J. Algebra Comb. Discrete Appl.
12(2) • 163–174

Received: 13 July 2024
Accepted: 3 October 2024

Journal of Algebra Combinatorics Discrete Structures and Applications

Good codes from twisted group algebras

Research Article

Samir Assuena

Abstract: In this paper, we shall give an explicit proof that constacyclic codes over finite commutative rings can be realized as ideals in some twisted group rings. Also, we shall study isometries between those codes and, finally, we shall study k-Galois LCD constacyclic codes over finite fields. In particular, we shall characterize constacyclic LCD codes with respect to Euclidean inner product in terms of its idempotent generators and the classical involution using the twisted group algebras structures and find some good LCD codes.

2020 MSC: 20C05, 16S34

Keywords: Twisted group algebras, Finite groups, Galois LCD constacyclic codes

1. Introduction

Linear codes with complementary duals (abbreviated LCD) are linear codes whose intersection with their dual is trivial. When they are binary, they play an important role in armoring implementations against side-channel attacks and fault injection attacks.

Linear complementary dual codes have importance in data storage, communications systems and security too.

These codes have been studied for improving the security of information on sensitive devices against side-channel attacks (SCA) and fault non-invasive attacks, see [4], and have found use in data storage and communications systems.

Carlet and Guilley, in [5], also investigated the application of binary LCD codes against side-channel attacks (SCA) and fault tolerant injection attacks (FIA). Also, in [13], the authors constructed explicity LCD codes and have explicit efficient encoding and decoding algorithms .

In [11], Fan and Zhang, introduced the concept of *k-Galois form*, which is a generalization of Euclidean and Hermitian inner products and Liu, Fan and Liu, in [16], studied k-Galois LCD codes.

Samir Assuena; Centro Universitário da FEI Av. Humberto de Alencar Castelo Branco, 3972 São Bernardo do Campo, SP, Brazil. CEP: 09210-580 (email: samir.assuena@fei.edu.br).

So, this paper is devoted to study constacyclic codes in terms of twisted group rings of cyclic groups and to classify the k-Galois LCD constacyclic codes over finite fields in terms of idempotents. Using that approach, we can find some good code from twisted group ring.

Also, in [6], the authors proved that linear codes are equivalent to LCD codes over finite fields $\mathbb{F}_q$, for $q > 3$.

Let R be a finite commutative ring, $\mathcal{C}$ be a linear code over R^n, that is, $\mathcal{C}$ is a R-submodule of R^n and let λ be an element of $\mathcal{U}(R)$, the group of units of R. We say that $\mathcal{C}$ is a λ-*constacyclic code* if

$$(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C} \Longrightarrow (\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$$

for all $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$.

When $\lambda = 1$, we have so called *cyclic codes* and, when $\lambda = -1$, we have *negacyclic codes*. Thus, constacyclic codes are generalization of cyclic and negacyclic codes and they have been studied for many authors ([1], [2], [10]). Also, constacyclic codes can be realized as ideals in polinomial factor ring $\dfrac{R[x]}{\langle x^n - \lambda \rangle}$.

Given $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ two elements of a linear code $\mathcal{C}$, the *Hamming distance* between x and y is the number

$$d_H(x, y) = |\{i : x_i \neq y_i,\ 0 \leq i \leq n-1\}|.$$

and the *weight* of x is

$$w_H(x) = d(x, 0) = |\{i : x_i \neq 0,\ 0 \leq i \leq n-1\}|.$$

It is well known that, for a linear code $\mathcal{C}$, we have $d_H(x, y) = w_H(x - y)$, for all $x, y \in \mathcal{C}$.

Let G be a group and A be an abelian group. A map

$$\alpha : G \times G \longrightarrow A$$

is a 2-*cocycle* if , for all x, y and z in G, we have

$$\alpha(x, y)\alpha(xy, z) = \alpha(y, z)\alpha(x, yz).$$

and a map $t : G \times G \longrightarrow A$ is a 2-*coboundary* if there is a map $\delta : G \longrightarrow A$ such that

$$t(x, y) = \delta(x)\delta(y)\delta(xy)^{-1}.$$

As usual, the set of all 2-cocycles will be denoted by $Z^2(G, A)$ and the set of all 2-coboundary will be denoted by $B^2(G, A)$. Finally, we say that a 2-cocycle α is *normalized* if $\alpha(x, 1) = \alpha(1, x) = \alpha(1, 1) = 1$, for all $x \in G$. Notice that, if α is a 2-cocycle, we can replace α by α' given by

$$\alpha'(x, y) = \frac{\alpha(x, y)}{\alpha(1, 1)}$$

which is a normalized 2-cocycle. From now on, we assume that all 2-cocycle are normalized.

Let R be a commutative ring and G be a group. The *twisted group ring* $R^\gamma G$ *of* G *over* R is the associative ring with basis $\overline{G} = \{\overline{g},\ g \in G\}$, which is a copy of G, and the multiplication is defined on the basis as

$$\overline{g} \cdot \overline{h} = \gamma(g,h)\overline{gh}$$

where $\gamma(g,h)$ is an element of $\mathcal{U}(R)$, the group of units of R.

The mapping $\gamma : G \times G \longrightarrow \mathcal{U}(R)$ is called *twisting* and there are many different possibilities for $R^\gamma G$ depending on the choice of the twisting. For instance, the group ring RG of G over R is a twisted group ring with $\gamma(g,h) = 1$. Furthermore, the associative condition on the multiplication implies that

$$\gamma(g,h)\gamma(gh,k) = \gamma(h,k)\gamma(g,hk)$$

and, for this reason, γ is a 2-cocycle.

When $G = C_n = \langle g \rangle$, a cyclic group of order n and $R = \mathbb{F}$, a field, we have the following well-known result. See for example, [14], Theorem 3.1.

Lemma 1.1. *Let $C_n = \langle g \rangle$ be a cyclic group of order n and A be a finite C_n-module, i.e., A is a finite abelian group with an action of C_n in A. Let $A^{C_n} = \{a \in A : a^{g^i} = a \text{ for all } g^i \in C_n\}$. Also, define the norm map $N : A \to A^{C_n}$ by $N(a) = \prod_{i=0}^{n-1} a^{g^i}$.*

Then, for every $\lambda \in A^{C_n}$, we have that $\gamma_\lambda : C_n \times C_n \to A$ defined by

$$\gamma_\lambda(g^i, g^j) = \begin{cases} 1, & i+j < n \\ \lambda, & i+j \geq n \end{cases}$$

is a 2-cocycle and $H^2(C_n, A) = \{[\gamma_\lambda] : \lambda \in A\} \cong A^{C_n}/Im(N)$.

It is possible make a *diagonal* change of basis by replacing each $\overline{g}$ by $\widetilde{g} = \delta(g)\overline{g}$ for some $\delta(g) \in \mathcal{U}(R)$ and, with this change of basis, $R^\gamma G$ is realized in a second way as a twisted group ring of G over R with twisting

$$\widetilde{\gamma}(g,h) = \delta(g)\delta(h)\delta(gh)^{-1}\gamma(g,h).$$

In this case, we say that γ and $\widetilde{\gamma}$ are *cohomologous*.

Lemma 1.2. [17, Lemma 2.1] *The following relations hold in $R^\gamma G$*

i. $1 = \gamma(1,1)^{-1}\overline{1}$

ii. For all $g \in G$,

$$\overline{g}^{-1} = \gamma(g,g^{-1})^{-1}\gamma(1,1)^{-1}\overline{g^{-1}} = \gamma(g^{-1},g)^{-1}\gamma(1,1)^{-1}\overline{g^{-1}}$$

Let $C_n = \langle g \mid g^n = 1 \rangle$ be a cyclic group of order n, R be a commutative ring and $R^\gamma C_n$ the twisted group algebra with

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n \end{cases}$$

where λ is a unit element of R. Thus, $\overline{g}^2 = \overline{g} \cdot \overline{g} = \gamma(g,g)\overline{g^2}$, so we can make a diagonal change of basis and replace $\overline{g^k}$ by $\overline{g}^k$, for all k, $1 \leq k \leq n$. Thus, there exists a unit element $a \in R$ such that $\overline{g}^n = a \cdot 1$ which implies that $R^\gamma C_n$ is a commutative ring.

2. Constacyclic codes over finite commutative rings

In this section, we shall study constacyclic codes over a finite commutative ring. The next result was proved for finite fields in [8], Example 2.5. We shall generalize this result and give an explicit proof for finite commutative rings.

Theorem 2.1. *Let R be a finite commutative ring , $C_n = \langle g \mid g^n = 1\rangle$ a cyclic group of order n and $\mathcal{C}$ be a linear code over R^n. Consider the linear mapping $\varphi : R^n \longrightarrow R^\gamma C_n$ given by $\varphi(c_0, c_1, \cdots, c_{n-1}) = c_0\overline{1} + c_1\overline{g} + \cdots + c_{n-1}\overline{g^{n-1}}$. Then, $\mathcal{C}$ is a λ-constacyclic code if and only if $\varphi(\mathcal{C})$ is an ideal of $R^\gamma C_n$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j + k \geq n \\ 1, & \text{if } j + k < n. \end{cases}$$

Proof. Let $\mathcal{C}$ be a linear code over $\mathbb{F}$. Suppose that $\mathcal{C}$ is a λ-constacyclic code and let $x = \varphi(c_0, c_1, \cdots, c_{n-1})$. Then, $x = c_0\overline{1} + c_1\overline{g} + \cdots + c_{n-1}\overline{g^{n-1}}$ and

$$\begin{aligned} &\overline{g} \cdot x = \\ &= \overline{g} \cdot (c_0\overline{1} + c_1\overline{g} + \cdots + c_{n-1}\overline{g^{n-1}}) = c_0\overline{g} \cdot \overline{1} + c_1\overline{g} \cdot \overline{g} + \cdots + c_{n-1}\overline{g} \cdot \overline{g^{n-1}} \\ &= c_0 \cdot \overline{g} + c_1\overline{g^2} + \cdots + c_{n-1}\lambda \cdot \overline{1} \\ &= \varphi(\lambda c_{n-1}, c_0, \cdots, c_{n-2}). \end{aligned}$$

Since $\mathcal{C}$ is λ-constacyclic, by hypothesis, we have $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$, this implies $\varphi(\mathcal{C})$ is an ideal of $R^\gamma C_n$.

On the other hand, if $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, then $\overline{g} \cdot \varphi(c_0, c_1, \cdots, c_{n-1}) \in \varphi(\mathcal{C})$, so $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$ and $\mathcal{C}$ is λ-constacyclic. □

Now, we shall study *isometries* between constacyclic codes.

Definition 2.2. *Let R be a finite commutative ring, G be a finite group and let λ, μ be elements of $\mathcal{U}(R)$. We say that an isomorphism of R algebra*

$$\varphi : R^\lambda G \longrightarrow R^\mu G.$$

is an isometry if it preserves the Hamming distance on the algebras, i.e.,

$$d_H(\varphi(a), \varphi(a')) = d_H(a, a').$$

In [12], Ginosar and Moreno have obtained a criterion for isometries between *crossed products*. Since twisted group algebras consist a particular case of crossed product, the result is also true for constacyclic codes.

So, given a commutative ring R and a group G, we say the twisted group algebras $R^{\gamma_1}G$, with basis $\overline{G}$, and $R^{\gamma_2}G$, with basis $\widetilde{G}$, are *equivalent* if there exists an R-algebra isomorphism

$$f : R^{\gamma_1}G \longrightarrow R^{\gamma_2}G$$

and a mapping $\delta : G \longrightarrow \mathcal{U}(R)$ such that $f(\overline{g}) = \delta(g)\widetilde{g}$, for all $g \in G$.

Lemma 2.3. [15, Lemma 1.1] *Let R be a finite commutative ring and G be a group. The twisted group algebras $R^{\gamma_1}G$ and $R^{\gamma_2}G$ are equivalent if and only if γ_1 and γ_2 are cohomologous.*

Proposition 2.4. [12, Theorem 3.5] *Let R be a commutative ring, G be a finite group of order n. There exists an isometry between the twisted group algebras $R^{\gamma_1}G$ and $R^{\gamma_2}G$ if and only if γ_1 and γ_2 are cohomologous.*

Now, we have the following

Proposition 2.5. *Let R be a commutative ring, $C_n = \langle g \mid g^n = 1\rangle$ be a cyclic group of order n and λ, β elements of $\mathcal{U}(R)$. Then, the twisted group algebras $R^{\gamma_\lambda}C_n$ and $R^{\gamma_\beta}C_n$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases} \quad \gamma_\beta(g^j, g^k) = \begin{cases} \beta, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

are equivalent if and only if there exists a unity a of R such that $\lambda = a^n\beta$.

Proof. Suppose that $R^{\gamma_\lambda}C_n$ and $R^{\gamma_\beta}C_n$ are equivalent. By Lemma 2.3, there exist a mapping $\theta : C_n \longrightarrow \mathcal{U}(R)$ such that $\gamma_\lambda(g^j, g^k) = \theta(g^j)\theta(g^k)\theta(g^{j+k})^{-1}\gamma_\beta(g^j, g^k)$, for all $0 \leq i, k \leq n-1$. So, $1 = \gamma_\lambda(1, g) = \theta(1)\theta(g)\theta(g)^{-1}\gamma_\beta(1, g) = \theta(1)$. Furthermore, $1 = \gamma_\lambda(g, g) = \theta(g)\theta(g)\theta(g^2)^{-1}\gamma_\beta(g, g) \Rightarrow \theta(g^2) = \theta(g)^2$. Now, $1 = \gamma_\lambda(g, g^2) = \theta(g)\theta(g^2)\theta(g^3)^{-1}\gamma_\beta(g, g^2) \Rightarrow \theta(g^3) = \theta(g)^3$.

Consequently, for all $k < n$, we have

$$1 = \gamma_\lambda(g, g^{k-1}) = \theta(g)\theta(g^{k-1})\theta(g^k)^{-1}\gamma_\beta(g, g^{k-1}) \Rightarrow \theta(g^k) = \theta(g)^k.$$

This shows us $\lambda = \gamma_\lambda(g, g^{n-1}) = \theta(g)\theta(g^{n-1})\theta(1)^{-1}\gamma_\beta(g, g^{n-1}) = \theta(g)^n\beta$ and, taking $a = \theta(g)$, we have $\lambda = a^n\beta$.

On the other hand, if $\lambda = a^n\beta$, for some $a \in \mathcal{U}(R)$, we can define $\theta : C_n \longrightarrow \mathcal{U}(R)$ by $\theta(g^i) = a^i$ and it is not difficult to see that $\gamma_\lambda(g^j, g^k) = \theta(g^j)\theta(g^k)\theta(g^{i+k})^{-1}\gamma_\beta(g^j, g^k)$, for all $0 \leq i, k \leq n-1$. □

Corollary 2.6. *Let R be a commutative ring and let $C_n = \langle g \mid g^n = 1\rangle$ be a cyclic group of order n. Then, the twisted group algebra $R^\gamma C_n$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

is equivalent to the group algebra RC_n if and only if there exists a unity a of R such that $\lambda = a^n$.

Notice that if we take $R = \mathbb{F}_q$, a finite field with q elements, in Proposition 2.5 and Corollary 2.6, we have Theorem 3.2 and Corollary 3.4 obtained in [3]. Also, taking $\lambda = -1$, we obtain Lemma 4.8 of [12].

Corollary 2.7. [3, Corollary 3.5] *Let n be a positive integer such that gcd(n,q-1)=1, $\mathbb{F}_q$ be a finite field with q elements and let $C_n = \langle g \mid g^n = 1\rangle$ be a cyclic group of order n. Then, the twisted group algebra $\mathbb{F}_q^\gamma C_n$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

is equivalent to the group algebra $\mathbb{F}_qC_n$.

3. The k-Galois form

In this section, we shall give definitions and some known results which have elementary proofs in twisted group algebras language.

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, G be a finite group and $\mathbb{F}_q^\gamma G$ the twisted group algebra of G over $\mathbb{F}_q$. Given $\alpha = \sum_{g\in G} \alpha_g \overline{g}$, $\beta = \sum_{g\in G} \beta_g \overline{g}$ two elements of $\mathbb{F}_q^\gamma G$, for each k, $0 \leq k < m$, we define the *k-Galois form* on $\mathbb{F}_q^\gamma G$ as

$$[\alpha,\beta]_k = \sum_{g\in G} \alpha_g \beta_g^{p^k}.$$

It is not difficult to see that k-Galois form is just the Euclidean inner product if $k = 0$. Thus, given a twisted group code $\mathcal{C}$, we can define the *k-Galois dual code of $\mathcal{C}$* as

$$\mathcal{C}^{\perp_k} = \{\beta \in \mathbb{F}_q^\gamma G \mid [\alpha,\beta]_k = 0, \forall\, \alpha \in \mathcal{C}\}.$$

Given two non-zero elements λ and β of $\mathbb{F}_q$, we say that a linear code $\mathcal{C}$ is *$\lambda-\beta$-constacyclic* if $\mathcal{C}$ is $\lambda-$constacyclic and β-constacyclic. Dinh, in [9], proved if $\lambda \neq \beta$, the only $\lambda-\beta$-constacyclic codes are $\{0\}$ and $\mathbb{F}_q^n$.

In terms of twisted group algebras, we have

Lemma 3.1. [9, Proposition] *Let $\mathbb{F}_q$ be a finite field with $p = q^m$ elements and let $C_n = \langle g \mid g^n = 1\rangle$ be a cyclic group of order n and λ, β non-zero elements of $\mathbb{F}_q$. Consider the twisted group algebras $\mathbb{F}_q^{\gamma_\lambda} C_n$ and $\mathbb{F}_q^{\gamma_\beta} C_n$ where*

$$\gamma_\lambda(g^j,g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases} \quad \gamma_\beta(g^j,g^k) = \begin{cases} \beta, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

If $\mathcal{C}$ is a non-zero λ-constacyclic and also β-constacyclic code, then $\lambda = \beta$.

Proposition 3.2. [11, Lemma 4.3] *Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda} C_n$ the twisted group algebra of C_n over $\mathbb{F}_q$ where*

$$\gamma_\lambda(g^j,g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

Then, if $\mathcal{C}$ is a λ-constacyclic code, its k-Galois dual $\mathcal{C}^{\perp_k}$ is a $\lambda^{-p^{m-k}}$-constacyclic code.

Definition 3.3. *Let $\mathcal{C}$ be a constacyclic code over a finite field $\mathbb{F}_q$. We say that $\mathcal{C}$ is a linear complementary k-Galois dual code (k-Galois LCD code for shorty) if $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$.*

By Lemma 3.1 and Proposition 3.2, we get

Corollary 3.4. [16, Corollary 3.3] *If $\lambda^{1+p^{m-k}} \neq 1$, then any λ-constacyclic code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-Galois LCD code.*

Notice that, since $\mathcal{C}^{\perp_k}$ is a linear subspace and the $k-$Galois form is non-degenerate, we have that $\dim \mathcal{C} + \dim \mathcal{C}^{\perp_k} = n$.

4. The classical involution

Let R be a commutative ring with identity and let G be a group. Consider the following mapping $^* : R^\gamma G \longrightarrow R^\gamma G$ given by $\left(\sum_{g\in G} \alpha_g \overline{g}\right)^* = \sum_{g\in G} \alpha_g \overline{g}^{-1}$.

It is not difficult to see the mapping * above defined has the following property $(\alpha+\beta)^* = \alpha^* + \beta^*$

Now, since, by Lemma 1.2, $\overline{g}^{-1} = \gamma(g,g^{-1})^{-1}\overline{g^{-1}} = \gamma(g^{-1},g)^{-1}\overline{g^{-1}}$, we have that

$$(\overline{g}^*)^* = \left(\overline{g}^{-1}\right)^* = \left(\gamma(g,g^{-1})^{-1}\overline{g^{-1}}\right)^*$$
$$= \gamma(g^{-1},g)^{-1}\overline{g^{-1}}^{-1}$$
$$= \gamma(g^{-1},g)^{-1}\gamma(g^{-1},g)^{-1}\overline{(g^{-1})^{-1}} = \gamma(g,g^{-1})^{-2}\overline{g}$$

for all $g \in G$. So, we can conclude if $\gamma(g,g^{-1})^2 = 1$, then $(\alpha^*)^* = \alpha$, for all $\alpha \in R^\gamma G$. Now,

$$\left(\overline{g}\cdot\overline{h}\right)^* = \left(\gamma(g,h)\overline{gh}\right)^* = \gamma(g,h)\overline{gh}^{-1}$$
$$= \gamma(g,h)\gamma(gh,h^{-1}g^{-1})\overline{h^{-1}g^{-1}}$$

Since γ is a 2-cocycle, we get that

$$\gamma(gh,h^{-1}g^{-1}) = \gamma(g,g^{-1})\gamma(h,h^{-1})\gamma(g,h)^{-1}\gamma(h^{-1},g^{-1})^{-1},$$

so $\left(\overline{g}\cdot\overline{h}\right)^* = \gamma(g,g^{-1})\gamma(h,h^{-1})\gamma(h^{-1},g^{-1})^{-1}\overline{h^{-1}g^{-1}}$.

On the other hand,

$$\overline{h}^*\overline{g}^* = \overline{h}^{-1}\cdot\overline{g}^{-1} = \gamma(h,h^{-1})\gamma(g,g^{-1})\overline{h^{-1}}\cdot\overline{g^{-1}}$$
$$= \gamma(h,h^{-1})\gamma(g,g^{-1})\gamma(h^{-1},g^{-1})\overline{h^{-1}g^{-1}}.$$

Thus, $\left(\overline{g}\cdot\overline{h}\right)^* = \overline{h}^*\overline{g}^*$ if and only if $\gamma(h^{-1},g^{-1})^{-1} = \gamma(h^{-1},g^{-1})$, for all $g, h \in G$. Consequently, we conclude $(\alpha\beta)^* = \beta^*\alpha^*$, for all $\alpha, \beta \in R^\gamma G$ if, and only if, $\gamma(g,h)^2 = 1$, for all $g, h \in G$.

Definition 4.1. *Let R be a commutative ring with identity and let G be a group. The mapping $^*: R^\gamma G \longrightarrow R^\gamma G$ given by $\left(\sum_{g\in G}\alpha_g\overline{g}\right)^* = \sum_{g\in G}\alpha_g\overline{g}^{-1}$ with $\gamma(g,h)^2 = 1$, is called the classical involution of $R^\gamma G$.*

Lemma 4.2. *Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda}C_n$ the twisted group algebra of C_n over $\mathbb{F}_q$ where*

$$\gamma_\lambda(g^j,g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

Given two arbitrary elements $\alpha = \sum_{i=0}^{n-1}\alpha_i\overline{g}^i$ and $\beta = \sum_{i=0}^{n-1}\beta_i\overline{g}^i$ of $\mathbb{F}_q^{\gamma_\lambda}C_n$, let us denote by $\beta^{(p^k)}$ the element $\sum_{i=0}^{n-1}\beta_i^{p^k}\overline{g}^i$. If $\alpha\left(\beta^{(p^k)}\right)^* = 0$ and $\lambda^2 = 1$, then $[\alpha,\beta]_k = 0$.

Proof. It is not difficult to see, the coefficient of $1 = \overline{1}$ in the product $\alpha\left(\beta^{(p^k)}\right)^*$ is exactly $[\alpha,\beta]_k$. Since, by hypothesis, $\alpha\left(\beta^{(p^k)}\right)^* = 0$, we have $[\alpha,\beta]_k = 0$. □

5. Euclidean constacyclic LCD codes

In this section, we shall characterize negacyclic LCD codes in terms of its idempotent generator with respect to Euclidean inner product.

Let $\mathbb{F}_q$ be a finite field, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda}C_n$ the twisted group algebra of C_n over $\mathbb{F}_q$ where

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

for some non-zero $\lambda \in \mathbb{F}_q$. Given $\alpha = \sum_{g \in C_n} \alpha_g \overline{g}$, $\beta = \sum_{g \in C_n} \beta_g \overline{g}$ two elements of $\mathbb{F}_q^{\gamma_\lambda} C_n$, we define the *Euclidean inner product* on $\mathbb{F}_q^{\gamma_\lambda} C_n$ as

$$[\alpha, \beta] = \sum_{g \in G} \alpha_g \beta_g.$$

Let $\mathcal{C}$ be a constacyclic code over $\mathbb{F}_q^{\gamma} C_n$, that is, an ideal of $\mathbb{F}_q^{\gamma_\lambda} C_n$. It is well-known that the set $\mathcal{C}^\perp = \{x \in R^\gamma G \mid [x, \alpha] = 0, \forall \alpha \in \mathcal{C}\}$ is an ideal in the twisted group algebra $\mathbb{F}_q^{\gamma_{\lambda^{-1}}} C_n$ where

$$\gamma_{\lambda^{-1}}(g^j, g^k) = \begin{cases} \lambda^{-1}, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

Definition 5.1. *Let $\mathcal{C}$ be a constacyclic code over a finite field $\mathbb{F}_q$. We say that $\mathcal{C}$ is a linear complementary dual code (LCD code for shorty) if $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$.*

Notice that, the Corollary 3.4 shows us if $\lambda^2 \neq 1$, any λ-constacyclic code $\mathcal{C}$ is LCD. Also, the proof o the next result is similar to the proof in the case of cyclic codes given by [7] in Theorem 3.1.

Proposition 5.2. *Let $\mathbb{F}_q$ be a finite field, $C_n = \langle g, g^n = 1 \rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda} C_n$ the twisted group algebra of C_n over $\mathbb{F}_q$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

for some non-zero $\lambda \in \mathbb{F}_q$. If $\lambda^2 = 1$, then $\mathcal{C}$ is a λ-constacyclic LCD code if and only if $\mathcal{C}$ is generated by an idempontent e such that $e = e^*$.

Corollary 5.3. [7, Theorem 3.1] *Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, $C_n = \langle g, g^n = 1 \rangle$ be a cyclic group of order n. A cyclic code $\mathcal{C}$ is a LCD code with respect the Euclidean inner product if and only if $\mathcal{C} = \langle e \rangle$ such that $e^2 = e$ and $e = e^*$.*

6. Some good LCD codes

In this section, we shall exhibit some LCD codes obtained from twisted group algebras. These codes have the same weight of the best codes known, thus they are good LCD codes.

Example 6.1. *Let $C_{10} = \langle g, g^{10} = 1 \rangle$ be a cyclic group of order 10 and let $\mathbb{F}_3$ be a finite field with 3 elements. Consider the twisted group algebra $\mathbb{F}_3^{\gamma_2} C_{10}$, thus in this case, we have $\overline{g}^{10} = 2$. Finally, taking the elements $e = \overline{g}^8 + 2\overline{g}^6 + \overline{g}^4 + 2\overline{g}^2 + 2$ and $f = 2\overline{g}^8 + \overline{g}^6 + 2\overline{g}^4 + \overline{g}^2 + 2$.*

It is not difficult to see $e^2 = e$ and $e^* = 2 \cdot 2\overline{g}^2 + 2 \cdot \overline{g}^4 + 2 \cdot 2 \cdot \overline{g}^6 + 2 \cdot \overline{g}^8 + 2 = e$.

So, by Proposition 5.2, the code $\mathcal{C}$ generated by e is a LCD code of dimension of dimension 8 and weight 2 which are exactly the parameters of the best [10,8] code known.

Finally, notice that $f = 1 - e$, so it is also an idempotent with $f^* = f$ and the code generated by f is LCD of dimension 2 and weight 5 and the best [10,2] code known has weight 7.

Example 6.2. *Let $C_9 = \langle g,\ g^9 = 1\rangle$ be a cyclic group of order 5 and let $\mathbb{F}_5$ be a finite field with 5 elements. Consider the twisted group algebra $\mathbb{F}_5^{\gamma_4}C_9$, thus in this case, we have $\overline{g}^9 = 4$. Finally, taking the elements $e = \overline{g}^8+4\overline{g}^7+3\overline{g}^6+4\overline{g}^5+\overline{g}^4+2\overline{g}^3+\overline{g}^2+4\overline{g}+3$ and $f = 4\overline{g}^8+\overline{g}^7+2\overline{g}^6+\overline{g}^5+4\overline{g}^4+3\overline{g}^3+4\overline{g}^2+\overline{g}+3$.*

It is not difficult to see $e^2 = e$ and

$$e^* = 4\overline{g} + 4\cdot 4\cdot \overline{g}^2 + 3\cdot 4\cdot \overline{g}^3 + 4\cdot 4\cdot \overline{g}^4 + 4\cdot \overline{g}^5 + 2\cdot 4\cdot \overline{g}^6 + 4\cdot \overline{g}^7 + 4\cdot 4\cdot \overline{g}^8 + 3 = e.$$

So, by Proposition 5.2, the code $\mathcal{C}$ generated by e is a LCD code of dimension of dimension 7 and weight 2 which are exactly the parameters of the best [9,7] code known.

Finally, notice that $f = 1 - e$, so it is also an idempotent with $f^* = f$ and the code generated by f is LCD of dimension 2 and weight 6 and the best [9,2] code known has weight 7.

Example 6.3. *Let $C_{21} = \langle g,\ g^{21} = 1\rangle$ be a cyclic group of order 21 and let $\mathbb{F}_5$ be a finite field with 5 elements. Consider the twisted group algebra $\mathbb{F}_5^{\gamma_4}C_{21}$, thus in this case, we have $\overline{g}^{21} = 4$. Finally, taking the element*

$$e = 4\overline{g}^{19} + 4\overline{g}^{18} + \overline{g}^{15} + 2\overline{g}^{14} + 4\overline{g}^{13} + 4\overline{g}^{12} + 4\overline{g}^{11} + \overline{g}^{10} + \overline{g}^9 + \overline{g}^8 + 3\overline{g}^7 + 4\overline{g}^6 + \overline{g}^3 + \overline{g}^2 + 1$$

and

$$f = \overline{g}^{19} + \overline{g}^{18} + 4\overline{g}^{15} + 3\overline{g}^{14} + \overline{g}^{13} + \overline{g}^{12} + \overline{g}^{11} + 4\overline{g}^{10} + 4\overline{g}^9 + 4\overline{g}^8 + 2\overline{g}^7 + \overline{g}^6 + 4\overline{g}^3 + 4\overline{g}^2\ .$$

It is not difficult to see $e^2 = e$ and

$$e^* = 4\cdot 4\overline{g}^2 + 4\cdot 4\cdot \overline{g}^3 + 4\cdot \overline{g}^6 + 2\cdot 4\cdot \overline{g}^7 + 4\cdot\cdot 4\overline{g}^8 + 4\cdot 4\cdot \overline{g}^9 + 4\cdot\cdot 4\overline{g}^{10} + 4\cdot \overline{g}^{11}$$
$$+4\cdot \overline{g}^{12} + 4\cdot \overline{g}^{13} + 3\cdot 4\cdot \overline{g}^{14} + 4\cdot 4\cdot \overline{g}^{15} + 4\cdot \overline{g}^{18} + 4\cdot \overline{g}^{19} = e.$$

So, by Proposition 5.2, the code $\mathcal{C}$ generated by e is a LCD code of dimension of dimension 6 and weight 12 which are exactly the parameters of the best [21,6] code known.

Finally, notice that $f = 1 - e$, so it is also an idempotent with $f^* = f$ and the code generated by f is LCD of dimension 15 and weight 3 and the best [21,15] code known has weight 5.

Example 6.4. *Let $C_{19} = \langle g,\ g^{19} = 1\rangle$ be a cyclic group of order 19 and let $\mathbb{F}_7$ be a finite field with 7 elements. Consider the twisted group algebra $\mathbb{F}_7^{\gamma_6}C_{19}$, thus in this case, we have $\overline{g}^{19} = 6$. Finally, taking the elements*

$$e = 3\overline{g}^{18} + 6\overline{g}^{17} + \overline{g}^{16} + 5\overline{g}^{15} + \overline{g}^{14} + 5\overline{g}^{13} + 3\overline{g}^{12} + 4\overline{g}^{11} + 2\overline{g}^{10} + 5\overline{g}^9 + 3\overline{g}^8 + 4\overline{g}^7$$
$$+2\overline{g}^6 + 6\overline{g}^5 + 2\overline{g}^4 + 6\overline{g}^3 + \overline{g}^2 + 4\overline{g}$$

and

$$f = 4\overline{g}^{18} + \overline{g}^{17} + 6\overline{g}^{16} + 2\overline{g}^{15} + 6\overline{g}^{14} + 2\overline{g}^{13} + 4\overline{g}^{12} + 3\overline{g}^{11} + 5\overline{g}^{10} + 2\overline{g}^9 + 4\overline{g}^8 + 3\overline{g}^7$$
$$+5\overline{g}^6 + \overline{g}^5 + 5\overline{g}^4 + \overline{g}^3 + 6\overline{g}^2 + 3\overline{g} + 1\ .$$

It is not difficult to see $e^2 = e$ and

$$e^* = 3\cdot 6\overline{g} + 6\cdot 6\overline{g}^2 + 6\overline{g}^3 + 5\cdot 6\overline{g}^4 + 6\overline{g}^5 + 5\cdot 6\overline{g}^6 + 3\cdot 6\overline{g}^7 + 4\cdot 6\overline{g}^8$$
$$+2\cdot 6\overline{g}^9 + 5\cdot 6\overline{g}^{10} + 3\cdot 6\overline{g}^{11} + 4\cdot 6\overline{g}^{12} + 2\cdot 6\overline{g}^{13} + 6\cdot 6\overline{g}^{14} + 2\cdot 6\overline{g}^{15} + 6\cdot 6\overline{g}^{16}$$
$$+6\cdot \overline{g}^{17} + 4\cdot 6\overline{g}^{18} = e.$$

So, by Proposition 5.2, the code $\mathcal{C}$ generated by e is a LCD code of dimension of dimension 7 and weight 10 which are exactly the parameters of the best [19,7] code known.

Finally, notice that $f = 1 - e$, so it is also an idempotent with $f^* = f$ and the code generated by f is LCD of dimension 12 and weight 6 which are exactly the parameters of the best [19,12] code known.

Now, we shall summarize those codes obtained above in the following table.

Field	Best $[n,k,d]$ code known	$[n,k,d]$ code obtained
$\mathbb{F}_3$	[10,8,2]	[10,8,2]
$\mathbb{F}_3$	[10,2,7]	[10,2,5]
$\mathbb{F}_5$	[9,7,2]	[9,7,2]
$\mathbb{F}_5$	[9,2,7]	[9,2,6]
$\mathbb{F}_5$	[21,6,12]	[21,6,12]
$\mathbb{F}_5$	[21,15,5]	[21,15,3]
$\mathbb{F}_7$	[19,7,10]	[19,7,10]
$\mathbb{F}_7$	[19,12,6]	[19,12,6]

7. k-Galois constacyclic LCD codes

In this section, we shall prove some results about k-Galois constacyclic LCD codes.

Theorem 7.1. *Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda} C_n$ the twisted group algebra of C_n over $\mathbb{F}_q$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

Let e be an idempotent of $\mathbb{F}_q^{\gamma_\lambda} C_n$ and $\lambda^2 = 1$. Then $e = e(e^{(p^k)})^*$ if, and only if $[e, 1-e]_k = 0$.

Proof. Suppose that e is an idempotent such that $e = e(e^{(p^k)})^*$. Then, $e - e(e^{(p^k)})^* = e(1 - (e^{(p^k)})^*) = e\left((1-e)^{(p^k)}\right)^* = 0$ and, by Lemma 4.2, $[e, 1-e]_k = 0$.

On the other hand, if $[e, 1-e]_k = 0$, we have that $[1, e^*(1-e)^{(p^k)}]_k = 0$. Now, given $a = \sum_{i=0}^{n-1} a_i \overline{g}^i$ and $b = \sum_{i=0}^{n-1} b_i \overline{g}^i$ two arbitrary elements of $\mathbb{F}_q^{\gamma_\lambda} C_n$, since $\lambda^{p^k} = \lambda^{-1}$, then

$$[\overline{g}a, \overline{g}b]_k = a_0 b_0^{p^k} + a_1 b_1^{p^k} + \cdots + a_{n-2} b_{n-2}^{p^k} + (a_{n-1}\lambda)(b_{n-1}^{p^k}\lambda^{p^k}) = [a,b]_k$$

So $[\overline{g}, \overline{g}e^*(1-e)^{(p^k)}]_k = 0$, for all $g \in G$. Since the k-Galois form is non-degenerated, we get that $e^*(1-e)^{(p^k)} = 0$ and $e^* = e^* e^{(p^k)}$. Then, $e = (e^*)^* = (e^* e^{(p^k)})^* = e(e^{(p^k)})^*$. □

Now, we have the following

Proposition 7.2. *Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda} C_n$ the twisted group algebra of C_n over $\mathbb{F}_q$ where*

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

If $\lambda^2 = 1$, then $\mathcal{C}$ is a λ-constacyclic code generated by an idempontent e such that $e = e(e^{(p^k)})^*$ if, and only if $\mathcal{C}$ is k-Galois LCD code.

Proof. First of all, if $\mathcal{C}$ is a λ-constacyclic code which is also k-Galois LCD, we have the following decomposition of ideals $\mathbb{F}_q^{\gamma}C_n = \mathcal{C} \oplus \mathcal{C}^{\perp_k}$ since $\lambda^{1+p^{m-k}} = 1$.

It is well-know that there exist idempotents e and f such that $1 = e + f$, $e \cdot f = 0$, $\mathcal{C} = \langle e \rangle$ and $\mathcal{C}^{\perp_k} = \langle f \rangle$. Then, writing $f = 1 - e$, we get $[e, 1-e]_k = 0$, so, by Theorem 7.1, the equality $e = e(e^{(p^k)})^*$ holds.

If $\mathcal{C}$ is generated by an idempontent e such that $e = e(e^{(p^k)})^*$, by Theorem 7.1, we have $[e, 1-e]_k = 0$. Then, writing $1 = e + (1 - e)$ we have $\mathbb{F}_q^{\gamma}C_n = \mathcal{C} \oplus \mathbb{F}_q^{\gamma}C_n(1 - e)$. Since $[e, 1 - e]_k = 0$ and $dim_{\mathbb{F}_q}\mathcal{C} + dim_{\mathbb{F}_q}\mathbb{F}_q^{\gamma}C_n(1 - e) = n$, we conclude that $\mathcal{C}^{\perp_k} = \mathbb{F}_q^{\gamma}C_n(1 - e)$. Thus, $\mathcal{C}$ is a λ-constacyclic k-Galois LCD code. □

8. Conclusion and future remarks

In this paper, we have characterized k-Galois LCD constacyclic codes over finite fields using twisted group algebras structure and we have found some good LCD codes.

For future research, we shall consider constacyclic codes over finite commutative chain rings and investigate if the characterization obtained for LCD codes is also true.

Data availability.

All data are available from the authors upon reasonable request.

Conflict of interest

All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.

This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript

References

[1] G. K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, Finite Fields Their Applications 18 (2012) 362–377.
[2] B. Chen, H. Q. Dinh, H. Liu, L. Wang, Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u \cdot \mathbb{F}_{p^m}$, Finite Fields Their Applications, 37 (2016) 108–130.
[3] H. B. Chen, Y. Fan, L. Lin, H. B. Liu, Constacyclic codes over finite fields, Finite Fields Their Applications, 18 (2012) 1217–1231.
[4] C. Carlet Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monograph Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge

University Press, Cambridge (2010) 257–397.
[5] C. Carlet, S. Guilley, Complementary dual codes for counter measures to side-channel attacks, E.R. Pinto et. al. (Eds) Coding Theory and applications, CIM series in Mathematical Sciences, 97-105, Springer Verlag 2014, J. Adv. in Math. of Comm. 10(1) (2016) 131–150
[6] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pelikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, IEEE Transactions on Information Theory, 64(04) (2018) 3010–3017
[7] J. de la Cruz, W. Willems, On group codes with complementary duals, Des. Codes Cryptogr. 86 (2018) 2065–2073.
[8] J. de la Cruz, W. Willems, Twisted group codes, IEEE Transaction on Information Theory, 67, issue 08 (2021) 5178–5184.
[9] H. Q. Dinh, Repeated-root cyclic codes of length $6p^s$, AMS Contemp. Math. 609 (2014) 69–87.
[10] H. Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Finite Fields Their Applications, 324 (2010) 940–950.
[11] Y. Fan, L. Zhang, Galois self-dual constacyclic codes, Des. Codes Cryptogr. 84 (2016) 473–492.
[12] Y. Ginosar, A. R. Moreno, Crossed Products and Coding Theory, IEEE Transaction on Information Theory, 65. issue 10 (2019) 6224–6233.
[13] T. Hurley, D. Hurley, Coding theory: the unit-derived methodology, Int. J. Informationand Coding Theory, 5(1) (2018) 55–80.
[14] G. Karpilovsky, Projective representations of finite groups, Marcel Dekker, Inc., New Yourk (1985).
[15] G. Karpilovsky, Group representation II, North-Holland Mathematics Studies (1992).
[16] X. Liu, Y. Fan, H. Liu, Galois LCD codes over finite fields, Finite Fields Their Applications, 49 (2018) 227–242.
[17] D. S. Passman, The algebraic structure of group rings, John Wiley & Sons, Inc., New York (1940).