

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



Knowledge for Tomorrow

Outline

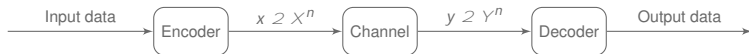
- 1 Introduction
- 2 The Lee Channel
- 3 Error Pattern Construction
- 4 Scalar Multiplication in the Lee Metric

Outline

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

Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.

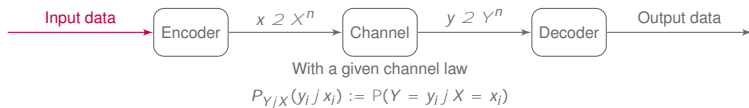


With a given channel law

$$P_{Y|X}(y_j | x_i) := P(Y = y_j | X = x_i)$$

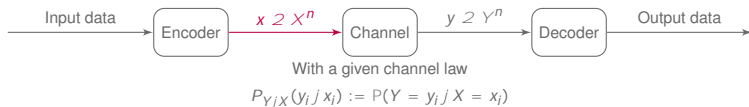
Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



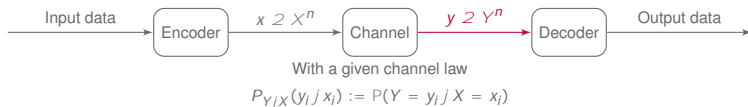
Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



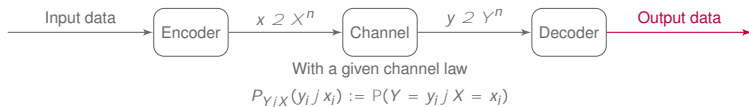
Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



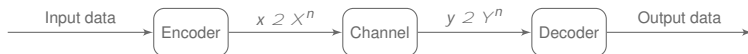
Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.

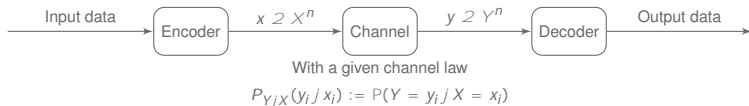


With a given channel law

$$P_{Y|X}(y_j | x_i) := P(Y = y_j | X = x_i)$$

Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



Example: q -ary Symmetric Channel (q SC)

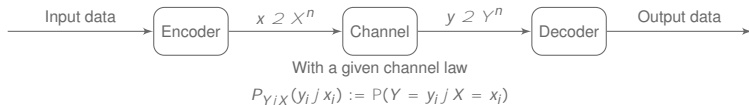
Alphabets:

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

Input	Output
0	0
1	1
⋮	⋮
$q-1$	$q-1$

Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



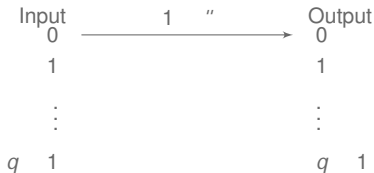
Example: q -ary Symmetric Channel (q SC)

Alphabets:

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

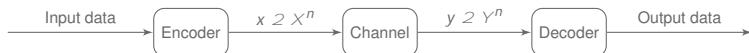
Probability of correct transmission:

$$1 - \frac{1}{q}$$



Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



With a given channel law

$$P_{Y_j|X}(y_j | x_i) := P(Y = y_j | X = x_i)$$

Example: q -ary Symmetric Channel (q SC)

Alphabets:

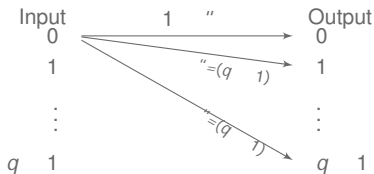
$$X = Y = \{0, 1, \dots, q-1\}$$

Probability of correct transmission:

$$1 - \frac{1}{q}$$

Probability of error for every possible

$$\text{outcome: } \frac{1}{q}$$



Channel Coding

Let X and Y the input and output alphabet of the channel, respectively.



With a given channel law

$$P_{Y|X}(y_j | x_i) := P(Y = y_j | X = x_i)$$

Example: q -ary Symmetric Channel (q SC)

Alphabets:

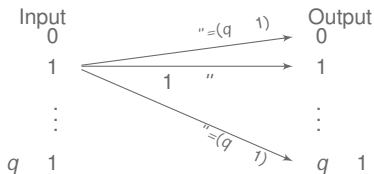
$$X = Y = \{0, 1, \dots, q-1\}$$

Probability of correct transmission:

$$1/q$$

Probability of error for every possible

$$\text{outcome: } (q-1)/q$$



Linear Block Codes

Let 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 $C \subseteq F_q^n$ is a k -dimensional subspace of F_q^n . The elements of C are called *codewords*.

Linear Block Codes

Let 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 $C \subseteq F_q^n$ is a k -dimensional subspace of F_q^n . The elements of C are called codewords.

Example

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

Linear Block Codes

Let 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 $C \subseteq F_q^n$ is a k -dimensional subspace of F_q^n . The elements of C are called codewords.

Example

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

Definition [Hamming Weight/Distance]

For any two codewords $x; y \in C$ we define

the Hamming weight of x , $wt_H(x) = \sum_{i=1}^n \mathbb{1}_{x_i \neq 0}$

the Hamming distance between x and y , $d_H(x; y) := wt_H(x - y)$

The Lee Metric

We will denote by Z_q the ring of integers modulo q .

Definition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is defined as

$$wt_L(a) := \min(|a|, q - |a|) \quad (1)$$

The Lee Metric

We will denote by Z_q the ring of integers modulo q .

Definition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is defined as

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

Example: Consider Z_5 . The Lee weight of $a = 3$ is

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

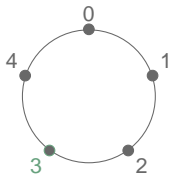
The Lee Metric

We will denote by Z_q the ring of integers modulo q .

Definition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is defined as

$$wt_L(a) := \min(|a|, q - |a|) \quad (1)$$



Example: Consider Z_5 . The Lee weight of $a = 3$ is

$$wt_L(3) = \min(|3|, 5 - |3|) = 2$$

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

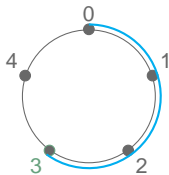
The Lee Metric

We will denote by Z_q the ring of integers modulo q .

Definition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is defined as

$$wt_L(a) := \min(|a|, q - |a|) \quad (1)$$



Example: Consider Z_5 . The Lee weight of $a = 3$ is

$$wt_L(3) = \min(|3|, 5 - |3|) = 2$$

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

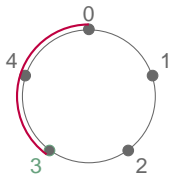
The Lee Metric

We will denote by Z_q the ring of integers modulo q .

Definition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is defined as

$$wt_L(a) := \min(|a|, q - |a|) \quad (1)$$



Example: Consider Z_5 . The Lee weight of $a = 3$ is

$$wt_L(3) = \min(|3|, 5 - |3|) = 2$$

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

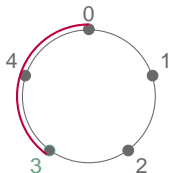
The Lee Metric

We will denote by Z_q the ring of integers modulo q .

Definition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is defined as

$$wt_L(a) := \min(|a|, q - |a|) \quad (1)$$



Example: Consider Z_5 . The Lee weight of $a = 3$ is

$$wt_L(3) = \min(|3|, 5 - |3|) = 2$$

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

$$\Rightarrow wt_L(3) = 2$$

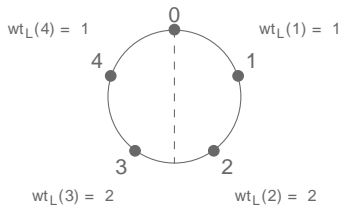
The Lee Metric

Properties

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

$$wt_L(a) = wt_L(q - a)$$

Example



The Lee Metric

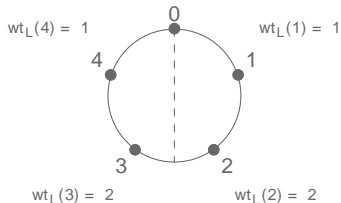
Properties

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

$$wt_L(a) = wt_L(q - a)$$

$$wt_L(a) \leq \lfloor q/2 \rfloor$$

Example



The Lee Metric

Properties

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

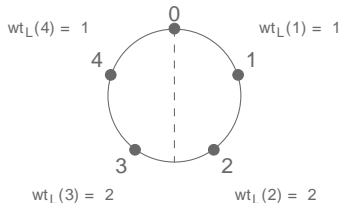
$$wt_L(a) = wt_L(q - a)$$

$$wt_L(a) \leq \lfloor \frac{q}{2} \rfloor$$

$$wt_H(a) \leq wt_L(a)$$

If $q \equiv 2 \pmod{4}$, the Lee weight is equivalent to the Hamming weight.

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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

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.,

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

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

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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

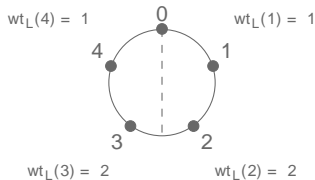
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) =$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

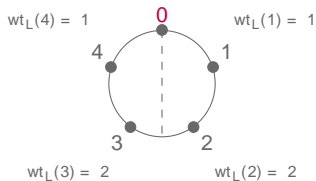
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

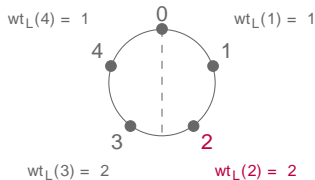
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

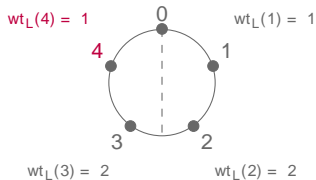
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2 + 1$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

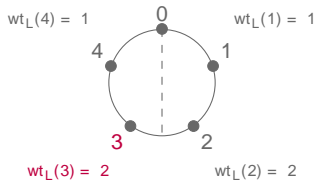
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2 + 1 + 2$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

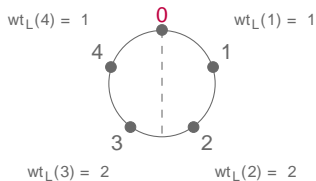
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2 + 1 + 2 + 0$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

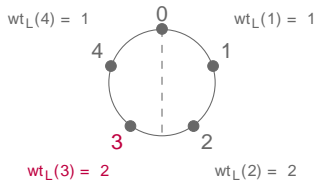
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2 + 1 + 2 + 0 + 2$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

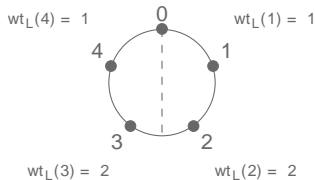
The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2 + 1 + 2 + 0 + 2 = 7$$



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.,

$$wt_L(x) := \sum_{i=1}^n wt_L(x_i) \quad (2)$$

The Lee distance between two tuples $x, y \in \mathbb{Z}_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x - y)$.

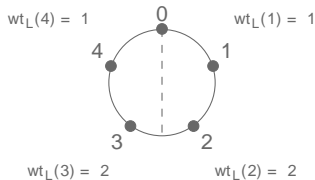
Example:

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

$$x = (0; 2; 4; 3; 0; 3)$$

$$wt_L(x) = 0 + 2 + 1 + 2 + 0 + 2 = 7$$

$$wt_H(x) = 4$$



Why Lee Metric?

Transmitting symbols over a nonbinary noisy channel
! 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

! 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

! 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

! 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

! 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 Metric¹

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

²Paolo 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

! 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 Metric¹
- | Low-Lee-Density Parity-Check Codes were defined²

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

²Paolo 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

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

The Lee Channel

Originally introduced by Chiang and Wolf³.

³J 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 Wolf³.

Assume the alphabet is Z_q .

Goal: Describe $P(i \rightarrow j) = P(i \rightarrow j + 0)$.

0

$b \ q=2c$

\vdots

1

0

1

\vdots

$bq=2c$

³J 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

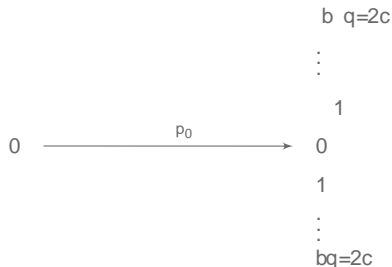
Originally introduced by Chiang and Wolf³.

Assume the alphabet is Z_q .

Goal: Describe $P(i|j) = P(i \rightarrow j|0)$.

Define for every $i = 0; \dots; bq=2c$

$$p_i := P(i|j) = P(i \rightarrow j|0)$$



³J 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

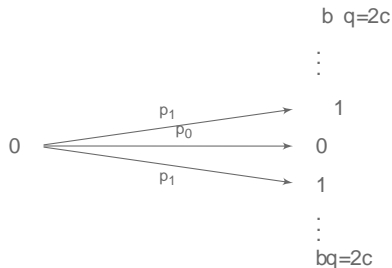
Originally introduced by Chiang and Wolf³.

Assume the alphabet is Z_q .

Goal: Describe $P(i|j) = P(i \rightarrow j|0)$.

Define for every $i = 0, \dots, bq=2c$

$$p_i := P(i|j) = P(i \rightarrow j|0)$$



³J 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

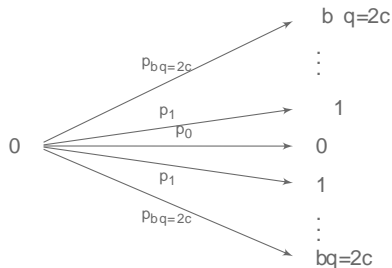
Originally introduced by Chiang and Wolf³.

Assume the alphabet is Z_q .

Goal: Describe $P(i|j) = P(i \text{ } j|j|0)$.

Define for every $i = 0; \dots; bq=2c$

$$p_i := P(i|j|0) = P(i \text{ } j|0)$$



³J 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 Law

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

$$\begin{array}{c} y \\ \text{channel output} \end{array} = \begin{array}{c} x \\ \text{channel input} \end{array} + \begin{array}{c} e \\ \text{additive error term} \end{array} \quad (3)$$

The Lee Channel Law

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

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

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

$$P(E = e) / \exp(-\text{wt}_L(e)); \quad > 0;$$

$$P_{Y|X}(y|x) = \frac{1}{Z} \exp(-d_L(x; y)); \quad Z := \sum_{e=0}^{q-1} \exp(-\text{wt}_L(e))$$

The Lee Channel Law

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

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

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

$$P(E = e) \propto \exp(-wt_L(e)); \quad w > 0;$$

$$P_{Y|X}(y|x) = \frac{1}{Z} \exp(-d_L(x; y)); \quad Z := \sum_{e=0}^{q-1} \exp(-wt_L(e))$$

Note

The expectation of $wt_L(E)$, $\mathbb{E}[wt_L(E)]$, can be written as $\mathbb{E}[wt_L(E)] = \frac{d \log Z(\cdot)}{d}$:

Defining $p_i := P(wt_L(e) = i) = \frac{1}{Z} \exp(-i)$ for $i \in \{0, 1, \dots, bq=2c\}$, we easily see

$$p_0 > p_1 \quad \text{and} \quad p_i = \frac{p_1^i}{p_0^{i-1}} \quad \text{for all } i = 2, \dots, bq=2c:$$

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 $S_{t;q}^n := \{x \in \mathbb{Z}_q^n \mid \text{wt}_L(x) = t\}$:

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 $S_{t;q}^n := \{x \in \mathbb{Z}_q^n \mid \text{wt}_L(x) = t\}$:

Theorem

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

$$p_i := P(\text{wt}_L(e_j) = i) = \frac{1}{\sum_{j=0}^{q-1} \exp(-\text{wt}_L(j))} \exp(-i); \quad i \in \{0, \dots, bq=2c\}$$

where $\lambda > 0$ is the solution to $\frac{t}{n} = \frac{(r-1)e^{(r+1)} - re^r + e}{(e^r - 1)(e - 1)}$ with $r = bq=2c + 1$.

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 $S_{t;q}^n := \{x \in \mathbb{Z}_q^n \mid \text{wt}_L(x) = t\}$:

Theorem

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

$$p_i := P(\text{wt}_L(e_j) = i) = \frac{1}{\sum_{j=0}^{bq-1} \exp(-\frac{r}{2} \text{wt}_L(j))} \exp(-\frac{r}{2} i); \quad i \in \{0, \dots, bq-1\}; \quad bq=2c$$

where $r > 0$ is the solution to $\frac{t}{n} = \frac{(r-1)e^{(r+1)} - re^r + e}{(e^{r-1}-1)(e^r-1)}$ with $r = bq=2c + 1$.

Proof idea.

Solve an optimization problem to find a distribution $(p_0; p_1; \dots; p_{bq=2c})$ that is

$$\begin{aligned} \dots & \text{ maximizing } H(p_0; \dots; p_{bq=2c}) := \sum_{i=0}^{bq=2c} p_i \log(p_i), \\ \dots & \text{ subject to } \sum_{i=0}^{bq=2c} p_i = \frac{t}{n}. \end{aligned}$$

Outline

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

Integer Partitions

Definition [Integer Partition]

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

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

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 $\lambda = (\lambda_1; \dots; \lambda_k)$ satisfying

1. $\lambda_1 + \dots + \lambda_k = n$,
2. $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$.

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 $\lambda = (\lambda_1; \dots; \lambda_k)$ satisfying

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

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 $\lambda = (\lambda_1; \dots; \lambda_k)$ satisfying

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

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 $V_t^{(n)}$.

Tuples of type λ over Z_q

Note: Integer partitions of some type λ over Z_q have part sizes not exceeding $bq=2c$.

Example

Consider Z_5 , $t = n = 4$ and $\lambda = (2; 1; 1)$ a partition of t over Z_5 . Then:

$$V_{4;(2; 1; 1)}^{(4)} = f(2; 1; 1; 0); (2; 1; 0; 1); \dots; (1; 2; 1; 0); \dots; (3; 4; 1; 0); \dots; g$$

Tuples of type λ over Z_q

Note: Integer partitions of some type λ over Z_q have part sizes not exceeding $bq=2c$.

Example

Consider Z_5 , $t = n = 4$ and $\lambda = (2; 1; 1)$ a partition of t over Z_5 . Then:

$$V_{4;(2; 1; 1)}^{(4)} = f(2; 1; 1; 0); (2; 1; 0; 1); \dots; (1; 2; 1; 0); \dots; (3; 4; 1; 0); \dots; g$$

Tuples of type λ over Z_q

Note: Integer partitions of some type λ over Z_q have part sizes not exceeding $bq=2c$.

Example

Consider Z_5 , $t = n = 4$ and $\lambda = (2; 1; 1)$ a partition of t over Z_5 . Then:

$$V_{4;(2; 1; 1)}^{(4)} = f(2; 1; 1; 0); (2; 1; 0; 1); \dots; (1; 2; 1; 0); \dots; (3; 4; 1; 0); \dots; g$$

Lemma

Let $n; q$ and t be positive integers and consider the set of partitions $P_{bq=2c}(t)$ of t with part sizes not exceeding $bq=2c$. For any $\lambda \in P_{bq=2c}(t)$ the number of vectors of length n over Z_q of type λ is given by

$$V_{t;\lambda}^{(n)} = \begin{cases} 2^{\sum_j j} \cdot j! \cdot n^{\sum_j j} & \text{if } q \text{ is odd;} \\ 2^{\sum_j c_{bq=2c; j}} \cdot j! \cdot n^{\sum_j j} & \text{else} \end{cases} \quad (4)$$

where $c_{bq=2c; j} = \sum_i f_i \cdot 2^i \cdot 1; \dots; \sum_j g_j \cdot i = bq=2cg_j$.

Drawing Tuples of Fixed Lee Weight

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

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \bigcup_{\substack{G \\ 2^P \mid |G| = 2c(t)}} V_{t;G}^{(n)}$$

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \sum_{\substack{G \\ 2^P \mid b_{q=2c}(t)}} V_{t; }^{(n)}$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1; \dots; \lambda_k)$ of t with probability

$$p = \frac{V_{t; }^{(n)}}{\sum_{\substack{G \\ 2^P \mid b_{q=2c}(t)}} V_{t; }^{(n)}} \text{ over } Z_q.$$

Drawing Tuples of Fixed Lee Weight

Let $S_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $wt_L(x) = t$.

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

$$S_q^n(t) = \sum_{\substack{G \\ 2^P \mid bq=2c(t)}} V_{t_i}^{(n)}$$

Idea

1. Choose an integer partition $\rho = (\rho_1; \dots; \rho_k)$ of t with probability

$$p = \frac{V_{t_i}^{(n)}}{\sum_{\substack{G \\ 2^P \mid bq=2c(t)}} V_{t_i}^{(n)}} \text{ over } \mathbb{Z}_q.$$

2. Assign to ρ_i an element $a_i \in \mathbb{Z}_q$ with $wt_L(a_i) = \rho_i$.

Drawing Tuples of Fixed Lee Weight

Let $S_q^n(t)$ the set of all tuples $x \in Z_q^n$ with $w_L(x) = t$.

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

$$S_q^n(t) = \sum_{\substack{G \\ 2^P \mid b_{q=2c}(t)}} V_{t_i}^{(n)}$$

Idea

1. Choose an integer partition $\rho = (\rho_1; \dots; \rho_k)$ of t with probability

$$p = \frac{V_{t_i}^{(n)}}{\sum_{\substack{G \\ 2^P \mid b_{q=2c}(t)}} V_{t_i}^{(n)}} \text{ over } Z_q.$$

2. Assign to ρ_i an element $a_i \in Z_q$ with $w_L(a_i) = \rho_i$.
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 $S_q^n(t)$ the set of all tuples $x \in \mathbb{Z}_q^n$ with $wt_L(x) = t$.

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

$$S_q^n(t) = \sum_{\substack{G \\ 2^P \mid bq=2c(t)}} V_{t; i}^{(n)}$$

Idea

1. Choose an integer partition $\rho = (i_1; \dots; i_k)$ of t with probability

$$p = \frac{V_{t; i}^{(n)}}{\sum_{\substack{G \\ 2^P \mid bq=2c(t)}} V_{t; i}^{(n)}} \text{ over } \mathbb{Z}_q.$$

2. Assign to i_j an element $a_i \in \mathbb{Z}_q$ with $wt_L(a_i) = i_j$.
3. Choose randomly k positions of the tuple x and assign the values $a_1; \dots; a_k$ to them.
4. The remaining entries are zero.

Drawing Tuples of Fixed Lee Weight

Example

Consider $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ where $7=2c+3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (x_1, x_2, x_3, x_4, x_5, x_6)$ of length 6 with Lee weight $t = 4$.

Drawing Tuples of Fixed Lee Weight

Example

Consider $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. $b = 7 = 2c = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (x_1; x_2; x_3; x_4; x_5; x_6)$ 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 $Z_7 = b$ $7=2c = 3$ 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:

$$\begin{array}{cccc}
 (1; 1; 1; 1) & (2; 1; 1) & (2; 2) & (3; 1) \\
 V_{4;(1;1;1;1)}^{(6)} = 240 & V_{4;(2;1;1)}^{(6)} = 480 & V_{4;(2;2)}^{(6)} = 60 & V_{4;(3;1)}^{(6)} = 120
 \end{array}$$

Drawing Tuples of Fixed Lee Weight

Example

Consider $Z_7 = b$ $7=2c = 3$ 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:

$$\begin{array}{cccc}
 (1; 1; 1; 1) & (2; 1; 1) & (2; 2) & (3; 1) \\
 V_{4;(1;1;1;1)}^{(6)} = 240 & V_{4;(2;1;1)}^{(6)} = 480 & V_{4;(2;2)}^{(6)} = 60 & V_{4;(3;1)}^{(6)} = 120
 \end{array}$$

Say we pick $(1; 2; 3) = (2; 1; 1)$.

Drawing Tuples of Fixed Lee Weight

Example

Consider $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. $b = 7 = 2c = 3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (x_1; x_2; x_3; x_4; x_5; x_6)$ of length 6 with Lee weight $t = 4$.

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

$$\begin{array}{cccc}
 (1; 1; 1; 1) & (2; 1; 1) & (2; 2) & (3; 1) \\
 V_{4;(1;1;1;1)}^{(6)} = 240 & V_{4;(2;1;1)}^{(6)} = 480 & V_{4;(2;2)}^{(6)} = 60 & V_{4;(3;1)}^{(6)} = 120
 \end{array}$$

Say we pick $(x_1; x_2; x_3) = (2; 1; 1)$.

2. Assign to each x_i an element $a_i \in Z_7$ with $\text{wt}_L(a_i) = x_i$:

$$x_1 = 2! \quad 5; \quad x_2 = 1! \quad 1; \quad x_3 = 1! \quad 6$$

Drawing Tuples of Fixed Lee Weight

Example

Consider $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. $7=2c+3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (x_1; x_2; x_3; x_4; x_5; x_6)$ of length 6 with Lee weight $t = 4$.

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

$$\begin{array}{cccc}
 (1; 1; 1; 1) & (2; 1; 1) & (2; 2) & (3; 1) \\
 V_{4;(1;1;1;1)}^{(6)} = 240 & V_{4;(2;1;1)}^{(6)} = 480 & V_{4;(2;2)}^{(6)} = 60 & V_{4;(3;1)}^{(6)} = 120
 \end{array}$$

Say we pick $(x_1; x_2; x_3) = (2; 1; 1)$.

2. Assign to each x_i an element $a_i \in Z_7$ with $\text{wt}_L(a_i) = x_i$:

$$x_1 = 2! \quad 5; \quad x_2 = 1! \quad 1; \quad x_3 = 1! \quad 6$$

3. Choose randomly 3 positions of x and assign them to one of the above values

$$x = (x_1; 6; x_2; 5; 1; x_3)$$

Drawing Tuples of Fixed Lee Weight

Example

Consider $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. $7=2c+3$ is the maximal Lee weight for an entry. Say we want a tuple $x = (x_1; x_2; x_3; x_4; x_5; x_6)$ of length 6 with Lee weight $t = 4$.

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

$$\begin{array}{cccc}
 (1; 1; 1; 1) & (2; 1; 1) & (2; 2) & (3; 1) \\
 V_{4;(1;1;1;1)}^{(6)} = 240 & V_{4;(2;1;1)}^{(6)} = 480 & V_{4;(2;2)}^{(6)} = 60 & V_{4;(3;1)}^{(6)} = 120
 \end{array}$$

Say we pick $(x_1; x_2; x_3) = (2; 1; 1)$.

2. Assign to each x_i an element $a_i \in Z_7$ with $\text{wt}_L(a_i) = x_i$:

$$x_1 = 2! \quad 5; \quad x_2 = 1! \quad 1; \quad x_3 = 1! \quad 6$$

3. Choose randomly 3 positions of x and assign them to one of the above values

$$x = (x_1; 6; x_2; 5; 1; x_3)$$

4. $x = (0; 6; 0; 5; 1; 0)$

Distribution

Theorem

Let n ; q and t be positive integers. When sampling a sufficiently large number of n -tuples using the before shown algorithm, we obtain a uniform distribution on $S_q^n(t)$.

Outline

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

Generic Decoding

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

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.

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

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 .

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 $\text{wt}_L(x) = 7$; Hamming $\text{wt}_H(x) = 4$

Introduction to the Problem

Example 1

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

$2x = (0; 4; 1; 2; 0; 1) \in \mathbb{Z}_5^6$

Lee Hamming
 $wt_L(x) = 7; \quad wt_H(x) = 4$

$wt_L(x) = 5; \quad wt_H(x) = 4$

Introduction to the Problem

Example 1

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

$2x = (0; 4; 1; 2; 0; 1) \in \mathbb{Z}_5^6$

Lee $wt_L(x) = 7$; Hamming $wt_H(x) = 4$

$wt_L(2x) = 5$; $wt_H(2x) = 4$

Example 2

Let $x = (0; 1; 3; 4; 1; 1) \in \mathbb{Z}_5^6$

Lee $wt_L(x) = 5$; Hamming $wt_H(x) = 5$

Introduction to the Problem

Example 1

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

$$2x = (0; 4; 1; 2; 0; 1) \in \mathbb{Z}_5^6$$

$$\begin{array}{ll} \text{Lee} & \text{Hamming} \\ \text{wt}_L(x) = 7; & \text{wt}_H(x) = 4 \end{array}$$

$$\text{wt}_L(2x) = 5; \quad \text{wt}_H(2x) = 4$$

Example 2

$$\text{Let } x = (0; 1; 3; 4; 1; 1) \in \mathbb{Z}_5^6$$

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

$$\begin{array}{ll} \text{Lee} & \text{Hamming} \\ \text{wt}_L(x) = 5; & \text{wt}_H(x) = 5 \end{array}$$

$$\text{wt}_L(2x) = 9; \quad \text{wt}_H(2x) = 5$$

Introduction to the Problem

Example 1

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

$$2x = (0; 4; 1; 2; 0; 1) \in \mathbb{Z}_5^6$$

$$\begin{array}{ll} \text{Lee} & \text{Hamming} \\ \text{wt}_L(x) = 7; & \text{wt}_H(x) = 4 \end{array}$$

$$\text{wt}_L(2x) = 5; \quad \text{wt}_H(2x) = 4$$

Example 2

$$\text{Let } x = (0; 1; 3; 4; 1; 1) \in \mathbb{Z}_5^6$$

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

$$\begin{array}{ll} \text{Lee} & \text{Hamming} \\ \text{wt}_L(x) = 5; & \text{wt}_H(x) = 5 \end{array}$$

$$\text{wt}_L(2x) = 9; \quad \text{wt}_H(2x) = 5$$

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

Example 1

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

$$2x = (0; 4; 1; 2; 0; 1) \in \mathbb{Z}_5^6$$

$$\begin{array}{ll} \text{Lee} & \text{Hamming} \\ \text{wt}_L(x) = 7; & \text{wt}_H(x) = 4 \end{array}$$

$$\text{wt}_L(2x) = 5; \quad \text{wt}_H(2x) = 4$$

Example 2

$$\text{Let } x = (0; 1; 3; 4; 1; 1) \in \mathbb{Z}_5^6$$

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

$$\begin{array}{ll} \text{Lee} & \text{Hamming} \\ \text{wt}_L(x) = 5; & \text{wt}_H(x) = 5 \end{array}$$

$$\text{wt}_L(2x) = 9; \quad \text{wt}_H(2x) = 5$$

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 Z_q , with $q > 3$. Given a tuple $x \in Z_q^n$ of average Lee weight $\bar{w} = t/n$ per entry. Let $a \in Z_q$ be a nonzero element, and the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x , i.e.

$$P(\text{wt}_L(a \cdot x) < \text{wt}_L(x)) \quad (5)$$

Problem Statement

Problem

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

$$P(\text{wt}_L(a \cdot x) < \text{wt}_L(x)) \quad (5)$$

Note

To give an answer to that question we need to understand

Problem Statement

Problem

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

$$P(\text{wt}_L(a \cdot x) < \text{wt}_L(x)) \quad (5)$$

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 Z_q , with $q > 3$. Given a tuple $x \in Z_q^n$ of average Lee weight $\bar{w} = t/n$ per entry. Let $a \in Z_q$ be a nonzero element, and the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x , i.e.

$$P(\text{wt}_L(a \cdot x) < \text{wt}_L(x)) \quad (5)$$

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 Z_q , with $q > 3$. Given a tuple $x \in Z_q^n$ of average Lee weight $\bar{w} = t/n$ per entry. Let $a \in Z_q$ be a nonzero element, and the probability that the Lee weight of $a \cdot x$ is less than the Lee weight of x , i.e.

$$P(\text{wt}_L(a \cdot x) < \text{wt}_L(x)) \quad (5)$$

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 $\bar{w} = t/n$ 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 $\bar{w} = t/n$ drawn as shown,

Q the empirical distribution of the entries of x

$a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,

Preparation

Let us consider the following setup.

$x \in \mathbb{Z}_q^n$ with average Lee weight $\bar{w}_L(x) = t/n$ drawn as shown,

Q the empirical distribution of the entries of x

$a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,

$F := \{x \in \mathbb{Z}_q^n \mid \bar{w}_L(ax) < \bar{w}_L(x)\}$.

Preparation

Let us consider the following setup.

$x \in \mathbb{Z}_q^n$ with average Lee weight $\bar{w} = t/n$ drawn as shown,

Q the empirical distribution of the entries of x

$a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,

$F := \{x \in \mathbb{Z}_q^n \mid \text{wt}_L(ax) < \text{wt}_L(x)\}$.

B the marginal distribution of the constant Lee weight channel model

$p_i := \mathbb{P}(\text{wt}_L(x_j) = i) = \frac{1}{q} \exp(-\beta i) ; i \in \{0, \dots, q-1\}$.

Preparation

Let us consider the following setup.

$x \in \mathbb{Z}_q^n$ with average Lee weight $\bar{w} = t/n$ drawn as shown,

Q the empirical distribution of the entries of x

$a \in \mathbb{Z}_q \setminus \{0\}$ be chosen uniformly at random,

$F := \{w \mid \text{wt}_L(a \cdot x) < \text{wt}_L(x)\}$.

B the marginal distribution of the constant Lee weight channel model

$p_i := \mathbb{P}(\text{wt}_L(x_j) = i) = \exp(-\beta i) / \sum_{i=0}^{q-1} \exp(-\beta i)$.

Applying the union bound, we have

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

"Close" Distributions

Definition [Kullback-Leibler divergence]

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

$$D(Q \parallel P) := \sum_{x \in X} Q(x) \log \frac{Q(x)}{P(x)} \quad (6)$$

Note

By convention: $0 \log(0) = 0$.

An approximated distribution Q is *close* to the exact distribution P , if $D(Q \parallel P) < \epsilon$, for some $\epsilon > 0$.

Conditional Limit Theorem

Theorem

Conditional Limit Theorem

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

$$P(X_1 = a | P_{X^n} \in E) \rightarrow P^?(a)$$

in probability as n grows large for any $a \in X$.

4

⁴Thomas 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 X and let Q be a distribution over X but not in E . Let X_1, \dots, X_n be discrete random variables drawn i.i.d. Q . Define $X^n = (X_1, \dots, X_n)$ and let $P^? = \arg \min_{P \in E} D(P \parallel Q)$. Then

$$P(X_1 = a \mid P_{X^n} \in E) \rightarrow P^?(a)$$

in probability as n grows large for any $a \in X$.

4

In our case:

$Q = U(Z_q)$; E set of distributions of tuples in $S_q^n(t)$. Then $B = \arg \min_{P \in E} D(P \parallel Q)$.

⁴Cover, *Elements of information theory*

Asymptotic Regime

Recall, $F = \{x \in \mathbb{F}_q^n : wt_L(x) \leq \alpha n\}$ and

$$P(F) = P(wt_L(x) \leq \alpha n) = P(Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Asymptotic Regime

Recall, $F = \{x \in \mathbb{Z}_q^n \mid \text{wt}_L(x) \leq \alpha n\}$ and

$$P(F) = P(\text{wt}_L(a \cdot x) \leq \alpha n) \approx P(Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Theorem

Let $x \in \mathbb{Z}_q^n$, for some positive integer $q > 3$, of average Lee weight αn be drawn randomly from $S_q^n(\alpha n)$ 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

$$P(Q \text{ not close to } B) \rightarrow 0 \text{ as } n \rightarrow \infty$$

Asymptotic Regime

Recall, $F = \{x \in \mathbb{Z}_q^n : \text{wt}_L(a \cdot x) < \text{wt}_L(x)\}$ and

$$P(F) = P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Theorem

Let $x \in \mathbb{Z}_q^n$, for some positive integer $q > 3$, of average Lee weight $\bar{w} = t/n$ be drawn randomly from $S_q^n(t)$ 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

$$P(Q \text{ not close to } B) \rightarrow 0 \text{ as } n \rightarrow \infty$$

Hence

As $n \rightarrow \infty$, $P(F) = P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \text{ is "close" to } B)$.

Asymptotic Regime

Recall, $F = \{x \in \mathbb{Z}_q^n : \text{wt}_L(a \cdot x) < \text{wt}_L(x)\}$ and

$$P(F) = P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Theorem

Let $x \in \mathbb{Z}_q^n$, for some positive integer $q > 3$, of average Lee weight $\bar{w} = t/n$ be drawn randomly from $S_q^n(t)$ 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

$$P(Q \text{ not close to } B) \rightarrow 0 \text{ as } n \rightarrow \infty$$

Hence

As $n \rightarrow \infty$, $P(F) \rightarrow P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \text{ is "close" to } B)$.

By CLT $P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \text{ is "close" to } B) \rightarrow \Phi(\frac{\bar{w} - \text{wt}_L(a \cdot x)}{\sigma})$

Asymptotic Regime

$$\begin{aligned}
 P(F) &= P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \in B) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i \text{wt}_L([a \cdot i]_q)} < \sum_{i=1}^{bq-2c} e^{-iA}\right) \\
 &= P\left(0 < \sum_{i=1}^{bq-2c} e^{-i(i \text{wt}_L([a \cdot i]_q))A}\right)
 \end{aligned}$$

Asymptotic Regime

$$\begin{aligned}
 P(F) &= P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q \in B) \\
 &= P\left(\sum_{i=1}^n e^{-i \text{wt}_L([a \cdot i]_q)} < \sum_{i=1}^n e^{-i A}\right) \\
 &= P\left(\sum_{i=1}^n e^{-i (i \text{wt}_L([a \cdot i]_q))} < A\right)
 \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \rightarrow \infty$.

Asymptotic Regime

$$\begin{aligned}
 P(F) &= P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q = B) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i \text{wt}_L([a \cdot i]_q)} < \sum_{i=1}^{bq-2c} e^{-iA}\right) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i(i \text{wt}_L([a \cdot i]_q))} < A\right)
 \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \rightarrow \infty$.

The difference $(i \text{wt}_L([a \cdot i]_q))$ **depends on** q .

Asymptotic Regime

$$\begin{aligned}
 P(F) &= P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q = B) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i \text{wt}_L([a \cdot i]_q)} < \sum_{i=1}^{bq-2c} e^{-iA}\right) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i(j - \text{wt}_L([a \cdot i]_q))A}\right)
 \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \rightarrow \infty$.

The difference $(j - \text{wt}_L([a \cdot i]_q))$ **depends on** q .

Question: What is the maximal value β of the average Lee weight per entry such that $\sum_{i=1}^{bq-2c} e^{-i(j - \text{wt}_L([a \cdot i]_q))\beta} > 0$?

Asymptotic Regime

$$\begin{aligned}
 P(F) &= P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q = B) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i \text{wt}_L([a \cdot i]_q)} < \sum_{i=1}^{bq-2c} e^{-iA}\right) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i(i \text{wt}_L([a \cdot i]_q))} < A\right)
 \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \rightarrow \infty$.

The difference $(i \text{wt}_L([a \cdot i]_q))$ **depends on** q .

Question: What is the maximal value β of the average Lee weight per entry such that $\sum_{i=1}^{bq-2c} e^{-i(i \text{wt}_L([a \cdot i]_q))} > 0$?

q	5	7	8	9	11	31	33	53
$bq=2c$	2	3	4	4	5	15	16	26
β	1	1.5	1.534	1.703	2.5	7.5	7.03	13

Asymptotic Regime

$$\begin{aligned}
 P(F) &= P(\text{wt}_L(a \cdot x) < \text{wt}_L(x) \mid Q = B) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i \text{wt}_L([a \cdot i]_q)} < \sum_{i=1}^{bq-2c} e^{-iA}\right) \\
 &= P\left(\sum_{i=1}^{bq-2c} e^{-i(i \text{wt}_L([a \cdot i]_q))} < \sum_{i=1}^{bq-2c} e^{-iA}\right)
 \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \rightarrow \infty$.

The difference $(i \text{wt}_L([a \cdot i]_q))$ **depends on** q .

Question: What is the maximal value β of the average Lee weight per entry such that $\sum_{i=1}^{bq-2c} e^{-i(i \text{wt}_L([a \cdot i]_q))} > 0$?

q	5	7	8	9	11	31	33	53
$bq=2c$	2	3	4	4	5	15	16	26
β	1	1.5	1.534	1.703	2.5	7.5	7.03	13

Thank you for your attention!