Open Problems in the Lee Metric

Violetta Weger

Math Seminars, Sabancı University

November 29, 2023

The history of the Lee metric/ why do we care about it

- Introduced in 1958 by Lee for non-binary codes
- Some good non-linear binary codes can be represented as linear codes in the Lee metric over $\mathbb{Z}/4\mathbb{Z}$
- Introduced to code-based cryptography
- First Lee-metric signature scheme

C. Lee. "Some properties of nonbinary error-correcting codes.", IRE Transactions on Information Theory, 1958.

A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J. Sloane, P. Solé. "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes."IEEE Transactions on Information Theory, 1994.

A.-L. Horlemann, **V.W.** "Information set decoding in the Lee metric with applications to cryptography."Advances in Mathematics of Communications, 2019.

S. Ritterhoff, G. Maringer, S. Bitzer, **V.W.**, P. Karl, T. Schamberger, J. Schupp, A. Wachter-Zeh. "FuLeeca: A Lee-based Signature Scheme.", NIST Submission 2023.

What is a ring-linear code?

$\mathcal{C} \subseteq \mathbb{F}_q^n$ is a code if $\mathcal{C}$ is a linear subspace

Generator matrix in systematic form

$$\begin{pmatrix} \mathrm{Id}_k & A \end{pmatrix}$$

dimension $k = \log_q(\mid \mathcal{C} \mid)$ number of generators

What is a ring-linear code?

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

$$\mathcal{C} \cong (\mathbb{Z}/p^s\mathbb{Z})^{k_0} \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{k_1} \times \cdots \times (\mathbb{Z}/p\mathbb{Z})^{k_{s-1}}$$

Generator matrix in systematic form

$$\begin{pmatrix} \mathrm{Id}_{k_0} & A_{1,2} & \cdots & A_{1,s} & A_{1,s+1} \\ 0 & p\mathrm{Id}_{k_1} & \cdots & pA_{2,s} & pA_{2,s+1} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & p^{s-1}\mathrm{Id}_{k_{s-1}} & p^{s-1}A_{s,s+1} \end{pmatrix},$$

- **subtype** $(k_0, \dots, k_{s-1})$,
- **rank** $K = \sum_{i=0}^{s-1} k_i$,
- **type** $k = \sum_{i=0}^{s-1} \frac{s-i}{s} k_i = \log_{p^s}(\mid \mathcal{C} \mid)$,
- $0 \leq k \leq K \leq n$ and if $k = K$ **free code**

The Lee metric

Hamming metric

- $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad \mathrm{wt}_H(x) = \mid \{i \in \{1, \dots, n\} \mid x_i \neq 0\} \mid$
- $x, y \in (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad d_H(x, y) = \mid \{i \in \{1, \dots, n\} \mid x_i \neq y_i\} \mid = \mathrm{wt}_H(x - y)$
- $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad d_H(\mathcal{C}) = \min\{\mathrm{wt}_H(x) \mid 0 \neq x \in \mathcal{C}\}$

$$e \quad \begin{array}{|c|c|c|c|c|c|}\hline & 0 & 0 & & & 0 \\ \hline \end{array}$$

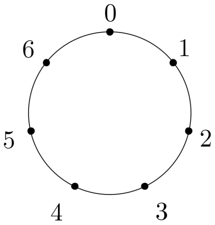
Example

- $(1, 2, 3, 0, 0, 2) \in (\mathbb{Z}/4\mathbb{Z})^6$: $\quad \mathrm{wt}_H(x) = 4,$
- $\langle (1, 2, 3), (2, 0, 0) \rangle \subseteq (\mathbb{Z}/4\mathbb{Z})^3$: $\quad d_H(\mathcal{C}) = 1,$

The Lee metric

Lee metric

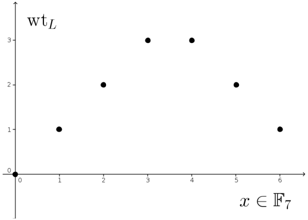
- $x \in \mathbb{Z}/p^s\mathbb{Z} = \{0, \dots, p^s - 1\}$ $\rightarrow$ $\mathrm{wt}_L(x) = \min\{x, |p^s - x|\}$



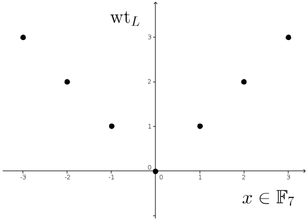
The Lee metric

Lee metric

- $x \in \{-\lfloor \frac{p^s}{2} \rfloor, \dots, \lfloor \frac{p^s}{2} \rfloor\}$ $\quad \rightarrow \quad \mathrm{wt}_L(x) = |x|$



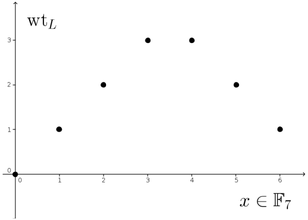
$\rightarrow$



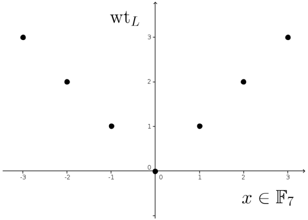
The Lee metric

Lee metric

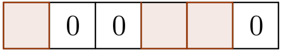
- $x \in \{-\lfloor \frac{p^s}{2} \rfloor, \dots, \lfloor \frac{p^s}{2} \rfloor\}$ $\rightarrow$ $\mathrm{wt}_L(x) = |x|$



$\rightarrow$

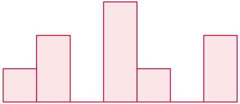


e



$\rightarrow$

e



The Lee metric

Lee metric

- $x \in \{-\lfloor \frac{p^s}{2} \rfloor, \dots, \lfloor \frac{p^s}{2} \rfloor\}$ $\rightarrow$ $\mathrm{wt}_L(x) = |x|$
- $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$ $\rightarrow$ $\mathrm{wt}_L(x) = \sum_{i=1}^n \mathrm{wt}_L(x_i)$
- $x, y \in (\mathbb{Z}/p^s\mathbb{Z})^n$ $\rightarrow$ $d_L(x,y) = \mathrm{wt}_L(x-y)$
- $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code $\rightarrow$ $d_L(\mathcal{C}) = \min\{\mathrm{wt}_L(x) \mid x \in \mathcal{C}, x \neq 0\}$

Example

- $(1,2,3,0,0,2) \in (\mathbb{Z}/4\mathbb{Z})^6$: $\mathrm{wt}_H(x) = 4$, $\mathrm{wt}_L(x) = 6$
- $\langle (1,2,3),(2,0,0) \rangle \subseteq (\mathbb{Z}/4\mathbb{Z})^3$: $d_H(\mathcal{C}) = 1$, $d_L(\mathcal{C}) = 2$

$\rightarrow$ Maximal Lee weight $M = \left\lfloor \frac{p^s}{2} \right\rfloor$ $\rightarrow$ $d_H(\mathcal{C}) \leq d_L(\mathcal{C}) \leq M d_H(\mathcal{C})$

What is a ring-linear code?

Filtration:

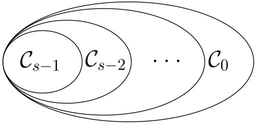
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, define for all $i \in \{0, \ldots, s-1\}$:

$$\mathcal{C}_i = \mathcal{C} \cap \langle p^i \rangle \subseteq p^i \, (\mathbb{Z}/p^s\mathbb{Z})^n \cong \left(\mathbb{Z}/p^{s-i}\mathbb{Z}\right)^n$$

What is a ring-linear code?

Filtration:
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, define for all $i \in \{0, \dots, s-1\}$:

$$\mathcal{C}_i = \mathcal{C} \cap \langle p^i \rangle \subseteq p^i \left(\mathbb{Z}/p^s\mathbb{Z}\right)^n \cong \left(\mathbb{Z}/p^{s-i}\mathbb{Z}\right)^n$$



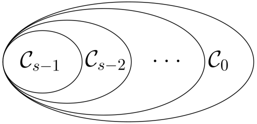
- new maximal Lee weight in $\mathcal{C}_i$ is $M_i = \lfloor \frac{p^{s-i}}{2} \rfloor p^i$
- $\mathcal{C}_{s-1} \subseteq \mathcal{C}_{s-2} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathcal{C}$

$\rightarrow$ $d_L(\mathcal{C}) \leq d_L(\mathcal{C}_1) \leq \cdots \leq d_L(\mathcal{C}_{s-2}) \leq d_L(\mathcal{C}_{s-1})$

What is a ring-linear code?

Filtration:
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, define for all $i \in \{0, \dots, s-1\}$:

$$\mathcal{C}_i = \mathcal{C} \cap \langle p^i \rangle \subseteq p^i \, (\mathbb{Z}/p^s\mathbb{Z})^n \cong \left(\mathbb{Z}/p^{s-i}\mathbb{Z}\right)^n$$



- new maximal Lee weight in $\mathcal{C}_i$ is $M_i = \lfloor \frac{p^{s-i}}{2} \rfloor p^i$
- $\mathcal{C}_{s-1} \subseteq \mathcal{C}_{s-2} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathcal{C}$

$\rightarrow$ $d_L(\mathcal{C}) \leq d_L(\mathcal{C}_1) \leq \cdots \leq d_L(\mathcal{C}_{s-2}) \leq d_L(\mathcal{C}_{s-1})$

$$\mathcal{C}_{s-1} = \{xG \mid x \in p^{s-1}\mathbb{Z}/p^s\mathbb{Z}^{k_0} \times p^{s-2}\mathbb{Z}/p^s\mathbb{Z}^{k_1} \times \cdots \times \mathbb{Z}/p^s\mathbb{Z}^{k_{s-1}}\}$$

- $\mathcal{C}_{s-1}$ socle of $\mathcal{C}$
- $|\mathcal{C}_{s-1}| = p^{k_0 + k_1 + \cdots + k_{s-1}} = p^K$

$\rightarrow$ $\mathcal{C}_{s-1} \subseteq \mathbb{F}_p^n$ of dimension K

$$\begin{pmatrix} p^{s-1}\star \\ p^{s-2}\star \\ \vdots \\ \star \end{pmatrix} \begin{pmatrix} \mathrm{Id}_{k_0} & & & \star \\ 0 & p\mathrm{Id}_{k_1} & & p\star \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & p^{s-1}\mathrm{Id}_{k_{s-1}} & p^{s-1}\star \end{pmatrix}$$

What do we know?

Quite an old metric, but how much do we know?

What do we know?

Quite an old metric, but how much do we know?

$\mathbb{F}_q$ and Hamming metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $q \to \infty$ random codes attain the Singleton bound w.h.p.
- Many bounds: Hamming, Plotkin, Elias-Bassalygo, Griesmer, Johnson
- Characterizations and constructions for optimal codes

What do we know?

Quite an old metric, but how much do we know?

$\mathbb{F}_q$ and Hamming metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $q \to \infty$ random codes attain the Singleton bound w.h.p.
- Many bounds: Hamming, Plotkin, Elias-Bassalygo, Griesmer, Johnson
- Characterizations and constructions for optimal codes

$\mathbb{Z}/p^s\mathbb{Z}$ and Lee metric:

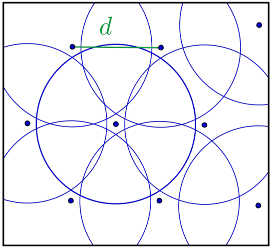
- If $n \to \infty$ do we know the d_L of a random code?
- If $p \to \infty$ do we know the d_L of a random code?
- Which bounds are known?
- Do we have characterizations and constructions for optimal codes?

Sphere covering and packing bounds

$A_H(q,n,d)$: largest size of code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of minimum distance $d = 2t+1$

Sphere covering/ Gilbert-Varshamov bound

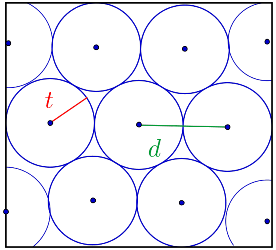
$$A_H(q,n,d) \geq \frac{q^n}{|B_H(q,n,d-1)|}$$



optimal codes are dense for $n \to \infty$

Sphere packing/ Hamming bound

$$A_H(q,n,d) \leq \frac{q^n}{|B_H(q,n,t)|}$$



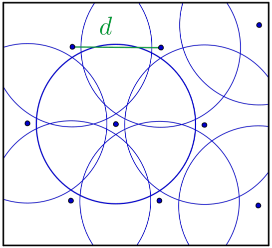
optimal codes: perfect codes

Lee-metric sphere covering and packing bounds

$A_L(p^s, n, d)$: largest size of code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of minimum Lee distance $d = 2t + 1$

Sphere covering/ Gilbert-Varshamov bound

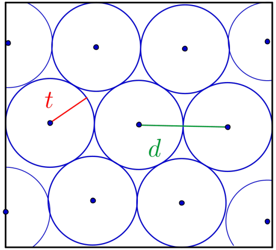
$$A_L(p^s, n, d) \geq \frac{p^{sn}}{|B_L(p^s, n, d-1)|}$$



optimal codes are dense for $n \to \infty$

Sphere packing/ Hamming bound

$$A_L(p^s, n, d) \leq \frac{p^{sn}}{|B_L(p^s, n, t)|}$$



optimal codes: perfect code

E. Byrne, A.-L. Horlemann, K. Khathuria, **V.W.** "Density of free modules over finite chain rings." Linear Algebra and its Applications, 2022

Golomb-Welch conjecture

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ with minimum Lee distance $d = 2t + 1$ is perfect

$\rightarrow$ for every $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$ there exists a unique $c \in \mathcal{C}$ with $d_L(x, c) \leq t$

Golomb-Welch Conjecture:

- weak version:
  There exists no perfect code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ for $n \geq 3$ with minimum Lee distance $5 \leq d \leq p^s$.
- strong version :
  There exists no perfect code $\mathcal{C} \subset \mathbb{Z}^n$ for $n \geq 3$ with minimum L1 distance $5 \leq d$.

S. Golomb, L. Welch. "Perfect codes in the Lee metric and the packing of polyominoes."SIAM Journal on Applied Mathematics, 1970

Golomb-Welch conjecture

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ with minimum Lee distance $d = 2t + 1$ is perfect

$\rightarrow$ for every $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$ there exists a unique $c \in \mathcal{C}$ with $d_L(x, c) \leq t$

Golomb-Welch Conjecture:

- weak version:
  There exists no perfect code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ for $n \geq 3$ with minimum Lee distance $5 \leq d \leq p^s$.
- strong version :
  There exists no perfect code $\mathcal{C} \subset \mathbb{Z}^n$ for $n \geq 3$ with minimum L1 distance $5 \leq d$.

S. Golomb, L. Welch. "Perfect codes in the Lee metric and the packing of polyominoes."SIAM Journal on Applied Mathematics, 1970

50 years later: How much do we know?

Golomb-Welch conjecture

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ with minimum Lee distance $d = 2t + 1$ is perfect

$\rightarrow$ for every $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$ there exists a unique $c \in \mathcal{C}$ with $d_L(x, c) \leq t$

Golomb-Welch Conjecture:

- weak version:
  There exists no perfect code $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ for $n \geq 3$ with minimum Lee distance $5 \leq d \leq p^s$.
- strong version :
  There exists no perfect code $\mathcal{C} \subset \mathbb{Z}^n$ for $n \geq 3$ with minimum L1 distance $5 \leq d$.

S. Golomb, L. Welch. "Perfect codes in the Lee metric and the packing of polyominoes."SIAM Journal on Applied Mathematics, 1970

50 years later: How much do we know?

- true for $n < (t+2)^2/2.1, t \geq 285$
- true for $n \geq 6, t \geq \frac{\sqrt{2}}{2} - \frac{3}{4}\sqrt{2} - \frac{1}{2}$

What do we know?

Quite an old metric, but how much do we know?

$\mathbb{F}_q$ and Hamming metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $q \to \infty$ random codes attain the Singleton bound w.h.p.
- Many bounds: Hamming, Plotkin, Elias-Bassalygo, Griesmer, Johnson
- Characterizations and constructions for optimal codes

$\mathbb{Z}/p^s\mathbb{Z}$ and Lee metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $p \to \infty$ do we know the d_L of a random code?
- Hamming, others?
- perfect codes, others?

The Singleton bound

- Hamming metric: Singleton 1964

→ Optimal codes: Maximum Distance Separable (MDS)

- MDS dense for $q \to \infty$
- MDS sparse for $n \to \infty$

R. Singleton. "Maximum distance q-nary codes.", IEEE Transactions on Information Theory, 1964.

B. Segre. "Curve razionali normali e k-archi negli spazi finiti.", Annali di Matematica Pura ed Applicata, 1955.

The Singleton bound

- Hamming metric: Singleton 1964

→ Optimal codes: Maximum Distance Separable (MDS)

- MDS dense for $q \to \infty$
- MDS sparse for $n \to \infty$

- Rank metric: Gabidulin 1985

→ Optimal codes: Maximum Rank Distance (MRD)

- $\mathbb{F}_{q^m}$-linear MRD dense for $m, q \to \infty$
- $\mathbb{F}_q$-linear MRD sparse for $q \to \infty$

R. Singleton. "Maximum distance q-nary codes.", IEEE Transactions on Information Theory, 1964.

B. Segre. "Curve razionali normali e k-archi negli spazi finiti.", Annali di Matematica Pura ed Applicata, 1955.

E. M. Gabidulin. "Theory of codes with maximum rank distance.", Problemy peredachi informatsii, 1985

A. Neri, A.-L. Horlemann, T. Randrianarisoa, J. Rosenthal. "On the genericity of maximum rank distance and Gabidulin codes.", Designs, Codes and Cryptography, 2018.

A. Gruica, A. Ravagnani. "Common complements of linear subspaces and the sparseness of MRD codes.", SIAM Journal on Applied Algebra and Geometry, 2022.

The Singleton bound

- Hamming metric: Singleton 1964

→ Optimal codes: Maximum Distance Separable (MDS)

- MDS dense for $q \to \infty$
- MDS sparse for $n \to \infty$

- Rank metric: Gabidulin 1985

→ Optimal codes: Maximum Rank Distance (MRD)

- $\mathbb{F}_{q^m}$-linear MRD dense for $m, q \to \infty$
- $\mathbb{F}_q$-linear MRD sparse for $q \to \infty$

- Lee metric: Shiromoto 2000

→ Optimal codes and their densities?

R. Singleton. "Maximum distance q-nary codes.", IEEE Transactions on Information Theory, 1964.

B. Segre. "Curve razionali normali e k-archi negli spazi finiti.", Annali di Matematica Pura ed Applicata, 1955.

E. M. Gabidulin. "Theory of codes with maximum rank distance.", Problemy peredachi informatsii, 1985

A. Neri, A.-L. Horlemann, T. Randrianarisoa, J. Rosenthal. "On the genericity of maximum rank distance and Gabidulin codes.", Designs, Codes and Cryptography, 2018.

A. Gruica, A. Ravagnani. "Common complements of linear subspaces and the sparseness of MRD codes.", SIAM Journal on Applied Algebra and Geometry, 2022.

K. Shiromoto "Singleton bounds for codes over finite rings.", Journal of Algebraic Combinatorics, 2000

The Singleton bound

Singleton bound:

For $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear code of minimum Hamming distance $d_H(\mathcal{C})$ has dimension:

$$k \leq n - d_H(\mathcal{C}) + 1$$

The Singleton bound

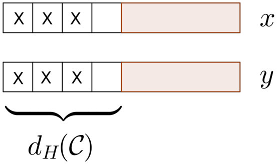
Singleton bound:
For $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear code of minimum Hamming distance $d_H(\mathcal{C})$ has dimension:

$$k \leq n - d_H(\mathcal{C}) + 1$$

- Puncture in $d_H(\mathcal{C}) - 1$ positions

$\rightarrow$ new code $\mid \mathcal{C}' \mid = \mid \mathcal{C} \mid$

$\rightarrow$ $\mathcal{C}' \subseteq \mathbb{F}_q^{n-(d_H(\mathcal{C})-1)}$



The Singleton bound

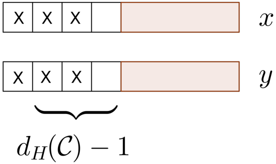
Singleton bound:
For $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear code of minimum Hamming distance $d_H(\mathcal{C})$ has dimension:

$$k \leq n - d_H(\mathcal{C}) + 1$$

- Puncture in $d_H(\mathcal{C}) - 1$ positions

$\rightarrow$ new code $\mid \mathcal{C}' \mid = \mid \mathcal{C} \mid$

$\rightarrow$ $\mathcal{C}' \subseteq \mathbb{F}_q^{n-(d_H(\mathcal{C})-1)}$



The Singleton bound

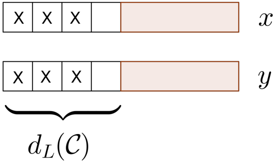
Lee-metric Singleton bound:
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code of minimum Lee distance $d_L(\mathcal{C})$ has type:

$$k \leq n - \left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor$$

- Puncture in $\left\lfloor \frac{d_L(\mathcal{C})-1}{M} \right\rfloor$ positions

$\rightarrow$ new code $\mid \mathcal{C}' \mid = \mid \mathcal{C} \mid$

$\rightarrow$ $\mathcal{C}' \subseteq (\mathbb{Z}/p^s\mathbb{Z})^{n - \left\lfloor \frac{d_L(\mathcal{C})-1}{M} \right\rfloor}$



K. Shiromoto "Singleton bounds for codes over finite rings.", Journal of Algebraic Combinatorics, 2000

The Singleton bound

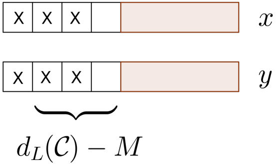
Lee-metric Singleton bound:
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code of minimum Lee distance $d_L(\mathcal{C})$ has type:

$$k \leq n - \left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor$$

- Puncture in $\left\lfloor \frac{d_L(\mathcal{C})-1}{M} \right\rfloor$ positions

$\rightarrow$ new code $\mid \mathcal{C}' \mid = \mid \mathcal{C} \mid$

$\rightarrow$ $\mathcal{C}' \subseteq (\mathbb{Z}/p^s\mathbb{Z})^{n - \left\lfloor \frac{d_L(\mathcal{C})-1}{M} \right\rfloor}$



K. Shiromoto "Singleton bounds for codes over finite rings.", Journal of Algebraic Combinatorics, 2000

Optimal codes

Lee-metric Singleton bound:
$\mathcal{C}$ length n, type k, $M = \lfloor \frac{p^s}{2} \rfloor$:

$$k \leq n - \left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor$$

Example:
$\mathcal{C} = \langle (1, 2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$

$$1 = 2 - \left\lfloor \frac{3 - 1}{2} \right\rfloor$$

Optimal codes

Lee-metric Singleton bound:

$\mathcal{C}$ length n, type k, $M = \lfloor \frac{p^s}{2} \rfloor$:

$$k \leq n - \left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor$$

Example:

$\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$

$$1 = 2 - \left\lfloor \frac{3-1}{2} \right\rfloor$$

This is the **only** linear non-trivial optimal code!

E. Byrne, **V.W.** "Bounds in the Lee metric and optimal codes.", Finite Fields and Their Applications, 2022

Optimal codes

Lee-metric Singleton bound:
$\mathcal{C}$ length n, type k, $M = \lfloor \frac{p^s}{2} \rfloor$:

$$k \leq n - \left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor$$

Example:
$\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$

$$1 = 2 - \left\lfloor \frac{3-1}{2} \right\rfloor$$

This is the **only** linear non-trivial optimal code!

E. Byrne, **V.W.** "Bounds in the Lee metric and optimal codes.", Finite Fields and Their Applications, 2022

Many bounds are derived from classical arguments

$\rightarrow$ Need new techniques!

Other Singleton bounds

Maximum Distance with respect to Rank (MDR)

For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code with rank K:

$$d_H(\mathcal{C}) \leq n - K + 1 \qquad (\leq n - k + 1)$$

S. Dougherty, K. Shiromoto. "MDR codes over $\mathbb{Z}_k$.", IEEE TIT, 2000

Other Singleton bounds

Maximum Distance with respect to Rank (MDR)

For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code with rank K:

$$d_H(\mathcal{C}) \leq n - K + 1 \qquad (\leq n - k + 1)$$

S. Dougherty, K. Shiromoto. “MDR codes over $\mathbb{Z}_k$.”, IEEE TIT, 2000

$$d_H(\mathcal{C}) \leq d_H(\mathcal{C}_{s-1}) \leq n - K + 1 \qquad \mathcal{C}_{s-1} \subseteq \mathbb{F}_p^n \text{ dimension } K$$

optimal codes: dense for $p \to \infty$, sparse for $n \to \infty$

Other Singleton bounds

Maximum Distance with respect to Rank (MDR)

For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code with rank K:

$$d_H(\mathcal{C}) \leq n - K + 1 \qquad (\leq n - k + 1)$$

S. Dougherty, K. Shiromoto. "MDR codes over $\mathbb{Z}_k$.", IEEE TIT, 2000

$$d_H(\mathcal{C}) \leq d_H(\mathcal{C}_{s-1}) \leq n - K + 1 \qquad \mathcal{C}_{s-1} \subseteq \mathbb{F}_p^n \text{ dimension } K$$

optimal codes: dense for $p \to \infty$, sparse for $n \to \infty$

- $\to$ can do the same to get $d_L(\mathcal{C}) \leq M(n - K + 1)$
- ∘ for $1 < k < n$ integer Alderson-Huntemann: $d_L(\mathcal{C}) \leq M(n - k)$
- $\to$ full characterization and only few optimal codes exist
- $\to$ always sparse for n or $p \to \infty$

T. Alderson, S. Huntemann. "On maximum Lee distance codes.", Journal of Discrete Mathematics, 2013

Generalized Hamming weights

J. Bariffi, **V.W.** "Better bounds on the minimal Lee distance.", 2023

Support and weight of code:

$x \in \mathbb{F}_q^n :$ $\quad \mathrm{supp}_H(x) = \{i \in \{1, \dots, n\} \mid x_i \neq 0\} \quad \longrightarrow \mathrm{wt}_H(x) = |\mathrm{supp}_H(x)|$

$\mathcal{C} \subseteq \mathbb{F}_q^n :$ $\quad \mathrm{supp}_H(\mathcal{C}) = \{i \in \{1, \dots, n\} \mid \exists x \in \mathcal{C} : x_i \neq 0\} \quad \longrightarrow \mathrm{wt}_H(\mathcal{C}) = |\mathrm{supp}_H(\mathcal{C})|$

Generalized Hamming weights

J. Bariffi, **V.W.** "Better bounds on the minimal Lee distance.", 2023

Support and weight of code:

$x \in \mathbb{F}_q^n :$ $\quad \mathrm{supp}_H(x) = \{i \in \{1, \dots, n\} \mid x_i \neq 0\}$ $\quad \longrightarrow \mathrm{wt}_H(x) = |\mathrm{supp}_H(x)|$

$\mathcal{C} \subseteq \mathbb{F}_q^n :$ $\quad \mathrm{supp}_H(\mathcal{C}) = \{i \in \{1, \dots, n\} \mid \exists x \in \mathcal{C} : x_i \neq 0\}$ $\quad \longrightarrow \mathrm{wt}_H(\mathcal{C}) = |\mathrm{supp}_H(\mathcal{C})|$

Generalized weights:

$\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k. For all $r \in \{1, \dots, k\}$:

$$d_H^r(\mathcal{C}) = \min\{\mathrm{wt}_H(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of dimension } r\}$$

Generalized Hamming weights

J. Bariffi, **V.W.** "Better bounds on the minimal Lee distance.", 2023

Support and weight of code:

$x \in \mathbb{F}_q^n$: $\quad \mathrm{supp}_H(x) = \{i \in \{1, \dots, n\} \mid x_i \neq 0\} \quad \longrightarrow \mathrm{wt}_H(x) = |\mathrm{supp}_H(x)|$

$\mathcal{C} \subseteq \mathbb{F}_q^n$: $\quad \mathrm{supp}_H(\mathcal{C}) = \{i \in \{1, \dots, n\} \mid \exists x \in \mathcal{C} : x_i \neq 0\} \quad \longrightarrow \mathrm{wt}_H(\mathcal{C}) = |\mathrm{supp}_H(\mathcal{C})|$

Generalized weights:

$\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k. For all $r \in \{1, \dots, k\}$:

$$d_H^r(\mathcal{C}) = \min\{\mathrm{wt}_H(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of dimension } r\}$$

Example:

$\mathcal{C} \subseteq \mathbb{F}_2^4$ generated by $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

$$d_H^1(\mathcal{C}) = 1$$
$$d_H^2(\mathcal{C}) = 3$$
$$d_H^3(\mathcal{C}) = 4$$

Generalized Hamming weights

J. Bariffi, **V.W.** "Better bounds on the minimal Lee distance.", 2023

Support and weight of code:

$x \in \mathbb{F}_q^n$: $\mathrm{supp}_H(x) = \{i \in \{1, \dots, n\} \mid x_i \neq 0\}$ $\longrightarrow \mathrm{wt}_H(x) = |\mathrm{supp}_H(x)|$

$\mathcal{C} \subseteq \mathbb{F}_q^n$: $\mathrm{supp}_H(\mathcal{C}) = \{i \in \{1, \dots, n\} \mid \exists x \in \mathcal{C} : x_i \neq 0\}$ $\longrightarrow \mathrm{wt}_H(\mathcal{C}) = |\mathrm{supp}_H(\mathcal{C})|$

Generalized weights:

$\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k. For all $r \in \{1, \dots, k\}$:

$$d_H^r(\mathcal{C}) = \min\{\mathrm{wt}_H(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of dimension } r\}$$

Properties:

- $d_H(\mathcal{C}) = d_H^1(\mathcal{C})$
- $d_H^r(\mathcal{C}) < d_H^{r+1}(\mathcal{C})$ for $r < k$
- $d_H^k(\mathcal{C}) = \mathrm{wt}_H(\mathcal{C})$

$\rightarrow d_H(\mathcal{C}) = \underbrace{d_H^1(\mathcal{C}) < d_H^2(\mathcal{C}) < \cdots < d_H^k(\mathcal{C})}_{k-1} = \mathrm{wt}_H(\mathcal{C}) \rightarrow$ Singleton Bound: $d_H(\mathcal{C}) \leq n-k+1$

Generalizations to Lee metric

- over $\mathbb{Z}/4\mathbb{Z}$ S. Dougherty, M. Gupta, K. Shiromoto. "On Generalized weights for codes over finite rings.", 2002

Generalizations to Lee metric

- over $\mathbb{Z}/4\mathbb{Z}$ S. Dougherty, M. Gupta, K. Shiromoto. "On Generalized weights for codes over finite rings.", 2002

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Generalizations to Lee metric

- over $\mathbb{Z}/4\mathbb{Z}$ S. Dougherty, M. Gupta, K. Shiromoto. "On Generalized weights for codes over finite rings.", 2002

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

- using the **join Lee support**

$$\mathrm{supp}_L(x) = (\mathrm{wt}_L(x_1), \dots, \mathrm{wt}_L(x_n)) = s, \ \mid s \mid = \sum s_i$$

$$\mathrm{wt}_L(\mathcal{C}) = \mid \bigvee_{c \in \mathcal{C}} \mathrm{supp}_L(c) \mid = \sum_{i=1}^n \max\{\mathrm{wt}_L(c_i) \mid c \in \mathcal{C}\}$$

$\longrightarrow$ Resulting Bound $\quad d_L(\mathcal{C}) \leq \lfloor \frac{p}{2} \rfloor p^{s-1}(n - K + 1)$

Generalizations to Lee metric

- over $\mathbb{Z}/4\mathbb{Z}$ S. Dougherty, M. Gupta, K. Shiromoto. "On Generalized weights for codes over finite rings.", 2002

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

- using the **join Lee support**

$$\mathrm{supp}_L(x) = (\mathrm{wt}_L(x_1), \dots, \mathrm{wt}_L(x_n)) = s, \ \mid s \mid = \sum s_i$$

$$\mathrm{wt}_L(\mathcal{C}) = \mid \bigvee_{c \in \mathcal{C}} \mathrm{supp}_L(c) \mid = \sum_{i=1}^n \max\{\mathrm{wt}_L(c_i) \mid c \in \mathcal{C}\}$$

$\longrightarrow$ Resulting Bound $\quad d_L(\mathcal{C}) \leq \lfloor \frac{p}{2} \rfloor p^{s-1}(n-K+1)$

- using the **column Lee weight**

$$\mathrm{colwt}_L(a_1^\top \cdots a_n^\top) = |(\max \mathrm{supp}_L(a_1), \dots, \max \mathrm{supp}_L(a_n))|$$

$$\mathrm{wt}_L(\mathcal{C}) = \min\{\mathrm{colwt}_L(G) \mid \langle G \rangle = \mathcal{C}\}$$

$\longrightarrow$ Resulting bound

$$d_L(\mathcal{C}) \leq \sum_{i=0}^{s-1} p^i k_i + \sum_{i=0}^{s-1} \mu_i M_i - \sum_{i=0}^{\sigma-1} \left(\sum_{j=0}^{i} k_j \right) \lfloor \tfrac{p}{2} \rfloor p^i - (k_\sigma - 1)p^\sigma$$

Generalizations to Lee metric

- over $\mathbb{Z}/4\mathbb{Z}$ S. Dougherty, M. Gupta, K. Shiromoto. "On Generalized weights for codes over finite rings.", 2002

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \ldots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Very few optimal codes

- using the **join Lee support**

$$\mathrm{supp}_L(x) = (\mathrm{wt}_L(x_1), \ldots, \mathrm{wt}_L(x_n)) = s, \ \mid s \mid = \sum s_i$$

$$\mathrm{wt}_L(\mathcal{C}) = \mid \bigvee_{c \in \mathcal{C}} \mathrm{supp}_L(c) \mid = \sum_{i=1}^n \max\{\mathrm{wt}_L(c_i) \mid c \in \mathcal{C}\}$$

→ Resulting Bound

$$d_L(\mathcal{C}) \leq \lfloor \tfrac{p}{2} \rfloor p^{s-1}(n - K + 1)$$

- using the **column Lee weight**

$$\mathrm{colwt}_L(a_1^\top \cdots a_n^\top) = |(\max \mathrm{supp}_L(a_1), \ldots, \max \mathrm{supp}_L(a_n))|$$

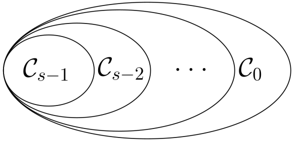
$$\mathrm{wt}_L(\mathcal{C}) = \min\{\mathrm{colwt}_L(G) \mid \langle G \rangle = \mathcal{C}\}$$

→ Resulting bound

$$d_L(\mathcal{C}) \leq \sum_{i=0}^{s-1} p^i k_i + \sum_{i=0}^{s-1} \mu_i M_i - \sum_{i=0}^{\sigma-1} \left(\sum_{j=0}^{i} k_j \right) \lfloor \tfrac{p}{2} \rfloor p^i - (k_\sigma - 1) p^\sigma$$

Filtration bound

Filtration:
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, define for all $i \in \{0, \ldots, s-1\}$: $\quad \mathcal{C}_i = \mathcal{C} \cap \langle p^i \rangle$
maximal Lee weight in $\mathcal{C}_i$ is $M_i = \lfloor \frac{p^{s-i}}{2} \rfloor p^i$

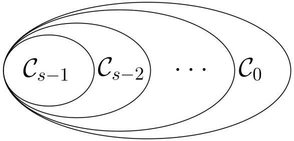


$$\mathcal{C}_{s-1} \subseteq \mathcal{C}_{s-2} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathcal{C}$$

$$\rightarrow d_L(\mathcal{C}) \leq d_L(\mathcal{C}_1) \leq \cdots \leq d_L(\mathcal{C}_{s-2}) \leq d_L(\mathcal{C}_{s-1})$$

Filtration bound

Filtration:
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, define for all $i \in \{0, \dots, s-1\}$: $\mathcal{C}_i = \mathcal{C} \cap \langle p^i \rangle$
maximal Lee weight in $\mathcal{C}_i$ is $M_i = \lfloor \frac{p^{s-i}}{2} \rfloor p^i$



$$\mathcal{C}_{s-1} \subseteq \mathcal{C}_{s-2} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathcal{C}$$

$$\to d_L(\mathcal{C}) \leq d_L(\mathcal{C}_1) \leq \cdots \leq d_L(\mathcal{C}_{s-2}) \leq d_L(\mathcal{C}_{s-1})$$

New Lee-metric Singleton bound:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, subtype $(k_0, \dots, k_\sigma)$, ℓ: max prime power $\ell \neq \sigma, s$ in G, appears n' times:

$$d_L(\mathcal{C}) \leq p^{s-\ell+\sigma} + (n - K - n')\lfloor \frac{p^{\ell-\sigma}}{2} \rfloor p^{s-\ell+\sigma}$$

Examples

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

$\mathbb{Z}/9\mathbb{Z}, \quad d_L(\langle G_1 \rangle) = 3$

- Shiromoto: $d_L \leq 5$
- Join: $d_L \leq 6$
- Column weight: $d_L \leq 5$
- Filtration: $d_L \leq 3$

Examples

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 1 & 10 & 4 & 20 & 9 \\ 0 & 3 & 9 & 18 & 9 \end{pmatrix}$$

$\mathbb{Z}/9\mathbb{Z}, \quad d_L(\langle G_1 \rangle) = 3$

- Shiromoto: $d_L \leq 5$
- Join: $d_L \leq 6$
- Column weight: $d_L \leq 5$
- Filtration: $d_L \leq 3$

$\mathbb{Z}/27\mathbb{Z}, \quad d_L(\langle G_2 \rangle) = 9$

- Shiromoto: $d_L \leq 40$
- Join: $d_L \leq 36$
- Column weight: $d_L \leq 38$
- Filtration: $d_L \leq 9$

Examples

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

$\mathbb{Z}/9\mathbb{Z}, \quad d_L(\langle G_1 \rangle) = 3$

- Shiromoto: $d_L \leq 5$
- Join: $d_L \leq 6$
- Column weight: $d_L \leq 5$
- Filtration: $d_L \leq 3$

$$G_2 = \begin{pmatrix} 1 & 10 & 4 & 20 & 9 \\ 0 & 3 & 9 & 18 & 9 \end{pmatrix}$$

$\mathbb{Z}/27\mathbb{Z}, \quad d_L(\langle G_2 \rangle) = 9$

- Shiromoto: $d_L \leq 40$
- Join: $d_L \leq 36$
- Column weight: $d_L \leq 38$
- Filtration: $d_L \leq 9$

$$G_3 = \begin{pmatrix} 1 & 0 & 25 & 50 & 75 & 100 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\mathbb{Z}/125\mathbb{Z}, \quad d_L(\langle G_3 \rangle) = 5$

- Shiromoto: $d_L \leq 249$
- Join: $d_L \leq 200$
- Column weight: $d_L \leq 247$
- Filtration: $d_L \leq 5$

Examples

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 4 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 1 & 10 & 4 & 20 & 9 \\ 0 & 3 & 9 & 18 & 9 \end{pmatrix} \qquad G_3 = \begin{pmatrix} 1 & 0 & 25 & 50 & 75 & 100 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\mathbb{Z}/9\mathbb{Z}, \quad d_L(\langle G_1 \rangle) = 3$

- Shiromoto: $d_L \leq 5$
- Join: $d_L \leq 6$
- Column weight: $d_L \leq 5$
- Filtration: $d_L \leq 3$

$\mathbb{Z}/27\mathbb{Z}, \quad d_L(\langle G_2 \rangle) = 9$

- Shiromoto: $d_L \leq 40$
- Join: $d_L \leq 36$
- Column weight: $d_L \leq 38$
- Filtration: $d_L \leq 9$

$\mathbb{Z}/125\mathbb{Z}, \quad d_L(\langle G_3 \rangle) = 5$

- Shiromoto: $d_L \leq 249$
- Join: $d_L \leq 200$
- Column weight: $d_L \leq 247$
- Filtration: $d_L \leq 5$

Are the optimal codes dense?

Examples

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

$\mathbb{Z}/9\mathbb{Z}, \quad d_L(\langle G_1 \rangle) = 3$

- Shiromoto: $d_L \leq 5$
- Join: $d_L \leq 6$
- Column weight: $d_L \leq 5$
- Filtration: $d_L \leq 3$

$$G_2 = \begin{pmatrix} 1 & 10 & 4 & 20 & 9 \\ 0 & 3 & 9 & 18 & 9 \end{pmatrix}$$

$\mathbb{Z}/27\mathbb{Z}, \quad d_L(\langle G_2 \rangle) = 9$

- Shiromoto: $d_L \leq 40$
- Join: $d_L \leq 36$
- Column weight: $d_L \leq 38$
- Filtration: $d_L \leq 9$

$$G_3 = \begin{pmatrix} 1 & 0 & 25 & 50 & 75 & 100 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\mathbb{Z}/125\mathbb{Z}, \quad d_L(\langle G_3 \rangle) = 5$

- Shiromoto: $d_L \leq 249$
- Join: $d_L \leq 200$
- Column weight: $d_L \leq 247$
- Filtration: $d_L \leq 5$

Are the optimal codes dense? NO

Examples

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 4 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 1 & 10 & 4 & 20 & 9 \\ 0 & 3 & 9 & 18 & 9 \end{pmatrix} \qquad G_3 = \begin{pmatrix} 1 & 0 & 25 & 50 & 75 & 100 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\mathbb{Z}/9\mathbb{Z}, \quad d_L(\langle G_1 \rangle) = 3$

- Shiromoto: $d_L \leq 5$
- Join: $d_L \leq 6$
- Column weight: $d_L \leq 5$
- Filtration: $d_L \leq 3$

$\mathbb{Z}/27\mathbb{Z}, \quad d_L(\langle G_2 \rangle) = 9$

- Shiromoto: $d_L \leq 40$
- Join: $d_L \leq 36$
- Column weight: $d_L \leq 38$
- Filtration: $d_L \leq 9$

$\mathbb{Z}/125\mathbb{Z}, \quad d_L(\langle G_3 \rangle) = 5$

- Shiromoto: $d_L \leq 249$
- Join: $d_L \leq 200$
- Column weight: $d_L \leq 247$
- Filtration: $d_L \leq 5$

Are the optimal codes dense? NO

Open Problem:
Find a tighter Lee-metric Singleton bound, for which optimal codes are dense

What do we know?

Quite an old metric, but how much do we know?

$\mathbb{F}_q$ and Hamming metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $q \to \infty$ random codes attain the Singleton bound w.h.p.
- Many bounds: Hamming, Plotkin, Elias-Bassalygo, Griesmer, Johnson
- Characterizations and constructions for optimal codes

$\mathbb{Z}/p^s\mathbb{Z}$ and Lee metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $p \to \infty$ we still do not know the d_L of a random code
- Hamming, others?
- perfect, others?

Plotkin bound

Plotkin bound

$\mathcal{C} \subset \mathbb{F}_q^n$ has minimum Hamming distance

$$d_H(\mathcal{C}) \leq \frac{|\mathcal{C}|}{|\mathcal{C}|-1} n \frac{q-1}{q}.$$

- Weight of non-zero codeword is at least $d_H(\mathcal{C})$:

$$(|\mathcal{C}|-1) d_H(\mathcal{C}) \leq \sum_{c \in \mathcal{C}} \mathrm{wt}_H(c)$$

- average weight of code

$$\overline{\mathrm{wt}}_H(\mathcal{C}) = \frac{1}{|\mathcal{C}|} \sum_{c \in \mathcal{C}} \mathrm{wt}_H(c) \leq \overline{\mathrm{wt}}_H(\mathbb{F}_q^n)$$

- additive weight

$$\overline{\mathrm{wt}}_H(\mathbb{F}_q^n) = n \overline{\mathrm{wt}}_H(\mathbb{F}_q) = n \frac{q-1}{q}$$

Plotkin bound

Plotkin bound

$\mathcal{C} \subset \mathbb{F}_q^n$ has minimum Hamming distance

$$d_H(\mathcal{C}) \leq \frac{|\mathcal{C}|}{|\mathcal{C}|-1} n \frac{q-1}{q}.$$

- Weight of non-zero codeword is at least $d_H(\mathcal{C})$:

$$(|\mathcal{C}|-1) d_H(\mathcal{C}) \leq \sum_{c \in \mathcal{C}} \mathrm{wt}_H(c)$$

- average weight of code

$$\overline{\mathrm{wt}}_H(\mathcal{C}) = \frac{1}{|\mathcal{C}|} \sum_{c \in \mathcal{C}} \mathrm{wt}_H(c) \leq \overline{\mathrm{wt}}_H(\mathbb{F}_q^n)$$

- additive weight

$$\overline{\mathrm{wt}}_H(\mathbb{F}_q^n) = n \overline{\mathrm{wt}}_H(\mathbb{F}_q) = n \frac{q-1}{q}$$

optimal codes: constant Hamming weight codes $\to$ ℓ-fold duplicates of simplex code

Lee-metric Plotkin bound

Plotkin bound

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ has minimum Lee distance

$$d_L \leq \frac{|\mathcal{C}|}{|\mathcal{C}|-1} n D_L = n D_L \frac{1}{1-p^{-sk}}.$$

- average Lee weight in $\mathbb{Z}/p^s\mathbb{Z}$:

$$D_L = \begin{cases} \frac{p^{2s}-1}{4p^s} & \text{if } p \neq 2 \\ 2^{s-2} & \text{if } p = 2 \end{cases}$$

R. Graham, A. Wyner. "An upper bound on the minimum distance for a q-ary code.", Information and Control, 1968

Lee-metric Plotkin bound

Plotkin bound

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ has minimum Lee distance

$$d_L \leq \frac{|\mathcal{C}|}{|\mathcal{C}|-1} nD_L = nD_L \frac{1}{1-p^{-sk}}.$$

- average Lee weight in $\mathbb{Z}/p^s\mathbb{Z}$:

$$D_L = \begin{cases} \frac{p^{2s}-1}{4p^s} & \text{if } p \neq 2 \\ 2^{s-2} & \text{if } p = 2 \end{cases}$$

R. Graham, A. Wyner. "An upper bound on the minimum distance for a q-ary code.", Information and Control, 1968

Plotkin bound

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ has minimum Lee distance

$$d_L(\mathcal{C}) \leq (n - k_0 + 1) D_L \frac{1}{1-p^{-s}}.$$

J. Chiang, J. Wolf. "On channels and codes for the Lee metric.", Information and Control, 1971

Lee-metric Plotkin bound

Plotkin bound

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ has minimum Lee distance

$$d_L \leq \frac{|\mathcal{C}|}{|\mathcal{C}|-1} n D_L = n D_L \frac{1}{1-p^{-sk}}.$$

- average Lee weight in $\mathbb{Z}/p^s\mathbb{Z}$:

$$D_L = \begin{cases} \frac{p^{2s}-1}{4p^s} & \text{if } p \neq 2 \\ 2^{s-2} & \text{if } p = 2 \end{cases}$$

R. Graham, A. Wyner. "An upper bound on the minimum distance for a q-ary code.", Information and Control, 1968

Plotkin bound

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ has minimum Lee distance

$$d_L(\mathcal{C}) \leq (n - k_0 + 1) D_L \frac{1}{1-p^{-s}}.$$

using $d_L(\mathcal{C}) \leq d_L(\langle c \rangle)$

J. Chiang, J. Wolf. "On channels and codes for the Lee metric.", Information and Control, 1971

Improvements

Support subtype

$\mathcal{C}$ has **support subtype** $(n_0, \ldots, n_s)$:

$$n_i(\mathcal{C}) = |\{j \in \{1, \ldots, n\} \mid \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|$$

for π_j projection on jth coordinate

Improvements

Support subtype

$\mathcal{C}$ has **support subtype** $(n_0, \dots, n_s)$:

$$n_i(\mathcal{C}) = |\{j \in \{1, \dots, n\} \mid \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|$$

for π_j projection on jth coordinate

Example

$\mathcal{C} \subset \mathbb{Z}/8\mathbb{Z}^5$ generated by

$$G = \begin{pmatrix} 1 & 3 & 5 & 0 & 2 \\ 0 & 2 & 4 & 2 & 6 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 4 & 4 \end{pmatrix}$$

has subtype $(1, 1, 2)$ and support subtype $(3, 2, 0, 0)$

Improvements

Support subtype

$\mathcal{C}$ has **support subtype** $(n_0, \dots, n_s)$:

$$n_i(\mathcal{C}) = |\{j \in \{1, \dots, n\} \mid \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|$$

for π_j projection on jth coordinate

Example

$\mathcal{C} \subset \mathbb{Z}/8\mathbb{Z}^5$ generated by

$$G = \begin{pmatrix} 1 & 3 & 5 & 0 & 2 \\ 0 & 2 & 4 & 2 & 6 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 4 & 4 \end{pmatrix}$$

has subtype $(1, 1, 2)$ and support subtype $(3, 2, 0, 0)$

Improvements

Support subtype

$\mathcal{C}$ has **support subtype** $(n_0, \dots, n_s)$:

$$n_i(\mathcal{C}) = |\{j \in \{1, \dots, n\} \mid \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|$$

for π_j projection on jth coordinate

Example

$\mathcal{C} \subset \mathbb{Z}/8\mathbb{Z}^5$ generated by

$$G = \begin{pmatrix} 1 & 3 & 5 & 0 & 2 \\ 0 & 2 & 4 & 2 & 6 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 4 & 4 \end{pmatrix}$$

has subtype $(1, 1, 2)$ and support subtype $(3, 2, 0, 0)$

Improvements

$$\overline{\mathrm{wt}}_L(\mathcal{C}) \leq nD_L = n \begin{cases} \frac{p^{2s}-1}{4p^s} & \text{if } p \neq 2 \\ 2^{s-2} & \text{if } p = 2 \end{cases} \quad \rightarrow \quad \overline{\mathrm{wt}}_L(\mathcal{C}) = \begin{cases} \left(p^{2s}n - \sum_{i=0}^{s-1} p^{2i} n_i\right)/4p^s & \text{if } p \neq 2 \\ 2^{s-2}n & \text{if } p = 2 \end{cases}$$

Plotkin bound

$\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ has minimum Lee distance

$$\left\lfloor \frac{d_L - 1}{A} \right\rfloor \leq n - K \quad \text{for} \quad A = \begin{cases} p^{s-1}(p+1)/4 & \text{if } p \neq 2 \\ 2^{s-1} & \text{if } p = 2 \end{cases}$$

E. Byrne, **V.W.** "Bounds in the Lee metric and optimal codes.", Finite Fields and Their Applications, 2022

optimal codes: constant Lee weight codes

- characterization and construction by Wood for $s = 1$ or $p = 2$
- else $K \leq 2$: finished construction

J. Wood. "The structure of linear codes of constant weight.", Transactions of the American Mathematical Society, 2002

Other bounds

- MacWilliams identity not possible in Lee metric

→ No Linear Programming bound

- Elias-Bassalygo bound

→ and improvements

- Griesmer bound

→ only over $\mathbb{Z}/4\mathbb{Z}$

A. Noha, J. Wood. "Failure of the MacWilliams identities for the Lee weight enumerator over $\mathbb{Z}/m\mathbb{Z}, m \geq 5$.", Discrete Mathematics , 2020

T. Lepistö. "A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric.", Information and Control, 1981

J. Astola. "An Elias-type bound for Lee codes over large alphabets and its application to perfect codes.", IEEE TIT, 1982.

A. Ashikhmin. "On generalized Hamming weights for Galois ring linear codes.", Designs, Codes and Cryptography, 1998.

Open Problems:

- Improve existing bounds
- Generalize bounds to any $\mathbb{Z}/p^s\mathbb{Z}$
- Johnson bound?
- Other bounds?

What do we know?

Quite an old metric, but how much do we know?

$\mathbb{F}_q$ and Hamming metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $q \to \infty$ random codes attain the Singleton bound w.h.p.
- Many bounds: Hamming, Plotkin, Elias-Bassalygo, Griesmer, Johnson
- Characterizations and constructions for optimal codes

$\mathbb{Z}/p^s\mathbb{Z}$ and Lee metric:

- If $n \to \infty$ random codes attain the Gilbert-Varshamov bound w.h.p.
- If $p \to \infty$ we still do not know the d_L of a random code
- Hamming, Plotkin, Elias-Bassalygo, Griesmer over $\mathbb{Z}/4\mathbb{Z}$, no Johnson
- perfect codes, constant Lee weight, others?

Questions?

Summary:

- Many Lee-metric bounds only exist over $\mathbb{Z}/4\mathbb{Z}$
- Many bounds obtained by classic arguments

$\rightarrow$ Need new techniques to generalize and get tighter bounds

Questions?

Summary:

- Many Lee-metric bounds only exist over $\mathbb{Z}/4\mathbb{Z}$
- Many bounds obtained by classic arguments

$\rightarrow$ Need new techniques to generalize and get tighter bounds

Thank you!

Generalized Filtration Weight

$$\mathcal{C} = \langle G_{sys} \rangle$$

$$\max \sigma : \quad k_\sigma \neq 0$$

$$G_{sys} = \begin{pmatrix} \mathrm{Id}_{k_1} & & & & \star \\ 0 & p\mathrm{Id}_{k_2} & & & p\star \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & p^\sigma \mathrm{Id}_{k_\sigma} & p^\sigma \star \end{pmatrix}$$

Generalized Filtration Weight

$$\mathcal{C} = \langle G_{sys} \rangle$$

$$\max \sigma : \quad k_\sigma \neq 0$$

$$\downarrow$$

$$\mathcal{C}_\sigma$$

$$G_{sys} = \begin{pmatrix} \mathrm{Id}_{k_1} & & & \star \\ 0 & p\mathrm{Id}_{k_2} & & p\star \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & p^\sigma \mathrm{Id}_{k_\sigma} & p^\sigma \star \end{pmatrix}$$

$$\downarrow$$

$$G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix}$$

Generalized Filtration Weight

$$\mathcal{C} = \langle G_{sys} \rangle$$

$$\max \sigma : \quad k_\sigma \neq 0$$

$$\downarrow$$

$$\mathcal{C}_\sigma$$

ℓ : max prime power in $p^\sigma A_\sigma$

$$G_{sys} = \begin{pmatrix} \mathrm{Id}_{k_1} & & & & \star \\ 0 & p\mathrm{Id}_{k_2} & & & p\star \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & p^\sigma \mathrm{Id}_{k_\sigma} & p^\sigma \star \end{pmatrix}$$

$$\downarrow$$

$$G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix}$$

n': max number of p^ℓ in one row

Generalized Filtration Weight

$$\mathcal{C} = \langle G_{sys} \rangle$$

$$\max \sigma : \quad k_\sigma \neq 0$$

$$G_{sys} = \begin{pmatrix} \mathrm{Id}_{k_1} & & & & \star \\ 0 & p\mathrm{Id}_{k_2} & & & p\star \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & p^\sigma \mathrm{Id}_{k_\sigma} & p^\sigma \star \end{pmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\mathcal{C}_\sigma \qquad\qquad G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix}$$

ℓ : max prime power in $p^\sigma A_\sigma$

n': max number of p^ℓ in one row

1. If $\ell = \sigma$ $\quad\rightarrow\quad$ $d_L(\mathcal{C}_\sigma) \leq p^\sigma + (n-K)M_\sigma$

Generalized Filtration Weight

$$\mathcal{C} = \langle G_{sys} \rangle$$

$$\max \sigma : \quad k_\sigma \neq 0$$

$$G_{sys} = \begin{pmatrix} \mathrm{Id}_{k_1} & & & \star \\ 0 & p\mathrm{Id}_{k_2} & & p\star \\ \vdots & & \ddots & \vdots \\ 0 & 0 & p^\sigma \mathrm{Id}_{k_\sigma} & p^\sigma \star \end{pmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\mathcal{C}_\sigma \qquad\qquad G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix}$$

ℓ : max prime power in $p^\sigma A_\sigma$

n': max number of p^ℓ in one row

1. If $\ell = \sigma$ $\rightarrow$ $d_L(\mathcal{C}_\sigma) \leq p^\sigma + (n-K)M_\sigma$
2. If $\ell = s$ $\rightarrow$ $d_L(\mathcal{C}_\sigma) \leq p^\sigma + (n-K-n')M_\sigma$

Generalized Filtration Weight

$$\mathcal{C} = \langle G_{sys} \rangle$$

$$\max \sigma : \quad k_\sigma \neq 0$$

$$G_{sys} = \begin{pmatrix} \mathrm{Id}_{k_1} & & & \star \\ 0 & p\mathrm{Id}_{k_2} & & p\star \\ \vdots & & \ddots & \vdots \\ 0 & 0 & p^\sigma \mathrm{Id}_{k_\sigma} & p^\sigma \star \end{pmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\mathcal{C}_\sigma \qquad\qquad G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix}$$

ℓ : max prime power in $p^\sigma A_\sigma$

n': max number of p^ℓ in one row

1. If $\ell = \sigma$ $\quad\rightarrow\quad$ $d_L(\mathcal{C}_\sigma) \leq p^\sigma + (n-K)M_\sigma$
2. If $\ell = s$ $\quad\rightarrow\quad$ $d_L(\mathcal{C}_\sigma) \leq p^\sigma + (n-K-n')M_\sigma$
3. If $\ell \neq \sigma, \ell \neq s$ $\quad\rightarrow\quad$ go to $\mathcal{C}_{s-\ell+\sigma}$: multiply with $p^{s-\ell}$

Generalized Filtration Weight

$$\begin{array}{ccc} \mathcal{C}_\sigma & & G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix} \\ \downarrow & & \downarrow \\ \mathcal{C}_{s-\ell+\sigma} & & G_{s-\ell+\sigma} = \begin{pmatrix} p^{s-\ell+\sigma} \mathrm{Id}_K & p^{s-\ell+\sigma} A_{s-\ell+\sigma} \end{pmatrix} \end{array}$$

Generalized Filtration Weight

$$\mathcal{C}_\sigma \qquad G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix} \qquad (\underbrace{0 p^\sigma 0}_{K} \ \underbrace{p^\ell \cdots p^\ell}_{n'} \ \underbrace{\star \cdots \star}_{n-K-n'})$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$\mathcal{C}_{s-\ell+\sigma} \qquad G_{s-\ell+\sigma} = \begin{pmatrix} p^{s-\ell+\sigma} \mathrm{Id}_K & p^{s-\ell+\sigma} A_{s-\ell+\sigma} \end{pmatrix} \qquad (\underbrace{0 p^{s-\ell+\sigma} 0}_{K} \ \underbrace{0 \cdots 0}_{n'} \ \underbrace{\star \cdots \star}_{n-K-n'})$$

Generalized Filtration Weight

$$\mathcal{C}_\sigma \qquad G_\sigma = \begin{pmatrix} p^\sigma \mathrm{Id}_K & p^\sigma A_\sigma \end{pmatrix} \qquad (\underbrace{0p^\sigma 0}_{K}\ \underbrace{p^\ell \cdots p^\ell}_{n'}\ \underbrace{\star \cdots \star}_{n-K-n'})$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$\mathcal{C}_{s-\ell+\sigma} \qquad G_{s-\ell+\sigma} = \begin{pmatrix} p^{s-\ell+\sigma} \mathrm{Id}_K & p^{s-\ell+\sigma} A_{s-\ell+\sigma} \end{pmatrix} \qquad (\underbrace{0p^{s-\ell+\sigma} 0}_{K}\ \underbrace{0 \cdots 0}_{n'}\ \underbrace{\star \cdots \star}_{n-K-n'})$$

New Lee-metric Singleton bound:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, subtype $(k_0, \ldots, k_\sigma)$, max prime power $\ell \neq \sigma, s$, appears n' times:

$$d_L(\mathcal{C}) \leq p^{s-\ell+\sigma} + (n-K-n')\lfloor \frac{p^{\ell-\sigma}}{2} \rfloor p^{s-\ell+\sigma}$$

Support and Weights of Codes: Lee Metric

Support and weight of code:

$$x \in (\mathbb{Z}/p^s\mathbb{Z})^n : \quad \mathrm{supp}_H(x) = \{i \in \{1,\dots,n\} \mid x_i \neq 0\} \subseteq \{1,\dots,n\} \quad \longrightarrow \mathrm{wt}_H(x) = |\mathrm{supp}_H(x)|$$

$$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n : \quad \mathrm{supp}_H(\mathcal{C}) = \{i \in \{1,\dots,n\} \mid \exists x \in \mathcal{C} : x_i \neq 0\} \quad \longrightarrow \mathrm{wt}_H(\mathcal{C}) = |\mathrm{supp}_H(\mathcal{C})|$$

Support and Weights of Codes: Lee Metric

Support and weight of code:

$x \in (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad \mathrm{supp}_H(x) = (\mathrm{wt}_H(x_1), \ldots, \mathrm{wt}_H(x_n)) \subset \mathbb{N}^n \quad \to \mathrm{wt}_H(x) = |\mathrm{supp}_H(x)|$

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad \mathrm{supp}_H(\mathcal{C}) = \bigvee_{c \in \mathcal{C}} \mathrm{supp}_H(c) \quad \to \mathrm{wt}_H(\mathcal{C}) = |\mathrm{supp}_H(\mathcal{C})|$

$s, t \in \mathbb{N}^n$:

- **size** $|s| = \sum_{i=1}^n s_i$
- **join** $s \vee t = (\max\{s_1, t_1\}, \ldots, \max\{s_n, t_n\})$

Support and Weights of Codes: Lee Metric

Support and weight of code:

$x \in (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad \mathrm{supp}_L(x) = (\mathrm{wt}_L(x_1), \dots, \mathrm{wt}_L(x_n)) \quad \rightarrow \quad \mathrm{wt}_L(x) = |\mathrm{supp}_L(x)|$

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: $\quad \mathrm{supp}_L(\mathcal{C}) = \bigvee_{c \in \mathcal{C}} \mathrm{supp}_L(c) \quad \rightarrow \quad \mathrm{wt}_L(\mathcal{C}) = |\mathrm{supp}_L(\mathcal{C})|$

$s, t \in \mathbb{N}^n$:

- **size** $|s| = \sum_{i=1}^n s_i$
- **join** $s \vee t = (\max\{s_1, t_1\}, \dots, \max\{s_n, t_n\})$

Generalized Lee weights:

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Generalized Lee Weights

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \ldots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Generalized Lee Weights

Generalized Lee weights:

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Example:

$\mathcal{C} \subseteq (\mathbb{Z}/9\mathbb{Z})^4$ generated by $\begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & 3 \end{pmatrix}$

$d_L(\mathcal{C}) = 2$

$d_L^1(\mathcal{C}) = 6$

$d_L^2(\mathcal{C}) = 9$

$d_L^3(\mathcal{C}) = 12$

$\mathrm{wt}_L(\mathcal{C}) = 16$

Generalized Lee Weights

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \ldots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Properties:

- $d_L(\mathcal{C}) \leq d_L^1(\mathcal{C})$
- $d_L^r(\mathcal{C}) \leq d_L^{r+1}(\mathcal{C})$ for $r < K$
- $d_L^K(\mathcal{C}) \leq \mathrm{wt}_L(\mathcal{C})$

Generalized Lee Weights

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

socle: $\mathcal{C}_{s-1} = \mathcal{C} \cap \langle p^{s-1} \rangle$ of maximal Lee weight $M_{s-1} = \lfloor \frac{p}{2} \rfloor p^{s-1}$

Properties:
All subcodes attaining the rth generalized Lee weights are in the socle: $d_L^r(\mathcal{C}) = d_H^r(\mathcal{C}) M_{s-1}$

Generalized Lee Weights

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \ldots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

socle: $\mathcal{C}_{s-1} = \mathcal{C} \cap \langle p^{s-1} \rangle$ of maximal Lee weight $M_{s-1} = \lfloor \frac{p}{2} \rfloor p^{s-1}$

New Lee-metric Singleton bound:

$$d_L(\mathcal{C}) \leq M_{s-1}(n - K + 1)$$

Better than previous $d_L(\mathcal{C}) \leq M(n - K + 1)$

Generalized Lee Weights

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \dots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

socle: $\mathcal{C}_{s-1} = \mathcal{C} \cap \langle p^{s-1} \rangle$ of maximal Lee weight $M_{s-1} = \lfloor \frac{p}{2} \rfloor p^{s-1}$

New Lee-metric Singleton bound:

$$d_L(\mathcal{C}) \leq M_{s-1}(n - K + 1)$$

Better than previous $d_L(\mathcal{C}) \leq M(n - K + 1)$

only codes with $p = 3$ can attain it

Need different approach

Lee Column Weight

Example:

$\mathcal{C} \subseteq \mathbb{F}_2^4$ generated by

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$G_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix} \to d_H^1(\mathcal{C}) = 1$$

$$G_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \to d_H^2(\mathcal{C}) = 3$$

$$G \to d_H^3(\mathcal{C}) = 4$$

Lee Column Weight

Example:

$\mathcal{C} \subseteq \mathbb{F}_2^4$ generated by

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$G_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix} \to d_H^1(\mathcal{C}) = 1 \quad = \mathrm{colwt}(G_1)$$

$$G_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \to d_H^2(\mathcal{C}) = 3 = \mathrm{colwt}(G_2)$$

$$G \to d_H^3(\mathcal{C}) = 4 \quad = \mathrm{colwt}(G)$$

Lee Column Weight

Example:

$\mathcal{C} \subseteq \mathbb{F}_2^4$ generated by

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$G_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix} \to d_H^1(\mathcal{C}) = 1 \ = \mathrm{colwt}(G_1)$$

$$G_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \to d_H^2(\mathcal{C}) = 3 = \mathrm{colwt}(G_2)$$

$$G \to d_H^3(\mathcal{C}) = 4 \ = \mathrm{colwt}(G)$$

Lee column weight:

$$A = \begin{pmatrix} \vdots & & \vdots \\ a_1^\top & \cdots & a_n^\top \\ \vdots & & \vdots \end{pmatrix} \quad \to \quad \mathrm{colwt}_L(A) = |(\max \mathrm{supp}_L(a_1), \dots, \max \mathrm{supp}_L(a_n))|$$

Lee Column Weight

Lee column weight:

$$A = \begin{pmatrix} \vdots & & \vdots \\ a_1^\top & \cdots & a_n^\top \\ \vdots & & \vdots \end{pmatrix} \quad \rightarrow \quad \mathrm{colwt}_L(A) = |(\max \mathrm{supp}_L(a_1), \ldots, \max \mathrm{supp}_L(a_n))|$$

Lee Column Weight

Lee column weight:

$$A = \begin{pmatrix} \vdots & & \vdots \\ a_1^\top & \cdots & a_n^\top \\ \vdots & & \vdots \end{pmatrix} \quad \to \quad \mathrm{colwt}_L(A) = |(\max \mathrm{supp}_L(a_1), \dots, \max \mathrm{supp}_L(a_n))|$$

Example: $G = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & 3 \end{pmatrix} \quad \to \quad \mathrm{colwt}_L(G) = |(1, 1, 3, 3)| = 8$

Lee Column Weight

Lee column weight:

$$A = \begin{pmatrix} \vdots & & \vdots \\ a_1^\top & \cdots & a_n^\top \\ \vdots & & \vdots \end{pmatrix} \quad \rightarrow \quad \mathrm{colwt}_L(A) = |(\max \mathrm{supp}_L(a_1), \dots, \max \mathrm{supp}_L(a_n))|$$

Example: $G = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & 3 \end{pmatrix} \quad \rightarrow \quad \mathrm{colwt}_L(G) = |(1,1,3,3)| = 8$

Lee column weight:

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: $\mathrm{colwt}_L(\mathcal{C}) = \min\{\mathrm{colwt}(G) \mid \langle G \rangle = \mathcal{C}\}$

Lee Column Weight

Lee column weight:

$$A = \begin{pmatrix} \vdots & & \vdots \\ a_1^\top & \cdots & a_n^\top \\ \vdots & & \vdots \end{pmatrix} \quad \to \quad \mathrm{colwt}_L(A) = |(\max \mathrm{supp}_L(a_1), \dots, \max \mathrm{supp}_L(a_n))|$$

Example: $G = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & 3 \end{pmatrix} \quad \to \quad \mathrm{colwt}_L(G) = |(1,1,3,3)| = 8$

Lee column weight:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: $\mathrm{colwt}_L(\mathcal{C}) = \min\{\mathrm{colwt}(G) \mid \langle G \rangle = \mathcal{C}\}$

Highly depends on the choice of generator matrix

Lee Column Weight

Generalized Lee column weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \ldots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{colwt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Lee Column Weight

Generalized Lee column weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank K. For all $r \in \{1, \ldots, K\}$:

$$d_L^r(\mathcal{C}) = \min\{\mathrm{colwt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of rank } r\}$$

Properties:

- $d_L(\mathcal{C}) = d_L^1(\mathcal{C})$
- $d_L^r(\mathcal{C}) < d_L^{r+1}(\mathcal{C})$ for $r < K$
- $d_L^K(\mathcal{C}) = \mathrm{colwt}_L(\mathcal{C})$

Lee Column Weight

support subtype of a code is $(n_0, \dots, n_{s-1})$, where

$$n_i = |\{j \in \{1, \dots, n\} \mid \langle c_j \rangle = \langle p^i \rangle\}|$$

$\rightarrow$ Remainder support subtype $(\mu_0, \dots, \mu_{s-1})$ is support subtype in $C_{n-K,\dots,n}$

$$\mathrm{colwt}_L(\mathcal{C})m \leq \sum_{i=0}^{s-1} p^i k_i + \sum_{i=0}^{s-1} \mu_i M_i,$$

where $M_i = \lfloor \frac{p^{s-1}}{2} \rfloor p^i$

Singleton bound:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ with subtype $(k_0, \dots, k_{s-1})$, σ largest with $k_\sigma \neq 0$, support subtype in redundant part $(\mu_{n-K}, \dots, \mu_n)$,

$$d_L(\mathcal{C}) \leq \sum_{i=0}^{s-1} p^i k_i + \sum_{i=n-K}^{n} \mu_i M_i - \left(\sum_{i=0}^{\sigma-1} \left(\sum_{j=0}^{i} k_j \right) \lfloor \frac{p}{2} \rfloor p^i + (k_\sigma - 1)p^\sigma \right)$$

Much better than previous bound $d_L(\mathcal{C}) \leq M(n-K+1)$

Torsion Codes

Torsion codes:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: for $i \in \{1, \dots, s\}$: $\tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

Torsion Codes

Torsion codes:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: for $i \in \{1, \dots, s\}$: $\quad \tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

$$p^{s-i}\tilde{\mathcal{C}}_i \subseteq \mathcal{C}_{s-i} = \mathcal{C} \cap \langle p^{s-i} \rangle \text{ with } \mathrm{rank}(p^{s-i}\tilde{\mathcal{C}}_i) = k_0 + \cdots + k_{i-1} < \mathrm{rank}(\mathcal{C}_{s-i}) = K$$

Torsion Codes

Torsion codes:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: for $i \in \{1, \ldots, s\}$: $\tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

$$p^{s-i}\tilde{\mathcal{C}}_i \subseteq \mathcal{C}_{s-i} = \mathcal{C} \cap \langle p^{s-i} \rangle \text{ with } \mathrm{rank}(p^{s-i}\tilde{\mathcal{C}}_i) = k_0 + \cdots + k_{i-1} < \mathrm{rank}(\mathcal{C}_{s-i}) = K$$

$$\mathcal{C} : G = \begin{pmatrix} \mathrm{Id}_{k_0} & & & & \star \\ 0 & p\mathrm{Id}_{k_1} & & & p\star \\ \vdots & & & & \vdots \\ 0 & & p^{i-1}k_{i-1} & & p^{i-1}\star \\ \vdots & & & & \vdots \\ 0 & & & p^{s-1}\mathrm{Id}_{k_s-1} & p^{s-1}\star \end{pmatrix}$$

Torsion Codes

Torsion codes:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: for $i \in \{1, \dots, s\}$: $\tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

$$p^{s-i}\tilde{\mathcal{C}}_i \subseteq \mathcal{C}_{s-i} = \mathcal{C} \cap \langle p^{s-i} \rangle \text{ with } \operatorname{rank}(p^{s-i}\tilde{\mathcal{C}}_i) = k_0 + \cdots + k_{i-1} < \operatorname{rank}(\mathcal{C}_{s-i}) = K$$

$$\mathcal{C}_{s-i} : G_{s-i} = \begin{pmatrix} p^{s-i}\mathrm{Id}_{k_0} & & & & p^{s-i}\star \\ 0 & p^{s-i}\mathrm{Id}_{k_1} & & & p^{s-i}\star \\ \vdots & & & & \vdots \\ 0 & & p^{s-i}k_{i-1} & & p^{s-i}\star \\ \vdots & & & & \vdots \\ 0 & & & p^{s-1}\mathrm{Id}_{k_s-1} & p^{s-1}\star \end{pmatrix}$$

Torsion Codes

Torsion codes:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: for $i \in \{1, \dots, s\}$: $\quad \tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

$$p^{s-i}\tilde{\mathcal{C}}_i \subseteq \mathcal{C}_{s-i} = \mathcal{C} \cap \langle p^{s-i} \rangle \text{ with } \operatorname{rank}(p^{s-i}\tilde{\mathcal{C}}_i) = k_0 + \cdots + k_{i-1} < \operatorname{rank}(\mathcal{C}_{s-i}) = K$$

$$\tilde{\mathcal{C}}_i : \tilde{G}_i = \begin{pmatrix} \mathrm{Id}_{k_0} & & & \star \\ 0 & p\mathrm{Id}_{k_1} & & p\star \\ \vdots & & & \vdots \\ 0 & & p^{i-1}k_{i-1} & p^{i-1}\star \\ & & & \end{pmatrix}$$

Torsion Codes

Torsion codes:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$: for $i \in \{1, \ldots, s\}$: $\quad \tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

$$p^{s-i}\tilde{\mathcal{C}}_i \subseteq \mathcal{C}_{s-i} = \mathcal{C} \cap \langle p^{s-i} \rangle \text{ with } \operatorname{rank}(p^{s-i}\tilde{\mathcal{C}}_i) = k_0 + \cdots + k_{i-1} < \operatorname{rank}(\mathcal{C}_{s-i}) = K$$

$$d_L(\mathcal{C}) \leq d_L(\mathcal{C}_{s-i}) \leq d_L(p^{s-i}\tilde{\mathcal{C}}_i) \leq \text{upper bound}$$

Fixing the subtype

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of subtype $(k_0, \ldots, k_{s-1})$. For all $(\tilde{k_0}, \ldots, \tilde{k}_{s-1})$ with $\tilde{k}_i \leq k_i$

$$d_L^{(\tilde{k_0}, \ldots, \tilde{k}_{s-1})}(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of subtype } (\tilde{k_0}, \ldots, \tilde{k}_{s-1})\}$$

Fixing the subtype

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of subtype $(k_0, \ldots, k_{s-1})$. For all $(\tilde{k_0}, \ldots, \tilde{k}_{s-1})$ with $\tilde{k}_i \leq k_i$

$$d_L^{(\tilde{k_0}, \ldots, \tilde{k}_{s-1})}(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of subtype } (\tilde{k_0}, \ldots, \tilde{k}_{s-1})\}$$

$$\supset$$

$$\begin{array}{c|c|c|c|c}
 & (k_0, \ldots, k_{s-1}) & (k_0, \ldots, k_{s-1} - 1) & \cdots & (k_0, \cdots, 0) \\
 & (k_0 - 1, \ldots, k_{s-1}) & (k_0 - 1, \ldots, k_{s-1} - 1) & \cdots & (k_0 - 1, \ldots, 0) \\
 & \vdots & & & - \\
\cup & (k_0 - i, \ldots, k_{s-1}) & \cdots & (k_0 - i, \ldots, k_{s-1} - i) & - \\
 & \vdots & & & - \\
 & (0, \ldots, k_{s-1}) & (0, \ldots, k_{s-1} - 1) & - & -
\end{array}$$

Fixing the subtype

Generalized Lee weights:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of subtype $(k_0, \dots, k_{s-1})$. For all $(\tilde{k_0}, \dots, \tilde{k}_{s-1})$ with $\tilde{k}_i \leq k_i$

$$d_L^{(\tilde{k_0}, \dots, \tilde{k}_{s-1})}(\mathcal{C}) = \min\{\mathrm{wt}_L(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ of subtype } (\tilde{k_0}, \dots, \tilde{k}_{s-1})\}$$

all our bounds go to the socle or the subcode of subtype $(0, \dots, 0, k_i, 0, \dots, 0)$ $\rightarrow$ already considered

Alderson-Huntemann

Alderson-Hunteman:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of integer type $1 < k < n$:

$$d_L(\mathcal{C}) \leq (n-K)M$$

T. Alderson, S. Huntemann. "On maximum Lee distance codes.", Discrete Math, 2013

Alderson-Huntemann

Alderson-Hunteman:
$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of integer type $1 < k < n$:

$$d_L(\mathcal{C}) \leq (n-K)M$$

T. Alderson, S. Huntemann. "On maximum Lee distance codes.", Discrete Math, 2013

only optimal codes:

- p odd: $p^s = 5, k+1 \leq n \leq k+3$ or $p^s \in \{7,9\}, n = k+1$
- $p = 2$: free, $s = 2, k+1 \leq n \leq k+2$ or $s = 3$, $n = k+1$ or $k+1 = K \in \{n, n+1\}$

$\rightarrow$ sparse

E. Byrne, **V.W.** "Bounds in the Lee metric and optimal codes.", Finite Fields and Their Applications, 2022