IEEE GLOBECOM 2022 Conference, Communication Theory Symposium
Rio de Janeiro, December 6, 2022.

Analysis of Low-Density Parity-Check Codes over Finite Integer Rings for the Lee Channel

Jessica Bariffi

German Aerospace Center, DLR
Institute of Communications and Navigation

joint work with Hannes Bartz, Gianluigi Liva and Joachim Rosenthal (UZH)

Outline

1. Ring-linear Codes and the Lee Metric

2. Channel Coding in the Lee Metric

3. Performance Analysis of LDPC Codes

Outline

Ring Linear Codes

Notation:

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

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

Ring Linear Codes

Notation:

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

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

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

Parameters:

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

Ring Linear Codes

Notation:

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

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

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

Parameters:

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

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

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

The Lee Metric

We will denote by $\mathbb{Z}/q\mathbb{Z} = \{0, 1, \ldots, q-1\}$ the ring of integers modulo q.

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

$$\mathrm{wt_L}(a) := \min(a, |\,q-a\,|) \quad \text{and} \quad \mathrm{wt_L}(x) := \sum_{i=1}^{n} \mathrm{wt_L}(x_i)$$

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

The Lee Metric

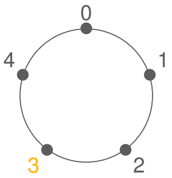
We will denote by $\mathbb{Z}/q\mathbb{Z} = \{0, 1, \ldots, q-1\}$ the ring of integers modulo q.

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

$$\mathrm{wt_L}(a) := \min(a, |\, q - a\,|) \quad \text{and} \quad \mathrm{wt_L}(x) := \sum_{i=1}^{n} \mathrm{wt_L}(x_i)$$

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

Example: $\mathbb{Z}/5\mathbb{Z}$



The Lee weight of $a \in \mathbb{Z}/q\mathbb{Z}$ is the *minimal number* of arcs separating a from 0.

The Lee Metric

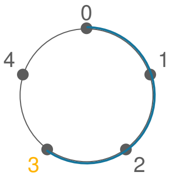
We will denote by $\mathbb{Z}/q\mathbb{Z} = \{0, 1, \dots, q-1\}$ the ring of integers modulo q.

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

$$\mathrm{wt_L}(a) := \min(a, |\, q - a\,|) \quad \text{and} \quad \mathrm{wt_L}(x) := \sum_{i=1}^{n} \mathrm{wt_L}(x_i)$$

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

Example: $\mathbb{Z}/5\mathbb{Z}$



The Lee weight of $a \in \mathbb{Z}/q\mathbb{Z}$ is the *minimal number* of arcs separating a from 0.

The Lee Metric

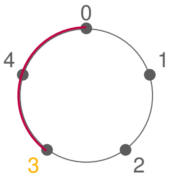
We will denote by $\mathbb{Z}/q\mathbb{Z} = \{0, 1, \dots, q-1\}$ the ring of integers modulo q.

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

$$\mathrm{wt_L}(a) := \min(a, |\, q-a\,|) \quad \text{and} \quad \mathrm{wt_L}(x) := \sum_{i=1}^{n} \mathrm{wt_L}(x_i)$$

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

Example: $\mathbb{Z}/5\mathbb{Z}$



The Lee weight of $a \in \mathbb{Z}/q\mathbb{Z}$ is the *minimal number* of arcs separating a from 0.

The Lee Metric

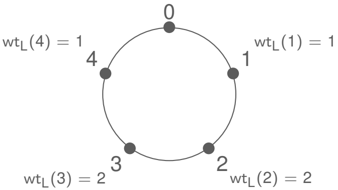
We will denote by $\mathbb{Z}/q\mathbb{Z} = \{0, 1, \ldots, q-1\}$ the ring of integers modulo q.

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

$$\mathrm{wt_L}(a) := \min(a, |\,q-a\,|) \quad \text{and} \quad \mathrm{wt_L}(x) := \sum_{i=1}^{n} \mathrm{wt_L}(x_i)$$

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

Example: $\mathbb{Z}/5\mathbb{Z}$



Properties

For every $a \in \mathbb{Z}/q\mathbb{Z}$ and $x \in (\mathbb{Z}/q\mathbb{Z})^n$

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

The Lee Metric

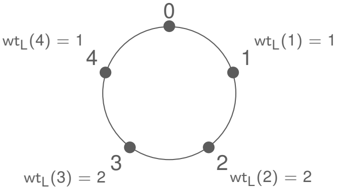
We will denote by $\mathbb{Z}/q\mathbb{Z} = \{0, 1, \ldots, q-1\}$ the ring of integers modulo q.

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

$$\mathrm{wt_L}(a) := \min(a, |\,q - a\,|) \quad \text{and} \quad \mathrm{wt_L}(x) := \sum_{i=1}^{n} \mathrm{wt_L}(x_i)$$

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

Example: $\mathbb{Z}/5\mathbb{Z}$



Properties

For every $a \in \mathbb{Z}/q\mathbb{Z}$ and $x \in (\mathbb{Z}/q\mathbb{Z})^n$

- $\mathrm{wt_L}(a) = \mathrm{wt_L}(q - a)$
- $\mathrm{wt_H}(a) \leq \mathrm{wt_L}(a) \leq \lfloor q/2 \rfloor =: M$
- $\mathrm{wt_H}(x) \leq \mathrm{wt_L}(x) \leq nM$

The Expected Lee Weight

Let $a \in \mathbb{Z}/q\mathbb{Z}$ be chosen uniformly at random.

Lemma

The expected Lee weight of a is then given by

$$\delta_q := \mathbb{E}(\mathrm{wt_L}(a)) = \begin{cases} \frac{q^2-1}{4q} & \text{if } q \text{ is odd,} \\ \frac{q}{4} & \text{if } q \text{ is even.} \end{cases}$$

The Expected Lee Weight

Let $a \in \mathbb{Z}/q\mathbb{Z}$ be chosen uniformly at random.

Lemma

The expected Lee weight of a is then given by

$$\delta_q := \mathbb{E}(\mathrm{wt_L}(a)) = \begin{cases} \frac{q^2-1}{4q} & \text{if } q \text{ is odd,} \\ \frac{q}{4} & \text{if } q \text{ is even.} \end{cases}$$

Let $e \in \mathcal{S}_{t,q}^n := \left\{ x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt_L}(x) = t \right\}$ be chosen uniformly at random.

How does the distribution for each entry e_i look like?

DLR

The Marginal Distribution

Let $T := \lim_{n \longrightarrow \infty} t(n)/n$ be the asymptotic relative Lee weight of e.
Let E be the random variable corresponding to the realization of a random entry of e.

The Marginal Distribution

Let $T := \lim_{n \longrightarrow \infty} t(n)/n$ be the asymptotic relative Lee weight of e.
Let E be the random variable corresponding to the realization of a random entry of e.

Theorem [1]

Assume that the asymptotic relative Lee weight is $T := \lim_{n\rightarrow\infty} \frac{t(n)}{n}$. For every $i \in \mathbb{Z}/q\mathbb{Z}$ the marginal distribution of E is given by

$$p_i := \mathbb{P}(E = i) = \frac{1}{\sum_{j=0}^{q-1} \exp(-\beta \, \mathrm{wt_L}(j))} \exp\left(-\beta i\right)$$

where β is the solution to $T = \sum_{i=0}^{M} \mathrm{wt_L}(i) p_i$.

The Marginal Distribution

Let $T := \lim_{n \longrightarrow \infty} t(n)/n$ be the asymptotic relative Lee weight of e.
Let E be the random variable corresponding to the realization of a random entry of e.

Theorem [1]

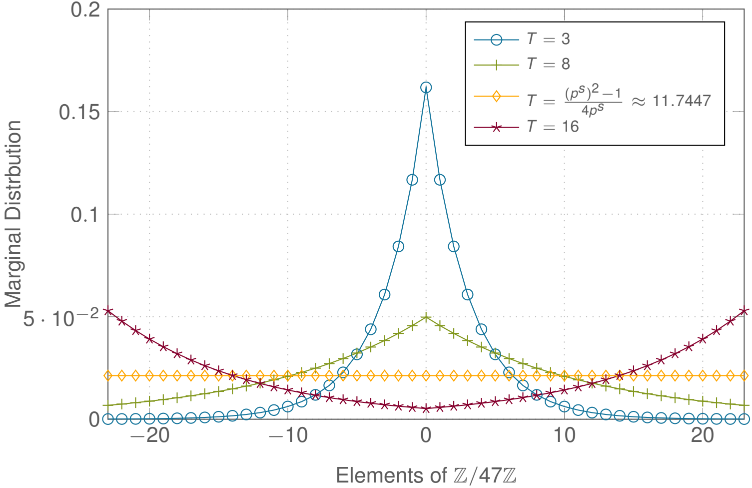
Assume that the asymptotic relative Lee weight is $T := \lim_{n\to\infty} \frac{t(n)}{n}$. For every $i \in \mathbb{Z}/q\mathbb{Z}$ the marginal distribution of E is given by

$$p_i := \mathbb{P}(E = i) = \frac{1}{\sum_{j=0}^{q-1} \exp(-\beta \, \mathrm{wt_L}(j))} \exp(-\beta i)$$

where β is the solution to $T = \sum_{i=0}^{M} \mathrm{wt_L}(i) p_i$.

Note $T < \delta_q \iff \beta > 0$

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



Outline

Channel Coding

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

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

With given channel law

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

Channel Coding

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

With given channel law

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

We consider here an additive channel, i.e., $\quad y = x + e.$

Memoryless Lee Channel

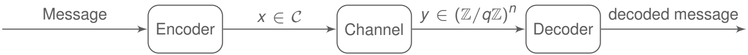
Restrict, for every $i = 1, \dots, n$, to e_i as a realization of a random variable E_i with

$$\mathbb{P}(E_i = e_i) \propto \exp(-\lambda \, \mathrm{wt_L}(e_i)), \qquad \lambda > 0,$$

$$P_{Y_i|X_i}(y_i|x_i) = \frac{1}{Z(\lambda)} \exp\left(-\lambda \, \mathrm{d_L}(x_i, y_i)\right), \qquad Z(\lambda) := \sum_{e_i=0}^{q-1} \exp(-\lambda \, \mathrm{wt_L}(e_i))$$

Channel Coding

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



With given channel law

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

We consider here an additive channel, i.e., $\quad y = x + e.$

Memoryless Lee Channel

Restrict, for every $i = 1, \ldots, n$, to e_i as a realization of a random variable E_i with

$$\mathbb{P}(E_i = e_i) \propto \exp(-\lambda \, \mathrm{wt_L}(e_i)), \qquad \lambda > 0,$$

$$P_{Y_i|X_i}(y_i|x_i) = \frac{1}{Z(\lambda)} \exp\left(-\lambda \, \mathrm{d_L}(x_i, y_i)\right), \qquad Z(\lambda) := \sum_{e_i=0}^{q-1} \exp(-\lambda \, \mathrm{wt_L}(e_i))$$

Constant Lee Weight Channel

The error e has fixed Lee weight t and is chosen uniformly at random from $\{z \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt_L}(z) = t\}$.

Random Coding Union Bounds

$\mathcal{C}$: best random (n, nR) code over $\mathbb{Z}/q\mathbb{Z}$

δ : normalized weight of error

$P_B(\mathcal{C})$: Error probability

$$\mathrm{H}_\delta^+ := \begin{cases} \mathrm{H}_\delta & \text{if } \delta \leq \delta_q \\ \log q & \text{otherwise.} \end{cases}$$

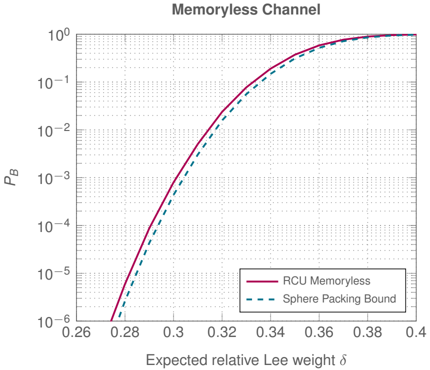
RCU bound

Constant Lee Weight Channel

$$\mathbb{E}\left[P_B(\mathcal{C})\right] < \exp\left(-n\left[(1-R)\log q - \mathrm{H}_\delta^+\right]^+\right)$$

Memoryless Channel

$$\mathbb{E}\left[P_B(\mathcal{C})\right] < \mathbb{E}\left[\exp\left(-n\left[(1-R)\log q - \mathrm{H}_{D/n}^+\right]^+\right)\right]$$



DLR

Outline

LDPC Codes over $\mathbb{Z}/q\mathbb{Z}$

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

LDPC Codes over $\mathbb{Z}/q\mathbb{Z}$

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

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

- variable nodes (VN) $\{v_1, \ldots, v_n\}$
- check nodes (CN) $\{c_1, \ldots, c_m\}$

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

LDPC Codes over $\mathbb{Z}/q\mathbb{Z}$

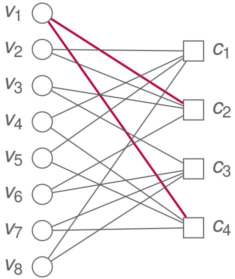
An $[n, k]_q$ **LDPC code** over $\mathbb{Z}/q\mathbb{Z}$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $(\mathbb{Z}/q\mathbb{Z})^\times$.

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

- variable nodes (VN) $\{v_1, \dots, v_n\}$
- check nodes (CN) $\{c_1, \dots, c_m\}$

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

$$H = \begin{bmatrix} 0 & 1 & 0 & 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 3 & 1 \\ 1 & 0 & 0 & 3 & 4 & 0 & 1 & 0 \end{bmatrix} \in (\mathbb{Z}/5\mathbb{Z})^{4\times 8}$$



LDPC Codes over $\mathbb{Z}/q\mathbb{Z}$

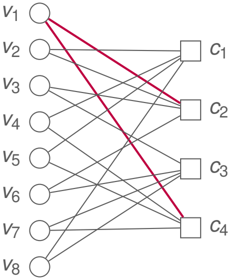
An $[n, k]_q$ **LDPC code** over $\mathbb{Z}/q\mathbb{Z}$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $(\mathbb{Z}/q\mathbb{Z})^\times$.

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

- variable nodes (VN) $\{v_1, \ldots, v_n\}$
- check nodes (CN) $\{c_1, \ldots, c_m\}$

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

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 5 & 0 & 0 & 1 \\ 1 & 5 & 1 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 5 & 1 \\ 1 & 0 & 0 & 5 & 5 & 0 & 1 & 0 \end{bmatrix} \in (\mathbb{Z}/6\mathbb{Z})^{4\times 8}$$



LDPC Codes over $\mathbb{Z}/q\mathbb{Z}$

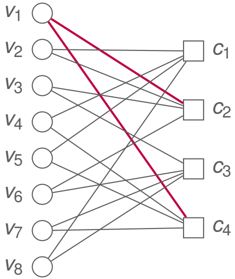
An $[n, k]_q$ **LDPC code** over $\mathbb{Z}/q\mathbb{Z}$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $(\mathbb{Z}/q\mathbb{Z})^\times$.

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

- variable nodes (VN) $\{v_1, \ldots, v_n\}$
- check nodes (CN) $\{c_1, \ldots, c_m\}$

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

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 5 & 0 & 0 & 1 \\ 1 & 5 & 1 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 5 & 1 \\ 1 & 0 & 0 & 5 & 5 & 0 & 1 & 0 \end{bmatrix} \in (\mathbb{Z}/6\mathbb{Z})^{4\times 8}$$



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.

Simulation Set-up

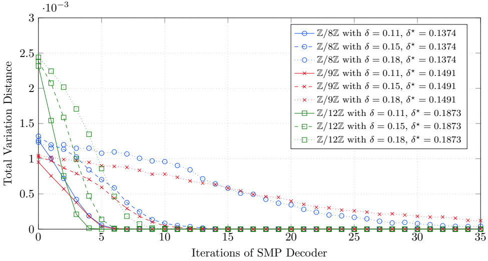
- Consider regular nonbinary LDPC codes obtained from Monte Carlo Simulations
- Parity-check matrices are designed via the progressive edge growth
- Belief Propagation Decoding
- Symbol Message Passing Decoding

Simulation Set-up

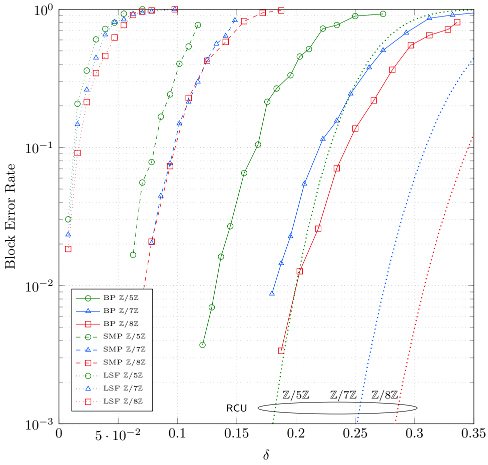
- Consider regular nonbinary LDPC codes obtained from Monte Carlo Simulations
- Parity-check matrices are designed via the progressive edge growth
- Belief Propagation Decoding
- Symbol Message Passing Decoding
  - Assumption: The CN to VN messages are modelled as observations from a q-ary symmetric channel.
    $\longrightarrow$ true (in limits of the block length) if q is prime.

Simulation Set-up

- Consider regular nonbinary LDPC codes obtained from Monte Carlo Simulations
- Parity-check matrices are designed via the progressive edge growth
- Belief Propagation Decoding
- Symbol Message Passing Decoding
  - Assumption: The CN to VN messages are modelled as observations from a q-ary symmetric channel.
    $\longrightarrow$ true (in limits of the block length) if q is prime.
    $\longrightarrow$ valid for q nonprime as the total variation distance tends to zero



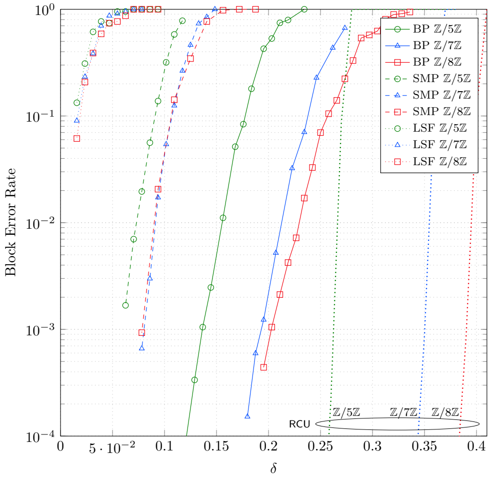
Simulation - Memoryless Lee Channel



Parameters:

- length $n = 256$
- regular $(3, 6)$ LDPC Codes
- Considered residue rings: $\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$
- Decoders:
  - Lee Symbol Flipping
  - Message Passing
  - Belief Propagation

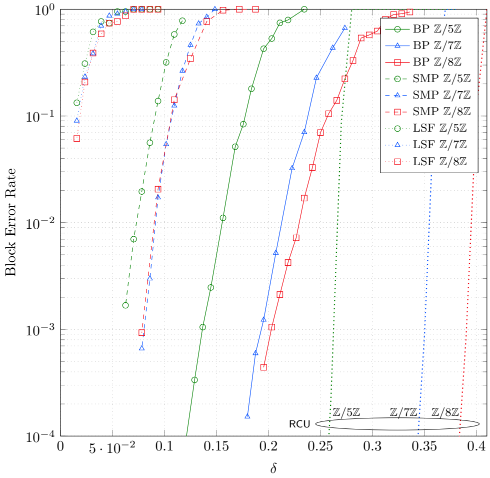
Simulation - Constant Lee Weight Channel



Parameters:

- length $n = 256$
- regular $(3, 6)$ LDPC Codes
- Considered residue rings: $\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$
- Decoders:
  - Lee Symbol Flipping
  - Message Passing
  - Belief Propagation

Simulation - Constant Lee Weight Channel



Parameters:

- length $n = 256$
- regular $(3, 6)$ LDPC Codes
- Considered residue rings: $\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$
- Decoders:
  - Lee Symbol Flipping
  - Message Passing
  - Belief Propagation

Thank you for your attention!