16.09.2021
PICSeminar

Channel Coding in the Lee Metric

Jessica Bariffi

German Aerospace Center (DLR) &
University of Zurich

joint work with Hannes Bartz, Gianluigi Liva
and Joachim Rosenthal

Outline

DLR

Outline

1. Introduction
2. The Lee Channel
3. Error Pattern Construction
4. Scalar Multiplication in the Lee Metric

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Channel Coding

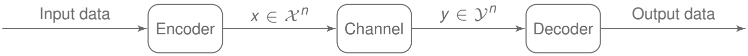
Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.



With a given channel law

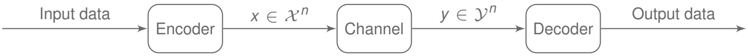
$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Example: q-ary Symmetric Channel (qSC)

- Alphabets:
  $\mathcal{X} = \mathcal{Y} = \{0, 1, \dots, q-1\}$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.



With a given channel law

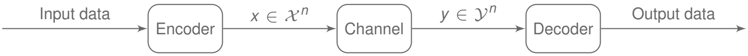
$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Example: q-ary Symmetric Channel (qSC)

- Alphabets:
  $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, q-1\}$
- Probability of correct transmission:
  $1 - \varepsilon$

Channel Coding

Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

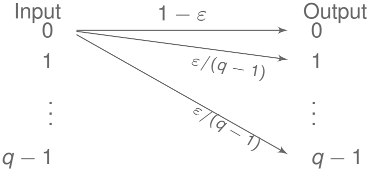


With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Example: q-ary Symmetric Channel (qSC)

- Alphabets: $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, q-1\}$
- Probability of correct transmission: $1 - \varepsilon$
- Probability of error for every possible outcome: $\varepsilon/(q-1)$



DLR

Channel Coding

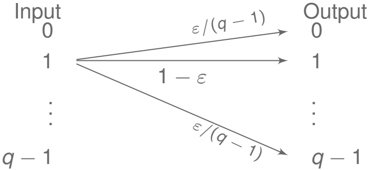
Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y_i \mid x_i) := \mathbb{P}(Y = y_i \mid X = x_i)$$

Example: q-ary Symmetric Channel (qSC)

- Alphabets: $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, q-1\}$
- Probability of correct transmission: $1 - \varepsilon$
- Probability of error for every possible outcome: $\varepsilon/(q-1)$



Linear Block Codes

Let $\mathbb{F}_q$ be a finite field of order q and let n be a positive integer.

Definition [Linear Code]

An $[n, k]_q$-*linear code* $\mathcal{C} \subset \mathbb{F}_q^n$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are called *codewords*.

Linear Block Codes

Let $\mathbb{F}_q$ be a finite field of order q and let n be a positive integer.

Definition [Linear Code]

An $[n, k]_q$-*linear code* $\mathcal{C} \subset \mathbb{F}_q^n$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are called *codewords*.

Example

$\mathcal{C} = \{(0,0,0,0), (1,1,0,0), (0,0,1,1), (1,1,1,1)\}$ is a $[4,2]_2$-linear code.

Linear Block Codes

Let $\mathbb{F}_q$ be a finite field of order q and let n be a positive integer.

Definition [Linear Code]

An $[n, k]_q$-*linear code* $\mathcal{C} \subset \mathbb{F}_q^n$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are called *codewords*.

Example

$\mathcal{C} = \{(0,0,0,0),\ (1,1,0,0),\ (0,0,1,1),\ (1,1,1,1)\}$ is a $[4,2]_2$-linear code.

Definition [Hamming Weight/Distance]

For any two codewords $x, y \in \mathcal{C}$ we define

- the *Hamming weight* of x, $\mathrm{wt}_H(x) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|$
- the *Hamming distance* between x and y, $\mathrm{d}_H(x, y) := \mathrm{wt}_H(x - y)$

The Lee Metric

We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Lee weight]

For any integer $a \in \mathbb{Z}_q$ its *Lee weight* is defined as

$$\mathrm{wt}_L(a) := \min(a, q - a) \tag{1}$$

The Lee Metric

We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Lee weight]

For any integer $a \in \mathbb{Z}_q$ its *Lee weight* is defined as

$$\mathrm{wt}_L(a) := \min(a, q - a) \quad (1)$$

Example: Consider $\mathbb{Z}_5$. The Lee weight of $a = 3$ is

$$\mathrm{wt}_L(3) = \min(3, 5 - 3) = 2$$

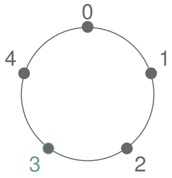
The Lee Metric

We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Lee weight]

For any integer $a \in \mathbb{Z}_q$ its *Lee weight* is defined as

$$\mathrm{wt}_L(a) := \min(a, q-a) \tag{1}$$



Example: Consider $\mathbb{Z}_5$. The Lee weight of $a = 3$ is

$$\mathrm{wt}_L(3) = \min(3, 5-3) = 2$$

The Lee weight of an element a describes also the minimal number of arcs separating a from 0.

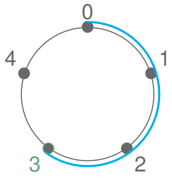
The Lee Metric

We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Lee weight]

For any integer $a \in \mathbb{Z}_q$ its *Lee weight* is defined as

$$\mathrm{wt}_L(a) := \min(a, q - a) \tag{1}$$



Example: Consider $\mathbb{Z}_5$. The Lee weight of $a = 3$ is

$$\mathrm{wt}_L(3) = \min(3, 5 - 3) = 2$$

The Lee weight of an element a describes also the minimal number of arcs separating a from 0.

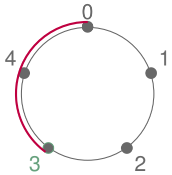
The Lee Metric

We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Lee weight]

For any integer $a \in \mathbb{Z}_q$ its *Lee weight* is defined as

$$\mathrm{wt}_L(a) := \min(a, q - a) \tag{1}$$



Example: Consider $\mathbb{Z}_5$. The Lee weight of $a = 3$ is

$$\mathrm{wt}_L(3) = \min(3, 5 - 3) = 2$$

The Lee weight of an element a describes also the minimal number of arcs separating a from 0.

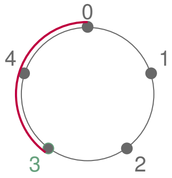
The Lee Metric

We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Lee weight]

For any integer $a \in \mathbb{Z}_q$ its *Lee weight* is defined as

$$\mathrm{wt}_L(a) := \min(a, q - a) \tag{1}$$



Example: Consider $\mathbb{Z}_5$. The Lee weight of $a = 3$ is

$$\mathrm{wt}_L(3) = \min(3, 5 - 3) = 2$$

The Lee weight of an element a describes also the minimal number of arcs separating a from 0.
$\Longrightarrow \mathrm{wt}_L(3) = 2$

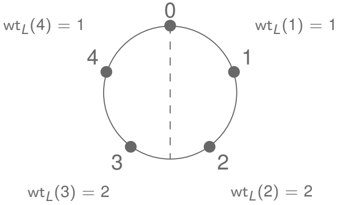
The Lee Metric

Properties

For every $a \in \mathbb{Z}_q$ it holds:

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

Example



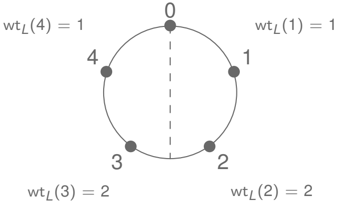
The Lee Metric

Properties

For every $a \in \mathbb{Z}_q$ it holds:

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

Example



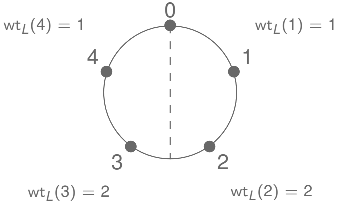
The Lee Metric

Properties

For every $a \in \mathbb{Z}_q$ it holds:

- $\mathrm{wt}_L(a) = \mathrm{wt}_L(q-a)$
- $\mathrm{wt}_L(a) \leq \lfloor q/2 \rfloor$
- $\mathrm{wt}_H(a) \leq \mathrm{wt}_L(a)$
  If $q \in \{2, 3\}$, the Lee weight is equivalent to the Hamming weight.

Example



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \dots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \dots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

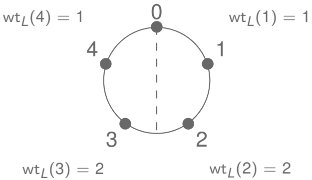
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) =$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

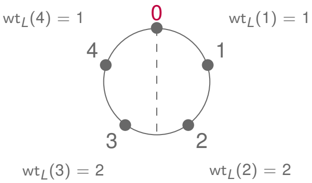
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

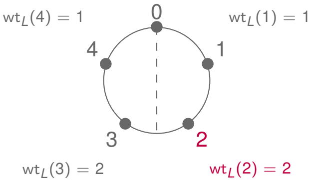
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

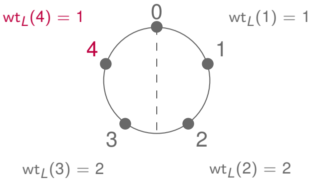
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2 + 1$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \dots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

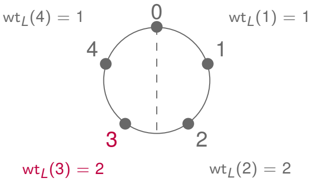
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2 + 1 + 2$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \dots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

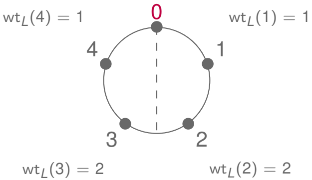
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2 + 1 + 2 + 0$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

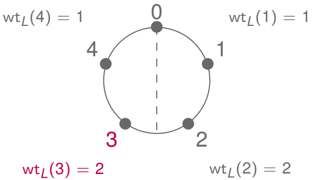
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2 + 1 + 2 + 0 + 2$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

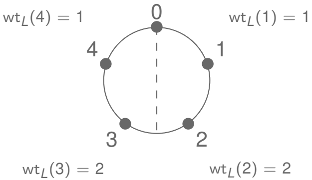
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2 + 1 + 2 + 0 + 2 = 7$$



The Lee Metric

Definition [Lee weight]

Let $x = (x_1, \dots, x_n) \in \mathbb{Z}_q^n$ be a tuple of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

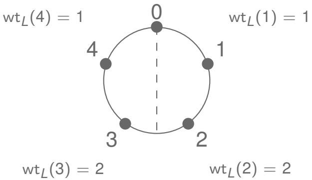
$$\mathrm{wt}_L(x) := \sum_{i=1}^{n} \mathrm{wt}_L(x_i) \tag{2}$$

The *Lee distance* between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $\mathrm{d}_L(x, y) = \mathrm{wt}_L(x - y)$.

Example:

Take again the ring of integers $\mathbb{Z}_5$

$$x = (0, 2, 4, 3, 0, 3)$$
$$\mathrm{wt}_L(x) = 0 + 2 + 1 + 2 + 0 + 2 = 7$$
$$\mathrm{wt}_H(x) = 4$$



Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *Applied and Computational Mathematics* (2019).

[2] Paolo Santini et al. "Low-Lee-Density Parity-Check Codes". In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation
- Design code-based cryptosystems with reduced key sizes

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. “Information set decoding in the Lee metric with applications to cryptography”. In: *Applied and Computational Mathematics* (2019).

[2] Paolo Santini et al. “Low-Lee-Density Parity-Check Codes”. In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation
- Design code-based cryptosystems with reduced key sizes
- Used in magnetic and DNA storage systems.

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. “Information set decoding in the Lee metric with applications to cryptography”. In: *Applied and Computational Mathematics* (2019).

[2] Paolo Santini et al. “Low-Lee-Density Parity-Check Codes”. In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation
- Design code-based cryptosystems with reduced key sizes
- Used in magnetic and DNA storage systems.
- Recently: gained attention in cryptographic applications

---

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *Applied and Computational Mathematics* (2019).

[2] Paolo Santini et al. "Low-Lee-Density Parity-Check Codes". In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation
- Design code-based cryptosystems with reduced key sizes
- Used in magnetic and DNA storage systems.
- Recently: gained attention in cryptographic applications
  - Generic decoding is NP-hard in the Lee Metric[1]

---

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. “Information set decoding in the Lee metric with applications to cryptography”. In: *Applied and Computational Mathematics* (2019).

[2] Paolo Santini et al. “Low-Lee-Density Parity-Check Codes”. In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation
- Design code-based cryptosystems with reduced key sizes
- Used in magnetic and DNA storage systems.
- Recently: gained attention in cryptographic applications
  - Generic decoding is NP-hard in the Lee Metric[1]
  - Low-Lee-Density Parity-Check Codes were defined[2]

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. “Information set decoding in the Lee metric with applications to cryptography”. In: *Applied and Computational Mathematics* (2019).

[2] Paolo Santini et al. “Low-Lee-Density Parity-Check Codes”. In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Outline

The Lee Channel

Originally introduced by Chiang and Wolf[3].

[3] J Chung-Yaw Chiang and Jack K Wolf. “On channels and codes for the Lee metric”. In: *Information and Control* 19.2 (1971), pp. 159–173.

The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is $\mathbb{Z}_q$.
Goal: Describe $\mathbb{P}(i \mid j) = \mathbb{P}(i - j \mid 0)$.

$-\lfloor q/2 \rfloor$
$\vdots$
-1
0 $\quad$ 0
1
$\vdots$
$\lfloor q/2 \rfloor$

[3] J Chung-Yaw Chiang and Jack K Wolf. “On channels and codes for the Lee metric”. In: *Information and Control* 19.2 (1971), pp. 159–173.

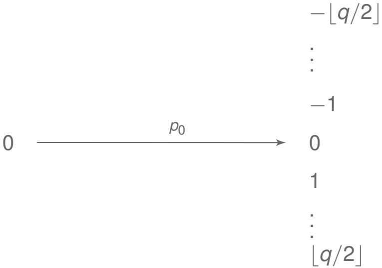
The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is $\mathbb{Z}_q$.
Goal: Describe $\mathbb{P}(i \mid j) = \mathbb{P}(i - j \mid 0)$.

Define for every $i = 0, \ldots, \lfloor q/2 \rfloor$

$$p_i := \mathbb{P}(i \mid 0) = \mathbb{P}(-i \mid 0)$$



[3] J Chung-Yaw Chiang and Jack K Wolf. "On channels and codes for the Lee metric". In: *Information and Control* 19.2 (1971), pp. 159–173.

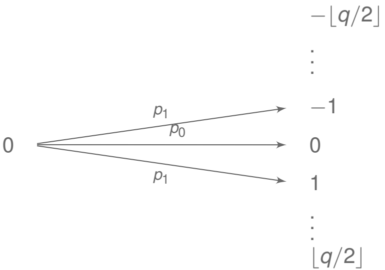
The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is $\mathbb{Z}_q$.
Goal: Describe $\mathbb{P}(i \mid j) = \mathbb{P}(i - j \mid 0)$.

Define for every $i = 0, \ldots, \lfloor q/2 \rfloor$

$$p_i := \mathbb{P}(i \mid 0) = \mathbb{P}(-i \mid 0)$$



[3] J Chung-Yaw Chiang and Jack K Wolf. "On channels and codes for the Lee metric". In: *Information and Control* 19.2 (1971), pp. 159–173.

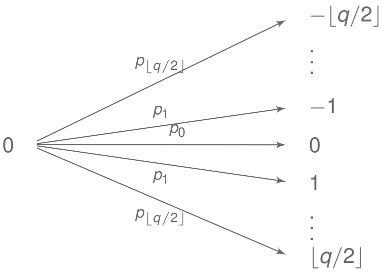
The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is $\mathbb{Z}_q$.
Goal: Describe $\mathbb{P}(i \mid j) = \mathbb{P}(i - j \mid 0)$.

Define for every $i = 0, \ldots, \lfloor q/2 \rfloor$

$$p_i := \mathbb{P}(i \mid 0) = \mathbb{P}(-i \mid 0)$$



[3] J Chung-Yaw Chiang and Jack K Wolf. “On channels and codes for the Lee metric”. In: *Information and Control* 19.2 (1971), pp. 159–173.

DLR

The Lee Channel Law

For $y, x, e \in \mathbb{Z}_q$, consider a discrete memoryless channel (DMC)

$$\underset{\text{channel output}}{y} = \underset{\text{channel input}}{x} + \underset{\text{additive error term}}{e} \tag{3}$$

The Lee Channel Law

For $y, x, e \in \mathbb{Z}_q$, consider a discrete memoryless channel (DMC)

$$\underbrace{y}_{\text{channel output}} = \underbrace{x}_{\text{channel input}} + \underbrace{e}_{\text{additive error term}} \tag{3}$$

Restrict to: e a realization of a random variable E with

$$\mathbb{P}(E = e) \propto \exp(-\lambda \, \mathrm{wt}_L(e)), \qquad \lambda > 0,$$

$$P_{Y|X}(y|x) = \frac{1}{Z} \exp\left(-\lambda \, \mathrm{d}_L(x, y)\right), \qquad Z := \sum_{e=0}^{q-1} \exp(-\lambda \, \mathrm{wt}_L(e))$$

The Lee Channel Law

For $y, x, e \in \mathbb{Z}_q$, consider a discrete memoryless channel (DMC)

$$\underset{\text{channel output}}{y} = \underset{\text{channel input}}{x} + \underset{\text{additive error term}}{e} \tag{3}$$

Restrict to: e a realization of a random variable E with

$$\mathbb{P}(E = e) \propto \exp(-\lambda \, \mathrm{wt}_L(e)), \qquad \lambda > 0,$$

$$P_{Y|X}(y|x) = \frac{1}{Z} \exp\left(-\lambda \, \mathrm{d}_L(x, y)\right), \qquad Z := \sum_{e=0}^{q-1} \exp(-\lambda \, \mathrm{wt}_L(e))$$

Note

- The expectation of $\mathrm{wt}_L(E)$, δ, can be written as $\delta = \frac{\mathrm{d} \log Z(\lambda)}{\mathrm{d} \, \lambda}$.
- Defining $p_i := \mathbb{P}(\mathrm{wt}_L(e) = i) = \frac{1}{Z} \exp\left(-\lambda i\right)$ for $i \in \{0, 1, \dots, \lfloor q/2 \rfloor\}$, we easily see

$$p_0 > p_1 \quad \text{and} \quad p_i = \frac{p_1^i}{p_0^{i-1}} \quad \text{for all } i = 2, \dots, \lfloor q/2 \rfloor.$$

The Constant Lee Weight Channel

Consider now $y, x, e \in \mathbb{Z}_q^n$ and $y = x + e$, where e has a fixed Lee weight $t \in \mathbb{Z}$ and is drawn uniformly at random from $\mathcal{S}_{t,q}^n := \left\{ x \in \mathbb{Z}_q^n \;\middle|\; \mathrm{wt}_L(x) = t \right\}$.

The Constant Lee Weight Channel

Consider now $y, x, e \in \mathbb{Z}_q^n$ and $y = x + e$, where e has a fixed Lee weight $t \in \mathbb{Z}$ and is drawn uniformly at random from $\mathcal{S}_{t,q}^n := \left\{x \in \mathbb{Z}_q^n \,\middle|\, \mathrm{wt}_L(x) = t\right\}$.

Theorem

For every $j \in \{1, \ldots, n\}$ the marginal weight distribution of an entry e_j is given by

$$p_i := \mathbb{P}(\mathrm{wt}_L(e_j) = i) = \frac{1}{\sum_{j=0}^{q-1} \exp(-\beta \, \mathrm{wt}_L(j))} \exp\left(-\beta i\right), \forall i \in \{0, \ldots, \lfloor q/2 \rfloor\}$$

where $\beta > 0$ is the solution to $\frac{t}{n} = \frac{(r-1)\mathrm{e}^{(r+1)\beta} - r\mathrm{e}^{r\beta} + \mathrm{e}^{\beta}}{(\mathrm{e}^{\beta r} - 1)(\mathrm{e}^{\beta} - 1)}$ with $r = \lfloor q/2 \rfloor + 1$.

The Constant Lee Weight Channel

Consider now $y, x, e \in \mathbb{Z}_q^n$ and $y = x + e$, where e has a fixed Lee weight $t \in \mathbb{Z}$ and is drawn uniformly at random from $\mathcal{S}_{t,q}^n := \left\{ x \in \mathbb{Z}_q^n \;\middle|\; \mathrm{wt}_L(x) = t \right\}$.

Theorem

For every $j \in \{1, \ldots, n\}$ the marginal weight distribution of an entry e_j is given by

$$p_i := \mathbb{P}(\mathrm{wt}_L(e_j) = i) = \frac{1}{\sum_{j=0}^{q-1} \exp(-\beta\, \mathrm{wt}_L(j))} \exp\left(-\beta i\right), \forall i \in \{0, \ldots, \lfloor q/2 \rfloor\}$$

where $\beta > 0$ is the solution to $\frac{t}{n} = \frac{(r-1)\mathrm{e}^{(r+1)\beta} - r\mathrm{e}^{r\beta} + \mathrm{e}^{\beta}}{(\mathrm{e}^{\beta r} - 1)(\mathrm{e}^{\beta} - 1)}$ with $r = \lfloor q/2 \rfloor + 1$.

Proof idea.
Solve an optimization problem to find a distribution $(p_0, p_1, \ldots, p_{\lfloor q/2 \rfloor})$ that is

... maximizing $H(p_0, \ldots, p_{\lfloor q/2 \rfloor}) := -\sum_{i=0}^{\lfloor q/2 \rfloor} p_i \cdot \log(p_i)$,

... subject to $\sum_{i=0}^{\lfloor q/2 \rfloor} p_i \cdot i = \frac{t}{n}$.

Outline

Integer Partitions

Definition [Integer Partition]

Let $n \in \mathbb{Z}$. An *(integer) partition* of n of length k is a k-tuple $\lambda = (\lambda_1, \ldots, \lambda_k)$ satisfying

1. $\lambda_1 + \ldots + \lambda_k = n$,
2. $\lambda_1 \geq \ldots \geq \lambda_k$.

The elements λ_i are called *parts* and their corresponding values are the *part sizes*.

Integer Partitions

Definition [Integer Partition]

Let $n \in \mathbb{Z}$. An *(integer) partition* of n of length k is a k-tuple $\lambda = (\lambda_1, \ldots, \lambda_k)$ satisfying

1. $\lambda_1 + \ldots + \lambda_k = n$,
2. $\lambda_1 \geq \ldots \geq \lambda_k$.

The elements λ_i are called *parts* and their corresponding values are the *part sizes*.

Example

The following are partitions of $n = 4$: (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)

Integer Partitions

Definition [Integer Partition]

Let $n \in \mathbb{Z}$. An *(integer) partition* of n of length k is a k-tuple $\lambda = (\lambda_1, \ldots, \lambda_k)$ satisfying

1. $\lambda_1 + \ldots + \lambda_k = n$,
2. $\lambda_1 \geq \ldots \geq \lambda_k$.

The elements λ_i are called *parts* and their corresponding values are the *part sizes*.

Example

The following are partitions of $n = 4$: (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)

Definition [Type λ]

Let $t, n \in \mathbb{Z}$, and λ a partition of t. We say an n-tuple x is *of type* λ *over* $\mathbb{Z}_q$ if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of λ.

Integer Partitions

Definition [Integer Partition]

Let $n \in \mathbb{Z}$. An *(integer) partition* of n of length k is a k-tuple $\lambda = (\lambda_1, \ldots, \lambda_k)$ satisfying

1. $\lambda_1 + \ldots + \lambda_k = n$,
2. $\lambda_1 \geq \ldots \geq \lambda_k$.

The elements λ_i are called *parts* and their corresponding values are the *part sizes*.

Example

The following are partitions of $n = 4$: (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)

Definition [Type λ]

Let $t, n \in \mathbb{Z}$, and λ a partition of t. We say an n-tuple x is *of type* λ *over* $\mathbb{Z}_q$ if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of λ.

For a partition λ of t, we will denote the set of all n-tuples of type λ by $\mathcal{V}_{t,\lambda}^{(n)}$.

Tuples of type λ over $\mathbb{Z}_q$

Note: Integer partitions of some type λ over $\mathbb{Z}_q$ have part sizes not exceeding $\lfloor q/2 \rfloor$.

Example

Consider $\mathbb{Z}_5$, $t = n = 4$ and $\lambda = (2, 1, 1)$ a partition of t over $\mathbb{Z}_5$. Then:
$\mathcal{V}^{(4)}_{4,(2,1,1)} = \{(2, 1, 1, 0), (2, 1, 0, 1), \ldots, (1, 2, 1, 0), \ldots, (3, 4, 1, 0), \ldots\}$

Tuples of type λ over $\mathbb{Z}_q$

Note: Integer partitions of some type λ over $\mathbb{Z}_q$ have part sizes not exceeding $\lfloor q/2 \rfloor$.

Example

Consider $\mathbb{Z}_5$, $t = n = 4$ and $\lambda = (2, 1, 1)$ a partition of t over $\mathbb{Z}_5$. Then:
$\mathcal{V}^{(4)}_{4,(2,1,1)} = \{(2, 1, 1, 0), (2, 1, 0, 1), \dots, (1, 2, 1, 0), \dots, (3, 4, 1, 0), \dots\}$

Tuples of type λ over $\mathbb{Z}_q$

Note: Integer partitions of some type λ over $\mathbb{Z}_q$ have part sizes not exceeding $\lfloor q/2 \rfloor$.

Example

Consider $\mathbb{Z}_5$, $t = n = 4$ and $\lambda = (2, 1, 1)$ a partition of t over $\mathbb{Z}_5$. Then:
$\mathcal{V}^{(4)}_{4,(2,1,1)} = \{(2, 1, 1, 0), (2, 1, 0, 1), \ldots, (1, 2, 1, 0), \ldots, (3, 4, 1, 0), \ldots\}$

Lemma

Let n, q and t be positive integers and consider the set of partitions $\mathcal{P}_{\lfloor q/2 \rfloor}(t)$ of t with part sizes not exceeding $\lfloor q/2 \rfloor$. For any $\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)$ the number of vectors of length n over $\mathbb{Z}_q$ of type λ is given by

$$\left|\mathcal{V}^{(n)}_{t,\lambda}\right| = \begin{cases} 2^{\ell_\lambda} \left|\Pi_\lambda\right| \binom{n}{\ell_\lambda} & \text{if } q \text{ is odd,} \\ 2^{\ell_\lambda - c_{\lfloor q/2 \rfloor,\lambda}} \left|\Pi_\lambda\right| \binom{n}{\ell_\lambda} & \text{else} \end{cases} \tag{4}$$

where $c_{\lfloor q/2 \rfloor,\lambda} = |\{i \in \{1, \ldots, \ell_\lambda\} \mid \lambda_i = \lfloor q/2 \rfloor\}|$.

Drawing Tuples of Fixed Lee Weight

Let $\mathcal{S}_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $\mathtt{wt}_L(x) = t$.

Drawing Tuples of Fixed Lee Weight

Let $\mathcal{S}_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$.

Goal: We want to pick an n-tuple x uniformly at random from

$$\mathcal{S}_q^n(t) = \bigsqcup_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \mathcal{V}_{t,\lambda}^{(n)}.$$

Drawing Tuples of Fixed Lee Weight

Let $\mathcal{S}_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$.

Goal: We want to pick an n-tuple x uniformly at random from

$$\mathcal{S}_q^n(t) = \bigsqcup_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \mathcal{V}_{t,\lambda}^{(n)}.$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of t with probability $p_\lambda = \frac{\left|\mathcal{V}_{t,\lambda}^{(n)}\right|}{\sum_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \left|\mathcal{V}_{t,\lambda}^{(n)}\right|}$ over $\mathbb{Z}_q$.

Drawing Tuples of Fixed Lee Weight

Let $\mathcal{S}_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$.
Goal: We want to pick an n-tuple x uniformly at random from

$$\mathcal{S}_q^n(t) = \bigsqcup_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \mathcal{V}_{t,\lambda}^{(n)}.$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of t with probability $p_\lambda = \frac{\left|\mathcal{V}_{t,\lambda}^{(n)}\right|}{\sum_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \left|\mathcal{V}_{t,\lambda}^{(n)}\right|}$ over $\mathbb{Z}_q$.
2. Assign to λ_i an element $a_i \in \mathbb{Z}_q$ with $\mathrm{wt}_L(a_i) = \lambda_i$.

Drawing Tuples of Fixed Lee Weight

Let $\mathcal{S}_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$.
Goal: We want to pick an n-tuple x uniformly at random from

$$\mathcal{S}_q^n(t) = \bigsqcup_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \mathcal{V}_{t,\lambda}^{(n)}.$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1, \dots, \lambda_k)$ of t with probability $p_\lambda = \frac{\left|\mathcal{V}_{t,\lambda}^{(n)}\right|}{\sum_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \left|\mathcal{V}_{t,\lambda}^{(n)}\right|}$ over $\mathbb{Z}_q$.
2. Assign to λ_i an element $a_i \in \mathbb{Z}_q$ with $\mathrm{wt}_L(a_i) = \lambda_i$.
3. Choose randomly k positions of the tuple x and assign the values $a_1, \dots, a_k$ to them.

Drawing Tuples of Fixed Lee Weight

Let $\mathcal{S}_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$.

Goal: We want to pick an n-tuple x uniformly at random from

$$\mathcal{S}_q^n(t) = \bigsqcup_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \mathcal{V}_{t,\lambda}^{(n)}.$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of t with probability $p_\lambda = \frac{\left|\mathcal{V}_{t,\lambda}^{(n)}\right|}{\sum_{\lambda \in \mathcal{P}_{\lfloor q/2 \rfloor}(t)} \left|\mathcal{V}_{t,\lambda}^{(n)}\right|}$ over $\mathbb{Z}_q$.
2. Assign to λ_i an element $a_i \in \mathbb{Z}_q$ with $\mathrm{wt}_L(a_i) = \lambda_i$.
3. Choose randomly k positions of the tuple x and assign the values $a_1, \ldots, a_k$ to them.
4. The remaining entries are zero.

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \Longrightarrow \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_, \_, \_, \_, \_, \_)$ of length 6 with Lee weight $t = 4$.

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \implies \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_,\_,\_,\_,\_,\_)$ of length 6 with Lee weight $t = 4$.

1. The partitions of $t = 4$ with no part exceeding 3 are:
   $(1, 1, 1, 1)$ $(2, 1, 1)$ $(2, 2)$ $(3, 1)$

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \Longrightarrow \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_, \_, \_, \_, \_, \_)$ of length 6 with Lee weight $t = 4$.

1. The partitions of $t = 4$ with no part exceeding 3 are:

(1, 1, 1, 1)	(2, 1, 1)	(2, 2)	(3, 1)
$\left\lvert \mathcal{V}^{(6)}_{4,(1,1,1,1)} \right\rvert = 240$	$\left\lvert \mathcal{V}^{(6)}_{4,(2,1,1)} \right\rvert = 480$	$\left\lvert \mathcal{V}^{(6)}_{4,(2,2)} \right\rvert = 60$	$\left\lvert \mathcal{V}^{(6)}_{4,(3,1)} \right\rvert = 120$

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \Longrightarrow \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_, \_, \_, \_, \_, \_)$ of length 6 with Lee weight $t = 4$.

1. The partitions of $t = 4$ with no part exceeding 3 are:

(1,1,1,1)	(2,1,1)	(2,2)	(3,1)
$\left\|\mathcal{V}^{(6)}_{4,(1,1,1,1)}\right\| = 240$	$\left\|\mathcal{V}^{(6)}_{4,(2,1,1)}\right\| = 480$	$\left\|\mathcal{V}^{(6)}_{4,(2,2)}\right\| = 60$	$\left\|\mathcal{V}^{(6)}_{4,(3,1)}\right\| = 120$

   Say we pick $(\lambda_1, \lambda_2, \lambda_3) = (2, 1, 1)$.

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \Longrightarrow \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_, \_, \_, \_, \_, \_)$ of length 6 with Lee weight $t = 4$.

1. The partitions of $t = 4$ with no part exceeding 3 are:

$(1,1,1,1)$	$(2,1,1)$	$(2,2)$	$(3,1)$
$\left\lvert \mathcal{V}^{(6)}_{4,(1,1,1,1)} \right\rvert = 240$	$\left\lvert \mathcal{V}^{(6)}_{4,(2,1,1)} \right\rvert = 480$	$\left\lvert \mathcal{V}^{(6)}_{4,(2,2)} \right\rvert = 60$	$\left\lvert \mathcal{V}^{(6)}_{4,(3,1)} \right\rvert = 120$

   Say we pick $(\lambda_1, \lambda_2, \lambda_3) = (2, 1, 1)$.
2. Assign to each λ_i an element $a_i \in \mathbb{Z}_7$ with $\mathtt{wt}_L(a_i) = \lambda_i$:

$$\lambda_1 = 2 \longrightarrow 5, \quad \lambda_2 = 1 \longrightarrow 1, \quad \lambda_3 = 1 \longrightarrow 6$$

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \implies \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_, \_, \_, \_, \_, \_)$ of length 6 with Lee weight $t = 4$.

1. The partitions of $t = 4$ with no part exceeding 3 are:
   $(1, 1, 1, 1)$ $\left|\mathcal{V}^{(6)}_{4,(1,1,1,1)}\right| = 240$ $(2, 1, 1)$ $\left|\mathcal{V}^{(6)}_{4,(2,1,1)}\right| = 480$ $(2, 2)$ $\left|\mathcal{V}^{(6)}_{4,(2,2)}\right| = 60$ $(3, 1)$ $\left|\mathcal{V}^{(6)}_{4,(3,1)}\right| = 120$
   Say we pick $(\lambda_1, \lambda_2, \lambda_3) = (2, 1, 1)$.
2. Assign to each λ_i an element $a_i \in \mathbb{Z}_7$ with $\mathrm{wt}_L(a_i) = \lambda_i$:
   $$\lambda_1 = 2 \longrightarrow 5, \quad \lambda_2 = 1 \longrightarrow 1, \quad \lambda_3 = 1 \longrightarrow 6$$
3. Choose randomly 3 positions of x and assign them to one of the above values
   $$x = (\_, 6, \_, 5, 1, \_)$$

DLR

Drawing Tuples of Fixed Lee Weight

Example

Consider $\mathbb{Z}_7 \Longrightarrow \lfloor 7/2 \rfloor = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (\_,\_,\_,\_,\_,\_)$ of length 6 with Lee weight $t = 4$.

1. The partitions of $t = 4$ with no part exceeding 3 are:

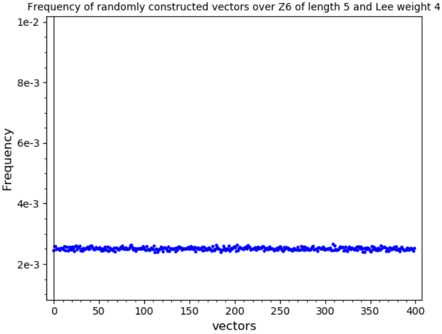
$(1,1,1,1)$	$(2,1,1)$	$(2,2)$	$(3,1)$
$\left\lvert \mathcal{V}^{(6)}_{4,(1,1,1,1)} \right\rvert = 240$	$\left\lvert \mathcal{V}^{(6)}_{4,(2,1,1)} \right\rvert = 480$	$\left\lvert \mathcal{V}^{(6)}_{4,(2,2)} \right\rvert = 60$	$\left\lvert \mathcal{V}^{(6)}_{4,(3,1)} \right\rvert = 120$

   Say we pick $(\lambda_1, \lambda_2, \lambda_3) = (2, 1, 1)$.
2. Assign to each λ_i an element $a_i \in \mathbb{Z}_7$ with $\mathrm{wt}_L(a_i) = \lambda_i$:
   $$\lambda_1 = 2 \longrightarrow 5, \quad \lambda_2 = 1 \longrightarrow 1, \quad \lambda_3 = 1 \longrightarrow 6$$
3. Choose randomly 3 positions of x and assign them to one of the above values
   $$x = (\_, 6, \_, 5, 1, \_)$$
4. $x = (0, 6, 0, 5, 1, 0)$

Distribution

Theorem

Let n, q and t be positive integers. The when sampling a sufficiently large number of n-tuples using the before shown algorithm, we obtain a uniform distribution on $\mathcal{S}_q^n(t)$.



Outline

Generic Decoding

Assume we receive a vector $y = \underbrace{x}_{\text{original message}} + \underbrace{e}_{\text{error vector}}$.

Generic Decoding

Assume we receive a vector $y = \underbrace{x}_{\text{original message}} + \underbrace{e}_{\text{error vector}}$.

Generic Decoding

An adversary wants to find either the message or the random error.

Generic Decoding

Assume we receive a vector $y = \underset{\text{original message}}{x} + \underset{\text{error vector}}{e}$.

Generic Decoding

An adversary wants to find either the message or the random error.

Solutions to this problem

- A unique solution exists if the weight of the error is relatively small.

Generic Decoding

Assume we receive a vector $y = \underbrace{x}_{\text{original message}} + \underbrace{e}_{\text{error vector}}$.

Generic Decoding

An adversary wants to find either the message or the random error.

Solutions to this problem

- A unique solution exists if the weight of the error is relatively small.
- Information set decoding (ISD) is a method to find e.

Generic Decoding

Assume we receive a vector $y = \underset{\text{original message}}{x} + \underset{\text{error vector}}{e}$.

Generic Decoding

An adversary wants to find either the message or the random error.

Solutions to this problem

- A unique solution exists if the weight of the error is relatively small.
- Information set decoding (ISD) is a method to find e.

  Is NP-hard for the Hamming- and the Lee metric.

Introduction to the Problem

Example 1

Let $x = (0, 2, 3, 1, 0, 3) \in \mathbb{Z}_5^6$

Lee $\mathrm{wt}_L(x) = 7$, Hamming $\mathrm{wt}_H(x) = 4$

Introduction to the Problem

Example 1	Lee	Hamming
Let $x = (0, 2, 3, 1, 0, 3) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 7,$	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 1, 2, 0, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 4$

DLR

Introduction to the Problem

	Lee	Hamming
Example 1		
Let $x = (0, 2, 3, 1, 0, 3) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 7$,	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 1, 2, 0, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5$,	$\mathrm{wt}_H(x) = 4$

	Lee	Hamming
Example 2		
Let $x = (0, 1, 3, 4, 1, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5$,	$\mathrm{wt}_H(x) = 5$

DLR

Introduction to the Problem

	Lee	Hamming
Example 1		
Let $x = (0, 2, 3, 1, 0, 3) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 7,$	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 1, 2, 0, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 4$
Example 2		
Let $x = (0, 1, 3, 4, 1, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 5$
$2x = (0, 2, 1, 3, 2, 2) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 9,$	$\mathrm{wt}_H(x) = 5$

DLR

Introduction to the Problem

Example 1	Lee	Hamming
Let $x = (0, 2, 3, 1, 0, 3) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 7,$	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 1, 2, 0, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 4$

Example 2	Lee	Hamming
Let $x = (0, 1, 3, 4, 1, 1) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 5$
$2x = (0, 2, 1, 3, 2, 2) \in \mathbb{Z}_5^6$	$\mathrm{wt}_L(x) = 9,$	$\mathrm{wt}_H(x) = 5$

Why can decreasing the Lee weight be a problem?

Generic (or syndrome) decoding is based on the weight of the error term.

- The smaller this weight, the easier to find a solution.

Introduction to the Problem

	Lee	Hamming
Example 1		
Let $x = (0,2,3,1,0,3) \in \mathbb{Z}_5^6$	$\text{wt}_L(x) = 7$,	$\text{wt}_H(x) = 4$
$2x = (0,4,1,2,0,1) \in \mathbb{Z}_5^6$	$\text{wt}_L(x) = 5$,	$\text{wt}_H(x) = 4$
Example 2		
Let $x = (0,1,3,4,1,1) \in \mathbb{Z}_5^6$	$\text{wt}_L(x) = 5$,	$\text{wt}_H(x) = 5$
$2x = (0,2,1,3,2,2) \in \mathbb{Z}_5^6$	$\text{wt}_L(x) = 9$,	$\text{wt}_H(x) = 5$

Why can decreasing the Lee weight be a problem?

Generic (or syndrome) decoding is based on the weight of the error term.

- The smaller this weight, the easier to find a solution.

Risk: From a cryptographic point of view, an attacker could decrease the weight and retrieve the original message.

Problem Statement

Problem

Consider the ring of integers $\mathbb{Z}_q$, with $q > 3$. Given a tuple $x \in \mathbb{Z}_q^n$ of average Lee weight $\delta = t/n$ per entry. Let $a \in \mathbb{Z}_q$ be a nonzero element, find the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x, i.e.

$$\mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\right) \tag{5}$$

Problem Statement

Problem

Consider the ring of integers $\mathbb{Z}_q$, with $q > 3$. Given a tuple $x \in \mathbb{Z}_q^n$ of average Lee weight $\delta = t/n$ per entry. Let $a \in \mathbb{Z}_q$ be a nonzero element, find the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x, i.e.

$$\mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\right) \tag{5}$$

Note

To give an answer to that question we need to understand

Problem Statement

Problem

Consider the ring of integers $\mathbb{Z}_q$, with $q > 3$. Given a tuple $x \in \mathbb{Z}_q^n$ of average Lee weight $\delta = t/n$ per entry. Let $a \in \mathbb{Z}_q$ be a nonzero element, find the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x, i.e.

$$\mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\right) \tag{5}$$

Note

To give an answer to that question we need to understand

1. the way x is generated,

Problem Statement

Problem

Consider the ring of integers $\mathbb{Z}_q$, with $q > 3$. Given a tuple $x \in \mathbb{Z}_q^n$ of average Lee weight $\delta = t/n$ per entry. Let $a \in \mathbb{Z}_q$ be a nonzero element, find the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x, i.e.

$$\mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\right) \tag{5}$$

Note

To give an answer to that question we need to understand

1. the way x is generated,
2. the distribution of the entries of x.

Problem Statement

Problem

Consider the ring of integers $\mathbb{Z}_q$, with $q > 3$. Given a tuple $x \in \mathbb{Z}_q^n$ of average Lee weight $\delta = t/n$ per entry. Let $a \in \mathbb{Z}_q$ be a nonzero element, find the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x, i.e.

$$\mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\right) \tag{5}$$

Note

To give an answer to that question we need to understand

1. the way x is generated,
2. the distribution of the entries of x.

Goal: We want this probability to be small!

Preparation

Let us consider the following setup.

- $x \in \mathbb{Z}_q^n$ with average Lee weight $\delta = t/n$ drawn as shown,
- Q the empirical distribution of the entries of x

Preparation

Let us consider the following setup.

- $x \in \mathbb{Z}_q^n$ with average Lee weight $\delta = t/n$ drawn as shown,
- Q the empirical distribution of the entries of x
- $a \in \mathbb{Z}_q \backslash \{0\}$ be chosen uniformly at random,

Preparation

Let us consider the following setup.

- $x \in \mathbb{Z}_q^n$ with average Lee weight $\delta = t/n$ drawn as shown,
- Q the empirical distribution of the entries of x
- $a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,
- $F := \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$.

Preparation

Let us consider the following setup.

- $x \in \mathbb{Z}_q^n$ with average Lee weight $\delta = t/n$ drawn as shown,
- Q the empirical distribution of the entries of x
- $a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,
- $F := \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$.
- $\mathcal{B}$ the marginal distribution of the constant Lee weight channel model $p_i := \mathbb{P}(\mathrm{wt}_L(x_j) = i) = \kappa \exp(-\beta i), \forall i \in \{0, \ldots, \lfloor q/2 \rfloor\}$.

Preparation

Let us consider the following setup.

- $x \in \mathbb{Z}_q^n$ with average Lee weight $\delta = t/n$ drawn as shown,
- Q the empirical distribution of the entries of x
- $a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,
- $F := \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$.
- $\mathcal{B}$ the marginal distribution of the constant Lee weight channel model $p_i := \mathbb{P}(\mathrm{wt}_L(x_j) = i) = \kappa \exp(-\beta i), \forall i \in \{0, \dots, \lfloor q/2 \rfloor\}$.

Applying the union bound, we have

$$\begin{aligned}\mathbb{P}(F) &= \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right)\mathbb{P}\left(Q \text{ is "close" to } \mathcal{B}\right) \\ &\quad + \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "not close" to } \mathcal{B}\right)\mathbb{P}\left(Q \text{ is "not close" to } \mathcal{B}\right) \\ &\leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right) + \mathbb{P}\left(Q \text{ is "not close" to } \mathcal{B}\right)\end{aligned}$$

"Close" Distributions

Definition [Kullback-Leibler divergence]

Let X be a random variable over an alphabet $\mathcal{X}$ with probability distribution P, where $P(x) := \mathbb{P}(X = x)$. Furthermore, let us assume that X can approximated by another distribution $Q \neq P$. We define the *Kullback-Leibler divergence* of Q and P by

$$D(Q \,||\, P) := \sum_{x \in \mathcal{X}} Q(x) \log \left(\frac{Q(x)}{P(x)} \right) \tag{6}$$

Note

- By convention: $0 \log(0) = 0$.
- An approximated distribution Q is *close* to the exact distribution P, if $D(Q \,||\, P) \leq \varepsilon$, for some $\varepsilon > 0$.

DLR

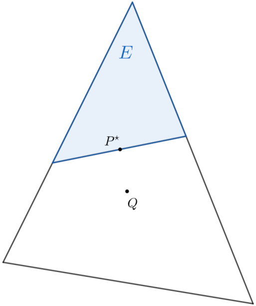
Conditional Limit Theorem

Theorem
Conditional Limit Theorem

Let E be a closed convex set of probability distributions over an alphabet $\mathcal{X}$ and let Q be a distribution over $\mathcal{X}$ but not in E. Let $X_1, \ldots, X_n$ be discrete random variables drawn i.i.d. $\sim Q$. Define $X^n = (X_1, \ldots, X_n)$ and let $P^\star = \arg\min_{P \in E} D(P \,||\, Q)$. Then

$$\mathbb{P}\left(X_1 = a \,|\, P_{X^n} \in E\right) \longrightarrow P^\star(a)$$

in probability as n grows large for any $a \in \mathcal{X}$.
[4]



[4] Thomas M Cover. *Elements of information theory*. John Wiley & Sons, 1999

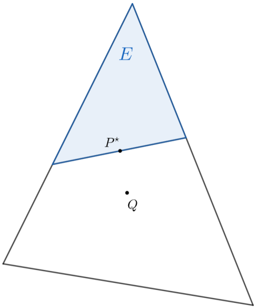
Conditional Limit Theorem

Theorem
Conditional Limit Theorem

Let E be a closed convex set of probability distributions over an alphabet $\mathcal{X}$ and let Q be a distribution over $\mathcal{X}$ but not in E. Let $X_1, \ldots, X_n$ be discrete random variables drawn i.i.d. $\sim Q$. Define $X^n = (X_1, \ldots, X_n)$ and let $P^\star = \arg\min_{P \in E} D(P \,||\, Q)$. Then

$$\mathbb{P}\left(X_1 = a \,|\, P_{X^n} \in E\right) \longrightarrow P^\star(a)$$

in probability as n grows large for any $a \in \mathcal{X}$.
[4]



In our case:

$Q \sim \mathcal{U}(\mathbb{Z}_q)$; E set of distributions of tuples in $\mathcal{S}_q^n(t)$. Then $\mathcal{B} = \arg\min_{P \in E} D(P \,||\, Q)$.

[4] Cover, *Elements of information theory*

Asymptotic Regime

Recall, $F = \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$ and

$$\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right) + \mathbb{P}\left(Q \text{ is "not close" to } \mathcal{B}\right)$$

Asymptotic Regime

Recall, $F = \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$ and

$$\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right) + \mathbb{P}\left(Q \text{ is "not close" to } \mathcal{B}\right)$$

Theorem

Let $x \in \mathbb{Z}_q^n$, for some positive integer $q > 3$, of average Lee weight $\delta = t/n$ be drawn randomly from $\mathcal{S}_q^n(t)$ with the shown algorithm. Let Q denote the empirical distribution of the entries of x. For any nonzero $a \in \mathbb{Z}_q$ it holds

$$\mathbb{P}\left(Q \text{ not close to } \mathcal{B}\right) \longrightarrow 0 \text{ as } n \longrightarrow \infty.$$

Asymptotic Regime

Recall, $F = \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$ and

$$\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right) + \mathbb{P}\left(Q \text{ is "not close" to } \mathcal{B}\right)$$

Theorem

Let $x \in \mathbb{Z}_q^n$, for some positive integer $q > 3$, of average Lee weight $\delta = t/n$ be drawn randomly from $\mathcal{S}_q^n(t)$ with the shown algorithm. Let Q denote the empirical distribution of the entries of x. For any nonzero $a \in \mathbb{Z}_q$ it holds

$$\mathbb{P}\left(Q \text{ not close to } \mathcal{B}\right) \longrightarrow 0 \text{ as } n \longrightarrow \infty.$$

Hence

As $n \longrightarrow \infty$, $\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right)$.

Asymptotic Regime

Recall, $F = \{\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x)\}$ and

$$\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right) + \mathbb{P}\left(Q \text{ is "not close" to } \mathcal{B}\right)$$

Theorem

Let $x \in \mathbb{Z}_q^n$, for some positive integer $q > 3$, of average Lee weight $\delta = t/n$ be drawn randomly from $\mathcal{S}_q^n(t)$ with the shown algorithm. Let Q denote the empirical distribution of the entries of x. For any nonzero $a \in \mathbb{Z}_q$ it holds

$$\mathbb{P}\left(Q \text{ not close to } \mathcal{B}\right) \longrightarrow 0 \text{ as } n \longrightarrow \infty.$$

Hence

As $n \longrightarrow \infty$, $\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \text{ is "close" to } \mathcal{B}\right)$.
By CLT $\leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \sim \mathcal{B}\right)$

DLR

Asymptotic Regime

$$\begin{aligned}\mathbb{P}(F) &\leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \sim \mathcal{B}\right) \\ &= \mathbb{P}\left(\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}\, \mathrm{wt}_L([a \cdot i]_q) < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i} i\right) \\ &= \mathbb{P}\left(0 < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q))\right)\end{aligned}$$

Asymptotic Regime

$$
\begin{aligned}
\mathbb{P}(F) &\leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \,|\, Q \sim \mathcal{B}\right) \\
&= \mathbb{P}\left(\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}\, \mathrm{wt}_L([a \cdot i]_q) < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i} i\right) \\
&= \mathbb{P}\left(0 < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q))\right)
\end{aligned}
$$

Note

- Recall: β **depends on** t/n but stays invariant as $n \longrightarrow \infty$.

Asymptotic Regime

$$\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \sim \mathcal{B}\right)$$
$$= \mathbb{P}\left(\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}\, \mathrm{wt}_L([a \cdot i]_q) < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i} i\right)$$
$$= \mathbb{P}\left(0 < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q))\right)$$

Note

- Recall: β **depends on** t/n but stays invariant as $n \longrightarrow \infty$.
- The difference $(i - \mathrm{wt}_L([a \cdot i]_q))$ **depends on** q.

Asymptotic Regime

$$
\begin{aligned}
\mathbb{P}(F) &\leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \sim \mathcal{B}\right) \\
&= \mathbb{P}\left(\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}\, \mathrm{wt}_L([a \cdot i]_q) < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i} i\right) \\
&= \mathbb{P}\left(0 < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q))\right)
\end{aligned}
$$

Note

- Recall: β **depends on** t/n but stays invariant as $n \longrightarrow \infty$.
- The difference $(i - \mathrm{wt}_L([a \cdot i]_q))$ **depends on** q.

Question: What is the maximal value $\delta^\star$ of the average Lee weight per entry such that $\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q)) \leq 0$?

Asymptotic Regime

$$\mathbb{P}(F) \leq \mathbb{P}\left(\mathrm{wt}_L(a \cdot x) < \mathrm{wt}_L(x) \mid Q \sim \mathcal{B}\right)$$
$$= \mathbb{P}\left(\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}\, \mathrm{wt}_L([a \cdot i]_q) < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i} i\right)$$
$$= \mathbb{P}\left(0 < \sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q))\right)$$

Note

- Recall: β **depends on** t/n but stays invariant as $n \longrightarrow \infty$.
- The difference $(i - \mathrm{wt}_L([a \cdot i]_q))$ **depends on** q.

Question: What is the maximal value $\delta^\star$ of the average Lee weight per entry such that $\sum_{i=1}^{\lfloor q/2 \rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a \cdot i]_q)) \leq 0$?

q	5	7	8	9	11	31	33	53
$\lfloor q/2 \rfloor$	2	3	4	4	5	15	16	26
$\delta^\star$	1	1.5	1.534	1.703	2.5	7.5	7.03	13

Asymptotic Regime

$$\begin{aligned}\mathbb{P}(F) &\leq \mathbb{P}\left(\mathrm{wt}_L(a\cdot x) < \mathrm{wt}_L(x) \mid Q\sim\mathcal{B}\right)\\ &= \mathbb{P}\left(\sum_{i=1}^{\lfloor q/2\rfloor} \mathrm{e}^{-\beta i}\,\mathrm{wt}_L([a\cdot i]_q) < \sum_{i=1}^{\lfloor q/2\rfloor} \mathrm{e}^{-\beta i} i\right)\\ &= \mathbb{P}\left(0 < \sum_{i=1}^{\lfloor q/2\rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a\cdot i]_q))\right)\end{aligned}$$

Note

- Recall: β **depends on** t/n but stays invariant as $n \longrightarrow \infty$.
- The difference $(i - \mathrm{wt}_L([a\cdot i]_q))$ **depends on** q.

Question: What is the maximal value $\delta^\star$ of the average Lee weight per entry such that $\sum_{i=1}^{\lfloor q/2\rfloor} \mathrm{e}^{-\beta i}(i - \mathrm{wt}_L([a\cdot i]_q)) \leq 0$?

q	5	7	8	9	11	31	33	53
$\lfloor q/2\rfloor$	2	3	4	4	5	15	16	26
$\delta^\star$	1	1.5	1.534	1.703	2.5	7.5	7.03	13

Thank you for your attention!