# On the search for the right support: Better bounds for the Lee metric

**Violetta Weger**

Joint work with Jessica Bariffi

SIAM AG23
Conference on Applied Algebraic Geometry

July 13, 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. Weger. "Information set decoding in the Lee metric with applications to cryptography."Advances in Mathematics of Communications, 2019.

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

## The Hamming metric

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

## 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

## The Lee metric

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

## Example

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

# The Lee metric

## The Lee metric

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

## Example

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

**One of the main tasks: Bound minimum distance**

# The Singleton Bound

- Hamming metric: Singleton 1964 (Komamiya 1953)

→ Optimal codes: MDS dense for $q \to \infty$

→ Assuming MDS conjecture: 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 (Komamiya 1953)

→ Optimal codes: MDS dense for $q \to \infty$

→ Assuming MDS conjecture: sparse for $n \to \infty$

- Rank metric: Gabidulin 1985

→ $\mathbb{F}_{q^m}$-linear optimal codes: MRD dense for $m, q \to \infty$

→ $\mathbb{F}_q$-linear optimal codes: 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 (Komamiya 1953)

→ Optimal codes: MDS dense for $q \to \infty$

→ Assuming MDS conjecture: sparse for $n \to \infty$

- Rank metric: Gabidulin 1985

→ $\mathbb{F}_{q^m}$-linear optimal codes: MRD dense for $m, q \to \infty$

→ $\mathbb{F}_q$-linear optimal codes: 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

**Hamming-metric Singleton Bound**

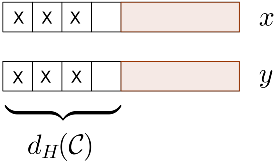
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code of type $k$:

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

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

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

$\rightarrow$ $\mathcal{C}' \subseteq (\mathbb{Z}/p^s\mathbb{Z})^{n-(d_H(\mathcal{C})-1)}$



# The Singleton Bound

**Hamming-metric Singleton Bound**

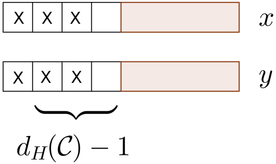
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code of type $k$:

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

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

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

$\rightarrow$ $\mathcal{C}' \subseteq (\mathbb{Z}/p^s\mathbb{Z})^{n-(d_H(\mathcal{C})-1)}$



# The Singleton Bound

**Lee-metric Singleton Bound**

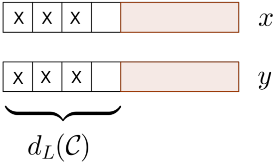
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code of type $k$, for $M = \lfloor \frac{p^s}{2} \rfloor$:

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

- 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**

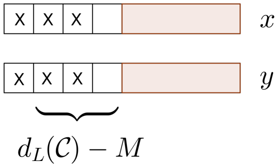
For $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ linear code of type $k$, for $M = \lfloor \frac{p^s}{2} \rfloor$:

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

- 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 $k$, $M = \lfloor \frac{p^s}{2} \rfloor$ :

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

**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 $k$, $M = \lfloor \frac{p^s}{2} \rfloor$ :

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

**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. Weger. "Bounds in the Lee metric and optimal codes.", Finite Fields and Their Applications, 2022

**Need better Lee-metric Singleton Bound!**

**→ Need new technique**

# Generalized Hamming Weights

**Support and Weight of Code**

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

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

# Generalized Hamming Weights

**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

## Support and Weight of Code

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

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

## Generalized Weights

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

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

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

## 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: $d_H(\mathcal{C}) \leq \mathrm{wt}_H(\mathcal{C}) - (k-1) \leq n - k + 1$

# 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 $r \in \{1, \ldots, K\}$ :

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

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

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

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

# 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 $r \in \{1, \ldots, K\}$ :

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

- using the **join Lee support** $\mathrm{supp}_L(x) = (\mathrm{wt}_L(x_1), \ldots, \mathrm{wt}_L(x_n)) = s, \ \mid s \mid = \sum s_i$

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

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

→ better than previous bound $d_L(\mathcal{C}) \leq \lfloor \frac{p^s}{2} \rfloor (n-K+1)$

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

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

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

→ better than previous bound $d_L(\mathcal{C}) \leq \lfloor \frac{p^s}{2} \rfloor (n - K + 1)$

→ Problem can only be attained for $p = 3$

# 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 $r \in \{1, \ldots, K\}$ :

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

- using the **column Lee weight**

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

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

# 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 **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 $r \in \{1, \dots, K\}$ :

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

- using the **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

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

$\longrightarrow$ Problem still sparse

**Hard to control subcodes of smaller ranks**

# Generalized Filtration Weight

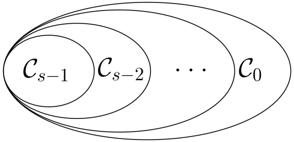
**Filtration**

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

# Generalized Filtration Weight

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




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

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

# Generalized Filtration Weight

**Filtration**

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

**Generalized Lee Weights**

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$. For all $r \in \{1, \dots, s\}$ : $\quad d_L^r(\mathcal{C}) = d_L(\mathcal{C}_{r-1})$

# Generalized Filtration Weight

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

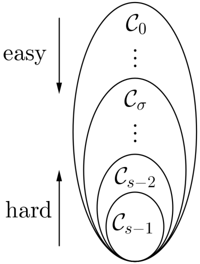
## Generalized Lee Weights

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$. For all $r \in \{1, \ldots, s\}$ : $\quad d_L^r(\mathcal{C}) = d_L(\mathcal{C}_{r-1})$

## Properties

- $d_L(\mathcal{C}) = d_L^1(\mathcal{C})$
- $d_L^r(\mathcal{C}) \leq d_L^{r+1}(\mathcal{C})$ for $r < s$
- $d_L^r(\mathcal{C}) \leq p^{r-1} + (n-K)M_{r-1}$

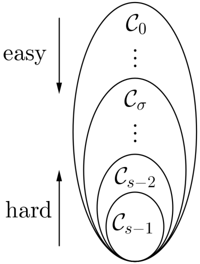
# Generalized Filtration Weight




using information from $G$

how far down should we go?

# Generalized Filtration Weight

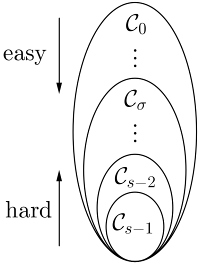



$\leftarrow$ stop at $\mathcal{C}_\sigma$

using information from $G$

how far down should we go?

# Generalized Filtration Weight



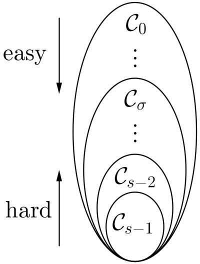

$\leftarrow$ stop at $\mathcal{C}_\sigma$

$\leftarrow$ stop at $\mathcal{C}_{s-1}$

using information from $G$

how far down should we go?

# Generalized Filtration Weight




$\leftarrow$ stop at $\mathcal{C}_\sigma$

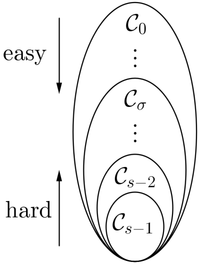
$\leftarrow$ stop at $\mathcal{C}_{s-1}$

using information from $G$

how far down should we go?

$\rightarrow$ Singleton bound with several conditions

# Generalized Filtration Weight




$\leftarrow$ stop at $\mathcal{C}_\sigma$

$\leftarrow$ stop at $\mathcal{C}_{s-1}$

using information from $G$

how far down should we go?

$\rightarrow$ Singleton bound with several conditions

**New Lee-Metric Singleton Bound**

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, subtype $(k_0, \ldots, k_\sigma)$, $\ell$: 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

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

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

- 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: $d_L \leq 9$

# 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: $d_L \leq 5$

# Density

Are the optimal codes dense?

# Density

## Are the optimal codes dense?

$p \to \infty$

→ $\mathcal{C}$ is a free code: $\sigma = 0$, $\ell = 0$

→ Recover Shiromoto:
$d_L(\mathcal{C}) \leq 1 + (n - K)\lfloor \frac{p^s}{2} \rfloor$

→ Optimal codes are sparse

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

# Density

## Are the optimal codes dense?

$p \to \infty$

- $\to$ $\mathcal{C}$ is a free code: $\sigma = 0$, $\ell = 0$
- $\to$ Recover Shiromoto: $d_L(\mathcal{C}) \leq 1 + (n-K)\lfloor \frac{p^s}{2} \rfloor$
- $\to$ Optimal codes are sparse

$n \to \infty$

- $\to$ Only way to not get sparse: $n' = n - K$:
- $\to$ $\mathbb{P}$ whole row is $p^\ell$ : $\frac{1}{p^{n-K}}$
- $\to$ Optimal codes are sparse

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

# Density

## Are the optimal codes dense?

$p \to \infty$

- $\to$ $\mathcal{C}$ is a free code: $\sigma = 0$, $\ell = 0$
- $\to$ Recover Shiromoto: $d_L(\mathcal{C}) \leq 1 + (n-K)\lfloor \frac{p^s}{2} \rfloor$
- $\to$ Optimal codes are sparse

$n \to \infty$

- $\to$ Only way to not get sparse: $n' = n - K$:
- $\to$ $\mathbb{P}$ whole row is $p^\ell$ : $\frac{1}{p^{n-K}}$
- $\to$ Optimal codes are sparse

## But for $s \to \infty$: not sparse!

density $\left(\frac{p-1}{p}\right)^{K(n-K)}$

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

# Questions?

**Summary**

- several definitions of generalized Lee weights
- new (tighter) Lee-metric Singleton bounds
- new Singleton bound for which MLD codes are not sparse for $s \to \infty$

**Open Question**

- MLD codes construction
- technique for Lee-metric bounds with dense optimal codes

# Questions?

## Summary

- several definitions of generalized Lee weights
- new (tighter) Lee-metric Singleton bounds
- new Singleton bound for which MLD codes are not sparse for $s \to \infty$

## Open Question

- MLD codes construction
- technique for Lee-metric bounds with dense optimal codes

**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

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

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

$$\downarrow$$

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

$\ell$ : 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 $p^\ell$ in one row

# Generalized Filtration Weight

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

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

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

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

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

$\ell$ : max prime power in $p^\sigma A_\sigma$ $\qquad$ $n'$: max number of $p^\ell$ 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

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

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

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

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

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

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

$n'$: max number of $p^\ell$ in one row

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

# Generalized Filtration Weight

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

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

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

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

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

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

$n'$: max number of $p^\ell$ in one row

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

# Generalized Filtration Weight

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

$$\downarrow \qquad \downarrow$$

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

# Generalized Filtration Weight

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

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

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

# Generalized Filtration Weight

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

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

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

**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**

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

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

# Support and Weights of Codes: Lee Metric

**Support and Weight of Code**

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

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

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

- **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**

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

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

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

- **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 $r \in \{1, \dots, K\}$ :

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

# Generalized Lee Weights

**Generalized Lee Weights**

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

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

# 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 $r \in \{1, \ldots, K\}$ :

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

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

**Properties**

All subcodes attaining the $r$th 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 $r \in \{1, \dots, K\}$ :

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

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

# 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

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

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

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

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

# Lee Column Weight

## Example

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

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

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

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

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

## Lee Column Weight

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

# 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**

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

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**

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

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**

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

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**

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

**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 $r \in \{1, \ldots, K\}$ :

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

# Lee Column Weight

## Generalized Lee Column Weights

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

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

## Properties

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

# 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 $(k_0, \dots, k_{s-1})$, $\sigma$ 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 $i \in \{1, \ldots, s\}$: $\tilde{\mathcal{C}}_i = \mathcal{C} \mod p^i \subseteq \left(\mathbb{Z}/p^i\mathbb{Z}\right)^n$

# Torsion Codes

**Torsion Codes**

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

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

# Torsion Codes

**Torsion Codes**

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

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

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

# Torsion Codes

**Torsion Codes**

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

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

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

# Torsion Codes

**Torsion Codes**

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

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

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

# Torsion Codes

**Torsion Codes**

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

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

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

# 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 $(k_0, \dots, k_{s-1})$. For all $(\tilde{k_0}, \dots, \tilde{k}_{s-1})$ with $\tilde{k}_i \leq k_i$

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

$\supset$

| | | | | |
|---|---|---|---|---|
| | $(k_0, \dots, k_{s-1})$ | $(k_0, \dots, k_{s-1} - 1)$ | $\cdots$ | $(k_0, \cdots, 0)$ |
| | $(k_0 - 1, \dots, k_{s-1})$ | $(k_0 - 1, \dots, k_{s-1} - 1)$ | $\cdots$ | $(k_0 - 1, \dots, 0)$ |
| | $\vdots$ | | | - |
| $\cup$ | $(k_0 - i, \dots, k_{s-1})$ | $\cdots$ | $(k_0 - i, \dots, k_{s-1} - i)$ | - |
| | $\vdots$ | | | - |
| | $(0, \dots, k_{s-1})$ | $(0, \dots, k_{s-1} - 1)$ | - | - |

# 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 $\tilde{k}_i \leq k_i$

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

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

# Alderson-Huntemann

**Alderson-Huntemann Bound**

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ 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-Huntemann Bound

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ 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. Weger. "Bounds in the Lee metric and optimal codes.", Finite Fields and Their Applications, 2022