

Lee Metric Decoding and ℓ_1 Norm Lattices

Marc Newman

(jointly with Anna-Lena Horlemann, Karan Khathuria, and Carlos Vela-Cabello)

2024.02.08

University of St. Gallen—Institute of Computer Science



University of St.Gallen

Institute of Computer Science



Table of contents

Preliminaries

Reductions

Ongoing Work

Preliminaries

Definition (Lee Weight and Distance)

For $m, n \in \mathbb{N}$ and $\mathbf{x} \in (\mathbb{Z}/m\mathbb{Z})^n$, define the **Lee weight** to be

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

For $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}/m\mathbb{Z})^n$, define the **Lee distance** to be

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

Lee Metric Decoding Problem

Definition (Lee Decoding Problem)

Given a linear code C over $\mathbb{Z}/m\mathbb{Z}$ of length n , some $t \in \mathbb{N}$, and a vector $\mathbf{r} \in (\mathbb{Z}/m\mathbb{Z})^n$, find $\mathbf{c} \in C$ such that $\text{wt}_L(\mathbf{r} - \mathbf{c}) \leq t$.

Definition (ℓ_1 Norm)

Given $\mathbf{v} \in \mathbb{R}^n$, the ℓ_1 **norm** of $\mathbf{v}$ is defined to be

$$\|\mathbf{v}\|_1 := \sum_{i=1}^n |v_i|.$$

Definition (Lattice)

Given k linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$, the **lattice** generated by them is given by

$$\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_k) := \left\{ \sum_{i=1}^k x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}.$$

Definition (i th Successive Minimum)

Given a lattice $\mathcal{L}$, let $\lambda_1(\mathcal{L})$ be the length of the shortest vector in $\mathcal{L}$ with respect to the ℓ_1 norm, i.e.,

$$\lambda_1(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L}} \|\mathbf{v}\|_1.$$

More generally, let $\lambda_i(\mathcal{L})$ be the smallest radius r containing i linearly independent lattice points in $\mathcal{L}$, i.e.,

$$\lambda_i(\mathcal{L}) := \min_{\substack{L \subseteq \mathcal{L} \\ \dim L = i}} \max_{\mathbf{v} \in L} \|\mathbf{v}\|_1.$$

Definition (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 $\text{dist}(\mathbf{r}, \mathcal{L}) < \alpha \lambda_1(\mathcal{L})$, find $\mathbf{v} \in \mathcal{L}$ such that $\text{dist}(\mathbf{r}, \mathbf{v})$ is minimal.

Definition (γ -unique Shortest Vector Problem (γ -uSVP))

Given a lattice $\mathcal{L}$ such that $\lambda_2(\mathcal{L}) > \gamma \lambda_1(\mathcal{L})$, find a nonzero vector $\mathbf{v} \in \mathcal{L}$ of length $\lambda_1(\mathcal{L})$.

Reductions

Lee Metric Codes as Lattices

Given an $[n, k, d]$ linear code C over $\mathbb{Z}/m\mathbb{Z}$ with generator matrix $\mathbf{G}$, we can associate a lattice to C given by

$$\mathcal{L}(C) = \{c \in \mathbb{Z}^n \mid c = G^\top x \pmod{m} \text{ for some } x \in \mathbb{Z}^k\}.$$

This lattice is independent of the choice of generator matrix.

Furthermore, if $\begin{bmatrix} \mathbf{I}_k & \mathbf{G}' \end{bmatrix}$ is the systematic generator matrix for C , then the rows of

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

form a basis of the lattice $\mathcal{L}(C)$.

Reduction from Lee Decoding Problem to α -BDD

Proposition

$\lambda_1(\mathcal{L}(C)) = d$ with respect to the ℓ_1 norm.

Theorem

The Lee decoding problem whose input is an $[n, k, d]$ code C over $\mathbb{Z}/m\mathbb{Z}$, a weight $t \leq \lfloor \frac{d}{2} \rfloor$, and a received word $\mathbf{r} \in (\mathbb{Z}/m\mathbb{Z})^n$ reduces to $(\ell_1 \text{ norm})$ α -BDD with lattice $\mathcal{L}(C)$, vector $\mathbf{r}$, and $\alpha = \frac{1}{2}$.

Reduction from α -BDD to γ -uSVP

Theorem

In the ℓ_2 norm, for any $\gamma \geq 1$, $\frac{1}{2\gamma}$ -BDD reduces to γ -uSVP.[LM09]

Proposition

In the ℓ_1 norm, for any $\gamma \geq 1$, $\frac{1}{2\gamma}$ -BDD with a lattice associated to an n -length Lee-metric linear code reduces to γ -uSVP (over $\mathbb{R}^{n+1}$).

Lee Decoding Problem to γ -uSVP

Specifically, given an instance of the Lee decoding problem with an $[n, k, d]$ code $\mathcal{C}$ with systematic generator matrix $\begin{bmatrix} \mathbf{I}_k & \mathbf{G}' \end{bmatrix}$, $\gamma \geq 1$, and received word $\mathbf{r} \in (\mathbb{Z}/m\mathbb{Z})^n$ with $\text{dist}_L(\mathbf{r}, \mathcal{C}) \leq t = \left\lfloor \frac{d}{2\gamma} \right\rfloor$, we construct the following lattice basis:

$$\mathbf{B} = \begin{bmatrix} t & \mathbf{r} & \cdots \\ 0 & \mathbf{I}_k & \mathbf{G}' \\ 0 & \mathbf{0} & m\mathbf{I}_{n-k} \end{bmatrix}.$$

This lattice satisfies $\lambda_2(\mathcal{L}(\mathbf{B})) > \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$ and the solution to γ -uSVP on $\mathcal{L}(\mathbf{B})$ will also be the solution to the Lee decoding problem on $\mathcal{C}$.

Ongoing Work

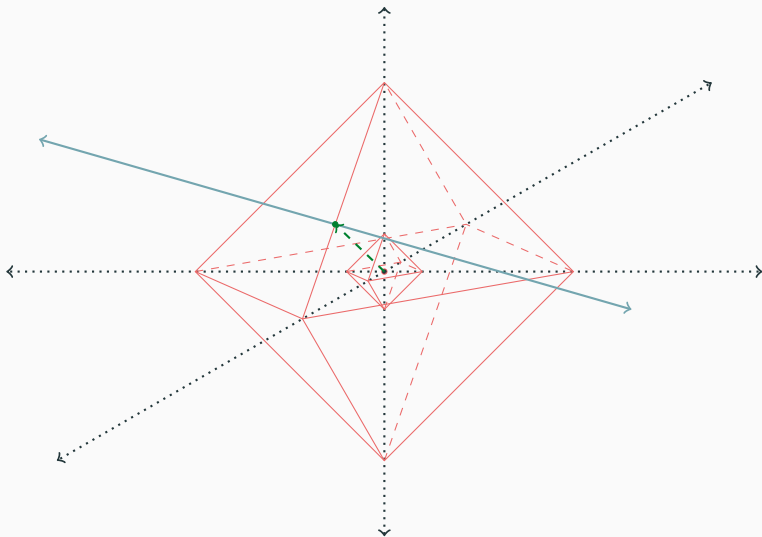
Nice polynomial-time reductions exist from many lattice problems in the ℓ_2 norm to other ℓ_p (for $1 \leq p \leq \infty$) norms using embeddings, e.g., [RR06].

However, reductions in the other direction are less common in the literature and generally worse performing.

Can we use ℓ_1 norm projections in order to get something like Gram-Schmidt and LLL but for the ℓ_1 norm? Two big questions:

- What properties do we need in order to make LLL work in our case?
- Can we efficiently compute these projections?

Norm Balls



An Inefficient Algorithm

Given the $n \times k$ basis $\mathbf{B}$ of some k -dimensional subspace in $\mathbb{R}^n$, we want to project some vector $\mathbf{u}$ onto it; i.e., we want to compute

$$\operatorname{argmin}_{\mathbf{x} \in \mathbb{R}^k} \|\mathbf{B}\mathbf{x} - \mathbf{u}\|_1.$$

For $S = (s_1, \dots, s_n) \in \{-1, 1\}^n$, consider

$$\begin{aligned} X_S &= \left\{ \mathbf{x} \in \mathbb{R}^k \mid \|\mathbf{B}\mathbf{x} - \mathbf{u}\|_1 = \sum_{i=1}^n s_i \left(-u_i + \sum_{j=1}^k b_{ji}x_j \right) \right\} \\ &= \left\{ \mathbf{x} \in \mathbb{R}^k \mid s_i \left(-u_i + \sum_{j=1}^k b_{ji}x_j \right) \geq 0 \text{ for all } i \in [n] \right\}. \end{aligned}$$

These sets are convex (and some may be empty).

An Inefficient Algorithm (cont.)

- Intersecting $h + 1$ of these gives a similarly defined set corresponding to some $T = (t_1, \dots, t_n) \in \{-1, 0, 1\}^n$ representing a $(k - h)$ -dimensional set where at least h values of t_i are equal to 0.
- $\|\mathbf{B}\mathbf{x} - \mathbf{u}\|_1$ is linear when restricted to some such X_T and the minimum will happen on the boundary of these sets.
- So we walk through all $I \subset [n]$ with $|I| = k$ and find $\mathbf{x} \in \mathbb{R}^k$ such that $\mathbf{B}\mathbf{x} - \mathbf{u}$ has zeros in all I coordinates and calculate the corresponding norms.

An Inefficient Algorithm (cont.)

This is then equivalent to finding

$$I' = \operatorname{argmin}_{\substack{I \subseteq [n] \\ |I|=k}} \left\| \mathbf{B}_J \mathbf{B}_I^{-1} \mathbf{u}_I - \mathbf{u}_J \right\|_1$$

where $\mathbf{B}_I$ are the I -indexed rows of $\mathbf{B}$ and $J = [n] \setminus I$. Then the projection is $\mathbf{B} \mathbf{B}_{I'}^{-1} \mathbf{u}_{I'}$.

Or we can just use linear programming. For projecting $\mathbf{u}$ onto the subspace given by basis $\mathbf{B}$:

Find $\mathbf{z} = (\underbrace{\mathbf{x}_1^+, \dots, \mathbf{x}_n^+, \mathbf{x}_1^-, \dots, \mathbf{x}_n^-}_{\mathbf{x}}, \underbrace{\mathbf{y}_1^+, \dots, \mathbf{y}_k^+, \mathbf{y}_1^-, \dots, \mathbf{y}_k^-}_{\mathbf{y}})^T \in \mathbb{R}^{2n+2k}$

that minimizes $\mathbf{1}_{2k}^T \mathbf{y}$

such that $\begin{bmatrix} \mathbf{B} & -\mathbf{B} & -\mathbf{I}_k & \mathbf{I}_k \end{bmatrix} \mathbf{z} = \mathbf{u}$

and $z_i \geq 0$ for all $1 \leq i \leq 2n + 2k$.

- Are there known methods for doing lattice reductions specifically in the ℓ_1 norm?
- Are there any known results on uSVP in the ℓ_1 norm?
- What properties do we need to do something like LLL?
- Are there reasonable ways of computing projections in ℓ_1 ?



Ravi Kannan. **“Minkowski’s convex body theorem and integer programming”**. In: *Mathematics of operations research* 12.3 (1987), pp. 415–440.



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



Oded Regev and Ricky Rosen. **“Lattice problems and norm embeddings”**. In: *Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing*. 2006, pp. 447–456.

Thank you!