then there exists an $i$, $1 \leq i \leq n$, such that

$$0 \neq c_i \notin \{\alpha b_i | \alpha \in \mathrm{GF}(q), \alpha \neq 0\}$$

But then

$$0(\{c_i\} u \{\alpha b_i | \alpha \in \mathrm{GF}(q), \alpha \neq 0\}) = q$$

and every element of the set is non-zero – a contradiction. Hence $c$ is a scalar multiple of $b$. Thus, given any $n-k+1$ positions, there are exactly $q-1$ code words with non-zero entries at these positions. Since $n-k+1$ positions can be chosen out of the $n$ positions in

$$\binom{n}{n-k+1} \text{ ways}$$

the total number of code words of weight $n-k+1$ is

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

**Examples 9.3**

***Case (i)***

In the code of Case (vi) in Examples 9.1, there are 6 code words of weight 2, 2 code words of weight 3 and 1 code word of weight 0. Therefore

$$W_{\mathscr{C}}(x, y) = x^3 + 6xy^2 + 2y^3$$

also

$$W_{\mathscr{C}^\perp} = x^3 + 2y^3$$

***Case (ii)***

Let $\mathscr{C}$ be the $[4, 2, -]$ code of question 2 in Exercise 9.1. Also, the code words of $\mathscr{C}$ are:

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

Therefore

$$W_{\mathscr{C}} = x^4 + 8xy^3$$

Observe that

$$8 = (3-1)\binom{4}{4-2+1}$$

The dual $\mathscr{C}^\perp$ is generated by the matrix

$$\begin{pmatrix} -1 & 1 & 1 & 0 \\ -1 & -1 & 0 & 1 \end{pmatrix}$$

and all the code words of $\mathscr{C}^{\perp}$ are

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

and

$$W_{\mathscr{C}^{\perp}} = x^4 + 8xy^3$$

Observe that $\mathscr{C}^{\perp} = \mathscr{C}$ and so this code is self dual.

**Exercise 9.3**

Find the number of minimum distance code words in the codes of question 1 in Exercise 9.1, and Case (iv) of Examples 9.1. Find also the weight enumerators of these codes.

## 9.3 AN EXISTENCE PROBLEM

In this section we throw some light on the following problems.

**Problem 9.1**
Given $k$ and $q$, find the largest value of $n$ for which an $[n, k, n-k+1]$ MDS code exists over GF($q$). We denote this largest value of $n$ by $m(k, q)$. When $q = 2$ and $k \neq 1$, it follows from Proposition 9.2 that

$$m(k, 2) = k + 1 \quad \text{or} \quad m(k, 2) = k$$

We shall obtain here a general theorem of which this is a particular case. But we first translate this problem into one of linear algebra.

In view of the corollary to Theorem 9.2, it follows that this problem is equivalent to the following.

**Problem 9.2**
Given $k$ and $q$, find the largest $n$ for which there is a $k \times n$ matrix over GF($q$), every $k$ columns of which are linearly independent.

Given a $k \times n$ matrix $\mathbf{G}$ over GF($q$) every $k$ columns of which are linearly independent, let $V$ be a vector space generated by some $k$ columns of $\mathbf{G}$. The vector space $V$ then has a set of $n$ vectors (i.e. the set of all columns of $\mathbf{G}$) such that every $k$ vectors of these are linearly independent. On the other hand, if $V$ is a $k$-dimensional vector space having a set of $n$ vectors, every $k$ elements of which are linearly independent, regarding these $n$ vectors as columns of length $k$, we obtain a $k \times n$ matrix $\mathbf{G}$ over GF($q$) such that every $k$ columns of $\mathbf{G}$ are linearly independent. In view of this, Problem 9.2 translates into the following.

**Problem 9.3**
Given a $k$-dimensional vector space $V$ over GF($q$), what is the order of a largest subset of $V$ with the property that every $k$ of these vectors form a basis of $V$?

It has been conjectured that

$$m(k,q) = \begin{cases} q+1 & \text{for } 2 \le k \le q-1 \\ k+1 & \text{for } q \le k \end{cases}$$

except that

$$m(3,q) = m(q-1,q) = q+2 \quad \text{if } q = 2^m$$

**Theorem 9.6**

$$m(2,q) = q+1$$

for any prime power $q$.

***Proof***

Let $V$ be a 2-dimensional vector space over GF($q$) and let $\alpha$ be a primitive element of GF($q$). Let $S$ be a largest subset of $V$ with the property that every two elements of $S$ are linearly independent over GF($q$). The set $S$ contains at least two elements, say $\mathbf{e}_1$ and $\mathbf{e}_2$. Every other element of $S$ is then of the form

$$\alpha^i \mathbf{e}_1 + \alpha^j \mathbf{e}_2$$

for suitable non-negative integers $i, j$. Given $i$, $0 \le i \le q-2$, let

$$S_i = \{\beta(\mathbf{e}_1 + \alpha^i \mathbf{e}_2) | 0 \ne \beta \in \mathrm{GF}(q)\}$$

Any two elements of $S_i$ are linearly dependent, and at the most one element from each $S_i$, $0 \le i \le q-2$, belongs to $S$. Also no element from an $S_i$ is a scalar multiple of any element from $S_j$ for $j \ne i$. Hence, at least one element from each $S_i$, $0 \le i \le q-2$, belongs to $S$, for otherwise the set $S$ can be enlarged without upsetting the linear independence of any two elements. Thus $S$ contains $q+1$ elements and

$$m(2,q) = q+1$$

**Theorem 9.7**

$$m(k,q) = k+1 \quad \text{for } q \le k$$

***Proof***

Let $V$ be a $k$-dimensional vector space over GF($q$). Let $S$ be a largest subset of $V$ with the property that any $k$ vectors from the set $S$ are linearly independent. Choose any $k$ vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_k$ from the set $S$. Every other element of $S$ is then of the form

$$\sum_{1 \le i \le k} a_i \mathbf{e}_i$$

where $a_i$ belong to the multiplicative group GF($q$)* of GF($q$). Suppose two

elements of this form

$$\sum_{1 \le i \le k} a_i \mathbf{e}_i \quad \text{and} \quad \sum_{1 \le i \le k} b_i \mathbf{e}_i$$

where $a_i, b_j \in \mathrm{GF}(q)^*$ are in $S$.

Consider the $k$ equations

$$a_i x_i = b_i \quad 1 \le i \le k$$

Each of these $k$ equations has a unique solution in $\mathrm{GF}(q)^*$. Since the order of $\mathrm{GF}(q)^*$ is $q - 1 < k$, at least two of these equations have the same solution. Without loss of generality, we may assume that

$$a_1 x = b_1 \quad \text{and} \quad a_2 x = b_2$$

have the same solution, say $x$. Then the vector

$$x\left(\sum_{1 \le i \le k} a_i x_i\right) - \sum_{1 \le i \le k} b_i x_i$$

is a linear combination of the $k - 2$ vectors $\mathbf{e}_3, \ldots, \mathbf{e}_k$. The vectors

$$\mathbf{e}_3, \ldots, \mathbf{e}_k \quad \sum_{1 \le i \le k} a_i \mathbf{e}_i \quad \text{and} \quad \sum_{1 \le i \le k} b_i \mathbf{e}_i$$

are thus linearly dependent. This is a contradiction and hence $S$ can contain at the most one element of the form

$$\sum_{1 \le i \le k} a_i \mathbf{e}_i \quad a_i \in \mathrm{GF}(q)^*$$

Thus

$$m(k, q) \le k + 1$$

Moreover, $S$ must contain at least one element of the form

$$\sum_{1 \le i \le k} a_i \mathbf{e}_i \quad a_i \in \mathrm{GF}(q)^*$$

for otherwise $S$ can be enlarged to a set $S^*$ in which any $k$ vectors are linearly independent. Therefore

$$m(k, q) = k + 1$$

## 9.4 REED–SOLOMON CODES

A class of examples of MDS codes is provided by Reed–Solomon codes. Let $F = \mathrm{GF}(q)$ be a field of order $q$ where $q$ is a prime power. A Reed–Solomon code is a BCH code of length $n = q - 1$ over $F$.

Recall that, for the construction of a BCH code of length $n$ over $F$, we need to find a primitive element $\alpha$ in an extension field $K$ of $F$ with the degree $[K:F]$ equal to $r$, where $r$ is the least positive integer satisfying

$$q^r \geq n+1$$

Therefore, for a Reed–Solomon code $r=1$ and $\alpha$ is a primitive element of $F$ itself. Then $X-\alpha^i$ is the minimal polynomial of $\alpha^i$. Generator polynomial of the Reed–Solomon code $\mathscr{C}$ with minimum distance $d$ is given by

$$g(X)=(X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{d-1})$$

which is of degree $d-1$. Hence the dimension $k$ of $\mathscr{C}$ is

$$k=n-(d-1)=n-d+1 \quad \text{and} \quad d=n-k+1.$$

Therefore, we have the following theorem.

**Theorem 9.8**
A Reed–Solomon code is an MDS code.

**Examples 9.4**

***Case (i)***
Consider $F=\mathrm{GF}(7)$ in which 3 is a primitive element. The Reed–Solomon code with minimum distance $d=5$ has generator polynomial

$$\begin{aligned} g(X) &= (X-3)(X-2)(X-6)(X-4) \\ &= (X^2+2X+6)(X^2-3X+3) \\ &= X^4+6X^3+3X^2+2X+4 \end{aligned}$$

All the code words of this code are given by

$$\begin{aligned} &(aX+b)(X^4+6X^3+3X^2+2X+4) \\ &= aX^5+(6a+b)X^4+(3a+6b)X^3+(2a+3b)X^2+(4a+2b)X+4b \end{aligned}$$

where $a, b \in \mathrm{GF}(7)$.

***Case (ii)***
Consider again $F=\mathrm{GF}(7)$ in which 3 is a primitive element. The Reed–Solomon code with minimum distance $d=6$ has generator polynomial

$$\begin{aligned} g(X) &= (X-3)(X-2)(X-6)(X-4)(X-5) \\ &= X^5+X^4+X^3+X^2+X+1 \end{aligned}$$

and the code words are $aaaaaa$, where $a \in \mathrm{GF}(7)$.

***Case (iii)***

The polynomial $X^2 + X + 1$ is irreducible over $\mathbb{B}$ and so

$$F = \mathbb{B}[X]/\langle X^2 + X + 1 \rangle$$

is a field of 4 elements. If

$$\alpha = X + \langle X^2 + X + 1 \rangle$$

then $\alpha$ is a primitive element of $F$ and we can take

$$F = \{0, 1, \alpha, \alpha + 1\}$$

A generator polynomial of the Reed–Solomon code $\mathscr{C}$ of length 3 over $F$ and minimum distance $d = 2$ is

$$g(X) = X + \alpha$$

All the elements of $\mathscr{C}$ are

$$(aX + b)(X + \alpha) = aX^2 + (b + a\alpha)X + \alpha b$$

where $a, b \in F$ or

$$000 \quad \alpha 10 \quad \alpha^2\alpha 0 \quad 110 \quad 0\alpha 1 \quad \alpha\alpha^2 1 \quad \alpha^2 01 \quad 111 \quad 0\alpha^2\alpha \quad \alpha 1\alpha \quad \alpha^2 1\alpha$$

$$10\alpha \quad 01\alpha^2 \quad \alpha 0\alpha^2 \quad \alpha^2 1\alpha^2 \quad 1\alpha\alpha^2$$

(Remember! $\alpha^2 = \alpha + 1$.)

***Case (iv)***

Let $F = \mathrm{GF}(3) = \{0, 1, 2\}$. Then 2 is a primitive element of $F$ and a generator polynomial of the Reed–Solomon code with minimum distance 2 is

$$g(X) = X - 2 = X + 1$$

The code words of this code are given by $(aX + b)(X + 1)$, where $a, b \in F$ or

$$000 \quad 110 \quad 220 \quad 011 \quad 121 \quad 201 \quad 022 \quad 102 \quad 212$$