19.10.2021
Eindhoven University of Technology (TU/e)

Analysis and Properties of Error Patterns in the Lee Channel

Jessica Bariffi

German Aerospace Center (DLR) &
University of Zurich

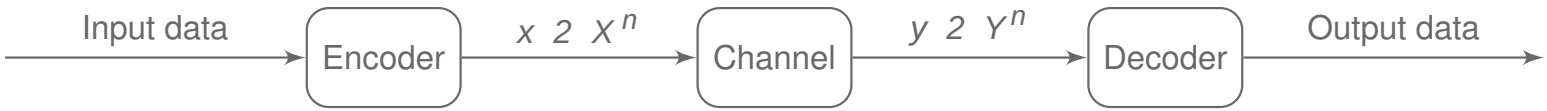
joint work with Hannes Bartz, Gianluigi Liva
and Joachim Rosenthal

Outline

Outline

Channel Coding

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

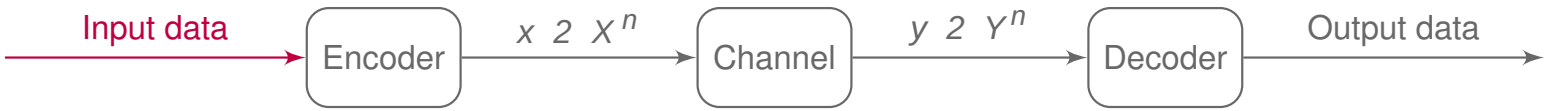


With a given channel law

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

Channel Coding

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

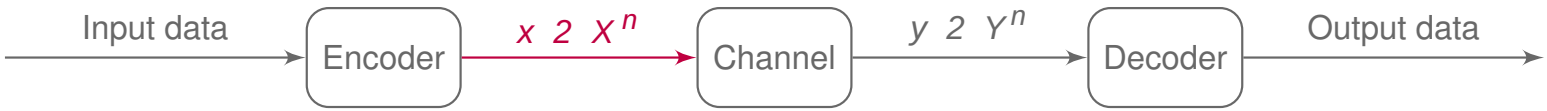


With a given channel law

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

Channel Coding

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

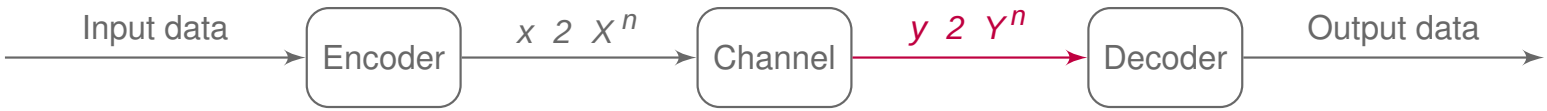


With a given channel law

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

Channel Coding

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

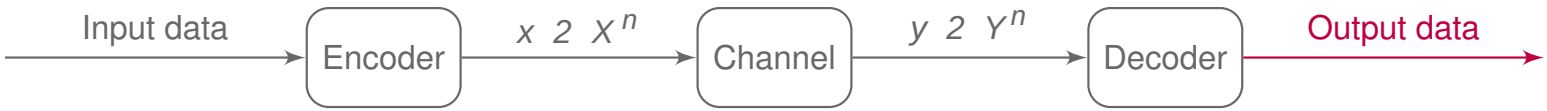


With a given channel law

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

Channel Coding

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

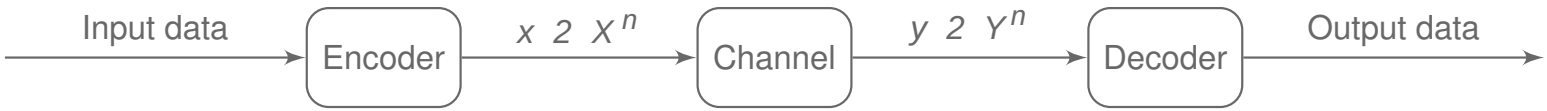


With a given channel law

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

Channel Coding

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

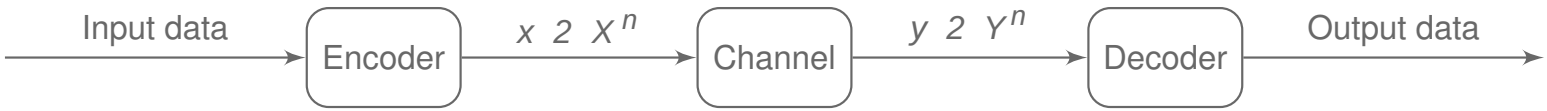


With a given channel law

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

Channel Coding

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



With a given channel law

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

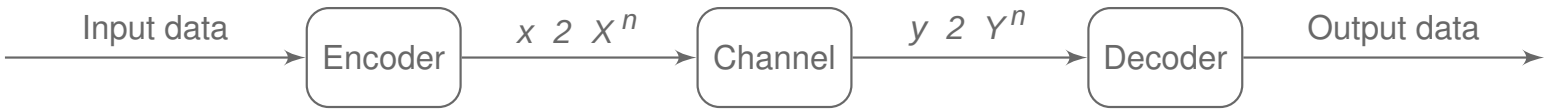
Example: q-ary Symmetric Channel (qSC)

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

Input	Output
0	0
1	1
$\vdots$	$\vdots$
$q-1$	$q-1$

Channel Coding

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



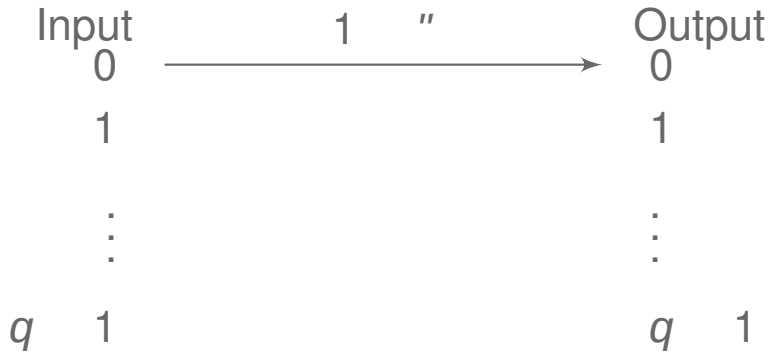
With a given channel law

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

Example: q-ary Symmetric Channel (qSC)

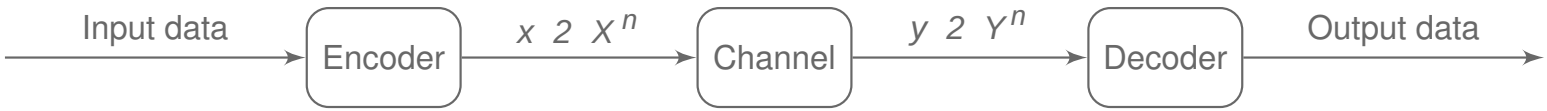
Alphabets:
$X = Y = \{0, 1, \ldots, q-1\}$

Probability of correct transmission:
$1 - p$



Channel Coding

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



With a given channel law

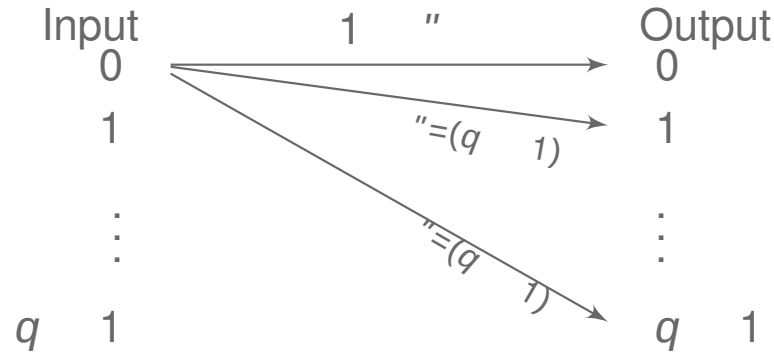
$$P_{Y|X}(y_i \mid x_i) := \mathrm{P}(Y = y_i \mid X = x_i)$$

Example: q-ary Symmetric Channel (qSC)

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

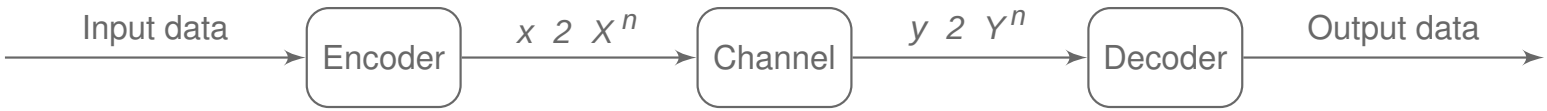
Probability of correct transmission:
$1-\varepsilon$

Probability of error for every possible outcome: $\varepsilon/(q-1)$



Channel Coding

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



With a given channel law

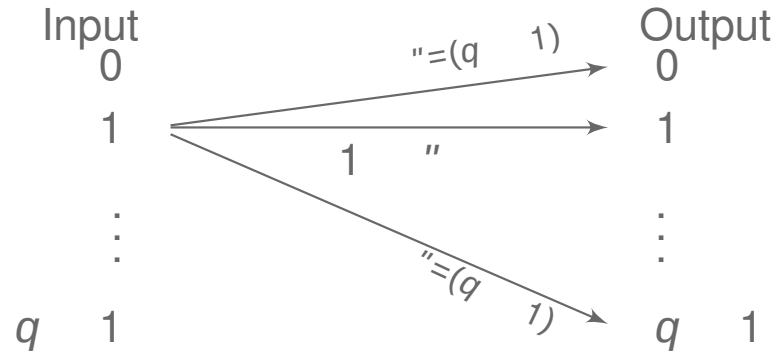
$$P_{Y|X}(y_i \mid x_i) := \mathrm{P}(Y = y_i \mid X = x_i)$$

Example: q-ary Symmetric Channel (qSC)

Alphabets:
$X = Y = f0; 1; : : : ; q \quad 1g$

Probability of correct transmission:
$1 \quad "$

Probability of error for every possible outcome: $"=(q \quad 1)$



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 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 nite eld of order q and let n be a positive integer.

De nition [Linear Code]

An $[n; k]_q$-linear code C 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 nite eld of order q and let n be a positive integer.

De nition [Linear Code]

An $[n; k]_q$-linear code C F_q^n is a k-dimensional subspace of F_q^n. The elements of C are called codewords.

Example

C = f (0; 0; 0; 0); (1; 1; 0; 0); (0; 0; 1; 1); (1; 1; 1; 1)g is a $[4; 2]_2$-linear code.

De nition [Hamming Weight/Distance]

For any two codewords x; y 2 C we de ne

the Hamming weight of x, $wt_H(x) =$ jf i 2 f 1; : : : ; ng j x_i 6= 0gj

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

The Lee Metric

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

De nition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is de ned 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.

De nition [Lee weight]

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

$$wt_L(a) := \min(a; q - a) \tag{1}$$

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

$$wt_L(3) = \min(3; 5 - 3) = 2$$

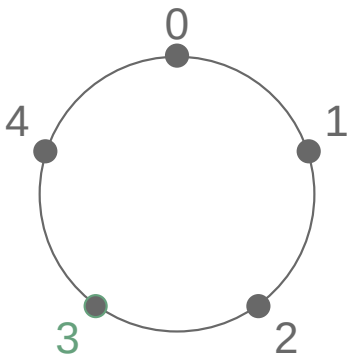
The Lee Metric

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

De nition [Lee weight]

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

$$wt_L(a) := \min(a; q - a) \tag{1}$$



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.

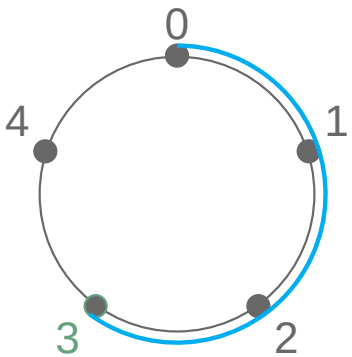
The Lee Metric

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

De nition [Lee weight]

For any integer a 2 Z_q its Lee weight is de ned as

$$wt_L(a) := \min(\ a; q \quad a) \tag{1}$$



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

$$wt_L(3) = \min(\ 3; 5 \quad 3) = \ 2$$

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

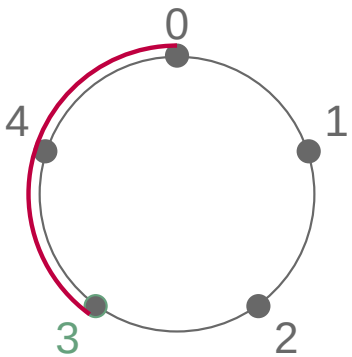
The Lee Metric

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

De nition [Lee weight]

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

$$wt_L(a) := \min(a; q - a) \tag{1}$$



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.

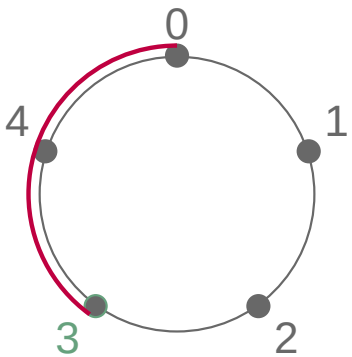
The Lee Metric

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

De nition [Lee weight]

For any integer $a \in Z_q$ its Lee weight is de ned 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.
=) $wt_L(3) = 2$

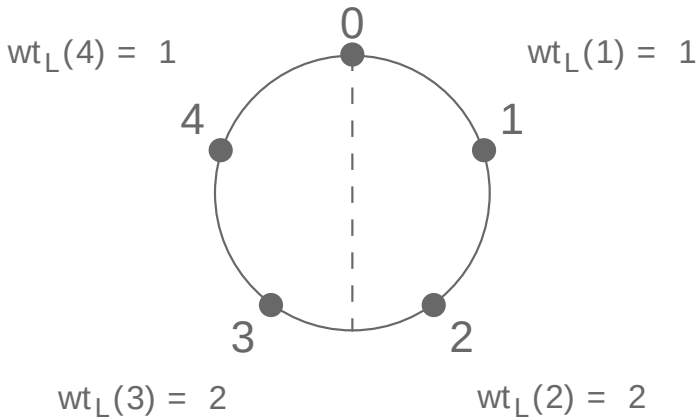
The Lee Metric

Properties

For every a 2 Z_q it holds:

$$wt_L(a) = wt_L(q \quad a)$$

Example



The Lee Metric

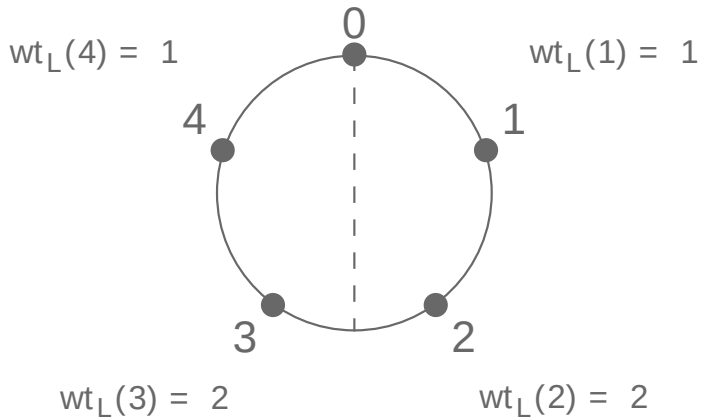
Properties

For every a 2 Z_q it holds:

$$wt_L(a) = wt_L(q \quad a)$$

$$wt_L(a) \quad b \; q=2c$$

Example



The Lee Metric

Properties

For every a 2 Z_q it holds:

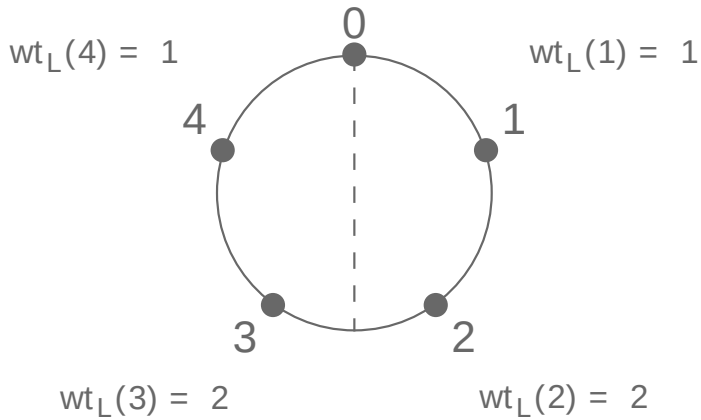
$wt_L(a) = wt_L(q \quad a)$

$wt_L(a)$ b $q=2c$

$wt_H(a) \quad wt_L(a)$

If q 2 f 2; 3g, the Lee weight is equivalent to the Hamming weight.

Example



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n) \ 2 \ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

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

The Lee distance between two tuples $x; y \ 2 \ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n) \ 2 \ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

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

The Lee distance between two tuples $x; y \ 2 \ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

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

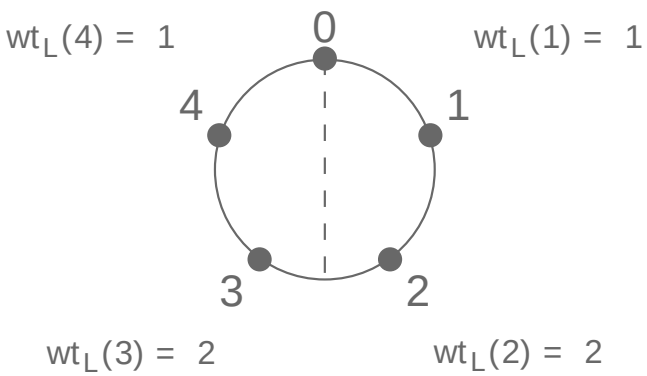
The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

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

$$wt_L(x) =$$



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

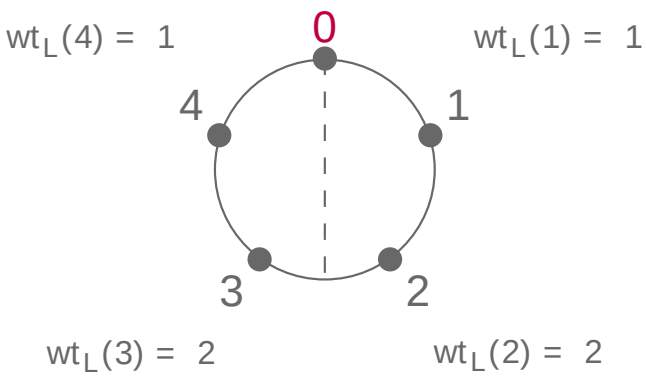
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

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



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

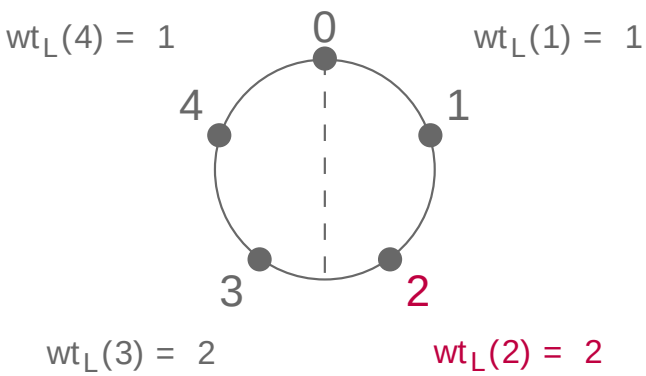
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

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



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

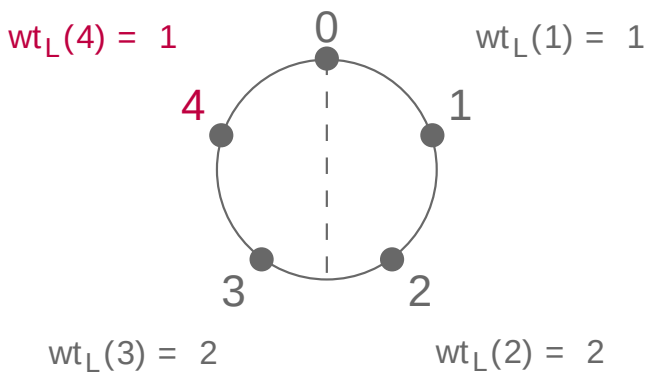
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

$$x = (0; 2; 4; 3; 0; 3)$$
$$wt_L(x) = 0 + 2 + 1$$



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

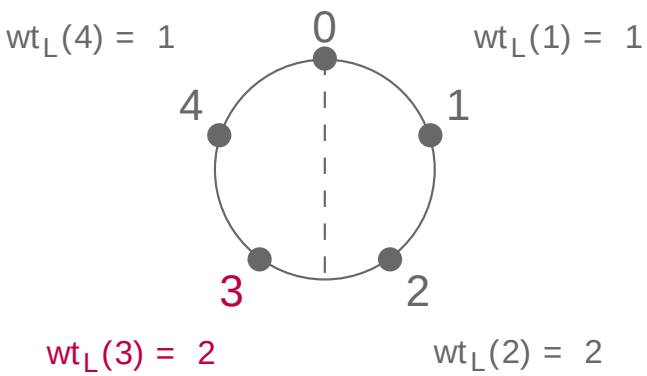
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

$$x = (0; 2; 4; 3; 0; 3)$$
$$wt_L(x) = 0 + 2 + 1 + 2$$



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

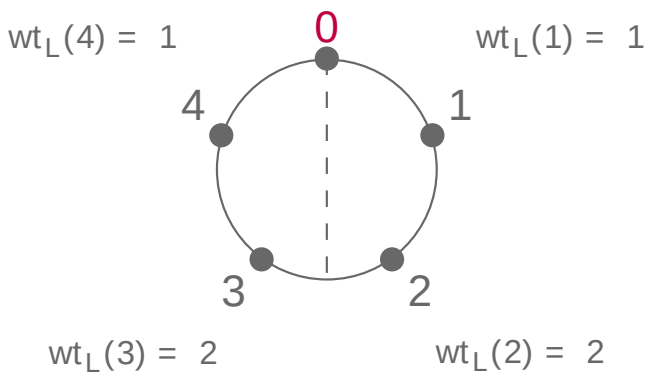
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

$$x = (0; 2; 4; 3; 0; 3)$$
$$wt_L(x) = 0 + 2 + 1 + 2 + 0$$



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

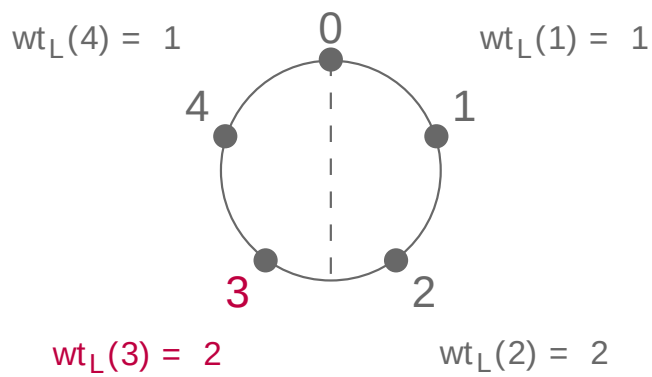
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \tag{2}$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

$$x = (0; 2; 4; 3; 0; 3)$$
$$wt_L(x) = 0 + 2 + 1 + 2 + 0 + 2$$



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

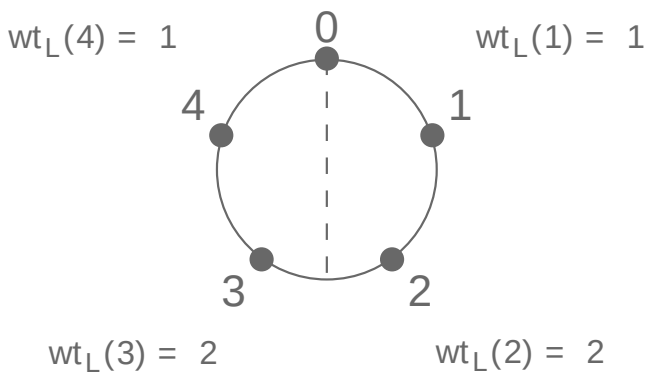
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers Z_5

$$x = (0; 2; 4; 3; 0; 3)$$
$$wt_L(x) = 0 + 2 + 1 + 2 + 0 + 2 = 7$$



The Lee Metric

De nition [Lee weight]

Let $x = (x_1; : : : ; x_n)\ 2\ Z_q^n$ be a tuple of length n. The Lee weight of x is the sum of the Lee weight of its entries, i.e.,

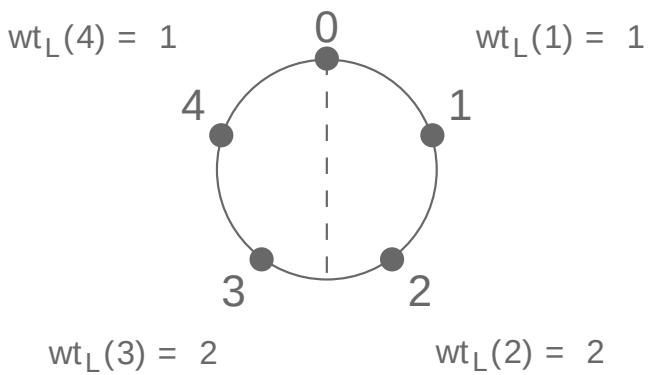
$$wt_L(x) := \sum_{i=1}^{n} wt_L(x_i) \qquad (2)$$

The Lee distance between two tuples $x; y\ 2\ Z_q^n$ is the Lee weight of their difference, $d_L(x; y) = wt_L(x \quad y)$.

Example:

Take again the ring of integers 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 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
! 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 de ned [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

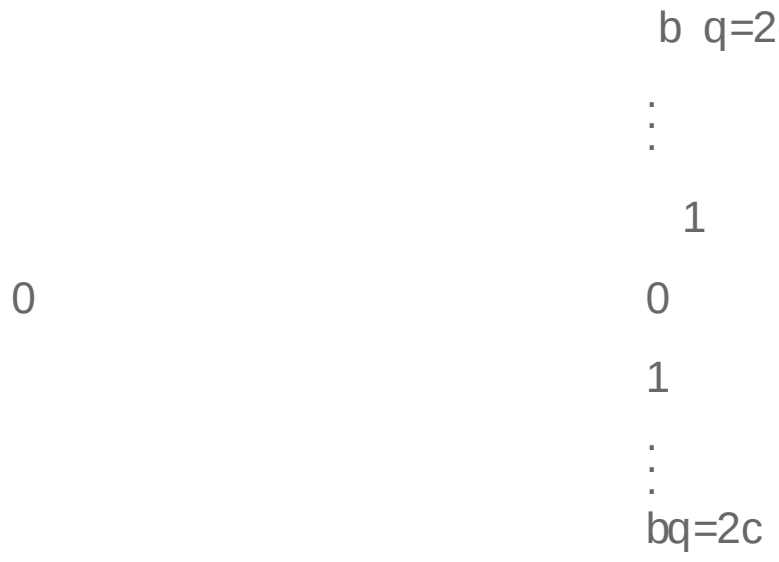
Originally introduced by Chiang and Wolf[3].

[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 Z_q.
Goal: Describe $P(i \mid j) = P(i - j \mid 0)$.



[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.

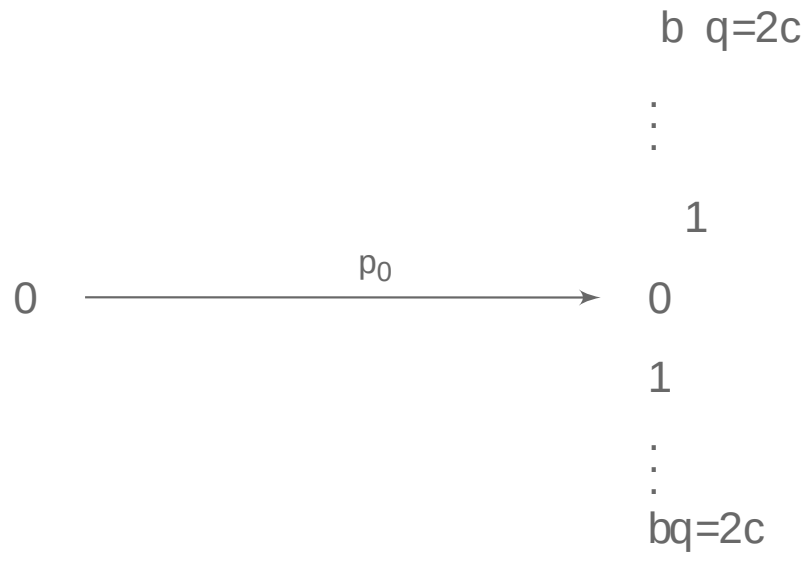
The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is Z_q.
Goal: Describe $P(i\ j\ j) = P(i\ \ j\ j\ 0)$.

De ne for every $i = 0; : : : ; bq=2c$

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



[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.

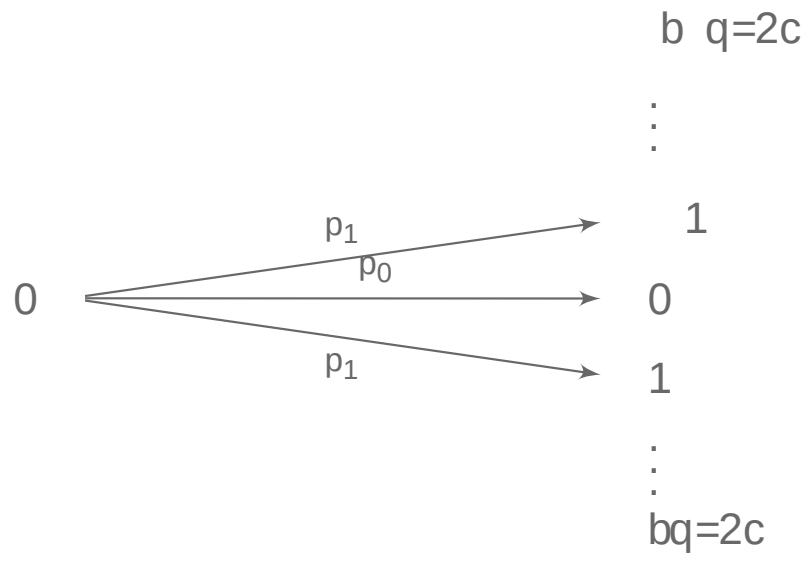
The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is Z_q.
Goal: Describe $P(i\,j\,j) = P(i \quad j\,j\,0)$.

De ne for every $i = 0; : : : ; bq=2c$

$$p_i := P(i\,j\,0) = P(\quad i\,j\,0)$$



[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.

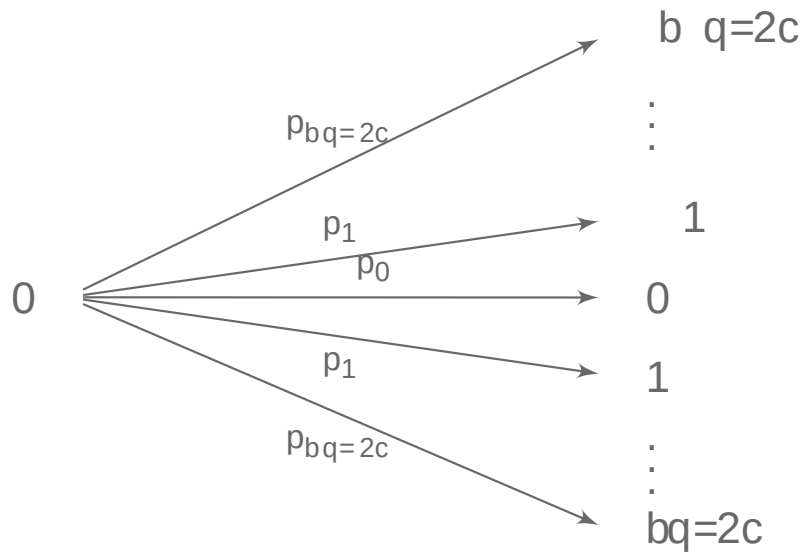
The Lee Channel

Originally introduced by Chiang and Wolf[3].

Assume the alphabet is Z_q.
Goal: Describe $P(i\ j\ j) = P(i\ \ j\ j\ 0)$.

De ne for every $i = 0; : : : ; bq=2c$

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



[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

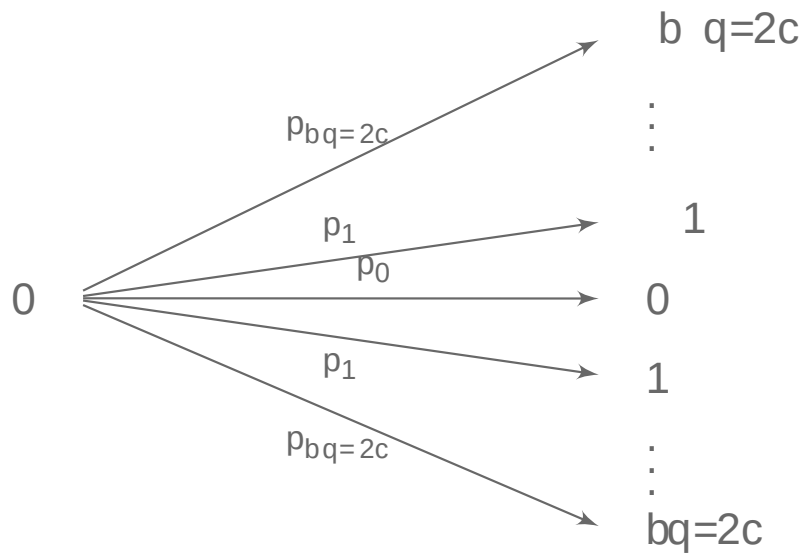
Originally introduced by Chiang and Wolf[3].

Assume the alphabet is Z_q.
Goal: Describe $P(i\ j\ j) = P(i\ \ j\ j\ 0)$.

De ne for every $i = 0; : : : ; bq/2c$

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

Question: How is p_i de ned?



[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 Law

For $y; x; e \; 2 \; Z_q$, 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 $y; x; e \in Z_q$, 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

$$P(E = e) / \exp(-\lambda\, wt_L(e)); \qquad \lambda > 0;$$

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

The Lee Channel Law

For $y; x; e \in Z_q$, 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

$$P(E = e) / \exp(\ \ wt_L(e)); \qquad > 0;$$

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

Note

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

De ning $p_i := P(wt_L(e) = i) = \frac{1}{Z}\exp(\ \ i)$ for $i \in \{0; 1; \ldots; bq=2cg$, we easily see

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

The Constant Lee Weight Channel

Consider now $y; x; e \in Z_q^n$ and $y = x + e$, where e has a fixed Lee weight $t \in Z$ and is drawn uniformly at random from $S_{t;q}^n := \{x \in Z_q^n \mid wt_L(x) = t\}$:

The Constant Lee Weight Channel

Consider now $y; x; e \ 2 \ Z_q^n$ and $y = x + e$, where e has a xed Lee weight $t \ 2 \ Z$ and is drawn uniformly at random from $S_{t;q}^n := \ x \ 2 \ Z_q^n \ \ wt_L(x) = t \ :$

Theorem

For every $j \ 2 \ f \ 1; : : : ; ng$ the marginal weight distribution of an entry e_j is given by

$$p_i := P(wt_L(e_j) = i) = \frac{1}{\sum_{j=0}^{q \ 1} \exp(\ \ wt_L(j))} \exp(\ \ i) \ ; 8i \ 2 \ f \ 0; : : : ; bq=2cg$$

where $> \ 0$ 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 $y; x; e \in Z_q^n$ and $y = x + e$, where e has a fixed Lee weight $t \in Z$ and is drawn uniformly at random from $S_{t;q}^n := \{x \in Z_q^n \mid wt_L(x) = t\}$.

Theorem

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

$$p_i := P(wt_L(e_j) = i) = \frac{1}{\sum_{j=0}^{q-1} \exp(\alpha\, wt_L(j))} \exp(\alpha i); \forall i \in \{0; \ldots; bq/2c\}$$

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

Proof idea.
Solve an optimization problem to find a distribution $(p_0; p_1; \ldots; p_{bq/2c})$ that is

- ... maximizing $H(p_0; \ldots; p_{bq/2c}) := \sum_{i=0}^{bq/2c} p_i \log(p_i)$,
- ... subject to $\sum_{i=0}^{bq/2c} p_i\, i = \frac{t}{n}$.

Outline

Integer Partitions

De nition [Integer Partition]

Let t be a positive integer. An (integer) partition of t of length k is a k-tuple $= (\ _1; : : : ;\ _k)$ satisfying

1. $\ _1 + : : : + \ _k = t,$
2. $\ _1 \quad : : : \quad \ _k > 0.$

The elements $\ _i$ are called parts and their corresponding values are the part sizes.

Integer Partitions

De nition [Integer Partition]

Let t be a positive integer. An (integer) partition of t of length k is a k-tuple $= (\ _1; : : : ;\ _k)$ satisfying

1. $\ _1 + : : : + \ _k = t,$
2. $\ _1 \quad : : : \quad \ _k > 0.$

The elements $\ _i$ are called parts and their corresponding values are the part sizes.

Notation:
$P(t)$: Set of integer partitions of a positive integer $t \ 2 \ Z$.
$P_s(t) := \ f \quad = (\ _1; : : : ;\ _k) \ 2 \ P \ (t) \ j \ _1 \quad sg.$

Integer Partitions

De nition [Integer Partition]

Let t be a positive integer. An (integer) partition of t of length k is a k-tuple $= (\ _1; : : : ;\ _k)$ satisfying

1. $\ _1 + : : : + \ _k = t,$
2. $\ _1 \quad : : : \quad \ _k > 0.$

The elements $\ _i$ are called parts and their corresponding values are the part sizes.

Notation:
$P(t)$: Set of integer partitions of a positive integer $t \ 2 \ Z$.
$P_s(t) := f \quad = (\ _1; : : : ;\ _k) \ 2 \ P(t) \ j \ _1 \quad sg.$

Example

Let us consider $t = 4$.

$$P(4) = f(3; 1); (2; 2); (2; 1; 1); (1; 1; 1; 1)g$$
$$P_2(4) = f(2; 2); (2; 1; 1); (1; 1; 1; 1)g$$
$$P_1(4) = f(1; 1; 1; 1)g$$

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Note: This de nition makes only sense when considering an integer partition over Z_q having part sizes not exceeding bq=2c. ! restrict to $P_{bq=2c}(t)$.

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Note: This de nition makes only sense when considering an integer partition over Z_q having part sizes not exceeding bq=2c. ! restrict to $P_{bq=2c}(t)$.

De ne $V^{(n)}_{q;t;}$:= f x 2 Z^n_q j $wt_L(x)$ = t and x has weight decomp. g.

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Note: This de nition makes only sense when considering an integer partition over Z_q having part sizes not exceeding bq=2c. ! restrict to $P_{bq=2c}(t)$.

De ne $V^{(n)}_{q;t;} := \{ x \in Z_q^n \mid wt_L(x) = t \text{ and } x \text{ has weight decomp.} \}$.

Example

Consider Z_5, $t = n = 4$ and $= (2; 1; 1)$ a partition of t over Z_5.
Vectors of weight decomposition $(2; 1; 1)$ over Z_5 are all vectors over Z_5^4 consisting of:

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Note: This de nition makes only sense when considering an integer partition over Z_q having part sizes not exceeding bq=2c. ! restrict to $P_{bq=2c}(t)$.

De ne $V^{(n)}_{q;t;} := \{ x \in Z_q^n \mid wt_L(x) = t \text{ and } x \text{ has weight decomp.} \}$.

Example

Consider Z_5, t = n = 4 and = (2; 1; 1) a partition of t over Z_5.
Vectors of weight decomposition (2; 1; 1) over Z_5 are all vectors over Z_5^4 consisting of:

1 element of Lee weight 2 (e.g. 2 or 3)

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Note: This de nition makes only sense when considering an integer partition over Z_q having part sizes not exceeding bq=2c. ! restrict to $P_{bq=2c}(t)$.

De ne $V^{(n)}_{q;t;} := \{ x \in Z_q^n \mid wt_L(x) = t \text{ and } x \text{ has weight decomp.} \}$.

Example

Consider Z_5, t = n = 4 and = (2; 1; 1) a partition of t over Z_5.
Vectors of weight decomposition (2; 1; 1) over Z_5 are all vectors over Z_5^4 consisting of:

- 1 element of Lee weight 2 (e.g. 2 or 3)
- 2 elements of Lee weight 1 (e.g. 1 and/or 4)

Tuples of Weight Decomposition over Z_q

De nition [Vectors of Weight Decomposition]

For a positive integer n and a given partition 2 tr of a positive integer t, we say that a length-n vector x has weight decomposition over Z_q if there is a one-to-one correspondence between the Lee weight of the nonzero entries of x and the parts of .

Note: This de nition makes only sense when considering an integer partition over Z_q having part sizes not exceeding bq=2c. ! restrict to $P_{bq=2c}(t)$.

De ne $V^{(n)}_{q;t;} := \{ x \in Z_q^n \mid wt_L(x) = t \text{ and } x \text{ has weight decomp.} \}$.

Example

Consider Z_5, t = n = 4 and = (2; 1; 1) a partition of t over Z_5.
Vectors of weight decomposition (2; 1; 1) over Z_5 are all vectors over Z_5^4 consisting of:

- 1 element of Lee weight 2 (e.g. 2 or 3)
- 2 elements of Lee weight 1 (e.g. 1 and/or 4)

$V^{(4)}_{4;(2;\,1;\,1)} = \{ (2;1;1;0); (2;1;0;1); \ldots; (1;2;1;0); \ldots; (3;4;1;0); \ldots \}$

Number of Tuples of weight decomposition over Z_q

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 $2 P_{bq=2c}(t)$ the number of vectors of length n over Z_q of type is given by

$$V^{(n)}_{q;t;} = \begin{cases} 2^{`} \; j \quad j \; {}^{`n} & \text{if } q \text{ is odd;} \\ 2^{`} \quad c_{bq=2c;} \; j \quad j \; {}^{`n} & \text{else} \end{cases} \tag{4}$$

where $c_{bq=2c;} = jf\, i\, 2\, f\, 1; : : : ; ` \; g\, j \;_i = bq=2cgj.$

Drawing Tuples of Fixed Lee Weight

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

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \bigsqcup_{2P \; bq = 2c(t)} V_{q;t;}^{(n)} :$$

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \bigcup_{\substack{\lambda \vdash t \\ \lambda_1 \le q-1}} V_{q;t;\lambda}^{(n)} :$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1; \ldots; \lambda_k)$ of t with probability $p_\lambda = \frac{V_{q;t;\lambda}^{(n)}}{\sum_{\mu \vdash t,\ \mu_1 \le q-1} V_{q;t;\mu}^{(n)}}$ over Z_q.

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \bigsqcup_{2P \; bq=2c(t)} V_{q;t;}^{(n)} :$$

Idea

1. Choose an integer partition $= (\ _1; : : : ;\ _k)$ of t with probability $p = \frac{V_{q;t;}^{(n)}}{\bigsqcup_{2P \; bq=2c(t)} V_{q;t;}^{(n)}}$ over Z_q.
2. Assign to $_i$ an element $a_i \in Z_q$ with $wt_L(a_i) =\ _i$.

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \bigcup_{\lambda \vdash t,\ |\lambda| \le n} V_{q;t;\lambda}^{(n)} :$$

Idea

1. Choose an integer partition $\lambda = (\lambda_1; \ldots; \lambda_k)$ of t with probability $p = \frac{V_{q;t;\lambda}^{(n)}}{\sum_{\lambda \vdash t,\ |\lambda| \le n} V_{q;t;\lambda}^{(n)}}$ over Z_q.
2. Assign to λ_i an element $a_i \in Z_q$ with $wt_L(a_i) = \lambda_i$.
3. Choose randomly k positions of the tuple x and assign the values $a_1; \ldots; a_k$ to them.

Drawing Tuples of Fixed Lee Weight

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

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

$$S_q^n(t) = \bigsqcup_{2P \; \sum b_q = 2c(t)} V_{q;t;}^{(n)} :$$

Idea

1. Choose an integer partition $= (\ _1; : : : ;\ _k)$ of t with probability $p = \frac{\prod V_{q;t;}^{(n)}}{\sum_{2P \; \sum b_q = 2c(t)} V_{q;t;}^{(n)}}$ over Z_q.
2. Assign to $\ _i$ an element $a_i \in Z_q$ with $wt_L(a_i) = \ _i$.
3. Choose randomly k positions of the tuple x and assign the values $a_1; : : : ; a_k$ to them.
4. The remaining entries are zero.

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.

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:
   (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:

$(1;1;1;1)$ $(2;1;1)$ $(2;2)$ $(3;1)$

$V^{(6)}_{4;(1;1;1;1)} = 240$ $V^{(6)}_{4;(2;1;1)} = 480$ $V^{(6)}_{4;(2;2)} = 60$ $V^{(6)}_{4;(3;1)} = 120$

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:
   $(1;1;1;1)$ $(2;1;1)$ $(2;2)$ $(3;1)$
   $V^{(6)}_{4;(1;1;1;1)} = 240$ $V^{(6)}_{4;(2;1;1)} = 480$ $V^{(6)}_{4;(2;2)} = 60$ $V^{(6)}_{4;(3;1)} = 120$
   Say we pick ($_1$; $_2$; $_3$) = (2; 1; 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:
   (1; 1; 1; 1) (2; 1; 1) (2; 2) (3; 1)
   $V^{(6)}_{4;(1;1;1;1)} = 240$ $V^{(6)}_{4;(2;1;1)} = 480$ $V^{(6)}_{4;(2;2)} = 60$ $V^{(6)}_{4;(3;1)} = 120$
   Say we pick ($_1$; $_2$; $_3$) = (2; 1; 1).
2. Assign to each $_i$ an element a_i 2 Z_7 with $wt_L(a_i) = _i$:

$$_1 = 2 ! 5; \quad _2 = 1 ! 1; \quad _3 = 1 ! 6$$

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:
   (1; 1; 1; 1) (2; 1; 1) (2; 2) (3; 1)
   $V^{(6)}_{4;(1;1;1;1)}$ = 240 $V^{(6)}_{4;(2;1;1)}$ = 480 $V^{(6)}_{4;(2;2)}$ = 60 $V^{(6)}_{4;(3;1)}$ = 120
   Say we pick ($_1$; $_2$; $_3$) = (2; 1; 1).
2. Assign to each $_i$ an element a_i 2 Z_7 with $wt_L(a_i)$ = $_i$:

   $$_1 = 2 ! 5; \quad _2 = 1 ! 1; \quad _3 = 1 ! 6$$

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

   $$x = (_; 6; _; 5; 1; _)$$

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:
   (1; 1; 1; 1) (2; 1; 1) (2; 2) (3; 1)
   $V^{(6)}_{4;(1;1;1;1)} = 240$ $V^{(6)}_{4;(2;1;1)} = 480$ $V^{(6)}_{4;(2;2)} = 60$ $V^{(6)}_{4;(3;1)} = 120$
   Say we pick ($_1$; $_2$; $_3$) = (2; 1; 1).
2. Assign to each $_i$ an element a_i 2 Z_7 with $wt_L(a_i) = _i$:

   $$_1 = 2 ! 5; \quad _2 = 1 ! 1; \quad _3 = 1 ! 6$$

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 suf ciently large number of n-tuples using the before shown algorithm, we obtain a uniform distribution on $S_q^n(t)$.

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 nd either the message or the random error.

Generic Decoding

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

Generic Decoding

An adversary wants to nd 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 $y = \underbrace{x}_{\text{original message}} + \underbrace{e}_{\text{error vector}}$.

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.

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

Introduction to the Problem

Example 1
Let $x = (0; 2; 3; 1; 0; 3) \in Z_5^6$

Lee
$wt_L(x) = 7;$

Hamming
$wt_H(x) = 4$

Introduction to the Problem

Example 1

Let $x = (0; 2; 3; 1; 0; 3) \in Z_5^6$

$2x = (0; 4; 1; 2; 0; 1) \in Z_5^6$

	Lee	Hamming
x	$wt_L(x) = 7;$	$wt_H(x) = 4$
$2x$	$wt_L(x) = 5;$	$wt_H(x) = 4$

Introduction to the Problem

Example 1

Let $x = (0; 2; 3; 1; 0; 3) \in Z_5^6$

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

$2x = (0; 4; 1; 2; 0; 1) \in Z_5^6$

Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 4$

Example 2

Let $x = (0; 1; 3; 4; 1; 1) \in Z_5^6$

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

Introduction to the Problem

Example 1

Let $x = (0; 2; 3; 1; 0; 3) \in Z_5^6$ — Lee: $wt_L(x) = 7$; Hamming: $wt_H(x) = 4$

$2x = (0; 4; 1; 2; 0; 1) \in Z_5^6$ — Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 4$

Example 2

Let $x = (0; 1; 3; 4; 1; 1) \in Z_5^6$ — Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 5$

$2x = (0; 2; 1; 3; 2; 2) \in Z_5^6$ — Lee: $wt_L(x) = 9$; Hamming: $wt_H(x) = 5$

Introduction to the Problem

Example 1

Let $x = (0; 2; 3; 1; 0; 3) \in Z_5^6$ — Lee: $wt_L(x) = 7$; Hamming: $wt_H(x) = 4$

$2x = (0; 4; 1; 2; 0; 1) \in Z_5^6$ — Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 4$

Example 2

Let $x = (0; 1; 3; 4; 1; 1) \in Z_5^6$ — Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 5$

$2x = (0; 2; 1; 3; 2; 2) \in Z_5^6$ — Lee: $wt_L(x) = 9$; Hamming: $wt_H(x) = 5$

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

Example 1

Let $x = (0; 2; 3; 1; 0; 3) \in Z_5^6$ — Lee: $wt_L(x) = 7$; Hamming: $wt_H(x) = 4$

$2x = (0; 4; 1; 2; 0; 1) \in Z_5^6$ — Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 4$

Example 2

Let $x = (0; 1; 3; 4; 1; 1) \in Z_5^6$ — Lee: $wt_L(x) = 5$; Hamming: $wt_H(x) = 5$

$2x = (0; 2; 1; 3; 2; 2) \in Z_5^6$ — Lee: $wt_L(x) = 9$; Hamming: $wt_H(x) = 5$

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

$$P(wt_L(a \ x) < wt_L(x)) \tag{5}$$

Problem Statement

Problem

Consider the ring of integers Z_q, with $q > 3$. Given a tuple $x \ 2 \ Z_q^n$ of average Lee weight $= t=n$ per entry. Let $a \ 2 \ Z_q$ be a nonzero element, nd the probability that the Lee weight of $a \ x$ is less than the Lee weight of x, i.e.

$$P(wt_L(a \ x) < wt_L(x)) \tag{5}$$

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 $= t=n$ per entry. Let $a \in Z_q$ be a nonzero element, nd the probability that the Lee weight of $a \quad x$ is less than the Lee weight of x, i.e.

$$P(wt_L(a \quad x) < wt_L(x)) \tag{5}$$

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

$$P(wt_L(a \ x) < wt_L(x)) \tag{5}$$

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

$$P(wt_L(a \ x) < wt_L(x)) \tag{5}$$

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.

- $x \in Z_q^n$ with average Lee weight $= t=n$ drawn as shown,
- Q the empirical distribution of the entries of x

Preparation

Let us consider the following setup.

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

Preparation

Let us consider the following setup.

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

Preparation

Let us consider the following setup.

- $x \in Z_q^n$ with average Lee weight $= t=n$ drawn as shown,
- Q the empirical distribution of the entries of x
- $a \in Z_q \setminus \{0\}$ be chosen uniformly at random,
- $F := \{ wt_L(a \quad x) < wt_L(x) \}$.
- B the marginal distribution of the constant Lee weight channel model $p_i := P(wt_L(x_j) = i) = \quad \exp(\quad i) ; 8i \in \{ 0; : : : ; bq=2c \}$.

Preparation

Let us consider the following setup.

- $x \in Z_q^n$ with average Lee weight $= t/n$ drawn as shown,
- Q the empirical distribution of the entries of x
- $a \in Z_q \setminus \{0\}$ be chosen uniformly at random,
- $F := \{wt_L(a \cdot x) < wt_L(x)\}$.
- B the marginal distribution of the constant Lee weight channel model $p_i := P(wt_L(x_j) = i) = \exp(\quad i)$; $\forall i \in \{0, \ldots, bq/2c\}$.

Applying the union bound, we have

$$\begin{aligned} P(F) = {} & P(wt_L(a \cdot x) < wt_L(x) \mid Q \text{ is "close" to } B)\, P(Q \text{ is "close" to } B) \\ & + P(wt_L(a \cdot x) < wt_L(x) \mid Q \text{ is "not close" to } B)\, P(Q \text{ is "not close" to } B) \\ & P(wt_L(a \cdot x) < wt_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B) \end{aligned}$$

"Close" Distributions

De nition [Kullback-Leibler divergence]

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

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

Note

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

The two distributions Q and P are close to each other if $D(Q \,||\, P) \quad "$, for some $" > 0$.

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 $X_1; : : : ; X_n$ be discrete random variables drawn i.i.d. Q. De ne $X^n = (X_1; : : : ; X_n)$ and let $P^? = \arg\min_{P 2 E} D(P \,jj\, Q)$. Then

$$P(X_1 = a \,j\, P_{X^n} 2 E) ! \quad P^?(a)$$

in probability as n grows large for any $a 2 X$.

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 X and let Q be a distribution over X but not in E. Let $X_1; : : : ; X_n$ be discrete random variables drawn i.i.d. Q. De ne $X^n = (X_1; : : : ; X_n)$ and let $P^? = \arg\min_{P 2 E} D(P \,jj\, Q)$. Then

$$P(X_1 = a \,j\, P_{X^n} 2 E) ! \quad P^?(a)$$

in probability as n grows large for any $a 2 X$.

4

In our case:

$Q \quad U \ (Z_q)$; E set of distributions of tuples in $S_q^n(t)$. Then $B = \arg\min_{P 2 E} D(P \,jj\, Q)$.

[4] Cover, Elements of information theory

Asymptotic Regime

Recall, $F = \{ wt_L(a \quad x) < wt_L(x) \}$ and

$$P(F) \quad P(wt_L(a \quad x) < wt_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Asymptotic Regime

Recall, $F = \{ wt_L(a \quad x) < wt_L(x) \}$ and

$$P(F) \quad P(wt_L(a \quad x) < wt_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Theorem

Let $x \ 2 \ Z_q^n$, for some positive integer $q > 3$, of average Lee weight $= t=n$ 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 $a \ 2 \ Z_q$ it holds

$$P(Q \text{ not close to } B) \ ! \quad 0 \text{ as } n \ ! \ 1 \quad :$$

Asymptotic Regime

Recall, $F = \{ wt_L(a \quad x) < wt_L(x) g$ and

$$P(F) \quad P(wt_L(a \quad x) < wt_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Theorem

Let $x \ 2 \ Z_q^n$, for some positive integer $q > 3$, of average Lee weight $= t=n$ 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 $a \ 2 \ Z_q$ it holds

$$P(Q \text{ not close to } B) \ ! \quad 0 \text{ as } n \ ! \ 1 \quad :$$

Hence

As $n \ ! \ 1$, $P(F) \quad P(wt_L(a \quad x) < wt_L(x) \mid Q \text{ is "close" to } B)$.

Asymptotic Regime

Recall, $F = \{ wt_L(a \quad x) < wt_L(x) \}$ and

$$P(F) \quad P(wt_L(a \quad x) < wt_L(x) \mid Q \text{ is "close" to } B) + P(Q \text{ is "not close" to } B)$$

Theorem

Let $x \ 2 \ Z_q^n$, for some positive integer $q > 3$, of average Lee weight $= t=n$ 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 $a \ 2 \ Z_q$ it holds

$$P(Q \text{ not close to } B) \ ! \quad 0 \text{ as } n \ ! \ 1 \quad :$$

Hence

As $n \ ! \ 1$, $P(F) \quad P(wt_L(a \quad x) < wt_L(x) \mid Q \text{ is "close" to } B)$.
By CLT $P(wt_L(a \quad x) < wt_L(x) \mid Q \quad B \ )$

Asymptotic Regime

$$
\begin{aligned}
P(F) &= P\left(wt_L(a \star x) < wt_L(x) \mid Q \star B\right) \\
&= P\left(\sum_{i=1}^{\lfloor q/2 \rfloor} e^{\,i\, wt_L([a \star i]_q)} < \sum_{i=1}^{\lfloor q/2 \rfloor} e^{\,i\, i} \cdot A\right) \\
&= P\left(0 < \sum_{i=1}^{\lfloor q/2 \rfloor} e^{\,i\,(i - wt_L([a \star i]_q))} \cdot A\right)
\end{aligned}
$$

Asymptotic Regime

$$\begin{aligned} \mathrm{P}(F) &\quad \mathrm{P}\left(\mathrm{wt}_L(a \quad x) < \mathrm{wt}_L(x) \, j \, Q \quad B\right) \\ &= \mathrm{P}\left(\sum_{i=1}^{bq=2c} \mathrm{e}^{\quad i} \, \mathrm{wt}_L([a \quad i]_q) < \sum_{i=1}^{bq=2c} \mathrm{e}^{\quad i} \, i\right) \\ &= \mathrm{P}\left(0 < \sum_{i=1}^{bq=2c} \mathrm{e}^{\quad i} (i \quad \mathrm{wt}_L([a \quad i]_q))\right) \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \quad ! \quad 1$.

Asymptotic Regime

$$
\begin{aligned}
\mathrm{P}(F) &\quad \mathrm{P}\left(\mathrm{wt}_L(a \quad x) < \mathrm{wt}_L(x) \, j \, Q \quad B\right) \\
&= \mathrm{P}\left(\sum_{i=1}^{bq=2c} \mathrm{e}^{\quad i} \, \mathrm{wt}_L([a \quad i]_q) < \sum_{i=1}^{bq=2c} \mathrm{e}^{\quad i} \, i\right) \\
&= \mathrm{P}\left(0 < \sum_{i=1}^{bq=2c} \mathrm{e}^{\quad i} (i \quad \mathrm{wt}_L([a \quad i]_q))\right)
\end{aligned}
$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \quad ! \quad 1$.

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

Asymptotic Regime

$$\begin{aligned} \mathrm{P}(F) &\quad \mathrm{P}\left(\mathrm{wt}_L(a \quad x) < \mathrm{wt}_L(x) \, j \, Q \quad B\right) \\ &= \mathrm{P}\left(0 \overset{bq=2c}{\underset{i=1}{\sum}} \mathrm{e}^{\quad i} \mathrm{wt}_L([a \quad i]_q) < \overset{bq=2c}{\underset{i=1}{\sum}} \mathrm{e}^{\quad i} i \, 1 \mathrm{A}\right) \\ &= \mathrm{P}\left(0 < \overset{bq=2c}{\underset{i=1}{\sum}} \mathrm{e}^{\quad i} (i \quad \mathrm{wt}_L([a \quad i]_q)) \, 1 \mathrm{A}\right) \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \quad ! \quad 1$.

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

Question: What is the maximal value $\quad ?$ of the average Lee weight per entry such that $\mathrm{P}_{i=1}^{bq=2c} \mathrm{e}^{\quad i} (i \quad \mathrm{wt}_L([a \quad i]_q)) \quad 0$?

Asymptotic Regime

$$\begin{aligned} P(F) &\quad P\left(\mathrm{wt}_L(a \quad x) < \mathrm{wt}_L(x) \, j \, Q \quad B\right) \\ &= P\left(\sum_{i=1}^{bq=2c} e^{\quad i} \, \mathrm{wt}_L([a \quad i]_q) < \sum_{i=1}^{bq=2c} e^{\quad i} \, i \right) \\ &= P\left(0 < \sum_{i=1}^{bq=2c} e^{\quad i} (i \quad \mathrm{wt}_L([a \quad i]_q)) \right) \end{aligned}$$

Note

Recall: **depends on** $t=n$ but stays invariant as $n \quad ! \quad 1$.

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

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

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

Open Questions and Future Work

1. What is the probability that the average weight decomposition of an n-tuple drawn uniformly at random from $S_q^n(t)$ is less than $bq{=}4c$?

Open Questions and Future Work

1. What is the probability that the average weight decomposition of an n-tuple drawn uniformly at random from $S_q^n(t)$ is less than $bq{=}4c$?
2. Can we estimate $\mathrm{P}(F)$ in the finite regime? If yes, how?

Open Questions and Future Work

1. What is the probability that the average weight decomposition of an n-tuple drawn uniformly at random from $S_q^n(t)$ is less than $bq{=}4c$?
2. Can we estimate $\mathsf{P}(F)$ in the finite regime? If yes, how?
3. Can we improve ISD by multiplying the received word with a “suitable” nontrivial scalar?

Open Questions and Future Work

1. What is the probability that the average weight decomposition of an n-tuple drawn uniformly at random from $S_q^n(t)$ is less than $bq{=}4c$?
2. Can we estimate $\mathsf{P}(F)$ in the finite regime? If yes, how?
3. Can we improve ISD by multiplying the received word with a “suitable” nontrivial scalar?

Thank you for your attention!