Journal of Algebra and Its Applications
(2025) 2550045 (12 pages)

DOI: 10.1142/S0219498825500458



# Crossed product codes

A. Duarte*

*Instituto de Matemãątica e Estatãdstica*
*Universidade de São Paulo, Caixa Postal 66281*
*CEP 05315-970, São Paulo, Brazil*
*alsduarte@usp.br*

A. Pereira

*Universidade Federal Rural do Rio de Janeiro*
*Seropedica, RJ, Brazil, CEP Seropãl'dica - RJ, 23890-000*
*almp1980@ufrrj.br*

C. Polcino Milies

*Instituto de Matemãątica e Estatãdstica*
*Universidade de São Paulo, Caixa Postal 66281*
*CEP 05315-970, São Paulo, Brazil*
*polcino@ime.usp.br*

Received 6 September 2022
Revised 8 December 2022
Accepted 19 January 2023
Published 4 October 2023

Communicated by A. Srivastava

*Dedicated to André Leroy on his retirement*

Bernal *et al.* provided a necessary and sufficient condition for a linear code to be realized as an ideal in a finite group algebra and De La Cruz and Willems proved a similar result for ideals in twisted group algebras. In this paper, we extend this characterization to crossed products. Furthermore, we determine conditions for some crossed product codes to be self-dual.

*Keywords*: Crossed product; coding theory; duality.

Mathematics Subject Classification 2020: 11T71

## 1. Introduction

Let $G = \{1 = g_1, g_2, \ldots, g_n\}$ be a finite group and $\mathbb{F}$ a (finite) field. We denote by $\mathbb{F}^\times$ the group of units in $\mathbb{F}$, i.e. the set of its nonzero elements. A group homomorphism

*Corresponding author.

$\sigma : G \to \mathrm{Aut}(\mathbb{F})$ is called an *action* of $G$ on $\mathbb{F}$. For each $i = 1, \ldots, n$, we denote $\sigma_i = \sigma(g_i) \in \mathrm{Aut}(\mathbb{F})$. Given $\lambda \in \mathbb{F}$, we write ${}^g\lambda = \sigma(g)(\lambda)$, for all $g \in G$. We also denote by

$$\mathbb{F}^\sigma = \{x \in \mathbb{F} \mid \sigma_i(x) = x \text{ for all } 1 \leq i \leq n\},$$

the fixed field of $\sigma(G)$. Furthermore, if $M = [M_{ij}]$ is a matrix over $\mathbb{F}$, we set $\sigma_k(M) = [\sigma_k(M_{ij})]$, for all $k = 1, \ldots, n$.

The map $t : G \times G \to \mathbb{F}^\times$ is called a (*normalized*) *twisting* if

$$\begin{aligned} t(x,y).t(xy,z) &=^x t(y,z).t(x,yz), \\ t(x,1) &= t(1,x) = 1, \end{aligned} \tag{1}$$

for all $x, y, z \in G$.

The *crossed product* $\mathbb{F} *_t^\sigma G$ of $G$ over $\mathbb{F}$ is an associative ring which contains $\mathbb{F}$ and has a copy $\overline{G}$ of $G$ as an $\mathbb{F}$-basis. Each element of $\mathbb{F} *_t^\sigma G$ is uniquely a finite sum $\sum_{i=1}^n a_i \bar{g}_i$, where $a_i \in \mathbb{F}$. The multiplication in $\mathbb{F} *_t^\sigma G$ is defined by the following rules:

$$\bar{x} \cdot \bar{y} = t(x,y)\overline{xy} \quad \text{for all } x, y \in G,$$

$$\bar{x}\lambda = {}^x\lambda\bar{x} \quad \text{for all } x \in G \text{ and } \lambda \in \mathbb{F}.$$

The twisting and action are interrelated by conditions precisely equivalent to $\mathbb{F} *_t^\sigma G$ being associative. The property $\bar{x}\lambda = {}^x\lambda\bar{x}$, for all $x \in G$ and $\lambda \in \mathbb{F}$, implies that the crossed product $\mathbb{F} *_t^\sigma G$ is not a $\mathbb{F}$-algebra unless $\sigma(g)$ is the identity map of $\mathbb{F}$, for all $g \in G$. However, it is a $\mathbb{F}^\sigma$-algebra.

In order to establish a relationship between linear codes in $\mathbb{F}^n$ and ideals in $\mathbb{F} *_t^\sigma G$ we define the function $\varphi : \mathbb{F}^n \to \mathbb{F} *_t^\sigma G$ by

$$\varphi(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^n \lambda_i \bar{g}_i. \tag{2}$$

We shall denote $e_i = (\delta_{i1}, \ldots, \delta_{in}) \in \mathbb{F}^n$, where $\delta_{ij}$ is the Kronecker delta. Then $\varphi$ carries the basis $\{e_1, \ldots, e_n\}$ of $\mathbb{F}^n$ onto the basis $\overline{G}$ of $\mathbb{F} *_t^\sigma G$ and is thus a linear isomorphism.

Let $\mathcal{C} \subset \mathbb{F}^n$ be a subset. We say that $\mathcal{C}$ is a *left crossed product code* if $\mathcal{C}$ is a linear subspace over $\mathbb{F}$ and $\varphi(\mathcal{C})$ is a left ideal of $\mathbb{F} *_t^\sigma G$.

On the other hand, if $\mathcal{C}$ is a right ideal of $\mathbb{F} *_t^\sigma G$, its preimage by $\varphi$ may not be a linear subspace of $\mathbb{F}^n$. Since $\mathbb{F}^n$ is also a vector space over $\mathbb{F}^\sigma$, we call $\mathcal{C}$ a *right crossed product code* if $\mathcal{C}$ is a linear subspace over $\mathbb{F}^\sigma$ and $\varphi(\mathcal{C})$ is a right ideal of $\mathbb{F} *_t^\sigma G$. If $\varphi(\mathcal{C})$ is a two-sided ideal of $\mathbb{F} *_t^\sigma G$ we say that $\mathcal{C}$ is a *crossed product code*.

In the case $\sigma(g)$ is the identity map of $\mathbb{F}$, for all $g \in G$, we say that $\mathcal{C}$ is a *twisted group code* and if $t(x,y) = 1$ for all $x, y \in G$, then $\mathcal{C}$ is a *skew group code*.

Define a bilinear form $\langle \cdot, \cdot \rangle$ on $\mathbb{F} *_t^\sigma G$ by

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

extended linearly to $\mathbb{F} *_t^\sigma G$. As an immediate consequence of the definition, we have $\langle \cdot, \cdot \rangle$ as nondegenerate.

Let $\mathcal{C} \subset \mathbb{F} *_t^\sigma G$. The subset

$$\mathcal{C}^\perp = \{\alpha \in \mathbb{F} *_t^\sigma G \,|\, \langle \alpha, c \rangle = 0, \text{ for all } c \in \mathcal{C}\},$$

of $\mathbb{F} *_t^\sigma G$ is called the *dual* of $\mathcal{C}$. The code $\mathcal{C} \subset \mathbb{F} *_t^\sigma G$ is *self-orthogonal* if $C \subset \mathcal{C}^\perp$ and self-dual if $\mathcal{C} = \mathcal{C}^\perp$.

Let $\mathbb{F} \subset \mathbb{E}$ be an extension of finite fields. An $\mathbb{F}$-*linear* $\mathbb{E}$-*code* of length $n$ is an $\mathbb{F}$-linear subspace of $\mathbb{E}^n$. An additive code over $\mathbb{E}$ is simply an $\mathbb{F}$-linear $\mathbb{E}$-code, where $\mathbb{F}$ is the prime field of $\mathbb{E}$. In [3], self-orthogonal additive codes over $\mathbb{F}_4$ under the trace inner product were connected to binary quantum codes; a similar connection was given in the nonbinary case in [10]. Right crossed product codes are special kind of $\mathbb{F}^\sigma$-linear $\mathbb{F}$-codes of length $n$.

We shall determine conditions for a linear code over $\mathbb{F}^\sigma$ to be a right crossed product code and linear code over $\mathbb{F}$ to be a left crossed product code. In [1, 4] this question was answered for group codes and twisted group codes, respectively, using conditions on the automorphism group of the code. We will follow the same path. Furthermore, we will offer sufficient conditions for crossed product codes to be self-dual.

## 2. Crossed Product Codes

Denote by $\mathrm{Mon}_n(\mathbb{F})$ the group of all monomial $n \times n$ matrices over $\mathbb{F}$. Recall that

$$\mathrm{Aut}(\mathcal{C}) = \{M \in \mathrm{Mon}_n(\mathbb{F}) \,|\, \mathcal{C}M \subset \mathcal{C}\},$$

is the *automorphism group of the code* $\mathcal{C} \subset \mathbb{F}^n$.

Consider a right action of $G$ on $\{1, \ldots, n\}$ given by

$$i.g = j \quad \text{if and only if } g_i g = g_j, \quad \text{for all } 1 \le i,\ j \le n. \tag{3}$$

Let $E_{i,j} = [e_{k\ell}]$ denote the matrix with entries $e_{k\ell} = 1$ if $k = i$ and $\ell = j$, and $e_{k\ell} = 0$ otherwise. For each $g \in G$, we denote

$$[g]_r = \sum_{i=1}^{n} t(g_i, g) E_{i,i.g}.$$

For each $\lambda \in \mathbb{F}$, we set

$$A(\lambda) = \begin{bmatrix} \sigma_1(\lambda) & & \\ & \ddots & \\ & & \sigma_n(\lambda) \end{bmatrix}.$$

**Lemma 1.** *Let $t : G \times G \to \mathbb{F}^\times$ be a twisting. Then*

$$G_r(t) = \{A(\lambda)[g]_r \mid \lambda \in \mathbb{F}^\times, g \in G\},$$

*is a subgroup of the group of monomial matrices.*

**Proof.** For $\lambda, \mu \in \mathbb{F}^\times$ and $g, h \in G$, we have

$$\begin{aligned} A(\lambda)A(\mu) &= A(\lambda\mu), \\ [g]_r[h]_r &= A(t(g,h))[gh]_r, \\ [g]_r A(\lambda) &= A({}^g\lambda)[g]_r, \end{aligned}$$

are all elements of $G_r(t)$. Furthermore, $A(\lambda)^{-1} = A(\lambda^{-1})$ and $([g]_r)^{-1} = A(\gamma)[g^{-1}]_r$ where $\gamma = {}^{g^{-1}}[t(g, g^{-1})^{-1}]$. □

We can now state the following.

**Theorem 2.** *Let $t$ be a twisting of $G$ over $\mathbb{F}$ and $\mathcal{C} \subset \mathbb{F}^n$ a linear code over $\mathbb{F}^\sigma$. Then $\mathcal{C}$ is a right crossed product code if and only if $G_r(t) < \mathrm{Aut}(\mathcal{C})$.*

**Proof.** Let $c = (c_1, \ldots, c_n) \in \mathbb{F}^n$. Since

$$cA(\lambda) = (c_1, \ldots, c_n).\sum_{i=1}^{n} \sigma_i(\lambda)E_{i,i} = \sum_{i=1}^{n} c_i\sigma_i(\lambda)e_i$$

and

$$c[g]_r = (c_1, \ldots, c_n).\sum_{i=1}^{n} t(g_i, g)E_{i,i.g} = \sum_{i=1}^{n} c_i t(g_i, g)e_{i.g},$$

for all $g \in G$ and $\lambda \in \mathbb{F}^\times$, it follows that

$$\begin{aligned} \varphi(cA(\lambda)) &= \varphi\left(\sum_{i=1}^{n} c_i\sigma_i(\lambda)e_i\right) \\ &= \sum_{i=1}^{n} c_i\sigma_i(\lambda)\bar{g}_i \\ &= \varphi(c)\lambda \end{aligned}$$

and

$$\begin{aligned} \varphi(c[g]_r) &= \varphi\left(\sum_{i=1}^{n} c_i t(g_i, g)e_{i.g}\right) \\ &= \sum_{i=1}^{n} c_i t(g_i, g)\overline{g_{i.g}}. \end{aligned}$$

Because of formula (3), $\overline{g_{i.g}} = \overline{g_i g}$, for all $i = 1, \ldots, n$. Then

$$\begin{aligned} \varphi(c[g]_r) &= \sum_{i=1}^{n} c_i t(g_i, g)\overline{g_i g} \\ &= \varphi(c)\bar{g}. \end{aligned}$$

As $\varphi(c[g]_r) = \varphi(c)\bar{g}$ and $\varphi(cA(\lambda)) = \varphi(c)\lambda$, for each $g \in G$ and $\lambda \in \mathbb{F}^\times$, the result follows. □

We can define a left action of $G$ on $\{1, \ldots, n\}$ by

$$g.i = j \quad \text{if and only if } gg_i = g_j, \quad \text{for all } 1 \leq i, j \leq n.$$

Let $\mathbb{F} *_t^\sigma G$ be the crossed product with an action $\sigma : G \to \mathrm{Aut}(\mathbb{F})$ and twisting $t$. Consider $\varphi$ defined as in formula (2). For each $g \in G$, we define

$$[g]_\ell = \sum_{i=1}^{n} t(g, g_i) E_{g.i,i}.$$

For $\lambda \in \mathbb{F}$ denote $B(\lambda) = \mathrm{Diag}(\lambda, \ldots, \lambda)$. Then

$$G_\ell(t) = \{B(\lambda)[g]_\ell \mid \lambda \in \mathbb{F}^\times, g \in G\},$$

is a group with the operation $\star$ defined by

$$B(\lambda)[g]_\ell \star B(\mu)[h]_\ell = B(\lambda \cdot {}^g\mu \cdot t(g, h))[gh]_\ell.$$

The group $G_\ell(t)$ acts on $\mathbb{F}^n$ on the left:

$$[g]_\ell.(c_1, \ldots, c_n) = ({}^g c_1, \ldots, {}^g c_n)[g]_\ell^T,$$

$$B(\lambda).(c_1, \ldots, c_n) = (c_1, \ldots, c_n)B(\lambda),$$

for every $(c_1, \ldots, c_n) \in \mathbb{F}^\times$.

Since $\varphi([g]_\ell.c) = \bar{g}\varphi(c)$ and $\varphi(B(\lambda).c) = \lambda\varphi(c)$, for each $g \in G$ and $\lambda \in \mathbb{F}^\times$, it follows that $\mathcal{C} \subset \mathbb{F}^n$, a linear code (over $\mathbb{F}$), is a left crossed product code if and only if $G_\ell(t).\mathcal{C} \subset \mathcal{C}$.

The remarks above imply the following.

**Theorem 3.** *Let $t$ be a twisting of $G$ over $\mathbb{F}$ and $\mathcal{C} \subset \mathbb{F}^n$ a linear code over $\mathbb{F}$. Then, $\mathcal{C}$ is a crossed product code if and only if $G_r(t)$ is a subgroup of* $\mathrm{Aut}(\mathcal{C})$ *and $G_\ell(t).\mathcal{C} \subset \mathcal{C}$.*

## 3. Dual Crossed Product Codes

Let $\mathbb{F} *_t^\sigma G$ be a crossed product with twisting $t$ and action $\sigma$. Since $t(x, y).t(xy, z) = {}^x t(y, z) \cdot t(x, yz)$, and $({}^x t(y, z))^{-1} = {}^x(t(y, z)^{-1})$, for all $x, y, z \in G$, we get

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

for all $x, y, z \in G$. Based on this observation, we define the twisting $\tau : G \times G \to \mathbb{F}^\times$, with action $\sigma$, by $\tau(g, h) = t(g, h)^{-1}$, for all $g, h \in G$. We consider a crossed product $\mathbb{F} *_\tau^\sigma G$ with elements

$$\sum_{g \in G} a_g \tilde{g},$$

where the product is given by

$$\tilde{g}\tilde{h} = \tau(g,h)\widetilde{gh} \quad \text{and} \quad {}^{g}\lambda\tilde{g} = \tilde{g}\lambda,$$

for all $h, g \in G$ and $\lambda \in \mathbb{F}$.

We define $^* : \mathbb{F} *_t^\sigma G \to \mathbb{F} *_\tau^\sigma G$ by

$$\left(\sum_{g\in G} a_g \bar{g}\right)^* = \sum_{g\in G} {}^{g^{-1}}a_g \, t(g^{-1}, g)\widetilde{g^{-1}}.$$

**Proposition 4.** *The map $\alpha \mapsto \alpha^*$ induces an $\mathbb{F}^\sigma$-algebra anti-isomorphism of $\mathbb{F} *_t^\sigma G$ onto $\mathbb{F} *_\tau^\sigma G$.*

**Proof.** Since $^*$ is an $\mathbb{F}^\sigma$-linear isomorphism, it is enough to prove that

$$(\lambda\bar{g}\mu\bar{h})^* = (\mu\bar{h})^*(\lambda\bar{g})^*,$$

for every $\lambda, \mu \in \mathbb{F}$ and $g, h \in G$.

In fact,

$$(\lambda\bar{g}\mu\bar{h})^* = {}^{h^{-1}g^{-1}}(\lambda\, t(g,h))\; {}^{h^{-1}}(\mu)\; t(h^{-1}g^{-1}, gh)\; \widetilde{h^{-1}g^{-1}}$$

and

$$(\mu\bar{h})^*(\lambda\bar{g})^* = {}^{h^{-1}g^{-1}}(\lambda)\; {}^{h^{-1}}(\mu\, t(g^{-1}, g))\; t(h^{-1}, h)\; \tau(h^{-1}, g^{-1})\, \widetilde{h^{-1}g^{-1}}.$$

As the equality

$$\begin{aligned} t(h^{-1}g^{-1}, gh)\; {}^{h^{-1}g^{-1}}(t(g,h))\, t(h^{-1}, g^{-1}) &= t(h^{-1}g^{-1}, g)t(h^{-1}, h)t(h^{-1}, g^{-1}) \\ &= {}^{h^{-1}}t(g^{-1}, g)\; t(h^{-1}, h), \end{aligned}$$

holds, we have $(\lambda\bar{g}\mu\bar{h})^* = (\mu\bar{h})^*(\lambda\bar{g})^*$, as desired. □

Recall that $^*$ is an *involution* on $\mathbb{F} *_t^\sigma G$ if it is an additive homomorphism satisfying: $(\alpha^*)^* = \alpha$ and $(\alpha\beta)^* = \beta^*\alpha^*$, for all $\alpha, \beta \in \mathbb{F} *_t^\sigma G$.

**Corollary 4.1.** *Assume that $\tau = t$. Then $\alpha \mapsto \alpha^*$ defines an involution on $\mathbb{F} *_t^\sigma G$.*

**Proof.** We shall denote $\bar{g} = \tilde{g}$, for all $g \in G$, because $\tau = t$. Also, note that $t(g,h)^2 = 1$, for all $g, h \in G$. By Proposition 4, it suffices to show that $(\alpha^*)^* = \alpha$, for all $\alpha \in \mathbb{F} *_t^\sigma G$. If $\alpha = \sum_{g\in G} a_g\bar{g}$, then

$$(\alpha^*)^* = \left(\sum_{g\in G} {}^{g^{-1}}(a_g)\, t(g^{-1}, g)\overline{g^{-1}}\right)^* = \sum_{g\in G} {}^{g}({}^{g^{-1}}(a_g)\, t(g^{-1}, g))t(g, g^{-1})\bar{g}.$$

Since ${}^{g}(t(g^{-1}, g)) = t(g, g^{-1})$, we have $(\alpha^*)^* = \alpha$ and the result follows. □

Recall that a finite dimensional $\mathbb{F}$-algebra $A$ is called a *Frobenius algebra* if there exists $f \in \mathrm{Hom}_{\mathbb{F}}(A, \mathbb{F})$ such that the kernel of $f$ contains no proper left or right ideals of $A$.

**Proposition 5.** *The crossed product $\mathbb{F} *_t^\sigma G$ is a Frobenius algebra over $\mathbb{F}^\sigma$.*

**Proof.** Define $f : \mathbb{F} *_t^\sigma G \to \mathbb{F}^\sigma$ by

$$f\left(\sum_{g\in G} a_g \bar{g}\right) = \mathrm{Tr}(a_1), \tag{4}$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}/\mathbb{F}^\sigma}$ is the trace map on the field extension $\mathbb{F}/\mathbb{F}^\sigma$. Since $f$ is linear over $\mathbb{F}^\sigma$, it is enough to prove that $ker(f)$ does not contain left or right ideals of $\mathbb{F} *_t^\sigma G$. By way of contradiction, assume that $I$ is a right ideal of $\mathbb{F} *_t^\sigma G$ such that $\{0\} \neq I \subset ker(f)$. Take $0 \neq \alpha \in I$, and $h \in G$. For every $\lambda \in \mathbb{F}$, we have

$$\alpha(\lambda\overline{h^{-1}}) = \sum_{g\in G} a_g \lambda^g t(g, h^{-1})\overline{gh^{-1}} \in I,$$

implying that

$$0 = f(\alpha(\lambda\overline{h^{-1}})) = \mathrm{Tr}(a_h \lambda^h t(h, h^{-1})).$$

Since the last equality holds for all $\lambda \in \mathbb{F}$, we conclude that $a_h\, t(h, h^{-1}) = 0$, which implies that $a_h = 0$, for all $h \in G$, a contradiction. The proof for left ideals follows in a similar way. □

**Remark.** By [8, Theorem 16.21], the $\mathbb{F} *_t^\sigma G$ is a Frobenius ring. As we observed in the introduction, $\mathbb{F} *_t^\sigma G$ is not a Frobenius algebra over $\mathbb{F}$ unless the action $\sigma$ is trivial, because it is not an associative $\mathbb{F}$-algebra.

Let $f : \mathbb{F} *_t^\sigma G \to \mathbb{F}^\sigma$ be that map defined by the formula (4). The bilinear form $\langle \alpha, \beta \rangle_f = f(\alpha\beta)$ is called the *Frobenius form* of $\mathbb{F} *_t^\sigma G$. Let $\mathcal{C} \subset \mathbb{F} *_t^\sigma G$, we denote by

$$\mathrm{Ann}_r(\mathcal{C}) = \{\alpha \in \mathbb{F} *_t^\sigma G \,|\, c\alpha = 0 \text{ for all } c \in \mathcal{C}\}$$

and by

$$\mathrm{Ann}_\ell(\mathcal{C}) = \{\alpha \in \mathbb{F} *_t^\sigma G \,|\, \alpha c = 0 \text{ for all } c \in \mathcal{C}\},$$

the *right annihilator* and *left annihilator* of $\mathcal{C}$ in $\mathbb{F} *_t^\sigma G$, respectively. We refer to [8, Lemma 16.38] for a proof of the following result.

**Lemma 6.** *The following statements hold*:

(i) *If $\mathcal{C}$ is a left ideal of $\mathbb{F} *_t^\sigma G$, then* $\mathrm{Ann}_r(\mathcal{C}) = \{\alpha \in \mathbb{F} *_t^\sigma G \,|\, \langle c, \alpha \rangle_f = 0$ *for all* $c \in \mathcal{C}\}$.
(ii) *If $\mathcal{C}$ is a right ideal of $\mathbb{F} *_t^\sigma G$, then* $\mathrm{Ann}_\ell(\mathcal{C}) = \{\alpha \in \mathbb{F} *_t^\sigma G \,|\, \langle \alpha, c \rangle_f = 0$ *for all* $c \in \mathcal{C}\}$.

We need the following observation. Once $^*$ is an anti-isomorphism, the proof follows easily.

**Lemma 7.** *If* $\mathcal{C} \subset \mathbb{F} *_t^\sigma G$, *then* $\mathrm{Ann}_\ell(\mathcal{C}^*) = \mathrm{Ann}_r(\mathcal{C})^*$ *and* $\mathrm{Ann}_r(\mathcal{C}^*) = \mathrm{Ann}_\ell(\mathcal{C})^*$.

Consider the map $\psi : \mathbb{F} *_\tau^\sigma G \to \mathbb{F} *_t^\sigma G$ defined by

$$\psi\left(\sum_{g\in G} a_g \tilde{g}\right) = \sum_{g\in G} a_g \bar{g}. \tag{5}$$

**Theorem 8.** *Let* $\psi$ *be the map defined in* (5). *If* $\mathcal{C} \subset \mathbb{F} *_t^\sigma G$ *is a left crossed product code, then*

$$\mathcal{C}^\perp = \psi(\mathrm{Ann}_\ell(\mathcal{C}^*)) = \psi(\mathrm{Ann}_r(\mathcal{C})^*).$$

**Proof.** Assume that $\mathcal{C} \subset \mathbb{F} *_t^\sigma G$ is a left crossed product code. Let $\beta = \sum_{g\in G} b_g \widetilde{g} \in \mathrm{Ann}_\ell(\mathcal{C}^*)$. For every $c = \sum_{g\in G} c_g \overline{g} \in \mathcal{C}$, one has

$$\begin{aligned}\beta c^* &= \left(\sum_{g\in G} b_g \widetilde{g}\right)\left(\sum_{h\in G} {}^{h^{-1}}c_h\, t(h^{-1},h)\widetilde{h^{-1}}\right)\\ &= \sum_{g,h\in G} b_g^{gh^{-1}} c_h\, {}^g t(h^{-1},h)\,\tau(g,h^{-1})\widetilde{gh^{-1}}.\end{aligned}$$

Moreover, the coefficient of $\widetilde{1}$ in the expression of $\beta c^*$ is

$$\sum_{g\in G} b_g\, c_g^g t(g^{-1},g)\,\tau(g,g^{-1}).$$

Since $t$ is a twisting, if we take $x = g$, $y = g^{-1}$ and $z = g$ in the formula (1), we have ${}^g t(g^{-1},g) = t(g,g^{-1})$. By definition of $\tau$, we obtain $\tau(g,g^{-1}) = t(g,g^{-1})^{-1}$. Then, it follows that

$$\begin{aligned}0 = \langle \beta c^*, \tilde{1}\rangle &= \sum_{g\in G} b_g\, c_g^g t(g^{-1},g)\tau(g,g^{-1})\\ &= \sum_{g\in G} b_g c_g\\ &= \langle \psi(\beta), c\rangle,\end{aligned}$$

which imply $\psi(\mathrm{Ann}_\ell(\mathcal{C}^*)) \subset \mathcal{C}^\perp$. By [8, Theorem 16.40] and Lemma 7, we have

$$\begin{aligned}\dim_{\mathbb{F}^\sigma} \psi(\mathrm{Ann}_\ell(\mathcal{C}^*)) &= \dim_{\mathbb{F}^\sigma}(\mathrm{Ann}_\ell(\mathcal{C}^*))\\ &= \dim_{\mathbb{F}^\sigma}(\mathrm{Ann}_r(\mathcal{C}))\\ &= [\mathbb{F} : \mathbb{F}^\sigma]\cdot|G| - \dim_{\mathbb{F}^\sigma}(\mathcal{C}) = \dim_{\mathbb{F}^\sigma}\mathcal{C}^\perp.\end{aligned}$$

□

**Theorem 9.** *Assume that* $t = t^{-1}$ *and let* $\mathcal{C} = (\mathbb{F} *_t^\sigma G)e$ *be a crossed product code, where* $e$ *is an idempotent. Then, the following properties are equivalent*:

(1) $\mathcal{C} = \mathcal{C}^\perp$
(2) $e \cdot e^* = 0$ *and* $\bar{1} - e^* = e(\bar{1} - e^*)$.

**Proof.** Note that $\mathrm{Ann}_r(\mathcal{C}) = (\bar{1} - e)\mathbb{F} *_t^\sigma G$. Then

$$\mathcal{C}^\perp = \mathrm{Ann}_r(\mathcal{C})^* = \mathbb{F} *_t^\sigma G(\bar{1} - e^*).$$

$(1 \Rightarrow 2)$ If $C = C^\perp$, then

$$C = (\mathbb{F} *_t^\sigma G)e = \mathbb{F} *_t^\sigma G(\bar{1} - e^*),$$

implying that $(\bar{1} - e^*)e = e$ and $e(\bar{1} - e^*) = (\bar{1} - e^*)$.

$(2 \Rightarrow 1)$ If $\bar{1} - e^* = e(\bar{1} - e^*)$ then $\mathbb{F} *_t^\sigma G \cdot (\bar{1} - e^*) \subseteq \mathbb{F} *_t^\sigma G \cdot e$. The condition $e^*e = 0$, which is equivalent to $(\bar{1} - e^*)e = e$, shows that

$$\mathcal{C} = \mathbb{F} *_t^\sigma G \cdot e \subseteq \mathbb{F} *_t^\sigma G(\bar{1} - e^*) = \mathcal{C}^\perp. \qquad \square$$

## 4. Examples

Let $\mathbb{F} *_t^\sigma G$ be a crossed product. If $G$ is cyclic and $t$ is a twisting satisfying that $t^2$ is the trivial twisting, i.e. $t^2(g, h) = 1$, for all $g, h \in G$, the crossed product codes are skew cyclic or skew negacyclic codes. In [2] there are interesting examples of these type of codes that have best possible weight. We will provide two examples with $G$ being a dihedral group.

**Example 1.** Consider $\mathbb{F}_9 = \mathbb{F}_3(\omega)$ where $\omega^2 = \omega + 1$ and let $\theta$ be the Frobenius automorphism $\theta : \alpha \mapsto \alpha^3$. Let

$$D_6 = \langle a, b \,|\, a^6 = b^2 = 1,\ bab = a^{-1} \rangle,$$

be the Dihedral group of order 12. The map $\sigma : D_6 \to \mathrm{Aut}(\mathbb{F}_9) = \{id, \theta\}$ defined by $a \mapsto \theta$, $b \mapsto id$, is an action of $D_6$ in $\mathbb{F}_9$. Consider the map $t : D_6 \times D_6 \to \mathbb{F}_9^\times$ defined by

$$t(a^{i_1}b^{i_2}, a^{j_1}b^{j_2}) = (-1)^{i_2 j_1},$$

for all $0 \le i_1, j_1 \le 1$ and $0 \le i_2, j_2 \le 5$. Let $x = a^{i_1}b^{i_2}$, $y = a^{j_1}b^{j_2}$ and $z = a^{k_1}b^{k_2}$ in $D_{12}$. Since $-1$ has multiplicative order 2 in $\mathbb{F}_9$ and $-1 \in \mathbb{F}_9^\sigma$, we have

$$\begin{aligned} t(x, y)\, t(xy, z) &= (-1)^{i_2 j_1}\, (-1)^{(i_2 + j_2)k_1} \\ &= (-1)^{j_2 k_1}\, (-1)^{i_2(j_1 + (-1)^{j_2} k_1)} \\ &= (-1)^{j_2 k_1}\, (-1)^{i_2(j_1 + k_1)} \\ &= {}^x t(y, z)\, t(x, yz), \end{aligned}$$

implying the $t$ is a twisting.

Consider the crossed product $\mathbb{F}_9 *_t^\sigma D_6$. Set

$$\alpha = -\bar{1} + \bar{a} - \omega^3\bar{a}^2 + \bar{a}^3 + (-\bar{1} - \bar{a} + \omega\bar{a}^2 - \omega\bar{a}^3 + \omega^2\bar{a}^4 + \bar{a}^5)\bar{b},$$

an element of $\mathbb{F}_9 *_t^\sigma D_6$. The left ideal $\mathcal{C} = (\mathbb{F}_9 *_t^\sigma D_6)\alpha$, generated by $\alpha$, has a basis

$$\alpha, \bar{a}\alpha, \bar{a}^2\alpha, \bar{a}^3\alpha, \bar{b}\alpha, \bar{b}\bar{a}\alpha, \bar{b}\bar{a}^2\alpha, \bar{b}\bar{a}^3\alpha.$$

With respect to the basis

$$\bar{1}, \bar{a}, \bar{a}^2, \bar{a}^3, \bar{a}^4, \bar{a}^5, \bar{b}, \bar{a}\bar{b}, \bar{a}^2\bar{b}, \bar{a}^3\bar{b}, \bar{a}^4\bar{b}, \bar{a}^5\bar{b},$$

of $\mathbb{F}_9 *_t^\sigma D_6$, one has\

$$\begin{bmatrix} -1 & 1 & -\omega^3 & 1 & 0 & 0 & -1 & -1 & \omega & -\omega & \omega^2 & 1 \\ 0 & -1 & 1 & -\omega & 1 & 0 & 1 & -1 & -1 & \omega^3 & -\omega^3 & -\omega^2 \\ 0 & 0 & -1 & 1 & -\omega^3 & 1 & \omega^2 & 1 & -1 & -1 & \omega & -\omega \\ -1 & -1 & \omega^2 & \omega & \omega & 1 & -1 & 0 & 0 & -1 & -\omega^3 & -1 \\ 1 & \omega^2 & -\omega^3 & -\omega^3 & -1 & 1 & 0 & 0 & 1 & \omega & 1 & 1 \\ \omega^2 & \omega & \omega & 1 & -1 & -1 & 0 & -1 & -\omega^3 & -1 & -1 & 0 \end{bmatrix},$$

a generator matrix of $\mathcal{C}$.

It can be checked using GAP [5] that $\mathcal{C}$ is a $[12, 6, 6]_9$ linear code, which has best possible weight. Note that this code is different from one given in [6].

**Example 2.** Consider $\mathbb{F}_{25} = \mathbb{F}_5(\omega)$ where $\omega^2 = \omega - 2$ and $\theta$ is the Frobenius automorphism $\theta : \alpha \mapsto \alpha^5$. Let

$$D_{10} = \langle a, b \,|\, a^{10} = b^2 = 1, bab = a^{-1} \rangle,$$

be the Dihedral group of order 20. The map $\sigma : D_{10} \to \mathrm{Aut}(\mathbb{F}_{25}) = \{id, \theta\}$ defined by $a \mapsto \theta$, $b \mapsto id$, is an action of $D_{10}$ in $\mathbb{F}_{25}$. In addition, the map $t : D_{10} \times D_{10} \to \mathbb{F}_{25}^\times$ defined by

$$t(a^{i_1}b^{i_2}, a^{j_1}b^{j_2}) = (-1)^{i_2 j_1},$$

for all $0 \leq i_1, j_1 \leq 1$ and $0 \leq i_2, j_2 \leq 9$, is a twisting. We denote $\mathbb{F}_{25} *_t^\sigma D_{10}$ the crossed product. Let

$$\begin{aligned} \beta = {} & \omega^4\bar{1} + \omega\bar{a} + 2\bar{a}^2 + \omega^5\bar{a}^3 + \omega^{16}\bar{a}^4 + \bar{a}^5 \\ & + (\omega^4\bar{1} + \omega^{11}\bar{a} - \omega^8\bar{a}^2 + \omega^7\bar{a}^3 + 3\bar{a}^4 + \omega^{11}\bar{a}^5 + \omega^4\bar{a}^6 + \omega^7\bar{a}^7 - \omega^8\bar{a}^8 + \bar{a}^9)\bar{b}, \end{aligned}$$

be an element of $\mathbb{F}_9 *_t^\sigma D_6$. The elements

$$\beta, \bar{a}\beta, \bar{a}^2\beta, \bar{a}^3\beta, \bar{a}^4\beta\bar{b}\beta, \bar{b}\bar{a}\beta, \bar{b}\bar{a}^2\beta, \bar{b}\bar{a}^3\beta, \bar{b}\bar{a}^4\beta,$$

form a basis of $\mathcal{C} = (\mathbb{F}_9 *_t^\sigma D_6)\alpha$. With respect to the basis

$$\bar{1}, \bar{a}, \bar{a}^2, \bar{a}^3, \bar{a}^4, \bar{a}^5, \bar{a}^6, \bar{a}^7, \bar{a}\bar{b}, \bar{a}^2\bar{b}, \bar{a}^8, \bar{a}^9, \bar{a}^3\bar{b}, \bar{a}^4\bar{b}, \bar{a}^5\bar{b}, \bar{a}^6\bar{b}, \bar{a}^7\bar{b}, \bar{a}^8\bar{b}, \bar{a}^9\bar{b},$$

of $\mathbb{F}_{25} *_t^\sigma D_{10}$, the matrix $H = [-A^t | I_{10}]$, where

$$A = \begin{bmatrix}
\omega^4 & -\omega^{11} & 2 & -\omega^4 & 1 & -\omega^8 & \omega^5 & \omega^{11} & \omega^2 & -\omega^5 \\
\omega^{11} & \omega^9 & \omega^8 & -1 & \omega^3 & 2 & \omega^{10} & 0 & -\omega & -\omega^{10} \\
-\omega & \omega^5 & 1 & -\omega^3 & 0 & \omega^5 & -\omega & -1 & -\omega^5 & 3 \\
-\omega^5 & \omega^2 & \omega^4 & 2 & \omega & 1 & -\omega^7 & -\omega & -\omega^{11} & \omega^{11} \\
\omega^2 & -\omega^5 & \omega & 2 & \omega^2 & -\omega^5 & -\omega^{11} & 3 & \omega^7 & \omega^{11} \\
\omega^5 & -\omega & \omega^7 & 0 & -1 & -\omega^5 & \omega^{11} & 2 & \omega^7 & -\omega^{11} \\
\omega^9 & \omega^{11} & \omega^{10} & -\omega^5 & -\omega & -\omega^7 & \omega^7 & \omega^{11} & 0 & -\omega^7 \\
-\omega^{11} & \omega^4 & -\omega & -\omega^2 & 3 & \omega^7 & 0 & -\omega^7 & -\omega^{11} & 2 \\
0 & 0 & \omega^8 & -\omega^7 & \omega^5 & \omega & -\omega^{10} & -\omega & \omega^9 & \omega^7 \\
0 & 0 & \omega^7 & \omega^9 & -\omega & -\omega^{10} & \omega & \omega^5 & -\omega^7 & \omega^9
\end{bmatrix}$$

and $I_{10}$ is the $10 \times 10$ identity matrix over $\mathbb{F}_{25}$, is a parity-check matrix of $\mathcal{C}$.

It can be checked using GAP [5] that 7 is the smallest integer for which there are linearly dependent columns in $H$, which implies that $\mathcal{C}$ is $[20, 10, 7]_{25}$ linear code. However, if we consider the subspace of $\mathcal{C}$ generated by

$$\beta, \bar{a}\beta, \bar{a}^2\beta, \bar{a}^3\beta, \bar{a}^4\beta\bar{b}\beta, \bar{b}\bar{a}\beta, \bar{b}\bar{a}^2\beta,$$

we get a linear code $[20, 8, 10]_{25}$ which meets the Gilbert–Varshamov bound.


## Acknowledgments

The third author was partially supported by FAPESP, proc. 2015/09162-9. The authors are grateful to the referee and the editor for their valuable suggestions.



## ORCID

A. Duarte https://orcid.org/0000-0001-9449-1231


## References


[1] J. J. Bernal, Á. del Río and J. J. Simón, An intrinsical description of group codes, *Des. Codes Cryptogr.* **51** (2009) 289–300.

[2] R. D. Boulanouar, A. Batoul and D. Boucher, An overview on skew constacyclic codes and their subclass of LCD codes, *Adv. Math. Commun.* **15**(4) (2021) 611–632.

[3] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory*, **IT-44** (1998) 1369–1387.

[4] J. De La Cruz and W. Willems, Twisted group codes, *IEEE Trans. Inf. Theory* **67**(8) (2021) 5178–5184.

[5] The GAP-Group, *GAP — Groups, Algorithms, and Programming, Version 4.12.1*, preprint (2022), https://www.gap-system.org.

[6] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, preprint (2022), http://www.codetables.de.
[7] R. Hill, *A First Course in Coding Theory* (Oxford University Press, 1986).
[8] T. Y. Lam, *Lectures on Modules and Rings* (Springer, Berlin, 1998).
[9] D. S. Passman, *Infinite Crossed Products* (Academic Press, Inc., Boston, 1989).
[10] E. M. Rains, Nonbinary quantum codes, *IEEE Trans. Inform. Theory* **IT-45** (1999) 1827–1832.
[11] S. Roman, *Coding and Information Theory* (Springer, New York, 1992).