[1]Multi-twisted additive codes over finite fields

Sandeep Sharma
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.

q		a prime power
$m_1, m_2, \cdots, m_\ell$		positive integers coprime to q
n	$=$	$m_1 + m_2 + \cdots + m_\ell$
$\mathbb{F}_q$		the finite field of order q
$\mathbb{F}_q^n$		the vector space of all n-tuples over $\mathbb{F}_q$

q		a prime power
$m_1, m_2, \cdots, m_\ell$		positive integers coprime to q
n	$=$	$m_1 + m_2 + \cdots + m_\ell$
$\mathbb{F}_q$		the finite field of order q
$\mathbb{F}_q^n$		the vector space of all n-tuples over $\mathbb{F}_q$

We shall represent each element $a \in \mathbb{F}_q^n$ as

$$a = (a_{1,0}, a_{1,1}, \cdots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \cdots, a_{2,m_2-1}; \cdots\cdots; a_{\ell,0}, a_{\ell,1}, \cdots, a_{\ell,m_\ell-1}),$$

where $a_{i,j} \in \mathbb{F}_q$ for $1 \leq i \leq \ell$ and $0 \leq j \leq m_i - 1$.

q		a prime power
$m_1, m_2, \cdots, m_\ell$		positive integers coprime to q
n	$=$	$m_1 + m_2 + \cdots + m_\ell$
$\mathbb{F}_q$		the finite field of order q
$\mathbb{F}_q^n$		the vector space of all n-tuples over $\mathbb{F}_q$

We shall represent each element $a \in \mathbb{F}_q^n$ as

$$a = (a_{1,0}, a_{1,1}, \cdots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \cdots, a_{2,m_2-1}; \cdots\cdots; a_{\ell,0}, a_{\ell,1}, \cdots, a_{\ell,m_\ell-1}),$$

where $a_{i,j} \in \mathbb{F}_q$ for $1 \leq i \leq \ell$ and $0 \leq j \leq m_i - 1$.

Definition

A linear code of length n over $\mathbb{F}_q$ is defined as an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

$\lambda_1, \lambda_2, \cdots, \lambda_\ell$ non-zero elements of $\mathbb{F}_q$

$\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$

$\lambda_1, \lambda_2, \cdots, \lambda_\ell$ non-zero elements of $\mathbb{F}_q$

$\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$

MT shift operator

A map $T_\Lambda : \mathbb{F}_q^n \to \mathbb{F}_q^n$, defined by

$$\begin{aligned} T_\Lambda(a) &= T_\Lambda(a_{1,0}, a_{1,1}, \cdots, a_{1,m_1-1}; \cdots\cdots; a_{\ell,0}, a_{\ell,1}, \cdots, a_{\ell,m_\ell-1}) \\ &= (\lambda_1 a_{1,m_1-1}, a_{1,0}, \cdots, a_{1,m_1-2}; \cdots\cdots; \lambda_\ell a_{\ell,m_\ell-1}, a_{\ell,0}, \cdots, a_{\ell,m_\ell-2}) \end{aligned}$$

for all $a \in \mathbb{F}_q^n$, is called a Λ-MT shift operator on $\mathbb{F}_q^n$.

$\lambda_1, \lambda_2, \cdots, \lambda_\ell$ non-zero elements of $\mathbb{F}_q$

$\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$

MT shift operator

A map $T_\Lambda : \mathbb{F}_q^n \to \mathbb{F}_q^n$, defined by

$$\begin{aligned} T_\Lambda(a) &= T_\Lambda(a_{1,0}, a_{1,1}, \cdots, a_{1,m_1-1}; \cdots\cdots; a_{\ell,0}, a_{\ell,1}, \cdots, a_{\ell,m_\ell-1}) \\ &= (\lambda_1 a_{1,m_1-1}, a_{1,0}, \cdots, a_{1,m_1-2}; \cdots\cdots; \lambda_\ell a_{\ell,m_\ell-1}, a_{\ell,0}, \cdots, a_{\ell,m_\ell-2}) \end{aligned}$$

for all $a \in \mathbb{F}_q^n$, is called a Λ-MT shift operator on $\mathbb{F}_q^n$.

Multi-twisted (MT) code [Aydin and Halilović (2017)]

A Λ-MT code $\mathscr{C}$ of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_q$ is a linear code, which is invariant under the Λ-MT shift operator T_Λ, that is,

$$T_\Lambda(\mathscr{C}) = \mathscr{C}.$$

t	an integer ≥ 2
$\mathbb{F}_{q^t}^n$	(tn)-dimensional vector space over $\mathbb{F}_q$

t	an integer ≥ 2
$\mathbb{F}_{q^t}^n$	(tn)-dimensional vector space over $\mathbb{F}_q$

Additive code

An additive code of length n over $\mathbb{F}_{q^t}$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^t}^n$.

t	an integer ≥ 2
$\mathbb{F}_{q^t}^n$	(tn)-dimensional vector space over $\mathbb{F}_q$

Additive code

An additive code of length n over $\mathbb{F}_{q^t}$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^t}^n$.

Multi-twisted additive code [S. ____ & A. Sharma (2021)]

A Λ-MT additive code $\mathscr{C}$ of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ is an additive code, which is invariant under the Λ-MT shift operator, that is,

$$T_\Lambda(\mathscr{C}) = \mathscr{C}.$$

t	an integer ≥ 2
$\mathbb{F}_{q^t}^n$	(tn)-dimensional vector space over $\mathbb{F}_q$

Additive code

An additive code of length n over $\mathbb{F}_{q^t}$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^t}^n$.

Multi-twisted additive code [S. ____ & A. Sharma (2021)]

A Λ-MT additive code $\mathscr{C}$ of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ is an additive code, which is invariant under the Λ-MT shift operator, that is,

$$T_\Lambda(\mathscr{C}) = \mathscr{C}.$$

- $\ell = 1 \implies \lambda_1$-constacyclic additive codes of length m_1 over $\mathbb{F}_{q^t}$
  [Cao et al. (2015), Kaur and Sharma (2017)]
- $\ell = 1$ & $\lambda = 1 \implies$ cyclic additive codes of length m_1 over $\mathbb{F}_{q^t}$
  [Huffman (2010)]

$$\mathcal{V}_i = \mathbb{F}_{q^t}[x]/\langle x^{m_i} - \lambda_i \rangle \text{ for } 1 \leq i \leq \ell$$

$$\mathcal{V} = \prod_{i=1}^{\ell} \mathcal{V}_i, \text{ a } \Lambda\text{-MT module}$$

$$\mathcal{V}_i = \mathbb{F}_{q^t}[x]/\langle x^{m_i} - \lambda_i \rangle \text{ for } 1 \leq i \leq \ell$$

$$\mathcal{V} = \prod_{i=1}^{\ell} \mathcal{V}_i, \text{ a } \Lambda\text{-MT module}$$

Define $\psi : \mathbb{F}_{q^t}^n \longrightarrow \mathcal{V}$ as

$$\psi(c) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \text{ for each } c \in \mathbb{F}_{q^t}^n,$$

where

$$c_i(x) = c_{i,0} + c_{i,1}x + c_{i,2}x^2 + \cdots + c_{i,m_i-1}x^{m_i-1} \in \mathcal{V}_i \text{ for all } 1 \leq i \leq \ell.$$

- ψ is an $\mathbb{F}_q$-linear vector space isomorphism.
- A subset $\mathscr{C}$ of $\mathbb{F}_{q^t}^n$ is a Λ-MT additive code if and only if $\psi(\mathscr{C})$ is an $\mathbb{F}_q[x]$-submodule of $\mathcal{V}$.

$$\mathcal{V}_i = \mathbb{F}_{q^t}[x]/\langle x^{m_i} - \lambda_i \rangle \text{ for } 1 \leq i \leq \ell$$

$$\mathcal{V} = \prod_{i=1}^{\ell} \mathcal{V}_i, \text{ a } \Lambda\text{-MT module}$$

Define $\psi : \mathbb{F}_{q^t}^n \longrightarrow \mathcal{V}$ as

$$\psi(c) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \text{ for each } c \in \mathbb{F}_{q^t}^n,$$

where

$$c_i(x) = c_{i,0} + c_{i,1}x + c_{i,2}x^2 + \cdots + c_{i,m_i-1}x^{m_i-1} \in \mathcal{V}_i \text{ for all } 1 \leq i \leq \ell.$$

- ψ is an $\mathbb{F}_q$-linear vector space isomorphism.
- A subset $\mathscr{C}$ of $\mathbb{F}_{q^t}^n$ is a Λ-MT additive code if and only if $\psi(\mathscr{C})$ is an $\mathbb{F}_q[x]$-submodule of $\mathcal{V}$.

In order to study Λ-MT additive codes of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$, it is enough to study $\mathbb{F}_q[x]$-submodules of $\mathcal{V}$.

Let $g_1(x), g_2(x), \cdots, g_r(x)$ be all the distinct irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$.

Let $g_1(x), g_2(x), \cdots, g_r(x)$ be all the distinct irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$.

For $1 \leq u \leq r$, let us define

$$\begin{aligned} d_u &= \deg g_u(x) \\ a_u &= \gcd(t, d_u) \\ g_u(x) &= g_{u,0}(x) g_{u,1}(x) \cdots g_{u,a_u-1}(x), \text{ the irreducible factorization of the} \\ &\quad \text{polynomial } g_u(x) \text{ in } \mathbb{F}_{q^t}[x] \end{aligned}$$

Let $g_1(x), g_2(x), \cdots, g_r(x)$ be all the distinct irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$.

For $1 \leq u \leq r$, let us define

$$\begin{array}{lcl} d_u & = & \deg g_u(x) \\ a_u & = & \gcd(t, d_u) \\ g_u(x) & = & g_{u,0}(x) g_{u,1}(x) \cdots g_{u,a_u-1}(x), \text{ the irreducible factorization of the} \\ & & \text{polynomial } g_u(x) \text{ in } \mathbb{F}_{q^t}[x] \end{array}$$

The polynomials $g_{u,h}(x)$ for $1 \leq u \leq r$ and $0 \leq h \leq a_u - 1$ are all the distinct irreducible factors of the polynomials $x^{m_i} - \lambda_i$ over $\mathbb{F}_{q^t}$ for $1 \leq i \leq \ell$.

For $1 \leq u \leq r,\ 1 \leq i \leq \ell$ and $0 \leq h \leq a_u - 1$, let us define

$$\begin{aligned}
\epsilon_{u,i} &= \begin{cases} 1 & \text{if } g_u(x) \text{ divides } x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise,} \end{cases} \\
\epsilon_u &= \sum_{i=1}^{\ell} \epsilon_{u,i} \\
\mathcal{F}_u &= \frac{\mathbb{F}_q[x]}{\langle g_u(x) \rangle} \\
\mathcal{F}_{u,h} &= \frac{\mathbb{F}_{q^t}[x]}{\langle g_{u,h}(x) \rangle}
\end{aligned}$$

For $1 \leq u \leq r$, $1 \leq i \leq \ell$ and $0 \leq h \leq a_u - 1$, let us define

$$\begin{aligned}
\epsilon_{u,i} &= \begin{cases} 1 & \text{if } g_u(x) \text{ divides } x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise,} \end{cases} \\
\epsilon_u &= \sum_{i=1}^{\ell} \epsilon_{u,i} \\
\mathcal{F}_u &= \frac{\mathbb{F}_q[x]}{\langle g_u(x) \rangle} \\
\mathcal{F}_{u,h} &= \frac{\mathbb{F}_{q^t}[x]}{\langle g_{u,h}(x) \rangle}
\end{aligned}$$

By the Chinese Remainder Theorem, we have

$$\mathcal{V} \simeq \bigoplus_{u=1}^{r} \underbrace{\bigoplus_{h=0}^{a_u-1} \left(\epsilon_{u,1}\mathcal{F}_{u,h}, \epsilon_{u,2}\mathcal{F}_{u,h}, \cdots, \epsilon_{u,\ell}\mathcal{F}_{u,h} \right)}_{\mathcal{G}_u} = \bigoplus_{u=1}^{r} \mathcal{G}_u.$$

Note that $\mathcal{G}_u$ is an $\epsilon_u t$-dimensional vector space over $\mathcal{F}_u$ under the component-wise addition and the component-wise scalar multiplication.

Theorem [S. ____ & A. Sharma (2021)]

- Each Λ-MT additive code $\mathscr{C}$ of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ can be uniquely expressed as
$$\mathscr{C} = \bigoplus_{u=1}^{r} \mathscr{C}_u,$$
where $\mathscr{C}_u$ is an $\mathcal{F}_u$-subspace of $\mathcal{G}_u$ for each u.
- Conversely, if $\mathscr{C}_u$ is an $\mathcal{F}_u$-subspace of $\mathcal{G}_u$ for $1 \leq u \leq r$, then the direct sum
$$\mathscr{C} = \bigoplus_{u=1}^{r} \mathscr{C}_u$$
is a Λ-MT additive code of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$.

The subspaces $\mathscr{C}_1, \mathscr{C}_2, \cdots, \mathscr{C}_r$ are called the constituents of $\mathscr{C}$.

Enumeration formula for Λ-MT additive codes of length n over $\mathbb{F}_{q^t}$

For positive integers k, n with $1 \leq k \leq n$ and a prime power q, the number of distinct k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the Gaussian binomial coefficient

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

Recall that $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$.

Enumeration formula for Λ-MT additive codes of length n over $\mathbb{F}_{q^t}$

For positive integers k, n with $1 \leq k \leq n$ and a prime power q, the number of distinct k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the Gaussian binomial coefficient

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

Recall that $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$.

Theorem [S. ____ & A. Sharma (2021)]

The total number of distinct Λ-MT additive codes of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$N_\Lambda = \prod_{u=1}^{r} \left(\sum_{b=0}^{\epsilon_u t} \begin{bmatrix} \epsilon_u t \\ b \end{bmatrix}_{q^{d_u}} \right).$$

Are MT additive codes over finite fields asymptotically good?

Kabatyansky (1977)	Cyclic additive codes of length p^a over finite field $\mathbb{F}_{q^t}$ are asymptotically good	q is a primitive root modulo a prime p satisfying $q^{p-1} \not\equiv 1 \pmod{p^2}$ and by assuming Artin's conjecture on primitive roots
Chepyzhov (1992)	Cyclic additive codes of prime lengths over finite fields are asymptotically good	By applying Chebyshev's Theorem for prime numbers
Shi *et al.* (2018)	λ-constacyclic additive codes of prime power length m over $\mathbb{F}_{q^t}$ are asymptotically good	The polynomial $x^m - \lambda$ is irreducible over $\mathbb{F}_q$
Shi *et al.* (2018)	Cyclic additive codes of prime power lengths over finite fields are asymptotically good	By assuming Artin's conjecture on primitive roots

Are MT additive codes over finite fields asymptotically good?

Kabatyansky (1977)	Cyclic additive codes of length p^a over finite field $\mathbb{F}_{q^t}$ are asymptotically good	q is a primitive root modulo a prime p satisfying $q^{p-1} \not\equiv 1 \pmod{p^2}$ and by assuming Artin's conjecture on primitive roots
Chepyzhov (1992)	Cyclic additive codes of prime lengths over finite fields are asymptotically good	By applying Chebyshev's Theorem for prime numbers
Shi *et al.* (2018)	λ-constacyclic additive codes of prime power length m over $\mathbb{F}_{q^t}$ are asymptotically good	The polynomial $x^m - \lambda$ is irreducible over $\mathbb{F}_q$
Shi *et al.* (2018)	Cyclic additive codes of prime power lengths over finite fields are asymptotically good	By assuming Artin's conjecture on primitive roots

Artin's conjecture on primitive roots (1927)

An integer a, which is neither a perfect square nor equal to -1, is a primitive root modulo infinitely many primes.

Let $\mathscr{F} = \{\mathscr{C}_i\}_{i \geq 1}$ be a sequence of additive codes $\mathscr{C}_i$ of length n_i, dimension k_i and Hamming distance d_i over $\mathbb{F}_{q^t}$ such that $\lim_{i \to \infty} \{n_i\} = \infty$.

- The rate $R_{\mathscr{F}}$ of the sequence $\mathscr{F}$ is defined as $R_{\mathscr{F}} := \limsup_{i \to \infty} \left\{ \frac{k_i}{n_i} \right\}$.
- The relative Hamming distance $\Delta_{\mathscr{F}}$ of the sequence $\mathscr{F}$ is defined as $\Delta_{\mathscr{F}} := \liminf_{i \to \infty} \left\{ \frac{d_i}{n_i} \right\}$.

Let $\mathscr{F} = \{\mathscr{C}_i\}_{i\geq 1}$ be a sequence of additive codes $\mathscr{C}_i$ of length n_i, dimension k_i and Hamming distance d_i over $\mathbb{F}_{q^t}$ such that $\lim_{i\to\infty}\{n_i\} = \infty$.

- The rate $R_{\mathscr{F}}$ of the sequence $\mathscr{F}$ is defined as $R_{\mathscr{F}} := \limsup_{i\to\infty}\left\{\frac{k_i}{n_i}\right\}$.
- The relative Hamming distance $\Delta_{\mathscr{F}}$ of the sequence $\mathscr{F}$ is defined as $\Delta_{\mathscr{F}} := \liminf_{i\to\infty}\left\{\frac{d_i}{n_i}\right\}$.

Definition

A sequence $\mathscr{F} = \{\mathscr{C}_i\}_{i\geq 1}$ of additive codes over $\mathbb{F}_{q^t}$ is said to be asymptotically good if it satisfies $\Delta_{\mathscr{F}} R_{\mathscr{F}} > 0$.

p odd prime number satisfying $\gcd(p, q) = \gcd(p, q-1) = 1$

$m_i = p^\gamma, \gamma \geq 1$ for $1 \leq i \leq \ell$

$\lambda_i = \lambda$ for $1 \leq i \leq \ell$

e multiplicative order of λ

η fixed primitive (ep^γ)-th root of unity

$\mathcal{S} = \frac{\mathbb{F}_q[x]}{\langle x^{p^\gamma} - \lambda \rangle}$

$\mathcal{R} = \frac{\mathbb{F}_{q^t}[x]}{\langle x^{p^\gamma} - \lambda \rangle}$

p odd prime number satisfying $\gcd(p, q) = \gcd(p, q-1) = 1$

$m_i = p^\gamma, \gamma \geq 1$ for $1 \leq i \leq \ell$

$\lambda_i = \lambda$ for $1 \leq i \leq \ell$

e multiplicative order of λ

η fixed primitive (ep^γ)-th root of unity

$\mathcal{S} = \frac{\mathbb{F}_q[x]}{\langle x^{p^\gamma} - \lambda \rangle}$

$\mathcal{R} = \frac{\mathbb{F}_{q^t}[x]}{\langle x^{p^\gamma} - \lambda \rangle}$

In view of this, any Λ-MT additive code of length $n = p^\gamma \ell$ and block lengths $(p^\gamma, p^\gamma, \cdots, p^\gamma)$ over $\mathbb{F}_{q^t}$ can be viewed as an $\mathcal{S}$-submodule of $\mathcal{R}^\ell$.

$O_T(q)$ the multiplicative order of q modulo T

$\Theta = O_{ep^\gamma}(q)$

$O_T(q)$ the multiplicative order of q modulo T

$\Theta = O_{ep^\gamma}(q)$

Let $O_p(q) = f$. Let us write $q^f = 1 + p^d c$, where $d \geq 1$ and c are integers with $\gcd(p, c) = 1$. Further, we see that

$$\Theta = O_{ep^\gamma}(q) = O_{p^\gamma}(q) = \begin{cases} fp^{\gamma-d} & \text{if } \gamma \geq d+1; \\ f & \text{if } \gamma \leq d. \end{cases}$$

From now on, we assume that the integer γ satisfies $\gamma \geq d+1$, so that we have $\Theta = fp^{\gamma-d}$.

Let $h_1(x)$ be the minimal polynomial of the element η over $\mathbb{F}_q$. Note that $h_1(x)$ divides $x^{p^\gamma} - \lambda$ in $\mathbb{F}_q[x]$ and $\deg h_1(x) = \Theta$. Now let us define

$$\mathcal{J}_{p^\gamma} = \left\langle \frac{x^{p^\gamma}-\lambda}{h_1(x)} \right\rangle_{\mathcal{S}}$$

$$\mathcal{K}_{p^\gamma} = \left\langle \frac{x^{p^\gamma}-\lambda}{h_1(x)} \right\rangle_{\mathcal{R}}$$

Let $h_1(x)$ be the minimal polynomial of the element η over $\mathbb{F}_q$. Note that $h_1(x)$ divides $x^{p^\gamma} - \lambda$ in $\mathbb{F}_q[x]$ and $\deg h_1(x) = \Theta$. Now let us define

$$\begin{aligned} \mathcal{J}_{p^\gamma} &= \left\langle \tfrac{x^{p^\gamma}-\lambda}{h_1(x)} \right\rangle_{\mathcal{S}} \\ \mathcal{K}_{p^\gamma} &= \left\langle \tfrac{x^{p^\gamma}-\lambda}{h_1(x)} \right\rangle_{\mathcal{R}} \end{aligned}$$

By the Chinese Remainder Theorem, we get

$$\mathcal{S} \cong \langle h_1(x) \rangle_{\mathcal{S}} \oplus \mathcal{J}_{p^\gamma} \quad \text{and} \quad \mathcal{R} \cong \langle h_1(x) \rangle_{\mathcal{R}} \oplus \mathcal{K}_{p^\gamma}.$$

To study the asymptotic properties of MT additive codes of length $p^\gamma \ell$ over $\mathbb{F}_{q^t}$, we will view the set $\mathcal{K}_{p^\gamma}^{\ell}$ as a sample space, where each sample of $\mathcal{K}_{p^\gamma}^{\ell}$ is chosen with equal probability.

Let $h_1(x)$ be the minimal polynomial of the element η over $\mathbb{F}_q$. Note that $h_1(x)$ divides $x^{p^\gamma} - \lambda$ in $\mathbb{F}_q[x]$ and $\deg h_1(x) = \Theta$. Now let us define

$$\begin{aligned} \mathcal{J}_{p^\gamma} &= \left\langle \tfrac{x^{p^\gamma}-\lambda}{h_1(x)} \right\rangle_{\mathcal{S}} \\ \mathcal{K}_{p^\gamma} &= \left\langle \tfrac{x^{p^\gamma}-\lambda}{h_1(x)} \right\rangle_{\mathcal{R}} \end{aligned}$$

By the Chinese Remainder Theorem, we get

$$\mathcal{S} \cong \langle h_1(x) \rangle_{\mathcal{S}} \oplus \mathcal{J}_{p^\gamma} \quad \text{and} \quad \mathcal{R} \cong \langle h_1(x) \rangle_{\mathcal{R}} \oplus \mathcal{K}_{p^\gamma}.$$

To study the asymptotic properties of MT additive codes of length $p^\gamma \ell$ over $\mathbb{F}_{q^t}$, we will view the set $\mathcal{K}_{p^\gamma}^{\ell}$ as a sample space, where each sample of $\mathcal{K}_{p^\gamma}^{\ell}$ is chosen with equal probability.

Theorem [S. ____ & A. Sharma (2022)]

Multi-twisted additive codes over finite fields are asymptotically good.

Outline of the proof I

Let $\{\gamma_i\}_{i\geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\gamma_i \geq d+1$ for all $i \geq 1$ and $\lim_{i\to\infty}\{\gamma_i\} = \infty$.

For each positive integer i, let us take

$$\Theta_i \quad = \quad O_{p^{\gamma_i}}(q) = fp^{\gamma_i - d}$$

Outline of the proof I

Let $\{\gamma_i\}_{i\geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\gamma_i \geq d+1$ for all $i \geq 1$ and $\lim_{i\to\infty}\{\gamma_i\} = \infty$.

For each positive integer i, let us take

$$\Theta_i \quad = \quad O_{p^{\gamma_i}}(q) = fp^{\gamma_i - d}$$

For each positive integer i and $a_i(x) = (a_{i_1}(x), a_{i_2}(x), \cdots, a_{i_\ell}(x)) \in \mathcal{K}^{\ell}_{p^{\gamma_i}}$, let

$$\mathscr{C}_{a_i} = \{(f(x)a_{i_1}(x), f(x)a_{i_2}(x), \cdots, f(x)a_{i_\ell}(x)) : f(x) \in \mathcal{J}_{p^{\gamma_i}}\} \subseteq \mathcal{K}^{\ell}_{p^{\gamma_i}}$$

be the random MT additive code of length $p^{\gamma_i}\ell$ and block lengths $(p^{\gamma_i}, p^{\gamma_i}, \cdots, p^{\gamma_i})$ over $\mathbb{F}_{q^t}$ defined over the probability space $\mathcal{K}^{\ell}_{p^{\gamma_i}}$.

Outline of the proof II

Theorem [S. ____ & A. Sharma (2022)]

If δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$, then we have

$$\lim_{i \to \infty} \left\{ \Pr\left(\Delta(\mathscr{C}_{a_i}) > \delta \right) \right\} = 1,$$

where $h_{q^t}(\cdot)$ is the q^t-ary entropy function.

Outline of the proof II

Theorem [S. ____ & A. Sharma (2022)]

If δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$, then we have

$$\lim_{i\to\infty} \left\{\Pr\left(\Delta(\mathscr{C}_{a_i}) > \delta\right)\right\} = 1,$$

where $h_{q^t}(\cdot)$ is the q^t-ary entropy function.

Theorem [S. ____ & A. Sharma (2022)]

Let $\{\gamma_i\}_{i\geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\gamma_i \geq d+1$. Then we have

$$\lim_{i\to\infty} \left\{R(\mathscr{C}_{a_i})\right\} = \frac{f}{p^d \ell t}.$$

Outline of the proof III

Theorem [S. ____ & A. Sharma (2022)]

Let δ be a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$. There exists an infinite sequence $\mathcal{F} = \{\mathscr{C}_i\}_{i \geq 1}$ of MT additive codes $\mathscr{C}_i$ of length $p^{\gamma_i}\ell$, block length p^{γ_i} and dimension $\frac{fp^{\gamma_i - d}}{t}$ over $\mathbb{F}_{q^t}$ with $\lim_{i \to \infty} \{p^{\gamma_i}\} = \infty$, such that

(i) $R_{\mathcal{F}} = \lim_{i \to \infty} \{R(\mathscr{C}_i)\} = \dfrac{f}{p^d \ell t} > 0$, and

(ii) $\Delta_{\mathcal{F}} = \lim_{i \to \infty} \{\Delta(\mathscr{C}_i)\} > \delta$.

Outline of the proof III

Theorem [S. ____ & A. Sharma (2022)]

Let δ be a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$. There exists an infinite sequence $\mathcal{F} = \{\mathscr{C}_i\}_{i \geq 1}$ of MT additive codes $\mathscr{C}_i$ of length $p^{\gamma_i}\ell$, block length p^{γ_i} and dimension $\frac{fp^{\gamma_i - d}}{t}$ over $\mathbb{F}_{q^t}$ with $\lim_{i \to \infty} \{p^{\gamma_i}\} = \infty$, such that

(i) $R_{\mathcal{F}} = \lim_{i \to \infty} \{R(\mathscr{C}_i)\} = \dfrac{f}{p^d \ell t} > 0$, and

(ii) $\Delta_{\mathcal{F}} = \lim_{i \to \infty} \{\Delta(\mathscr{C}_i)\} > \delta$.

As a consequence of the above theorem, we deduce that

- The class of λ-constacyclic additive codes of length p^γ over $\mathbb{F}_{q^t}$ is asymptotically good when the polynomial $x^{p^\gamma} - \lambda$ is reducible over $\mathbb{F}_q$.
- The class of cyclic additive codes of odd prime power lengths over finite fields is asymptotically good without applying Chebyshev's Theorem and without assuming the unresolved Artin's conjecture on primitive roots.

$\mathrm{Tr}_{q^t,q}$ trace map from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$

$\mathrm{Tr}_{q^t,q}$ trace map from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$

Ordinary trace bilinear form [Huffman (2010)]

The ordinary trace bilinear form on $\mathbb{F}_{q^t}^n$ is a map $\langle \cdot, \cdot \rangle_0 : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$, defined as

$$\langle a, b \rangle_0 = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} \mathrm{Tr}_{q^t,q}(a_{i,j} b_{i,j}) \ \forall \ a, b \in \mathbb{F}_{q^t}^n .$$

- The ordinary trace bilinear form $\langle \cdot, \cdot \rangle_0$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_{q^t}^n$.

The Hermitian trace bilinear form on $\mathbb{F}_{q^t}^n$ is defined only when t is an even integer.

$t = 2AU$ $\quad$ $A = 2^{a-1}$, where $a \geq 1$ and the integer U is odd

γ $\quad$ a non-zero element of $\mathbb{F}_{q^{2A}}$ satisfying $\gamma + \gamma^{q^A} = 0$

The Hermitian trace bilinear form on $\mathbb{F}_{q^t}^n$ is defined only when t is an even integer.

$t = 2AU$ $\quad A = 2^{a-1}$, where $a \geq 1$ and the integer U is odd

γ $\quad$ a non-zero element of $\mathbb{F}_{q^{2A}}$ satisfying $\gamma + \gamma^{q^A} = 0$

Hermitian trace bilinear form [Huffman (2010)]

The Hermitian trace bilinear form on $\mathbb{F}_{q^t}^n$ is a map $\langle \cdot, \cdot \rangle_\gamma : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$, defined as

$$\langle a, b \rangle_\gamma = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i - 1} \mathrm{Tr}_{q^t, q}(\gamma a_{i,j} b_{i,j}^{q^{t/2}}) \ \forall \ a, b \in \mathbb{F}_{q^t}^n.$$

- The Hermitian trace bilinear form $\langle \cdot, \cdot \rangle_\gamma$ is a non-degenerate, reflexive and alternating bilinear form on $\mathbb{F}_{q^t}^n$.

Let $t \geq 2$ be an integer satisfying $t \not\equiv 1 \pmod{p}$. Define $\phi : \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$ as

$$\phi(\alpha) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{t-1}} \text{ for each } \alpha \in \mathbb{F}_{q^t}.$$

Note that

- $\phi(\alpha) = \mathrm{Tr}_{q^t,q}(\alpha) - \alpha$ for all $\alpha \in \mathbb{F}_{q^t}$.
- ϕ is an $\mathbb{F}_q$-linear vector space isomorphism.

Let $t \geq 2$ be an integer satisfying $t \not\equiv 1 \pmod{p}$. Define $\phi : \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$ as

$$\phi(\alpha) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{t-1}} \text{ for each } \alpha \in \mathbb{F}_{q^t}.$$

Note that

- $\phi(\alpha) = \mathrm{Tr}_{q^t,q}(\alpha) - \alpha$ for all $\alpha \in \mathbb{F}_{q^t}$.
- ϕ is an $\mathbb{F}_q$-linear vector space isomorphism.

$*$ Trace bilinear form [Sharma & Kaur (2017)]

The $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$ is a map $\langle \cdot, \cdot \rangle_* : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$, defined as

$$\langle a, b \rangle_* = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i - 1} \mathrm{Tr}_{q^t,q}(a_{i,j}\phi(b_{i,j})) \ \forall \ a, b \in \mathbb{F}_{q^t}^n.$$

- The $*$ trace bilinear form $\langle \cdot, \cdot \rangle_*$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_{q^t}^n$, and is alternating in the case when q is even.

$$\Lambda' \quad = \quad (\lambda_1^{-1}, \lambda_2^{-1}, \cdots, \lambda_\ell^{-1})$$

$$\Lambda' \quad = \quad (\lambda_1^{-1}, \lambda_2^{-1}, \cdots, \lambda_\ell^{-1})$$

The δ-dual code

If $\mathscr{C}$ is a Λ-MT additive code of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$, then its δ-dual code $\mathscr{C}^{\perp_\delta}$ is defined as

$$\mathscr{C}^{\perp_\delta} = \left\{ a \in \mathbb{F}_{q^t}^n : \langle a, c \rangle_\delta = 0 \text{ for all } c \in \mathscr{C} \right\}.$$

The δ-dual code $\mathscr{C}^{\perp_\delta}$ of a Λ-MT additive code $\mathscr{C}$ is a Λ'-MT additive code of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$.

Definition

A Λ-MT additive code $\mathscr{C}$ of length n over $\mathbb{F}_{q^t}$ is said to be

1. δ-self-orthogonal if it satisfies $\mathscr{C} \subseteq \mathscr{C}^{\perp_\delta}$.
2. δ-self-dual if it satisfies $\mathscr{C} = \mathscr{C}^{\perp_\delta}$.
3. δ-complementary dual if it satisfies $\mathscr{C} \cap \mathscr{C}^{\perp_\delta} = \{\mathbf{0}\}$.

Definition

A Λ-MT additive code $\mathscr{C}$ of length n over $\mathbb{F}_{q^t}$ is said to be

1. δ-self-orthogonal if it satisfies $\mathscr{C} \subseteq \mathscr{C}^{\perp_\delta}$.
2. δ-self-dual if it satisfies $\mathscr{C} = \mathscr{C}^{\perp_\delta}$.
3. δ-complementary dual if it satisfies $\mathscr{C} \cap \mathscr{C}^{\perp_\delta} = \{0\}$.

Reciprocal polynomial

If $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ is a non-zero polynomial of degree k in $\mathbb{F}_q[x]$ such that $f(0) \neq 0$, then its reciprocal polynomial is defined as

$$f^\dagger(x) = \frac{x^k}{f(0)} f(x^{-1}) = a_0^{-1}(a_k + a_{k-1}x + \cdots + a_0 x^k).$$

- A non-zero polynomial $f(x)$ in $\mathbb{F}_q[x]$ is called a self-reciprocal polynomial if it satisfies $\langle f^\dagger(x) \rangle = \langle f(x) \rangle$.
- Two non-zero coprime polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ form a reciprocal pair if they satisfy $\langle f^\dagger(x) \rangle = \langle g(x) \rangle$.

Suppose (by relabelling $g_{u,h}(x)$'s if required) that

- $g_{1,0}(x), , \cdots , g_{1,a_1-1}(x), \cdots , g_{e_1,0}(x), \cdots , g_{e_1,a_{e_1}-1}(x)$ are all the distinct self-reciprocal polynomials,
- $g_{e_1+1,0}(x), g^{\dagger}_{e_1+1,0}(x), \cdots , g_{e_1+1,a_{e_1+1}-1}(x), g^{\dagger}_{e_1+1,a_{e_1+1}-1}(x), \cdots , g_{e_2,0}(x), g^{\dagger}_{e_2,0}(x), \cdots , g_{e_2,a_{e_2}-1}(x), g^{\dagger}_{e_2,a_{e_2}-1}(x)$ are all the polynomials forming reciprocal pairs, and
- $g_{e_2+1,0}(x), \cdots , g_{e_2+1,a_{e_2+1}-1}(x), \cdots , g_{e_3,0}(x), \cdots , g_{e_3,a_{e_3}-1}(x)$ are the remaining polynomials that appear in the irreducible factorizations of the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots , x^{m_\ell} - \lambda_\ell$ over $\mathbb{F}_{q^t}$.

Recall that for $1 \leq u \leq r$ and $1 \leq i \leq \ell$, we have

$$\epsilon_{u,i} = \begin{cases} 1 & \text{if } g_u(x) \mid x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise.} \end{cases}$$

For $e_1 + 1 \leq w \leq e_2$ and $1 \leq i \leq \ell$, let

$$\epsilon^{\dagger}_{w,i} = \begin{cases} 1 & \text{if } g^{\dagger}_w(x) \mid x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise.} \end{cases}$$

$$\begin{array}{lll} \mathcal{J}_1 := \{v : 1 \leq v \leq e_1, d_v = 1\} & & \eta_w := \sum_{i \in \mathcal{I}_w} \epsilon_{w,i} \\ \mathcal{J}_2 := \{1, 2, \cdots, e_1\} \setminus \mathcal{J}_1 & & \tau_w := \sum_{i \in \mathcal{I}'_w} \epsilon^{\dagger}_{w,i} \\ \mathcal{I}_w := \{i : 1 \leq i \leq \ell, \epsilon_{w,i} = \epsilon^{\dagger}_{w,i}\} & & \varrho_w := \sum_{i \in \mathcal{I}'_w} \epsilon_{w,i} \\ \mathcal{I}'_w := \{1, 2, \cdots, \ell\} \setminus \mathcal{I}_w & & \end{array}$$

Necessary and sufficient conditions for the existence of a δ-self-dual Λ-MT additive code

Theorem [S. ____ & A. Sharma (2021)]

There exists a δ-self-dual Λ-MT additive code of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ if and only if the irreducible factors of the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_{q^t}[x]$ are either self-reciprocal or they form reciprocal pairs and $\epsilon_v t$ is an even integer for $1 \leq v \leq e_1$.

Enumeration formula for δ-self-dual Λ-MT additive codes

Theorem [S. ____ & A. Sharma (2021)]

If all the irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots$ $x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_{q^t}[x]$ are either self-reciprocal or form reciprocal pairs (i.e., $e_3 \leq e_2$) and $\epsilon_v t$ is even for $1 \leq v \leq e_1$, then for $\delta \in \{0, *, \gamma\}$, the number $\mathfrak{N}$ of distinct δ-self-dual Λ-MT additive codes of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{N} = \prod_{v \in \mathcal{J}_1} \mathfrak{N}_v \prod_{v \in \mathcal{J}_2} \left(\prod_{b=0}^{(\epsilon_v t/2)-1} (q^{\frac{d_v(\epsilon_v t - 2b - 1)}{2}} + 1) \right) \prod_{w=e_1+1}^{e_2} \left(\sum_{d=0}^{\eta_w t} \begin{bmatrix} \eta_w t \\ d \end{bmatrix}_{q^{dw}} \right),$$

where for each $v \in \mathcal{J}_1$, the number $\mathfrak{N}_v$ equals

- $\prod_{a=0}^{(\epsilon_v t/2)-1} \left(q^{\frac{\epsilon_v t - 2a - 2}{2}} + 1 \right)$ when $\delta \in \{0, *\}$, $q \equiv 3 \pmod 4$ and $\epsilon_v t \equiv 2 \pmod 4$.
- $\prod_{a=0}^{(\epsilon_v t/2)-2} \left(q^{\frac{\epsilon_v t - 2a - 2}{2}} + 1 \right)$ when $\delta = 0$ and q is even.
- $\prod_{a=0}^{(\epsilon_v t/2)-1} \left(q^{\frac{\epsilon_v t - 2a}{2}} + 1 \right)$ when either $\delta = \gamma$ or $\delta = *$ and q is even.

Enumeration formula for δ-self-orthogonal Λ-MT additive codes I

Theorem [S. ____ & A. Sharma (2021)]

For $\delta \in \{0, *, \gamma\}$, the number $\mathfrak{M}$ of distinct δ-self-orthogonal Λ-MT additive codes of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{M} = \prod_{v=1}^{e_1} \mathfrak{M}_v \prod_{w=e_1+1}^{e_2} \left(\sum_{k_1=0}^{\eta_w t} \begin{bmatrix} \eta_w t \\ k_1 \end{bmatrix}_{q^{d_w}} \sum_{k_2=0}^{\eta_w t - k_1} \begin{bmatrix} \eta_w t - k_1 \\ k_2 \end{bmatrix}_{q^{d_w}} \right),$$

where for $1 \leq v \leq e_1$, the number $\mathfrak{M}_v$ equals

- $\sum_{k=0}^{(\epsilon_v t-2)/2} \begin{bmatrix} (\epsilon_v t-2)/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_v t-2d}{2}} + 1 \right)$ when $v \in \mathcal{J}_1$ and $\delta \in \{0, *\}$ with either $\epsilon_v t$ is even and $q \equiv 1 \pmod 4$ or $\epsilon_v t \equiv 0 \pmod 4$ and $q \equiv 3 \pmod 4$.
- $\sum_{k=0}^{\epsilon_v t/2} \begin{bmatrix} \epsilon_v t/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_v t-2d-2}{2}} + 1 \right)$ when $v \in \mathcal{J}_1$, $\delta \in \{0, *\}$, $q \equiv 3 \pmod 4$ and $\epsilon_v t \equiv 2 \pmod 4$.

Enumeration formula for δ-self-orthogonal Λ-MT additive codes II

- $\sum_{k=0}^{(\epsilon_v t-2)/2} \begin{bmatrix} (\epsilon_v t-2)/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_v t-2d-2}{2}}+1\right) +$
  $\sum_{k'=1}^{\epsilon_v t/2} q^{\epsilon_v t-2k'} \begin{bmatrix} (\epsilon_v t-2)/2 \\ k'-1 \end{bmatrix}_q \prod_{d'=0}^{k'-2} \left(q^{\frac{\epsilon_v t-2d'-2}{2}}+1\right)$ when $v \in \mathcal{J}_1$, $\delta = 0$ and both $\epsilon_v t, q$ are even.
- $\sum_{k=0}^{(\epsilon_v t-1)/2} \begin{bmatrix} (\epsilon_v t-1)/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_v t-2d-1}{2}}+1)$ when $v \in \mathcal{J}_1$ with either $\delta = *$ and both $\epsilon_v t$, q are odd or $\delta = 0$ and $\epsilon_v t$ is odd.
- $\sum_{k=0}^{\epsilon_v t/2} \begin{bmatrix} \epsilon_v t/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_v t-2d}{2}}+1\right)$ when $v \in \mathcal{J}_1$ with either $\delta = \gamma$ or $\delta = *$ and both $\epsilon_v t, q$ are even.

Enumeration formula for δ-self-orthogonal Λ-MT additive codes III

- $\sum_{k=0}^{\epsilon_v t/2} \begin{bmatrix} \epsilon_v t/2 \\ k \end{bmatrix}_{q^{d_v}} \prod_{b=0}^{k-1} \left(q^{\frac{d_v(\epsilon_v t-2b-1)}{2}} + 1 \right)$ when $v \in \mathcal{J}_2$ and $\epsilon_v t$ is even.
- $\sum_{k=0}^{(\epsilon_v t-1)/2} \begin{bmatrix} (\epsilon_v t-1)/2 \\ k \end{bmatrix}_{q^{d_v}} \prod_{b=0}^{k-1} \left(q^{\frac{d_v(\epsilon_v t-2b)}{2}} + 1 \right)$ when $v \in \mathcal{J}_2$ and $\epsilon_v t$ is odd.

Enumeration formula for δ-complementary dual Λ-MT additive codes I

Theorem [S. ____ & A. Sharma (2022)]

For $\delta \in \{0, *, \gamma\}$, the number $\mathfrak{D}$ of distinct δ-complementary dual Λ-MT additive codes of length n and block lengths $(m_1, m_2, \cdots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{D} = \prod_{v=1}^{e_1} \mathfrak{D}_v \prod_{w=e_1+1}^{e_2} \mathfrak{D}_w \prod_{s=e_2+1}^{e_3} \left(\sum_{a=0}^{\epsilon_s t} \begin{bmatrix} \epsilon_s t \\ a \end{bmatrix}_{q^{d_s}} \right),$$

where for $e_1 + 1 \leq w \leq e_2$, the number $\mathfrak{D}_w$ equals

$$\sum_{k=0}^{\eta_w t} \sum_{k_1=0}^{\varrho_w t} \sum_{k_2=0}^{\tau_w t} \left(q^{k d_w (\eta_w t - k)} \begin{bmatrix} \eta_w t \\ k \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \varrho_w t \\ k_1 \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \tau_w t \\ k_2 \end{bmatrix}_{q^{d_w}} \right),$$

and for $1 \leq v \leq e_1$, the number $\mathfrak{D}_v$ equals

- $2 + \sum_{\substack{k=2 \\ k \text{ is even}}}^{\epsilon_v t - 1} q^{\frac{k(\epsilon_v t - k)}{2}} \begin{bmatrix} \epsilon_v t/2 \\ k/2 \end{bmatrix}_{q^2}$ when $v \in \mathcal{J}_1$ with either $\delta = \gamma$ and $\epsilon_v t$ is even

  or $\delta = *$ and both $\epsilon_v t, q$ are even.

Enumeration formula for δ-complementary dual Λ-MT additive codes II

- $$2+\sum_{\substack{k=1\\ k \text{ is even}}}^{\epsilon_v t-1} q^{\frac{k(\epsilon_v t-k+1)}{2}} \begin{bmatrix}(\epsilon_v t-1)/2\\ k/2\end{bmatrix}_{q^2} + \sum_{\substack{k=1\\ k \text{ is odd}}}^{\epsilon_v t-1} q^{\frac{(\epsilon_v t-k)(k+1)}{2}} \begin{bmatrix}(\epsilon_v t-1)/2\\ (k-1)/2\end{bmatrix}_{q^2}$$
  when $v \in \mathcal{J}_1$, $\delta \in \{0,*\}$ and both $\epsilon_v t$, q are odd.
- $$2+\sum_{\substack{k=1\\ k \text{ is even}}}^{\epsilon_v t-1} q^{\frac{k(\epsilon_v t-k)}{2}} \begin{bmatrix}\epsilon_v t/2\\ k/2\end{bmatrix}_{q^2} + \sum_{\substack{k=1\\ k \text{ is odd}}}^{\epsilon_v t-1} q^{\frac{\epsilon_v tk-k^2-1}{2}} (q^{\frac{\epsilon_v t}{2}}+1) \begin{bmatrix}(\epsilon_v t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}$$ when
  $v \in \mathcal{J}_1$ and $\delta \in \{*,0\}$ with either $\epsilon_v t$ even and $q \equiv 1 \pmod 4$ or

  $\epsilon_v t \equiv 0 \pmod 4$ and $q \equiv 3 \pmod 4$.
- $$2+\sum_{\substack{k=1\\ k \text{ is even}}}^{\epsilon_v t-1} q^{\frac{k(\epsilon_v t-k)}{2}} \begin{bmatrix}\epsilon_v t/2\\ k/2\end{bmatrix}_{q^2} + \sum_{\substack{k=1\\ k \text{ is odd}}}^{t-1} q^{\frac{\epsilon_v tk-k^2-1}{2}} (q^{\frac{\epsilon_v t}{2}}-1) \begin{bmatrix}(\epsilon_v t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}$$
  when $v \in \mathcal{J}_1$, $\delta \in \{0,*\}$, $q \equiv 3 \pmod 4$ and $\epsilon_v t \equiv 2 \pmod 4$.

Enumeration formula for δ-complementary dual Λ-MT additive codes III

- $$2+\sum_{\substack{k=1\\ k \text{ is even}}}^{\epsilon_v t-1} q^{\frac{k(\epsilon_v t-k+1)}{2}} \begin{bmatrix}(\epsilon_v t-1)/2\\ k/2\end{bmatrix}_{q^2} + \sum_{\substack{k=1\\ k \text{ is odd}}}^{\epsilon_v t-1} q^{\frac{(\epsilon_v t-k)(k+1)}{2}} \begin{bmatrix}(\epsilon_v t-1)/2\\ (k-1)/2\end{bmatrix}_{q^2}$$

  when $v \in \mathcal{J}_1$, $\delta = 0$, q is even and $\epsilon_v t$ is odd.

- $$2+\sum_{\substack{k=1\\ k \text{ is even}}}^{\epsilon_v t-1} q^{\frac{\epsilon_v tk-k^2-2}{2}} \Bigg\{(q^k+q-1)\begin{bmatrix}(\epsilon_v t-2)/2\\ k/2\end{bmatrix}_{q^2} + (q^{\epsilon_v t-k+1}-q^{\epsilon_v t-k}+1) \times \begin{bmatrix}(\epsilon_v t-2)/2\\ (k-2)/2\end{bmatrix}_{q^2}\Bigg\} + \sum_{\substack{k=1\\ k \text{ is odd}}}^{\epsilon_v t-1} q^{\frac{\epsilon_v t(k+1)-(k^2+1)}{2}} \begin{bmatrix}(\epsilon_v t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}$$ when $v \in \mathcal{J}_1$, $\delta = 0$

  and both $\epsilon_v t, q$ are even.

- $$2+\sum_{k=1}^{\epsilon_v t-1} q^{\frac{k(\epsilon_v t-k)d_v}{2}} \prod_{a=0}^{k-1}\left(\frac{q^{\frac{(\epsilon_v t-a)d_v}{2}}-(-1)^{\epsilon_v t-a}}{q^{\frac{(k-a)d_v}{2}}-(-1)^{k-a}}\right)$$ when $v \in \mathcal{J}_2$.

Some open questions

- Classification of δ-self-dual, δ-self-orthogonal and δ-complementary dual MT additive codes over finite fields up to equivalence.
- Generator theory for MT additive codes over finite fields.
- The study of skew MT additive codes over finite fields, their duality and asymptotic properties.
- The study of MT additive codes over finite commutative chain rings and their duality properties.

References I


Aydin, N. and Halilović, A.,
A generalization of quasi-twisted codes: multi-twisted codes,
Finite Fields Appl. 45, pp. 96-106 (2017).


Cao, Y., Chang, X. and Cao, Y.,
Constacyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^\ell}$-codes,
Appl. Algebra Engrg. Comm. Comput. 26(4), pp. 369–388 (2015).


Chepyzhov, V. V.,
New lower bounds for minimum distance of linear quasi-cyclic and almost linear cyclic codes,
Probl. Peredachi Inf. 28(1), pp. 39-51 (1992).


Huffman, W. C.,
Cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes,
Int. J. Inf. Coding Theory 1(3), pp. 249-284 (2010).


Kabatiansky, G. A.,
On existence of good cyclic almost linear codes over nonprime fields,
Probl. Peredachi Inf. 13(3), pp. 18-21 (1977).

References II


Kaur, T. and Sharma, A.,
Constacyclic additive codes over finite fields,
Discrete Math. Algorithms Appl. 9(3), 1750037, pp. 35 (2017).


Sharma, A. and Kaur, T.,
On cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes,
Int. J. Inform. Coding Theory 4(1), pp. 19–46 (2017).


Sharma, S. and Sharma, A.,
Multi-twisted additive codes over finite fields,
Beiträge Algebra Geom. 63(2), pp. 287-320 (2021).


Sharma, S., Sharma, A.,
Multi-twisted additive codes over finite fields with complementary duals,
Probl. Inf. Transm. 58(1), pp. 32-57 (2022).


Sharma, S., Sharma, A.,
Multi-twisted additive codes over finite fields are asymptotically good,
Cryptogr. Commun. pp. 1-17 (2022).


Shi, M., Wu, R. and Solé, P.,
Asymptotically good additive cyclic codes exist,
IEEE Communications Letters 22(10), pp. 1980-1983 (2018).

Thank you...