Bounds and optimal codes in the Lee metric

Violetta Weger

Technical University of Munich

PICS: Postgraduate International Coding theory Seminar
January 27, 2022

joint work with Eimear Byrne

Motivation

- From an information theoretic perspective:
  The Lee metric is best suited for channels, where the error $+x, -x$ are equally likely and the magnitude matters.
- From an algebraic perspective:
  Some excellent but non-linear binary codes can be represented as linear codes over $\mathbb{Z}/4\mathbb{Z}$ endowed with the Lee metric.

  A. Roger Hammons, P. Vijay Kumar, A. Robert Calderbank, Neil J.A. Sloane and Patrick Solé "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes", IEEE Transactions on Information Theory, 1994.
- From a cryptographic perspective:
  The Lee metric promises lower key sizes/signature sizes, since one can insert more errors.

Outline

	Classical	$\mathbb{Z}/p^s\mathbb{Z}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	
Linear code	$\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace	
Parameters	length n dimension k	

Ring-Linear Coding Theory

	Classical	$\mathbb{Z}/p^s\mathbb{Z}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	Integer residue ring $\mathbb{Z}/p^s\mathbb{Z}$
Linear code	$\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace	$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ $\mathbb{Z}/p^s\mathbb{Z}$-submodule
Parameters	length n dimension k	length n ?

Example

- $\mathcal{C} = \langle (1,2,3),(2,2,0) \rangle \subseteq \mathbb{F}_5^3$ has length 3, dimension 2 and thus $\mid \mathcal{C} \mid = 5^2$.

Example

- $\mathcal{C} = \langle (1,2,3),(2,2,0) \rangle \subseteq \mathbb{F}_5^3$ has length 3, dimension 2 and thus $\mid \mathcal{C} \mid = 5^2$.
- $\mathcal{C} = \langle (1,2,3),(1,2,0) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has length 3 and $\mid \mathcal{C} \mid = 4^2$.

Example

- $\mathcal{C} = \langle (1,2,3),(2,2,0)\rangle \subseteq \mathbb{F}_5^3$ has length 3, dimension 2 and thus $\mid \mathcal{C} \mid = 5^2$.
- $\mathcal{C} = \langle (1,2,3),(1,2,0)\rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has length 3 and $\mid \mathcal{C} \mid = 4^2$.
- $\mathcal{C} = \langle (1,2,3),(2,2,0)\rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has length 3 and $\mid \mathcal{C} \mid = 8$.

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code, then

$$\mathcal{C} \cong (\mathbb{Z}/p^s\mathbb{Z})^{k_1} \times \left(\mathbb{Z}/p^{s-1}\mathbb{Z}\right)^{k_2} \times \cdots \times (\mathbb{Z}/p\mathbb{Z})^{k_s}.$$

Then we say $\mathcal{C}$ has

- **subtype** $(k_1, \ldots, k_s)$,
- **type** $k = \sum_{i=1}^{s} \frac{s-i+1}{s} k_i = \log_{p^s}(|\mathcal{C}|)$,
- **rate** $R = k/n$,
- **rank** $K = \sum_{i=1}^{s} k_i$,
- **free rank** k_1.

$$0 \leq k_1 \leq k \leq K \leq n.$$

If $k_1 = k = K$, we say that $\mathcal{C}$ is a **free code**.

Example

- $\mathcal{C} = \langle (1,2,3),(1,2,0) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has length 3 and subtype $(2,0)$, thus $k = K = 2$ and $\mid \mathcal{C} \mid = 4^2$.
- $\mathcal{C} = \langle (1,2,3),(2,2,0) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has length 3 and subtype $(1,1)$, thus $K = 2$, $k = 3/2$ and $\mid \mathcal{C} \mid = 4^{3/2} = 8$.

Systematic Form

If $\mathcal{C}$ has subtype $(k_1, \ldots, k_s)$ and rank K then

$$G = \begin{pmatrix} \mathrm{Id}_{k_1} & * & \cdots & * & * \\ 0 & p\mathrm{Id}_{k_2} & \cdots & p* & p* \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & p^{s-1}\mathrm{Id}_{k_s} & p^{s-1}* \end{pmatrix} \in (\mathbb{Z}/p^s\mathbb{Z})^{K\times n}.$$

If $\mathcal{C}$ is a free code, then

$$G = \begin{pmatrix} \mathrm{Id}_k & A \end{pmatrix} \in (\mathbb{Z}/p^s\mathbb{Z})^{k\times n}.$$

Lee Metric

Definition (Lee Metric)

$$\begin{array}{lcrcl} x \in \mathbb{Z}/p^s\mathbb{Z} & : & \mathrm{wt}_L(x) & = & \min\{x, \mid p^s - x \mid\}, \\ x \in (\mathbb{Z}/p^s\mathbb{Z})^n & : & \mathrm{wt}_L(x) & = & \sum_{i=1}^{n} \mathrm{wt}_L(x_i), \\ x, y \in (\mathbb{Z}/p^s\mathbb{Z})^n & : & d_L(x, y) & = & \mathrm{wt}_L(x - y). \end{array}$$

Example ($\mathbb{Z}/4\mathbb{Z}$)

$$\mathrm{wt}_L(0) = 0 \quad \mathrm{wt}_L(2) = 2$$

$$\mathrm{wt}_L(1) = 1 \quad \mathrm{wt}_L(3) = 1$$

Important parameter: Maximal Lee weight:

$$M = \left\lfloor \frac{p^s}{2} \right\rfloor.$$

Connection to Hamming metric:

$$0 \leq \mathrm{wt}_H(x) \leq \mathrm{wt}_L(x) \leq M \mathrm{wt}_H(x) \leq Mn.$$

Lee Metric

For a linear code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ its **minimum Lee distance** is given by

$$d_L(\mathcal{C}) = \min\{\mathrm{wt}_L(x) \mid x \in \mathcal{C}, x \neq 0\}.$$

Example

- $\mathcal{C} = \langle (1,2,3), (1,2,0) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has minimum Lee distance $d_L = 1$.
- $\mathcal{C} = \langle (1,2,3), (2,2,0) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ has minimum Lee distance $d_L = 2$.

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of subtype $(k_1, \ldots, k_s)$ and rank K.

- Define the subcodes $\mathcal{C}_i = \mathcal{C} \cap \langle p^{s-1-i} \rangle$ for $i \in \{0, \ldots, s-1\}$.
- We have a sequence of subcodes $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_{s-1} = \mathcal{C}$.
- The socle $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ can be seen as

Techniques

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of subtype $(k_1, \ldots, k_s)$ and rank K.

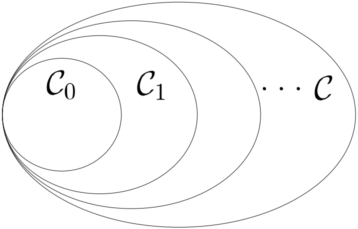
- Define the subcodes $\mathcal{C}_i = \mathcal{C} \cap \langle p^{s-1-i} \rangle$ for $i \in \{0, \ldots, s-1\}$.
- We have a sequence of subcodes $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_{s-1} = \mathcal{C}$.
- The socle $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ can be seen as

$$\{xG \mid x \in p^{s-1}(\mathbb{Z}/p^s\mathbb{Z})^{k_1} \times p^{s-2}(\mathbb{Z}/p^s\mathbb{Z})^{k_2} \times \cdots \times (\mathbb{Z}/p^s\mathbb{Z})^{k_s}\}$$

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

$$\mid \mathcal{C}_0 \mid = p^{k_1+k_2+\cdots+k_s} = p^K.$$

Techniques

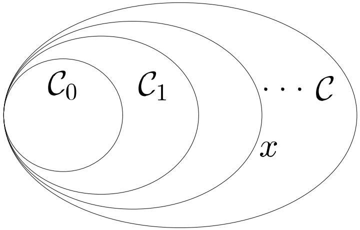


1. Use the socle:
   $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ can be identified with a $[n, K]$ linear code over $\mathbb{F}_p$.
2. Use the Hamming metric:

$$d_H(\mathcal{C}) \leq d_L(\mathcal{C}) \leq M d_H(\mathcal{C}).$$

We always find minimal Hamming weight codewords in the socle.

Techniques

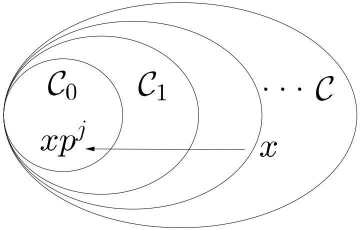


1. Use the socle:
   $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ can be identified with a $[n, K]$ linear code over $\mathbb{F}_p$.
2. Use the Hamming metric:

$$d_H(\mathcal{C}) \leq d_L(\mathcal{C}) \leq M d_H(\mathcal{C}).$$

We always find minimal Hamming weight codewords in the socle.

Techniques



1. Use the socle:
   $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ can be identified with a $[n, K]$ linear code over $\mathbb{F}_p$.
2. Use the Hamming metric:

$$d_H(\mathcal{C}) \leq d_L(\mathcal{C}) \leq M d_H(\mathcal{C}).$$

We always find minimal Hamming weight codewords in the socle.

Classical Singleton Bound

Recall that for $x \in \mathbb{F}_q^n$ the Hamming weight is

$$\mathrm{wt}_H(x) = \mid \{i \in \{1, \ldots, n\} \mid x_i \neq 0\} \mid .$$

Theorem (Singleton Bound)

A code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k has minimum Hamming distance

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

Proof Idea

- Puncture $\mathcal{C}$ in $d_H(\mathcal{C}) - 1$ positions to get $\mathcal{C}'$.
- Any two codewords of $\mathcal{C}'$ are still distinct: $\mid \mathcal{C}' \mid = q^k$.
- Since $\mathcal{C}' \subseteq \mathbb{F}_q^{n-d_H(\mathcal{C})+1}$, we have $k \leq n - d_H(\mathcal{C}) + 1$.

General Singleton Bound

More in general: for any finite ring R of size r and additive weight wt with maximum weight $M = \max\{\mathrm{wt}(x) \mid x \in R\}$.

Theorem (Singleton Bound)

A code $\mathcal{C} \subseteq R^n$ of size r^k has minimum distance

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

Proof Idea

- Puncture $\mathcal{C}$ in $\left\lfloor \frac{d(\mathcal{C})-1}{M} \right\rfloor$ positions to get $\mathcal{C}'$.
- Any two codewords of $\mathcal{C}'$ are still distinct: $\mid \mathcal{C}' \mid = r^k$.
- Since $\mathcal{C}' \subseteq R^{n - \left\lfloor \frac{d(\mathcal{C})-1}{M} \right\rfloor}$, we have $k \leq n - \left\lfloor \frac{d(\mathcal{C})-1}{M} \right\rfloor$.

MDS Codes

Codes that achieve this bound are called *maximum distance separable (MDS) codes.*

- For $n \leq q+1$ we have a construction of MDS codes: (extended) RS codes.
- For $q \to \infty$ MDS codes have density 1.
- For $n \to \infty$ MDS codes have density 0 (assuming the MDS conjecture).
- Dual of MDS codes are also MDS codes.
- Binary MDS codes are trivial, that is $k \in \{1, n, n-1\}$.

Singleton Bound

Clearly for $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type k

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

Singleton Bound

Clearly for $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type k

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

Theorem (Dougherty, Shiromoto)

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a linear code of rank K, then

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

Steven T. Dougherty and Keisuke Shiromoto "MDR codes over $\mathbb{Z}_k$.", IEEE Transactions on Information Theory, 2000.

We can identify $\mathcal{C}_0$ with an $[n, K]$ linear code over $\mathbb{F}_p$, for which we know

$$d_H(\mathcal{C}) \leq d_H(\mathcal{C}_0) \leq n - K + 1.$$

Singleton Bound in the Lee Metric

Theorem (Shiromoto)

For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type k, we have that

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

Keisuke Shiromoto "Singleton bounds over finite rings.", Journal of Algebraic Combinatorics, 2000.

Singleton Bound in the Lee Metric

Theorem (Shiromoto)

For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type k, we have that

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

Keisuke Shiromoto "Singleton bounds over finite rings.", Journal of Algebraic Combinatorics, 2000.

Example

Let us consider the code $\mathcal{C} = \langle (1, 2) \rangle$ over $\mathbb{Z}/5\mathbb{Z}$, which has $M = 2, n = 2, k = 1$ and $d_L = 3$. This code attains the bound of Shiromoto as

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

Singleton Bound in the Lee Metric

Theorem (Byrne, W.)

The only non-trivial linear codes that attain this Singleton bound are equivalent to $\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$.

Singleton Bound in the Lee Metric

Theorem (Byrne, W.)

The only non-trivial linear codes that attain this Singleton bound are equivalent to $\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$.

- MLD codes have density 0 for $p \to \infty$.
- MLD codes have density 0 for $n \to \infty$.

Is the dual of an MLD code also an MLD code?

Theorem (Byrne, W.)

The only non-trivial linear codes that attain this Singleton bound are equivalent to $\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$.

- MLD codes have density 0 for $p \to \infty$.
- MLD codes have density 0 for $n \to \infty$.

Is the dual of an MLD code also an MLD code?

Yes

Since $\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$ is self-dual.

Classical Plotkin Bound

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be linear code of dimension k, then

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

Proof

- $$d_H(\mathcal{C})(\mid \mathcal{C} \mid -1) \leq \sum_{c \in \mathcal{C}} \mathrm{wt}_H(c).$$
- Define the average weight of a code
$$\overline{\mathrm{wt}}_H(\mathcal{C}) = \frac{1}{\mid \mathcal{C} \mid} \sum_{c \in \mathcal{C}} \mathrm{wt}_H(c).$$
- Note that
$$\overline{\mathrm{wt}}_H(\mathcal{C}) \leq n\overline{\mathrm{wt}}_H(\mathbb{F}_q) = n\frac{q-1}{q}.$$

General Plotkin Bound

In general: for any finite ring R and additive weight wt.

Theorem

Let $\mathcal{C} \subseteq R^n$ be linear code, then

$$d(\mathcal{C}) \leq \frac{\mid \mathcal{C} \mid}{\mid \mathcal{C} \mid -1} n\overline{wt}(R).$$

Proof

- $$d(\mathcal{C})(\mid \mathcal{C} \mid -1) \leq \sum_{c \in \mathcal{C}} \mathrm{wt}(c).$$
- Define the average weight of a code
$$\overline{\mathrm{wt}}(\mathcal{C}) = \frac{1}{\mid \mathcal{C} \mid} \sum_{c \in \mathcal{C}} \mathrm{wt}(c).$$
- Note that
$$\overline{\mathrm{wt}}(\mathcal{C}) \leq n\overline{\mathrm{wt}}(R).$$

The average Lee weight over $\mathbb{Z}/p^s\mathbb{Z}$ is given by

$$\overline{D} = \begin{cases} \frac{p^{2s}-1}{4p^s} & \text{if } p \text{ is odd,} \\ 2^{s-2} & \text{if } p = 2. \end{cases}$$

Theorem (Wyner and Graham)

For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type k we have that

$$d_L(\mathcal{C}) \leq \frac{n\overline{D}}{1 - 1/p^{sk}}.$$

Since

$$1 - 1/p^{sk} = \frac{\mid \mathcal{C} \mid}{\mid \mathcal{C} \mid - 1}.$$

Aaron D. Wyner and Ronald L. Graham "An upper bound on minimum distance for a k-ary code.", Inf. Control., 1968.

Plotkin Bound in the Lee Metric

Theorem (Chiang and Wolf (adapted))

For a linear code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ *of free rank* k_1 *we have that*

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

J. Chung-Yaw Chiang and Jack K. Wolf "On channels and codes for the Lee metric", Information and Control, 1971.

Plotkin Bound in the Lee Metric

Theorem (Chiang and Wolf (adapted))

For a linear code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of free rank k_1 we have that

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

J. Chung-Yaw Chiang and Jack K. Wolf "On channels and codes for the Lee metric", Information and Control, 1971.

Theorem (Wyner and Graham)

For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type k we have that

$$d_L(\mathcal{C}) \leq \frac{n\overline{D}}{1-1/p^{sk}}.$$

Plotkin Bound in the Lee Metric

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

Proof

For any subcode $\mathcal{C}' \subseteq \mathcal{C}$

$$d_L(\mathcal{C}) \leq d_L(\mathcal{C}') \leq \frac{\mid \mathcal{C}' \mid}{\mid \mathcal{C}' \mid -1}\overline{\mathrm{wt}_L}(\mathcal{C}').$$

Plotkin Bound in the Lee Metric

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

Proof

For any $c \in \mathcal{C}$

$$d_L(\mathcal{C}) \leq d_L(\langle c \rangle) \leq \frac{\mid \langle c \rangle \mid}{\mid \langle c \rangle \mid -1} \overline{\mathrm{wt}_L}(\langle c \rangle).$$

Plotkin Bound in the Lee Metric

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

Proof

For any $c \in \mathcal{C}$ in the free part

$$d_L(\mathcal{C}) \leq d_L(\langle c \rangle) \leq \frac{1}{1-1/p^s} \mathrm{wt}_H(c)\overline{D}.$$

Plotkin Bound in the Lee Metric

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

Proof

For any $c \in \mathcal{C}$ in the free part

$$d_L(\mathcal{C}) \leq d_L(\langle c \rangle) \leq \frac{1}{1-1/p^s}\mathrm{wt}_H(c)\overline{D}.$$

- Let G be a $K \times n$ generator matrix for the code $\mathcal{C}$.

$$G = \begin{pmatrix} \mathrm{Id}_{k_1} & A \\ 0 & pB \end{pmatrix}.$$

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

Proof

For any $c \in \mathcal{C}$ in the free part

$$d_L(\mathcal{C}) \leq d_L(\langle c \rangle) \leq \frac{1}{1-1/p^s}\mathrm{wt}_H(c)\overline{D}.$$

- Let G be a $K \times n$ generator matrix for the code $\mathcal{C}$.
- Let G' be the $k_1 \times n$ generator matrix for the free part $\mathcal{C}' \subseteq \mathcal{C}$.

$$G' = \begin{pmatrix} \mathrm{Id}_{k_1} & A \end{pmatrix}.$$

$$d_L(\mathcal{C}) \leq \frac{(n-k_1+1)\overline{D}}{1-1/p^s}.$$

Proof

For any $c \in \mathcal{C}$ in the free part

$$d_L(\mathcal{C}) \leq d_L(\langle c \rangle) \leq \frac{1}{1-1/p^s}\mathrm{wt}_H(c)\overline{D}.$$

- Let G be a $K \times n$ generator matrix for the code $\mathcal{C}$.
- Let G' be the $k_1 \times n$ generator matrix for the free part $\mathcal{C}' \subseteq \mathcal{C}$.
- $c \in \mathcal{C}'$ with $\mathrm{wt}_H(c) \leq n - k_1 + 1$.

$$G' = \begin{pmatrix} \mathrm{Id}_{k_1} & A \end{pmatrix}.$$

Plotkin Bound in the Lee Metric

$$d_L(\mathcal{C}) \leq \frac{|\langle c \rangle|}{|\langle c \rangle| - 1} \overline{\mathrm{wt}}_L(\langle c \rangle),$$

for a minimum Hamming weight codeword c.

- If we can take c in the free part: we get the Chiang and Wolf bound with k_1.
- If $c \in \langle p^{s-\ell} \rangle$: how do we bound $\overline{\mathrm{wt}}_L(\langle c \rangle)$?

We introduce the support subtype

- For $j \in \{1, \ldots, n\}$ let π_j be the j-th coordinate map.
- Define

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

- For a code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, we call $(n_0, \ldots, n_s)$ its support subtype.

We introduce the support subtype

- For $j \in \{1, \ldots, n\}$ let π_j be the j-th coordinate map.
- Define

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

- For a code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, we call $(n_0, \ldots, n_s)$ its support subtype.

Example

Let $\mathcal{C}$ be the code over $\mathbb{Z}/8\mathbb{Z}$ generated by

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

then $\mathcal{C}$ has subtype $(1, 1, 2)$ and support subtype $(3, 2, 0, 0)$.

We introduce the support subtype

- For $j \in \{1, \dots, n\}$ let π_j be the j-th coordinate map.
- Define

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

- For a code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, we call $(n_0, \dots, n_s)$ its support subtype.

Example

Let $\mathcal{C}$ be the code over $\mathbb{Z}/8\mathbb{Z}$ generated by

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

then $\mathcal{C}$ has subtype $(1, 1, 2)$ and support subtype $(3, 2, 0, 0)$.

Plotkin Bound in the Lee Metric

Lemma (Byrne, W.)

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a linear code of support subtype $(n_0, \ldots, n_s)$. Then

$$\overline{wt}_L(\mathcal{C}) = \begin{cases} \frac{1}{4p^s}\left(p^{2s}|n-n_s| - \sum_{i=0}^{s-1} p^{2i} n_i\right) & \text{if } p \text{ is odd,} \\ 2^{s-2}|n-n_s| & \text{if } p = 2. \end{cases}$$

Plotkin Bound in the Lee Metric

Theorem (Byrne, W.)

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be linear code. Let $\ell \in \{1, \dots, s\}$ be maximal such that there exists $y \in \mathcal{C}$ satisfying $wt_H(y) = d_H(y)$ and $y \in \langle p^{s-\ell} \rangle$. Then

$$d_L(\mathcal{C}) \leq \begin{cases} \frac{p^{s-\ell}(p^\ell + 1)}{4} d_H(\mathcal{C}) & \text{if } p \text{ is odd,} \\ \frac{2^{s-2+\ell}}{2^\ell - 1} d_H(\mathcal{C}) & \text{if } p = 2. \end{cases}$$

Plotkin Bound in the Lee Metric

We can always choose $\ell = 1$ (there is always a minimal Hamming weight codeword in the socle)

Corollary (Byrne, W.)

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a linear code of rank K. Then

$$\left\lfloor \frac{d_L(\mathcal{C}) - 1}{A} \right\rfloor \leq n - K,$$

for

$$A := \begin{cases} \dfrac{p^{s-1}(p+1)}{4} & \text{if } p \text{ is odd,} \\ 2^{s-1} & \text{if } p = 2. \end{cases}$$

Example

We consider the code $\mathcal{C} = \langle (0,1,1),(2,0,0),(0,0,2) \rangle \subset (\mathbb{Z}/4\mathbb{Z})^3$. This code attains the new bound for $\ell = 1$ since

$$d_L = 2 = 2(n - K + 1).$$

It does not attain the bound of Chiang and Wolf with k_1, as

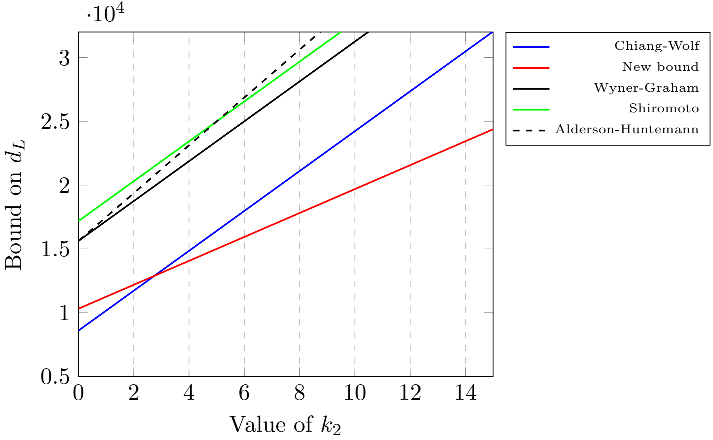
$$d_L \leq \frac{4}{3}(3 - 1 + 1) = 4.$$

We also note that we cannot choose $\ell = 2$, since the only codewords that have minimal Hamming weight are divisible by 2. In fact:

$$d_L = 2 \not\leq \frac{4}{3} = \frac{4}{3}(3 - 3 + 1).$$

Comparison of Bounds

Comparison of bounds for codes over $\mathbb{Z}/5^5\mathbb{Z}$ of type $(10, k_2, 0, 0, 0)$ and length $2K, K = 10 + k_2$.



Density

Note that in order to meet the new bound with $\ell = 1$, we need:

1. The socle $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ is an MDS code, we can identify it with a $[n, K]$ linear code over $\mathbb{F}_p$.
2. There is an $x \in \mathcal{C}_0$ which generates a Lee-equidistant code.

Density

Note that in order to meet the new bound with $\ell = 1$, we need:

1. The socle $\mathcal{C}_0 = \mathcal{C} \cap \langle p^{s-1} \rangle$ is an MDS code, we can identify it with a $[n, K]$ linear code over $\mathbb{F}_p$.
2. There is an $x \in \mathcal{C}_0$ which generates a Lee-equidistant code.

$$\Downarrow$$

1. Due to the MDS conjecture: density is 0 if $n \to \infty$.
2. Due to the characterization of Lee-equidistant codes of Wood: x consists of repetitions of $(\pm 1, \ldots, \pm \frac{p-1}{2})$, hence the density is 0 if $p \to \infty$.

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

Constant Hamming-Weight Codes

Codes that attain the Plotkin bound are such that all non-zero codewords have the same weight d_H, thus called constant Hamming-weight codes.

- Let $m \in \mathbb{N}$, define $n = \frac{q^m-1}{q-1}$. The simplex code of length n, dimension m and $d_H = q^{m-1}$ is defined through a generator matrix G, which has one representative of each 1-dimensional subspace $\langle x \rangle \subseteq \mathbb{F}_q^m$ as column.

Example

Let $q = m = 3$ and thus $n = 13$.

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 \\ 1 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \end{bmatrix}.$$

- Any constant Hamming-weight code is an ℓ-fold duplicate of simplex codes.

Constant Lee-Weight Codes

- If $s = 1$: any cyclic module is a constant Hamming-weight code.
- If $s > 1$: any cyclic module with support subtype $(0, \dots, 0, n_i, 0, \dots, 0, n_s)$ is constant Hamming-weight over $\mathbb{Z}/p^s\mathbb{Z}$.

Constant Lee-Weight Codes

- If $s = 1$: any cyclic module is a constant Hamming-weight code.
- If $s > 1$: any cyclic module with support subtype $(0, \ldots, 0, n_i, 0, \ldots, 0, n_s)$ is constant Hamming-weight over $\mathbb{Z}/p^s\mathbb{Z}$.

Example

- $\mathcal{C} = \langle(1, 4)\rangle \subseteq \mathbb{Z}/5\mathbb{Z}^2$ is a constant Hamming-weight code.
- $\mathcal{C} = \langle(1, 0, 3)\rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ is a constant Hamming-weight code.

Constant Lee-Weight Codes

- If $s = 1$: any cyclic module is a constant Hamming-weight code.
- If $s > 1$: any cyclic module with support subtype $(0, \dots, 0, n_i, 0, \dots, 0, n_s)$ is constant Hamming-weight over $\mathbb{Z}/p^s\mathbb{Z}$.

Example

- $\mathcal{C} = \langle (1, 4) \rangle \subseteq \mathbb{Z}/5\mathbb{Z}^2$ is a constant Hamming-weight code. $\mathcal{C}$ is not a constant Lee-weight code, since $(2, 3) \in \mathcal{C}$ has Lee weight 4, while $(1, 4)$ has Lee weight 2.
- $\mathcal{C} = \langle (1, 0, 3) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ is a constant Hamming-weight code. $\mathcal{C}$ is not a constant Lee-weight code, since $(2, 0, 2) \in \mathcal{C}$ has Lee weight 4, while $(1, 0, 3)$ has Lee weight 2.

Constant Lee-Weight Codes

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

Theorem

Any constant Lee-weight code is equivalent to an ℓ-fold duplicate of shortest length constant Lee-weight codes.

Constant Lee-Weight Codes

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

Theorem

Any constant Lee-weight code is equivalent to an ℓ-fold duplicate of shortest length constant Lee-weight codes.

Let U be the collection of orbits of $(\mathbb{Z}/p^s\mathbb{Z})^K$ under the action of $\{1, -1\}$.

1. If $s = 1$: a representative of each member of U appears as a column of a generator matrix with the same multiplicity.

Constant Lee-Weight Codes

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

Theorem

Any constant Lee-weight code is equivalent to an ℓ-fold duplicate of shortest length constant Lee-weight codes.

Let U be the collection of orbits of $(\mathbb{Z}/p^s\mathbb{Z})^K$ under the action of $\{1, -1\}$.

1. If $s = 1$: a representative of each member of U appears as a column of a generator matrix with the same multiplicity.

Example

$\mathcal{C} = \langle (1, 2) \rangle \subseteq \mathbb{Z}/5\mathbb{Z}^2$ is a constant Lee-weight code.

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

2. If $p = 2$: every non-zero element of $(\mathbb{Z}/2^s\mathbb{Z})^K$ appears as a column of the generator matrix with the same multiplicity.

Constant Lee-Weight Codes

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

2. If $p = 2$: every non-zero element of $(\mathbb{Z}/2^s\mathbb{Z})^K$ appears as a column of the generator matrix with the same multiplicity.

Example

$\mathcal{C} = \langle (1,2,3) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ is a constant Lee-weight code.

Constant Lee-Weight Codes

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

2. If $p = 2$: every non-zero element of $(\mathbb{Z}/2^s\mathbb{Z})^K$ appears as a column of the generator matrix with the same multiplicity.

Example

$\mathcal{C} = \langle (1, 2, 3) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$ is a constant Lee-weight code.

3. We have $K \leq 2$.

Constant Lee-Weight Codes

Theorem (Byrne, W.)

Let $\mathcal{C}$ be a shortest-length constant Lee-weight code over $\mathbb{Z}/p^s\mathbb{Z}$ of rank $K = 1$ and weight w. Let i be such that $k_i = 1$. Then $\mathcal{C}$ has support subtype $(0, \ldots, 0, n_{i-1}, n_i, \ldots, n_{s-1}, 0)$ with

$$w = \frac{p+1}{4} p^{s-1} n_{i-1},$$
$$n_{i-1}(p-1) = p^{j-i+2} n_j \ \forall j \in \{1, \ldots, s\}.$$

Proof idea:

Use the exact average weight, i.e.,

$$(|\mathcal{C}| - 1)\overline{\mathrm{wt}_L}(\mathcal{C}) = \frac{|\mathcal{C}|}{4p^s} \sum_{i=0}^{s-1} n_i \left(p^{2s} - p^{2i}\right)$$

inductively on the subcodes $\mathcal{C}_{j-i+1} = \mathcal{C} \cap \langle p^{j-i+2} \rangle$ of size p^{j-i+2} and support subtype $(0, \ldots, 0, n_{i-1}, \ldots, n_j, z)$.

Theorem (Byrne, W.)

Let $g \in \langle p^{i-1} \rangle$ consist of

- *p repetitions of all elements in $\langle p^{i-1} \rangle \setminus \langle p^i \rangle$ up to ± 1 and*
- *$p-1$ repetitions of all elements in $\langle p^j \rangle \setminus \langle p^{j+1} \rangle$ up to ± 1 for all $j \in \{i, \ldots, s-1\}$,*

then $\langle g \rangle$ is a shortest constant Lee-weight code over $\mathbb{Z}/p^s\mathbb{Z}$ with $k_i = 1$.

Example

Over $\mathbb{Z}/9\mathbb{Z}$ for $k_1 = 1$ we have

$$g = (1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 4).$$

Constant Lee-Weight Codes

Theorem (Byrne, W.)

A constant Lee-weight code over $\mathbb{Z}/p^s\mathbb{Z}$ of rank 2 with $k_{s-1} = 0$ cannot exist.

Example

Over $\mathbb{Z}/27\mathbb{Z}$ for $k_2 = k_3 = 1$ we have

$$G = \begin{bmatrix} 3 & 3 & 3 & 6 & 6 & 6 & 12 & 12 & 12 & 9 & 9 & 0 \\ 0 & 9 & 18 & 0 & 9 & 18 & 0 & 9 & 18 & 9 & 18 & 9 \end{bmatrix}.$$

Summary

- The density of MLD codes is 0 for $n \to \infty$.
- The density of MLD codes is 0 for $p \to \infty$.
- Plotkin-optimal linear codes in the Lee metric are sparse.

Summary

- The density of MLD codes is 0 for $n \to \infty$.
- The density of MLD codes is 0 for $p \to \infty$.
- Plotkin-optimal linear codes in the Lee metric are sparse.

Open Questions

- Establish a 'better' Singleton bound for the Lee metric.
- How close do codes get to this bound, i.e., are there almost-MLD codes?
- What about other ambient spaces, other metrics, other bounds?

Eimear Byrne and Violetta Weger "Bounds in the Lee metric and optimal codes", 2021.

Thank you!