Complete classification and encoding for cyclic codes over $\mathbb{Z}_4$ of length $4n$

Yonglin Cao

Shandong University of Technology

ylcao@sdut.edu.cn

(Joint work with Yuan Cao and Minjia Shi)

The 5th Sino-Korea Conference on Coding Theory and Its Related Topics

Shanghai University, Shanghai, China, July 4, 2018

Contents

Contents

Contents

Codes over $\mathbb{Z}_4$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Codes $\emptyset \neq \mathcal{C} \subseteq \mathbb{Z}_4^n$.

A subgroup $\mathcal{C}$ of $(\mathbb{Z}_4^n, +)$ is called a linear codes over $\mathbb{Z}_4$ of length n. If $\mathcal{C}$ has a minimum generator set with
▷ α generators of order 4; and
▷ β generators of order 2,
$\mathcal{C}$ is said to be of type $4^\alpha 2^\beta$. In this case, $|\mathcal{C}| = 2^{2\alpha+\beta}$.

Cyclic codes over $\mathbb{Z}_4$ of length n: a linear code $\mathcal{C}$ over $\mathbb{Z}_4$ of length n satisfies

$$(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}, \ \forall (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}.$$

Gray map from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$

Define $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ via

$$0 \mapsto 00,\ 1 \mapsto 01,\ 2 \mapsto 11,\ 3 \mapsto 10.$$

Define Lee weight on $\mathbb{Z}_4$ by
$\mathrm{w}_L(0) = \mathrm{w}_H(0,0) = 0,\ \mathrm{w}_L(1) = \mathrm{w}_H(0,1) = 1$
$\mathrm{w}_L(2) = \mathrm{w}_H(1,1) = 2,\ \mathrm{w}_L(3) = \mathrm{w}_H(1,0) = 1.$

Extend $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ to $\Phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ by

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto (\phi(a_0), \phi(a_1), \ldots, \phi(a_{n-1})).$$

Gray map from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$

The Gray map $\Phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ is a bijection preserving distance from $(\mathbb{Z}_4^n, \text{Lee distance})$ onto $(\mathbb{F}_2^{2n}, \text{Hamming distance})$ and preserves orthogonality.

For any code $\mathcal{C} \subseteq \mathbb{Z}_4^n$, let $D = \Phi(\mathcal{C}) \subseteq \mathbb{F}_2^{2n}$. D is called the **binary image** of $\mathcal{C}$ which is a binary code of length $2n$. In particular, we have

$$\Phi(\mathcal{C}^\perp) \subseteq D^\perp.$$

Gray map from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$

In particular, if $\mathcal{C}$ is a self-dual $\mathbb{Z}_4$-code of length n, the binary image $D = \Phi(\mathcal{C})$ is a binary self-dual code of length $2n$.

Moreover, the Hamming weight distribution of D is the same as the Lee weight distribution of $\mathcal{C}$, i.e.,

$$W_D^{(H)}(X, Y) = W_{\mathcal{C}}^{(L)}(X, Y).$$

A breakthrough in coding theory (cf. IEEE 1994)

In the early 1990s, a connection was made between linear codes over $\mathbb{Z}_4$ and non-linear binary codes in the landmark paper:

Calderbank, A.R., Hammons Jr., A.R., Kumar, P.V., Sloane, N.J.A. and Solé, P.: The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory **40** (1994), 301–319.

For an example, the **binary images** of the $\mathbb{Z}_4$-dual codes of the Kerdock codes are Preparata-like codes, having essentially the same properties as Preparata's original codes.

Constructing binary codes from $\mathbb{Z}_4$-codes

It has been an efficient way to construct good binary codes from $\mathbb{Z}_4$-codes with certain special structures (e.g., cyclic codes and self-dual codes over $\mathbb{Z}_4$).

Therefore, it is an meaningful topic to study linear codes over $\mathbb{Z}_4$ and $\mathbb{Z}_{2^k}$ $(k \geq 3)$ with certain algebraic structures. For example, cyclic codes, negacyclic codes, constacyclic codes, quasi-cyclic codes, quasi-twisted codes, ...

Constructing binary codes from $\mathbb{Z}_4$-codes

Compared with existing rich theory for binary cyclic codes, there are a lot of work to do for cyclic codes over $\mathbb{Z}_4$, especially, for cyclic codes over $\mathbb{Z}_4$ of even length.

Our goals

Let n be odd. In this talk, we consider cyclic codes over $\mathbb{Z}_4$ of length $4n$:

- Give a explicit representation for every cyclic code over $\mathbb{Z}_4$ of length $4n$ and a complete classification for all these codes.
- Determine the dual code and its self-duality for every cyclic code over $\mathbb{Z}_4$ of length $4n$.
- Provide an efficient encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$ (and their binary images).

Cyclic codes over $\mathbb{Z}_4$ of even length

Abualrub and Oehmk in [1] determined the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form 2^k, and Blackford in [2] presented the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form $2n$ where n is odd. The case for odd n follows from results in [3] and also appears in more detail in [9].

[1] T. Abualrub and R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. IT **49** (2003).

[2] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Discrete Appl. Math. **128** (2003).

[3] A. R. Calderbank and N. J. A. Sloane, Modular and p-adic cyclic codes, Des. Codes Cryptogr. **6** (1995).

[9] V. S. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. IT **42** (1996).

Des. Codes Cryptogr. **39** (2006)

Dougherty and Ling in [8] determined the structure of cyclic codes over $\mathbb{Z}_4$ for arbitrary even length giving the generator polynomial for these codes, described the number and dual codes of cyclic codes for a given length and presented the form of cyclic codes that are self-dual.

[8] S. T. Dougherty and S. Ling, Cyclic codes over $\mathbb{Z}_4$ of even length, Des. Codes Cryptogr. **39** (2006), 127–153.

Des. Codes Cryptogr. **39** (2006)

Cyclic codes over $\mathbb{Z}_4$ of length $2^k n \longleftrightarrow$ ideals of $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$. Let

$$\mathcal{R} = \frac{\mathbb{Z}_4[u]}{\langle u^{2^k}-1\rangle}.$$

By $x^{2^k n}-1 = u^{2^k}-1$, where $u = x^n$ satisfies $u^{2^k} = 1$ in the ring $\mathcal{R}$, the following diagram commutes

$$\begin{array}{ccc} \frac{\mathcal{R}[x]}{\langle x^n-u\rangle} & \longleftrightarrow & \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle} \\ \downarrow & & \downarrow \\ \mathcal{R}^n & \longleftrightarrow & \mathbb{Z}_4^{2^k n} \end{array}.$$

Des. Codes Cryptogr. **39** (2006)

Ideals of the ring $\frac{\mathcal{R}[x]}{\langle x^n - u \rangle} \longleftrightarrow$ ideals of $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1 \rangle}$.

u-constacyclic codes over $\mathcal{R}$ of length $n \longleftrightarrow$ cyclic codes over $\mathbb{Z}_4$ of length $2^k n$.

Then the ideals of $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1 \rangle}$ are determine by the following two steps.

Des. Codes Cryptogr. **39** (2006)

• For a positive integer m, and a monic basic irreducible polynomial $h_m(x)$ in $\mathbb{Z}_4[x]$ of degree m that divides $x^{2^m-1}-1$, define the following Galois ring:

$$\mathrm{GR}(4,m)=\frac{\mathbb{Z}_4[x]}{\langle h_m(x)\rangle}=\{\sum_{i=0}^{m-1}a_ix^i \mid a_0,a_1,\ldots,a_{m-1}\in\mathbb{Z}_4\}$$

in which the arithmetic is done modulo $h_m(x)$. Then $|\mathrm{GR}(4,m)|=4^m$.

Des. Codes Cryptogr. **39** (2006)

Then determine all ideals and their annihilator of the ring

$$\begin{aligned} R_4(u,m) &= \frac{\mathrm{GR}(4,m)[u]}{\langle u^{2^k}-1\rangle} \\ &= \{\sum_{j=0}^{2^k-1} \alpha_j u^j \mid \alpha_0,\alpha_1,\ldots,\alpha_{2^k-1} \in \mathrm{GR}(4,m)\} \end{aligned}$$

in which the arithmetic is done modulo $u^{2^k}-1$ (see Lemma 2.3, Proposition 2.5 and Theorem 2.6 in [8]). In particular, $|R_4(u,m)| = 4^{2^k m}$.

Des. Codes Cryptogr. **39** (2006)

• Let $M = \min\{l \in \mathbb{Z}^+ \mid 2^l \equiv 1 \pmod{n}\}$ and constructs a Galois ring $\mathrm{GR}(4, M)$ of 4^M elements. Let ζ denote a primitive nth root of unity in $\mathrm{GR}(4, M)$.

As n is odd, there exists integer n', $1 \leq n' \leq 2^k - 1$, such that

$$nn' \equiv 1 \pmod{2^k}.$$

Des. Codes Cryptogr. **39** (2006)

The map (DFT)

$$\widehat{\gamma} : \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1\rangle} \to \bigoplus_{l=0}^{n-1} \frac{\mathrm{GR}(4, m_l)[u]}{\langle u^{2^k} - 1\rangle}$$

defined by

$$\widehat{\gamma}(c(x)) = (\widehat{c}_l)_{l=0}^{n-1},$$

is an injective homomorphism of rings from $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$ into the **direct product ring** $\bigoplus_{l=0}^{n-1} \frac{\mathrm{GR}(4,m_l)[u]}{\langle u^{2^k}-1\rangle}$, where

$$\widehat{c}_l = c(u^{n'}\zeta^l) = \sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j}\zeta^{il} \in \frac{\mathrm{GR}(4, m_l)[u]}{\langle u^{2^k} - 1\rangle}.$$

Des. Codes Cryptogr. **39** (2006)

• Let $\mathcal{J}$ denote a complete set of representatives of the 2-cyclotomic cosets modulo n and, for each $\alpha \in \mathcal{J}$, let m_α denote the size of the 2-cyclotomic coset $J_\alpha^{(2)}$ containing α, i.e.,

$$m_\alpha = |J_\alpha^{(2)}| \text{ where } J_\alpha^{(2)} = \{2^l\alpha \pmod n \mid l = 0, 1, \ldots\}.$$

Then $n = \sum_{\alpha\in\mathcal{J}} |J_\alpha^{(2)}|$.

Des. Codes Cryptogr. **39** (2006)

It is known that $\frac{\mathrm{GR}(4,m_l)[u]}{\langle u^{2^k}-1\rangle} \cong \frac{\mathrm{GR}(4,m_\alpha)[u]}{\langle u^{2^k}-1\rangle}$ for every $l \in J_\alpha^{(2)}$ as rings, for any $c(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} x^{i+jn} \in \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$.
Furthermore, in [8] the authors defined

$$\gamma(c(x)) = (\widehat{c}_\alpha)_{\alpha \in \mathcal{J}},$$

where

$$\widehat{c}_\alpha = c(u^{n'}\zeta^\alpha) = \sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j} \zeta^{\alpha i} \in \frac{\mathrm{GR}(4, m_\alpha)[u]}{\langle u^{2^k}-1\rangle}.$$

Des. Codes Cryptogr. **39** (2006)

[8] Theorem 3.2

The map $\gamma : \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle} \to \bigoplus_{\alpha\in\mathcal{J}} \frac{\mathrm{GR}(4,m_\alpha)[u]}{\langle u^{2^k}-1\rangle}$ is a ring isomorphism.

[8] Corollary 3.3

If $\mathcal{C}$ is a cyclic code of length $2^k n$ over $\mathbb{Z}_4$, then $\mathcal{C}$ is isomorphic to $\bigoplus_{\alpha\in\mathcal{J}} C_\alpha$, where, for each $\alpha \in \mathcal{J}$, C_α is an ideal in the ring $R_4(u, m_\alpha) = \frac{\mathrm{GR}(4,m_\alpha)[u]}{\langle u^{2^k}-1\rangle}$.

There are **29 cases** for all ideals and their annihilators of $R_4(u, m_\alpha)$ ([8] Theorem 5.3) for arbitrary positive integer k.

Des. Codes Cryptogr. **39** (2006)

In [8],

$$\mathrm{GR}(4, m_l) = \{ \sum_{j=0}^{m_l-1} a_j \zeta^{jl} \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, m_l - 1 \}.$$

Let $\alpha \in \mathcal{J}$. For any $l \in J_\alpha^{(2)}$, where $0 \leq l \leq n-1$, it need to determine

$$\widehat{c}_l \in R_4(u, m_l) = \frac{\mathrm{GR}(4, m_l)[x]}{\langle x^{2^k} - 1 \rangle}$$

from

$$\widehat{c}_\alpha \in R_4(u, m_\alpha) = \frac{\mathrm{GR}(4, m_\alpha)[x]}{\langle x^{2^k} - 1 \rangle}.$$

Des. Codes Cryptogr. **39** (2006)

Then the inverse (determined by "Inverse discrete Fourier transform") $\gamma^{-1} : \bigoplus_{\alpha\in\mathcal{J}} \frac{\mathrm{GR}(4,m_\alpha)[u]}{\langle u^{2^k}-1\rangle} \to \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$ of γ is given by

$$\gamma^{-1}((\widehat{c}_\alpha)_{\alpha\in\mathcal{J}}) = \Psi\left(\frac{1}{n}(\widehat{c}(1), u^{-n\prime}\widehat{c}(\zeta), \ldots, u^{-(n-1)n\prime}\widehat{c}(\zeta^{n-1}))\right),$$

where $\widehat{c}(\zeta^l) = \sum_{h=0}^{n-1} \widehat{c}_{n-h}\zeta^{hl}$ (in which $\widehat{c}_n = \widehat{c}_0$) and

Des. Codes Cryptogr. **39** (2006)

$\Psi : \left(\frac{\mathbb{Z}_4[u]}{\langle u^{2^k}-1\rangle}\right)^n \to \mathbb{Z}_4^{2^k n}$ is defined by

$$\begin{aligned}
&\Psi\left(\sum_{j=0}^{2^k-1} a_{0,j}u^j, \ldots, \sum_{j=0}^{2^k-1} a_{n-1,j}u^j\right) \\
= \quad &(a_{0,0}, a_{1,0}, \ldots, a_{n-1,0}, a_{0,1}, a_{1,1}, \ldots, a_{n-1,1}, \\
&\ldots, a_{0,2^k-1}, a_{1,2^k-1}, \ldots, a_{n-1,2^k-1}).
\end{aligned}$$

Des. Codes Cryptogr. **39** (2006)

It may be some inconvenient to construct cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ by use of the representation given in [8], as the following lacks:

- How to determine $\mathrm{GR}(4, m_\alpha) = \{\sum_{j=0}^{m_\alpha - 1} a_j \zeta^{j\alpha} \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, m_\alpha - 1\}$ explicitly?

- How to determine $\widehat{c}_l$ from $\widehat{c}_\alpha \in R_4(u, m_\alpha) = \frac{\mathrm{GR}(4, m_\alpha)[x]}{\langle x^{2^k} - 1 \rangle}$, for all $l \in J_\alpha^{(2)}$?

[4] AAECC **27** (2016)

In fact,

$$\mathrm{GR}(4, m_\alpha) = \frac{\mathbb{Z}_4[y]}{\langle f_\alpha(y)\rangle},$$

where $f_\alpha(y)$ is the minimal polynomial of ζ^α in $\mathbb{Z}_4[y]$ and

$$y^n - 1 = \prod_{\alpha\in\mathcal{J}} f_\alpha(y).$$

We can give an isomorphism from $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$ onto the direct ring $\prod_{\alpha\in\mathcal{J}} \frac{\mathbb{Z}_4[y]/\langle f_\alpha(y)\rangle}{\langle x^{2^k}-y\rangle}$ directly.

Hence we don't need to determine $\widehat{c}_l$ from $\widehat{c}_\alpha \in R_4(u, m_\alpha) = \frac{\mathrm{GR}(4,m_\alpha)[x]}{\langle x^{2^k}-1\rangle}$, for any $l \in J_\alpha^{(2)}$.

AAECC **27** (2016)

Let $\mathcal{A} = \frac{\mathbb{Z}_4[y]}{\langle y^n - 1 \rangle}$. By $x^{2^k n} - 1 = y^n - 1$, where $y = x^{2^k}$ in the ring $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1 \rangle}$, we have the following diagram

$$\begin{array}{ccc} \frac{\mathcal{A}[x]}{\langle x^{2^k} - y \rangle} & = & \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1 \rangle} \\ \downarrow & & \downarrow \\ \mathcal{A}^{2^k} & \longleftrightarrow & \mathbb{Z}_4^{2^k n} \end{array} .$$

[4] Y. Cao, Y. Cao and Q. Li, Concatenated structure of cyclic codes over $\mathbb{Z}_4$ of length $4n$, Appl. Algebra in Engrg. Comm. Comput. **10** (2016), 279–302.

AAECC **27** (2016)

$\mathcal{C}$ is a cyclic code of length $2^k n$ over $\mathbb{Z}_4$ if and only if $\mathcal{C}$ is an ideal of the ring $\frac{\mathcal{A}[x]}{\langle x^{2^k} - y \rangle}$, where

$$\begin{aligned} \mathcal{A} &= \frac{\mathbb{Z}_4[y]}{\langle y^n - 1 \rangle} \\ &= \{ \sum_{i=0}^{n-1} a_i y^i \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_4 \} \end{aligned}$$

in which the arithmetic is done modulo $y^n - 1$.

AAECC **27** (2016)

Assume

$$y^n - 1 = f_1(y) f_2(y) \dots f_r(y),$$

where $f_1(y), f_2(y), \dots, f_r(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$. We assume $\deg(f_i(y)) = m_i$ and denote

$$R_i = \frac{\mathbb{Z}_4[y]}{\langle f_i(y) \rangle} = \{ \sum_{j=0}^{m_i - 1} b_j y^j \mid b_0, b_1, \dots, b_{m_i - 1} \in \mathbb{Z}_4 \}$$

in which the arithmetic is done modulo $f_i(y)$, for all $i = 1, \dots, r$.

Then $\mathcal{A} \cong R_1 \times R_2 \times \ldots \times R_r$.

AAECC **27** (2016)

Let $1 \leq i \leq r$ and denote $F_i(y) = \frac{y^n-1}{f_i(y)} \in \mathbb{Z}_4[y]$.
Then there are polynomials $u_i(y), v_i(y) \in \mathbb{Z}_4[y]$ such that $u_i(y)F_i(y) + v_i(y)f_i(y) = 1$. Set $\varepsilon_i(y) \in \mathcal{A}$ satisfying

$$\varepsilon_i(y) \equiv u_i(y)F_i(y) = 1 - v_i(y)f_i(y) \pmod{y^n - 1}.$$

and denote

$$\mathcal{A}_i = \varepsilon_i(y)\mathcal{A} = \left\langle \frac{y^n - 1}{f_i(y)} \right\rangle \trianglelefteq \mathcal{A}.$$

AAECC **27** (2016)

- $\mathcal{A}_i$ is a cyclic code over $\mathbb{Z}_4$ of length n having parity check polynomial $f_i(y)$, and $|\mathcal{A}_i| = 4^{m_i}$.
- The map

$$\varphi_i : b(y) \mapsto \varepsilon_i(y)b(y) \ (\forall b(y) \in R_i)$$

is a ring isomorphism from the Galois ring R_i onto the cyclic code $\mathcal{A}_i$.

AAECC **27** (2016)

Let

$$\frac{R_i[x]}{\langle x^{2^k}-y\rangle} = \{\sum_{j=0}^{2^k-1} \beta_j x^j \mid \beta_j \in R_i, j = 0, 1, \ldots, 2^k-1\}$$

in which the arithmetic is done modulo $x^{2^k}-y$.

- C_i is a y-constacyclic code over $R_i = \frac{\mathbb{Z}_4[y]}{\langle f_i(y)\rangle}$ of length 2^k if and only if C_i is an ideal of the ring $\frac{R_i[x]}{\langle x^{2^k}-y\rangle}$

AAECC **27** (2016)

[4] Theorem 2.6

$\mathcal{C}$ is a cyclic code over $\mathbb{Z}_4$ of length $2^k n$ if and only if for each $1 \leq i \leq r$, there is a unique ideal C_i of $\frac{R_i[x]}{\langle x^{2^k}-y\rangle}$, such that

$$\mathcal{C} = (\mathcal{A}_1 \square_{\varphi_1} C_1) \oplus \ldots \oplus (\mathcal{A}_r \square_{\varphi_r} C_r),$$

where

$$\begin{aligned} \mathcal{A}_i \square_{\varphi_i} C_i \quad = \quad & \{(\varphi_i(\beta_0), \varphi_i(\beta_1), \ldots, \varphi_i(\beta_{2^k-1}) \\ & \mid (\beta_0, \beta_1, \ldots, \beta_{2^k-1}) \in C_i\} \end{aligned}$$

which is the concatenated code of $\mathcal{A}_i$ and C_i, for all $i = 1, \ldots, r$.

AAECC **27** (2016)

As n is odd, there is a positive integer e, $1 \leq e < n$, such that $2^k e \equiv -1 \pmod{n}$. We denote

$$\theta_i(y) = y^e \pmod{f_i(y)},$$

and set

$$\pi_i = y^e x - 1 = \theta_i(y)x - 1 \in R_i[x]/\langle x^{2^k} - y \rangle.$$

From now on, let $k = 2$. Then all distinct y-constacyclic codes C_i over the Galois ring R_i of length $2^2 = 4$, i.e. all distinct ideals of the ring $\frac{R_i[x]}{\langle x^4 - y \rangle}$, and their annihilating ideals are given by one of the following **20 cases**:

AAECC **27** (2016)

[4] Theorem 3.3

case	C_i	$\lvert C_i\rvert$	$\mathrm{Ann}(C_i)$	L_C
1.	$\langle 0\rangle$	1	$\langle 1\rangle$	1
2.	$\langle 1\rangle$	2^{8m_i}	$\langle 0\rangle$	1
3.	$\langle \pi_i^j\rangle$ $(j=1,2)$	$2^{2m_i(4-j)}$	$\langle \pi_i^{4-j}+2\pi_i^{2-j}\rangle$	2
4.	$\langle 2\rangle$	2^{4m_i}	$\langle 2\rangle$	1
5.	$\langle 2\pi_i^s\rangle$ $(s=1,2,3)$	$2^{m_i(4-s)}$	$\langle \pi_i^{4-s},2\rangle$	3
6.	$\langle \pi_i+2h\rangle$ $(h\in\mathcal{T}_i\setminus\{0\})$	2^{6m_i}	$\langle \pi_i^3+2\pi_i(1+\pi_i h)\rangle$	$2^{m_i}-1$
7.	$\langle \pi_i^2+2\pi_i h\rangle$ $(h\in\mathcal{T}_i\setminus\{0\})$	2^{4m_i}	$\langle \pi_i^2+2(1+\pi_i h)\rangle$	$2^{m_i}-1$
8.	$\langle \pi_i^2+2(h+\pi_i g)\rangle$ $(h\in\mathcal{T}_i\setminus\{0,1\}, g\in\mathcal{T}_i)$	2^{4m_i}	$\langle \pi_i^2+2(1+h+\pi_i g)\rangle$	$2^{2m_i}-2^{m_i+1}$
9.	$\langle \pi_i^2+2(1+\pi_i h)\rangle$ $(h\in\mathcal{T}_i\setminus\{0\})$	2^{4m_i}	$\langle \pi_i^2+2\pi_i h\rangle$	$2^{m_i}-1$
10.	$\langle \pi_i^3+2\pi_i(3+\pi_i h)\rangle$ $(h\in\mathcal{T}_i\setminus\{0\})$	2^{2m_i}	$\langle \pi_i+2h\rangle$	$2^{m_i}-1$

AAECC **27** (2016)

[4] Theorem 3.3

case	C_i	$\lvert C_i\rvert$	$\mathrm{Ann}(C_i)$	L_C
11.	$\langle \pi_i^3 + 2h\rangle$ $(h \in \mathcal{T}_i)$	2^{4m_i}	$\langle \pi_i^3 + 2h\rangle$	2^{m_i}
13.	$\langle \pi_i^j + 2\pi_i^{j-2}\rangle$ $(j = 2, 3)$	$2^{2m_i(4-j)}$	$\langle \pi_i^{4-j}\rangle$	2
14.	$\langle \pi_i^j, 2\rangle$ $(j = 1, 2, 3)$	$2^{m_i(8-j)}$	$\langle 2\pi_i^{4-j}\rangle$	3
15.	$\langle \pi_i^2 + 2, 2\pi_i\rangle$	2^{5m_i}	$\langle \pi_i^3, 2\pi_i^2\rangle$	1
16.	$\langle \pi_i^3, 2\pi_i^2\rangle$	2^{3m_i}	$\langle \pi_i^2 + 2, 2\pi_i\rangle$	1
17.	$\langle \pi_i^3 + 2\pi_i, 2\pi_i^2\rangle$	2^{3m_i}	$\langle \pi_i^2, 2\pi_i\rangle$	1
18.	$\langle \pi_i^2, 2\pi_i\rangle$	2^{5m_i}	$\langle \pi_i^3 + 2\pi_i, 2\pi_i^2\rangle$	1
19.	$\langle \pi_i^2 + 2h, 2\pi_i\rangle$ $(h \in \mathcal{T}_i \setminus \{0, 1\})$	2^{5m_i}	$\langle \pi_i^3 + 2\pi_i(1 + h), 2\pi_i^2\rangle$	$2^{m_i} - 2$
20.	$\langle \pi_i^3 + 2\pi_i h, 2\pi_i^2\rangle$ $(h \in \mathcal{T}_i \setminus \{0, 1\})$	2^{3m_i}	$\langle \pi_i^2 + 2(1 + h), 2\pi_i\rangle$	$2^{m_i} - 2$

where $\mathcal{T}_i = \{\sum_{j=0}^{m_i-1} t_j y^j \mid t_0, t_1, \ldots, t_{m_i-1} \in \{0, 1\}\}$ and L_C is the number of codes in the same row.

AAECC **27** (2016)

There are still some inconvenient to construct cyclic codes over $\mathbb{Z}_4$ of length $4n$ by use of the representation given in [4], as we have not to give the expression of

$$\pi_i = y^e x - 1 = \theta_i(y)x - 1 \in R_i[x]/\langle x^4 - y \rangle$$

explicitly, for each different i: $1 \leq i \leq r$.

AAECC **27** (2016)

When $n = 7$, we have $y^7 - 1 = f_1(y)f_2(y)f_3(y)$ where $f_1(y) = y - 1$, $f_2(y) = y^3 + 2y^2 + y + 3$ and $f_3(y) = y^3 + 3y^2 + 2y + 3$. In page 296 of [4], we have

- $\pi_1 = x - 1 \in R_1[x]/\langle x^4 - y\rangle$;
- $\pi_2 = (y^2 + 3y + 3)x - 1 \in R_2[x]/\langle x^4 - y\rangle$;
- $\pi_3 = (2y^2 + 3y + 3)x - 1 \in R_3[x]/\langle x^4 - y\rangle$.

Main idea

Recall that $f_i(y)$ is a monic basic irreducible divisor of $y^n - 1$ in $\mathbb{Z}_4[y]$, $\deg(f_i(y)) = m_i$, and

$$R_i = \frac{\mathbb{Z}_4[y]}{\langle f_i(y) \rangle}.$$

In [4], we determine the ideals of $\frac{R_i[x]}{\langle x^4 - y \rangle}$ by the ring isomorphism

$$\frac{R_i[u]}{\langle u^4 - 1 \rangle} \to \frac{R_i[x]}{\langle x^4 - y \rangle} \text{ via } u \mapsto y^e x \pmod{f_i(y)}.$$

Main idea

In fact, we have

$$\frac{R_i[x]}{\langle x^4 - y\rangle} \cong \frac{\mathbb{Z}_4[x,y]}{\langle f_i(y), y - x^4\rangle} \cong \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}.$$

Then will determine the ideals of the ring

$$\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$$

directly. Denote $\overline{\mathcal{K}_i} = \frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x)^4\rangle} = \mathcal{K}_i \pmod 2$ and $\mathcal{T}_i = \{\sum_{j=0}^{m_i-1} t_j x^j \mid t_j \in \{0,1\},\ j = 0,\ldots,m_i-1\}$.

Properties of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4) \rangle}$

Lemma 3.3

There exists a unique ordered pair $(w_{i,0}(x), w_{i,1}(x))$ of elements in $\mathcal{T}_i = \text{“}\frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x) \rangle}\text{”}$ such that

$$f_i(x)^4 = 2f_i(x)^2 \left(w_{i,0}(x) + w_{i,1}(x)\overline{f}_i(x)\right) \text{ in } \mathcal{K}_i \text{ and } w_{i,0}(x) \neq 0.$$

Ideals of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$

Lemma 3.5

Let C be a nonzero ideal of $\mathcal{K}_i$. Then there is a unique ordered pair (l, s) of integers, $0 \leq s \leq l \leq 4$, and there exists $v(x) \in \overline{\mathcal{K}}_i$ such that

$$C = \langle f_i(x)^l + 2v(x), 2\overline{f}_i(x)^s \rangle \text{ with } |C| = 2^{m_i(8-(l+s))}.$$

Ideals of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$

Theorem 3.6

All distinct ideals of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$ and their annihilating ideals are given by the following table (**10 cases**)

L	C_i	$\lvert C_i\rvert$	$\mathrm{Ann}(C_i)$
1	• $\langle 0\rangle$	1	$\langle 1\rangle$
1	• $\langle 1\rangle$	2^{8m_i}	$\langle 0\rangle$
4	• $\langle 2\overline{f}_i(x)^s\rangle$ $(s=0,1,2,3)$	$2^{m_i(4-s)}$	$\langle f_i(x)^{4-s}, 2\rangle$
3	• $\langle f_i(x)^l, 2\rangle$ $(l=1,2,3)$	$2^{m_i(8-l)}$	$\langle 2\overline{f}_i(x)^{4-l}\rangle$
2^{m_i}	• $\langle f_i(x)+2h(x)\rangle$	2^{6m_i}	$\langle f_i(x)^3 + 2\overline{f}_i(x)(w_{i,0}(x) + \vartheta_i(x)\overline{f}_i(x))\rangle$ $\vartheta_i(x) = w_{i,1}(x) + h(x)$
2^{m_i}	• $\langle f_i(x)^2 + 2h(x), 2\overline{f}_i(x)\rangle$	2^{5m_i}	$\langle f_i(x)^3 + 2\overline{f}_i(x)t_i(x), 2\overline{f}_i(x)^2\rangle$ $t_i(x) = w_{i,0}(x) + h(x)$

Ideals of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$

Theorem 3.6 (continue)

L	C_i	$\lvert C_i\rvert$	$\mathrm{Ann}(C_i)$
4^{m_i}	• $\langle 2(h_0(x)+h_1(x)\overline{f}_i(x)) + f_i(x)^2\rangle$	2^{4m_i}	$\langle 2(\delta_{i,0}(x)+\delta_{i,1}(x)\overline{f}_i(x)) + f_i(x)^2\rangle$ $\delta_{i,j}(x) = w_{i,j}(x)+h_j(x)$
2^{m_i}	• $\langle f_i(x)^3+2h(x), 2\overline{f}_i(x)\rangle$	2^{4m_i}	$\langle f_i(x)^3+2h(x), 2\overline{f}_i(x)\rangle$
2^{m_i}	• $\langle f_i(x)^3+2\overline{f}_i(x)h(x), 2\overline{f}_i(x)^2\rangle$	2^{3m_i}	$\langle f_i(x)^2+2t_i(x), 2\overline{f}_i(x)\rangle$ $t_i(x) = w_{i,0}(x)+h(x)$
2^{m_i}	• $\langle f_i(x)^3+2\overline{f}_i(x)(w_{i,0}(x) + h(x)\overline{f}_i(x))\rangle$	2^{2m_i}	$\langle f_i(x)+2\vartheta_i(x)\rangle$ $\vartheta_i(x) = w_{i,1}(x)+h(x)$

where L is the number of ideals C in the same row and $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$. Therefore, the number of ideals in $\mathcal{K}_i$ is equal to $9 + 5\cdot 2^{m_i} + 4^{m_i}$.

Idempotents of the ring $\mathcal{B} = \mathbb{Z}_4[x]/\langle x^{4n} - 1\rangle$

By $y^n - 1 = f_1(y)f_2(y)\dots f_r(y)$, we have

$$x^{4n} - 1 = (x^4)^n - 1 = f_1(x^4)f_2(x^4)\dots f_r(x^4).$$

As $u_i(y)F_i(y) + v_i(y)f_i(y) = 1$, where $F_i(y) = \frac{y^n-1}{f_i(y)}$ and $u_i(y), v_i(y) \in \mathbb{Z}_4[y]$, we define

$$e_i(x) \equiv u_i(x^4)F_i(x^4) = 1 - v_i(x^4)f_i(x^4) \pmod{x^{4n} - 1}.$$

Then $e_1(x) + \ldots + e_r(x) = 1$, $e_i(x)^2 = e_i(x)$ and $e_i(x)e_j(x) = 0$ for all $1 \le i \ne j \le r$ in the ring $\mathcal{B} = \mathbb{Z}_4[x]/\langle x^{4n} - 1\rangle$.

Cyclic codes over $\mathbb{Z}_4$ of length $4n$

$\mathcal{C}$ is a cyclic code over $\mathbb{Z}_4$ of length $4n$, i.e. $\mathcal{C}$ is an ideal of

$$\mathcal{B} = \frac{\mathbb{Z}_4[x]}{\langle x^{4n} - 1 \rangle}$$

if and only if for each integer i, $1 \leq i \leq r$, there is a unique ideal C_i of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4) \rangle}$ such that

$$\mathcal{C} = \bigoplus_{i=1}^{r} e_i(x) C_i = \sum_{i=1}^{r} e_i(x) C_i \pmod{x^{4n} - 1}.$$

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Lemma 4.1

Let $C_i = \langle f_i(x)^l + 2v(x), 2\overline{f}_i(x)^s \rangle$ an ideal of $\mathcal{K}_i$, where $v(x) \in \overline{\mathcal{K}}_i$ and $0 \leq s \leq l \leq 4$. For any $\underline{a} = (a_0, a_1, \ldots, a_{(4-l)m_i-1}) \in \mathbb{Z}_4^{(4-l)m_i}$ and $\underline{b} = (b_0, b_1, \ldots, b_{(l-s)m_i-1}) \in \mathbb{Z}_2^{(l-s)m_i}$), we define a map ϱ by

$$\varrho(\underline{a}, \underline{b}) = \sum_{j=0}^{(4-l)m_i-1} a_j x^j \left(f_i(x)^l + 2v(x) \right) + \sum_{t=0}^{(l-j)m_i-1} 2b_t x^t \overline{f}_i(x)^s$$

Then ϱ is an isomorphism of additive groups from $\mathbb{Z}_4^{(4-l)m_i} \times \mathbb{Z}_2^{(l-s)m_i}$ onto C_i. Hence C_i is an abelian group of type $4^{(4-l)m_i} 2^{(l-s)m_i}$.

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Theorem 4.2

Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $4n$ with canonical form decomposition $\mathcal{C} = \bigoplus_{i=1}^{r} \mathcal{C}_i$, where $\mathcal{C}_i = e_i(x)C_i \subseteq \mathcal{C}$ and C_i is an ideal of $\mathcal{K}_i$ listed by Theorem 3.6. Then for each integer i, $1 \leq i \leq r$, the type of $\mathcal{C}_i$ is given by the following table:

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Theorem 4.2 (continue)

Case	C_i	the type of $\mathcal{C}_i$
1.	$\langle 0 \rangle$	$4^0 2^0$
2.	$\langle 1 \rangle$	$4^{4m_i} 2^0$
3.	$\langle 2\overline{f}_i(x)^s \rangle$ $(s = 0, 1, 2, 3)$	$4^0 2^{(4-s)m_i}$
4.	$\langle f_i(x)^l, 2 \rangle$ $(l = 1, 2, 3)$	$4^{(4-l)m_i} 2^{lm_i}$
5.	$\langle f_i(x) + 2h(x) \rangle$	$4^{3m_i} 2^0$
6.	$\langle f_i(x)^2 + 2h(x), 2\overline{f}_i(x) \rangle$	$4^{2m_i} 2^{m_i}$
7.	$\langle f_i(x)^2 + 2(h_0(x) + h_1(x)\overline{f}_i(x)) \rangle$	$4^{2m_i} 2^0$
8.	$\langle f_i(x)^3 + 2h(x), 2\overline{f}_i(x) \rangle$	$4^{m_i} 2^{2m_i}$
9.	$\langle f_i(x)^3 + 2\overline{f}_i(x)h(x), 2\overline{f}_i(x)^2 \rangle$	$4^{m_i} 2^{m_i}$
10.	$\langle f_i(x)^3 + 2\overline{f}_i(x)\left(w_{i,0}(x) + h(x)\overline{f}_i(x)\right) \rangle$	$4^{m_i} 2^0$

where $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$.

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Theorem 4.2 (continue)

Precisely, an encoder of the subcode $\mathcal{C}_i$ is given by the following:

Case 1. $\mathcal{C}_i = \{0\}$.

Case 2. $\mathcal{C}_i = \{\sum_{j=0}^{4m_i-1} a_j x^j e_i(x) \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, 4m_i - 1\}$.

Case 3. $\mathcal{C}_i = \{\sum_{t=0}^{(4-s)m_i-1} 2b_t x^t \overline{f}_i(x)^s e_i(x) \mid b_0, b_1, \ldots, b_{(4-s)m_i-1} \in \mathbb{Z}_2\}$.

Case 4. $\mathcal{C}_i = \{\sum_{j=0}^{(4-l)m_i-1} a_j x^j f_i(x)^l e_i(x) + \sum_{t=0}^{lm_i-1} 2b_t x^t e_i(x) \mid a_j \in \mathbb{Z}_4,\ b_t \in \mathbb{Z}_2, j = 0, 1, \ldots, (4-l)m_i - 1$ and $t = 0, 1, \ldots, lm_i - 1\}$.

Case 5. $\mathcal{C}_i = \{\sum_{j=0}^{3m_i-1} a_j x^j \left(f_i(x) + 2h(x)\right) e_i(x) \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, 2, \ldots, 3m_i - 1\}$.

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Theorem 4.2 (continue)

Case 6.

$$\mathcal{C}_i = \{ \sum_{j=0}^{2m_i-1} a_j x^j \left(f_i(x)^2 + 2h(x)\right) e_i(x) + \sum_{t=0}^{md_i-1} 2b_t x^t \overline{f}_i(x) e_i(x) \mid a_j \in \mathbb{Z}_4,\ b_t \in \mathbb{Z}_2,\ j = 0, 1, \ldots, 2m_i - 1 \text{ and } t = 0, 1, \ldots, m_i - 1\}.$$

Case 7. $\mathcal{C}_i = \{\sum_{j=0}^{2m_i-1} a_j x^j \left(f_i(x)^2 + 2\left(h_0(x) + h_1(x)\overline{f}_i(x)\right)\right) e_i(x) \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, 2m_i - 1\}$.

Case 8.

$$\mathcal{C}_i = \{ \sum_{j=0}^{m_i-1} a_j x^j \left(f_i(x)^3 + 2h(x)\right) e_i(x) + \sum_{t=0}^{2m_i-1} 2b_t x^t \overline{f}_i(x) e_i(x) \mid a_j \in \mathbb{Z}_4,\ b_t \in \mathbb{Z}_2,\ j = 0, 1, \ldots, m_i - 1 \text{ and } t = 0, 1, \ldots, 2m_i - 1\}.$$

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Theorem 4.2 (continue)

Case 9.

$$\begin{aligned}\mathcal{C}_i &= \{\sum_{j=0}^{m_i-1} a_j x^j \left(f_i(x)^3 + 2\overline{f}_i(x)h(x)\right) e_i(x) + \sum_{t=0}^{m_i-1} 2b_t x^t \overline{f}_i(x)^2 e_i(x) \\ &\quad \mid a_j s \in \mathbb{Z}_4,\ b_t \in \mathbb{Z}_2,\ j = 0, 1, \ldots, m_i - 1 \text{ and } t = 0, 1, \ldots, m_i - 1\}.\end{aligned}$$

Case 10.

$$\begin{aligned}\mathcal{C}_i &= \{\sum_{j=0}^{d_i-1} a_j x^j \left(f_i(x)^3 + 2\overline{f}_i(x)\left(w_{i,0}(x) + h(x)\overline{f}_i(x)\right)\right) e_i(x) \\ &\quad \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, m_i - 1\}.\end{aligned}$$

Encoder for any cyclic code over $\mathbb{Z}_4$ of length $4n$

Theorem 4.2 (continue)

Moreover, if the subcode $\mathcal{C}_i$ is of type $4^{k_{0,i}}2^{k_{1,i}}$ for all $1 \leq i \leq r$, then $\mathcal{C}$ is of type

$$4^{\sum_{i=1}^{r} k_{0,i}} 2^{\sum_{i=1}^{r} k_{1,i}}.$$

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

For any polynomial $f(y) = \sum_{j=0}^{d} c_j y^j \in \mathbb{Z}_4[y]$ of degree $d \geq 1$, the *reciprocal polynomial* of $f(y)$ is defined as

$$\widetilde{f}(y) = \widetilde{f(y)} = y^d f(\frac{1}{y}) = \sum_{j=0}^{d} c_j y^{d-j}.$$

Then $f(y)$ is said to be *self-reciprocal* if $\widetilde{f}(y) = \delta f(y)$ for some $\delta \in \mathbb{Z}_4^{\times} = \{1, -1\}$. After a rearrangement of $f_1(y), \ldots, f_r(y)$ there are integers λ, ϵ such that

- $\lambda \geq 1, \epsilon \geq 0$ and $\lambda + 2\epsilon = r$;
- $f_i(y)$ is reciprocal, for all $i = 1, \ldots, \lambda$;
- $\widetilde{f}_{\lambda+j}(y) = \delta_{\lambda+j} f_{\lambda+\epsilon+j}(y)$, for all $j = 1, \ldots, \epsilon$.

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $4n$ with canonical form decomposition $\mathcal{C} = \oplus_{i=1}^{r} e_i(x)C_i$, where C_i is an ideal of $\mathcal{B}_i$. Then $\mathcal{C}$ is self-dual if and only if for each integer i, $1 \leq i \leq r$, C_i satisfies one of the following conditions.

(i) *If $1 \leq i \leq \lambda$, C_i is given by one of the following three cases:*

(i-1) $C_i = \langle 2 \rangle$.

(i-2) $C_i = \langle f_i(x)^2 + 2(h_0(x) + h_1(x)\overline{f}_i(x)) \rangle$, *where* $h_0(x), h_1(x) \in \mathcal{T}_i = \{\sum_{j=0}^{m_i-1} a_j x^j \mid a_0, a_1, \ldots, a_{m_i-1} \in \{0,1\}\}$ *s.t.*

$$h_0(x) + x^{2m_i}(w_{i,0}(x^{-1}) + h_0(x^{-1})) \equiv 0 \pmod{\langle \overline{f}_i(x), 2 \rangle},$$

$$h_1(x) + x^{m_i}(w_{i,1}(x^{-1}) + h_1(x^{-1})) \equiv 0 \pmod{\langle \overline{f}_i(x), 2 \rangle}.$$

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

(i-3) $C_i = \langle f_i(x)^3 + 2h(x), 2\overline{f}_i(x)\rangle$, *where* $h(x) \in \mathcal{T}_i$ *satisfying the following condition*:

$$h(x) + x^{3m_i} h(x^{-1}) \equiv 0 \pmod{\langle \overline{f}_i(x), 2\rangle}.$$

(ii) *If* $i = \lambda + j$ *where* $1 \leq j \leq \epsilon$, $(C_i, C_{i+\epsilon})$ *is given by one of the following eleven cases*:

(ii-1) $C_i = \langle 0\rangle$ *and* $C_{i+\epsilon} = \langle 1\rangle$;

(ii-2) $C_i = \langle 1\rangle$ *and* $C_{i+\epsilon} = \langle 0\rangle$;

(ii-3) $C_i = \langle 2\overline{f}_i(x)^s\rangle$ *and* $C_{i+\epsilon} = \langle f_{i+\epsilon}(x)^{4-s}, 2\rangle$, *where* $s = 0, 1, 2, 3$;

(ii-4) $C_i = \langle f_i(x)^l, 2\rangle$ *and* $C_{i+\epsilon} = \langle 2\overline{f}_{i+\epsilon}(x)^{4-l}\rangle$, *where* $l = 1, 2, 3$;

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

(ii-5) $C_i = \langle f_i(x) + 2h(x) \rangle$ *and*

$$C_{i+\epsilon} = \left\langle f_{i+\epsilon}(x)^3 + 2\overline{f}_{i+\epsilon}(x)\left(x^{2m_i} w_{i,0}(x^{-1}) + \widehat{\vartheta}_i(x)\overline{f}_{i+\epsilon}(x)\right)\right\rangle,$$

where $\widehat{\vartheta}_i(x) = x^{m_i}(w_{i,1}(x^{-1}) + h(x^{-1}))$ *and* $h(x) \in \mathcal{T}_i$;

(ii-6) $C_i = \langle f_i(x)^2 + 2h(x), 2\overline{f}_i(x) \rangle$ *and*

$$C_{i+\epsilon} = \left\langle f_{i+\epsilon}(x)^3 + 2\overline{f}_{i+\epsilon}(x)\widehat{t}_i(x), 2\overline{f}_{i+\epsilon}(x)^2 \right\rangle,$$

where $\widehat{t}_i(x) = x^{2m_i}(w_{i,0}(x^{-1}) + h(x^{-1}))$ *and* $h(x) \in \mathcal{T}_i$;

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

(ii-7) $C_i = \langle f_i(x)^2 + 2(h_0(x) + h_1(x)\overline{f}_i(x))\rangle$ *and*

$$C_{i+\epsilon} = \left\langle f_{i+\epsilon}(x)^2 + 2(\widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\overline{f}_{i+\epsilon}(x))\right\rangle,$$

where $\widehat{\delta}_{i,0}(x) = x^{2m_i}(w_{i,0}(x^{-1}) + h_0(x^{-1}))$,
$\widehat{\delta}_{i,1}(x) = x^{m_i}(w_{i,1}(x^{-1}) + h_1(x^{-1}))$ *and* $h_0(x), h_1(x) \in \mathcal{T}_i$;

(ii-8) $C_i = \langle f_i(x)^3 + 2h(x), 2\overline{f}_i(x)\rangle$ *and*

$$C_{i+\epsilon} = \left\langle f_{i+\epsilon}(x)^3 + 2x^{3m_i}h(x^{-1}), 2\overline{f}_{i+\epsilon}(x)\right\rangle,$$

where $h(x) \in \mathcal{T}_i$;

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

(ii-9) $C_i = \langle f_i(x)^3 + 2\overline{f}_i(x)h(x), 2\overline{f}_i(x)^2 \rangle$ *and*

$$C_{i+\epsilon} = \left\langle f_{i+\epsilon}(x)^2 + 2\widehat{t}_i(x), 2\overline{f}_{i+\epsilon}(x) \right\rangle,$$

where $\widehat{t}_i(x) = x^{2m_i}(w_{i,0}(x^{-1}) + h(x^{-1}))$ *and* $h(x) \in \mathcal{T}_i$;

(ii-10) $C_i = \langle f_i(x)^3 + 2\overline{f}_i(x)(w_{i,0}(x) + h(x)\overline{f}_i(x)) \rangle$ *and*

$$C_{i+\epsilon} = \left\langle f_{i+\epsilon}(x) + 2\widehat{\vartheta}_i(x) \right\rangle,$$

where $\widehat{\vartheta}_i(x) = x^{m_i}(w_{i,1}(x^{-1}) + h(x^{-1}))$ *and* $h(x) \in \mathcal{T}_i$.

Self-dual cyclic codes over $\mathbb{Z}_4$ of length 28

We list all distinct 339 self-dual codes over $\mathbb{Z}_4$ of length 28.

Let d_H, d_L and d_E be the minimum Hamming distance, Lee distance and Euclidean distance of a $\mathbb{Z}_4$-code, respectively. Among the 339 self-dual codes over $\mathbb{Z}_4$ of length 28, we have 50 new good codes with basic parameters $(28, |C| = 2^{28}, d_H = 4, d_L = 8, d_E = 8)$, these self-dual and cyclic $\mathbb{Z}_4$-codes do not exist in [11] and [14]

[11] M. Shi, L. Qian, L. Sok, N. Aydin, P. Solé, On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ and their Gray images, Finite Fields Appl. **45** (2017), 86–95.

[14] Database of $\mathbb{Z}_4$ codes [online], http://www.z4codes.info (accessed on 03 September 2016).

Thank you for your attention!