[1]Enumeration formulae for self-orthogonal, self-dual and LCD codes over finite commutative chain rings

Monika Yadav
Department of Mathematics
INDRAPRASTHA INSTITUTE *of* INFORMATION TECHNOLOGY **DELHI**

Coding Theory and Cryptography
A conference in honour of Prof. Joachim Rosenthal's 60th birthday
July 11-15, 2022
Zurich, Switzerland

[1]This is a joint work with Prof. Anuradha Sharma, Department of Mathematics, IIIT-Delhi.

Definition

A commutative ring $\mathcal{R}$ with unity is called a chain ring if all its ideals form a chain under the set-theoretic inclusion.

Examples of finite commutative chain rings are:

(i) Finite fields

(ii) Galois rings

(iii) Quasi-Galois rings

Definition

A commutative ring $\mathcal{R}$ with unity is called a chain ring if all its ideals form a chain under the set-theoretic inclusion.

Examples of finite commutative chain rings are:

(i) Finite fields
(ii) Galois rings
(iii) Quasi-Galois rings

Theorem

A finite commutative ring $\mathcal{R}$ with unity is a chain ring if and only if $\mathcal{R}$ is a principal ideal ring and has a unique maximal ideal.

The nilpotency index of a finite commutative chain ring $\mathcal{R}$ is defined as the nilpotency index of the unique maximal ideal of $\mathcal{R}$.

$\mathcal{R}_e$	a finite commutative chain ring with the nilpotency index e
u	a generator of the maximal ideal of $\mathcal{R}_e$
$\overline{\mathcal{R}}_e$	$\mathcal{R}_e/\langle u\rangle$, the residue field of $\mathcal{R}_e$
$\lvert\overline{\mathcal{R}}_e\rvert$	p^r, where p is a prime number and r is a positive integer
n	positive integer
$\mathcal{R}_e^n$	$\mathcal{R}_e$-module consisting of all n-tuples over $\mathcal{R}_e$

$\mathcal{R}_e$	a finite commutative chain ring with the nilpotency index e
u	a generator of the maximal ideal of $\mathcal{R}_e$
$\overline{\mathcal{R}}_e$	$\mathcal{R}_e/\langle u\rangle$, the residue field of $\mathcal{R}_e$
$\lvert\overline{\mathcal{R}}_e\rvert$	p^r, where p is a prime number and r is a positive integer
n	positive integer
$\mathcal{R}_e^n$	$\mathcal{R}_e$-module consisting of all n-tuples over $\mathcal{R}_e$

Linear code

A linear code $\mathcal{C}$ of length n over $\mathcal{R}_e$ is defined as an $\mathcal{R}_e$-submodule of $\mathcal{R}_e^n$.

Generator matrix for a linear code

A generator matrix for a linear code $\mathcal{C}$ over $\mathcal{R}_e$ is defined as a matrix over $\mathcal{R}_e$ whose rows form a minimal generating set of the code $\mathcal{C}$.

Next for positive integers k and ℓ, let $M_{k\times\ell}(\mathcal{R}_e)$ denote the set of all $k\times\ell$ matrices over $\mathcal{R}_e$.

Theorem [Norton and Sălăgean (2000)]

Every linear code $\mathcal{C}$ of length n over $\mathcal{R}_e$ is permutation equivalent to a code with a generator matrix G in the standard form

$$G=\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} & \cdots & A_{1,e-1} & A_{1,e} \\ 0 & uI_{k_2} & uA_{2,2} & \cdots & uA_{2,e-1} & uA_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u^{e-2}A_{e-1,e-1} & u^{e-2}A_{e-1,e} \\ 0 & 0 & 0 & \cdots & u^{e-1}I_{k_e} & u^{e-1}A_{e,e} \end{bmatrix}, \qquad (1)$$

where the columns of the matrix G are grouped into blocks of sizes $k_1,\ k_2,\ \cdots,\ k_{e-1}$, $k_e,\ k_{e+1}=n-(k_1+k_2+\cdots+k_e)$, the matrix I_{k_i} is the $k_i\times\ k_i$ identity matrix over $\mathcal{R}_e$ and the matrix $A_{i,j}\in M_{k_i\times k_{j+1}}(\mathcal{R}_e)$ is considered modulo u^{j-i+1} for $1\leq i\leq j\leq e$.

A linear code $\mathcal{C}$ of length n over $\mathcal{R}_e$ is said to be of the type $\{k_1,k_2,k_3,\cdots,k_e\}$ if it is permutation equivalent to a code with a generator matrix G of the form (1).

Euclidean bilinear form

The Euclidean bilinear form is a mapping $\langle \cdot, \cdot \rangle : \mathcal{R}_e^n \times \mathcal{R}_e^n \to \mathcal{R}_e$, defined as

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

for $x = (x_1, x_2, \cdots, x_n)$, $y = (y_1, y_2, \cdots, y_n) \in \mathcal{R}_e^n$.

The dual code

The dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ of length n over $\mathcal{R}_e$ is defined as

$$\mathcal{C}^\perp = \{y \in \mathcal{R}_e^n \mid \langle x, y \rangle = 0 \text{ for all } x \in \mathcal{C}\}.$$

Note that

1. the dual code $\mathcal{C}^\perp$ is also a linear code of length n over $\mathcal{R}_e$.
2. if the code $\mathcal{C}$ is of the type $\{k_1, k_2, \cdots, k_{e-1}, k_e\}$, then the dual code $\mathcal{C}^\perp$ is of the type $\{n - (k_1 + k_2 + \cdots + k_e), k_e, k_{e-1}, \cdots, k_2\}$.

Definition

A linear code $\mathcal{C}$ of length n over $\mathcal{R}_e$ is said to be

1. self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp}$.
2. self-dual if it satisfies $\mathcal{C} = \mathcal{C}^{\perp}$.
3. linear with complementary dual (LCD) if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$.

Pless (1968)	Self-orthogonal codes over finite fields
Betty and Munemasa (2009)	Self-orthogonal codes over $\mathbb{Z}_{p^2}$
Nagata *et al.* (2009)	Self-dual codes over $\mathbb{Z}_{p^3}$
Nagata *et al.* (2008, 2013)	Self-dual codes over $\mathbb{Z}_{p^s}$
Betty *et al.* (2018)	Self-dual codes over $\mathbb{F}_q[u]/<u^3>$
Vasquez and Petalcorin (2019)	Self-dual codes over $GR(p^3, r)$

Here p is a prime number, and $GR(p^3, r)$ denotes the Galois ring with characteristic p^3 and cardinality p^{3r}.

Enumeration formula for self-orthogonal codes over finite fields

For an integer k satisfying $0 \leq k \leq n$ and a prime power q, let $\sigma_q(n,k)$ denote the number of distinct (Euclidean) self-orthogonal codes of length n and dimension k over the finite field $\mathbb{F}_q$. We have $\sigma_q(n,0) = 1$ and $\sigma_q(n,k) = 0$ for all $k > \frac{n}{2}$.

Enumeration formula for self-orthogonal codes over finite fields

For an integer k satisfying $0 \leq k \leq n$ and a prime power q, let $\sigma_q(n,k)$ denote the number of distinct (Euclidean) self-orthogonal codes of length n and dimension k over the finite field $\mathbb{F}_q$. We have $\sigma_q(n,0) = 1$ and $\sigma_q(n,k) = 0$ for all $k > \frac{n}{2}$.

Theorem [Pless (1968)]

For an integer k satisfying $1 \leq k \leq \frac{n}{2}$ and a prime power q, we have

$$\sigma_q(n,k) = \begin{cases} \dfrac{\prod_{i=0}^{k-1}(q^{n-1-2i}-1)}{\prod_{j=1}^{k}(q^j-1)} & \text{if } n \text{ is odd;} \\[2ex] \dfrac{(q^{n-k}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{j=1}^{k}(q^j-1)} & \text{if both } n \text{ and } q \text{ are even;} \\[2ex] \dfrac{(q^{n-k}-q^{\frac{n}{2}-k}+q^{\frac{n}{2}}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{j=1}^{k}(q^j-1)} & \text{if } n \text{ is even, } q \text{ is odd and } (-1)^{\frac{n}{2}} \text{ is a square in } \mathbb{F}_q; \\[2ex] \dfrac{(q^{n-k}+q^{\frac{n}{2}-k}-q^{\frac{n}{2}}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{j=1}^{k}(q^j-1)} & \text{if } n \text{ is even, } q \text{ is odd and } (-1)^{\frac{n}{2}} \text{ is not a square in } \mathbb{F}_q. \end{cases}$$

Enumeration formula for self-dual codes of length n over $\mathbb{F}_q$

- If $\mathcal{C}$ is a self-dual code of length n and dimension k over $\mathbb{F}_q$, then n must be an even integer and $k = \frac{n}{2}$.
- When n is an even integer and q is an odd prime power, we have

$$\sigma_q\left(n, \frac{n}{2}\right) = \begin{cases} 2\prod_{i=1}^{\frac{n}{2}-1}(q^i+1) & \text{if } (-1)^{\frac{n}{2}} \text{ is a square in } \mathbb{F}_q; \\ 0 & \text{otherwise.} \end{cases}$$

- When both n, q are even, we have

$$\sigma_q\left(n, \frac{n}{2}\right) = \prod_{j=1}^{\frac{n}{2}-1}(q^j+1).$$

Enumeration formula for self-dual codes of length n over $\mathbb{F}_q$

- If $\mathcal{C}$ is a self-dual code of length n and dimension k over $\mathbb{F}_q$, then n must be an even integer and $k = \frac{n}{2}$.
- When n is an even integer and q is an odd prime power, we have

$$\sigma_q\left(n, \frac{n}{2}\right) = \begin{cases} 2\prod_{i=1}^{\frac{n}{2}-1}(q^i+1) & \text{if } (-1)^{\frac{n}{2}} \text{ is a square in } \mathbb{F}_q; \\ 0 & \text{otherwise.} \end{cases}$$

- When both n, q are even, we have

$$\sigma_q\left(n, \frac{n}{2}\right) = \prod_{j=1}^{\frac{n}{2}-1}(q^j+1).$$

Gaussian binomial coefficient

For $1 \leq k \leq n$ and a prime power q, the Gaussian binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

(Recall that the Gaussian binomial coefficient $\begin{bmatrix} n \\ 0 \end{bmatrix}_q$ is assigned the value 1.)

The number of distinct k-dimensional subspaces of an n-dimensional vector space over the finite field $\mathbb{F}_q$ equals $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for $0 \leq k \leq n$.

From now on, let

$k_1, k_2, \cdots, k_{e+1}$ non-negative integers, not all zero

$$n = k_1 + k_2 + \cdots + k_{e+1}$$

For integers t, ℓ satisfying $2 \leq t \leq \lceil \frac{e+1}{2} \rceil$ and $1 \leq \ell \leq t-1$, let us define

$$\begin{aligned}
h_\ell(k_1, k_2, \cdots, k_t) &= (k_1 + k_2 + \cdots + k_\ell)\Big(n - (k_1 + k_2 + \cdots + k_{\ell+1}) - 1\Big), \\
n_\ell(k_1, k_2, \cdots, k_t) &= (k_1 + k_2 + \cdots + k_\ell)\Big(n - (k_1 + k_2 + \cdots + k_{\ell+1}) - 1\Big) \\
&\quad + \Big((k_1 + k_2 + \cdots + k_{t-\beta}) + (k_1 + k_2 + \cdots + k_t) \\
&\quad - (k_1 + k_2 + \cdots + k_{\ell+1})\Big)\Big(n - (k_1 + k_2 + \cdots + k_{t-\beta}) \\
&\quad - (k_1 + k_2 + \cdots + k_t)\Big),
\end{aligned}$$

where $\beta = 1$ if e is even, while $\beta = 0$ if e is odd.

Enumeration formula for self-orthogonal codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ I

Theorem [____ & Sharma (2021)]

Let $\mathcal{N}_e(n; k_1, k_2, \cdots, k_e)$ denote the number of distinct self-orthogonal codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$. Let $|\overline{\mathcal{R}}_e| = p^r$, where p is an odd prime and r is a positive integer.

- When e is odd, we have

$$\mathcal{N}_e(n; k_1, k_2, \cdots, k_{e-1}, k_e)$$

$$= \begin{cases} \sigma_{p^r}\left(n, k_1 + k_2 + \cdots + k_{\frac{e+1}{2}}\right) \prod\limits_{i=1}^{\frac{e+1}{2}} \begin{bmatrix} k_1+k_2+\cdots+k_i \\ k_i \end{bmatrix}_{p^r} \\ \times \prod\limits_{j=2}^{\frac{e+1}{2}} \begin{bmatrix} k_j + k_{e+1-k_1} \\ k_j \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{\ell=1}^{\frac{e-1}{2}} n_\ell(k_1, k_2, \cdots, k_{\frac{e+1}{2}})} \\ \text{if } k_1 \leq k_{e+1} \text{ and } k_s = k_{e-s+2} \text{ for } 2 \leq s \leq e; \\ 0 \qquad \text{otherwise.} \end{cases}$$

Enumeration formula for self-orthogonal codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ II

- When e is even, we have

$$\mathcal{N}_e(n; k_1, k_2, \cdots, k_{e-1}, k_e)$$

$$= \begin{cases} \sigma_{p^r}\left(n, k_1 + k_2 + \cdots + k_{\frac{e}{2}}\right) \prod_{i=1}^{\frac{e}{2}} {k_1+k_2+\cdots+k_i \brack k_i}_{p^r} \\ \times \prod_{j=2}^{\frac{e}{2}+1} {k_j+k_{e+1}-k_1 \brack k_j}_{p^r} (p^r)^{\sum_{\ell=1}^{\frac{e}{2}} n_\ell(k_1,k_2,\cdots,k_{\frac{e}{2}+1}) + \Theta_e^\star(k_1,k_2,\cdots,k_{\frac{e}{2}+1})} \\ \quad \text{if } k_1 \le k_{e+1} \text{ and } k_s = k_{e-s+2} \text{ for } 2 \le s \le e; \\ 0 \quad\quad \text{otherwise,} \end{cases}$$

where

$$\Theta_e^\star(k_1, k_2, \cdots, k_{\frac{e}{2}+1}) = -(k_1 + k_2 + \cdots + k_{\frac{e}{2}})\left(\frac{k_1+k_2+\cdots+k_{\frac{e}{2}}+2k_{e+1}-2k_1-1}{2}\right).$$

Outline of the proof I

Let $\mathcal{C}$ be a linear code of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ with a generator matrix

$$G = \begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} & \cdots & A_{1,e-1} & A_{1,e} \\ 0 & uI_{k_2} & uA_{2,2} & \cdots & uA_{2,e-1} & uA_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u^{e-2}A_{e-1,e-1} & u^{e-2}A_{e-1,e} \\ 0 & 0 & 0 & \cdots & u^{e-1}I_{k_e} & u^{e-1}A_{e,e} \end{bmatrix} = \begin{bmatrix} T_1 \\ uT_2 \\ \vdots \\ u^{e-2}T_{e-1} \\ u^{e-1}T_e \end{bmatrix},$$

where $k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathcal{R}_e$ and $A_{i,j} \in M_{k_i \times k_{j+1}}(\mathcal{R}_e)$ is considered modulo u^{j-i+1} for $1 \leq i \leq j \leq e$.

Then the code $\mathcal{C}$ is self-orthogonal if and only if $k_1 \leq k_{e+1}$, $k_s = k_{e-s+2}$ for $2 \leq s \leq e$, and

$$T_i T_j^t \equiv 0 \pmod{u^{e-i-j+2}}$$

for all integers i and j satisfying $1 \leq i \leq j \leq e$ and $i + j \leq e + 1$.

Further, the self-orthogonal code $\mathcal{C}$ of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ is self-dual if and only if $k_1 = k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$.

Outline of the proof II

For an integer $e \geq 4$, the quotient ring $\mathcal{R}_e/\langle u^{e-2}\rangle$ is a finite commutative chain ring with the nilpotency index $e-2$ and with the unique maximal ideal as $\langle u + \langle u^{e-2}\rangle\rangle$, which we shall denote by $\mathcal{R}_{e-2}$.

Outline of the proof II

For an integer $e \geq 4$, the quotient ring $\mathcal{R}_e/\langle u^{e-2}\rangle$ is a finite commutative chain ring with the nilpotency index $e-2$ and with the unique maximal ideal as $\langle u + \langle u^{e-2}\rangle\rangle$, which we shall denote by $\mathcal{R}_{e-2}$.

Now for $e \geq 4$, let $k_1, k_2, \cdots, k_{e+1}$ be non-negative integers satisfying $k_1 \leq k_{e+1}$ and $k_j = k_{e-j+2}$ for $2 \leq j \leq e$, and let $n = k_1 + k_2 + \cdots + k_{e+1}$.

Outline of the proof II

For an integer $e \geq 4$, the quotient ring $\mathcal{R}_e/\langle u^{e-2}\rangle$ is a finite commutative chain ring with the nilpotency index $e-2$ and with the unique maximal ideal as $\langle u + \langle u^{e-2}\rangle\rangle$, which we shall denote by $\mathcal{R}_{e-2}$.

Now for $e \geq 4$, let $k_1, k_2, \cdots, k_{e+1}$ be non-negative integers satisfying $k_1 \leq k_{e+1}$ and $k_j = k_{e-j+2}$ for $2 \leq j \leq e$, and let $n = k_1 + k_2 + \cdots + k_{e+1}$.

- There exists a self-orthogonal code of the type $\{k_1, k_2, \cdots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_e$ if and only if there exists a self-orthogonal code of the type $\{k_1 + k_2, k_3, \cdots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2}$.

Outline of the proof II

For an integer $e \geq 4$, the quotient ring $\mathcal{R}_e/\langle u^{e-2}\rangle$ is a finite commutative chain ring with the nilpotency index $e-2$ and with the unique maximal ideal as $\langle u + \langle u^{e-2}\rangle\rangle$, which we shall denote by $\mathcal{R}_{e-2}$.

Now for $e \geq 4$, let $k_1, k_2, \cdots, k_{e+1}$ be non-negative integers satisfying $k_1 \leq k_{e+1}$ and $k_j = k_{e-j+2}$ for $2 \leq j \leq e$, and let $n = k_1 + k_2 + \cdots + k_{e+1}$.

- There exists a self-orthogonal code of the type $\{k_1, k_2, \cdots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_e$ if and only if there exists a self-orthogonal code of the type $\{k_1 + k_2, k_3, \cdots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2}$.
- Moreover, each self-orthogonal code of the type $\{k_1 + k_2, k_3, k_4, \cdots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2}$ gives rise to precisely

$$\begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)+\sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)}$$

distinct self-orthogonal codes of the type $\{k_1, k_2, k_3, \cdots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_e$.

Outline of the proof III

- For $e \geq 4$, we have

$$\mathcal{N}_e(n; k_1, k_2, \cdots, k_e) = \mathcal{N}_{e-2}(n; k_1 + k_2, k_3, \cdots, k_{e-1}) \begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \times \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)+\sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)}.$$

Outline of the proof III

- For $e \geq 4$, we have

$$\mathcal{N}_e(n; k_1, k_2, \cdots, k_e) = \mathcal{N}_{e-2}(n; k_1 + k_2, k_3, \cdots, k_{e-1}) \begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \times \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)+\sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)}.$$

The case $e = 2$

$$\mathcal{N}_2(n; k_1, k_2) = \begin{cases} \sigma_{p^r}(n, k_1) \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_{p^r} (p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}} & \text{if } n \geq 2k_1 + k_2; \\ 0 & \text{otherwise.} \end{cases}$$

Outline of the proof III

- For $e \geq 4$, we have

$$\mathcal{N}_e(n; k_1, k_2, \cdots, k_e) = \mathcal{N}_{e-2}(n; k_1 + k_2, k_3, \cdots, k_{e-1}) \begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \times \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)+\sum_{i=1}^{e-1} k_i(k_{e+1}-k_1)}.$$

The case $e = 2$

$$\mathcal{N}_2(n; k_1, k_2) = \begin{cases} \sigma_{p^r}(n, k_1) \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_{p^r} (p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}} & \text{if } n \geq 2k_1 + k_2; \\ 0 & \text{otherwise.} \end{cases}$$

The case $e = 3$

$$\mathcal{N}_3(n; k_1, k_2, k_3) = \begin{cases} \sigma_{p^r}(n, k_1 + k_2) \begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} n-2k_1-k_2 \\ k_2 \end{bmatrix}_{p^r} (p^r)^{k_1(2n-3k_1-1)+k_2(n-5k_1-2k_2)} \\ \text{if } k_2 = k_3 \text{ and } n \geq 2k_1 + 2k_2; \\ 0 \quad \text{otherwise.} \end{cases}$$

$\mathcal{N}_e(n)$ the number of distinct self-orthogonal codes of length n over $\mathcal{R}_e$

$$\mathcal{N}_e(n) = \sum_{\substack{k_1,k_2,\cdots,k_{e+1}\geq 0\\ n=k_1+k_2+\cdots+k_{e+1}}} \mathcal{N}_e(n;k_1,k_2,\cdots,k_e)$$

Theorem [____ & Sharma (2021)]

Let $|\overline{\mathcal{R}}_e| = p^r$, where p is an odd prime and r is a positive integer.

- When e is odd, we have

$$\mathcal{N}_e(n) = \sum_{\substack{k_1,k_2,\cdots,k_{\frac{e+1}{2}}\geq 0\\ 0\leq k_1+k_2+\cdots+k_{\frac{e+1}{2}}\leq \lfloor \frac{n}{2}\rfloor}} \sigma_{p^r}\left(n, k_1+k_2+\cdots+k_{\frac{e+1}{2}}\right)$$

$$\times \prod_{i=1}^{\frac{e+1}{2}} \begin{bmatrix} k_1+k_2+\cdots+k_i \\ k_i \end{bmatrix}_{p^r} (p^r)^{\sum_{\ell=1}^{\frac{e-1}{2}} n_\ell(k_1,k_2,\cdots,k_{\frac{e+1}{2}})}$$

$$\times \prod_{j=2}^{\frac{e+1}{2}} \begin{bmatrix} k_j+n-2(k_1+k_2+\cdots+k_{\frac{e+1}{2}}) \\ k_j \end{bmatrix}_{p^r}.$$

- When e is even, we have

$$\mathcal{N}_e(n) = \sum_{\substack{k_1,k_2,\cdots,k_{\frac{e}{2}+1}\geq 0\\ 0\leq 2k_1+\cdots+2k_{\frac{e}{2}}+k_{\frac{e}{2}+1}\leq n}} \sigma_{p^r}\left(n, k_1+k_2+\cdots+k_{\frac{e}{2}}\right)$$

$$\times \prod_{i=1}^{\frac{e}{2}} \begin{bmatrix} k_1+k_2+\cdots+k_i \\ k_i \end{bmatrix}_{p^r} (p^r)^{\sum_{\ell=1}^{\frac{e}{2}} n_\ell(k_1,k_2,\cdots,k_{\frac{e}{2}+1})+\Theta_e(k_1,k_2,\cdots,k_{\frac{e}{2}+1})}$$

$$\times \prod_{j=2}^{\frac{e}{2}+1} \begin{bmatrix} k_j+n-2(k_1+k_2+\cdots+k_{\frac{e}{2}})-k_{\frac{e}{2}+1} \\ k_j \end{bmatrix}_{p^r},$$

where

$$\Theta_e(k_1,k_2,\cdots,k_{\frac{e}{2}+1}) = -(k_1+k_2+\cdots+k_{\frac{e}{2}})\left(\frac{2n-3(k_1+k_2+\cdots+k_{\frac{e}{2}})-2k_{\frac{e}{2}+1}-1}{2}\right).$$

Enumeration formula for self-dual codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ I

Recall that a self-orthogonal code $\mathcal{C}$ of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ is self-dual if and only if $k_1 = k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$.

Enumeration formula for self-dual codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ I

Recall that a self-orthogonal code $\mathcal{C}$ of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ is self-dual if and only if $k_1 = k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$.

Theorem [____ & Sharma (2021)]

Let $\mathcal{M}_e(n; k_1, k_2, \cdots, k_e)$ denote the number of distinct self-dual codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$. Let $|\overline{\mathcal{R}}_e| = p^r$, where p is an odd prime and r is a positive integer.

- When e is odd, we have

$$\mathcal{M}_e(n; k_1, k_2, \cdots, k_e)$$

$$= \begin{cases} 2 \prod_{b=1}^{\frac{n}{2}-1} (p^{rb}+1) \prod_{i=1}^{\frac{e+1}{2}} \begin{bmatrix} k_1+k_2+\cdots+k_i \\ k_i \end{bmatrix}_{p^r} (p^r)^{\sum_{\ell=1}^{\frac{e-1}{2}} h_\ell(k_1, k_2, \cdots, k_{\frac{e+1}{2}})} \\ \text{if } n \text{ is even, } (-1)^{\frac{n}{2}} \text{ is a square in } \overline{\mathcal{R}}_e \text{ and } k_s = k_{e-s+2} \text{ for } 1 \leq s \leq e+1; \\ 0 \qquad \text{otherwise.} \end{cases}$$

Enumeration formula for self-dual codes of the type $\{k_1, k_2, \cdots, k_e\}$ and length n over $\mathcal{R}_e$ II

- When e is even, we have

$\mathcal{M}_e(n; k_1, k_2, \cdots, k_e)$

$$= \begin{cases} \sigma_{p^r}\left(n, k_1 + k_2 + \cdots + k_{\frac{e}{2}}\right) \prod_{i=1}^{\frac{e}{2}} {k_1+k_2+\cdots+k_i \brack k_i}_{p^r} \\ \times (p^r)^{\sum_{\ell=1}^{\frac{e}{2}} h_\ell(k_1,k_2,\cdots,k_{\frac{e}{2}+1}) + \lambda_e(k_1,k_2,\cdots,k_{\frac{e}{2}+1})} \\ \text{if } k_s = k_{e-s+2} \text{ for } 1 \le s \le e+1; \\ 0 \quad \text{otherwise,} \end{cases}$$

where $\lambda_e(k_1, k_2, \cdots, k_{\frac{e}{2}+1}) = -(k_1 + k_2 + \cdots + k_{\frac{e}{2}}) \binom{\frac{k_1+k_2+\cdots+k_{\frac{e}{2}}-1}{2}}{}$.

Enumeration formula for self-dual codes of length n over $\mathcal{R}_e$ I

$\mathcal{M}_e(n)$ the number of distinct self-dual codes of length n over $\mathcal{R}_e$

$$\mathcal{M}_e(n) = \sum_{\substack{k_1,k_2,\cdots,k_e\geq 0\\ n=2k_1+k_2+\cdots+k_e}} \mathcal{M}_e(n;k_1,k_2,\cdots,k_e)$$

Theorem [____ & Sharma (2021)]

Let $|\overline{\mathcal{R}}_e| = p^r$, where p is an odd prime and r is a positive integer.

- When e is even, we have

$$\mathcal{M}_e(n) = \sum_{\substack{k_1,k_2,\cdots,k_{\frac{e}{2}}\geq 0\\ 0\leq k_1+k_2+\cdots+k_{\frac{e}{2}}\leq \lfloor\frac{n}{2}\rfloor}} \sigma_{p^r}(n, k_1+k_2+\cdots+k_{\frac{e}{2}}) \prod_{i=1}^{\frac{e}{2}} \begin{bmatrix} k_1+k_2+\cdots+k_i \\ k_i \end{bmatrix}_{p^r}$$

$$\times (p^r)^{\sum_{\ell=1}^{\frac{e}{2}-1} h_\ell(k_1,k_2,\cdots,k_{\frac{e}{2}})+\lambda'_e(k_1,k_2,\cdots,k_{\frac{e}{2}})},$$

where $\lambda'_e(k_1,k_2,\cdots,k_{\frac{e}{2}}) = (k_1+k_2+\cdots+k_{\frac{e}{2}})\left(\frac{k_1+k_2+\cdots+k_{\frac{e}{2}}-1}{2}\right)$.

Enumeration formula for self-dual codes of length n over $\mathcal{R}_e$ II

- When e is odd, we have

$$\mathcal{M}_e(n) = \begin{cases} \displaystyle\sum_{\substack{k_1,k_2,\cdots,k_{\frac{e-1}{2}}\geq 0 \\ 0\leq k_1+k_2+\cdots+k_{\frac{e-1}{2}}\leq \frac{n}{2}}} 2\prod_{b=1}^{\frac{n}{2}-1}(p^{rb}+1)\prod_{i=1}^{\frac{e-1}{2}}\begin{bmatrix} k_1+k_2+\cdots+k_i \\ k_i \end{bmatrix}_{p^r} \\ \times \begin{bmatrix} \frac{n}{2} \\ k_1+k_2+\cdots+k_{\frac{e-1}{2}} \end{bmatrix}_{p^r} (p^r)^{\sum_{\ell=1}^{\frac{e-3}{2}} h_\ell(k_1,k_2,\cdots,k_{\frac{e-1}{2}})+\lambda_e^*(k_1,k_2,\cdots,k_{\frac{e-1}{2}})} \\ \quad \text{if } n \text{ is even and } (-1)^{\frac{n}{2}} \text{ is a square in } \overline{\mathcal{R}}_e; \\ 0 \qquad \text{otherwise,} \end{cases}$$

where $\lambda_e^*(k_1,k_2,\cdots,k_{\frac{e-1}{2}}) = \left(\frac{n}{2}-1\right)\left(k_1+k_2+\cdots+k_{\frac{e-1}{2}}\right)$.

Classification of self-orthogonal and self-dual codes

Two self-orthogonal (resp. self-dual) codes of length n over $\mathcal{R}_e$ are said to be equivalent if one code can be obtained from the other by a combination of operations of the following two types:

A. Permutation of the n coordinate positions of the code.

B. Multiplication of the code symbols appearing in a given coordinate position by the element $-1 \in \mathcal{R}_e$.

Let $\mathcal{E}_n$ denote the group generated by transformations of the types A and B.

Classification of self-orthogonal and self-dual codes

Two self-orthogonal (resp. self-dual) codes of length n over $\mathcal{R}_e$ are said to be equivalent if one code can be obtained from the other by a combination of operations of the following two types:

A. Permutation of the n coordinate positions of the code.

B. Multiplication of the code symbols appearing in a given coordinate position by the element $-1 \in \mathcal{R}_e$.

Let $\mathcal{E}_n$ denote the group generated by transformations of the types A and B.

Mass formula for self-orthogonal codes of length n over $\mathcal{R}_e$

$$\mathcal{N}_e(n) = \sum_{\mathcal{C}} \frac{|\mathcal{E}_n|}{|\mathcal{A}\mathrm{ut}(\mathcal{C})|},$$

where the summation $\sum_{\mathcal{C}}$ runs over all the inequivalent self-orthogonal codes $\mathcal{C}$ of length n over $\mathcal{R}_e$.

Mass formula for self-dual codes of length n over $\mathcal{R}_e$

$$\mathcal{M}_e(n) = \sum_{\mathcal{C}} \frac{|\mathcal{E}_n|}{|\mathcal{A}\mathrm{ut}(\mathcal{C})|},$$

where the summation $\sum_{\mathcal{C}}$ runs over all the inequivalent self-dual codes $\mathcal{C}$ of length n over $\mathcal{R}_e$.

Numerics

n	q	Total number of non-zero self-orthogonal codes of length n over $\mathbb{F}_q[u]/\langle u^2\rangle$	Number of inequivalent non-zero self-orthogonal codes of length n over $\mathbb{F}_q[u]/\langle u^2\rangle$
2	5	8	5
3	5	99	14
4	5	3195	63
5	5	227191	321
2	7	9	4
3	7	179	19
4	7	12598	118

Numerics

A self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathbb{F}_q[u]/ < u^2 >$ is self-dual if and only if

$$2k_1 + k_2 = n.$$

n	q	Total number of self-dual codes of length n over $\mathbb{F}_q[u]/\langle u^2\rangle$	Number of inequivalent self-dual codes of length n over $\mathbb{F}_q[u]/\langle u^2\rangle$
2	5	7	2
3	5	7	2
4	5	97	5
5	5	937	8
2	7	1	1
3	7	9	2
4	7	177	6

LCD codes over $\mathcal{R}_e$

Theorem [Bhowmick *et al.* (2020)]

Any LCD code C of length n over the finite commutative local Frobenius ring R is a free code, i.e., the code C is a free R-submodule of R^n.

Any LCD code $\mathcal{C}$ of length n over the finite commutative chain ring $\mathcal{R}_e$ is a free code, i.e., the code $\mathcal{C}$ is a free $\mathcal{R}_e$-submodule of $\mathcal{R}_e^n$.

As a consequence, the LCD code $\mathcal{C}$ is permutation equivalent to a code whose generator matrix G is in the standard form

$$G = [I_k \mid A],$$

where I_k is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix over $\mathcal{R}_e$.

The integer k is called the rank of the code $\mathcal{C}$.

Enumeration formula for LCD codes of length n and rank k over $\mathcal{R}_e$ I

Theorem [____ & Sharma (2022)]

Let $\mathcal{L}_e(n;k)$ denote the number of distinct LCD codes of length n and rank k over $\mathcal{R}_e$. Let $|\overline{\mathcal{R}}_e| = p^r$, where p is a prime number and r is a positive integer. We have $\mathcal{L}_e(n;0) = \mathcal{L}_e(n;n) = 1$.

Enumeration formula for LCD codes of length n and rank k over $\mathcal{R}_e$ I

Theorem [____ & Sharma (2022)]

Let $\mathcal{L}_e(n;k)$ denote the number of distinct LCD codes of length n and rank k over $\mathcal{R}_e$. Let $|\overline{\mathcal{R}}_e| = p^r$, where p is a prime number and r is a positive integer. We have $\mathcal{L}_e(n;0) = \mathcal{L}_e(n;n) = 1$. For $1 \leq k \leq n-1$, we have the following:

- When $p = 2$, we have

$$\mathcal{L}_e(n;k) = \begin{cases} 2^{\frac{r(n-k)(2k\ell-k+1)}{2}} {(n-1)/2 \brack (k-1)/2}_{2^{2r}} & \text{if both } k \text{ and } n \text{ are odd;} \\ 2^{\frac{r(k(n-k)(2\ell-1)+n-1)}{2}} {(n-2)/2 \brack (k-1)/2}_{2^{2r}} & \text{if } k \text{ is odd and } n \text{ is even;} \\ 2^{\frac{rk((n-k)(2\ell-1)+1)}{2}} {(n-1)/2 \brack k/2}_{2^{2r}} & \text{if } k \text{ is even and } n \text{ is odd;} \\ 2^{\frac{r(k(n-k)(2\ell-1)-2)}{2}} \Big((2^{rk}+2^r-1) {(n-2)/2 \brack k/2}_{2^{2r}} & \\ +(2^{r(n-k+1)} - 2^{r(n-k)} + 1) {(n-2)/2 \brack (k-2)/2}_{2^{2r}} \Big) & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

Enumeration formula for LCD codes of length n and rank k over $\mathcal{R}_e$ II

- When p is an odd prime, we have

$$\mathcal{L}_e(n;k) = \begin{cases} p^{\frac{r(n-k)(2k\ell-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \text{if both } k \text{ and } n \text{ are odd;} \\ p^{\frac{r(k(n-k)(2\ell-1)-1)}{2}} (p^{\frac{rn}{2}}-1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \text{if } k \text{ is odd and } n \text{ is even} \\ \text{with either } p^r \equiv 1 \pmod 4 \text{ or } n \equiv 0 \pmod 4 \text{ and } p^r \equiv 3 \pmod 4; & \\ p^{\frac{r(k(n-k)(2\ell-1)-1)}{2}} (p^{\frac{rn}{2}}+1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \text{if } k \text{ is odd, } n \text{ is even,} \\ p^r \equiv 3 \pmod 4 \text{ and } n \equiv 2 \pmod 4; & \\ p^{\frac{rk((n-k)(2\ell-1)+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{p^{2r}} & \text{if } k \text{ is even and } n \text{ is odd;} \\ p^{\frac{rk(n-k)(2\ell-1)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{p^{2r}} & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

Outline of the proof I

For $0 \leq k \leq n$,

$\mathcal{S}_q(n;k)$ the number of distinct LCD codes of length n and dimension k over the finite field $\mathbb{F}_q$

Note that $\mathcal{S}_q(n;0) = \mathcal{S}_q(n;n) = 1$.

Theorem [____ & Sharma (2022)]

Let q be an even prime power. For $1 \leq k \leq n-1$, we have

$$\mathcal{S}_q(n;k) = \begin{cases} q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are odd;} \\ q^{\frac{nk-k^2+n-1}{2}} \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd and } n \text{ is even;} \\ q^{\frac{k(n-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even and } n \text{ is odd;} \\ q^{\frac{nk-k^2-2}{2}} \Big((q^k+q-1) \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{q^2} & \\ +(q^{n-k+1}-q^{n-k}+1) \begin{bmatrix} (n-2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2} \Big) & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

Outline of the proof II

Theorem [____ & Sharma (2022)]

Let q be an odd prime power. For $1 \le k \le n-1$, we have

$$\mathcal{S}_q(n;k) = \begin{cases} q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are odd;} \\ q^{\frac{nk-k^2-1}{2}} (q^{\frac{n}{2}} - 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd and } n \text{ is even with either} \\ & q \equiv 1 \pmod 4 \text{ or } n \equiv 0 \pmod 4 \text{ and} \\ & q \equiv 3 \pmod 4; \\ q^{\frac{nk-k^2-1}{2}} (q^{\frac{n}{2}} + 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd, } q \equiv 3 \pmod 4 \text{ and} \\ & n \equiv 2 \pmod 4; \\ q^{\frac{k(n-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even and } n \text{ is odd;} \\ q^{\frac{k(n-k)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

Outline of the proof II

Theorem [____ & Sharma (2022)]

Let q be an odd prime power. For $1 \leq k \leq n-1$, we have

$$\mathcal{S}_q(n;k) = \begin{cases} q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are odd;} \\ q^{\frac{nk-k^2-1}{2}} (q^{\frac{n}{2}} - 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd and } n \text{ is even with either } q \equiv 1 \pmod 4 \text{ or } n \equiv 0 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ q^{\frac{nk-k^2-1}{2}} (q^{\frac{n}{2}} + 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd, } q \equiv 3 \pmod 4 \text{ and } n \equiv 2 \pmod 4; \\ q^{\frac{k(n-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even and } n \text{ is odd;} \\ q^{\frac{k(n-k)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

- Carlet *et al.* (2018) determined the number $\mathcal{S}_q(n,k)$ for $0 \leq k \leq n$ when either $q = 2$ or q is an odd prime power.
- Liu and Wang (2019) determined the number $\mathcal{S}_q(n,k)$ for $0 \leq k \leq n$ by using cogredience theories of certain special matrices.
- Our proof technique is different and is based on concepts from groups and geometry.

Outline of the proof III

Theorem [____ & Sharma (2022)]

Let $|\overline{\mathcal{R}}_e| = p^r$, where p is a prime number and r is a positive integer.

- There exists an LCD code of length n and rank k over $\mathcal{R}_e$ if and only if there exists a k-dimensional LCD code of length n over $\overline{\mathcal{R}}_e$.
- Each k-dimensional LCD code of length n over $\overline{\mathcal{R}}_e$ gives rise to precisely $p^{rk(n-k)(e-1)}$ distinct LCD codes of length n and rank k over $\mathcal{R}_e$.
- We have $\mathcal{L}_e(n;k) = \mathcal{S}_{p^r}(n;k)p^{rk(n-k)(e-1)}$.

Enumeration formula for LCD codes of length n over $\mathcal{R}_e$ I

$\mathcal{L}_e(n)$ the number of distinct LCD codes of length n over $\mathcal{R}_e$

$$\mathcal{L}_e(n) = \sum_{k=0}^{n} \mathcal{L}_e(n;k) = 2 + \sum_{k=1}^{n-1} \mathcal{L}_e(n;k).$$

Enumeration formula for LCD codes of length n over $\mathcal{R}_e$ I

$\mathcal{L}_e(n)$ the number of distinct LCD codes of length n over $\mathcal{R}_e$

$$\mathcal{L}_e(n) = \sum_{k=0}^{n} \mathcal{L}_e(n;k) = 2 + \sum_{k=1}^{n-1} \mathcal{L}_e(n;k).$$

Theorem [____ & Sharma (2022)]

Let $|\overline{\mathcal{R}}_e| = p^r$, where p is a prime and r is a positive integer.

- When $p = 2$, we have

$$\mathcal{L}_e(n) = \begin{cases} 2 + \sum\limits_{\substack{k=1 \\ k\equiv 0 \pmod 2}}^{n-1} 2^{\frac{rk((n-k)(2\ell-1)+1)}{2}} {\begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}}_{2^{2r}} \\ + \sum\limits_{\substack{k=1 \\ k\equiv 1 \pmod 2}}^{n-1} 2^{\frac{r(n-k)(2k\ell-k+1)}{2}} {\begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}}_{2^{2r}} & \text{if } n \text{ is odd;} \\ \\ 2 + \sum\limits_{\substack{k=1 \\ k\equiv 1 \pmod 2}}^{n-1} 2^{\frac{r(k(n-k)(2\ell-1)+n-1)}{2}} {\begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}}_{2^{2r}} \\ + \sum\limits_{\substack{k=1 \\ k\equiv 0 \pmod 2}}^{n-1} 2^{\frac{r(k(n-k)(2\ell-1)-2)}{2}} \Big((2^{rk} + 2^r - 1) {\begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}}_{2^{2r}} \\ +(2^{r(n-k+1)} - 2^{r(n-k)} + 1) {\begin{bmatrix} (n-2)/2 \\ (k-2)/2 \end{bmatrix}}_{2^{2r}} \Big) & \text{if } n \text{ is even.} \end{cases}$$

Enumeration formula for LCD codes of length n over $\mathcal{R}_e$ II

- When p is an odd prime and n is even, we have

$$\mathcal{L}_e(n) = \begin{cases} 2 + \sum\limits_{\substack{k=1 \\ k\equiv 0 \pmod 2}}^{n-1} p^{\frac{rk(n-k)(2\ell-1)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{p^{2r}} \\ \quad + \sum\limits_{\substack{k=1 \\ k\equiv 1 \pmod 2}}^{n-1} p^{\frac{r(k(n-k)(2\ell-1)-1)}{2}} (p^{\frac{rn}{2}} - 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} \\ \quad \text{if either } p^r \equiv 1 \pmod 4 \text{ or } n \equiv 0 \pmod 4 \text{ and } p^r \equiv 3 \pmod 4; \\ 2 + \sum\limits_{\substack{k=1 \\ k\equiv 0 \pmod 2}}^{n-1} p^{\frac{rk(n-k)(2\ell-1)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{p^{2r}} \\ \quad + \sum\limits_{\substack{k=1 \\ k\equiv 1 \pmod 2}}^{n-1} p^{\frac{r(k(n-k)(2\ell-1)-1)}{2}} (p^{\frac{rn}{2}} + 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} \\ \quad \text{if } p^r \equiv 3 \pmod 4 \text{ and } n \equiv 2 \pmod 4. \end{cases}$$

Enumeration formula for LCD codes of length n over $\mathcal{R}_e$ III

- When p is an odd prime and n is odd, we have

$$\mathcal{L}_e(n) = 2 + \sum_{\substack{k=1 \\ k\equiv 1 \pmod 2}}^{n-1} p^{\frac{r(n-k)(2k\ell-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} + \sum_{\substack{k=1 \\ k\equiv 0 \pmod 2}}^{n-1} p^{\frac{rk((n-k)(2\ell-1)+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{p^{2r}}.$$

Classification of LCD codes

Two linear codes $\mathcal{C}$ and $\mathcal{D}$ of length n over $\mathcal{R}_e$ are said to be equivalent if one code can be obtained from the other by a combination of operations of the following two types:

A. Permutation of the n coordinate positions of the code.

B. Multiplication of the code symbols appearing in a given coordinate position by the units in the ring $\mathcal{R}_e$.

Otherwise the codes $\mathcal{C}$ and $\mathcal{D}$ are said to be inequivalent.

Classification of LCD codes

Two linear codes $\mathcal{C}$ and $\mathcal{D}$ of length n over $\mathcal{R}_e$ are said to be equivalent if one code can be obtained from the other by a combination of operations of the following two types:

A. Permutation of the n coordinate positions of the code.

B. Multiplication of the code symbols appearing in a given coordinate position by the units in the ring $\mathcal{R}_e$.

Otherwise the codes $\mathcal{C}$ and $\mathcal{D}$ are said to be inequivalent.

Numerics

n	q	Total number of non-zero LCD codes of length n over $\mathbb{F}_q[u]/\langle u^2\rangle$	Number of inequivalent non-zero LCD codes of length n over $\mathbb{F}_q[u]/\langle u^2\rangle$
2	2	5	3
3	2	33	9
4	2	449	26
5	2	10753	85
2	3	13	4
3	3	163	11
4	3	8587	38

Some open questions

- Enumeration of self-orthogonal and self-dual codes over $\mathcal{R}_e$ when $|\overline{\mathcal{R}_e}|$ is a power of 2.
- Classification of LCD codes of length n, rank k and Hamming distance d over $\mathcal{R}_e$ when $2 \leq k \leq n-2$.
- Classification of self-orthogonal and self-dual codes over $\mathcal{R}_e$.
- Are self-orthogonal codes over $\mathcal{R}_e$ asymptotically good?
- Are self-dual codes over $\mathcal{R}_e$ asymptotically good?

Betty, R. A. and Munemasa, A.,
A mass formula for self-orthogonal codes over $\mathbb{Z}_{p^2}$,
J. Combinator. Inform. Syst. Sci. 34, pp. 51-66 (2009).

Betty, R. A., Nemenzo, F. and Vasquez, T. L.,
Mass formula for self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$,
J. Appl. Math. Comput. 57, pp. 523-546 (2018).

Bhowmick, S., Tabue, A. F., Moro, E. M., Bandi, R. and Bagchi, S.,
Do non-free LCD codes over finite commutative Frobenius ring exist?,
Des. Codes Cryptogr. 88, pp. 825-840 (2020).

Carlet, C., Mesnager, S., Tang, C. and Qi, Y.,
New characterization and parametrization of LCD codes,
IEEE Trans. Inform. Theory 65(1), pp. 39-49 (2018).

Huffman, W. C. and Pless, V.,
Fundamentals of error-correcting codes,
Cambridge Univ. Press, Cambridge, New York, USA (2003).

Liu, Z. and Wang, J.:
Further results on Euclidean and Hermitian linear complementary dual codes,
Finite Fields Appl. 59, pp. 104-133 (2019).

McDonald, B. R.,
Finite rings with identity,
New York, USA: Marcel Dekker (1974).

Nagata, K., Nemenzo, F. and Wada, H.,
The number of self-dual codes over $\mathbb{Z}_{p^3}$,
Des. Codes Cryptogr. 50, pp. 291-303 (2009).

Nagata, K., Nemenzo, F. and Wada, H.,
Constructive algorithm of self-dual error correcting codes,
Proceedings of the Eleventh International Workshop on Algebraic and Combinatorial Coding Theory (ISSN1313-423X), pp. 215-220 (2008).

Norton, G. H. and Sălăgean, A.,
On the structure of linear and cyclic codes over a finite chain ring,
AAECC 10, pp. 489-506 (2000).

Pless, V.,
On the uniqueness of Golay codes,
J. Combin. Theory 5(3), pp. 215–228 (1968).

Vasquez, T. L. and Petalcorin, G. J.,
Mass formula for self-dual codes over Galois ring $GR(p^3, r)$,
Eur. J. Pure Appl. Math. 12(4), pp. 1701–1716 (2019).

Yadav, M. and Sharma, A.,
Mass formulae for self-orthogonal and self-dual codes over finite commutative chain rings,
Discrete Mathematics 344 (1), 112152, pp. 1-24 (2021).

Yadav, M. and Sharma, A.,
On the enumeration and classification of σ-LCD codes over finite commutative chain rings,
Discrete Mathematics 345 (8), 112915, pp. 1-25 (2022).

Thank you...