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)
  $\longrightarrow$ Alternative metrics are considered

Motivation

- Code-based cryptography for quantum secure cryptosystems
- The original McEliece cryptosystem suffers from large key sizes (even though unbroken)
  $\longrightarrow$ Alternative metrics are considered
- The security relies on the hardness of the syndrome decoding problem
  $\longrightarrow$ Generic decoding in the Lee metric has a large cost
  $\longrightarrow$ 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

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

Ring-Linear Codes

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

Definition

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

Parameters:

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

The Lee Metric

Definition

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

$$\mathrm{wt_L}(a) := \min(a, \left| p^s - a \right|),$$

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

The Lee Metric

Definition

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

$$\mathrm{wt_L}(a) := \min(a, \lvert p^s - a \rvert),$$

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

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 $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$

- $\mathrm{wt_L}(a) = \mathrm{wt_L}(p^s - a)$
- $\mathrm{wt_H}(a) \leq \mathrm{wt_L}(a) \leq \lfloor p^s/2 \rfloor =: M$
- $\mathrm{wt_H}(e) \leq \mathrm{wt_L}(e) \leq nM$

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

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

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

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

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

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

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

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

How does the distribution for each entry e_i look like?

DLR

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

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

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

How does the distribution for each entry e_i look like?

Let $T := \lim_{n \longrightarrow \infty} t(n)/n$ 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

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

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

[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

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

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

$$\mathbb{P}(\mathrm{wt_L}(E) = j) = \begin{cases} \mathbb{P}(E = j) & \text{if } (j = 0) \text{ or } (j = M \text{ and } p \text{ is even}), \\ 2\mathbb{P}(E = j) & \text{if } (1 \leq j \leq M - 1) \text{ or } (j = M \text{ and } p \text{ is odd}). \end{cases}$$

[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

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

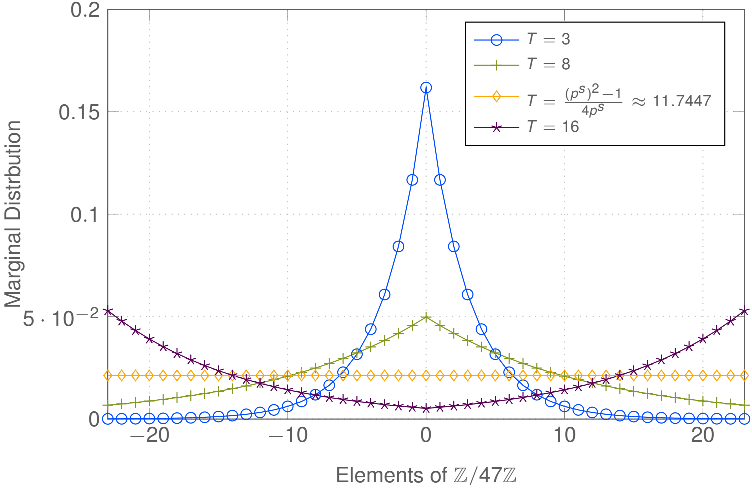
where β is the solution to $T = \sum_{i=0}^{M} \mathrm{wt_L}(i) p_i$.

$$\mathbb{P}(\mathrm{wt_L}(E) = j) = \begin{cases} \mathbb{P}(E = j) & \text{if } (j = 0) \text{ or } (j = M \text{ and } p \text{ is even}), \\ 2\mathbb{P}(E = j) & \text{if } (1 \leq j \leq M - 1) \text{ or } (j = M \text{ and } p \text{ is odd}). \end{cases}$$

Note: $T < \delta_{p^s} \iff \beta > 0$

DLR

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



Outline

Information Set Decoding Algorithms

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

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

Information Set Decoding Algorithms

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

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

- Information set decoding (ISD) algorithms to solve the LSDP

DLR

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
  $\longrightarrow$ 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.

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

$\longrightarrow$ 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 $\tilde{\mathcal{O}}(2^{0.054n})$". 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):

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

- Information set decoding (ISD) algorithms to solve the LSDP

$\longrightarrow$ 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):

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

- Information set decoding (ISD) algorithms to solve the LSDP

$\longrightarrow$ 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):

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

- Information set decoding (ISD) algorithms to solve the LSDP

  $\longrightarrow$ 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

$$\text{nr. of iterations} \times \text{cost per iteration}$$

Information Set Decoding Algorithms

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

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

- Information set decoding (ISD) algorithms to solve the LSDP

  $\longrightarrow$ 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

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

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

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

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

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

2. Transform the syndrome equation accordingly to

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} UH^\top = \begin{pmatrix} s_1 & s_2 \end{pmatrix} = sU$$

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

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

2. Transform the syndrome equation accordingly to

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} UH^\top = \begin{pmatrix} s_1 & s_2 \end{pmatrix} = sU$$

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

$$\begin{aligned} e_1 + e_2 A^\top &= s_1 \\ e_2 B^\top &= s_2 \end{aligned}$$

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
$$UH^\top = \begin{pmatrix} \mathbb{I}_{n-k-\ell} & 0 \\ A^\top & B^\top \end{pmatrix}$$
2. Transform the syndrome equation accordingly to
$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} UH^\top = \begin{pmatrix} s_1 & s_2 \end{pmatrix} = sU$$
3. Assume, $\mathrm{wt}_L(e_1) = t - v$ and $\mathrm{wt}_L(e_2) = v$. Hence, we need to solve
$$e_1 + e_2 A^\top = s_1$$
$$e_2 B^\top = s_2$$
4. Solve the smaller instance of the LSDP. Immediately check whether $e_1 = s_1 - e_2 A^\top$ has Lee weight $t - v$.

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

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

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

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

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

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

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.

New Framework: using Restricted Spheres

Focus on the small instance of the Lee syndrome decoding problem

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

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

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

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.

New Framework: using Restricted Spheres

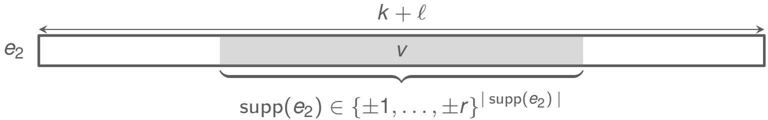
Focus on the small instance of the Lee syndrome decoding problem

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

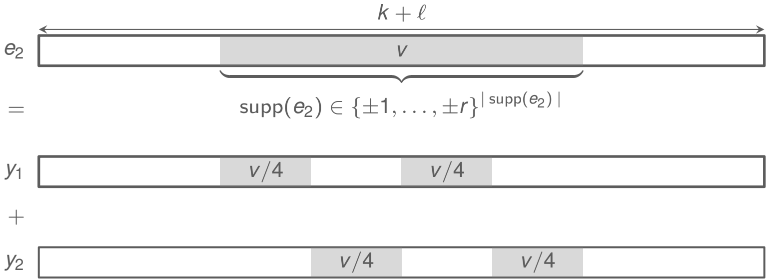
Main Idea and Difference

- 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 $\{0, \pm 1, \ldots, \pm r\}^{k+\ell}$ or in $\{\pm r, \ldots, \pm M\}^{k+\ell}$, respectively.

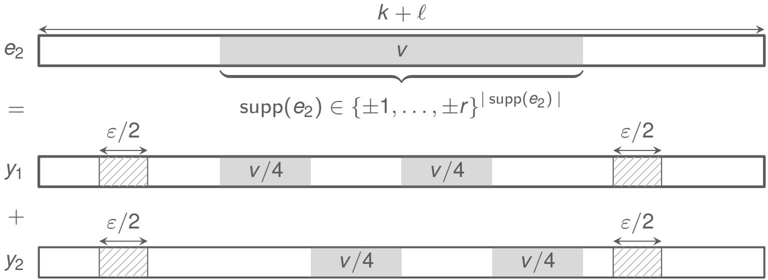
Up to Minimum Distance Decoding - The BJMM Approach



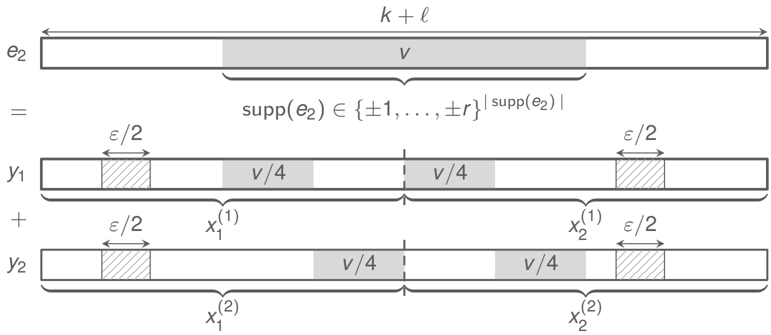
Up to Minimum Distance Decoding - The BJMM Approach



Up to Minimum Distance Decoding - The BJMM Approach



Up to Minimum Distance Decoding - The BJMM Approach



$$\mathcal{B}_i = \left\{ \nu(x) \mid x_{\mathcal{E}_i^c} \in \{0, \ldots, \pm r\}^{(k+\ell-\varepsilon)/2}, \mathrm{wt}_{\mathrm{L}}(x_{\mathcal{E}_i^c}) = v/4, x_{\mathcal{E}_i} \in \left(\mathbb{Z}/p^s\mathbb{Z}\right)^{\varepsilon/2}, \nu \in S_{(k+\ell)/2} \right\}$$

Minimum Distance Decoding - The BJMM Approach

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

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 $x_1^{(i)}, x_2^{(i)} \in \mathcal{B}_i$ 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.

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

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 $x_1^{(i)}, x_2^{(i)} \in \mathcal{B}_i$ 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 $\mathcal{L}_i$.

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 $x_1^{(i)}, x_2^{(i)} \in \mathcal{B}_i$ 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 $\mathcal{L}_i$.
3. For each $y_1 \in \mathcal{L}_1$ and $y_2 \in \mathcal{L}_2$ check that

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 $x_1^{(i)}, x_2^{(i)} \in \mathcal{B}_i$ 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 $\mathcal{L}_i$.
3. For each $y_1 \in \mathcal{L}_1$ and $y_2 \in \mathcal{L}_2$ check that
   a) the smaller instance is solved

$$s_2 = (y_1 + y_2) B^\top \;\text{ and }\; \mathrm{wt}_\mathrm{L}(y_1 + y_2) = v,$$

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 $x_1^{(i)}, x_2^{(i)} \in \mathcal{B}_i$ satisfying

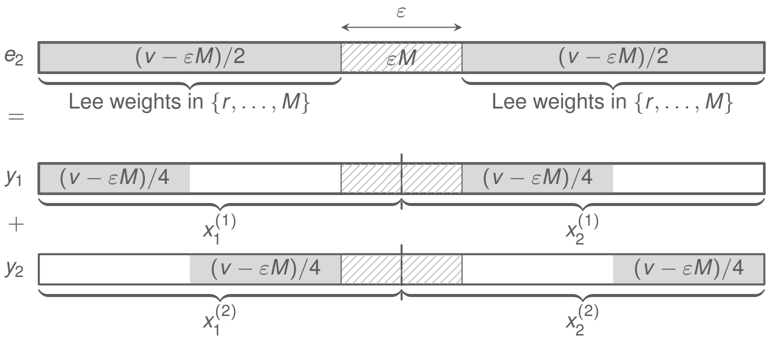
$$x_1^{(1)} B_1^\top =_u -x_2^{(1)} B_2^\top,$$
$$x_1^{(2)} B_1^\top =_u s_2 - x_2^{(2)} B_2^\top.$$

   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 $\mathcal{L}_i$.
3. For each $y_1 \in \mathcal{L}_1$ and $y_2 \in \mathcal{L}_2$ check that
   a) the smaller instance is solved
   $$s_2 = (y_1 + y_2) B^\top \ \text{ and } \ \mathrm{wt}_L(y_1 + y_2) = v,$$
   b) the original LSDP is fulfilled as well
   $$\mathrm{wt}_L(s_1 - (y_1 + y_2) A^\top) = t - v$$

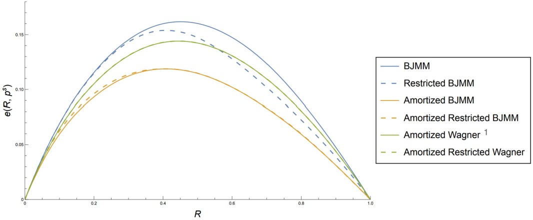
Decoding Beyond the Minimum Distance



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 - $\mathbb{Z}/47\mathbb{Z}$

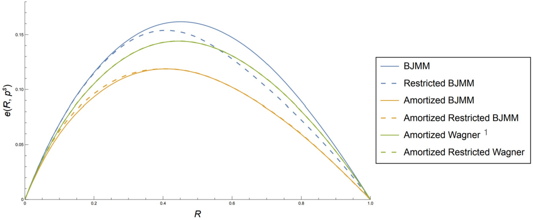


[1]

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 - $\mathbb{Z}/47\mathbb{Z}$



[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.