

Article

Cyclicity of Binary Group Codes

Beatriz García García , Consuelo Martínez López  and Ignacio F. Rúa 

Department of Mathematics, University of Oviedo, 33007 Oviedo, Spain

* Correspondence: garciagbeatriz@uniovi.es

Abstract

In this paper, we study the cyclicity of binary group codes, identifying them as ideals in a group algebra. We focus on the construction of $\omega|\bar{\omega}$ codes, proving that they are self-dual group codes over the abelian group $C_2 \times C_k$. We demonstrate that for even integers $k > 2$, if the polynomial $x^k - 1$ splits into self-reciprocal irreducible factors, these codes are not permutationally equivalent to any cyclic code. Additionally, we present computational results for binary group codes of length $n < 24$ using the MAGMA software (V2.29-4). These results confirm that while all cyclic codes in this range are equivalent to abelian group codes, there exist non-cyclic group codes that cannot be realized as ideals in a cyclic group algebra, highlighting the strictly larger scope of the class of group codes.

Keywords: codes; rings; modules

1. Introduction

Error-correcting codes have gained importance in post-quantum cryptography, given that some promising post-quantum schemes are based on families of error-correcting codes with good properties. The first proposal in this direction, which has not yet been improved upon, uses binary Goppa codes. This is the well-known McEliece proposal [1].

Group codes are an important family that has been widely studied. In general, “group code” is used as a synonym for “left group code”; that is, the code can be identified with a left ideal of the group algebra $\mathbb{F}[G]$, where $\mathbb{F}$ is a finite field and G is a group. We have studied group codes, specifically, two-sided ideals of the group algebra $\mathbb{F}[G]$ in our research group. In particular, we have proved that there are group codes that can be obtained using a non-abelian group but cannot be obtained using abelian groups of the same order as G (see [2,3]). Furthermore, such codes exist over arbitrary finite fields (see [4]), and some of them have better parameters than any linear code with the same length and dimension. Specific decoding algorithms for group codes in the semisimple case have been studied (see [5–7]).

To better understand group codes, the MAGMA software [8] has been used to find all group codes over the field of two elements, $\mathbb{F}_2$, up to permutation equivalence. We do this for the case of groups of length ≤ 23 , given that we know that if $|G| < 24$, every G -code can be viewed as an abelian group code, which facilitates calculations. A list of such group codes can be found in [9]. Therefore, we know the parameters (length, dimension, minimum distance, weight distribution, and a generator matrix) of all group codes of length < 24 .



Academic Editor: Patrick Solé

Received: 11 February 2026

Revised: 26 February 2026

Accepted: 2 March 2026

Published: 4 March 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article

distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

Attribution (CC BY) license.

2. Some Elementary Results

2.1. Group Codes

Hereinafter, $\mathbb{F}$ will denote a finite field and $G := \{g_1 = e, g_2, \dots, g_n\}$ a finite group of order n . The set of all formal linear combinations of elements of G , $\mathbb{F}[G] := \left\{ \sum_{g \in G} \alpha_g g : \alpha_g \in \mathbb{F} \right\}$, has the structure of an algebra over $\mathbb{F}$, called the *group algebra of G over $\mathbb{F}$* . Its product is defined such that, given two elements $a = \sum_{g \in G} a_g g \in \mathbb{F}[G]$ and $b = \sum_{g \in G} b_g g \in \mathbb{F}[G]$:

$$a \cdot b = \sum_{g \in G} a_g g \cdot \sum_{h \in G} b_h h = \sum_{g \in G} \sum_{h \in G} (a_g b_h)(gh).$$

Definition 1. A linear code $\mathcal{C}$ over $\mathbb{F}$ is said to be a G -code of length $n = |G|$ if there exists a bijective map $v : \{1, \dots, n\} \rightarrow G$ mapping $i \rightarrow g_i$ such that $\{\sum_{i=1}^n a_i g_i : (a_1, \dots, a_n) \in \mathcal{C}\}$ is a two-sided ideal of $\mathbb{F}[G]$.

Definition 2. A code $\mathcal{C}$ is called a group code if there exists a group G such that $\mathcal{C}$ is a G -code.

Remark 1. If the ideal of $\mathbb{F}[G]$ is a right ideal (resp. a left ideal), the group code $\mathcal{C}$ it defines is said to be a right group code (resp. left group code). Thus, it will be understood that all ideals are two-sided unless specified as right or left.

Definition 3. The group code $\mathcal{C}$ is called an abelian (resp. metabelian, cyclic, metacyclic, etc.) group code if there exists an abelian (resp. metabelian, cyclic, metacyclic, etc.) group G such that $\mathcal{C}$ is a G -code.

Hereinafter, n will always denote the length of a code, which, in the case of a group code, will coincide with the order of the group; k will always denote the dimension of the code; and d its minimum distance. The weight distribution of a code will be denoted by WD and will be the set of pairs $\langle w, s \rangle$, where s is the number of codewords of weight w . Furthermore, an $[n, k, d]$ -code denotes a code of length n , dimension k , and minimum distance d .

2.2. The Dual of a Group Code

Recall that if $\mathcal{C}$ is an $[n, k]$ -linear code over the field $\mathbb{F}$, the *dual code* of $\mathcal{C}$ is the $[n, n - k]$ -linear code $\mathcal{C}^\perp := \{x \in \mathbb{F}^n : x \cdot y = 0 \ \forall y \in \mathcal{C}\}$, where $\cdot$ is the usual scalar product. It is said to be *self-dual* if $\mathcal{C}^\perp = \mathcal{C}$. Furthermore, if M is a generator matrix of the code $\mathcal{C}$, then the transpose of M , M^T , is a parity-check matrix of its dual code, and $\mathcal{C}^\perp := \{x \in \mathbb{F}^n : xM^T = 0\}$ (see [10], pp. 1–37). A characterization of linear codes that are group codes can be found in [11]:

Proposition 1. Let $\mathcal{C}$ be a linear code of length n over a field $\mathbb{F}$ and G a finite group of order n .

1. $\mathcal{C}$ is a left G -code if and only if G is isomorphic to a transitive subgroup of S_n contained in $\text{PAut}(\mathcal{C})$.
2. $\mathcal{C}$ is a G -code if and only if G is isomorphic to a transitive subgroup H of S_n such that $H \cup C_{S_n}(H) \subseteq \text{PAut}(\mathcal{C})$, where $C_{S_n}(H)$ denotes the centralizer of H in S_n .

Corollary 1. Since $\mathcal{C}$ and $\mathcal{C}^\perp$ have the same permutation automorphism group, $\mathcal{C}$ is a G -code if and only if $\mathcal{C}^\perp$ is also a G -code, where G is a group of order n .

It is clear that for any length n , there exists only one group code of dimension 1: the repetition code $[n, 1, n]$, which is cyclic and associated with the ideal $\langle g_1 + \dots + g_n \rangle$ of $\mathbb{F}[G]$,

$G = \{g_1 = e, g_2, \dots, g_n\}$. Likewise, there exists only one group code of dimension $n - 1$, corresponding to the parity-check code $[n, n - 1, 2]$. Note that the latter is the dual of the repetition code. Thus, the study of group codes can be restricted to dimensions k between 2 and $n - 2$, and taking duality into account, it is possible to limit the analysis to dimensions $k \leq \lfloor \frac{n}{2} \rfloor$.

2.3. Cyclic and Non-Cyclic Group Codes

The notion of a group code naturally extends that of a cyclic code. Recall that a linear code $\mathcal{C}$ is *cyclic* if it satisfies that $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}$ if and only if $(a_1, \dots, a_{n-1}, a_0) \in \mathcal{C}$. Thus, a linear cyclic code is a G -code where G is a cyclic group. Another alternative view of these codes is through polynomial codes. In this way, a linear cyclic code can be seen as an ideal in the quotient ring $\mathbb{F}[x]/\langle x^n - 1 \rangle$, generated by a (unique) monic polynomial $g(x)$ such that $g(x) \mid (x^n - 1)$ (see [10], pp. 188–215). The decomposition of this polynomial into irreducible factors allows for the generation of cyclic codes of a certain length and dimension.

In this study, we work with codes up to permutation equivalence. Thus, if $\mathcal{C}_1$ and $\mathcal{C}_2$ are two linear codes over $\mathbb{F}$ of the same length n , we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *permutationally equivalent*, denoted $\mathcal{C}_1 \sim \mathcal{C}_2$, if there exists a permutation σ of the set $\{1, \dots, n\}$ such that $(a_1, \dots, a_n) \in \mathcal{C}_1$ if and only if $(a_{\sigma(1)}, \dots, a_{\sigma(n)}) \in \mathcal{C}_2$ (see [10], pp. 188–215). Similarly, if M is a generator matrix of $\mathcal{C}_1$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if and only if MP is a generator matrix of $\mathcal{C}_2$, where P is a permutation matrix [12].

Definition 4. Given a polynomial $g(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x^1 + a_0$, its *reciprocal polynomial*, denoted $g^*(x)$, is calculated as: $g^*(x) = x^m g(\frac{1}{x}) = a_0 x^m + a_1 x^{m-1} + \dots + a_{m-1} x^1 + a_m$. It is said to be *self-reciprocal* if $g(x) = g^*(x)$.

Proposition 2. Two cyclic linear codes generated by reciprocal polynomials are permutationally equivalent.

Proof. Let $\mathcal{C}_1$ be an $[n, k]$ -cyclic code over $\mathbb{F}$ generated by $g(x) = \sum_{i=0}^m a_i x^i$, where $m = n - k$. By definition (see [10], pp. 188–215), the code $\mathcal{C}_2$ generated by the reciprocal polynomial $g^*(x) = \sum_{i=0}^m a_{m-i} x^i$ is the reciprocal code of $\mathcal{C}_1$. This implies that a codeword $(c_0, c_1, \dots, c_{n-1})$ belongs to $\mathcal{C}_1$ if and only if the codeword $(c_{n-1}, c_{n-2}, \dots, c_0)$ belongs to $\mathcal{C}_2$. Since the operation of coordinate reversal is a permutation of the component indices (specifically the permutation $\sigma(i) = n - 1 - i$ for $i = 0, \dots, n - 1$), $\mathcal{C}_1$ and $\mathcal{C}_2$ are permutationally equivalent. $\square$

3. Some Code Constructions

3.1. The Product Code

Recall that the *Kronecker product* of two matrices, $A = (a_{ij}) \in \mathcal{M}_{p \times q}(\mathbb{F})$ and $B = (b_{ij}) \in \mathcal{M}_{r \times s}(\mathbb{F})$, denoted by $A \otimes B$, is performed by replacing each element a_{ij} of matrix A with the block formed by the product of that element a_{ij} and the entire matrix B . This results in a matrix of size equal to the product of the matrix sizes, $A \otimes B \in \mathcal{M}_{pr \times qs}(\mathbb{F})$. In this way, the *product code* of two linear codes, $\mathcal{C}_1 \otimes \mathcal{C}_2$, is constructed. If $\mathcal{C}_1$ is an $[n_1, k_1]$ -linear code with generator matrix $M_1 \in \mathcal{M}_{k_1 \times n_1}(\mathbb{F})$ and $\mathcal{C}_2$ is an $[n_2, k_2]$ -linear code with generator matrix $M_2 \in \mathcal{M}_{k_2 \times n_2}(\mathbb{F})$, the product code admits $M_1 \otimes M_2 \in \mathcal{M}_{k_1 k_2 \times n_1 n_2}(\mathbb{F})$ as a generator matrix. It will have length equal to the product of the lengths and dimension equal to the product of the dimensions. Furthermore, this product of codes is associative but not commutative, although the product code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is permutationally equivalent to $\mathcal{C}_2 \otimes \mathcal{C}_1$ (see [10], pp. 567–580).

3.2. $\omega|\overline{\omega}$ Codes

Definition 5. Let k be a positive integer. The $\omega|\overline{\omega}$ code is the binary linear code $\mathcal{C}$ of length $2k$ and dimension k that admits as a generator matrix the matrix whose first k columns form the identity matrix and the last k columns form the matrix with zeros on the diagonal and ones on the off-diagonal elements. That is, the $\omega|\overline{\omega}$ code admits the matrix $M := (I_k|\overline{I}_k)$ as a generator matrix, where:

$$\overline{I}_k = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{k \times k}(\mathbb{F}_2).$$

Proposition 3. If k is even, then the code $\mathcal{C} = \omega|\overline{\omega}$ of length $2k$ and dimension k is an $\mathbb{F}_2 G$ group code, where G is the non-cyclic abelian group $C_2 \times C_k$. Furthermore, $\mathcal{C}$ has minimum distance 4 if $k > 2$.

Proof. Let $\mathcal{C}$ be the code of $\mathbb{F}_2^{2k}$ generated by the rows of $(I_k|\overline{I}_k)$. Then the permutations $\sigma = (1, 2, \dots, k)(k+1, \dots, 2k) \in S_{2k}$ and $\tau = (1, k+1) \dots (k, 2k) \in S_{2k}$ have order k and 2, respectively, and generate an abelian group $\langle \tau, \sigma \rangle$ isomorphic to $C_2 \times C_k$, and $\langle \tau, \sigma \rangle = C_{S_{2k}}(\langle \tau, \sigma \rangle) \subseteq \text{PAut}(\mathcal{C})$. By Proposition 1 the $\omega|\overline{\omega}$ code is an $\mathbb{F}_2[C_2 \times C_k]$ group code. Every word in $\mathcal{C}$ is the sum of elements in $\mathcal{B}$, the basis linked to the matrix M (see Definition 5). If the word is the sum of r elements in $\mathcal{B}$, then the weight of the word is $2r$ if r is even and k if r is odd. In particular, if $k > 2$, every element in $\mathcal{C}$ has weight ≥ 4 , and elements obtained with $r = 2$ have weight 4. $\square$

Proposition 4. If k is even, the code $\mathcal{C} = \omega|\overline{\omega}$ is self-dual.

Proof. $\mathcal{C}$ is self-dual; it suffices to check that all rows of $M = (I_k|\overline{I}_k)$ are orthogonal to each other. $\square$

Proposition 5. Let $k > 2$ be an even integer. If the polynomial $x^k - 1 \in \mathbb{F}_2[x]$ only admits self-reciprocal irreducible factors, then the code $\mathcal{C} = \omega|\overline{\omega}$ of dimension k is not permutationally equivalent to a cyclic code; that is, the code is not a cyclic group code.

Proof. Suppose, for the sake of contradiction, that $\mathcal{C}$ is permutationally equivalent to a cyclic code $\mathcal{D}$. We know from Proposition 4 that $\mathcal{C}$ is a self-dual code. Since permutation equivalence preserves the dot product and dimension, the cyclic code $\mathcal{D}$ must necessarily be self-dual.

A cyclic code of length $n = 2k$ is self-dual if and only if its generator polynomial $g(x)$ (which is a divisor of $x^{2k} - 1$ of degree k) satisfies the self-duality condition:

$$g(x)g^*(x) \equiv 0 \pmod{x^{2k} - 1} \implies g(x)g^*(x) = x^{2k} - 1$$

where $g^*(x)$ denotes the reciprocal polynomial of $g(x)$. In a field of characteristic 2, we have the identity $x^{2k} - 1 = (x^k - 1)^2$, so the condition is rewritten as:

$$g(x)g^*(x) = (x^k - 1)^2 \tag{1}$$

Let us analyze the structure of $g(x)$ under the hypothesis of the statement. Let

$$x^k - 1 = \prod_i p_i(x)^{e_i}$$

be the decomposition into irreducible factors. By hypothesis, each factor $p_i(x)$ is self-reciprocal, that is, $p_i^*(x) = p_i(x)$. Since $g(x)$ divides $(x^k - 1)^2$, its irreducible factors must belong to the set $\{p_i(x)\}$. Since all these factors are self-reciprocal, the product of any combination of them will also be self-reciprocal. Consequently, $g(x)$ is necessarily self-reciprocal:

$$g^*(x) = g(x)$$

Substituting this into Equation (1), we obtain:

$$(g(x))^2 = (x^k - 1)^2$$

Taking the square root (a unique operation in characteristic 2, since the Frobenius endomorphism is injective), we conclude that the generator polynomial is unique:

$$g(x) = x^k - 1$$

If the generator is $g(x) = x^k - 1$, the code $\mathcal{D}$ contains the codeword corresponding to the polynomial:

$$c(x) = 1 \cdot g(x) = x^k - 1 \equiv x^k + 1 \pmod{2}$$

The weight of this codeword is $w(c) = 2$. This implies that the minimum distance of the cyclic code is $d(\mathcal{D}) \leq 2$. However, by Proposition 3, we know that for $k > 2$ (and even), the minimum distance of the original code is $d(\mathcal{C}) = 4$. This contradiction ($2 \geq d(\mathcal{D}) = d(\mathcal{C}) = 4$) demonstrates that the initial assumption is false. Therefore, $\mathcal{C}$ cannot be equivalent to a cyclic code. $\square$

Corollary 2. *If $k = 2p$, with p a prime number such that 2 is a primitive root modulo p (that is, $\langle 2 \rangle = \mathbb{F}_p^*$), then the code $\mathcal{C} = \omega|\overline{\omega}$ of length $2k$ and dimension k is not permutationally equivalent to any cyclic code.*

Proof. Consider the factorization of $x^k - 1$ over $\mathbb{F}_2$. Given that $k = 2p$, we have $x^{2p} - 1 = (x^p - 1)^2 = ((x - 1)\Phi_p(x))^2$. The condition $\langle 2 \rangle = \mathbb{F}_p^*$ guarantees that the cyclotomic polynomial $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ is irreducible in $\mathbb{F}_2[x]$. The result follows from the previous proposition. $\square$

4. Cyclicity of Binary Abelian Group Codes

As a particular case of computational interest, it has been verified that for any positive integer $n < 24$, every cyclic linear code $\mathcal{C}$ of length n over the field of two elements $\mathbb{F}_2$ is permutationally equivalent to a group code over the group algebra $\mathbb{F}_2G$, for any non-cyclic abelian group G of order n . This verification has been carried out exhaustively using the MAGMA software [8]. For each length $n < 24$ and each dimension $2 \leq k \leq \lfloor \frac{n}{2} \rfloor$, all existing binary linear cyclic codes have been generated. Subsequently, it has been verified that each of them is, up to permutation equivalence, a group code over the algebra $\mathbb{F}_2G$ for any non-cyclic abelian group G of order n . This allows us to ask whether this fact holds for non-cyclic binary group codes and whether it can be generalized to non-abelian groups or extended to other lengths.

In the case of non-cyclic abelian binary group codes, this fact does not hold. There exist non-cyclic group codes that cannot be viewed as G -codes for some abelian group G .

For example, if $G = \langle a \rangle \times \langle b \rangle \cong C_4 \times C_4$, in $\mathbb{F}_2 G$ we can consider the ideal generated by $1_G + b + b^2 + b^3$ and $1_G + a + a^2 + a^3$. The corresponding G -code $\mathcal{C}$ is a $[16, 7, 4]$ -binary code, with weight distribution

$$WD = \{\langle 0, 1 \rangle, \langle 4, 8 \rangle, \langle 6, 16 \rangle, \langle 8, 78 \rangle, \langle 10, 16 \rangle, \langle 12, 8 \rangle, \langle 16, 1 \rangle\}$$

and is non-cyclic.

Indeed, the only binary cyclic codes with parameters $[16, 7, 4]$ are permutationally equivalent to the code generated by the polynomial $g(x) = (x + 1)^9 = x^9 + x^8 + x + 1$, whose weight distribution is

$$WD_2 = \{\langle 0, 1 \rangle, \langle 4, 28 \rangle, \langle 8, 70 \rangle, \langle 12, 28 \rangle, \langle 16, 1 \rangle\}.$$

Therefore, $\mathcal{C}$ cannot be equivalent to a cyclic code. This code cannot be viewed as a K -code for the group $K = C_2 \times C_8$, but it can be viewed as an H -code for $H = C_2 \times C_2 \times C_4$ or $H = C_2 \times C_2 \times C_2 \times C_2$.

If $H = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \cong C_2 \times C_2 \times C_4$, the code $\mathcal{C}$ is permutationally equivalent to the H -code defined by the ideal generated by $1_H + c + c^2 + c^3$ and $1_H + a + b + ab$. And if $H = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \times \langle d \rangle \cong C_2 \times C_2 \times C_2 \times C_2$, the code $\mathcal{C}$ is permutationally equivalent to the H -code defined by the ideal generated by $1_H + a + d + ad$ and $1_H + b + c + bc$.

Similarly, if $G = C_2 \times C_2 \times C_2 \times C_2$, the G -code defined by the ideal generated by $1_G + a + b + ba + c + d$ is a $[16, 8, 4]$ -code with weight distribution

$$WD = \{\langle 0, 1 \rangle, \langle 4, 12 \rangle, \langle 6, 64 \rangle, \langle 8, 102 \rangle, \langle 10, 64 \rangle, \langle 12, 12 \rangle, \langle 16, 1 \rangle\}.$$

This code is not permutationally equivalent to any other non-cyclic abelian code in $\mathbb{F}_2[G]$ where G is an abelian group other than $G = C_2 \times C_2 \times C_2 \times C_2$.

5. Group Codes Associated with a Non-Principal Ideal

In contrast to the semisimple case, in the non-semisimple case, there exist ideals that are not principal. In fact, there exist group codes that are not permutationally equivalent to any group code obtained via a principal ideal. For example, the $[16, 7, 4]$ -binary group code $\mathcal{C}$ over $\mathbb{F}_2[G]$ for $G = C_4 \times C_4$ from the previous section is not permutationally equivalent to any group code linked to a principal ideal.

In other cases, there exist group codes constructed with a non-principal ideal that are permutationally equivalent to group codes obtained with principal ideals. For example, if $G = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \times \langle d \rangle \cong C_2 \times C_2 \times C_2 \times C_2$, in $\mathbb{F}_2 G$ we can consider the ideal generated by $1_G + a + b + c + ca + cb + d + dc$ and $1_G + a + b + ba + d + da + db + dba$.

The corresponding G -code $\mathcal{D}$ is a $[16, 5, 8]$ -binary code, with weight distribution

$$WD = \{\langle 0, 1 \rangle, \langle 8, 30 \rangle, \langle 16, 1 \rangle\}$$

and is non-cyclic. Indeed, the only binary cyclic codes have parameters $[16, 5, 4]$ and are permutationally equivalent to the code generated by the polynomial $g(x) = (x + 1)^{11} = x^{11} + x^{10} + x^9 + x^8 + x^3 + x^2 + x + 1$. Therefore, $\mathcal{D}$ cannot be equivalent to a cyclic code.

For this group code $\mathcal{D}$, one cannot find a principal ideal of $\mathbb{F}_2[G]$ with $G = C_2 \times C_2 \times C_2 \times C_2$ that generates a code permutationally equivalent to it. However, one can find a principal ideal of $\mathbb{F}_2[H]$ with $H = C_2 \times C_2 \times C_4$, $H = C_4 \times C_4$, or $H = C_2 \times C_8$, that generates a code permutationally equivalent to it.

If $H = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \cong C_2 \times C_2 \times C_4$, the code $\mathcal{D}$ is permutationally equivalent to the H -code defined by the ideal generated by $c^2 + a + b + ba + c^3 + ca + cb + cba$. If $H = \langle a \rangle \times \langle b \rangle \cong C_4 \times C_4$, the code $\mathcal{D}$ is permutationally equivalent to the H -code defined

by the ideal generated by $1_H + a^2 + a + ab^2 + b + b^3 + ba + ba^3$. And if $H = \langle a \rangle \times \langle b \rangle \cong C_2 \times C_8$, the code $\mathcal{D}$ is permutationally equivalent to the H -code defined by the ideal generated by $b^4 + b^6 + a + ab^2 + b + b^3 + ba + b^3a$.

6. Some Properties

In [13], it is shown that every abelian group code associated with a minimal ideal in a semisimple algebra is permutationally equivalent to a cyclic one. The result is not true if the condition of minimality is removed. For example, if $G = \langle a \rangle \times \langle b \rangle \cong C_3 \times C_3$, the ideal in $\mathbb{F}_2[G]$ generated by $1_G + a + b + ab$ defines a $[9, 4, 4]$ -code, which is the product code of the cyclic code in C_3 of length 3 and dimension 2 generated by the polynomial $g(x) = x + 1$, with itself, and has weight distribution

$$WD = \{\langle 0, 1 \rangle, \langle 4, 9 \rangle, \langle 6, 6 \rangle\}.$$

This code is not minimal (the only minimal ideals have dimensions 1 and 2) and is not cyclic.

What happens if we do not require the semisimplicity of the group algebra? For $n < 24$ (where we know that all group codes are abelian group codes), the result remains true if $\mathbb{F} = \mathbb{F}_2$. However, it is not known what happens in the general case.

7. Conclusions

In this work, we have investigated the relationship between cyclicity and group codes over binary fields. We have formally defined and analyzed $\omega|\bar{\omega}$ codes, proving their self-duality and establishing conditions under which they are strictly non-cyclic. Our computational survey of codes with length $n < 24$ confirms that while every binary cyclic code in this range is equivalent to an abelian group code, the class of group codes is strictly larger, containing optimal codes that do not possess a cyclic structure. These findings highlight the richness of group codes beyond the cyclic case. Future research will focus on extending these classifications to non-abelian groups and exploring the decoding capabilities of these non-cyclic structures.

Author Contributions: All authors equally working on the topic. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the European Union through the Spanish National Cybersecurity Institute (INCIBE) within the Recovery, Transformation and Resilience Plan–Next Generation EU, under the Spain Digital Agenda 2026 framework (project MRR-MAETD:24-INCIBE-001). PECIEE project, funded by INCIBE. This project is part of the actions of Axis 2 of C15.I7, of the Recovery, Transformation, and Resilience Plan, whose objective includes the “Promotion of Industry,” Pillar (2): “Support for R&D&I in Cybersecurity as a transformative element of the country.” Specifically, it contributes to the activities of CID 453, an indicator established by the European Commission (“Launch of the program to support the national cybersecurity industry, the global security innovation program, and related actions”), fulfilling the objectives set out in the indicator description: development of high value-added solutions and services in the field of cybersecurity; and training and development of specialized talent in the field of cybersecurity”.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy restrictions.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. McEliece, J. *A Public-Key Cryptosystem Based on Algebraic Coding Theory*; DSN Progress Report; Jet Propulsion Laboratory: La Cañada Flintridge, CA, USA, 1978; pp. 114–116.
2. García, C.; González, S.; Markov, V.; Martínez, C.; Nechaev, A. Group codes which are not Abelian group codes. *J. Algebra Its Appl.* **2013**, *12*, 123–127.
3. García, C.; González, S.; Markov, V.; Martínez, C.; Nechaev, A. New examples of non-abelian group codes. *Adv. Math. Commun.* **2016**, *10*, 1–10. [[CrossRef](#)]
4. García, C.; González, S.; Markov, V.; Martínez, C. Non-abelian group codes over an arbitrary finite field. *J. Math. Sci.* **2017**, *223*, 504–507. [[CrossRef](#)]
5. Martínez, C.; Molina, F. The syndromes decoding algorithm in group codes. *Finite Fields Their Appl.* **2023**, *89*, 102166. [[CrossRef](#)]
6. Martínez, C.; Molina, F. Two Decoding Algorithms in Group Codes. In *Libro de Actas XVII Reunión Española sobre Criptología y Seguridad de la Información*; Universidad de Cantabria: Santander, Spain, 2022; pp. 157–161.
7. Bernal, J.J.; del Río, A.; Simón, J.J. Partial Permutation Decoding for Abelian Codes. *IEEE Trans. Inf. Theory* **2013**, *59*, 5152–5170. [[CrossRef](#)]
8. Bosma, W.; Cannon, J.; Playoust, C. The Magma Algebra System I: The User Language. *J. Symb. Comput.* **1997**, *24*, 235–265. [[CrossRef](#)]
9. García, B.; Rúa, I.F. Clasificación de códigos grupo binarios de longitud menor que 24. In *XVIII Reunión Española sobre Criptología y Seguridad de la Información*; Universidad de León: León, Spain, 2024; pp. 193–197.
10. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error-Correcting Codes*; Elsevier/North-Holland: New York, NY, USA, 1977.
11. Bernal, J.J.; del Río, A.; Simón, J.J. An intrinsical description of group codes. *Des. Codes Cryptogr.* **2009**, *51*, 289–300. [[CrossRef](#)]
12. Pless, V.S.; Huffman, W.C.; Brualdi, R.A. An Introduction to Algebraic Codes. In *Handbook of Coding Theory*; Elsevier: Amsterdam, The Netherlands, 1998; Volume I; pp. 13–17.
13. Chalom, G.; Ferraz, R.A.; Polcino, C. Essential idempotents and simplex codes. *J. Algebra Comb. Discret. Struct. Appl.* **2017**, *4*, 181–188. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.