Chapter 5

Linear Codes

The space is $V(n,q) = ((\mathbf{F}_q)^n, +, \times)$. For $x \in V(n,q)$, write

$$x = (x_1, x_2, \ldots, x_n) = x_1 x_2 \cdots x_n.$$

Definition 5.1. (i) A *linear code* is a subspace of $V(n,q)$.

(ii) If $\dim C = k$, then C is an

$$[n,k]\text{-code or } [n,k]_q\text{-code},$$

or, if $d(C) = d$, it is an

$$[n,k,d]\text{-code or } [n,k,d]_q\text{-code}.$$

Note 5.2. A q-ary $[n,k,d]$-code is a q-ary (n, q^k, d)-code.

Definition 5.3. The *weight* $w(x)$ of x in $V(n,q)$ is

$$w(x) = d(x, 0);$$

that is, $w(x)$ is the number of non-zero elements in x.

Lemma 5.4. *$d(x,y) = w(x-y)$ for $x, y \in V(n,q)$.*

Proof $x - y$ has non-zero entries in those coordinates where x and y differ. □

Theorem 5.5. *For a linear code C,*

$$d(C) = \min_{x \neq 0} w(x).$$

Proof Show the two inequalities. First,

$$d(C) = \min_{x \neq y} d(x,y) = \min_{x \neq y} w(x-y) \leq \min_{x \neq 0} w(x).$$

Conversely, there exist $y, z \in C$ such that

$$d(C) = d(y,z) = w(y-z) \geq \min_{x \neq 0} w(x),$$

since $y - z \in C$. □

Example 5.6. The perfect $(7, 16, 3)$-code.

This is a binary $[7, 4, 3]$-code

$$C = \{u, z, l_1, \dots, l_7, m_1, \dots, m_7\}$$

based on PG(2, 2) and has $d(C) = 3$ since $w(u) = 7,\ w(l_i) = 3,\ w(m_i) = 4.$

To specify a linear code of dimension k, only k basis vectors are required!

Definition 5.7. A *generator matrix* G of an $[n, k]$-code C is a $k \times n$ matrix whose rows form a basis for C.

Example 5.8. From Example 4.1,

$$C_1 = \{00, 01, 10, 11\}$$

is a binary $[2, 2]$-code with generator matrix

$$G = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad \cdots .$$

Similarly,

$$C_2 = \{000, 011, 101, 110\}$$

is a binary $[3, 2]$-code with generator matrix

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},$$

and

$$C_3 = \{00000, 01101, 10110, 11011\}$$

is a binary $[5, 2]$-code with generator matrix

$$G = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Theorem 5.9. *By definition,* rank $G = \dim C$.

Definition 5.10. Two linear codes C and C' in $V(n, q)$ are *equivalent* if C' can be obtained from C by one of the following operations:

(A) some permutation of the coordinates in every codeword;

(B) multiplying the coordinate in a fixed position by a non-zero scalar.

This can be also described as follows. If $\sigma \in S_n$ and $\lambda_1, \dots, \lambda_n \in \mathbf{F}_q \setminus \{0\}$,

(A) $x_1\, x_2\, x_3 ... x_{n-1}\, x_n \longrightarrow x_{1\sigma}\, x_{2\sigma}\, \cdots\, x_{(n-1)\sigma}\, x_{n\sigma};$

(B) $x_1\, x_2\, x_3 \cdots x_{n-1}\, x_n \longrightarrow \lambda_1 x_1\, \lambda_2 x_2\, \cdots\, \lambda_n x_n.$

The point about (A) and (B) is that they preserve the distance of any two codewords, and the minimum distance of the code, as well as the dimension.

Theorem 5.11. *If $f : C \to C'$ is a transformation obtained by using (A) and (B), with $f(C) = C'$, then*

(i) $d(x, y) = d(f(x), f(y))$;

(ii) $d(C) = d(C')$;

(iii) $\dim C = \dim C'$.

Recall the row operations (R1), (R2), (R3). Now, what column operations do (A) and (B) give? Let (C1), (C2), (C3) be the corresponding column operations.

(A) $\to$ (C2) $c_i \leftrightarrow c_j$;

(B) $\to$ (C1) $c_i \to \lambda c_i$.

Theorem 5.12. *Two $k \times n$ matrices G, G' generate equivalent linear $[n, k]$-codes over $\mathbf{F}_q$ if G' can be obtained from G by a sequence of operations* (R1), (R2), (R3), (C1), (C2).

Proof The (Ri) change the basis of a code; the (Cj) change G to G' for an equivalent code. □

Note 5.13. Column operations generally change the code!

Theorem 5.14. *Let G be a generator matrix of an $[n, k]$-code. Then, by the elementary operations, G can be transformed to* standard form,

$$[I_k \quad A],$$

where I_k is the $k \times k$ identity and A is $k \times (n - k)$.

Proof By row or column operations obtain a non-zero pivot g_{11}. Then use row operations to obtain $g_{i1} = 0, \quad i > 1$.

$$G' = \begin{array}{c|ccccc} 1 & * & . & . & . & * \\ \hline 0 & & & & & \\ 0 & & & & & \\ . & & & H & & \\ . & & & & & \\ . & & & & & \\ 0 & & & & & \end{array}$$

Use row or column operations on G' to obtain $h_{11} \neq 0$. Continue. Then use row operations to get I, unless column operations are required. □

Example 5.15. (i) C is a binary $[5, 3]$-code

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

(ii) C is a binary $[6, 4]$-code

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

(iii) C is a ternary $[6, 4]$-code

$$G = \begin{bmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 2 & 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 1 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{bmatrix}$$

Corollary 5.16. *If $G_1 = [I_k\, A_1]$ and $G_2 = [I_k\, A_2]$ are generator matrices of the same code C, then $A_1 = A_2$.*

Proof The first row of G_2 must be a linear combination of the rows of G_1, and hence is the first row of G_1. Similarly for the other rows of G_2. $\square$