The Geometry and Error Probability of the Lee Channel

Workshop on Combinatorics in Digital Communications
Eindhoven University of Technology, April 19-21, 2023

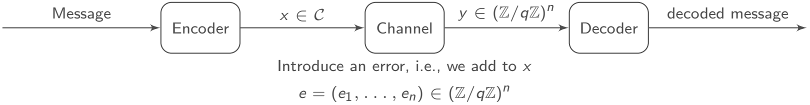
Jessica Bariffi

DLR, Institute for Communications and Navigation

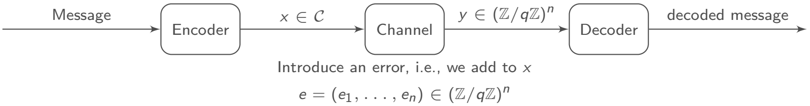
19.04.2023

Motivation
Code-based Cryptography

Take a linear code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$.



Take a linear code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$.



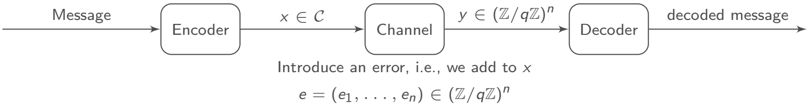
Generic Decoding

Given $y = x + e$, recover either the original message x or the error term e.

- NP-hard problem
- Has a unique solution for errors of relatively small "weight"

Motivation
Code-based Cryptography

Take a linear code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$.



Generic Decoding

Given $y = x + e$, recover either the original message x or the error term e.

- NP-hard problem
- Has a unique solution for errors of relatively small “weight”

We consider a random error of fixed weight (Lee weight).

Outline

Outline

Ring Linear Codes

Notation:

$\mathbb{Z}/q\mathbb{Z} := \{0, 1, 2, \ldots, q-1\}$	integer residue ring
$(\mathbb{Z}/q\mathbb{Z})^\times$	set of units (i.e. integers coprime to q)

Note: If q is prime, then $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_q$ is a finite field of q elements.

Ring Linear Codes

Notation:

$\mathbb{Z}/q\mathbb{Z} := \{0, 1, 2, \ldots, q-1\}$	integer residue ring
$(\mathbb{Z}/q\mathbb{Z})^\times$	set of units (i.e. integers coprime to q)

Note: If q is prime, then $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_q$ is a finite field of q elements.

A *linear code* $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ is a $\mathbb{Z}/q\mathbb{Z}$-submodule of $(\mathbb{Z}/q\mathbb{Z})^n$. The elements of $\mathcal{C}$ are called *codewords* of length n.

Parameters:

- n is called the *length* of $\mathcal{C}$
- $k := \log_q \left| \mathcal{C} \right|$ is the $\mathbb{Z}/q\mathbb{Z}$-*dimension* of $\mathcal{C}$
- $R := k/n$ denotes the *rate* of $\mathcal{C}$.

Ring Linear Codes

Notation:

$\mathbb{Z}/q\mathbb{Z} := \{0, 1, 2, \dots, q-1\}$	integer residue ring
$(\mathbb{Z}/q\mathbb{Z})^\times$	set of units (i.e. integers coprime to q)

Note: If q is prime, then $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_q$ is a finite field of q elements.

A *linear code* $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ is a $\mathbb{Z}/q\mathbb{Z}$-submodule of $(\mathbb{Z}/q\mathbb{Z})^n$. The elements of $\mathcal{C}$ are called *codewords* of length n.

Parameters:

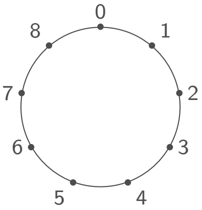
- n is called the *length* of $\mathcal{C}$
- $k := \log_q \left| \mathcal{C} \right|$ is the $\mathbb{Z}/q\mathbb{Z}$-*dimension* of $\mathcal{C}$
- $R := k/n$ denotes the *rate* of $\mathcal{C}$.

The *Hamming weight* of a codeword $c \in \mathcal{C}$ is the number of nonzero entries of c, i.e.,

$$\mathrm{wt_H}(c) := \left| \ \{i \in \{1, \dots, n\} \mid c_i \neq 0\} \ \right|$$

The Lee Metric

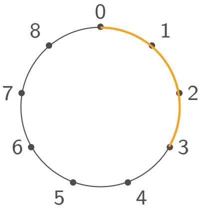
Example: $\mathbb{Z}/9\mathbb{Z}$



The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0.

The Lee Metric

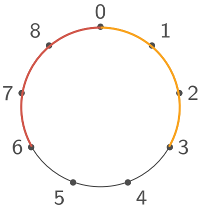
Example: $\mathbb{Z}/9\mathbb{Z}$



The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0.

The Lee Metric

Example: $\mathbb{Z}/9\mathbb{Z}$



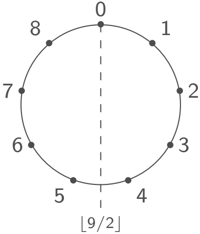
The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0. Hence,

$$\mathrm{wt_L}(a) = \mathrm{wt_L}(q-a)$$

$$\mathrm{wt_H}(a) \leq \mathrm{wt_L}(a) \leq \lfloor q/2 \rfloor$$

The Lee Metric

Example: $\mathbb{Z}/9\mathbb{Z}$



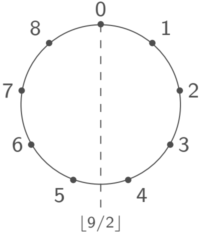
The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0. Hence,

$$\mathrm{wt}_\mathrm{L}(a) = \mathrm{wt}_\mathrm{L}(q - a)$$

$$\mathrm{wt}_\mathrm{H}(a) \leq \mathrm{wt}_\mathrm{L}(a) \leq \lfloor q/2 \rfloor$$

The Lee Metric

Example: $\mathbb{Z}/9\mathbb{Z}$



The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0. Hence,

$$\mathrm{wt}_L(a) = \mathrm{wt}_L(q-a)$$

$$\mathrm{wt}_H(a) \leq \mathrm{wt}_L(a) \leq \lfloor q/2 \rfloor$$

For any integer $a \in \mathbb{Z}/q\mathbb{Z}$ and any vector $x, y \in (\mathbb{Z}/q\mathbb{Z})^n$ we define their *Lee weight* as

$$\mathrm{wt}_L(a) := \min(a, \left| q-a \right|)$$

$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i)$$

The *Lee distance* between x and y is given by $\mathrm{d}_L(x,y) := \mathrm{wt}_L(x-y)$.

Size of n-Dimensional Lee Sphere

Consider the n-dimensional Lee sphere of radius t in $\mathbb{Z}/q\mathbb{Z}$ denoted by

$$\mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt}_{\mathsf{L}}(x) = t\}\,.$$

Size of *n*-Dimensional Lee Sphere

Consider the n-dimensional Lee sphere of radius t in $\mathbb{Z}/q\mathbb{Z}$ denoted by

$$\mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt}_\mathsf{L}(x) = t\}.$$

Example

Consider the 3-dimensional Lee sphere of radius $t = 2$ over $\mathbb{Z}/5\mathbb{Z}$.

$$\mathcal{S}_{2,5}^{(3)} = \{(1,1,0), \dots, (1,4,0), \dots, (4,4,0), \dots, (2,0,0), \dots, (3,0,0), \dots\}$$

Size of n-Dimensional Lee Sphere

Consider the n-dimensional Lee sphere of radius t in $\mathbb{Z}/q\mathbb{Z}$ denoted by

$$\mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt_L}(x) = t\}\,.$$

Example

Consider the 3-dimensional Lee sphere of radius $t = 2$ over $\mathbb{Z}/5\mathbb{Z}$.

$$\mathcal{S}_{2,5}^{(3)} = \{(1,1,0), \dots, (1,4,0), \dots, (4,4,0), \dots, (2,0,0), \dots, (3,0,0), \dots\}$$

For $a \in \mathcal{S}_{t,q}^{(n)}$ denote by $\omega_a = (\omega_a(0), \dots, \omega_a(q-1))$ denote the Lee weight decomposition of a, i.e.,

$$\omega_a(i) := \left|\ \{k = 1, \dots, n \mid a_k = i\}\ \right| \quad \text{and} \quad \sum_{i=0}^{q-1} \omega_a(i)\, \mathrm{wt_L}(i) = t \qquad (*)$$

Size of n-Dimensional Lee Sphere

Consider the n-dimensional Lee sphere of radius t in $\mathbb{Z}/q\mathbb{Z}$ denoted by

$$\mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt_L}(x) = t\}\,.$$

Example

Consider the 3-dimensional Lee sphere of radius $t = 2$ over $\mathbb{Z}/5\mathbb{Z}$.

$$\mathcal{S}_{2,5}^{(3)} = \{(1,1,0),\dots,(1,4,0),\dots,(4,4,0),\dots,(2,0,0),\dots,(3,0,0),\dots\}$$

For $a \in \mathcal{S}_{t,q}^{(n)}$ denote by $\omega_a = (\omega_a(0),\dots,\omega_a(q-1))$ denote the Lee weight decomposition of a, i.e.,

$$\omega_a(i) := \left|\ \{k = 1,\dots,n \mid a_k = i\}\ \right| \quad \text{and} \quad \sum_{i=0}^{q-1} \omega_a(i)\,\mathrm{wt_L}(i) = t \qquad (*)$$

The number of permutations of a is given by the multinomial coefficient $\binom{n}{\omega_a(0),\dots,\omega_a(q-1)} = \frac{n!}{\omega_a(0)!\cdot\ldots\cdot\omega_a(q-1)!}$. Hence,

$$\left|\ \mathcal{S}_{t,q}^{(n)}\ \right| = \sum_{\omega \text{ satisfying } (*)} \binom{n}{\omega(0),\dots,\omega(q-1)}$$

Outline

Typical Sequence in the Lee Sphere

Example

$$\mathcal{S}_{2,5}^{(3)} = \left\{ (1,1,0),\ldots,(1,4,0),\ldots,(4,4,0),\ldots,\ (2,0,0),\ldots,(3,0,0),\ldots \right\}$$

Draw $a \in \mathcal{S}_{2,5}^{(3)}$ uniformly at random, then

- smaller Lee weights are more likely to occur in the vector a.
- some sequences are more likely $\longrightarrow$ typical sequence.

Typical Sequence in the Lee Sphere

Example

$$\mathcal{S}_{2,5}^{(3)} = \left\{ (1,\,1,\,0),\ldots,\,(1,\,4,\,0),\ldots,(4,\,4,\,0),\ldots,\;(2,\,0,\,0),\ldots,\,(3,\,0,\,0),\ldots \right\}$$

Draw $a \in \mathcal{S}_{2,5}^{(3)}$ uniformly at random, then

- smaller Lee weights are more likely to occur in the vector a.
- some sequences are more likely $\longrightarrow$ typical sequence.

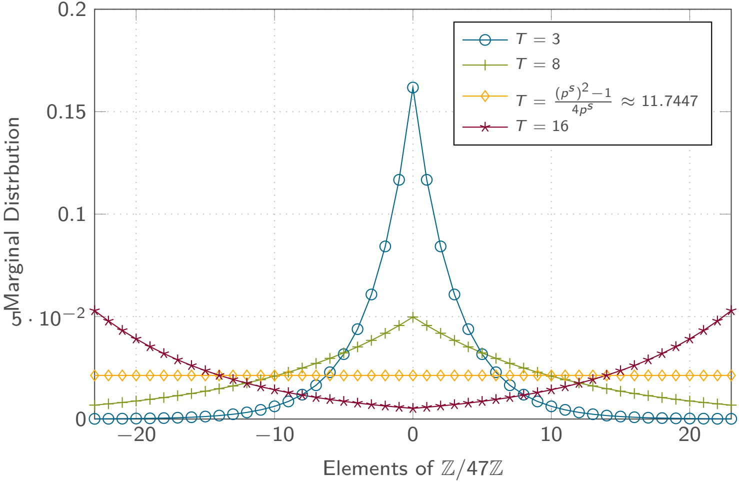
Lemma - Marginal Distribution in the Lee Sphere

Consider a random vector $A \in \mathcal{S}_{n\delta,q}^{(n)}$ and let $P(a)$ be the marginal distribution of an element of A. Then, for every $a \in \mathbb{Z}/q\mathbb{Z}$ we have

$$P(a) \longrightarrow B_\delta(a) := \frac{1}{Z(\beta)} \exp\left(-\beta\, \mathrm{wt_L}(a)\right),$$

where β is the unique real solution to the Lee weight constraint
$\delta = \sum_{i=0}^{q-1} \mathrm{wt_L}(i)\mathbb{P}(X = i)$ and $Z(\beta)$ denotes the normalization constant

The Marginal Distribution - Example over $\mathbb{Z}/47\mathbb{Z}$



Growth Rate of Lee Sphere Spectrum

Consider the *surface spectrum*, i.e., the sequence $\left|\mathcal{S}_{0,q}^{(n)}\right|, \left|\mathcal{S}_{1,q}^{(n)}\right|, \ldots, \left|\mathcal{S}_{n\lfloor q/2\rfloor,q}^{(n)}\right|$ and define their normalized logarithmic surface spectrum and its asymptotic counterpart, respectively, as

$$\sigma_{\delta n}^{(n)} := \frac{1}{n}\log_2\left(\left|\mathcal{S}_{n\delta,q}^{(n)}\right|\right) \quad \text{and} \quad \sigma_\delta := \lim_{n\to\infty}\sigma_{\delta n}^{(n)}.$$

Consider the *surface spectrum*, i.e., the sequence $\left|\mathcal{S}_{0,q}^{(n)}\right|, \left|\mathcal{S}_{1,q}^{(n)}\right|, \ldots, \left|\mathcal{S}_{n\lfloor q/2\rfloor,q}^{(n)}\right|$ and define their normalized logarithmic surface spectrum and its asymptotic counterpart, respectively, as

$$\sigma_{\delta n}^{(n)} := \frac{1}{n}\log_2\left(\left|\mathcal{S}_{n\delta,q}^{(n)}\right|\right) \quad \text{and} \quad \sigma_\delta := \lim_{n\to\infty}\sigma_{\delta n}^{(n)}.$$

Lemma

For any positive integer δn we can upper bound the surface spectrum by

$$\sigma_{\delta n}^{(n)} \leq H_\delta^+ := \begin{cases} H(B_\delta) & 0 \leq \delta \leq \delta_q \\ \log_2(q) & \delta_q < \delta < \lfloor q/2 \rfloor \end{cases}.$$

In particular, as n grows large it holds $\sigma_\delta = H(B_\delta)$[1].

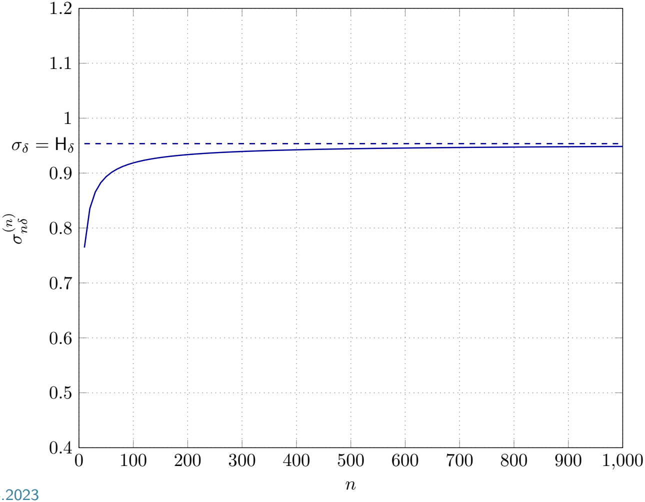
---

[1] $H(B_\delta) = -\sum_{a\in\mathbb{Z}/q\mathbb{Z}} B_\delta(a)\log_2(B_\delta(a))$ denotes the binary entropy function.

Growth Rate of Lee Sphere Spectrum

Example

Convergence of $\sigma_{\delta n}^{(n)}$ to $\sigma_\delta = H_\delta$ as a function of n for $\delta = 0.2$ over $\mathbb{Z}/7\mathbb{Z}$.



Outline

1. The Lee Metric
2. The Boltzmann Distribution
3. Error Probability for the Constant Lee Channel

Constant Lee Weight Channel

Let $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ be a linear code.

$$\xrightarrow{x \in \mathcal{C}} \boxed{\text{Channel}} \xrightarrow{y \in (\mathbb{Z}/q\mathbb{Z})^n}$$

Error added has fixed Lee weight t, i.e.,

$$y = x + e, \quad \text{where } e \in \mathcal{S}_{t,q}^{(n)}$$

Channel Transition probability

$$P(Y = y \mid X = x) = \begin{cases} \dfrac{1}{\left| \mathcal{S}_{\delta n,q}^{(n)} \right|} & \text{if } \mathrm{d_L}(y, x) = \delta n \\ 0 & \text{otherwise.} \end{cases}$$

Constant Lee Weight Channel

Let $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ be a linear code.

$$x \in \mathcal{C} \longrightarrow \boxed{\text{Channel}} \longrightarrow y \in (\mathbb{Z}/q\mathbb{Z})^n$$

Error added has fixed Lee weight t, i.e.,

$$y = x + e, \quad \text{where } e \in \mathcal{S}_{t,q}^{(n)}$$

Channel Transition probability

$$P(Y = y \mid X = x) = \begin{cases} \dfrac{1}{\left| \mathcal{S}_{\delta n, q}^{(n)} \right|} & \text{if } \mathrm{d_L}(y, x) = \delta n \\ 0 & \text{otherwise.} \end{cases}$$

Maximum Likelihood Decoding

Given the channel output $y \in (\mathbb{Z}/q\mathbb{Z})^n$ decode to the codeword $\hat{x}_{\mathrm{ML}}$ maximizing the channel probability, i.e.,

$$\hat{x}_{\mathrm{ML}} = \underset{x \in \mathcal{C}}{\operatorname{argmax}} \, P(Y = y \mid X = x)$$

Minimum Distance Decoding

Given the channel output $y \in (\mathbb{Z}/q\mathbb{Z})^n$ decode to the codeword $\hat{x}_{\mathrm{MD}}$ of smallest Lee distance from y, i.e.,

$$\hat{x}_{\mathrm{MD}} = \underset{x \in \mathcal{C}}{\operatorname{argmin}} \, \mathrm{d_L}(x, y)$$

Error Probability

Random Coding Union Bound, ML decoding

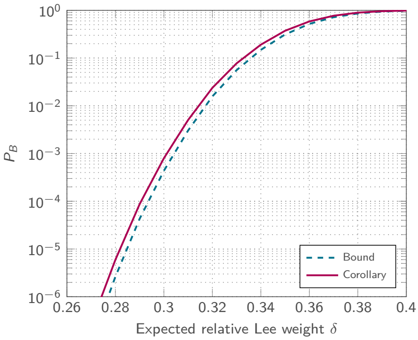
The average ML decoding error probability, $P_{\mathrm{B}}(\mathcal{C})$, of $\mathcal{C}$ used to transmit over a constant Lee weight channel satisfies

$$\mathbb{E}(P_{\mathrm{B}}(\mathcal{C})) < 2^{-n\left[\log_2 q - \sigma_{\delta n}^{(n)} - R_2\right]^+}.$$

Corollary

There average ML decoding error probability of $\mathcal{C}$ used to transmit over a constant Lee weight channel satisfies

$$\mathbb{E}(P_{\mathrm{B}}(\mathcal{C})) < 2^{-n[\log_2 q - H_\delta - R_2]^+}$$



Error Probability

Random Coding Union Bound, ML decoding

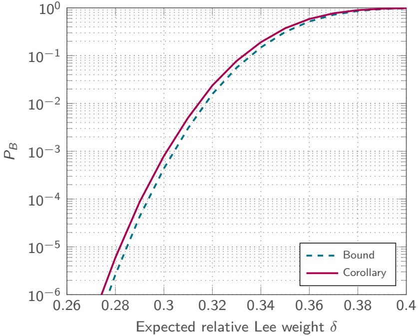
The average ML decoding error probability, $P_{\mathrm{B}}(\mathcal{C})$, of $\mathcal{C}$ used to transmit over a constant Lee weight channel satisfies

$$\mathbb{E}(P_{\mathrm{B}}(\mathcal{C})) < 2^{-n\left[\log_2 q - \sigma_{\delta n}^{(n)} - R_2\right]^+}.$$

Corollary

There average ML decoding error probability of $\mathcal{C}$ used to transmit over a constant Lee weight channel satisfies

$$\mathbb{E}(P_{\mathrm{B}}(\mathcal{C})) < 2^{-n[\log_2 q - H_\delta - R_2]^+}$$



Thank you for your attention!