International Workshop on Code-Based Cryptography (CBCrypto) 2022

Information Set Decoding for Lee-Metric Codes using Restricted Spheres

Jessica Bariffi

joint work with Karan Khathuria (UT) and Violetta Weger (TUM)

Institute for Communications and Navigation
German Aerospace Center, DLR

Motivation

Code-based cryptography for quantum secure cryptosystems

Motivation

Code-based cryptography for quantum secure cryptosystems

The original McEliece cryptosystem suffers from large key sizes (even though unbroken)

- ! Alternative metrics are considered

Motivation

Code-based cryptography for quantum secure cryptosystems

The original McEliece cryptosystem suffers from large key sizes (even though unbroken)

- ! Alternative metrics are considered

The security relies on the hardness of the syndrome decoding problem

- ! Generic decoding in the Lee metric has a large cost
- ! NP-hard in the Lee metric

Outline

1. Preliminaries

2. Information Set Decoding using Restricted Spheres
   - Up to Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance

3. Comparison

Outline

DLR

Ring-Linear Codes

Let p a prime number and s and n two positive integers.

Definition

A *linear code* C $(\mathbb{Z}/p^s\mathbb{Z})^n$ is a $\mathbb{Z}/p^s\mathbb{Z}$-submodule of $(\mathbb{Z}/p^s\mathbb{Z})^n$.

Ring-Linear Codes

Let p a prime number and s and n two positive integers.

Definition

A *linear code* C $(\mathbb{Z}/p^s\mathbb{Z})^n$ is a $\mathbb{Z}/p^s\mathbb{Z}$-submodule of $(\mathbb{Z}/p^s\mathbb{Z})^n$.

Parameters:

n is called the *length* of C

$k := \log_{p^s} |C|$ is the $\mathbb{Z}/p^s\mathbb{Z}$-*dimension* of C

$R := k/n$ denotes the *rate* of C.

The Lee Metric

Definition

For $a \in \mathbb{Z}/p^s\mathbb{Z}$ and $e = (e_1, \ldots, e_n) \in (\mathbb{Z}/p^s\mathbb{Z})^n$ we define their *Lee weight*, respectively, by

$$\mathrm{wt}_L(a) := \min(a, p^s - a),$$

$$\mathrm{wt}_L(e) := \sum_{i=1}^{n} \mathrm{wt}_L(e_i).$$

The Lee Metric

Definition

For $a \in \mathbb{Z}/p^s\mathbb{Z}$ and $e = (e_1, \ldots, e_n) \in (\mathbb{Z}/p^s\mathbb{Z})^n$ we define their *Lee weight*, respectively, by

$$\mathrm{wt}_L(a) := \min(a, p^s - a),$$

$$\mathrm{wt}_L(e) := \sum_{i=1}^{n} \mathrm{wt}_L(e_i).$$

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

$0: \quad \mathrm{wt}_L(0) = 0$

$1: \quad \mathrm{wt}_L(1) = 1$

$2: \quad \mathrm{wt}_L(2) = 2$

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

$4: \quad \mathrm{wt}_L(4) = 1$

The Lee Metric

Definition

For $a \in \mathbb{Z}/p^s\mathbb{Z}$ and $e = (e_1, \ldots, e_n) \in (\mathbb{Z}/p^s\mathbb{Z})^n$ we define their *Lee weight*, respectively, by

$$\mathrm{wt}_L(a) := \min(a, p^s - a),$$

$$\mathrm{wt}_L(e) := \sum_{i=1}^{n} \mathrm{wt}_L(e_i).$$

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

$0: \quad \mathrm{wt}_L(0) = 0$

$1: \quad \mathrm{wt}_L(1) = 1$

$2: \quad \mathrm{wt}_L(2) = 2$

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

$4: \quad \mathrm{wt}_L(4) = 1$

Properties:

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

$$\mathrm{wt}_L(a) = \mathrm{wt}_L(p^s - a)$$

$$\mathrm{wt}_H(a) \quad \mathrm{wt}_L(a) \quad bp^s/2c =: M$$

$$\mathrm{wt}_H(e) \quad \mathrm{wt}_L(e) \quad nM$$

The Expected Lee Weight

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

Lemma

The expected Lee weight of a is then given by

$$\mu_{p^s} := \mathrm{E}(\mathrm{wt}_{\mathrm{L}}(a)) = \begin{cases} \frac{(p^s)^2 - 1}{4p^s} & \text{if } p^s \text{ is odd;} \\ \frac{p^s}{4} & \text{if } p^s \text{ is even:} \end{cases}$$

The Expected Lee Weight

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

Lemma

The expected Lee weight of a is then given by

$$\mu_{p^s} := \mathrm{E}(\mathrm{wt}_{\mathrm{L}}(a)) = \begin{cases} \frac{(p^s)^2 - 1}{4p^s} & \text{if } p^s \text{ is odd;} \\ \frac{p^s}{4} & \text{if } p^s \text{ is even:} \end{cases}$$

Let $e \in S^n_{t;p^s} := \{x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid \mathrm{wt}_{\mathrm{L}}(x) = t\}$ be chosen uniformly at random.

The Expected Lee Weight

Let $a \in Z/p^s Z$ be chosen uniformly at random.

Lemma

The expected Lee weight of a is then given by

$$\mu_{p^s} := \mathrm{E}(\mathrm{wt}_L(a)) = \begin{cases} \frac{(p^s)^2 - 1}{4p^s} & \text{if } p^s \text{ is odd;} \\ \frac{p^s}{4} & \text{if } p^s \text{ is even:} \end{cases}$$

Let $e \in S^n_{t;p^s} := \{x \in (Z/p^s Z)^n \mid \mathrm{wt}_L(x) = t\}$ be chosen uniformly at random.

How does the distribution for each entry e_i look like?

The Expected Lee Weight

Let $a \in Z/p^s Z$ be chosen uniformly at random.

Lemma

The expected Lee weight of a is then given by

$$\mu_{p^s} := \mathrm{E}(\mathrm{wt}_L(a)) = \begin{cases} \frac{(p^s)^2 - 1}{4p^s} & \text{if } p^s \text{ is odd;} \\ \frac{p^s}{4} & \text{if } p^s \text{ is even:} \end{cases}$$

Let $e \in S^n_{t;p^s} := \{ x \in (Z/p^s Z)^n \mid \mathrm{wt}_L(x) = t \}$ be chosen uniformly at random.

How does the distribution for each entry e_i look like?

Let $T := \lim_{n \to \infty} t(n)/n$ be the asymptotic relative Lee weight of e.

The Marginal Distribution

Let E be the random variable corresponding to the realization of a random entry of e.

The Marginal Distribution

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 $i \in \mathbb{Z}/p^s\mathbb{Z}$ the marginal distribution of E is given by

$$p_i := \mathrm{P}(E = i) = \frac{1}{\sum_{j=0}^{p^s-1} \exp(\lambda \mathrm{wt_L}(j))} \exp(\lambda i)$$

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

[1] "On the Properties of Error Patterns in the Constant Lee Weight Channel". In: *International Zurich Seminar on Information and Communication (IZS)*. 2022, pp. 44–48.

The Marginal Distribution

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 $i \in \mathbb{Z}/p^s\mathbb{Z}$ the marginal distribution of E is given by

$$p_i := \mathrm{P}(E = i) = \frac{1}{\sum_{j=0}^{p^s} \exp(\quad \mathrm{wt_L}(j))} \exp(\quad i)$$

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

$$\mathrm{P}(\mathrm{wt_L}(E) = j) = \begin{cases} \mathrm{P}(E = j) & \text{if } (j = 0) \text{ or } (j = M \text{ and } p \text{ is even}); \\ 2\mathrm{P}(E = j) & \text{if } (1 \quad j \quad M \quad 1) \text{ or } (j = M \text{ and } p \text{ is odd}): \end{cases}$$

[1] "On the Properties of Error Patterns in the Constant Lee Weight Channel". In: *International Zurich Seminar on Information and Communication (IZS)*. 2022, pp. 44–48.

The Marginal Distribution

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 $i \in \mathbb{Z}/p^s\mathbb{Z}$ the marginal distribution of E is given by

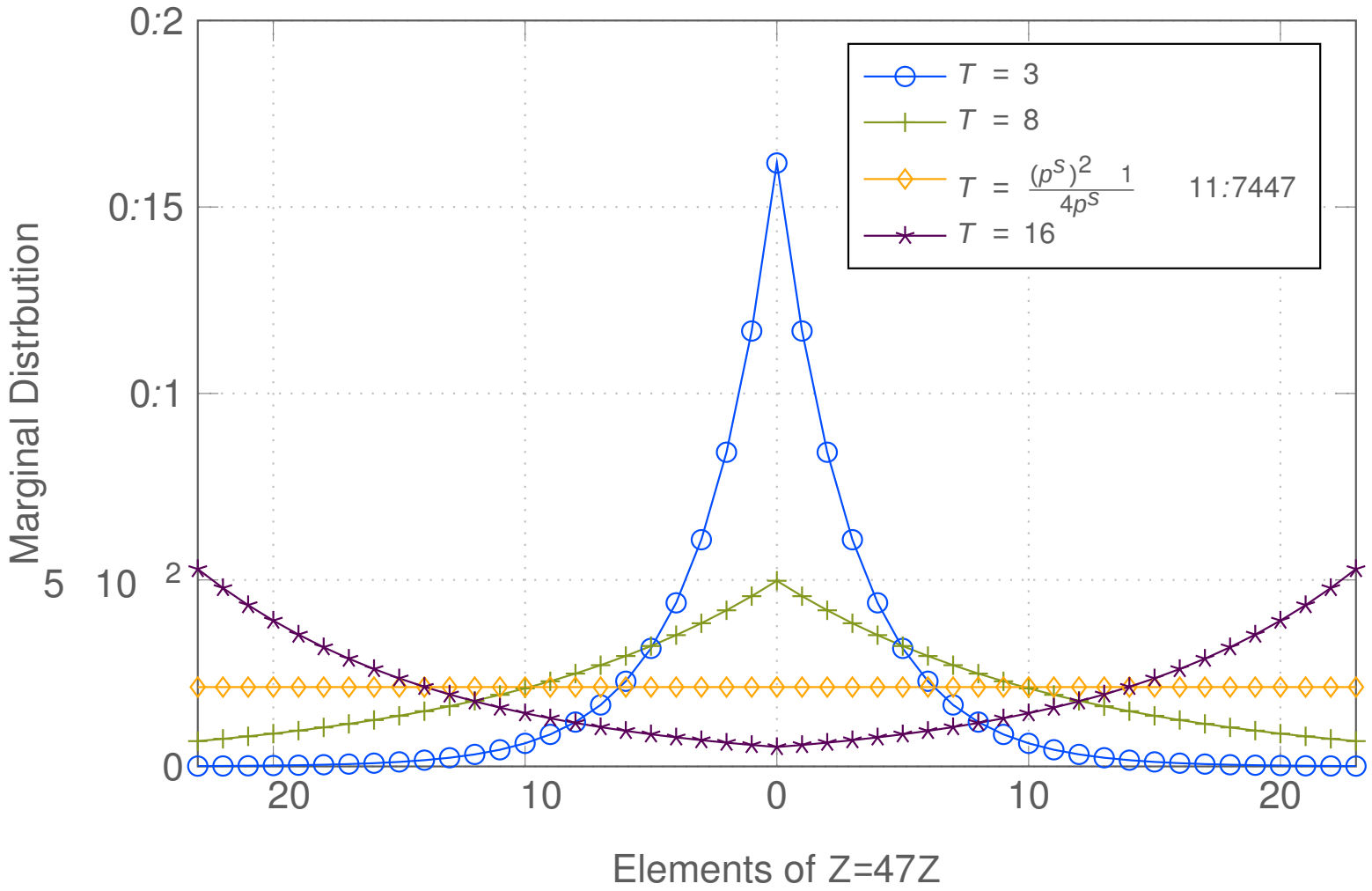
$$p_i := \mathrm{P}(E = i) = \frac{1}{\sum_{j=0}^{p^s-1} \exp(\quad \mathrm{wt_L}(j))} \exp(\quad i)$$

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

$$\mathrm{P}(\mathrm{wt_L}(E) = j) = \begin{cases} \mathrm{P}(E = j) & \text{if } (j = 0) \text{ or } (j = M \text{ and } p \text{ is even}); \\ 2\mathrm{P}(E = j) & \text{if } (1 \quad j \quad M \quad 1) \text{ or } (j = M \text{ and } p \text{ is odd}): \end{cases}$$

Note: $T < \quad _{p^s} \quad (\quad) \quad > 0$

The Marginal Distribution - Example over Z=47Z



Outline

DLR

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

Given $H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n}$, $s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k}$ and $t \in \mathbb{N}$,
find $e \in (\mathbb{Z}/p^s\mathbb{Z})^n$ s.t. $\mathrm{wt}_L(e) = t$ and $s = eH^\top$:

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

$$\text{Given } H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n}, s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k} \text{ and } t \in \mathbb{N},$$
$$\text{find } e \in (\mathbb{Z}/p^s\mathbb{Z})^n \text{ s.t. } \mathrm{wt}_L(e) = t \text{ and } s = eH^T.$$

Information set decoding (ISD) algorithms to solve the LSDP

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

$$\text{Given } H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n},\ s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k} \text{ and } t \in \mathbb{N};$$
$$\text{find } e \in (\mathbb{Z}/p^s\mathbb{Z})^n \text{ s.t. } \mathrm{wt}_L(e) = t \text{ and } s = eH^T:$$

Information set decoding (ISD) algorithms to solve the LSDP

- ! Recent improvements: using partial Gaussian elimination[1]

[1] Matthieu Finiasz and Nicolas Sendrier. "Security bounds for the design of code-based cryptosystems". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2009, pp. 88–105.

DLR

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

Given $H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n}$, $s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k}$ and $t \in \mathbb{N}$,
find $e \in (\mathbb{Z}/p^s\mathbb{Z})^n$ s.t. $\mathrm{wt}_L(e) = t$ and $s = eH^T$.

Information set decoding (ISD) algorithms to solve the LSDP

! Recent improvements: using partial Gaussian elimination

::: Representation technique[1] or Wagner's approach[2]

[1] Anja Becker et al. "Decoding random binary linear codes in $2^{n/20}$: How 1+ 1= 0 improves information set decoding". In: *Annual international conference on the theory and applications of cryptographic techniques*. Springer. 2012, pp. 520–536.

[2] Alexander May, Alexander Meurer, and Enrico Thomae. "Decoding Random Linear Codes in $\mathcal{O}(2^{0.054n})$". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2011, pp. 107–124.

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

$$\text{Given } H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n},\ s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k} \text{ and } t \in \mathbb{N};$$
$$\text{find } e \in (\mathbb{Z}/p^s\mathbb{Z})^n \text{ s.t. } \mathrm{wt}_L(e) = t \text{ and } s = eH^\top.$$

Information set decoding (ISD) algorithms to solve the LSDP

- ! Recent improvements: using partial Gaussian elimination
  - ::: Representation technique or Wagner's approach
  - ::: BJMM on 2 Levels is fastest in the Lee metric (non-amortized)[1]
  - ::: Wagner's approach is fastest in the Lee metric (amortized)[2]

[1] Violetta Weger et al. "On the hardness of the Lee syndrome decoding problem". In: *Advances in Mathematics of Communications* (2019). DOI: 10.3934/amc.2022029.

[2] André Chailloux, Thomas Debris-Alazard, and Simona Etinski. "Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric". In: *International Conference on Post-Quantum Cryptography*. Springer. 2021, pp. 44–62.

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

$$\text{Given } H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n},\ s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k} \text{ and } t \in \mathbb{N},$$
$$\text{find } e \in (\mathbb{Z}/p^s\mathbb{Z})^n \text{ s.t. } \mathrm{wt}_L(e) = t \text{ and } s = eH^T.$$

Information set decoding (ISD) algorithms to solve the LSDP

- Recent improvements: using partial Gaussian elimination
  - ::: Representation technique or Wagner's approach
  - ::: BJMM on 2 Levels is fastest in the Lee metric (non-amortized)
  - ::: Wagner's approach is fastest in the Lee metric (amortized)

The cost of an ISD algorithm is given by

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

$$\text{Given } H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n},\ s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k} \text{ and } t \in \mathbb{N},$$
$$\text{find } e \in (\mathbb{Z}/p^s\mathbb{Z})^n \text{ s.t. } \mathrm{wt}_L(e) = t \text{ and } s = eH^T.$$

Information set decoding (ISD) algorithms to solve the LSDP

- Recent improvements: using partial Gaussian elimination
  - ::: Representation technique or Wagner's approach
  - ::: BJMM on 2 Levels is fastest in the Lee metric (non-amortized)
  - ::: Wagner's approach is fastest in the Lee metric (amortized)

The cost of an ISD algorithm is given by

nr. of iterations cost per iteration

Information Set Decoding Algorithms

Consider an instance of the Lee Syndrome Decoding Problem (LSDP):

$$\text{Given } H \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k)\times n};\ s \in (\mathbb{Z}/p^s\mathbb{Z})^{n-k} \text{ and } t \in \mathbb{N};$$
$$\text{find } e \in (\mathbb{Z}/p^s\mathbb{Z})^n \text{ s.t. } \mathrm{wt}_L(e) = t \text{ and } s = eH^T:$$

Information set decoding (ISD) algorithms to solve the LSDP

- Recent improvements: using partial Gaussian elimination
  - Representation technique or Wagner's approach
  - BJMM on 2 Levels is fastest in the Lee metric (non-amortized)
  - Wagner's approach is fastest in the Lee metric (amortized)

The cost of an ISD algorithm is given by

$$\underbrace{\text{nr. of iterations}}_{\frac{1}{\text{success probability per iter.}}} \quad \text{cost per iteration}$$

General Framework

We use the idea of partial Gaussian elimination to solve the problem:

1. Find $U \in \mathrm{GL}_{n-k}(\mathbb{Z}/p^s\mathbb{Z})$ such that

$$UH^{\top} = \begin{pmatrix} \mathrm{I}_{n-k} & 0 \\ A^{\top} & B^{\top} \end{pmatrix}$$

General Framework

We use the idea of partial Gaussian elimination to solve the problem:

1. Find $U \in \mathrm{GL}_{n-k}(\mathbb{Z}/p^s\mathbb{Z})$ such that

$$UH^{\top} = \begin{pmatrix} \mathrm{I}_{n-k} & 0 \\ A^{\top} & B^{\top} \end{pmatrix}$$

2. Transform the syndrome equation accordingly to

$$e_1 \quad e_2 \; UH^{\top} = s_1 \quad s_2 = sU$$

General Framework

We use the idea of partial Gaussian elimination to solve the problem:

1. Find $U \in \mathrm{GL}_{n-k}(\mathbb{Z}/p^s\mathbb{Z})$ such that

$$UH^{\top} = \begin{pmatrix} \mathrm{I}_{n-k} & 0 \\ A^{\top} & B^{\top} \end{pmatrix}$$

2. Transform the syndrome equation accordingly to

$$e_1 \quad e_2 \; UH^{\top} = s_1 \quad s_2 = sU$$

3. Assume, $\mathrm{wt}_L(e_1) = t - v$ and $\mathrm{wt}_L(e_2) = v$. Hence, we need to solve

$$e_1 + e_2 A^{\top} = s_1$$
$$e_2 B^{\top} = s_2$$

General Framework

We use the idea of partial Gaussian elimination to solve the problem:

1. Find $U \in \mathrm{GL}_{n-k}(\mathbb{Z}/p^s\mathbb{Z})$ such that

$$UH^\top = \begin{pmatrix} \mathrm{I}_{n-k} & 0 \\ A^\top & B^\top \end{pmatrix}$$

2. Transform the syndrome equation accordingly to

$$e_1 \quad e_2 \quad UH^\top = s_1 \quad s_2 = sU$$

3. Assume, $\mathrm{wt}_L(e_1) = t - v$ and $\mathrm{wt}_L(e_2) = v$. Hence, we need to solve

$$e_1 + e_2A^\top = s_1$$
$$e_2B^\top = s_2$$

4. Solve the smaller instance of the LSDP. Immediately check whether $e_1 = s_1 - e_2A^\top$ has Lee weight $t - v$.

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

Given $B \in (\mathbb{Z}/p^s\mathbb{Z})^{(k+\ell)}$, $s_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{\ell}$ and $v, t \in \mathbb{N}$

find $e_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{k+\ell}$ s.t. $\mathrm{wt}_L(e_2) = v$ and $s_2 = e_2 B^T$:

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

$$\text{Given } B \in (\mathbb{Z}/p^s\mathbb{Z})^{(k+\ell)}, s_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{\ell} \text{ and } v, t \in \mathbb{N}$$
$$\text{find } e_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{k+\ell} \text{ s.t. } \mathrm{wt}_L(e_2) = v \text{ and } s_2 = e_2 B^{\top}.$$

Main Idea and Difference

Use the marginal distribution, i.e.,

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

$$\text{Given } B \in (\mathbb{Z}/p^s\mathbb{Z})^{k\times n},\ s_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{n} \text{ and } v, t \in \mathbb{N}$$
$$\text{find } e_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{k+n} \text{ s.t. } \mathrm{wt}_L(e_2) = v \text{ and } s_2 = e_2 B^{\top}:$$

Main Idea and Difference

Use the marginal distribution, i.e.,

for $t=n < M=2$, with high probability 0 is the most likely Lee weight in e, followed by the Lee weight 1 until the least likely Lee weight M.

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

$$\text{Given } B \in (\mathbb{Z}/p^s\mathbb{Z})^{(k+\ell)}, s_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{\ell} \text{ and } v, t \in \mathbb{N}$$
$$\text{find } e_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{k+\ell} \text{ s.t. } \mathrm{wt}_L(e_2) = v \text{ and } s_2 = e_2 B^{\top}.$$

Main Idea and Difference

Use the marginal distribution, i.e.,

for $t=n < M=2$, with high probability 0 is the most likely Lee weight in e, followed by the Lee weight 1 until the least likely Lee weight M.

for $t=n > M=2$ the contrary is true

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

$$\text{Given } B \in (\mathbb{Z}/p^s\mathbb{Z})^{(k+\ell)\times n},\ s_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{\ell} \text{ and } v, t \in \mathbb{N}$$
$$\text{find } e_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{k+\ell} \text{ s.t. } \mathrm{wt}_L(e_2) = v \text{ and } s_2 = e_2 B^T.$$

Main Idea and Difference

Use the marginal distribution, i.e.,

for $t=n < M=2$, with high probability 0 is the most likely Lee weight in e, followed by the Lee weight 1 until the least likely Lee weight M.

for $t=n > M=2$ the contrary is true

With high probability the least probable entries of e lie **outside** the information set, hence are not in e_2.

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

$$\text{Given } B \in (\mathbb{Z}/p^s\mathbb{Z})^{(k+\ell)}, s_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{\ell} \text{ and } v, t \in \mathbb{N}$$
$$\text{find } e_2 \in (\mathbb{Z}/p^s\mathbb{Z})^{k+\ell} \text{ s.t. } \mathrm{wt}_L(e_2) = v \text{ and } s_2 = e_2 B^{\top}.$$

Main Idea and Difference

Use the marginal distribution, i.e.,

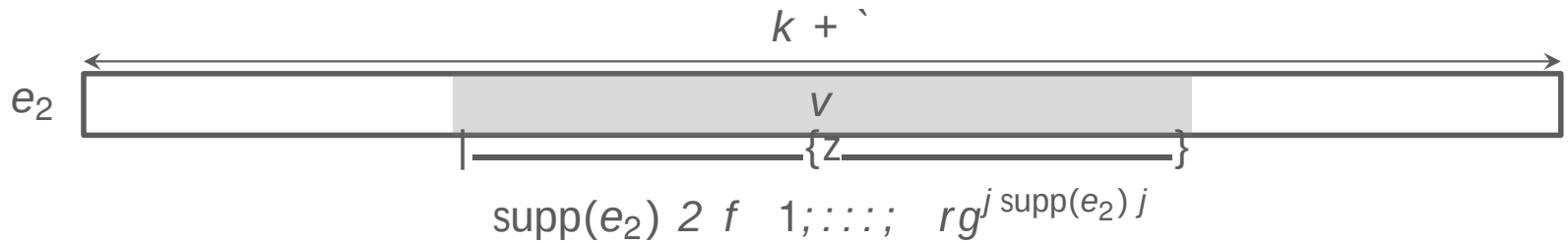
for $t=n < M=2$, with high probability 0 is the most likely Lee weight in e, followed by the Lee weight 1 until the least likely Lee weight M.

for $t=n > M=2$ the contrary is true

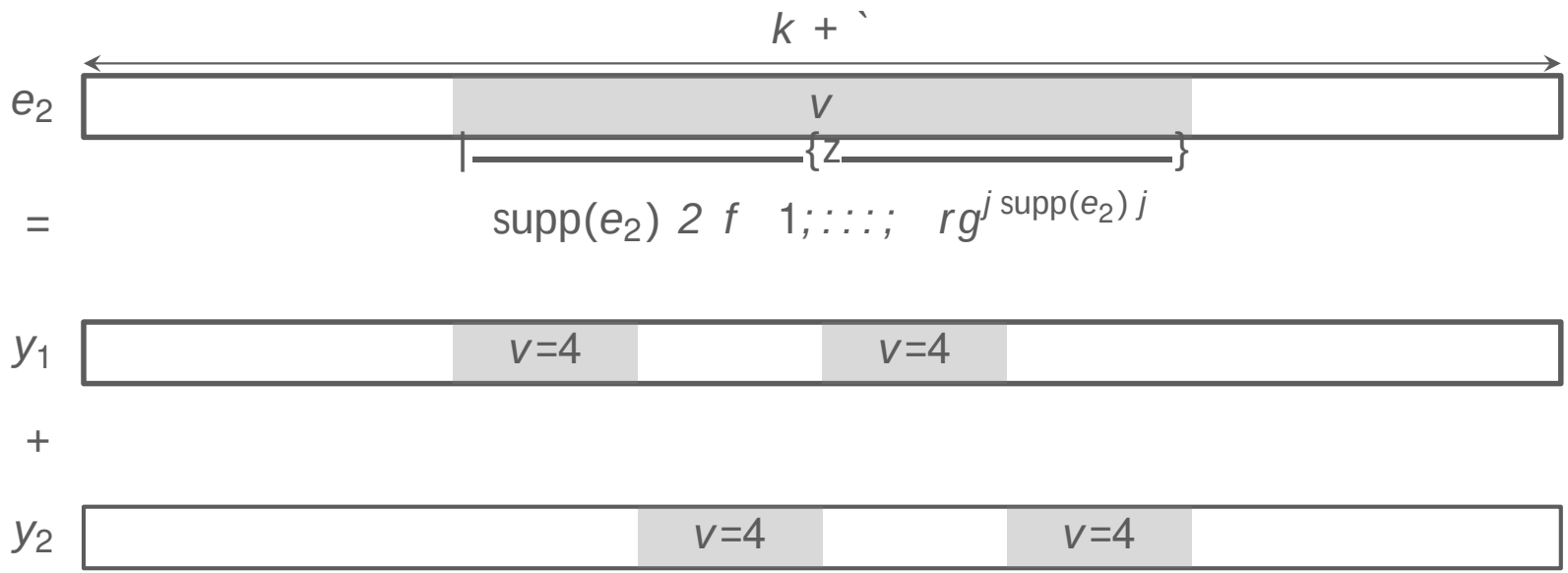
With high probability the least probable entries of e lie **outside** the information set, hence are not in e_2.

We will restrict e_2 to live either in $\{0, 1, \dots, r\}^{k+\ell}$ or in $\{r, \dots, M\}^{k+\ell}$, respectively.

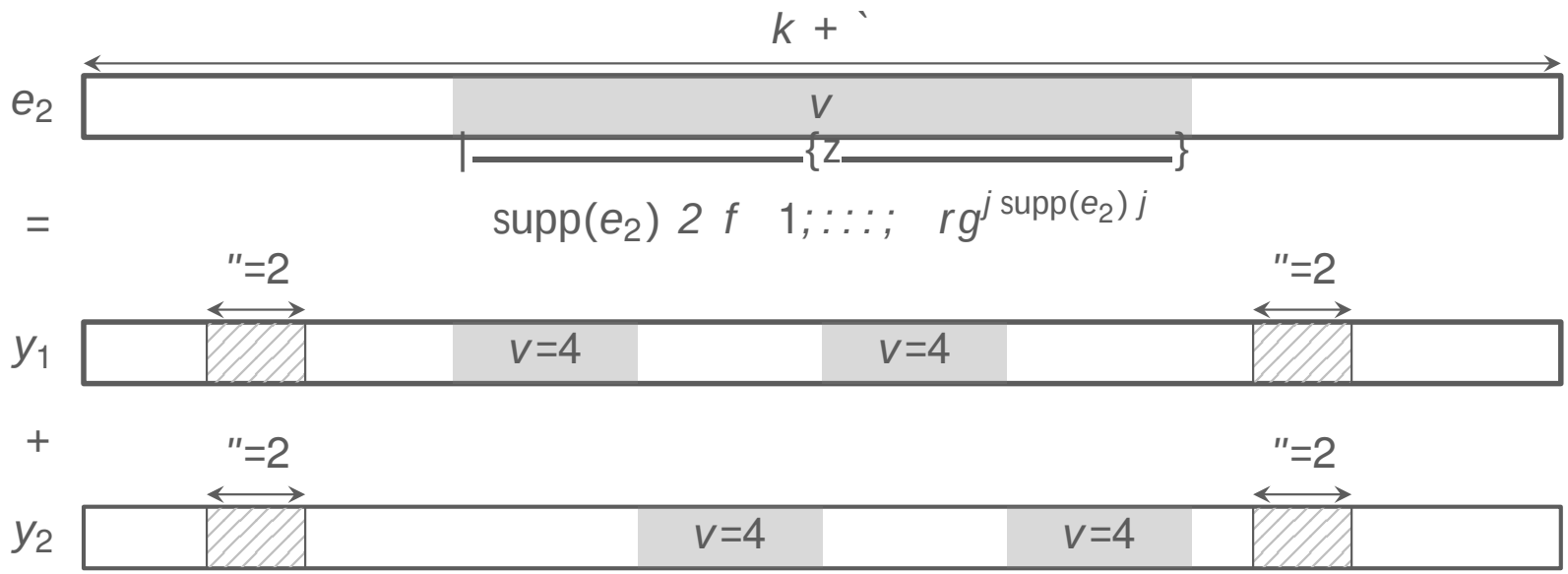
Up to Minimum Distance Decoding - The BJMM Approach



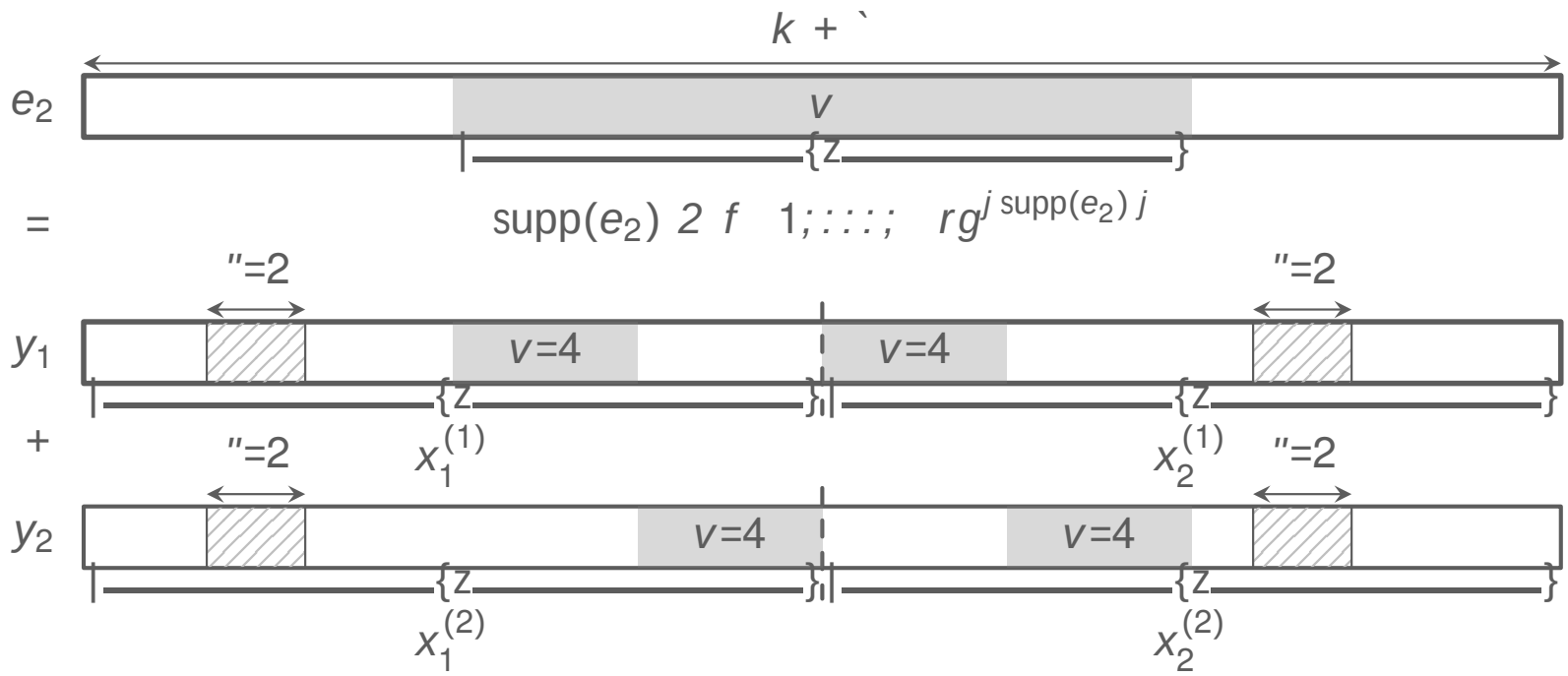
Up to Minimum Distance Decoding - The BJMM Approach



Up to Minimum Distance Decoding - The BJMM Approach



Up to Minimum Distance Decoding - The BJMM Approach



$$B_i = \{(x) \; j \; x_{E_i^c} \; 2 \; f0; : : : ; \; rg^{(k+`\ \ ")=2}; \mathrm{wt_L}(x_{E_i^c}) = v=4; x_{E_i} \; 2 \; \mathbb{Z}=p^s\mathbb{Z}^{\ \ "=2}; \; 2 \; S_{(k+`)=2}\}$$

Minimum Distance Decoding - The BJMM Approach

Recall, $s_2 = e_2 B^{>}$, where $e_2 = y_1 + y_2 = (x_1^{(1)}; x_2^{(1)}) + (x_1^{(2)}; x_2^{(2)})$.

Minimum Distance Decoding - The BJMM Approach

Recall, $s_2 = e_2 B^\top$, where $e_2 = y_1 + y_2 = (x_1^{(1)}; x_2^{(1)}) + (x_1^{(2)}; x_2^{(2)})$.

1. Splitting $B = (B_1\ B_2)$, for $i = 1; 2$ concatenate all $x_1^{(i)}; x_2^{(i)} \in B_i$ satisfying

$$x_1^{(1)} B_1^\top = u \quad x_2^{(1)} B_2^\top;$$
$$x_1^{(2)} B_1^\top = u\ s_2 \quad x_2^{(2)} B_2^\top:$$

They imply the syndrome equations for y_1 and y_2, respectively.

$$y_1 B^\top = 0 \text{ and } y_2 B^\top = s_2$$

Minimum Distance Decoding - The BJMM Approach

Recall, $s_2 = e_2 B^\top$, where $e_2 = y_1 + y_2 = (x_1^{(1)}; x_2^{(1)}) + (x_1^{(2)}; x_2^{(2)})$.

1. Splitting $B = (B_1\ B_2)$, for $i = 1; 2$ concatenate all $x_1^{(i)}; x_2^{(i)} \in B_i$ satisfying

$$x_1^{(1)} B_1^\top = u \quad x_2^{(1)} B_2^\top;$$
$$x_1^{(2)} B_1^\top = u\ s_2 \quad x_2^{(2)} B_2^\top:$$

   They imply the syndrome equations for y_1 and y_2, respectively.

$$y_1 B^\top = 0 \text{ and } y_2 B^\top = s_2$$

2. Store them in a list L_i.

Minimum Distance Decoding - The BJMM Approach

Recall, $s_2 = e_2 B^\top$, where $e_2 = y_1 + y_2 = (x_1^{(1)}; x_2^{(1)}) + (x_1^{(2)}; x_2^{(2)})$.

1. Splitting $B = (B_1\ B_2)$, for $i = 1; 2$ concatenate all $x_1^{(i)}; x_2^{(i)} \in B_i$ satisfying

$$x_1^{(1)} B_1^\top =_u x_2^{(1)} B_2^\top;$$
$$x_1^{(2)} B_1^\top =_u s_2 - x_2^{(2)} B_2^\top:$$

   They imply the syndrome equations for y_1 and y_2, respectively.

$$y_1 B^\top = 0 \text{ and } y_2 B^\top = s_2$$

2. Store them in a list L_i.
3. For each $y_1 \in L_1$ and $y_2 \in L_2$ check that

Minimum Distance Decoding - The BJMM Approach

Recall, $s_2 = e_2 B^{>}$, where $e_2 = y_1 + y_2 = (x_1^{(1)}; x_2^{(1)}) + (x_1^{(2)}; x_2^{(2)})$.

1. Splitting $B = (B_1\ B_2)$, for $i = 1; 2$ concatenate all $x_1^{(i)}; x_2^{(i)} \in B_i$ satisfying

$$x_1^{(1)} B_1^{>} =_u x_2^{(1)} B_2^{>};$$
$$x_1^{(2)} B_1^{>} =_u s_2 - x_2^{(2)} B_2^{>}:$$

   They imply the syndrome equations for y_1 and y_2, respectively.

$$y_1 B^{>} = 0 \text{ and } y_2 B^{>} = s_2$$

2. Store them in a list L_i.
3. For each $y_1 \in L_1$ and $y_2 \in L_2$ check that
   a) the smaller instance is solved

$$s_2 = (y_1 + y_2) B^{>} \text{ and } \mathrm{wt}_L(y_1 + y_2) = v;$$

Minimum Distance Decoding - The BJMM Approach

Recall, $s_2 = e_2 B^{>}$, where $e_2 = y_1 + y_2 = (x_1^{(1)}; x_2^{(1)}) + (x_1^{(2)}; x_2^{(2)})$.

1. Splitting $B = (B_1\ B_2)$, for $i = 1; 2$ concatenate all $x_1^{(i)}; x_2^{(i)} \in B_i$ satisfying

$$x_1^{(1)} B_1^{>} =_u x_2^{(1)} B_2^{>};$$
$$x_1^{(2)} B_1^{>} =_u s_2 - x_2^{(2)} B_2^{>}:$$

   They imply the syndrome equations for y_1 and y_2, respectively.

$$y_1 B^{>} = 0 \text{ and } y_2 B^{>} = s_2$$

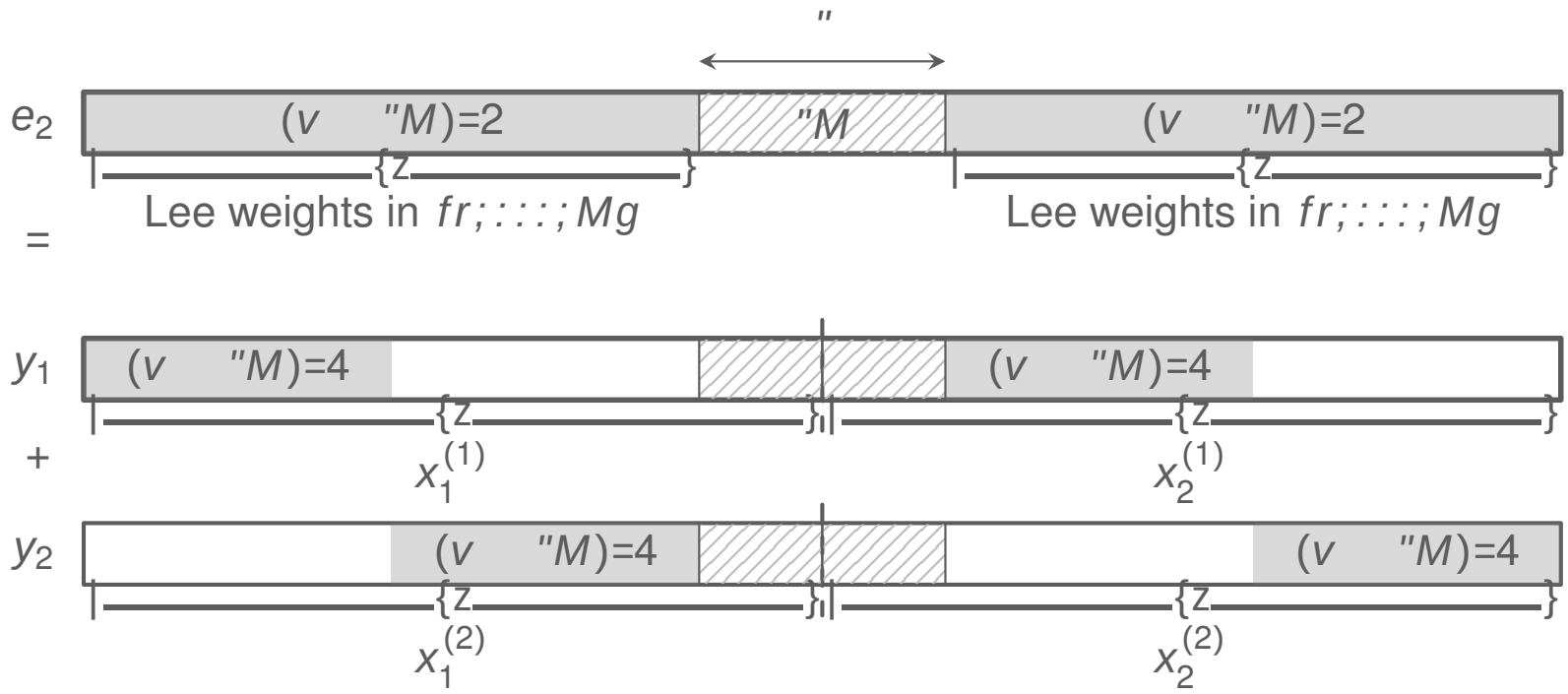
2. Store them in a list L_i.
3. For each $y_1 \in L_1$ and $y_2 \in L_2$ check that
   a) the smaller instance is solved

$$s_2 = (y_1 + y_2) B^{>} \text{ and } \mathrm{wt}_L(y_1 + y_2) = v;$$

   b) the original LSDP is fulfilled as well

$$\mathrm{wt}_L(s_1 - (y_1 + y_2) A^{>}) = t - v$$

Decoding Beyond the Minimum Distance



Outline

1. Preliminaries
2. Information Set Decoding using Restricted Spheres
   - Up to Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
3. Comparison

Up to Minimum Distance Decoding - Z=47Z

1

Algorithm	$e(R\ ; p^S)$	R
Lee-BJMM	0.1618	0.451
Restricted Lee-BJMM for $r = 5$	0.1539	0.408
Amortized Lee-BJMM	0.1205	0.396
Amortized Restricted Lee-BJMM	0.1189	0.406
Amortized Lee-Wagner	0.1441	0.445
Amortized Restricted Lee-Wagner	0.1441	0.445

[1] André Chailloux, Thomas Debris-Alazard, and Simona Etinski. "Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric". In: *International Conference on Post-Quantum Cryptography*. Springer. 2021, pp. 44–62.

Up to Minimum Distance Decoding - Z=47Z

[1]

Algorithm	$e(R\ ; p^S)$	R
Lee-BJMM	0.1618	0.451
Restricted Lee-BJMM for $r = 5$	0.1539	0.408
Amortized Lee-BJMM	0.1205	0.396
Amortized Restricted Lee-BJMM	0.1189	0.406
Amortized Lee-Wagner	0.1441	0.445
Amortized Restricted Lee-Wagner	0.1441	0.445

Thank you for your attention!

[1] André Chailloux, Thomas Debris-Alazard, and Simona Etinski. "Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric". In: *International Conference on Post-Quantum Cryptography*. Springer. 2021, pp. 44–62.