Applicable Algebra in Engineering, Communication and Computing
https://doi.org/10.1007/s00200-020-00471-7

ORIGINAL PAPER

One-weight codes in some classes of group rings

Raul Antonio Ferraz[1] · **Ruth Nascimento Ferreira**[2]

Received: 22 July 2019 / Revised: 28 September 2020 / Accepted: 29 October 2020

Abstract
Let $\mathbb{F}_q$ be a finite field with q elements and G be a finite abelian group. In this work we gave conditions to ensure that a code in $\mathbb{F}_q G$ is a one-weight code in the case when G is a cyclic group with n elements, such that $\gcd(n, q) = 1$, and also when G is an abelian group.

Keywords One weight codes · Cyclic group · Abelian group

Mathematics Subject Classification 94B05

1 Introduction

A type of code of particular interest is the case when the code has constant weight, that is, all its non zero words have the same Hamming weight. Many works in this area consider binary one-weight codes which have many applications, for example in mobile communication. Nowadays, the interest in non binary one-weight codes is also increasing (see for example [4]).

In [11], Vega characterized one-weight codes in $\mathbb{F}_q C_n$, with $n = \frac{\lambda(q^k-1)}{q-1}$, where λ divides $q - 1$, and obtained the number of one-weight codes in this ring. His paper made use of polynomial tools, specially linear recurrence sequences.

Inspired by these results, we use group ring theory to extend his results to codes in $\mathbb{F}_q C_n$, with n arbitrary such that $gcd(n, q) = 1$, that is, when the group ring is semi-simple. We then characterize one-weight codes in abelian group rings, first when the group ring is semisimple and then in the general case.

✉ Raul Antonio Ferraz
raul@ime.usp.br

Ruth Nascimento Ferreira
ruthnascimento@utfpr.edu.br

[1] Departamento de Matemática, Universidade de São Paulo, Rua do Matão, 1010, 05508-090 São Paulo SP, Brazil

[2] Universidade Tecnológica Federal do Paraná, Avenida Professora Laura Pacheco Bastos, 800, 85053-510 Guarapuava PR, Brazil

Published online: 20 November 2020

We recall that, in the context of group rings, a q-ary code is an ideal of a group ring $\mathbb{F}_q G$, and we shall use throughout these words as synonyms. This view point started with the works of Berman [1, 2] and MacWilliams [8] who worked mainly with Abelian groups. Since then, many authors have used group rings to study error-correcting codes. See, for example, [6, 7, 9, 10].

Throughout the paper, all codes considered are linear cyclic (or Abelian) over a field $\mathbb{F}_q$ are viewed as ideals in appropriate group rings. All the groups considered in this paper are finite.

2 Cyclic groups

Let n, q be positive integers, q a power of a prime rational integer such that $gcd(n, q) = 1$. Let $\mathbb{F}_q$ be the finite field with q elements and G be an abelian group of order n. Then the group ring $\mathbb{F}_q G$ is semisimple. Given a subgroup H of G, we denote by $\widehat{H}$ the element $\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h \in \mathbb{F}_q G$ which is an idempotent in $\mathbb{F}_q G$. In [3], the following definition is given:

Definition 1 ([3, Definition 2.2]) A primitive idempotent e in $\mathbb{F}_q G$ is called **essential** if $e\widehat{H} = 0$, for all subgroups H of G such that $H \neq 1$.

Let e be a non essential primitive idempotent in $\mathbb{F}_q G$. Set $\mathcal{H}_e = \{H < G; \widehat{H}e = e\}$. Since $\widehat{H_1 H_2} = \widehat{H_1}\widehat{H_2}$, if $H_1, H_2 \in \mathcal{H}_e$, then $H_1 H_2 \in \mathcal{H}_e$. Let $H_e := \prod_{H \in \mathcal{H}_e} H$. Then $H_e \in \mathcal{H}_e$, and it is the biggest subgroup H in G such that $e\widehat{H} = e$.

Let e be a primitive idempotent. Given an idempotent k, it is easy to see that either $ek = 0$ or $ek = e$. So, if $K \nsubseteq H_e$, then $e\widehat{K} = 0$. In fact, as $\widehat{KH_e}$ is an idempotent, if $e\widehat{K} \neq 0$, we have $e = e\widehat{K} = e\widehat{KH_e}$, contradicting the maximality of H_e. Thus $e\widehat{K} = e$ if, and only if, $K \subseteq H_e$.

Lemma 1 ([3], Theorem 3.1) *Let e be a primitive idempotent of $\mathbb{F}_q G$ and H_e as defined above. The map*

$$\Psi : \mathbb{F}_q G\widehat{H}_e \to \mathbb{F}_q[G/H_e]$$

given by

$$\sum_{g \in G} \alpha_g g\widehat{H}_e \mapsto \sum_{g \in G} \alpha_g \bar{g}$$

is a ring isomorphism, and $\Psi(e)$ is an essential idempotent.

Lemma 2 ([3], *Proposition* 2.3) *Let G be a finite abelian group and e a primitive idempotent in $\mathbb{F}_q G$. Then e is essential if, and only if, $G \simeq Ge$ via the homomorphism $\pi : G \to Ge$ given by $g \mapsto ge$, for all $g \in G$.*

We shall need the following results.

Lemma 3 *Let $\mathcal{C}$ be a one-weight code of dimension k in a group ring $\mathbb{F}_q G$. Then, the weight of any word $\alpha \in \mathcal{C}$ is*

$$\omega(\alpha) = \frac{q^{k-1}(q-1)n}{q^k - 1}.$$

Proof For any linear code, the j^{th}-projection $\pi_j : \mathcal{C} \to \mathbb{F}_q$ which maps $\alpha \in \mathcal{C}$ to its j^{th} component a_j is an $\mathbb{F}_q$-linear functional. Then π_j is either the zero mapping or it is surjective. Since the code is cyclic, π_j is non-zero. In fact, write $G = \{g_1, g_2, \ldots, g_n\}$ and let $\alpha = a_1 g_1 + a_2 g_2 + \cdots + a_n g_n$ be a non-zero word in $\mathbb{C}$. Then $a_i \neq 0$ for some index i. Hence for every index j, $1 \leq j \leq n$ there exists a word $\alpha_j \in \mathbb{C}$ such that the coefficient of g_j in α_j is non zero. Actually, if $g \in G$ is such that $g g_i = g_j$ then $\alpha_j = g\alpha$ is one such word.

Thus. each π_j is surjective and every element of $\mathbb{F}_q$ is an image of $|Ker(\pi_j)|$ elements. Hence

$$\sum_{c \in \mathcal{C}} \omega(c) = \sum_{j=1}^{n} |Ker(\pi_j)| \sum_{a \in \mathbb{F}_q} \omega(a) = n q^{k-1}(q-1).$$

Since the code is of constant weight, the result follows. □

As an immediate consequence we have the following.

Lemma 4 *A code of constant weight in a cyclic group algebra is minimal.*

Proof Let $\mathcal{C}$ be a code of constant weight of dimension k in a group algebra $\mathbb{F}_q G$ and let $\mathcal{C}_1 \subset \mathcal{C}$ be another code of dimension k_1. For an element $\alpha \in \mathcal{C}_1$ we have

$$\omega(\alpha) = \frac{q^{k_1 - 1}(q-1)n}{q^{k_1} - 1}.$$

As also $\alpha \in \mathcal{C}$ we have

$$\omega(\alpha) = \frac{q^{k-1}(q-1)n}{q^k - 1}.$$

Therefore

$$q^{k_1 - 1}(q^k - 1) = q^{k-1}(q^{k_1} - 1).$$

If $k_1 < k$, after cancelling $q^{k_1 - 1}$, the right-hand member of the equation is a multiple of q while the left hand member is not. So $k_1 = k$ and $\mathcal{C}_1 = \mathcal{C}$. □

We recall the following elementary result.

Lemma 5 *If G is a cyclic group and H_1, H_2 are subgroups of G, then $|H_1H_2| = lcm(|H_1|, |H_2|)$, and $|H_1 \cap H_2| = gcd(|H_1, H_2|)$.*

We are now ready to state the main result of this section.

Theorem 1 *Let $\mathbb{F}_q$ be a field with q elements, n a positive integer such that $gcd(q, n) = 1$, $C_n = \langle g \rangle$ a cyclic group with n elements, and $\mathbb{F}_qC_n$ the group ring of C_n over $\mathbb{F}_q$. Let e be a primitive idempotent of $\mathbb{F}_qC_n$ and $\mathcal{C} = \mathbb{F}_qC_ne$ the minimal code it generates. Set $dim_{\mathbb{F}_q}\mathcal{C} = k$. The following assertions are equivalent*:

1. *$\mathcal{C}$ has constant weight*;
2. *Every non zero element of $\mathcal{C}$ has weight $\frac{q^{k-1}(q-1)n}{q^k-1}$*;
3. *There is an element in $\mathcal{C}$ whose weight is $\frac{q^{k-1}(q-1)n}{q^k-1}$*;
4. *The set of non zero elements in $\mathbb{F}_qC_ne$ is*

$$(\mathbb{F}_qC_ne)^* = \mathbb{F}_q^*e \cdot C_ne.$$

Proof (1 $\Rightarrow$ 2) It is Lemma 3. (2 $\Rightarrow$ 3) It is trivial.

(3 $\Rightarrow$ 4) Assume first that e is essential. In this case, $|C_ne| = n$, according to Lemma 2 and by Lemma 5 we have $\mu = |C_ne \cap \mathbb{F}_q^*e| = gcd(|C_ne|, |\mathbb{F}_q^*e|)$ and $|C_ne\mathbb{F}_q^*e| = lcm(|C_ne|, |\mathbb{F}_q^*e|)$. Set $t = n/\mu$. There is only one subgroup of order μ in $(\mathbb{F}_qC_ne)^*$, which is $\langle (g^te) \rangle$. As $C_ne \cap \mathbb{F}_q^*e$ is of that order, it follows that $C_ne \cap \mathbb{F}_q^*e = \langle g^te \rangle$. So $g^te = \lambda e$, for some $\lambda \in \mathbb{F}_q^*$.

Let α be an element of $\mathbb{C}$ of weight $[q^{k-1}(q-1)n]/(q^k-1)$. As e is the unity in $\mathbb{F}_qC_ne$, $g^t\alpha = g^te\alpha = \lambda e\alpha = \lambda\alpha$. Write

$$\alpha = \alpha_0 + \alpha_1 g + \cdots + \alpha_{n-1}g^{n-1},$$

so

$$\alpha g^t = \alpha_0 g^t + \alpha_1 g^{t+1} + \cdots + \alpha_{n-t} + \alpha_{n-t+1}g + \cdots + \alpha_{n-1}g^{n+t-1} = \lambda\alpha.$$

Thus $\alpha_0 = \alpha_t\lambda$, $\alpha_t = \alpha_{2t}\lambda$, that is, $\alpha_{2t} = \alpha_t\lambda^{-1} = \alpha_0\lambda^{-2}$, and in general, $\alpha_{i+kt} = \alpha_i\lambda^{-k}$, $0 \le i \le t-1$, $0 \le k \le \mu - 1$.

Denote $\beta = \alpha_0 + \alpha_1 g + \cdots + \alpha_{t-1}g^{t-1}$. So

$$\begin{aligned}\alpha =& \beta + \lambda^{-1}\beta g^t + \lambda^{-2}\beta g^{2t} + \cdots + \lambda^{-(\mu-1)}\beta g^{(\mu-1)t} \\ =& \sum_{i=0}^{\mu-1} \lambda^{-i}g^{it}\beta,\end{aligned}$$

with $supp(\lambda^{-i}g^{it}\beta) \cap supp(\lambda^{-j}g^{it}\beta) = \emptyset$, if $i \neq j$. From this we have

$$\omega(\alpha) = \omega(\beta) + \cdots + \omega(\lambda^{\mu-1}\beta g^{(\mu-1)t}) = \mu\omega(\beta)$$

and then $\mu = gcd(\left|C_n e\right| = gcd(n, q-1), \left|\mathbb{F}_q^* e\right|)$ divides $[q^{k-1}(q-1)n]/(q^k-1)$.

As $gcd(q^{k-1}, gcd(n, q-1)) = 1$, it follows that $gcd(n, q-1)$ divides $\frac{(q-1)n}{q^k-1}$.

So $q^k - 1$ divides $[(q-1)n]/gcd(n, q-1) = lcm(q-1, n)$. That is, $\left|(\mathbb{F}_q C_n e)^*\right|$ divides $\left|\mathbb{F}_q^* e C_n e\right|$. But $\mathbb{F}_q^* e C_n e$ is a subgroup of $(\mathbb{F}_q C_n e)^*$, therefore $(\mathbb{F}_q C_n e)^* = \mathbb{F}_q^* e C_n e$.

Suppose now that e is not essential. Take H_e the biggest subgroup of C_n such that $eH_e = e$. As seen before $\mathbb{F}_q C_n \widehat{H_e} \simeq \mathbb{F}_q[C_n/H_e]$ via the isomorphism ψ such that $\Psi(g\widehat{H_e}) = \bar{g}$. Consider $\left|H_e\right| = d_1, \left|C_n/H_e\right| = d_2$, with $H_e = \left\langle g^{d_2} \right\rangle$. Let $\alpha \in \mathbb{F}_q C_n \widehat{H_e}$ be an element of weight $[q^{k-1}(q-1)n](q^k-1)$. Then, as $\alpha\widehat{H_e} = \alpha$, it follows as before that

$$\begin{aligned}\alpha =& (\alpha_0 + \alpha_1 g + \cdots + \alpha_{d_2-1} g^{d_2-1}) + \alpha_0 g^{d_2} + \cdots \\ =& (\alpha_0 + \alpha_1 g + \cdots + \alpha_{d_2-1} g^{d_2-1})\widehat{H_e},\end{aligned}$$

and so

$$\omega(\alpha) = \omega(\alpha_0 + \alpha_1 g + \cdots + \alpha_{d_2-1} g^{d_2-1})\left|H_e\right|.$$

but

$$\Psi(\alpha) = \alpha_0 + \alpha_1 \bar{g} + \cdots + \alpha_{d_2-1} \bar{g}^{d_2-1},$$

therefore $\omega(\Psi(\alpha)) = \omega(\alpha)/d_1$, and thus

$$\omega(\Psi(\alpha)) = \left(\frac{q^{k-1}(q-1)n}{q^k-1}\right)/d_1 = \frac{q^{k-1}(q-1)d_2}{q^k-1}.$$

But $\Psi(e)$ is essential in $\mathbb{F}_q[C_n/H_e]\Psi(e)$ and, in this case,

$$\mathbb{F}_q^* \Psi(e)[C_n/H_e]\Psi(e) = (\mathbb{F}_q[C_n/H_e]\Psi(e))^*$$

and we have that every element is of the form $\lambda \bar{g}^i \Psi(e)$. So, applying Ψ^{-1}, it follows that the elements in $(\mathbb{F}_q C_n e)^*$ have the form $\lambda g^i e$, and the result follows also in this case.

$(4 \Rightarrow 1)$: As $(\mathbb{F}_q C_n e)^* = \mathbb{F}_q^* e C_n e$, the non zero elements of $\mathbb{F}_q C_n e$ are the form $\lambda g^i e$, with $\lambda \in \mathbb{F}_q^*$, so they all have the same weight as e. □

An immediate consequence of this result is the following:

Corollary 1 *If $\mathcal{C}$ is a code of $\mathbb{F}_q C_n$ (with $gcd(n, q) = 1$), then $\mathcal{C}$ has constant weight if, and only if, $\mathcal{C} = \{0\} \cup \{kg^i e | k \in \mathbb{F}_q^*, g^i \in C_n\}$.*

From the Theorem 1 the following result, found in the paper of Vega [11], also follows in a simple way. Recall that for a polynomial of positive degree $h \in \mathbb{F}_q[X]$, such that $h(0) \neq 0$, the *quasi-order* of h, denoted $qord(h)$, is the least positive integer ρ such that X^ρ is congruent to an element in $\mathbb{F}_q$ modulo $h(X)$.

Corollary 2 [[11], *Theorem* 9] *Let* $\mathbb{F}_q$ *be a field with* q *elements,* $n = \lambda(q^k - 1)/(q-1)$, *with* λ *dividing* $(q-1)$, *and* $\mathcal{C}$ *be a cyclic code of* $\mathbb{F}_q$ *with length* n *and dimension* k *generated by* $g(x)$, *and with check polynomial* $h(x)$. *Then* $qord(ge) = (q^k - 1)/(q-1)$ *if, and only if,* $\omega(ge) = \lambda(q^{k-1})$.

Proof Indeed, $o(ge)/gcd(o(ge), q-1)$ is equal to $(q^k-1)/(q-1)$ if, and only if $o(ge)(q-1)/gcd(o(ge), q-1) = q^k - 1$, that is if, and only if, $(\mathbb{F}_q C_n e) = \mathbb{F}_q^* e C_n e$ which, according to Theorem 1, occurs if and only if $\mathcal{C}$ has constant weight. So, this occurs if and only if $\omega(ge) = q^{k-1}(q-1)n/(q^k-1)$. Since $\lambda = n(q-1)/(q^k-1)$, this happens if and only if $\omega(ge) = \lambda(q-1)$. □

3 The number of one-weight codes in $\mathbb{F}_q C_n$

We shall use Theorem 1, as well as properties of essential idempotents found in [3], to extend Theorem 12 in [11] to codes in $\mathbb{F}_q C_n$ with $gcd(n, q) = 1$.

Let $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$. So $C_n = P_1 \times \cdots \times P_t$, where P_i is the p_i-Sylow of C_n. As C_n is cyclic, its subgroups are cyclic then there exists one minimal subgroup $K_i \subseteq P_i$, for each $i, 1 \leq i \leq t$. Then

$$e_0 = (1 - \widehat{K_1})(1 - \widehat{K_2}) \cdots (1 - \widehat{K_t})$$

is an idempotent. A primitive idempotent e of $\mathbb{F}_q C_n$ is essential if, and only if, $ee_0 = e$ and $e_0 = \sum_{e \text{ essential}} e$ (see [3, Theorem 2.6]).

Theorem 2 ([3], Theorem 4.2) *Let* C_n *be a cyclic group with* n *elements generated by* g, *and* m *be the least positive integer such that* $n|(q^m - 1)$. *Then*:

1. $dim(\mathbb{F}_q C_n)e_0 = \varphi(n)$, *where* φ *denotes the Euler function.*
2. *There are precisely* $\frac{\varphi(n)}{m}$ *essential idempotents in* $\mathbb{F}_q C_n$.

Theorem 3 *Let* $\mathbb{F}_q$ *be the field with* q *elements,* n *a positive integer with*$gcd(q, n) = 1$, $C_n = \langle g \rangle$ *a cyclic group with* n *elements, and* $\mathbb{F}_q C_n$ *the group ring of* C_n *over* $\mathbb{F}_q$. *The number of cyclic one-weight codes of length* n *and dimension* k *is*

$$\sum_{d|n} \delta_{r,s} \frac{\varphi(d)}{k}$$

where φ *is the Euler function,* $r = q^k - 1, s = lcm(d, q-1)$ *and* δ *denotes Kronecker's symbol.*

Proof By Theorem 1, given a primitive idempotent e of $\mathbb{F}_q C_n$, the ideal $\mathbb{F}_q C_n e$ of dimension k has constant weight if and only if $(\mathbb{F}_q C_n e)^* = \mathbb{F}_q^* e C_n e$ and, since $d = o(ge)$, this happens if and only if $q^k - 1 = lcm(q-1, d)$.

Given a divisor d of n such that $q^k - 1 = lcm(q-1, d)$, taking the primitive essential idempotents in $\mathbb{F}_q C_n$ with $o(ge) = d$, we have:

$$\mathbb{F}_q C_d e_0 = \bigoplus_{e \text{ essential}} \mathbb{F}_q C_d e$$

$$\text{so} \quad dim_{\mathbb{F}_q} \mathbb{F}_q C_d e_0 = \sum_{e \text{ essential}} dim_{\mathbb{F}_q} \mathbb{F}_q C_d e$$

$$\varphi(d) = l \cdot k$$

thus

$$l = \varphi(d)/k.$$

As the number of essential idempotents will determine the number of different one-weight codes we have, for such d, that the number of one-weight codes is $\varphi(n)/k$. Adding, for each $d|n$ satisfying $q^k - 1 = lcm(q-1, d)$, the result follows. □

4 Abelian groups

In this section we shall extend the results above to the case when A in an Abelian group.

Theorem 4 *Let $\mathbb{F}_q$ field with q elements, n a positive integer with $gcd(q, n) = 1$, A an Abelian group with n elements, and $\mathbb{F}_q A$ be the group ring of A over $\mathbb{F}_q$. Consider e a primitive idempotent of $\mathbb{F}_q A$ and let $\mathcal{C} = \mathbb{F}_q Ae$ be the corresponding minimal code. Set $k = dim_{\mathbb{F}_q} \mathcal{C}$. Then, the following statements are equivalent*:

1. *$\mathcal{C}$ is a one-weight code*;
2. *Every non zero element of $\mathcal{C}$ has weight $\frac{q^{k-1}(q-1)n}{q^k-1}$*;
3. *There is an element in $\mathcal{C}$ with weight $\frac{q^{k-1}(q-1)n}{q^k-1}$*;
4. $(\mathbb{F}_q Ae)^* = \mathbb{F}_q^* Ae$.

Proof: The implications $(1 \Rightarrow 2)$, $(2 \Rightarrow 3)$ and $(4 \Rightarrow 1)$ follow as in the proof of Theorem 1. Now consider the case $(3 \Rightarrow 4)$. If the idempotent e is essential, the proof is similar to that in the Theorem 1, since the arguments use only the fact that $\mathbb{F}_q Ae$ is a field, which implies that $(\mathbb{F}_q Ae)^*$ is a cyclic group, and this is still true when A is Abelian.

Assume that e in non essential. Observe that in the proof of Theorem 1 for this case, the arguments depend only on the fact that C_n/H_e is a cyclic group. We will show that A/H_e is cyclic, also in this case.

Consider the homomorphism

$$\varphi : A \to (\mathbb{F}_q Ae)^*$$
$$a \mapsto ae.$$

Let $a \in Ker(\varphi)$. Then $ae = e$, thus $a^i e = e$, therefore $\frac{1}{|\langle a\rangle|}\Sigma a^i e = e$ and, as a consequence, $\langle a\rangle \in \mathcal{H}e$, that is, $\langle a\rangle \subset H_e$, so $Ker(\varphi) \subset H_e$. If $h \in H_e$, then $he = h\widehat{H}_e e = e$, so $\ker(\varphi) = H_e$. Thus, A/H_e is isomorphic to a subgroup of $(\mathbb{F}_q Ae)^*$, which is cyclic. Hence $(3 \Rightarrow 4)$. □

Now we consider case when A is an Abelian group with n elements, but without the hypothesis that $gcd(n, q) = 1$. Write $A = A_{p'} \times A_p$, where $gcd(p, |A_{p'}|) = 1$ and A_p is the p-Sylow subgroup of A. Then $\mathbb{F}_q A_{p'}$ is semi-simple, of the form $\mathbb{F}_q A_{p'} = \mathbb{F}_q A_{p'} e_1 \oplus \cdots \oplus \mathbb{F}_q A_{p'} e_t$, where e_i, $1 \le i \le t$ are primitive idempotents, and $\mathbb{F}_q A_{p'} e_i = K_i$, is a field. In this case, we have $\mathbb{F}_q A = \mathbb{F}_q(A_{p'} \times A_p) = (\mathbb{F}_q A_{p'})A_p = (K_1 \oplus \cdots \oplus K_t)A_p = K_1 A_p \oplus \cdots \oplus K_t A_p$.

Lemma 6 *With the notation above, $K_i A_p$ is a local ring, $1 \le i \le t$, whose radical is its augmentation ideal.*

Proof Given $\alpha \in K_i A_p$, we shall denote by $\epsilon(\alpha)$, its augmentation. It suffices to prove that $\epsilon(\alpha) \neq 0$ implies that α is a unit.

We observe that if $\alpha = \sum_{g\in A_p} \alpha_g g$ and p^s is the exponent of A_p, we have

$$\alpha^{p^s} = \left(\sum_{g\in A_p} \alpha_g g\right)^{p^s} = \sum_{g\in A_p} \alpha_g^{p^s} = \left(\sum_{g\in A_p} \alpha_g\right)^{p^s} = \epsilon(\alpha)^{p^s} \neq 0.$$

Since K_i is a field it follows that α^{p^s} is a unit, and hence α is a unit. □

Denote by $\tilde{A_p} = \sum_{a\in A_p} a$ and let $\left\langle \tilde{A_p} \right\rangle = K_i A_p \tilde{A_p}$ be the ideal of $K_i A_p$ generated by $\tilde{A_p}$. Then we have:

Lemma 7 *With the notation above, $\left\langle \tilde{A_p} \right\rangle$ is the unique minimal ideal of $K_i A_p$.*

Then, the minimal ideals in $\mathbb{F}_q A$ are of the form $\mathbb{F}_q A_{p'} e_i \tilde{A_p}$. We also call these minimal ideals as **irreducible Abelian codes**. The same proof as in Lemma 6 shows the following.

Lemma 8 *Let $\mathbb{F}_q$ be a field with q elements and A be an Abelian group with n elements. If a code in $\mathbb{F}_q A$ is a one-weight code, then it is irreducible.*

So, for a code in $\mathbb{F}_q A$ to be a one-weight code, it must be minimal; then by Lemma 7, the code has to be of the form $\mathbb{F}_q A_{p'} e_i \tilde{A_p}$. As an element of such a set is of the form $\alpha = \alpha_1 \tilde{A_p}$ with $\alpha_1 \in \mathbb{F}_q A_{p'} e_i$, (and for each $g \neq h \in A_p$, $supp(\alpha_1 g)$ and $supp(\alpha_1 h)$ are disjoint sets), its weight is $\omega(\alpha_1)\left|\tilde{A_p}\right|$, that is, the study of the weight

of the elements of the code is reduced to the study of the weight of the elements in $\mathbb{F}_q A_{p'} e_i$. Then we have:

Theorem 5 *Let $\mathbb{F}_q$ a field with q elements, n a positive integer with $gcd(q,n) \neq 1$, A an Abelian group with n elements, and $\mathbb{F}_q A$ the group ring of A over $\mathbb{F}_q$. Consider a primitive idempotent e of $F_q A$ and let $\mathcal{C} = \mathbb{F}_q Ae = \mathbb{F}_q A_{p'} e\tilde{A}_p$ be the respective minimal code. Set $dim_{\mathbb{F}_q} \mathcal{C} = k$. Then $\mathcal{C}$ is a one-weight code if, and only if, given any element $\alpha = \alpha_1 \tilde{A}_p$, with $\alpha_1 \in \mathbb{F}_q A_{p'} e$, $\omega(\alpha) = (q^{k-1}n)/(q^k - 1)$, that is, if, and only if, $\mathbb{F}_q A_{p'} e_i$ is a one-weight code.*

5 A two-weight code

In this section we construct two-weight codes, using the information he have about one-weight codes from the previous sections.

Let $\langle g \rangle \cong \langle h \rangle$ be two cyclic subgroups of order $p^n - 1$. Denote by $e(g)$ an essential idempotent of $\mathbb{F}_q \langle g \rangle$ and denote by $e(h)$ the essential idempotent of $\mathbb{F}_q \langle h \rangle$ obtained by exchanging g with h. As $\widehat{g}$ and $\widehat{h}$ are idempotents then also $e(g)\widehat{h}$ and $e(h)\widehat{g}$ are idempotents. Set $e_0 = e(g)\widehat{h} + e(h)\widehat{g}$.

We now consider the code

$$\mathbb{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$$

and wish to determine the weights of the non zero elements in this code. We first determine which are the elements of this code.

Theorem 6 *With the notation above, the non zero elements of $\mathbb{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$ are of the form $g^i e(g)\widehat{h}$, $1 \leq i \leq q^m - 1$, $h^i e(h)\widehat{g}, 1 \leq i \leq q^m - 1$, and $g^t h^s e_0$, $1 \leq t, s \leq q^m - 1$.*

Proof: Consider $L = \{0\} \cup \{g^i e(g)\widehat{h}\} \cup \{h^j e(h)\widehat{g}\} \cup \{g^t h^s e_0\}$. We claim that $L = \langle e_0 \rangle$.

The inclusion $L \subseteq \langle e_0 \rangle$ holds because $e(h)$ and $e(g)$ are essential in $\langle h \rangle$ and $\langle g \rangle$, respectively. In particular, we have that $e(h) \cdot \widehat{h} = 0$ so $e(h)\widehat{g} = e(h)\widehat{g}e_0$. A similar argument shows that $e(g)\widehat{h} \in e(h)\widehat{g}e_0$.

To verify that $\langle e_0 \rangle \subseteq L$, since $e_0 \in L$, it is enough to show that L is an ideal. We show first that L is closed under addition.

We start analysing $g^t h^s e_0 + g^{t_1} h^{s_1} e_0$. We have

$$\begin{aligned} g^t h^s e_0 + g^{t_1} h^{s_1} e_0 =& g^t h^s (e(g)\widehat{h} + e(h)\widehat{g}) + g^{t_1} h^{s_1} (e(g)\widehat{h} + e(h)\widehat{g}) \\ =& g^t e(g)\widehat{h} + g^{t_1} e(g)\widehat{h} + h^s e(h)\widehat{g} + h^{s_1} e(h)\widehat{g} \\ =& ((g^t + g^{t_1})e(g))\widehat{h} + ((h^s + h^{s_1})e(h))\widehat{g}. \end{aligned}$$

Note that $(g^t + g^{t_1})e(g)$ is an element of $\mathbb{F}_q C_{q^m-1}e(g)$. Suppose first that $g^t + g^{t_1}$ is different from zero. As $\mathbb{F}_q C_{q^m-1}e(g)$ has constant weight we have, by Theorem 1, that $(\mathbb{F}_q C_{q^m-1}e(g))^* = \mathbb{F}_q^* e(g) C_{q^m-1}e(g)$. As $e(g)$ is essential, by Lemma 2,$C_{q^m-1}e(g) \simeq C_{q^m-1}$, hence $\left|C_{q^m-1}e(g)\right| = q^m - 1$ and thus $\left|\mathbb{F}_q C_{q^m-1}e(g)\right| = q^m - 1$, so $\left|(\mathbb{F}_q C_{q^m-1}e(g))^*\right| = q^m - 1$. As $e(g)$ is essential, $g^i e(g) \neq g^j e(g)$, if $i \neq j$, and then $\left|\{g^i e(g)\}\right| = q^m - 1$ so $(g^t + g^{t_1})e(g) = g^i e(g)$, for some index i, $1 \leq i \leq q^m - 1$.

The same holds for $(h^s + h^{s_1})e(h)$. So

$$\begin{aligned} g^t h^s e_0 + g^{t_1} h^{s_1} e_0 =& ((g^t + g^{t_1})e(g))\widehat{h} + ((h^s + h^{s_1})e(h))\widehat{g} \\ =& g^i e(g)\widehat{h} + h^j e(h)\widehat{g} = g^i h^j e_0, \end{aligned}$$

as $\widehat{g} = g^i\widehat{g}$, and $\widehat{h} = h^i\widehat{h}$.

If one of these sums is 0, the element is in either $\langle e(g)\rangle$ or $\langle e(h)\rangle$, which is an ideal, so closed under addition.

Finally, $g^t h^s e_0 + g^i e(g)\widehat{h} = g^t e(g)\widehat{h} + h^s e(h)\widehat{g} + g^i e(g)\widehat{h} = (g^t + g^i)e(g)\widehat{h} + h^s e(h)\widehat{g} \in L$, as above. A similar argument applies to $g^t h^s e_0 + h^j e(h)\widehat{g}$. Thus L is closed under addition.

Moreover, given $0 \neq r \in \mathbb{F}_q$, we have $rL = L$. Indeed, $rg^i e(g)\widehat{h} = g^j e(g)\widehat{h}$, because $\langle e(g)\rangle$ is essential. Similarly, $rh^j e(h)\widehat{g} = h^l e(h)\widehat{g}$ and by the same argument $rg^t h^s e_0 = r(g^t e(g)\widehat{h} + h^s e(h)\widehat{g}) = g^{t_1} e(g)\widehat{h} + h^{s_1} e(h)\widehat{g} = g^{t_1} h^{s_1} e_0$.

It is clear that $gL = L$ (as well as $hL = L$) and hence L is an ideal. □.

We have the following:

Corollary 3 *The code $\mathbb{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$ is a two-weight code.*

Proof Notice that elements in $\{g^i e(g)\widehat{h}\}$ and $\{h^j e(h)\widehat{g}\}$ have the same weight and the elements in $\{g^t h^s e_0\}$ are also of constant weight, different from the previous one. □

Example 1 Consider the group ring $\mathbb{F}_3 C_8$, where C_8 denotes a cyclic group with 8 elements generated by g.

The element $e(g) = 1 + g + g^3 - g^4 - g^5 - g^7$, is an essential idempotent. In fact, the non trivial proper subgroups of C_8 are $\{1, g^2, g^4, g^6\}$ and $\{1, g^4\}$, and $e \times (1 + g^4) = 0 = e \times (1 + g^2 + g^4 + g^6), e \times \widehat{g} = 0$.

Let $\langle h\rangle$ be another cyclic group of order 8, set $e(h) = 1 + h + h^3 - h^4 - h^5 - h^7$

Notice that, since $\mathbb{F}_3 C_8 e$ is a code of length 8, and dimension 2 and $w(e(g)) = 6$, part (3) of Theorem 2.1 shows that $\mathbb{F}_3 C_8 e$ has constant weight.

Set $e_0 = e(g)\widehat{h} + e(h)\widehat{g}$ we have that $\mathbb{F}_3(C_8 \times C_8)(e(g)\widehat{h} + e(h)\widehat{g})$ is a two-weight code in $\mathbb{F}_3(C_8 \times C_8)$,

The weights of this code are given by $w(e(g)\widehat{h}) = w((1 + g + g^3 - g^4 - g^5 - g^7)(1 + h + h^2 + h^3 + h^4 + h^5 + h^6 + h^7)) = 48$, and since

$$
\begin{aligned}
&(1+g+g^3-g^4-g^5-g^7)(1+h+h^2+h^3+h^4+h^5+h^6+h^7)+\\
&+(1+g+g^2+g^3+g^4+g^5+g^6+g^7)(1+h+h^3-h^4-h^5-h^7)=\\
&2+2g+h^6+2g^3+2h-2g^4h^7+2g^3h+g^3h^2+2g^3h^3+g^3h^6\\
&+g^2h+g^2h^3-g^2h^4-g^2h^5-g^2h^7+2gh+gh^2+2gh^3+gh^6+g^2\\
&+2h^3-g^7h^2-2g^7h^4-2g^7h^5-g^7h^6-2g^7h^7+g^6h+g^6h^3-g^6h^4-g^6h^5\\
&-g^6h^7-g^5h^2-2g^5h^4-2g^5h^5-g^5h^6-2g^5h^7-g^4h^2-2g^4h^4-2g^4h^5\\
&-g^4h^6+h^2+g^6
\end{aligned}
$$

we have $w(e(g)\widehat{h}+e(h)\widehat{g})=42$.

Acknowledgements The authors are very grateful to Prof. César Polcino Milies for useful conversations while this work was done. The first author was partially supported by FAPESP Proc. 2015/09162-9. The second author was partially supported by CAPES-PROEX and CNPq Proc. 163425/2013-2. The authors are very grateful to Thiago Augusto S. Dourado for his help in the text processing.

References

1. Berman, S.D.: On the theory of group codes. Kibernetika **3**(1), 31–39 (1967)
2. Berman, S.D.: Semisimple cyclic and Abelian codes II. Kibernetika **3**, 17–23 (1967)
3. Chalom, G., Ferraz, R.A., Milies, C.Polcino: Essential idempotents and simplex codes. J. Algebra Comb. Discrete Struct. Appl. **4**(2), 181–188 (2017)
4. Chee, Y.M., Ling, S.: Constructions for q-ary constant-weight codes. IEEE Trans. Inf. Theory **53**(1), 135–146 (2007)
5. Ferraz, R.A., Polcino Milies, C., Guerreiro, M.: G-equivalence in group algebras and minimal Abelian codes. IEEE Trans. Inf. Theory **60**(1), 252–260 (2014)
6. Keralev, A., Solé, P.: Error-correcting codes as ideals in group rings. Contemporary. Math. **273**, 11–18 (2001)
7. Landrock, P., Manz, O.: Classical codes as ieals in group algebras. Des. Codes Cryptogr. **2**(3), 273–285 (1992)
8. MacWilliams, F.J.: Binary codes which are ideals in the group algebra of an Abelian group. Bell Syst. Tech. J. **49**, 987–1011 (1970)
9. Melo, F., Polcino Milies, C.: On cyclic and Abelian codes. IEEE Trans. Inf. Theory **59**(11), 7314–7319 (2013)
10. Sabin, R.E., Lomonaco, S.J.: Metacyclic error-correcting codes. Appl. Algebra Eng. Commun. Comput. **6**, 191–210 (1995)
11. Vega, G.: Determining the number of one-weight cyclic codes when length and dimension are given. Lect. Notes Comput. Sci. **4547**, 284–293 (2007)