



HAL
open science

ON THE ALGEBRAIC STRUCTURE OF QUASI GROUP CODES

Martino Borello, Wolfgang Willems

► **To cite this version:**

Martino Borello, Wolfgang Willems. ON THE ALGEBRAIC STRUCTURE OF QUASI GROUP CODES. Journal of Algebra and Its Applications, 2022, 10.1142/S0219498823502225 . hal-03852311

HAL Id: hal-03852311

<https://hal.science/hal-03852311>

Submitted on 14 Nov 2022

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.

ON THE ALGEBRAIC STRUCTURE OF QUASI GROUP CODES

MARTINO BORELLO AND WOLFGANG WILLEMS

ABSTRACT. In this note, an intrinsic description of some families of linear codes with symmetries is given, showing that they can be described more generally as quasi group codes, that is, as linear codes allowing a group of permutation automorphisms which acts freely on the set of coordinates. An algebraic description, including the concatenated structure, of such codes is presented. This allows to construct quasi group codes from codes over rings, and vice versa. The last part of the paper is dedicated to the investigation of self-duality of quasi group codes.

1. INTRODUCTION

In the theory of error correcting codes linear codes play a central role due to their algebraic structure which allows, for example, an easy description and storage. Quite early in coding theory it appeared convenient to add additional algebraic structure in order to get more information about the parameters and to speed up the decoding process. In 1957, E. Prange introduced the now well-known class of cyclic codes [27], which are the forefathers of many other families of codes with symmetries discovered thereafter. In particular, abelian codes [4], group codes [24], quasi-cyclic codes [12], quasi-abelian codes [28], and twisted group codes [13] are distinguished descendants of cyclic codes. All of them have nice algebraic structures, and many remarkable and optimal codes belong to these families. Moreover it is proved that the family of group codes is asymptotically good [3, 9, 11], as the family of quasi-cyclic and quasi-abelian codes [8, 21, 22].

The aim of the current note is to give an intrinsic description of these classes in terms of their permutation automorphism groups and to deduce some structural properties from that. We show that all of them admit a subgroup of the full group of permutation automorphisms which acts freely on the set of coordinates. A linear code with this property will be called a quasi group code. So all families cited above can be described in this way. Note that quasi group codes (over Frobenius rings) have also been introduced in a recent paper by S. Dougherty et al. [14]. It turns out that the families of quasi group codes, quasi-abelian codes and quasi-cyclic codes coincide. Furthermore, we give the most general algebraic description of quasi group codes (Theorem 4.1) and describe their concatenated structure (Theorem 4.2) without any restriction on the group which acts on. In addition, no assumption on semi-simplicity (unlike in previous papers on the subject) is needed. In contrast with the concatenated structure of quasi-abelian codes, quasi group codes for a non-abelian group can be decomposed as concatenations of codes over non-necessary commutative (Frobenius) rings, such as matrix rings. There is an active research on codes over (Frobenius) rings over the last decades (see for example [1, 2, 15]). In particular, codes over matrix rings may be used in applications to Space-Time Coded Modulations [25]. From the investigation of good quasi group codes we get, as a byproduct, constructions of good codes over (Frobenius) rings, and vice versa.

In the last part of the paper, we deal with self-duality of quasi group codes. We prove a necessary and sufficient condition for the existence of self-dual quasi group codes depending on the underlying field and on the index.

M. Borello is with Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France.

W. Willems is with Otto-von-Guericke Universität, Magdeburg, Germany and Universidad del Norte, Barranquilla, Colombia.

2. BACKGROUND

In this section we collect some preliminaries which are crucial in the subsequent sections.

Let K be a finite field of cardinality q . A *linear code* \mathcal{C} of length n is a K -linear subspace of K^n . An element $c = (c_1, \dots, c_n) \in \mathcal{C}$ is called a *codeword* and its (Hamming) *weight* is given by

$$\text{wt}(c) := |\{i \in \{1, \dots, n\} \mid c_i \neq 0\}|.$$

The *minimum distance* of \mathcal{C} is defined by $d(\mathcal{C}) := \min_{c \in \mathcal{C} \setminus \{0\}} \text{wt}(c)$. An $[n, k, d]_q$ code is a linear code of length n , dimension k and minimum distance d over a field of cardinality q . These, i.e., n, k, d and q are usually called *the parameters* of the code.

There is a standard way of combining codes to obtain a code of larger length. To describe this process, let $K \subseteq L$ be a field extension, m an integer greater than or equal to $[L : K]$ and let $\pi : L \rightarrow K^m$ be a K -linear injection. In the concatenation process, L -linear codes in L^n are called *outer codes* and the K -linear code $\mathcal{I} := \pi(L)$ is called an *inner code*. If $\mathcal{C} \subseteq L^n$ is an L -linear code, then the K -linear code

$$\mathcal{I} \square_{\pi} \mathcal{C} := \{(\pi(c_1), \dots, \pi(c_n)) \mid (c_1, \dots, c_n) \in \mathcal{C}\} \subseteq K^{n \cdot m}$$

is called the *concatenation of \mathcal{C} with \mathcal{I} by π* , or simply the *concatenated code*.

This construction obviously depends on the choice of π , but there are some properties independent of π . For example, the length of $\mathcal{I} \square_{\pi} \mathcal{C}$ is $n \cdot m$, the K -dimension of $\mathcal{I} \square_{\pi} \mathcal{C}$ is the product $\dim_K(\mathcal{I}) \cdot \dim_L(\mathcal{C})$, and we have the bound $d(\mathcal{I} \square_{\pi} \mathcal{C}) \geq d(\mathcal{I}) \cdot d(\mathcal{C})$ (see for example [18]).

There are some natural group actions associated to linear codes. The symmetric group S_n acts on the set $\{1, \dots, n\}$ of coordinates by definition. This action induces an *action on the elements* of K^n , namely for $v \in K^n$ and $\sigma \in S_n$ we have

$$v^{\sigma} := (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \dots, v_{\sigma^{-1}(n)}),$$

which induces an *action on subsets* of K^n (and in particular on linear codes). For $\mathcal{C} \subseteq K^n$ we put

$$\mathcal{C}^{\sigma} := \{c^{\sigma} \mid c \in \mathcal{C}\}.$$

An element $\sigma \in S_n$ is an *automorphism* of \mathcal{C} if $\mathcal{C}^{\sigma} = \mathcal{C}$. The stabilizer

$$\text{PAut}(\mathcal{C}) := \{\sigma \in S_n \mid \mathcal{C}^{\sigma} = \mathcal{C}\}$$

is called the *permutation automorphism group* of \mathcal{C} . Moreover, a linear code \mathcal{C}_1 is *equivalent* or better *permutation equivalent* to a linear code \mathcal{C}_2 if there exists $\sigma \in S_n$ such that $\mathcal{C}_1^{\sigma} = \mathcal{C}_2$. This is not the most general definition of equivalence but it is sufficient for our purpose. Finally, it is easy to see that $\text{PAut}(\mathcal{C}^{\sigma}) = \text{PAut}(\mathcal{C})^{\sigma}$ (*the conjugate of $\text{PAut}(\mathcal{C})$ in S_n by σ*).

From group theory we recall that a (right) action of a group G on a set X is called

- *transitive* if $X \neq \emptyset$ and for all $x, y \in X$ there exists $g \in G$ such that $x^g = y$;
- *free* if $x^g = x$ for some $x \in X$ and $g \in G$, then g is the unit in G ;
- *regular* if it is both transitive and free.

In the case that the group G is finite and acts freely, it immediately follows that all orbits have cardinality $|G|$. In particular, $|G|$ divides $|X|$ and $\ell = \frac{|X|}{|G|}$ is called the *index* of the action. Moreover, if G is regular, then $|G| = |X|$.

A subgroup H of the symmetric group S_n is called *transitive* (resp. *regular*) if of the action of H on the set of coordinates $\{1, \dots, n\}$ is transitive (resp. regular).

Finally, given a group G and a field K , the *group algebra* KG is the set of formal sums

$$KG := \left\{ a = \sum_{g \in G} a_g g \mid a_g \in K \right\},$$

which is a K -vector space in a natural way and which becomes a K -algebra via the multiplication

$$ab := \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g} \right) g,$$

$$\text{for } a = \sum_{g \in G} a_g g \text{ and } b = \sum_{g \in G} b_g g.$$

3. CODES WITH A FREE ACTING GROUP OF SYMMETRIES

Let G be a finite group of cardinality n and let K be a finite field. Recall that the group algebra KG is isomorphic to K^n as a K -vector space, where $n = |G|$. There is a standard way of constructing such an isomorphism, which allows us to transfer many coding theoretical properties from K^n to KG . Once an ordering g_1, \dots, g_n of the elements of G is chosen, we may define $\varphi : g_i \mapsto e_i$, where $\{e_1, \dots, e_n\}$ is the standard basis of K^n . Then we extend this map K -linearly so that

$$(1) \quad \varphi : \sum_{i=1}^n a_i g_i \mapsto (a_1, \dots, a_n).$$

The isomorphism φ obtained in this way is not canonical, since it depends on the ordering of the group. But different orderings lead only to a permutation of the coordinates, hence to permutation equivalent codes.

Via the isomorphism φ , we may transfer the Hamming metric from K^n to KG . For $a \in KG$, we define $\text{wt}(a) := \text{wt}(\varphi(a))$. So, from a coding theoretical point of view, we can consider linear codes either in KG or in K^n without any difference. However, the algebraic structure of KG allows us to consider codes with more structure than linearity.

Definition 3.1 ([4, 24]). A G -code is a right ideal \mathcal{C} in the group algebra KG . If the group G is cyclic (resp. abelian), then the code \mathcal{C} is called a *cyclic* (resp. *abelian*) G -code. In the case we do not specialize the group G explicitly we briefly speak of a group code.

The restriction to right ideals is only for convention, which means that everything in the following may be stated equally for left ideals.

The particular class of cyclic G -codes is nothing else than the family of well known cyclic codes. If G is cyclic, hence generated by a certain $g \in G$, and the isomorphism φ sends $g^i \rightarrow e_{i+1}$ for all $i \in \{0, \dots, n-1\}$, then $\varphi(\mathcal{C})$ is *cyclic*. In fact, in this case $KG \cong K[x]/(x^n - 1)$ via the map $g \mapsto x + (x^n - 1)$. Thus, a cyclic code turns out to be an ideal in the factor algebra $K[x]/(x^n - 1)$, which is the classical definition.

Now let \mathcal{C} be a G -code with $n = |G|$. Observe that the right multiplication on G by one of its elements, say g , induces a permutation $\sigma_g \in S_n$ defined by

$$(2) \quad \sigma_g(i) = j \quad \text{iff} \quad g_i g = g_j.$$

Note that $g \mapsto \sigma_g$ is a faithful permutation representation of G , which depends on the chosen ordering of G . If this map coincides with that chosen for φ , then $\sigma(G) := \{\sigma_g \mid g \in G\}$ is a subgroup of $\text{PAut}(\varphi(\mathcal{C}))$. This is due to the fact that a right ideal is stable by multiplication on the right. Since the action of right multiplication is regular, $\sigma(G)$ is a regular subgroup of S_n .

Suppose that \mathcal{C} is a linear code in K^n admitting a regular subgroup G of $\text{PAut}(\mathcal{C})$. Since G is a group of automorphisms, \mathcal{C} becomes a right KG -module via the action

$$(3) \quad c \cdot \left(\sum_{g \in G} a_g g \right) := \sum_{g \in G} a_g c^g$$

for $c \in \mathcal{C}$ and $a_g \in K$, where $c^g \in \mathcal{C}$ is the image of c under the action of g . Moreover, as every regular action of G is isomorphic to the action of G on itself given by right multiplication, there is an ordering of G such that $\varphi^{-1}(\mathcal{C})$ is a G -code in KG . Thus we have proved, in our framework, the known characterization of group codes.

Theorem 3.2 ([5]). *Let G be a group of order n and let \mathcal{C} be a linear code in K^n . Then \mathcal{C} is a G -code if and only if G is isomorphic to a regular subgroup H of $\text{PAut}(\mathcal{C})$.*

We would like to mention here that a G -code may also be an H -code where H is not isomorphic to G . For instance, the binary extended [24,12,8] Golay code is a G -code for the symmetric group S_4 [6] and the dihedral group D_{24} [23]. Furthermore, there are abelian G -codes which are not group codes for cyclic groups. As an example may serve the binary extended [8,4,4] Hamming code. It is a $G = C_2 \times C_4$ code, but not equivalent to a cyclic code (in fact, its automorphism group is isomorphic to $\text{AGL}_3(2)$ that does not contain an element of order 8).

Definition 3.3. Let G be a finite group. A K -linear code \mathcal{C} is called a *quasi- G code of index ℓ* if \mathcal{C} is a right KG -submodule of $KG^\ell = KG \oplus \dots \oplus KG$ (ℓ -times) for some $\ell \in \mathbb{N}$. A quasi group code is a quasi- G code for some group G . In the case that G is cyclic (resp. abelian) we call \mathcal{C} a *cyclic* (resp. *abelian*) *quasi group code*.

Clearly, in the case $\ell = 1$, a quasi G -code is a G -code, just by definition. The trivial quasi- G codes over K (i.e., $G = 1$) are nothing else than the linear codes over K .

Remark 3.4. If \mathcal{C} is a G -code, then \mathcal{C} is a quasi- H code of index $\ell = \frac{|G|}{|H|}$ for any subgroup H of G . This follows immediately from the fact that $KG = \bigoplus_{t \in T} tKH$ if T is a left transversal of H in G .

Theorem 3.5. *Let G be a group of order $|G| = \frac{n}{\ell}$ and let \mathcal{C} be a linear code in K^n . Then \mathcal{C} is a quasi- G code of index ℓ if and only if G is isomorphic to a subgroup H of $\text{PAut}(\mathcal{C})$ which acts freely of index ℓ on the coordinates.*

Proof. Suppose that \mathcal{C} is a right KG -submodule of $A = KG^\ell$. Note that G acts regularly on the index set $\{g \in G\}$ of each component KG . Hence G acts freely of index ℓ on the set of all coordinates of A . Furthermore, the matrix group $P(G) = \{P(g) \mid g \in G\}$ induced by the right action of G on A leaves \mathcal{C} invariant since \mathcal{C} is a right KG -submodule of A . Hence $G \cong P(G)$ is a subgroup of $\text{PAut}(\mathcal{C})$ which acts freely of index ℓ on the coordinates.

Now suppose that G is isomorphic to a subgroup H of $\text{PAut}(\mathcal{C})$ which acts freely of index ℓ on the coordinates. Let $P : G \rightarrow H$ be an isomorphism from G to H . We define an action of G on $\{1, \dots, n\}$ by $ig = j$ if and only if $e_i P(G) = e_j$ where the e_i is the standard basis of K^n . Since $P(G) = H$ acts freely of index ℓ on the coordinates, G has exactly ℓ orbits \mathcal{O}_j of length $|G|$ on $\{1, \dots, n\}$. Next we fix representatives i_1, \dots, i_ℓ of $\mathcal{O}_1, \dots, \mathcal{O}_\ell$ and identify $e_r \in \mathcal{O}_j$ with $g \in G$ if $i_j g = r$. Thus

$$\bigoplus_{r \in \mathcal{O}_j} K e_r = KG$$

as a right KG -module and

$$K^n = \bigoplus_{j=1}^{\ell} (\bigoplus_{r \in \mathcal{O}_j} K e_r) = \bigoplus_{j=1}^{\ell} KG = KG^\ell.$$

Since H is a subgroup of $\text{PAut}(\mathcal{C})$ the code \mathcal{C} is a right KG -submodule of KG^ℓ . \square

Note that a cyclic quasi group code of index ℓ is nothing else than a quasi-cyclic code in the classical sense of index ℓ . Thus, by Remark 3.4, a nontrivial quasi group code is a quasi-cyclic code.

Corollary 3.6. *The class of nontrivial group codes of length $n > 1$ coincides with the class of quasi-cyclic codes of length $n > 1$.*

Example 3.7. The extended binary Golay code of length 24 can be seen in many different ways. For example, it is a quasi group code for D_6 of index 4 (see Example 4.4), but also a quasi group code for A_4 of index 2, and even a group code for S_4 , D_{24} , $C_3 \times D_8$, $C_2 \times A_4$ and $(C_6 \times C_2) \rtimes C_2$ [6, 14].

Remark 3.8. A natural question is the following. What can we say about the code if a group does not act freely? In this case, the situation gets more complicated to be treated in a general framework, since there are many possible configurations of the fixed points of the automorphisms which give rise to different module structures. Some results in this direction can be found in [10] for very small groups and in the case of self-dual codes.

4. THE CONCATENATED STRUCTURE OF QUASI GROUP CODES

It is well-known (see [19, Chapter VII, §12]) that every group algebra KG can be uniquely decomposed (up to a permutation of the components) into a direct sum of indecomposable two-sided ideals as

$$(4) \quad KG = \underbrace{f_0 KG}_{\mathcal{B}_0} \oplus \cdots \oplus \underbrace{f_s KG}_{\mathcal{B}_s},$$

where the \mathcal{B}_i 's are called *blocks* and the f_i 's are primitive orthogonal idempotents in the center of KG with $1 = f_0 + \cdots + f_s$. Note that each \mathcal{B}_i is a Frobenius ring. The image $\varphi(\mathcal{B}_i)$ of \mathcal{B}_i under the map φ defined as in (1) is a linear code of length $|G|$ over K , which is uniquely determined by G (up to equivalence, from the choice of φ).

Moreover, for every KG -module \mathcal{C} , we have a “blockwise” direct decomposition

$$(5) \quad \mathcal{C} = \underbrace{\mathcal{C}f_0}_{\mathcal{C}_0} \oplus \cdots \oplus \underbrace{\mathcal{C}f_s}_{\mathcal{C}_s},$$

of \mathcal{C} into KG -modules $\mathcal{C}_i = \mathcal{C}f_i$. Observe that \mathcal{C}_i is indeed a KG -module since f_i lies in the center of KG . Clearly, \mathcal{C}_i is a \mathcal{B}_i -module too.

Now let G be a subgroup of S_n which acts freely on $\{1, \dots, n\}$. Let $m = |G|$ and $n = m\ell$. Then

$$\varphi^\ell : KG^\ell \rightarrow K^n,$$

where φ is defined as in (1), is an isomorphism of vector spaces. This map can be restricted to \mathcal{B}_i^ℓ for every i , getting a \mathcal{B}_i -module isomorphism between \mathcal{B}_i^ℓ and the \mathcal{B}_i -modules in K^n .

Theorem 4.1. *Every quasi- G code \mathcal{C} can be blockwise decomposed as*

$$\mathcal{C} = \mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_s,$$

where each \mathcal{C}_i is a linear code (eventually trivial) of length ℓ over the ring \mathcal{B}_i , i.e. a \mathcal{B}_i -submodule of \mathcal{B}_i^ℓ .

Proof. By definition, \mathcal{C} is a right KG -submodule of $KG^\ell = KG \oplus \cdots \oplus KG$. According to (5) there is a decomposition

$$\mathcal{C} = \mathcal{C}f_0 \oplus \cdots \oplus \mathcal{C}f_s = \mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_s$$

where

$$\mathcal{C}_i = \mathcal{C}f_i \leq (KG \oplus \cdots \oplus KG)f_i \leq KGf_i \oplus \cdots \oplus KGf_i = \mathcal{B}_i^\ell.$$

Thus \mathcal{C}_i is a code over \mathcal{B}_i of length ℓ . Clearly this code is linear over \mathcal{B}_i (from the right) since \mathcal{C}_i is a right KG -module. \square

For each $i \in \{1, \dots, \ell\}$ we fix a K -linear injection

$$\pi_i : \mathcal{B}_i \longrightarrow K^m.$$

Similar to the concatenation in Section 2

$$\mathcal{B}_i \square_{\pi_i} \mathcal{C}_i := \{(\pi_i(c_1), \dots, \pi_i(c_\ell)) \mid (c_1, \dots, c_\ell) \in \mathcal{C}_i\} \subseteq K^{m\ell} = K^n.$$

This is a linear code over K which we also call a *concatenated code*.

With the previous notations we have the following.

Theorem 4.2. a) *Every quasi- G code \mathcal{C} can be decomposed*

$$\mathcal{C} = (\mathcal{B}_0 \square_{\pi_0} \mathcal{C}_0) \oplus \dots \oplus (\mathcal{B}_s \square_{\pi_s} \mathcal{C}_s),$$

where each \mathcal{C}_i is a linear code (eventually trivial) of length ℓ over a the block algebra \mathcal{B}_i .

b) *If $d(\mathcal{B}_0) \leq \dots \leq d(\mathcal{B}_s)$, then the minimum distance of \mathcal{C} is bounded below by*

$$d(\mathcal{C}) \geq \min_{0 \leq i \leq s} \{d(\mathcal{C}_i) \cdot d(\mathcal{B}_0 \oplus \dots \oplus \mathcal{B}_i)\},$$

where the minimum distance of \mathcal{C}_i is defined exactly as for linear codes over fields.

Proof. a) This follows directly by Theorem 4.1.

b) The proof is exactly as in [7] for linear codes over fields. □

Remark 4.3. In general the determination of the blocks \mathcal{B}_i of KG is a hard problem and the algebraic structure may be quite complicated. If G is abelian and the characteristic of K does not divide $|G|$, then each block is explicitly known and isomorphic to a finite extension field of K , by Wedderburn's Theorem. In [8] the authors exploit the concatenated structure of abelian quasi group codes to find good codes. For instance, they construct a binary quasi group code for $G = C_3 \times C_3$ of index 4 with parameters [36, 6, 16], which are optimal according to Grassl's list [16].

If $\text{char}K$ does not divide $|G|$, then, by Maschke's Theorem, the algebra KG is semisimple. By Wedderburn's Theorem, we get that the blocks in (4) are isomorphic to full matrix rings over skew fields which are field extensions of K if $|K|$ is finite. The same happens, also in the non-semisimple case, for blocks of defect 0 [17, Chapter 16, Remark 16.3.6.]. In order to exploit the concatenation we need an explicit isomorphism from the abstract matrix ring to \mathcal{B}_i . Clearly, the identity matrix is mapped to the idempotent f_i . Then one should look at the action of G on the idempotent f_i , to get a representation of G in the matrix ring. Note that the isomorphism is completely determined by the images of the generators of G . For blocks of positive defect, the isomorphism can be more complicated, but still the investigation of the structure of the Jacobson radical may help. The next examples serve as an illustration of different types of blocks and isomorphisms. We also emphasize how the concatenated construction allows to find optimal codes.

Example 4.4. We consider $G = \langle \alpha, \beta \mid \alpha^3 = \beta^2 = 1, \beta\alpha\beta = \alpha^2 \rangle \cong D_6$, the dihedral group of order 6, and $K = \mathbb{F}_2$. Then

$$f_0 = 1 + \alpha + \alpha^2 \text{ and } f_1 = \alpha + \alpha^2$$

are the central primitive orthogonal idempotents of KG . Let us fix the ordering $\{1, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$. The the corresponding blocks \mathcal{B}_0 and \mathcal{B}_1 are the codes with generator matrices

$$B_0 := \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \text{ and } B_1 := \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

The ring \mathcal{B}_0 is isomorphic to $\mathbb{F}_2 + u\mathbb{F}_2$, with $u^2 = 0$, so that we get the map $\pi_0 : \mathcal{B}_0 \rightarrow \mathbb{F}_2^6$,

$$1 \mapsto B_{0,1}, 1 + u \mapsto B_{0,2},$$

where $B_{0,j}$ is the j -th line of B_0 . Codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are studied for example in [1, 15]. The ring \mathcal{B}_1 is isomorphic to $M_2(\mathbb{F}_2)$, so that we get the map $\pi_1 : \mathcal{B}_1 \rightarrow \mathbb{F}_2^6$,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto B_{1,1}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \mapsto B_{1,2}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto B_{1,3}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \mapsto B_{1,4},$$

where $B_{1,j}$ is the j -th line of B_1 . Codes over $M_2(\mathbb{F}_2)$ are studied for example in [2, 25].

A G -code $\mathcal{C} \subseteq \mathbb{F}_2^{6\ell}$ can be then decomposed as $(\mathcal{B}_0 \square_{\pi_0} \mathcal{C}_0) \oplus (\mathcal{B}_1 \square_{\pi_1} \mathcal{C}_1)$, where $\mathcal{C}_0 \subseteq (\mathbb{F}_2 + u\mathbb{F}_2)^\ell$ and $\mathcal{C}_1 \subseteq M_2(\mathbb{F}_2)^\ell$.

Let us consider $\ell = 4$. If \mathcal{C}_0 is the code over $\mathbb{F}_2 + u\mathbb{F}_2$ generated by

$$\begin{bmatrix} 1 & 0 & 1+u & u \\ 0 & 1 & u & 1+u \end{bmatrix}$$

and \mathcal{C}_1 is the code over $M_2(\mathbb{F}_2)$ generated by

$$\left[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right],$$

then the code $\mathcal{C} = (\mathcal{B}_0 \square_{\pi_0} \mathcal{C}_0) \oplus (\mathcal{B}_1 \square_{\pi_1} \mathcal{C}_1)$ is a $[24, 12, 8]$ code, with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Note that \mathcal{C} is a code with the best possible minimum distance for the length 24 and dimension 12, by the Griesmer bound (see [16]). Moreover, it is self-dual, hence equivalent to the extended binary Golay code.

Example 4.5. Let us consider $G = \langle \alpha, \beta, \gamma \mid \alpha^3 = \beta^2 = \gamma^3 = 1, \beta\alpha\beta = \alpha^2, [\alpha, \gamma] = [\beta, \gamma] = 1 \rangle \cong S_3 \times C_3$ and $K = \mathbb{F}_2$. Let $A = \langle \alpha \rangle = \{1, \alpha, \alpha^2\}$ and $A^* = \{\alpha, \alpha^2\}$. Then

$$f_0 = \sum_{g \in A \cup A\gamma \cup A\gamma^2} g, \quad f_1 = \sum_{g \in A\gamma \cup A\gamma^2} g, \quad f_2 = \sum_{g \in A^* \cup A^*\gamma \cup A^*\gamma^2} g \quad \text{and} \quad f_3 = \sum_{g \in A^*\gamma \cup A^*\gamma^2} g$$

are the central primitive orthogonal idempotents of KG . Let us fix the ordering

$$\{1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma, \gamma^2, \alpha\gamma^2, \alpha^2\gamma^2, \beta, \alpha\beta, \alpha^2\beta, \beta\gamma, \alpha\beta\gamma, \alpha^2\beta\gamma, \beta\gamma^2, \alpha\beta\gamma^2, \alpha^2\beta\gamma^2\}.$$

The corresponding blocks \mathcal{B}_0 , \mathcal{B}_1 , \mathcal{B}_2 and \mathcal{B}_3 are the codes with generator matrices

$$B_0 := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad B_1 := \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 \end{bmatrix},$$

$$B_2 := \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad B_3 := \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The ring \mathcal{B}_0 is isomorphic to $\mathbb{F}_2 + u\mathbb{F}_2$, with $u^2 = 0$, so that we get the map $\pi_0 : \mathcal{B}_0 \rightarrow \mathbb{F}_2^{18}$,

$$1 \mapsto B_{0,1}, 1 + u \mapsto B_{0,2}.$$

The ring \mathcal{B}_1 is isomorphic to $\mathbb{F}_4 + u\mathbb{F}_4$, with $u^2 = 0$ and $\mathbb{F}_4 = \mathbb{F}_2[\zeta]$, so that we get the map $\pi_1 : \mathcal{B}_1 \rightarrow \mathbb{F}_2^{18}$,

$$\zeta \mapsto B_{1,1}, 1 \mapsto B_{1,2}, \zeta + u \mapsto B_{1,3}, 1 + u(1 + \zeta) \mapsto B_{1,4}.$$

The ring \mathcal{B}_2 is isomorphic to $M_2(\mathbb{F}_2)$, so that we get the map $\pi_2 : \mathcal{B}_2 \rightarrow \mathbb{F}_2^{18}$,

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \mapsto B_{2,1}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto B_{2,2}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \mapsto B_{2,3}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto B_{2,4}.$$

The ring \mathcal{B}_3 is isomorphic to $M_2(\mathbb{F}_4)$, with $\mathbb{F}_4 = \mathbb{F}_2[\zeta]$, so that we get the map $\pi_3 : \mathcal{B}_3 \rightarrow \mathbb{F}_2^{18}$,

$$\begin{bmatrix} \zeta^2 & 0 \\ \zeta & 1 \end{bmatrix} \mapsto B_{3,1}, \begin{bmatrix} \zeta & 0 \\ 0 & \zeta \end{bmatrix} \mapsto B_{3,2}, \begin{bmatrix} \zeta & 0 \\ 1 & \zeta^2 \end{bmatrix} \mapsto B_{3,3}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto B_{4,4}$$

$$\begin{bmatrix} 1 & 1 \\ \zeta & 1 \end{bmatrix} \mapsto B_{3,5}, \begin{bmatrix} \zeta^2 & \zeta^2 \\ \zeta & \zeta^2 \end{bmatrix} \mapsto B_{3,6}, \begin{bmatrix} \zeta^2 & \zeta^2 \\ 1 & \zeta^2 \end{bmatrix} \mapsto B_{3,7}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \mapsto B_{4,8}.$$

A G -code $\mathcal{C} \subseteq \mathbb{F}_2^{18\ell}$ can then be decomposed as $(\mathcal{B}_0 \square_{\pi_0} \mathcal{C}_0) \oplus (\mathcal{B}_1 \square_{\pi_1} \mathcal{C}_1) \oplus (\mathcal{B}_2 \square_{\pi_2} \mathcal{C}_2) \oplus (\mathcal{B}_3 \square_{\pi_3} \mathcal{C}_3)$, where $\mathcal{C}_0 \subseteq (\mathbb{F}_2 + u\mathbb{F}_2)^\ell$, $\mathcal{C}_1 \subseteq (\mathbb{F}_4 + u\mathbb{F}_4)^\ell$, $\mathcal{C}_2 \subseteq M_2(\mathbb{F}_2)^\ell$ and $\mathcal{C}_3 \subseteq M_2(\mathbb{F}_4)^\ell$.

Let us consider $\ell = 3$. If \mathcal{C}_3 is the code over $M_2(\mathbb{F}_4)$ generated by

$$\left[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ \zeta & \zeta \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right],$$

then $\mathcal{C} = \mathcal{B}_3 \square_{\pi_3} \mathcal{C}_3$ is a $[54, 8, 24]$ code. Note that this code has the best possible minimum distance for linear codes of length 54 and dimension 8, by the Griesmer bound (see [16]).

Example 4.6. Next we consider $G = \langle \alpha, \beta \mid \alpha^{11} = \beta^2 = 1, \beta\alpha\beta = \alpha^{10} \rangle \cong D_{22}$, the dihedral group of order 22, and $K = \mathbb{F}_2$. Then

$$f_0 = 1 + \alpha + \dots + \alpha^{10} \text{ and } f_1 = \alpha + \dots + \alpha^{10}$$

are the central primitive orthogonal idempotents of KG . Let us fix the ordering

$$\{1, \alpha, \dots, \alpha^{10}, \beta, \beta\alpha, \dots, \beta\alpha^{10}\}.$$

Then the corresponding blocks \mathcal{B}_0 and \mathcal{B}_1 are codes with generator matrices

$$B_0 := \begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 1 \end{bmatrix} \text{ and } B_1 := \begin{bmatrix} 0 & 1 & \dots & 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 1 & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 1 & 1 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & & 0 & 0 & 1 & \dots & 1 & 1 \\ 0 & \dots & & 0 & 1 & 0 & \dots & 1 & 1 \\ \vdots & & & \vdots & \vdots & & \ddots & & \vdots \\ 0 & \dots & & 0 & 1 & 1 & \dots & 0 & 1 \end{bmatrix}.$$

The ring \mathcal{B}_0 is isomorphic to $\mathbb{F}_2 + u\mathbb{F}_2$, with $u^2 = 0$, so that we get the map $\pi_0 : \mathcal{B}_0 \rightarrow \mathbb{F}_2^{22}$,

$$1 \mapsto B_{0,1}, 1 + u \mapsto B_{0,2}.$$

The ring \mathcal{B}_1 is isomorphic to $M_2(\mathbb{F}_{32})$, where $\mathbb{F}_{32} = \mathbb{F}_2[\zeta]$ with $\zeta^5 + \zeta^2 + 1 = 0$, so that we get the map $\pi_1 : \mathcal{B}_1 \rightarrow \mathbb{F}_2^{22}$,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto B_{1,1}, \begin{bmatrix} 1 & \zeta^9 \\ \zeta^9 & \zeta \end{bmatrix} \mapsto B_{1,2}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto B_{1,11}.$$

A G -code $\mathcal{C} \subseteq \mathbb{F}_2^{22\ell}$ can then be decomposed as $(\mathcal{B}_0 \square_{\pi_0} \mathcal{C}_0) \oplus (\mathcal{B}_1 \square_{\pi_1} \mathcal{C}_1)$, where $\mathcal{C}_0 \subseteq (\mathbb{F}_2 + u\mathbb{F}_2)^\ell$ and $\mathcal{C}_1 \subseteq M_2(\mathbb{F}_{32})^\ell$.

Let us consider $\ell = 5$. If \mathcal{C}_1 is the code over $M_2(\mathbb{F}_{32})$ generated by

$$\left[\begin{bmatrix} \zeta^{18} & 1 \\ \zeta^9 & \zeta^{21} \end{bmatrix} \quad \begin{bmatrix} \zeta^{15} & \zeta^5 \\ \zeta^{23} & \zeta^{12} \end{bmatrix} \quad \begin{bmatrix} \zeta & \zeta^{28} \\ \zeta^{20} & \zeta^{24} \end{bmatrix} \quad \begin{bmatrix} \zeta^{25} & \zeta^{20} \\ \zeta^{11} & \zeta^{15} \end{bmatrix} \quad \begin{bmatrix} \zeta^{19} & \zeta^{28} \\ \zeta & \zeta^{18} \end{bmatrix} \right],$$

$$\left[\begin{bmatrix} \zeta^{25} & \zeta^{27} \\ \zeta^{29} & \zeta^3 \end{bmatrix} \quad \begin{bmatrix} \zeta^3 & \zeta^2 \\ \zeta^5 & \zeta^{19} \end{bmatrix} \quad \begin{bmatrix} \zeta^{26} & \zeta^{26} \\ \zeta^{16} & \zeta^9 \end{bmatrix} \quad \begin{bmatrix} \zeta^{23} & \zeta^{23} \\ \zeta^{15} & \zeta^8 \end{bmatrix} \quad \begin{bmatrix} \zeta^{23} & \zeta^{17} \\ \zeta & \zeta^7 \end{bmatrix} \right],$$

then the code $\mathcal{C} = \mathcal{B}_1 \square_{\pi_1} \mathcal{C}_1$ is a $[110, 40, 22]$ code. Note that the best known minimum distance of a linear binary $[110, 40]$ code is 24 (see [16]).

5. SELF-DUALITY OF QUASI GROUP CODES

Let K be a finite field and let G be a finite group of order n . For $\ell \in \mathbb{N}$, there is a Euclidean bilinear form on $KG^\ell = KG \oplus \cdots \oplus KG$ which is defined by

$$\left\langle \sum_{i=1}^{\ell} a_i, \sum_{i=1}^{\ell} b_i \right\rangle = \sum_{i=1}^{\ell} \varphi(a_i) \cdot \varphi(b_i)$$

where φ is the isomorphism defined in (1) and $\varphi(a_i) \cdot \varphi(b_i)$ is the standard inner product on K^n . Thus $KG^\ell = KG \perp \cdots \perp KG$.

For a linear code \mathcal{C} over K of length $n\ell$, the *dual code* is classically defined as the linear code $\mathcal{C}^\perp = \{v \in K^{n\ell} \mid v \cdot c = 0 \text{ for all } c \in \mathcal{C}\}$. The definition is the same for a quasi- G code, but it can be formulated also in terms of the above Euclidean bilinear form: if \mathcal{C} is a KG -submodule of KG^ℓ , then

$$\mathcal{C}^\perp = \{v \in KG^\ell \mid \langle v, c \rangle = 0 \text{ for all } c \in \mathcal{C}\}.$$

The two definitions coincide via the isomorphism φ^ℓ . In both cases, \mathcal{C} is called *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

However, another notion of duality is used in representation theory, as we see in the following definition.

Definition 5.1. Let \mathcal{V} be a (right) KG -module. The vector space $\text{Hom}_K(\mathcal{V}, K)$ of all K -linear maps from \mathcal{V} to K becomes a right KG -module by

$$(\alpha g)v = \alpha(vg^{-1})$$

for $v \in \mathcal{V}, g \in G$ and $\alpha \in \text{Hom}_K(\mathcal{V}, K)$. This module is denoted by \mathcal{V}^* and called the *dual module* of \mathcal{V} . If $\mathcal{V} \cong \mathcal{V}^*$, we say that \mathcal{V} is a *self-dual KG -module*.

Observe that the trivial KG -module K_G is always self-dual. Furthermore, for any KG -module \mathcal{V} , we have $\dim \mathcal{V} = \dim \mathcal{V}^*$.

In [29] it has been shown that a self-dual group code in KG exists if and only if the characteristic of K is 2 and $|G|$ is even. For quasi group codes we have the following generalization. Note that for finite fields of odd cardinality the group G does not play any role.

Theorem 5.2. *For any finite group G there exists a self-dual quasi- G code over K of index ℓ if and only if one of the following holds true.*

- (i) $|K| \equiv 1 \pmod{4}$ and $2 \mid \ell$.
- (ii) $|K| \equiv 3 \pmod{4}$ and $4 \mid \ell$.
- (iii) $|K|$ is even and $2 \mid \ell$ or $2 \mid |G|$.

Proof. Suppose that $|K|$ is odd. Let $\mathcal{C} \leq KG^\ell =: \mathcal{V}$ be a quasi group code and suppose that $\mathcal{C} = \mathcal{C}^\perp$ is self-dual. We argue now similar as in [29]. First note that $\mathcal{V}/\mathcal{C} = \mathcal{V}/\mathcal{C}^\perp \cong \mathcal{C}^*$ as KG -modules. Thus the multiplicity of the trivial KG -module K_G as a composition factor of \mathcal{V} is even, since K_G is a self-dual irreducible KG -module. In particular, if T is a Sylow 2-subgroup of G , then the multiplicity of the trivial KT -module K_T in the restriction $\mathcal{V}|_T$ is even. On the other hand, by Maschke's Theorem, the multiplicity of K_T in KT is one. Thus the multiplicity of K_T in $KG|_T$ is $|G : T|$. It follows that the multiplicity of K_T in $\mathcal{V}|_T$ is $\ell|G : T|$. Since $|G : T|$ is odd, we see that ℓ must be even.

(i) By the above we only have to show that KG^2 contains a self-dual quasi group code. Since $|K| \equiv 1 \pmod{4}$ there exists $x \in K$ such that $x^2 = -1$. Now we consider the KG -module

$$\mathcal{C} = \{a \oplus xa \mid a \in KG\} \leq KG^2.$$

Clearly $\dim \mathcal{C} = |G| = \frac{\dim \mathcal{V}}{2}$. Furthermore, since

$$\langle a \oplus xa, b \oplus xb \rangle = (a, b) + (xa, xb) = (a, b) + x^2(a, b) = 0,$$

the quasi group code \mathcal{C} is self-dual. For $\ell \geq 2$, it is enough to take direct sums of this code.

(ii) Suppose that there exists a self-dual quasi- G code of index ℓ . As shown in the first paragraph of the proof we have $\ell = 2m$. Let T be a Sylow 2-subgroup of G . We consider $\mathcal{V}|_T$ which is a semi-simple KT -module. Note that the maximal submodule \mathcal{M} of $\mathcal{V}|_T$ on which T acts trivially has dimension $|G : T|\ell$. The Gram matrix $G(\mathcal{M})$ of the form restricted to \mathcal{M} is a diagonal matrix of type $(|G : T|\ell, |G : T|\ell)$ with entries $|T|$ in the diagonal. On the other hand, \mathcal{C} must intersect \mathcal{M} in a totally isotropic subspace of dimension $|G : T|m$. By ([20], Satz 7.3.12), we get $|T|^{|G:T|\ell}(-1)^{|G:T|m} = \det G(\mathcal{M})(-1)^{|G:T|m} = (-1)^m \in K^{*2}$. This forces $2 \mid m$ since $|G| \equiv 3 \pmod{4}$. Thus $4 \mid \ell$.

To prove the converse we only have to show that KG^4 contains a quasi group code. We choose x and y in K such that $x^2 + y^2 = -1$. Such elements exist since $\{-1 - x^2 \mid x \in K\}$ and $\{y^2 \mid y \in K\}$ are two sets of cardinality $(|K| + 1)/2$, so that their intersection is non-empty. Next we put

$$\mathcal{C} = \{(xa, ya, a, 0), (0, -b, yb, xb) \mid a, b \in KG\} \leq KG^4.$$

Clearly, \mathcal{C} is a KG -module of dimension $|G|^2 = \frac{\dim V}{2}$ and $\mathcal{C} \subseteq \mathcal{C}^\perp$. Thus \mathcal{C} is a self-dual quasi group code. For $\ell \geq 4$, it is enough to take direct sums of this code.

(iii) Suppose that $\mathcal{C} = \mathcal{C}^\perp \in KG^\ell =: \mathcal{V}$ where ℓ is odd. Thus $2 \mid \dim \mathcal{V} = \ell|G|$, hence $2 \mid |G|$.

Conversely, if ℓ is odd and $|G|$ is even the existence of $\mathcal{C} = \mathcal{C}^\perp \in KG^\ell$ follows immediately from [29] since $KG^\ell = KG \perp \dots \perp KG$. For ℓ even we copy the proof of (i) with $x = 1$. \square

Remark 5.3. Let K be a finite field such that $|K| \equiv 3 \pmod{4}$. Already in the early paper [26], it is proved that there exists a self-dual code in K^n if and only if $4 \mid n$.

Remark 5.4. The ternary $[12, 6, 6]_3$ self-dual extended Golay code is not a group code. According to [6], it is a right ideal in a twisted group algebra $\mathbb{F}_3^\alpha A_4$ where A_4 denotes the alternating group on 4 letters. Actually, it is also a self-dual quasi group code of index $\ell = 4$ for a cyclic group of order 3.

REFERENCES

- [1] T. Abualrub and I. Siap. *Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$* . Designs, Codes and Cryptography, 42(3), (2007): 273-287.
- [2] A. Alahmadi, H. Sboui, P. Solé and O. Yemen. *Cyclic codes over $M_2(\mathbb{F}_2)$* . Journal of the Franklin Institute, 350(9) (2013): 2837-2847.
- [3] L.M.J. Bazzi and S.K. Mitter. *Some randomized code constructions from group actions*. IEEE Trans. Inform. Theory 52 (2006): 3210-3219.
- [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 intrinsic description of group codes*. Designs, Codes and Cryptography 51.3 (2009): 289-300.
- [6] F. Bernhardt, P. Landrock and O. Manz. *The extended Golay codes considered as ideals*. J. Comb. Theory, Series A 55 (1990): 235-246.
- [7] E.L. Blokh and V.V. Zyablov. *Coding of generalized concatenated codes*. Probl. Inform. Transm., vol. 10 (1974): 218-222.
- [8] M. Borello, C. Güneri, E. Saçıkara and P. Solé. *The concatenated structure of quasi-abelian codes*. to appear in Designs, Codes and Cryptography.
- [9] M. Borello, P. Moree and P. Solé. *Asymptotic performance of metacyclic codes*. Discrete Mathematics, 343.7 (2020): 111885.
- [10] M. Borello and W. Willems. *Automorphisms of Order $2p$ in Binary Self-Dual Extremal Codes of Length a Multiple of 24*. IEEE Transactions on Information Theory, 59.6 (2013): 3378-3383.
- [11] M. Borello and W. Willems. *Group codes over fields are asymptotically good*. Finite Fields and Their Applications, 68 (2020): 101738.
- [12] C.L. Chen, W.W. Peterson and E.J. Weldon Jr. *Some results on quasi-cyclic codes*. Information and Control, 15.5 (1969): 407-423.
- [13] J. de la Cruz and W. Willems. *Twisted group codes*. IEEE Trans. Inform. Theory (2021).
- [14] S.T. Dougherty, J. Gildea, R. Taylor, and A. Tylyshchak. *Group rings, G -codes and constructions of self-dual and formally self-dual codes*. Designs, Codes and Cryptography, 86.9 (2018): 2115-2138.
- [15] S. T. Dougherty and K. Shiromoto. *Maximum distance codes over rings of order 4*. IEEE Transactions on Information Theory, 47.1 (2001): 400-404.

- [16] Markus Grassl. *Bounds on the minimum distance of linear codes and quantum codes*. Online available at <http://www.codetables.de>. Accessed on 2021-10-11.
- [17] W.C. Huffman, J.L. Kim, and P. Solé. *Concise Encyclopedia of Coding Theory*. Chapman and Hall/CRC, 2021.
- [18] W.C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.
- [19] B. Huppert and N. Blackburn. *Finite Groups II*. Springer, Berlin, 1982.
- [20] B. Huppert and W. Willems. *Lineare Algebra*. Teubner, Wiesbaden, 2006.
- [21] S. Jitman and S. Ling. *Quasi-abelian codes*. Designs, Codes and Cryptography, 74.3 (2015): 511-531.
- [22] T. Kasami. *A Gilbert-Varshamov bound for quasi-cycle codes of rate 1/2* (Corresp.). IEEE Transactions on Information Theory, 20.5 (1974): 679-679.
- [23] I. McLoughlin and T. Hurley. *A group ring construction of the extended binary Golay code*. IEEE Trans. Inform. Theory 54 (2008):4381-4383.
- [24] F.J. MacWilliams. *Codes and ideals in group algebras*. Comb. Math. and its Appl. Proceedings ed. by R.C. Bose and T.A. Dowling, Chap. 18 (1967): 317-328.
- [25] F. Oggier, P. Solé and J.C. Belfiore. *Codes over matrix rings for space-time coded modulations*. IEEE transactions on information theory, 58(2), (2012): 734-746.
- [26] V. Pless. *The number of isotropic subspaces in a finite geometry*. Rend. Cl. Scienze fisiche, matematiche e naturali, Acc. Naz. Lincei 39 (1965): 418-421.
- [27] E. Prange. *Cyclic Error-Correcting Codes in Two Symbols*. Air Force Cambridge Research Center, Cambridge, MA, Tech. Rep. AFCRC-TN-57-103 (1957).
- [28] S.K. Wasan. *Quasi abelian codes*. Publ. Inst. Math. 35 (1977): 201-206.
- [29] W. Willems. *A note on self-dual group codes*. IEEE Trans. Inform. Theory 48 (2007): 3107-3109.