Chapter 7

The Dual Code and the Parity-Check Matrix

Definition 7.1. Let $x, y \in V(n, q)$. Then

$$x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

is the *scalar product* of x and y.

If $x \cdot y = 0$, then x and y are *orthogonal*.

Note 7.2. The scalar product satisfies the following:

(i) $(x + y) \cdot z = x \cdot y + y \cdot z$;

(ii) $(\lambda x \cdot y) = \lambda(x \cdot y)$;

(iii) $x \cdot y = y \cdot x$.

Definition 7.3. Given an $[n, k]$-code C, the *dual code* $C^\perp$ is given by

$$C^\perp = \{x \in V(n, q) \mid x \cdot y = 0, \text{ for all } y \in C\}.$$

Example 7.4. (i)

$$\begin{aligned} C &= \{0000, 1001, 0110, 1111\}, \\ C^\perp &= \{0000, 1001, 0110, 1111\}. \end{aligned}$$

(ii)

$$\begin{aligned} C &= \{0000, 1000, 0100, 1100\}, \\ C^\perp &= \{0000, 0010, 0001, 0011\}. \end{aligned}$$

Lemma 7.5. *If C is an $[n, k]$-code with generator matrix G, then*

(i) *$C^\perp$ is a linear code;*

(ii) *$C^\perp = \{x \in V(n, q) \mid xG^T = 0\}$; that is, x is orthogonal to every row of G.*

Proof (i) If $y, y' \in C^\perp$, then

$$\begin{aligned} x \cdot y = x \cdot y' = 0 \text{ for all } x \in C \\ \Rightarrow x \cdot (y + y') = 0 \text{ for all } x \in C, \\ x \cdot (\lambda y) = 0 \text{ for all } x \in C. \end{aligned}$$

(ii)

$$xG^T = 0 \Longleftrightarrow x[r_1^T, \ldots, r_k^T] = 0 \Longleftrightarrow x \cdot r_i^T = 0 \text{ for all } i \Longleftrightarrow x \cdot r_i = 0 \text{ for all } i,$$

where $r_1, \ldots, r_k$ are the rows of G. □

Definition 7.6. A *parity-check matrix* H for an $[n, k]$-code C is an $(n-k) \times n$ matrix which is a generator matrix for $C^\perp$.

Theorem 7.7. (i) *If C is an $[n, k]$-code over $\mathbf{F}_q$, then $C^\perp$ is an $[n, n-k]$-code over $\mathbf{F}_q$.*

(ii) *If $G = [I_k\, A]$, then a generator matrix for $C^\perp$ is $H = [-A^T\, I_{n-k}]$.*

Proof (i) By Lemma 7.5, $C^\perp$ is a linear code of length n over $\mathbf{F}_q$. If G is a generator matrix for C, with rows $r_1, \ldots, r_k$ and columns $c_1, \ldots, c_n$, then

$$G = [c_1, \ldots, c_n] = \begin{bmatrix} r_1 \\ \vdots \\ r_k \end{bmatrix}.$$

Consider $\varphi : V(n, q) \longrightarrow V(k, q)$ given by

$$\begin{aligned} x \longmapsto xG^T &= x[r_1^T, \ldots, r_k^T] \\ &= (x \cdot r_1, \ldots, x \cdot r_k) \\ &= x_1 c_1^T + \cdots + x_n c_n^T \end{aligned}$$

Then

$$n = \dim(\ker \varphi) + \dim(\text{im } \varphi). \tag{7.1}$$

As rank $G = k$, considering im φ in terms of the columns of G, so $\dim(\text{im } \varphi) = k$. Hence, from (7.1) $\dim(\ker \varphi) = n - k$.

Aliter, let $G = [I_k\, A]$ be a generator matrix for C, then $x \in C^\perp \Leftrightarrow Gx^T = 0$:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & a_{11} & \cdots & a_{1,n-k} \\ 0 & 1 & \cdots & 0 & a_{21} & \cdots & a_{2,n-k} \\ \vdots & & & & \vdots & & \\ 0 & & \cdots & 1 & a_{k1} & \cdots & a_{k,n-k} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_k \\ \vdots \\ x_n \end{bmatrix};$$

$$\begin{aligned} x_1 + a_{11}x_{k+1} + \cdots + a_{1,n-k}x_n &= 0, \\ x_2 + a_{21}x_{k+1} + \cdots + a_{2,n-k}x_n &= 0, \\ \vdots \qquad\qquad\qquad\qquad\qquad\qquad &\vdots \\ x_k + a_{k1}x_{k+1} + \cdots + a_{k,n-k}x_n &= 0. \end{aligned}$$

So any choice can be made for $x_{k+1}, \ldots, x_n$; then $x_1, \ldots, x_k$ are determined. Hence $C^\perp = q^{n-k}$. Hence dim $C^\perp = n - k$.

(ii) $G = [I_k\, A]$, $\quad H = [-A^T\, I_{n-k}]$, $\quad$ rank $H = n - k$. Then

$$GH^T = \begin{bmatrix} I_k & A \end{bmatrix} \begin{bmatrix} -A \\ I_{n-k} \end{bmatrix} = I_k(-A) + AI_{n-k} = -A + A = 0.$$

So $HG^T = 0$; that is, the rows $s_1, \ldots, s_{n-k}$ of H are in $C^\perp$. But rank $H = n - k$; so H is a generator matrix for $C^\perp$. □

Example 7.8. $C_2 = \{000, 011, 101, 110\}$ is a $[3, 2]_2$-code

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

Theorem 7.9. *The following are equivalent conditions on H:*

(i) *H is a parity-check matrix for C;*

(ii) *$Hx^T = 0$ for all $x \in C$;*

(iii) *$xH^T = 0$ for all $x \in C$.*

Note 7.10. (i) rank $G = k$, rank $H = n - k$;

(ii) C is equally well-specified by G or H;

(iii) If $G = [I_k\, A]$ then a suitable parity-check matrix is $H = [-A^T\, I_{n-k}]$.

Theorem 7.11. *If C is an $[n, k]_q$-code then $(C^\perp)^\perp = C$.*

Proof If $x \in C$, then $x \cdot y = 0$ for all $y \in C^\perp$. So $x \in (C^\perp)^\perp$. But

$$\dim\,(C^\perp)^\perp = n - (n - k) = k.$$

Hence $C \subset (C^\perp)^\perp$. As dim $C =$ dim $(C^\perp)^\perp$, so $C = (C^\perp)^\perp$. □

Definition 7.12. If $H = [B, I_{n-k}]$ it is in *standard form.*

Example 7.13. $C_3 = \{00000, 01101, 10110, 11011\}$ is a $[5, 2]$-code. Then, with

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

If $x = (x_1, x_2, x_1 + x_2, x_1, x_2) \in C_3$,

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1 + x_4 &= 0, \\ x_2 + x_5 &= 0, \\ x &= (x_1, x_2, x_1 + x_2, x_1, x_2). \end{aligned}$$

Note that $C_3^\perp$ is a $[5, 3]$-code.

Explanation for the term *parity-check matrix* If $u = u_1 \cdots u_k v_1 \cdots v_{n-k}$, where the message symbols are $u_1 \cdots u_k$,

$$Hu^T = 0,$$

$$\begin{bmatrix} c_1 & c_2 & \cdots & c_k & e_1 & e_2 & \cdots & e_{n-k} \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_k \\ v_1 \\ \vdots \\ v_{n-k} \end{bmatrix},$$

$$\begin{bmatrix} B & | & I_{n-k} \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_k \\ v_1 \\ \vdots \\ v_{n-k} \end{bmatrix} = 0,$$

$$\begin{bmatrix} b_{11} & \cdots & b_{1k} & 1 & 0 & \cdots & 0 \\ b_{21} & \cdots & b_{2k} & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \\ b_{n-k,1} & \cdots & b_{n-k,k} & 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_k \\ v_1 \\ \vdots \\ v_{n-k} \end{bmatrix} = 0,$$

$$\sum_{j=1}^{k} b_{ij} u_j + v_i = 0, \quad \text{for } i = 1, \ldots, n-k.$$

As $b_{ij} = -a_{ji}$, so the symbols v_i are determined.

Syndrome Decoding

Definition 7.14. Let H be a parity-check matrix for the $[n, k]$-code C. Then for any $y \in V(n, q)$,

$$s_H(y) = yH^T = (Hy^T)^T$$

is the *syndrome* of y, a vector of length $n - k$.

Lemma 7.15. (i) $yH^T = 0 \iff y \in C$;

(ii) $x + C = y + C \iff x$ *and* y *have the same syndrome;*

(iii) *There exists a one to one correspondence between cosets and syndrome.*

Proof (i) This is by definition.

(ii) $x + C = y + C \iff x - y \in C \iff (x - y)H^T = 0 \iff xH^T = yH^T$.

(iii) This follows from (ii).

□

Algorithm 7.16. I. Set up 1-1 correspondence between coset leaders and syndromes.

II. If y is a received vector, calculate the syndrome $s = yH^T$.

III. Find coset leader e associated to s.

IV. Correct y to $y - e$.

Now much less needs to be stored, namely just coset leaders and syndromes.

Example 7.17. $C_3 = \{00000, 10110, 01101, 11011\}$ Single error-correcting $[5, 2]$-code.

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right] \qquad H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

coset leader	00000	10000	01000	00100	00010	00001	11000	10001
syndrome	000	110	101	100	010	001	011	111

If the received message appears in the last two cosets we need to ask for retransmission, since the weight of the coset leader is 2.

(i) $y = 11110$, $yH^T = 101$, $e = 01000$,

$$x = y - e = y + e = 10110.$$

(ii) $y = 01100$, $yH^T = s = 001$, $e = 00001$,

$$x = y + e = 01101.$$

(iii) $y = 11100$, $yH^T = 111$, $e = 10001$,

ask for retransmission.

Theorem 7.18. *Let C be an $[n, k]$-code with parity-check matrix H. Then*

$$d(C) = d = \min_{x \neq y} d(x, y)$$

if and only if some d columns of H are linearly dependent but every $d-1$ columns are linearly independent.

Proof Let the columns of H be $c_1, \ldots, c_n$, that is, $H = [c_1, \ldots, c_n]$. Then $x \in C$, with $x = x_1 \cdots x_n$, if and only if $Hx^T = 0$; that is,

$$x_1 c_1 + \cdots + x_n c_n = 0.$$

Now, x has weight $d - 1 \iff \exists j_1, \ldots, j_{d-1} \in \mathbf{N}$ such that $x_{j_1}, \ldots, x_{j_{d-1}} \neq 0$ and all other $x_j = 0 \iff x_{j_1} c_{j_1} + \cdots + x_{j_{d-1}} c_{j_{d-1}} = 0$. Hence there exists no word of weight $d - 1$ if and only if every $d - 1$ columns are linearly independent.

Similarly x is a word of weight d if and only if there exists $i_1, \ldots, i_d \in \mathbf{N}$ such that $x_{i_1}, \ldots, x_{i_d} \neq 0$ and all other $x_i = 0$; this occurs if and only if $x_{i_1} c_{i_1} + \cdots + x_{i_d} c_{i_d} = 0$. Hence there exists a word of weight d if and only some d columns are linearly dependent. $\square$

Corollary 7.19. (Singleton bound) *For an $[n, k, d]$-code,*

$$d \leq n - k + 1.$$

Proof As every $d - 1$ columns of H are linearly independent, rank $(H) = n - k \geq d - 1$. □

Example 7.20. (i) Ternary $[4, 2]$-code with parity-check matrix

$$H = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 0 & 2 & 1 & 2 \end{bmatrix}, \qquad d = 3.$$

(ii) Binary $[5, 2]$-code with parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}, \qquad d = 3.$$

(iii) Binary $[8, 4]$-code with parity-check matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}, \qquad d = 4.$$

Definition 7.21. An $[n, k, d]$-code over $\mathbf{F}_q$ with $d = n-k+1$ is *maximum distance separable*, abbreviated MDS.