ECC HW2

2021年10月17日　　上午 03:24

100

3.5 Let C be a linear code with both even- and odd-weight codewords. Show that the number of even-weight codewords is equal to the number of odd-weight codewords.

Let $\begin{cases} C_{even} \text{ be the set of code with even weights} \\ C_{odd} \text{ " odd "} \end{cases}$

Take $\underline{x} \in C_{odd}$, then $\forall \underline{v} \in C_{odd}$

$\underline{v}+\underline{x}$ is even weight codeword $\Rightarrow \underline{v}+\underline{x} \in C_{even}$

$\therefore |C_{odd}| \leq |C_{even}|$

Similarly, $\forall \underline{u} \in C_{even}$, $\underline{u}+\underline{x} \in C_{odd} \Rightarrow |C_{even}| \leq |C_{odd}|$

$\therefore |C_{even}| = |C_{odd}|$ #

3.6 Consider an (n, k) linear code C whose generator matrix $\mathbf{G}$ contains no zero column. Arrange all the codewords of C as rows of a 2^k-by-n array.

a. Show that no column of the array contains only zeros.

b. Show that each column of the array consists of 2^{k-1} zeros and 2^{k-1} ones.

c. Show that the set of all codewords with zeros in a particular component position forms a subspace of C. What is the dimension of this subspace?

a. Since the k rows in G are all codewords.
No column of the array contains only zeros.
Otherwise, if the column j $(1 \leq j \leq n)$ contains only zeros,
Column j of G are all zeros $\rightarrow\leftarrow$.

b. For any column l, Let S_0 be the set
of code word that has '0' in the l^{th} column;
S_1 be the set of codeword that has '1' in l^{th} position.

Take any $\underline{x}$ in S_1, then $\forall\, \underline{v} \in S_0$

$\underline{v} + \underline{x} \in S_1 \Rightarrow |S_0| \le |S_1|$

Similarly, $\forall\, \underline{u} \in S_1$; $\underline{u} + \underline{x} \in S_0 \Rightarrow |S_1| \le |S_0|$

Therefore, $|S_0| = |S_1|$, that is number of '1' & '0' in the l^{th} column are both 2^{k-1} #

C. Following the S_0 definition in b.

We have $\forall\, \underline{u}, \underline{v} \in S_0$, $\underline{u} + \underline{v} \in S_0$

$\therefore$ S_0 is a subspace of S (the codeword array) with dimension $(k-1)$ #

3.14 Show that the (8, 4) linear code C given in Problem 3.1 is self-dual.

$$v_0 = u_1 + u_2 + u_3,$$

$$v_1 = u_0 + u_1 + u_2,$$

$$v_2 = u_0 + u_1 + u_3,$$

$$v_3 = u_0 + u_2 + u_3.$$

We first form its generating matrix G,

$$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [P|I]$$

where $P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ and I is the identity matrix

The generating matrix of dual code C_d is the parity check matrix H

We know that $H = [I \mid P^T]$

We will then prove that G & H has the same column space.

$\because$ P is full rank $\therefore$ $col(H) = col(PH)$

$= col([P \mid PP^T]) = col([P \mid I]) = col(G)$

That is the code C is self-dual #

3.15 For any binary (n, k) linear code with minimum distance (or minimum weight) $2t+1$ or greater, show that the number of parity-check digits satisfies the following inequality:

$$n - k \geq \log_2 \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right].$$

The preceding inequality gives an upper bound on the random-error-correcting capability t of an (n, k) linear code. This bound is known as the *Hamming bound* [14]. (*Hint:* For an (n, k) linear code with minimum distance $2t + 1$ or greater, all the n-tuples of weight t or less can be used as coset leaders in a standard array.)

From the hint, we have

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t} \leq 2^{n-k}$$

$$\Rightarrow \quad n-k \geq \log_2 \left(1 + \binom{n}{1} + \cdots + \binom{n}{t} \right) \#$$

3.16 Show that the minimum distance d_{min} of an (n, k) linear code satisfies the following inequality:

$$d_{min} \leq \frac{n \cdot 2^{k-1}}{2^k - 1}.$$

(*Hint:* Use the result of Problem 3.6(b). This bound is known as the *Plotkin bound* [1-3].)

From 3.6(b), there are 2^{k-1} '1's in each column. Therefore, total number of '1's in the code array is $n \cdot 2^{k-1}$

There are $2^k - 1$ non-zero codewords, $\therefore$

$$n 2^{k-1} \geq d_{min}(2^k - 1) \Rightarrow d_{min} \leq \frac{n 2^{k-1}}{2^k - 1} \#$$

4.9 Prove that the $(m-r-1)$th-order RM code, $\mathrm{RM}(m-r-1, m)$, is the dual code of the rth-order RM code, $\mathrm{RM}(r, m)$.

For any code $u \in RM(r,m)$ & $v \in RM(m-r-1,m)$

It is clear that $\underset{\text{element-wise product}}{u \odot v} \in RM(m-1,m)$

Also, the weight in $RM(m-1,m)$ are all even.

This implies $u \cdot v = 0$

Moreover, $RM(r,m)$ has $\binom{m}{0} + \cdots \binom{m}{r}$ codes,

and $RM(m-r-1,m)$ has $\binom{m}{0} + \cdots + \binom{m}{m-r-1}$

$$\Rightarrow \binom{m}{0} + \cdots + \binom{m}{r} + \binom{m}{0} + \cdots \binom{m}{m-r-1}$$

$$= \binom{m}{0} + \cdots + \binom{m}{r} + \binom{m}{m} + \cdots + \binom{m}{r+1} = 2^m$$

$\therefore$ $RM(m-r-1,m)$ is dual code of $RM(m,r)$ #

4.11 Find a parity-check matrix for the RM(1, 4) code.

From 4.9, Dual code of $RM(1,4)$ is $RM(2,4)$

Generating matrix of $RM(2,4)$ is:

$$\begin{array}{cc}
\left[\begin{array}{cccc}
1111 & 1111 & 1111 & 1111 \\
0000 & 0000 & 1111 & 1111 \\
0000 & 1111 & 0000 & 1111 \\
0011 & 0011 & 0011 & 0011 \\
0101 & 0101 & 0101 & 0101 \\
0000 & 0000 & 0000 & 1111 \\
0000 & 0000 & 0011 & 0011 \\
0000 & 0000 & 0101 & 0101 \\
0000 & 0011 & 0000 & 0011 \\
0000 & 0101 & 0000 & 0101 \\
0001 & 0001 & 0001 & 0001
\end{array}\right]
&
\begin{array}{l}
\bar{v}_0 \\
\bar{v}_1 \\
\bar{v}_2 \\
\bar{v}_3 \\
\bar{v}_4 \\
\bar{v}_3 \bar{v}_4 \\
\bar{v}_2 \bar{v}_4 \\
\bar{v}_1 \bar{v}_4 \\
\bar{v}_2 \bar{v}_3 \\
\bar{v}_1 \bar{v}_3 \\
\bar{v}_1 \bar{v}_2
\end{array}
\end{array}$$

which is the parity check matrix of RM(1,4) #

Q.8 Find a parity check matrix for the RM(2,4) code.

Similar to 4.11, Dual code of RM(2,4) is RM(1,4)

Generating matrix of RM(1,4) is:

$$\begin{array}{cc} \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 0000 & 0000 & 1111 & 1111 \\ 0000 & 1111 & 0000 & 1111 \\ 0011 & 0011 & 0011 & 0011 \\ 0101 & 0101 & 0101 & 0101 \end{bmatrix} & \begin{array}{c} v_0 \\ \bar{v}_1 \\ \bar{v}_2 \\ \bar{v}_3 \\ \bar{v}_4 \end{array} \end{array}$$

which is the parity check matrix of RM(1,4) #