Divisibility of weights for ideals in group algebras

Javier de la Cruz
Universidad del Norte, Barranquilla, Colombia
and
Wolfgang Willems
Otto-von-Guericke Universität, Magdeburg, Germany
and Universidad del Norte, Barranquilla, Colombia

Dedicated to Pham Huu Tiep on the occasion of his 60th birthday.

Keywords. Group code, weight, divisor, monomial kernel
MSC classification. 94B05, 20C05

Abstract

In this short note we clarify some questions on the greatest common divisor of all weights of a group code. In particular we discuss Ward's condition (E) in [10], and extend a result of Damgård and Landrock on the principal block to self-dual blocks. Furthermore, we give an upper bound for the dimension of a group code in terms of its monomial kernel.

1 Introduction

Throughout this paper let $\mathbb{F} = \mathbb{F}_q$ be a finite field of size q and characteristic p, and let G be a finite group. By a *group code* C, we always mean a right ideal in a group algebra $\mathbb{F}G$ and denote this property by $C \leq \mathbb{F}G$. To look only at right ideals is just for convention. Everything holds equally true for left ideals. If we want to specify the group G and the field $\mathbb{F}$, we also say that C is a *G-code over* $\mathbb{F}$. For $a = \sum_{g\in G} a_g g \in \mathbb{F}G$ ($a_g \in \mathbb{F}$ are called the *coordinates* of a), the *weight* $\mathrm{wt}(a)$ of a is defined by

$$\mathrm{wt}(a) = |\{g \in G \mid a_g \neq 0\}|.$$

Note that $C \neq 0$ has no 0 coordinate, i.e., for each $g \in G$, there exists $c \in C$ with $c_g \neq 0$. We endow $\mathbb{F}G$ with the symmetric non-degenerate bilinear form $\langle \cdot\,, \cdot \rangle$ given by

$$\langle \sum_{g\in G} a_g g, \sum_{g\in G} b_g g \rangle = \sum_{g\in G} a_g b_g \text{ for } a_g, b_g \in \mathbb{F}.$$

For a right $\mathbb{F}G$-module C, the dual space $C^* = \mathrm{Hom}_{\mathbb{F}}(C, \mathbb{F})$ carries the structure of a right $\mathbb{F}G$-module via

$$c(\alpha g) = (cg^{-1})\alpha,$$

where $c \in C, g \in G$ and $\alpha \in C^*$. We call C^* the *dual module* of C. Note that $\mathbb{F}G/C^{\perp} \cong C^*$ as $\mathbb{F}G$-modules ([13], Proposition 2.3).

Finally, let $\hat{}: \mathbb{F}G \longrightarrow \mathbb{F}G$ denote the $\mathbb{F}$-algebra anti-automorphism of $\mathbb{F}G$ defined by $g \mapsto g^{-1}$ for $g \in G$.

Definition 1.1 [2] Let $C \leq \mathbb{F}G$ be a group code.

a) The *kernel* $K(C)$ of C is defined by

$$K(C) = \{g \in G \mid cg = c \text{ for all } \ c \in C\}.$$

Thus $K(C)$ is the largest subgroup of G which acts trivially on C.

b) The *monomial kernel* $K_M(C)$ of C is defined by

$$K_M(C) = \{g \in G \mid gc = a(g)c \text{ with } a(g) \in \mathbb{F} \text{ for all } \ c \in C\}.$$

Observe that $K_M(C)$ is defined via a left action of G on C. Also note that $K(C)$ is a normal subgroup of G, but $K_M(C)$ is in general only a subgroup.

Recall that a linear code C is r-divisible for $r \in \mathbb{N}$ if $r \mid \mathrm{wt}(c)$ for all $c \in C$. In the following, we denote by $\Delta(C)$ the greatest common divisor of all weights of codewords in C. Usually, $\Delta(C)$ is called the *divisor* of C and has been intensively studied by H. Ward (see [9], [10], [11]). For a survey, the reader is also referred to ([14], Section 8).

If C is a G-code over $\mathbb{F}_q$ of dimension $k \geq 1$, then the average weight equation says that

$$\sum \mathrm{wt}(c) = |G|q^{k-1},$$

where the sum runs over representatives of all 1-dimensional subspaces of C (see for instance ([12], Lemma 4.5.1)). Thus $\Delta(C)_{p'} \mid |G|$.

Example 1.2 Let C be the $[\frac{q^k-1}{q-1}, k, q^{k-1}]$ simplex code over $\mathbb{F} = \mathbb{F}_q$ where $k \geq 2$ and $\gcd(k, q-1) = 1$. Then C is a group code in $\mathbb{F}G$ with G cyclic of order $\frac{q^k-1}{q-1}$. Moreover, $\Delta(C) = \Delta(C)_p = q^{k-1}$, but $\Delta(C) \nmid |G| = \frac{q^k-1}{q-1}$.

The p'-part of the divisor $\Delta(C)$ of a group code C can be determined by the monomial kernel $K_M(C)$ of C as follows. Note that Theorem 1.3 generalizes Theorem 3 of [11].

Theorem 1.3 ([2], Theorem 3.2) *Let* $\mathrm{char}\, \mathbb{F} = p$ *and* $0 \neq C \leq \mathbb{F}G$ *be a group code. Then the following two conditions hold true.*

a) $|K_M(C)|$ *divides* $\Delta(C)$*.*

b) $|K_M(C)|_{p'} = \Delta(C)_{p'}$*.*

The determination of the p-part $\Delta(C)_p$ of the divisor $\Delta(C)$ seems to be more subtle (see [7], [4], [10]). In order to state a crucial result of Ward on $\Delta(C)_p$ we need the following.

Condition (E) We say that a group code $C \leq \mathbb{F}G$ satisfies condition (E) if the following holds true. Whenever $f \in C^* = \mathrm{Hom}_{\mathbb{F}}(C, \mathbb{F})$, then there exists $\eta \in \mathrm{End}_{\mathbb{F}G}(C)$ such that $f(c) = \langle c\eta, 1\rangle$ for all $c \in C$.

Theorem 1.4 ([10], Theorem 4.4) *Let* $C = e\mathbb{F}_pG$ *where* p *is a prime and* $e = e^2 \neq 0$*. Suppose that* C *satisfies condition* (E)*. Then* $\Delta(C)_p = p^{r-1}$*, where* r *is the least positive integer for which* C *has a nontrivial* G*-invariant multilinear form* f *of degree* $r(p-1)$*, i.e.,* $0 \neq f \in \mathrm{Hom}_{\mathbb{F}G}(C^{\otimes r(p-1)}, \mathbb{F}_p)$ *where* $C^{\otimes r(p-1)} = C \otimes \cdots \otimes C$ *(*$r(p-1)-$*times).*

Note that $C = e\mathbb{F}_pG$ with $e = e^2$ is equivalent to Ward's condition (D) in [10].

There also exists a version of Theorem 1.4 over extension fields. For the exact statement we refer the reader to [10].

The paper is organized as follows. In section 2 we characterize all group codes which satisfy condition (E). It turns out that for group codes $C \leq \mathbb{F}G$ the condition (E) holds true if and only if C is a 2-sided ideal in $\mathbb{F}G$ (Theorem 2.2). As a consequence a projective cover P_0 of the trivial module inside $\mathbb{F}G$ satisfies (E) if and only if G is p-nilpotent (Theorem 2.4). Section 3 mainly deals with the divisor of a group code. In Theorem 3.2 we extend a result of Damgård and Landrock on the principal block to self-dual blocks provided the underlying field is the prime field. In characteristic 2 we completely determine the divisor $\Delta(P_0)$ (Theorem 3.5). In the last section we prove for group codes $C \leq \mathbb{F}G$ a counterpart of $|G| \leq \mathrm{d}(C)\dim C$ ([1], Corollary 2.6). More precisely we show that $|G| \geq |K_M(C)| \dim C$.

2 Ward's condition (E)

In this section we characterize group codes which satisfy condition (E).

Lemma 2.1 *If* $C \leq \mathbb{F}G$ *is a group code, then* $\dim \mathrm{End}_{\mathbb{F}G}(C) \leq \dim C$*.*

Proof: For $\eta \in \mathrm{End}_{\mathbb{F}G}(C)$, we define $f_\eta \in C^*$ by $f_\eta(c) = \langle c\eta, 1\rangle$ for $c \in C$. Suppose that $\langle c\eta, 1\rangle = \langle c\eta', 1\rangle$ for some $\eta' \in \mathrm{End}_{\mathbb{F}G}(C)$ and all $c \in C$. Since

$$\langle c\eta, g^{-1}\rangle = \langle (c\eta)g, 1\rangle = \langle (cg)\eta, 1\rangle = \langle (cg)\eta', 1\rangle = \langle c\eta', g^{-1}\rangle$$

for all $g \in G$, we obtain

$$\langle c\eta, a\rangle = \langle c\eta', a\rangle$$

for all $a \in \mathbb{F}G$. Thus $c\eta = c\eta'$ for all $c \in C$, which implies $\eta = \eta'$. This shows that the map $\eta \mapsto f_\eta$ is injective. Hence

$$\dim \operatorname{End}_{\mathbb{F}G}(C) \leq \dim C^* = \dim C.$$

$\square$

Theorem 2.2 *If $C \leq \mathbb{F}G$ is a group code, then the following conditions are equivalent.*

a) $\dim C = \dim \operatorname{End}_{\mathbb{F}G}(C)$.

b) C satisfies (E).

c) C is a 2-sided ideal in $\mathbb{F}G$.

Proof: a) $\Longrightarrow$ b) In the proof of Lemma 2.1 we have seen that the map

$$\alpha : \operatorname{End}_{\mathbb{F}G}(C) \ni \eta \mapsto f_\eta \in C^*$$

defined by $f_\eta(c) = \langle c\eta, 1\rangle$ is injective. Thus, by assumption in a), α is an $\mathbb{F}$-linear isomorphism, which says that C satisfies (E).
b) $\Longrightarrow$ c) For $g \in G$, we define $f_g \in C^*$ by

$$f_g(c) = \langle gc, 1\rangle,$$

for $c \in C$. By the assumption in b), there exists $\eta_g \in \operatorname{End}_{\mathbb{F}G}(C)$ such that

$$\langle gc, 1\rangle = \langle c\eta_g, 1\rangle,$$

for all $c \in C$. Again, since C is a right ideal, we get

$$\langle gc, h^{-1}\rangle = \langle gch, 1\rangle = \langle (ch)\eta_g, 1\rangle = \langle (c\eta_g)h, 1\rangle = \langle c\eta_g, h^{-1}\rangle,$$

hence

$$gc = c\eta_g \in C$$

for all $g \in G$ and all $c \in C$. Thus C is a 2-sided ideal in $\mathbb{F}G$.
c) $\Longrightarrow$ a) Let $\alpha : \mathbb{F}G \longrightarrow \operatorname{End}_{\mathbb{F}G}(C)$ be defined by $\mathbb{F}G \ni a \mapsto \alpha_a$ with $c\alpha_a = ac$ for $c \in C$. Clearly, $\operatorname{Ker}(\alpha) = \operatorname{Ann}_l(C)$, where $\operatorname{Ann}_l(C)$ denotes the left annihilator of C, i.e.,

$$\operatorname{Ann}_l(C) = \{a \in \mathbb{F}G \mid ac = 0 \text{ for all } c \in C\}.$$

A well-known result of MacWilliams [6] says that

$$\widehat{\operatorname{Ker}(\alpha)} = \widehat{\operatorname{Ann}_l(C)} = C^\perp.$$

It follows that

$$\dim \mathbb{F}G/C^\perp = \dim \mathbb{F}G/\operatorname{Ann}_l(C) \leq \dim \operatorname{End}_{\mathbb{F}G}(C) \leq \dim C,$$

by Lemma 2.1. On the other hand, as mentioned in the introduction, we have

$$\dim \mathbb{F}G/C^{\perp} = \dim C^* = \dim C,$$

which proves the condition in a). $\square$

For an $\mathbb{F}G$-module V, we denote by $\mathrm{Soc}(V)$ the socle of V, i.e., the largest completely reducible $\mathbb{F}G$-submodule of V.

Proposition 2.3 *Let $C \leq \mathbb{F}G$ be a group code. If C satisfies* (E)*, then* $\mathrm{Soc}(C)$ *contains all composition factors of C up to isomorphism.*

Proof: Let X be an irreducible $\mathbb{F}G$-module which occurs as a composition factor of C. We choose a composition series

$$C = V_1 > \cdots > V_n > 0$$

of C with $V_i/V_{i+1} \cong X$, for some i. Now let $f \in C^*$ with V_{i+1} in the kernel of f, but $0 \neq f$ on V_i. Since C satisfies (E) there exists $\eta \in \mathrm{End}_{\mathbb{F}G}(C)$ such that

$$f(c) = \langle c\eta, 1\rangle,$$

for all $c \in C$. It follows that V_{i+1} is in the kernel of η, but V_i is not. This means that η maps C on a submodule of C whose socle contains X. $\square$

In the rest of this note let $P_0 \leq \mathbb{F}G$ be the projective cover of the principal indecomposable module with trivial head. Note that P_0 is unique only up to isomorphism. But every projective cover P_0 contains the trivial ideal $\mathbb{F}(\sum_{g\in G} g)$.

Theorem 2.4 *If P_0 is the projective cover of the trivial module in $\mathbb{F}G$, then the following are equivalent.*

a) *P_0 satisfies condition* (E).

b) *G is p-nilpotent.*

Proof: *a)* $\Longrightarrow$ *b)* By Theorem 2.2, the module P_0 is the principal p-block. Hence this block contains only one irreducible module. Thus, by ([5], Chap. VII, Theorem 14.9), the group G must be p-nilpotent.
b) $\Longrightarrow$ *a)* We put $H = \mathrm{O}_{p'}(G)$ and $e = \frac{1}{|H|}\sum_{h\in H} h$. Note that $e = e^2$ and e lies in the center of $\mathbb{F}G$. Furthermore $\mathbb{F}G = e\mathbb{F}G \oplus (1-e)\mathbb{F}G$ and $P_0 \cong P = e\mathbb{F}G \cong \mathbb{F}(G/H)$ is the principal p-block of $\mathbb{F}G$, since $G = HT$ with T a Sylow p-subgroup of G. Thus P is an algebra and it follows that $\dim P = \dim \mathrm{End}_{\mathbb{F}G}(P)$. By Theorem 2.2, we get the assertion in a). $\square$

Example 2.5 Let $G = \mathrm{A}_4$ and let $\mathbb{F} = \mathbb{F}_3$. Then G is 3-nilpotent and by Theorem 2.4, the projective cover of the trivial module satisfies (E). Furthermore $\mathbb{F}G$ contains an absolutely irreducible projective submodule V of dimension 3, which is a direct summand of $\mathbb{F}G$. Since $\dim \mathrm{End}_{\mathbb{F}G}(V) = 1$, we see that V does not satisfy (E).

3 Divisibility of projective group codes

Recall that the characteristic of $\mathbb{F}$ is always p.

Theorem 3.1 [2] *If B_0 denotes the principal p-block of $\mathbb{F}G$, then $\Delta(B_0) = |\mathrm{O}_{p'}(G)|$.*

Note that $\mathrm{O}_{p'}(G) = K_M(B_0)$: This can be seen as follows. By a result of Brauer [5, Chap. VII, Theorem 14.8], we have $K(B_0) = \mathrm{O}_{p'}(G)$. Thus $K_M(B_0)$ is a p'-group, since $K(B_0) \leq K_M(B_0)$ and obviously $p \nmid |K_M(B_0)/K(B_0)|$. The claim now follows by the fact that $K_M(B_0)$ is a normal subgroup of G as B_0 is a 2-sided ideal.

We can extend this result to self-dual blocks over prime fields. Note that B_0 is always self-dual, since the trivial module is obviously self-dual.

Theorem 3.2 *Let B be a self-dual block over the prime field $\mathbb{F} = \mathbb{F}_p$. Then $\Delta(B) = |K_M(B)| = |K_M(B)|_{p'}$, except $p = 2$ and $B \neq B_0$ for which we have $\Delta(B) = 2|K_M(B)|$.*

Proof: First note that $|K_M(B)|$ is a p'-group since $|K_M(B)/K(B)|$ is prime to p and $K(B)$ is a p'-group by ([5], Chap. VII, Theorem 14.7). First we assume that p is odd, hence $p-1$ is even. Since $B = B^*$ we get $\mathrm{Hom}_{\mathbb{F}G}(B \otimes B, \mathbb{F}) \cong \mathrm{Hom}_{\mathbb{F}G}(B, B^*) \neq 0$. Thus $B \otimes B$ carries a nonzero G-invariant bilinear form. Consequently, since $p-1$ is even, $B^{\otimes(p-1)}$ has a nonzero G-invariant multilinear form. Observe that B satisfies condition (D) since a block is generated by an idempotent, and condition (E) by Theorem 2.2. Thus by ([10], Theorem 4.4), we get $\Delta(B)_p = 1$ and we are done. Now let $p = 2$. If $B = B_0$, then we are also done by Theorem 3.1, since B_0 contains P_0. If $B \neq B_0$, then $\Delta(B)_2 = 2$ as $\mathrm{Hom}_{\mathbb{F}G}(B, \mathbb{F}) = 0$. We conclude the proof by applying Theorem 1.3. $\square$

Note that Theorem 3.2 implies Theorem 3.1 since field extensions take the principal block over a small field to the principal block over field extensions.

Lemma 3.3 *We have $P_0 = e\mathbb{F}G$ for some $e = e^2 = \widehat{e}$.*

Proof: Since P_0 is a projective $\mathbb{F}G$-module, we have $P_0 = e\mathbb{F}G$ with $e = e^2$. Suppose that $P_0 \cap P_0^\perp \neq 0$. Since this is a right ideal we obtain $\sum_{g \in G} g \in P_0 \cap P_0^\perp$. It follows that $e\sum_{g\in G} g = 0$. Since $1 = e + (1-e)$, we get $\sum_{g\in G} g = (1-e)\sum_{g\in G} g \in (1-e)\mathbb{F}G$. That means that $\mathbb{F}G$ has at least two different irreducible submodules isomorphic to the trivial module, a contradiction. Hence P_0 is an LCD group code, which implies $e = \hat{e}$, by ([3], Theorem 3.1). $\square$

Proposition 3.4 *We have $K_M(P_0) = \mathrm{O}_{p'}(G)$. In particular, $\Delta(P_0)_{p'} = |\mathrm{O}_{p'}(G)|$.*

Proof: By ([5], Chap. VII, Theorem 14.6 and 14.7), $\mathrm{O}_{p'}(G)$ is the largest subgroup of G which acts trivially from the right on P_0. According to Lemma 3.3, we have $P_0 = e\mathbb{F}G$ for some $e = e^2 = \hat{e}$. We put

$$K_I(P_0) := \{g \in G \mid gx = x \text{ for all } x \in P_0 = e\mathbb{F}G\} = \{g \in G \mid xg = x \text{ for all } x \in \mathbb{F}Ge = \widehat{P_0}\}.$$

But $\mathbb{F}Ge$ is the projective cover of the trivial left $\mathbb{F}G$-module. Thus, again by ([5], Chap. VII, Theorem 14.6 and 14.7), $K_I(P_0) = \mathrm{O}_{p'}(G)$.

Now let $g \in K_M(P_0)$. Then

$$gx = a(g)x$$

for all $x \in P_0$, where $a(g) \in \mathbb{F}^*$. If we take $v = \sum_{h \in G} h \in P_0$, then

$$v = gv = a(g)v.$$

Thus $a(g) = 1$, which shows that $K_M(P_0) = K_I(P_0)$. It follows that $K_M(P_0) = \mathrm{O}_{p'}(G)$. Finally, by Theorem 1.3, we obtain $\Delta(P_0)_{p'} = |\mathrm{O}_{p'}(G)|$.

□

In characteristic 2 we are able to determine the divisor of P_0.

Theorem 3.5 *For $p = 2$, we have $\Delta(P_0)_2 = 1$. In particular, $\Delta(P_0) = |\mathrm{O}_{2'}(G)|$.*

Proof: Recall that $P_0 = e\mathbb{F}G$ with $e^2 = e = \hat{e}$, according to Lemma 3.3. Clearly,

$$\langle e, e \rangle = \langle e\hat{e}, 1 \rangle = \langle e, 1 \rangle.$$

By ([3], Proposition 3.6), we have $\langle e, 1 \rangle = 1_{\mathbb{F}}$. Suppose for a moment that $\mathbb{F} = \mathbb{F}_2$ is the prime field. Thus $\mathrm{wt}(e)$ is odd since

$$\mathrm{wt}(e)1_{\mathbb{F}} = \langle e, e \rangle.$$

This implies $\Delta(P_0)_2 = 1$ for any projective cover of the trivial module over the binary field $\mathbb{F}_2$.

Now let P_0 be the projective cover of the trivial module over $\mathbb{F}$, where $\mathbb{F}$ is a finite extension field of $\mathbb{F}_2$. Clearly, $P_0|_{\mathbb{F}_2 G}$, which is P_0 considered as an $\mathbb{F}_2 G$-module, is projective and contains the module $T = (\sum_{g \in G} g)\mathbb{F}_2$. Thus $P_0|_{\mathbb{F}_2 G}$ contains a projective cover, say P_0', of T over $\mathbb{F}_2$. Hence, by the above, we get

$$\Delta(P_0)_2 \mid \Delta(P_0')_2 = 1.$$

Applying Proposition 3.4, we obtain $\Delta(P_0) = |\mathrm{O}_{2'}(G)|$, where P_0 is the projective cover of the trivial module over any finite field of characteristic 2. □

Note that $2 \mid \Delta(P)$ if $P_0 \neq P \leq \mathbb{F}_2 G$ where P is projective indecomposable. This follows immediately from the fact that P is contained in the kernel of the augmentation epimorphism which is equal to the even weight subspace of $\mathbb{F}_2 G$.

Question 3.6 What can we say about $\Delta(P_0)_p$ for p odd? Note that in general P_0 does not satisfy (E). Even for p-solvable groups we do not know that for any P_0 we always have $\Delta(P_0)_p = 1$.

Recall that, according to Massey [8], a linear code C in $\mathbb{F}^n$ is called an LCD code (linear complementary dual) if $C \oplus C^\perp = \mathbb{F}^n$.

Proposition 3.7 *Let $\mathbb{F} = \mathbb{F}_2$ or $\mathbb{F} = \mathbb{F}_3$, hence $p = 2$ or $p = 3$. Let* C $\leq \mathbb{F}G$ *be an* LCD *group code. If $p \mid \Delta(C)$, then $p \nmid \Delta(C^\perp)$.*

Proof: Note that $C = e\mathbb{F}G$ with $e^2 = e = \hat{e}$ and $C^\perp = (1-e)\mathbb{F}G$, by ([3], Theorem 3.1). Furthermore, we have

$$\mathrm{wt}(e)1_{\mathbb{F}} = \langle e, e\rangle = \langle e\hat{e}, 1\rangle = \langle e, 1\rangle.$$

Thus if $p \mid \Delta(C)$, then $p \mid \mathrm{wt}(e)$, hence $\langle e, 1\rangle = 0$. It follows that $1 \in \mathrm{supp}(1-e)$. Consequently $\mathrm{wt}(1-e)1_{\mathbb{F}} \neq 0$, which shows that $p \nmid \mathrm{wt}(1-e)$. In particular $p \nmid \Delta(C^\perp)$. □

4 An upper bound for $\dim C$ in terms of $|K_M(C)|$

Let $0 \neq C \leq \mathbb{F}G$ be a group code with minimum distance $\mathrm{d}(C)$. In [1] we proved

$$|G| \leq \mathrm{d}(C)\dim C,$$

by using an uncertainty principle. This may be seen as a lower bound for $\dim C$ in terms of $\mathrm{d}(C)$. Suppose that we have equality. By ([1], Theorem 2.10), this holds true exactly if and only if there exists $H \leq G$ such $C = c\mathbb{F}G$ with $c \in \mathbb{F}H$ and $\dim c\mathbb{F}H = 1$. Furthermore, $\mathrm{d}(C) = |H| = \mathrm{wt}(c)$. At the end of the proof of Theorem 2.10 it is shown that in the case $|G| = \mathrm{d}(C)\dim C$ we have

$$C = \oplus_{i=1}^{\dim C}(c\mathbb{F}H)g_i.$$

Thus $\mathrm{d}(C) = \Delta(C)$. Next we claim that $C_0 = c\mathbb{F}H$ is also a left ideal in $\mathbb{F}H$. Suppose that for $g \in H$ we have $gC_0 \neq C_0$. It follows that

$$\mathbb{F}H = P(C_0) \oplus P(gC_0) \oplus ....$$

where $P(X)$ denotes the projective cover of $X \leq \mathbb{F}H$ as a right module. Clearly $P(C_0) \cong P(gC_0)$ since $C_0 \cong gC_0$ are isomorphic as right $\mathbb{F}H$-modules. On the other hand, the multiplicity of $P(C_0)$ in $\mathbb{F}H$ is 1 since $\dim C_0 = 1$, a contradiction. This shows that C_0 is a left ideal in $\mathbb{F}H$. It follows $H \leq K_M(C)$. Now Theorem 1.3 tells us that $|K_M(C)|$ divides $\Delta(C) = |H|$. Thus $H = K_M(C)$.

Theorem 4.1 *If $C \leq \mathbb{F}G$, then $|K_M(C)|\dim C \leq |G|$.*

Proof: Note that $K_M(C)$ acts monomially from the left on C. Write $G = \cup_{i=1}^t K_M(C)g_i$ with distinct right cosets. Let C_i be the projection of C into $\mathbb{F}K_M(C)g_i$ with kernel $\oplus_{j\neq i}\mathbb{F}K_M(C)g_j$. If $c \in C$, then $c = (c_1, \ldots, c_t)$ with $c_i \in C_i$. Let $c_i = (c_x)_{x\in K_M(C)g_i}$. Since $g \in K_M(C)$ acts monomially from the left on C_i we get

$$c_{g^{-1}x} = \alpha(g)c_x$$

for $g \in K_M(C)$. In particular, either $c_i = 0$ or $\mathrm{wt}(c_i) = |K_M(C)|$. Next we claim that $\dim C_i \leq 1$. Suppose that $c_i \neq 0 \neq c_i' \in C_i$. For $g \in K_M(C)$, we obtain

$$c_{g^{-1}g_i} = \alpha(g)c_{g_i} = \alpha(g)\mu c'_{g_i} = \mu c'_{g^{-1}g_i}$$

for some $\mu \in \mathbb{F}^*$. Thus $c_i = \mu c_i'$ which shows that $\dim C_i \leq 1$. Consequently $\dim C \leq t = |G : K_M(C)|$, hence $|K_M(C)| \dim C \leq |G|$. $\square$

Suppose that $|K_M(C)| \dim C = |G|$. Thus, by using the notation of the proof of Theorem 4.1, we have $t = \dim C = |G : K_M(C)|$ and $C = C_1 \oplus \cdots \oplus C_t$ with $\dim C_i = 1$ and $\mathrm{d}(C_i) = |K_M(C)| = \mathrm{d}(C)$. It follows that $\mathrm{d}(C) \dim C = |G|$. Conversely, suppose that $\mathrm{d}(C) \dim C = |G|$. If $|K_M(C)| \dim C < |G|$ we have $\dim C < |G : K_M(C)|$, hence $C_i = 0$ for some i by the proof of Theorem 4.1. This contradicts $C \neq 0$ and the transitive action of G from the right. Thus we have shown that $|K_M(C)| \dim C = |G|$ if and only if $\mathrm{d}(C) \dim C = |G|$.

Remark 4.2 Let $0 \neq C \leq \mathbb{F}G$ and let $K = K_M(C) \neq 1$. If $\mathrm{d}(C) < |G| \left(\frac{|K|-1}{|K|} \right) + 1$, then the upper bound on $\dim C$ in Theorem 4.1 is stronger than the bound given by the Singleton bound

$$\mathrm{d}(C) + \dim C - 1 \leq |G|.$$

To see this we have to show that $\frac{|G|}{|K|} < |G| - \mathrm{d}(C) + 1$. This inequality is equivalent to $\frac{|K|-1}{|K|} > \frac{\mathrm{d}(C)-1}{|G|}$ which holds true by the assumption.

References

[1] M. Borello, W. Willems and G. Zini, On ideals in group algebras: an uncertainty principle and the Schur product, to appear Forum Mathematicum 2023. arXiv:2202.12621.

[2] I. Damgård and P. Landrock, Ideals and codes in group algebras, *Aarhus Preprint Series*, (1986).

[3] J. de la Cruz and W. Willems, On group codes with complementary duals, *Des. Codes and Cryptogr.* 86 (2018), 2065-2073.

[4] P. Delsarte and R. J. McEliece, Zeros of functions in finite abelian group algebras, *Amer. J. Math.* 98 (1976), 197-224.

[5] B. Huppert and N. Blackburn, *Finite Groups II*, Springer, Berlin 1982.

[6] F.J. MacWilliams, Codes and ideals in group algebras, *Combinatorial Mathematics and Appl., Proceedings, Eds. R. C. Bose and T. A. Dowing*, 317-328 (1967).

[7] R.J. McElies, Weight congruences of p-ary cyclic codes, *Discrete Math.* 3 (1972), 1972.

[8] J.L. Massey, Linear codes with complementary duals, *Discrete Math.* 106/107 (1992), 337-342.

[9] H. Ward, Divisible codes, *Archiv der Mathematik* 36 (1981), 485-494.

[10] H. Ward, Multilinear forms and divisors of codeword weights, *Quart. J. Math. Oxford* 34 (1983), 115-128.

[11] H. Ward, Divisible codes - a survey, *Serdicia Math. J.* 27 (2001), 263-278.

[12] W. Willems, *Codierungstheorie*, de Gruyter, Berlin 1999.

[13] W. Willems, A note on self-dual group codes, *IEEE Trans. Inform. Theory* 48 (2007), 3107-3109.

[14] W. Willems, Codes in group algebras, Chap. 16 in *Concise Encyclopidia of Coding Theory*, Eds. W. C. Huffman, J.-L. Kim and P. Solé, CRC Press, Boca Raton 2021.