

Information-theoretic Bounds on the Size of Spheres in the Lee Metric

Jessica Bariffi

SIAM Conference on Applied Algebraic Geometry (AG25)

July 9th, 2025



TUM Uhrenturm

- Crucial task in Coding Theory: understand limits in performance of error-correction
 - ⇒ Sphere-packing bounds, Gilbert-Varshamov bound, ...
 - ⇒ Derived using bounds on n -dimensional spheres in corresponding metrics

- Crucial task in Coding Theory: understand limits in performance of error-correction
 - ⇒ Sphere-packing bounds, Gilbert-Varshamov bound, ...
 - ⇒ Derived using bounds on n -dimensional spheres in corresponding metrics
- Hamming metric: compact closed form for size of n -dimensional sphere of given Hamming radius.

- Crucial task in Coding Theory: understand limits in performance of error-correction
 - ⇒ Sphere-packing bounds, Gilbert-Varshamov bound, ...
 - ⇒ Derived using bounds on n -dimensional spheres in corresponding metrics
- Hamming metric: compact closed form for size of n -dimensional sphere of given Hamming radius.
- Other additive metrics: Similar expressions can get hard to manipulate → bounds needed!

- Crucial task in Coding Theory: understand limits in performance of error-correction
 - ⇒ Sphere-packing bounds, Gilbert-Varshamov bound, ...
 - ⇒ Derived using bounds on n -dimensional spheres in corresponding metrics
- Hamming metric: compact closed form for size of n -dimensional sphere of given Hamming radius.
- Other additive metrics: Similar expressions can get hard to manipulate → bounds needed!

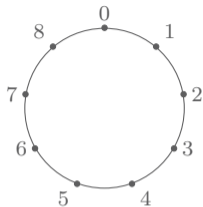
Disclaimer

Method presented can be used for any additive metric.

1. Lee Metric and Spheres
2. Information-Theoretic Tools
3. Bounds in the Lee Metric

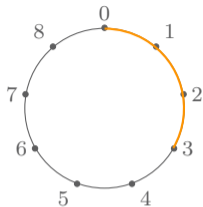
1. Lee Metric and Spheres
2. Information-Theoretic Tools
3. Bounds in the Lee Metric

The Lee Metric

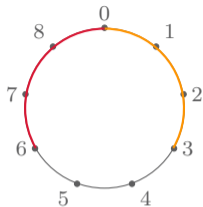


The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0.

The Lee Metric



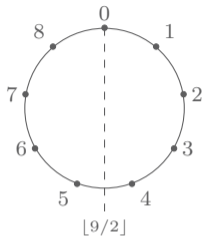
The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0.



The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0. Hence,

$$\text{wt}_L(a) = \text{wt}_L(q - a)$$

$$\text{wt}_H(a) \leq \text{wt}_L(a) \leq \lfloor q/2 \rfloor$$

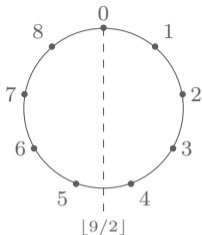


The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0. Hence,

$$\text{wt}_L(a) = \text{wt}_L(q - a)$$

$$\text{wt}_H(a) \leq \text{wt}_L(a) \leq \lfloor q/2 \rfloor$$

The Lee Metric



The *Lee weight* of an element $a \in \mathbb{Z}/q\mathbb{Z}$ defines the **minimum number of arcs** separating a from the origin 0. Hence,

$$\text{wt}_L(a) = \text{wt}_L(q - a)$$

$$\text{wt}_H(a) \leq \text{wt}_L(a) \leq \lfloor q/2 \rfloor$$

Definition

For any integer $a \in \mathbb{Z}/q\mathbb{Z}$ and any vector $x, y \in (\mathbb{Z}/q\mathbb{Z})^n$ we define their *Lee weight* as

$$\text{wt}_L(a) := \min(a, |q - a|) \quad \text{and} \quad \text{wt}_L(x) := \sum_{i=1}^n \text{wt}_L(x_i)$$

The *Lee distance* between x and y is given by $d_L(x, y) := \text{wt}_L(x - y)$.

$$\begin{array}{ll} n\text{-dimensional Lee sphere of radius } t & \mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) = t\} \\ n\text{-dimensional Lee ball of radius } t & \mathcal{B}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) \leq t\} \end{array}$$

$$\begin{aligned} n\text{-dimensional Lee sphere of radius } t & \quad \mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) = t\} \\ n\text{-dimensional Lee ball of radius } t & \quad \mathcal{B}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) \leq t\} \end{aligned}$$

Example Lee weight $t = 2$ in $\mathbb{Z}/5\mathbb{Z}$

→ vectors containing either 2 elements of Lee weight 1 or 1 element of Lee weight 2.

$$\begin{aligned} n\text{-dimensional Lee sphere of radius } t & \quad \mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) = t\} \\ n\text{-dimensional Lee ball of radius } t & \quad \mathcal{B}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) \leq t\} \end{aligned}$$

Example Lee weight $t = 2$ in $\mathbb{Z}/5\mathbb{Z}$

→ vectors containing either 2 elements of Lee weight 1 or 1 element of Lee weight 2.

$$\mathcal{S}_{2,5}^{(3)} = \{(1, 1, 0), \dots, (1, 4, 0), \dots, (4, 4, 0), \dots, (2, 0, 0), \dots, (3, 0, 0), \dots\}.$$

$$\begin{aligned} n\text{-dimensional Lee sphere of radius } t & \mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) = t\} \\ n\text{-dimensional Lee ball of radius } t & \mathcal{B}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) \leq t\} \end{aligned}$$

Example Lee weight $t = 2$ in $\mathbb{Z}/5\mathbb{Z}$

→ vectors containing either 2 elements of Lee weight 1 or 1 element of Lee weight 2.

$$\mathcal{S}_{2,5}^{(3)} = \{(1, 1, 0), \dots, (1, 4, 0), \dots, (4, 4, 0), \dots, (2, 0, 0), \dots, (3, 0, 0), \dots\}.$$

Theorem - [Roth, '06]

Whenever $t \leq q/2$, we have $\left| \mathcal{S}_{t,q}^{(n)} \right| = \sum_{i=0}^n 2^i \binom{n}{i} \binom{t}{i}.$

$$\begin{aligned} n\text{-dimensional Lee sphere of radius } t & \quad \mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) = t\} \\ n\text{-dimensional Lee ball of radius } t & \quad \mathcal{B}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) \leq t\} \end{aligned}$$

Example Lee weight $t = 2$ in $\mathbb{Z}/5\mathbb{Z}$

→ vectors containing either 2 elements of Lee weight 1 or 1 element of Lee weight 2.

$$\mathcal{S}_{2,5}^{(3)} = \{(1, 1, 0), \dots, (1, 4, 0), \dots, (4, 4, 0), \dots, (2, 0, 0), \dots, (3, 0, 0), \dots\}.$$

Theorem - [Roth, '06]

Whenever $t \leq q/2$, we have $\left| \mathcal{S}_{t,q}^{(n)} \right| = \sum_{i=0}^n 2^i \binom{n}{i} \binom{t}{i}.$

Other ways to compute the sphere size:

- Generating functions
- Convolutions
- Counting integer partitions
- Typical sequences
- ...

$$\begin{aligned} n\text{-dimensional Lee sphere of radius } t & \mathcal{S}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) = t\} \\ n\text{-dimensional Lee ball of radius } t & \mathcal{B}_{t,q}^{(n)} := \{x \in (\mathbb{Z}/q\mathbb{Z})^n \mid \text{wt}_L(x) \leq t\} \end{aligned}$$

Example Lee weight $t = 2$ in $\mathbb{Z}/5\mathbb{Z}$

→ vectors containing either 2 elements of Lee weight 1 or 1 element of Lee weight 2.

$$\mathcal{S}_{2,5}^{(3)} = \{(1, 1, 0), \dots, (1, 4, 0), \dots, (4, 4, 0), \dots, (2, 0, 0), \dots, (3, 0, 0), \dots\}.$$

Theorem - [Roth, '06]

Whenever $t \leq q/2$, we have $|\mathcal{S}_{t,q}^{(n)}| = \sum_{i=0}^n 2^i \binom{n}{i} \binom{t}{i}.$

Other ways to compute the sphere size:

- Generating functions
- Typical sequences
- Convolutions
- ...
- Counting integer partitions

Stay tuned for Hugo's talk right after this! ;)

1. Lee Metric and Spheres
2. Information-Theoretic Tools
3. Bounds in the Lee Metric

Types and Spheres

- Finite alphabet \mathcal{A} with additive weight function wt
- Maximum weight over \mathcal{A} : $\mu = \max_{a \in \mathcal{A}} (\text{wt}(a))$

Definition: type

The *type* of any tuple $x \in \mathcal{A}^n$ is defined as the tuple $\theta(x) := (\theta_0(x), \dots, \theta_{|\mathcal{A}|-1}(x))$, where

$$\theta_i(x) = \frac{1}{n} |\{k = 1, \dots, n \mid x_k = i\}|.$$

Types and Spheres

- Finite alphabet \mathcal{A} with additive weight function wt
- Maximum weight over \mathcal{A} : $\mu = \max_{a \in \mathcal{A}} (\text{wt}(a))$

Definition: type

The *type* of any tuple $x \in \mathcal{A}^n$ is defined as the tuple $\theta(x) := (\theta_0(x), \dots, \theta_{|\mathcal{A}|-1}(x))$, where

$$\theta_i(x) = \frac{1}{n} |\{k = 1, \dots, n \mid x_k = i\}|.$$

\implies Can recover weight from type: $\text{wt}(x) = n \sum_{i=0}^{\mu} \theta_i(x) \text{wt}(i)$

\implies If $\text{wt}(x) = t$, the type induces an integer partition of t of parts of size at most μ .

Types and Spheres

- Finite alphabet \mathcal{A} with additive weight function wt
- Maximum weight over \mathcal{A} : $\mu = \max_{a \in \mathcal{A}} (\text{wt}(a))$

Definition: type

The *type* of any tuple $x \in \mathcal{A}^n$ is defined as the tuple $\theta(x) := (\theta_0(x), \dots, \theta_{|\mathcal{A}|-1}(x))$, where

$$\theta_i(x) = \frac{1}{n} |\{k = 1, \dots, n \mid x_k = i\}|.$$

\implies Can recover weight from type: $\text{wt}(x) = n \sum_{i=0}^{\mu} \theta_i(x) \text{wt}(i)$

\implies If $\text{wt}(x) = t$, the type induces an integer partition of t of parts of size at most μ .

Sphere size via types

$$\left| \mathcal{S}_{t, \mathcal{A}}^{(n)} \right| = \sum_{\theta \in \Theta_t^{(n)}} \frac{n!}{(n\theta_0)! \cdots (n\theta_{|\mathcal{A}|-1})!} =: \sum_{\theta \in \Theta_t^{(n)}} \binom{n}{n\theta}$$

Bounds via Entropy

- Random variable X over finite alphabet \mathcal{A}
- P_X probability distribution of X : $P_X(a) = \mathbb{P}(X = a)$, $a \in \mathcal{A}$.
- Q another probability distribution over \mathcal{A}

Definition: Entropy and Kullback-Leibler Divergence

$$H(P_X) = \sum_{\substack{a \in \mathcal{A} \\ P_X(a) \neq 0}} P_X(a) \log_2(P_X(a))$$

$$D(P_X \parallel Q) = - \sum_{a \in \mathcal{A}} P_X(a) \log \left(\frac{P_X(a)}{Q(a)} \right)$$

Bounds via Entropy

- Random variable X over finite alphabet \mathcal{A}
- P_X probability distribution of X : $P_X(a) = \mathbb{P}(X = a)$, $a \in \mathcal{A}$.
- Q another probability distribution over \mathcal{A}

Definition: Entropy and Kullback-Leibler Divergence

$$H(P_X) = \sum_{\substack{a \in \mathcal{A} \\ P_X(a) \neq 0}} P_X(a) \log_2(P_X(a))$$

$$D(P_X \parallel Q) = - \sum_{a \in \mathcal{A}} P_X(a) \log \left(\frac{P_X(a)}{Q(a)} \right)$$

Theorem [Cover & Thomas]

$$\frac{1}{(n+1)^{|\mathcal{A}|-1}} 2^{nH(\theta)} \leq \binom{n}{n\theta} \leq 2^{nH(\theta)}$$

Bounds via Entropy

- Random variable X over finite alphabet \mathcal{A}
- P_X probability distribution of X : $P_X(a) = \mathbb{P}(X = a)$, $a \in \mathcal{A}$.
- Q another probability distribution over \mathcal{A}

Definition: Entropy and Kullback-Leibler Divergence

$$H(P_X) = \sum_{\substack{a \in \mathcal{A} \\ P_X(a) \neq 0}} P_X(a) \log_2(P_X(a))$$

$$D(P_X \parallel Q) = - \sum_{a \in \mathcal{A}} P_X(a) \log \left(\frac{P_X(a)}{Q(a)} \right)$$

Theorem [Cover & Thomas]

$$\frac{1}{(n+1)^{|\mathcal{A}|-1}} 2^{nH(\theta)} \leq \binom{n}{n\theta} \leq 2^{nH(\theta)}$$

Sphere size: Bounded by sequence whose type maximizes the entropy.

Example

$$\mathcal{S}_{2,5}^{(3)} = \left\{ (1, 1, 0), \dots, (1, 4, 0), \dots, (4, 4, 0), \dots, (2, 0, 0), \dots, (3, 0, 0), \dots \right\}$$

Draw $a \in \mathcal{S}_{2,5}^{(3)}$ uniformly at random, then ...

- smaller Lee weights are more likely to occur in the vector a .
- some sequences are more likely \longrightarrow typical sequence.

Example

$$\mathcal{S}_{2,5}^{(3)} = \left\{ (1, 1, 0), \dots, (1, 4, 0), \dots, (4, 4, 0), \dots, (2, 0, 0), \dots, (3, 0, 0), \dots \right\}$$

Draw $a \in \mathcal{S}_{2,5}^{(3)}$ uniformly at random, then ...

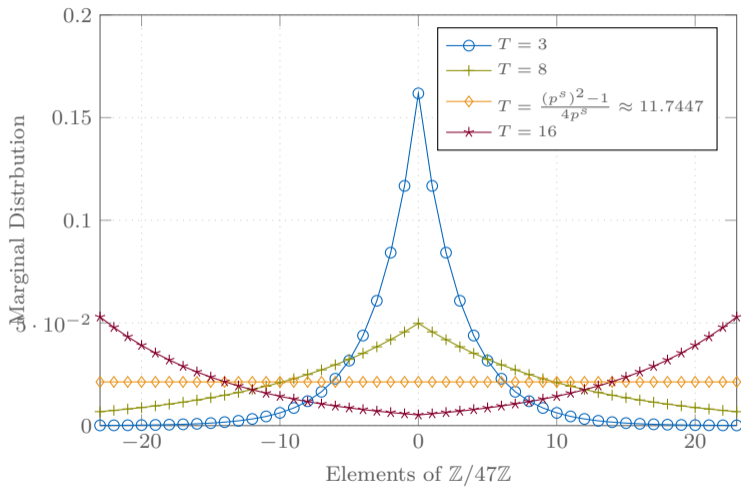
- smaller Lee weights are more likely to occur in the vector a .
- some sequences are more likely \rightarrow typical sequence.
- Define $E := \left\{ P = (p_0, \dots, p_{q-1}) \mid \sum_{i=0}^{q-1} p_i \text{wt}_L(i) = \delta \right\} \rightarrow$ distributions of tuples in $\mathcal{S}_{\delta n, q}^{(n)}$.

Theorem - [B., Bartz, Liva, Rosenthal - 21⁴]

The distribution in E maximizing the entropy is given by $B_\delta = (B_\delta(0), \dots, B_\delta(q-1))$, where

$$B_\delta(i) := \frac{1}{Z(\beta)} \exp(-\beta \text{wt}_L(i)).$$

Lee-Boltzmann Distribution - Example over $\mathbb{Z}/47\mathbb{Z}$

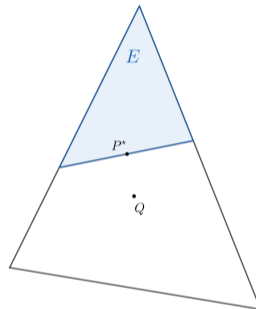


Conditional Limit Theorem - [Cover & Thomas]

Let E be a closed convex set of probability distributions over an alphabet \mathcal{X} and let Q be a distribution over \mathcal{X} but not in E . Let X_1, \dots, X_n be discrete random variables drawn i.i.d. $\sim Q$. Define $X^n = (X_1, \dots, X_n)$ and let $P^* = \arg \min_{P \in E} D(P \parallel Q)$. Then

$$\mathbb{P}(X_1 = a \mid P_{X^n} \in E) \longrightarrow P^*(a)$$

in probability as n grows large for any $a \in \mathcal{X}$.

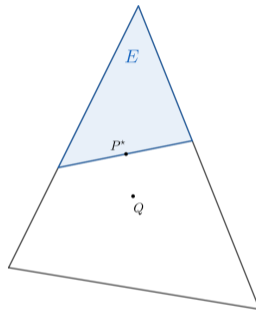


Conditional Limit Theorem - [Cover & Thomas]

Let E be a closed convex set of probability distributions over an alphabet \mathcal{X} and let Q be a distribution over \mathcal{X} but not in E . Let X_1, \dots, X_n be discrete random variables drawn i.i.d. $\sim Q$. Define $X^n = (X_1, \dots, X_n)$ and let $P^* = \arg \min_{P \in E} D(P \parallel Q)$. Then

$$\mathbb{P}(X_1 = a \mid P_{X^n} \in E) \longrightarrow P^*(a)$$

in probability as n grows large for any $a \in \mathcal{X}$.



In our case

- $Q \sim \mathcal{U}(\mathbb{Z}/q\mathbb{Z})$
- E set of distributions of tuples in $\mathcal{S}_{t,q}^{(n)}$
- $P^* = B_\delta$, for $\delta = t/n$

Lemma - Marginal Distribution in the Lee Sphere [BBLR, '21]

Consider a random vector $A \in \mathcal{S}_{\delta n, q}^{(n)}$ and let $P(a)$ be the marginal distribution of an element of A . Then, for every $a \in \mathbb{Z}/q\mathbb{Z}$ we have

$$P(a) \longrightarrow B_{\delta}(a) := \frac{1}{Z(\beta)} \exp(-\beta \text{wt}_{\mathbb{L}}(a)),$$

where β is the unique real solution to the Lee weight constraint $\delta = \sum_{i=0}^{q-1} \text{wt}_{\mathbb{L}}(i) \mathbb{P}(X = i)$ and $Z(\beta)$ denotes the normalization constant

1. Lee Metric and Spheres
2. Information-Theoretic Tools
3. Bounds in the Lee Metric

Definition (Boltzmann-like Distribution)

For any $a \in \mathcal{A}$ and $0 < \delta < \mu$, we define the probability distribution

$$P_{\beta}(a) := \frac{q^{-\beta \text{wt}(a)}}{Z(\beta)}$$

where β is the unique solution to the weight constraint $\mathbb{E}[\text{wt}(a)] = \sum_{a \in \mathcal{A}} P_{\beta}(a) \text{wt}(a) = \delta$ and $Z(\beta)$ is chosen s.t. $\sum_{a \in \mathcal{A}} P_{\beta}(a) = 1$, i.e. $Z(\beta) = \sum_{a \in \mathcal{A}} q^{-\beta \text{wt}(a)}$.

Definition (Boltzmann-like Distribution)

For any $a \in \mathcal{A}$ and $0 < \delta < \mu$, we define the probability distribution

$$P_\beta(a) := \frac{q^{-\beta \text{wt}(a)}}{Z(\beta)}$$

where β is the unique solution to the weight constraint $\mathbb{E}[\text{wt}(a)] = \sum_{a \in \mathcal{A}} P_\beta(a) \text{wt}(a) = \delta$ and $Z(\beta)$ is chosen s.t. $\sum_{a \in \mathcal{A}} P_\beta(a) = 1$, i.e. $Z(\beta) = \sum_{a \in \mathcal{A}} q^{-\beta \text{wt}(a)}$.

- one-to-one correspondence between β and δ
- Denote $H_\delta = H(P_\beta)$

Definition (Boltzmann-like Distribution)

For any $a \in \mathcal{A}$ and $0 < \delta < \mu$, we define the probability distribution

$$P_\beta(a) := \frac{q^{-\beta \text{wt}(a)}}{Z(\beta)}$$

where β is the unique solution to the weight constraint $\mathbb{E}[\text{wt}(a)] = \sum_{a \in \mathcal{A}} P_\beta(a) \text{wt}(a) = \delta$ and $Z(\beta)$ is chosen s.t. $\sum_{a \in \mathcal{A}} P_\beta(a) = 1$, i.e. $Z(\beta) = \sum_{a \in \mathcal{A}} q^{-\beta \text{wt}(a)}$.

- one-to-one correspondence between β and δ
- Denote $H_\delta = H(P_\beta)$

Theorem [Lölicher, 1994]

For any $0 < \delta \leq \bar{w}$ and $n \in \mathbb{N}$ we have $\frac{1}{n} \log_q \left| \mathcal{B}_{\delta n}^{(n)} \right| \leq H_\delta$.

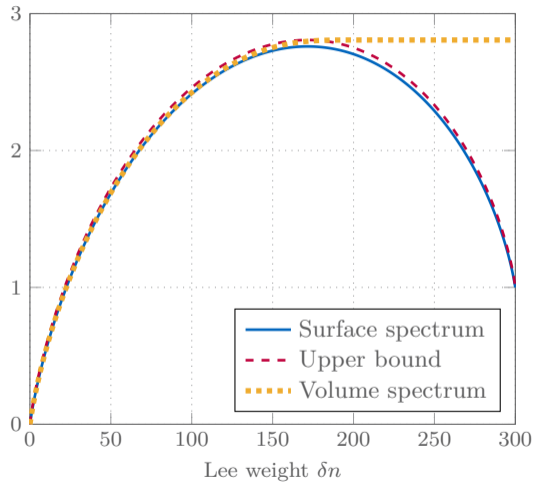
Theorem - [BBLR, 22'] and [SCJB, 24']

For any $0 < \delta \leq \mu$ we have

$$\frac{1}{n} \log_q \left| \mathcal{B}_{\delta n}^{(n)} \right| \leq \begin{cases} H_\delta & \text{if } 0 < \delta \leq \bar{w} \\ \log_q(|\mathcal{A}|) & \text{if } \bar{w} < \delta \leq \mu \end{cases}.$$

Moreover, it holds

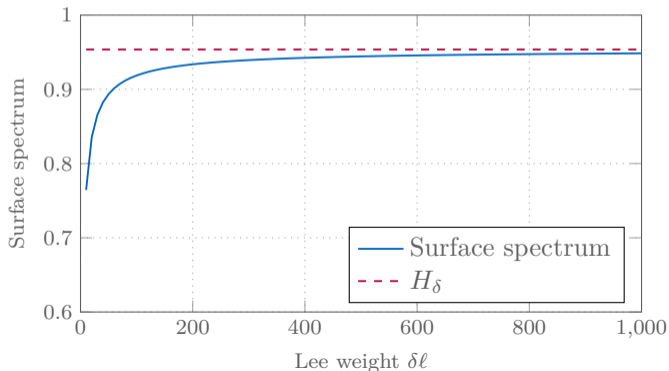
$$\frac{1}{n} \log_q \left| \mathcal{S}_{\delta n}^{(n)} \right| \leq H_\delta$$



Theorem (Continuation)

The bounds provided are asymptotically tight, i.e.,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log_q \left| \mathcal{S}_{\delta n}^{(n)} \right| = H_\delta \quad \text{and} \quad \lim_{n \rightarrow \infty} \frac{1}{n} \log_q \left| \mathcal{B}_{\delta n}^{(n)} \right| = \begin{cases} H_\delta & \text{if } 0 < \delta \leq \bar{w} \\ \log_q(|A|) & \text{if } \bar{w} < \delta \leq \mu \end{cases}.$$



Definition

A linear code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ is a $\mathbb{Z}/q\mathbb{Z}$ -submodule of $(\mathbb{Z}/q\mathbb{Z})^n$.

Parameters

- Blocklength n
- $\mathbb{Z}/q\mathbb{Z}$ -dimension $k := \log_q(|\mathcal{C}|)$
- Rate of the code $R := k/n$ rate of the code

Definition

A linear code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ is a $\mathbb{Z}/q\mathbb{Z}$ -submodule of $(\mathbb{Z}/q\mathbb{Z})^n$.

Parameters

- Blocklength n
- $\mathbb{Z}/q\mathbb{Z}$ -dimension $k := \log_q(|\mathcal{C}|)$
- Rate of the code $R := k/n$ rate of the code

◦ Memoryless Lee Channel

Transmit $x \in \mathcal{C}$

Receive: $y = x + e \in (\mathbb{Z}/q\mathbb{Z})^n$ where $e_i \sim B_\delta$ for some δ

\implies Channel matching to the Lee metric under ML decoding.

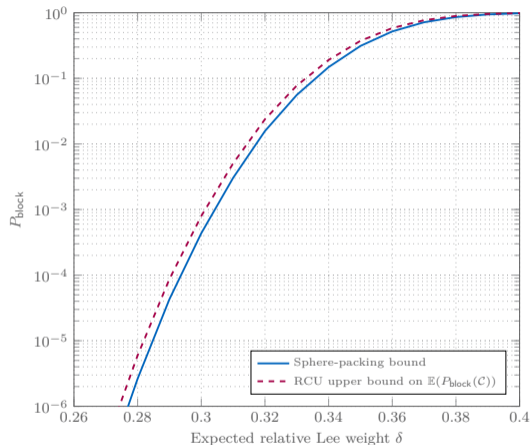
Theorem - [BBLR, '23]

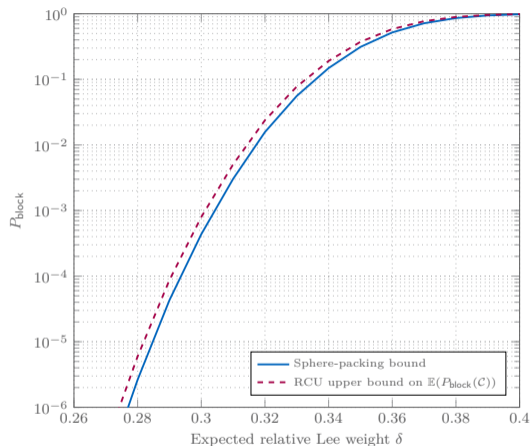
The block error probability of **any** code $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ of rate R over a memoryless Lee channel is lower bounded as

$$P_{\text{block}}(\mathcal{C}) > \frac{1}{Z(\beta)^n} \sum_{d=d_0+1}^{rn} \left| \mathcal{S}_{d,q}^{(n)} \right| \mathbb{E}(-\beta d) + \frac{1}{Z(\beta)^n} \left(\left| \mathcal{S}_{d_0,q}^{(n)} \right| - \xi \right) \mathbb{E}(-\beta d_0)$$

where d_0 and ξ are chosen so that

$$\sum_{d=0}^{d_0-1} \left| \mathcal{S}_{d,q}^{(n)} \right| + \xi = 2^{n(\log_2(q)-R)} \quad \text{and} \quad 0 < \xi \leq \left| \mathcal{S}_{d_0,q}^{(n)} \right|.$$





Thank you for your attention!