Around LCD Group Codes

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 the memory of Kai-Uwe Schmidt

Keywords. Group code · LCD code · MDS code · projective module · almost LCD code · divisor of a code

MSC classification. 94B05 · 94B15 · 20C05

Abstract

In this note we answer some questions on LCD group codes posed in [4] and [5]. Furthermore, over prime fields we determine completely the p-part of the divisor of an LCD group code. In addition we present a natural construction of almost LCD codes.

1 Introduction

Throughout this note let K always denote a finite field, i.e., $K = \mathbb{F}_q$ where q is a power of a prime p. According to Massey [9], a linear code $C \leq K^n$ is called an LCD code if $K^n = C \oplus C^{\perp}$. Like self-dual codes, LCD codes are of particular interest since they play a crucial role not only in error correction but also in information protection [2].

Many of the well-known good linear codes can be described as group codes, or more precisely as G-codes, i.e., as right ideals in a group algebra KG where G is a finite group. For more information on group codes, the reader is referred to the survey article [12].

In this note we may look more closely on LCD group codes. A complete characterization of such codes has been given in [4]. More precisely, a group code C, denoted by $C \leq KG$, is an LCD code if and only if $C = eKG$ with $e^2 = e = \widehat{e}$ where $\widehat{\ }$ is the K-linear map on KG which inverts the group elements $g \in G$.

In what follows we continue our investigation on LCD group codes, in particular on those which are also MDS codes. Note that LCD MDS codes are somehow optimal when

*The author is supported by Leading House for the Latin American Region, University of St. Gallen, Switzerland. email: jdelacruz@uninorte.edu.co

†Corresponding author; email: willems@ovgu.de

used in the protection of information against side-channel or fault injection attacks [2]. Furthermore, we completely determine the p-part of the divisor of an LCD group code over a prime field which is the greatest common divisor of all weights. Essentially, we answer some open questions posed in [4] and [5] for LCD codes and present a method to construct nearly LCD codes, i.e., group codes C for which $C \cap C^{\perp}$ is an irreducible KG-module.

To a large extend the methods which we use are from representation theory of finite groups. The basics can be found in [12] or [8, Chap. VII]. Throughout the paper group codes are always right ideals and KG-modules right KG-modules.

2 LCD MDS group codes

LCD MDS group codes seem to be rather rare. If such a code exists, then the ambient space KG has to be semisimple in the case that G is abelian [4, Lemma 4.4]. We extend this result to arbitrary finite groups in the case that the underlying field is $\mathbb{F}_2$.

In the following we call a group code $C \leq KG$ *non-trivial* if $0 \neq C \neq KG$.

Definition 2.1 (H. Ward [10]) For a code C, the divisor $\Delta(C)$ of C is defined as the greatest common divisor of all weights of C.

The first result answers Question 4.6 of [4] in the case of a binary field $\mathbb{F}_2$. Unfortunately we do not know what happens if the underlying field is a proper extension of $\mathbb{F}_2$ or if it is of odd characteristic.

Theorem 2.2 *If $C \leq \mathbb{F}_2G$ is a non-trivial* LCD MDS *group code, then $|G|$ is odd, i.e., $\mathbb{F}_2G$ is a semisimple algebra.*

Proof: Suppose that $2 \mid |G|$. According to [4], the code C is a projective $\mathbb{F}_2G$-module, hence a direct sum of indecomposable projective $\mathbb{F}_2G$-modules, which are uniquely determined up to isomorphism, by the Krull-Schmidt Theorem (see for instance [1, Chap. II, Theorem 3]).

We first assume that C does not contain the projective cover of the trivial module (up to isomorphism). By Dickson's theorem [8, Chap. VII, Corollary 7.16], we have $2 \mid \dim C$. Since C is an MDS code, we also have

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

Thus $\mathrm{d}(C)$ is odd. Since the cover of the trivial module is not contained in C, we have $\mathrm{Hom}_{\mathbb{F}_2G}(C, \mathbb{F}_2) = 0$. Applying [10, Theorem 4.1 and Theorem 4.4] we get

$$2 \mid \Delta(G) \mid \mathrm{d}(C),$$

a contradiction.

Finally, suppose that the projective cover of the trivial module is contained in C. Now we look at $C^{\perp}$ which is obviously also an LCD code. Since $C^{\perp} \neq 0$, it is also an MDS code. Furthermore, $C^\perp$ does not contain the projective cover of the trivial module since its multiplicity in the group algebra KG is equal to 1. Now we apply the same arguments as above to $C^\perp$ to get the final contradiction. □

Remark 2.3 [2, Lemma 1] If $K = \mathbb{F}_q$, $q = 2^m$ and $0 < k < n = q - 1$, then there exist LCD Reed-Solomon codes of length n and dimension k. Note that these codes are LCD MDS group codes over a cyclic group.

Remark 2.4 If K is any finite field of characteristic p and $p \nmid |G|$, then, for any finite group G, there exist LCD MDS group codes $0 \neq C < KG$, namely the unique trivial submodule $T = (\sum_{g\in G} g)K = K(\sum_{g\in G} g)$.

For $a = \sum_{g\in G} a_g g$ we define the *adjoint* $\widehat{a}$ of a by $\widehat{a} = \sum_{g\in G} a_g g^{-1}$. Note that $\widehat{\ }$ defines an anti-algebra automorphism of KG.

In order to prove Theorem 2.2 over a general finite field $\mathbb{F}_q$ we may assume that $q = p$ is a prime.

Lemma 2.5 *Let E be an extension field of K. If there exists a non-trivial* LCD MDS *group code over K, then there exists a non-trivial* LCD MDS *group code over E as well.*

Proof: Let $C \leq KG$ be an LCD MDS group code. We consider $C' = C \otimes_K E \leq EG$. If $C = eKG$ with $e = e^2 = \widehat{e}$ (see [4, Theorem 3.1]), then $C' = eEG$. Hence C' is an LCD group code, by [4, Theorem 3.1]. According to [7, Proposition 12], the extension C' has the same parameters as C. Thus C' is an MDS code and we are done. □

Definition 2.6 For $a = \sum_{g\in G} a_g g \in KG$ ($a_g \in K$) we define the *support* of a by

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

The proof of the next result is an adaption of the proof of [4, Lemma 4.4].

Proposition 2.7 *Let $0 \neq C = eKG < KG$ with $e^2 = e = \hat{e}$ be an* LCD MDS *code. Then $G = \langle \mathrm{supp}(e) \rangle$, i.e., the group G is generated by the support of e.*

Proof: Let p be the characteristic of K and let $H = \langle \mathrm{supp}(e) \rangle$. By [4], we have $C^\perp = (1-e)KG$. Furthermore, $|\mathrm{supp}(1-e)| \leq |\mathrm{supp}(e)| + 1$. Since $C^\perp$ is an MDS code as well, it follows that

$$|G| + 2 = \mathrm{d}(C) + \mathrm{d}(C^\perp) \leq 2\,|\mathrm{supp}(e)| + 1 \leq 2|H| + 1,$$

hence $|H| > \frac{|G|}{2}$. As H is a subgroup of G, we obtain $H = G$, by elementary group theory. □

Definition 2.8 *A group code C is called self-adjoint if $C = \widehat{C}$.*

Note that a self-adjoint group code is a two-sided ideal since $\widehat{\ }$ defines an anti-algebra automorphism of a group algebra.

Proposition 2.9 *Let* char $K = p$ *and let N be a normal subgroup of G of index p. Then there does not exist a non-trivial self-adjoint* LCD MDS *group code C.*

Proof: Let C be a non-trivial self-adjoint LCD MDS group code in KG. According to [4, Corollary 3.3] we have $C = fKG$ where $f = f^2 = \widehat{f}$ and f lies in the center $Z(KG)$ of KG. Now, a well-known theorem of Osima [8, Chap. VII, Theorem 12.8] tells us that $\mathrm{supp}(f)$ consists only of p'-elements. Thus $\mathrm{supp}(f) \subseteq N$, hence $\langle \mathrm{supp}(f) \rangle \leq N$, contradicting Proposition 2.7. □

Proposition 2.10 *Let G be a p-solvable group where the characteristic p of K divides $|G|$. Suppose that*

$$\mathrm{O}_{p',p}(G) = \mathrm{O}_{p'}(G) \times \mathrm{O}_p(G).$$

If B is a self-adjoint p-block, i.e., a 2-sided indecomposable self-adjoint LCD *code, then B is not* MDS.

Proof: Since B is a two-sided ideal, we may write $B = fKG$ where $f = f^2 = \widehat{f}$ is centrally primitive and suppose that B is an MDS code. Since $\mathrm{O}_p(G)$ is contained in every defect group [1, Chap. IV, Theorem 6], we get by [11, Corollary] that $\langle \mathrm{supp}(f) \rangle \leq \mathrm{O}_{p'}(G)$. On the other hand, by Proposition 2.7 we have $G = \langle \mathrm{supp}(f) \rangle$, a contradiction to $p \mid |G|$.

□

Remark 2.11 ([4], Example 4.1) Under the condition of Proposition 2.9 there may exist non-trivial self-adjoint LCD group codes which are almost MDS codes. Recall that a linear $[n, k, d]$ code is called an *almost* MDS code if $d = n - k$:
Let $G = S_3$ be the symmetric group on 3 letters and let K be a field of characteristic 2. If $g \in G$ is of order 3, then $e = g + g^2 = e^2 = \hat{e}$ is a central self-adjoint idempotent in KG. The group code $C = eKG$ is a self-adjoint LCD almost MDS code with parameters $[6, 4, 2]$. Note that $C^\perp$ has parameters $[6, 2, 3]$. Hence $C^\perp$ is not an almost MDS code.

Proposition 2.12 *Let $0 \neq C = eKG < KG$ with $e^2 = e = \hat{e}$ be an* LCD *code. Suppose that C and $C^\perp$ as well are almost* MDS *codes. Then $|G : \langle \mathrm{supp}(e) \rangle| \leq 2$.*

Proof: Let p be the characteristic of K and let $H = \langle \mathrm{supp}(e) \rangle$. Since C and $C^\perp$ are almost MDS codes, we get, as in the proof of Proposition 2.7, that

$$|G| = \mathrm{d}(C) + \mathrm{d}(C^\perp) \leq 2\,|\mathrm{supp}(e)| + 1 \leq 2|H| + 1.$$

Since $|H| \mid |G|$ we even have $\frac{|G|-1}{2} < |H|$. If $|G|$ is odd, then $\frac{|G|+1}{2} \leq |H|$, hence $G = H$. If $2 \mid |G|$, then $\frac{|G|}{2} \leq |H|$. Thus $H = G$ or H is a normal subgroup of G of index 2. □

Lemma 2.13 *Let K be of characteristic p. If $0 \neq C \leq KG$ is an* LCD MDS *group code, then* $\mathrm{d}(C) \equiv 1 \bmod |G|_p$. *In particular,* $p \nmid \Delta(C)$.

Proof: Since C is an MDS code, we have

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

The assertion follows by applying $|G|_p \mid \dim C$ due to Dickson's theorem [8, Chap. VII, Corollary 7.16].

□

3 Divisors of LCD group codes

According to [3, Theorem 3.2] the p'-part of the divisor $\Delta(C)$ of a group code C can easily be determined by a suitable subgroup of the underlying group G. However, the computation of the p-part $\Delta(C)_p$ seems to be more subtle. In this section we give an answer for LCD group codes over the prime field $\mathbb{F}_p$.

Definition 3.1 If M is a (right) KG-module, then the dual vector space $M^* = \mathrm{Hom}_K(M, K)$ becomes a KG-module via

$$m(fg) = (mg^{-1})f$$

where $m \in M, f \in M^*$ and $g \in G$. With this action M^* is called the *dual module* of M.

According to [5, Theorem 1.3] we know how to compute the p'-part of the divisor $\Delta(C)$ of a group code C via the underlying group. The determination of the p-part turns out to be more subtle. However, over prime fields the next two results give an answer.

Theorem 3.2 *Let $K = \mathbb{F}_p$ where p is an odd prime. If $0 \neq C \leq KG$ is an* LCD *group code, then $\Delta(C)_p = 1$, i.e., $\Delta(C)$ is not divisible by p.*

Proof: Since C is an LCD group code, we may write $C = eKG$ with $e = e^2 = \widehat{e}$. Note that

$$C^* \cong \widehat{e}KG = eKG = C,$$

by [4, Lemma 2.3]. Thus $\mathrm{Hom}_{KG}(C \otimes C, K) = \mathrm{Hom}_{KG}(C, C^*) \neq 0$. Since p is odd, we get

$$\mathrm{Hom}_{KG}(C^{(p-1)}, K) \neq 0$$

with $C^{(p-1)} = C \otimes \cdots \otimes C$, where C has been taken $(p-1)$-times in the tensor product. Now, an application of [10, Theorem 4.4] yields $p \nmid \Delta(C)$. □

Theorem 3.3 *Let $K = \mathbb{F}_2$ and let P_0 be the projective cover of the trivial module. If $0 \neq C \leq KG$ is an* LCD *group code, then*

$$\Delta(C)_2 = \begin{cases} 1 & \text{if } P_0 \leq C \text{ (up to isomorphism)} \\ 2 & \text{otherwise.} \end{cases}$$

Proof: The proof follows the same lines as for Theorem 3.2. □

The following corollary answers Question 3.6 of [5].

Corollary 3.4 *Let K be any finite field of characteristic p and let P_0 denote the projective cover of the trivial module in KG. Then $\Delta(P_0) = |\mathrm{O}_{p'}(G)|$.*

Proof: According to [5, Lemma 3.3] and [4, Theorem 3.1], P_0 is an LCD group code. If $p = 2$, then the assertion has already been proved in [5]. Thus let p be odd. First we assume that $K = \mathbb{F}_p$. By Theorem 3.2, we know that $\Delta(P_0)_p$ =1, and by [5, Proposition 3.4] we have $\Delta(P_0) = |\mathrm{O}_{p'}(G)|$. Thus we are done over the prime field $\mathbb{F}_p$.

Now, let K be any finite field of odd characteristic p. Let $\mathbb{F}_p$ be the prime field of K. Clearly, $P_0|_{\mathbb{F}_pG}$, which is P_0 considered as an $\mathbb{F}_pG$-module, is projective and contains the module $T = \mathbb{F}_p(\sum_{g \in G} g)$. Thus $P_0|_{\mathbb{F}_pG}$ contains a projective cover, say P_0', of T over $\mathbb{F}_p$. More precisely, $P_0 = P_0' \otimes_{\mathbb{F}_p} K$.

Hence, by the above, we get

$$\Delta(P_0) \mid \Delta(P_0') = |\mathrm{O}_{p'}(G)|.$$

Finally, by [5, Proposition 3.4], we know that $|\mathrm{O}_{p'}(G)| \mid \Delta(P_0)$ and the proof is complete. □

4 Orthogonal indecomposable LCD codes

In order to construct nearly LCD group codes (what we do in the next section) we need a characterisation of orthogonal indecomposable group codes C. We shall prove that C has at most two indecomposable direct summands if C is an orthogonal indecomposable LCD group code.

Definition 4.1 A G-code C is called *orthogonal indecomposable* if C can not be written as $C = C_1 \perp C_2$ with nonzero G-codes C_i.

Recall that an indecomposable LCD G-code is always orthogonal indecomposable, since it is an indecomposable projective KG-module, but not vice versa.

Theorem 4.2 *Let $C \leq KG$ be an orthogonal indecomposable LCD code. Then one of the following holds.*

a) *$C = P$ is an indecomposable projective module whose socle is self-orthogonal if C is not irreducible.*

b) *$C = P_1 \oplus P_2$ where $0 \neq P_i$ are indecomposable projective G-codes and $P_1 \cong P_2^*$. Moreover, all irreducible submodules of C are self-orthogonal.*

Proof: Observe that C is a projective KG-module. First suppose that C is an indecomposable KG-module which is not irreducible. If the socle of C, denoted by $\mathrm{soc}(C)$, is not self-orthogonal, then $KG = \mathrm{soc}(C) \oplus \mathrm{soc}(C)^{\perp}$. On the other hand we have $KG = C \oplus C^{\perp}$. Thus $\mathrm{soc}(C)$ is a projective KG-module by the Krull-Schmidt theorem, which means that C must be irreducible, a contradiction. Hence $\mathrm{soc}(C)$ is self-orthogonal and we have the case in a).

Thus we may write

$$C = P_1 \oplus \cdots \oplus P_s \quad (s \geq 2)$$

with indecomposable projective KG-modules $P_i \neq 0$. Let $S_i = \mathrm{soc}(P_i)$. If S_i is regular, i.e., not self-orthogonal, then $C = S_i$, a contradiction to $s \geq 2$. This shows that all irreducible submodules of C are self-orthogonal. Next observe that $\langle \cdot \, , \cdot \rangle$ is regular on C. Furthermore $\langle S_1, P_1 \rangle = 0$ since otherwise $C = P_1$, again a contradiction to $s \geq 2$. Therefore we may assume (eventually we have to change the labelling of the P_i) that

$$\langle S_1, P_2 \rangle \neq 0.$$

In the rest of the proof we show that $\langle \cdot \, , \cdot \rangle$ is regular on $P_1 \oplus P_2$ which completes the proof. Suppose that the form has a non-zero radical on $P_1 \oplus P_2$ and let S be an irreducible module contained in the radical. By the assumption $\langle S_1, P_2 \rangle \neq 0$, we see that S is not the socle S_1 of P_1. Thus we have

$$S = \{ s_2 + s_2\alpha \mid s_2 \in S_2 \}$$

where α is a homomorphism from S_2 into S_1 Next observe that

$$0 = \langle s_2 + s_2\alpha, P_2 \rangle = \langle s_2\alpha, P_2 \rangle$$

for all $s_2 \in S_2$. Since $\langle S_1, P_2 \rangle \neq 0$, we get $\alpha = 0$. Thus $S = S_2$ and $\langle P_1, S_2 \rangle = 0$. Considering the map $\beta : P_1 \longrightarrow P_2^*$ defined by

$$\beta(x)(y) = \langle x, y \rangle$$

for $x \in P_1$ and $y \in P_2$, we see that β is injective since $\langle S_1, P_2 \rangle \neq 0$. Thus P_1 is a submodule of P_2^*. As P_1 is an injective KG-module and P_2^* is indecomposable, we get $P_1 \cong P_2^*$. This means that $\langle \cdot \, , \cdot \rangle$ is regular on $P_1 \oplus P_2$. Hence $C = P_1 \oplus P_2$, since C is orthogonal indecomposable. □

Example 4.3 Let $K = \mathbb{F}_4$. Then $\langle \omega \rangle = \mathbb{F}_4^*$ is a cyclic group of order 3. Furthermore, let $G = \mathrm{S}_3$ be the symmetric group on 3 letters, generated by an element g of order 3 and an involution.

We put $e_0 = 1 + g + g^2$, $e_1 = 1 + \omega g + \omega^2 g^2$ and $e_2 = 1 + \omega^2 g + \omega g^2$. One easily sees that

$$KG = P_0 \perp (P_1 \oplus P_2)$$

where the $P_i = e_i KG$ are indecomposable KG-modules of dimension 2. Furthermore, $P_1 \oplus P_2$ is an orthogonal indecomposable LCD code.

5 Nearly LCD group codes

Definition 5.1 If $C \leq KG$ is a group code, then

$$\text{hull}(C) = C \cap C^{\perp}$$

is called the *hull* of C. Note that hull(C) is a KG-submodule of KG, hence a group code.

Definition 5.2 We say that C is a *nearly* LCD *group code* if hull(C) $= C \cap C^{\perp}$ is an irreducible (or equivalently a simple) KG-module, i.e., C is a minimal ideal in KG.

Clearly, if C is a nearly LCD code, then hull(C) is a self-orthogonal code, i.e., hull(C) $\leq$ hull$(C)^{\perp}$.

Now let

$$KG = C_1 \perp \cdots \perp C_s$$

with orthogonal indecomposable ideals $C_i \leq KG$. Let

$$\emptyset \neq I \subset \{1, \ldots s\}.$$

and put $C_I = \oplus_{i \in I} C_i$. Note that the C_I is an LCD group code. We choose a self-orthogonal irreducible ideal

$$S_0 \leq C_{j_0}$$

for some $j_0 \in \overline{I} = \{1, \ldots, s\} \setminus I$ and put $C = C_I \oplus S_0$. With this notation we get the following result.

Theorem 5.3 *$C = C_I \oplus S_0$ is a nearly* LCD *group code.*

Proof: First, we suppose that C_{j_0} is an indecomposable KG-module. Clearly,

$$S_0^{\perp} = C_I \perp C_{\overline{I} \setminus j_0} \perp M$$

where M is the unique maximal submodule of C_{j_0}. Note that $M \neq 0$, since S has been chosen self-orthogonal. Thus, we obtain

$$\begin{aligned} C \cap C^{\perp} = C \cap (C_I \oplus S_0)^{\perp} &= (C \cap C_I^{\perp}) \cap S_0^{\perp} \\ &= S_0 \cap M = S_0 \end{aligned}$$

since C_{j_0} is orthogonal indecomposable, and we are done. Thus, according to Proposition 4.2, the module C_{j_0} is the direct sum of two indecomposable modules, i.e., $C_{j_0} = P_1 \oplus P_2$ with indecomposable projective modules P_i. We may assume that S_0 is the socle of P_1 since C_{j_0} contains a projective cover of S_0 which is an injective module, and therefore has a complement in C_{j_0}. With the notation as in the first case we get

$$C \cap C^{\perp} = S_0 \cap M$$

where M is the orthogonal of S_0 in C_{j_0}, which contains S_0 since S_0 is self-orthogonal. This completes the proof. □

Of special interest for applications are nearly LCD codes C which have a 1-dimensional hull. Such codes have recently been considered in [6] for dihedral groups. The examples given there are constructed exactly along the lines above, i.e., as in Theorem 5.3. The final result generalizes ([6], Theorem 3.9).

Lemma 5.4 *The trivial module in a group algebra KG is the hull of a nearly* LCD *code if and only if* char $K \mid |G|$.

Proof: Note that $T = K \sum_{g \in G} g$ is the unique submodule of KG which is trivial. Furthermore, if char $K \nmid |G|$, then

$$\langle \sum_{g \in G} g, \sum_{g \in G} g \rangle = |G| \neq 0$$

and T can not the the hull of an almost LCD code. Now suppose that char $K \mid |G|$. If P_0 is a projective cover of T, then

$$KG = P_0 \perp P_0^{\perp},$$

otherwise KG allows an epimorphism onto $T \oplus T$, a contraction. Now we put

$$C = T \oplus P_0^{\perp}.$$

Then

$$C^{\perp} = (T \oplus P_0^{\perp})^{\perp} = T^{\perp} \cap P_0 = P_0 J(KG)$$

where $J(KG)$ denotes the Jacobson radical of KG. Thus

$$C \cap C^{\perp} = C \cap P_0 J(KG) = T.$$

□

There may exist 1-dimensional hulls of a nearly LCD group codes in the case that the characteristic of the underlying field does not divide the order of the group. This happens if the group algebra has an irreducible module which is not self-dual.

Example 5.5 Let char $K = p \nmid |G|$, hence KG is semisimple. Suppose that C_0 is a 1-dimensional ideal in KG with $C_0 \ncong C_0^*$. This means that C_0 is self-orthogonal. Thus, by Theorem 4.2, we may write

$$KG = (C_0 \oplus C_0^*) \perp P$$

where P is a direct sum of irreducible modules, since KG is semisimple. We put $C = C_0 \oplus P$. Clearly, by dimension, we have $C_0^{\perp} = C_0 \oplus P$. Thus $C \cap C^{\perp} = C_0$.

References

[1] Alperin, J.L.: Local representation theory. Cambridge University Press, Cambridge (1986).

[2] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. In *Coding Theory and Applications*. Eds. R. Pinto, P. Rocha Malonek and P. Vettory, CIM Series in Math. Sciences 3, 97-105 (2015).

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

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

[5] de la Cruz, J., Willems, W.: Divisibility of weights for ideals in group algebras. Vietnam J. Math. 51, 721-729 (2023).

[6] Dougherty, S.T., Şahinkaya, S., Ustun, D.: Dihedral codes with 1-dimensional hulls and 1-dimensional linear complementary pairs of dihedral codes. AAECC, July 2023.

[7] Faldum, A., Willems, W.: Codes of small defect. Des. Codes Cryptogr. 10, 341-350 (1997).

[8] Huppert, B., Blackburn, N.: Finite groups II. Springer, Berlin, Heidelberg, New York (1982).

[9] Massey, J.L.: Linear codes with complementary duals. A collection of contributions in honour of Jack van Lint. Discrete Math. 106/107, 337-342 (1992).

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

[11] Willems, W.: A note on the support of block idempotents. Archiv Math. 62, 21-25 (1994).

[12] Willems, W.: Codes in Group Algebras. In W.C. Huffman, J.-L. Kim and P. Solé, editors, Concise Encyclopedia of Coding Theory, Chap. 16, 363-384, CRC Press, Chapman and Hall, Boca Raton, USA (2021).