On Group Codes with Complementary Duals

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

Keywords. Group code, LCD code, self-dual code, cyclic code, projective module
MSC classification. 94B05, 94B15, 20C05

Abstract

We investigate and characterize ideals in a group algebra KG which have complementary duals, i.e., ideals C in KG which satisfy $KG = C \oplus C^\perp$. In the special case that G is a cyclic group we get an early result of Yang and Massey as an easy consequence.

1 Introduction

Throughout this note let K be a finite field. According to Jim Massey [12], a *linear* code $C \leq K^n$ is called *complementary dual*, or shortly an LCD code, if $K^n = C \oplus C^\perp$ which is obviously equivalent to the property that $C \cap C^\perp = \{0\}$. Like self-dual codes, LCD codes are of particular interest. For instance, the class of LCD codes is asymptotically good [12], LCD codes achieve the Gilbert-Varshamov bound [13], and recently it has been shown that they play a crucial role in information protection [3].

A *linear code* C is called a *group code* (*for a group* G *over the field* K) if C is a right ideal in a group algebra $KG = \{a = \sum_{g\in G} a_g g \mid a_g \in G\}$ where G is a finite group. The vector space KG with basis $g \in G$ serves as the ambient space with the weight function $\mathrm{wt}(a) = |\{g \in G \mid a_g \neq 0\}|$. Note that KG carries in a natural way a K-algebra structure via the multiplication in G. More precisely, if $a = \sum_{g\in G} a_g g$ and $b = \sum_{g\in G} b_g g$ are given, then

$$ab = \sum_{g\in G}(\sum_{h\in G} a_h b_{h^{-1}g})g.$$

In this sense cyclic codes are group codes for a cyclic group G, Reed Muller codes over prime fields $\mathbb{F}_p$ are group codes for an elementary abelian p-group G [10] and there are many other remarkable record codes which have been detected as group codes [7], [4], [2].

Furthermore, the group algebra KG carries a natural symmetric non-degenerate G-invariant bilinear form $\langle .\,,. \rangle$ which is defined by

$$\langle g, h \rangle = \begin{cases} 1 & \text{if } g = h \\ 0 & \text{otherwise.} \end{cases}$$

Here G-invariance means that $\langle ag, bg \rangle = \langle a, b \rangle$ for all $a, b \in KG$ and all $g \in G$. With respect to this form we may define the orthogonal code $C^\perp$ of $C \leq KG$ as usual and say that C is self-dual if $C = C^\perp$. In [16] we classified completely group algebras which contain a self-dual ideal. More precisely, a self-dual group code for G exists over the field K if and only if $|G|$ and the characteristic of K are even.

In this note we investigate LCD group codes. Since the methods we are going to use are from representation theory we give some basic facts of algebras, specially group algebras and their modules in the next section. Everything there is known and written up only for the reader's convenience. For more facts in group and representation theory one may confer with [1], chapter VII of [9] or [6].

2 Basic facts on algebras and their modules

Let A be a finite dimensional K-algebra. All modules respectively ideals which we consider are from the right, if nothing else is mentioned, and of finite dimension over K. Recall that $e \in A$ is called an *idempotent* if $e^2 = e$.

Lemma 2.1 *The following are equivalent.*

a) *If $A = A_1 \oplus A_2$ with ideals A_i, then there exists $e = e^2 \in A$ such that $A_1 = eA$ and $A_2 = (1-e)A$.*

b) *If $e = e^2 \in A$, then $A = eA \oplus (1-e)A$.*

Proof: a) Let $1 = e_1 + e_2$ with $e_i \in A_i$. We obtain $e_1 = 1e_1 = (e_1 + e_2)e_1 = e_1^2 + e_2e_1$. Since $e_1, e_1^2 \in A_1$ and $e_2e_1 \in A_2$ we get $e_1 = e_1^2$ and $e_2e_1 = 0$. Similarly $e_2 = e_2^2$ and $e_1e_2 = 0$. Since $e_iA \leq A_i$ and obviously $e_1A \oplus e_2A = A$ we can take $e = e_1$.
b) If $ex = (1-e)y \in eA \cap (1-e)A$ with $x, y \in A$, then

$$ex = e(ex) = e(1-e)y = 0$$

since $e^2 = e$. Thus $eA \cap (1-e)A = 0$. Furthermore for $x \in A$ we obviously have

$$x = ex + (1-e)x \in eA + (1-e)A$$

which proves that $A = eA + (1-e)A$. □

Note that in the lemma above e is a central idempotent, i.e., e is an element in the center $Z(A) = \{b \in A \mid ab = ba \text{ for all } a \in A\}$ of A if and only if the ideals A_i are 2-sided.

Furthermore, eA is called *indecomposable* (i.e., it is not the direct sum of two non-zero ideals) if and only if e is *primitive* (i.e., e can not be written as $e = e_1 + e_2$ with $e_i^2 = e_i$ and $e_1e_2 = e_2e_1 = 0$.)

For our purpose the most appropriate way to define a projective module is the following. An A-module P is *projective* if it is a direct summand of a finitely generated free A-module, i.e.,

$$P \oplus P' \cong A \oplus \ldots \oplus A = A^n$$

where P' is also an A-module. In case P is projective and indecomposable, one easily sees that P is a direct summand of A. Thus by Lemma 2.1, we have $P = eA$ with a primitive idempotent e.

Finally, for each irreducible A-module M there exists (up to isomorphism) a unique indecomposable projective A-module $P(M)$ called the *projective cover* of M such that M is a factor module of $P(M)$. Actually, a indecomposable projective A-module P has only one irreducible factor module which means it has only one maximal A-submodule.

We may write $A = B_1 \oplus \ldots \oplus B_s$ where the B_i are 2-sided ideals which are 2-sided indecomposable. By Lemma 2.1, we get $B_i = f_iA = Af_i$ with f_i in the center of A and $f_if_j = \delta_{ij}f_i$. The ideals B_i and idempotents f_i are uniquely determined and called the *blocks of A*.

Now we restrict to the group algebra $A = KG$.

Definition 2.2 If M is a 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.

To each $a = \sum_{g\in G} a_g g \in KG$ $(a_g \in K)$ the *adjoint* of a is defined by $\hat{a} = \sum_{g\in G} a_g g^{-1}$. We call *a self-adjoint* if $a = \hat{a}$. Note that the map $\hat{}\, : KG \longrightarrow KG$ defines an anti-isomorphism of KG and for all $a, b \in KG$ the bilinear form defined in the introduction satisfies

$$\langle a, b\rangle = \langle \hat{b}a, 1\rangle = \langle 1, \hat{a}b\rangle.$$

Lemma 2.3 *If $e = e^2 \in KG$, then $\hat{e}KG \cong eKG^*$.*

Proof: We may assume that $e \neq 0$ and define a map $\alpha : \hat{e}KG \longrightarrow eKG^*$ by

$$x(y\alpha) = \langle x, y\rangle \in K,$$

for $x \in eKG$ and $y \in \hat{e}KG$. Obviously, α is K-linear. But α is even KG-linear since

$$x((yg)\alpha) = \langle x, yg\rangle = \langle xg^{-1}, y\rangle = (xg^{-1})(y\alpha) = x((y\alpha)g),$$

where Definition 2.2 has been used in the last equality. Furthermore, α is a monomorphism since $x(y\alpha) = 0$ for all $x \in eKG$ and some $y = \hat{e}a$ implies

$$0 = \langle eg, \hat{e}a\rangle = \langle g, \hat{e}^2a\rangle = \langle g, \hat{e}a\rangle$$

for all g $\in G$, hence $y = \hat{e}a = 0$. Thus we are done since $\dim \hat{e}KG = \dim eKG = \dim eKG^*$. □

Now let C be an LCD group code, i.e., $KG = C \oplus C^\perp$ where C is a right ideal in KG. Note that $C^\perp$ must be a right ideal as well since for all $c \in C, c^\perp \in C^\perp$ and $g \in G$ we have

$$\langle c, c^\perp g\rangle = \langle cg^{-1}, c^\perp\rangle = 0.$$

This shows that C is a projective KG-module inside KG. Furthermore $KG/C^\perp \cong C$ since $KG = C \oplus C^\perp$. According to ([16], Proposition 2.3) we also have $KG/C^\perp \cong C^*$ as KG-modules, hence $C \cong C^*$. Thus a LCD group code is a projective self-dual module (ideal) inside KG.

Lemma 2.4 *Let p be the characteristic of K. If C is an LCD group code for G over K, then $|G|_p \mid \dim C$.*

Proof: As we have seen already C is a projective KG-module. The assertion now follows by a well-known result of Dickson (see for instance ([9], Chap. VII, Corollary 7.16)). □

3 LCD group codes

We start with the main result of this section from which we easily deduce in Corollary 3.7 an early result of Yang and Massey.

Theorem 3.1 *If $C \leq KG$ is a right ideal in KG, then the following are equivalent.*

a) *C is an LCD code.*

b) *$C = eKG$ where $e^2 = e = \hat{e}$.*

Proof: First suppose that b) holds true, hence $C = eKG$ with $e^2 = e = \hat{e} \in KG$. Since e is an idempotent we have $KG = eKG \oplus (1-e)KG$, by Lemma 2.1. Recall that $\langle ab, c\rangle = \langle b, \hat{a}c\rangle$ for all $a, b, c \in KG$. Thus, for $a, b \in KG$ we obtain

$$\langle ea, (1-e)b\rangle = \langle a, \hat{e}(1-e)b\rangle = \langle a, e(1-e)b\rangle =$$

$$= \langle a, 0\rangle = 0.$$

This shows that $(1-e)KG \leq C^\perp$. Since

$$\dim(1-e)KG = |G| - \dim C = \dim C^\perp$$

we get the desired result $(1-e)KG = C^\perp$.

Conversely suppose that a) holds true. Let $KG = C \oplus C^\perp$ and write $1 = e + f$ with $e \in C$ and $f \in C^\perp$. It follows

$$e = e^2 + fe \text{ and } f = ef + f^2.$$

Since C and $C^\perp$ are KG-modules we get $e^2 = e, f^2 = f$ and $ef = fe = 0$. Furthermore, $KG = eKG \oplus fKG$ which implies that $C = eKG$ and $C^\perp = fKG$. If $a, b \in KG$, then

$$0 = \langle ea, fb \rangle = \langle a, \hat{e}fb \rangle = \langle a, \hat{e}(1-e)b \rangle.$$

Since the bilinear form is non-degenerate on KG we get $\hat{e}(1-e) = 0$ or equivalently $\hat{e} = \hat{e}e$. Finally

$$e = \hat{\hat{e}} = \widehat{\hat{e}e} = \hat{e}e = \hat{e},$$

and we are done. □

The Theorem above says that C is an LCD group code exactly if it is generated by a self-adjoint idempotent of KG.

Recall from group theory that a finite group G is called p-solvable (p a prime number) if G has a chain of subgroups G_i such that

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

where G_{i-1} is a normal subgroup of G_i and the factor groups G_i/G_{i-1} ($i = 1, \ldots, n$) are either abelian or a group whose order is not divisible by p.

Example 3.2 Let G be a p-solvable group. If $|G| = p^s m$ where $p \nmid m$, then G has a subgroup H with $|H| = m$. (The subgroup H is usually called a *p-complement* of G.) We put $e = \frac{1}{|H|}\sum_{h\in H} h$. One easily computes $e^2 = e = \hat{e}$. Thus eKG is an LCD group code. Actually, eKG is the projective cover $P(1_G)$ of the trivial KG-module denoted by 1_G. For $n \in \mathbb{N}$ we write $n = n_p n_{p'}$ where n_p is the p-part of n and $n_{p'}$ the part which is not divisible by p. With this notation we have $\dim eKG = |G|_p$ and for the minimum distance we get $|G|_{p'}$. Hence eKG is not very much of interest for error correction since apart from trivial cases the minimum distance $|G|_{p'}$ is much smaller than the Singleton bound $|G| - |G|_p + 1$.

We call a group code C *self-adjoint* if $C = \hat{C} = \{\hat{c} \mid c \in C\}$. Note that $\hat{C}$ is a left KG-module, but also a right KG-module in case G is abelian. If G is a cyclic group of order n generated by g and we order G by $1, g, g^2, \ldots, g^{n-1}$, then $(c_0, c_1, \ldots, c_{n-1})$ corresponds to $c = \sum_{i=0}^{n-1} c_i g^i$. Thus $\hat{c}$ corresponds to $(c_0, c_{n-1}, \ldots, c_1)$. Since C is cyclic $(c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$ corresponds also to a code word. This shows that self-adjointness for cyclic groups means nothing else than reversibility (see [11]).

Corollary 3.3 *Let $C \leq KG$ be a right ideal in KG. Then the following are equivalent.*

a) *C is a self-adjoint LCD code.*

b) *$C = fKG$ where $f^2 = f = \hat{f}$ where f lies in the center of KG.*

Proof: The direction from b) to a) is obvious. Thus let C be a self-adjoint LCD group code. According to Theorem 3.1 we may assume that $C = fKG$ with $f^2 = f = \hat{f}$. Self-adjointness of C means

$$C = fKG = \widehat{fKG} = KG\hat{f} = KGf = fKGf.$$

Now we write $KG = fKG \oplus eKG$ where $1 = f + e$. From this we obtain

$$KGe = fKGfe \oplus eKGe = eKGe,$$

since $fe = 0$. Thus $KGe = eKGe \leq eKG$. In addition $\dim KGe = \dim eKG$ implies that $eKG = KGe$. This shows that

$$KG = fKG \oplus eKG$$

is a decomposition of KG into a direct sum of two-sided ideals. Therefore, for any $a \in KG$ we have

$$a = af + ae = fa + ea \in fKG \oplus eKG.$$

Thus $af = fa$ for all $a \in KG$ which shows that f is in the center of KG. □

In the language of representation theory condition b) in the corollary above means in particular that C is a direct sum of blocks.

Recall that in case char $K = 2$ a K-vector space V with a non-degenerate K-bilinear form $\langle .\,,.\rangle$ is called *symplectic* if $\langle v, v\rangle = 0$ for all $v \in V$. Obviously, a self-dual code is symplectic, but not vise versa.

Corollary 3.4 *If* char $K = 2$ *and* $C \leq KG$ *is a right ideal in* KG*, then the following are equivalent.*

a) *C is a symplectic* LCD *group code.*

b) $e^2 = e = \hat{e}$ *and* $\langle 1, e\rangle = 0$*, i.e., the coefficient of* e *at* 1 *is zero.*

Proof: Suppose that a) holds true. According to Theorem 3.1 we only have to check $\langle 1, c\rangle = 0$ for all $c \in C = eKG$. Since $\langle c, c\rangle = 0$ for all c in C we have in particular

$$0 = \langle e, e\rangle = \langle 1, \hat{e}e\rangle = \langle 1, e^2\rangle = \langle 1, e\rangle.$$

Conversely, suppose that $\langle 1, e\rangle = 0$. Again by Theorem 3.1 we know that $C = eKG$ is an LCD group code. First note that

$$\langle eg, eg\rangle = \langle e, e\rangle = \langle 1, \hat{e}e\rangle = \langle 1, e\rangle = 0$$

for all $g \in G$. Thus for $a = \sum_{g\in G} a_g g$ and $e = \sum_{g\in G} e_g g$ with $a_g, e_g \in K$ we obtain

$$\langle ea, ea\rangle = \sum_{g,h\in G} a_g a_h \langle eg, eh\rangle = \sum_{\{g,h\}|g\neq h} a_g a_h (\langle eg, eh\rangle + \langle eh, eg\rangle) = 0,$$

where in the last equality we have used that the form $\langle . \, , . \rangle$ is symmetric and char $K = 2$. Therefore $\langle . \, , . \rangle$ is symplectic on C. □

Note that for the binary field $K = \mathbb{F}_2$ the condition a) in Corollary 3.4 means that C is 2-divisible. It can not be 4-divisible except $C = 0$ since a 4-divisible code is always self-orthogonal. Furthermore, if C is 2-divisible, then $C^\perp$ is not 2-divisible and vice versa.

Remark 3.5 Let $C = eKG$ with $e^2 = e = \hat{e}$ be an LCD code and let char $K = 2$. Suppose that $C^\perp = (1-e)KG$ does not contain the projective cover $P(1_G)$ of the trivial module as a direct summand (up to isomorphism). By ([5], Proposition 2.2) it follows that $\langle \cdot \, , \cdot \rangle|_{C^\perp}$ is the polarization of a G-invariant quadratic form on $C^\perp$. This means that there is a G-invariant quadratic form q on $C^\perp$ such that

$$q(a+b) - q(a) - q(b) = \langle a, b \rangle$$

for $a, b \in C^\perp$. Since the characteristic of K is 2, the form $\langle \cdot \, , \cdot \rangle|_{C^\perp}$ is symplectic. Thus by Corollary 3.4, we obtain $\langle 1, 1-e \rangle = 0$. This has the following interesting consequence in representation theory.

Proposition 3.6 *Let* char $K = 2$ *and let* $P(1_G) = eKG$ *be the projective cover of the trivial module where* $e = e^2 \in KG$. *Then* $e = 1 + \sum_{g \neq 1} \lambda_g g$.

Proof: First note that for any characteristic p the projective cover $P(1_G) = eKG$ of the trivial module is always an LCD group code. This follows from ([15], Satz 2.15) since the multiplicity of $P(1_G)$ in KG is 1. It also says that $P(1_G)$ is not a direct summand in $(1-e)KG$. According to Theorem 3.1 we have $e^2 = e = \hat{e}$. By Remark 3.5, the element $1-e$ does not contain 1 in its support. Since $1 = e + (1-e)$ the assertion follows. □

If we specialize Theorem 3.1 to cyclic groups we immediately get an early result of Yang and Massey as a corollary.

Corollary 3.7 [17] *If* $g(x)$ *is the generator polynomial of an* $[n, k]$ *cyclic code* C *of block length* n *(the characteristic of* K *and* n *not necessarily coprime), then* C *is an LCD code if and only if* $g(x)$ *is self-reciprocal and all the monic irreducible factors of* $g(x)$ *have the same multiplicity in* $g(x)$ *and in* $x^n - 1$.

Proof: Let C be a cyclic LCD group code for G over the field K of characteristic p. Clearly, C is self-adjoint since G is abelian. We consider C in $K[x]/(x^n - 1)$. In particular, as mentioned in the section below Example 3.2, C is reversible. Thus if $g(x) = g_0 + g_1 x + \ldots + x^r$ is a generator polynomial of C, then $g^*(x) = g_0 x^r g(1/x)$ is also a generator polynomial, hence $g^*(x) = a g(x)$ with $a \in K^\times$. Since both polynomials are monic we get $a = 1$, hence $g(x)$ is self-reciprocal. The assertion on the multiplicity is an immediate consequence of a well-known fact in representation theory. For the reader's convenience we give a short argument to see this fact. We write $G = P \times Q$ where P is a Sylow p-subgroup of G and H is a p-complement. Thus $KG \cong KP \otimes KQ$ where the group algebra KP is uniserial with exactly $|G|_p$ composition factors isomorphic to the trivial module and KQ is a semisimple algebra. Hence each projective indecomposable KG-module is uniserial (i.e., the submodules form a chain) with $|G|_p$ isomorphic composition factors and the multiplicity of a fixed irreducible KG-module in KG equals $|G|_p$ as well. Finally note that an irreducible module corresponds to a normed irreducible polynomial. □

4 Examples, remarks and questions

Example 4.1 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 code of dimension 4 and minimum distance 2. In particular, C is a $[6, 4, 2]$ almost MDS code, which is optimal as a $[6, 4]$ code.

Example 4.2 Let $G = A_4$ be the alternating group on 4 letters and let K be a field of characteristic 3. We put $e = g + h + gh \in KG$ where g, h generate a Klein four group in G. The group code $C = eKG$ is a self-adjoint LCD code of dimension 9 and minimum distance 2. In particular, C a $[12, 9, 2]$ code, which is optimal as an LCD code (see [14]).

Example 4.3 Let $G = A_5$ be the alternating group on 5 letters and let K be the binary field. Let e be the sum of all elements of order 3 and 5. Thus $\mathrm{wt}(e) = 44$. The group code $C = eKG$ is a self-adjoint LCD code of dimension 16 and minimum distance 18. Furthermore $\langle \cdot\,, \cdot\rangle|_C$ is symplectic, by Corollary 3.4. Note that according to Grassl's table [8] the minimum distance of a binary optimal $[60, 16]$ code is between 20 and 22.
If we take analogously the 2-block of defect 0 of $\mathrm{GL}(3, 2)$ we get an $[168, 64, 14]$ LCD code. An optimal binary $[168, 64]$ code has at least minimum distance 32 (see [8]).

Lemma 4.4 *Let G be abelian and let $C = eKG \leq KG$ with $e^2 = e = \hat{e} \neq 1$, hence C is an LCD code. If in addition C is an* MDS *code, then the characteristic of K does not divide $|G|$, i.e., KG is a semisimple algebra.*

Proof: Let p denote the characteristic of K. Since $e^p = e$ one easily sees that e has coefficients different from 0 only at p'-elements, hence only in $H = O_{p'}(G)$ (the largest normal p'-subgroup of G). Furthermore, $\mathrm{supp}(1 - e) \leq \mathrm{supp}(e) + 1$. With C the dual $C^\perp$ is an MDS code as well. It follows

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

hence $|H| > \frac{|G|}{2}$. Since H is a subgroup of G we obtain $G = H$. Thus p does not divide $|G|$. □

Remark 4.5 There are LCD MDS group codes over $\mathbb{F}_q$ and dimension k with $0 < k < n$ and length $n = q - 1$, if
a) (Carlet-Guilley [3]) q is even and k arbitrary or

b) q is odd and k is even.
The codes may be chosen as Reed-Solomon codes. A proof for a) is given in [3]. It uses the characterization of cyclic LCD codes given in Corollary 3.7. The same argument works also in part b). For q and k odd the Reed-Solomon codes are not LCD codes.

Question 4.6 Let G be an arbitrary finite group and suppose that KG contains an LCD group code which is also an MDS code. Does this imply that the characteristic of K does not divide $|G|$?

Remark 4.7 On $A = K^{n\times n}$ the rank metric is defined by $\mathrm{d}(a,b) = \mathrm{rank}(a-b)$ for $a, b \in A$. We may endow A with the Delsarte bilinear form

$$\langle a, b\rangle = tr(ab^t)$$

for $a, b \in A$ where tr denotes the trace and $\cdot^t$ the transpose of matrices. In A we consider rank metric codes. Similarly to group codes one can prove that a right ideal $\mathcal{C} \leq A$ is an LCD code if and only if $\mathcal{C} = eA$ where $e^2 = e = e^t$. Unfortunately, if $e \neq 0$, then $\mathcal{C}$ has minimal distance 1. This can be seen as follows:
We may assume $e \neq 1$. The minimal polynomial $m_e(x)$ of $e = e^2$ is $m_e = x(x-1)$. Therefore 0 and 1 are the only eigenvalues of e and there exists a regular matrix g such that

$$e^g = g^{-1}eg = \mathrm{diag}(1, \dots, 1, 0, \dots, 0)$$

where $1 \leq k < n$ entries are equal 1. Thus the rank metric code $\mathcal{C}^g = (eA)^g = e^gA$ has minimum distance 1 as

$$e^gA = \{\begin{pmatrix} a \\ 0 \end{pmatrix} \mid a \in K^{k\times n}\}.$$

This implies that $\mathcal{C}$ has minimum distance 1 as well.

References

[1] J.L. Alperin and R.B. Bell,“Groups and representations.” *Graduate Text in Math.*, Springer, New York, Heidelberg 1995.

[2] F. Bernhardt, P. Landrock and O. Manz, “The extended Golay codes considered as ideals.” *J. Comb. Theory, Series A*, vol. 55, pp. 235-246, 1990.

[3] C. Carlet and S. Guilley, “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.* vol. 3, pp. 97-105, Springer 2015.

[4] J.H. Conway, S.J. Lomonaco Jr and N.J.A. Sloane, “A [45, 13] code with minimal distance 16.” *Discrete Math.*, vol. 83, pp. 213-217, 1990.

[5] R. Gow and W. Willems, “Quadratic geometries, projective modules and idempotents.” *J. Algebra*, vol. 160, pp. 257-272, 1993.

[6] R. Gow, B. Huppert, R. Knőrr, O. Manz and W. Willems, Representation theory in arbitrary characteristic. Centro Internationale Per La Ricerca Mathematica, Trento 1993.

[7] A. vom Felde, “A new presentation of Cheng-Sloane’s $[32, 17, 8]$-code.” *Arch. Math.*, vol. 60, pp. 508-511, 1993.

[8] M. Grassl “Bounds on the minimum distance of linear codes.” Available by `www.codetables.de`

[9] B. Huppert and N. Blackburn, “Finite groups II.” Springer, Berlin, Heidelberg, New York 1982.

[10] P. Landrock and O. Manz, “Classical codes as ideals in group algebras.” *Designs, Codes and Cryptography*, vol. 2, pp. 273-285, 1992.

[11] J.L. Massey, “Reversible codes.” *Inform. and Control* vol. 7, pp. 369-380, 1964.

[12] J.L. Massey, “Linear codes with complementary duals.” A collection of contributions in honour of Jack van Lint. *Discrete Math.*, vol. 106/107, 337-342, 1992.

[13] N. Sendrier, “Linear codes with complementary duals meet the Gilbert-Varshamov bound.” *Discrete Mathematics*, vol. 285, pp. 345-347, 2004.

[14] A. Wassermann, “LCD codes from matrix groups.” First Colombian Workshop on Coding Theory, Barranquilla, Nov. 2015.

[15] W. Willems, “Metrische Moduln über Gruppenringen.” PhD Thesis, Universität Mainz 1976.

[16] W. Willems, ”A note on self-dual group codes.” *IEEE Trans. Inf. Theory*, vol. 48, pp. 3107-3109, 2002.

[17] X. Yang and J.L. Massey, ”The necessary and sufficient condition for a cyclic code to have a complementary dual.” *Discrete Math.*, vol. 126, pp. 391-393, 1994.