Hamming code. We may thus define a Hamming code as the matrix code defined by the parity check matrix **H**, the ith column of which is the binary representation of the number i, $1 \leq i \leq 2^r - 1$, subject also to the conditions given in Steps 1 and 2 of the procedure (p. 42).

In Chapter 1, we had required the last $n - m$ columns of a parity check matrix to form an identity matrix. However, Theorem 1.5 does not need this strong restriction and is valid in the general case, i.e. when a parity check matrix is required to be of rank $n - m$. Since the columns of the parity check matrix $\mathbf{M}'$ constructed for the Hamming code are non-zero and distinct, Theorem 1.5 shows that Hamming codes are single error correcting codes.

Exercise 3.2

Write down a parity check matrix of the (11, 15) Hamming code.

4

Finite fields and BCH codes

4.1 FINITE FIELDS

For the construction of BCH codes, we need to study construction of finite fields. However, the construction of finite fields depends heavily on some results on commutative rings. We first recall these results on rings, although briefly.

Definition 4.1

Let R be a ring and I be an ideal of R. Consider the set $R/I = \{x + I | x \in R\}$, where $x + I = \{x + a: a \in R\}$ are cosets of the ideal I in R. It is easy to check, using the ideal properties of I, that for $x, y \in R$,

$$(x + I) + (y + I) = (x + y) + I$$
$$(x + I)(y + I) = xy + I$$

are independent of the choice of the elements x, y in the cosets $x + I$ and $y + I$ respectively. Also w.r.t. these compositions R/I is a ring called the **ring of quotients** or the **difference ring** of R relative to the ideal I. If R is a commutative ring with identity, then so is R/I.

Definition 4.2

Let R be a commutative ring with identity and $a \in R$. Then $\langle a \rangle = aR = \{ar : r \in R\}$ is an ideal of R and is called a **principal ideal** generated by a. If every ideal of R is of this form, R is called a **principal ideal ring**.

Theorem 4.1

The polynomial ring $F[X]$, where F is a field, is a principal ideal ring.

Proof

The ring $F[X]$ is already a commutative ring with identity. Let I be an ideal of $F[X]$. If $I=0$, then I is a principal ideal generated by 0 and we, therefore, suppose that $I \neq 0$. Choose a $0 \neq f(X) \in I$ such that

$$\deg f(X) \leq \deg g(X) \forall 0 \neq g(X) \in I$$

This choice is possible because the set of non-negative integers is well ordered. Let $g(X) \in F[X]$, $g(X) \neq 0$. We claim that

$$g(X) = q(X)f(X) + r(X)$$

for some $q(X)$, $r(X) \in F[X]$ where either $r(X)=0$ or $\deg r(X) < \deg f(X)$. If $\deg g(X) < \deg f(X)$, we can take $q(X)=0$ and $r(X)=f(X)$. Suppose that

$$n = \deg f(X) \leq \deg g(X)$$

Let

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$$

$$g(X) = b_0X^m + b_1X^{m-1} + \cdots + b_m$$

Then $a_0 \neq 0$ and

$$g(X) = a_0^{-1}b_0X^{m-n}f(X) + g_1(X)$$

where $\deg g_1(X) \leq m-1$. Induction on the degree of $g(X)$ then shows that there exist $q_1(X)$, $r(X) \in F[X]$ such that

$$g_1(X) = q_1(X)f(X) + r(X)$$

where either $r(X)=0$ or $\deg r(X) < \deg f(X)$. Then

$$g(X) = q(X)f(X) + r(X)$$

where

$$q(X) = a_0^{-1}b_0X^{m-n} + q_1(X) \in F[X]$$

This proves the claim. Now, if $r(X) \neq 0$, then

$$r(X) = g(X) - q(X)f(X) \in F[X]$$

and $\deg r(X) < \deg f(X)$. This contradicts the choice of $f(X)$. Hence $g(X) = q(X)f(X)$ and I is a principal ideal generated by $f(X)$. ■

Definition 4.3

A non-constant polynomial $f(X) \in R[X]$, where R is a commutative ring with identity, is called **irreducible** if

$$f(X) = g(X)h(X) \quad \text{for } g(X), h(X) \in R[X]$$

$$\Rightarrow \deg g(X) = 0 \quad \text{or} \quad \deg h(X) = 0$$

Otherwise, we say that $f(X)$ is **reducible**.

Theorem 4.2

Let F be a field and $f(X) \in F[X]$ be an irreducible polynomial. Then $F[X]/\langle f(X)\rangle$ is a field.

Proof

Let I denote the ideal $\langle f(X)\rangle$ of $F[X]$ generated by $f(X)$. If $I = F[X]$, then $1 = f(X)g(X)$ for some $g(X) \in F[X]$. Comparing the degrees of the two sides of this relation implies that $f(X)$ is a constant polynomial which is a contradiction. Hence $F[X]/I$ has at least two elements. Already $F(X)/I$ is a commutative ring with identity.

Let $g(X) \in F[X]$, $g(X) \notin I$. Then

$$J = \{a(X)f(X) + b(X)g(X) \colon a(X), b(X) \in F[X]\}$$

is an ideal of $F[X]$ and there exists $h(X) \in F[X]$ such that $J = \langle h(X)\rangle$. Now

$$f(X) = 1 \times f(X) + 0 \times g(X)$$

is in J and, therefore,

$$f(X) = a(X)h(X) \quad \text{for some } a(X) \in F[X]$$

Irreducibility of $f(X)$ shows that $\deg h(X) = 0$ or $\deg a(X) = 0$. If $\deg a(X) = 0$, then $a(X)$ is a unit in $F[X]$ so that $h(X) \in I$ which implies that $J = I$. This is a contradiction because $g(X) \in J$ but $g(X) \notin I$. Hence $h(X)$ is a unit in $F[X]$ and $J = F[X]$. Therefore

$$1 = a(X)f(X) + b(X)g(X) \quad \text{for some } a(X), b(X) \in F[X]$$

and

$$1 + I = (b(X) + I)(g(X) + I)$$

Thus $g(X) + I$ is invertible and $F[X]/I$ is a field.

Definition 4.4

Let K be a field and F be a subfield of K. Then K is called an **extension** of the field F. The fact that K is an extension of F is expressed by writing

$$K|_F$$

Observe that K can be regarded as a vector space over F by using the multiplication in K. The dimension of the vector space K over F is called the **degree** of the extension K of F and is denoted by $[K{:}F]$. The extension $K|_F$ is called a **finite extension** if the degree $[K{:}F]$ is finite.

The intersection of all subfields of a field F is called a **prime subfield** of F. It is unique and is, in fact, the smallest subfield of F. In general, a field which has no proper subfield is called a **prime field**.

Let $K|_F$ be an extension of a field F. An element $\alpha \in K$ is said to be **algebraic over** F if there exists a polynomial $f(X) \in F[X]$ which has α as a root. Let $\alpha \in K$

be algebraic over F and consider

$$A = \{f(X) \in F[X] : f(\alpha) = 0\}$$

Then A is an ideal of $F[X]$ and $F[X]$ is a principal ideal domain. Let $m_1(X) \in F[X]$ be a generator of the ideal A. If a is the coefficient of the highest power of X in $m_1(X)$, then $m(X) = a^{-1}m_1(X)$ is a monic polynomial with $\deg m(X) = \deg m_1(X)$ which is also a generator of A. If

$$m(X) = r(X)s(X) \quad \text{for some } r(X), s(X) \in F[X]$$

then either $r(\alpha) = 0$ or $s(\alpha) = 0$, i.e. either $m(X) | r(X)$ or $m(X) | s(X)$. But

$$\deg m(X) = \deg r(X) + \deg s(X)$$

and, therefore, either $\deg r(X) = 0$ or $\deg s(X) = 0$. Thus $m(X)$ is irreducible. Also, it is clear from the choice of $m(X)$ that it is a monic, irreducible polynomial of the least possible degree which has α as a root. It is easily seen that $m(X)$ with these properties is unique and is called the **minimal polynomial** of α over F. Observe that the minimal polynomial of α depends on the subfield F. For example, the minimal polynomial of $\alpha = \sqrt{2}$ over Q is $X^2 - 2$ while over $\mathbb{R}$ – the field of real numbers – it is $X - \sqrt{2}$. Also observe that every element of the field F is algebraic over F.

Proposition 4.1

The order of a finite field is p^n for some prime p and some positive integer n.

Proof

Let F be a finite field. Since F is a finite group w.r.t. addition, it follows from Lagrange's theorem on finite groups (order of every subgroup of a finite group divides the order of the group) that $O(F)a = 0 \forall a \in F$. Choose m to be the smallest positive integer with $ma = 0$ for every $a \in F$. Let e denote the identity of F. Suppose that $m = rs$, where r, s are integers with $r > 1$, $s > 1$. Then

$$0 = me = (rs)e = (re)(se)$$

Therefore either $re = 0$ or $se = 0$. For any $a \in F$ and positive integer k, $ka = (ke)a$. Therefore, either $ra = 0 \forall a \in F$ or $sa = 0 \forall a \in F$ which contradicts the choice of m. Hence m must be a prime p (say). It is easy to check that

$$K = \{re : 0 \le r < p\}$$

is a subfield of F. Since F is finite, F is a finite dimensional vector space over K. If $\dim_K F = n$, and $x_1, x_2, \ldots, x_n$ is a basis of F over K, then every element of F can be uniquely written as

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n, a_i \in K$$

Since each a_i has exactly p choices and choice of any a_j is independent of the choice of other a_i, there are exactly p^n elements in F, i.e. $O(F) = p^n$.

Let F be a finite field of order p^n. Then $F^* = F \setminus \{0\}$ is a multiplicative group of order $p^n - 1$. Therefore, it follows from the Lagrange theorem, that

$$a^{p^n-1} = 1 \forall a \in F^*$$

or that

$$a^{p^n} = a \forall a \in F^*$$

Since this result is trivially true for the element $0 \in F$, we have

$$a^{p^n} = a \forall a \in F \tag{4.1}$$

Observe that every element of F is algebraic over the prime subfield of F.

Proposition 4.2

Let F be a finite field of order p^n with k as its prime subfield. Then α and α^p have the same minimal polynomial over k for every $\alpha \in F$.

Proof

Define a map $\theta: F \to F$ by $\theta(a) = a^p$, $a \in F$. Since

$$pa = 0 \forall a \in F$$

$$ab = ba \forall a, b \in F$$

and p divides the binomial coefficient

$$\binom{p}{i} \forall i \quad 1 \leq i \leq p-1$$

it follows that θ is a homomorphism of fields. Since $a^p \neq 0$ for $a \neq 0$, θ is a monomorphism. For any $a \in k$, $a^p = a$ (by (4.1)) and therefore θ keeps the elements of the prime subfield k fixed. Thus $\theta: F \to F$ is a monomorphism of finite dimensional vector space F over k into itself and hence θ is onto as well.

Let $a \in F$ and $m(X)$ be the minimal polynomial of α. Then $m(\alpha) = 0$ and θ being a field-homomorphism $m(\alpha^p) = 0$, i.e. α^p is also a root of $m(X)$. If $m_1(X)$ is the minimal polynomial of α^p, then $m_1(X) | m(X)$. But $m(X)$ is an irreducible, monic polynomial. Therefore $m_1(X) = m(X)$.

A finite field is called a **Galois field** and if F is a field of order p^n, we write $F = \mathrm{GF}(p^n)$.

For the proof of the next theorem, we need the following result about Abelian groups.

Lemma 4.1

Let G be a non-cyclic Abelian group of finite order m. Then there is a proper divisor k of m such that $x^k = 1 \forall x \in G$.

Theorem 4.3

In any finite field $F = \mathrm{GF}(p^n)$, the multiplicative group F^* of all non-zero elements is cyclic.

Proof

The multiplicative group F^* of F is an Abelian group of order $q-1$, where $q = p^n$. If F^* is not cyclic, there exists an integer r, $1 < r < q-1$ such that $a^r = 1 \forall a \in F^*$. Thus, every $a \in F$ is a root of the polynomial $X^{r+1} - X$ and hence

$$X - a | X^{r+1} - X \forall a \in F$$

Also $X - a, X - b$ are relatively coprime for $a, b \in F, a \neq b$. Therefore

$$\prod_{a \in F} (X - a) | X^{r+1} - X$$

But

$$\deg \prod_{a \in F} (X - a) = \mathrm{O}(F) = q$$

and

$$r + 1 < q - 1 + 1 = q$$

Thus, a polynomial of degree q divides a polynomial of degree $< q$ – which is a contradiction. This proves that there is no r with $1 < r < q-1$ such that $a^r = 1 \forall a \in F^*$. Hence F^* is cyclic.

Definition 4.5

A generator of the cyclic group F^* of the finite field F is called a **primitive element** of F.

We know that there are

$$\phi(\mathrm{O}(F^*)) = \phi(\mathrm{O}(F) - 1) = \phi(q - 1) \quad q = p^n = \mathrm{O}(F)$$

elements in F^*, every one of which generates F^*. Therefore, in a field of order p^n there are $\phi(p^n - 1)$ primitive elements. Here ϕ is Euler's ϕ-function.

Proposition 4.3

Let K be a finite extension of F and L be a finite extension of K. Then L is a finite extension of F and

$$[L:F] = [L:K][K:F]$$

Proof

Let $[L:K] = m$ and $[K:F] = n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis of the vector space K over F and $\beta_1, \ldots, \beta_m$ be a basis of the vector space L over K. Let $x \in L$. Then there exist elements $y_1, \ldots, y_m \in K$ such that

$$x = \sum_{i=1}^{m} y_i \beta_i$$