Advances in Mathematics of Communications
Volume 14, No. 2, 2020, 233–245
doi:10.3934/amc.2020017

CYCLIC CODES OF LENGTH $2p^n$ OVER FINITE CHAIN RINGS

Anderson Silva
Departamento de Matemática
Universidade Federal de Viçosa
Viçosa, 36570-000, Brazil

C. Polcino Milies
Instituto de Matemática e Estatística
Universidade de São Paulo
São Paulo, 05311-970, Brazil

(Communicated by Vitaly Skachek)

Abstract. We use group algebra methods to study cyclic codes over finite chain rings and under some restrictive hypotheses, described in section 2, for codes of length $2p^n$, p a prime, we are able to compute the minimum weights of all possible cyclic codes of that length.

1. Introduction

Let R be a finite commutative ring with unity. A linear code of length n over R is a submodule C of R^n. A linear code C is cyclic if, for every codeword $x = (x_0, \ldots, x_{n-1}) \in C$, its cyclic shift $(x_{n-1}, x_0, \ldots, x_{n-2})$ is also in C and many of the important codes in use are of this type. It is well-known that cyclic codes of length n over a ring R can be identified with the ideals of the group ring RA, where A is the cyclcic group of order n.

The Hamming weight of an element in R^n is the number of its non-zero coordinates. We denote by $w(C)$ the minimum weight of the code, which is the smallest Hamming weight of non-zero elements in the code.

A commutative ring R is a chain ring, or a uniserial ring, if the set of all ideals of R is a chain under set-theoretic inclusion. A ring R is local if it has a unique maximal ideal which is actually two-sided. We recall the following.

Proposition 1.1. ([3, Proposition 2.1]) *For a commutative ring R the following conditions are equivalent:*

(i) R is a local ring and the maximal ideal M of R is principal.
(ii) R is a local principal ideal ring.
(iii) R is a chain ring.

Notice that, since M is maximal, then $\overline{R} = R/M$ is a field and M is the set of non units of R and its Jacobson radical; hence, it is nilpotent. Let a be a (fixed) generator of the maximal ideal M. Then a is a nilpotent element and we denote its nilpotency index by t.

2010 *Mathematics Subject Classification:* Primary: 94B15, 06F25, 20C05; Secondary: 94A05, 94B05.

Key words and phrases: Cyclic codes, chain rings, weights.

This work was partially supported by CNPq., Proc. 300243/79-0(RN) and FAPESP, Proc 2015/09162-9.

Proposition 1.2. ([3, Proposition 2.2]) *Let R be a finite chain ring, with maximal ideal $M = \langle a \rangle$. Then:*

(a) For some prime q and positive integers k and l with $k \geq l$, we have

$$|R| = q^k, \quad |\overline{R}| = q^l$$

and the characteristic of R and $\overline{R}$ are powers of q.

(b)

$$|\langle a^i \rangle| = |\overline{R}|^{t-i}, \quad 0 \leq i \leq t.$$

In particular, $|R| = |\overline{R}|^t$, so $k = lt$.

Codes over chain rings have been the object of intensive recent research; see, for example, [2], [3], [4], [7], [8] and [9].

Minimum weights and dimensions are very important parameters of codes, as they determine the error-correcting capacity and the amount of information the code is capable of transmitting, respectively. In what follows, we compute the minimum Hamming weights and dimensions of an extensive family of cyclic codes of length $2p^n$, extending results from [1]. It should be noted that, to this end, we are using the Hamming weight while others weights are possible for codes over rings, such as the homogeneous weight (see [11]). Under some restrictive hypothesis described below, the family we consider is the family of all minimal codes.

2. Minimum weights

In what follows, R will denote a finite commutative chain ring with unity of order $|R| = q^k$, where q denotes a prime rational integer, and maximal ideal $M = \langle a \rangle$. Let t denote the nilpotency index of a. Set $\overline{R} = R/M$. Then $|\overline{R}| = q^l$ with $\ell = k/t$.

Also, we shall denote by A a cyclic group of order $2p^n$, such that $gcd(q, p) = 1$, and write $A = B \times G$ where G is the p-Sylow subgroup of A and $B = \{1, d\}$ is its 2-Sylow subgroup.

We denote by φ Euler's φ-function; i.e., for a positive integer m, $\varphi(m)$ denotes the number of positive integers smaller that m that are relatively prime to m. We denote by $o(q)$ the multiplicative order of q in the group of units $U(\mathbb{Z}_{2p^n})$. Notice that $o(q) = \varphi(p^n)$ if and only if q is a generator in $U(\mathbb{Z}_{2p^n})$.

Given a field K and a subgroup H of a group G such that $gcd(char(K), |H|) = 1$, the element

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h,$$

is an idempotent of KG known as the idempotent *determined* by H.

Ferraz and Polcino Milies proved the following.

Theorem 2.1 ([5], Teorema 3.2)**.** *Let K be a field with q elements and A a cyclic group of order $2p^n$ as above, where p an odd prime, such that $o(q) = \varphi(p^n)$ in $U(\mathbb{Z}_{2p^n})$.*

If e_i, $0 \leq i \leq s$, denote the primitive idempotents of KG, then, the primitive idempotents of KA are $\left(\frac{1+d}{2}\right)e_i$ and $\left(\frac{1-d}{2}\right)e_i$, $0 \leq i \leq s$.

Since G is a cyclic group of order p^n its chain of subgroups is:

$$G = H_0 \supset G_1 \supset \cdots \supset G_n = \{0\},$$

where G_i is the unique subgroup of G of order p^{n-i} and the primitive idempotents of KG are

$$e_0 = \widehat{G} \quad \text{and } e_i = \widehat{G}_i - \widehat{G}_{i-1},\ 1 \le i \le n.$$

In what follows, we shall always assume that $o(q) = \varphi(p^n)$ in $U(Z_{2p^n})$, just to be able to consider these codes as minimal. In the general case, they are not necessarily minimal but are still a significant family of codes.

The proof of the following result is straightforward.

Proposition 2.2. *Let R be a chain ring and M the maximal ideal of R. then*

$$\frac{RG}{MG} \cong \left(\frac{R}{M}\right) G.$$

As $gcd(q, n) = 1$, by Maschke's Theorem [10, Corollary 3.4.8], we have that $[R/M]G$ is semisimple and there exist orthogonal primitive idempotents $\overline{e}_0, \ldots, \overline{e}_m$ such that $\overline{R}G = \overline{R}G\overline{e}_0 \oplus \ldots \oplus \overline{R}G\overline{e}_m$. By [6, Proposition 7.14], there exists a unique family of orthogonal primitive idempotents $\{e_0, \ldots, e_m\}$ on RG such that $RG = RGe_0 \oplus \ldots \oplus RGe_m$.

The minimum weight of a code of the form $KA\left[\left(\frac{1\pm d}{2}\right)e_i\right]$ was computed in [5]. A very similar result holds over chain rings, but requires new arguments.

Theorem 2.3. *Let $C = RA(a^k(\frac{1\pm d}{2})e_i)$ be a code, with $0 \le k < t$. Then*

$$w(C) = \begin{cases} 4|G_i|, \text{if } 0 < i \le n \\ |A|, \text{if } i = 0 \end{cases}$$

Proof. We consider first the case of an index i with $0 < i \le n$. Let $T = \{\tau_1, \ldots, \tau_n\}$ be a transversal of G_i in G; i.e., a full set of representatives of cosets of G_i in G. As

$$a^k\Big(\frac{1 \pm d}{2}\Big)e_i = \Big(a^k\Big(\frac{1 \pm d}{2}\Big)e_i\Big) \cdot \widehat{G}_i,$$

we have that $C \subset RA\Big(a^k\Big(\frac{1\pm d}{2}\Big)\widehat{G}_i\Big)$. Thus, an element $\alpha \ne 0 \in C$, is of the form

$$\alpha = (x_1\tau_1 + \ldots + x_n\tau_n)\Big(a^k\Big(\frac{1 \pm d}{2}\Big)\widehat{G}_i\Big).$$

If only one coefficient x_ia^k is different from 0, then $\alpha = (x_i\tau_i)\Big(a^k\Big(\frac{1\pm d}{2}\Big)\widehat{G}_i\Big)$ and there exist $\beta_i \in RA$ such that

$$\alpha = (x_i\tau_i)\Big(a^k\Big(\frac{1 \pm d}{2}\Big)\widehat{G}_i\Big) = \beta_i \cdot \Big(a^k\Big(\frac{1 \pm d}{2}\Big)e_i\Big).$$

As $\widehat{G}_{i-1} \cdot G_i = \widehat{G}_{i-1}$ and $e_i \cdot G_{i-1} = 0$, multipying the equality above by $\widehat{G}_{i-1}$ we get $(x_i\tau_i)\Big(a^k\Big(\frac{1\pm d}{2}\Big)\widehat{G}_{i-1}\Big) = 0$. Since $(x_ia^k\tau_i) \cdot \widehat{G}_{i-1}$ and $(x_ia^k\tau_i) \cdot d\widehat{G}_{i-1}$ have disjoint supports we must have $(x_ia^k\tau_i) \cdot \widehat{G}_{i-1} = 0$, and thus $x_ia^k = 0$, a contradiction. Consequently, $w(C) \ge 4|G_j|$.

Choose an element $g_0 \in G_{i-1} \setminus G_i$. Notice that $(1-g_0)\cdot \widehat{G}_{i-1} = 0$. Take

$$\begin{aligned}\alpha &= (1-g_0)a^k\Big(\frac{1\pm d}{2}\Big)\widehat{G}_i \\ &= (1-g_0)a^k\Big(\frac{1\pm d}{2}\Big)(\widehat{G}_i - G_{i-1}) \\ &= (1-g_0)a^k\Big(\frac{1\pm d}{2}\Big)e_i,\end{aligned}$$

so $\alpha = (1-g_0)a^k\Big(\frac{1\pm d}{2}\Big)\widehat{G}_i \in C$. As $w(\alpha) = 4|G_i|$, it follows that $w(C) = 4|G_i|$.

Finally, consider a code of the form $C = RA\left[a^k\Big(\frac{1\pm d}{2}e_0\Big)\right]$ and take $0 \neq \alpha \in C$. We can write α in the form

$$\alpha = \sum_{g\in G} x_g g a^k \left(\frac{1\pm d}{2}\right)e_0 + \sum_{g\in G} y_g dg a^k\left(\frac{1\pm d}{2}\right)e_0,$$

with $x_g, y_g \in R$.

As $g\cdot e_0 = e_0 = \widehat{G}$ e $d\cdot(\frac{1\pm d}{2}) = \pm(\frac{1\pm d}{2})$, we have that

$$\alpha = \Big(\sum a^k r_g\Big)\left(\frac{1\pm d}{2}\right)e_0 \quad \text{with} \quad r_g \in R.$$

As $\big(\sum a^k r_g\big) \in R$ and $w(e_0) = |A|$, it follows that $w(C) = 2|G| = |A|$. □

3. Non minimal codes

A non minimal code is the direct sum of codes of the form $RA\left(a^{k_i}\left(\frac{1\pm d}{2}\right)e_i\right)$. We shall consider first the case when all the idempotents involved are of the form $a^{k_i}(\frac{1+d}{2})e_i$. The case when e_0 is not involved is simpler.

To simplify notations, we shall denote an ideal of the form $RA\left(a^{k_i}\left(\frac{1\pm d}{2}\right)e_i\right)$ as $\langle a^{k_i}\frac{1\pm d}{2}e_i\rangle$.

Theorem 3.1. *Let C be a code of the form*

$$C = \left\langle a^{k_{i_1}}\left(\frac{1+d}{2}\right)e_{i_1}\right\rangle \oplus \ldots \oplus \left\langle a^{k_{i_l}}\left(\frac{1+d}{2}\right)e_{i_\ell}\right\rangle,$$

where $0 \le k_{i_j} < t$, $1 \le j \le \ell$, and $0 < i_1 < i_2 < \ldots < i_\ell$. Then

$$w(C) = 4|G_{i_\ell}|.$$

Proof. First, note that $w(C) \le w(\langle a^{k_{i_\ell}}(\frac{1+d}{2})e_{i_l}\rangle) = 4|G_{i_\ell}|$.

As $G_{i_\ell} \subset G_{i_j}$, for $i_j < i_\ell$, we have $\widehat{G}_{i_\ell}.e_{i_j} = e_{i_j}, 1 \le j \le \ell$. Thus $\alpha = \alpha\widehat{G_{i_\ell}}$ so $C \subset \langle a^k(\frac{1+d}{2})\widehat{G}_{i_\ell}\rangle$, where $k = min\{k_{i_1}, \ldots, k_{i_\ell}\}$.

Let $T = \{\tau_1, \ldots, \tau_n\}$ be a transversal of G_{i_ℓ} in G and set $\alpha \in C$, $\alpha \neq 0$. We can write

$$\alpha = (x_1\tau_1 + \ldots + x_n\tau_n)a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i_\ell}, \text{ with } x_i \in R.$$

If there exist just one coefficient x such that $xa^k \neq 0$ we write α in the form

$$\alpha = x\tau a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i_\ell} \quad \text{with} \quad \tau \in \Gamma.$$

On the other hand, as $C = \langle a^{k_{i_1}}(\frac{1+d}{2})e_{i_1}\rangle \oplus \ldots \oplus \langle a^{k_{i_\ell}}(\frac{1+d}{2})e_{i_\ell}\rangle$, there exist $\beta_1, \ldots, \beta_\ell \in RA$ such that

$$\alpha = \beta_1 a^{k_{i_1}} \left(\frac{1+d}{2}\right) e_{i_1} + \ldots + \beta_l a^{k_{i_\ell}} \left(\frac{1+d}{2}\right) e_{i_\ell} = x\tau a^k \left(\frac{1+d}{2}\right) \widehat{G}_{i_\ell}.$$

As $G_{i_1-1} \supset G_{i_j}$, for $1 \leq j \leq \ell$, we have $\widehat{G}_{i_1-1}.e_{i_j} = 0$.

Thus, multiplying the equation above by $\widehat{G}_{i_1-1}$ we get

$$x\tau(a^k \left(\frac{1+d}{2}\right) \widehat{G}_{i_1-1}) = 0.$$

As $x\tau(a^k\widehat{G}_{i_1-1})$ and $x\tau(a^k d\widehat{G}_{i_1-1})$ have disjoint support, we have $xa^k = 0$, a contradiction. Therefore $w(\alpha) \geq 4|G_{i_\ell}|$.

Consequently $w(C) = 4|G_{i_\ell}|$. □

When the code involves e_0 there are two different cases. We consider first the case when all the idempotents from e_0 to idempotents e_ℓ are involved.

Theorem 3.2. *Let C be a code of the form*

$$C = \left\langle a^{k_0} \left(\frac{1+d}{2}\right) e_0 \right\rangle \oplus \left\langle a^{k_1} \left(\frac{1+d}{2}\right) e_1 \right\rangle \oplus \ldots \oplus \left\langle a^{k_\ell} \left(\frac{1+d}{2}\right) e_\ell \right\rangle,$$

where $0 \leq k_j < t, 0 \leq j \leq \ell$.

Then $w(C) = 2|G_\ell|$.

Proof. As $a^k \left(\frac{1+d}{2}\right) e_i = a^{k_i} \left(\frac{1+d}{2}\right) e_i \widehat{G}_\ell$, for $0 \leq i \leq \ell$, we have, as before, $C \subset \langle a^{k_i} \left(\frac{1+d}{2}\right) \widehat{G}_\ell\rangle$.

Set $k = max\{k_0, \ldots, k_\ell\}$. Note that

$$\begin{aligned} a^k \left(\frac{1+d}{2}\right) \widehat{G}_\ell &= a^k \left(\frac{1+d}{2}\right) \left[\widehat{G}_\ell - \widehat{G}_{\ell-1} + \widehat{G}_{\ell-1} - \cdots + \widehat{G}_1 - \widehat{G}_0 + \widehat{G}_0\right] \\ &= a^k \left(\frac{1+d}{2}\right) \left[e_\ell + e_{\ell-1} + \ldots + e_2 + e_1 + e_0\right]. \end{aligned}$$

Since $\langle a^k(\frac{1+d}{2})e_i\rangle \subset \langle a^{k_i}(\frac{1+d}{2})e_i\rangle \subset C$ for $0 \leq i \leq \ell$, we have

$$\langle a^k(\frac{1+d}{2})\widehat{G}_\ell\rangle \subset C.$$

Then, $C = \langle a^k(\frac{1+d}{2})\widehat{G}_\ell\rangle$. As $a^k\widehat{G}_\ell$ and $a^k d\widehat{G}_\ell$ have disjoint supports, we have that:

$$w(C) = w\left(\langle a^k(\frac{1+d}{2})\widehat{G}_\ell\rangle\right) = 2|G_\ell|.$$

□

Now we consider codes involving e_0 but different from the above.

Theorem 3.3. *Let C be a code of the form*

$$C = \left\langle a^{k_0} \left(\frac{1+d}{2}\right) e_0 \right\rangle \oplus \left\langle a^{k_{i_1}} \left(\frac{1+d}{2}\right) e_{i_1} \right\rangle \oplus \ldots \oplus \left\langle a^{k_\ell} \left(\frac{1+d}{2}\right) e_{i_\ell} \right\rangle,$$

where $k_0 < t$, and $\{i_1, \ldots, i_\ell\} \subsetneq \{1, \ldots, i_\ell\}$. Then, $w(C) = 4|G_{i_\ell}|$.

Proof. First, note that $w(C) \leq w(a^{k_{i_\ell}}(\frac{1+d}{2})e_{i_l}) = 4|G_{i_\ell}|$.

As $G_{i_\ell} \subset G_j$, for $j < i_\ell$, we have $\widehat{G}_{i_\ell}.e_j = e_j$. Thus, as above, $C \subset \langle a^k(\frac{1+d}{2})\widehat{G}_{i_\ell}\rangle$, where $k = max\{k_{i_1}, \ldots, k_{i_\ell}\}$.

Let $T = \{\tau_1, \ldots, \tau_n\}$ be a transversal of G_{i_ℓ} in G and take $\alpha \in C$, $\alpha \neq 0$. We can write $\alpha = (x_1\tau_1 + \ldots + x_n\tau_n)(a^k(\frac{1+d}{2})\widehat{G}_{i_\ell})$, where $x_i \in R$.

Assume now, by way of contradiction, that there exists only one coefficiente x of α such that $xa^k \neq 0$. Then $\alpha = x\tau a^k(\frac{1+d}{2})\widehat{G}_{i_\ell}$, with $\tau \in T$. As

$$C = \left\langle a^{k_0}\left(\frac{1+d}{2}\right)e_0\right\rangle \oplus \left\langle a^{k_{i_1}}\left(\frac{1+d}{2}\right)e_{i_1}\right\rangle \oplus \cdots \oplus \left\langle a^{k_{i_\ell}}\left(\frac{1+d}{2}\right)e_{i_\ell}\right\rangle,$$

there exist $\beta_0, \beta_1, \ldots, \beta_\ell \in RA$, such that

$$\begin{aligned}\alpha &= \beta_0 a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \beta_1 a^{k_{i_1}}\left(\frac{1+d}{2}\right)e_{i_1} + \ldots + \beta_l a^{k_{i_\ell}}\left(\frac{1+d}{2}\right)e_{i_\ell} \\ &= x\tau a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i_\ell}.\end{aligned}$$

As $\{i_1, \ldots, i_\ell\} \subsetneqq \{1, \ldots, i_\ell\}$, there exists an index $i_r \in \{1, \ldots, i_\ell\}$ such that the idempotent $(\frac{1+d}{2})e_{i_r}$ is not in the initial sum. Let i_r be the smallest such index.

Multiplying both sides of the equality above by $\widehat{G}_{i_r}$, we get

$$\begin{aligned}\alpha\widehat{G}_{i_r} &= x\tau a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i_r} \\ &= \beta_0 a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \beta_1 a^{k_{i_1}}\left(\frac{1+d}{2}\right)e_{i_1} + \cdots \\ &\quad \cdots + \beta_l a^{k_{i_r-1}}\left(\frac{1+d}{2}\right)e_{i_r-1}.\end{aligned}$$

Notice that the ideal

$$J = \left\langle a^{k_0}\left(\frac{1+d}{2}\right)e_0\right\rangle \oplus \left\langle a^{k_1}\left(\frac{1+d}{2}\right)e_{i_1}\right\rangle \oplus \cdots \oplus \left\langle a^{k_{i_{r-1}}}\left(\frac{1+d}{2}\right)e_{i_r-1}\right\rangle$$

is as in Theorem 3.3 so its minimum weight is $w(J) = 2|G_{i_r-1}| = 2p^{n-i_r+1}$ and $\alpha\widehat{G}_{i_r} \in J$.

As $w(\alpha\widehat{G}_{i_r}) = w\left(x\tau a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i_\ell}\right) = 2|G_{i_r}| = 2p^{n-i_r} < w(J)$ we get a contradiction.

Thus there exist at least two coefficients x_r, x_s such that $x_r a^k$ and $x_s a^k$ are non zero, so $w(C) \geq 4|G_{i_\ell}|$ and thus $w(C) = 4|G_{i_\ell}|$. □

The case when all the idempotents involved are of the form $a^{k_i}(\frac{1-d}{2})e_i$ is not different.

Now, we will compute the minimum weight of codes that involve ideals of both forms. As before, we study first codes not involving e_0.

Theorem 3.4. *Let C be a code of the form*

$$C = \left\langle a^{k_{i_1}}\left(\frac{1\pm d}{2}\right)e_{i_1}\right\rangle \oplus \cdots \oplus \left\langle a^{k_{i_\ell}}\left(\frac{1\pm d}{2}\right)e_{i_\ell}\right\rangle,$$

where $0 \leq k_{i_j} < t$, $1 \leq j \leq \ell$, $0 < i_1 \leq i_2 \leq \ldots \leq i_{\ell-1} < i_\ell$, and assume that at least one idempotent of the form $(\frac{1+d}{2})e_i$ and one idempotent of the form $(\frac{1-d}{2})e_j$ are involved in C.

Then $w(C) = 4|G_{i_\ell}|$.

Proof. Note that $w(C) \leq w(\langle a^{k_{i_l}}(\frac{1\pm d}{2})e_{i_\ell}\rangle) = 4|G_{i_\ell}|$.

Also, as in the previous results, we have that $C \subset \langle a^k \widehat{G}_{i_\ell}\rangle$, where $k = min\{k_{i_1}, \ldots, k_{i_\ell}\}$. Let $T = \{\tau_1, \ldots, \tau_n\}$ be a transversal of G_{i_ℓ} in G and set $\alpha \in C$, $\alpha \neq 0$. Then we can write

$$\alpha = (x_1\tau_1 + \ldots + x_n\tau_n + x_1^{'}d\tau_1 + \ldots + x_n^{'}d\tau_n)a^k\widehat{G}_{i_l\ell},$$

with $x_j, x_j^{'} \in R$.

Assume first, by way of contradiction, that there exists only one coefficient x in the expression of α such that $xa^k \neq 0$, so that $\alpha = xa^k d^\delta \tau \widehat{G}_{i_\ell}$, where δ is equal to either 0 or 1, and $\tau \in T$.

As $\alpha \in C$, there exist $\beta_{i_1}, \ldots, \beta_{i_\ell} \in RA$ such that

$$\alpha = \beta_{i_1}a^{k_{i_1}}\left(\frac{1\pm d}{2}\right)e_{i_1} + \ldots + \beta_{i_\ell}a^{k_{i_\ell}}\left(\frac{1\pm d}{2}\right)e_{i_\ell},$$

and we can write

$$\alpha = xa^k d^\delta \tau \widehat{G}_{i_\ell} = \beta_{i_1}a^{k_{i_1}}\left(\frac{1\pm d}{2}\right)e_{i_1} + \ldots + \beta_{i_\ell}a^{k_{i_l\ell}}\left(\frac{1\pm d}{2}\right)e_{i_\ell}.$$

Multiplying the equality above by $\widehat{G}_{i_1-1}$, we get

$$xa^k d^\delta \tau \widehat{G}_{i_1-1} = 0.$$

Thus, $xa^k = 0$, a contradiction.

Assume now that there exist precisely two coefficients x_1, x_2 in the expression of α such that $x_1a^k \neq 0$ and $x_2a^k \neq 0$. Then,

$$\begin{aligned}\alpha &= (x_1d^\delta\tau + x_2d^{\delta'}\tau^{'})a^k\widehat{G}_{i_\ell} \\ &= \beta_{i_1}a^{k_{i_1}}\left(\frac{1\pm d}{2}\right)e_{i_1} + \ldots + \beta_{i-\ell}a^{k_{i_\ell}}\left(\frac{1\pm d}{2}\right)e_{i_\ell},\end{aligned}$$

where both of δ and δ' are equal to either 0 or 1, and $\tau, \tau' \in T$. Suppose that the last idempotent in this expression is $(\frac{1+d}{2})e_{i_\ell}$, the other possibility being similar.

As $(\frac{1+d}{2})(\frac{1-d}{2}) = 0$, multiplying by $(\frac{1-d}{2})$ we get

$$\begin{aligned}\alpha\left(\frac{1-d}{2}\right) &= (x_1d^\delta\tau + x_2d^{\delta'}\tau^{'})a^k\left(\frac{1-d}{2}\right)\widehat{G}_{i_\ell} \\ &= \beta_{j_1}a^{k_{j_1}}\left(\frac{1-d}{2}\right)e_{j_1} + \ldots + \beta_{j_s}a^{k_{j_s}}\left(\frac{1-d}{2}\right)e_{j_s},\end{aligned}$$

where $j_s < i_\ell$.

This shows that $\alpha(\frac{1-d}{2})$ belongs to code

$$C^{'} = \left\langle a^{k_{j_1}}\left(\frac{1-d}{2}\right)e_{j_1}\right\rangle \oplus \cdots \oplus \left\langle a^{k_{j_s}}\left(\frac{1-d}{2}\right)e_{j_s}\right\rangle,$$

which is as in the previous theorem.

But $w(\alpha(\frac{1-d}{2})) = w((x_1d^\delta\tau + x_2d^{\delta'}\tau^{'})a^k\left(\frac{1-d}{2}\right)\widehat{G}_{i_l\ell}) = 4|G_{i_\ell}|$ and $w(C^{'}) = 4|G_{j_s}|$. As $|G_{i_\ell}| < |G_{j_s}|$, a contradiction.

A very similar argument shows that if there are precisely three coefficients x_1, x_2, x_3 such that x_1a^k, x_2a^k and x_1a^k are non zero, we get again a contradiction.

Therefore, $w(C) \geq 4|G_{i_\ell}|$ and thus $w(C) = 4|G_{i_\ell}|$. □

To complete the study of ideals not involving e_0 we need to consider first a particular case.

Lemma 3.5. *Set*

$$C = \left\langle a^{k_1}\left(\frac{1+d}{2}\right)e_i\right\rangle \oplus \left\langle a^{k_2}\left(\frac{1-d}{2}\right)e_i\right\rangle,$$

where $i \neq 0$, and $k_1, k_2 \neq t$.

Then $w(C) = 2|G_i|$.

Proof. Let $k = min\{k_1, k_2\}$. Then

$$\begin{aligned} C &\subset \left\langle a^{k}\left(\frac{1+d}{2}\right)e_i\right\rangle \oplus \left\langle a^{k}\left(\frac{1-d}{2}\right)e_i\right\rangle \\ &\subset \left\langle a^{k}\left(\frac{1+d}{2}\right)\widehat{G}_i\right\rangle + \left\langle a^{k}\left(\frac{1-d}{2}\right)\widehat{G}_i\right\rangle \\ &\subset \left\langle a^{k}\widehat{G}_i\right\rangle. \end{aligned}$$

Let $T = \{\tau_1, \ldots, \tau_n\}$ be a transversal of G_i in G and $\alpha \in C$, $\alpha \neq 0$. Then $\alpha = (x_1\tau_1 + \ldots + x_n\tau_n + x_1^{'}d\tau_1 + \ldots + x_n^{'}d\tau_n)a^k\widehat{G}_i$, with x_j e $x_j^{'} \in R$.

Suppose that there exists only one coefficient x of α such that $xa^k \neq 0$. Then, there exist β_1 and $\beta_2 \in RA$ such that

$$\alpha = xd^{\delta}\tau a^k\widehat{G}_i = \beta_1 a^{k_i}\left(\frac{1+d}{2}\right)e_i + \beta_2 a^{k_j}\left(\frac{1-d}{2}\right)e_i,$$

where $\delta = 0$ or $\delta = 1$ and $\tau \in T$.

Multiplying the equality above by $\widehat{G}_{i-1}$, we get $xa^kd^{\delta}\tau\widehat{G}_{i-1} = 0$. Thus, $xa^k = 0$, a contradiction. Therefore $w(C) \geq 2|G_i|$.

Now, take $g_0 \in G_{i-1} \setminus G_i$ and consider $\alpha = (1-g_0)a^k\widehat{G}_i$, where $k = max\{k_i, k_j\}$ so $w(\alpha) = 2|G_i|$. Also,

$$\alpha = (1-g_0)a^k\widehat{G}_i = (1-g_0)a^k(\widehat{G}_i - \widehat{G}_{i-1} + \widehat{G}_{i-1}) = (1-g_0)a^k(e_i + \widehat{G}_{i-1}).$$

As $(1-g_0)\widehat{G}_{i-1} = 0$, because $g_0 \in G_{i-1}$, then

$$\alpha = (1-g_0)a^ke_i = (1-g_0)a^k\left(\frac{1+d}{2}\right)e_i + (1-g_0)a^k\left(\frac{1-d}{2}\right)e_i \in C.$$

Thus $w(C) \leq w(\alpha) = 2|G_i|$. Then $w(C) = 2|G_i|$. □

We are now ready to complete this case.

Theorem 3.6. *Let C be a code of the form*

$$C = \left\langle a^{k_{i_1}}\left(\frac{1\pm d}{2}\right)e_{i_1}\right\rangle \oplus \cdots \oplus \left\langle a^{k_{i_\ell}}\left(\frac{1+d}{2}\right)e_{i_\ell}\right\rangle \oplus \left\langle a^{h_{i_\ell}}\left(\frac{1-d}{2}\right)e_{i_\ell}\right\rangle,$$

where $0 \leq k_{i_j}, h_{i_j} < t$, $1 \leq j \leq \ell$, $0 < i_1 \leq i_2 \leq \ldots \leq i_{\ell-1} < i_l\ell$.

Then $w(C) = 2|G_{i_\ell}|$.

Proof. By the previous lemma, we have

$$w(C) \leq w\left(\left\langle a^{k_{i_\ell}}\left(\frac{1+d}{2}\right)e_{i_\ell}\right\rangle \oplus \left\langle a^{h_{i_\ell}}\left(\frac{1-d}{2}\right)e_{i_\ell}\right\rangle\right) = 2|G_{i_\ell}|.$$

Let $T = \{\tau_1, \ldots, \tau_n\}$ be a transversal of G_{i_ℓ} in G and $\alpha \in C$, $\alpha \neq 0$.

We can write

$$\alpha = (x_1\tau_1 + \ldots + x_n\tau_n + x_1^{'}d\tau_1 + \ldots + x_n^{'}d\tau_n)a^k\widehat{G}_{i_\ell}.$$

Suppose, again, that there exist only one coefficient x in the expression above such that $xa^k \neq 0$.

As $\alpha \in C$, there exist $\beta_{i_1}, \ldots, \beta_{\ell_1}, \beta_{\ell_2} \in RA$ such that

$$\alpha = \beta_{i_1}a^{k_{i_1}}\left(\frac{1 \pm d}{2}\right)e_{i_1} + \cdots + \beta_{\ell_1}a^{k_{i_\ell}}\left(\frac{1+d}{2}\right)e_{i_\ell} + \beta_{\ell_2}a^{h_{i_\ell}}\left(\frac{1-d}{2}\right)e_{i_\ell}.$$

Then

$$\begin{aligned}\alpha &= xa^k d^\delta \tau \widehat{G}_{i_\ell} \\ &= \beta_{i_1}a^{k_{i_1}}\left(\frac{1 \pm d}{2}\right)e_{i_1} + \cdots + \beta_{\ell_1}a^{k_{i\ell_1}}\left(\frac{1+d}{2}\right)e_{i_\ell} + \beta_{\ell_2}a^{k_{i\ell_2}}\left(\frac{1-d}{2}\right)e_{i_\ell}.\end{aligned}$$

Multiplying the above equality by $\widehat{G}_{i_1-1}$, we get $xa^k d^\delta \tau \widehat{G}_{i_1-1} = 0$. Thus $xa^k = 0$, a contradiction. Therefore $w(C) \geq 2|G_{i_\ell}|$ and thus $w(C) = 2|G_{i_\ell}|$ □

Now we consider ideals involving e_0. As a first step, we will assume that if j is the greatest subindex such that e_j is involved, then $\left(\frac{1+d}{2}\right)e_j$ is involved, say, but $\left(\frac{1-d}{2}\right)e_j$ is not, the symmetric case being identical.

Theorem 3.7. *Let C be a code of the form*

$$\begin{aligned}C &= \left\langle a^{k_0}\left(\frac{1+d}{2}\right)e_0\right\rangle \oplus \left\langle a^{h_0}\left(\frac{1-d}{2}\right)e_0\right\rangle \oplus \cdots \\ &\quad \oplus \left\langle a^{k_i}\left(\frac{1+d}{2}\right)e_i\right\rangle \oplus \left\langle a^{h_i}\left(\frac{1-d}{2}\right)e_i\right\rangle \oplus \cdots \oplus \left\langle a^{k_j}\left(\frac{1+d}{2}\right)e_j\right\rangle,\end{aligned}$$

where $0 \leq k_i, h_i \leq t$, for $0 < i < j$, $k_j < t$ and k_0 or $h_0 < t$. Then $w(C) = 4|G_j|$.

Proof. Note that $w(C) \leq 4|G_j|$ and $C \subset a^k\widehat{G}_j$, where k is the minimal non zero exponent of a. Let $T = \{\tau_1, \ldots, \tau_n\}$ a transversal of G_j in G and $\alpha \in C$, $\alpha \neq 0$. We can write

$$\alpha = (x_1\tau_1 + \ldots + x_n\tau_n + x_1'd\tau_1 + \ldots + x_n'd\tau_n)a^k\widehat{G}_j$$

Using exactly the same technique as in Theorem 4.4, we can show that there are at least four coefficients whose product with a^k is non zero.

Therefore $w(C) \geq 4|G_j|$ and thus $w(C) = 4|G_j|$. □

Finally, we consider the case when the code C involves e_0 and both $\left(\frac{1+d}{2}\right)e_j$ and $\left(\frac{1-d}{2}\right)e_j$.

Theorem 3.8. *Let C be a code of the form*

$$\begin{aligned}C &= \left\langle a^{k_0}\left(\frac{1+d}{2}\right)e_0\right\rangle \oplus \left\langle a^{h_0}\left(\frac{1-d}{2}\right)e_0\right\rangle \oplus \cdots \\ &\quad \oplus \left\langle a^{k_i}\left(\frac{1+d}{2}\right)e_i\right\rangle \oplus \left\langle a^{h_i}\left(\frac{1-d}{2}\right)e_i\right\rangle \oplus \cdots \\ &\quad \oplus \left\langle a^{k_j}\left(\frac{1+d}{2}\right)e_j\right\rangle \oplus \left\langle a^{h_j}\left(\frac{1-d}{2}\right)e_j\right\rangle,\end{aligned}$$

where at least either k_0 or h_0 is less than t and $k_j < t$ and $h_j < t$. Then $w(C) = |G_j|$ or $w(C) = 2|G_j|$.

Proof. We shall assume first that all idempotents of the form $\left(\frac{1\pm d}{2}\right) e_i$ are involved in C, for $0 \leq i \leq j$; i.e., that k_i, $h_i < t$, for $0 \leq i \leq j$.

As before, we have that $C \subset \langle \widehat{G}_j \rangle$. Therefore, $w(C) \geq w(\langle \widehat{G}_j \rangle) = |G_j|$.

As in the proof of Theorem 4.2, one can show that $\langle a^k \widehat{G}_j \rangle \subset C$ so actually $w(C) = |G_j|$.

Now, assume that there exists an index r such that either k_r or h_r is equal to t.

Note that $\left\langle a^{k_j} \left(\frac{1+d}{2}\right) e_j \right\rangle \oplus \left\langle a^{h_j} \left(\frac{1-d}{2}\right) e_j \right\rangle \subset C$ and thus, by Lemma 3.5 we have $w(C) \leq 2|G_j|$.

If k denotes the minimum of all exponents of a, we have as always that $C \subset < a^k \widehat{G}_j >$ and, taking a transversal $T = \{\tau_1, \ldots, \tau_n\}$ of G_j in G, and element $\alpha \in C$, $\alpha \neq 0$, we can write

$$\alpha = (x_1\tau_1 + \ldots + x_n\tau_n + x_1^{'} d\tau_1 + \ldots + x_n^{'} d\tau_n) a^k \widehat{G}_j.$$

One can show, as in the proof of Theorem 4.3, that there exist at least two coefficients in this expression above, whose product by a^k is non zero. Hence $w(\alpha) \geq 2|G_j|$ and, in this case, $w(C) = 2|G_j|$. □

4. The number of words in a code

Since most of the codes over chain rings are not free, we cannot compute dimensions and is then relevant to find the number of words in each code. We begin with a simple case.

Theorem 4.1. *If $C = \left\langle a^k \left(\frac{1\pm d}{2}\right) e_i \right\rangle$, then, the number of words of C is*

$$|C| = \begin{cases} |\overline{R}|^{t-k} & \text{if } i = 0, \\ |\overline{R}|^{(t-k)(p^i - p^{i-1})}, & \text{if } i > 0. \end{cases}$$

Proof. Since $e_0 = \widehat{G}$ we have that $RAa^k \left(\frac{1\pm d}{2}\right) e_0 = Ra^k e_0$, so

$$\left| \left\langle a^k \left(\frac{1 \pm d}{2}\right) e_0 \right\rangle \right| = |Ra^k| = |\overline{R}|^{t-k}.$$

When $i > 0$,

$$a^k \left(\frac{1+d}{2}\right) e_i = a^k \left(\frac{1+d}{2}\right) (\widehat{G}_i - \widehat{G}_{i-1}).$$

so

$$a^k \left(\frac{1+d}{2}\right) \widehat{G}_i = a^k \left(\frac{1+d}{2}\right) e_i + a^k \left(\frac{1+d}{2}\right) \widehat{G}_{i-1},$$

where $e_i \left(\frac{1+d}{2}\right) \widehat{G}_{i-1} = 0$. Hence

$$[RA]a^k \left(\frac{1+d}{2}\right) \widehat{G}_i = [RA]a^k \left(\frac{1+d}{2}\right) e_i \oplus [RA]a^k \left(\frac{1+d}{2}\right) \widehat{G}_{i-1}.$$

Notice that

$$\begin{aligned} [RA]a^k \left(\frac{1+d}{2}\right) \widehat{G}_i &= [Ra^k A] \left(\frac{1+d}{2}\right) \widehat{G}_i = [Ra^k G] \left(\frac{1+d}{2}\right) \widehat{G}_i \\ &= [Ra^k G] \widehat{G}_i \left(\frac{1+d}{2}\right). \end{aligned}$$

As $[Ra^k G]\widehat{G}_i \cong Ra^k[G/G_i]$ (see [10, Lemma 3.6.6]) we have

$$\left| [RA]a^k \left(\frac{1+d}{2}\right) \widehat{G}_i \right| = |\overline{R}|^{t-k}(|G|/|G_i|) = |\overline{R}|^{(t-k)(p^n/p^{n-i})}.$$

As a similar computation holds for $[RA]a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i-1}$, we get

$$\left|[RA]a^k\left(\frac{1+d}{2}\right)e_i\right| = |\overline{R}|^{(t-k)(p^i+p^{i-1})},$$

as claimed. □

Corollary 4.2. *Let C be a code of the form*

$$\begin{aligned} C &= \left\langle a^{k_0}\left(\frac{1+d}{2}\right)e_0\right\rangle \oplus \left\langle a^{h_0}\left(\frac{1-d}{2}\right)e_0\right\rangle \oplus \cdots \\ &\quad \cdots \oplus \left\langle a^{k_m}\left(\frac{1+d}{2}\right)e_m\right\rangle \oplus \left\langle a^{h_m}\left(\frac{1-d}{2}\right)e_m\right\rangle. \end{aligned}$$

Then

$$|C| = |\overline{R}|^{\gamma},$$

where $\gamma = \sum_{j=1}^{m}(2t-k_j-h_j)(p^j-p^{j-1}) + (2t-k_0-h_0)$.

5. Free cyclic codes over finite chain rings of lenght $2p^n$

Let A be a cyclic group of order $2p^n$, R a chain ring with $gcd(|\,R\,|,|\,A\,|) = 1$ and orthogonal primitive idempotents $(\frac{1\pm d}{2})e_i$, $0 \le i \le n$.

Theorem 5.1. *Let γ be a transversal of G_{i-1} in G and τ a transversal of G_i in G_{i-1}. Then $RA(\frac{1\pm d}{2})e_i$ is a free code with basis*

$$\mathcal{B} = \left\{c(1-b)\Big(\frac{1\pm d}{2}\Big)\widehat{G}_i | c \in \gamma, b \in \tau \setminus \{1\}\right\}$$

over R, where the positive sign in the base elements refers to the ideal $RA(\frac{1+d}{2})e_i$ and the negative sign to $RA(\frac{1-d}{2})e_i$.

Proof. We will prove that the code $RA(\frac{1+d}{2})e_i$ is free. The proof that $RA(\frac{1-d}{2})e_i$ is free being similar. First we show that elements in $\mathcal{B}$ belong to the code.

For $b \in \tau \setminus \{1\}$, we have

$$(1-b)\left(\frac{1+d}{2}\right)\widehat{G}_{i-1} = \left(\frac{1+d}{2}\right)\widehat{G}_{i-1} - \left(\frac{1+d}{2}\right)b\widehat{G}_{i-1} = 0,$$

because $b\cdot\widehat{G}_{i-1} = \widehat{G}_{i-1}$.

Then, $c(1-b)\left(\frac{1+d}{2}\right)\widehat{G}_i = c(1-b)\left(\frac{1+d}{2}\right)(\widehat{G}_i - \widehat{G}_{i-1} + \widehat{G}_{i-1}) = c(1-b)\left(\frac{1+d}{2}\right)e_i + c(1-b)\left(\frac{1+d}{2}\right)\widehat{G}_{i-1} = c(1-b)\left(\frac{1+d}{2}\right)e_i$. Therefore, $\mathcal{B} \subset RA\left(\frac{1+d}{2}\right)e_i$.

Now, we show that $\mathcal{B}$ is linearly independent.

Let $x_{cb} \in R$, where $c \in \gamma$, and $b \in \tau \setminus \{1\}$ be such that

$$\sum_{c\in\gamma}\sum_{b\in\tau\setminus\{1\}} x_{cb}c(1-b)\left(\frac{1+d}{2}\right)\widehat{G}_i = 0.$$

Thus

$$0 = \sum_{c\in\gamma}\Big(\sum_{b\in\tau} x_{cb}c(1-b)\left(\frac{1+d}{2}\right)\widehat{G}_i\Big)$$

$$\begin{aligned} &= \sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}c\left(\frac{1+d}{2}\right)\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}cb\left(\frac{1+d}{2}\right)\widehat{G}_i \\ &= \tfrac{1}{2}(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}c\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}cb\widehat{G}_i) + \frac{1}{2}(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}dc\widehat{G}_i) \\ &\quad - \sum_{c\in\gamma\ b\in\tau} x_{cb}dcb\widehat{G}_i). \end{aligned}$$

The elements of the sum $(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}c\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}cb\widehat{G}_i)$ have supports that are disjoint with the elements of the sum $(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}dc\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}dcb\widehat{G}_i)$. Thus,

$$\begin{aligned} \left(\sum_{c\in\gamma}(\sum_{b\in\tau}\ x_{cb}c\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}cb\widehat{G}_i\right) &= \\ \left(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}dc\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}dcb\widehat{G}_i\right) &= 0. \end{aligned}$$

We prove now that the elements of the sum $(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}c\widehat{G}_i) - \sum_{c\in\gamma\ b\in\tau} x_{cb}cb\widehat{G}_i)$ has disjoint supports. To this end, we prove that, for every c, b fixed, the element $cb\widehat{G}_i$ has disjoint support with any other element in this linear combination. As $b \in \tau$, then $\widehat{G}_i$ and $b\widehat{G}_i$ have disjoint supports. Thus $c\widehat{G}_i$ and $cb\widehat{G}_i$ have disjoint supports. If $c_j \neq c_k$, then $c_j\widehat{G}_i$ and $c_k\widehat{G}_i$ have disjoint supports. As τ is a transversal of G_i in G_{i-1}, we have that for $b_j \neq b_k \in \tau$, $c_jb_j\widehat{G}_i$ and $c_kb_k\widehat{G}_i$ have disjoint supports. Therefore, $x_{cb} = 0$, $\forall c \in \gamma$ and $b \in \tau$.

By Theorem 4.1, the number of elements of $RA(\frac{1+d}{2})e_i$ is given by

$$|\ \overline{R}\ |^{t(p^i-p^{i-1})} = |\ R\ |^{(p^i-p^{i-1})}\ .$$

The number of elements of the code generated by $\mathcal{B}$ over R is given by $|\ R\ |^{(|\gamma|\cdot(|\tau|-1))}$ where $(|\ \gamma\ |\cdot(|\ \tau\ |-1)) = \frac{|G|}{|G_{i-1}|}\cdot(\frac{|G_{i-1}|}{|G_i|}-1) = (p^i - p^{i-1})$.

As this code is contained in $RA(\frac{1+d}{2})e_i$, equality follows. Therefore $RA(\frac{1+d}{2})e_i$ is a free code with basis $\mathcal{B}$. □

A code $C = RAa^k\left(\frac{1+d}{2}\right)e_i$, with $0 < k < t$, is not free, because $\alpha \cdot a^{t-k} \cdot a^k\left(\frac{1+d}{2}\right)e_i = 0$, for all $\alpha \in RA$.

REFERENCES

[1] S. K. Arora and M. Pruthi, Minimal cyclic codes of length $2p^n$, *Finite Fields Appl.*, **5** (1999), 177–187.

[2] Y. L. Cao, On constacyclic codes over finite chain rings, *Finite Fields Appl.*, **24** (2013), 124–135.

[3] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Transactions on Information Theory*, **50** (2004), 1728–1744.

[4] S. T. Dougherty, J.-L. Kim and H. W. Liu, Construction of self-dual codes over finite commutative chain rings, *Int. Journal on Information and Coding Theory*, **1** (2010), 171–190.

[5] R. A. Ferraz and C. Polcino Milies, Idempotents in group algebras and minimal abelian codes, *Finite Fields and Their Appl.*, **13** (2007), 382–393.

[6] N. Jacobson, *Basic Algebra. II*, W. H. Freeman and Company, San Francisco, Calif., 1980.

[7] Z. H. Liu, Notes on linear codes over finite chain rings, *Acta Mathematicae Applicatae Sinica*, **27** (2011), 141–148.

[8] E. Martinez-Moro and I. F. Rúa, On repeated-root multivariable codes over a finite chain ring, *Designs, Codes Cryptography*, **45** (2007), 219–227.

[9] G. H. Norton and A. Sălăgean-Mandache, On the structure of linear cyclic codes over finite chain rings, *Appl. Algebra Eng. Commun. Comput.*, **10** (2000), 489–506.

[10] C. Polcino Milies and S. K. Sehgal, *An Introduction to Group Rings*, Algebra and Applications, 1. Kluwer Academic Publishers, Dordrecht, 2002.
[11] P. Solé and V. Sison, Bounds on the minimum homogeneous dis-tance of the p^r-ary image of linear block codes over the galois ring $GR(p^r, m)$, *IEEE Trans. Information Theory*, **53** (2007), 2270–2273.

Received February 2018; revised March 2019.

E-mail address: anderson.tiago@ufv.br
E-mail address: polcino@ime.usp.br