On an Algorithm for Classification of Binary Self-dual Codes with Minimum Distance Four

Iliya Bouyukliev, Mariya Dzhumalieva-Stoeva

Institute of Mathematics and Informatics
Bulgarian Academy of Science

Pomorie 2012

Main Problem

1. Classification of all self-dual codes for a given length.

2. Classification of all self-dual codes for a given length and minimum distance 4.

History

1975	Vera Pless – $n \leq 20$
1980-90	Conway, Pless, Sloane – $n \leq 30$
2006	Bilous, Van Rees – $n = 32, 34$
2008	Melchor, Gaborit – $n = 36$ (Optimal)
2011	Harada, Munemasa – $n = 38$ (Optimal)
2011	Harada, Munemasa; C. Aguilar-Melchor, Ph. Gaborit, Jon-Lark Kim, L. Sok, P. Sole – $n = 38$ (Optimal)
2011	Bouyuklieva, Bouyukliev – $n = 38$
2011	Betsumiya, Harada, Munemasa – $n = 40$ (Doubly even)
2011	Bouyuklieva, Bouyukliev – $n = 40$ (Optimal)

Number of inequivalent codes

If U is the set of all inequivalent self-dual codes of length n and minimum distance $\leq d$, then

$$\sum_{C\in U} \frac{n!}{|Aut(C)|} \,|\,\{x \in C | wt(x) = d\}\,| = \binom{n}{d} \prod_{i=1}^{n/2-2} (2^i + 1).$$

Aim

n	$\sharp$	$d=2$	$d=4$	$d=6$	$d=8$
20	16	9	7		
22	25	16	8	1	
24	55	25	28	1	1
26	103	55	47	1	
28	261	103	155	3	
30	731	261	457	13	
32	3 295	731	2 482	74	8
34	24 147	3 295	19 914	938	
36	519 492	24 147	436 633	58 671	41
38	38 682 183	519 492	27 463 982	10 695 965	2 744
40	?	38 682 183	?	?	10 184 954

Main Construction

Let C be a binary self-dual $[n, k = n/2, 4]$ code and $x = (110\ldots011)$ 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 C_1.

Equivalence

Let $Aut(C_1)$ be the automorphism group of the self-dual $[n-4, n/2-2]$ code C_1 from the main construction, and let G_1 be the generator matrix of this code. If a and b belong to the same orbit under the action of $Aut(C_1)$ on $\mathbb{F}_2^{k-2}$, then the matrices

$$\begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & x & 0 & 1 \\ 00 & G_1 & a^T & a^T \end{pmatrix}, \quad \begin{pmatrix} 11 & 00\cdots0 & 1 & 1 \\ 01 & y & 0 & 1 \\ 00 & G_1 & b^T & b^T \end{pmatrix}$$

generate equivalent codes.

Parent test

- B - self-dual $[2k-4, k-2]$ code;
- $\overline{B}$ - $[2k, k, 4]$ code obtained from B;
- $\rho(\overline{B})$ - canonical representative of $\overline{B}$;
- $L(\overline{B})$ - set of all canonical permutations of $\overline{B}$;

$$\sigma : \overline{B} \mapsto \rho(\overline{B}), \sigma \in L(\overline{B})$$

Parent test

- x - vector of weight 4 in $\rho(\overline{B})$ which is lexicographically first within the set of codewords of weight 4;
- (i_1, i_2, i_3, i_4) - support of x, $1 \leq i_1 < i_2 < i_3 < i_4 \leq n$.

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 $\{i_3, i_4\}$.

Parent test

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.

Algorithm

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
  $V_{s+2} := \emptyset$;
  for all codes A from U_s do the following:
  begin
    find the automorphism group of A;
    Augmentation(A);
  end;
end;

Algorithm

Procedure Augmentation(A: binary self-dual code);
begin
Find the set $Child(A)$ of all inequivalent child type codes of A;
(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
$V_{s+2} := V_{s+2} \bigcup B$;
PRINT(B, $Aut(B)$);
end;
end;

Algorithm

Theorem 1 *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 consists of all inequivalent self-dual* $[2s+4, s+2, 4]$ *codes,* $s \geq 1$.

As a conclusion

Optimal self-dual codes

[38,19,8]	2 744
[40,20,8]	10 184 954
[42,21,8]	??
[44,22,8]	?
[46,23,10]	1
[48,24,12]	1