Lemma 6.1
If $a_1, a_2, \ldots, a_k$ are non-negative numbers with

$$a_1 + a_2 + \cdots + a_k = N$$

then

$$\sum_{i=1}^{k} a_i^2$$

is the least where

$$a_1 = a_2 = \cdots = a_k = N/k$$

Proof
We prove the lemma by induction on k. For $k = 2$,

$$\begin{aligned} a_1^2 + a_2^2 &= a_1^2 + (N - a_1)^2 \\ &= 2\left\{\frac{N^2}{4} + \left(a_1 - \frac{N}{2}\right)^2\right\} \end{aligned}$$

which is the least when $a_1 - N/2 = 0$, i.e. $a_1 = N/2$. But then $a_2 = N/2$ also. Suppose that the result holds for k numbers. Consider non-negative numbers $a_1, a_2, \ldots, a_{k+1}$ with

$$a_1 + a_2 + \cdots + a_{k+1} = N$$

Then

$$\sum_{i=1}^{k} a_i = N - a_{k+1}$$

Now

$$\begin{aligned} \sum_{i=1}^{k+1} a_i^2 &= \sum_{i=1}^{k} a_i^2 + a_{k+1}^2 \\ &\geq k\left(\frac{N - a_{k+1}}{k}\right)^2 + a_{k+1}^2 \qquad \text{(by induction hypothesis)} \\ &= \frac{1}{k}\{N^2 - 2Na_{k+1} + (k+1)a_{k+1}^2\} \\ &= \frac{k+1}{k}\left\{\frac{N^2}{k+1} + \left(a_{k+1} - \frac{N}{k+1}\right)^2 - \left(\frac{N}{k+1}\right)^2\right\} \end{aligned}$$

and this is the least when

$$a_{k+1} = \frac{N}{k+1}$$

Already for

$$\sum_{i=1}^{k} a_i^2$$

minimum, we have by the induction hypothesis that

$$a_1 = a_2 = \cdots = a_k = \frac{N - a_{k+1}}{k}$$

But

$$\frac{N - a_{k+1}}{k} = \frac{N - N/(k+1)}{k} = \frac{N}{k+1}$$

Therefore,

$$\sum_{i=1}^{k+1} a_i^2$$

is minimum only when

$$a_1 = a_2 = \cdots = a_{k+1} = N/(k+1)$$

Theorem 6.7 (Plotkin bound)
If $\mathscr{C}$ is a block code of length n, order N and minimum distance d over an alphabet set of order q, then

$$d \leq \frac{nN(q-1)}{(N-1)q}$$

Proof
Consider the number

$$A = \sum_{u,v \in \mathscr{C}} d(u,v)$$

where as usual $d(u,v)$ denotes the distance between u and v. If $u \neq v$, then $d(u,v) \geq d$ and is 0 otherwise. We can choose $u \neq v$ in $N(N-1)$ ways. Therefore $A \geq N(N-1)d$. We next obtain an upper bound for the number A. We consider the first entry of all the code words in $\mathscr{C}$. Write $0, 1, 2, \ldots, q-1$ as the elements of the set over which the code $\mathscr{C}$ is given. Among the first entries of all the code words of $\mathscr{C}$, let b_i be each equal to i, $0 \leq i \leq q-1$. Then

$$\sum_{i=0}^{q-1} b_i = N$$

If u, v are two words in $\mathscr{C}$ with the first entry i, then the first entries of u, v contribute 0 to the sum A. Consider now u with the first entry i. There are $N - b_i$ words in $\mathscr{C}$ with first entry $\neq i$. Therefore u with each of these $N - b_i$

words contributes $N - b_i$ to the sum A. There being b_i such code words the total contribution of the first entries of these words taken with the rest is $b_i(N - b_i)$. Considering all other j's, we find that the contribution to A because of the first entries of all words of $\mathscr{C}$ is B (say) where

$$B = \sum_{i=0}^{q-1} b_i(N - b_i)$$

Now

$$\begin{aligned} B &= \sum_{i=0}^{q-1} b_i(N - b_i) \\ &= N \sum_{i=0}^{q-1} b_i - \sum_{i=0}^{q-1} b_i^2 \\ &= N^2 - \sum_{i=0}^{q-1} b_i^2 \end{aligned}$$

B takes the largest value when

$$\sum_{i=0}^{q-1} b_i^2$$

is the least which in turn happens when

$$b_1 = b_2 = \cdots = b_{q-1} = \frac{N}{q}$$

Hence

$$B \leq N^2 - q\left(\frac{N}{q}\right)^2 = \frac{N^2(q-1)}{q}$$

Since ith entries of all the words of $\mathscr{C}$ contribute the same number B to the sum A for all i, $1 \leq i \leq n$,

$$A = nB \leq \frac{nN^2(q-1)}{q}$$

Using the lower bound obtained earlier for A, gives

$$N(N-1)d \leq \frac{nN^2(q-1)}{q}$$

or

$$d \leq \frac{nN(q-1)}{(N-1)q}$$

Remark 6.2

The bound for d is attained iff each symbol i occurs exactly N/q times in jth entries of all the code words of $\mathscr{C}$ for $1 \leq j \leq n$. This means that N/q must be an integer, i.e. q must divide N. Observe that for linear codes, this is no restriction for if $\mathscr{C}$ is of dimension k over GF(q), then $N = q^k$.

6.5 IDEMPOTENTS

Theorem 6.8

Let $\mathscr{C}$ be a cyclic code of length n over F and I be the ideal of $F[X]$ generated by $X^n - 1$. Then there exists a unique element $c(X) + I \in \mathscr{C}$ such that:

(i) $c(X) + I = c^2(X) + I$
(ii) $c(X) + I$ generates $\mathscr{C}$
(iii) $\forall f(X) + I$ in $\mathscr{C}$

$$c(X)f(X) + I = f(X) + I$$

i.e. $c(X) + I$ is an identity for $\mathscr{C}$.

Proof

Let $g(X) \in F[X]$ be a generator of $\mathscr{C}$ and $h(X)$ be its check polynomial. Then

$$g(X)h(X) = X^n - 1$$

Since $(n, q) = 1$ where $q = \mathrm{O}(F)$, $X^n - 1$ does not have multiple zeros. Therefore $(g(X), h(X)) = 1$ and there exist elements $a(X), b(X)$ in the Euclidean ring $F[X]$ such that

$$g(X)a(X) + h(X)b(X) = 1 \tag{6.2}$$

Take $c(X) = g(X)a(X)$. Multiplying both sides of the relation (6.2) by $c(X)$ and working in the quotient ring $F[X]/I$, gives

$$c^2(X) + g(X)h(X)a(X)b(X) + I = c(X) + I$$

or

$$c^2(X) + I = c(X) + I$$

This proves part (i).

Clearly

$$\langle c(X) + I \rangle \subseteq \langle g(X) + I \rangle$$

Again, multiplying both sides of the relation (6.2) by $g(X)$ and going to the quotient ring $F[X]/I$, gives

$$g(X)c(X) + g(X)h(X)b(X) + I = g(X) + I$$

or

$$g(X)c(X) + I = g(X) + I \tag{6.3}$$

This shows that

$$\langle g(X)+I\rangle \subseteq \langle c(X)+I\rangle$$

and hence

$$\langle g(X)+I\rangle = \langle c(X)+I\rangle$$

which proves part (ii). The relation (iii) also follows from (6.3).

Let $d(X)\in F[X]$ be another polynomial with the properties (i), (ii) and (iii). Since $c(X)$ and $d(X)$ both satisfy (iii), we have

$$c(X)d(X)+I=c(X)+I=d(X)+I$$

Definition 6.5

The unique element $c(X)+I\in\mathscr{C}$ with the properties (i), (ii) and (iii) of the theorem is called the **idempotent of** $\mathscr{C}$.

Remarks 6.3

(i) In a ring R, an element e is called an idempotent if $e^2=e$. In general, a ring R may have many idempotents. For example, if R is a ring with identity and e is an idempotent, then $1-e$ is another idempotent in R. Thus, we are in the above taking a very special idempotent in the ideal – namely the one that generates $\mathscr{C}$.

(ii) From the definition of $c(X)$, $g(X)|c(X)$. Also $g(X)|(X^n-1)$. Therefore $g(X)|d(x)$, where

$$d(x)=\text{g.c.d.}(c(X),X^n-1)$$

Let $d(X)=g(X)\lambda(X)$. Then $\lambda(X)|\text{g.c.d.}(h(X),c(X))$. But it follows from (6.2) that

$$\text{g.c.d.}(c(X),h(X))=1$$

Therefore $\lambda(X)=1$ and $g(X)=\text{g.c.d.}(c(X),X^n-1)$.

(iii) Let β be a root of X^n-1 such that $c(\beta)=0$. Then β is a common root of $c(X)$ and X^n-1 and hence is a root of $g(X)$. As $g(X)|c(X)$, every root of $g(X)$ is a root of $c(X)$. Hence if α is a primitive nth root of unity in a suitable extension of F, then $c(\alpha^i)=0$ iff $g(\alpha^i)=0$.

From this it follows that the polynomial $c(X)$ such that $c(X)+I$ is the unique idempotent in $\mathscr{C}$ that generates it is a power of $g(X)$ multiplied by a power of X.

Examples 6.3

Case (i)

Let $\mathscr{C}$ be the binary cyclic code of length 7 generated by $g(X)=X^3+X^2+1$. Then

$$h(X)=(X+1)(X^3+X+1)=X^4+X^3+X^2+1$$

Observe that

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

Therefore

$$c(X) + \langle X^7 - 1 \rangle = X^3 g(X) + I = X^6 + X^5 + X^3 + I$$

is the unique idempotent in $\mathscr{C}$ that generates it.

Case (ii)

Let $\mathscr{C}$ be the binary cyclic code of length 15 generated by $g(X) = X^4 + X + 1$. Then

$$\begin{aligned} h(X) &= \frac{(X^{15}+1)}{g(X)} \\ &= (X+1)(X^4+X^3+1)(X^6+X^4+X^3+X^2+1) \\ &= X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1 \end{aligned}$$

Observe that

$$\begin{aligned} g(X)^3 &= (X^4+X+1)^3 \\ &= X^{12} + X^9 + X^8 + X^6 + X^4 + X^3 + X^2 + X + 1 \end{aligned}$$

Therefore,

$$g(X)^3 + Xh(X) = 1$$

and hence

$$c(X) = g(X)^3 = X^{12} + X^9 + X^8 + X^6 + X^4 + X^3 + X^2 + X + 1$$

and $c(X) + \langle X^{15} + 1 \rangle$ is the unique idempotent in $\mathscr{C}$ that generates it.

6.6 SOME SOLVED EXAMPLES AND AN INVARIANCE PROPERTY

Examples 6.4

Case (i)

A (3,9) binary linear code V is defined by $(a_1, a_2, \ldots, a_9) \in V$ iff $a_1 = a_2 = a_3$, $a_4 = a_5 = a_6$ and $a_7 = a_8 = a_9$. Show that V is equivalent to a cyclic code and determine the generator.

Solution

$$\begin{aligned} X^9 - 1 &= (X^3 - 1)(X^6 + X^3 + 1) \\ &= (X-1)(X^2+X+1)(X^6+X^3+1) \end{aligned}$$