LATTICES FROM CODES

MSc MATHEMATICS

2024-26

LATTICES FROM CODES

Exam Code : 62023402

Programme Code : 620

Course Code : MM 545

Certificate

This is to certify that the dissertation entitled **"LATTICES FROM CODES"** is a record of studies carried out by **ANAMIKA A S**, M.Sc Mathematics student of the year **2024-2026** at **T.K.M College of Arts and Science**, under my guidance and submitted to the University of Kerala in partial fulfillment of the Degree of Master of Science in Mathematics.

Kollam

July 2026

Dr. ADERSH V K

Associate Professor

Department of Mathematics

T.K.M College of Arts and Science

Dr. ASWATHY M R

H.O.D and Assistant Professor

Department of Mathematics

T.K.M College of Arts and Science

Contents

Introduction

Coding theory is an important branch of mathematics that deals with the reliable transmission and storage of information over noisy communication channels. Among the various classes of error-correcting codes, linear codes occupy a central position because of their elegant algebraic structure and computational efficiency. Cyclic codes form an important subclass of linear codes and admit a polynomial representation that facilitates efficient encoding and decoding. Several well-known families of linear and cyclic codes, including BCH codes, Maximum Distance Separable (MDS) codes, Reed–Solomon codes, Generalized Reed–Solomon codes, Reed–Muller codes, and Quadratic Residue codes, have been extensively studied due to their excellent error-correcting capabilities and their applications in digital communications, data storage, and information security.

A lattice is a discrete additive subgroup of the Euclidean space generated by a basis of linearly independent vectors and possesses rich algebraic and geometric properties. One of the most important links between these two areas is the construction of lattices from linear codes. Among the various construction techniques, **Construction A** provides a simple and elegant method for associating an Integer lattice with a linear code over a finite field.

Ideal lattices constitute a special class of lattices possessing additional algebraic structure. Cyclic lattices are another important class of lattices characterized by invariance under cyclic shifts of their coordinates. A close relationship exists between cyclic codes and cyclic lattices.

In this project, the first chapter deals with fundamental concepts of linear and

cyclic codes together with several important families of error-correcting codes. Second chapter deals with focuses on the construction of lattices from linear codes using **Construction A**. Third chapter deals with the study of ideal lattices and a criterion that facilitates the identification of whether a given lattice is an ideal lattice and introduced cyclic lattices and examined the relationship between cyclic codes and cyclic lattices, showing how cyclic codes give rise to cyclic lattices through **Construction A**.

Chapter 1

Introduction to Linear Codes

In this chapter, we recall some basic definitions and theorems that will be used throughout the project.

Definition 1.1. Let $\mathbb{F}_q$ be the finite field of order q and let $\mathbb{F}_q^n$ be the set of all vectors of length n with entries in $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(v_1, v_2, ..., v_n) : v_i \in \mathbb{F}_q\}. \tag{1.1}$$

We define vector addition and scalar multiplication for $\mathbb{F}_q^n$ component-wise using the addition and multiplication of $\mathbb{F}_q$: that is if

$$\mathbf{u} = (u_1, u_2, ..., u_n) \in \mathbb{F}_q^n \text{ and } \mathbf{v} = (v_1, v_2, ..., v_n) \in \mathbb{F}_q^n \ , \ \lambda \in \mathbb{F}_q \tag{1.2}$$

then

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1, ..., u_n + v_n) \in \mathbb{F}_q^n \ , \ \lambda\mathbf{u} = (\lambda u_1, \lambda u_2, ..., \lambda u_n) \in \mathbb{F}_q^n \tag{1.3}$$

let 0 denote the zero vector $(0, 0, ..., 0) \in \mathbb{F}_q^n$. Note that F_q^n is a vector space of dimension n over F_q.

Definition 1.2. A non empty subset C of $\mathbb{F}_q^n$ is a said to be a subspace [5] if it

satisfy the following conditions :

$$if\ \mathbf{u}, \mathbf{v} \in C \text{ and } \lambda, \mu \in \mathbb{F}_q,\ then\ \lambda\mathbf{u} + \mu\mathbf{v} \in C \tag{1.4}$$

Definition 1.3. Let $A = \{a_1, a_2, ..., a_q\}$ be a set of size q, which we refer to as a code alphabet and whose elements are called code symbols.[4]

(i) A q-ary word of length n over A is a sequence $w = w_1w_2...w_n$ with each $w_i \in$ A for all i. Equivalently, w may also be regarded as the vector $(w_1, ..., w_n)$.

(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 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 $(\log_q |C|)/n$.

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

Definition 1.4. For a code C containing at least two words, the (minimum) distance of C , denoted by $d(C)$, is

$$d(C) = min\{d(x, y) : x, y \in C, x \neq y\}$$

Definition 1.5. A code C of length n over $\mathbb{F}_q$ is said to be a linear code of length n over $\mathbb{F}_q$ if it is a subspace of $\mathbb{F}_q^n$.

A linear code C of length n and dimension k over $\mathbb{F}_q$ with a distance d is called $[n, k, d]$-code.

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

(ii) $C^{\perp}$ is the **dualcode** of C . It is the orthogonal complement of subspace C over $\mathbb{F}_q^n$.

$$C^{\perp} = \{x \in \mathbb{F}_q^n : x.c = 0 \text{ for all } c \in C\}.$$

We state the following properties of linear codes without proofs.

Theorem 1.1. *Let C be a linear code of length n over $\mathbb{F}_q$. then,*

(i) $|C| = q^{\dim(C)}$

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

(iii) $(C^{\perp})^{\perp} = C$

Definition 1.6. C be a linear code,

(a) C is self orthogonal if $C \subseteq C^{\perp}$

(b) C is self dual if $C = C^{\perp}$

Example 1. The following is the binary linear code C of length 3 . C = { 1,1,0} . $C^{\perp}$ = { 000,110 001,111 } . here $C \subseteq C^{\perp}$. So C is self orthogonal .

Definition 1.7 (Hamming weight)**.** Let $\mathbf{x}$ be a word in $\mathbb{F}_q^n$, The **Hamming weight** of $\mathbf{x}$, denoted by $wt(\mathbf{x})$, is defined to be the number of nonzero coordinates in $\mathbf{x}$;

$$wt(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}),\ d(\mathbf{x}, \mathbf{0}) = \begin{cases} 1\ ; & \mathbf{x} \neq 0 \\ 0\ ; & \mathbf{x} = 0 \end{cases} \tag{1.5}$$

where $\mathbf{0}$ is the zero word .

Definition 1.8. (a) A **Generator matrix** for a linear code C is a matrix G whose rows form a basis for C.

(b) A **Parity check matrix** H for a linear code C is a generator matrix for the dual code $C^{\perp}$.

Theorem 1.2. *The standard form generator matrix of an $[n,k]$-code C is $G = \left[\begin{array}{c|c} I_k & X \end{array}\right]$. Then a parity check matrix for C is $H = \left[\begin{array}{c|c} -X^T & I_{n-k} \end{array}\right]$.*

Definition 1.9. (Cyclic codes) A subset S of $\mathbb{F}_q^n$ is cyclic if $(a_{n-1}, a_0, a_1, ..., a_{n-2}) \in S$ whenever $(a_0, a_1, .., a_{n-1}) \in S$. A linear code C is called a cyclic code if C is a cyclic set .

Example 2. The following code is a cyclic codes:

(i) {000, 111, 101, 110, 011, 100, 001, 010} is binary cyclic code of length 3.

Remark. In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following correspondence :

$$\Lambda : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1),\ (a_0, a_1, ...a_{n-1}) \to a_0 + a_1 x + ... + a_{n-1}x^{n-1} \qquad (1.6)$$

Then Λ is an $\mathbb{F}_q$-linear transformation of vector spaces over $\mathbb{F}_q$.

Example 3. Consider the cyclic code $C = \{000, 111, 101, 110, 011, 100, 001, 010\}$; The $\Lambda(C) = \{0, 1 + x + x^2, 1 + x^2, 1 + x, x + x^2, 1, x^2, x\} \quad \subseteq \quad \mathbb{F}_2[x]/(x^3 - 1)$

Theorem 1.3. *Let Λ be the linear map defined in (2.6) .Then a nonempty subset C of $\mathbb{F}_q^n$ is a cyclic code if and only if $\Lambda(C)$is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$.*

Theorem 1.4. *Let I be a non zero ideal in $\mathbb{F}_q[x]/(x^n - 1)$ and $g(x)$ be a non zero monic polynomial of the least degree in I.Then $g(x)$ is a generator of I and divides $(x^n - 1)$.*

Theorem 1.5. *There is a unique monic polynomial $g(x)$ of the least degree in every non zero ideal I of $\mathbb{F}_q[x]/(x^n - 1)$ then $g(x)$ is the generator of I.*

Definition 1.10. The unique monic polynomial of the least degree of a non zero ideal I of $\mathbb{F}_q[x]/(x^n - 1)$ is called the generator polynomial of I . For a cyclic code C,the generator polynomial of $\Lambda(C)$ is also called the generator polynomial of C.

Theorem 1.6. *let* $(x^n - 1) \in F_q$ *have the factorization*

$$(x^n - 1) = \prod_{i=1}^{r} p_i^{e_i}(x) \tag{1.7}$$

where $p_1(x), p_2(x), ..., p_r(x)$ *are distinct monic irreducible polynomials and* $e_i \geq 1$ *for all i= 1, 2, 3 ..., r . Then there are* $\prod_{i=1}^{r}(e_i + 1)$ *cyclic codes of length n over* F_q.

Definition 1.11. Let $g(x)$ be the generator polynomial of an ideal of $\mathbb{F}_q[x]/(x^n-1)$. Then the corresponding cyclic code has dimension k if the degree of $g(x)$ is $n-k$.

Definition 1.12. Let $g(x) = g_0 + g_1x + ... + g_{n-k}x^{n-k}$ be the generator polynomial of a cyclic code C in F_q^n with $\deg(g(x)) = n - k$. Then the matrix

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

is a generator matrix of C.

1.1 Special Cases of Linear Codes

1.1.1 BCH Codes

The Bose, Chaudhuri and Hocquenghem (BCH) code is the generalization of multiple error correction .

Definition 1.13. let α be a primitive element of F_{q^m} and $M^{(i)}(x)$ be the the minimal polynomial of $\alpha^{(j)}$with respect toF_q. A BCH Code over F_q is a cyclic code of length $n = q^m - 1$ with designed distance δ whose generator polynomial is

the least common multiple of the minimal polynomials of $\alpha^a, \alpha^{a+1}, ..., \alpha^{a+\delta-2}$ where $g(x) := lcm(M^{(a)}(x), M^{(a+1)}(x), ..., M^{(a+\delta-2)}(x))$ for some integer $0 \leq a \leq n-1$. if a=1, the code is called narrow sense.

We state the following properties of BCH-codes without proofs .

Theorem 1.7. *(i) The dimension of a q-ary BCH Code of length $q^m - 1$ generated by $g(x) := lcm(M^{(a)}(x), M^{(a+1)}(x), ..., M^{(a+\delta-2)}(x))$ is independent of the choice of primitive element α.*

(ii) A q ary BCH Code of length $q^m - 1$ with designed distance δ has dimension at least $q^m - 1 - m(\delta - 1)$.

(iii) A BCH Code with designed distance δ has minimum distance at least δ.

1.1.2 BCH Codes in SageMath

In SageMath, BCH codes can be generated using the command

```
C = codes.BCHCode(F, n, delta)
```

where

- $F = \mathrm{GF}(q)$ is the base field,
- n is the code length,
- δ is the designed distance.

For example, the binary BCH code with length 15 and designed distance 5 is generated by

```
F = GF(2)
C = codes.BCHCode(F, 15, 5)
```

The parameters and generator matrix of the code can be obtained using

```
print(C.length())
print(C.dimension())
print(C.minimum_distance())

G = C.generator_matrix()
print(G)
```

The generator polynomial is obtained by

```
g = C.generator_polynomial()
print(g)
```

1.1.3 REED - SOLOMON Codes

The most important subclass of BCH codes is the class of Reed-Solomom (RS) Codes. Consider a BCH Code C of length $q^m - 1$ generated by

$$g(x) := lcm(M^{(a)}(x), M^{(a+1)}(x), ..., M^{(a+\delta-2)}(x))$$

in RS $m = 1$, we obtain a q-ary BCH code C of length $q - 1$.

Definition 1.14. A q-ary Reed Solomon code is a q-ary BCH code of length q - 1 generated by

$$g(x) = lcm(x-\alpha^{a+1})(x-\alpha^{a+2})...(x-\alpha^{a+\delta-1}) = (x-\alpha^{a+1})(x-\alpha^{a+2})...(x-\alpha^{a+\delta-1}) \tag{1.8}$$

since, α^i's are pair wise distinct. with a ≥ 0 and $2 \leq \delta \leq q - 1$, where α is a primitive element of F_q .

We never consider binary RS code as, in this case, the length is $q - 1 = 1$.

We state the following properties of linear codes without proofs.

Theorem 1.8. *Reed-Solomon codes are MDS ; that is q-ary Reed-Solomon code*

of length $q-1$ *generated by* $g(x) = \prod_{i=a+1}^{a+\delta-1}(x-\alpha^i)$ *is a* $[q-1, q-\delta, \delta]$ *-cyclic code for any* $2 \leq \delta \leq q-1$.

Theorem 1.9. *Let* α *be a primitive element of the finite field* $\mathbb{F}_q$*, and let* $q-1 \geq \delta \geq 2$ *. The narrow-sense q-ary RS code with generator polynomial*

$$g(x) = (x-\alpha)(x-\alpha^2)...(x-\alpha^{\delta-1})$$

is equal to

$$\{\big(f(1),\, f(\alpha),\, f(\alpha^2),\, \ldots,\, f(\alpha^{q-2})\big) : f(x) \in \mathbb{F}_q[x] \text{ and } deg(f(x)), q-\delta\}.$$

Corollary 1.10. *Let* α *be a primitive element of* $\mathbb{F}_q$ *, and let* $q-1 \geq \delta \geq 2$ *. The matrix*

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{q-\delta-1} & \alpha^{2(q-\delta-1)} & \cdots & \alpha^{(q-\delta-1)(q-2)} \end{pmatrix}$$

is a generator matrix for the RS code generated by the polynomial

$$g(x) = (x-\alpha)(x-\alpha^2)...(x-\alpha^{\delta-1}).$$

1.1.4 Reed-Solomon Code in Sagemath

```
F = GF(11)
C = codes.ReedSolomonCode(F, 10, 6)
print(C)
G = C.generator_matrix()
print(G)
```

1.1.5 Generalized Reed-Solomon codes

Definition 1.15. Let $n \leq q$. Let $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$, where $\alpha_i (1 \leq i \leq n)$ are distinct elements of $\mathbb{F}_q$ .Let $\mathbf{v} = (v_1, v_2, ..., v_n)$, where$v_i \in \mathbb{F}_q^*$ for all $1 \leq i \leq n$. For $k \leq n$, the generalized Reed-Muller code $GRS_k(\alpha, \mathbf{v})$ is defined to be

$$\{(v_1 f(\alpha_1), v_2 f(\alpha_2), ..., v_n f(\alpha_n)) : f(x) \in \mathbb{F}_q[x] \text{ and } deg(f(x)) < k\}.$$

The elements $\alpha_1, \alpha_2, ..., \alpha_n$ are called the *codelocators* of $GRS_k(\alpha, \mathbf{v})$.

We state the following properties of linear codes without proofs.

Theorem 1.11. *The dual of the generalized Reed-Solomon code $GRS_k(\alpha, \mathbf{v})$ over $\mathbb{F}_q$ of length n is $GRS_k(\alpha, \mathbf{v}')$ for some $v' \in (\mathbb{F}_q^*)^n$.*

Corollary 1.12. *A parity-check matrix of $GRS_k(\alpha, \mathbf{v})$ is*

$$H = \begin{pmatrix} v_1' & v_2' & \cdots & v_n' \\ v_1'\alpha_1 & v_2'\alpha_2 & \cdots & v_n'\alpha_n \\ v_1'\alpha_1^2 & v_2'\alpha_2^2 & \cdots & v_n'\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1'\alpha_1^{n-k-1} & v_2'\alpha_2^{n-k-1} & \cdots & v_n'\alpha_n^{n-k-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix} \begin{pmatrix} v_1' & 0 & \cdots & 0 \\ 0 & v_2' & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & v_n' \end{pmatrix}.$$

1.1.6 GRS-Code in Sagemath

```
F = GF(13)

alpha = F.list()[:8]
```

```
v = [F(1)]*8
C = codes.GeneralizedReedSolomonCode(alpha, 5, v)
print(C)
G = C.generator_matrix()
print(G)
```

1.1.7 MDS Codes

A linear code with parameter $[n, k, d]$ such that $k + d = n + 1$ is called Maximum Distance Separable (MDS) codes.

Theorem 1.13. *Let C be a linear code over $\mathbb{F}_q$ with parameter $[n, k, d]$. Let G and H are generator matrix and parity check matrix for C. Then the following are equivalent :*

(i) C is an MDS Code.

(ii) Every set of $n - k$ columns of H is linearly dependent.

(iii) Every set of k columns of G is linearly independent.

(iv) $C^{\perp}$ is an MDS Code.

Theorem 1.14. *The generalized RS code $GRS_k(\alpha, \mathbf{v})$ has parameters $[n, k, n - k + 1]$, so it is an MDS code.*

1.1.8 Reed - Muller Codes

Reed - Muller Codes are among the oldest kmown codes and have widespread applications. For each positive integer m and each integer r satisfying $0 \leq r \leq m$, there is an rth order Reed - Muller code R(r, m),, which is a binary linear code of parameters $\left[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}\right]$.

Definition 1.16. The (first order) Reed-Muller codes R$(1, m)$ are binary codes defined, for all integers m ≥ 1, recursively as follows:

(i) $\mathrm{R}(1,1) = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$;

(ii) For m ≥ 1, $\mathrm{R}(1, m+1) = \{(u, u) : u \in \mathrm{R}(1, m)\} \cup \{(u, u+1) : u \in \mathrm{R}(1, m)\}$.

Definition 1.17. For m ≥ 1, the Reed Muller code $\mathrm{R}(1, m)$ is a binary $[2^m, m+1, 2^{m-1}]$ - linear code, in which every codeword except 0 and 1 has weight 2^{m-1}.

Definition 1.18. (i) The generator matrix of $\mathrm{R}(1,1)$ is $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

(ii) If G_m is a generator matrix for $\mathrm{R}(1, m)$, then the generator matrix for $\mathrm{R}(1, m+1)$ is $G_m = \begin{bmatrix} G_m & G_m \\ 0...0 & 1...1 \end{bmatrix}$.

Definition 1.19. (i) The zeroth order Reed Muller codes $\mathrm{R}(0, m)$, for $m \geq 0$, are defined to be the repetition codes {0,1} of length 2^m .

(ii) For any r $\geq$ 2, the rth order Reed Muller codes $\mathrm{R}(r, m)$ are defined, m $\geq r-1$, recursively by

$$\mathrm{R}(r, m+1) = \begin{cases} \mathbb{F}_2^{2^r} & \text{if } m = r-1, \\ \{(u, u+v) \mid u \in R(r, m),\ v \in R(r-1, m)\}, & \text{if } m > r-1. \end{cases}$$

1.1.9 RM-Code in Sagemath

```
F = GF(2)
C = codes.ReedMullerCode(F, 1, 3)
print(C)
G = C.generator_matrix()
print(G)
```

1.1.10 Quadratic-residue Codes

Definition 1.20. Let p and l be two distinct primes such that l is a quadratic residue modulo p . Choose an integer $m \geq 1$ such that $l^m - 1$ is divisible by p.

Let θ be a primitive element of $\mathbb{F}_{l^m}$ and put $\alpha = \theta^{(l^m-1)/p}$. The divisors of $x^p - 1$

$$g_Q(x) := \prod_{r \in Q_p} (x - \alpha^r), \qquad g_N(x) := \prod_{n \in N_p} (x - \alpha^n).$$

are defined over $\mathbb{F}_l$. Q_p and N_p are the set of non zero quadratic residues and quadratic non residues modulo p . The l-ary cyclic codes $C_Q =< g_Q(x) >$ *and* $C_N =< g_N(x) >$ of length p are called quadratic residue codes(QR).

Remark. The two l-ary quadratic residue codes C_Q *and* C_N are equivalent and the dimension is $p - (p-1)/2 = (p+1)/2$.

1.1.11 QR-Code in Sagemath

```
F = GF(2)
C = codes.QuadraticResidueCode(23,F)
print(C)
G = C.generator_matrix()
print(G)
```

Chapter 2

LATTICES FROM CODES

In this chapter , we discuss the definition of lattices and q-ary lattices . Explain construction A method for constructing lattices from codes and conclude with an example illustrating the construction.

2.1 Lattices

Lattices are the discrete additive subgroups of $\mathbb{R}^m$. It is the set of vectors consisting of integer linear combination of independent vectors .[3]

Definition 2.1. Let $b_1, b_2, ..., b_n$ be linearly independent vectors in $\mathbb{R}^m$. A lattice $\mathbf{L}(\mathbf{B})$ with basis $\{b_1, b_2, ..., b_n\}$ is defined as

$$\mathbf{L}(\mathbf{B}) = \{x_1 b_1 + x_2 b_2 + \cdots + x_n b_n \mid x_i \in \mathbb{Z}\} \tag{2.1}$$

The integer n is called rank of $\mathbf{L}(\mathbf{B})$. If $m = n$, we say that $\mathbf{L}(\mathbf{B})$ is full rank .

Definition 2.2. A generator matrix $\mathbf{B}$ for a lattice $\mathbf{L}(\mathbf{B})$ is matrix whose rows

are a basis for it .

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \tag{2.2}$$

A vector $v = (v_1, v_2, ..., v_m) \in \mathbb{R}^m$ is in $\mathbf{L}(\mathbf{B})$ if and only if it can be written as

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}, x_i \in \mathbb{Z}$$

in other words,

$$\mathbf{L}(\mathbf{B}) = \{\mathbf{xB} : \mathbf{x} \in \mathbb{Z}^n\}$$

Definition 2.3. (**Integer Lattice**) An integer lattice is a lattice with all of whose vectors have integer coordinates. An integer lattice is an additive subgroup of $\mathbb{Z}^n$ for some $n \geq 1$.

Definition 2.4. (**q-ary Lattice**) A q-ary lattice is a lattice $\mathbf{L}(\mathbf{B})$ satisfying $q\mathbb{Z}^m \subseteq \mathbf{L}(\mathbf{B}) \subseteq \mathbb{Z}^m$, where q is a positive integer.

Remark. We use the method construction A for creating lattice in $\mathbb{R}^m$ from a linear code in $\mathbb{Z}_q^m$ which lattices are called q-ary lattices .

A linear code C in $\mathbb{Z}_q^m$ is by definition a subset which is an additive subgroup of $\mathbb{Z}_q^m$. If q = p , a linear code C is a subspace of dimension k of vector space $\mathbb{Z}_p^m$.

2.2 Connection between linear codes in $\mathbb{Z}_q^m$ and lattices

Define a map :

$$\rho : \mathbb{Z} \to \mathbb{Z}_q \ ; \ v \to v \pmod{q}$$

$$\rho^{-1}(a) = \{\, a + bq \mid b \in \mathbb{Z} \,\} \tag{2.3}$$

$\rho^{-1}(a)$ is the set of integers that are mapped to a by ρ .

Now consider cartesian product of integers modulo q .

$$\rho : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_q \times \mathbb{Z}_q \ ;$$

$$(v_1, v_2) \mapsto (v_1 \mod q, v_2 \mod q)$$

then $\rho^{-1}(a_1, a_2)$ is the 2 dimensional vectors with integer entries that is mapped to a_1, a_2 by ρ .

So , the map ρ can be defined component wise over an arbitrary number m to $\mathbb{Z}_q$:

$$\rho : \mathbb{Z}^m \to \mathbb{Z}_q^m \tag{2.4}$$

$$(v_1, v_2, \ldots, v_m) \mapsto (v_1 \bmod q, \ldots, v_m \bmod q)$$

Remark. Let $\mathbf{S}$ be an arbitrary subset of $\mathbb{Z}_q^m$. By computing $\rho^{-1}(S)$ it is more interesting to start with S a subset has a structure and to understand how this structure carried over $\rho^{-1}(S)$.[2]

Proposition 2.1. Given a subset $\mathbf{S} \subset \mathbb{Z}_q^m$, then $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^m$ if and only if $\mathbf{S}$ is a linear code in $\mathbb{Z}_q^m$.

Proof. Suppose $\mathbf{S} \subset \mathbb{Z}_q^m$ is a linear code .we need to show that $\rho^{-1}(S)$ is a lattice . $\rho^{-1}(S)$ is a discrete addictive subgroup of $\mathbb{R}^m$. So $\rho^{-1}(S) \subset \mathbb{Z}^m$ so it is a discrete subset of $\mathbb{R}^m$. Now we have to show that it is an additive subgroup of $\mathbb{R}^m$. Let

$\mathbf{x}, \mathbf{y} \in \rho^{-1}(S)$ for closure under addition , show that $\mathbf{x}+\mathbf{y} \in \rho^{-1}(S)$, So it is enough to show that

$$\rho(\mathbf{x}+\mathbf{y}) \in (S).$$

$$\rho(\mathbf{x}+\mathbf{y}) = \rho(x_1+y_1, \ldots, x_m+y_m) = (x_1+y_1 \bmod q, \ldots, x_m+y_m \bmod q) =$$

$$(x_1 \bmod q, \ldots, x_m \bmod q) + (y_1 \bmod q, \ldots, y_m \bmod q) = \rho(x)+\rho(y)$$

Since $\mathbf{x}, \mathbf{y} \in \rho^{-1}(\mathbf{S})$ then $\rho(x)$ and $\rho(y)$ are codewords . we know that linear codes are additive subgroup , then $\rho(\mathbf{x}+\mathbf{y}) \in (S)$. Since $0 \in \mathbb{Z}_q^m$ *then* $0 \in$ *of* $\rho^{-1}(S) \in \mathbb{Z}^m$ and also $\mathbf{x} \in \rho^{-1}(S)$ *then* $-x \in \rho^{-1}(S)$. Therefore , $\rho^{-1}(S)$ is a discrete additive subgroup of $\mathbb{R}^m$.

Conversely , Let $\rho^{-1}(S)$ is a lattice . We have to show that $\mathbf{S}$ is a linear code in $\mathbb{Z}_q^m$.that is ; $\mathbf{S}$ is a additive group in $\mathbb{Z}_q^m$. Let $\rho(x)$ and $\rho(y) \in \mathbf{S}$ we need to show that $\rho(x+y) \in \mathbf{S}$ so we know that $\rho^{-1}(S)$ is a discrete additive subgroup of $\mathbb{Z}_q^m$. So $\rho^{-1}(x+y) \in \mathbb{Z}^m$ then $\rho(x+y) \in \mathbf{S}$, then by definition itself we can say that $\mathbf{S}$ is a linear code of $\mathbb{Z}_q^m$. □

Definition 2.5. Let C be a linear code in $\mathbb{Z}_q^m$ the integers modulo a positive integer $q \geq 2$, where q is either prime or composite . Let $\rho : \mathbb{Z}^m \to \mathbb{Z}_q^m$ be the component wise reduction modulo q. Then the lattice $\mathbf{L}(\mathbf{C}) = \rho^{-1}(C)$ is said to have been obtained via Construction A .

Remark. (a) If C be a linear code in $\mathbb{Z}_p^m$ with dimension k, then the generator matrix of standard form ,

$$G = \left[\begin{array}{c|c} I_k & A \end{array}\right]$$

where $\mathbf{I_k}$ is the k-dimensional identity matrix and A is the $k \times (m-k)$ matrix

(b) If C be a linear code in $\mathbb{Z}_q^m$. We also have generator matrix which contain vectors that generate C, however these vectors do not always form a basis and we may not have a generator matrix of standard form .

2.2.1 Generator Matrix of A Lattice $L(C)$

Let C be a linear code , then each codeword $a \in C$ can be written using a set of generator ,

$$a = \sum_{i=1}^{\ell} a_i v_i, \qquad v_i = (v_{i1}, \ldots, v_{im}), \quad i = 1, \ldots, \ell$$

Now,

$$a = \sum_{i=1}^{\ell} a_i v_i \in C \iff \rho^{-1}(a) = \sum_{i=1}^{\ell} a_i v_i + \sum_{i=1}^{m} q h_i e_i \in \mathbb{R}^m \tag{2.5}$$

where $0 \leq a_i, v_{ij} \leq n-1$ **for all** $i, j, e_i, i = 1, 2, ...m$ form the canonical basis of $\mathbb{R}^m and\ h_1, ..., h_m \in \mathbb{Z}$. In other words , $\rho^{-1}(a)$ is an integral linear combination of $\mathbf{v_1}, ...\mathbf{v_l}, \mathbf{qe_1}, ..., \mathbf{qe_m}$.

2.2.2 Hermite Normal Form

Definition 2.6. Column-HNF An integer matrix of full row rank is in column-HNF if it is of the form $[H\,\mathbf{0}]$ where $H = (h_{ij})$ is a square matrix and

(i) H is a lower triangular matrix, i.e. $h_{i,j} = 0$ if $i < j$.

(ii) $h_{ii} > 0$ for every i.

(iii) $0 \leq h_{ji} < h_{ii}$ for $j < i$.

Definition 2.7. Row-HNF An integer matrix of full rank is in Row-HNF if it is of the form $\begin{bmatrix} H \\ 0 \end{bmatrix}$ where $H = (h_{ij})$ is a square matrix and

(i) H is an upper triangular matrix, i.e. $h_{i,j} = 0$ if $i > j$.

(ii) $h_{ii} > 0$ for every i.

(iii) $0 \leq h_{ij} < h_{ii}$ for $j > i$.

Lemma 2.1. *For any lattice* $\mathbf{L} \subset \mathbb{Z}^m$ *,there exist a unique basis* H *in HNF . We call* H *the HNF basis for* $\mathbf{L}$.

Proposition 2.2. Let $v_1, ..., v_l$ be generators for the linear code C over $\mathbb{Z}_q$ and $e_1..., e_m$ be the canonical basis of $\mathbb{R}^m$. Then a generator matrix for the lattice $\rho^{-1}(C)$ is given by the $m \times m$ full rank matrix H obtained by computing the Hermite normal form of $\begin{bmatrix} H \\ 0 \end{bmatrix}$ of $[v_1, ..., v_l, qe_1, ..., qe_m]^T$. If the generator matrix of C can be put in stantard form

$$G = \left[\begin{array}{c|c} I_k & A \end{array} \right]$$

(if $q = p$ then $l = k$) ,then a generator matrix of $\mathbf{L}(\mathbf{C})$ is

$$H = \begin{bmatrix} I_l & A \\ 0_{(m-l)\times l} & qI_{m-l} \end{bmatrix} \tag{2.6}$$

Proof. We know that we can generate a lattice from $v_1, ..., v_l, qe_1, ..., qe_m$. So we have to find a basis by Hermite normal form out of $(m + l) \times m$ matrix

$$[v_1, ..., v_l, qe_1, ..., qe_m]^T$$

which look like

$$\begin{bmatrix} H \\ 0 \end{bmatrix}$$

, and clearly contain a basis . In case C has a generator matrix in standard form ,then we need to compute a Hermite normal form out of

$$\begin{bmatrix} I_l & A \\ qI_l & 0_{l\times(m-l)} \\ 0_{(m-l)\times l} & qI_{m-l} \end{bmatrix}$$

Multiply first l columns by $-q$ and adding them to the next l columns gives

$$\begin{bmatrix} I_l & A \\ 0_l & -qA \\ 0_{(m-l)\times l} & qI_{m-l} \end{bmatrix}$$

then for eliminating $-q$A (Every entry of $-q$A is divisible by q, rows of qI_{m-l} can cancel them) this gives:

$$\begin{bmatrix} I_l & A \\ 0_{(m-l)\times l} & qI_{m-l} \end{bmatrix}$$

□

Example 4. Find the generator matrix for a lattice $L(C)$ created from a Binary $[7, 4]$ cyclic code C with generator polynomial $g(x) = 1 + x^2 + x^3$.

The generator matrix of this code C is ,

$$\begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ x^3g(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

then the standard matrix is ,

$$G = \left[\begin{array}{c|c} I_k & A \end{array}\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Then,

$$[v_1, ..., v_l, qe_1, ..., qe_m]^T = \begin{bmatrix} I_4 & A \\ 2I_4 & 0_{4\times 3} \\ 0_{3\times 4} & 2I_3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

then by eliminating columns; we get ,

$$H = \begin{bmatrix} I_4 & A \\ 0_{3\times 4} & 2I_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

H is the generator matrix of the lattice generated from the binary-$[7, 4]$ cyclic code.

Chapter 3

Ideal Lattices and Cyclic Lattices

In this chapter, we discuss about the Ideal lattices which are lattices associated with ideals in a polynomial quotient ring. Also presents the Incomplete Hermite Normal Form (IHNF) and the fundamental lemmas used to characterize when a lattice is an ideal lattice. This chapter also defines cyclic lattices and explains the peculiarity of lattices generated from cyclic codes.

3.1 Ideal lattices

3.1.1 Coefficient embedding ideal lattice

Denote by $\mathbb{Z}^{(n)}[x]$ the set of all the polynomials in $\mathbb{Z}[x]$ with degree $\leq n-1$. We use σ to represent the following linear map :

$$\sigma : \mathbb{Z}^{(n)}[x] \to \mathbb{Z}^n$$

$$\Sigma_{i=1}^{n} a_i x^{i-1} \mapsto (a_1, ..., a_n)$$

We can also define its inverse also which is linear too:

$$\sigma^{-1} : \mathbb{Z}^n \to \mathbb{Z}^{(n)}[x] \tag{3.1}$$

$$(a_1, ..., a_n) \mapsto \Sigma_{i=1}^{n} a_i x^{i-1}$$

We focus on ideal lattice induced by ideals of the ring $\mathbb{Z}[x]/f(x)$, where $f(x)$ is a monic polynomial of degree n . Any element in $\mathbb{Z}^{(n)}[x]$ can be viewed as a representative in the ring $\mathbb{Z}[x]/f(x)$ with $degree(f(x) \geq n$. So we use σ to represent the following coefficient embedding .

$$\sigma : \mathbb{Z}[x]/f(x) \to \mathbb{Z}^n \tag{3.2}$$

$$\Sigma_{i=1}^{n} a_i x^{i-1} \to (a_1, ..., a_n)$$

So, under coefficient embedding, any ideal of $\mathbb{Z}[x]/f(x)$ can be viewed as an integer lattice .

Definition 3.1. (*Coefficient embedding ideal lattice*) Given $\mathbb{Z}[x]/f(x)$, where $f(x)$ is a monic polynomial of degree n, and any ideal I of $\mathbb{Z}[x]/f(x)$, $\sigma(I)$ is called Coefficient embedding ideal lattice, which is an integer lattice.[1]

Lemma 3.1. *For any integer matrix A, there exists a uni-modular matrix U such that $H = UA$ is in HNF .*

Lemma 3.2. *For any lattice $L \subset \mathbb{Z}^n$, there exist a unique basis H in HNF. We call H the HNF basis of L*

Definition 3.2. (Incomplete Hermite Normal Form) A non-singular matrix $B \in \mathbb{Z}^{n \times n}$ is said to be in Incomplete Normal Form, if

i $b_{n,n} > 0$

ii $b_{i,n} = 0$ for $1 \leq i \leq n-1$

Given a full-rank integer matrix B,

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

it is well-known that by the Extended Euclidean Algorithm we can find a uni-modular matrix U, such that

$$U \begin{bmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{nn} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ d \end{bmatrix}$$

where $d = \gcd(b_{1n}, b_{2n}, ..., b_{nn})$. Then we have

$$B' = UB = \begin{bmatrix} D & 0 \\ b' & d \end{bmatrix}$$

is in Incomplete Hermite Normal Form, where $D \in \mathbb{Z}^{(n-1)\times(n-1)}$, $b' \in \mathbb{Z}^{(n-1)}$

By Incomplete Hermite Normal Form, it is easy to conclude the following lemma .

Lemma 3.3. *For any non-singular matrix $B \in \mathbb{Z}^{n\times n}$, the following properties are satisfied:*

1. *We can find a uni-modular matrix U in polynomial time, such that $B' = UB$ is in Incomplete Hermite Normal Form.*

2. *For any uni-modular matrix U and V such that $B' = UB$ and $B'' = VB$ both in Incomplete Hermite Normal Form, B' and B'' are not necessarily*

equal, but

$$b'_{nn} = b''_{nn} = \gcd(b_{1,n}, b_{2,n}, ..., b_{n,n}).$$

Specially, notice that the HNF $\mathbf{H}$ *of* B *is also in Incomplete Hermite Normal Form. We immediately have*

$$h_{nn} = \gcd(b_{1n}, b_{2n}, ..., b_{nn})$$

Lemma 3.4. *Let* $\mathbf{H}$ *be the HNF basis of the full rank coefficient embedding ideal lattice* $L(B)$ *in the ring* $\mathbb{Z}[x]/f(x)$.

$$H = \begin{bmatrix} h_{1,1} & 0 & 0 & \cdots & 0 \\ h_{2,1} & h_{2,2} & 0 & \cdots & 0 \\ h_{3,1} & h_{3,2} & h_{3,3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n,1} & h_{n,2} & h_{n,3} & \cdots & h_{n,n} \end{bmatrix}$$

Then $h_{i,i}|h_{j,l},\ for 1 \leq l \leq j \leq i \leq n$. *specially,* $h_{n,n}|h_{i,j}, i, j \leq n$.

Proof. We prove this by mathematical induction on i,

if i=1 $h_{i,i}|h_{i,i} = h_{1,1}|h_{1,1}$, it is trivial.

Assume that result holds for $i \leq k \leq n-1$. So, we have to prove for i=k+1 , $h_{i,i}|h_{i,i} = h_{k+1,k+1}|h_{j,l}$ where $1 \leq l \leq j \leq k+1 \leq n$.

Let h_i be the row of $\mathbf{H}$. Note that for any ideal I of $\mathbb{Z}[x]/f(x)$ and for all $g(x)$ $\in I,\ xg(x) \in I$.

Specially $x\sigma^{-1}(h_k) \in I$, where σ is the coefficient embedding. Since $\mathbf{H}$ is a basis of ideal lattice, it is very simple to imply that there must exist $y_i \in \mathbb{Z}$, for all i= 1,2,...,k+1 such that:

$$x\sigma^{-1}(h_k) = (0, h_{k,1}, h_{k,2}, ..., h_{k,k}, 0, 0, ...) = \Sigma_{i=1}^{k+1} y_i h_i$$

Hence, compare the coordinates and terms;

$$\begin{aligned} h_{k,k} &= y_{k+1} h_{k+1,k+1} \\ h_{k,k-1} &= y_k h_{k,k} + y_{k+1} h_{k+1,k} \\ &\vdots \\ h_{k,1} &= \sum_{i=2}^{k+1} y_i h_{i,2} \\ 0 &= \sum_{i=1}^{k+1} y_i h_{i,1} \end{aligned}$$

From this, we get $y_{k+1} = \frac{h_{k,k}}{h_{k+1,k+1}} \in \mathbb{Z}$,and

$$\begin{aligned} h_{k+1,k} &= \frac{h_{k,k-1} - y_k h_{k,k}}{h_{k,k}} h_{k+1,k+1} \\ h_{k+1,k-1} &= \frac{h_{k,k-2} - y_{k-1} h_{k-1,k-1} - y_k h_{k,k-1}}{h_{k,k}} h_{k+1,k+1} \\ &\vdots \\ h_{k+1,2} &= \frac{h_{k,1} - \sum_{i=2}^{k} y_i h_{i,2}}{h_{k,k}} h_{k+1,k+1} \\ h_{k+1,1} &= \frac{-\sum_{i=1}^{k} y_i h_{i,1}}{h_{k,k}} h_{k+1,k+1} \end{aligned}$$

From this induction hypothesis, we have $h_{k,k} | h_{j,l}$ for $1 \leq l \leq j \leq k \leq n$. So, the co efficient of $h_{k+1,k+1}$ in each equations is in fact an integer . Therefore, $h_{k+1,k+1} | h_{k+1,l}$, $1 \leq l \leq k+1$. Since, $h_{k+1,k+1} | h_{k,k}$, we know $h_{k+1,k+1} | h_{j,l}$, where $1 \leq l \leq j \leq k+1 \leq n$. Then the result holds foe $i = k+1$.

By induction , $h_{i,i} | h_{j,l}$, $for 1 \leq l \leq j \leq i \leq n$. specially, $h_{n,n} | h_{i,j}, i, j \leq n$. □

Now , we show an easy way to find a given lattice is a coefficient embedding ideal lattice or not in $\mathbb{Z}[x]/f(x)$.

Lemma 3.5. *For any monic polynomial $f(x) \in \mathbb{Z}[x]$ with degree n, a lattice $L(B)$ with any basis B is a coefficient-embedding ideal lattice in $\mathbb{Z}[x]/f(x)$ if and only if $\sigma(x\sigma^{-1}(b_i) \mod f(x)) \in L(B)$ for i=1,2,...,n, where b_i is the i^{th} row vector of*

B, and $\sigma : \mathbb{Z}[x]/f(x) \to \mathbb{Z}^n$.

Proof. If $L(B)$ is a coefficient embedding ideal lattice in $\mathbb{Z}[x]/f(x)$, Then $\sigma^{-1}(b_i) = b_{i,1}, b_{i,2}x, ..., b_{i,n}x^{n-1}$,i=1,2,...,n. are in the corresponding ideal .By the property of ideal, it is obvious that $x\sigma^{-1}(b_i) \mod f(x) \in I$, *then* $\sigma(x\sigma^{-1}(b_i) \mod f(x)) \in \sigma(I) \in L(B)$.

Conversely, Assume that there exist a monic polynomial $f(x) \in \mathbb{Z}[x]$ with degree n, such that $\sigma(x\sigma^{-1}(b_i) \mod f(x)) \in \sigma(I) \in L(B)$ for i= 1,2,...,n. We have to show that $\sigma^{-1}(L(B))$ must be an ideal lattice in $\mathbb{Z}[x]/f(x)$.

So, first we have to show that $\sigma^{-1}(L(B))$ is an additive group, we know that σ is an additive homomorphism. Since, for any $p(x), q(x) \in \mathbb{Z}[x]/f(x)$, $\sigma(p(x) + q(x)) = \sigma(p(x)) + \sigma(q(x))$. So $\sigma^{-1}(L(B))$ is an additive group.

Since, $\sigma(x\sigma^{-1}(b_i) \mod f(x)) \in \sigma(I) \in L(B)$,then for any vector $\mathbf{v} = \sum_{i=1}^{n} z_i b_i \in \mathbb{Z}$, we have

$$\sigma(x\sigma^{-1}(v) \mod f(x)) = \sum_{i=1}^{n} z_i \sigma(x\sigma^{-1}(b_i) \mod f(x)) \in \sigma(I) \in L(B)$$

Apply this result on the lattice vector $\sigma(x^2\sigma^{-1}(v) \mod f(x))$,

We will have

$$\sigma(x^2\sigma^{-1}(v)) = \sigma(x\sigma^{-1}(\sigma(xv \mod f(x)))) \in L(B)$$

Hence, for any positive integer k, we know that

$$\sigma(x^2\sigma^{-1}(v) \in L(B)$$

Then for any $g(x) = \sum_{i=1}^{n} g_i x^{i-1} \in \mathbb{Z}[x]/f(x)$ any lattice vector $\mathbf{v}$,

$$\sigma(g(x)\sigma^{-1}(v) \mod f(x)) = \sum_{i=1}^{n} g_i \sigma(x^{i-1}\sigma^{-1}(v) \mod f(x)) \in L(B).$$

So, $\sigma^{-1}(L(B))$ is an ideal lattice in $\mathbb{Z}[x]/f(x)$. □

Theorem 3.6. *Given a full rank integer lattice $L(B)$, let* $B' = \begin{bmatrix} D & 0 \\ b' & b'_{n,n} \end{bmatrix}$ *be any Incomplete Hermite Normal form of B. Then $L(B)$ is an ideal lattice if and only if there exist a* $\mathbf{T} \in \mathbb{Z}^{(n-1)\times n}$, *so that* $(\mathbf{0}\ \mathbf{D}) = \mathbf{TB}$. *Specially , if $L(B)$ is an ideal lattice, then taking any* $g(x) = x^n + g_n x^{n-1} + \cdots + g_1$ *with* $(g_1, g_2, ...g_n) \in \frac{1}{b'_{n,n}}((0\ \mathbf{b}') + L(B))$, *$L(B)$ is also an ideal lattice in the ring* $\mathbb{Z}[x]/g(x)$.

Proof. Assume that $L(B)$ is an ideal lattice in $\mathbb{Z}[x]/g(x)$. $g(x)$ is the monic polynomial of $\mathbb{Z}[x]$ with degree n.

By lemma 3.5, $\sigma(x\sigma^{-1}(b'_i) \mod g(x)) \in L(B)$, $1 \le i \le n$.

Let $\begin{bmatrix} D & 0 \\ b' & b'_{n,n} \end{bmatrix}$ be the IHNF of B.

For each $i = 1, 2, ..., n-1$, the i th row of B' is $b'_i = (D_i\ 0)$.

D_i is the i th row of D, Then $\sigma(x\sigma^{-1}(b'_i)) = (D_i\ 0) \in L(B)$.

We know that $L(B) = \{xB : x \in \mathbb{Z}^{1\times n}\}$,

then there exist a row vector $t_i \in \mathbb{Z}^{1\times n}$ *such that* $t_i B = (0\ D_i)$, $1 \le i \le n-1$

$$T = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-2} \\ t_{n-1} \end{bmatrix} \in \mathbb{Z}^{n-1\times n}$$

Then ,

$$TB = \begin{bmatrix} t_1B \\ t_2B \\ \vdots \\ t_{n-2}B \\ t_{n-1}B \end{bmatrix} = \begin{bmatrix} 0 & D_1 \\ 0 & D_2 \\ \vdots & \\ 0 & D_{n-2} \\ 0 & D_{n-1} \end{bmatrix} = (0\ D)$$

$$(0\ \ \mathrm{D}) = \mathrm{TB}\ ,\ \text{Where}\ T \in \mathbb{Z}^{n-1\times n}.$$

Conversely, Assume that there exist a $T \in \mathbb{Z}^{n-1\times n}$ such that $(0\ D) = TB$ where $B' = \begin{bmatrix} D & 0 \\ b' & b'_{n,n} \end{bmatrix}$ be any Incomplete Hermite Normal form of B.

claim: $L(B)$ is an ideal lattice in $\mathbb{Z}[x]/g(x)$. that is, $\sigma(x\sigma^{-1}(b'_i) \mod g(x)) \in L(B)\ ,\ 1 \le i \le n$.

Consider first $n-1$ rows

$$[D\ 0] = B'_i\ ,\ 1 \le i \le n-1$$

Hence,

$$\sigma(x\sigma^{-1}(b'_i)) = (0\ D_i)$$

$$(0\ D) \in L(B)$$

For last row ,

$$b'_n = [b'\ b'_{n,n}]$$

claim: $\sigma(x\sigma^{-1}(b'_n) \mod g(x)) \in L(B)$

Let

$$g(x) = x^n + g_n x^{n-1} + \cdots + g_1$$
$$x^n = -g_1 - g_2 x - ... - g_n x^{n-1}$$

$$\sigma^{-1}(b'_n) = b_{n,1} + b_{n,2}x + ... + b'_{n,n}x^{n-1}$$
$$x\sigma^{-1}(b'_i) = b_{n,1}x + b_{n,2}x^2 + ... + b'_{n,n}x^n$$
$$= b_{n,1}x + b_{n,2}x^2 + ... + b_{n,n}(-g_1 - g_2 x - ... - g_n x^{n-1})$$

Then,

$$\sigma(x\sigma^{-1}(b'_n) \mod g(x)) = (-b'_{n,n}g_1, (b_{n,1} - b'_{n,n}g_2), ..., (b_{n.n-1} - b'_{n,n}g_n))$$
$$= (0\ b') - b'_{n,n}(g_1, g_2, ..., g_n) \in L(B)$$

Here,

$$(g_1, g_2, ..., g_n) \in \frac{1}{b'_{n,n}}((0\ b') + L(B)).$$

Therefore, $L(B)$ is an ideal lattice. □

3.2 Cyclic Lattices

Definition 3.3. A Lattice $L(B)$ is called a cyclic lattice if $\sigma(L(B)) = L(B)$, Where $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ is the cyclic shift operator defined by

$$\sigma(a_0, a_1, ..., a_{n-1}) = (a_{n-1}, a_0, ..., a_{n-2}).$$

Theorem 3.7. *Suppose C is a cyclic code in $\mathbb{F}_q^n$. Let $L(C)$ be the lattice obtained using **construction A** then $L(C)$ is a cyclic lattice.*

Proof. Suppose C is a cyclic code in $\mathbb{F}_q^n$. $L(C)$ is defined as,

$$L(C) = \{x \in \mathbb{Z}^n | x \mod q \in C\}$$

Let

$$\sigma : \mathbb{Z}^n \to \mathbb{Z}^n$$

$$\sigma((a_0, a_1, ..., a_{n-1})) = (a_{n-1}, a_0, ..., a_{n-2})$$

Since C is a cyclic code, then $\sigma(C) = C$. If $x \in L(C)$ then $\rho(x) \in C$.

Therefore, $\sigma(\rho(x)) \in C$

$$\begin{aligned}\sigma(\rho(x)) &= \sigma(a_0 \mod q, a_1 \mod q, ..., a_{n-1} \mod q) \\ &= (a_{n-1} \mod q, a_0 \mod q, ..., a_{n-2} \mod q) \\ &= \rho(a_{n-1}, a_0, ..., a_{n-2}) \\ &= \rho(\sigma(x))\end{aligned}$$

that is, $\rho(\sigma(x)) \in C$

which implies that, $\sigma(x) \in L(C)$

$L(C)$ is a cyclic lattice. □

Conclusion

This project presented a study of linear error-correcting codes, lattices, and their relationship through **Construction A**. It introduced the fundamental concepts of linear and cyclic codes, including generator matrices, parity-check matrices, code parameters, and generator polynomials.

The project examined **Construction A** as a fundamental method for constructing lattices from linear codes. The construction process and the associated generator matrix demonstrated how the algebraic structure of linear codes gives rise to integer lattices.

The study further focused on ideal lattices and their characterization using factor group of ring of polynomials. It examined the role of Hermite Normal Form (HNF) and Incomplete Hermite Normal Form (IHNF) in identifying ideal lattices and introduced cyclic lattices together with their relationship to cyclic codes.

Overall, this project highlights the progression from linear codes to lattice constructions and finally to ideal and cyclic lattices. These lattices have important applications in secure communication, information processing, and lattice-based cryptography, particularly in post-quantum encryption, digital signatures, and key establishment protocols.

References

[1] Yihang Cheng, Yansong Feng, and Yanbin Pan. "Embedding Integer Lattices as Ideals into Polynomial Rings". In: *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation (ISSAC '24)*. New York, NY, USA: Association for Computing Machinery (ACM), 2024, pp. 170–179.

[2] Sueli I. R. Costa et al. *Lattices Applied to Coding for Reliable and Secure Communications*. 1st ed. SpringerBriefs in Mathematics. Cham, Switzerland: Springer, 2017.

[3] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. 2nd ed. Undergraduate Texts in Mathematics. New York: Springer, 2014.

[4] San Ling and Chaoping Xing. *Coding Theory: A First Course*. Cambridge University Press, 2004.

[5] M. Thamban Nair and Arindama Singh. *Linear Algebra*. Singapore: Springer, 2018.