June 27, 2022
Institutskolloquium, KN-IColl

Information Set Decoding in the Lee Metric

Jessica Bariffi

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)
  $\longrightarrow$ Idea: What if we used alternative metrics?

Motivation

- Code-based cryptography for quantum-secure cryptosystems
- The original McEliece cryptosystem suffers from large key sizes (even though unbroken)
  $\longrightarrow$ Idea: What if we used alternative metrics?
- 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 different metrics (e.g. Hamming metric, Lee metric)

Outline

1. The Lee Metric
2. The Syndrome Decoding Problem
3. Information Set Decoding
4. Information Set Decoding using Restricted Spheres
   - Bounded Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
5. Comparison

Outline

1. The Lee Metric
2. The Syndrome Decoding Problem
3. Information Set Decoding
4. Information Set Decoding using Restricted Spheres
   - Bounded Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
5. Comparison

Ring-Linear Codes

Let p a prime number and s and n two positive integers. We focus on the ring of integers $\mathbb{Z}/p^s\mathbb{Z} = \{0, 1, \ldots, p^s - 1\}$.

Definition

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

Ring-Linear Codes

Let p a prime number and s and n two positive integers. We focus on the ring of integers $\mathbb{Z}/p^s\mathbb{Z} = \{0, 1, \ldots, p^s - 1\}$.

Definition

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

Parameters:

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

Example over $\mathbb{Z}/2\mathbb{Z}$

$\mathcal{C} = \{(0, 0, 0, 0), (0, 0, 1, 1), (1, 1, 0, 0), (1, 1, 1, 1)\}$

- length $n = 4$
- dimension $k = 2$
- rate $R = 1/2$

Ring-Linear Codes

Let p a prime number and s and n two positive integers. We focus on the ring of integers $\mathbb{Z}/p^s\mathbb{Z} = \{0, 1, \ldots, p^s - 1\}$.

Definition

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

Parameters:

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

Example over $\mathbb{Z}/2\mathbb{Z}$

$\mathcal{C} = \{(0,0,0,0), (0,0,1,1), (1,1,0,0), (1,1,1,1)\}$

- length $n = 4$
- dimension $k = 2$
- rate $R = 1/2$

The *Hamming weight* of a codeword $c \in \mathcal{C}$, $\mathrm{wt}_{\mathrm{H}}(c)$, is the number of nonzero elements in 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

$$\mathrm{wt_L}(a) := \min(a, \left| p^s - a \right|) \quad \text{and} \quad \mathrm{wt_L}(e) := \sum_{i=1}^{n} \mathrm{wt_L}(e_i).$$

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

$$\mathrm{wt_L}(a) := \min(a, \left| p^s - a \right|) \quad \text{and} \quad \mathrm{wt_L}(e) := \sum_{i=1}^{n} \mathrm{wt_L}(e_i).$$

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

$$\mathrm{wt_L}(a) := \min(a, |\, p^s - a\,|) \quad \text{and} \quad \mathrm{wt_L}(e) := \sum_{i=1}^{n} \mathrm{wt_L}(e_i).$$

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

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

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

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

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

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

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

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

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

How does the distribution for each entry e_i look like?

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

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

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

How does the distribution for each entry e_i look like?

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

[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

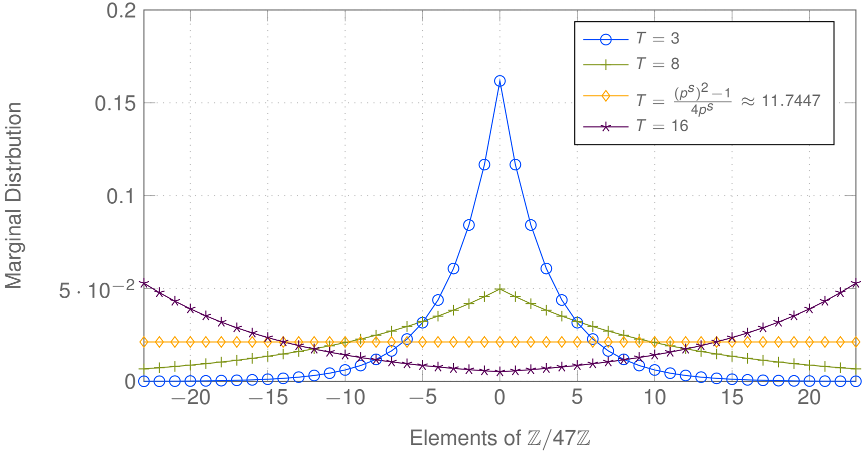
$$p_i := \mathbb{P}(E = i) = \frac{1}{\sum_{j=0}^{p^s-1} \exp(-\beta \, \mathrm{wt_L}(j))} \exp(-\beta i)$$

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

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

[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 - Example over $\mathbb{Z}/47\mathbb{Z}$



Outline

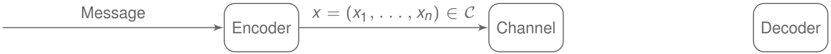
1. The Lee Metric
2. The Syndrome Decoding Problem
3. Information Set Decoding
4. Information Set Decoding using Restricted Spheres
   - Bounded Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
5. Comparison

Channel Coding

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

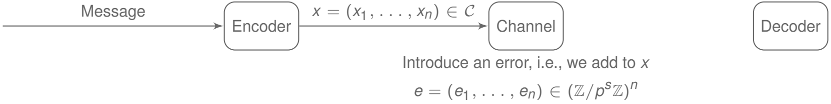
Channel Coding

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



Channel Coding

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



Channel Coding

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

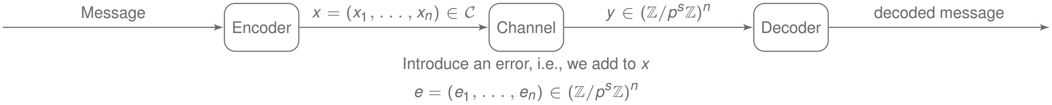
$$\xrightarrow{\text{Message}} \boxed{\text{Encoder}} \xrightarrow{x = (x_1, \dots, x_n) \in \mathcal{C}} \boxed{\text{Channel}} \xrightarrow{y \in (\mathbb{Z}/p^s\mathbb{Z})^n} \boxed{\text{Decoder}}$$

Introduce an error, i.e., we add to x

$e = (e_1, \dots, e_n) \in (\mathbb{Z}/p^s\mathbb{Z})^n$

Channel Coding

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



Channel Coding

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

$$\xrightarrow{\text{Message}} \boxed{\text{Encoder}} \xrightarrow{x = (x_1, \ldots, x_n) \in \mathcal{C}} \boxed{\text{Channel}} \xrightarrow{y \in (\mathbb{Z}/p^s\mathbb{Z})^n} \boxed{\text{Decoder}} \xrightarrow{\text{decoded message}}$$

Introduce an error, i.e., we add to x

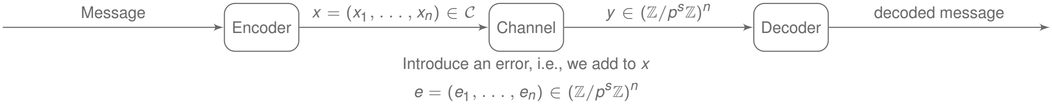
$e = (e_1, \ldots, e_n) \in (\mathbb{Z}/p^s\mathbb{Z})^n$

Generic Decoding

Given $y = x + e$, recover either the original message x or the error term e.

Channel Coding

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



Generic Decoding

Given $y = x + e$, recover either the original message x or the error term e.

- NP-hard problem
- Has a unique solution for errors of relatively small “weight”

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{ x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0 \right\}.$$

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{ x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0 \right\}.$$

Transforming the generic decoding problem

$$y = x + e$$

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{ x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0 \right\}.$$

Transforming the generic decoding problem

$$\begin{aligned} y &= x + e \\ yH^\top &= (x+e)H^\top \end{aligned}$$

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0\right\}.$$

Transforming the generic decoding problem

$$\begin{aligned} y &= x + e \\ yH^\top &= xH^\top + eH^\top \end{aligned}$$

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{ x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0 \right\}.$$

Transforming the generic decoding problem

$$\begin{aligned} y &= x + e \\ yH^\top &= xH^\top + eH^\top \\ s &= eH^\top \end{aligned}$$

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{ x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0 \right\}.$$

Transforming the generic decoding problem

$$\begin{aligned} y &= x + e \\ yH^\top &= xH^\top + eH^\top \\ s &= eH^\top \end{aligned}$$

Syndrome decoding

Given a parity-check matrix H and a syndrome $s = yH^\top$, recover e from $s = eH^\top$.

Representation of Codes

An linear code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of dimension k can be represented by the kernel of a *parity-check matrix* H. That is an $(n-k) \times n$ matrix H over $\mathbb{Z}/p^s\mathbb{Z}$ satisfying

$$\mathcal{C} = \ker(H) = \left\{ x \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid xH^\top = 0 \right\}.$$

Transforming the generic decoding problem

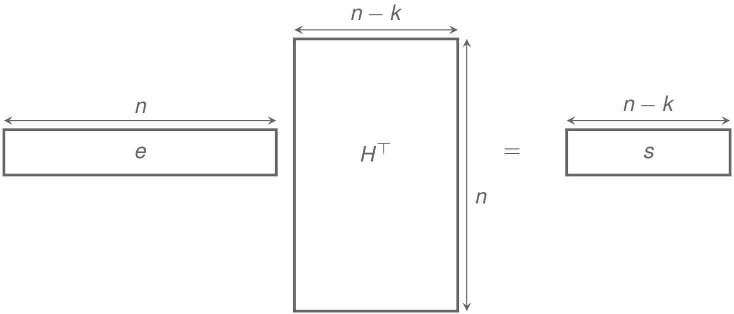
$$\begin{aligned} y &= x + e \\ yH^\top &= xH^\top + eH^\top \\ s &= eH^\top \end{aligned}$$

Syndrome decoding

Given a parity-check matrix H and a syndrome $s = yH^\top$, recover e from $s = eH^\top$ with $\mathrm{wt}_{\mathrm{H}}(e) = t$.

Syndrome Decoding Problem

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. $\mathrm{wt}(e) = t$ and $s = eH^\top$.



Transforming the Syndrome Decoding Problem

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. $\mathrm{wt}(e) = t$ and $s = eH^\top$.

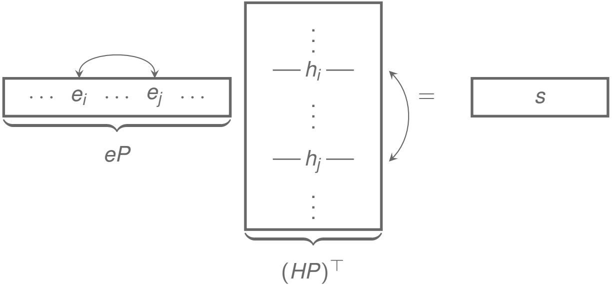
$$\boxed{\quad e \quad} \; \boxed{H^\top} \; = \; \boxed{\quad s \quad}$$

Transforming the Syndrome Decoding Problem

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. $\mathrm{wt}(e) = t$ and $s = eH^\top$.

1. Permute e and H with a permutation matrix P,

$$eP \cdot (HP)^\top = s$$



Transforming the Syndrome Decoding Problem

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. $\mathrm{wt}(e) = t$ and $s = eH^\top$.

1. Permute e and H with a permutation matrix P,

$$eP \cdot (HP)^\top = s$$

2. Diagonalize H by an invertible matrix U,

$$eP \cdot (UHP)^\top = sU^\top =: s'$$

$$\boxed{\quad eP \quad} \begin{bmatrix} \mathbb{I}_{n-k} \\ \hline (H')^\top \end{bmatrix} = \boxed{\quad sU^\top \quad}$$

Transforming the Syndrome Decoding Problem

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. $\mathrm{wt}(e) = t$ and $s = eH^\top$.

1. Permute e and H with a permutation matrix P,

$$eP \cdot (HP)^\top = s$$

2. Diagonalize H by an invertible matrix U,

$$e_1 + e_2(H')^\top = s'$$

$$\begin{pmatrix} \underbrace{e_1}_{\mathrm{wt}(e_1) = t - v} & \underbrace{e_2}_{\mathrm{wt}(e_2) = v} \end{pmatrix} \begin{pmatrix} \mathbb{I}_{n-k} \\ \hline (H')^\top \end{pmatrix} = \begin{pmatrix} s' \end{pmatrix}$$

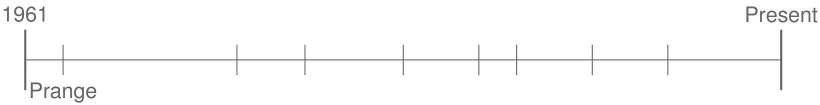
Outline

1. The Lee Metric
2. The Syndrome Decoding Problem
3. Information Set Decoding
4. Information Set Decoding using Restricted Spheres
   - Bounded Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
5. Comparison

Information Set Decoding - Overview

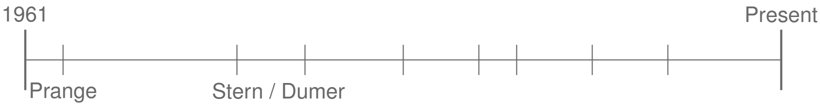
- Information Set Decoding (ISD) algorithms are the fastest attacks to the syndrome decoding problem.

Information Set Decoding - Overview



- Information Set Decoding (ISD) algorithms are the fastest attacks to the syndrome decoding problem.
- Prange: First ISD algorithm (based only on the linear transformations)

Information Set Decoding - Overview

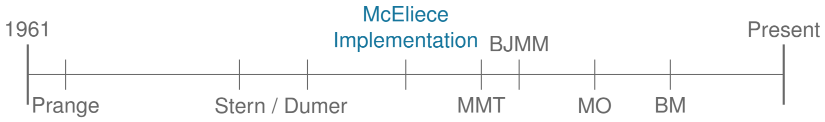


- Information Set Decoding (ISD) algorithms are the fastest attacks to the syndrome decoding problem.
- Prange: First ISD algorithm (based only on the linear transformations)
- Stern and Dumer: Extension of Prange's Algorithm using the Birthday Problem

Information Set Decoding - Overview

- Information Set Decoding (ISD) algorithms are the fastest attacks to the syndrome decoding problem.
- Prange: First ISD algorithm (based only on the linear transformations)
- Stern and Dumer: Extension of Prange's Algorithm using the Birthday Problem

Information Set Decoding - Overview



- Information Set Decoding (ISD) algorithms are the fastest attacks to the syndrome decoding problem.
- Prange: First ISD algorithm (based only on the linear transformations)
- Stern and Dumer: Extension of Prange's Algorithm using the Birthday Problem
- Series of improvements using "representation technique" or Wagner's algorithm

Information Set Decoding - Overview

- Information Set Decoding (ISD) algorithms are the fastest attacks to the syndrome decoding problem.
- Prange: First ISD algorithm (based only on the linear transformations)
- Stern and Dumer: Extension of Prange's Algorithm using the Birthday Problem
- Series of improvements using "representation technique" or Wagner's algorithm

Prange

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. $\text{wt}(e) = t$ and $s = eH^\top$.

- Assume that $\text{wt}(e_2) = v = 0$.
  That is:

$$e_2 = (0, \ldots, 0)$$

- Then we get the equation

$$e_1 = s'$$

$$\begin{pmatrix} \underbrace{e_1}_{\text{wt}(e_1) = t} & \underbrace{0 \ldots 0}_{\text{wt}(e_2) = 0} \end{pmatrix} \begin{pmatrix} \mathbb{I}_{n-k} \\ \hline (H')^\top \end{pmatrix} = \begin{pmatrix} s' \end{pmatrix}$$

Stern / Dumer - Partial Gaussian Elimination

Goal: Given $\mathrm{wt}(e_1) = t - v$ and $\mathrm{wt}(e_2) = v$, solve $e_1 + e_2(H')^\top = s'$.

Stern / Dumer - Partial Gaussian Elimination

Goal: Given $\mathrm{wt}(e_1) = t - v$ and $\mathrm{wt}(e_2) = v$, solve $e_1 + e_2(H')^\top = s'$.

1. Bring H into partial systematic form

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} \begin{pmatrix} \mathbb{I}_{n-k-\ell} & 0 \\ A^\top & B^\top \end{pmatrix} = \begin{pmatrix} s_1 & s_2 \end{pmatrix}$$

Stern / Dumer - Partial Gaussian Elimination

Goal: Given $\mathrm{wt}(e_1) = t - v$ and $\mathrm{wt}(e_2) = v$, solve $e_1 + e_2(H')^\top = s'$.

1. Bring H into partial systematic form
2. Solve two equations

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

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} \begin{pmatrix} \mathbb{I}_{n-k-\ell} & 0 \\ A^\top & B^\top \end{pmatrix} = \begin{pmatrix} s_1 & s_2 \end{pmatrix}$$

Stern / Dumer - Partial Gaussian Elimination

Goal: Given $\mathrm{wt}(e_1) = t - v$ and $\mathrm{wt}(e_2) = v$, solve $e_1 + e_2(H')^\top = s'$.

1. Bring H into partial systematic form
2. Solve two equations

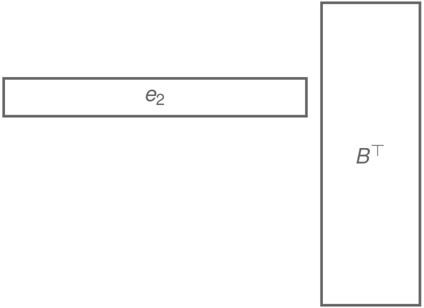
$$\begin{aligned} e_1 + e_2 A^\top &= s_1 \\ e_2 B^\top &= s_2 \end{aligned}$$

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} \begin{pmatrix} \mathbb{I}_{n-k-\ell} & 0 \\ A^\top & B^\top \end{pmatrix} = \begin{pmatrix} s_1 & s_2 \end{pmatrix}$$

Note: Finding e_2 directly yields e_1.

Stern / Dumer - Finding e_2 by Birthday Decoding

Focus on $e_2 B^\top = s_2$, with $\mathtt{wt}(e_2) = v$



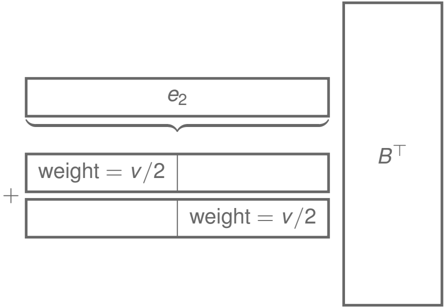
Stern / Dumer - Finding e_2 by Birthday Decoding

Focus on $e_2 B^\top = s_2$, with $\mathrm{wt}(e_2) = v$

- Represent e_2 as

$$e_2 = y_1 + y_2,$$

where $\mathrm{wt}(y_1) = \mathrm{wt}(y_2) = v/2$.



Stern / Dumer - Finding e_2 by Birthday Decoding

Focus on $e_2 B^\top = s_2$, with $\mathrm{wt}(e_2) = v$

- Represent e_2 as

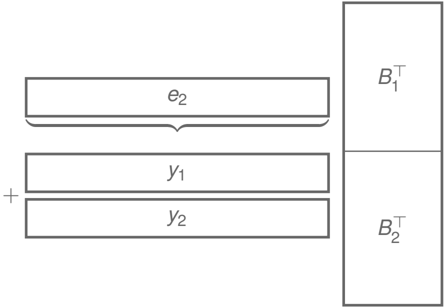
$$e_2 = y_1 + y_2,$$

where $\mathrm{wt}(y_1) = \mathrm{wt}(y_2) = v/2$.

- Enumerate the following sets

$$\mathcal{L}_1 := \left\{ y_1 B_1^\top \mid \mathrm{wt}(y_1) = v/2 \right\}$$

$$\mathcal{L}_2 := \left\{ y_2 B_2^\top \mid \mathrm{wt}(y_2) = v/2 \right\}$$



Becker-Joux-May-Meurer (BJMM) Algorithm

Core idea is the same as in Stern/Dumer, including several levels.

Becker-Joux-May-Meurer (BJMM) Algorithm

Core idea is the same as in Stern/Dumer, including several levels.

Example - 2 Levels

Write $e_2 = x_1 + x_2 + x_3 + x_4$.

1. successively merge $y_1 = x_1 + x_2$ and $y_2 = x_3 + x_4$ on some positions
2. Finally merge $y_1 + y_2$

Becker-Joux-May-Meurer (BJMM) Algorithm

Core idea is the same as in Stern/Dumer, including several levels.

Example - 2 Levels

Write $e_2 = x_1 + x_2 + x_3 + x_4$.

1. successively merge $y_1 = x_1 + x_2$ and $y_2 = x_3 + x_4$ on some positions
2. Finally merge $y_1 + y_2$

Another difference: Allows some freedom in the representation of the vectors y_i, i.e., use the lists

$$\mathcal{L}_1 := \left\{ y_1 B_1^\top \mid \mathrm{wt}(y_1) = v/2 + \varepsilon \right\}$$
$$\mathcal{L}_2 := \left\{ y_2 B_2^\top \mid \mathrm{wt}(y_2) = v/2 + \varepsilon \right\},$$

where two vectors $y_1 \in \mathcal{L}_1$ and $y_2 \in \mathcal{L}_2$ share ε nonzero positions. The expected weight of $y_1 + y_2$ is still v.

ISD in the Lee Metric

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

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

ISD in the Lee Metric

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

ISD in the Lee Metric

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[2]

[2] 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.

ISD in the Lee Metric

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[2] or Wagner's approach[3]

[2] 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.

[3] 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.

ISD in the Lee Metric

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)[2]

... Wagner's approach is fastest in the Lee metric (amortized)[3]

---

[2] 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.

[3] 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.

ISD in the Lee Metric

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

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

Outline

1. The Lee Metric
2. The Syndrome Decoding Problem
3. Information Set Decoding
4. Information Set Decoding using Restricted Spheres
   - Bounded Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
5. Comparison

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

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

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

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

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

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

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
- 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

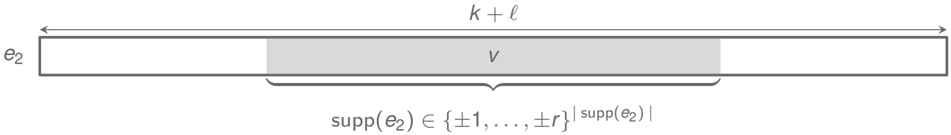
Focus on the small instance of the Lee syndrome decoding problem

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

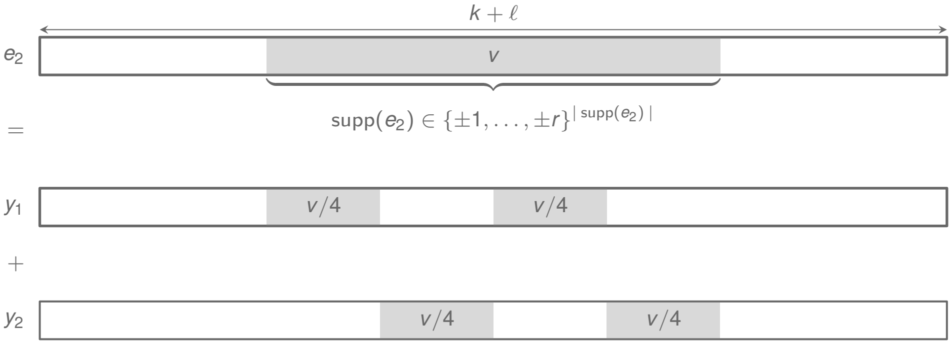
Main Idea and Difference

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

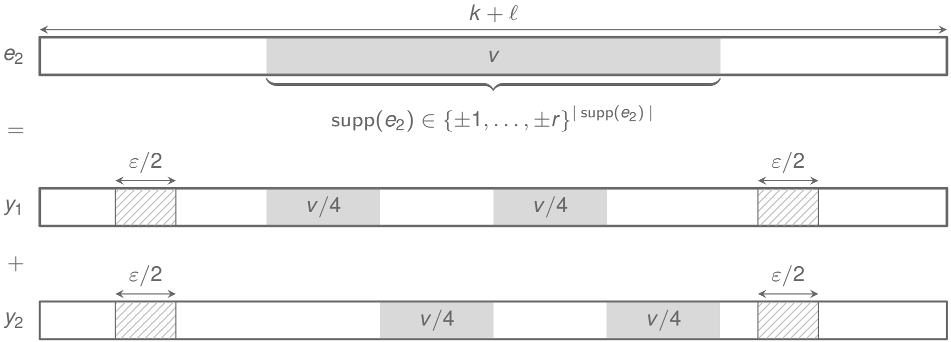
Up to Minimum Distance Decoding - The BJMM Approach



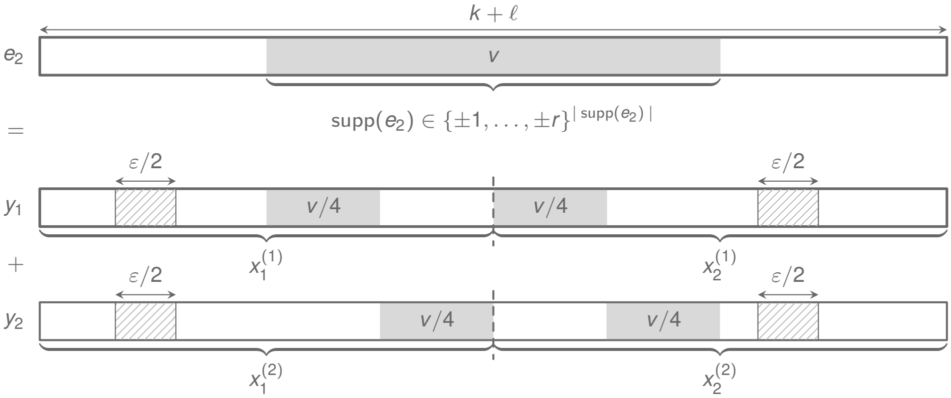
Up to Minimum Distance Decoding - The BJMM Approach



Up to Minimum Distance Decoding - The BJMM Approach



Up to Minimum Distance Decoding - The BJMM Approach



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

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
$$s_2 = (y_1 + y_2) B^\top \ \text{ and } \ \mathrm{wt_L}(y_1 + y_2) = v,$$

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.

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

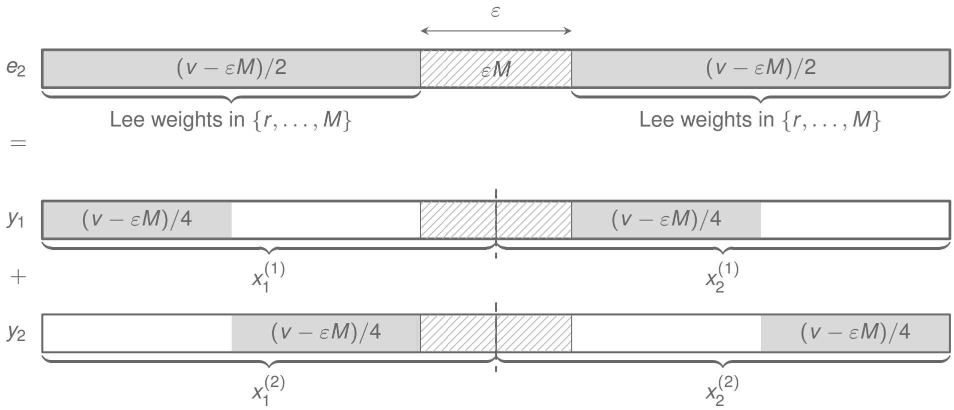
2. Store them in a list $\mathcal{L}_i$.
3. For each $y_1 \in \mathcal{L}_1$ and $y_2 \in \mathcal{L}_2$ check that
   a) the smaller instance is solved

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

   b) the original LSDP is fulfilled as well

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

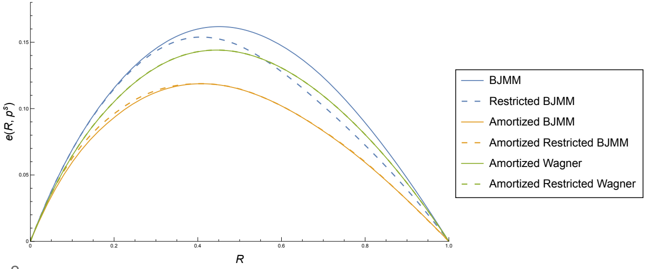
Decoding Beyond the Minimum Distance



Outline

1. The Lee Metric
2. The Syndrome Decoding Problem
3. Information Set Decoding
4. Information Set Decoding using Restricted Spheres
   - Bounded Minimum Distance Decoding
   - Decoding Beyond the Minimum Distance
5. Comparison

Up to Minimum Distance Decoding - $\mathbb{Z}/47\mathbb{Z}$

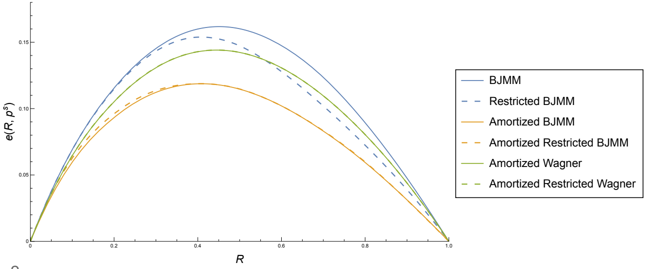


2

Algorithm	$e(R^*, p^s)$	R^*
BJMM	0.1618	0.451
Restricted BJMM for $r = 5$	0.1539	0.408
Amortized BJMM	0.1205	0.396
Amortized Restricted BJMM	0.1189	0.406
Amortized Wagner	0.1441	0.445
Amortized Restricted Wagner	0.1441	0.445

[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.

Up to Minimum Distance Decoding - $\mathbb{Z}/47\mathbb{Z}$



2

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

Thank you for your attention

[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.