J. Algebra Comb. Discrete Appl.
4(2) • 181–188

Received: 15 June 2015
Accepted: 22 February 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

Essential idempotents and simplex codes*

Research Article

Gladys Chalom, Raul A. Ferraz, C. Polcino Milies

Abstract: We define essential idempotents in group algebras and use them to prove that every mininmal abelian non-cyclic code is a repetition code. Also we use them to prove that every minimal abelian code is equivalent to a minimal cyclic code of the same length. Finally, we show that a binary cyclic code is simplex if and only if is of length of the form $n = 2^k - 1$ and is generated by an essential idempotent.

2010 MSC: 16S34, 20C05, 94B15

Keywords: Group code, Essential idempotent, Simplex code

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and m a positive integer. We recall that a linear code of length n over $\mathbb{F}_q$ is any proper subspace $\mathcal{C}$ of $\mathbb{F}_q^n$. Given a vector $v = (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathcal{C}$, its *shift* is the vector $v_1 = (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. A linear code $\mathcal{C}$ is *cyclic* if, for every vector $v \in \mathcal{C}$, its shift also belongs to $\mathcal{C}$. Notice that the definition implies that if a vector $v_1 = (a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ is in $\mathcal{C}$, then every vector obtained as a circular permutation of v is also in $\mathcal{C}$.

The map $\psi : \mathbb{F}_q^n \to \mathbb{F}_q[X]/\langle X^n - 1\rangle$ given by $\psi(a_0, a_1, \ldots, a_{m-2}, a_{m-1}) = a_0 + a_1X + \cdots, a_{m-2}X^{m-2} + a_{m-1}X^{m-1}$ is an isomorphism of linear spaces and it is easy to see that a code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is cyclic if and only its image $\psi(\mathcal{C})$ is an ideal of the ring $\mathbb{F}_q[X]/\langle X^n - 1\rangle$.

Since this ring is isomorphic to the group algebra of a cyclic group C, of order n, over $\mathbb{F}_q$, we can think of cyclic codes as ideals in the group algebra $\mathbb{F}_qC$.

More generally, an **abelian code** over $\mathbb{F}_q$ is any ideal in the group algebra $\mathbb{F}_qA$ of a finite abelian group A. These codes were introduced independently by S.D. Berman [1] and MacWilliams [8].

* *This work was supported by FAPESP proc. 2009/52665-0 and CNPq 300243/79-0.*
Gladys Chalom, Raul A. Ferraz; Universidade de Sao Paulo, Brazil (email: agchalom@ime.usp.br, raul@ime.usp.br).
C. Polcino Milies (Corresponding Author); Universidade de Sao Paulo and Univeersidade Federal do ABC, Brazil (email: polcino@ime.usp.br).

Since in the case when $char(\mathbb{F}) \nmid |A|$ the group algebra $\mathbb{F}A$ is semisimple and all ideals are direct sums of the minimal ones, it is only natural to study minimal abelian code - or - equivalently, primitive idempotents - and these has been done by several authors (see, for example [6], [5], [4] [9] [12] [14]). Also, Sabin and Lomonaco [15] have shown that central codes in metacyclic group algebras are equivalent to abelian codes.

In what follows, we shall show that these are not better than minimal cyclic codes. First, we prove in Corollary 2.5 that every minimal abelian non-cyclic code is a repetition code. Then, we show, in Theorem 3.3, that every minimal abelian code is equivalent to a minimal cyclic code of the same length.

Finally, in section § 4, we show that essential idempotents can be used to characterize simplex codes.

2. Basic facts

Throughout this paper all groups will be finite, and we shall always assume that the fields $\mathbb{F}$ considered are such that $char(\mathbb{F}) \nmid |G|$.

For an element α in the group algebra $\mathbb{F}G$, the *Hamming weight* of α is the number of elements in its support; i.e., if $\alpha = \sum_{g\in G} \alpha_g g$, then

$$\omega(\alpha) = |\{g \in G \mid \alpha_g \neq 0\}|.$$

Given an ideal $I \subset \mathbb{F}G$ the *weight distribution* of I is the map which assigns, to each possible weight t, the number of elements of I having weight t.

Let $H \neq \{1\}$ be a normal subgroup of a group G. Then

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

is a central idempotent of $\mathbb{F}G$ and

$$\mathbb{F}G = \mathbb{F}G \cdot \widehat{H} \oplus \mathbb{F}G \cdot (1 - \widehat{H}).$$

Remark 2.1. As shown in [11, Proposition 3.6.7] we have that $\mathbb{F}G \cdot (1 - \widehat{H}) = \Delta(G, H)$, the kernel of the natural projection $\pi : \mathbb{F}G \to \mathbb{F}[G/H]$ and it is easy to see that $\mathbb{F}G \cdot \widehat{H} \cong \mathbb{F}[G/H]$ via the map $\psi : \mathbb{F}G \cdot \widehat{H} \to \mathbb{F}[G/H]$ defined by $g \cdot \widehat{H} \mapsto gH \in G/H$.

Also, if $\alpha \in \mathbb{F}A \cdot \widehat{H}$, taking a transversal T of H in A we can rewrite α as

$$\alpha = \sum_{t\in T} \sum_{h\in H} \alpha_{th} th.$$

As $\alpha \in \mathbb{F}A \cdot \widehat{H}$, we have that

$$\alpha = \alpha\widehat{H} = \sum_{t\in T} \sum_{h\in H} \alpha_{th} th\widehat{H} = \sum_{t\in T} \sum_{h\in H} \alpha_{th} t\widehat{H}.$$

So $\alpha_{th} = \alpha_{th'}$ for every $h, h' \in H$ and, setting $\alpha_t = \alpha_{th}, \forall h \in H$ we can write

$$\alpha = |H| \sum_{t\in T} \alpha_t t\widehat{H}. \tag{1}$$

Since $\widehat{H}$ is central, it is a sum of primitive central idempotents called its *constituents*. Given a primitive idempotent e we have that either $e\widehat{H} = e$ or $e\widehat{H} = 0$, depending on wheather e is, or is not, a constituent of H.

In the first case, e is an element in the ideal $\mathbb{F}G\widehat{H}$, and thus an element α in $\mathbb{F}Ge$ is also in $\mathbb{F}G\widehat{H}$. So, it can be written as in eqution 1.

Writing $T = \{t_1, t_2, \ldots, t_d\}$ and $H = \{h_1, h_2, \ldots, h_m\}$, the explicit expression of α is

$$\alpha = \alpha_1 t_1 h_1 + \alpha_1 t_1 h_2 + \cdots + \alpha_1 t_1 h_m + \cdots + \alpha_d t_d h_1 + \alpha_d t_d h_2 + \cdots + \alpha_d t_d h_m.$$

In terms of coding theory, this means that the code given by the minimal ideal $\mathbb{F}Ge$ is a *repetition code*. We shall be interested in idempotents that are not of this type.

Definition 2.2. *A primitive idempotent e in the group algebra $\mathbb{F}G$, is an* **essential idempotent** *if $e \cdot \widehat{H} = 0$, for every subgroup $H \neq (1)$ in G.*

A minimal ideal of $\mathbb{F}G$ is called an **essential ideal** *if it is generated by an essential idempotent and* **non essential** *otherwise.*

Notice that, if e is a central idempotent, then the map $\pi : G \to Ge$, given by $\pi(g) = g \cdot e$ is a group epimorphism. We can use this map to characterize essential idempotents.

Proposition 2.3. *Let $e \in \mathbb{F}G$ be a primitive central idempotent. Then e is essential if and only if the map $\pi : G \to Ge$, is a group isomorphism.*

Proof. Let e be essential and assume, by way of contradiction, that π is not a monomorphism. Then, there exists $1 \neq g \in G$ such that $\pi(g) = ge = e$, hence also $g^i e = e$ for every positive integer i. Thus $\widehat{\langle g \rangle} \cdot e = e$, a contradiction.

Conversely, assume that e is not essential. Then, there exists $H \neq (1)$ such that $e\widehat{H} = e$. For every $h \in H$, we have that $h \cdot e = h \cdot e\widehat{H} = \widehat{H} \cdot e = e$. Hence $H \subset Ker(\pi)$ and thus π is not injective. Consequently, if π is an isomorphism, e is essential. □

Corollary 2.4. *If G is abelian and $\mathbb{F}G$ contains an essential idempotent, then G is cyclic.*

Proof. If $e \in \mathbb{F}G$ is essential, then $G \cong Ge \subset \mathbb{F}Ge$. As G is abelian, a simple component $\mathbb{F}Ge$ of $\mathbb{F}G$ is a field and Ge, being a finite subgroup contained in it, is cyclic. □

In terms of coding theory, the result above gives the following.

Corollary 2.5. *Let A be an abelian non-cyclic group. Then, for any finite field $\mathbb{F}_q$, all the minimal codes of $\mathbb{F}_q A$ are repetition codes.*

We wish to show, on the other hand, that if G is a cyclic group, then $\mathbb{F}G$ always contains an essential idempotent.

To do so, assume that G is cyclic of order $n = p_1^{n_1} \cdots p_t^{n_t}$. Then, G can be written as a direct product $G = C_1 \times \cdots \times C_t$, where C_i is cyclic, of order $p_i^{n_i}$, $1 \leq i \leq t$. Let K_i be the minimal subgroup of C_i; i.e. the unique subgroup of order p_i in C_i and denote by a_i a generator of this subgroup, $1 \leq i \leq t$. Set

$$\begin{aligned} e_0 &= (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t}) \\ &= \left(1 - \frac{(1 + a_1 + \cdots + a_1^{p_1^{n_1 - 1}})}{p_1}\right) \cdots \left(1 - \frac{(1 + a_t + \cdots + a_t^{p_t^{n_t - 1}})}{p_t}\right). \end{aligned}$$

Then e_0 is a central idempotent and we claim that it is non zero. In fact, it is easy to see that the coefficient of $a_1 \cdots a_t$ in this expression is $(-1)^t (1/p_1) \cdots (1/p_t)$ so, $e_0 \neq 0$.

Theorem 2.6. *Let G be a cyclic group. Then, a primitive idempotent $e \in \mathbb{F}G$ is essential if and only if $e \cdot e_0 = e$.*

Proof. Let $e \in \mathbb{F}G$ be essential. Then, in particular, $e\widehat{K_i} = 0$, so $e(1 - \widehat{K_i}) = e,\ 1 \leq i \leq t$. Hence

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

Conversely, if e is not essential then there exists a subgroup H of G such that $e \cdot \widehat{H} = e$. There exists a minimal subgroup $K_i \subset H$, and for this subgroup we have that $\widehat{H}(1 - \widehat{K_i}) = \widehat{H} - \widehat{H}\widehat{K_i} = 0$. Consequently $\widehat{H} \cdot e_0 = 0$. Hence:

$$e \cdot e_0 = (e \cdot \widehat{H}) \cdot e_0 = e \cdot (\widehat{H} \cdot e_0) = 0.$$

□

Remark 2.7. Notice that the previous theorem actually shows that e_0 is the sum of all the essential idempotents of $\mathbb{F}G$ and, consequently, the simple components of the ideal $\mathbb{F}Ge_0$ are precisely the essential ideals.

Since e_0 is non zero, we have the following.

Corollary 2.8. *Let G be a cyclic group and $\mathbb{F}$ a field such that $char(\mathbb{F}) \nmid |G|$. Then, $\mathbb{F}G$ always contains an essencial idempotent.*

3. The equivalence

Let $\mathbb{F}$ be a field, A be a finite abelian group such that $char(\mathbb{F}) \nmid |A|$ and $e \neq \widehat{A}$ an idempotent in $\mathbb{F}A$. Set

$$H_e = \{g \in G \mid ge = e\}. \tag{2}$$

Clearly, H_e is the unique maximal subgroup of G is such that $H_e e = e$ and it can be shown easily that $H_e = G$ if and only if $e = \widehat{G}$, the principal idempotent of $\mathbb{F}G$. Actually, H_e is the kernel of the irreducible representation associated to the simple component $\mathbb{F}G \cdot e$.

Theorem 3.1. *Let $e \neq \widehat{A}$ be a primitive idempotent of $\mathbb{F}A$ and ψ the natural projection defined in Remark 2.1. Then, the element $\psi(e)$ is an essential idempotent of $\mathbb{F}[A/H_e]$.*

Proof. Let $\mathcal{K} \neq 1$ be a non-trivial subgroup of A/H_e. Then, it is of the form $\mathcal{K} = K/H_e$ where $K \neq H_e$ is a subgroup of A containing H_e.

Let T be a transversal of H_e in K. Then

$$\widehat{K} = \frac{1}{|K|}\sum_{k \in K} k = \frac{|H_e|}{|K|}\sum_{t \in T} t\widehat{H_e} = \frac{1}{|\mathcal{K}|}\sum_{t \in T} t\widehat{H_e}.$$

As $\psi(\widehat{H_e})$=1, we have

$$\psi(\widehat{K}) = \frac{1}{|\mathcal{K}|}\sum_{t \in T} \psi(t) = \frac{1}{|\mathcal{K}|}\sum_{t \in T} tH_e = \widehat{\mathcal{K}}.$$

Then $\psi(e) \cdot \mathcal{K} = \psi(e) \cdot \psi(\widehat{K}) = \psi(e \cdot \widehat{K}) = 0$, as $K \not\subset H_e$. □

Corollary 3.2. *Let $e \neq \widehat{A}$ be a primitive idempotent of $\mathbb{F}A$. Then, the factor group A/H_e is cyclic.*

Proof. This fact follows immediately from Proposition 3.1 above and Corollary 2.4. □

Let G_1 and G_2 denote two finite groups of the same order, $\mathbb{F}$ a field, and let $\gamma : G_1 \to G_2$ be a biijection. Denote by $\overline{\gamma} : \mathbb{F}G_1 \to \mathbb{F}G_2$ its linear extension to the corresponding group algebras.

Clearly, $\overline{\gamma}$ is a Hamming isometry; i.e., elements corresponding under this map have the same Hamming weight. Ideals $I_1 \subset \mathbb{F}G_1$ and $I_2 \subset \mathbb{F}G_2$ such that $\overline{\gamma}(I_1) = I_2$ are thus equivalent, in the sense that they have the same dimension and the same weight distribution. In this case, the codes I_1 and I_2 are said to be *permutation equivalent* and were called *combinatorially equivalent* in [15].

In what follows, we will show that every minimal ideal of an abelian group algebra $\mathbb{F}A$ is permutation equivalent to a minimal ideal of the group algebra of a cyclic group of the same length.

Let A be an abelian group of order n, $\mathbb{F}$ a field, I a minimal ideal of $\mathbb{F}A$ and e be the primitive idempotent generating I. Let H_e be the subgroup defined in (2) and let C be a cyclic group of the same order n. If $H_e = A$ then $e = \widehat{A}$ and any bijection $\sigma : A \to C$ is such that $I = \mathbb{F}Ae = \mathbb{F}e$ is mapped to $\mathbb{F}C\widehat{C}$, so I is equivalent to $\mathbb{F}C\widehat{C}$.

So, assume that $H_e \neq A$. Since the order d of the factor group A/H_e is a divisor of n, there exists a unique subgroup K of C such that $|A/H_e| = |C/K| = d$ and, as they are both cyclic groups, we have that

$$A/H_e \cong C/K. \tag{3}$$

So, also

$$\mathbb{F}[A/H_e] \cong \mathbb{F}[C/K] \text{ and}$$
$$\mathbb{F}A \cdot \widehat{H_e} \cong \mathbb{F}[A/H_e] \cong \mathbb{F}[C/K] \cong \mathbb{F}C \cdot \widehat{K}.$$

Denote by $\mu : \mathbb{F}[A/H_e] \to \mathbb{F}[C/K]$ and $\theta : \mathbb{F}A \cdot \widehat{H_e} \to \mathbb{F}C \cdot \widehat{K}$ realizing these isomorphisms.

Let $a \in A$ be an element such that $\overline{a} = aH_e$ is a generator of A/H_e. Then $\{1, a, a^2, \ldots, a^{d-1}\}$ is a transversal of H_e in A and we can write

$$A = \{a^i h \mid 0 \leq i \leq d-1,\ h \in H_e\}.$$

Similarly, if $t \in C$ is such that $\overline{t} = tK = \mu(aH_e)$, it is a generator of C/K and we can write

$$C = \{t^i k \mid 0 \leq i \leq d-1,\ k \in K\}.$$

As H_e and K have the same order, we can choose a bijection $f : H_e \to K$ and define a map $\eta : A \to C$ by $\eta(a^i h) = t^i f(h)$, for all $a^i h \in A$.

Given an element $\alpha \in \mathbb{F}A \cdot \widehat{H_e}$, using formula (1) we can write it in the form

$$\alpha = |H_e| \sum_{i=0}^{d-1} \alpha_i a^i \cdot \widehat{H_e},$$

and, taking into account that $|H_e| = |K|$, we compute

$$\theta(\alpha) = \mu\left(|H_e| \sum_{i=0}^{d-1} \alpha_i \bar{a}^i\right) = |K| \sum_{i=0}^{d-1} \alpha_i t^i \widehat{K} = \sum_{i=0}^{d-1} \alpha_i t^i \left(\sum_{h \in H_e} f(h)\right).$$

Comparing the expressions of α and $\theta(\alpha)$ it is clear that the linear extension of $\eta : A \to C$ to $\mathbb{F}A$ coincides with θ on $\mathbb{F}A \cdot \widehat{H_e}$, and it is such that $\theta(\mathbb{F}A \cdot \widehat{H_e}) = \mathbb{F}C \cdot \widehat{K}$.

Notice that $\mathbb{F}A \cdot e \subset \mathbb{F}A \cdot \widehat{H_e}$ and thus e is primitive also in $\mathbb{F}A \cdot \widehat{H_e}$, so $e' = \theta(e)$ is primitive in $\mathbb{F}C \cdot \widehat{K}$.

We claim that e' is also primitive in $\mathbb{F}C$. In fact, assume that $e' = f_1 + f_2$, with f_1, f_2 orthogonal idempotents in $\mathbb{F}C$. Then $e' \cdot \widehat{K} = f_1\widehat{K} + f_2\widehat{K}$ is a decomposition of e' in $\mathbb{F}C \cdot \widehat{K}$. Hence, either $f_1\widehat{K} = 0$ and $f_2\widehat{K} = e'$ or vice-versa. So either $f_1 = f_1e' = f_1e'\widehat{K} = 0$ or, in a similar way, $f_2 = 0$.

Hence, we have shown the following.

Theorem 3.3. *Every minimal ideal in the semisimple group algebra $\mathbb{F}A$ of a finite abelian group A is permutation equivalent to a minimal ideal in the group algebra $\mathbb{F}C$ of a cyclic group C of the same order.*

It should be noted that non minimal abelian codes can actually be more convenient than the cyclic ones (see, for example, [7], [10] and [13]).

4. Binary simplex codes

Set $r = dim_{\mathbb{F}_q}\mathcal{C}$ and let $\mathcal{B} = \{v_1, v_2, \ldots, v_r\}$ be a basis of $\mathcal{C}$ over $\mathbb{F}_q$. We shall denote by $G_{\mathcal{B}}$ the generating matrix of $\mathcal{C}$; i.e. the matrix whose rows are the componentes of the vectors of $\mathcal{B}$, when written in the basis $\mathcal{B}$ of $\mathbb{F}_qC$.

We start with a very simple remark.

Lemma 4.1. *The matrix $G_{\mathcal{B}}$ contains no zero columns.*

Proof. In fact, assume that the j^{th} column of the given matrix is zero. Then, the j^{th} component of every vector in $\mathcal{C}$ is equal to 0. Take any non-zero vector $v \in \mathcal{C}$. So it has at least one component which is equal to 1. Since every shift of v is in $\mathcal{C}$, there exists a vector in $\mathcal{C}$ whose j^{th} component is equal to 1, a contradiction. □

Notice also that, if a matrix $G_{\mathcal{B}}$ has two columns, in positions i and j, say, that are equal to one another, then the i^{th} component of every vector in $\mathcal{C}$ is equal to its j^{th} component. Hence, we have shown the following.

Lemma 4.2. *The columns of a matrix $G_{\mathcal{B}}$ are pairwise different for a given basis $\mathcal{B}$ of $\mathcal{C}$, if and only if the columns of generating matrices are pairwise different, for every basis of $\mathcal{C}$.*

Set $\overline{\mathbb{F}} = \mathbb{F}_q \cdot e$. Then $\overline{\mathbb{F}}$ is an isomorphic copy of $\mathbb{F}_q$ contained in $\mathbb{F}_qC \cdot e$. Notice that, since g is a generator of C, we have that $\overline{\mathbb{F}}[ge] = \mathbb{F}_qC \cdot e$. Then, the evaluation mapping $\varphi : \overline{\mathbb{F}}[X] \to \mathbb{F}_qC \cdot e$ given by $\varphi(f) = f(ge)$, for all $f \in \overline{\mathbb{F}}[X]$, is an epimorphism and we have that

$$\mathbb{F}_qC \cdot e \cong \frac{\overline{\mathbb{F}}[X]}{Ker(\varphi)}.$$

Notice that $Ker(\varphi) = \langle h \rangle$, for some $h \in \overline{\mathbb{F}}[X]$, which is a polinomial of minimal degree having ge as a root. Since $dim_{\mathbb{F}}\mathbb{F}_qC \cdot e = dim_{\mathbb{F}_q}\mathbb{F}_qC \cdot e = r$ we have that the degree of h is precisely r and there exist coeficients $b_0, \ldots, b_{r-1}$ in $\overline{\mathbb{F}}$ such that

$$g^r e = b_{r-1}g^{r-1}e + \cdots + b_0.$$

This clearly implies that $\mathcal{B}_0 = \{e, ge, \ldots, g^{r-1}e\}$ is a basis of $\mathbb{F}_qC \cdot e$ over $\overline{\mathbb{F}}$ and also over $\mathbb{F}_q$.

Moreover, we have the following.

Theorem 4.3. *For every basis $\mathcal{B}$ of $\mathcal{C}$ the generating matrix $G_{\mathcal{B}}$ has pairwise different columns if and only if the mapping $\psi : C \to C \cdot e$ is an isomorphism.*

Proof. Notice that $\mathbb{F}_q C \cdot e$ is of dimension r over $\mathbb{F}_q$, it contains q^r elements.

Suppose, by way of contradiction, the ψ is not injective. Then, there exists an index j, $0 < j < n$, such that $e = g^j e$.

Write $e = a_0 + a_1 g + \cdots + a_{n-1} g^{n-1}$. Then $g^j e = a_0 g^j + a_1 g^{j+1} + \cdots + a_{n-1} g^{j+n-1}$.

Since $e = g^j e$, we have that $a_i = a_{i+j}$, $0 \leq i \leq n-1$, where the subindexes are taken modulo n. This shows that if G denotes the generating matrix with respect to the basis $\mathcal{B}$ then, the first column of G is equal to its j^{th} column.

Conversely, assume that ψ is an isomorphism and, by way of contradiction, that there exists a basis whose corresponding generating matrix has two equal columns, in positions i and j, say. In view of Lemma 4.2 we can assume, without loss of generality, that this basis is precisely the basis $\mathcal{B}_0$. This means that $a_{i+t} = a_{j+t}$ or, equivalently, that $a_t = a_{t+j-i}$, for all t, where indexes are taken, again, modulo n. This readily implies that $e = g^{j-i} e$. □

Recall that a binary linear code of dimension k and length n is called *simplex* if a generating matrix for the code contains all possible non zero columns of length k. Since these are $2^k - 1$ in number, this matrix must be of size $k \times (2^k - 1)$ so, we must have $n = 2^k - 1$.

Theorem 4.4. *Let $\mathcal{C}$ be a binary linear code of dimension k and length $n = 2^k - 1$. Then $\mathcal{C}$ is a simplex code if and only if it is essential.*

Proof. Assume that $\mathcal{C}$ is simplex. Since all its columns are different, it follows from Theorem 4.3 that the mapping $\psi : C \to C \cdot e$ is an isomorphism. To prove thar e is an essential idempotent we are only left to prove that it is primitive.

Notice that $C \cdot e \subset \mathbb{F}_2 C \cdot e \setminus \{0\}$. Since $\mathbb{F}_2 C \cdot e = \mathcal{C}$ is of dimension k over $\mathbb{F}_2$, it contains 2^k elements. Hence $|\mathbb{F}_2 C \cdot e \setminus \{0\}| = n = |C|$, showing that actually $C \cdot e = \mathbb{F}_2 C \cdot e \setminus \{0\}$. This means that every non zero element in $\mathbb{F}C \cdot e$ is invertible and thus, it is a field. Consequently, e is primitive. □

As a consequence, and taking the results in [3] into account, we can state the following.

Corollary 4.5. *Every binary linear code of constant weight is a repetition of a code generated by an essential idempotent.*

References

[1] S. D. Berman, Semisimple cyclic and abelian codes. II, Kibernetika 3(3) (1967) 21–30.
[2] S. D. Berman, On the theory of group codes, Kibernetika 3(1) (1967) 31–39.
[3] A. Bonisoli, Every equidistant linear code is a sequence of dual Hamming codes, Ars Combin. 18 (1984) 181–186.
[4] R. A. Ferraz, M. Guerreiro, C. P. Milies, $G-$equivalence in group algebras and minimal abelian codes, IEEE Trans. Inform. Theory 60(1) (2014) 252–260.
[5] R. A. Ferraz, C. P. Milies, Idempotents in group algebras and minimal abelian codes, Finite Fields Appl. 13(2) (2007) 382–393.
[6] P. Grover, A. K. Bhandari, Explicit determination of certain minimal abelian codes and their minimum distance, Asian–European J. Math. 5(1) (2012) 1–24.
[7] J. Jensen, The concatenated structure of cyclic and abelian codes, IEEE Trans. Inform. Theory 31(6) (1985) 788–793.
[8] F. J. Mac Williams, Binary codes which are ideals in the group algebra of an abelian group, Bell System Tech. J. 49(6) (1970) 987–1011.

[9] R. L. Miller, Minimal codes in abelian group algebras, J. Combinatorial Theory Ser A 26(2) (1979) 166–178.
[10] C. P. Milies, F. D. de Melo, On cyclic and abelian codes, IEEE Trans. Information Theory 59(11) (2013) 7314–7319.
[11] C. Polcino Milies, S. K. Sehgal, An Introduction to Group Rings, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.
[12] A. Poli, Construction of primitive idempotents for a variable codes, Applied Algebra, Algorithmics and Error–Correcting Codes: 2nd International Conference, AAECC–2 Toulouse, France, October 1–5, 1984 Proceedings (1986) 25–35.
[13] R. E. Sabin, On minimum distance bounds for abelian codes, Appl. Algebra Engrg. Comm. Comput. 3(3) (1992) 183–197.
[14] R. E. Sabin, On determining all codes in semi–simple group rings, Applied Algebra, Algebraic Algorithms and Error–Correcting Codes: 10th International Symposium,AAECC-10 San Juan de Puerto Rico, Puerto Rico, May 10–14, 1993 Proceedings (1993) 279–290.
[15] R. E. Sabin, S. J. Lomonaco, Metacyclic error–correcting codes, Appl. Algebra Engrg. Comm. Comput. 6(3) (1995) 191–210.