# 5

# Linear codes

We have earlier studied codes which are Abelian groups. These codes were called group codes. Also these codes were considered over $\mathbb{B}$ the field of two elements. In this chapter, we study codes over a finite field GF($q$) of $q$ elements which generalize the concept of group codes studied earlier. Codes studied here are called **linear codes**.

Let $F = \mathrm{GF}(q)$, where $q$ is a prime power, be a field of $q$ elements. Let $V(n, q)$ denote the set of all vectors or sequences of length $n$ over $F$. Then $V(n, q)$ is a vector space of dimension $n$ over $F$. (Observe the change of notation here).

**Definition 5.1**
A subspace $\mathscr{C}$ of $V(n, q)$ is called a **linear code** of length $n$ over $F$.

A vector space is first of all an Abelian group w.r.t. addition. It therefore follows that a linear code is always a group code. In view of this, we have the following proposition.

**Proposition 5.1**
The minimum distance $d$ of a linear code $\mathscr{C}$ equals the minimum among the weights of non-zero code words.

## 5.1 GENERATOR AND PARITY CHECK MATRICES

Let $\mathscr{C}$ be a linear code of length $n$ over $F$. Let $k(\leq n)$ be the dimension of $\mathscr{C}$ over $F$ and choose a basis

$$X^{(1)}, X^{(2)}, \ldots, X^{(k)}$$

of $\mathscr{C}$ over $F$. Then any element of (or code word in) $\mathscr{C}$ is of the form

$$a_1 X^{(1)} + a_2 X^{(2)} + \cdots + a_k X^{(k)} = (a_1 \quad a_2 \quad \cdots \quad a_k)\mathbf{G}$$

where

$$\mathbf{G} = \begin{pmatrix} X^{(1)} \\ X^{(2)} \\ \vdots \\ X^{(k)} \end{pmatrix}$$

is a $k \times n$ matrix over $F$. The rows of the matrix $\mathbf{G}$ being linearly independent, the matrix $\mathbf{G}$ is of rank $k$. Thus $\mathscr{C}$ is a matrix code with a generator matrix $\mathbf{G}$. By choosing a different basis of $\mathscr{C}$ over $F$, we produce another generator matrix of $\mathscr{C}$.

Let $\mathbf{A} = (a_{ij})$ be a non-singular square matrix of order $k$ over $F$. Then $\mathbf{AG}$ is a $k \times n$ matrix over $F$ and $\forall i$, $1 \leq i \leq k$, the $i$th row of $\mathbf{AG}$ is

$$a_{i1}X^{(1)} + a_{i2}X^{(2)} + \cdots + a_{ik}X^{(k)}$$

Therefore, the rows of $\mathbf{AG}$ generate a subspace of $\mathscr{C}$.

**Proposition 5.2**
$\mathbf{AG}$ is a generator matrix of $\mathscr{C}$.

***Proof***
We know that

$$\text{rank } \rho(\mathbf{AG}) \leq \min\{\text{rank}(\mathbf{A}), \text{rank}(\mathbf{G})\} \leq \text{rank } \mathbf{G} = \rho(\mathbf{G}) = k$$

Again,

$$k = \rho(\mathbf{G}) = \rho(\mathbf{A}^{-1}\mathbf{AG}) \leq \min\{\rho(\mathbf{A}^{-1}), \rho(\mathbf{AG})\} \leq \rho(\mathbf{AG})$$

Hence $\rho(\mathbf{AG}) = \rho(\mathbf{G}) = k$ and the rows of $\mathbf{AG}$ are linearly independent. Thus the rows of $\mathbf{AG}$ generate a subspace of dimension $k$ of $\mathscr{C}$ which itself is of dimension $k$. Then any element of $\mathscr{C}$ is of the form $a(\mathbf{AG})$ for some $a \in V(k, q)$. Hence $\mathbf{AG}$ is a generator matrix of $\mathscr{C}$.

If $\mathscr{C}$ is a linear code of length $n$, the dimension of $\mathscr{C}$ is $k$, and $d$ is the minimum distance of $\mathscr{C}$, we then say that $\mathscr{C}$ is a linear $[n, k, d]$ code over $F$.

**Definition 5.2**
Two codes $\mathscr{C}$ and $\mathscr{C}'$ of length $n$ are said to be **equivalent** if there exists a permutation $\sigma$ of the $n$-symbols $\{1, 2, \ldots, n\}$ such that $c' = (c'_1, c'_2, \ldots, c'_n) \in \mathscr{C}'$ iff $c' = \sigma(c)$ for some $c \in \mathscr{C}$, where

$$\sigma(c) = \sigma(c_1, \ldots, c_n) = (c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)})$$

Observe that equivalent codes have the same minimum distance and, therefore, the same error detection/correction capability. Therefore, for studying error detection/correction, we may work with equivalent code if that helps our study.

Let $\sigma$ be a permutation of the set $\{1,2,\ldots,n\}$. Suppose that $\sigma(j)=i_j$, $1\leq j\leq n$, so that

$$\{i_1,,\ldots,i_n\}=\{1,2,\ldots,n\}$$

Let $\mathbf{P}$ be a square matrix of order $n$ in which $(i_j,j)$ entry is 1 for every $j$, $1\leq j\leq n$, and every other entry is 0. The matrix $\mathbf{P}$ has exactly one non-zero entry (which is in fact 1) in every row and in every column. Such a matrix is called a **permutation matrix** and is clearly non-singular. Let $\mathbf{P}=(p_{ij})$. For any vector $\mathbf{c}=(c_1 \quad \cdots \quad c_n)$, the $j$th entry of $\mathbf{cP}$ is

$$c_1p_{1j}+c_2p_{2j}+\cdots+c_np_{nj}=c_{i_j}$$

as $p_{kj}=0$ for $k\neq i_j$. Therefore,

$$\mathbf{cP}=(c_{i_1} \quad c_{i_2} \quad \cdots \quad c_{i_n})=\sigma(\mathbf{c})$$

Conversely, given a permutation matrix $\mathbf{P}$ of order $n$, we can define a permutation $\sigma$ of the set $\{1,2,\ldots,n\}$ such that for any vector $\mathbf{c}\in V(n,q)$, $\mathbf{cP}=\sigma(\mathbf{c})$. (This justifies the name permutation matrix.) We thus have the following proposition.

**Proposition 5.3**
Two codes $\mathscr{C}$ and $\mathscr{C}'$ of length $n$ are equivalent iff there exists a permutation matrix $\mathbf{P}$ of order $n$ such that $\mathscr{C}=\{\mathbf{cP}/\mathbf{c}\in\mathscr{C}\}$.

**Corollary**
If $\mathscr{C}$ is a linear $[n,k,d]$ code, then so is its equivalent code $\mathscr{C}'$.

**Theorem 5.1**
Given a linear $[n,k,d]$ code $\mathscr{C}$ over $F$, there exists an equivalent code $\mathscr{C}'$ having a generator matrix, the first $k$ columns of which form the identity matrix $\mathbf{I}_k$.

***Proof***
Let $\mathbf{G}$ be a generator matrix of $\mathscr{C}$. Let $\mathbf{G}_1,\mathbf{G}_2,\ldots,\mathbf{G}_n$ denote the columns of $\mathbf{G}$ and suppose that

$$\mathbf{G}_{i_1},\mathbf{G}_{i_2},\ldots,\mathbf{G}_{i_k} \quad \text{for} \quad 1\leq i_1<i_2<\cdots<i_k\leq n$$

are linearly independent. Let $\sigma$ be a permutation of the set $\{1,2,\ldots,n\}$ with $\sigma(j)=i_j$, $1\leq i\leq k$. Let $\mathbf{P}=(p_{ij})$ be the permutation matrix of order $n$ associated with the permutation $\sigma$. Then, for $1\leq j\leq k$, $p_{\ell j}=0$ for $\ell\neq i_j$ and $p_{i_jj}=1$. In the matrix

$$\mathbf{M}=\mathbf{GP}=(\mathbf{G}_1 \quad \cdots \quad \mathbf{G}_n)\begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix}$$

$$= \left( \sum_j \mathbf{G}_j p_{j1} \quad \sum_j \mathbf{G}_j p_{j2} \quad \cdots \quad \sum_j \mathbf{G}_j p_{jk} \quad \cdots \quad \sum_j \mathbf{G}_j p_{jn} \right)$$

$$= (\mathbf{G}_{i_1} \quad \mathbf{G}_{i_2} \quad \cdots \quad \mathbf{G}_{i_k} \quad \cdots)$$

the first $k$ columns are linearly independent. Let $\mathscr{C}'$ be the code of length $n$ with $\mathbf{M}$ as a generator matrix. Now

$$\begin{aligned} \mathscr{C}' &= \{\mathbf{aM} | \mathbf{a} \in V(k, q)\} \\ &= \{\mathbf{aGP} | \mathbf{a} \in V(k, q)\} \\ &= \{\mathbf{cP} | \mathbf{c} \in \mathscr{C}\} \end{aligned}$$

and, therefore, $\mathscr{C}'$ is equivalent to $\mathscr{C}$. The code $\mathscr{C}'$ is linear.

Let

$$\mathbf{A} = (\mathbf{G}_{i_1} \quad \mathbf{G}_{i_2} \quad \cdots \quad \mathbf{G}_{i_k})$$

The columns $\mathbf{G}_{i_1}, \ldots, \mathbf{G}_{i_k}$ being linearly independent, $\mathbf{A}$ is a non-singular square matrix of order $k$. Therefore $\mathbf{A}^{-1}\mathbf{M}$ is also a generator matrix of $\mathscr{C}'$. Writing $\mathbf{M} = (\mathbf{A} \quad \mathbf{B})$, where $\mathbf{B}$ is a $k \times (n-k)$ matrix, we find that a generator matrix (of $\mathscr{C}'$) is

$$\mathbf{A}^{-1}\mathbf{M} = \mathbf{A}^{-1}(\mathbf{A} \quad \mathbf{B}) = (\mathbf{A}^{-1}\mathbf{A} \quad \mathbf{A}^{-1}\mathbf{B}) = (\mathbf{I}_k \quad \mathbf{A}^{-1}\mathbf{B})$$

**Proposition 5.4**
If $\mathscr{C}$ is a linear $[n, k, d]$ code over $F$, then $d \leq n - k + 1$.

***Proof***
Since equivalent codes have the same minimum distance, we may assume that $\mathscr{C}$ is a linear code with a generator matrix $\mathbf{G}$ such that the first $k$ columns of $\mathbf{G}$ form the identity matrix. Let $e^i$ be a message word with 1 in the $i$th position and zero everywhere else. The corresponding code word $\mathbf{e}^i\mathbf{G}$ is the $i$th row of $\mathbf{G}$ which has at least $k-1$ zero entries. So the weight of this non-zero code word is at most $n-(k-1)$, i.e. $n-k+1$. Hence $d \leq n-k+1$.

In the case of binary codes with generator matrix $\mathbf{G} = (\mathbf{I}_k \quad \mathbf{A})$ and parity check matrix $\mathbf{H} = (\mathbf{B} \quad \mathbf{I}_{n-k})$ we have seen that $\mathbf{B} = \mathbf{A}^t$. However, in the case of codes over an arbitrary finite field $F$, the relationship between the generator matrix and parity check matrix is given by the following proposition.

**Proposition 5.5**
If $\mathscr{C}$ is a linear $[n, k, d]$ code over $F$ with parity check matrix $\mathbf{H} = (\mathbf{A} \quad \mathbf{I}_{n-k})$ where $\mathbf{A}$ is an $(n-k) \times k$ matrix over $F$, then a generator matrix of $\mathscr{C}$ is given by $\mathbf{G} = (\mathbf{I}_k \quad -\mathbf{A}^t)$.

***Proof***
Let $u = u_1 \cdots u_n$ be the code word corresponding to the message word $a = a_1 \cdots a_k$. Let $\mathbf{u} = (\mathbf{v} \quad \mathbf{w})$, where $\mathbf{v}$ is $1 \times k$ and $\mathbf{w}$ is $1 \times (n-k)$ matrix. From the

definition of the code given by parity check matrix $\mathbf{H}$, $\mathbf{v} = \mathbf{a}$ and then $\mathbf{Hu}^t = 0$ implies that

$$(\mathbf{A} \quad \mathbf{I}_{n-k})\begin{pmatrix} \mathbf{a}^t \\ \mathbf{w}^t \end{pmatrix} = 0 \quad \text{or} \quad \mathbf{Aa}^t + \mathbf{w}^t = 0$$

Thus $\mathbf{w} = -\mathbf{aA}^t$ and hence $\mathbf{u} = \mathbf{a}(\mathbf{I}_k \quad -\mathbf{A}^t)$. Thus $u$ is a code word corresponding to the message word $a$ in the code defined by the generator matrix $\mathbf{G} = (\mathbf{I}_k \quad -\mathbf{A}^t)$.

Conversely, consider the code word $u$ with

$$\mathbf{u} = \mathbf{aG} = (\mathbf{a} \quad -\mathbf{aA}^t)$$

corresponding to the message word $a$ in the code defined by $\mathbf{G} = (\mathbf{I}_k \quad -\mathbf{A}^t)$. Then

$$\mathbf{Hu}^t = (\mathbf{A} \quad \mathbf{I}_{n-k})\begin{pmatrix} \mathbf{a}^t \\ -\mathbf{Aa}^t \end{pmatrix} = \mathbf{Aa}^t - \mathbf{Aa}^t = 0$$

Therefore, $u$ is the code word corresponding to $a$ in the code given by $\mathbf{H}$.

**Examples 5.1**

***Case (i)***
Every binary group code is a linear code.

***Case (ii)***
Every polynomial code and every matrix code is a linear code. In particular, BCH codes are linear codes and so are Hamming codes.

***Case (iii)***
Every group code over the field of three elements is a linear code. (A code over the field of three elements is called a **ternary code**.)

***Case (iv)***
The following binary codes are linear codes:

(a)
$$\begin{matrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{matrix}$$

(b)
$$\begin{matrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{matrix}$$

(c)
$$\begin{matrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

The generator matrices of these codes are respectively

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

***Case (v)***
The matrices

$$\mathbf{P}=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\quad\text{and}\quad \mathbf{Q}=\begin{pmatrix}0&0&0&1\\0&1&0&0\\1&0&0&0\\0&0&1&0\end{pmatrix}$$

are permutation matrices and with **A**, **B**, **C** as in Case (iv) above we have

$$\mathbf{B}=\mathbf{AP}\quad \mathbf{A}=\mathbf{CQ}$$

Thus, the codes (a) and (b) of Case (iv) are equivalent and so are the codes (a) and (c). But then the codes (b) and (c) are also equivalent. This could also be observed from the relation $\mathbf{B}=\mathbf{C}(\mathbf{QP})$, as the product of permutation matrices is again a permutation matrix.

***Case (vi)***
Observe the following:

(a) The permutation matrix **P** corresponding to the permutation $\sigma=(1,2,3)$ of the set $\{1,2,3,4\}$ is given by

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

(b) That corresponding to $\sigma=(1,2)(3,4)$ of the set $\{1,2,3,4\}$ is given by

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

(c) The permutation matrix **P** corresponding to the permutation $\sigma=(1,3)(2,4)$ of the set $\{1,2,3,4\}$ is given by

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