Article

Not peer-reviewed version

On Small Automorphism Groups of Binary Self-Dual Codes

Carolin Hannusch * and Sándor Roland Major

Posted Date: 25 June 2025

doi: 10.20944/preprints202506.2100.v1

Keywords: permutation groups; error-correcting codes; small groups

Article

On Small Automorphism Groups of Binary Self-Dual Codes

Carolin Hannusch [1,*,†] and S. Roland Major [2,†]

[1] Department of Computer Science, Faculty of Informatics, University of Debrecen, Debrecen, Hungary
[2] Department of Information Technology, Faculty of Informatics, University of Debrecen, Debrecen, Hungary
* Correspondence: hannusch.carolin@inf.unideb.hu
† These authors contributed equally to this work.

Abstract

In this paper, we investigate the structure of small automorphism groups of binary self-dual codes and present new theoretical results. We prove that the automorphism group of a binary self-dual code cannot be generated by a single cycle permutation of length 2 or 3, and that no automorphism can act exclusively on one half of the code's coordinates. Additionally, we provide new constraints for binary self-dual codes with trivial automorphism groups. These findings have significant implications for the classification and construction of such codes, particularly in cases where the existence of a self-dual code remains unresolved, for example, in the case of a binary self-dual $(72, 36, 16)$-code. Our results concerning such a code with automorphism group isomorphic to the cyclic group of order 5 offer valuable insight for both constructive approaches and exhaustive computational searches in this context.

Keywords: permutation groups; error-correcting codes; small groups

1. Introduction

Binary self-dual codes are important objects in Coding Theory due to their good error-correcting properties. One possibility to classify and to characterize them is to investigate their automorphism groups. Automorphism groups of binary self-dual codes were studied for example in [1–3]. Those binary self-dual codes which have the highest possible minimum distance appear to have very large automorphism groups, like the famous Golay code whose automorphism group is the Mathieu group $\mathcal{M}_{24}$ [4]. In this paper, we investigate how small automorphism groups of binary self-dual codes can be generated. The existence of a binary self-dual code of length 72 with highest possible minimum distance has been an open question [5] for a long time. For its solution several monetary prizes are proposed [6]. The paper is structured as follows. In Section 2 we give all necessary definitions and recall classical coding theoretical results that are important for our proofs. In Section 3 we show on which sets of coordinates can act an automorphism. In Section 4 we investigate binary self-dual codes whose automorphism group can be generated by exactly one transposition or by exactly one 3-cycle permutation. Finally, in Section 6 we give new restrictions for the construction of a self-dual binary $(72, 36, 16)$-code based on its mutual automorphism group.

2. Preliminaries

We denote the finite field of two elements by $\mathbb{F}_2$ and the n-dimensional vectorspace over $\mathbb{F}_2$ by $V^n(\mathbb{F}_2)$. A *binary (linear) code* of dimension k is a k-dimensional subspace of $V^n(\mathbb{F}_2)$. The elements of a code are called *codewords*. The *weight* of a codeword is the number of its nonzero coordinates. The weight of a linear code is the minimum of all of the weights of all of its codewords. The weight of a code is also called *minimum distance* and is denoted by d. Usually, a linear code is denoted as (n, k, d)-code, where n is the codelength, k the dimension as subspace and d the minimum distance.

 doi:10.20944/preprints202506.2100.v1

The *inner product* of two codewords is computed as the sum of all coordinatewise products, i.e. if C is a linear code and $c_1, c_2 \in C$, then the inner product of c_1 and c_2 is computed by

$$\langle c_1, c_2 \rangle = \sum_{i=1}^{n} c_1[i] \cdot c_2[i].$$

We say that c_1 and c_2 are *orthogonal* to each other if $\langle c_1, c_2 \rangle = 0$. The dual code of C is denoted by $C^\perp$ and is defined by

$$C^\perp = \{u \mid u \in V^n(\mathbb{F}_2) \text{ and } \langle u, c \rangle = 0 \text{ for all } c \in C\}.$$

A code is called *self-dual* if $C = C^\perp$. For two codewords c_1 and c_2, we denote the number of coinciding 1 coordinates by $\mu(c_1, c_2) = \#\{i \mid c_1[i] = c_2[i] = 1\}$. If C is self-dual, then for every $c_1, c_2 \in C$ we have $\mu(c_1, c_2) \equiv 0 \mod 2$.

Every $k \times n$ matrix that is a basis for C as subspace is called *generator matrix* of C.

Let σ be a permutation on a set of n elements. We apply permutations on the columns of matrices. If C is a linear code with generator matrix G, then G^σ generates a code C_σ which is *permutation equivalent* to C. If $C_\sigma = C$, then σ is an *automorphism* of C. All automorphisms of a linear code form a group, called the *automorphism group* of C denoted by $Aut(C)$.

It is well known that every linear code C is permutation equivalent to a code generated by a matrix in standard form $G_C = (I_k, A)$, where I_k denotes the identity matrix of order k and A is a $k \times (n-k)$ matrix. If C is generated by a matrix in standard form, then its dual $C^\perp$ is generated by a matrix of the form $H_C = (-A^t, I_{n-k})$, where A^t denotes the transponed of A. Note, that if C is binary, then $-A = A$.

3. Automorphisms Acting on the Coordinates

We assume that C is a self-dual binary code generated by a matrix in standard form. One may wonder then if an automorphism of C may act only on one half of the coordinates, namely on the part of the identity matrix, either in $G_C = (I_k, A)$ or in $H_C = (-A^t, I_{n-k})$. In the following we show that this is not possible and every automorphism of C is acting on both halfs.

Theorem 1. *Let C be a self-dual binary (n, k, d)-code generated by a matrix in standard form with $d > 2$. Then every non trivial automorphism of C acts on $\{1, \ldots, k\}$ and on $\{k+1, \ldots, 2k = n\}$.*

Proof. We assume indirectly that there exists $\sigma \in Aut(C)$ acting only on $\{1, \ldots, k\}$. By assumption, C can be generated by $G_C = (I_k, A)$, and we denote

$$I = \begin{pmatrix} i_1 \\ \vdots \\ i_k \end{pmatrix}, G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \text{ and } A = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}.$$

Then $G_C^\sigma = (I_k^\sigma, A)$. Since $\{g_1, \ldots, g_k\}$ are codewords of C and σ acts on at least two coordinates - denotes by s and t -, then $g_s = (i_s, a_s)$, $g_t = (i_t, a_t)$ and we have $g_s^\sigma = (i_t, a_s)$. But there is only one codeword with exactly one 1 in the first k coordinates in coordinate t. Therefore, $a_t = a_s$. This implies $d = 2$, which is a contradiction. If σ is acting on $\{k+1, \ldots, 2k = n\}$, then we have a similar discussion since $H_c = (A^t, I_k)$ generates C as well. □

In order to standardize a generator matrix of a code we can use the well-known Gauß elimination, which allows to add rows to each other and the change of rows (note that column change is not allowed).

Theorem 2. *Let C be a binary self-dual (n, k, d)-code with $d \geq 4$ and generator matrix $G_C = (I_k, A)$. Then $\sigma \in Aut(C) \Leftrightarrow G_C = Gauß(G_c^\sigma)$.*

 doi:10.20944/preprints202506.2100.v1

Proof. First, we prove the direction $\Rightarrow$: Applying σ to the columns of G_C, we get a matrix in non-standard form. (By Theorem 1 we know that σ cannot act only on A.) We apply now the steps of Gauß elimination in order to achieve I_k on the lefthand side. Since $\sigma \in Aut(C)$, the set of codewords generated by G_C and G_C^σ coincide. Therefore, every codeword with only one 1 in the first k coordinates is uniquely determined. Thus Gauß$(G_C^\sigma) = G_C$. The other direction $\Leftarrow$ follows from the fact that Gauß(G_C^σ) and G_C generate the same code, thus by definition $\sigma \in Aut(C)$. □

4. Small Automorphism Groups

4.1. Automorphism Groups Generated by One Transposition

Let C be a linear code. If $Aut(C) = C_2 = \langle (ab) \rangle$, then there is exactly one transposition (i.e. switch of columns) which fixes the set of codewords of C. In the following we show that this case is impossible if C is a binary self-dual code.

Theorem 3. *Let C be a self-dual binary code of length n and (ab) a transposition acting on the coordinates of C. Then $Aut(C) \neq \langle (ab) \rangle$.*

Proof. We assume indirectly, that there exists $C - (n, k, d)$ self-dual binary code with generator matrix $G_C = (I_k, A)$ and automorphism group isomorphic to $\langle \sigma = (ab) \rangle$. Without loss of generality, we may assume by Theorem 1 that $a \in \{1, \ldots, k\}$ and $b \in \{k+1, \ldots, 2k = n\}$. With the notations

$$I = \begin{pmatrix} i_1 \\ \vdots \\ i_k \end{pmatrix}, G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \text{ and } A = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix},$$

we then can differ into two cases.

First case, we assume $g_a[b] = 0$. We know that $g_a[a] = 1$ and that there exists $t \neq a$, such that $g_t[b] = 1$. But $g_t[a] = 0$, since $i_t[a] = 0$ iff $t \neq a$. Then $g_t^\sigma[a] = g_t[b] = 1$ and $g_a^\sigma[a] = g_a[b] = 0$. Now, we consider the codeword with $g_t[t] = 1$ and

$$g_t[a] = 1 \text{ and } g_t[j] = 0 \text{ for } j \in \{1, \ldots, k\} \setminus \{t, a\} \tag{1}$$

There is exactly one codeword c with this property. We have $c = g_t + g_a$. Also, g_t^σ fulfills property 1, since $i_t^\sigma[t] = 1, i_t^\sigma[a] = 1$ and $i_t^\sigma[j] = 0 \; \forall j \in \{1, \ldots, k\} \setminus \{t, a\}$. But, $g_t^\sigma[b] = 0$, whereas $g_t[b] + g_a[b] = 1$. Therefore, $c \neq g_t^\sigma$, and we reached a contradiction.

Second case, we assume $g_a[b] = 1$. Since there are at least $d - 1$ 1's in column b, there exists t such that $g_t[b] = 1$. Again, we have $g_a[a] = 1$. Therefore, the codeword $c = g_t + g_a$ is the only codeword with $c[a] = c[t] = 1$ and $c[j] = 0 \; \forall j \in \{1, \ldots, k\} \setminus \{t, a\}$. Since $\mu(g_i, g_j) \equiv 0 \mod 2$, for all possible indices i, j we have that $\mu(a_a, a_t) \geq 2$. Thus, there exists $s \in \{k+1, \ldots, 2k\} \setminus \{b\}$ such that $g_a[s] = g_t[s] = 1$ and thus $c[s] = 0$. But $g_t^\sigma[a] = g_t[b] = 1$, and therefore g_t^σ is the codeword fulfilling $g_t^\sigma[t] = g_t^\sigma[a] = 1$ and $g_t^\sigma[j] = 0 \; \forall j \in \{1, \ldots, k\} \setminus \{t, a\}$. Further, $g_t^\sigma[s] = g_t[s] = 1$, thus $g_t^\sigma \neq c$, therefore we get a contradiction. □

4.2. Automorphism Groups Generated by Exactly One 3-Cycle

Theorem 4. *Let C be a self-dual binary code of length n and (abc) a transposition acting on the coordinates of C. Then $Aut(C) \neq \langle (abc) \rangle$.*

Proof. We may assume that C can be generated by $G_C = (I_k, A)$ and $H_C = (A^T, I_k)$. Then, either in G_C or in H_C, the 3-cycle (abc) is acting on only one column of the identity matrix. Therefore, similarly to the proof of Theorem 3, we get a contradiction. □

 doi:10.20944/preprints202506.2100.v1

5. Self-Dual Codes with Trivial Automorphism Group

In this section we assume, that C is a binary self-dual code with $Aut(C) = \langle 1 \rangle$. This means that for every possible permutation σ on a set of n elements, applying σ to the codewords of C, then there is at least one $c \in C$ such that $c^\sigma \notin C$.

Theorem 5. *Let C be a binary self-dual (n,k,d)-code generated by $G_C = (I_k, A)$. Further, we assume $Aut(C) = \langle 1 \rangle$. Then $\{u \mid u \text{ is a row of } A\} \neq \{v \mid v \text{ is a row of } A^t\}$.*

Proof. We know that G_C and H_C both generate C. Since $Aut(C)$ is trivial, there does not exist a permutation $\sigma \in S_n$ such that $H_C = G_C^\sigma$. Since $(1,k+1)(2,k+2)\dots(k,n)$ is a permutation mapping I_k in G_C to I_k in H_C, there must not exist a permutation mapping the rows of A to the rows of A^t. □

Corollary 1. *If C is a binary self-dual (n,k,d)-code and $Aut(C) = \langle 1 \rangle$. Let $G_C = \begin{pmatrix} I_k & A \end{pmatrix}$ be a generator matrix of C. Then A is not symmetric.*

6. Binary Self-Dual Doubly-Even Code of Length 72

The question if a self-dual binary doubly-even $(72,36,16)$-code exists has its origin in [7]. Doubly even means that all weights of all codewords are divisible by 4. Until today, the highest minimum distance for known binary self-dual codes of length 72 is 12. And the existence of such a code with minimum distance 16 is still unsolved. Over the years, this problem has got some attention among coding theorists, and even monetary prizes were called out for its solution [6]. The automorphisms of a possibly optimal binary self-dual code of length 72 were studied in [8–12]. As the strongest result in this series of studies, the structure of the automorphism group of an optimal binary self-dual code of length 72 can be determined to be one of the following few possibilities.

Theorem 6 ([12])**.** *Let C be a self-dual $(72,36,16)$ code. Then $Aut(C)$ is trivial or isomorphic to $C_2, C_3, C_2 \times C_2$ or C_5.*

In the following we try to put some light on the case if $C - (72,36,16)$ exists with $Aut(C)$ isomorphic to the cyclic group of order 5.

Theorem 7. *Let C be a binary self-dual $(72,36,16)$-code generated by $G_C = (I_{36}, A)$ with $Aut(C) = C_5$ and exactly two fixpoints u and v with $u,v \in \{1,\dots,k\}$ or $u,v \in \{k+1,\dots,2k=n\}$. Then G_C has two rows of weight 16 and no common 1's, i.e. $\mu(g_u, g_v) = 0$.*

Proof. It is clear that if $Aut(C) = C_5$, then at least two coordinates are fix (i.e. not moved by any automorphism), since $Aut(C)$ is generated by a permutation of order 5, i.e. all powers of this permutation act on 5-sets. Further, we assume that there are exactly two fixpoints, u and v and we assume first that $u,v \in \{1,\dots,k\}$. With the notations

$$I = \begin{pmatrix} i_1 \\ \vdots \\ i_{36} \end{pmatrix}, G = \begin{pmatrix} g_1 \\ \vdots \\ g_{36} \end{pmatrix} \text{ and } A = \begin{pmatrix} a_1 \\ \vdots \\ a_{36} \end{pmatrix},$$

and $Aut(C) = \langle \sigma \rangle$ we have $i_u^{\sigma^j} = i_u$ and $i_v^{\sigma^j} = i_v$ for any power j of σ. Since g_u and g_v are the only codewords with exactly one 1 in the first k coordinates, namely in coordinate u (respectively v), we get that $a_u^{\sigma^j} = a_u$ and $a_v^{\sigma^j} = a_v$. Thus the 5-sets on which the powers of σ act under A, are all-1 or all-0 in a_u and a_v. We know that $\mu(a_u, a_v) \equiv 0 \mod 2$ and $w(a_u + a_v) \geq 14 \equiv 2 \mod 4$. Thus, if there are no more fixpoints, then the number of 1's in a_u and a_v are congruent to 0 modulo 5. We need $w(a_i) + 1 \equiv 0 \mod 4 \Rightarrow w(a_i) \equiv 3 \mod 4$. Thus $w(a_u), w(a_v) \in \{35, 15\}$. If $w(a_u) = 35$, then in row v, the 5-sets on which σ is acting consist of either all-1 or all-0. But $\mu(a_u, a_v) \equiv 0 \mod 2$. Therefore, the only possibility

 doi:10.20944/preprints202506.2100.v1

is $w(a_v) = 21$, but then $w(g_v) = 22$, which is a contradiction to the fact, that C is a doubly-even code. Thus $w(a_u) = w(a_v) = 15$ and $\mu(a_u, a_v) = 0$. is the only possibility. For $u, v \in \{k+1, \ldots, 2k = n\}$ the discussion is similar since C can be also generated by $H_C = (A^t, I_{36})$. □

7. Discussion

In this paper, small automorphism groups of binary self-dual codes are investigated and new results are presented. We have proved that the automorphism group cannot be generated by only one cycle permutation, neither of length 2, nor of length 3. No automorphism can act only on one half of the coordinates. Further, some restrictions for binary self-dual codes with trivial automorphism groups are given. These new findings are especially important for the construction of such codes. This question is extremely interesting in cases where the existence of a mutual binary self-dual code is still an open question, like for $n = 72, k = 36, d = 16$. Our current findings on such a code with automorphism group isomorphic to the cyclic group of order 5, can help in the construction of such a code and for exhaustive computational research.

Author Contributions: Conceptualization, C.H.; methodology, C.H. and S.R.M.; formal analysis, S.R.M.; writing—original draft preparation, C.H.; writing—review and editing, C.H. and S.R.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable

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

References

1. Nebe, G.; Rains, E.M.; Sloane, N.J.A. *Self-dual codes and invariant theory*; Vol. 17, Springer: Berlin, 2006.
2. Yorgov, V.; Yorgov, D. The Automorphism Group of a Self-Dual [72, 36, 16] Code Does Not Contain Z_4. *IEEE Transactions on Information Theory* **2014**, *60*, 3302–3307.
3. Conway, J.H.; Pless, V. On the enumeration of self-dual codes. *Journal of Combinatorial Theory, Series A* **1980**, *28*, 26–53.
4. Conway, J.H. A characterisation of Leech's lattice. *Inventiones Mathematicae* **1968**, *7*, 137–142. https://doi.org/10.1007/BF01425459.
5. Dougherty, S.T.; Gulliver, T.A.; Harada, M. Extremal binary self-dual codes. *IEEE Transactions on Information Theory* **1997**, *43*, 2036–2047.
6. https://sites.google.com/site/professorstevendougherty/length72. *Steven Dougherty - Length72*.
7. Sloane, N. Is there a (72, 36) d= 16 self-dual code?(Corresp.). *IEEE Transactions on Information Theory* **1973**, *19*, 251–251.
8. Huffman, W.; Yorgov, V. A [72,36,16] doubly even code does not have an automorphism of order 11 (Corresp.). *IEEE Transactions on Information Theory* **1987**, *33*, 749–752. https://doi.org/10.1109/TIT.1987.1057339.
9. Borello, M. The Automorphism Group of a Self-Dual [72, 36, 16] Binary Code Does Not Contain Elements of Order 6. *IEEE Transactions on Information Theory* **2012**, *58*, 7240–7245.
10. Borello, M.; Willems, W. Automorphisms of order $2p$ in binary self-dual extremal codes of length a multiple of 24. *IEEE Transactions on Information Theory* **2013**, *59*, 3378–3383.
11. Borello, M. The automorphism group of a self-dual [72, 36, 16] code is not an elementary abelian group of order 8. *Finite Fields and Their Applications* **2014**, *25*, 1–7.
12. Borello, M.; Volta, F.D.; Nebe, G. The automorphism group of a self-dual [72, 36, 16] code does not contain S3, A4 or D8. *Advances in Mathematics of Communications* **2013**, *7*, 503–510. https://doi.org/10.3934/amc.2013.7.503.