RING-LINEAR CODES

DIFFERENCE TO CLASSICAL CODES:

	classical	Ring-linear
Ambient space	finite field $\mathbb{F}_q$	finite ring R

DEFINITION

$(K,+,\cdot)$ = field if

1. $(K,+)$ = abelian group
   - $+$ is associate
   - $+$ is commutative
   - $+$ has a neutral element 0
   - $+$ has inverses
2. $(K\setminus\{0\},\cdot)$ = abelian group
3. Distributivity

$(R,+,\cdot)$ = ring if

1. $(R,+)$ = abelian group
2. $(R,\cdot)$ = semigroup
   - is associative
3. Distributivity

Difference: R does not necessarily have

- a neutral element for multiplication (usually denoted by 1)
- commutative multiplication
- multiplicative inverses

We restrict ourselves to the rings $\mathbb{Z}/p^s\mathbb{Z}$

- We do have a neutral element for multiplication
- multiplication is commutative
- no multiplicative inverses

EXAMPLE:

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ with $\alpha^2 = \alpha+1$

$\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

2 has no multiplicative inverse

Units of $\mathbb{Z}/p^s\mathbb{Z}$:

$$\mathbb{Z}/p^s\mathbb{Z}^\times = \{a \in \{1, \dots, p^s - 1\} \mid p \nmid a\}$$

$$|\mathbb{Z}/p^s\mathbb{Z}^\times| = p^{s-1}(p-1)$$

DIFFERENCE TO CLASSICAL CODES:

	classical	Ring-linear
Ambient space	finite field $\mathbb{F}_q$	finite ring $\mathbb{Z}/p^s\mathbb{Z}$
Linear code	subspace of $\mathbb{F}_q^n$	$\mathbb{Z}/p^s\mathbb{Z}$-submodule of $(\mathbb{Z}/p^s\mathbb{Z})^n$

DEFINITION

If $(K, +, \cdot)$ is a field then $(V, \oplus, \odot)$ is a vectorspace if

1. $(V, \oplus)$ is an abelian group
2. $\odot : K \times V \to V$
   - is distributive with $\oplus$
   - $(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v)$
   - $1 \odot v = v$

If $(R, +, \cdot)$ is a ring then $(M, \oplus, \odot)$ is a module if

1. $(M, \oplus)$ is an abelian group
2. $\odot : R \times M \to M$
   - is distributive with $\oplus$
   - $(\alpha \cdot \beta) \odot m = \alpha \odot (\beta \odot m)$

Important difference

A vector space has a basis: Recall $(b_1, \dots, b_r)$ = basis for V if every $v \in V$ can be written as linear combination $v = \sum_{i=1}^{n} b_i \lambda_i$ for some $\lambda_i \in K$ UNIQUELY

EXAMPLE

$R = \mathbb{Z}/4\mathbb{Z}$, $M = 2\mathbb{Z}/4\mathbb{Z} = \{0, 2\}$

$\{2\}$ ≠ basis !

$0 = 2 \cdot 0 = 2 \cdot 2$ and $2 = 2 \cdot 1 = 2 \cdot 3$

DEFINITION

If $(V, \oplus, \odot)$ is a vectorspace with neutral additive element 0 then $C \subseteq V$ is a subspace if

$\forall x, y \in C \quad \forall r \in K$

1. $x + y \in C$
2. $0 \in C$
3. $r \cdot x \in C$

If $(M, \oplus, \odot)$ is a module with neutral element 0 then $C \subseteq M$ is a submodule if

$\forall x, y \in C \quad \forall r \in R$

1. $x + y \in C$
2. $0 \in C$
3. $r \cdot x \in C$

That is : we want the same as in the classical case

EXAMPLE :

- $C_0 = \langle (\alpha+1, 1, \alpha) \rangle \subseteq \mathbb{F}_4^3$

  $= \{(0,0,0), (\alpha+1, 1, \alpha), (1, \alpha, \alpha+1), (\alpha, \alpha+1, 1)\}$

  parameters: length $n = 3$, dimension $k = 1$

  $q = 4$

  $\Rightarrow \quad |C_0| = q^k = 4$

EXAMPLE

- $C_1 = \langle (1,2,3) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$
  $= \{(0,0,0), (1,2,3), (2,0,2), (3,2,1)\}$
  parameters: length $n = 3$, 1 generator, $p^s = 4$
  $|C_1| = 4$

- $C_2 = \langle (2,0,2) \rangle \subseteq \mathbb{Z}/4\mathbb{Z}^3$
  $= \{(0,0,0), (2,0,2)\}$
  parameters: length $n = 3$, 1 generator, $p^s = 4$
  $|C_2| = 2$

DIFFERENCE TO CLASSICAL CODES:

	classical	Ring-linear
Ambient space	finite field $\mathbb{F}_q$	finite ring $\mathbb{Z}/p^s\mathbb{Z}$
Linear code	subspace of $\mathbb{F}_q^n$	$\mathbb{Z}/p^s\mathbb{Z}$-submodule of $\mathbb{Z}/p^s\mathbb{Z}^n$
parameters	length n dimension k	length n type k subtype $(k_1, \dots, k_s)$ rank k

DEFINITION

For a code $\mathcal{C} \subseteq \mathbb{Z}/p^s\mathbb{Z}^n$

- type $k = \log_{p^s}(|\mathcal{C}|)$
- subtype $(k_1, \dots, k_s)$ where k_i = number of generators with $p^{i-1} \mid k_i$ but $p^i \nmid k_i$
- rank K - minimal number of generators

SYSTEMATIC FORM OF GENERATOR MATRIX

- $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k then

$$G = \begin{bmatrix} Id_k & A \end{bmatrix} \in \mathbb{F}_q^{k \times n}$$

$$A \in \mathbb{F}_q^{k \times n-k}$$

- $\mathcal{C} \subseteq \mathbb{Z}/p^s\mathbb{Z}^n$ of subtype $(k_1, \dots, k_s)$, rank K

$$G = \begin{bmatrix} Id_{k_1} & & & & * \\ & pId_{k_2} & & & \\ & & p^2Id_{k_3} & & \\ & & & \ddots & \\ 0 & & & & p^{s-1}Id_{k_s} \end{bmatrix}$$

$$\in \mathbb{Z}/p^s\mathbb{Z}^{K \times n}$$

Relations:

- $\sum_{i=1}^{s} k_i = \overline{k}$
- $\sum_{i=1}^{s} k_i (s-i+1)/s = k$

EXAMPLE

$\ell = \langle (2,2,0), (1,2,3) \rangle \leq \mathbb{Z}/4\mathbb{Z}^3$, $p=2$, $s=2$

$= \{ (0,0,0), (1,0,1), (2,0,2), (3,0,3), (0,2,2), (1,2,3), (2,2,0), (3,2,1) \}$

$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \end{bmatrix}$ $k_1 = 1$, $k_2 = 1$, $\overline{k} = 2$

$k = k_1 + k_2 \frac{s-1}{s} = 3/2$

$|\ell| = p^{s \cdot k} = 4^{3/2} = 4 \cdot 2 = 8$

Over $\mathbb{Z}/p^s\mathbb{Z}$ have several choices of metrics

- Hamming
- Rank
- Homogeneous
- Lee

LEE METRIC

DEFINITION:

for $x \in \mathbb{Z}/p^s\mathbb{Z}$ represented in $\{0, \dots, p^s-1\}$

- $Wt_L(x) = \min\{x, |p^s - x|\}$

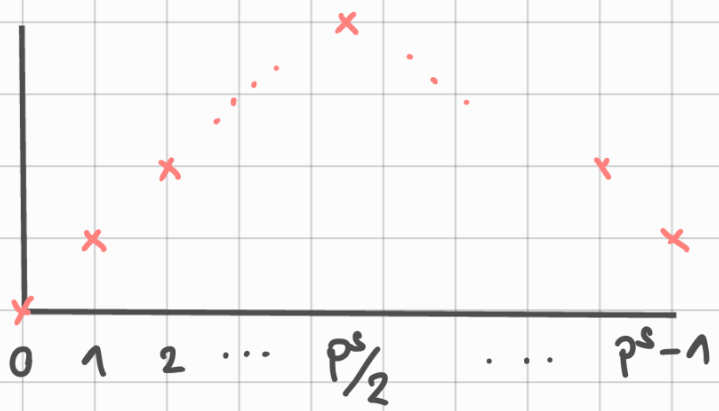
for $y, z \in (\mathbb{Z}/p^s\mathbb{Z})^n$

- $Wt_L(y) = \sum_{i=1}^{n} Wt_L(y_i)$

- $d_L(y,z) = Wt_L(y-z)$

EXAMPLE $\mathbb{Z}/9\mathbb{Z}$

- $wt_L(0) = 0$
- $wt_L(1) = 1$
- $wt_L(2) = 2$
- $wt_L(3) = 3$
- $wt_L(4) = 4$
- $wt_L(5) = 4$
- $wt_L(6) = 3$
- $wt_L(7) = 2$
- $wt_L(8) = 1$



like L_1-Norm but modulo p^s

Define $M = \lfloor \frac{p^s}{2} \rfloor$

For any $x \in \mathbb{Z}/p^s\mathbb{Z}^n$

$$0 \leq Wt_H(x) \leq Wt_L(x) \leq M \cdot Wt_H(x) \leq M \cdot n \quad \} \circledast$$

DEFINITION

For $\mathcal{C} \subseteq \mathbb{Z}/p^s\mathbb{Z}^n$ the minimum Lee distance of $\mathcal{C}$

$$d_L(\mathcal{C}) = \min \{ wt_L(x) \mid x \in \mathcal{C}, x \neq 0 \}$$

$\circledast \Rightarrow \quad d_L(\mathcal{C}) \geq d_H(\mathcal{C})$

→ The Lee metric has a larger error correction capacity

EXAMPLE

$\mathcal{C} = \langle (1,1,1,3) \rangle \subseteq \mathbb{Z}/8\mathbb{Z}^4$

$= \{ (0,0,0,0), (1,1,1,3), (2,2,2,6), (3,3,3,0), (4,4,4,3), (5,5,5,6), (6,6,6,0), (7,7,7,3), (8,8,8,6) \}$

$d_H(\mathcal{C}) = 3$ min wt codewords: $(3,3,3,0)$ & $(6,6,6,0)$

→ can correct 1 error

$d_L(\mathcal{C}) = 5$ min wt codewords: $(1,1,1,3), (8,8,8,6)$

→ can correct 2 errors

BOUNDS

Singleton bound:

Let $C \leq \mathbb{F}_q^n$ of dimension k, then

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

Proof idea:

puncture C in $d_H(C) - 1$ positions:
resulting codewords are still all different
$\rightarrow q^k$ many, new length of the code: $n - d_H(C) + 1$
$\rightarrow \quad k \leq n - d_H(C) + 1$

MDS codes: $d_H(C) = n - k + 1$

- have a construction for $n \leq q+1$
  (extended) Reed-Solomon codes
- MDS conjecture: for $n > q+1$ (q odd)
  there are No MDS codes

  $\Rightarrow$ if q is fixed & $n \to \infty$
  MDS codes are sparse
- If n is fixed and $q \to \infty$: MDS codes are dense

Lee-metric Singleton bound

(Shiromoto, 2000)

Let $\mathcal{C} \leq \mathbb{Z}/p^s\mathbb{Z}^n$ have type k, then

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

Proof idea:

- $d_L(\mathcal{C}) \leq M \cdot d_H(\mathcal{C})$
- $d_H(\mathcal{C}) \leq n-k+1$
- If $d_L(\mathcal{C}) \leq a\, d_H(\mathcal{C})$ for some a, then $\left\lfloor \frac{d_L(\mathcal{C})-1}{a} \right\rfloor \leq d_H(\mathcal{C})-1$

How good is this bound?

→ It's sharp: EXAMPLE

$\mathcal{C} = \langle (1,2) \rangle \leq \mathbb{Z}/6\mathbb{Z}^2$ attains the bound since $d_L(\mathcal{C}) = 3$, $M = 2$, $k = 1$

$$\left\lfloor \frac{d_L - 1}{M} \right\rfloor = 1 = n-k$$

How many codes attain this bound?

The only linear code that attains the Lee-metric Singleton bound is equivalent to

$$\ell = \langle (1,2) \rangle \leq \mathbb{Z}/5\mathbb{Z}^2$$

⇒ There are no maximum lee-distance codes for $\mathbb{Z}/p^s\mathbb{Z}$ if $p^s \neq 5$ or for length $n \neq 2$

⇒ super sparse