Lee Metric Decoding and ℓ_1 Norm Lattices

Marc Newman (joint work with Anna-Lena Horlemann, Karan Khathuria, and Carlos Vela Cabello)

2024.06.07

University of St. Gallen—Institute of Computer Science

Context

- Post-quantum cryptography: codes, lattices, isogenies, multivariate polynomials.
- Within code-based crypto: Hamming, rank, and Lee metrics.

Hamming Metric	Lee Metric	(ℓ_2) Lattices
"ℓ_0-norm"	ℓ_1-norm	ℓ_2-norm
Information Set Decoding	$\leftarrow$ Both $\rightarrow$	Lattice Reduction Methods

Lee Metric

Lee Weight

For $q, n \in \mathbb{N}$ and $\mathbf{x} \in \mathbb{Z}_q^n$, define the Lee weight to be

$$\mathsf{wt}_L(\mathbf{x}) := \sum_{i=1}^{n} \min\{x_i, q - x_i\}.$$

Lee Distance

For $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$, define the Lee distance to be

$$\mathsf{dist}_L(\mathbf{x}, \mathbf{y}) := \mathsf{wt}_L(\mathbf{x} - \mathbf{y}).$$

Lee Metric Codes

Minimum Lee Distance

Given a linear code $\mathcal{C} \subseteq \mathbb{Z}_q^n$, the minimum Lee distance of $\mathcal{C}$ is

$$\begin{aligned} \mathsf{dist}_L(\mathcal{C}) &:= \mathsf{min}\{\mathsf{dist}_L(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\} \\ &= \mathsf{min}\{\mathsf{wt}_L(\mathbf{x}) | \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq \mathbf{0}\}. \end{aligned}$$

Lee Decoding Problem

Given a linear code $\mathcal{C} \subseteq \mathbb{Z}_q^n$, some $t \in \mathbb{N}$, and a vector $\mathbf{r} \in \mathbb{Z}_q^n$, find $\mathbf{c} \in \mathcal{C}$ such that $\mathsf{wt}_L(\mathbf{r} - \mathbf{c}) \leq t$.

Lattices

Lattice

Given k linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{R}^n$, let $\mathbf{B} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_k \end{bmatrix}$. The lattice generated by the lattice basis $\mathbf{B}$ is given by

$$\mathcal{L}(\mathbf{B}) := \left\{ \sum_{i=1}^{k} x_i \mathbf{b}_i \;\middle|\; x_i \in \mathbb{Z} \right\} = \mathbf{B} \cdot \mathbb{Z}^k.$$

Distance from a Lattice

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice and $p \geq 1$ or $p = \infty$. For $\mathbf{v} \in \mathbb{R}^n$, define

$$\mathsf{dist}_p(\mathbf{v}, \mathcal{L}) := \min_{\mathbf{x} \in \mathcal{L}} ||\mathbf{v} - \mathbf{x}||_p.$$

First Successive Minima and α-BDD

First Successive Minimum

Let $p \geq 1$ or $p = \infty$. Given a lattice $\mathcal{L}$, let $\lambda_1^{(p)}(\mathcal{L})$ be the length of the shortest nonzero vector in $\mathcal{L}$ with respect to the ℓ_p norm, i.e.,

$$\lambda_1^{(p)}(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}} ||\mathbf{v}||_p.$$

α-Bounded Distance Decoding (α-BDD)

Given a lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and a vector $\mathbf{r} \in \mathbb{R}^n$ such that $\mathsf{dist}_p(\mathbf{r}, \mathcal{L}) < \alpha \lambda_1^{(p)}(\mathcal{L})$, find $\mathbf{v} \in \mathcal{L}$ such that $||\mathbf{r} - \mathbf{v}||_p$ is minimal.

Lee Metric Codes as Lattices

Construction A

Let $\mathcal{C}$ be a linear code with generator matrix $\mathbf{G} \in \mathbb{Z}_q^{k \times n}$.
Define

$$\begin{aligned}\mathcal{L}_A(\mathcal{C}) :=& \{\mathbf{v} \in \mathbb{Z}^n | \mathbf{v} = \mathbf{c} \pmod{q} \text{ for some } \mathbf{c} \in \mathcal{C}\} \\ =& \mathbf{G}^\top \cdot \mathbb{Z}^k + q\mathbb{Z}^n.\end{aligned}$$

- Independent of choice of generator matrix.
- Lattice has dimension n (i.e., is full rank).
- A lattice basis can be extracted from the columns of

$$\begin{bmatrix}\mathbf{G}^\top & q \cdot \mathbf{I}_n\end{bmatrix}.$$

Examples of Lee Metric Codes as Lattices

Basis of $\mathcal{L}_A$ for q prime

If q is prime, $\mathbf{G}$ can be written as $\begin{bmatrix} \mathbf{I}_k & \mathbf{G}' \end{bmatrix}$ and $\mathcal{L}_A(\mathcal{C})$ can be given by the basis

$$\begin{bmatrix} \mathbf{I}_k & \mathbf{0} \\ \mathbf{G}' & q\mathbf{I}_{n-k} \end{bmatrix}.$$

Examples of Lee Metric Codes as Lattices

Basis of $\mathcal{L}_A$ for q a power of a prime

If $q = p^s$ is a power of a prime, $\mathcal{C}$ is permutation equivalent to a some code $\mathcal{C}'$ where we have a lattice basis for $\mathcal{L}_A(\mathcal{C}')$ given by

$$\begin{bmatrix} \mathbf{I}_{k_0} & \mathbf{A}_{0,1} & \mathbf{A}_{0,2} & \cdots & \mathbf{A}_{0,s-1} & \mathbf{A}_{0,s} \\ 0 & p\mathbf{I}_{k_1} & p\mathbf{A}_{1,2} & \cdots & p\mathbf{A}_{1,s-1} & p\mathbf{A}_{1,s} \\ 0 & 0 & p^2\mathbf{I}_{k_2} & \cdots & p^2\mathbf{A}_{2,s-1} & p^2\mathbf{A}_{2,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p^{s-1}\mathbf{I}_{k_{s-1}} & p^{s-1}\mathbf{A}_{s-1,s} \\ 0 & 0 & 0 & \cdots & 0 & p^s\mathbf{I}_{n-(k_0+\cdots+k_{s-1})} \end{bmatrix}^\top.$$

Reduction from Lee Decoding Problem to α-BDD

Proposition

$\lambda_1^{(1)}(\mathcal{L}_A(\mathcal{C})) = \min\{q, \mathsf{dist}_L(\mathcal{C})\}$.

Theorem

Given a code $\mathcal{C} \subseteq \mathbb{Z}_q^n$ with minimum Lee distance $d < q$ and a vector $\mathbf{r} \in \mathbb{Z}_q^n$ where $\mathsf{dist}_L(\mathbf{r}, \mathbf{c}) < \alpha \cdot d$ for some $\mathbf{c} \in \mathcal{C}$ and some $\alpha \in (0, 1)$, the LDP reduces to ℓ_1-norm α-BDD with lattice $\mathcal{L}_A(\mathcal{C}) \subseteq \mathbb{R}^n$ and (integer) vector $\mathbf{r} \in \mathbb{R}^n$.

Lattices with a Smaller Dimension

Construction A_{sub}

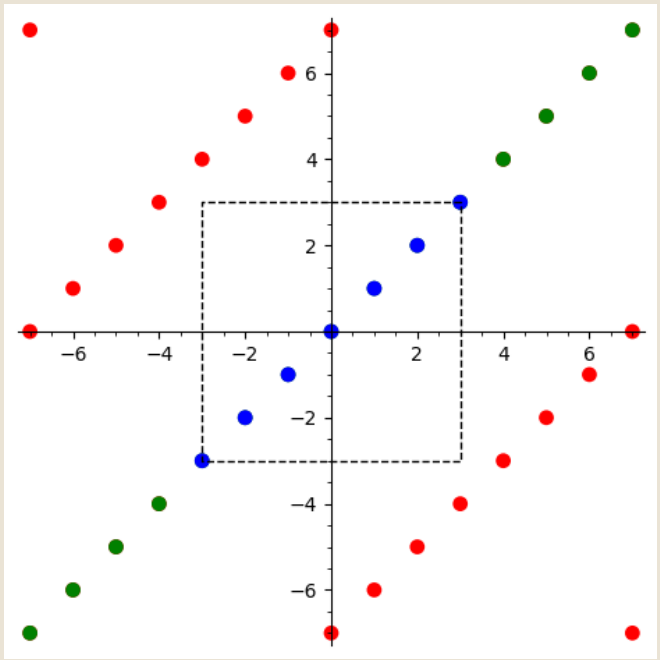
Let $\mathcal{C}$ be a linear code with generator matrix $\mathbf{G} \in \mathbb{Z}_q^{k \times n}$.
Define

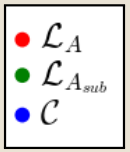
$$\mathcal{L}_{A_{\text{sub}}}(\mathbf{G}) := \{\mathbf{G}^\top \cdot \mathbf{x} \in \mathbb{Z}^n | \mathbf{x} \in \mathbb{Z}^k\} = \mathbf{G}^\top \cdot \mathbb{Z}^k.$$

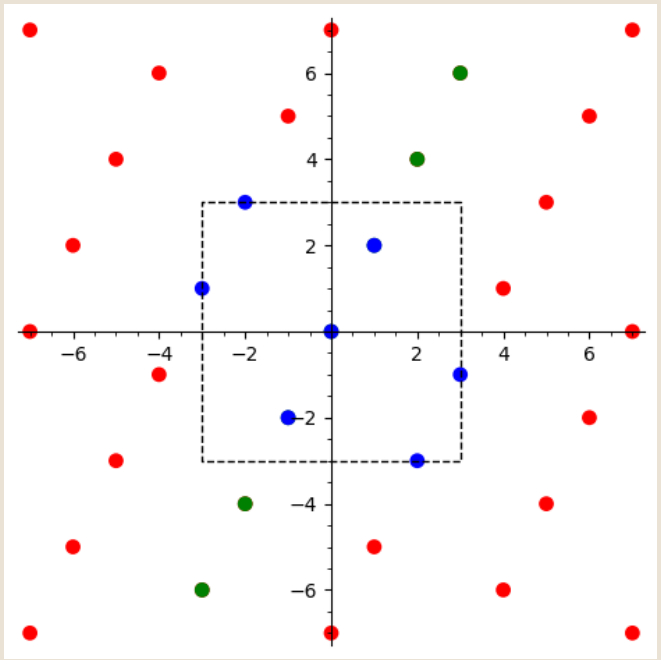
- Depends on choice of generator matrix.
- Lattice has dimension k.
- The lattice basis is simply $\mathbf{G}^\top$ (but considered with entries in $\mathbb{Z}$).
- $\mathcal{L}_{A_{\text{sub}}}(\mathbf{G}) \subseteq \mathcal{L}_A(\mathcal{C})$.
- $\mathcal{C}$ is not necessarily wholly contained in $\mathcal{L}_{A_{\text{sub}}}(\mathbf{G})$.

Examples of Construction A_{sub} in 2 Dimensions

Simple Examples in $\mathbb{Z}_7^2$





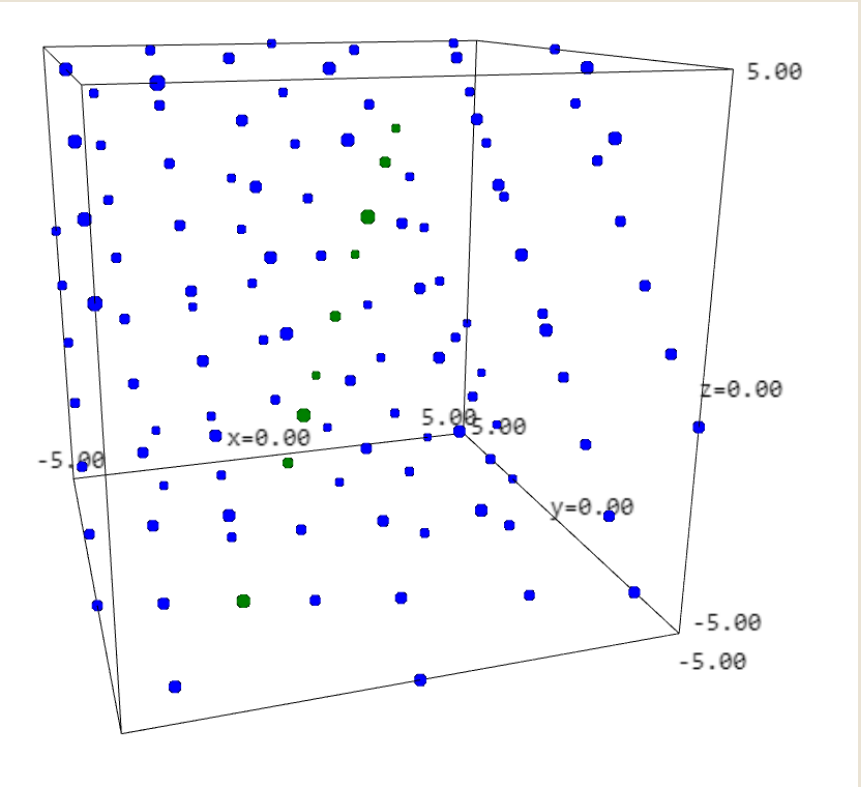


$\mathcal{C} = \langle (1,1) \rangle \subseteq \mathbb{Z}_7^2$

$\mathcal{C} = \langle (1,2) \rangle \subseteq \mathbb{Z}_7^2$

Example of a Construction A_{sub} in 3 Dimensions

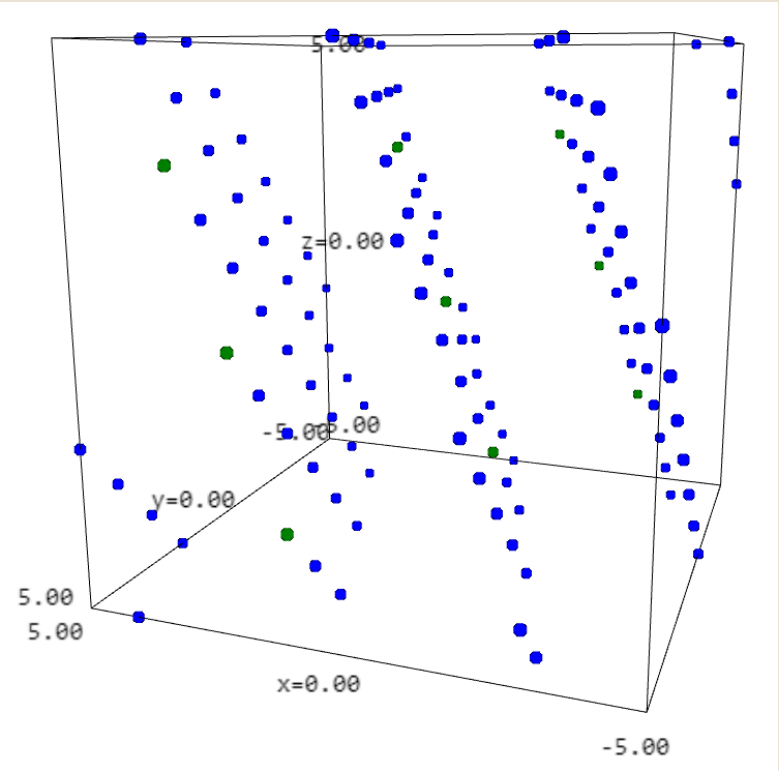
Less Simple Example in $\mathbb{Z}_{11}^3$



$$\mathcal{C} = \left\langle \begin{bmatrix} 1 & 0 & 3 \\ 2 & 5 & 0 \end{bmatrix} \right\rangle \subseteq \mathbb{Z}_{11}^3$$

Example of a Construction A_{sub} in 3 Dimensions

Less Simple Example in $\mathbb{Z}_{11}^3$



$$\mathcal{C} = \left\langle \begin{bmatrix} 1 & 0 & 3 \\ 2 & 5 & 0 \end{bmatrix} \right\rangle \subseteq \mathbb{Z}_{11}^3$$

Bounds on the Number of Codewords in A_{sub}

Note $\mathcal{L}_{A_{\text{sub}}}(\mathbf{G}) \cap [-\lfloor q/2 \rfloor, \lfloor q/2 \rfloor]^n \subseteq \mathcal{C}$. Using Blichfeldt's theorem, we get the following lower bound (and a trivial upper bound):

$$2\left\lfloor \frac{(q-1)^k}{2^k\sqrt{\det(\mathbf{G}\mathbf{G}^\top)}} \right\rfloor \leq |\mathcal{C} \cap \mathcal{L}_{A_{\text{sub}}}(\mathbf{G})| \leq |\mathcal{C}|\,.$$

Open Problems

- Can we get better bounds on the number of codewords in the A_{sub} lattices for given generator matrices?
- Can we get general bounds on the number of codewords in the A_{sub} lattices for broad parameters (e.g., n, q)?
- Can we reduce the hardness of LDP by choosing a good generator matrix?
- Ultimately, which parameters of Lee metric codes are cryptographically secure and useful?

Thank you!

 Bariffi, Jessica (2024). “Analysis and Decoding of Linear Lee-Metric Codes with Application to Code-Based Cryptography”. https://user.math.uzh.ch/bariffi/PhD_Thesis.pdf. PhD thesis. University of Zurich.

 Horlemann-Trautmann, Anna-Lena and Violetta Weger (2021). “Information set decoding in the Lee metric with applications to cryptography.”. In: Advances in Mathematics of Communications 15.4.

 Hörmann, Felicitas and Wessel van Woerden (2024). FuLeakage: Breaking FuLeeca by Learning Attacks. Cryptology ePrint Archive, Paper 2024/353. URL: https://eprint.iacr.org/2024/353.

 Lyubashevsky, Vadim and Daniele Micciancio (2009). “On bounded distance decoding, unique shortest vectors, and the minimum distance problem”. In: Annual International Cryptology Conference. Springer, pp. 577–594.

 Weger, Violetta et al. (2024). “On the hardness of the Lee syndrome decoding problem”. In: Advances in Mathematics of Communications 18.1, pp. 233–266. ISSN: 1930-5346. DOI: 10.3934/amc.2022029.