remark and others that are valid over any finite field.

## 2

# Polynomial codes

---

We have considered earlier one algebraic technique for obtaining/studying codes namely that of **matrix techniques**. We now introduce another important algebraic technique (not totally unrelated to the matrix techniques) for studying codes. This technique is through **polynomial multiplication**. The codes thus obtained are called polynomial codes. Most of the important codes studied today are polynomial codes.

## 2.1 DEFINITION OF VECTOR SPACE AND POLYNOMIAL RING

### Definition 2.1 – vector spaces

Let  $F$  be a field. A non-empty set  $V$  is called a **vector space over  $F$**  if:

- (i) there is defined an addition in  $V$ , w.r.t. which  $V$  is an Abelian group;
- (ii) for every  $a \in F$ ,  $v \in V$ , there is defined a unique element  $av \in V$  such that for  $v, v_1, v_2 \in V$ ,  $a, b \in F$  and 1 the identity of  $F$ ,
  - (a)  $a(v_1 + v_2) = av_1 + av_2$
  - (b)  $(a + b)v = av + bv$
  - (c)  $(ab)v = a(bv)$
  - (d)  $1 \times v = v$

Let  $V$  be a vector space over a field  $F$ . A set  $\{v_1, v_2, \dots, v_n\}$  of elements of  $V$  is called **linearly independent** if whenever

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$$

where  $a_1, a_2, \dots, a_n$  are in  $F$ , then

$$a_1 = a_2 = \cdots = a_n = 0$$

If the elements  $v_1, v_2, \dots, v_n \in V$  are linearly independent over  $F$  and every element  $v$  of  $V$  can be expressed in the form  $a_1v_1 + \cdots + a_nv_n$ ,  $a_i \in F$ ,  $1 \leq i \leq n$ , then  $\{v_1, \dots, v_n\}$  is called a **basis of  $V$** . Also then  $V$  is said to be of **dimension  $n$**  over  $F$  and we express it by  $\dim V = n$ .

Let  $V, W$  be two vector spaces over the same field  $F$ . A map  $f: V \rightarrow W$  is called an **isomorphism** if the map  $f$  is one-one and onto and  $\forall v, v_1, v_2 \in V, a \in F$ ,

$$f(v_1 + v_2) = f(v_1) + f(v_2) \quad f(av) = af(v)$$

### **Proposition 2.1**

If  $V, W$  are vector spaces of equal finite dimension over the same field  $F$ , then  $V$  and  $W$  are isomorphic.

#### **Proof**

Let  $\dim V = \dim W = n < \infty$ . Let  $\{x_1, \dots, x_n\}$  be a basis of  $V$  over  $F$  and  $\{y_1, \dots, y_n\}$  be a basis of  $W$  over  $F$ . Since every element of  $V$  can be uniquely written as  $a_1x_1 + \dots + a_nx_n$ , with  $a_i \in F$ , the map  $\theta: V \rightarrow W$  given by

$$\theta(a_1x_1 + \dots + a_nx_n) = a_1y_1 + \dots + a_ny_n \quad a_i \in F$$

is well defined. It is fairly easy to see that  $\theta$  is a homomorphism. Also, if

$$\theta(a_1x_1 + \dots + a_nx_n) = 0$$

then

$$a_1y_1 + \dots + a_ny_n = 0$$

which implies that

$$a_1 = \dots = a_n = 0$$

the elements  $y_1, \dots, y_n$  being linearly independent.

Thus  $a_1x_1 + \dots + a_nx_n = 0$  and  $\theta$  is one-one. As every element of  $W$  is of the form

$$a_1y_1 + \dots + a_ny_n = \theta(a_1x_1 + \dots + a_nx_n)$$

for some  $a_1, \dots, a_n \in F$ ,  $\theta$  is onto as well and, hence, an isomorphism. ■

Let  $F$  be a field and  $X$  be a variable. Let  $F[X]$  denote the set of all polynomials in the variable  $X$  over  $F$ , i.e.  $F[X]$  is the set of all finite formal sums of the form

$$a_0 + a_1X + \dots + a_nX^n$$

where  $a_i \in F$ . The set  $F[X]$  with the usual addition and multiplication, i.e. for

$$a(X) = a_0 + a_1X + \dots + a_mX^m$$

$$b(X) = b_0 + b_1X + \dots + b_nX^n$$

in  $F[X]$

$$a(X) + b(X) = c_0 + c_1X + c_2X^2 + \dots$$

and

$$a(X)b(X) = d_0 + d_1X + \dots + d_{m+n}X^{m+n}$$