Chapter 1

Preliminaries

This chapter is mainly devoted to the collection of definitions and basic results, which are used in the subsequent chapters of the thesis. The chapter is organized into three sections: Basic Algebraic Structures, Basic Notions of Coding Theory, and Quantum-Error Correction.

1.1 Basic Algebraic Structures

In this section, we recall some basic algebraic structures and their properties which will serve as building blocks for subsequent coding theory. Unless otherwise cited, the material is derived from the books [32, 35]. For a more comprehensive understanding, readers are encouraged to consult these references.

Definition 1.1.1 (Group)**.** A *group* is a nonempty set G equipped with a binary operation $\cdot : G \times G \to G$, denoted $(a, b) \mapsto a \cdot b$, satisfying the following axioms for all $a, b, c \in G$:

(i) (Associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(ii) (Identity element) There exists an element $e \in G$ (called the identity element) such that $e \cdot a = a \cdot e = a$ for all $a \in G$.

(iii) (Inverse element) For every $a \in G$, there exists an element $b \in G$ (called the inverse of a) such that $a \cdot b = b \cdot a = e$.

Definition 1.1.2 (Abelian Group)**.** An *abelian group* (or *commutative group*) is a group G in which the binary operation $\cdot$ is commutative, i.e., for all $a, b \in G$,

$$a \cdot b = b \cdot a.$$

Definition 1.1.3 (Ring)**.** A *ring* is a nonempty set R equipped with two binary operations (say) addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$, satisfying the following axioms:

(I) $(R, +)$ is an abelian group.

(II) Multiplication is associative: For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(III) Distributive laws hold:

(i) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$.

(ii) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$.

Further, if $a \cdot b = b \cdot a, \ \forall \ a, b \in R$ then R is called a commutative ring. Moreover, if R has a multiplicative identity element $1 \neq 0$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$, then R is called a ring with unity.

Example 1.1.4. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ form rings under the usual addition and multiplication.

Example 1.1.5. The set of $n \times n$ matrices over a ring is also a ring under the usual addition and multiplication of matrices.

Definition 1.1.6. An element e of a ring R is called *idempotent* if $e^2 = e$, and two idempotent elements e_1 and e_2 of a ring R are said to be *orthogonal* if $e_1e_2 = e_2e_1 = 0$. An idempotent $e \in R$ is *primitive* if it can not be written as a sum of two nontrivial orthogonal idempotents.

Definition 1.1.7 (Subring)**.** A *subring* of a ring R is a subset $S \subseteq R$ that itself forms a ring under the induced binary operations of R.

Example 1.1.8. (i) The set of even integers $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(ii) The set of all diagonal matrices of order n is a subring of the ring of all $n \times n$ matrices over a ring.

Theorem 1.1.9 (Subring Test)**.** Let S be a nonempty subset of a ring R . Then S is a subring of R if and only if the following conditions hold:

(i) For all $a, b \in S$, $a - b \in S$

(ii) For all $a, b \in S$, $a \cdot b \in S$.

Definition 1.1.10 (Ideal)**.** An *ideal* of a ring R is a subset $I \subseteq R$ that satisfies the following conditions:

(i) I is a subring of R.

(ii) For all $a \in I$ and $r \in R$, both $r \cdot a \in I$ and $a \cdot r \in I$ (absorbs multiplication by elements of R).

Example 1.1.11. The set $2\mathbb{Z}$ of even integers is an ideal of $\mathbb{Z}$. In the ring $\mathbb{Z}[x]$, the set of all polynomials divisible by x is an ideal.

Definition 1.1.12. Let R and S be rings.

1. A ring homomorphism is a map $\varphi : R \to S$ satisfying the following conditions:

   (i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,

   so φ is a group homomorphism on the additive groups of R and S.

   (ii) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

2. The kernel of the ring homomorphism φ, denoted $\ker \varphi$, is the set of elements of R that map to 0 in S:

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}.$$

   This is the kernel of φ viewed as a homomorphism of additive groups.

3. A bijective ring homomorphism is called an **isomorphism**.

Definition 1.1.13 (Quotient Ring)**.** Let R be a ring and I be an ideal of R. The set of cosets of I in R is defined as:

$$R/I = \{a + I \mid a \in R\},$$

where $a+I = \{a+i \mid i \in I\}$. R/I forms a ring under the addition and multiplication in R/I defined as:

$$(a+I)+(b+I) = (a+b)+I \quad \text{and} \quad (a+I)(b+I) = (a \cdot b)+I.$$

The ring R/I is called the **quotient ring** of R by I.

Example 1.1.14. Consider the ring $\mathbb{Z}$ and the ideal $I = (3)$, the set of all multiples of 3. The quotient ring $\mathbb{Z}/(3)$ consists of the cosets:

$$\mathbb{Z}/(3) = \{0 + (3), 1 + (3), 2 + (3)\} = \{[0], [1], [2]\}.$$

This quotient ring is isomorphic to $\mathbb{Z}_3$, the ring of integers modulo 3.

Definition 1.1.15 (Prime Ideal)**.** An ideal $P \subseteq R$ is called a *prime ideal* if whenever $a \cdot b \in P$, then either $a \in P$ or $b \in P$, $P \neq R$.

Example 1.1.16. In $\mathbb{Z}$, the ideal (p) generated by a prime number p is a prime ideal. In $\mathbb{Z}[x]$, the set of all polynomials divisible by an irreducible polynomial (e.g., $x^2 + 1$ over $\mathbb{R}$) forms a prime ideal.

Definition 1.1.17 (Maximal Ideal)**.** An ideal M of R is called a *maximal ideal* if $M \neq R$ and for any ideal I of R such that $M \subseteq I \subseteq R$, we have $I = M$ or $I = R$.

Example 1.1.18. In $\mathbb{Z}$, the ideal (p) generated by a prime number p is a maximal ideal. In $\mathbb{Z}[x]$, the ideal $(x - 1)$ is a maximal ideal.

Theorem 1.1.19. Let P be a prime ideal of a ring R. Then the quotient ring R/P is an integral domain.

Theorem 1.1.20. Let R be a commutative ring with unity. An ideal M of R is a maximal ideal if and only if the quotient ring R/M is a field.

Example 1.1.21. In the ring $\mathbb{Z}$, the ideal (5) is a maximal ideal. The quotient ring $\mathbb{Z}/(5)$ is the field $\mathbb{Z}_5$ consisting of the elements $\{[0], [1], [2], [3], [4]\}$ with addition and multiplication modulo 5.

Definition 1.1.22. The ideals A and B of the ring R are said to be *comaximal* if $A + B = R$.

Theorem 1.1.23. (**Chinese Remainder Theorem**) Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \quad \text{defined by} \quad r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$, the ideals A_i and A_j are comaximal, then this map is surjective and

$$A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k,$$

so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Definition 1.1.24. A ring is a called local ring if it has a unique maximal ideal.

Local rings play an important role in coding theory because we often describe rings as the product of local rings via the Chinese Remainder Theorem and reduce much of the theory of codes to the case where the ring is local.

Example 1.1.25. Let $R = \mathbb{F}_2[x, y]/\langle x^2, y^2, xy - yx\rangle$. The ring R is a local ring and has cardinality 16. The maximal ideal is $\langle x, y\rangle$.

Definition 1.1.26. A principal ideal ring is a ring in which each ideal is generated by a single element, that is every ideal A can be written as $A = \langle a\rangle$ for some element a.

Example 1.1.27. It is well known that $\mathbb{Z}_k$ is a principal ideal ring for all $k > 1$.

Definition 1.1.28. A chain ring is a principal ideal ring such that the ideals are linearly ordered by set-theoretic containment.

It follows that if R is a finite chain ring then there is an element γ such that γ generates the unique maximal ideal and we have the following chain:

$$\{0\} \subseteq \langle \gamma^{e-1} \rangle \subseteq \langle \gamma^{e-2} \rangle \subseteq \ldots \subseteq \langle \gamma \rangle \subseteq R.$$

Example 1.1.29. The ring $\mathbb{Z}_{p^e}$ where p is a prime and $e > 0$ is a chain ring. Here, the maximal ideal is $\langle p \rangle$. A Galois ring is a ring of the form $\mathbb{Z}_{p^e}[x]/\langle q(x) \rangle$ where $q(x)$ is irreducible over $\mathbb{Z}_{p^e}$. Galois rings are also chain rings and the maximal ideal is again $\langle p \rangle$

It follows that a chain ring is necessarily a local ring, but a local ring need not be a chain ring, as in the following example.

Definition 1.1.30. A **non-chain ring** is a commutative ring with unity in which the lattice of ideals does not form a chain under inclusion. In other words, there exist two distinct ideals I and J such that neither $I \subseteq J$ nor $J \subseteq I$.

Example 1.1.31. Let $R = \mathbb{Z}_4[x]/\langle x^2 \rangle$. Then R is a ring of order 16 with maximal ideal $\langle 2, x \rangle = \{0, x, 2x, 3x, 2, 2+x, 2+2x, 2+3x\}$.But the ideals $\langle 2 \rangle = \{0, 2, 2x, 2+2x\}$ and $\langle x \rangle = \{0, x, 2x, 3x\}$ are not linearly ordered. Hence, R is a non-chain ring

Definition 1.1.32 (Field)**.** A *field* is a set F equipped with two binary operations, addition $+ : F \times F \to F$ and multiplication $\cdot : F \times F \to F$, such that:

1. $(F, +)$ is an abelian group with identity element 0.
2. $(F \setminus \{0\}, \cdot)$ is an abelian group with identity element 1.
3. Multiplication is distributive over addition: For all $a, b, c \in F$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Example 1.1.33. The set of rational numbers $\mathbb{Q}$ with usual addition and multiplication forms a field. Similarly, the set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$ are fields. The set of integers $\mathbb{Z}$ is **not** a field, as it does not have multiplicative inverses for all nonzero elements.

Definition 1.1.34 (Finite Field)**.** A field containing finitely many elements is called a *finite field*.

Lemma 1.1.35. For every element β of a finite field F with q elements, we have $\beta^q = \beta$.

Corollary 1.1.36. Let F be a subfield of E with $|F| = q$. Then an element β of E lies in F if and only if $\beta^q = \beta$.

Theorem 1.1.37. For any prime p and integer $n \geq 1$, there exists a unique finite field of p^n elements.

Definition 1.1.38. An element α in a finite field $\mathbb{F}_q$ is called a *primitive element* (or generator) of $\mathbb{F}_q$ if

$$\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}.$$

Example 1.1.39. Consider the field $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, where α is a root of the irreducible polynomial $1 + x + x^2 \in \mathbb{F}_2[x]$. Then we have:

$$\alpha^2 = -(1 + \alpha) = 1 + \alpha, \quad \alpha^3 = \alpha(\alpha^2) = \alpha(1 + \alpha) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1.$$

Thus,

$$\mathbb{F}_4 = \{0, \alpha, 1 + \alpha, 1\} = \{0, \alpha, \alpha^2, \alpha^3\},$$

so α is a primitive element.

Definition 1.1.40 (Vector Space)**.** A *vector space* over a field $\mathbb{F}$ is a nonempty set V equipped with two operations: vector addition $+ : V \times V \to V$ and scalar

multiplication $\cdot : \mathbb{F} \times V \to V$, satisfying the following axioms for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and $a, b \in \mathbb{F}$:

(I) $(V, +)$ is abelian group.

(II) (i) $a \cdot (b \cdot \mathbf{u}) = (ab) \cdot \mathbf{u}$.

(ii) $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$.

(iii) $(a + b) \cdot \mathbf{u} = a \cdot \mathbf{u} + b \cdot \mathbf{u}$.

(iv) $1 \cdot \mathbf{u} = \mathbf{u}$ for all $\mathbf{u} \in V$, where 1 is the multiplicative identity in $\mathbb{F}$.

Definition 1.1.41 (Subspace)**.** A subset $W \subseteq V$ of a vector space V is called a *subspace* if W itself is a vector space under the induced addition and scalar multiplication operations of V.

Theorem 1.1.42 (Subspace Test)**.** Let V be a vector space over a field F, and let $W \subseteq V$ be a nonempty subset. Then W is a subspace of V if and only if the following conditions hold:

(i) W is closed under addition: For all $u, v \in W$, $u + v \in W$.

(ii) W is closed under scalar multiplication: For all $u \in W$ and $c \in F$, $c \cdot u \in W$.

Definition 1.1.43 (Basis)**.** A *basis* of a vector space V is a set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} \subseteq V$ that satisfies the following two properties:

(i) The vectors are linearly independent: For any scalars $a_1, a_2, \ldots, a_n \in \mathbb{F}$, if $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$, then $a_1 = a_2 = \cdots = a_n = 0$.

(ii) The vectors span V: Every vector $\mathbf{u} \in V$ can be expressed as a linear combination of the basis vectors, i.e., $\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$ for some scalars $a_1, a_2, \ldots, a_n \in \mathbb{F}$.

Definition 1.1.44 (Dimension)**.** The *dimension* of a vector space V is the number of vectors in a basis of V. If V has a finite basis, the dimension is finite and denoted as $\dim V$. If no finite basis exists, V is said to have infinite dimension.

Definition 1.1.45 (Module)**.** A *module* over a ring R is a nonempty set M equipped with two operations, say:

- Addition: $+ : M \times M \to M$, denoted $(x, y) \mapsto x + y$,
- Scalar multiplication: $\cdot : R \times M \to M$, denoted $(r, x) \mapsto r \cdot x$,

such that for all $x, y, z \in M$ and $r, s \in R$, the following properties hold:

(I) $(M, +)$ is an abelian group.

(II) $r \cdot (x + y) = r \cdot x + r \cdot y$.

(III) $(r + s) \cdot x = r \cdot x + s \cdot x$.

(IV) $(r \cdot s) \cdot x = r \cdot (s \cdot x)$.

Further, if

$1 \cdot x = x$, where 1 is the multiplicative identity in R (if R is a ring with unity) then M is called a *unital module*

Definition 1.1.46 (Submodule)**.** A nonempty subset N of a module M over a ring R is called a *submodule* if it forms a module itself under the induced operations of M.

Theorem 1.1.47 (Submodule Test)**.** Let M be an R-module, and let $N \subseteq M$ be a nonempty subset. Then N is a submodule of M if and only if the following conditions hold:

(i) N is closed under addition: For all $u, v \in N$, $u + v \in N$.

(ii) N is closed under scalar multiplication: For all $u \in N$ and $c \in R$, $c \cdot u \in N$.

Theorem 1.1.48. Let $A_1, A_2, \ldots, A_n$ be left ideals of the ring R.

(i) The ring R can be written as a direct sum $R = A_1 \oplus A_2 \cdots \oplus A_n$ if and only if there exists a set $e_1, e_2, \cdots, e_n$ of orthogonal idempotents of R such that $A_j = Re_j$ for $1 \leq j \leq n$ and $e_1 + e_2 + \cdots + e_n = 1$.

(ii) The left ideals A_j in part (i) are two-sided ideals if and only if the corresponding idempotent elements belong to the center of R.

(iii) If condition (ii) holds, then every left R-left module can be written as a direct sum $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$, where $M_j = e_j M$ is a module over the ring A_j, for $1 \leq j \leq n$.

Definition 1.1.49 (Frobenius Ring)**.** Let G be a finite abelian group. A *character* is a homomorphism $\chi : G \to \mathbb{C}^*$, where $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, the nonzero complex numbers. Since G is abelian, the set of characters $\hat{G}$ is a group under function composition. The group $\hat{G}$ is isomorphic to G, but not in a canonical manner.

Given a finite ring R, R is a finite abelian group under addition, whether R is commutative or noncommutative, and hence has a character group $\hat{R}$. The ring R is both a left and right module over itself. We denote by ${}_R R$ the left module of R over itself and by R_R the right module of R over itself. Moreover, $\hat{R}$ is a module over R as well.

The ring R is **Frobenius** if and only if as a left module, $\hat{R} \cong {}_R R$ or equivalently, as a right module, $\hat{R} \cong R_R$.

Definition 1.1.50 (Algebra)**.** An *algebra* A over a commutative ring R is a structure that combines both a ring and a module. It satisfies the following conditions:

- A is a ring, meaning it has two binary operations: addition and multiplication, which satisfy the usual ring axioms (associativity, distributivity, existence of an additive identity, and existence of additive inverses).
- A is a left and right module over R, meaning that scalar multiplication is distributive and associative with respect to elements of R and elements of A. Specifically:

$$r(a+b) = ra + rb, \quad (r+s)a = ra + sa, \quad (rs)a = r(sa), \quad r(ab) = (ra)b$$

Theorem 1.1.51 (Frobenius Property and Finite-Dimensional Algebras)**.** Let A be a finite-dimensional algebra over a commutative ring R. The following are equivalent:

(1) A is a Frobenius algebra.

(2) As a left module, $\hat{A} \cong {}_AA$, where $\hat{A}$ is the character group of A, and ${}_RR$ is the left module of A over itself.

(3) As a right module, $\hat{A} \cong A_A$, where A_A is the right module of A over itself.

1.2 Basic Notions of Coding Theory

In this section, we introduce basic definitions, examples, and results related to coding theory. Starting with linear codes, we explore specific types like cyclic, constacyclic, skew cyclic, and skew constacyclic codes. Unless otherwise cited, the material is derived from the books [46, 60]. For a more comprehensive understanding, readers are encouraged to consult these books.

Definition 1.2.1. Let $A = \{a_1, a_2, \ldots, a_q\}$ be a finite set of size q, which we refer to as a **code alphabet** and whose elements are called **code symbols**.

(i) A q-ary word of length n over A is a sequence $w = w_1 w_2 \dots w_n$ with each $w_i \in A$ for all i. Equivalently, w may also be regarded as the vector $(w_1, w_2 \dots, w_n)$.

(ii) A q-ary block code of length n over A is a nonempty set C of q-ary words having the same length n.

(iii) An element $\mathbf{c}$ of C is called a **codeword** in C.

(iv) The number of codewords in C, denoted by $|C|$, is called the size of C.

(v) The (information) rate of a code C of length n is defined to be $\frac{log_q|C|}{n}$.

(vi) A code of length n and size M is called an (n, M)-code.

Definition 1.2.2. A linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$.

Example 1.2.3. The following are linear codes:

(i) $C = \{(\lambda, \lambda, \dots, \lambda) : \lambda \in \mathbb{F}_q\}$. This code is often called a repetition code.

(ii) (for $q = 2$) $C = \{000, 001, 010, 011\}$.

Definition 1.2.4. For a linear code C of length n over $\mathbb{F}_q$, its dual code is defined as

$$C^{\perp} = \{u \in \mathbb{F}_q^n : \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in \mathbb{F}_q^n\},$$

where

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=0}^{n-1} u_i v_i$$

for $\mathbf{u} = (u_0, u_1, \dots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_q^n$.

Definition 1.2.5. Let C be a linear code in $\mathbb{F}_q^n$.

(i) The dual code of C is $C^{\perp}$, the orthogonal complement of the subspace C of $\mathbb{F}_q^n$.

(ii) The dimension of the linear code C is the dimension of C as a vector space over $\mathbb{F}_q$, i.e., $\dim(C)$.

Theorem 1.2.6. Let C be a linear code of length n over $\mathbb{F}_q$. Then:

(i) $|C| = q^{\dim(C)}$, i.e., $\dim(C) = \log_q |C|$;

(ii) $C^\perp$ is a linear code and $\dim(C) + \dim(C^\perp) = n$;

(iii) $(C^\perp)^\perp = C$.

Example 1.2.7. (i) Let $q = 2$ and $C = \{0000, 1010, 0101, 1111\}$. Then,

$$\dim(C) = \log_2 |C| = \log_2 4 = 2.$$

It is easy to see that $C^\perp = \{0000, 1010, 0101, 1111\} = C$, so $\dim(C^\perp) = 2$.

(ii) Let $q = 3$ and $C = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$. Then,

$$\dim(C) = \log_3 |C| = \log_3 9 = 2.$$

One checks readily that $C^\perp = \{000, 100, 200\}$, so $\dim(C^\perp) = 1$.

Remark 1.2.8. A linear code C of length n and dimension k over $\mathbb{F}_q$ is often called a q-ary $[n, k]$-code or, if q is clear from the context, called an $[n, k]$-code. It is also an (n, q^k)-linear code. If the distance d of C is known, it is sometimes referred to as an $[n, k, d]$-linear code.

Theorem 1.2.9 (Singleton Bound)**.** Let C be a code of length n, dimension k, and minimum distance d over a finite field. The Singleton bound states that

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

Definition 1.2.10 (MDS Code)**.** A code C is called a *Maximum Distance Separable (***MDS***)* code if it meets the Singleton bound with equality, i.e., if

$$d = n - k + 1.$$

Moreover, an $[n, k, d]$ code is called almost MDS (**AMDS**) if $d = n - k$.

Definition 1.2.11. Let C be a linear code.

(i) C is *self-orthogonal* if $C \subseteq C^{\perp}$.

(ii) C is *self-dual* if $C = C^{\perp}$.

Proposition 1.2.12. The dimension of a self-orthogonal code of length n must be $\leq \frac{n}{2}$, and the dimension of a self-dual code of length n is $\frac{n}{2}$.

Definition 1.2.13. Let x be a word in $\mathbb{F}_q^n$. The (Hamming) weight of x, denoted by $\mathrm{wt}(x)$, is defined to be the number of nonzero coordinates in x; i.e.,

$$\mathrm{wt}(x) = d(x, 0),$$

where 0 is the zero word.

Remark 1.2.14. For every element x of $\mathbb{F}_q$, we can define the Hamming weight as follows:

$$\mathrm{wt}(x) = d(x, 0) = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

Writing $x \in \mathbb{F}_q^n$ as $x = (x_1, x_2, \ldots, x_n)$, the Hamming weight of x can also be equivalently defined as

$$\mathrm{wt}(x) = \mathrm{wt}(x_1) + \mathrm{wt}(x_2) + \cdots + \mathrm{wt}(x_n). \tag{4.1}$$

Lemma 1.2.15. If $x, y \in \mathbb{F}_q^n$, then $d(x, y) = \mathrm{wt}(x - y)$.

Theorem 1.2.16. Let C be a linear code over $\mathbb{F}_q$. Then

$$d(C) = \mathrm{wt}(C).$$

Example 1.2.17. Consider the binary linear code $C = \{0000, 1000, 0100, 1100\}$. We can calculate the weights of the non-zero codewords as follows:

$$\mathrm{wt}(1000) = 1,$$
$$\mathrm{wt}(0100) = 1,$$
$$\mathrm{wt}(1100) = 2.$$

Thus, the minimum distance $d(C)$ is given by the minimum weight of the non-zero codewords in C:

$$d(C) = 1.$$

Definition 1.2.18. Let C be a linear code.

(i) A generator matrix G for a linear code C is a matrix whose rows form a basis for C.

(ii) A parity-check matrix H for a linear code C is a generator matrix for the dual code $C^{\perp}$.

Definition 1.2.19. A subset S of $\mathbb{F}_q^n$ is *cyclic* if $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in S$ whenever $(a_0, a_1, \ldots, a_{n-1}) \in S$. A linear code C is called a *cyclic code* if C is a cyclic set.

The word $(u_{n-r}, \ldots, u_{n-1}, u_0, u_1, \ldots, u_{n-r-1})$ is said to be obtained from the word $(u_0, \ldots, u_{n-1}) \in \mathbb{F}_q^n$ by cyclically shifting r positions.

Proposition 1.2.20. The dual code of a cyclic code is also a cyclic code.

Example 1.2.21. The sets

$$\{(0,1,1,2),(2,0,1,1),(1,2,0,1),(1,1,2,0)\} \subseteq \mathbb{F}_3^4, \quad \{11111\} \subseteq \mathbb{F}_2^5$$

are cyclic sets, but they are not cyclic codes since they are not linear spaces.

Example 1.2.22. The following codes are cyclic codes:

(i) three trivial codes $\{0\}$, $\{\lambda \cdot 1 : \lambda \in \mathbb{F}_q\}$, and $\mathbb{F}_q^n$;

(ii) the binary $[3,2,2]$-linear code $\{000, 110, 101, 011\}$;

(iii) the simplex code $S(3,2) = \{0000000, 1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101\}$.

Theorem 1.2.23. Let $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[y]/(y^n-1)$ be a linear map defined as :

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}.$$

Then a nonempty subset C of $\mathbb{F}_q^n$ is a cyclic code if and only if $\pi(C)$ is an ideal of $\mathbb{F}_q[y]/(y^n-1)$.

Definition 1.2.24. The unique monic polynomial of the least degree of a nonzero ideal I of $\mathbb{F}_q[y]/(y^n-1)$ is called the **generator polynomial** of I. For a cyclic code C, the generator polynomial of $\pi(C)$ is also called the generator polynomial of C.

Example 1.2.25. (i) The generator polynomial of the cyclic code $\{000, 110, 011, 101\}$ is $1+y$.

(ii) The generator polynomial of the simplex code in Example 1.2.22(iii) is $1 + y^2 + y^3 + y^4$.

Theorem 1.2.26. Each monic divisor of $y^n - 1$ is the generator polynomial of some cyclic code in $\mathbb{F}_q^n$.

Theorem 1.2.27. Let $y^n - 1 \in \mathbb{F}_q[y]$ have the factorization

$$y^n - 1 = \prod_{i=1}^{r} p_i(y)^{e_i},$$

where $p_1(y), p_2(y), \ldots, p_r(y)$ are distinct monic irreducible polynomials and $e_i \geq 1$ for all $i = 1, 2, \ldots, r$. Then there are $\prod_{i=1}^{r}(e_i + 1)$ cyclic codes of length n over $\mathbb{F}_q$.

Theorem 1.2.28. Let $g(y)$ be the generator polynomial of an ideal of $\mathbb{F}_q[y]/(y^n - 1)$. Then the corresponding cyclic code has dimension k if the degree of $g(y)$ is $n - k$.

Theorem 1.2.29. Let $g(y) = g_0 + g_1 y + \cdots + g_{n-k} y^{n-k}$ be the generator polynomial of a cyclic code C in $\mathbb{F}_q^n$ with $\deg(g(y)) = n - k$. Then the matrix

$$G = \begin{pmatrix} g(y) \\ yg(y) \\ \vdots \\ y^{k-1}g(y) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

is a generator matrix of C (note that we identify a vector with a polynomial).

Definition 1.2.30. Let $h(y) = \sum_{i=0}^{k} a_i y^i$ be a polynomial of degree k ($a_k \neq 0$) over $\mathbb{F}_q$. The reciprocal polynomial $h_R(y)$ of $h(y)$ is defined by

$$h_R(y) := y^k h\left(\frac{1}{y}\right) = \sum_{i=0}^{k} a_{k-i} y^i.$$

Remark 1.2.31. If $h(y)$ is a divisor of $y^n - 1$, then so is $h_R(y)$.

Example 1.2.32. (i) For the polynomial $h(y) = 1 + 2y + 3y^5 + y^7 \in \mathbb{F}_5[y]$, the reciprocal of $h(y)$ is

$$h_R(y) = y^7 h\left(\frac{1}{y}\right) = y^7\left(1 + 2\left(\frac{1}{y}\right) + 3\left(\frac{1}{y^5}\right) + \frac{1}{y^7}\right) = 1 + 3y^2 + 2y^6 + y^7.$$

(ii) Consider the divisor $h(y) = 1 + y + y^3 \in \mathbb{F}_2[y]$ of $y^7 - 1$. Then

$$h_R(y) = 1 + y^2 + y^3$$

is also a divisor of $y^7 - 1$.

Definition 1.2.33. Let C be a q-ary cyclic code of length n. Put $h(y) = \frac{y^n-1}{g(y)}$. Then, $h_0^{-1}h_R(y)$ is called the **parity-check polynomial** of C, where h_0 is the constant term of $h(y)$.

Corollary 1.2.34. Let C be a q-ary $[n, k]$-cyclic code with generator polynomial $g(y)$. Put $h(y) = \frac{y^n-1}{g(y)}$. Let $h(y) = h_0 + h_1 y + \cdots + h_k y^k$. Then the matrix

$$H = \begin{pmatrix} h_R(y) \\ yh_R(y) \\ \vdots \\ y^{n-k-1}h_R(y) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}$$

is a parity-check matrix of C.

Example 1.2.35. Let C be the binary $[7, 4]$-cyclic code generated by $g(y) = 1+y^2+y^3$ as in Example 7.3.2. Put $h(y) = \frac{y^7-1}{g(y)} = 1+y^2+y^3+y^4$. Then $h_R(y) = 1+y+y^2+y^4$

is the parity-check polynomial of C. Hence,

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

is a parity-check matrix of C.

Definition 1.2.36. A linear code C of length n over $\mathbb{F}_q$ is called a *constacyclic code* if there exists a nonzero element $\lambda \in \mathbb{F}_q$ such that for every codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, the vector $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a codeword in C. The scalar λ is called the *constacyclic shift* or *consta-factor*.

Theorem 1.2.37. Let $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[y]/(y^n - \lambda)$ be a linear map defined as :

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}.$$

Then a nonempty subset C of $\mathbb{F}_q^n$ is a cyclic code if and only if $\pi(C)$ is an ideal of $\mathbb{F}_q[y]/(y^n - \lambda)$.

Definition 1.2.38. The unique monic polynomial of the least degree of a nonzero ideal I of $\mathbb{F}_q[y]/(y^n - \lambda)$ is called the **generator polynomial** of I. For a constacyclic code C, the generator polynomial of $\pi(C)$ is also called the generator polynomial of C.

Theorem 1.2.39. Let $g(y) = g_0 + g_1 y + \cdots + g_{n-k} y^{n-k}$ be the generator polynomial of a constacyclic code C of length n over $\mathbb{F}_q$, where $\deg(g(y)) = n - k$. Then the

matrix

$$G = \begin{pmatrix} g(y) \\ yg(y) \\ \vdots \\ y^{k-1}g(y) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

is a generator matrix of C.

Definition 1.2.40. Let θ be an automorphism of $\mathbb{F}_q$. Skew θ-cyclic shift of a vector $\mathbf{v} = (v_0, v_1, \ldots, v_n)$ is defined as $\sigma_\theta(\mathbf{v}) = (\theta(v_{n-1}), \theta(v_0), \theta v_1, \ldots, \theta(v_{n-2})$. A linear code C of length n over $\mathbb{F}_q$ is said to skew θ-cyclic if $\sigma_\theta(\mathbf{v}) \in C, \forall \mathbf{v} \in C$.

Remark 1.2.41. If θ is the identity map then C is cyclic code.

Theorem 1.2.42. Let $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[y;\theta]/(y^n - 1)$ be a linear map defined as :

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}.$$

Then π is an isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_q[y;\theta]/\langle y^n - 1\rangle$. Under this isomorphism, a linear code C is a skew cyclic code of length n if and only if $\pi(C)$ is a left submodule of $A_n = \mathbb{F}_q[y;\theta]/\langle y^n - 1\rangle$. If the order of θ divides n then A_n is a ring and a linear code C is a skew θ-cyclic code of length n if and only if $\pi(C)$ is a left ideal of A_n.

The monic generator polynomial $f(y) = \sum_{i=0}^{n-k-1} f_i y^i$ of this ideal is called the generator polynomial of this code and a generator matrix of this code is given as:

$$G = \begin{bmatrix} f_0 & f_1 & \ldots & f_{n-k-1} & 0 & \ldots & 0 \\ 0 & \theta(f_0) & \theta(f_1) & \ldots & \theta(f_{n-k-1}) & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \theta^{k-1}(f_0) & \theta^{k-1}(f_1) & \ldots & \theta^{k-1}(f_{n-k-1}) \end{bmatrix}$$

Definition 1.2.43. Let θ be an automorphism of $\mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$. Then the skew (θ, β)-constacyclic shift of a vector $\mathbf{v} = (v_0, v_1, \ldots, v_n)$ is defined as: $\sigma_{\theta,\beta}(\mathbf{v}) = (\beta\theta(v_{n-1}), \theta(v_0), \theta v_1, \ldots, \theta(v_{n-2}))$.

Remark 1.2.44. In particular, if $\beta = 1$, then C is a skew cyclic code. Further, if θ is the identity map then C is a β-constacyclic code. Moreover, if θ is the identity map and $\beta = 1$, then C becomes a cyclic code.

Theorem 1.2.45. Let $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[y;\theta]/(y^n - \beta)$ be a linear map defined as :

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}.$$

Then π is an isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_q[y;\theta]/\langle y^n - \beta\rangle$. Under this isomorphism, a linear code C is a skew (θ, β)-constacyclic code of length n if and only if $\pi(C)$ is a left submodule of $A_n = \mathbb{F}_q[y;\theta]/\langle y^n - \beta\rangle$. If the order of θ divides n and $\theta(\beta) = \beta$, then A_n is a ring and a linear code C is a skew (θ, β)-constacyclic code of length n if and only if $\pi(C)$ is a left ideal of A_n.

The monic generator polynomial $f(y) = \sum_{i=0}^{n-k-1} f_i y^i$ of this ideal is called the generator polynomial of this code and a generator matrix of this code is given as:

$$G = \begin{bmatrix} f_0 & f_1 & \ldots & f_{n-k-1} & 0 & \ldots & 0 \\ 0 & \theta(f_0) & \theta(f_1) & \ldots & \theta(f_{n-k-1}) & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \theta^{k-1}(f_0) & \theta^{k-1}(f_1) & \ldots & \theta^{k-1}(f_{n-k-1}) \end{bmatrix}.$$

1.3 Quantum-Error Correction

This section introduces the essential concepts and results in quantum error-correction, which is fundamental for reliable quantum computation and communication. Key

topics include stabilizer codes, quantum MDS codes, and methods for constructing quantum codes from classical codes. For an indepth knowledge, readers are encouraged to refer [54], [46, Chapter 27].

To set the stage for understanding quantum error-correcting codes, we start by examining the simplest two-state quantum system, which highlights the unique features of quantum mechanics. This two-state system, known as a **qubit** or quantum bit, differs from classical systems, where a bit can only exist in one of two states. In contrast, quantum mechanics enables a qubit to be in a coherent superposition of both states simultaneously, a fundamental property of quantum mechanics and quantum computing. In quantum mechanics, the general state of a qubit can be represented as a linear superposition of its orthonormal basis states, typically denoted as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. These two states $\{|0\rangle, |1\rangle\}$ form the computational basis. Qubit basis states can be combined to form product basis states.

For n qubits, the state is represented by a superposition in a 2^n-dimensional subspace of $\mathbb{C}^{2^n}$, which can be decomposed into the tensor product of n copies of $\mathbb{C}^2$, with each copy corresponding to one qubit.

The core idea behind quantum error correction is the encoding of k qubits into n qubits. This encoding is a linear mapping from $\mathbb{C}^{2^k}$ onto a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$. The error-correcting properties of the code depend not on the mapping itself, but on the subspace, which is referred to as the quantum error-correcting code.

Formally, for a prime power q, let $\mathbb{C}^q$ represent a q-dimensional complex vector space. The vectors of a distinguishable orthonormal basis of $\mathbb{C}^{q^n}$ are denoted $|x\rangle$, where x ranges over elements of $\mathbb{F}_q$, the finite field of size q. A q-ary quantum error-correcting code of length n is then a subspace of $\mathbb{C}^{q^n}$. For $q = 2$, this corresponds to a binary quantum error-correcting code.

1.3.1 Stabilizer Codes

In this subsection, we give a concise overview of stabilizer codes as discribed in [54].

Definition 1.3.1 (Error Bases)**.** Let q be a power of a prime p, and let $\mathcal{H}$ be a q-dimensional complex vector space representing the states of a quantum mechanical system. The error operators $X(a)$ and $Z(b)$ for $a, b \in \mathbb{F}_q$ are defined by

$$X(a)\left|x\right\rangle = \left|x+a\right\rangle, \quad Z(b)\left|x\right\rangle = \omega^{\mathrm{Tr}(bx)}\left|x\right\rangle,$$

where ω is a primitive pth root of unity, and Tr is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.

A set of operators $\mathcal{E} = \{\omega^c X(a)Z(b) : c \in \mathbb{F}_p, a, b \in \mathbb{F}_q\}$ forms a basis for the space of $q \times q$ complex matrices. Such a set is called a *nice error basis*.

Lemma 1.3.2. The set $\mathcal{E}$ defined above forms a nice error basis.

Definition 1.3.3. A *quantum stabilizer code* is a type of error-correcting code used in quantum computing that encodes a logical qubit into multiple physical qubits, protecting it from certain types of errors. The code is defined by a *stabilizer group*, which is a subgroup of the Pauli group, and the code space is the simultaneous $+1$ eigenspace of the operators in this group.

A quantum stabilizer code is defined by the following parameters:

- **Code Space**: The code space is the subspace of the Hilbert space that is invariant under the stabilizer group. If the stabilizer group is denoted as S, the code space is defined as:

  $$\mathcal{C} = \{|\psi\rangle \in \mathcal{H} : g|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}$$

  where S is the stabilizer group, and $\mathcal{H}$ is the Hilbert space of the system.

- **Stabilizer Group**: The stabilizer group S is a set of n-fold tensor products of Pauli operators ($\{I, X, Y, Z\}$), and is generated by a set of independent stabilizer generators. These generators are usually represented as $g_1, g_2, \ldots, g_k$, where each g_i is a Pauli operator, such that the code space is the set of simultaneous eigenstates with eigenvalue $+1$ for each generator:

$$g_i|\psi\rangle = |\psi\rangle \quad \text{for all } i = 1, 2, \ldots, k.$$

- **Length of the Code** (n): The length n is the number of physical qubits used in the code.

- **Dimension of the Code** (k): The dimension k of the code space is the number of logical qubits that the code can encode. This is related to the rank of the stabilizer group.

- **Distance** (d): The distance d of the code is the minimum number of qubits that need to be altered in any state of the code space in order to produce a state outside the code space. The distance is related to the number of errors the code can correct.

- **Pauli Group**: The Pauli group on n qubits is the group of operators consisting of all tensor products of the Pauli matrices:

$$P_n = \{\pm X^a Z^b : a, b \in \{0, 1\}^n\}$$

  where X is the Pauli-X operator (bit-flip), Z is the Pauli-Z operator (phase-flip), and the identity operator I is included in the group.

- **Stabilizer Code Parameters**: The stabilizer code is usually specified by the tuple (n, k, d), where:

- n is the number of physical qubits,
- k is the dimension of the code space (the number of logical qubits),
- d is the code distance (the number of qubits the code can correct).

Theorem 1.3.4. (Quantum Singleton Bound) [40] Let $\mathcal{Q} = [[n, k, d]]_q$ be a quantum error-correction code (QECC), then

$$k + 2d \leq n + 2. \tag{1.1}$$

Definition 1.3.5. (Quantum MDS code) A quantum code for which equality holds in (1.1), i.e. an $[[n, n - 2d + 2, d]]_q$ quantum code is called a quantum MDS code.

1.3.2 Construction of Quantum Codes from Classical Codes

A popular method for constructing quantum codes from classical codes is (Calderbank–Shor–Steane (CSS) Construction based on the works presented in [89, 22]. A formal statement of this method as stated in [54] is as follows:

Lemma 1.3.6. [CSS Code Construction][54, Lemma 20] Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two classical linear codes with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1$. Then there exists a stabilizer code with parameters $[\![n, k_1 + k_2 - n, \min(d_1, d_2)]\!]$.

Lemma 1.3.7. [5, Corollary 1] Let D be an $[n, (n-k)/2]_{q^2}$ Hermitian self-orthogonal code over $\mathbb{F}_{q^2}$ and let $d = \min\{\mathrm{wt}(v) : v \in D^{\perp_H} \setminus D\}$. Then there exists an $[[n, k]]_q$ quantum stabilizer code with minimum distance d.

1.3.3 Entanglement Assisted Quantum Error Correcting Codes

Entanglement plays a central role in quantum information processing. It enables the teleportation of quantum states without physically sending quantum systems. In 2006, Brun et al. [21] propsed a method for constructing quantum codes using shared entangled ebits. These codes are popularly known as EAQECCs.

Definition 1.3.8. A quantum code Q is called an $[[n, k, d; c]]_q$ EAQEC code if it encodes k logical qudits into n physical qudits using c copies of maximally entangled states and can correct $\lfloor \frac{d-1}{2} \rfloor$ quantum errors.

If $c = 0$, then the EAQEC code is a standard stabilizer code. EAQEC codes can be regarded as generalized quantum codes.

****