Algebraic Coding Theory e-Summer School - ACT21
June 9, 2021

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

Linear Block Codes

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 [Linear Code]

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

Linear Block Codes

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

Definition [Linear Code]

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

Definition [Hamming Weight/Distance]

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

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

Linear Block Codes

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 [Linear Code]

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

Definition [Hamming Weight/Distance]

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

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

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

$$\mathcal{C} = \ker(H).$$

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

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

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

LDPC Codes over Finite Integer Rings

According to Sridhara and Fuja

Definition [LDPC Code]

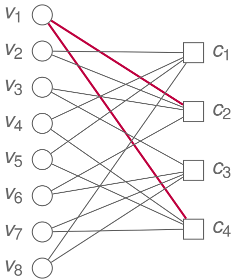
An $[n, k]_q$ LDPC code over $\mathbb{Z}_q$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $\mathbb{Z}_q^\times$.

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

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

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

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



LDPC Codes over Finite Integer Rings

According to Sridhara and Fuja

Definition [LDPC Code]

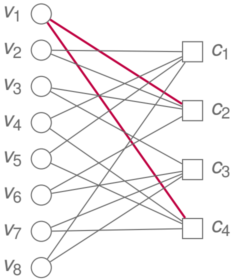
An $[n, k]_q$ LDPC code over $\mathbb{Z}_q$ is defined by a sparse parity-check matrix H, whose nonzero entries lie in the set of units $\mathbb{Z}_q^\times$.

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

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

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

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



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.

The Lee Metric

Definition [Lee weight]

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

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

The Lee weight of a vector $x \in \mathbb{Z}_q^n$ is the sum of the Lee weights of its entries, i.e.,

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

The Lee Metric

Definition [Lee weight]

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

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

The Lee weight of a vector $x \in \mathbb{Z}_q^n$ is the sum of the Lee weights of its entries, i.e.,

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

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

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

The Lee Metric

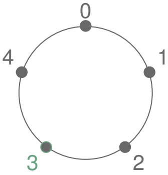
Definition [Lee weight]

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

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

The Lee weight of a vector $x \in \mathbb{Z}_q^n$ is the sum of the Lee weights of its entries, i.e.,

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



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

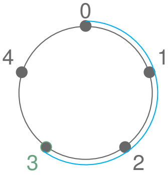
Definition [Lee weight]

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

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

The Lee weight of a vector $x \in \mathbb{Z}_q^n$ is the sum of the Lee weights of its entries, i.e.,

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



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

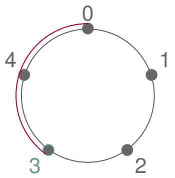
Definition [Lee weight]

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

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

The Lee weight of a vector $x \in \mathbb{Z}_q^n$ is the sum of the Lee weights of its entries, i.e.,

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



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

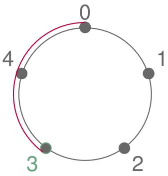
Definition [Lee weight]

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

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

The Lee weight of a vector $x \in \mathbb{Z}_q^n$ is the sum of the Lee weights of its entries, i.e.,

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



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

DLR

The Lee Metric

Properties

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

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

The Lee Metric

Properties

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

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

The Lee Metric

Properties

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

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

The Lee Metric

Properties

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

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

Definition [Lee Distance]

The Lee distance of two scalars $a, b \in \mathbb{Z}_q$ is $\mathrm{d}_L(a,b) := \mathrm{wt}_L(a-b)$. The Lee distance between two vectors $x, y \in \mathbb{Z}_q^n$ is

$$\mathrm{d}_L(x,y) = \sum_{i=1}^{n} \mathrm{d}_L(x_i, y_i).$$

Channel Coding

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

With a given channel law

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

Channel Coding

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

With a given channel law

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

Definition [Discrete Memoryless Channel]

A channel is called *discrete memoryless*, if the input and output alphabets are discrete, finite sets and the output $Y = y$ at time t only depends on the input $X = x$ at that time t, i.e.,

$$\mathbb{P}(Y_1 = y_1, \ldots, Y_n = y_n \mid X_1 = x_1, \ldots, X_n = x_n) = \prod_{i=1}^{n} \mathbb{P}(Y_i = y_i \mid X_i = x_i)$$

Channel Coding

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

With a given channel law

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

Definition [Discrete Memoryless Channel]

A channel is called *discrete memoryless*, if the input and output alphabets are discrete, finite sets and the output $Y = y$ at time t only depends on the input $X = x$ at that time t, i.e.,

$$\mathbb{P}(Y_1 = y_1, \dots, Y_n = y_n \mid X_1 = x_1, \dots, X_n = x_n) = \prod_{i=1}^{n} \mathbb{P}(Y_i = y_i \mid X_i = x_i)$$

Example: q-ary Symmetric Channel

Let $x \in \mathbb{Z}_q^n$ sent and $y \in \mathbb{Z}_q^n$ received.

DLR

Channel Coding

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

With a given channel law

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

Definition [Discrete Memoryless Channel]

A channel is called *discrete memoryless*, if the input and output alphabets are discrete, finite sets and the output $Y = y$ at time t only depends on the input $X = x$ at that time t, i.e.,

$$\mathbb{P}(Y_1 = y_1, \ldots, Y_n = y_n \mid X_1 = x_1, \ldots, X_n = x_n) = \prod_{i=1}^{n} \mathbb{P}(Y_i = y_i \mid X_i = x_i)$$

Example: q-ary Symmetric Channel

Let $x \in \mathbb{Z}_q^n$ sent and $y \in \mathbb{Z}_q^n$ received. Then $P_{Y_i|X_i}(y_i \mid x_i) := \begin{cases} 1 - \varepsilon & \text{if } y_i = x_i, \\ \frac{\varepsilon}{q-1} & \text{else.} \end{cases} \quad \forall i.$

Outline

The Lee Channel

Define the “Lee Channel” over $\mathbb{Z}_q$ as proposed by Chiang and Wolf:

$$p_i := \mathbb{P}(i \,|\, 0) = \mathbb{P}(-i \,|\, 0), \text{ for } i = 0, \dots, \lfloor q/2 \rfloor. \tag{3}$$

Due to symmetry: $\mathbb{P}(i \,|\, j) = \mathbb{P}(i - j \mod q \,|\, 0)$

The Lee Channel

Define the "Lee Channel" over $\mathbb{Z}_q$ as proposed by Chiang and Wolf:

$$p_i := \mathbb{P}(i \mid 0) = \mathbb{P}(-i \mid 0), \text{ for } i = 0, \dots, \lfloor q/2 \rfloor. \tag{3}$$

Due to symmetry: $\mathbb{P}(i \mid j) = \mathbb{P}(i - j \mod q \mid 0)$

Theorem (Chiang and Wolf)

The channel described in (3) is strictly matched to the Lee metric for maximum likelihood decoding if and only if the following two properties hold.

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

The Lee Channel

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

$$\underset{\text{channel output}}{y} = \underset{\text{channel input}}{x} + \underset{\text{additive error term}}{e} \tag{4}$$

The Lee Channel

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

$$\underbrace{y}_{\text{channel output}} = \underbrace{x}_{\text{channel input}} + \underbrace{e}_{\text{additive error term}} \tag{4}$$

The channel law is given by

$$\mathbb{P}(Y = y \,|\, X = x) =: P_{Y|X}(y|x) = \frac{1}{Z} \exp\left(-\lambda \, \mathrm{d}_L(x, y)\right), \tag{5}$$

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

Note:

- The channel defined in (5) is the DMC matched to the Lee metric.
- The conditional distribution (5) arises (in the limit of large n) as the marginal distribution of a 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?

The Constant-weight Lee Channel

Let $\mathbf{p} = (p_0, \ldots, p_{q-1})$, with $p_i := \mathbb{P}(i \mid 0)$ for all $i \in \mathbb{Z}_q$.

Lemma

The constant-weight Lee channel over $\mathbb{Z}_q$ has channel distribution

$$p_i^\star = \kappa \exp\left(-\lambda \operatorname{wt}_L(i)\right), \quad \kappa := \frac{1}{\sum_{j=0}^{q-1} \exp(-\lambda \operatorname{wt}_L(j))},$$

such that it matches under maximum likelihood decoding.

The Constant-weight Lee Channel

Let $\mathbf{p} = (p_0, \ldots, p_{q-1})$, with $p_i := \mathbb{P}(i \mid 0)$ for all $i \in \mathbb{Z}_q$.

Lemma

The constant-weight Lee channel over $\mathbb{Z}_q$ has channel distribution

$$p_i^\star = \kappa \exp\left(-\lambda \,\mathrm{wt}_L(i)\right), \quad \kappa := \frac{1}{\sum_{j=0}^{q-1} \exp(-\lambda \,\mathrm{wt}_L(j))},$$

such that it matches under maximum likelihood decoding.

Sketch of proof
We want that $\mathbf{p} = (p_0, \ldots, p_{q-1})$ maximizes the entropy function

$$H_e(\mathbf{p}) := -\sum_{i=0, p_i \neq 0}^{q-1} p_i \log p_i$$

under the constraint that $\sum_{i=0}^{q-1} \mathrm{wt}_L(i) p_i = t/n =: \delta$.

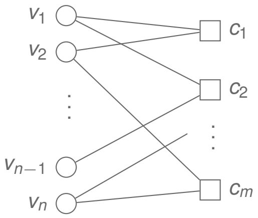
Outline

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.

Symbol Message Passing

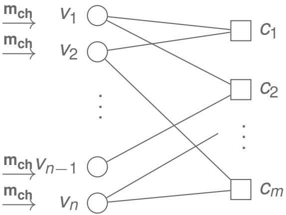
Consider a nonbinary LDPC code $\mathcal{C}$ with VNs $\{v_1, \ldots, v_n\}$ and CNs $\{c_1, \ldots, c_m\}$ and parity-check matrix H. Denote by $\mathcal{N}(v_j)$ and $\mathcal{N}(c_i)$ the set of all connecting elements to VN v_j and CN c_i, respectively.



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.

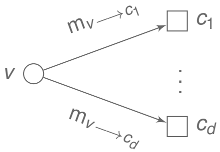
Every VN v receives the channel observation
$\mathbf{m_{ch}} := \left(P_{Y|X}(y \mid 0), \ldots, P_{Y|X}(y \mid q-1)\right)$



Symbol Message Passing

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

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

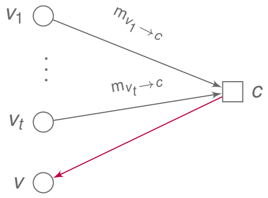


Symbol Message Passing

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

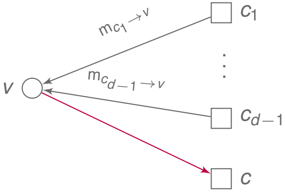
VN-to-CN step.

Define the aggregated extrinsic L-vector

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

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,

$$P_{M|X}(m|x) = \begin{cases} 1-\xi & \text{if } m = x \\ \xi/(q-1) & \text{otherwise} \end{cases}$$



Then the VN-to-CN messages are

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

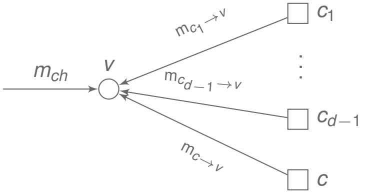
Symbol Message Passing

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

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.

The qSC-Assumption for SMP

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.
- Motivation behind this choice:

The qSC-Assumption for SMP

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.
- Motivation behind this choice:
  - Over finite fields, the extrinsic channel transition probabilities, averaged over a uniform distribution of nonzero elements the parity-check matrix, yield (in the limit of a large block length) a qSC.

The qSC-Assumption for SMP

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.
- Motivation behind this choice:
  - Over finite fields, the extrinsic channel transition probabilities, averaged over a uniform distribution of nonzero elements the parity-check matrix, yield (in the limit of a large block length) a qSC.
  - For a field $\mathbb{Z}_q$ this argument is *independent* of the channel law and hence also valid for the Lee channel.

The qSC-Assumption for SMP

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.
- Motivation behind this choice:
  - Over finite fields, the extrinsic channel transition probabilities, averaged over a uniform distribution of nonzero elements the parity-check matrix, yield (in the limit of a large block length) a qSC.
  - For a field $\mathbb{Z}_q$ this argument is *independent* of the channel law and hence also valid for the Lee channel.
- If q is not a prime, we treat the messages as qSC anyways, due to the following observations

DLR

The qSC-Assumption for SMP

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.
- Motivation behind this choice:
  - Over finite fields, the extrinsic channel transition probabilities, averaged over a uniform distribution of nonzero elements the parity-check matrix, yield (in the limit of a large block length) a qSC.
  - For a field $\mathbb{Z}_q$ this argument is *independent* of the channel law and hence also valid for the Lee channel.
- If q is not a prime, we treat the messages as qSC anyways, due to the following observations
  - The approximation is especially accurate when the fraction of elements of $\mathbb{Z}_q \setminus \{0\}$ that are in $\mathbb{Z}_q^\times$ is large.

The qSC-Assumption for SMP

- Following Lechner, Pedersen, and Kramer, the CN to VN messages are modelled as observations from a q-ary symmetric channel.
- Motivation behind this choice:
  - Over finite fields, the extrinsic channel transition probabilities, averaged over a uniform distribution of nonzero elements the parity-check matrix, yield (in the limit of a large block length) a qSC.
  - For a field $\mathbb{Z}_q$ this argument is *independent* of the channel law and hence also valid for the Lee channel.
- If q is not a prime, we treat the messages as qSC anyways, due to the following observations
  - The approximation is especially accurate when the fraction of elements of $\mathbb{Z}_q \setminus \{0\}$ that are in $\mathbb{Z}_q^{\times}$ is large.
  - The use of the qSC approximation is important from a practical viewpoint, i.e., decoding becomes particularly simple.

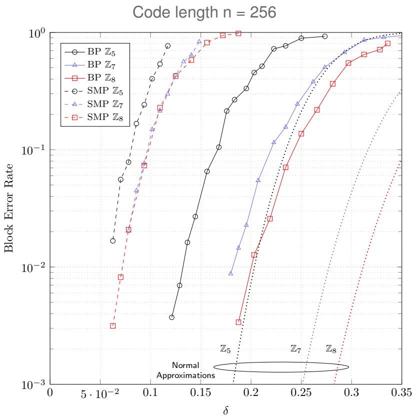
Simulations

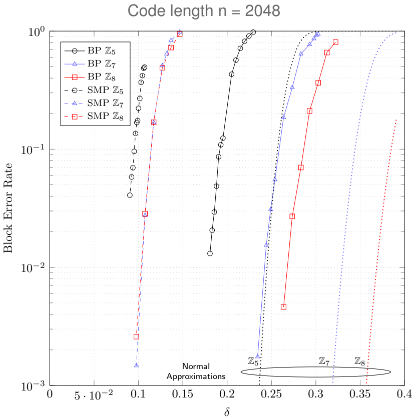
Decoding performance for both BP and SMP over both the Lee channel and the constant-weight Lee channel using

- $(3, 6)$ 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

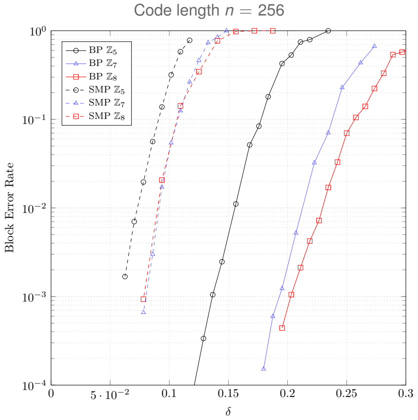
Block error rate vs. average Lee weight δ for regular $(3,6)$ nonbinary LDPC codes in the Lee channel for BP and SMP decoding.





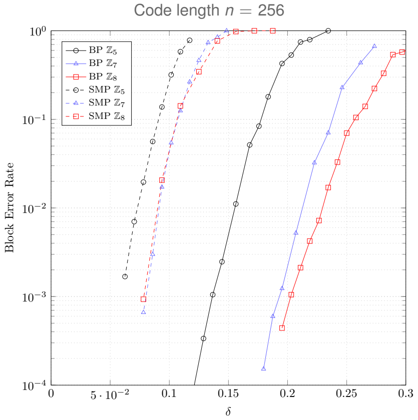
Simulations

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!