***Case B:* $a=0,\ 2a+b\neq 0$ *so that* $b\neq 0$**
Then the word becomes

$$0,\quad b,\quad 2b+c,\quad -b+2c+d,\quad b-c+2d+e,\quad -b+c-d+2e+1,$$
$$-b+c+d-e+2,\quad -c+d+e-1,\quad -d+e+1,\quad -e+1,\quad -1$$

Case B(i): $2b+c=0$ *so that* $c=-2b$
Then the word is

$$0,\quad b,\quad 0,\quad d,\quad 3b+2d+e,\quad 3b-d+2e+1,\quad 3b+d-e+2,$$
$$2b+d+e-1,\quad -d+e+1,\quad -e+1,\quad -1$$

If $d=0$, the word is

$$0,\quad b,\quad 0,\quad 0,\quad 3b+e,\quad 3b+2e+1,\quad 3b-e+2,\quad 2b+e-1,$$
$$e+1,\quad -e+1,\quad -1$$

If $3b+e=0$ so that $e=2b$, the word becomes

$$0,\quad b,\quad 0,\quad 0,\quad 0,\quad 2b+1,\quad b+2,\quad 4b-1,\quad 2b+1,\quad -2b+1,\quad -1$$

which is of weight at least 5.
A similar argument also shows that the word is of weight at least 5 in the cases:

(a) $d\neq 0, 3b+2d+e=0$ and
(b) $d\neq 0, 3b+2d+e\neq 0$ but $3b-d+2e+1=0$.

Case B(ii): $2b+c\neq 0$ *but* $-b+2c+d=0$
Then $b=2c+d$. The word then is

$$0,\quad b,\quad 2b+c,\quad 0,\quad c+3d+e,\quad -c-2d+2e+1,\quad -3c-e+2,$$
$$-c+d+e-1,\quad -d+e+1,\quad -e+1,\quad -1$$

Here b, $2b+c$ and -1 are three non-zero entries and by considering the cases

(a) $c+3d+e=0$
(b) $c+3d+e\neq 0$ but $-c-2d+2e+1=0$,

we can prove that there are at least two non-zero entries among the rest of the entries.

***Case C:* $a\neq 0,\ 2a+b=0$**
Then the word is

$$a,\quad 0,\quad c,\quad 3a+2c+d,\quad -a-c+2d+e,\quad a+c-d+2e+1,$$
$$2a+c+d-e+2,\quad -c+d+e-1,\quad -d+e+1,\quad -e+1,\quad -1$$

Again considering the subcases

(i) $c=0$
(ii) $c \neq 0$ but $3a+2c+d=0$ and
(iii) $c \neq 0$, $3a+2c+d \neq 0$ but $-a-c+2d+e=0$

we can prove that the word is of weight at least 5.

In the remaining two cases:

Case D: $a \neq 0$, $2c+b \neq 0$ but $-a+2b+c=0$
Case E: $a \neq 0$, $2a+b \neq 0$, $-a+2b+c \neq 0$ but $a-b+2c+d=0$

also we can prove similarly that there is no word of weight 4 in this code.

Hence the minimum distance of the code is 5.

Exercise 8.1

1. Prove that 2 is a quadratic residue modulo *a* prime p iff $p \equiv \pm 1 (\mathrm{mod}\, 8)$.
2. Determine all primes p for which 5 is a quadratic residue mod p.
3. Let p be a prime congruent to $\pm 1 (\mathrm{mod}\, 8)$. Then there exists a primitive pth root α of unity in some extension field of $\mathbb{B}$ such that $E_q(\alpha)=1$, where

$$E_q(x) = \sum_{r \in Q} x^r$$

4. Prove Theorems 8.10, 8.12 and 8.14.
5. Determine, if possible, weight distributions of some of the codes constructed.

9

Maximum distance separable codes

9.1 NECESSARY AND SUFFICIENT CONDITIONS FOR MDS CODES

In this chapter, we study an interesting class of linear codes – interesting because these codes have the maximum possible error detection/correction possibility. Another point of interest is a question of existence of such codes which translates into a question purely on vector spaces.

We have seen earlier that if $\mathscr{C}$ is a linear $[n, k, d]$ code over a field F, then $d \leq n - k + 1$.

Definition 9.1
A linear $[n, k, d]$ code over F with $d = n - k + 1$ is called a **maximum distance separable (MDS) code**.

In this chapter, unless explicitly stated to the contrary, we do not insist that the first k columns of a generator matrix of a linear $[n, k, d]$ form the identity matrix or that the last $n - k$ columns of a parity check matrix form the identity matrix.

We begin our study with the following simple observation.

Proposition 9.1
Let $\mathscr{C}$ be a linear $[n, k, d]$ code over a field F of q elements, q a prime power with a parity check matrix $\mathbf{H}$. Then $\mathscr{C}$ has a code word of eight $\leq l$ iff l columns of $\mathbf{H}$ are linearly dependent.

Proof
Let $b = b_1 b_2 \cdots b_n$ be a code word in $\mathscr{C}$ with $\text{wt}(b) = l$. Let $b_{i_1}, \ldots, b_{i_l}$ be the non-zero entries of b. Then

$$\mathbf{H}\mathbf{b}^t = \mathbf{0} \Rightarrow b_{i_1}\mathbf{H}_{i_1} + \cdots + b_{i_l}\mathbf{H}_{i_l} = 0$$

where $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_n$ denote the columns of **H**. Thus, l columns

$$\mathbf{H}_{i_1}, \ldots, \mathbf{H}_{i_l}$$

of **H** are linearly dependent.

Conversely, suppose that l columns of **H**, say

$$\mathbf{H}_{i_1}, \ldots, \mathbf{H}_{i_l}$$

are linearly dependent. Then there exist scalars

$$b_{i_1}, \ldots, b_{i_l}$$

not all zero such that

$$b_{i_1}\mathbf{H}_{i_1} + \cdots + b_{i_l}\mathbf{H}_{i_l} = 0$$

Take $c = c_1 \text{---} c_n$ with

$$c_{i_j} = b_{i_j},\ 1 \leq j \leq l \quad \text{and} \quad c_i = 0 \text{ for every other } i$$

Then c is a word of weight at most l and $\mathbf{H}\mathbf{c}^t = 0$. Thus c is a code word of weight at most l.

Theorem 9.1

Let $\mathscr{C}$ be a linear $[n, k, d]$ code over F with a parity check matrix **H**. Then $\mathscr{C}$ is an MDS code iff every $n - k$ columns of **H** are linearly independent.

Proof

Suppose that $\mathscr{C}$ is an MDS code. Then $d = n - k + 1$ and so there is no non-zero code word of weight at most $n - k$. It follows from Proposition 9.1 that every $n - k$ columns of **H** are linearly independent.

Conversely, suppose that every $n - k$ columns of **H** are linearly independent. Then there is no non-zero code word of weight at most $n - k$. Therefore

$$d \geq n - k + 1$$

But

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

always and, so

$$d = n - k + 1$$

Hence $\mathscr{C}$ is an MDS code.

Theorem 9.2

If a linear $[n, k, d]$ code $\mathscr{C}$ is MDS, then so is its dual $\mathscr{C}^\perp$.

Proof

As already seen $\mathscr{C}^\perp$ is a linear $[n, n - k, -]$ code. Let d_1 be the minimum distance of $\mathscr{C}^\perp$. Then

$$d_1 \leq n - (n - k) + 1 = k + 1$$

Let $\mathbf{H}$ be a parity check matrix of $\mathscr{C}$. The code $\mathscr{C}$ being MDS, every $n-k$ columns of $\mathbf{H}$ are linearly independent. Therefore, if any k columns of $\mathbf{H}$ are omitted, the remaining columns in that order (being linearly independent) form a square submatrix of $\mathbf{H}$ of rank $n-k$. Let a be a word of length $n-k$ and suppose that the code word $\mathbf{aH}$ of $\mathscr{C}^{\perp}$ has at least $n-k$ zeros. Let $\bar{\mathbf{H}}$ be the submatrix of $\mathbf{H}$ obtained by omitting k columns including those which correspond to the possible k non-zero entries of $\mathbf{aH}$. Then $\mathbf{a}\bar{\mathbf{H}}=\mathbf{0}$. As $\bar{\mathbf{H}}$ is a square matrix of order $n-k$ with rank $n-k$, $\bar{\mathbf{H}}$ is non-singular. It then follows from $\mathbf{a}\bar{\mathbf{H}}=\mathbf{0}$ that $\mathbf{a}=\mathbf{0}$ and, hence, $\mathbf{aH}=\mathbf{0}$. This proves that

$$d_1 \geq k+1$$

and, so

$$d_1 = k+1$$

Hence $\mathscr{C}^{\perp}$ is an MDS code.

Corollary

Let $\mathscr{C}$ be an $[n,k,d]$ linear code over $F=\mathrm{GF}(q)$. Then the following statements are equivalent:

(i) $\mathscr{C}$ is MDS.
(ii) Every k columns of a generator matrix $\mathbf{G}$ of $\mathscr{C}$ are linearly independent.
(iii) Every $n-k$ columns of a parity check matrix $\mathbf{H}$ of $\mathscr{C}$ are linearly independent.

Proof

Equivalence of (i) and (iii) has been proved in Theorem 9.1.

Let $\mathbf{G}$ be a generator matrix of $\mathscr{C}$. By Theorem 5.2 $\mathbf{G}$ is a parity check matrix of $\mathscr{C}^{\perp}$ which is an $[n, n-k, -]$ linear code. Therefore, by Theorem 9.1, $\mathscr{C}^{\perp}$ is an MDS code iff every k columns of $\mathbf{G}$ are linearly independent. As

$$(\mathscr{C}^{\perp})^{\perp}=\mathscr{C}$$

it follows from the above theorem that $\mathscr{C}$ is MDS iff $\mathscr{C}^{\perp}$ is MDS. Hence $\mathscr{C}$ is MDS iff every k columns of $\mathbf{G}$ are linearly independent.

Examples 9.1

Case (i)

Let F be a field of q elements, q a prime power and e be the word with every entry equal to 1. Let $\mathscr{C}$ be the linear space over F generated by e. Then every non-zero element of $\mathscr{C}$ has weight n. Thus $\mathscr{C}$ is a linear code of dimension 1 and minimum distance $n=n-1+1$. Hence, $\mathscr{C}$ is an $[n,1,n]$ MDS code.