Twisted group codes

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

Keywords. Twisted group algebra, 2-cocycle
MSC classification. 94B05, 20C05

Abstract

We investigate right ideals as codes in twisted group algebras. Such codes are called twisted group codes. It turns out that many interesting codes belong to this class; for instance, the ternary extended Golay code, Hamming codes and constacyclic codes. In particular we characterize all linear codes which are twisted group codes in terms of their automorphism group.

1 Introduction

Group codes, i.e., left or right ideals in group algebras over finite groups turned out to be a class of interesting linear codes [14], [1], [6], [8], [3], [16], [7], [5], [4]. Many optimal linear codes can be realized as group codes. The advantage to look at group codes is the algebra structure of the ambient space which may be used via representation theory to lead to surprising coding theoretical facts. However, there are other interesting codes which are still ideals in an algebra, namely a twisted group algebra, which in general is not a group algebra. For instance, the binary extended Golay code is a right ideal in the group algebra $\mathbb{F}_2\mathrm{S}_4$ where S_4 is the symmetric group on 4 letters [3]. The ternary extended Golay code is never a group code [16], but it turns out that it is a right ideal in the twisted group algebra $\mathbb{F}_3^\alpha\mathrm{A}_4$ where A_4 is the alternating group on 4 letters and α defines a twist in the algebra structure (section 5). Such ideals (right or left) are called twisted group codes. We shall see that all perfect linear codes are twisted group codes (section 6). As one of the main results we characterize in Theorem 3.2 all linear codes C which are twisted group codes. Similar to group codes [2] the answer depends on particular subgroups of $\mathrm{Aut}(C)$.

Throughout the paper G always denotes a finite multiplicative group and $\mathbb{F}$ a field, which is not necessarily assumed to be finite. In case of a finite field we write $\mathbb{F}_q$ for $\mathbb{F}$ if q is the size of the field $\mathbb{F}$. We use 1 for both, the identity $1 = 1_G$ in G and the identity $1 = 1_\mathbb{F}$ in the field $\mathbb{F}$. Finally, by $E = E_n$ we denote the identity matrix of type (n, n).

2 Preliminaries

Definition 2.1 a) A map $\alpha : G \times G \longrightarrow \mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is called a 2-*cocycle* of G if

$$\alpha(g_1, g_2g_3)\alpha(g_2, g_3) = \alpha(g_1g_2, g_3)\alpha(g_1, g_2)$$

for all $g_i \in G$. We denote the set of all 2-cocycles of G by $\mathrm{Z^2(G,\mathbb{F}^*)}$.
b) A 2-cocycle α is called a *coboundary* if there exists a map $\beta : G \longrightarrow \mathbb{F}^*$ with $\beta(1) = 1$ such that

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

for all $g, h \in G$. Let $\mathrm{B}^2(G, \mathbb{F}^*)$ denote the set of all coboundaries of G.

Note that we can replace a 2-cocycle α by the normalized 2-cocycle α' which is defined by

$$\alpha'(g, h) = \frac{\alpha(g, h)}{\alpha(1, 1)}.$$

In this case we obviously have

$$\alpha'(g, 1) = \alpha'(1, h) = \alpha'(1, 1) = 1.$$

for all $g, h \in G$.

In the following we always assume that 2-cocycles are normalized.

Definition 2.2 Let α be a 2-cocycle of G and let

$$\mathbb{F}^\alpha G = \{a = \sum_{g \in G} a_g \overline{g} \mid a_g \in \mathbb{F}\}$$

be the $\mathbb{F}$-vector space with basis $\{\overline{g} \in G\}$, which is in one to one correspondence with G, and multiplication

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

extended linearly. Observe that $\mathbb{F}^\alpha G$ is an associative $\mathbb{F}$-algebra of dimension $|G|$ called a *twisted group algebra.*

Remark 2.3 a) For $\alpha, \beta \in \mathrm{Z^2(G,\mathbb{F}^*)}$, we define $\alpha\beta \in \mathrm{Z^2(G,\mathbb{F}^*)}$ by $\alpha\beta(g, h) = \alpha(g, h)\beta(g, h)$ for all $g, h \in G$. With this operation $\mathrm{Z^2(G,\mathbb{F}^*)}$ becomes a multiplicative abelian group.
b) The set $\mathrm{B}^2(G, \mathbb{F}^*)$ of coboundaries forms a subgroup of the group $\mathrm{Z^2(G,\mathbb{F}^*)}$ and the factor group $\mathrm{H}^2(G, \mathbb{F}^*) = \mathrm{Z^2(G,\mathbb{F}^*)}/\mathrm{B^2(G,\mathbb{F}^*)}$ is usually called the second cohomology group of G with values in $\mathbb{F}^*$. For $\alpha \in \mathrm{Z^2(G,\mathbb{F}^*)}$ we denote its image in $\mathrm{H}^2(G, \mathbb{F}^*)$ by $[\alpha]$.
c) Let $\alpha, \beta \in \mathrm{Z^2(G,\mathbb{F}^*)}$. Then $\mathbb{F}^\alpha G \cong \mathbb{F}^\beta G$ as algebras if and only if $[\alpha] = [\beta]$ (see for instance ([13], Proposition 1.2.6)). More precisely, if $\alpha(g, h) = \beta(g, h)\gamma(g)\gamma(h)\gamma(gh)^{-1}$, then the isomorphism from $\mathbb{F}^\alpha G$ to $\mathbb{F}^\beta G$ is given by $g \mapsto \gamma(g)g$ for $g \in G$. Note that this isomorphism is distance preserving.

Definition 2.4 We call a right ideal C in a twisted group algebra $\mathbb{F}^\alpha G$ a *twisted group* code, more precisely a (G,α)-code over $\mathbb{F}$. We then briefly write $C \leq \mathbb{F}^\alpha G$. In case G is cyclic, abelian, dihedral, ... we say that C is a twisted cyclic, abelian, resp. dihedral group code.

To look at right ideals is just for convenience. Everything in the following holds equally true for left ideals.

Example 2.5 By definition a λ-constacyclic code of length n over $\mathbb{F}$ is an ideal in the algebra $A = \mathbb{F}[x]/(x^n - \lambda)$ where $\lambda \in \mathbb{F}^*$. Let G be a cyclic group of order n generated by g. We define a (normalized) 2-cocycle α_λ by

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

With this setting we have $A \cong \mathbb{F}^{\alpha_\lambda} G$. Thus constacyclic codes are twisted cyclic group codes. Note that $\mathbb{F}^{\alpha_\lambda} G$ is a commutative algebra.

Definition 2.6 As in the case of group algebras we define a symmetric non-degenerate bilinear form

$$\langle \cdot\,, \cdot \rangle : \mathbb{F}^\alpha G \times \mathbb{F}^\alpha G \longrightarrow \mathbb{F}$$

by setting

$$\langle \overline{g}, \overline{h} \rangle = \delta_{g,h}.$$

for $g, h \in G$.

Observe that in general the form $\langle \cdot\,, \cdot \rangle$ is no longer G-invariant since

$$\langle \overline{g}\,\overline{x}, \overline{h}\,\overline{x} \rangle = \langle \overline{g}, \overline{h} \rangle \alpha(g,x)\alpha(h,x)$$

for $g, h, x \in G$.

Definition 2.7 For $a = \sum_{g \in G} a_g g \in \mathbb{F}^\alpha G$ we put

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

The map $a \mapsto \widehat{a}$ is obviously an $\mathbb{F}$-linear isomorphism on $\mathbb{F}^\alpha G$, but in general neither an involution nor an anti-algebra isomorphism.

Lemma 2.8 *Let G be a finite group and let α be a 2-cocycle for G.*

a) *We have $\alpha(g, g^{-1}) = \alpha(g^{-1}, g)$ for all $g \in G$.*

b) *If $\alpha(g, g^{-1})\alpha(g^{-1}, g) = 1$ for all $g \in G$, then $\widehat{\widehat{a}} = a$ for all $a \in \mathbb{F}^\alpha G$.*

Proof: The statements are straight forward calculations.

□

Recall that the multiplication $\circ$ in the opposite algebra A^{op} of an algebra A is defined by $a \circ b = ba$.

Proposition 2.9 ([13], Proposition 1.6.9) *The map $a \mapsto \widehat{a}$ induces an algebra isomorphism from $(\mathbb{F}^{\alpha}G)^{op}$ onto $\mathbb{F}^{\alpha^{-1}}G$.*

As a direct consequence we have the following fact.

Theorem 2.10 *Suppose that $\alpha = \alpha^{-1}$ is a 2-cocycle for G. Then $a \mapsto \widehat{a}$ defines an anti-algebra isomorphism of $\mathbb{F}^{\alpha}G$ of order 2.*

Proof: The condition $\widehat{\widehat{a}} = a$ follows from Lemma 2.8 b). □

Recall that a finite dimensional $\mathbb{F}$-algebra A is called a *Frobenius algebra* if there exists an $\mathbb{F}$-linear function $\lambda \in \mathrm{Hom}_K(A, \mathbb{F})$ whose kernel contains no left or right ideal other than zero ([11], Chap. VII, Exercise 53). If $A = \mathbb{F}^{\alpha}G$ is a twisted group algebra, we may define $\lambda \in \mathrm{Hom}_K(A, \mathbb{F})$ by

$$\lambda(a) = a_1$$

for $a = a_1\overline{1} + \sum_{1\neq g\in G} a_g\overline{g}$. Suppose that I is a right ideal in $\mathbb{F}^{\alpha}G$ and $\lambda(I) = 0$. If $a = \sum_{g\in G} a_g\overline{g} \in I$ with $a_h \neq 0$ for some $h \in G$, then

$$0 = \lambda(a\overline{h^{-1}}) = \alpha(h, h^{-1})a_h \neq 0,$$

a contradiction since $a\overline{h^{-1}} \in I$. Thus twisted group algebras are Frobenius algebras. Note that by Lemma 2.8 a), we have $\lambda(ab) = \lambda(ba)$ for all $a, b \in A$. Thus twisted group algebras are even symmetric algebras ([11], Chap. VII, Exercise 54).

On $A = \mathbb{F}^{\alpha}G$ there is a non-degenerate bilinear form $\langle \cdot\,, \cdot \rangle_{\mathrm{Frob}}$ given by

$$\langle a, b\rangle_{\mathrm{Frob}} = \lambda(ab)$$

for $a, b \in A$. Note that $\langle ac, b\rangle_{\mathrm{Frob}} = \langle a, cb\rangle_{\mathrm{Frob}}$ for all $a, b, c \in A$. Thus, if $C \leq A$, then

$$\mathrm{Ann}_l(C) = L(C) := \{a \in A \mid \langle a, c\rangle_{\mathrm{Frob}} = 0 \text{ for all } c \in C\}.$$

This leads us to an extension of an early result of MacWilliams ([14], Theorem 1) to twisted group algebras.

Proposition 2.11 *Let $C \leq \mathbb{F}^{\alpha}G$ be a twisted group code. Then*

$$C^{\perp} = \widehat{\mathrm{Ann}_l(C)}.$$

Proof: Let $a \in \mathrm{Ann}_l(C)$. Thus for $c \in C$ we have

$$0 = \langle ac, \overline{1} \rangle = \langle c, \widehat{a} \rangle,$$

by Lemma 2.8 a). This proves that $\widehat{\mathrm{Ann}_l(C)} \leq \mathrm{C}^{\perp}$. Note that $\dim \widehat{\mathrm{Ann}_l(C)} = \dim \mathrm{Ann}_l(C)$ and $\dim C^{\perp} = |G| - \dim C$. Since $\mathbb{F}^{\alpha}G$ is a Frobenius algebra, we have $\dim \mathrm{Ann}_l(C) = \dim L(C) = |G| - \dim C$ (see [11], Chap. VII, Section 11) which completes the proof. □

Clearly, if $\alpha = \alpha^{-1}$, then for $C \leq \mathbb{F}^{\alpha}G$ the dual code $C^{\perp}$ is also a right ideal in $\mathbb{F}^{\alpha}G$, by Theorem 2.10. But in general $C^{\perp}$ is not a right ideal in $\mathbb{F}^{\alpha}G$. We only have $C^{\perp} \leq \mathbb{F}^{\alpha^{-1}}G$.

In the following we denote by $\mathrm{M}(\mathbb{F}_q, n)$ the set of the monomial matrices A of type $n \times n$. A monomial matrix which is a multiple of the identity matrix is called a scalar matrix. If $C \leq \mathbb{F}_q^n$ is a linear code, then

$$\mathrm{Aut}(C) = \{A \mid A \in \mathrm{M}(\mathbb{F}_q, n),\, CA = C\}$$

is the group of automorphisms of C. Recall that a monomial matrix A of type $n \times n$ over $\mathbb{F}_q$ is of the form

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

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

Lemma 2.12 *Let $C \leq \mathbb{F}_q^{\alpha}G$ be a twisted group code. Then $A = DP \in \mathrm{Aut}(C)$ if and only if $A' = D^{-1}P \in \mathrm{Aut}(C^{\perp})$.*

Proof: It is well-known that $\mathrm{Aut}(C^{\perp}) = \mathrm{Aut}(C)^T$ where A^T denotes the transpose of the matrix A. If $A = DP \in \mathrm{Aut}(C)$ is the matrix of the action of $g \in G$ on $\mathbb{F}^{\alpha}G$ (from the right), then $\alpha(h, g)$ is the entry at (h, g) in the diagonal matrix D. Since with A also $A^{-1} \in \mathrm{Aut}(C)$ we get

$$A' = A^{-1^T} = (P^{-1}D^{-1})^T = D^{-1^T}P^{-1^T} = D^{-1}P$$

and the assertion follows since $C^{\perp\perp} = C$. □

3 When is a linear code a twisted group code?

Let G be a finite group of order n. Then, according to ([2], Theorem 1.2), a linear code $C \leq \mathbb{F}_q^n$ is a G-code (i.e., a right ideal in the group algebra $\mathbb{F}_qG$) if and only if G is isomorphic to a regular subgroup of the group of permutation automorphisms of C which means that $G \cong H \leq \mathrm{Aut}(C)$ where H is a group of permutations which acts transitively on the set $\{1, \ldots, n\}$ of coordinates of C and the stabilizer of any coordinate in H is the trivial group. In this section we prove its analogue for twisted group codes.

To start with let α be a normalized 2-cocycle of G with values in $\mathbb{F}_q^*$. We put

$$G(\alpha) = \mathbb{F}_q^* \times G$$

and define a group structure on $G(\alpha)$ by setting

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

for $\lambda, \mu \in \mathbb{F}_q^*$ and $g, h \in G$. Note that

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

is a normal subgroup of $G(\alpha)$ and $G(\alpha)/N \cong G$. Furthermore, $G(\alpha)$ allows a monomial action on $\mathbb{F}_q^\alpha G$ by

$$\overline{g}(\lambda, h) = (\lambda\overline{g})\overline{h} = \lambda\alpha(g, h)\overline{gh}.$$

Observe that the only diagonal matrices of this action are scalar multiples of the identity.

Lemma 3.1 *Let C be a twisted group code in $\mathbb{F}_q^\alpha G$ for a suitable 2-cocycle α of G. Then there exists a subgroup $\widehat{G} \leq \mathrm{Aut}(C)$ in which the only diagonal matrices are scalar matrices and $G \cong \pi(\widehat{G})$ acts regularly on the coordinate set $\{\overline{g} \mid g \in G\}$ of $\mathbb{F}_q^\alpha G$.*

Proof: Let $c = \sum_{g \in G} c_g\overline{g} \in C$ and $(\lambda, h) \in G(\alpha)$. Then

$$c(\lambda, h) = \sum_{g \in G} c_g\overline{g}(\lambda, h) = \sum_{g \in G} c_g\overline{g}(\lambda, h) = \lambda c\overline{h} \in C$$

since C is a right ideal in $\mathbb{F}_q^\alpha G$. Thus if $\widehat{G}$ is the group of monomial matrices corresponding to the right action of $G(\alpha)$ on $\mathbb{F}_q^\alpha G$, then $\widehat{G} \leq \mathrm{Aut}(C)$. Clearly, $G \cong \pi(\widehat{G})$ acts regularly on the coordinate set $\{\overline{g} \mid g \in G\}$. □

Theorem 3.2 *Let $C \leq \mathbb{F}_q^n$ be a linear code. Then C is a twisted group code in $\mathbb{F}_q^\alpha G$ for a suitable 2-cocycle α of G if and only if there exists a subgroup $\widehat{G} \leq \mathrm{Aut}(C)$ where $G = \pi(\widehat{G})$ acts regularly on $\{1, \ldots, n\}$ and the only diagonal matrices in $\widehat{G}$ are scalar matrices.*

Proof: According to Lemma 3.1 we only have to prove that C is a twisted group code if there exists $\widehat{G} \leq \mathrm{Aut}(C)$ with the mentioned properties. For each $y \in G$ we choose an element $\widehat{y} \in \widehat{G}$ such that $\pi(\widehat{y}) = y$. Later on we will take $\widehat{y}$ with a particular property. Let $B = \{e_i \mid i = 1, \ldots, n\}$ denote the standard basis of $\mathbb{F}_q^n$. Since G acts regularly on $\{1, \ldots, n\}$ we may identify $i \in \{1, \ldots, n\}$ with the unique element $x \in G$ where $i = 1x$.

Thus $B = \{e_x \mid x \in G\}$. Note that for $y \in G$ we have $iy = (1x)y = 1(xy)$. Hence iy corresponds to xy. Now let

$$e_x\widehat{y} = a_x(\widehat{y})e_{xy}.$$

If $\widehat{y}' \in \widehat{G}$ with $\pi(\widehat{y}') = \pi(\widehat{y}) = y$, then $\widehat{y} = \lambda\widehat{y}'$ for some $\lambda \in \mathbb{F}_q^*$, by assumption. Thus for each $y \in G$ we may choose the unique $\widehat{y} \in \widehat{G}$ with $a_1(\widehat{y}) = 1$.

Now we define $\alpha : G \times G \longrightarrow \mathbb{F}_q^*$ by

$$\alpha(x, y) = a_x(\widehat{y}).$$

First we prove that α is a 2-cocycle. We have to show that

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

for all $x, y, z \in G$ or equivalently that

$$a_{xy}(\widehat{z})a_x(\widehat{y}) = a_x(\widehat{yz})a_y(\widehat{z}).$$

Computing $(e_x\widehat{y})\widehat{z} = e_x(\widehat{y}\widehat{z})$ we see that

$$(*) \qquad a_{xy}(\widehat{z})a_x(\widehat{y}) = a_x(\widehat{y}\widehat{z}).$$

Thus it needs to show that

$$a_x(\widehat{y}\widehat{z}) = a_x(\widehat{yz})a_y(\widehat{z}).$$

By $(*)$ we have $a_y(\widehat{z}) = a_1(\widehat{y}\widehat{z})$. Thus it needs to show that

$$a_x(\widehat{y}\widehat{z}) = a_x(\widehat{yz})a_y(\widehat{z}) = a_x(\widehat{yz})a_1(\widehat{y}\widehat{z})$$

which is obviously true since

$$\frac{1}{a_1(\widehat{y}\widehat{z})}\widehat{y}\widehat{z} = \widehat{yz}.$$

Thus α is a 2-cocycle of G.

Finally we consider the $\mathbb{F}_q$-linear isomorphism

$$\gamma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^\alpha G$$

defined by $e_x\gamma = \overline{x}$. For $\widehat{y} \in \widehat{G}$ we have on one hand side

$$(e_x\widehat{y})\gamma = (a_x(\widehat{y})e_{xy})\gamma = a_x(\widehat{y})\overline{xy},$$

on the other hand side

$$(e_x\gamma)\overline{y} = \overline{x}\,\overline{y} = \alpha(x, y)\overline{xy} = a_x(\widehat{y})\overline{xy}.$$

Thus, since C is invariant under $\widehat{G}$ we get that $C\gamma$ is a right ideal in $\mathbb{F}_q^\alpha G$ and the proof is complete. □

Example 3.3 Let C be the ternary $[4,2,3]$ Hamming code, often called the tetracode. An easy calculation with Magma shows that

$$\operatorname{Aut}(C) = \left\langle \operatorname{diag}(1,1,1,-1)\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \operatorname{diag}(1,1,1,-1)\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle$$

which is isomorphic to $\mathrm{GL}(2,3)$ of order 48.

If we put

$$\widehat{G} := \left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} \right\rangle \leq \operatorname{Aut}(C),$$

then $\widehat{G}$ is a group of order 8 (actually isomorphic to a quaternion group) in which the only diagonal matrices are $\pm E$. Clearly, $G = \pi(\widehat{G}) = \langle (12)(34), (13)(24) \rangle \cong V_4$ acts regularly on $\{1, \dots, 4\}$. Therefore, according to Theorem 3.2, the linear code C is a twisted group code in $\mathbb{F}_3^\alpha G$ for a suitable 2-cocycle α of G. Note that C is not a group code, by ([2], Theorem 1.2), since the subgroup of $\operatorname{Aut}(C)$ consisting of permutation matrices has order 3. In Proposition 6.1 we shall deal with arbitrary Hamming codes.

Remark 3.4 If α in Theorem 3.2 is a coboundary, then C is a group code since $\mathbb{F}_q^\alpha G \cong \mathbb{F}G$. The coboundary condition of α also means that the extension

$$1 \longrightarrow \operatorname{Ker}\pi \longrightarrow \widehat{G} \longrightarrow G = \pi(G) \longrightarrow 1$$

splits ([13], section preceding Theorem 1.2.12), i.e.,

$$\operatorname{Aut}(C) \geq \widehat{G} = \operatorname{Ker}\pi \rtimes H$$

with $G \cong H$ and H acts regularly on $\{1, \dots, n\}$. Note, that H may not be a group of permutation matrices. But we can replace H by an isomorphic group of permutation matrices in $\operatorname{Aut}(C)$, which acts regularly, as follows.

Since α is a 2-coboundary of G we have $\alpha(h,h') = \beta(h)\beta(h')\beta(hh')^{-1}$ for all $h, h' \in H$. Replacing the basis $\{e_x \mid x \in G\}$ by $\{f_h = \frac{1}{\beta(h)} e_h \mid h \in H\}$ we get

$$f_{h'}\,\widehat{h} = \beta(h) f_{h'h}.$$

Thus h acts on C by the matrix $\beta(h)P(\pi(h)) \in \operatorname{Aut}(C)$. Since obviously nonzero scalar matrices of type(n,n) are in $\operatorname{Aut}(C)$ we get $P(\pi(h)) \in \operatorname{Aut}(C)$ for all $h \in H$. This shows that in Theorem 3.2, in the case that α is a coboundary, $\operatorname{Aut}(C)$ contains a regular subgroup of permutation matrices of order n in agreement with ([2], Theorem 1.2).

4 Self-dual twisted group codes

According to [16], a group algebra $\mathbb{F}G$ contains a self-dual group code if and only if the characteristic of $\mathbb{F}$ is two and 2 divides the order of G. In twisted group algebras self-dual codes may also exist in odd characteristic as the next example shows.

Example 4.1 Let $V = \langle x, y \rangle$ be the Klein four group. We may define a twisted group algebra $\mathbb{F}_3^\alpha V$ by the multiplication table

	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{z}$
$\overline{1}$	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{z}$
$\overline{x}$	$\overline{x}$	$-\overline{1}$	$\overline{z}$	$-\overline{y}$
$\overline{y}$	$\overline{y}$	$-\overline{z}$	$-\overline{1}$	$\overline{x}$
$\overline{z}$	$\overline{z}$	$\overline{y}$	$-\overline{x}$	$-\overline{1}$

For $e = -\overline{1} + \overline{x} + \overline{y}$ we have $e = e^2$. Thus $C = e\mathbb{F}_3^\alpha V$ is a direct summand in $\mathbb{F}_q^\alpha V$. One easily computes that $\dim C = 2$ and for the minimum distance we get $\mathrm{d}(C) = 3$. Furthermore $C = C^\perp$ and C is an irreducible $\mathbb{F}_3^\alpha V$-module. Thus C is an irreducible self-dual $[4, 2, 3]_3$ twisted group code. Actually C is the ternary $[4, 2, 3]$ Hamming code of Example 3.3.

Theorem 4.2 *Let $C = C^\perp \leq \mathbb{F}_q^\alpha G$ and suppose that the only diagonal matrices in* $\mathrm{Aut}(C)$ *are scalar matrices. Then $\alpha = \alpha^{-1}$.*

Proof: If $A = \mathrm{diag}(\alpha(1, g), \ldots, \alpha(x, g), \ldots)P(\pi(g))$ is the matrix of the action of $g \in G$ on $\mathbb{F}^\alpha G$ from the right, then $A \in \mathrm{Aut}(C)$, and according to Lemma 2.12, we get

$$B = \mathrm{diag}(\alpha(1, g)^{-1}, \ldots, \alpha(x, g)^{-1}, \ldots)P(\pi(g)) \in \mathrm{Aut}(C^\perp) = \mathrm{Aut}(C).$$

Thus

$$D = AB^{-1} = \mathrm{diag}(\alpha(1, g)^2, \ldots, \alpha(x, g)^2, \ldots) \in \mathrm{Aut}(C).$$

Since α is normalized (what we always assume) we have $\alpha(1, g) = 1$ for all $g \in G$. Now the assumption that scalar matrices are the only diagonal automorphisms implies that $D = E$ is the identity matrix. Thus $\alpha = \alpha^{-1}$. □

Corollary 4.3 *If $C = C^\perp$ is a twisted group code over a finite field of characteristic* 2 *and suppose that the only diagonal matrices in* $\mathrm{Aut}(C)$ *are scalar matrices, then C is a group code.*

Proof: According to Theorem 4.2 we have $\alpha = \alpha^{-1}$. Furthermore, $\mathbb{F}^* = \mathbb{F}_q^*$ has odd order if $2 \mid q$. Thus $\alpha^2 = 1$ implies that $\alpha = 1$, i.e., $\alpha(g, h) = 1$ for all $g, h \in G$. □

Example 4.4 Let $C = C^{\perp}$ be a λ-constacyclic code with minimum distance $\mathrm{d}(C) \geq 2$. Thus, according to Example 2.5, we may assume that $0 \neq C = C^{\perp} < \mathbb{F}^{\alpha_\lambda}G$ where $G = \langle g \rangle$, say of order n. Furthermore,

$$\alpha_\lambda(x, g^{n-1}) = \lambda$$

for all $1 \neq x \in G$. If we order G by $1, g, g^2, \ldots, g^{n-1}$, then according to the proof of Theorem 4.2 we see that $D = \mathrm{diag}(1, 1, \cdots, \lambda^2) \in \mathrm{Aut}(C)$. Let $0 \neq c = \sum_{i=0}^{n-1} c_i\overline{g^i} \in C$. Clearly, we may assume that $c_{n-1} \neq 0$. Suppose that $\lambda \neq \pm 1$. Thus $0 \neq c' = c - cD \in \mathrm{Aut}(C)$ and $\mathrm{wt}(c') = 1$. This contradicts $C < \mathbb{F}^{\alpha_\lambda}G$. In particular, there are no nontrivial self-dual λ-constacyclic codes in the case that $\lambda \neq \pm 1$, a result earlier proved by Dinh in ([9], Proposition 3.2).

Theorem 4.5 *Suppose that $\alpha = \alpha^{-1}$ and let $C = e\mathbb{F}^{\alpha}G$ be a twisted group code where $e = e^2$. Then the following are equivalent.*

a) $C = C^{\perp}$.

b) $\widehat{e}e = 0$ *and* $1 - \widehat{e} = e(\overline{1} - \widehat{e})$.

In particular, if $e = \overline{1} - \widehat{e}$, *then* $C = C^{\perp}$.

Proof: First observe that $\mathrm{Ann}_l(e\mathbb{F}^{\alpha}G) = \mathbb{F}^{\alpha}G(\overline{1} - e)$. Applying Proposition 2.11 and Theorem 2.10 we see that

$$C^{\perp} = (\overline{1} - \widehat{e})\mathbb{F}^{\alpha}G.$$

a) $\Longrightarrow$ b) $C = C^{\perp}$ implies

$$C = e\mathbb{F}^{\alpha}G = (\overline{1} - \widehat{e})\mathbb{F}^{\alpha}G.$$

Thus $(\overline{1} - \widehat{e})e = e$ and $e(\overline{1} - \widehat{e}) = \overline{1} - \widehat{e}$.
b) $\Longrightarrow$ a) The condition $\overline{1} - \widehat{e} = e(\overline{1} - \widehat{e})$ forces $(\overline{1} - \widehat{e})\mathbb{F}^{\alpha}G \leq e\mathbb{F}^{\alpha}G$. The condition $\widehat{e}e = 0$ which is equivalent to $(\overline{1} - \widehat{e})e = e$ shows that $e\mathbb{F}^{\alpha}G \leq (\overline{1} - \widehat{e})\mathbb{F}^{\alpha}G$. □

Proposition 4.6 *Let V and α be as in* Example 4.1 *and let q be the power of an odd prime. Then $\mathbb{F}_q^{\alpha}V$ contains a self-dual nontrivial twisted group code.*

Proof: First note that in a finite field of odd characteristic each element is the sum of two squares. Thus we can solve the equation

$$-\left(\frac{1}{2}\right)^2 = b^2 + c^2$$

with suitable $b, c \in \mathbb{F}_q$. Now we put

$$e = \frac{1}{2}\overline{1} + b\overline{x} + c\overline{y}.$$

One easily shows that $e = e^2$ and $e = \overline{1} - \widehat{e}$. Thus the assertion follows by Theorem 4.5. □

5 The ternary extended Golay code

In [3] the authors already mentioned that the ternary extended Golay code C is a twisted group code. In this section we give an explicit construction of C as a right ideal in $\mathbb{F}_3^\alpha \mathrm{A}_4$. Moreover we show that C is generated by an idempotent, hence a projective module for $\mathbb{F}_3^\alpha \mathrm{A}_4$. Note that according to [3] the binary extended Golay code is a group code in $\mathbb{F}_2 \mathrm{S}_4$, but not projective.

We start with the following matrices.

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \text{ and } A = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

If $Z = XY = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, then $X^A = Y, Y^A = Z$ and $Z^A = X$. Since $X^2 = Y^2 = Z^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = E$, we see that

$$\mathrm{SL}(2,3) = \langle X, Y, A \rangle.$$

Let $\widetilde{\ }$ denote the natural group epimorphism

$$\mathrm{SL}(2,3) \longrightarrow \mathrm{SL}(2,3)/\{\pm E\} \cong \mathrm{A}_4.$$

If we put $x = \widetilde{X}, y = \widetilde{Y}, z = \widetilde{Z}$ and $a = \bar{A}$, then $V = \langle x, y \rangle$ is a Klein 4-group and $\langle x, y, a \rangle \cong \mathrm{A}_4$.

Let $G = \langle x, y, a \rangle \cong \mathrm{A}_4$. Then the multiplication in the twisted group algebra $\mathbb{F}_3^\alpha G$ is given by

	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{z}$	$\overline{a}$	$\overline{xa}$	$\overline{ya}$	$\overline{za}$	$\overline{a^2}$	$\overline{xa^2}$	$\overline{ya^2}$	$\overline{za^2}$
$\overline{1}$	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{z}$	$\overline{a}$	$\overline{xa}$	$\overline{y}$	$\overline{za}$	$\overline{a^2}$	$\overline{xa^2}$	$\overline{ya^2}$	$\overline{za^2}$
$\overline{x}$	$\overline{x}$	$-\overline{1}$	$\overline{z}$	$-\overline{y}$	$\overline{xa}$	$-\overline{a}$	$\overline{za}$	$-\overline{ya}$	$\overline{xa^2}$	$-\overline{a^2}$	$\overline{za^2}$	$-\overline{ya^2}$
$\overline{y}$	$\overline{y}$	$-\overline{z}$	$-\overline{1}$	$\overline{x}$	$\overline{ya}$	$-\overline{za}$	$-\overline{a}$	$\overline{xa}$	$\overline{ya}^2$	$-\overline{za}^2$	$-\overline{a}^2$	$\overline{xa}^2$
$\overline{z}$	$\overline{z}$	$\overline{y}$	$-\overline{x}$	$-\overline{1}$	$\overline{za}$	$\overline{ya}$	$-\overline{xa}$	$-\overline{a}$	$\overline{za}^2$	$\overline{ya}^2$	$-\overline{xa}^2$	$-\overline{a}^2$
$\overline{a}$	$\overline{a}$	$\overline{za}$	$\overline{xa}$	$\overline{ya}$	$\overline{a}^2$	$\overline{za}^2$	$\overline{xa^2}$	$\overline{ya}^2$	$\overline{1}$	$\overline{z}$	$\overline{x}$	$\overline{y}$
$\overline{xa}$	$\overline{xa}$	$-\overline{ya}$	$-\overline{a}$	$\overline{za}$	$\overline{xa}^2$	$-\overline{ya}^2$	$-\overline{a}^2$	$\overline{za}^2$	$\overline{x}$	$-\overline{y}$	$-\overline{1}$	$\overline{z}$
$\overline{ya}$	$\overline{ya}$	$\overline{xa}$	$-\overline{za}$	$-\overline{a}$	$\overline{ya}^2$	$\overline{xa}^2$	$-\overline{za}^2$	$-\overline{a}^2$	$\overline{y}$	$\overline{x}$	$-\overline{z}$	$-\overline{1}$
$\overline{za}$	$\overline{za}$	$-\overline{a}$	$\overline{ya}$	$-\overline{xa}$	$\overline{za}^2$	$-\overline{a}^2$	$\overline{ya}^2$	$-\overline{xa}^2$	$\overline{z}$	$-\overline{1}$	$\overline{y}$	$-\overline{x}$
$\overline{a}^2$	$\overline{a}^2$	$\overline{ya}^2$	$\overline{za}^2$	$\overline{xa}^2$	$\overline{1}$	$\overline{y}$	$\overline{z}$	$\overline{x}$	$\overline{a}$	$\overline{ya}$	$\overline{za}$	$\overline{xa}$
$\overline{xa}^2$	$\overline{xa}^2$	$\overline{za}^2$	$-\overline{ya}^2$	$-\overline{a}^2$	$\overline{x}$	$\overline{z}$	$-\overline{y}$	$-\overline{1}$	$\overline{xa}$	$\overline{za}$	$-\overline{ya}$	$-\overline{a}$
$\overline{ya}^2$	$\overline{ya}^2$	$-\overline{a}^2$	$\overline{xa}^2$	$-\overline{za}^2$	$\overline{y}$	$-\overline{1}$	$\overline{x}$	$-\overline{z}$	$\overline{ya}$	$-\overline{a}$	$\overline{xa}$	$-\overline{za}$
$\overline{za}^2$	$\overline{za}^2$	$-\overline{xa}^2$	$-\overline{a}^2$	$\overline{ya}^2$	$\overline{z}$	$-\overline{x}$	$-\overline{1}$	$\overline{y}$	$\overline{za}$	$-\overline{xa}$	$-\overline{a}$	$\overline{ya}$

For instance $\overline{x}\,\overline{za} = -\overline{ya}$ arises from the matrix equation $X(ZA) = -YA$.

Hence, for the 2-cocycle α of G we have the following matrix $(\alpha(g,h))_{g,h\in G}$.

	1	x	y	z	a	xa	ya	za	a^2	xa^2	ya^2	za^2
1	1	1	1	1	1	1	1	1	1	1	1	1
x	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
y	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1
z	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
a	1	1	1	1	1	1	1	1	1	1	1	1
xa	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1
ya	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
za	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
xa^2	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
ya^2	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
za^2	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1

Next we put
$$e = -\overline{1} + \overline{z} - \overline{xa} + \overline{za} + \overline{xa^2} - \overline{ya^2}.$$
One easily shows that $e^2 = e$. Furthermore,
$$\widehat{e} = -\overline{1} - \overline{z} + \overline{ya^2} - \overline{xa^2} - \overline{za} + \overline{xa}.$$

Thus $1 - \widehat{e} = e$. By Theorem 4.5, we get $C = C^{\perp}$. Since $\mathbb{F} = \mathbb{F}_3$ it follows that C is 3-divisible. Suppose that there exists $0 \neq c \in C$ with $\mathrm{wt}(c) = 3$. Since C is an ideal in $\mathbb{F}_3^{\alpha}\mathrm{A}_4$ we may assume that $\overline{1}$ occurs of c. Thus we may assume that
$$c = \overline{1} + \lambda\overline{g} + \mu\overline{h} \in C = C^{\perp}$$
with $\lambda, \mu \in \mathbb{F}_3^*$ and $1, g, h$ pairwise different. Let $t \in G$ such that $h = gt$. Since C is a right ideal we get
$$c\overline{t} = \overline{t} + \lambda\alpha(g,t)\overline{h} + \mu\alpha(h,t)\overline{ht} \in C.$$
The condition $0 = \langle c, c\overline{t}\rangle$ leads to one the following two cases:

(i) $g = t$ and $\mu\alpha(g,g) + 1 = 0$.
(ii) $g = ht = gt^2$ (hence $t^2 = 1$) and $\alpha(g,t) + \alpha(h,t) = 0$.

Case (i): The second condition in (i) shows that $\mu = -\frac{1}{\alpha(g,g)} = -\alpha(g,g)$. Thus
$$c = \overline{1} + \lambda\overline{g} - \alpha(g,g)\overline{g^2},$$

hence g has order 3 since $g \in \mathrm{A}_4$. Furthermore, note that

$$e = -\overline{1} + \overline{z} - (\overline{xa} + \overline{(xa)^2}) + (\overline{za} + \overline{(za)^2}).$$

Now, $0 = \langle e, c \rangle$ forces

$$\text{(i1)} \qquad c = \overline{1} + \overline{g} - \overline{g^2} \;\; (\lambda = 1,\; \alpha(g,g) = -1) \quad \text{or}$$

$$\text{(i2)} \qquad c = \overline{1} - \overline{g} + \overline{g^2} \;\; (\lambda = -1,\; \alpha(g,g) = 1).$$

Suppose the case (i1) holds, hence

$$c = \overline{1} + \overline{g} - \overline{g^2}.$$

Now, $\overline{g} \in \operatorname{supp}(e)$ and $\alpha(g,g) = -1$ leads to $g = xa$ or $g = za$. In both cases we have $\langle c, e \rangle = -1$, a contradiction. In the case (i2) we get by the same argument $g = xa^2$ or $g = ya^2$ and $\langle c, e \rangle = -1$, again a contradiction. Thus the case (i) can not occur.

Case (ii): First note that

$$\alpha(ht, t) = \alpha(g, t) = -\alpha(h, t)$$

and $c = \overline{1} + \lambda\overline{ht} + \mu\overline{h}$. With

$$c\overline{t} = \overline{t} + \lambda(ht,t)\overline{h} + \mu\alpha(h,t)\overline{ht} = \overline{t} - \lambda(h,t)\overline{h} + \mu\alpha(h,t)\overline{ht}$$

we obtain

$$0 = \langle c, c\overline{t} \rangle = -\lambda\alpha(h,t) + \lambda\mu\alpha(h,t),$$

hence $\mu = 1$. Thus

$$c = \overline{1} + \lambda\overline{ht} + \overline{h}.$$

First suppose that $\operatorname{Ord}(h) = 3$. We look at

$$c\overline{h^{-1}} = \overline{h^{-1}} + \lambda\alpha(ht, h^{-1})\overline{hth^{-1}} + \alpha(h, h^{-1})\overline{1}.$$

Now the assumption $\operatorname{Ord}(h) = 3$ shows that $h \notin \{h^{-1}, hth^{-1}\}$ and $ht \notin \{h^{-1}, hth^{-1}\}$. Thus

$$0 = \langle c, c\overline{h^{-1}} \rangle = \alpha(h, h^{-1}) \neq 0,$$

a contradiction. Therefore h and t are involutions, hence elements in $V^{\#} = \{x, y, z\}$. We write

$$c = \overline{1} + \lambda\overline{u} + \overline{v}$$

with $u, v \in V^{\#}$. The condition $0 = \langle e, c \rangle$ leads to $u = z$ and $\lambda = 1$ or $v = z$. Thus we have $c = \overline{1} + \overline{z} + \overline{v}$ or $c = \overline{1} + \lambda\overline{u} + \overline{z}$. In both cases we get $\langle e, c\overline{a^2} \rangle \neq 0$ since $\overline{a^2}$ and $\overline{za^2}$ are not in the support of e, but $\overline{xa^2}$ and $\overline{ya^2}$ are. This shows that C has minimum distance 6. Hence C is a ternary self-dual $[12, 6, 6]$ twisted group code which must be the ternary extended Golay code due to a well-known result of MacWilliams. Note that C is a projective $\mathbb{F}_3^{\alpha}\mathrm{A}_4$ module since it is generated by an idempotent. Thus we have shown the following.

Proposition 5.1 *The ternary extended Golay code C is a twisted group code for the alternating group* A_4. *Moreover, C is a projective* $\mathbb{F}_3^\alpha \mathrm{A}_4 -$ *module.*

Remark 5.2 Above we explicitly constructed the ternary extended Golay code C as a right ideal in the twisted group algebra $\mathbb{F}_3^\alpha \mathrm{A}_4$ which is a projective $\mathbb{F}_3^\alpha \mathrm{A}_4$-module. It is well-known that $\mathrm{Aut}(C) = \hat{M}_{12}$, the covering group of the Mathieu group M_{12}. By ([12], Section 14) the dihedral group D_{12} is a regular subgroup of M_{12}. Let $\hat{D}_{12}$ be the preimage of D_{12} in $\hat{M}_{12}$, hence $\hat{D}_{12} \leq \mathrm{Aut}(C)$. Since M_{12} acts doubly transitive on 12 letters, the only diagonal matrices in $\mathrm{Aut}(C)$ are scalar matrices (see for instance ([17], Proposition 1.2.26)) Thus we may apply Theorem 3.2 to see that the ternary extended Golay code C is also a right ideal in the twisted group $\mathbb{F}_3^\alpha D_{12}$ for some 2-cocycle α. In the case that $\alpha(g,h) = -1$ if g and h are involutions in D_{12} and otherwise $\alpha(g,h) = 1$ one can check with Magma that the ternary extended Golay code in $\mathbb{F}_3^\alpha D_{12}$ is not a projective module for $\mathbb{F}_3^\alpha D_{12}$.

6 The Hamming codes

Let $C = \mathcal{H}_{k,q}$ denote the $[n, n-k, 3]$ Hamming code over $\mathbb{F}_q$ where $n = \frac{q^k-1}{q-1}$. It is well-known that $\mathrm{Aut}(C) \cong \mathrm{Aut}(C^\perp) \cong \mathrm{GL}(k,q)$ and the only diagonal matrices in $\mathrm{Aut}(C)$ are the nonzero scalar matrices ([17], Satz 4.1.3). If H is a control matrix for C, then the isomorphism $\mathrm{Aut}(C^\perp) \longrightarrow \mathrm{GL}(k,q)$ can be defined by $M \mapsto X$ where $XH = HM$. We may identify the columns of H by the projective space $\mathbb{P}^{k-1}(q)$, i.e., the set of 1-dimensional subspaces of $\mathbb{F}_q^k$ and $\mathrm{Aut}(C^\perp)$ with $\mathrm{GL}(k,q)$.

Theorem 6.1 *For all k and q the Hamming code $C = \mathcal{H}_{k,q}$ is a twisted cyclic group code.*

Proof: Let $V = V(k,q) = \mathbb{F}_{q^k}$ and let γ be a generator of the multiplicative group $\mathbb{F}_{q^k}^*$. We consider the Singer cycle

$$\mathbb{F}_{q^k} \ni x \mapsto \gamma x \in \mathbb{F}_{q^k}.$$

Note that $\langle\gamma\rangle$ acts on the projective space $\mathbb{P}^{k-1}(q)$ via $\langle x\rangle \mapsto \langle\gamma x\rangle$. If $\langle\gamma^i x\rangle = \langle x\rangle$ for some $0 \neq x \in \mathbb{F}_{q^k}$ and some $i \in \mathbb{N}$, then $\gamma^i x = \lambda x$ for some $0 \neq \lambda \in \mathbb{F}_q$ which implies $\gamma^i = \lambda \in \mathbb{F}_q^*$. This happens if and only if $n \mid i$. Thus, if $S \in \mathrm{GL}(k,q)$ is the companion matrix of γ, then $S^i = \lambda E$ with $\lambda \in \mathbb{F}_q^*$ if and only if $n \mid i$. Thus $\mathrm{PGL}(n,q)$ has a cyclic subgroup $\langle\overline{S}\rangle$ of oder n which acts regularly on $\mathbb{P}^{k-1}(q)$. Since $\langle S\rangle \leq \mathrm{Aut}(C^\perp)$ and $\pi(\langle S\rangle) = \langle\overline{S}\rangle$ we get $C^\perp \leq \mathbb{F}_q^\alpha\langle\overline{S}\rangle$ for some 2-cocycle α, by Theorem 3.2. Thus $C \leq \mathbb{F}_q^{\alpha^{-1}}\langle\overline{S}\rangle$. □

Corollary 6.2 *Linear perfect codes are always twisted cyclic group codes, sometimes even cyclic group codes.*

Proof: Here we use the classification of linear perfect codes. Clearly the binary repetition codes of odd length is a cyclic group code. The automorphism group of the binary $[23, 12, 7]$ is the simple Mathieu group M_{23} consisting of permutation matrices. Since M_{12}

contains a cyclic group of order 23, the binary Golay code is a cyclic group code according to ([2], Theorem 1.2). The automorphism group of the ternary $[11, 6, 5]$ Golay code is the simple Mathieu group M_{11} which has a cyclic subgroup of order 11 consisting of permutations ([15], Ch. 20, Corollary 19). Thus again by ([2], Theorem 1.2), the ternary Golay code is a cyclic group code. For Hamming codes the assertion follows by Theorem 6.1. $\square$

Example 6.3 Let $C = \mathcal{H}_{2,q}$ be the $[n, n-2, 3]$ Hamming code over $\mathbb{F} = \mathbb{F}_q$ where $n = \frac{q^2-1}{q-1} = q + 1$.

a) In the case that $2 \mid q$ we have $\mathrm{SL}(2, q) = \mathrm{PSL}(2, q) \leq \mathrm{GL}(2, q)$ and there is a cyclic subgroup of order $q + 1$ in $\mathrm{PSL}(2, q)$ which acts transitively on the projective line $\mathbb{P}^1(q)$, by ([10], Kap.II, Satz 8.4). Thus C is a cyclic group code according to ([2], Theorem 1.2).

b) Now suppose that q is odd. According to ([12], Table 16.1) the group $\mathrm{PSL}(2, q)$ contains a metacyclic subgroup of order $q + 1$ acting regular on $\mathbb{P}^1(q)$. This group is a dihedral group by ([10], Kap. II, Satz 8.4). Taking its preimage in $\mathrm{SL}(2, q)$ we see that C is a twisted dihedral group code due to Theorem 3.2.

References

[1] S.D. Berman, On the theory of group codes. *Kibernetika* 3 (1967), 31-39.

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

[3] F. Bernhardt, P. Landrock and O. Manz, The extended Golay codes considered as ideals. *J. Comb. Theory, Series A* 55 (1990), 235-246.

[4] M. Borello and W.Willems, Group codes are asymptotically good, to appear Finite Fields and Appl.

[5] M. Borello, J. de la Cruz and W. Willems, A note on linear complementary pairs of codes, *Discrete Math. 343 (2020), 1-3.*

[6] P. Charpin, Une généralisation de la construction de Berman des codes de Reed-Muller p-aire, *Comm. Algebra* 16 (1988), 2231-2246.

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

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

[9] H.Q. Dinh, Repeated-root cyclic and negacyclic codes of length $6p^s$, *Contemporary Math.* 609 (2014) 69-87.

[10] B. Huppert, Endliche Gruppen, Springer, Berlin 1967.

[11] B. Huppert and N. Blackburn, Finite Groups II, Springer, Berlin 1982.

[12] M.W. Liebeck, C.E. Praeger and J. Saxl, Regular subgroups of primitive permutation groups, Memoirs of AMS 952, 2009

[13] M. Linckelmann, The block theory of finite groups, London Math. Soc., Textbook 92, Cambridge Uni. Press.

[14] F.J. MacWilliams, Codes and ideals in group algebras, *Combinatorial Mathematics and Appl., Proceedings, ed. by R.C. Bose and T.A. Dowing* 317-328 (1967).

[15] F.J. MacWilliams and N.J.A. Sloane, The theory of error correcting codes, North Holland, Amsterdam, Sixth Printing 1988.

[16] W. Willems, A note on self-dual group codes. *IEEE Trans. Inform. Theory* 48 (2007), 3107-3109.

[17] W. Willems, Codierungstheorie, deGruyter, Berlin 1999.