Lee 距離に基づく 2 次元格子上の誤り訂正符号

森田啓義

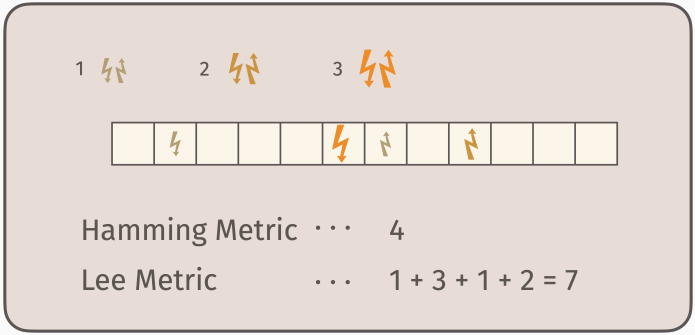
2021 年 3 月 5 日

電気通信大学大学院情報理工学研究科

Table of contents

Introduction

Symbols Errors in the Hamming/Lee Metrics



In case of $q = 17, n = 12, i = 4$ where q is the alphabet size, n is the length of word over $\mathbb{Z}_q$, i.e., *the ring of integer residues modulo* q, and i is the number of error locations:

# errors/$\binom{12}{4}$	Hamming metric	Lee metric
	65,536	1120

note: max. Lee metric is 8 for $q = 17$

Comments on the table in the previous slide

The vol. of a Hamming Sphere of radius t in $\mathbb{Z}_q^n$: [1]

$$V_{Hamming}(n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

$q = 17, i = 4,$ and $t = 8.$

$$\Rightarrow \quad (17-1)^4 = 65536$$

The vol. of a Lee Sphere of radius t in $\mathbb{Z}_q^n$: [2, 3]

$$V_{Lee}(n,t) = \sum_{i=0}^{n} 2^i \binom{n}{i} \binom{t}{i}$$

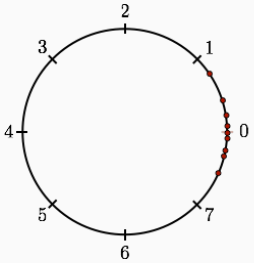
$$\Rightarrow \quad 2^4 \binom{8}{4} = 1120$$

Applications of Codes with the Lee Metric

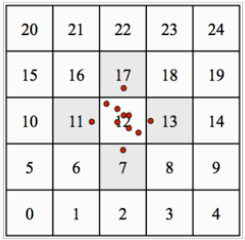
- coded modulations (PSK, QAM) [4, 5]
- peak-shift problems [6, 7, 8, 9, 10]
- insertion-deletion errors [9, 10]
- Rank modulation for Flash-memory [11, 12]
- DNA-Based Storage [13], etc.

Nearest Neighbor Errors on the Constellations

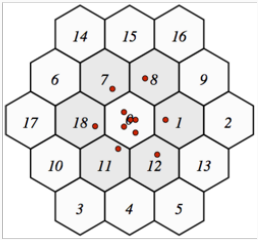
In the literature, M.[5, 14, 15, 16]



Circle Constellation



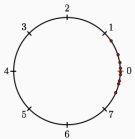
Square Constellation

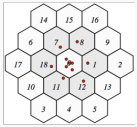


Hexagonal Constellation

- Nearest (and more) Neighbor Errors = Lee-Errors

Comparison on Codes assoc. with 3 Const.





$E_1 = \{\pm 1\} = \{1, \alpha^n\}$

$$H_1 = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \cdots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \cdots & \alpha^{5(n-1)} \end{pmatrix}$$

where α is a primitive element of $GF(q)$ for $q = 2n + 1$. [17, 9, 3]

$E_2 = \{\pm 1, \pm\alpha^n\}$

$$H_2 = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^5 & \cdots & \alpha^{5(n-1)} \\ 1 & \alpha^9 & \cdots & \alpha^{9(n-1)} \end{pmatrix}$$

where α is a primitive element of $GF(q)$ for $q = 4n + 1$. [4, 18, 19, 14]

$E_3 = \{\pm 1, \pm\alpha^n, \pm\alpha^{2n}\}$

$$H_3 = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^7 & \cdots & \alpha^{7(n-1)} \\ 1 & \alpha^{13} & \cdots & \alpha^{13(n-1)} \end{pmatrix}$$

where α is a primitive element of $GF(q)$ for $q = 6n + 1$. [20, 15, 16]

a double Lee-error correctable $[n, n-3]$ linear code: $C_d := \{\boldsymbol{c} \in \mathbb{Z}_q^n \mid \boldsymbol{c}H_d^T = 0 \mod q\}$ $(d = 1, 2, 3)$

$(c_0, \ldots, c_{n-2}, c_{n-1}) \in C_1$
$\Rightarrow (-c_{n-1}, c_0, \ldots, c_{n-2}) \in C_1$
(negacyclic code)

$(c_0, \ldots, c_{n-2}, c_{n-1}) \in C_2$
$\Rightarrow (\alpha^n c_{n-1}, c_0, \ldots, c_{n-2}) \in C_2$
($\pi/2$-cyclic code)

$(c_0, \ldots, c_{n-2}, c_{n-1}) \in C_3$
$\Rightarrow (\alpha^n c_{n-1}, c_0, \ldots, c_{n-2}) \in C_3$
($\pi/6$-cyclic code)

Volumes of Lee Spheres

Circle

$$V_1(n,t) = \sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t}{i}$$

[Golomb & Welch, '70], [Roth '06]

Square

$$V_2(n,r) = \sum_{i=0}^{n} 4^i \binom{n}{i}\binom{r+i}{2i}$$

Hexagon

$$V_3(n,r) = \sum_{i=0}^{n} 6^i \binom{n}{i}\binom{r+i}{2i}$$

Another Formula on Hexagon

$$V_3(n,r) = 1 + \sum_{l=1}^{r}\sum_{i=1}^{l} 6^i \binom{n}{i}\binom{l+i-1}{2i-1}$$

Landmark Papers on Previous Works (1/2)

Lee '58 [21], Ulrich '57 [22] described first codes for the Lee metric.

Berlekamp '66 [17] introduced the negacyclic codes in the Lee metric which an efficient decoding procedure.

Nakamura '79 [4] gave a construction of integer codes for the Lee metric over the ring of integers modulo 2^k that is capable of correcting up to two errors.

Roth & Siegel '94 [9] derived the $2r$ lower bound on the minimum distance of a large class of linear codes with the Lee metric where r is the number of redundant symbols.

Landmark Papers on Previous Works (2/2)

Nakamura '82 [23] separately applied his Lee metric codes [4] to the in-pase and the quadrature components of differentially encoded multilevel QAM.

Huber '94 showed two types of linear codes on the complex plane:

- One was constructed over $\mathbb{Z}[\sqrt{-1}]$ modulo a Gaussian prime to correct an error on the square lattice of Gaussian integers **[18]**.
- The other was so over $\mathbb{Z}[(-1+\sqrt{-3})/2]$ modulo an Eisenstein prime to correct an error on the hexagonal lattice of Eisenstein integers **[20]**.

Nishimura & Hiramatsu '08 [19] presented a class of codes to correct errors of the weight up to 2 over the Galois field with the Lee metric on the square lattice.

Error Correcting Codes in the Lee Metric

Definition 2.1

The Lee weight of a word $\boldsymbol{a} = (a_1\, a_2\, \ldots\, a_n)$ *in* $\mathbb{Z}_m^n$ *is defined as*

$$w_1(\boldsymbol{a}) = \sum_{i=1}^{n} \min\left\{ a_i,\, m - a_i \pmod m \right\}$$

□

For example, $\boldsymbol{a} = (0, 1, 4, 3, 2)$ in $\mathbb{Z}_5^5$, we have

$$w_1(\boldsymbol{a}) = 0 + 1 + 1 + 2 + 2 = 6$$

Berlekamp Codes for the Lee Metric

Let $F = GF(p)$ where $p > 2$ is an odd prime. And for $m \geq 1$ and $q = p^m$, let F_q be an extension field of F.

For $n \leq (q-1)/2$, consider the linear $[n, n-t]$ code C over F_q with a check matrix H_1:

$$H_1 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t-1} & \alpha^{2(2t-1)} & \cdots & \alpha^{(2t-1)(n-1)} \end{pmatrix}$$

where α is a primitive element of F_q.

Theorem 1 (Berlekamp, '66 [17])

For t such that $t < p/2$, the intersection $C \cap F^n$ (subspace subcode) corrects every error word with $w_1(e) \leq t$.

This code is called *Berlekamp code* denoted by C_1.

Generalized Lee Distance

ℓ-dimensional Lee Distance

- The Lee distance was extended to an ℓ-dimensional Lee ditance by Nishimura and Hiramatsu [24, 19].

Definition 3.1

For a prime p and $q = p^m = 4n + 1$ $(m \geq 1)$, we define the ℓ-dimensional Lee weight $\|a\|$ of $a \in F_q$ by

$$\|a\| = \min_{\substack{\boldsymbol{x}=(x_i)\in\mathbb{Z}^\ell \\ \varphi(\boldsymbol{x})=a}} \left\{ \sum_{i=1}^{\ell} |x_i| \right\}$$

where $|x_i|$ is the absolute value of $x_i \in \mathbb{Z}$ and φ is a homomorphism from $\mathbb{Z}^l$ to F_q.

The Generalized Lee Weight

For a word $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ in F_q^n, define the generalized Lee weight by

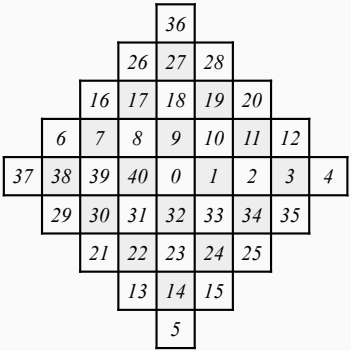
$$w_2(\boldsymbol{a}) = \sum_{i=1}^{n} \|a_i\| .$$

For example, a two-dimensional generalized Lee weight can be defined by a homomorphism

$$\varphi((1,0)) = 1, \quad \varphi((0,1)) = \alpha^n$$

where α is a primitive element of F_q.

Example ($q = 41, n = 10, \alpha = 7, \alpha^n = 9$)



Theorem 2

[Nishimura and Hiramatsu, '08] [19] A linear $[n, n-3]$ *code* C_2 *of length* n *over* F_q *with the check matrix*

$$H_2 := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^5 & \alpha^{10} & \cdots & \alpha^{5(n-1)} \\ 1 & \alpha^9 & \alpha^{18} & \cdots & \alpha^{9(n-1)} \end{pmatrix}$$

corrects any error word $\boldsymbol{e} \in F_q^n$ *such that* $w_2(\boldsymbol{e}) \leq 2$.

Hexagonal Constellations

The hexagonal constellation on two dimensional space is defined as a set which consists of points in

$$\{i\boldsymbol{h}_1 + j\boldsymbol{h}_3 | i, j \in \mathbb{Z}\}$$

where $\boldsymbol{h}_1 = (1, 0), \boldsymbol{h}_3 = (-1/2, \sqrt{3}/2)$. Furthermore, let $\boldsymbol{h}_2 = \boldsymbol{h}_1 + \boldsymbol{h}_3 = (1/2, \sqrt{3}/2)$ and $\boldsymbol{h}_{3+i} = -\boldsymbol{h}_i$ $(i = 1, 2, 3)$. Then the set of points on the lth hexagonal constellation is defined by

$$L_l = \begin{cases} \{\mathbf{0}\} & l = 0, \\ \{\boldsymbol{h}_1, \boldsymbol{h}_2, \dots, \boldsymbol{h}_6\} \cup L_0 & l = 1, \\ \left\{\sum_{k=1}^{l} \boldsymbol{a}_k \mid \boldsymbol{a}_k \in L_1\right\} & l \geq 2. \end{cases}$$

where $\mathbf{0} = (0, 0)$.

The weight of a point on a Hexagonal Constellaiton

Note that

- $L_0 \subset L_1 \subset \cdots \subset L_l \subset \cdots$, and
- $|L_l| = 3l(l+1) + 1 \ (l \geq 0)$.

Then, we define the weight of $\boldsymbol{x} \in L_l \backslash L_{l-1}$ by

$$\langle \boldsymbol{x} \rangle_H = l.$$

(*by the courtesy of Prof. S. Sakata, professor emeritus of UEC.*)

A Mapping ϕ from the Hexagonal Constellation to the corresponding Finite Field

Now, assume that $q = 3m(m+1)+1$ is a prime for $m \in \mathbb{N}$. Then let $n = (q-1)/6$ and construct a linear mapping $\phi : L_m \to F_q$ in the following way:

First assign $\{0\} \cup E_3$ to L_1 as follows:

$$\phi(\mathbf{0}) = 0, \qquad \phi(\boldsymbol{h}_k) = \alpha^{(k-1)n} \qquad (k = 1, \dots, 6)$$

Next, for $\boldsymbol{x} \in L_l \backslash L_{l-1}$ $(2 \le l \le m)$, there exists a *multiset* of points $[\boldsymbol{a}_1, \dots, \boldsymbol{a}_l]$ over L_1 such that $\boldsymbol{x} = \boldsymbol{a}_1 + \cdots + \boldsymbol{a}_l$. Then we define $\phi(\boldsymbol{x})$ by

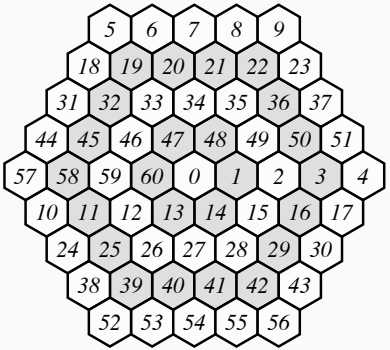
$$\phi(\boldsymbol{x}) = \phi(\boldsymbol{a}_1) + \cdots + \phi(\boldsymbol{a}_l).$$

And it is shown that

$$\phi : L_m \to F_q \text{ is an isomorphism [15].}$$

An example of ϕ

$q = 61,\ \ m = 4,\ \ \alpha = 2,\ \ n = 10\ \ (\boldsymbol{h}_1 = (0, 1),\ \ \boldsymbol{h}_3 = (-1/2, \sqrt{3}/2))$.



By means of ϕ, the lth surface of L_l is defined by

$$S_l = \begin{cases} \{0\} & (l = 0) \\ \{\, \phi(\boldsymbol{x}) \mid \boldsymbol{x} \in L_l \setminus L_{l-1} \,\} & (l \geq 1). \end{cases}$$

- Members in S_1 are called nearest neighbor (N-N) errors.

Definition 4.1

For $\boldsymbol{a} \in F_q$ and $k \geq 0$, the hexagonal Lee weight of $\boldsymbol{a}$, or shortly hex weight of $\boldsymbol{a}$, is defined by

$$\langle\!\langle a \rangle\!\rangle = \langle \phi^{-1}(a) \rangle_H \tag{1}$$

□

From Definition 4.1, the Lee weight of $\boldsymbol{a} = (a_1, \ldots, a_n) \in F_q^n$ on the hexagonal lattice is given by

$$w_3(\boldsymbol{a}) := \sum_{i=1}^{n} \langle\langle a_i \rangle\rangle$$

The hexagonal Lee distance between two words $\boldsymbol{a}, \boldsymbol{b} \in F_q^n$ is defined as

$$\rho_3(\boldsymbol{a}, \boldsymbol{b}) = w_3(\boldsymbol{a} - \boldsymbol{b})$$

Theorem 3 (M. '19 [16])

A linear code C_3 of length n over F_q with the check matrix

$$H_3 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^7 & \alpha^{14} & \cdots & \alpha^{7(n-1)} \\ 1 & \alpha^{13} & \alpha^{26} & \cdots & \alpha^{13(n-1)} \end{pmatrix}$$

corrects any error word $\boldsymbol{e} \in F_q^n$ such that $w_3(\boldsymbol{e}) \leq 2$.

- A class of check matrices including H_3 was presented in [20] where no proof on the decodability was given.
- A double error word $\boldsymbol{e}$ with $w_3(\boldsymbol{e}) = 2$ may occur only at two different positions but also at the same position of a codeword.

Errors of weight ≤ 2 on the Hexagonal Lattice

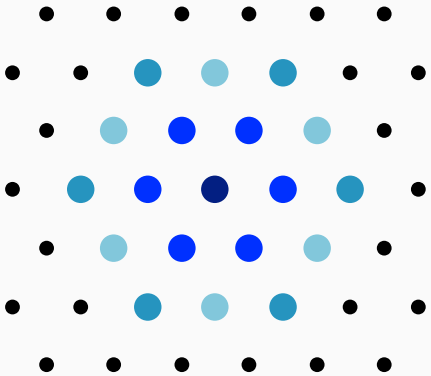


Figure 1: black: transmitted symbol, blue: errors of weight 1, dark blue and light blue: errors of type 1 and of type 2, respectively.

Basic Properties of Syndromes

Definition 5.1

Let C_3 be a linear code with check matrix H_3 defined above. Then the syndrome $\boldsymbol{s}$ of a received word $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ is defined by

$$\boldsymbol{s} = (s_1, s_7, s_{13}) = \boldsymbol{r}H_3^T = \boldsymbol{e}H_3^T \in F_q^3 \tag{2}$$

where $\boldsymbol{c} \in C_3$ and H^T is the transpose matrix of H. □

- The indices of the second and third components of the syndrome vector $\boldsymbol{s}$ match the definition of H_3.
- For $e \in E_3 = \{\pm 1, \pm\alpha^n, \pm\alpha^{2n}\}$ (See p.6)

$$e^6 \equiv 1 \pmod{q}\,.$$

- If $\boldsymbol{e} = (0, \dots, 0, \underset{\hat{i}}{e}, 0 \dots, 0)$ for $e \in S_1$, then

$$\begin{aligned} \boldsymbol{s} = \boldsymbol{r}H_3^T = (\boldsymbol{c} + \boldsymbol{e})H_3^T &= (e\alpha^i, e\alpha^{7i}, e\alpha^{13i}) \\ &\equiv (e\alpha^i, e^7\alpha^{7i}, e^{13}\alpha^{13i}) \pmod{q} \end{aligned}$$

  since $e^6 \equiv 1 \pmod{q}$. Let $\chi_i := e\alpha^i$. Then we have $s_1 = \chi_i, s_7 = \chi_i^7, s_{13} = \chi_i^{13}$.
- Similarly, if double errors $e_1, e_2 \in S_1$ occur on the ith and jth components of $\boldsymbol{e}$, respectively, then the corresponding syndromes are written as

$$s_1 = \chi_i + \chi_j, \ s_7 = \chi_i^7 + \chi_j^7, \ s_{13} = \chi_i^{13} + \chi_j^{13}. \tag{3}$$

  where $\chi_i = e_1\alpha^i, \ \chi_j = e_2\alpha^j$.

- The indexes i and j are not always distinct. Note that even if $i = j$, e_1 and e_2 are not necessary the same.

Suppose that χ is the product of α^i for i $(0 \le i < n)$ and $e \in E_3$. Then, by taking the discrete logarithm of χ with base α, that is, $\ell := \log_\alpha(\chi)$, i and e can be reproduced by

$$\left.\begin{array}{lll} i & \equiv \ell & \pmod{n}, \\ e & \equiv \alpha^{\ell - i} & \pmod{p}. \end{array}\right\} \tag{4}$$

Up to now, we know that the syndrome values in (3) can be represented as

$$s_k = \chi_i^k + \chi_j^k \qquad \text{for } k = 1, 7. \tag{5}$$

Now let us extend (5) to $k \in \mathbb{N} \cup \{0\}$ with $x := \chi_i \chi_j$ as follows:

$$s_k = \begin{cases} 2 & k = 0 \\ \chi_i + \chi_j & k = 1 \\ s_1 s_{k-1} - s_{k-2} x & k \geq 2\,. \end{cases} \tag{6}$$

Thus, s_k $(k \geq 0)$ can be represented as a polynomial $f_k(x)$ of x with a given s_1. Table 1 in the next slide shows $f_k(x)$ up to $k = 13$.

k	$s_k = f_k(x)$
0	$s_0 = 2$
1	$s_1 = s_1$
2	$s_2 = s_1^2 - 2x$
3	$s_3 = s_1^3 - 3s_1x$
4	$s_4 = s_1^4 - 4s_1^2x + 2x^2$
5	$s_5 = s_1^5 - 5s_1^3x + 5s_1x^2$
6	$s_6 = s_1^6 - 6s_1^4x + 9s_1^2x^2 - 2x^3$

k	$s_k = f_k(x)$
7	$s_7 = s_1^7 - 7s_1^5x + 14s_1^3x^2 - 7s_1x^3$
8	$s_8 = s_1^8 - 8s_1^6x + 20s_1^4x^2 - 16s_1^2x^3 + 2x^4$
9	$s_9 = s_1^9 - 9s_1^7x + 27s_1^5x^2 - 30s_1^3x^3 + 9s_1x^4$
10	$s_{10} = s_1^{10} - 10s_1^8x + 35s_1^6x^2 - 50s_1^4x^3 + 25s_1^2x^4 - 2x^5$
11	$s_{11} = s_1^{11} - 11s_1^9x + 44s_1^7x^2 - 77s_1^5x^3 + 55s_1^3x^4 - 11s_1x^5$
12	$s_{12} = s_1^{12} - 12s_1^{10}x + 54s_1^8x^2 - 112s_1^6x^3 + 105s_1^4x^4 - 36s_1^2x^5 + 2x^6$
13	$s_{13} = s_1^{13} - 13s_1^{11}x + 65s_1^9x^2 - 156s_1^7x^3 + 182s_1^5x^4 - 91s_1^3x^5 + 13s_1x^6$

Table 1: THE LIST OF THE SYNDROME EQUATIONS FOR $k \leq 13$

Building a Decoding Algorithm

Solving the Syndrome Equations (1/3)

From Table 1, we pick up the 7th and 13th polynomials and define

$$f(x) = s_1^{13} - s_{13} - 13s_1^{11}x + 65s_1^9x^2 - 156s_1^7x^3 + 182s_1^5x^4 - 91s_1^3x^5 + 13s_1x^6$$
$$g(x) = s_1^7 - s_7 - 7s_1^5x + 14s_1^3x^2 - 7s_1x^3.$$

Dividing $f(x)$ by $g(x)$ gives the quotient polynomial $Q_1(x)$ and the residue polynomial $r_1(x)$ as follows:

$$f(x) = Q_1(x)g(x) + r_1(x)$$
$$r_1(x) = -\frac{1}{49s_1}(A_0 + A_1x + A_2x^2)$$

where

$$\left.\begin{aligned} A_0 &= 29s_1^{14} - 65s_1^7s_7 + 49s_1s_{13} - 13s_7^2 \\ A_1 &= -182s_1^5(s_1^7 - s_7) \\ A_2 &= 273s_1^3(s_1^7 - s_7). \end{aligned}\right\} \quad (7)$$

Solving the Syndrome Equations (2/3)

Next, devide $g(x)$ by $r_1(x)$. Then we have $g(x) = Q(x)_2 r_1(x) + r_2(x)$.

Here, (Case 1) if $r_2(x) = 0$, then $r_1(x)$ must have a double root $x \equiv s_1^2/3 \pmod{q}$. □

(Case 2) Otherwise, $r_2(x)$ can be written as follows:

$$r_2(x) = C(B_0 - B_1 x)$$

where $C \in F_q$ and

$$\left.\begin{aligned} B_0 &= s_1^{16} + 26 s_1^9 s_7 - 196 s_1^3 s_{13} + 169 s_1^2 s_7^2 \\ B_1 &= 4 s_1^{14} + 104 s_1^7 s_7 - 147 s_1 s_{13} + 39 s_7^2 \end{aligned}\right\} \tag{8}$$

Hence, we obtain $x = \dfrac{B_0}{B_1}$. □

In the above argument, note that $r_2(x) = 0 \Leftrightarrow A_1^2 - 4A_0A_2 \equiv 0 \pmod{q}$.

Solving the Syndrome Equations (3/3)

Using x obtained in (Case 1) or (Case 2) with s_1, compute the two roots ξ_1 and ξ_2 in the following equation:

$$Z^2 - s_1 Z + x = (Z - \xi_1)(Z - \xi_2) \tag{9}$$

Then compute two pairs (i_1, e_1) and (i_2, e_2) of (4) for ξ_1 and ξ_2, respectively.

Classifying N-N Errors by Syndrome Values

- If $s_1 = 0$, then $s_7 = s_{13} = 0$ as well.

- For $s_1 \neq 0$,
  $s_1^7 \equiv s_7 \pmod{q}$ iff a single N-N error occurs.
  Hence, we can correct this error by applying Eq. (4) with $\chi = s_1$.

A Decoding Algorithm

Input: received word $\boldsymbol{r} = (r_1\ r_2\ \ldots r_n) \in F_q^n$.

Output: error word $\boldsymbol{e} = (e_1\ e_2\ \ldots\ e_n) \in F_q^n$ or no error indicator 's'.

---

1) comp. $(s_1\ s_7\ s_{13}) = \boldsymbol{r}H_3^T$
2) If $s_1 = 0$: return 's'. # for no errors
3) If $s_7 \equiv s_1^7 \pmod q$: # for a single error
4) calc. (i, e) of Eq. (4) with $\chi = s_1$.
5) return $\boldsymbol{e}$ with $e_i = e$ and $e_j = 0\ (j \neq i)$.
6) else:
7) compute A_0, A_1, A_2 in Eq. (7).
8) if $A_1^2 - 4A_0A_2 \equiv 0 \pmod q$:
9) $x = s_1^2/3$
10) else:
11) calc. B_0 and B_1 of Eq. (8)
12) $x = B_0/B_1$
13) compute ξ_1 and ξ_2 of Eq. (9) for x.
14) calc. $(i_1, e_1), (i_2, e_2)$ of Eq. (4) for ξ_1, ξ_2, resp.
15) return $\boldsymbol{e}$ with $e_{i_1} = e_1, e_{i_2} = e_2$ and $e_k = 0\ (k \neq i_1, i_2)$

Note: at the line 15) if $i = i_1 = i_2$, then $e_i \equiv e_1 + e_2 \pmod q$

Examples of the Decoding Processes

Conclusion and Future Works

- In this talk, we presented an approach how to generalize the concept of the Lee metric from one-dimensional to two-dimensional, square and hexagonal lattice.
- Along the line suggested by Huber's and Nishimura & Hiramatsu 's works, we proved that a linear code with H_3 as its parity check matrix corrects every errors of Lee weight up to two on the hexagonal constellation.
- Its proof was based on the rightness of the decoding algorithm given here. It is very simple and effective.
- In case of $d = 1, 2$, such algorithms similar to the case of $d = 3$ can be easily obtained.
- One of the most important open problems is how to construct more than 2 error correcting codes on two dimensional or multi-dimensional lattice.

References i

[1] R. W. Hamming, “Error detecting and error correcting codes,” *The Bell System Technical Journal*, pp. 147–160, 1950.

[2] S. W. Golomb and L. R. Welch, “Perfect codes in the lee metric and the packing of polyominoes,” *SIAM J. Appl. Math.*, vol. 18, pp. 302–317, 1970.

[3] R. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[4] K. Nakamura, “A class of error correcting codes for DPSK channels,” in *Proc. Int’l Conference on Communications (ICC’79)*, 1979, pp. 45.4.1–45.4.5.

[5] A. J. H. Vinck and H. Morita, “Codes over the ring of integers modulo $\boldsymbol{m}$,” *IEICE Trans. Fundamentals*, vol. E81-A, pp. 2013–2018, 1998.

[6] R. Karabed and P. H. Siegel, “Matched spectral-null codes for partial-response channels,” *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 818–855, 1991.

[7] V. Levenshtein and A. Vinck, “Perfect (d, k)-codes capable of correcting single peak-shifts,” *IEEE Trans. Inform. theory*, vol. 39, no. 2, pp. 656–662, 1993.

[8] A. V. Kuznetsov and A. J. H. Vinck, “A coding scheme for single peak-shift correction in (d, k)-constrained channels,” *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1444–1450, 1993.

[9] R. M. Roth and P. H. Siegel, “Lee-metric BCH codes and their application to constrained and partial-response channels,” *IEEE Trans. Inform. Theory*, vol. 40, pp. 1083–1096, 1994.

[10] P. A. H. Bours, “Construction of fixed-length insertion/deletion correcting runlength-limited codes,” *IEEE Trans. Inform. theory*, vol. 40, no. 6, pp. 1841–1856, 1994.

References iii

[11] A. Jiang, M. Schwartz, and J. Bruck, "Error-correcting codes for rank modulation," in *Proc. Int'l Symp. on Inform. Theory, Canada*, 2008, pp. 1736–1740.

[12] A. Barg and A. Mazumdar, "Codes in permutations and error correction for rank modulation," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3158–3165, 2010.

[13] R. Gabrys, H. M. Kiah, and O. Milenkovic, "Asymmetric lee distance codes for DNA-based storage," *IEEE Trans. Inform. Theory*, vol. 63, no. 8, pp. 4982–4995, 2017.

[14] H. Kostadinov, M., N. Iijima, A. J. H. Vinck, and N. Manev, "Soft decoding of integer codes and their application to coded modulation," *IEICE Trans. Fundamentals*, vol. E93-A, pp. 1363–1370, 2010.

[15] H. Morita, "Nearest-neighbor error correcting codes on a hexagonal signal constellation," in *Proc. IEEE ISIT2015*, 2015, pp. 2480–2484.

References iv

[16] ——, “Double nearest-neighbor error correcting codes on hexagonal signal constellation,” in *Proc. IEEE ISIT2019*, 2019, pp. 1617–1621.

[17] E. R. Berlekamp, “Negacyclic codes for the lee metric,” Institute of Statistics Mimeo Series, Tech. Rep. No. 495, November 1966.

[18] K. Huber, “Codes over Gaussian integers,” *IEEE Trans. on Inform. Theory*, vol. 40, no. 1, pp. 207–216, 1994.

[19] S. Nishimura and T. Hiramatsu, “A generalization of the lee distance and error correcting codes,” *Discrete Applied Mathematics*, vol. 156, pp. 588–595, 2008.

[20] K. Huber, “Codes over Eisenstein-Jacobi integers,” *Comtemporary Mathematics*, vol. 168, pp. 165–179, 1994.

[21] C. Y. Lee, “Some properties of nonbinary error-correcting codes,” *IRE Trans. on Inform. Theory*, pp. 77–82, 1958.

[22] W. Ulrich, “Non-binary error correction codes,” *Bell Syst. Techn. J.*, vol. 36, pp. 1341–1387, 1957.

[23] K. Nakamura, “Error correcting scheme for differentially encoded m-array quadrature amplitude modulation system,” in *Proc. SITA*, 1982, pp. 44–52.

[24] S. Nishimura and T. Hiramatsu, “Codes over cyclotomic fields,” in *Proceeding of the 20th Symposium on Information Theorey and its Applications (in Japanese)*, 1997, pp. 21–24.

Thank you!

本講演内容をまとめるにあたり，多大なご支援いただいた次のお二人に感謝します．

共同研究者：

阪田省二郎　（電気通信大学名誉教授）

藤沢匡哉　（東京理科大学准教授）