July 12, 2021
Institutskolloquium, KN-IColl

Decoding Performance of LDPC Codes over the Lee Channel

Jessica Bariffi

Institute for Communications and Navigation
German Aerospace Center, DLR

joint work with Hannes Bartz, Gianluigi Liva
and Joachim Rosenthal

Outline

Outline

Motivation

- Transmission of data over a noisy channel

Motivation

- Transmission of data over a noisy channel
- Error correction/detection

Motivation

- Transmission of data over a noisy channel
- Error correction/detection
- Fast encoding and decoding performance

Channel Coding

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

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Channel Coding

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

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Channel Coding

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

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Channel Coding

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

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Channel Coding

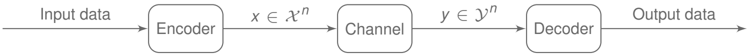
Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Channel Coding

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



With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Channel Coding

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

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

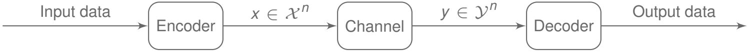
Example: q-ary Symmetric Channel (qSC)

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

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

Channel Coding

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



With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Example: q-ary Symmetric Channel (qSC)

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

Channel Coding

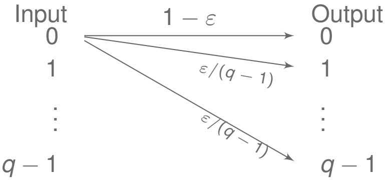
Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Example: q-ary Symmetric Channel (qSC)

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



Channel Coding

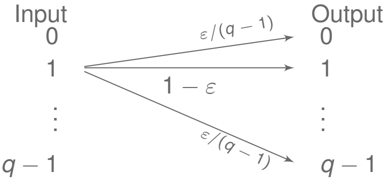
Let $\mathcal{X}$ and $\mathcal{Y}$ the input and output alphabet of the channel, respectively.

With a given channel law

$$P_{Y|X}(y \mid x) := \mathbb{P}(Y = y \mid X = x)$$

Example: q-ary Symmetric Channel (qSC)

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



The Hamming Weight

Let $\mathbb{F}_q$ be a finite field of order q and let n be a positive integer. We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

The Hamming Weight

Let $\mathbb{F}_q$ be a finite field of order q and let n be a positive integer. We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Hamming weight/distance]

For any two vectors $x, y \in \mathbb{F}_q^n$ we define

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

The Hamming Weight

Let $\mathbb{F}_q$ be a finite field of order q and let n be a positive integer. We will denote by $\mathbb{Z}_q$ the ring of integers modulo q.

Definition [Hamming weight/distance]

For any two vectors $x, y \in \mathbb{F}_q^n$ we define

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

An $[n, k]_q$-linear code $\mathcal{C}$ can be represented by an $(n-k) \times n$ matrix H satisfying

$$\mathcal{C} = \ker(H) = \{x \in \mathbb{F}_q^n \mid Hx^\top = 0\}.$$

We call H a *parity-check matrix* of $\mathcal{C}$.

Generic Decoding

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

Generic Decoding

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

Generic Decoding

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

Generic Decoding

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

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 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 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 small.
- Information set decoding (ISD) is a method to find e.

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

The Lee Metric

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

Definition [Lee weight]

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

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

The Lee Metric

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

Definition [Lee weight]

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

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

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

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

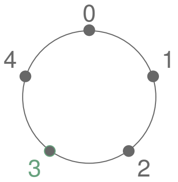
The Lee Metric

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

Definition [Lee weight]

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

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



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

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

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

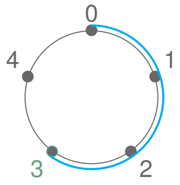
The Lee Metric

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

Definition [Lee weight]

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

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



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

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

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

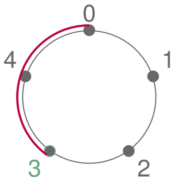
The Lee Metric

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

Definition [Lee weight]

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

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



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

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

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

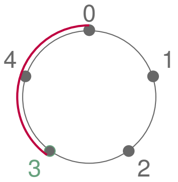
The Lee Metric

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

Definition [Lee weight]

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

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



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

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

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

$\Longrightarrow \mathrm{wt}_L(3) = 2$

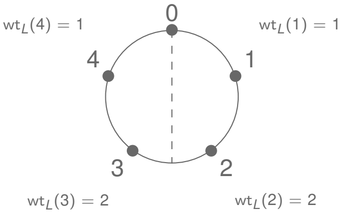
The Lee Metric

Properties

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

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

Example



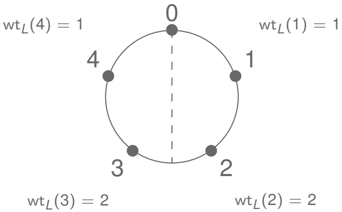
The Lee Metric

Properties

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

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

Example



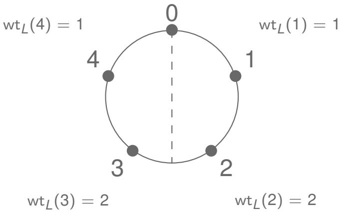
The Lee Metric

Properties

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

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

Example



The Lee Metric

Definition [Lee weight]

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

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

The Lee Metric

Definition [Lee weight]

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

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

Example:

The Lee Metric

Definition [Lee weight]

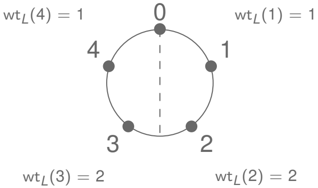
Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a vector of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

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

Example:

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

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



The Lee Metric

Definition [Lee weight]

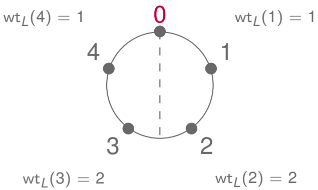
Let $x = (x_1, \dots, x_n) \in \mathbb{Z}_q^n$ be a vector of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

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

Example:

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

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



The Lee Metric

Definition [Lee weight]

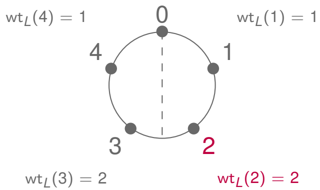
Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a vector of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

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

Example:

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

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



The Lee Metric

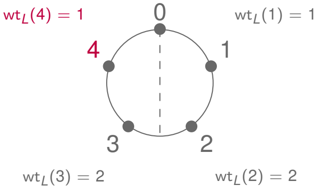
Definition [Lee weight]

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

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

Example:

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



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

The Lee Metric

Definition [Lee weight]

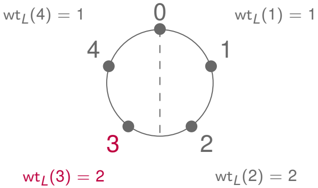
Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a vector of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

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

Example:

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

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



The Lee Metric

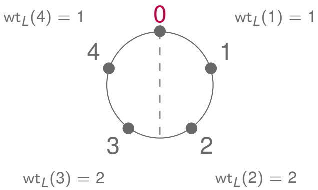
Definition [Lee weight]

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

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

Example:

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



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

The Lee Metric

Definition [Lee weight]

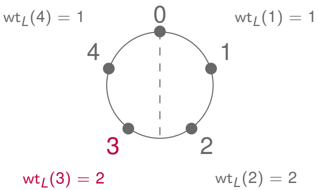
Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a vector of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

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

Example:

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

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



The Lee Metric

Definition [Lee weight]

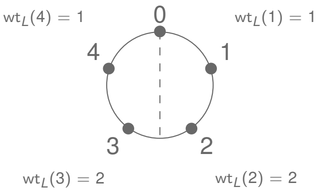
Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ be a vector of length n. The *Lee weight* of x is the sum of the Lee weight of its entries, i.e.,

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

Example:

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

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



The Lee Metric

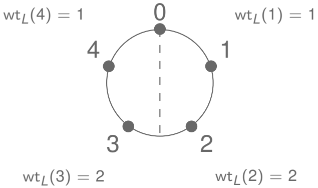
Definition [Lee weight]

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

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

Example:

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



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

DLR

Interesting Problem

Consider the same example as before over $\mathbb{Z}_5$.

	Lee	Hamming

Interesting Problem

Consider the same example as before over $\mathbb{Z}_5$.

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

Interesting Problem

Consider the same example as before over $\mathbb{Z}_5$.

	Lee	Hamming
$x = (0, 2, 4, 3, 0, 3)$	$\mathrm{wt}_L(x) = 7,$	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 3, 1, 0, 1)$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 4$

Interesting Problem

Consider the same example as before over $\mathbb{Z}_5$.

	Lee	Hamming
$x = (0, 2, 4, 3, 0, 3)$	$\mathrm{wt}_L(x) = 7,$	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 3, 1, 0, 1)$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 4$

Why can decreasing the Lee weight be a problem?

Complexity of generic (or information-set) decoding depends on the weight of the error vector.

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

Interesting Problem

Consider the same example as before over $\mathbb{Z}_5$.

	Lee	Hamming
$x = (0, 2, 4, 3, 0, 3)$	$\text{wt}_L(x) = 7,$	$\text{wt}_H(x) = 4$
$2x = (0, 4, 3, 1, 0, 1)$	$\text{wt}_L(x) = 5,$	$\text{wt}_H(x) = 4$

Why can decreasing the Lee weight be a problem?

Complexity of generic (or information-set) decoding depends on the weight of the error vector.

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

Risk: An attacker could decrease the weight and retrieve the original message.

Interesting Problem

Consider the same example as before over $\mathbb{Z}_5$.

	Lee	Hamming
$x = (0, 2, 4, 3, 0, 3)$	$\mathrm{wt}_L(x) = 7,$	$\mathrm{wt}_H(x) = 4$
$2x = (0, 4, 3, 1, 0, 1)$	$\mathrm{wt}_L(x) = 5,$	$\mathrm{wt}_H(x) = 4$

Why can decreasing the Lee weight be a problem?

Complexity of generic (or information-set) decoding depends on the weight of the error vector.

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

Risk: An attacker could decrease the weight and retrieve the original message.
Asymptotically: The probability of decreasing the weight is negligible as the length grows large.

Why Lee Metric?

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

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *arXiv preprint arXiv:1903.07692* (2019).

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

Why Lee Metric?

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

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *arXiv preprint arXiv:1903.07692* (2019).

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

Why Lee Metric?

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

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *arXiv preprint arXiv:1903.07692* (2019).

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

Why Lee Metric?

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

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *arXiv preprint arXiv:1903.07692* (2019).

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

Why Lee Metric?

- Transmitting symbols over a nonbinary noisy channel
  $\longrightarrow$ primarily those using phase-shift keying modulation
- Design code-based cryptosystems with reduced key sizes
- Used in magnetic and DNA storage systems.
- Recently: gained attention in cryptographic applications
  - ISD 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: *arXiv preprint arXiv:1903.07692* (2019).

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

Why Lee Metric?

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

[1] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information set decoding in the Lee metric with applications to cryptography". In: *arXiv preprint arXiv:1903.07692* (2019).

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

Outline

The Lee Channel

Originally introduced by Chiang and Wolf[3].

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

The Lee Channel

Originally introduced by Chiang and Wolf[3].

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

0

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

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

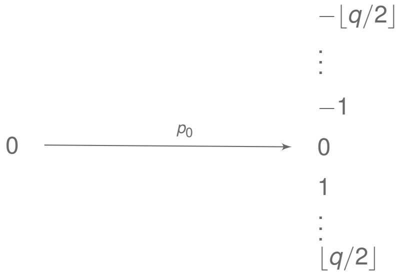
The Lee Channel

Originally introduced by Chiang and Wolf[3].

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

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

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



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

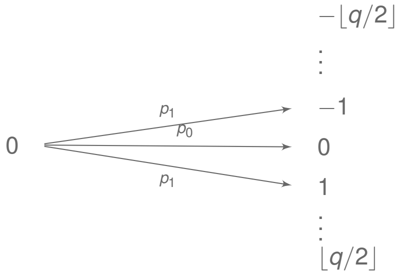
The Lee Channel

Originally introduced by Chiang and Wolf[3].

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

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

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



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

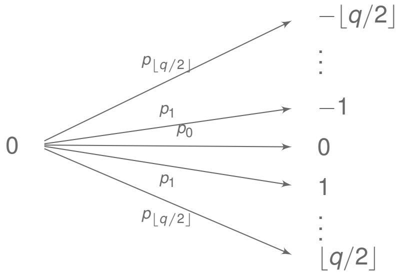
The Lee Channel

Originally introduced by Chiang and Wolf[3].

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

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

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



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

The Lee Channel

Theorem [Chiang and Wolf]

The channel described before is strictly matched to the Lee metric for maximum likelihood decoding if and only if the following two properties hold.

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

DLR

The Lee Channel

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

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

The Lee Channel

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

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

with channel law

$$\mathbb{P}(Y = y \,|\, X = x) =: P_{Y|X}(y|x) = \frac{1}{Z} \exp\left(-\lambda \, \mathrm{d}_L(x, y)\right), \tag{4}$$

where $Z := \sum_{e=0}^{q-1} \exp(-\lambda \, \mathrm{wt}_L(e))$ and $\lambda > 0$.

The Lee Channel

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

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

with channel law

$$\mathbb{P}(Y = y \,|\, X = x) =: P_{Y|X}(y|x) = \frac{1}{Z} \exp\left(-\lambda \, \mathrm{d}_L(x, y)\right), \tag{4}$$

where $Z := \sum_{e=0}^{q-1} \exp(-\lambda \, \mathrm{wt}_L(e))$ and $\lambda > 0$.

Note

- The channel defined in (4) is the DMC matched to the Lee metric.
- The conditional distribution (4) arises (in the limit of large n) as the marginal distribution of a constant-weight Lee channel.

The Constant-Weight Lee Channel

Let $y, x, e \in \mathbb{Z}_q^n$, where $\mathrm{wt}_L(e) = t$ for some fixed positive integer t. Consider again

$$y = x + e.$$

The Constant-Weight Lee Channel

Let $y, x, e \in \mathbb{Z}_q^n$, where $\mathrm{wt}_L(e) = t$ for some fixed positive integer t. Consider again

$$y = x + e.$$

Note

The error vector e is chosen uniformly at random from the set of all length-n vectors of Lee weight t:

$$\mathcal{S}_t^n := \left\{x \,\middle|\, x \in \mathbb{Z}_q^n, \mathrm{wt}_L(x) = t\right\}.$$

The Constant-Weight Lee Channel

Let $y, x, e \in \mathbb{Z}_q^n$, where $\mathrm{wt}_L(e) = t$ for some fixed positive integer t. Consider again

$$y = x + e.$$

Note

The error vector e is chosen uniformly at random from the set of all length-n vectors of Lee weight t:

$$\mathcal{S}_t^n := \left\{ x \,\middle|\, x \in \mathbb{Z}_q^n, \mathrm{wt}_L(x) = t \right\}.$$

Question

What would $P_{Y \mid X}(y \mid x)$ look like?

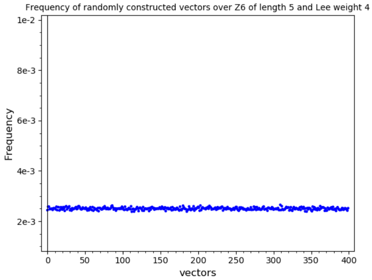
DLR

Channel Distribution

Theorem

Let $e \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$ be the error term from before. Then it holds

i. With our algorithm e is drawn uniformly from the set of all length-n vectors of Lee weight t over $\mathbb{Z}_q$.



Channel Distribution

Theorem

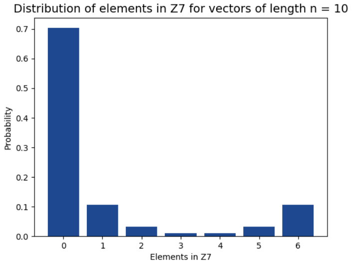
Let $e \in \mathbb{Z}_q^n$ with $\mathrm{wt}_L(x) = t$ be the error term from before. Then it holds

i. With our algorithm e is drawn uniformly from the set of all length-n vectors of Lee weight t over $\mathbb{Z}_q$.

ii. Every entry e_i has the following probability

$$\mathbb{P}(e_i = j) = \kappa \exp(-\lambda \,\mathrm{wt}_L(j)),$$

where $\kappa = \sum_{k=0}^{m-1} \exp(-\lambda \,\mathrm{wt}_L(k))$ and $j \in \mathbb{Z}_q$.



Outline

LDPC Codes over Finite Integer Rings

According to Sridhara and Fuja

Definition [LDPC Code]

An $[n, k]_q$ LDPC code over $\mathbb{Z}_q$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $\mathbb{Z}_q^\times$.

LDPC Codes over Finite Integer Rings

According to Sridhara and Fuja

Definition [LDPC Code]

An $[n, k]_q$ LDPC code over $\mathbb{Z}_q$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $\mathbb{Z}_q^\times$.

Can be described by a bipartite graph $\mathcal{G}$ consisting of

- variable nodes (VN) $\{v_1, \ldots, v_n\} \longrightarrow$ columns of H.
- check nodes (CN) $\{c_1, \ldots, c_m\} \longrightarrow$ rows of H.

LDPC Codes over Finite Integer Rings

According to Sridhara and Fuja

Definition [LDPC Code]

An $[n, k]_q$ LDPC code over $\mathbb{Z}_q$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $\mathbb{Z}_q^\times$.

Can be described by a bipartite graph $\mathcal{G}$ consisting of

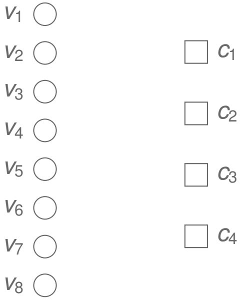
- variable nodes (VN) $\{v_1, \dots, v_n\} \longrightarrow$ columns of H.
- check nodes (CN) $\{c_1, \dots, c_m\} \longrightarrow$ rows of H.

VN v_j is connected to CN c_i if and only if $h_{ij} \neq 0$.

LDPC Codes over Finite Integer Rings

Example

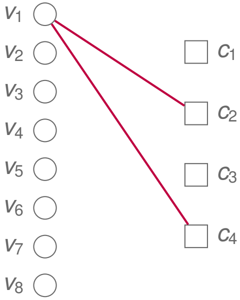
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

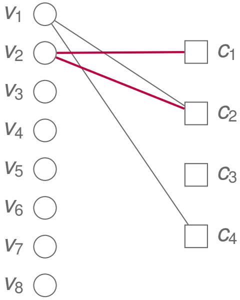
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

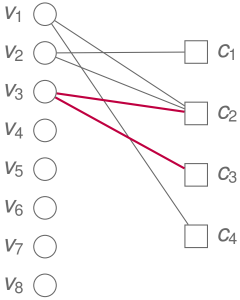
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

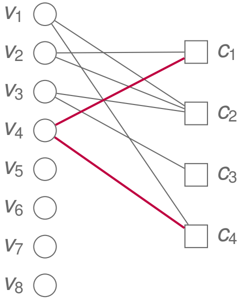
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

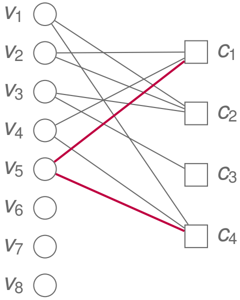
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

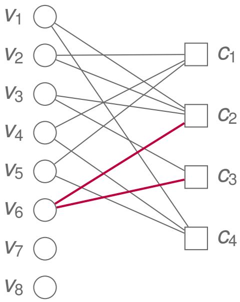
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

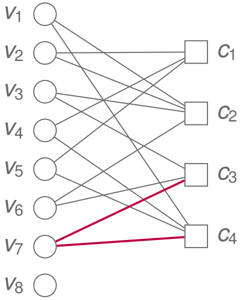
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

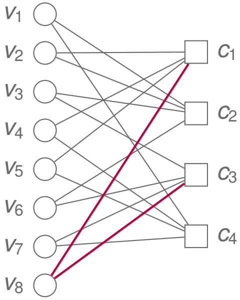
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

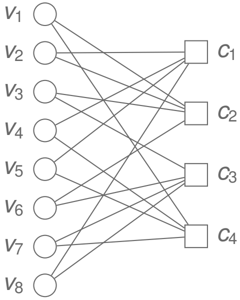
$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



LDPC Codes over Finite Integer Rings

Example

$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 1 & 4 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{Z}_5^{4\times 8}$$



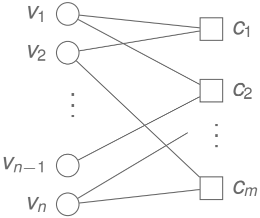
An LDPC code is (k, ℓ)-*regular*, if every VN connects to k CNs and every CN connects to ℓ VNs, for some fixed positive integer k and ℓ.

Symbol Message Passing

Consider a nonbinary LDPC code $\mathcal{C}$ with VNs $\{v_1, \dots, v_n\}$ and CNs $\{c_1, \dots, c_m\}$ and parity-check matrix H. Denote by $\mathcal{N}(v_j)$ and $\mathcal{N}(c_i)$ the set of all connecting elements to VN v_j and CN c_i, respectively.

Symbol Message Passing

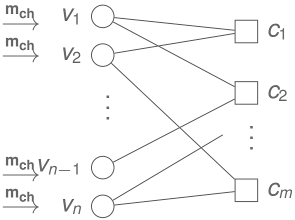
Consider a nonbinary LDPC code $\mathcal{C}$ with VNs $\{v_1, \dots, v_n\}$ and CNs $\{c_1, \dots, c_m\}$ and parity-check matrix H. Denote by $\mathcal{N}(v_j)$ and $\mathcal{N}(c_i)$ the set of all connecting elements to VN v_j and CN c_i, respectively.



Symbol Message Passing

Consider a nonbinary LDPC code $\mathcal{C}$ with VNs $\{v_1, \ldots, v_n\}$ and CNs $\{c_1, \ldots, c_m\}$ and parity-check matrix H. Denote by $\mathcal{N}(v_j)$ and $\mathcal{N}(c_i)$ the set of all connecting elements to VN v_j and CN c_i, respectively.

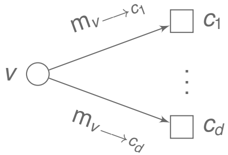
Every VN v receives the channel observation
$\mathbf{m_{ch}} := (P_{Y|X}(y \mid 0), \ldots, P_{Y|X}(y \mid q-1))$



Symbol Message Passing

Initialization.
Each VN v sends channel observation to the neighboring CNs $c \in \mathcal{N}(v)$

$$m_{v \longrightarrow c} = \mathbf{m_{ch}}.$$

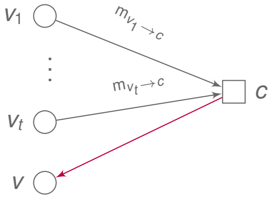


Symbol Message Passing

CN-to-VN step.
Each CN computes for every $v \in \mathcal{N}(c)$

$$m_{c\to v} = h_{c,v}^{-1} \sum_{v' \in \mathcal{N}(c)\setminus\{v\}} h_{c,v'} m_{v'\to c}.$$

Note: $h_{c,v}^{-1}$ exists, since we said the nonzero entries of H are units.



Symbol Message Passing

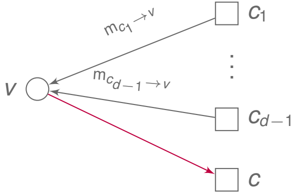
VN-to-CN step.

Define the aggregated extrinsic L-vector

$$E = L(y) + \sum_{c' \in \mathcal{N}(v) \setminus \{c\}} L\left(m_{c' \to v}\right),$$

where y is the channel output and
$L(y) = (L_0(y), \ldots, L_{q-1}(y))$ with
$L_x(y) = \log\left(P_{Y|X}(y \mid x)\right)$.
Note: We assume the CN-to-VN messages are modelled as a qSC.
Then the VN-to-CN messages are

$$m_{v \to c} = \arg\max_{x \in \mathbb{Z}_q} E_x.$$



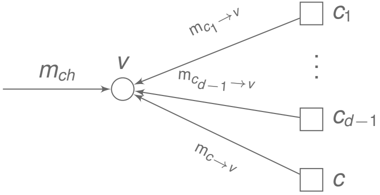
Symbol Message Passing

Final decision.
The final decision at each VN v is

$$\hat{x} = \arg\max_{x \in \mathbb{Z}_q} L_x^{\mathrm{FIN}}$$

where

$$L^{\mathrm{FIN}} = L(m_{\mathrm{ch}}) + \sum_{\mathrm{c} \in \mathcal{N}(\mathrm{v})} L\left(m_{\mathrm{c} \to \mathrm{v}}\right).$$



The qSC-Assumption for SMP

Motivation for the qSC assumption in the extrinsic channel

- Assumption is true for finite fields (i.e. $\mathbb{Z}_q$ with q a prime)

The qSC-Assumption for SMP

Motivation for the qSC assumption in the extrinsic channel

- Assumption is true for finite fields (i.e. $\mathbb{Z}_q$ with q a prime)
- Argument is *independent* of the channel law and hence also valid for the Lee channel.

The qSC-Assumption for SMP

Motivation for the qSC assumption in the extrinsic channel

- Assumption is true for finite fields (i.e. $\mathbb{Z}_q$ with q a prime)
- Argument is *independent* of the channel law and hence also valid for the Lee channel.

The qSC-Assumption for SMP

Motivation for the qSC assumption in the extrinsic channel

- Assumption is true for finite fields (i.e. $\mathbb{Z}_q$ with q a prime)
- Argument is *independent* of the channel law and hence also valid for the Lee channel.

If q is not a prime:

- The approximation is especially accurate when $\mathbb{Z}_q$ consists of many units.

The *q*SC-Assumption for SMP

Motivation for the *q*SC assumption in the extrinsic channel

- Assumption is true for finite fields (i.e. $\mathbb{Z}_q$ with q a prime)
- Argument is *independent* of the channel law and hence also valid for the Lee channel.

If q is not a prime:

- The approximation is especially accurate when $\mathbb{Z}_q$ consists of many units.
- Decoding becomes particularly simple.

Simulations

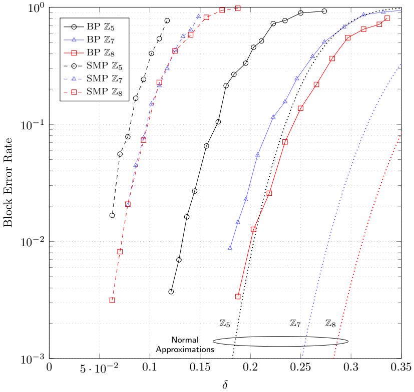
Decoding performance for both BP and SMP over both the Lee channel and the constant-weight Lee channel using

- $(3, 6)$ regular nonbinary LDPC codes of length 256 and 2048,
- For the constant-weight Lee channel, the error vectors are drawn uniformly at random from the set of vectors with a given weight.

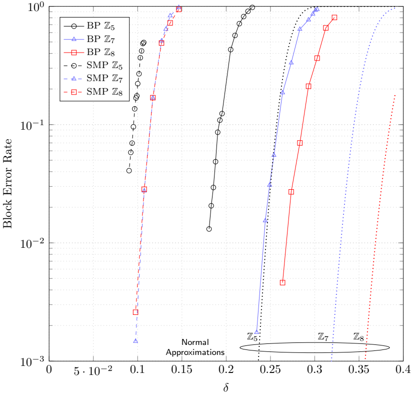
Simulations

Block error rate vs. average Lee weight δ for regular $(3, 6)$ nonbinary LDPC codes in the Lee channel for BP and SMP decoding.

Code length n = 256

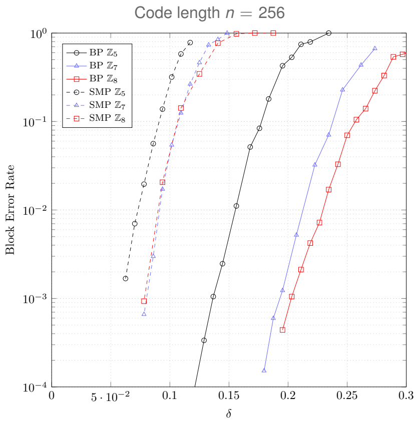


Code length n = 2048



Simulations

Block error rate vs. average Lee weight δ for regular $(3, 6)$ nonbinary LDPC codes in the constant-weight Lee channel for BP and SMP decoding.



Simulations

Block error rate vs. average Lee weight δ for regular $(3, 6)$ nonbinary LDPC codes in the constant-weight Lee channel for BP and SMP decoding.

Thank you very much for your attention!