Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 105–110*

On an algorithm for classification of binary self-dual codes with minimum distance four

Iliya Bouyukliev iliya@moi.math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria
Maria Dzhumalieva-Stoeva mdzhumalieva@gmail.com
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria

Abstract. An efficient algorithm for classification of binary self-dual codes with minimum distance four is presented.

1 Introduction

The classification of all self-dual codes for a given length is a quite interesting and challenging problem in coding theory. The main methods for classification have two parts - construction and test for equivalence. A detailed bibliography is presented in [7] and [4]. The number of the inequivalent codes grows very fast with respect to the length. After the classification of all binary self-dual codes of length 36 by Harada and Munemasa [6], the problem seemed to be infeasible for the larger lengths. The development of a new approach using an isomorph free generation gave the possibility to classify the codes of length 38 and even more [4]. Now we work on the classification of binary self-dual codes of length 40 (see also [1] and [5]). We consider two subproblems - classification of the codes with minimum distance ≥ 6, and classification of all self-dual $[40, 20, 4]$ codes (for other lengths see [2] and [3]). More than 70 percent of all inequivalent self-dual codes of length n for $n = 36$ and 38 have minimum distance four. That's why the classification of all self-dual $[40, 20, 4]$ codes separately will decrease drastically the complexity of the full classification. In this paper we present an algorithm for isomorph free generation [9] of binary self-dual codes with minimum distance 4 using the self-dual codes of length 36. This algorithm is similar to the recursive algorithm presented in [4] but it has a few essential differences.

Throughout this paper all codes are assumed to be binary. Two binary codes are called *equivalent* if one can be obtained from the other by a permutation of coordinates. The permutation $\sigma \in S_n$ is an *automorphism* of C, if $C = \sigma(C)$ and the set of all automorphisms of C forms a group called the *automorphism group* of C, which is denoted by $Aut(C)$ in this paper. If C has length n, then the number of codes equivalent to C is $n!/|Aut(C)|$.

2 Theoretical base of the algorithm

Let C be a linear $[n,k]$ code and T be a coordinate set of size t. Consider the set $C(T)$ of codewords whose i-th coordinate is 0 if $i \in T$. $C(T)$ is a subcode of C. Shortening $C(T)$ on T gives a code of length $n-t$ called shortened code of C on T. We can puncture C by deleting the same coordinate i in each codeword. The resulting code is still linear, its length is $n-1$, if $d>1$ its dimension is k, and its minimum weight is d or $d-1$. In general a code C can be punctured on a coordinate set T of size t. We denote the resulting code by C^T. The connection between shortened and punctured codes is described in details in [8].

We begin with a proposition about a punctured code of a self-dual code with minimum weight $d \geq 4$.

Proposition 1. *Let C be a binary self-dual $[n, k = n/2, d \geq 4]$, and $C_0 = \{x = (x_1, \dots, x_n) \in C,\ x_{n-1} = x_n\}$. If C_1 is the punctured code of C_0 on the coordinate set $T = \{n-1, n\}$ then C_1 is a self-dual $[n-2, k-1, d_1 \geq d-2]$ code.*

Let G_1 and $G_0 = (G_1\ a^T\ a^T)$ be generator matrices of the codes C_1 and C_0, respectively. Consider the elements of the automorphism group $\mathrm{Aut}(C_1)$ as permutation matrices of order $n-2$. To any permutation matrix $P \in \mathrm{Aut}(C_1)$ we can correspond an invertible matrix $A_P \in \mathrm{GL}(k-1,2)$ such that $G_1' = G_1P = A_PG_1$, since G_1' is another generator matrix of C_1. In this way we obtain a homomorphism $f : \mathrm{Aut}(C_1) \longrightarrow \mathrm{GL}(k-1,2)$. The following theorem was proven in [4] and partly in [6].

Theorem 1. *The matrices $(G_1\ a^T\ a^T)$ and $(G_1\ b^T\ b^T)$ generate equivalent codes if and only if the vectors a and b belong to the same orbit under the action of $Im(f)$ on $\mathbb{F}_2^{k-1}$.*

Now consider the codes with minimum distance 4.

Proposition 2. *Let C be a binary self-dual $[n, k = n/2, 4]$ code and $T = \{i_1, i_2, i_3, i_4\}$ be the support of a codeword of weight 4. If C_0 is the shortened code of C on the set $T1 = \{i_1, i_2\}$ then the punctured code $C_1 = C_0^{T2}$ of C_0 on the set $T2 = \{i_3, i_4\}$ is a self-dual $[n-4, n/2-2, \geq 2]$ code.*

Proof. Let $u, v \in C_1$. Without loss of generality we can suppose that $x = (110\dots011) \in C$ is a codeword of weight 4, $T1 = \{1,2\}$ and $T2 = \{n-1, n\}$. Then $(00, u, \alpha_1, \alpha_2), (00, v, \beta_1, \beta_2) \in C$ for some $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_2$. Since C is a self-dual code, we have $x \cdot (00, u, \alpha_1, \alpha_2) = x \cdot (00, v, \beta_1, \beta_2) = 0$ and therefore $\alpha_1 = \alpha_2 = \alpha$ and $\beta_1 = \beta_2 = \beta$. Moreover

$$(00, u, \alpha, \alpha) \cdot (00, v, \beta, \beta) = 0 \ \Rightarrow\ u \cdot v = 0.$$

It follows that C_1 is a self-orthogonal code. As its dimension is the half of its length, this code is self-dual. □

Corollary 1. *Let C be a binary self-dual $[n, k = n/2, 4]$ code and $x = (110\dots011)$ be a codeword of weight 4. Then C has a generator matrix in the form*

$$G = \begin{pmatrix} 11 & 00\cdots0 & 00\cdots0 & 1 & 1 \\ 01 & 00\cdots0 & v & 0 & 1 \\ 00 & I_{k-2} & A & a^T & a^T \end{pmatrix}$$

where a and v are binary vectors of length $k-2$. The matrix $(I_{k-2}|A)$ generates a self-dual $[n-4, n/2-2]$ code.

Proof. Let $G' = (I_{k-2}|A)$ be a generator matrix of the code C_1 defined in Proposition 2. According to the proof of the above proposition, the self-orthogonal code C_0 has a generator matrix in the form $G_0 = (I_{k-2}|A|a^T a^T)$ for a vector $a \in \mathbb{F}_2^{k-2}$. Then we can take a generator matrix of C in the form

$$\begin{pmatrix} 11 & 00\cdots0 & 00\cdots0 & 1 & 1 \\ 01 & x & y & \alpha & \beta \\ 00 & I_{k-2} & A & a^T & a^T \end{pmatrix} \sim \begin{pmatrix} 11 & 00\cdots0 & 00\cdots0 & 1 & 1 \\ 01 & 00\cdots0 & v & 0 & 1 \\ 00 & I_{k-2} & A & a^T & a^T \end{pmatrix}$$

□

Let us consider the automorphism group $\mathrm{Aut}(C_1)$ of the self-dual $[n-4, n/2-2]$ code C_1 from Corollary 1, and let G_1 be a generator matrix of this code. According to Theorem 1, if the vectors a and b from $\mathbb{F}_2^{k-2}$ belong to the same orbit under the action of $Im(f)$ on $\mathbb{F}_2^{k-2}$, then the matrices $(G_1\ a^T\ a^T)$ and $(G_1\ b^T\ b^T)$ generate equivalent codes. If $P \in \mathrm{Aut}(C_1)$, $x = (0, v)$ and $y = xP$ then

$$G \begin{pmatrix} I_2 & 0 & 0 \\ 0 & P & 0 \\ 0 & 0 & I_2 \end{pmatrix} = \begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & x & 0 & 1 \\ 00 & G_1 & a^T & a^T \end{pmatrix} \begin{pmatrix} I_2 & 0 & 0 \\ 0 & P & 0 \\ 0 & 0 & I_2 \end{pmatrix}$$

$$= \begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & xP & 0 & 1 \\ 00 & G_1P & a^T & a^T \end{pmatrix} = \begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & xP & 0 & 1 \\ 00 & A_PG_1 & A_Pb^T & A_Pb^T \end{pmatrix}$$

$$= \begin{pmatrix} I_2 & 0 \\ 0 & A_P \end{pmatrix} \begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & y & 0 & 1 \\ 00 & G_1 & b^T & b^T \end{pmatrix}$$

Hence the code C is equivalent to the code generated by the matrix

$$G' = \begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & y & 0 & 1 \\ 00 & G_1 & b^T & b^T \end{pmatrix}.$$

3 Description of the algorithm

We use the concept for a canonical representative and a canonical representative map as this is defined in [4]. The symmetric group S_n partitions the set of all self-dual codes of length n into orbits (or equivalence classes). The canonical representative map defines one special code in any equivalence class called the canonical representative of this class. We denote the set of all canonical permutations of C by $L(C)$. It is easy to see that $L(C)$ is a coset of the automorphism group $\mathrm{Aut}(C)$ in the symmetric group S_n.

Let B be a self-dual $[2k-4, k-2]$ code and $\overline{B}$ be a $[2k, k, 4]$ code obtained from B by the above construction. Let x be the vector of weight 4 in the canonical representative of $\overline{B}$ which is lexicographically first within the set of codewords of weight 4, and let (i_1, i_2, i_3, i_4) be its support, $1 \le i_1 < i_2 < i_3 < i_4 \le n$. We say that $\overline{B}$ passes the parent test if there is a permutation $\tau \in L(\overline{B})$ such that $\{\tau(1), \tau(2)\} = \{i_1, i_2\}$ or $\{i_3, i_4\}$.

Lemma 1. *If $\overline{B}_1$ and $\overline{B}_2$ are two equivalent self-dual $[2k, k, 4]$ codes which pass the parent test, then the self-dual $[2k-4, k-2]$ codes B_1 and B_2 are also equivalent.*

Proof. Since $\overline{B}_1$ and $\overline{B}_2$ are equivalent, they have the same canonical representative B. Then there are permutations $\tau_1 \in L(\overline{B}_1)$ and $\tau_2 \in L(\overline{B}_2)$ such that $\{\tau_1(1), \tau_1(2)\} = \{i_1, i_2\}$ or $\{i_3, i_4\}$, $\{\tau_2(1), \tau_2(2)\} = \{i_1, i_2\}$ or $\{i_3, i_4\}$, where (i_1, i_2, i_3, i_4) is the support of the weight 4 codeword $x \in B$ which is lexicographically first within the set of codewords of weight 4. For the permutation $\tau_2^{-1}\tau_1 : \overline{B}_1 \to \overline{B}_2$ we have $\{\tau_2^{-1}\tau_1(1), \tau_2^{-1}\tau_1(2)\} = \{1, 2\}$ or $\{n-1, n\}$, and $3 \le \tau_2^{-1}\tau_1(i) \le n-2$ for $3 \le i \le n-2$. Hence the restriction of $\tau_2^{-1}\tau_1(1)$ on the positions $3, 4, \ldots, n-2$ maps B_1 to B_2 and so these two codes are equivalent. $\square$

Theorem 2. *If the set U_s consists of all inequivalent binary self-dual $[2s, s]$ codes, then the set V_{s+2} obtained by the algorithm presented in Table 1 consists of all inequivalent self-dual $[2s+4, s+2, 4]$ codes, $s \ge 1$.*

Proof. We must show that the set V_{s+2} filled out in Procedure Augmentation, consists only of inequivalent codes, and any binary self-dual $[2s+4, s+2, 4]$ code is equivalent to a code in the set V_{s+2}.

Obviously, any self-dual $[2s+4, s+2, 4]$ code is equivalent to a code obtained by the above construction. Suppose that the codes $\overline{B}_1, \overline{B}_2 \in V_{s+2}$ are equivalent. Since these two codes have passed the parent test, the codes B_1 and B_2 are also equivalent according to Lemma 1. But the set U_s consists only in inequivalent codes. We have a contradiction here and therefore the codes $\overline{B}_1, \overline{B}_2 \in V_{s+2}$ cannot be equivalent. It follows that V_{s+2} consists of inequivalent codes.

Take now a binary self-dual $[n = 2s+4, s+2, 4]$ code C with a canonical representative B. Let $x \in B$ be the vector of weight 4 which is lexicographically first within the set of codewords of weight 4, and let (i_1, i_2, i_3, i_4) be its support,

$1 \le i_1 < i_2 < i_3 < i_4 \le n$. Consider the permutation $\sigma \in S_n$ defined by $\sigma(i_1) = 1$, $\sigma(i_2) = 2$, $\sigma(i_3) = n-1$, $\sigma(i_4) = n$, $\sigma(j) = j$ for $j = 3, \dots, n-2$. Obviously, the code $\sigma(B)$ is a self-dual $[n = 2s+4, s+2, 4]$, equivalent to C, which can be obtained by the above construction and which passes the parent test. There is a code $D \in U_s$ equivalent to the code obtained from $\sigma(B)$ by Proposition 2.

Hence B is equivalent to C and B passes the parent test. Since U_s consists of all inequivalent self-dual codes of dimension s, the parent of B is equivalent to a code $A \in U_s$. According to Lemma 1, there is a child type code B_A of A, equivalent to B, such that B_A passes the parent test. Since the codes B and B_A are equivalent, so are the codes C and B_A. In this way we find a code in V_{s+2} which is equivalent to C. $\square$

Table 1: The main algorithm

```
Procedure Augmentation(A: binary self-dual code);
begin
    Find the set Child(A) of all inequivalent child type codes of A with d = 4;
         (using already known Aut(A))
    For all codes B from the set Child(A) do the following:
          if B passes the parent test then
             begin
                V_{s+2} := V_{s+2} ⋃ B;
                PRINT(B, Aut(B));
             end;
end;
```

```
Procedure Main;
Input:    U_s – nonempty set of binary self-dual [2s, s] codes;
Output: V_{s+2} – set of [2s+4, s+2, 4] binary self-dual codes;
begin
   V_{s+2} := ∅;
   for all codes A from U_s do the following:
   begin
      find the automorphism group of A;
      Augmentation(A);
   end;
end.
```

Acknowledgments. The authors would like to thank Prof. Stefka Bouyuklieva for her help, useful discussions and valuable advices.

References

[1] K. Betsumiya, M. Harada and A. Munemasa, A complete classification of doubly even self-dual codes of length 40, preprint, [arXiv:1104.3727].

[2] R.T. Bilous, Enumeration of the binary self-dual codes of length 34, J.Combin. Math. Combin. Comput. 59 (2006), 173-211.

[3] R.T. Bilous, G.H.J. Van Rees, An enumeration of binary self-dual codes of length 32, Designs, Codes and Cryptography, 26 (2002), 61-68.

[4] S. Bouyuklieva and I. Bouyukliev, An algorithm for classification of binary self-dual codes, *IEEE Trans. Inform. Theory*, (to appear), arXiv:1106.5930.

[5] S. Bouyuklieva, I. Bouyukliev and M. Harada, Some extremal self-dual codes and unimodular lattices in dimension 40, preprint, [arXiv:1111.2637].

[6] M. Harada and A. Munemasa, Classification of self-dual codes of length 36, *Adv. Math. Commun.* (to appear), [arXiv:1012.5464].

[7] W.C.Huffman, On the Classification and enumeration of self-dual codes, Finite Fields Appl. 11 (2005), 451-490.

[8] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge Univ. Press, 2003.

[9] B. D. McKay, Isomorph-free exhaustive generation, *J. Algorithms* 26 (1998), 306–324.