Preprints.org

Article

Not peer-reviewed version

A Class of Binary Codes Using a Specific Automorphism Group

Driss HARZALLA *

Posted Date: 5 November 2024

doi: 10.20944/preprints202411.0345.v1

Keywords: binary linear code; self-orthogonal code; automorphism group; group actions; representation theory

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0345.v1

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.

Article

A Class of Binary Codes Using a Specific Automorphism Group

Driss Harzalla

Cadi Ayyad University, National School of Applied Sciences ENSAS, Route Sidi Bouzid BP 63 Rue Sidi M'Barek, Safi 46000, Morocco [1]; 68harzalla@gmail.com; Tel.: +212-6634-452-82

Abstract: In this article, we showcase $PSL(3,4)$ as the automorphism group for a specific class of three linear binary codes C_1, C_2 and C_3 with dimension 9. The demonstration involves leveraging the action of the group $PSL(3,4)$, represented by invertible matrices of size 9 by 9 up to isomorphism, on the vector space ${F_2}^9$. Additionally, we establish that these codes exhibit a 3−weight self-orthogonal property. All computations presented in this paper were conducted using guava package of GAP (Groups, Algorithms, Programming) a system designed for computational discrete algebra.

Keywords: binary linear code; self-orthogonal code; automorphism group; group actions; representation theory

---

1. Introduction

Doubly even self-orthogonal codes constitute a well-explored class of error-correcting codes that find significant applications, particularly in the construction of quantum error-correcting codes [1]. In this paper, our focus centers on self-orthogonal doubly even binary codes with dimension 9. Extensive research in the literature has already examined the algebraic and combinatorial properties of self-orthogonal doubly even binary codes, including the study of their automorphism groups, with a specific interest in codes possessing large automorphism groups [2,5]. In our investigation, we identify three-weight, self-orthogonal doubly even binary codes with a dimension of 9. We introduce the concept of linear codes to provide a theoretical foundation for our analysis. If C represents a k-dimensional subspace of ${F_2}^n$, where F_2 denotes the Galois field with 2 elements, then C is referred to as an $[n,\ k]_2$ binary linear code. Let A_i denote the number of codewords with Hamming weight i in a code C of length n. The weight enumerator of C is defined by

$$1\ +\ A_1 * z^1\ +\ A_2 * z^2\ +\ \dots\ +\ A_n * z^n \tag{1}$$

A code C is said to be a 3−weight code [10] if the number of nonzero A_i in the sequence $(A_1,\ A_2,\ \dots,A_n)$ is equal to 3. Overall, three-weight linear binary codes play a crucial role in various applications where error detection and correction, data security, network optimization, and data storage are paramount. Two common ways to represent a linear code are through a generator matrix or a parity check matrix. A generator matrix denoted G, for an $[n,\ k]_2$ code C is a $k \times n$ matrix whose rows form a basis for C. On the other hand, a parity check matrix denoted H, for the $[n,\ k]_2$ code C is an $(n-k)\times n$ matrix defned by [7,8]

$$C = \left\{x \in F_2^n\ :\ Hx^T = 0\right\} \tag{2}$$

The rows of H are independent and can also serve as the rows of a generator matrix for the dual or orthogonal code, denoted $C^{\perp}$. It is worth noting that $C^{\perp}$ is an $[n,\ n-k]_2$ code. Alternatively, the dual code $C^{\perp}$ can be defned through inner products as

$$C^{\perp} = \{x \in F_2^n\ :\ x.c = 0,\ \forall c \in C\} \tag{3}$$

Recall that the ordinary inner product of vectors $x = (x_1,\ x_2,\ x_n)$, $y = (y_1,\ y_2,\ y_n)$ in ${F_2}^n$ is

$$x.y = x_1.y_1 + x_2.y_2 + \ \dots\ + x_n.y_n \tag{4}$$

© 2024 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0345.v1

To delve into the automorphism properties of codes, we introduce the concept of the automorphism group, denoted $PAut\ (C)$. The permutations of coordinate places that preserve C form the automorphism group of C. In particular, the automorphism group of C, represented by an $n \times n$ matrix P, belongs to $PAut(C)$ if and only if $KG = GP$ for some nonsingular $k \times k$ matrix K. It is important to note that the group $PAut\ (C)$ is isomorphic to the group $PAut\ (C^{\perp})$ [7]. To explore the automorphism properties in our study, we focus on the group $PSL(3, 4)$ with an order of 20160, which serves as a large automorphism group for a family of three doubly even, 3−weight, and auto-orthogonal linear codes of dimension 9. By utilizing the group action notion of $GL(9,\ 2)$ on specifc vectors from the vector space ${F_2}^9$, we investigate the structural characteristics and properties of the codes under examination. Our analysis demonstrates that codes within this family, sharing the same Minimum Distance $d = 9$. If G and H are generator and parity check matrices, respectively, for C, then H and G are generator and parity check matrices, respectively, for $C^{\perp}$ [6]. We call a code C self-orthogonal if $C \subseteq C^{\perp}$ and C is called self-dual if $C = C^{\perp}$. We say that a binary vector is doubly-even if its weight is divisible by 4. A binary vector is singly-even if its weight is even but not divisible by 4. In general, we have the following definition [6].

Definition 1. *Let C be a binary linear code. C is called even if all of its codewords have even weight. C is called doubly-even if all of its codewords have weights a multiple of* 4*. An even binary code that is not doubly-even is singly-even.*

A self-orthogonal code must be even; one which is not doubly-even is called singly-even. If a binary code has only doubly-even vectors, the code is self-orthogonal as stated by the following theorem [6].

Theorem 1. *Let C be a binary linear code.*
(i) If C is self-orthogonal and has a generator matrix each of whose rows has weight divisible by four, then every codeword of C has weight divisible by four.
(ii) If every codeword of C has weight divisible by four, then C is self-orthogonal.

We also recall that the group $PAut(C)$ is isomorphic to the group $PAut(C^{\perp})$.

$$PAut(C) \cong PAut\left(C^{\perp}\right) \tag{5}$$

The general linear group $GL(9,\ 2)$ is the group of $n \times n$ invertible matrices with entries in the fnite feld F_2. $Mat_{9\times 9}(F_2)$ denotes the set of 9×9 matrices with entries in F_2, and $det\ (A)$ is the determinant of matrix A. The special linear group $SL(9,\ 2)$ is a subgroup of the general linear group $GL(9,\ 2)$. It consists of all 9×9 matrices with determinant equal to 1 in the fnite feld F_2. The Projective Special Linear Group $PSL(n,\ q)$ is defned in [9] as the set of left cosets.

A (left) natural group action ϕ of the group $GL(9,\ 2)$ on F_2^9 is a function

$$\phi : \begin{cases} GL(9,\ 2) \times F_2^9 \to F_2^9 \\ (M,\ v) \mapsto \phi(M,\ v) = M.v \end{cases}$$

which satisfies the following two axioms:
(Identity): $\forall v \in F_2^9, \phi(I_9,\ v) = v$ (Here, I_9 denotes the identity element of $GL(9,2)$)
(Compatibility): $\forall M, N \in GL(9,\ 2), \forall v \in F_2^9, \phi(M.N,\ v) = \phi(M,\ \phi(N,\ v))$
We define the orbit of a vector v_i by

$$Orb_i = Orb(v_i) = \{Mv_i\ ;\ M \in GL(9,\ 2)\} \tag{6}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0345.v1

and we denote p_i the number of its elements [8].
In the next section, we present three self-orthogonal doubly even binary codes of dimension 9 all are three-weight codes.

2. Definition of Binary Linear Codes C_i, $1 \le i \le 3$

let $G =< A, B >$ be the group generated by the two 9×9 binary matrices A and B defined over the Galois fIeld F_2

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

The group G of order 20160 is somorphic to the group $PSL(3,4)$ through an isomorphism f (These are classical results from the ATLAS of Finite Group Representations, and another way to verify this is by using GAP.). For A an element of $PSL(3,4)$ and X an element of F_2^9, we defne the product $A.X$ as follows:

$$A.X = f(A).X$$

Indeed, the previous formula is clarified by identifying A and $f(A)$ through the isomorphism f. We consider

$$v_1 = (000000001)^T$$
$$v_2 = (000000011)^T$$
$$v_3 = (000000111)^T$$

vectors of F_2^9 and the following integers

$$p_1 = 21, \quad p_2 = 210, \quad p_3 = 280$$

Consider the orbits of each vector v_i under the natural action of the group $GL(9,2)$ on F_2^9

$$Orb_i = Orb(v_i) = \{M_{i,j}v_i \ : \ M_{i,j} \in GL(9,\, 2)\}_{(1 \le j \le p_i)}\,,\ 1 \le i \le 3$$

We write each of these orbits as the $9 \times p_i$ matrix

$$G_i = \left[M_{i,1}v_i,\ M_{i,2}v_i,\ \ldots,\ M_{i,p_i}v_i\right],\ 1 \le i \le 3$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0345.v1

Consider C_i, $1 \leq i \leq 9$ binary linear codes of generator matrix G_i.

3. Properties of Binary Linear Codes C_i, $1 \leq i \leq 3$

Theorem 2. *For all C_i, $1 \leq i \leq 3$ the binary linear code C_i have dimension $k = 9$.*

Proof. To show this result, we put the $9 \times p_i$ matrix G_i in standard form $Q_i = [I_9|A_i]$, for some $9 \times (p_i - 9)$ matrix A_i and where I_9 is the 9×9 identity matrix. After a possible permutation σ_i of the columns, using elementary row operations, the matrix G_i can be reduced to standard form. Let Π_i the weight Enumerator of the code C_i. In the following, we give the method for the code C_1, the same method generalizes to the two other codes.

$$\sigma_1 = (9, 12)$$

$$A_1 = \begin{pmatrix} 110001010111 \\ 101111000101 \\ 001110111001 \\ 010011101101 \\ 011101100011 \\ 110110011100 \\ 101101011010 \\ 011000111110 \\ 000111110110 \end{pmatrix}$$

The length n, the dimension k, and the minimum distance d of each C_i, $1 \leq i \leq 3$ code is given in this table.

Table 1. Paramètres des codes linéaires binaires C_i, $1 \leq i \leq 3$.

	C_1	C_2	C_3
n	21	210	280
k	9	9	9
d	8	80	136

□

Lemma 1. *For all i, $1 \leq i \leq 3$ the code C_i is doubly-even $3-$weight code.*

Proof. For all i, $1 \leq i \leq 3$, the weight Enumerator of the code C_i is denoted by Π_i:

$$\Pi_1 = 21 * x^{16} + 280 * x^{12} + 210 * x^8 + 1$$

$$\Pi_2 = 280 * x^{108} + 210 * x^{104} + 21 * x^{80} + 1$$

$$\Pi_3 = 21 * x^{160} + 210 * x^{144} + 280 * x^{136} + 1$$

Note that the weight of each codeword of each code C_i is equal to zero modulo four. So we have the result from Theorem 1.1.

Theorem 3. *For all i, $1 \leq i \leq 3$ the code C_i is self-orthogonal*

Proof. Proof 2.6 By Theorem 1.2. □

Theorem 4. *For all i, $1 \leq i \leq 3$ the group $PSL(3,4)$ is an automorphism group of the code C_i*

Proof. The group $G =< A, B >$ generated by the two 9×9 binary matrices A and B defined over the Galois field F_2, is isomorphic to $PSL(3,4)$ and then considered as the same group. Let i, $1 \leq i \leq 3$ and

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0345.v1

$$\rho_i : \begin{cases} PSL(3,4) \to PAut(C_i) \\ \quad D \to \phi(D) = P \text{ such that } D.G_i = G_i.P \text{ where } D.G_i = f(D).G_i \end{cases}$$

□

Proof.

Step 1: The generator $9 \times p_i$ matrix G_i of the code C_i is deduced from the orbit Orb_i and defined by its p_i column vectors $M_{i,j}.v_i$ as the following

$$G_i = [M_{i,1}v_i,\ M_{i,2}v_i,\ \ldots,\ M_{i,p_i}v_i\ ]\ ,\ 1 \le i \le 3$$

vectors form exactly the orbit Orb_i. As a result, we have

$$\begin{aligned} D.G_i &= f(D).\Big[M_{i,1}v_i,\ M_{i,2}v_i,\ \ldots,\ M_{i,p_i}v_i\Big] \\ &= \Big[f(D).M_{i,1}v_i,\ f(D).M_{i,2}v_i,\ \ldots,\ f(D).M_{i,p_i}v_i\Big] \\ &= \Big[D.M_{i,1}v_i,\ D.M_{i,2}v_i,\ \ldots,\ D.M_{i,p_i}v_i\Big](by\ orbit\ Definition\ we\ have) \\ &= \Big[M_{i,\pi(1)}v_i,\ M_{i,\pi(2)}v_i,\ \ldots,\ M_{i,\pi(p_i)}v_i\Big](for\ some\ permutation\ \pi) \\ &= \Big[M_{i,1}v_i,\ M_{i,2}v_i,\ \ldots,\ M_{i,p_i}v_i\Big].P \end{aligned}$$

where P is the unique permutation matrix associated with the permutation π. we deduce that the application ρ_i is well defined.

□

Step 2: We consider $D_1, D_2 \in PSL(3,4)$ and $P \in PAut(C)$

$$\begin{aligned} \rho_i(D_1) = \rho_i(D_2)(= P) &\Rightarrow D_1.G_i = G_i.P\ and\ D_2.G_i = G_i.P \\ &\Rightarrow D_1.G_i = D_2.G_i \\ &\Rightarrow f(D_1).G_i = f(D_2).G_i \\ &\Rightarrow (f(D_2))^{-1}.f(D_1).G_i = G_i \\ &\Rightarrow (f(D_2))^{-1}.f(D_1) = I_9(since\ rank\ (G_i) = 9) \\ &\Rightarrow f(D_1) = f(D) \\ &\Rightarrow D_1 = D_2(since\ f\ is\ an\ isomorphism) \end{aligned}$$

So the application ρ_i is injective. □

Step 3: We consider $D_1, D_2 \in PSL(3,4)$ and $P_1, P_2 \in PAut(C)$ such as $\rho_i(D_1) = P_1$ and $\rho_i(D_2) = P_2$, then $D_1.G_i = G_i.P_1$ and $D_2.G_i = G_i.P_2$. We have

$$\begin{aligned} (D_1.D_2).G_i &= f(D_1.D_2).G_i \\ &= (f(D_1).f(D_2)).G_i \\ &= f(D_1).(f(D_2).G_i) \\ &= f(D_1).(D_2.G_i) \\ &= f(D_1).(G_i.P_2) \\ &= (f(D_1).G_i).P_2 \\ &= (D_1.G_i).P_2 \\ &= (D_1.G_i).P_2 \\ &= (G_i.P_1).P_2 \\ &= G_i.(P_1.P_2) \end{aligned}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0345.v1

We deduce that $\rho_i(D_1.D_2) = P_1.P_2 = \rho_i(D_1).\rho_i(D)$ and then ρ_i is an homomorphism. We conclude that $PSL(3,4) \cong \rho_i(PSL(3,4))$ is a subgroup of the full permutation automorphism group $PAut(C_i)$.

Remark: C_1 meet the Bounds on the Minimum Distance in the Code Tables [10] C_2 improoves the the lower Bound on the Minimum Distance in the Code Tables [10]. Indeed, lower bound: 101, upper bound: 102.

Funding: This research received no external finance.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: All information is in the manuscript.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Liang, F., Self-orthogonal codes with dual distance three and quantum codes with distance three over F_5. *Quantum Inf. Process* **2013**, *12*, 3617-3623. [CrossRef].
2. Huffman, W. Cary, Codes and groups. In: *Pless, V. S. (ed.) et al., Handbook of coding theory. Vol. 1. Part 1: Algebraic coding. Vol. 2. Part 2: Connections, Part 3: Applications. Elsevier,* **1998**, 1345-1440.
3. MacWilliams, F.J., Permutation decoding of systematic codes. *Bell System Tech. J.* **1964**, *43*, 485-505. [CrossRef].
4. Chigira, N., Permutation groups and binary self-orthogonal codes. *Journal of Algebra* **2007**, *309* iss. 2, 610-621. [CrossRef].
5. Tolhuizen, L.M.G.M.; Van Gils, W.J., A large automorphism group decreases the number of computations in the construction of an optimal encoder/decoder pair for linear block codes. *IEEE Transactions on Information Theory* **1988**, *34*, 333-338. [CrossRef].
6. Huffman, W.C.; Kim, J.L.; Solé, P., *Concise Encyclopedia of Coding Theory*, 1st Edition *Chapman and Hall CRC Taylor and Francis Group* **2021**, *10*. [CrossRef].
7. Betten, A.; Braun, M.; Fripertinger, H.; Kerber, A.; Kohnert, A.; Wassermann, A., *Error-Correcting Linear Codes: Classification by Isometry and Applications Algorithms and Computation in Mathematics*. Springer, **2006**, *18* [CrossRef].
8. Rotman, J.J., *Advanced Modern Algebra, Part 2 Graduate Studies in Mathematics*. American Mathematical Society. **2017**, *180*, 142-149. [CrossRef].
9. Ding, K.; Ding, C., Binary linear codes with three weights. *IEEE Communications Letters* **2014**, *18*, no. 11. [CrossRef].
10. Grassl, M., Bounds on the minimum distance of linear codes and quantum codes. Available online at: http://www.codetables.de. Consulté le **27 avril 2024**.

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.