



HAL
open science

Twisted skew G-codes

Angelot Behajaina, Martino Borello, Javier de La Cruz, Wolfgang Willems

► **To cite this version:**

Angelot Behajaina, Martino Borello, Javier de La Cruz, Wolfgang Willems. Twisted skew G-codes. Designs, Codes and Cryptography, 2024, 92 (6), pp.1803-1821. 10.1007/s10623-024-01367-0. hal-04746421

HAL Id: hal-04746421

<https://cnrs.hal.science/hal-04746421v1>

Submitted on 21 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Twisted skew G -codes

Angelot Behajaina¹, Martino Borello², Javier de la Cruz³, and Wolfgang Willems^{3,4}

¹Department of Mathematics, Technion - Israel Institute of Technology, Haifa, Israel

²Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France

³Department of Mathematics, Universidad del Norte, Barranquilla, Colombia

⁴Otto-von-Guericke-Universität, Magdeburg, Germany

Abstract

In this paper we investigate left ideals as codes in twisted skew group rings. The considered rings, which are often algebras over a finite field, allows us to detect many of the well-known codes. The presentation, given here, unifies the concept of group codes, twisted group codes and skew group codes.

Keywords. Twisted group algebra, skew group ring, twisted skew group ring

MSC classification. 94B05, 20C05

Introduction

Linear codes are fundamental objects in classical coding theory and they are simply subspaces of a vector space endowed with the Hamming metric. However, the linear structure is usually not enough to get good and useful codes. This is the main reason why more algebraic structure is added since the early days of the theory [4, 18, 22]. Many interesting codes have found an algebraic realization as group codes [23], twisted group codes [12] or skew group codes [10], where the ambient spaces are group algebras, twisted group algebras, or skew group rings, respectively. For example, the binary extended self-dual [24, 12, 8] Golay code is a group code, the ternary extended self-dual [12, 6, 6] Golay code is a twisted group code and skew cyclic codes are skew group codes. It turns out that the famous quaternary Hermitian self-dual [6, 3, 4] hexacode \mathcal{H}_6 is also a skew group code. Moreover, group codes have been shown to be asymptotically good [2, 8].

In this note we define and analyze a unified ambient space $K[G, \Theta, \alpha]$ in which we obtain all classes of the above codes as left ideals via specializations of the parameters Θ and α . Here K is a finite field, G a finite group, $\Theta \in \text{Hom}(G, \text{Aut}(K))$ and α a 2-cocycle of G stabilized by $\Theta(G)$. The object $K[G, \Theta, \alpha]$ is a ring, in general not a K -algebra, and called a twisted skew group ring. Specializing the parameters Θ and α we may obtain a group

algebra via $KG = K[G, 1, 1]$, a twisted group algebra via $K^\alpha G = K[G, 1, \alpha]$ or a skew group ring via $K \rtimes_\Theta G = K[G, \Theta, 1]$. Thus the advantage of the concept are unified proofs for coding theoretical properties of group codes, twisted group codes and skew group codes.

The paper is organized as follows. In the first section we define twisted skew group rings $R = K[G, \Theta, \alpha]$ and investigate the structure of R . In particular, we prove that R is a Frobenius ring. Moreover, R is semisimple if the characteristic of the underlying field does not divide the order of G . Section 2 is devoted to left ideals C of R which we call twisted skew group codes. We show that for cyclic groups we get nothing else then the skew λ -constacyclic codes. Furthermore, we extend a known result on group codes in which the minimum distance of C is bounded from below in terms of $|G|$ and $\dim C$. In section 3, we answer, in terms of automorphisms, the question when a given linear code is a twisted skew group code. Section 4 deals with duality questions and section 5 with codes which are generated by idempotents. In the last section we collect some twisted skew group codes which are optimal according to Grassl's list. In particular we realize the quaternary hexacode as a skew group code.

1 Twisted skew group rings

Let G be a finite group, let $K = \mathbb{F}_q$ be a finite field of characteristic p and let $\Theta \in \text{Hom}(G, \text{Aut}(K))$. Furthermore α always denotes a *normalized 2-cocycle* (to be brief a cocycle) of G , i.e.,

$\alpha : G \times G \rightarrow K^* = K \setminus \{0\}$ with $\alpha(g, 1) = \alpha(1, g) = \alpha(1, 1) = 1$ for all $g \in G$ satisfying

$$\alpha(g_1, g_2 g_3) \alpha(g_2, g_3) = \alpha(g_1 g_2, g_3) \alpha(g_1, g_2)$$

for all $g_i \in G$. We denote the set of all 2-cocycles for G by $Z^2(G, K^*)$. A 2-cocycle α is called a *coboundary* if there exists $\kappa : G \rightarrow K^*$ with $\kappa(1) = 1$ such that

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

for all $g, h \in G$. Let $B^2(G, K^*)$ denote the set of all coboundaries for G .

Remark 1.1. The set $B^2(G, K^*)$ of coboundaries forms a subgroup of the group $Z^2(G, K^*)$ and the factor group $H^2(G, K^*) = Z^2(G, K^*)/B^2(G, K^*)$ is usually called the *second cohomology group of G* with values in K^* . For $\alpha \in Z^2(G, K^*)$ we denote its image in $H^2(G, K^*)$ by $[\alpha]$. Note that $[\alpha] = [\beta]$ if and only if $\alpha(g, h) = \beta(g, h) \kappa(g) \kappa(h) \kappa(gh)^{-1}$ where $\kappa(1) = 1$.

In the sequel, we will always consider cocycles α , which are stabilized by the group $\Theta(G) \leq \text{Aut}(K)$, i.e.,

$$\Theta(g)\alpha(x, y) = \alpha(x, y) \tag{1}$$

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

Definition 1.2. Let $R := K[G, \Theta, \alpha]$ be the (left) K -vector space KG . On R , where the group elements are written with an overline, we define a multiplication by

$$\sum_{g \in G} a_g \bar{g} \cdot \sum_{h \in H} b_h \bar{h} = \sum_{g, h \in G} a_g (\Theta(g) b_h) \alpha(g, h) \bar{g} \bar{h} \tag{2}$$

for $a_g, b_h \in K$.

Theorem 1.3. R is an associative ring with identity $\bar{1}$, called a twisted skew group ring.

Proof. To prove that R is an associative ring, the only point that needs to be checked is the associativity, since the others are straightforward. To this end, let $a = \sum_g a_g \bar{g} \in R$, $b = \sum_h b_h \bar{h} \in R$ and $c = \sum_u c_u \bar{u} \in R$. On one hand side we have

$$\begin{aligned} (a \cdot b) \cdot c &= \left(\sum_{g,h} a_g (\Theta(g)b_h) \alpha(g,h) \overline{gh} \right) \left(\sum_u c_u \bar{u} \right) \\ &= \sum_{g,h,u} a_g (\Theta(g)b_h) \alpha(g,h) (\Theta(gh)c_u) \alpha(gh,u) \overline{(gh)u}, \end{aligned}$$

on the other hand (using that $\Theta(g)$ acts trivially on α (1))

$$\begin{aligned} a \cdot (b \cdot c) &= \left(\sum_g a_g \bar{g} \right) \left(\sum_{h,u} b_h (\Theta(h)c_u) \alpha(h,u) \overline{hu} \right) \\ &= \sum_{g,h,u} a_g \Theta(g) [b_h (\Theta(h)c_u) \alpha(h,u)] \alpha(g, hu) \overline{g(hu)} \\ &= \sum_{g,h,u} a_g (\Theta(g)b_h) (\Theta(gh)c_u) \alpha(h,u) \alpha(g, hu) \overline{g(hu)}, \end{aligned}$$

from which the associativity follows since α satisfies the cocycle condition. Finally, $\bar{1}$ is the identity since α is assumed to be normalized. \square

Remark 1.4. Note that $K[G, \Theta, \alpha]$ carries the structure of a natural K -left vector space since

$$k \cdot \sum_{g \in G} a_g \bar{g} = k\bar{1} \cdot \sum_{g \in G} a_g \bar{g} = \sum_{g \in G} k(\Theta(1)a_g) \bar{g} = \sum_{g \in G} k a_g \bar{g}.$$

Furthermore, $K[G, \Theta, \alpha]$ is in general not a K -algebra, since $\bar{g}(k\bar{1}) = (\Theta(g)k)\bar{g} \neq k\bar{g}$ for $g \in G$ and $k \in K$, if $\Theta(g)k \neq k$.

Lemma 1.5. Let $\Theta, \Theta' \in \text{Hom}(G, \text{Aut}(K))$ and let $\alpha, \alpha' \in Z^2(G, K^*)$. If $\delta : G \rightarrow G$ and $\kappa : G \rightarrow K^*$ with $\kappa(1) = 1$, then

$$\Psi : K[G, \Theta, \alpha] \rightarrow K[G, \Theta', \alpha'], \quad a_g \bar{g} \mapsto a_g \kappa(g) \overline{\delta(g)} \quad (3)$$

defines a K -left distance preserving isomorphism if and only if

- a) δ is a group automorphism satisfying $\Theta = \Theta'\delta$, and
- b) $\alpha(g, h) = \kappa(g)\Theta'(\delta(g))(\kappa(h))\kappa(gh)^{-1}\alpha'_\delta(g, h)$ for all $g, h \in G$,
where $\alpha'_\delta(g, h) = \alpha'(\delta(g), \delta(h))$ for all $g, h \in G$.

Proof. Suppose that the map in (3) is a K -left isomorphism. For $g, h \in G$ and $a, b \in K$, we have

$$\Psi(a\bar{g} \cdot b\bar{h}) = \Psi(a(\Theta(g)b)\alpha(g, h)\overline{gh}) = a(\Theta(g)b)\alpha(g, h)\kappa(gh)\overline{\delta(gh)}$$

and

$$\begin{aligned} \Psi(a\bar{g} \cdot b\bar{h}) &= \Psi(a\bar{g})\Psi(b\bar{h}) = \left(a\kappa(g)\overline{\delta(g)}\right) \cdot \left(b\kappa(h)\overline{\delta(h)}\right) \\ &= a\kappa(g)\Theta'(\delta(g))(b\kappa(h))\alpha'(\delta(g), \delta(h))\overline{\delta(g)\delta(h)}. \end{aligned}$$

Thus, $\delta(gh) = \delta(g)\delta(h)$ for $g, h \in G$. Since δ is clearly bijective, it is actually a group automorphism. Next, taking $a = b = 1$ in the equations above, we get

$$\alpha(g, h) = \kappa(g)\Theta'(\delta(g))\kappa(h)\kappa(gh)^{-1}\alpha'_\delta(g, h),$$

for $g, h \in G$. Similarly taking $a = 1$ and $h = 1$ we may deduce that $\Theta(g)(b) = \Theta'(\delta(g))(b)$ for all $g \in G$ and $b \in \mathbb{F}_q$, which implies $\Theta = \Theta'\delta$.

The converse follows from the computations above. \square

For a finite ring A , we write $\widehat{A} = \text{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$. Recall that \widehat{A} becomes a right A -module by $(\chi \cdot a)(a') = \chi(aa')$ for $a, a' \in A$ and $\chi \in \widehat{A}$. Furthermore, A is a Frobenius ring if and only if there is an isomorphism of right A -modules between A and \widehat{A} (see for instance [25, Theorem 3.10]).

Theorem 1.6. *The ring R is a Frobenius ring.*

Proof. Since K is a Frobenius ring, there is $\chi_K \in \widehat{K}$ such that

$$\Phi : x \in K \mapsto (\chi_K \cdot x) \in \widehat{K}$$

is an isomorphism of right K -modules. We define $\chi_R \in \widehat{R}$ by $\chi_R \left(\sum_g a_g \bar{g}\right) = \chi_K(a_1)$ and claim that the following morphism of right R -modules

$$\Psi : r \in R \mapsto \chi_R \cdot r \in \widehat{R}$$

is an isomorphism. Since $|R| = |\widehat{R}|$, it remains to prove that Ψ is injective. For that, let $r = \sum_g r_g \bar{g} \in R$ and $r' = \sum_g r'_g \bar{g} \in R$ such that $\Psi(r) = \Psi(r')$. For $g \in G$ and $x \in K$, we have

$$(\chi_R \cdot r) \left((\Theta(g^{-1})x)\overline{g^{-1}} \right) = (\chi_R \cdot r') \left((\Theta(g^{-1})x)\overline{g^{-1}} \right),$$

that is,

$$\chi_R \left(r \cdot \left((\Theta(g^{-1})x)\overline{g^{-1}} \right) \right) = \chi_R \left(r' \cdot \left((\Theta(g^{-1})x)\overline{g^{-1}} \right) \right),$$

and so,

$$\chi_K(r_g \alpha(g, g^{-1})x) = \chi_K(r'_g \alpha(g, g^{-1})x).$$

Since

$$(\chi_K \cdot (r_g \alpha(g, g^{-1}))) (x) = \chi_K(r_g \alpha(g, g^{-1})x),$$

we obtain $\chi_K \cdot (r_g \alpha(g, g^{-1})) = \chi_K \cdot (r'_g \alpha(g, g^{-1}))$. As Φ is bijective, we finally get $r_g \alpha(g, g^{-1}) = r'_g \alpha(g, g^{-1})$, and so $r_g = r'_g$ for all $g \in G$, which proves $r = r'$. Therefore, the proof is complete. \square

Next we prove an extension of Maschke's Theorem, which is well-known for twisted group algebras (see [17, Chap. 3, Theorem 2.10]).

Theorem 1.7. *If $\text{char } K \nmid |G|$, then R is a semisimple ring.*

Proof. Let V be an R -left module and W a submodule of V . We may write $V = W \oplus U$ with a K -vector space U . Let ρ be the projection of V onto W with kernel U . For $v \in V$ we define the map $\Lambda : V \rightarrow W$ by

$$\Lambda(v) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\alpha(g, g^{-1})} \bar{g} \rho(\bar{g}^{-1} v) = \frac{1}{|G|} \sum_{g \in G} \bar{g} \rho(\bar{g}^{-1} v).$$

If $a \in K$, then

$$\begin{aligned} \Lambda(av) &= \frac{1}{|G|} \sum_{g \in G} \bar{g} \rho(\bar{g}^{-1} av) \\ &= \frac{1}{|G|} \sum_{g \in G} \bar{g} \rho((\Theta(g^{-1})a) \bar{g}^{-1} v) \\ &= \frac{1}{|G|} \sum_{g \in G} \bar{g} (\Theta(g^{-1})a) \rho(\bar{g}^{-1} v) \\ &= \frac{1}{|G|} \sum_{g \in G} \Theta(g) (\Theta(g^{-1})a) \bar{g} \rho(\bar{g}^{-1} v) \\ &= \frac{1}{|G|} \sum_{g \in G} a \bar{g} \rho(\bar{g}^{-1} v) = a \Lambda(v). \end{aligned}$$

Thus Λ is K -linear. For $h \in G$, we obtain

$$\Lambda(\bar{h}v) = \frac{1}{|G|} \sum_{g \in G} \bar{g} \rho(\bar{g}^{-1} \bar{h}v) = \frac{1}{|G|} \sum_{x \in G} \bar{h}x \rho((\bar{h}x)^{-1} \bar{h}v).$$

Since $\bar{h}x^{-1} = \alpha(h, x) \bar{x}^{-1} \bar{h}^{-1}$ and $\Theta(g)\alpha(x, y) = \alpha(x, y)$, we get

$$\begin{aligned} \Lambda(\bar{h}v) &= \frac{1}{|G|} \sum_{x \in G} \alpha(h, x)^{-1} \bar{h} \bar{x} \rho((\alpha(h, x) \bar{x}^{-1} \bar{h}^{-1}) \bar{h}v) \\ &= \bar{h} \frac{1}{|G|} \sum_{x \in G} \alpha(h, x)^{-1} \bar{x} \rho((\alpha(h, x) \bar{x}^{-1} \bar{h}^{-1}) \bar{h}v) \\ &= \bar{h} \frac{1}{|G|} \sum_{x \in G} \bar{x} \rho(\bar{x}^{-1} v) \\ &= \bar{h} \Lambda(v). \end{aligned}$$

Thus Λ is R -linear and the identity on W . It follows that $V = W \oplus \text{Ker } \Lambda$ where $\text{Ker } \Lambda$ is a R -left module. \square

Definition 1.8. For $a = \sum_{g \in G} a_g \bar{g} \in R$ we define the adjoint \hat{a} of a by

$$\hat{a} = \sum_{g \in G} (\Theta(g^{-1})a_g) \alpha(g, g^{-1}) \bar{g}^{-1}.$$

Note that the map $\hat{}$ is not K -linear. If we consider $\hat{a} \in K[G, \Theta, \alpha^{-1}]$ we have the following.

Theorem 1.9. $\hat{} : R = K[G, \Theta, \alpha] \rightarrow K[G, \Theta, \alpha^{-1}]$ is distance preserving ring anti-isomorphism. Moreover, if $\alpha = \alpha^{-1}$, then $\hat{\hat{a}} = a$ for all $a \in R$.

Proof. Clearly, the map $\widehat{}$ is additive and maps the identity onto the identity since α is normalized. Furthermore, $\widehat{}$ defines a bijection. Thus, we only have to prove $\widehat{a\bar{b}} = \widehat{\bar{b}}\widehat{a}$, for $a, b \in R$. Let $a = \sum_{g \in G} a_g \bar{g}$ and $b = \sum_{h \in G} b_h \bar{h}$. One easily computes

$$\widehat{a\bar{b}} = \sum_{g, h \in G} (\Theta(h^{-1}g^{-1})a_g)(\Theta(h^{-1}b_h)\alpha(g, h)\alpha(gh, h^{-1}g^{-1})\overline{h^{-1}g^{-1}})$$

and

$$\widehat{\bar{b}}\widehat{a} = \sum_{g, h \in G} (\Theta(h^{-1}g^{-1})a_g)(\Theta(h^{-1}b_h)\alpha(h, h^{-1})\alpha(g, g^{-1})\alpha^{-1}(h^{-1}, g^{-1})\overline{h^{-1}g^{-1}}).$$

Applying the normalized cocycle condition, we see that

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

hence $\widehat{a\bar{b}} = \widehat{\bar{b}}\widehat{a}$. Finally note that

$$\widehat{\bar{a}} = \sum_{g \in G} \Theta(g) [(\Theta(g^{-1})a_g)\alpha(g, g^{-1})\alpha(g^{-1}, g)] \bar{g} = \sum_{g \in G} a_g \alpha(g, g^{-1})\alpha(g^{-1}, g) \bar{g},$$

which proves $\widehat{\bar{a}} = a$, since $\alpha(g, g^{-1}) = \alpha(g^{-1}, g)$ which follows from the cocycle condition, and $\alpha = \alpha^{-1}$, by assumption. \square

Let $K^\alpha G = K[G, 1, \alpha]$ be a twisted group code over a field K of characteristic p . The set $\widehat{G} = K^* \times G$ becomes a group via the multiplication

$$(\lambda, g) \cdot (\mu, h) = (\alpha(g, h)\lambda\mu, gh).$$

Since $\alpha(1, g) = \alpha(g, 1)$ for all $g \in G$, we see that

$$N = \{(\lambda, 1) \mid \lambda \in K^*\} \cong K^*$$

is a central subgroup of \widehat{G} and $G \cong \widehat{G}/N$.

Proposition 1.10. *Let $\text{char } K = p$. If G is p -nilpotent with a cyclic Sylow p -subgroup, then every left (right) ideal in a twisted group algebra is principal.*

Proof. By [19, Proposition 1.2.17], the K -linear map $\rho : K\widehat{G} \rightarrow K^\alpha G$ given by

$$(\lambda, g) \mapsto \lambda \bar{g}$$

defines an K -algebra epimorphism. Note that \widehat{G} is p -nilpotent with cyclic Sylow p -subgroups. Now let \overline{C} be a left ideal in $K^\alpha G$ and C its preimage in $K\widehat{G}$. By [6, Corollary 3.2], C is a principal ideal, i.e., $C = aK\widehat{G}$. Thus $\overline{C} = \rho(a)K^\alpha G$. \square

Question 1.11. Is there an extension of Proposition 1.10 to left ideals in twisted skew group rings?

2 Twisted skew group codes

We shall use R with the natural basis $\{\bar{g} \mid g \in G\}$ as an ambient space. Thus R carries the Hamming distance and the Euclidean bilinear form defined by $\langle \bar{g}, \bar{h} \rangle = \delta_{g,h}$.

Definition 2.1. A left ideal C in $R = K[G, \Theta, \alpha]$ is called a *twisted skew group code*, more precisely a (G, Θ, α) -code. We shortly write $C \leq R$ in this case.

Note that $(G, 1, 1)$ -codes are nothing else than group codes [23], and $(G, 1, \alpha)$ -codes are twisted group codes [12]. Inspired by [10] (see also [13]) we call $(G, \Theta, 1)$ -codes skew group codes.

For the reader's convenience we repeat a well-known definition.

Definition 2.2. Let $\theta \in \text{Aut}(K)$ and $\lambda \in K^*$. A linear code C in K^n is called

a) θ -cyclic (or skew-cyclic) if

$$(c_0, c_1, \dots, c_{n-1}) \in C \implies (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C,$$

b) (θ, λ) -constacyclic (or skew λ -constacyclic) if

$$(c_0, c_1, \dots, c_{n-1}) \in C \implies (\lambda\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C.$$

Let $C_n = \langle g \rangle$ and let $\theta \in \text{Aut}(K)$ with $\text{ord}(\theta) \mid n$. We define Θ by $\Theta(g^i) = \theta^i$ for $i = 0, \dots, n-1$, and for $\lambda \in K^*$, the cocycle α_λ by

$$\alpha_\lambda(g^i, g^j) = \begin{cases} 1 & \text{if } 0 \leq i+j < n \\ \lambda & \text{if } n \leq i+j \leq 2(n-1). \end{cases} \quad (4)$$

With this notation $(C_n, \Theta, 1)$ -codes are θ -cyclic codes [10], and $(C_n, \Theta, \alpha_\lambda)$ -codes are skew λ -constacyclic codes if $\theta(\lambda) = \lambda$ [1].

Thus with the Definition 2.1 we cover many classes of interesting codes in twisted skew group rings by specializing parameters.

The following result shows that all twisted skew group codes for a cyclic group are skew λ -constacyclic.

Proposition 2.3. *If $R = K[C_n, \Theta, \alpha]$ is a twisted skew group ring, then R is skew λ -constacyclic for some $\lambda \in K^*$ fixed by $\Theta(g)$.*

Proof. Let k denote the subfield of K which is fixed by $\Theta(g)$. By the assumption on α (see (1)), the cocycle α takes only values in k . Thus, by [20, Problem 16, Chapter 10] there exists $\lambda = \prod_{i=0}^{n-1} \alpha(g^i, g) \in k^*$ and $\kappa : G \rightarrow k^*$ with $\kappa(1) = 1$ such that

$$\alpha(g^i, g^j) = \kappa(g^i)\kappa(g^j)\kappa(g^{i+j})^{-1}\alpha_\lambda(g^i, g^j).$$

Using Lemma 1.5, with $\delta = id_G$, we have $K[G, \Theta, \alpha] \simeq K[G, \Theta, \alpha_\lambda]$. □

The next result was first proved for group codes in [9]. An extension to twisted group codes has been given in [24]. For the reader's convenience we repeat the proof here adapted to twisted skew group codes.

Theorem 2.4. *If $0 \neq C \leq K[G, \Theta, \alpha] = R$ is a twisted skew group code of minimum distance $d(C)$, then*

$$|G| \leq d(C) \cdot \dim C.$$

Proof. We obviously may replace C by $C = Rc$ with $\text{wt}(c) = d(C)$. Let $c = \sum_{g \in G} c_g \bar{g}$ and put $S = \text{supp}(c) = \{g \mid c_g \neq 0\} \subseteq G$. Let g_1, \dots, g_t be a maximal set of pairwise different elements of G such that

$$g_i S \not\subseteq \cup_{j < i} g_j S$$

for all $i = 1, \dots, t$. By maximality, we have $G = \cup_{i=1}^t g_i S$, hence $t \geq \frac{|G|}{|S|}$. Next we consider the map $T_c : R \rightarrow R$ defined by $a \mapsto T_c(a) = ac$. Note that T_c is K -linear from the left. Since $\text{rank } T_c = \dim C$, it is sufficient to prove that for $i = 1, \dots, t$ the vectors $T_c(\bar{g}_i)$ are K -linear independent. Suppose that $v = \sum_{i=1}^t \lambda_i T_c(\bar{g}_i) = 0$ with $\lambda_i \in K$. Let $r = \max\{i \mid \lambda_i \neq 0\}$. If

$$h = g_r s \in g_r S \setminus \cup_{j < r} g_j S$$

with $s \in S$, then the coefficient of \bar{h} in v is equal to

$$\lambda_r (\Theta(g_r) c_s) \alpha(g_r, s) \neq 0,$$

a contradiction. □

Group codes for which equality holds in the bound in Theorem 2.4 have been characterized completely in [9].

3 Equivalence and automorphism groups

Let $M(n, K)$ (resp., $\text{Diag}(n, K)$) be the set of monomial (resp., diagonal) matrices of type $n \times n$ over K . The group $\text{Aut}(K)$ acts naturally from the left on $M(n, K)$ by $\gamma \cdot A = (\gamma(a_{i,j}))$ for $\gamma \in \text{Aut}(K)$ and $A = (a_{i,j}) \in M(n, K)$. In the sequel, for convenience, we denote $\gamma \cdot A$ by $A^{\gamma^{-1}}$. In this way, we get the semidirect product $\Gamma L_n = \text{Aut}(K) \ltimes M(n, K)$ with multiplication

$$(\gamma, A) \cdot (\beta, B) = (\gamma\beta, A^\beta B)$$

for $(\gamma, A), (\beta, B) \in \Gamma L_n$. In this section, we regard elements of K^n as column vectors. The following defines a left action of ΓL_n on $(K^n, +)$. For $x = (x_1, \dots, x_n)^T \in K^n$ and $(\gamma, A) \in \Gamma L_n$, we put

$$(\gamma, A) \cdot x = A^{\gamma^{-1}} x^{\gamma^{-1}},$$

where $x^{\gamma^{-1}} = (\gamma(x_1), \gamma(x_2), \dots, \gamma(x_n))^T$. Observe that this map is semilinear since, for $k \in K$, we have

$$(\gamma, A) \cdot (kx) = \gamma(k) \cdot ((\gamma, A)x).$$

From now on, let Π_1 (resp., Π_2) be the projection of ΓL_n on $\text{Aut}(K)$ (resp., $M(n, K)$).

Lemma 3.1. *The action of ΓL_n on $(K^n, +)$ is faithful and (Hamming-)distance preserving. Hence we may identify ΓL_n as a subgroup of $\text{Aut}(K^n, +)$.*

Proof. The proof is classical. Consider the standard K -basis $\{e_1, \dots, e_n\}$ of K^n . Let $(\gamma, A) \in \Gamma L_n$ such that $(\gamma, A)x = x$, for all $x \in K^n$. Taking $x = e_j$ ($j = 1, \dots, n$), we deduce that $A^{\gamma^{-1}}e_j = e_j$, and so $A^\gamma = I_n$, or equivalently $A = I_n$. Therefore, $x^{\gamma^{-1}} = x$ for all $x \in K^n$, and so $\gamma = \text{Id}_K$. \square

Lemma 3.2. *ΓL_n is the group of semilinear isometries of the Hamming space $(K^n, +, d)$.*

Proof. Let f be a semilinear bijection of K^n , i.e.,

$$f(x + y) = f(x) + f(y) \quad \text{and} \quad f(kx) = \gamma(k)f(x)$$

for $x \in K^n$ and $k \in K$ where $\gamma \in \text{Aut}(K)$. Assume also that f is an isometry of $(K^n, +, d)$. We only have to show that $f \in \Gamma L_n$. If e_1, \dots, e_n is the standard basis of K^n , then

$$f(e_i) = \gamma(k_i)e_{\pi(i)}$$

for suitable $k_i \in K^*$, where π is a permutation of $\{1, \dots, n\}$. Thus, for $x_i \in K$, we get

$$f\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n \gamma(x_i)f(e_i) = \sum_{i=1}^n \gamma(x_i k_i)e_{\pi(i)} = \sum_{i=1}^n \gamma(x_{\pi^{-1}(i)} k_{\pi^{-1}(i)})e_i.$$

This obviously describes a map in ΓL_n . \square

Recall that for left ideals $C \leq R = K[G, \Theta, \alpha]$ the left multiplication of $g \in G$ is given by

$$g \cdot (kc) = (\Theta(g)k)(g \cdot c)$$

for $k \in K$ and $c \in C$, hence by a semilinear map. Thus C is invariant under a group of suitable semilinear maps and we may define the *automorphism group* of C as

$$\text{Aut}(C) = \{(\gamma, A) \in \Gamma L_n \mid (\gamma, A) \cdot C = C\},$$

which is clearly a subgroup of ΓL_n . Note that a monomial matrix $A \in M(n, K)$ over K is of the form

$$A = \text{diag}(a_1(A), \dots, a_n(A))P(A),$$

where $\text{diag}(a_1(A), \dots, a_n(A))$ is the diagonal matrix with entries $a_i(A) \in K^*$ and $P(A)$ is the permutation matrix of the permutation induced by A on $\{1, \dots, n\}$. We call the diagonal matrix $D(A) = \text{diag}(a_1(A), \dots, a_n(A))$ the *diagonal part* and $P(A)$ the *permutation part* of A .

Definition 3.3. Let $C \leq K[G, \Theta, \alpha]$ and $C' \leq K[G', \Theta', \alpha']$ with $|G| = |G'| = n$. Then we call C and C' *equivalent* if there exists $(\gamma, A) \in \Gamma L_n$ such that $(\gamma, A)C = C'$.

Remark 3.4. Note that the map $K[G, \Theta, \alpha] \ni a \mapsto \hat{a} \in K[G, \Theta, \alpha^{-1}]$ can be described by a suitable $(\gamma, A) \in \Gamma L_{|G|}$, but it maps a left ideal onto a right ideal (see Theorem 1.9).

Now let

$$G(\Theta, \alpha) = K^* \times G.$$

We define a group structure on $G(\Theta, \alpha)$ by:

$$(\lambda, g) \cdot (\mu, h) = (\lambda\Theta(g)(\mu)\alpha(g, h), gh),$$

for all $(\lambda, g), (\mu, h) \in G(\Theta, \alpha)$. Note that

$$N = \{(\lambda, 1) \mid \lambda \in K^*\} \simeq K^*$$

is a normal subgroup of $G(\Theta, \alpha)$ and $G(\Theta, \alpha)/N \simeq G$. On $(R, +)$, the group $G(\Theta, \alpha)$ acts faithfully in the following way: for $(\lambda, g) \in G(\Theta, \alpha)$, $\eta \in K$ and $h \in G$, we define

$$(\lambda, g) \cdot (\eta\bar{h}) = \lambda\Theta(g)(\eta)\alpha(g, h)\overline{gh}.$$

With respect to the K -basis $\{\bar{g}\}_{g \in G}$ of $R = K[G, \Theta, \alpha]$, we may identify $G(\Theta, \alpha)$ with a subgroup in ΓL_n .

From now on, if $u \in \Gamma L_n$, we let $P(u) = P(\Pi_2(u))$, the permutation part of $\Pi_2(u)$.

Theorem 3.5. *Let $C \leq K^n$ be a linear code. Then C is a twisted skew group code in $K[G, \Theta, \alpha]$ for a suitable Θ and a cocycle α of G if and only if there exists a subgroup $\tilde{G} \leq \text{Aut}(C)$ satisfying the following three conditions.*

- a) *The only diagonal matrices in $\tilde{G} \cap M(n, K)$ are scalar matrices.*
- b) *$G = P(\tilde{G})$ acts regularly on $\{1, \dots, n\}$.*
- c) *If $u, v \in \tilde{G}$ such that $P(u) = P(v)$, then $\Pi_1(u) = \Pi_1(v)$.*

Proof. To prove the if part we put $\tilde{G} = \xi(G(\Theta, \alpha))$. Let $c = \sum_h c_h \bar{h} \in C$ and $(\lambda, g) \in G(\Theta, \alpha)$. Then

$$\begin{aligned} (\lambda, g) \cdot c &= \sum_{h \in G} \lambda\Theta(g)(c_h)\alpha(g, h)\overline{gh} \\ &= (\lambda\bar{g}) \cdot \left(\sum_{h \in G} c_h \bar{h} \right) = (\lambda\bar{g}) \cdot c \in C, \end{aligned}$$

since C is a left ideal in $K[G, \Theta, \alpha]$. Thus, we get $\tilde{G} = \xi(G(\Theta, \alpha)) \leq \text{Aut}(C)$ and the three conditions are easily checked.

To prove the only if part, let $\tilde{G} \leq \text{Aut}(C)$ as in the statement. Let $B = \{e_i \mid i = 1, \dots, n\}$ be the standard basis of K^n . Since G acts regularly on $\{1, \dots, n\}$ we may identify $i \in \{1, \dots, n\}$ with the unique element $h \in G$ such that $h \cdot 1 = i$. Thus we can write $B = \{e_g \mid g \in G\}$. For any $g \in G$, note that $g \cdot i = g \cdot (h \cdot 1) = (gh) \cdot 1$ and so $g \cdot i$ corresponds to gh . Furthermore note that if $\tilde{g} \in \tilde{G}$ such that $P(\tilde{g}) = g$, then there exists $\beta \in K^*$ such that $\tilde{g} \cdot e_1 = \beta e_g$.

Claim: For any $g \in G$, there exists a unique $\tilde{g} \in \tilde{G}$ such that $P(\tilde{g}) = g$ and $\tilde{g}e_1 = e_g$. Indeed, let $\tilde{g}_1, \tilde{g}_2 \in \tilde{G}$ such that $P(\tilde{g}_1) = P(\tilde{g}_2) = g$. By condition c), we may write $\tilde{g}_1 = (\gamma, D_1 \cdot g)$ and $\tilde{g}_2 = (\gamma, D_2 \cdot g)$ for some $\gamma \in \text{Aut}(K)$ and some diagonal matrices D_1, D_2 . Thus we have

$$\tilde{g}_1 \tilde{g}_2^{-1} = (\gamma, D_1 \cdot g)(\gamma^{-1}, (D_2^{\gamma^{-1}} \cdot g^{\gamma^{-1}})^{-1}) = (\text{Id}_K, D_1^{\gamma^{-1}} (D_2^{\gamma^{-1}})^{-1}) \in \tilde{G}.$$

By condition a), we get $\tilde{g}_2 = (\text{Id}_K, \lambda \text{I}_n) \tilde{g}_1$ for some $\lambda \in K^*$. Thus the claim follows. In the sequel, we denote by $\Theta(g)$ the unique element γ as defined above.

Now let $g, h \in G$. Since $P(\tilde{g}h) = P(\tilde{g}h) = gh$, there exists a unique $\alpha(g, h) \in K^*$ such that

$$\tilde{g}h = (\text{Id}_K, \alpha(g, h) \text{I}_n) \tilde{g}h, \quad (5)$$

by the proof of the Claim.

Moreover, $\tilde{g}e_h = \alpha(g, h)e_{gh}$. Indeed, we have

$$\begin{aligned} \tilde{g}e_h &= \tilde{g}(\tilde{h}e_1) = (\tilde{g}\tilde{h})e_1 = (\text{Id}_K, \alpha(g, h) \text{I}_n) \tilde{g}\tilde{h}e_1 \quad (\text{using (5)}) \\ &= (\text{Id}_K, \alpha(g, h) \text{I}_n) e_{gh} = \alpha(g, h)e_{gh}. \end{aligned}$$

From now on, let $\Theta : g \in G \mapsto \Theta(g) \in \text{Aut}(K)$, where $\Theta(g)$ is defined as in the proof of the Claim. First, note that for all $g, h \in G$ and $\lambda \in K$, we have

$$\tilde{g} \cdot (\lambda e_h) = \Theta(g)(\lambda)(\tilde{g}e_h).¹$$

Next we claim that Θ is a morphism of groups. For this purpose, let $g, h \in G$ and $\lambda \in K$. We have

$$\begin{aligned} \tilde{g} \cdot (\tilde{h} \cdot (\lambda e_1)) &= \tilde{g} \cdot (\Theta(h)(\lambda)e_h) = (\Theta(g) \circ \Theta(h))(\lambda) \tilde{g}e_h \\ &= (\Theta(g) \circ \Theta(h))(\lambda) \alpha(g, h)e_{gh} \end{aligned}$$

and

$$\begin{aligned} \tilde{g} \cdot (\tilde{h} \cdot (\lambda e_1)) &= (\tilde{g} \cdot \tilde{h}) \cdot (\lambda e_1) = ((\text{Id}_K, \alpha(g, h) \text{I}_n) \tilde{g}\tilde{h}) \cdot (\lambda e_1) \quad (\text{using (5) again}) \\ &= (\text{Id}_K, \alpha(g, h) \text{I}_n) (\Theta(gh)(\lambda) (\tilde{g}\tilde{h}e_1)) \\ &= \alpha(g, h) \Theta(gh)(\lambda) e_{gh}. \end{aligned}$$

Thus $\Theta(g) \circ \Theta(h) = \Theta(gh)$. Since $P((\text{Id}_K, \text{I}_n)) = 1$ and $(\text{Id}_K, \text{I}_n)e_1 = e_1$, we conclude, by applying the Claim, that $1 = (\text{Id}_K, \text{I}_n)$ and so $\Theta(1) = \text{Id}_K$. Consequently, Θ is a morphism of groups.

Finally we show that α is a cocycle, that is,

$$\alpha(gh, l)\alpha(g, h) = \Theta(g)(\alpha(h, l))\alpha(g, hl),$$

¹Indeed, there exists a diagonal matrix D such that $\tilde{g} = (\Theta(g), D \cdot g)$. Then we have $\tilde{g}(\lambda e_h) = D^{\Theta(g^{-1})} \cdot g^{\Theta(g^{-1})}(\lambda e_h)^{\Theta(g^{-1})} = \lambda^{\Theta(g^{-1})} D^{\Theta(g^{-1})} \cdot g^{\Theta(g^{-1})}(e_h)^{\Theta(g^{-1})} = \Theta(g)(\lambda)(\tilde{g}e_h)$.

for all $g, h, l \in G$. This follows from

$$(\tilde{g}\tilde{h})e_l = \tilde{g}(\tilde{h}e_l) = \tilde{g}(\alpha(h, l)e_{hl}) = \Theta(g)(\alpha(h, l))(\tilde{g}e_{hl}) = \Theta(g)(\alpha(h, l))\alpha(g, hl)e_{ghl}.$$

and

$$(\tilde{g}\tilde{h})e_l = ((\text{Id}_K, \alpha(g, h)\mathbf{I}_n)\tilde{g}\tilde{h})e_l = (\text{Id}_K, \alpha(g, h)\mathbf{I}_n)(\alpha(gh, l)e_{ghl}) = \alpha(g, h)\alpha(gh, l)e_{ghl}.$$

Furthermore α is normalized. To prove this let $g \in G$. Since $\tilde{\mathbf{1}} = (\text{Id}_K, \mathbf{I}_n)$ we get

$$e_g = \tilde{\mathbf{1}}e_g = \alpha(1, g)e_g$$

and

$$e_g = \tilde{g}e_1 = \alpha(g, 1)e_g,$$

and so $\alpha(1, g) = \alpha(g, 1) = 1$.

To the final end we consider the K -linear isomorphism

$$\Psi : K^n \rightarrow K[G, \Theta, \alpha]$$

defined by $\Psi(e_g) = \bar{g}$. Let $c = \sum_h c_h e_h \in C$, $\beta \in K$ and $g \in G$. We have

$$\begin{aligned} \beta\bar{g}\Psi(c) &= \beta\bar{g} \left(\sum_h c_h \bar{h} \right) \\ &= \beta \sum_h \Theta(g)(c_h)\alpha(g, h)\bar{g}\bar{h} \\ &= \Psi \left(\beta \sum_h \Theta(g)(c_h)\alpha(g, h)e_{gh} \right) \\ &= \Psi((\text{Id}_K, \beta\mathbf{I}_n)\tilde{g} \cdot c) \in \Psi(C) \quad \text{since } \tilde{G} \cdot C \leq C. \end{aligned}$$

Hence $\Psi(C)$ is a left ideal of $K[G, \Theta, \alpha]$, which completes the proof. \square

Corollary 3.6. *Let $C \leq K^n$ be a linear code. Then C is a skew group code in $K[G, \Theta, 1]$ for a suitable Θ if and only if there exists a subgroup $\tilde{G} \leq \text{Aut}(C)$ satisfying the following two conditions.*

- a) $G = P(\tilde{G})$ acts regularly on $\{1, \dots, n\}$.
- b) If $u, v \in \tilde{G}$ such that $P(u) = P(v)$, then $\Pi_1(u) = \Pi_1(v)$.

4 Duality

As usual we denote by C^\perp the dual of a code C . The first result is an extension of a Theorem of MacWilliams [18].

Theorem 4.1. *If $C \leq R$ is a left ideal in R , then $C^\perp = \widehat{\text{Ann}_r(C)}$, where the right annihilator $\text{Ann}_r(C)$ of C is defined as $\text{Ann}_r(C) = \{a \in R \mid c \cdot a = 0 \text{ for all } c \in C\}$.*

Proof. If $c = \sum_{h \in G} c_h \bar{h} \in C$ and $a = \sum_{g \in G} a_g \bar{g} \in \text{Ann}_r(C)$, then

$$0 = ca = \sum_{g, h \in G} c_h (\Theta(h) a_g) \alpha(h, g) \bar{h} \bar{g}.$$

In particular,

$$0 = \sum_{g \in G} c_{g^{-1}} (\Theta(g^{-1}) a_g) \alpha(g^{-1}, g) = \sum_{g \in G} c_{g^{-1}} (\Theta(g^{-1}) a_g) \alpha(g, g^{-1}),$$

since $\alpha(g, g^{-1}) = \alpha(g^{-1}, g)$, which is a consequence of the cocycle condition of α . It follows that

$$\langle c, \hat{a} \rangle = \sum_{g \in G} c_{g^{-1}} (\Theta(g^{-1}) a_g) \alpha(g, g^{-1}) = 0,$$

hence $\widehat{\text{Ann}_r(C)} \subseteq C^\perp$. Next we consider the map

$$\Lambda : R \longrightarrow C^* = \text{Hom}_K(C, K)$$

where $\Lambda(a)c = (ca)_{\bar{1}}$, the scalar in ca at $\bar{1}$. Note that Λ is not K -linear, but a group homomorphism from $(R, +)$ into $(C^*, +)$. Suppose that $0 = (ca)_{\bar{1}}$ for all $c \in C$ and $ca = \sum_{g \in G} k_g \bar{g}$ with $k_x \neq 0$ for some $1 \neq x \in G$. Since C is a left ideal, we have $\overline{x^{-1}c} \in C$ and $(\overline{x^{-1}c})a$ has the scalar

$$(\Theta(x^{-1})k_x)\alpha(x^{-1}, x) \neq 0$$

at $\bar{1}$, a contradiction. This shows that $\text{Ker } \Lambda = \text{Ann}_r(C)$. It follows

$$|C^*| \geq \frac{|R|}{|\text{Ker } \lambda|} = \frac{|R|}{|\text{Ann}_r(C)|} = \frac{|R|}{|\widehat{\text{Ann}_r(C)}|} \geq \frac{|R|}{|C^\perp|} = |C| = |\text{Hom}_K(C, K)| = |C^*|,$$

hence $C^\perp = \widehat{\text{Ann}_r(C)}$. □

Remark 4.2. For group codes C the dual C^\perp is a group code as well. This is far away to be true in general for twisted group codes. Note, that according to Theorem 1.9 and Theorem 4.1, C^\perp is only a left ideal in $K[G, 1, \alpha^{-1}]$ if $C \leq K[G, 1, \alpha]$. This fact causes many problems when dealing with C^\perp in the case $\alpha \neq \alpha^{-1}$.

Definition 4.3. Let $|K| = q^2$ and let $C \leq R$.

- a) The Hermitian form $\langle \cdot, \cdot \rangle_h$ on R is defined by $\langle a, b \rangle_h = \sum_{g \in G} a_g (b_g)^q = \sum_{g \in G} a_g b_g^q$.
- b) We denote the dual of $C \leq R$ with respect to the Hermitian form by C^{\perp_h} .
- c) For $a = \sum_{g \in G} a_g \bar{g}$ we put $a^{(q)} = \sum_{g \in G} a_g^q \bar{g}$.
- d) $C^{(q)} = \{c^{(q)} \mid c \in C\}$.

Theorem 4.4. Let $|K| = q^2$ and let $C \leq R$ be a left ideal in R . If $\alpha(x, y)^q = \alpha(x, y)$ for all $x, y \in G$, then $C^{\perp_h} = \widehat{\text{Ann}_r(C^{(q)})}$.

Proof. If $c = \sum_{h \in G} c_h \bar{h} \in C$ and $a = \sum_{g \in G} a_g \bar{g} \in \text{Ann}_r(C^{(q)})$, then

$$0 = c^{(q)} a = \sum_{g, h \in G} c_h^q (\Theta(h) a_g) \alpha(h, g) \bar{h} g.$$

In particular,

$$0 = \sum_{g \in G} c_{g^{-1}}^q (\Theta(g^{-1}) a_g) \alpha(g^{-1}, g) = \sum_{g \in G} c_{g^{-1}} (\Theta(g^{-1}) a_g)^q \alpha(g, g^{-1}),$$

since $\alpha(g, g^{-1}) = \alpha(g^{-1}, g)$. It follows

$$\langle c, \hat{a} \rangle_h = \sum_{g \in G} c_{g^{-1}} (\Theta(g^{-1}) a_g)^q \alpha(g, g^{-1}) = 0,$$

hence $\widehat{\text{Ann}_r(C^{(q)})} \subseteq C^{\perp h}$. Note that $C^{(q)}$ is a left ideal in R since α is fixed by the Frobenius automorphism $x \mapsto x^q$. The equality $\widehat{\text{Ann}_r(C^{(q)})} = C_h^\perp$ now follows as in the Euclidean case. \square

5 Idempotent codes

Definition 5.1. A code $C \leq R$ is *idempotent* if there exists an idempotent $e \in R$, i.e., $e = e^2$ such that $C = Re$.

Definition 5.2. Let $C \leq R$ a twisted skew group code.

- a) C is called a *Euclidean self-dual*, resp. *Hermitian self-dual* code if $C = C^\perp$ resp. $C = C^{\perp h}$.
- b) C is *Euclidean LCD*, resp. *Hermitian LCD* if $C \oplus C^\perp = R$ resp. $C \oplus C^{\perp h} = R$.

Note that all twisted skew group codes are idempotent codes if $\text{char } K \nmid |G|$, by Theorem 1.7. Also in the case that R is not semisimple it turned out that some interesting examples are idempotent codes, for instance the ternary self-dual extended Golay code [12]. Note that a Euclidean LCD group code is always an idempotent code [11]. This does not hold true for a twisted LCD group code since C^\perp might not be a left ideal in R for $\alpha \neq \alpha^{-1}$.

Suppose now that the cocycle α satisfies $\alpha = \alpha^{-1}$, i.e., α takes only values ± 1 . In this case we have

$$\langle a \cdot b, c \rangle = \langle a, c \cdot \hat{b} \rangle \tag{6}$$

for all $a, b, c \in R$, by direct calculations.

Most of the following results have been proved already for group or twisted group codes in [11, 12]. The proofs for twisted skew group codes are obvious extensions. Thus, for the reader's convenience, we will give only one proof.

Proposition 5.3. *Assume that $\alpha = \alpha^{-1}$. If $C \leq R$ is a twisted skew group code, then the following are equivalent.*

- a) C is an Euclidean LCD code.
- b) $C = Re$ where $e^2 = e = \widehat{e}$.

Proof. First we assume b), that is $C = Re$ where $e^2 = e = \widehat{e}$. Clearly, $R = Re \oplus R(1 - e)$, since e is an idempotent. Using equation (6) we get

$$\langle ae, b(1 - e) \rangle = \langle a, b(1 - e)\widehat{e} \rangle = \langle a, b(1 - e)e \rangle = \langle a, 0 \rangle = 0,$$

for all $a, b \in R$. Hence $R(1 - e) \leq C^\perp$. Since

$$\dim_K(R(1 - e)) = |G| - \dim_K(C) = \dim_K(C^\perp),$$

we have $R(1 - e) = C^\perp$.

Conversely assume that a) holds. Note that C^\perp is a left ideal of R , which follows from Theorem 1.9 and Theorem 4.1, using $\alpha = \alpha^{-1}$. Let $R = C \oplus C^\perp$ and write $1 = e + f$ with $e \in C$ and $f \in C^\perp$. Clearly, $e = e^2 + ef$ and $f = fe + f^2$, which implies $e^2 = e$, $f^2 = f$ and $ef = fe = 0$. Furthermore, $R = Re \oplus Rf$, hence $C = Re$ and $C^\perp = Rf$. If $a \in R$, then

$$0 = \langle ae, f \rangle = \langle a, f\widehat{e} \rangle = \langle a, (1 - e)\widehat{e} \rangle.$$

Since $\langle \cdot, \cdot \rangle$ is nondegenerate, we obtain $(1 - e)\widehat{e} = 0$ or equivalently $\widehat{e} = e\widehat{e}$. Finally, using Theorem 1.9 again, we get

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

which completes the proof. □

Proposition 5.4. *Assume that $\alpha = \alpha^{-1}$. For $0 \neq C = Re \leq R$ with $e^2 = e$, the following conditions are equivalent.*

- a) C is an Euclidean self-dual code.
- b) $e\widehat{e} = 0$ and $\overline{1} - \widehat{e} = (\overline{1} - \widehat{e})e$.

The propositions above have the following Hermitian extension.

Proposition 5.5. *Assume that $\alpha = \alpha^{-1}$ and $|K| = q^2$. If $C \leq R$ is a twisted skew group code, then the following are equivalent.*

- a) C is an Hermitian LCD code.
- b) $C = Re$ where $e^2 = e = \widehat{e^{(q)}}$.

Proposition 5.6. *Assume that $\alpha = \alpha^{-1}$ and $|K| = q^2$. For $0 \neq C = Re \leq R$ with $e^2 = e$, the following conditions are equivalent.*

- a) C is an Hermitian self-dual code.
- b) $e\widehat{e^{(q)}} = 0$ and $\overline{1} - \widehat{e^{(q)}} = (\overline{1} - \widehat{e^{(q)}})e$.

6 Examples.

We conclude with some examples of optimal codes in twisted skew group algebras.

Example 6.1. Let $G = D_6 = \langle x, y \mid x^3 = y^2 = 1, x^y = x^{-1} \rangle$ be a dihedral group of order 6. Let \mathbb{F}_4 be the field with 4 elements and let ω be a primitive element of \mathbb{F}_4 . Finally, let θ be the non-trivial homomorphism from D_6 onto $\text{Aut}(\mathbb{F}_4)$, i.e., $\Theta(t)$ is the Frobenius automorphism of \mathbb{F}_4 for any involution $t \in G$ and trivial otherwise. We put

$$e = \omega 1 + y + xy + \omega x^2 y \in \mathbb{F}_4[G, \Theta, 1].$$

Then $e = e^2$ and the left ideal C generated by e in $\mathbb{F}_4[G, \Theta, 1]$ is the $[6, 3, 4]$ quaternary hexacode \mathcal{H}_6 . Since \widehat{C} is generated by an idempotent, C is a projective $\mathbb{F}_4[G, \Theta, 1]$ -left module. Note that $\widehat{e^{(2)}} = e + 1$. Applying Proposition 5.6, we see that C is Hermitian self-dual. To our knowledge skew group codes have been considered so far only for cyclic groups. The hexacode seems to be the first interesting example in which the group is not cyclic.

Remark 6.2. a) The hexacode $C = \mathcal{H}_6$ can not be realized as a proper twisted group code:

Let $K = \mathbb{F}_4$. Suppose that $C \leq K^\alpha G = K[G, 1, \alpha]$ where $G = D_6$ or $G = C_6$ and $[\alpha] \neq [1]$. (Note that D_6 and C_6 are the only groups of order 6.) If $G = D_6$, then $[\alpha] = [1]$ since $|\text{H}^2(D_6, K^*)| = 1$, a contradiction. Now suppose that $G = C_6$ and $C = \mathcal{H}_6 \leq K^\alpha G$. We may assume that $\alpha = \alpha_\lambda$ as in (4). Note that $K^\alpha G$ has no irreducible module of dimension 1, by [24, Corollary 2.7]. Thus C is an irreducible $K^\alpha G$ -module. Since $K^\alpha G$ is not semisimple by [21, Lemma 12.2], we see that C is the Jacobson radical $J(K^\alpha G)$. If y is an involution in G , then $(\lambda^2 - y)^2 = 0$. Thus $\lambda^2 - y$ generates a nilpotent ideal, hence $\lambda^2 - y \in J(K^\alpha G) = C$, a contradiction, since the minimum distance of C is 4.

b) The hexacode $C = \mathcal{H}_6$ can not be realized as a group code:

Let $C_6 = C_3 \times C_2 = \langle x \rangle \times \langle y \rangle$. The structure of KG can be described as

$$KG = P(V_0) \oplus P(V_1) \oplus P(V_2),$$

where $V_0 = 1_G, V_1, V_2$ are the irreducible modules, all of dimension 1, and $\dim P(V_i) = 2$ for all i . Again suppose that $C \leq KG$. If $C = V_0 \oplus V_1 \oplus V_2$, then C we get a contradiction, since

$$V_i = \underbrace{\langle (1 + \lambda^i x + \lambda^{2i} x^2) + (1 + \lambda^i x + \lambda^{2i} x^2)y \rangle}_{=v_i}$$

and $v_0 + v_1 + v_2$ has weight 2. In the remaining case we have $P(V_i) \leq C$ for some i . Since all $P(V_i)$ are induced from an ideal in $K\langle x \rangle$, the ideal C contains a vector of weight 3, a contradiction again. Finally, we have to consider $G = D_6$. In this case we have $KG = P(1_G) \oplus V_1 \oplus V_2$, where $V_1 \cong V_2$ is irreducible of dimension 2. As $\dim C = 3$, we see that C is the direct sum of the trivial ideal and an ideal V which is isomorphic to V_1 . Let x be an element of order 3, y of order 2, both in G , and $x^y = x^{-1} = x^2$. We put $N = \langle x \rangle$. Since V is a projective KN -module and K is a splitting field, we may write

$V|_N = \langle v \rangle \oplus \langle w \rangle$ where $xv = \lambda v$ and $xw = \lambda^2 w$ and $1 \neq \lambda \in K^*$. We write $v = v_1 + yv_2$ with $v_i \in KN$ and may assume that the coefficient of v_1 is equal to 1. Since $xv = \lambda v$, we get $xv_1 = \lambda v_1$ and $xv_2 = \lambda^2 v_2$. Thus

$$v = 1 + \lambda x + \lambda^2 x^2 + \mu y(1 + \lambda^2 x + \lambda x^2)$$

with some $\mu \in K^*$. With $u = \mu^{-1} yv$ we get

$$v + u = 1 + x + x^2 + (\mu + \mu^{-1})1 + (\mu\lambda^2 + \mu^{-1}\lambda)x + (\mu\lambda + \mu^{-1}\lambda^2)x^2.$$

If $\mu = 1$, then $(v + u)K$ is the trivial module, a contradiction. If $\mu = \lambda$, then $v + u$ has weight 5, a contradiction. The same happens if $\mu = \lambda^2$, which finishes the proof.

c) Using group theoretic arguments, we see that $\text{PAut}(\mathcal{H}_6)$ is a group of order 60 generated by the permutations $(1, 2, 6)(3, 5, 4)$ and $(1, 2, 3, 4, 5)$ (see for instance [15, Example 1.7.8]). With MAGMA we see that $\text{PAut}(\mathcal{H}_6)$ does not contain a regular subgroup of order 6. Thus, according to [5, Theorem 1.2] and [12, Theorem 3.2] the hexacode \mathcal{H}_6 is neither a group code nor a twisted group code.

Example 6.3. Let G be the same group as in Example 6.1 and let \mathbb{F}_9 be the field with 9 elements. We fix ω as a primitive element of \mathbb{F}_9 . Finally, let $\Theta(t)$ be again the Frobenius automorphism of \mathbb{F}_9 for any involution $t \in G$ and trivial otherwise. With MAGMA we see that

$$e = \omega + \omega^2 x + \omega^2 x^2 + x^2 y \in \mathbb{F}_9[G, \Theta, 1]$$

is a self-adjoint idempotent, i.e., $e = e^2 = \hat{e}$. Therefore, by Proposition 5.3, the left ideal $C = Re \leq R = \mathbb{F}_9[G, \Theta, 1]$ is an Euclidean LCD skew code. Using MAGMA we may check that C is an MDS $[6, 3, 4]_9$ code with weight enumerator $W(C) = 1 + 120x^4 + 240x^5 + 368x^6$. Note that the given construction of a $[6, 3, 4]_9$ code is much simpler than the one given in Grassl's list [16].

Remark 6.4. In [23, Theorem 6.2] it is proved that Dickson's theorem holds for twisted group algebras, i.e., if $C = eK[G, 1, \alpha]$ with $0 \neq e = e^2$ and $\text{char } K = p$, then $|G|_p \mid \dim C$. As Example 6.1 shows this does not hold true in general for skew twisted group algebras.

Example 6.5. Let $G = A_4$ be the alternating group on 4 letters, $K = \mathbb{F}_{27} = \mathbb{F}_3[\tau]$ with $\tau^3 + 2\tau + 1 = 0$, and Θ with kernel $H = C_2 \times C_2 \leq \text{Alt}(4)$. We choose α as in [12, §5]. (Note that there is an obvious misprint in Table II of [12]. We have $\alpha(za, xa^2) = -1$ and $\alpha(za, ya^2) = 1$, as you can see directly from Table I.)

The following is a self-adjoint idempotent:

$$e = \tau^6 \text{Id} + \tau^{10}(1, 2)(3, 4) + \tau^{22}(1, 3, 2) + \tau^6(1, 4, 3) + \tau^{21}(2, 3, 4) + \tau^{10}(1, 2, 4) + \tau^{22}(1, 3, 4) + \tau^{23}(1, 4, 2) + \tau^{24}(1, 2, 3) + \tau^6(1, 3)(2, 4) + \tau^{22}(1, 4)(2, 3).$$

Therefore by Proposition 5.3 it generates an Euclidean LCD code C with parameters $[12, 4, 9]_{27}$ and has the following as a generator matrix

$$\text{gen}(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & \tau^2 & \tau^{17} & \tau^5 & \tau^{19} & \tau^{23} & \tau^{10} & \tau^{12} & \tau^{25} \\ 0 & 1 & 0 & 0 & \tau^{11} & \tau^{12} & \tau^{15} & 2 & \tau^{24} & \tau^{21} & \tau^{25} & \tau^7 \\ 0 & 0 & 1 & 0 & \tau^{14} & \tau^7 & \tau^{14} & \tau^{10} & \tau^{12} & \tau^2 & \tau^{18} & 2 \\ 0 & 0 & 0 & 1 & \tau & \tau & \tau^{21} & 2 & \tau^{12} & \tau^6 & \tau^{16} & \tau^{25} \end{bmatrix}.$$

Note that C and its dual are MDS codes.

Example 6.6. Let G be the semidirect product $G = C_7 \rtimes C_3 = \langle a \rangle \rtimes \langle b \rangle$ and let $K = \mathbb{F}_8 = \mathbb{F}_2[\tau]$ with $\tau^3 + \tau + 1 = 0$. We choose Θ with kernel $H = C_7$ and α trivial. Then

$$c = \tau^3 1 + \tau^6 a + \tau a^2 + \tau^4 a^3 + \tau a^4 + a^6 + \tau^4 b + \tau b a + \tau^6 b a^2 + \tau^3 b a^3 + \tau^6 b a^4 + \tau^3 b a^5 + \tau^3 b a^6 + \tau^6 b^2 + \tau^2 b^2 a + \tau^2 b^2 a^2 + \tau^2 b^2 a^4 + \tau^3 b^2 a^5 + \tau^3 b^2 a^6$$

generates an LCD code C with parameters $[21, 14, 6]_8$. The dual has parameters $[21, 7, 12]_8$. Thus C and its dual are optimal according to Grassl's list [16]. A generator matrix of C is

$$\text{gen}(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^5 & 0 & \tau^3 & 0 & \tau^2 & \tau & \tau^4 & \tau \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^3 & 0 & \tau^4 & \tau^6 & \tau^2 & 1 & 1 & \tau^3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau & 0 & \tau^3 & \tau & 1 & \tau^6 & \tau^2 & \tau^3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^6 & 0 & 0 & \tau^4 & \tau^4 & \tau^4 & \tau^4 & \tau^4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^4 & 0 & \tau^4 & 1 & \tau^5 & 0 & \tau^3 & \tau^2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^2 & 0 & 1 & \tau^4 & 1 & \tau^5 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \tau^5 & \tau & \tau & 0 & \tau^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^6 & 0 & \tau^6 & \tau^6 & 0 & \tau & \tau^4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^5 & 0 & \tau^2 & 0 & 1 & 1 & 0 & \tau^4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \tau^4 & 0 & 0 & \tau^4 & \tau^2 & \tau^6 & \tau^6 & \tau^4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \tau^3 & 0 & \tau^4 & \tau & \tau^4 & \tau^3 & 1 & \tau^5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \tau^2 & 0 & \tau^6 & \tau^4 & 1 & 0 & \tau & \tau^3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \tau & 0 & \tau^4 & \tau^4 & 0 & \tau^4 & \tau^6 & \tau \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \tau^4 & \tau & \tau^5 & \tau^2 & \tau^6 & \tau^3 \end{bmatrix}.$$

Example 6.7. Let G be the dihedral group of order 20, $G = C_{10} \rtimes C_2 = \langle a \rangle \rtimes \langle b \rangle$ and let $K = \mathbb{F}_9 = \mathbb{F}_2[\tau]$ with $\tau^2 + 2\tau + 2 = 0$. We choose Θ with kernel $H = C_{10}$ and α as in Table 1. This cocycle, which is not a coboundary, has been determined thanks to the algorithm presented in [14].

Then

$$c = \tau^7 + a + \tau a^2 + \tau^2 a^3 + \tau^5 a^5 + \tau a^6 + 2a^7 + \tau^3 a^8 + 2a^9 + (\tau^6 + \tau a + \tau a^2 + \tau^6 a^3 + \tau^5 a^4 + \tau^2 a^5 + \tau^7 a^6 + \tau^5 a^7 + \tau^5 a^8 + \tau^3 a^9)b$$

generates an LCD code C with parameters $[20, 16, 4]_9$. The dual has parameters $[20, 4, 15]_9$. Thus C and its dual are optimal according to Grassl's list [16]. A generator matrix of C is

$$\text{gen}(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & \tau \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^3 & 0 & \tau & \tau^3 & \tau^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^7 & 0 & \tau^5 & \tau & \tau^7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^6 & \tau^5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^7 & 0 & 1 & \tau^3 & \tau^3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \tau & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^5 & 0 & 1 & 0 & \tau^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^5 & 0 & 2 & \tau & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \tau^7 & \tau^2 & \tau \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & \tau^3 & \tau^7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \tau^3 & 0 & \tau & \tau & \tau^5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & \tau^6 & 1 & \tau^6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \tau & 0 & \tau^2 & \tau^7 & \tau^6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \tau & 0 & 2 & \tau \\ 0 & \tau^3 & \tau^7 & 2 \end{bmatrix}.$$

	1	b	a	ab	a^2	b	a^3	a^3b	a^4	a^4b	a^5	a^5b	a^6	a^6b	a^7	a^7b	a^8	a^8b	a^9	a^9b
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
b	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
ab	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^2b	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^3	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^3b	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^4b	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^5	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^5b	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^6b	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^7	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^7b	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
a^8b	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^9	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
a^9b	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 1: $\alpha \in H^2(D_{20}, \mathbb{F}_9)$

Remark 6.8. We found the above optimal codes by extensive search in MAGMA. It would be extremely interesting to find a method to define twisted skew G -codes with prescribed minimum distance, as in the classical case of BCH codes. Note that this has been already done for particular G -codes in [3, 7]. Moreover, note that the product between minimum distance and dimension of these examples is far away from the lower bound given in Theorem 2.4.

Acknowledgements

The first author is grateful for the support of the Israel Science Foundation (grant no. 353/21). The second author was partially supported by the ANR-21-CE39-0009 - BAR-RACUDA (French *Agence Nationale de la Recherche*).

References

- [1] A. BATOUL, D. BOUCHER AND R. BOULANOUAR. On overview of skew constacyclic codes and their subclasses of LCD codes. *Adv. Math. Commun.* 15.4 (2021): 611-632.
- [2] L.M. BAZZI AND S.K. MITTER. Some randomized code constructions from group actions. *IEEE Trans. Inform. Theory*, 52.7 (2006): 3210-3219.
- [3] A. BEHAJAINA. On BCH split metacyclic codes. *Adv. Math. Commun.* (2021).
- [4] S.D. BERMAN. Semisimple cyclic and Abelian codes. II. *Kibernetika* (Kiev) no. 3 (1967): 21-30 (Russian).

- [5] J.J. BERNAL, A. DEL RÍO AND J.J. SIMÓN. An intrinsical description of group codes, *Des. Codes and Cryptogr.* 51 (2009): 289-300.
- [6] M. BORELLO, J. DE LA CRUZ AND W. WILLEMS. On checkable group codes. *J. Algebra and its Appl.* 21 (2022).
- [7] M. BORELLO AND A. JAMOUS. Dihedral codes with prescribed minimum distance. In: Bajard J.C., Topuzoglu A. (eds) Arithmetic of Finite Fields. WAIFI 2020. *Lecture Notes in Computer Science*, vol 12542. Springer, Cham. (2021).
- [8] M. BORELLO AND W. WILLEMS. Group codes over fields are asymptotically good. *Finite Fields Appl.*, 68 (2020): 101738.
- [9] M. BORELLO, W. WILLEMS AND G. ZINI. On ideals in group algebras: an uncertainty principle and the Schur product. *Forum Mathematicum* (2022) doi:10.1515/forum-2022-0064.
- [10] D. BOUCHER, W. GEISELMANN AND F. ULMER. Skew-cyclic codes. *App. Algebra in Eng. Comm. and Comp.* 18 (2007): 379-389.
- [11] J. DE LA CRUZ AND W. WILLEMS. On group codes with complementary duals, *Des. Codes and Cryptogr.* 86 (2018): 2065-2073.
- [12] J. DE LA CRUZ AND W. WILLEMS. Twisted group codes. *IEEE Trans. Inform. Theory.* 67 (2021): 5178-5184.
- [13] S.T. DOUGHERTY, S. SAHINKAYA AND B. YILDIZ. Skew G-codes. *J. Algebra and its Appl.*, (2021): 2350056.
- [14] G. ELLIS AND I. KHOLODNA. Computing second cohomology of finite groups with trivial coefficients. *Homology, Homotopy and Applications* 1.1 (1999): 163-168.
- [15] C.W. HUFFMAN AND V. PLESS. *Fundamentals of error correcting codes*. Cambridge University Press Cambridge 2003.
- [16] M. GRASSL. Bounds on the minimum distance of linear codes. Online <http://www.codetables.de>.
- [17] G. KARPILOVSKY. *Projective Representations of Finite Groups*. Marcel Dekker, New York, USA, 1985.
- [18] F.J. MACWILLIAMS. Codes and ideals in group algebras. *Combinatorial Mathematics and its Applications, Proceedings ed. by R.C. Bose and T.A. Dowling*, pages 317-328, 1967.
- [19] M. LINCKELMANN. *The Block Theory of Finite Group Algebras*. London Math. Soc., Student Text 91, Cambridge University Press 2018.
- [20] P. MORANDI. Field and Galois Theory. *Graduate Texts in Mathematics*. 167. New York, NY: Springer. xvi, 281 p. (1996).

- [21] D.S. PASSMAN. The Jacobson radical of group rings of locally finite groups. *Trans. Am. Math. Soc.* 349 (1997), 4693-4751.
- [22] E. PRANGE. Cyclic Error-Correcting Codes in Two Symbols. *Air Force Cambridge Research Center*, Cambridge, MA, Tech. Rep. AFCRC-TN-57-103 (1957).
- [23] W. WILLEMS. Codes in Group Algebras. In W.C. Huffman, J.-L. Kim and P. Solé, editors, *Concise Encyclopedia of Coding Theory*, Chap. 16, pages 363-384, CRC Press, Chapman and Hall, Boca Raton, USA, 2021.
- [24] W. WILLEMS. Codes in twisted group algebras. To appear.
- [25] Y.A. WOOD. Duality for modules over finite rings and applications to coding theory. *Am. J. Math.* 121 (1999): 555-575.