Case (ii)
Let F be any finite field and for i, $1 \leq i \leq n$, let e^i be the word of length n with 1 in the ith position and 0 everywhere else. Let $\mathscr{C}$ be the vector space over F generated by e^i, $1 \leq i \leq n$. Obviously the minimum distance of this code is 1. Also its dimension is n. Hence $\mathscr{C}$ is an $[n, n, 1]$ MDS code.

Case (iii)
Let F be any finite field and for any i, $1 \leq i \leq n-1$, let e^i be the word of length n with 1 in the ith and $(i+1)$th position and 0 everywhere else. These $n-1$ words are linearly independent over F and so generate a linear code $\mathscr{C}$ of dimension $n-1$. Clearly the minimum distance of this code is

$$2 = n - (n-1) + 1$$

Hence $\mathscr{C}$ is an $[n, n-1, 2]$ linear MDS code over F.

Case (iv)
For i, $1 \leq i \leq n-2$, let e^i be the binary word of length n with ith, $(i+1)$th and $(i+2)$th entry equal to 1 and every other entry equal to 0. These vectors are linearly independent and so generate a linear code of dimension $n-2$. Observe that $e^1 + e^2$ is a word of weight 2 and the minimum distance of this code is

$$2 < n - (n-2) + 1 = 3$$

This linear $[n, n-2, 2]$ code over any finite field F is not an MDS code.

Case (v)
The $[7, 4, 3]$ binary Hamming code is not MDS and then its dual also cannot be an MDS code.

Case (vi)
Let $F = \mathrm{GF}(3)$ – the field of three elements – and $\mathscr{C}$ be the code of length 3 generated by the matrix

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

It is a code of length 3 and dimension 2. Every two columns of the matrix $\mathbf{G}$ are linearly independent and, therefore, the code is MDS. Explicitly, all the code words of this code are:

$$0\ 0\ 0,\quad 1\ 0\ 1,\quad 0\ 1\ -1,\quad -1\ 0\ -1,\quad 0\ -1\ 1,\quad 1\ 1\ 0,\quad -1\ 1\ 1,$$
$$1\ -1\ -1,\quad -1\ -1\ 0$$

and the minimum distance is $2 = 3 - 2 + 1$.

The dual of this code is generated by

$$\mathbf{H} = (1 \quad -1 \quad 1)$$

and is of dimension 1. This minimum distance of this code is 3 as all the code words of this code are:

$$0\ 0\ 0,\quad 1\ -1\ 1,\quad -1\ 1\ -1$$

Exercise 9.1

1. Let α be a primitive cube root of unity and

$$F = \{0, 1, \alpha, \alpha^2\}$$

the field of 4 elements. Prove that the code $\mathscr{C}$ generated by the matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}$$

is an MDS code. Also find its dual and verify that $\mathscr{C}^{\perp}$ is also MDS.
Find the weight enumerator of $\mathscr{C}$ as well as $\mathscr{C}^{\perp}$.

2. Let

$$F = \{0, 1, -1\}$$

be the field of 3 elements and $\mathscr{C}$ be the code generated by

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

Is the code $\mathscr{C}$ MDS? Find $\mathscr{C}^{\perp}$ also.

3. Find the duals of the codes of Cases (i) – (iii) of Examples 9.1.

Definition 9.2
We have shown that linear $[n, 1, n]$, $[n, n-1, 2]$ and $[n, n, 1]$ codes exist over any finite field F and these are MDS codes. These are called **trivial MDS codes**.

Proposition 9.2
The only binary MDS codes are the trivial codes.

Proof
Let $\mathscr{C}$ be a binary $[n, k, d]$ MDS code. If $k = 1$, then $\mathscr{C}$ is a trivial MDS code and so we may suppose that $k > 1$. Let $\mathbf{G}$ be a generator matrix of $\mathscr{C}$ with the first k columns of $\mathbf{G}$ forming the identity matrix. If $n > k + 1$, then $\mathscr{C}$ has a column, say jth, of weight less than k and greater than 1. Suppose that the ith entry of this column is 0. Then the first k columns of $\mathbf{G}$ except the ith together with the jth column are linearly dependent. This proves that $\mathscr{C}$ cannot be an MDS code. Hence

$$k \leq n \leq k + 1$$

and $\mathscr{C}$ is a trivial MDS code. ■

We shall come to a similar property of MDS codes when we discuss the existence of MDS codes.

Using Theorem 9.1, we now prove another useful criterion for MDS codes.

Theorem 9.3
Let $\mathscr{C}$ be an $[n, k, -]$ code with parity check matrix

$$\mathbf{H} = (\mathbf{A} \quad \mathbf{I}_{n-k})$$

Then $\mathscr{C}$ is an MDS code iff every square submatrix of $\mathbf{A}$ is non-singular.

Proof
Let $\mathbf{B}_r$ be a square submatrix of $\mathbf{A}$ constituted by parts of the i_1th, i_2th, ..., i_rth rows of $\mathbf{A}$ with

$$i_1 < i_2 < \cdots < i_r (\leq n-k)$$

Let $\mathbf{M}_r$ be the square submatrix of $\mathbf{H}$ of order $n-k$ constituted by the columns of $\mathbf{A}$ parts of which occur in $\mathbf{B}_r$ and the remaining $n-k-r$ columns from the identity matrix $\mathbf{I}_{n-k}$ which are different from i_1th, i_2th, ..., i_rth columns of $\mathbf{I}_{n-k}$. Then

$$\det \mathbf{M}_r = \pm \det \mathbf{B}_r$$

so that $\mathbf{B}_r$ is non-singular iff $\mathbf{M}_r$ is. Therefore, every $n-k$ columns of $\mathbf{H}$ are linearly independent iff every square submatrix of $\mathbf{A}$ is non-singular. The result then follows from Theorem 9.1. ■

The above theorem can equally well be stated in terms of generator matrix.

Theorem 9.4
Let $\mathscr{C}$ be an $[n, k, -]$ code with generator matrix

$$\mathbf{G} = (\mathbf{I}_k \quad \mathbf{A})$$

Then $\mathscr{C}$ is an MDS code iff every square submatrix of $\mathbf{A}$ is non-singular.

Examples 9.2

Case (i)
Consider the matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 6 & 2 & 5 & 1 \\ 1 & 4 & 3 & 3 & 6 \\ 1 & 5 & 5 & 1 & 5 \end{pmatrix}$$

over GF(7). It is clear that every square submatrix of order 2 is non-singular.

There are ${}^5C_3 = 10$ square submatrices of order 3:

$$\det\begin{pmatrix}1&6&2\\1&4&3\\1&5&5\end{pmatrix}=2 \qquad \det\begin{pmatrix}1&6&5\\1&4&3\\1&5&1\end{pmatrix}=6 \qquad \det\begin{pmatrix}1&6&1\\1&4&6\\1&5&5\end{pmatrix}=4$$

$$\det\begin{pmatrix}1&2&5\\1&3&3\\1&5&1\end{pmatrix}=2 \qquad \det\begin{pmatrix}1&2&1\\1&3&6\\1&5&5\end{pmatrix}=3 \qquad \det\begin{pmatrix}1&5&1\\1&3&6\\1&1&5\end{pmatrix}=5$$

$$\det\begin{pmatrix}6&2&5\\4&3&3\\5&5&1\end{pmatrix}=3 \qquad \det\begin{pmatrix}6&2&1\\4&3&6\\5&5&5\end{pmatrix}=5 \qquad \det\begin{pmatrix}6&5&1\\4&3&6\\5&1&5\end{pmatrix}=2$$

$$\det\begin{pmatrix}2&5&1\\3&3&6\\5&1&5\end{pmatrix}=4$$

Thus every square submatrix of $\mathbf{A}$ is non-singular and $\mathbf{A}$ can be used to obtain two MDS codes:

(a) The $[8,3,-]$ code over GF(7) with generator matrix $\mathbf{G} = (\mathbf{I}_3 \quad \mathbf{A})$ is an MDS code.
(b) The $[8,5,-]$ code over GF(7) with parity check matrix $\mathbf{H} = (\mathbf{A} \quad \mathbf{I}_3)$ is an MDS code.

Case (ii)
Consider the matrix

$$\mathbf{A} = \begin{pmatrix}1&2&3&4\\1&3&1&2\end{pmatrix}$$

over GF(5). It is clear that every square submatrix of $\mathbf{A}$ is non-singular and, so, this matrix gives two MDS codes:

(a) The code with generator matrix $\mathbf{G} = (\mathbf{I}_2 \quad \mathbf{A})$ is a $[6,2,-]$ MDS code over GF(5).
(b) The code with parity check matrix $\mathbf{H} = (\mathbf{A} \quad \mathbf{I}_2)$ is a $[6,4,-]$ MDS code over GF(5).

Exercise 9.2

1. Does there exist a ternary MDS code of length $n \geq 5$ and dimension 2?
2. Construct a ternary MDS code of length 4 and dimension 2.
3. Does there exist a ternary MDS code of dimension 3 and length (i) 5? (ii) 6?
4. Does there exist an MDS code over GF(5) of length $n \geq 7$ and dimension 2?
5. Construct all possible MDS codes over GF(5) of dimension 2 and length (i) 4; (ii) 5; (iii) 6.

6. Give reasonable necessary and sufficient conditions for a polynomial code over GF(q) with generator polynomial $g(X)$ to be MDS.
7. Give reasonable necessary and sufficient conditions for a cyclic code of length n over GF(q), g.c.d.$(n, q) = 1$ to be MDS.

9.2 THE WEIGHT DISTRIBUTION OF MDS CODES

Proposition 9.3
Let $\mathscr{C}$ be an $[n, k, d]$ MDS code. Then any k symbols of the code words may be taken as message symbols.

Proof
Let $i_1, i_2, \ldots, i_k$ be the chosen k positions. Let $\mathbf{G}$ be a generator matrix of $\mathscr{C}$. Then $\mathbf{G}$ is a $k \times n$ matrix, every k columns of which are linearly independent. Take

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

where $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_n$ are the columns of $\mathbf{G}$. Then $\bar{\mathbf{G}}$ is an invertible matrix and so

$$\mathbf{G}' = \bar{\mathbf{G}}^{-1}\mathbf{G}$$

is also a generator matrix of $\mathscr{C}$. Given a message word $a = a_1, a_1 \text{---} a_k$, let

$$\mathbf{a}' = \mathbf{a}\bar{\mathbf{G}}^{-1}$$

Then

$$\mathbf{a} = \mathbf{a}'\bar{\mathbf{G}} = (\mathbf{a}'\mathbf{G}_{i_1} \quad \cdots \quad \mathbf{a}'\mathbf{G}_{i_k})$$

Now the code word in the code $\mathscr{C}$ corresponding to the message word a (and its associated vector $\mathbf{a}$) is

$$\mathbf{a}\mathbf{G}' = \mathbf{a}\bar{\mathbf{G}}^{-1}\mathbf{G} = \mathbf{a}'\mathbf{G} = (\cdots \quad a'\mathbf{G}_{i_1} \quad \cdots \quad a'\mathbf{G}_{i_k} \quad \cdots)$$

in which the entries in the i_1th, i_2th, $\ldots$, i_kth positions are $a_1, a_2, \ldots, a_k$ respectively.

Theorem 9.5
Let $\mathscr{C}$ be an $[n, k, d]$ code over GF(q). Then $\mathscr{C}$ is an MDS code iff $\mathscr{C}$ has a minimum distance code word with non-zero entries in any d coordinates.

Proof
Let $\mathscr{C}$ be an MDS code. By the above proposition, any k coordinates can be taken as positions of the message symbols. Let $d = n - k + 1$ coordinate positions be given. Take one of these, say ith, and the complementary $k - 1$ coordinates as message symbols. Consider the message word which has 1 in

the position corresponding to the ith position in code words and 0 elsewhere in the remaining $k-1$ positions. The code word corresponding to this message word has a non-zero entry in one of the chosen d positions (the ith position) and 0 in every one of the $k-1$ complementary positions. The weight of this code word being $n-k+1$, each one of the remaining $n-k$ chosen positions must be occupied by a non-zero entry.

Conversely, suppose that $\mathscr{C}$ has a code word of weight d in any d coordinate positions. If $d = n-k+1$, we have nothing to prove. Suppose that $d \leq n-k$.

Let $\mathbf{G}$ be a generator matrix of $\mathscr{C}$. Then $\mathbf{G}$ is a $k \times n$ matrix of rank k. Therefore $\mathbf{G}$ has a set of k linearly independent columns. For the sake of simplicity (of notation), let us assume that the first k columns of $\mathbf{G}$ are linearly independent. Let $\bar{\mathbf{G}}$ be the submatrix of $\mathbf{G}$ formed by the first k columns of $\mathbf{G}$. Set

$$\mathbf{G}' = \bar{\mathbf{G}}^{-1}\mathbf{G}$$

Then $\mathbf{G}'$ is also a generator matrix of $\mathscr{C}$ and the first k columns of $\mathbf{G}'$ form the identity matrix of order k. Let $\mathbf{b} = \mathbf{a}\mathbf{G}'$ be the vector associated with a code word of weight d with the non-zero entries in the last d coordinate positions. If

$$b = b_1 b_2 \cdots b_n \quad \text{and} \quad a = a_1 \cdots a_k$$

then $b_i = a_i$ for $1 \leq i \leq k$ and $b_i = 0$ for $1 \leq i \leq n-d$. Since $d \leq n-k$, $k \leq n-d$ and, therefore, $a_i = b_i = 0$ for $1 \leq i \leq k$, i.e. $a = 0$. But then $\mathbf{b} = \mathbf{a}\mathbf{G}' = \mathbf{0} - \mathbf{a}$ contradiction. Hence $d = n-k+1$ and $\mathscr{C}$ is an MDS code.

Corollary
The number of code words of weight $n-k+1$ in an $[n, k, d]$ MDS code over GF(q) is

$$(q-1)\binom{n}{n-k+1}$$

Proof
Let $n-k+1$ coordinate positions be given and let

$$b = b_1 b_2 \cdots b_n$$

be a code word of weight $n-k+1$ with non-zero entries at the given coordinate positions. Since every non-zero multiple of b gives a new code word of weight $n-k+1$ with non-zero entries at the given positions, we obtain $(q-1)$ code words with this property. Let

$$c = c_1 c_2 \cdots c_n$$

be a code word of weight $n-k+1$ with non-zero entries at the given positions. If

$$c \notin \{\alpha b \mid \alpha \in \mathrm{GF}(q),\ \alpha \neq 0\}$$