Quaternary and binary codes as Gray images of constacyclic codes over $\mathbb{Z}_{2^{k+1}}$

Henry Chimal Dzul
Depto. de Matemáticas, UAM-Iztapalapa

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

Noncommutative rings and their applications IV
University of Artois, Lens, France

8-11 June 2015

Outline

Outline

1. Preliminaries
2. Formulation of the problem
3. Some contributions

Constacyclic codes

Let R be a finite commutative ring with 1, $\gamma \in \mathcal{U}(R)$ and $n \geq \mathbb{N}$.

- $\mathcal{C} \subseteq R^n$ is a constacyclic code or a γ-cyclic code if $\nu_\gamma(\mathcal{C}) = \mathcal{C}$, where

$$\nu_\gamma : (a_0, a_1, \ldots, a_{n-1}) \mapsto (\gamma a_{n-1}, a_0, \ldots, a_{n-2}).$$

- $\mathcal{C} \subseteq R^n$ is a cyclic code if $\sigma(\mathcal{C}) = \mathcal{C}$, where $\sigma = \nu_1$.
- $\mathcal{C} \subseteq R^n$ is a negacyclic code if $\nu(\mathcal{C}) = \mathcal{C}$, donde $\nu = \nu_{-1}$.

Constacyclic codes

Let R be a finite commutative ring with 1, $\gamma \in \mathcal{U}(R)$ and $n \geq \mathbb{N}$.

- $\mathcal{C} \subseteq R^n$ is a constacyclic code or a γ-cyclic code if $\nu_\gamma(\mathcal{C}) = \mathcal{C}$, where

$$\nu_\gamma : (a_0, a_1, \ldots, a_{n-1}) \mapsto (\gamma a_{n-1}, a_0, \ldots, a_{n-2}).$$

- $\mathcal{C} \subseteq R^n$ is a cyclic code if $\sigma(\mathcal{C}) = \mathcal{C}$, where $\sigma = \nu_1$.
- $\mathcal{C} \subseteq R^n$ is a negacyclic code if $\nu(\mathcal{C}) = \mathcal{C}$, donde $\nu = \nu_{-1}$.

γ-quasi-cyclic codes

Let m be a positive integer

- $\mathcal{C} \subseteq (R^n)^m$ ia a γ-quasi-cyclic code of index m and length mn if $\nu_\gamma^{\otimes m}(\mathcal{C}) = \mathcal{C}$, where

$$\nu_\gamma^{\otimes m} : \left(\mathbf{A}^{(0)} | \cdots | \mathbf{A}^{(m-1)}\right) \mapsto \left(\nu_\gamma\left(\mathbf{A}^{(0)}\right) | \cdots | \nu_\gamma\left(\mathbf{A}^{(m-1)}\right)\right),$$

  with $\mathbf{A}^{(i)} \in R^n$, $0 \le i \le m-1$.

- $\mathcal{C} \subseteq (R^n)^m$ is quasi-cyclic if $\sigma^{\otimes m}(\mathcal{C}) = \mathcal{C}$.
- $\mathcal{C} \subseteq (R^n)^m$ es quasi-negacyclic if $\nu^{\otimes m}(\mathcal{C}) = \mathcal{C}$.

γ-quasi-cyclic codes

Let m be a positive integer

- $\mathcal{C} \subseteq (R^n)^m$ ia a γ-quasi-cyclic code of index m and length mn if $\nu_\gamma^{\otimes m}(\mathcal{C}) = \mathcal{C}$, where

$$\nu_\gamma^{\otimes m} : \left(\mathbf{A}^{(0)} | \cdots | \mathbf{A}^{(m-1)}\right) \mapsto \left(\nu_\gamma\left(\mathbf{A}^{(0)}\right) | \cdots | \nu_\gamma\left(\mathbf{A}^{(m-1)}\right)\right),$$

  with $\mathbf{A}^{(i)} \in R^n$, $0 \leq i \leq m-1$.

- $\mathcal{C} \subseteq (R^n)^m$ is quasi-cyclic if $\sigma^{\otimes m}(\mathcal{C}) = \mathcal{C}$.

- $\mathcal{C} \subseteq (R^n)^m$ es quasi-negacyclic if $\nu^{\otimes m}(\mathcal{C}) = \mathcal{C}$.

Beginings of the linear codes over rings

The history of linear codes over rings backs to the 70's with the works of

- I. F. Blake, *Codes over certain rings* **20** (1972), Inf. and Control
- E. Spiegel, *Codes over the ring $\mathbb{Z}_m$* **35** (1977), Inf. and Control

However the community did not pay a lot of attention.

The theory of codes over rings was really initiated

A. A. Nechaev, **Kerdock code in a cyclic form**, Discrete Math. and Appl. **1** (1991)

A. R. Hammons, et. al, **The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes**, IEEE Trans. Inf. Theory **40** (1994)

The classical Gray Map

$$
\begin{array}{cccc}
\phi : & \mathbb{Z}_4 & \rightarrow & \mathbb{F}_2 \times \mathbb{F}_2 \\
 & 0 & \mapsto & (0,0) \\
 & 1 & \mapsto & (0,1) \\
 & 2 & \mapsto & (1,1) \\
 & 3 & \mapsto & (1,0)
\end{array}
$$

$$
\begin{array}{ccc}
\mathcal{K} \subset \mathbb{Z}_4^n & \xrightarrow{\;dual\;} & \mathcal{K}^{\perp} = \mathcal{P} \subset \mathbb{Z}_4^n \\
\downarrow \phi & & \downarrow \phi \\
K = \phi(\mathcal{K}) \subset \mathbb{F}_2^{2n} & & P = \phi(\mathcal{P}) \subset \mathbb{F}_2^{2n}
\end{array}
$$

Analysis of the cyclic properties

J. Wolfman, **Negacyclic and cyclic codes over** $\mathbb{Z}_4$. IEEE Trans. Inf. Theory. **45** (1999)

$$\begin{array}{ccccc} \text{Linear Cyclic code} & \mathcal{C} \subset \mathbb{Z}_4^n & \xrightarrow{\mu} & \mathcal{D} \subset \mathbb{Z}_4^n & \text{Linear Negacyclic code} \\ & \downarrow \phi & & \downarrow \phi & \\ \text{quasi-cyclic} & \phi(\mathcal{C}) \subset \mathbb{F}_2^{2n} & \xrightarrow{\widetilde{\mathcal{N}}} & \phi(\mathcal{D}) \subset \mathbb{F}_2^{2n} & \text{Cyclic Code} \end{array}$$

Some generalizations

S. Ling, T. Blackford, $\mathbb{Z}_{p^{k+1}}$**-Linear Codes**. IEEE Tans. Info. Theory. **48** (2002)

$(1-p^k)$-cyclic codes over $\mathbb{Z}_{p^{k+1}}$

H. Tapia-Recillas, G. Vega, **Some Constacyclic Codes over** $\mathbb{Z}_{2^{k+1}}$ **and Binary Quasi-Cyclic Codes**. Disc. App. Math. **128** (2003)

$(1+2^k)$-cyclic codes over $\mathbb{Z}_{2^{k+1}}$

S. Jitman, P. Udomkavanich. **The Gray Image of Cyclic Codes over Finite Chaing Rings**. Inter. J. of Contemporary Mathematics **5** (2010).

$(1-\theta^k)$-cyclic codes over a finite chaing ring R with maximal ideal $\langle\theta\rangle$, $\theta^{k+1}=0$.

All the works aforementioned analyze the gray images of γ-cyclic codes where γ is

$$\gamma = 1 - \theta^k, \qquad k \text{ is the index of nilpotence of } R$$

In terms of the chain of ideals

$$R \supsetneq \langle\theta\rangle \supsetneq \langle\theta^2\rangle \supsetneq \cdots \supsetneq \langle\theta^{k-1}\rangle \supsetneq \langle\theta^k\rangle \supsetneq \langle 0\rangle$$

$$\langle\theta^k\rangle \xrightarrow{\text{unit}} \gamma = 1 - \theta^k$$

All the works aforementioned analyze the gray images of γ-cyclic codes where γ is

$$\gamma = 1 - \theta^k, \qquad k \text{ is the index of nilpotence of } R$$

In terms of the chain of ideals

$$R \supsetneq \langle \theta \rangle \supsetneq \langle \theta^2 \rangle \supsetneq \cdots \supsetneq \langle \theta^{k-1} \rangle \supsetneq \quad \langle \theta^k \rangle \quad \supsetneq \langle 0 \rangle$$

$$\langle \theta^k \rangle \xrightarrow{\;unit\;} \gamma = 1 - \theta^k$$

Outline

Formulation of the problem...

Take $R = \mathbb{Z}_{2^{k+1}}$

$$\mathbb{Z}_{2^{k+1}} \supsetneq \langle 2 \rangle \supsetneq \langle 2^2 \rangle \supsetneq \cdots \supsetneq \langle 2^{k-1} \rangle \supsetneq \langle 2^k \rangle \supsetneq \langle 0 \rangle$$

$\langle 2^{k-1} \rangle \xrightarrow{\ units\ }$ $\delta_1 = 1 + 2^{k-1}$, $\quad \delta_2 = 1 + 2^{k-1} + 2^k$

$\langle 2^k \rangle \xrightarrow{\ unit\ }$ $1 - 2^k,\ 1$, $\quad \gamma = 1 + 2^k,\ 1$

We will analyze the Gray image of $(1 + 2^{k-1})$, $(1 + 2^{k-1} + 2^k)$-cyclic codes, and the Gray image of quasi-cyclic codes and $(1 + 2^k)$-quasi-cyclic codes.

- The 2-adic representation of $z \in \mathbb{Z}_{2^{k+1}}$ is:

$$z = r_0(z) + 2r_1(z) + 2^2 r_2(z) + \cdots + 2^k r_k(z), \quad r_i(z) \in \mathbb{F}_2.$$

- The 2-adic representation of $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ is:

$$Z = r_0(Z) + 2r_1(Z) + 2^2 r_2(Z) + \cdots + 2^k r_k(Z),$$

where $r_i(Z) = (r_i(z_0), \ldots, r_i(z_{n-1})) \in \mathbb{F}_2^n$.

The homogeneous weight

- The homogeneous weight $\omega_h : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}$ is

$$\omega_h(0) = 0 \qquad \omega_h(2^k) = 2^k \qquad \omega_h(a) = 2^{k-1}, \quad a \neq 0, 2^k$$

- Extension to $\mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}$

$$\omega_h(a_0, \dots, a_{n-1}) = \omega_h(a_0) + \cdots + \omega_h(a_{n-1})$$

- The homogeneous distance $\delta_H : \mathbb{Z}_{2^{k+1}}^n \times \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}$

$$\delta_h(A, B) = \omega_h(A - B)$$

The Gray isometry

M. Greferath, S. Schmidt, **Gray Isometries over Finite Chaing Rings and a Nonlinear Ternary** $(36, 3^{12}, 15)$ **code**. IEEE Trans. Inf. Theory. **45** (1999)

Definition of $\Phi : \mathbb{Z}_{2^{k+1}}^{n} \to \mathbb{F}_2^{2^k n}$

$$\Phi(Z) = \left(c_0^k \otimes r_0(Z)\right) \oplus \left(c_1^k \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_k^k \otimes r_k(Z)\right)$$

Theorem

$\Phi : (\mathbb{Z}_{2^{k+1}}^{n}, \delta_h) \longrightarrow (\mathbb{F}_2^{2^k n}, \delta_H)$ *is an inyective isometry.*

Outline

An step isometry

Gray isometry

$$\mathbb{Z}_{2^{k+1}}^{n} \xrightarrow{\ \Phi\ } \mathbb{F}_2^{2^k n}$$

Definition of the step isometry

$$\begin{array}{ccc} \mathbb{Z}_{2^{k+1}}^{n} & \xrightarrow{\ \varphi\ } & \mathbb{Z}_4^{2^{k-1}n} \\ & \searrow^{\Phi} & \downarrow{\scriptstyle \phi} \\ & & \mathbb{F}_2^{2^k n} \end{array}$$

Image of quasi-ciclic codes

Theorem

The following statements are equivalents:

(1) $\mathcal{C} \subseteq \mathbb{Z}_{2^{k+1}}^{mn}$ *is a quasi-cyclic code of index* m.

(2) $\varphi(\mathcal{C})$ *is a quaternary quasi-cyclic code of index* $2^{k-1}m$ *and of length* $2^{k-1}mn$.

(3) $\Phi(\mathcal{C})$ *is a binary quasi-cyclic code of index* $2^k m$ *and of length* $2^k mn$.

Image of $(1+2^k)$-cyclic codes

Theorem

The following statements are equivalent

1. $\mathcal{C} \subseteq \mathbb{Z}_{2^{k+1}}^{mn}$ *is a* λ*-quasi-cyclic code of index* m.
2. $\varphi(\mathcal{C})$ *is a quaternary quasi-negacyclic code of index* $2^{k-1}m$ *and of length* $2^{k-1}mn$.
3. $\Phi(\mathcal{C})$ *is permutation equivalent to a binary quasi-cyclic code of index* $2^{k-1}m$ *and of length* $2^k mn$.

Let $\widetilde{\pi}$ the permutation on $\mathbb{Z}_4^{2^{k-1}n}$ induced by the permutation

$$\pi = (0 \quad l)(n \quad l+n)(2n \quad l+2n)\cdots((2^{k-2}-1)n \quad l+(2^{k-2}-1)n),$$

donde $l = 2^{k-2}n$.

$$\underbrace{\left(\overbrace{\underbrace{\underline{*\qquad}}_{n}\,\Big|\,\underbrace{\underline{\circledast\qquad}}_{n}\,\Big|\cdots\Big|\,\underbrace{\underline{\diamond\qquad}}_{n}}^{l}\,\Bigg|\,\overbrace{\underbrace{\underline{*\qquad}}_{n}\,\Big|\,\underbrace{\underline{\circledast\qquad}}_{n}\,\Big|\cdots\Big|\,\underbrace{\underline{\diamond\qquad}}_{n}}^{l}\right)}_{2^{k-1}n}$$

Images of $(1+2^{k-1})$ and $(1+2^{k-1}+2^k)$-cyclic codes

Theorem

Let $k \geq 3$. The following are equivalent.

(1) $\mathcal{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ is $(1+2^{k-1})$-cyclic ($(1+2^{k-1}+2^k)$-cyclic)

(2) $\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(c) + \widehat{c} \in \varphi(\mathcal{C}), \quad \forall\, c \in \varphi(\mathcal{C})$

($\widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}\right)(c) + \widehat{c} \in \varphi(\mathcal{C})$, resp.)

where $\widehat{c} = c_{k-1}^{k-1} \otimes (2, 0, \ldots, 0)$ if and only if the coordinates of c with index in $\{n-1, 2n-1, \ldots, 2^{k-1}n-1\}$ form a string t such that

$$t + (3, 1, \ldots, 3, 1) \in \langle 2c_0^{k-1}, \ldots, 2c_3^{k-1}, 2c_{k-1}^{k-1} \rangle.$$

On the contrary $\widehat{c} = (0)_{2^{k-1}n} \in \mathbb{Z}_4^{2^{k-1}n}$.

Example $k = n = 3$, $\mathcal{D} \subseteq \mathbb{Z}_{16}^3$

$$\mathcal{D}: \quad \begin{array}{ccc} (1,6,7) & (3,1,6) & (14,3,1) \\ (5,14,3) & (15,5,14) & (6,15,5) \\ (9,6,15) & (11,9,6) & (14,11,9) \\ (13,14,11) & (7,13,14) & (6,7,13) \end{array}$$

This non linear code is $(1+2^{k-1})$-cyclic, $1+2^{k-1} = 5$.

Verification of the property on $\varphi(\mathcal{D})$

$\varphi(c)$	101 123 123 101	110 112 312 310	211 011 031 231
$\tau(\varphi(c)) + \widehat{c}$	110 112 312 310	211 011 031 231	121 301 103 323
$\varphi(c)$	121 301 103 323	312 130 110 332	312 130 110 332
$\tau(\varphi(c)) + \widehat{c}$	312 130 110 332	031 213 211 033	303 321 321 303
$\varphi(c)$	303 321 321 303	303 321 321 303	233 033 013 213
$\tau(\varphi(c)) + \widehat{c}$	303 321 321 303	233 033 013 213	323 103 301 121
$\varphi(c)$	323 103 301 121	132 310 330 112	013 231 233 011
$\tau(\varphi(c)) + \widehat{c}$	132 310 330 112	132 310 330 112	101 123 123 101

$\tau = \widetilde{\pi} \circ (\sigma \otimes \nu)^{\otimes 2}$

3-cyclic and negacyclic codes over $\mathbb{Z}_8$

The situation for 3-cyclic and negacyclic codes over $\mathbb{Z}_8$ is very similar to the previous one. However we have a plus:

Theorem

The following are equivalents.

(1) $\mathcal{C} \subseteq \mathbb{Z}_8^n$ *is a* 3*-cyclic code;*

(2) $\varphi(\mathcal{C}) \subseteq \mathbb{Z}_4^{2n}$ *is a quaternary code such that*

$$\nu(c) + \widehat{d} \in \varphi(\mathcal{C}), \qquad \forall\, c \in \varphi(\mathcal{C})$$

where $\widehat{d} = (1,1) \otimes (2,0,\ldots,0)$ *if and only if* $t \in \{(3,3),(1,1)\}$*, and* t *is the string obtained by concatening the coordinates of* c *with index in* $\{n-1, 2n-1\}$*. On the contrary,* $\widehat{d} = (0)_{2n} \in \mathbb{Z}_4^{2n}$*.*

3-cyclic and negacyclic linear codes over $\mathbb{Z}_8$

Theorem

Let $\mathcal{C} \subseteq \mathbb{Z}_8^n$ linear code. The following are equivalents

1. *$\mathcal{C}$ is a 3-cyclic and negacyclic codes;*
2. *$\varphi(\mathcal{C}) \subseteq \mathbb{Z}_4^{2n}$ is a negacyclic code;*
3. *$\Phi(\mathcal{C}) \subseteq \mathbb{F}_2^{4n}$ is a cyclic code.*

Linear codes $\mathcal{C} \subset \mathbb{Z}_8^3$ which are 3-cyclic and negacyclic

Generators	Cardinality		Generatos	Cardinality	
$\langle 2 \rangle$	2^6	✓	$\langle 2^2 b_2 \rangle$	2	✓
$\langle 2^2 \rangle$	2^3	✓	$\langle b_1, 2b_2 \rangle$	2^8	✓
$\langle b_1 \rangle$	2^6	–	$\langle b_1, 2^2 b_2 \rangle$	2^7	✓
$\langle 2b_1 \rangle$	2^4	✓	$\langle b_2, 2b_1 \rangle$	2^7	✓
$\langle 2^2 b_1 \rangle$	2^2	✓	$\langle b_2, 2^2 b_1 \rangle$	2^5	✓
$\langle b_2 \rangle$	2^3	–	$\langle 2b_1, 2^2 b_2 \rangle$	2^5	✓
$\langle 2b_2 \rangle$	2^2	✓	$\langle 2b_2, 2^2 b_1 \rangle$	2^4	✓

$x^3 - 3 = b_1 b_2, \quad b_1 = x + 5, \quad b_2 = x^2 + 3x + 1$
✓: $\mathcal{C}$ is a 3-cyclic and a negacyclic code

Thanks you in advance!