# On the Quasi-cyclicity of the Gray Image of Codes over Finite Chain Rings

H. Tapia-Recillas
Departamento de Matemáticas
Universidad Autónoma Metropolitana-I
09340 México, D.F., MEXICO
(htr@xanum.uam.mx)

**Abstract**

A characterization of $\lambda$-cyclic codes defined over a finite chain ring in terms of its Gray map image is given. This generalize the corresponding result over the ring $\mathbb{Z}_4$ of integers modulo 4, treated by J. Wolfmann.

## 1 Introduction

After the work of [3], [4] and [7] where several binary non-linear codes are described as the Gray map image of a linear code over the ring $\mathbb{Z}_4$ of integers modulo 4, the study of codes over finite rings, including $\mathbb{Z}_{p^n}$ where $p$ is a prime and $n > 1$ and integer, Galois rings, finite chain rings and Frobenius rings has increased in recent years. In a series of papers J. Wolfmann undertook the study of various aspects of codes defined over the ring $\mathbb{Z}_4$ and, recently, other topics of Coding Theory. Since the ring $\mathbb{Z}_4$ is a particular case of the ring $\mathbb{Z}_{p^n}$ and these rings can be thought of as Galois rings, several results of codes over $\mathbb{Z}_4$ have been extended to codes over this latter ring. Furthermore, Galois rings are a subclass of the finite chain ring class, and a natural question to ask is to what extent the known results about codes defined over the just mentioned rings are valid for codes defined over finite chain rings. In this talk necessary and sufficient conditions for a code over a finite chain ring to be $\lambda$-cyclic is given in terms of its Gray image. This is an immediate consequence of a relation involving the Gray map, the usual cyclic shift and a mapping defined in terms of a special unit $\lambda$ of the ring (see §2 for definitions). If $R = \mathbb{Z}_4$ the $\lambda$-cyclic codes are called negacyclic, which J. Wolfmann has studied extensively ([10]).

## 2 The result

Let $R$ be a (commutative) finite chain ring of nilpotency index $t+1$. Let $\mathbb{F} = \mathbb{F}_q$ be its residue field, where $q = p^m$, $p$ is a prime, $M = \langle \pi \rangle$ the maximal ideal, $U$ the group of units and $T$ a Teichmüller set of representatives of $R$ (for details see [6]). Examples of such rings include $\mathbb{Z}_{p^n}$, the ring of integers modulo $p^n$; Galois rings $GR(p^n, m)$ of characteristic $p^n$ and, residue polynomial rings $K[x]/\langle f(x)^k \rangle$, where $K$ is a finite field and $f(x)$ is an irreducible polynomial.

For an integer $n > 1$ let

$$\Phi : R^n \longrightarrow \mathbb{F}^{nq^t},\ \Phi(A) = C_0 \otimes r_0(A) + \cdots + C_t \otimes r_t(A) \tag{1}$$

be the Gray map as introduced in [2].

Let $\lambda = 1 - \pi^t \in U$, $\sigma : R^n \longrightarrow R^n$ the usual cyclic shift, $\eta_\lambda : R^n \longrightarrow R^n$ defined as $\eta_\lambda(A) = (a_0, a_1, ..., \lambda a_{n-1})$ and let

$$\nu_\lambda : R^n \longrightarrow R^n,\ \nu_\lambda(A) = \sigma(\eta_\lambda(A)). \tag{2}$$

For integers $m, s > 1$, an element $\underline{a} \in \mathbb{F}^{ms}$ will be written as $\underline{a} = (a^{(1)}, ..., a^{(s)})$ where each $a^{(i)},\ i = 1, 2, ..., s$ has $m$ entries. If $\sigma$ is the usual cyclic shift, then.

$$\sigma^{\otimes s} : \mathbb{F}^{ms} \longrightarrow \mathbb{F}^{ms},\ \sigma^{\otimes s}(\underline{a}) = (\sigma(a^{(1)}), ..., \sigma(a^{(s)})), \tag{3}$$

i.e., $\sigma$ is applied to each block $a^{(i)}$ of length $m$. Then we have the following:

**Proposition 1** *With the notation as above,*

$$\Phi \circ \nu_\lambda = \sigma^{\otimes p^{mt-1}} \circ \Phi. \tag{4}$$

A code $\mathcal{C} \subset R^n$ is called $\lambda$-cyclic if $\nu_\lambda(\mathcal{C}) = \mathcal{C}$. Also, a code $C \subset \mathbb{F}^{sm}$ is said to be *quasi-cyclic of index* $s$ if $\sigma^{\otimes s}(C) = C$. As a consequence of Proposition 1 we have,

**Corollary 2** *Let $\mathcal{C}$ be a $R$-code of length $n$. Then $\mathcal{C}$ is $\lambda$-cyclic if and only if its Gray image $\Phi(\mathcal{C})$ is quasi-cyclic of index $p^{mt-1}$.*

*Proof:* If $\mathcal{C}$ is a $\lambda$-cyclic $R$-code of length $n$, from relation (4) it follows that

$$\Phi(\nu_\lambda(\mathcal{C})) = \Phi(\mathcal{C}) = \sigma^{\otimes p^{mt-1}}(\Phi(\mathcal{C})),$$

showing that $\Phi(\mathcal{C})$ is quasi-cyclic of index $p^{mt-1}$. The converse also follows from relation (4) and the fact that the Gray map $\Phi$ is injective. □

**Observation.** The case $R = \mathbb{Z}_4$ where $\lambda = 1 - 2 = -1$ was considered by J. Wolfmann in [9]; in this case the $\lambda$-cyclic codes are called *negacyclic*. These codes were

also studied over finite chain rings in [1]. The case of codes over the ring $R = \mathbb{Z}_{p^2}$ where $\lambda = 1 - p$ was treated in [5]. Several authors have obtained results related to $\lambda$-cyclicity over other rings including $\mathbb{Z}_{2^k}$ ([8]).

Due to constraints on space the full proof of Proposition 1 is not presented but an idea of it is given. Recall that if $A \in R^n$, then $\Phi(A) \in \mathbb{F}^{nq^t}$, so the right hand side of relation (4) says that $\Phi(A)$ can be thought of as $l = p^{mt-1}$ blocks, $\Phi(A) = (B_1, ..., B_l)$, each $B_i$ having $np$ entries. Similarly, if $\tilde{A} = \nu_\lambda(A)$, then $\Phi(\tilde{A}) = (\tilde{B}_1, ..., \tilde{B}_l)$ where each block $\tilde{B}_i$ also has $np$ entries. Then

$$(\tilde{B}_1, ..., \tilde{B}_l) = \Phi(\tilde{A}) = \sigma^{\otimes p^{mt-1}}(\Phi(A)) = (\sigma(B_1), ..., \sigma(B_l)).$$

In order to prove Proposition 1, the blocks $B_i$ and $\tilde{B}_i$ must be identified and then it must be shown that $\sigma(B_i) = \tilde{B}_i$ for all $i = 1, ..., l$.

For this purpose the elements of the residue field $\mathbb{F}$ will be taken in a special order and representation, as described below. Let $q = p^m$ and let $\{1, \omega, \omega^2, ..., \omega^{m-1}\}$ be a basis of $\mathbb{F} = \mathbb{F}_q$ over $\mathbb{F}_p$. Since there is a bijection between $\mathbb{Z}_{p^m}$ and $\mathbb{F}_{p^m}$ given by

$$h = h_0 + h_1 p + \cdots + h_{m-1} p^{m-1} \longrightarrow \omega_h = h_0 + h_1 \omega + \cdots + h_{m-1} \omega^{m-1},$$

where $0 \leq h_i \leq p - 1$ for $i = 0, 1, ..., m - 1$, the elements of the residue field $\mathbb{F}$ will be taken in the following order:

$$\mathbb{F}_q = \{\omega_h : h = 0, 1, 2, ..., p^m - 1\}.$$

Observe that,

$$\omega_{pi} + k = \omega_{pi+k} \text{ for } 0 \leq k \leq p - 1 \text{ and } 0 \leq i \leq p^{m-1}. \tag{5}$$

Let

$$\Omega_j = (\omega_{jp}, \omega_{jp+1}, ..., \omega_{jp+(p-1)}, \text{ for } j = 0, 1, ..., p^{m-1} - 1,$$

and let $u = (\omega_0, \omega_1, ..., \omega_{q-1}) = (\Omega_0, \Omega_1, ..., \Omega_{l-1}) \in \mathbb{F}_q^q$ be the vector that lists all the elements of the residue field in the above order. Let $v = (1, 1, ..., 1) = (1_p, ..., 1_p)$ be the all one-vector of length $q^t$ where $1_p = (1, ..., 1)$ is the all-one vector of length $p$.

Let $A = (a_0, ..., a_{n-1}) \in R^n$ which can be written as $A = \rho_0(A) + \rho_1(A)\pi + \cdots + \rho_t(A)\pi^t$ where $\rho_j(A) = (\rho_j(a_0), ..., \rho_j(a_{n-1}))$ and $\rho_j(a_i)$ are those elements of the Teichmüller set $T$ of $R$ appearing in the $\pi$-adic representation of $a_i$. If $\rho(a) \in T$ and $\mu : R \longrightarrow \mathbb{F}$ is the natural residue mapping, let $r(a) = \mu(\rho(a))$, so that $r_j(A) = (r_j(a_0), ..., r_j(a_{n-1}))$.

From properties of the Kronecker product it follows that

$$\begin{aligned} C_0 \otimes r_0(A) &= (\Omega_i \otimes (v \otimes \cdots \otimes v \otimes r_0(A)))_{i=0}^{p^{m-1}-1} \\ &\vdots \\ C_t \otimes r_t(A) &= (1_p \otimes (v \otimes \cdots \otimes v \otimes r_0(A)))_{i=0}^{p^{m-1}-1} \end{aligned}$$

and

$$\begin{aligned} \Omega_i \otimes r_0(A) &= (\omega_{pi} r_0(A), ..., \omega_{pi+(p-1)} r_0(A)) \\ &\vdots \\ 1_p \otimes r_t(A) &= (r_t(A), ..., r_t(A)). \end{aligned}$$

Observe that each term $\Omega_i \otimes r_0(A)$,...,$1_p \otimes r_t(A)$ has $np$ entries. From the definition of the Gray map it can be seen that the block $B_i$ of $\Phi(A)$ for $i = 1, 2, ..., p^{mt-1}$ is:

$$B_i = \Omega_i \otimes r_0(A) + \cdots + 1_p \otimes r_t(A). \tag{6}$$

If $A' = \eta_\lambda(A)$ then $r_j(A') = r_j(A)$ for $0 \leq j \leq t-1$ and $r_t(A') = r_t(A) + \theta$ where $\theta = (0, ..., 0, (p-1)r_0(a_{n-1}))$. Since $\tilde{A} = \nu_\lambda(A) = \sigma(A')$ the corresponding block of $\Phi(A')$ is:

$$\tilde{B}_i = \Omega_i \otimes r_0(\sigma(A')) + \cdots + 1_p \otimes r_t(\sigma(A')). \tag{7}$$

Observing that $\sigma$ is an automorphism and it commutes with the function $r_i$ (in the appropriate context), then:

$$\tilde{B}_i = (\sigma(r_t(A') + \cdots + \omega_{pi} r_0(A')), ..., \sigma(r_t(A') + \cdots + \omega_{pi+(p-1)} r_0(A'))).$$

Since

$$r_t(A) + \cdots + \omega_{pi+j} r_0(A) = (r_t(a_0) + \cdots + \omega_{pi+j} r_0(a_0), ..., r_t(a_{n-1}) + \cdots + \omega_{pi+j} r_0(a_{n-1}))$$

for $0 \leq j \leq p-1$ then:

$$\tilde{B}_i = (\sigma(r_t(A) + \cdots + \omega_{pi} r_0(A) + \theta), \ldots, \sigma(r_t(A) + \cdots + \omega_{pi+(p-1)} r_0(A) + \theta)).$$

The relations $\omega_{pi} + k = \omega_{pi+k}$ for $0 \leq k \leq p-1$ (cf. (5)) induce a permutation on the $np$ entries of $\tilde{B}_i$ in such a way that the $(jp)$-th entry goes to the $[(j+1)p]$-th entry for $1 \leq j \leq p-1$. In other words, we have a cyclic shift on the entries $(p, 2p, ..., (p-1)p)$ of $\tilde{B}_i$ leaving the other entries fixed. The composition of this permutation on the entries of $\tilde{B}_i$ together with the cyclic shift on each $\sigma(r_t(A) + \cdots + \omega_{pi+k} r_0(A) + \theta)$ for $0 \leq k \leq p-1$ determines the cyclic shift on the $np$ entries of $B_i$, showing that

$$\tilde{B}_i = \sigma(B_i)$$

for $1 \leq i \leq p^{mt} - 1$ and hence proving Proposition 1.

# References


[1] H.Q. Dinh and S. R. López-Permouth, "Cyclic and Negacyclic Codes Over Finite Chain Rings". *IEEE Trans. Inform. Theory*, vol.50, No.8, pp.1728-1744, 2004.

[2] M. Greferath and S.E. Schmidt , "Gray isometries for Finite Chain rings and a Nonlinear Ternary $(36, 3^{12}, 15)$ Code", IEEE *Trans. Inform. Theory*, vol. 45, pp.2522-2524, Nov., 1999.

[3] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $Z_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp.301-319, 1994.

[4] W. Heise, T. Honold, and A. A. Nechaev, "Weighted modules and representations of codes," in *Proc. ACCT 6* (Pskov, Russia, 1998), pp.123-129.

[5] S. Ling and T. Blackford. "$\mathbb{Z}_{p^{k+1}}$-linear Codes. *IEEE Trans. Inform. Theory*, vol. 48, No.9, pp.2592-2605, 2002.

[6] B.R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics. Marcel Deckker, vol. 28, New York, 1974.

[7] A.A. Nechaev, "The Kerdock code in a cyclic form". Math. Appl. vol.1, (1991), pp.365-384 (English translation of Diskret. Mat., 1989).

[8] H. Tapia-Recillas and G. Vega, "On the $\mathbb{Z}_{2^k}$-Linear and Quaternary Codes". *SIAM Journal on Discrete Mathematics*, vol.17, No.1, pp.103-113, 2003.

[9] J. Wolfmann, "Negacyclic and Cyclic Codes over $\mathbb{Z}_4$". *IEEE, Trans. Inform. Theory,* vol. 45, pp.2527-2532, 1999.

[10] J. Wolfmann, "Binary images of cyclic codes over $\mathbb{Z}_4$". *IEEE, Trans. Inform. Theory,* vol. 47, pp.1773-1779, 2001.