Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER
PUBLISHER

Research Article

Neighborhoods of Binary Self-Dual Codes

Carolin Hannusch*, **S. Roland Major**

Faculty of Informatics, University of Debrecen, Debrecen, Hungary
Email: hannusch.carolin@inf.unideb.hu

Received: 10 February 2023; **Revised:** 4 April 2023; **Accepted:** 6 July 2023

Abstract: In this paper, we introduce and investigate the neighborhood of binary self-dual codes. We prove that there is no better Type I code than the best Type II code of the same length. Further, we give some new necessary conditions for the existence of a singly-even (56,28,12)-code and a doubly-even (72,36,16)-code.

***Keywords*:** Type I codes, Type II codes, binary self-dual codes, neighborhood

MSC: 94B05

1. Introduction

Neighbors of self-dual codes were first investigated in [1] and [2]. Later, neighbors were used to find extremal (64,32,12) codes in [3] and to find new codes of length 68 in [4]. Recently, the graph of neighboring codes was investigated [5]. In the current paper, we introduce the definition of a neighborhood of binary self-dual codes. The paper is organized as follows: In Section 2, we mention the main definitions and preliminary results that were essential for our work. Section 3 contains some auxiliary results. In Section 4, we investigate the relationship between neighboring self-dual codes and introduce the neighborhood of self-dual codes. In Section 6, we show that equivalent codes can have different neighborhoods. Finally, in Section 7, we give some research problems.

2. Preliminaries

Let $\mathbb{F}_2$ denote the finite field of two elements, and let n be a positive integer. Then, a subspace of $\mathbb{F}_2^n$ is called a *binary linear code*. We denote a linear code by C. Then, its *dual code* $C^\perp$ is defined as

$$C^\perp = \left\{ x \in \mathbb{F}_2^n \middle| x \cdot c = 0 \ \forall c \in C \right\},$$

where $\cdot$ denotes the usual scalar product of two vectors. A code is called *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$. It is a well-known fact that the dimension of a self-dual code of length n is $\frac{n}{2}$, as for each linear code C, we have $\dim(C) + \dim\left(C^\perp\right) = n$, where $\dim(C)$ denotes the dimension of C as a vector space.

DOI: https://doi.org/10.37256/cm.4420232397

The *weight* of a codeword $c \in C$, denoted by $w(c)$ is the number of its nonzero coordinates. The *minimum weight* (or *minimum distance*) of a code C is the smallest nonzero weight of its codewords. We denote the minimum distance of C by $d(C)$. If a code C is a k-dimensional subspace of $\mathbb{F}_2^n$ with minimum distance d, then we say that C is an (n, k, d) -code.

Self-dual binary codes can be classified into Type I and Type II codes [6, 7]. A self-orthogonal binary code C is said to be *doubly-even* if all of its codewords have weight divisible by 4. If C has a codeword of weight not divisible by 4, then C is a singly-even code [8]. Singly-even self-dual codes are called Type I codes and doubly-even self-dual codes are called Type II codes [7]. It is well known that Type II codes only exist for length divisible by 8 [9].

We know that the minimum distance of a binary self-dual code is bounded by $d(C) \leq 2\left\lfloor \frac{n}{8} \right\rfloor + 2$ if C is a Type I code and $d(C) \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ if C is a Type II code [1, 9]. If a code reaches equality in this bound, then the code is called extremal. Especially for larger codelengths it seems that equality cannot be reached in many cases. Codes with the highest possible minimum distance are called optimal codes. The search for extremal and optimal binary codes is a difficult task for many codelengths n and several researchers have contributed to this theory (see e.g., [10, 11]). There are still many open problems about extremal and optimal binary codes [7].

3. Auxiliary results

Let a and b be two codewords (i.e., binary vectors) of the same length. We denote the numbers of coordinates, which are 1 in both codewords by $\mu(a, b)$, i.e.,

$$\mu(a,b) = \#\{i \mid a[i] = b[i] = 1, i \in \{1, \ldots, n\}\}.$$

The weight of the sum of two vectors is the following:

$$w(a+b) = w(a) + w(b) - 2\mu(a,b).$$

Lemma 1. Let a,b and c be vectors of the same length. Then, $\mu(a+b,c) = \mu(b,c) + \mu(a,b+c) - \mu(a,b)$.

Proof. Using the following equations in the given order, the proposition can be directly shown:

1. $w(a+b+c) = w(a+b) + w(c) - 2\mu(a+b,c)$
2. $w(a+b) = w(a) + w(b) - 2\mu(a,b)$
3. $w(a+b+c) = w(a) + w(b+c) - 2\mu(a,b+c)$
4. $w(b+c) = w(b) + w(c) - 2\mu(b,c)$

3.1 *Neighbors and neighborhoods*

The definition of neighbors among self-dual codes was introduced as follows:

Definition 2. Two self-dual codes of length n are called neighbors, provided their intersection is a code of dimension $\frac{n}{2} - 1$.

It is well known that a Type I code has a maximal doubly-even subcode of codimension 1 [1, 2]. Throughout the paper, we will denote this maximal doubly-even subcode by $C_{\max}$, further we denote the all-1 codeword by 1. If C is a self-dual code of even, then $1 \in C$, since $\forall c \in C$, we have $c \cdot c = 0$, which implies $w(c) \equiv 0 \bmod 2$, and therefore, $c \cdot 1 = 1$.

We know by [1] and [2] that if C is Type I, then it has two Type II neighbors.

Investigating the neighbors of self-dual codes leads us to some interesting facts about the relationship between neighboring codes. We find out that codes with the same maximal subcode have a special relationship with each other. Therefore, we come up with the definition of a neighborhood for binary self-dual codes.

We extend the definition of neighbors to a set of codes, which are pairwise neighbors. We will call this set of codes a neighborhood.

Definition 3. Let $C_{\max}$ be a self-orthogonal code of length *n*, and dimension $\frac{n}{2}-1$. Then, there exist three self-dual codes C_1, C_2, and C_3, which contain $C_{\max}$ as a maximal subcode of codimension 1, i.e., they are pairwise neighbors. Then, we say that $\{C_1, C_2, C_3\}$ are a neighborhood of codes. We will denote this set by $\mathcal{N}$.

Remark 4. The neighborhood $\mathcal{N}$ of a doubly-even self-dual code of length divisible by 8 always consists of three codes, one of Type I and two of Type II.

Proof. Let $\mathcal{N}=\{C_1,C_2,C_3\}$ be a neighborhood with $C_1=\langle C_{\max},\gamma_1\rangle$, $C_2=\langle C_{\max},\gamma_2\rangle$, and $C_3=\langle C_{\max},\gamma_1+\gamma_2\rangle$ for some $\gamma_1,\gamma_2\in C_{\max}^{\perp}$. Since C_1, C_2, and C_3 are self-dual, we immediately get that $\gamma_1 \perp/\gamma_2$, thus $\mu(\gamma_1,\gamma_2)\equiv 1 \bmod 2$. Since $w(c)\equiv 0 \bmod 4$ and $\forall c\in C_{\max}$, $2\mu(c,\gamma_1+\gamma_2)\equiv 0 \bmod 4$, and $2\mu(c+\gamma_1,\gamma_2)\equiv 2 \bmod 4$, we have by $w(c+\gamma_1+\gamma_2)\equiv w(c)+w(\gamma_1+\gamma_2)-2\mu(c,\gamma_1+\gamma_2)\equiv w(c+\gamma_1)+w(\gamma_2)-2\mu(c+\gamma_1,\gamma_2)$ that $w(\gamma_1+\gamma_2)\equiv w(c+\gamma_1)+w(\gamma_2)+2 \bmod 4$. This implies that if one of the codewords $\gamma_1+\gamma_2$, $c+\gamma_1$ and γ_2 is doubly-even, then among the other two codewords exactly one is doubly-even and one is singly-even.

In the following, we investigate the minimum distances of three members of a neighborhood $\mathcal{N}$ and their relations. First, it turns out that if the Type I member of a neighborhood $\mathcal{N}$ has a minimum distance 2, then the minimum distance of the two Type II members coincides.

Theorem 5. Let $\mathcal{N}$ be a neighborhood of binary self-dual codes of length divisible by 8. If the singly-even member of $\mathcal{N}$ has a minimum distance 2, then the minimum distance of the doubly-even members coincides.

Proof. We denote the members of $\mathcal{N}$ by C_1, C_2, and C_3. Their coinciding doubly-even subcode will be denoted by $C_{\max}$. Then, $C_1=\langle C_{\max},\gamma_1\rangle$, $C_2=\langle C_{\max},\gamma_2\rangle$, and $C_3=\langle C_{\max},\gamma_1+\gamma_2\rangle$ for suitable $\gamma_1,\gamma_2\in C_{\max}^{\perp}$. Furthermore, we assume that $w(\gamma_2)\equiv w(\gamma_1+\gamma_2)\equiv 0 \bmod 4$. Since $\mu(\gamma_2,\gamma_1+\gamma_2)\equiv 1 \bmod 2$, we have $w(\gamma_1)\equiv 2 \bmod 4$. Thus, C_1 is a singly-even code, and C_2 and C_3 are doubly-even codes. By assumption, we have $d(C_1)=2$, and thus, we can choose γ_1 such that $w(\gamma_1)=2$. Let us denote the minimum distance of C_2 by *d*. Then, we have for all $c\in C_{\max}$,

$$d\le w(c+\gamma_2)\le n-d.$$

We know

$$w(c+\gamma_1+\gamma_2)=w(c+\gamma_2)+w(\gamma_1)-2\mu(c+\gamma_2,\gamma_1).$$

Since $c+\gamma_2$ and γ_1 cannot be orthogonal, we have $\mu(c+\gamma_2,\gamma_1)=1$. Thus, $w(c+\gamma_1+\gamma_2)=w(c+\gamma_2)$ for all $c\in C_{\max}$, which implies $d(C_3)=d$.

Theorem 6. Let $\mathcal{N}=\{C_1,C_2,C_3\}$ be a neighborhood of self-dual codes of length divisible by 8. We assume that C_1 is Type I, and C_2 and C_3 are Type II. Then, $d(C_1)\le \max\{d(C_2),d(C_3)\}$.

Proof. For technical reasons and to keep the proof as simple as possible, we assume now that $C_1=\langle C_{\max},\gamma_1+\gamma_2\rangle$ is a singly-even code and $C_2=\langle C_{\max},\gamma_1\rangle$ and $C_3=\langle C_{\max},\gamma_2\rangle$ are doubly-even codes.

We assume indirectly that $d(C_1)>\max\{d(C_2),d(C_3)\}$. The assumption implies immediately $d(C_{\max})>\max\{d(C_2),d(C_3)\}$, and since $C_{\max}$ is doubly-even, we may assume that $d(C_{\max})\ge d+4$ and $d(C_1)\ge d+2$ for some $d\equiv 0 \bmod 4$. Then, for any $c_i\in C_{\max}$, we have

$$d+2\le w(c_i+\gamma_1+\gamma_2)\le n-d-2$$

and

$$d\le w(c_i+\gamma_1)\le n-d.$$

Further, we may assume $w(\gamma_1)=d$ and $w(\gamma_2)=\delta_1$, where $\delta_1\le d$.

Let $c_1\in C_{max}$ be such that $w(c_1+\gamma_1)=n-d$ and $\delta_1-2\mu(c_1+\gamma_1,\gamma_2)\ge 2$. (Such an element c_1 exists since $w(\gamma_2)=\delta_1\equiv 0 \bmod 4$ and $\mu(c_1+\gamma_1,\gamma_2)\equiv 1 \bmod 2$.) Then, $w(c_1+\gamma_1+\gamma_2)=w(c_1+\gamma_1)+w(\gamma_2)-2\mu(c_1+\gamma_1,\gamma_2)=n-d+\delta_1-2\mu(c_1+\gamma_1,\gamma_2)\ge n-d+2$, which is a contradiction.

Corollary 7. There is no better Type I code than the best possible Type II code of the same length.

This answers a question of Rains and Sloane [6] and Conway and Sloane ([1], p.1321, open question 1) who asked what is the smallest n such that a Type I code of length n is better than the best Type II code of the same length. Using the neighborhood approach, we can see that such a code cannot exist. This shows that the neighborhood approach enables us to see binary self-dual codes in a different way and thus to see relations and properties which were not obvious before.

3.2 *The existence of certain self-dual codes*

The existence of a Type I (56,28,12)-code is an open question [12]. It is known that Type II (56,28,12)-code exists [13-15]. Considering our previous results, we come to the following fact:

Corollary 8. If there exists a Type I (56,28,12)-code, then it is a neighbor of a Type II (56,28,12)-code, since 12 is the best possible minimum distance for a self-dual code of length 56.

Another unsolved question is the existence of a doubly-even (72,36,16)-code [12]. By Corollary 7, we can reduce the search of a Type II (72,36,16)-code to the search of a Type I (72,36,14)-code.

Corollary 9. If there exists a Type I (72,36,14)-code, then it has a doubly-even neighbor with greater minimum distance, i.e., it has a Type II (72,36,16)-code as a neighbor.

3.3 *Neighborhood is not unique*

The neighborhood of a self-dual code is not unique for permutation equivalent codes. Equivalent codes can be contained in neighborhoods whose members have different properties (minimum distance). For example, the well-known (24,12,8) Golay code is unique up to permutation equivalence, but it is contained in (at least) two distinct neighborhoods. The first neighborhood is $\mathcal{N}_1 = \{C_1, C_2, C_3\}$, where C_1 and C_2 are two permutation equivalent (24,12,8) -codes and C_3 is a (24,12,2)-code. The second neighborhood is $\mathcal{N}_2 = \{C_4, C_5, C_6\}$, where C_4 is a (24,12,6)-code, C_5 is a (24,12,4)-code, and C_6 is a (24,12,8)-code. Generator matrices for C_1, C_2, C_3, C_4, C_5, and C_6 are the following matrices G_1, G_2, G_3, G_4, G_5, and G_6 respectively.

$$G_1 = \begin{pmatrix} 100000000000111111111001 \\ 010000000000111111000100 \\ 001000000000111000111100 \\ 000100000000101110101010 \\ 000010000000011101011010 \\ 000001000001101000011011 \\ 000000100001011001001101 \\ 000000010001110010010101 \\ 000000001001000101101011 \\ 000000000101101100100101 \\ 000000000011011110000011 \\ 000000000000001011110111 \end{pmatrix} G_2 = \begin{pmatrix} 100000000000111111111001 \\ 010000000000111111000100 \\ 001000000000111000111100 \\ 000100000000101110101010 \\ 000010000000011101011010 \\ 000001000001101000011011 \\ 000000100001011001001101 \\ 000000010001110010010101 \\ 000000001001000101101011 \\ 000000000101101100100101 \\ 000000000011011110000011 \\ 000000000001001011110110 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 100000000001111111111001 \\ 010000000000111111000100 \\ 001000000000111000111100 \\ 000100000000101110101010 \\ 000010000000011101011010 \\ 000001000001101000011011 \\ 000000100001011001001101 \\ 000000010001110010010101 \\ 000000001001000101101011 \\ 000000000101101100100101 \\ 000000000011011110000011 \\ 000000000001000000000001 \end{pmatrix} G_4 = \begin{pmatrix} 100000000000111111111110 \\ 010000000001010110111000 \\ 001000000001010111000110 \\ 000100000001001010110110 \\ 000010000000011110010011 \\ 000001000000010011110101 \\ 000000100000001011001111 \\ 000000010001111010001010 \\ 000000001001011001101100 \\ 000000000101100011011100 \\ 000000000011001101011010 \\ 000000000001101001001001 \end{pmatrix}$$

$$G_5 = \begin{pmatrix} 100000000000111111111110 \\ 010000000001010110111000 \\ 001000000001010111000110 \\ 000100000001001010110110 \\ 000010000000011110010011 \\ 000001000000010011110101 \\ 000000100000001011001111 \\ 000000010001111010001010 \\ 000000001001011001101100 \\ 000000000101100011011100 \\ 000000000011001101011010 \\ 000000000000000110101000 \end{pmatrix} G_6 = \begin{pmatrix} 100000000000111111111110 \\ 010000000001010110111000 \\ 001000000001010111000110 \\ 000100000001001010110110 \\ 000010000000011110010011 \\ 000001000000010011110101 \\ 000000100000001011001111 \\ 000000010001111010001010 \\ 000000001001011001101100 \\ 000000000101100011011100 \\ 000000000011001101011010 \\ 000000000001101111100001 \end{pmatrix}$$

Remark 10. If C is a Type I code, then its maximal doubly-even subcode is unique, thus its neighborhood is unique as well.

4. Conclusion and further research

We are convinced that the investigation of binary self-dual codes through their neighborhoods opens new possibilities, both in finding codes whose existence is not known yet and in understanding the relations between self-dual codes better.

By Theorem 6, we know that the minimum distance of a singly-even self-dual code cannot be greater than the minimum distance of its best doubly-even neighbor, but it can be equal.

There are three non-equivalent (32,16,8) Type I codes [16]. All of them have a doubly-even neighbor with minimum distance 8, which we computed by the program package TORCH [17].

Therefore, the following questions arise, whose solutions may help to solve open questions like the existence of a Type I (56,28,12)-code or a Type II (72,36,16)-code.

Problem 11. Is there a condition for the codelength n, such that the minimum distance of the best Type II code coincides with the minimum distance of its Type I neighbor?

Problem 12. Given a neighborhood $\mathcal{N} = \{C_1, C_2, C_3\}$, is it possible that all three minimum distances coincide, i.e., $d(C_1) = d(C_2) = d(C_3)$?

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Conway JH, Sloane NJ. A new upper bound on the minimal distance of self-dual codes. *IEEE Transactions on Information Theory*. 1990; 36(6): 1319-1333. Available from: https://doi.org/10.1109/18.59931.

[2] Brualdi RA, Pless V. Weight enumerators of self-dual codes. *IEEE Transactions on Information Theory*. 1991; 37(4): 1222-1225. Available from: https://doi.org/10.1109/18.86979.

[3] Chigira N, Harada M, Kitazume M. Extremal self-dual codes of length 64 through neighbors and covering radii. *Designs, Codes and Cryptography*. 2007; 42(1): 93-101. Available from: https://doi.org/10.1007/s10623-006-9018-5.

[4] Dougherty ST, Gildea J, Korban A, Kaya A, Tylyshchak A, Yildiz B. Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes. *Finite Fields and Their Applications*. 2019; 57: 108-127. Available from: https://doi.org/10.1016/j.ffa.2019.02.004.

[5] Dougherty ST. The neighbor graph of binary self-dual codes. *Designs, Codes and Cryptography*. 2022; 90: 409-425. Available from: https://doi.org/10.1007/s10623-021-00985-2.

[6] Rains EM, Sloane N. Self-dual codes. In: Pless VS, Huffman WC. (eds.) *Handbook of coding theory.* Amsterdam: Elsevier; 1998. p.177-294.

[7] Joyner D, Kim J-L. *Selected unsolved problems in coding theory*. Boston: Springer Science & Business Media; 2011.

[8] Huffman WC, Pless V. *Fundamentals of error-correcting codes*. Cambridge University Press; 2012. Available from: https://doi.org/10.1017/CBO9780511807077.

[9] Huffman WC. On the classification and enumeration of self-dual codes. *Finite fields and Their Applications*. 2005; 11(3): 451-490. Available from: https://doi.org/10.1016/j.ffa.2005.05.012.

[10] Kim J-L. New extremal self-dual codes of lengths 36, 38, and 58. *IEEE Transactions on Information Theory*. 2001; 47(1): 386-393. Available from: https://doi.org/10.1109/18.904540.

[11] Bouyuklieva S. Some optimal self-dual codes having automorphisms of order 5. In: *Proceedings IEEE International Symposium on Information Theory*. Lausanne, Switzerland: IEEE; 2002. p.458. Available from: https://doi.org/10.1109/ISIT.2002.1023730.

[12] Dougherty S, Kim J-L, Solé P. Open problems in coding theory. In: Dougherty S, Facchini A, Leroy A, Puczyłowski E, Solé P. (eds.) *Noncommutative rings and their applications*. Contemporary Mathematics; 2015. p.79-99. Available from: https://doi.org/10.1090/conm/634.

[13] Harada M, Saito K. Singly even self-dual codes constructed from Hadamard matrices of order 28. *Australasian Journal of Combinatorics*. 2018; 70(2): 288-296.

[14] Yorgov V. A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Transactions on Information Theory*. 1987; 33(1): 77-82. Available from: https://doi.org/10.1109/TIT.1987.1057273.

[15] Bussemaker FC, Tonchev VD. New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28. *Discrete Mathematics*. 1989; 76(1): 45-49. Available from: https://doi.org/10.1016/0012-365X(89)90286-0.

[16] Bouyuklieva S, Willems W. Singly even self-dual codes with minimal shadow. *IEEE Transactions on Information Theory*. 2012; 58(6): 3856-3860. Available from: https://doi.org/10.1109/TIT.2012.2183114.

[17] Hannusch C, Major SR. Torch: Software package for the search of linear binary codes. In: *IEEE 2nd Conference on Information Technology and Data Science (CITDS)*. Debrecen, Hungary: IEEE; 2022. p.103-106. Available from: https://doi.org/10.1109/CITDS54976.2022.9914052.