Classification of Binary Linear Codes with Minimum distance 8

Iliya Bouyukliev[1] Erik Jacobsson[2]

[1]Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

[2]Department of Mathematical Sciences
University of Gothenburg/Chalmers University of Technology

Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2010

Objectives

First, we classify all binary linear codes with minimum distance 8 and codimension up to 14.

n/k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
11	**11**	7	6	5	4	4	3	2	2	2	1			
12	**12**	**8**	6	6	4	4	4	3	2	2	2	1		
13	**13**	**8**	7	6	5	4	4	4	3	2	2	2	1	
14	**14**	**9**	**8**	7	6	5	4	4	4	3	2	2	2	1
15	**15**	**10**	**8**	**8**	7	6	5	4	4	4	3	2	2	2
16	16	**10**	**8**	**8**	**8**	6	6	5	4	4	4	2	2	2
17	17	11	**9**	**8**	**8**	7	6	6	5	4	4	3	2	2
18	18	12	10	**8**	**8**	**8**	7	6	6	4	4	4	3	2
19	19	12	10	9	**8**	**8**	**8**	7	6	5	4	4	4	3
20	20	13	11	10	9	**8**	**8**	**8**	7	6	5	4	4	4
21	21	14	12	10	10	8	**8**	**8**	**8**	7	6	5	4	4
22	22	14	12	11	10	9	8	**8**	**8**	**8**	7	6	5	4
23	23	15	12	12	11	10	9	8	**8**	**8**	**8**	7	6	5
24	24	16	13	12	12	10	10	8	8	**8**	**8**	**8**	6	6
25	25	16	14	12	12	11	10	9	8	8	**8**	**8**	6	6
26	26	17	14	13	12	12	11	10	9	8	8	**8**	7	6
27	27	18	15	14	13	12	12	10	10	9	8	8	**8**	7
28	28	18	16	14	14	12	12	11	10	10	8	8	8	**8**

Objectives

Second, we prove the non-existence a $[33, 18, 8]$ code.

n/k	14	15	16	17	18	19	20	21	22	23	24	25	26	27
32	8-**9**	8	8	8	6-**7**	6	6	6	5	4	4	4	4	2
33	9-**10**	8-**9**	8	8	7-**8**	6-**7**	6	6	6	5	4	4	4	3
34	10	9-**10**	8-**9**	8	8	7-**8**	6-**7**	6	6	6	4	4	4	4
35	10	10	9-**10**	8	8	8	7-**8**	6-**7**	6	6	5	4	4	4
36	11	10	10	8-9	8	8	8	7-**8**	6-**7**	6	6	5	4	4
37	12	10-11	10	9-10	8-9	8	8	8	7-**8**	6-**7**	6	6	5	4
38	12	11-12	10-11	10	9-10	8-9	8	8	8	6-**8**	6-**7**	6	6	5
39	12	12	11-12	10-11	10	9-10	8-9	8	8	7-8	6-**8**	6-**7**	6	6
40	12-13	12	12	11-12	10-11	10	9-10	8-9	8	8	7-8	6-**8**	6-**7**	6
41	12-14	12-13	12	12	11-12	10-11	10	9-10	8-9	8	8	7-8	6-**8**	6
42	13-14	12-14	12-13	12	12	11-12	10	10	8-10	8-9	8	8	7-8	6-7

Preliminaries

Notation

$[n, k, d]^{d^\perp}$ *is an* $[n, k, d]$ *code with dual distance* $d^\perp$.

Definition

$n_2(k, d) =$ *the minimum length such that there exists a binary* $[n, k, d]$ *code.*

Definition

$d_2(n, k) =$ *the largest value of* d *such that there exists a binary* $[n, k, d]$ *code.*

Codes with parameters $[n_2(k, d), k, d]$ or $[n, k, d_2(n, k)]$ are called optimal.

Preliminaries

Definition

$L_2(k, d^\perp)$ = The maximum length n such that there exists a binary $[n, k]^{d^\perp}$ code.

Proposition

Let C be a binary $[n, k, d]^{d^\perp}$ code. Then $d \geq n - L(k-1, d^\perp)$.

In effect this means that we sometimes have a lower bound on the length of the possible residual codes we try to extend.

Preliminaries

Definition

A code C is called even if all its codewords have even weight.

Lemma

If the minimum distance of a linear code is even, then there is an even $[n, k, d]$ code.

Lemma

The parity check matrix of an even code has only odd weight columns.

Preliminaries

Definition (Residual Code)

Let G be a generator matrix of a linear binary $[n, k, d]$ code C and $c \in C$. Then the residual code $Res(C, c)$ of C with respect to c is the code generated by the restriction of G to the columns where c has a zero entry. If c has weight ω we write $Res_\omega(C)$.

Preliminaries

Lemma (Minimum distance of Residual Code)

Suppose C is a binary $[n, k, d]$ code and suppose $c \in C$ has weight ω, where $d > \omega/2$. Then $Res_\omega(C)$ is an $[n - \omega, k - 1, d']$ code with $d' \geq d - \omega + \lceil \omega/2 \rceil$.

Lemma (Dual distance of Residual Code)

Suppose C is a binary $[n, k, d]$ code with dual distance $d^\perp$, $c \in C$, and the dimension of $Res(C, c)$ is $k - 1$. Then the dual distance of $Res(C, c)$ is at least $d^\perp$.

Preliminaries

Proposition

A linear code has minimum weight d if and only if its parity check matrix has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns.

In the case of fixed minimum distance, it is therefore quite natural to instead consider extension of the parity check matrices.
For example, the extension

$$[n-1, k-1, d] \implies [n, k, d]$$

can then be viewed as the one coordinate extension

$$[n-1, k]^d \implies [n, k]^d$$

with fixed dual distance.

Extension algorithm BRUTEFORCE

Algorithm

INPUT: C_{inp} := *the set of all inequivalent* $[n,k]^{d^\perp}$ *codes represented by their generator matrices.*
OUTPUT: C_{out} := *the set of all inequivalent* $[n+1,k]^{d^\perp}$ *codes.*
Variable: A := *array of all* 2^k-1 *nonzero* k*-dimensional column vectors.*

For any code C in C_{inp} with generator matrix G do the following:

1. Delete all linear combinations of $d^\perp-2$ vectors from G from A.
2. For all vectors remaining in A, extend G with one coordinate to G'. If there are no codes in C_{out} equivalent to C' (generated by G'), add C' to C_{out}.

Classification results

With the algorithm BRUTEFORCE we construct all codes with length $n \leq 28$, dimension $k \leq 14$ and dual distance at least 8.

TABLE 1 - Classification results for $[n, k]^{d^{\perp} \geq 8}$ codes

n \ k	**14**	**13**	**12**	**11**	**10**	**n \ k**	**14**	**13**	**12**	**11**	**10**
10	0	0	0	0	1*	**19**	450	30	1	0	0
11	0	0	0	1*	4*	**20**	1863	27	1	0	0
12	0	0	1*	5*	1	**21**	11497	13	1	0	0
13	0	1*	6*	3	0	**22**	46701	10	1	0	0
14	1*	7*	7*	1	0	**23**	40289	9	1	0	0
15	8*	14*	4	1	0	**24**	5177	10	1	0	0
16	24*	16	5	1	0	**25**	536	8	0	0	0
17	50*	23	5	0	0	**26**	274	0	0	0	0
18	131	39	2	0	0	**27**	1	0	0	0	0
19	450	30	1	0	0	**28**	1	0	0	0	0

Extension from residual codes

Suppose there exists a $[33, 18, 8]$ code (WLOG we may assume it is even).

Then there exist even $[32, 17, 8]$ codes.

The duals are then $[32, 15, d]^8$ codes, for some d, whose generator matrices contain only odd weight columns.

Since $L(14, 8) = 28$ we have that $d \geq 32 - 28 = 4$ and from any table of the $d_2(n, k)$ function, $d_2(32, 15) = 8$, so $4 \leq d \leq 8$.

So a $[32, 15]^8$ code will have a residual code with parameters

$$[28, 14, 8]^8 \text{ or } [27, 14, 7]^8 \text{ or } \ldots \text{ or } [24, 14, d \geq 4]^8.$$

From the previous classification results, we know all these.

Extension from residual codes

$$G = \left[\begin{array}{cc|c} 00\ldots0 & 1 & 11\ldots1 \\ & 0 & \\ Res_d(C) & \vdots & X \\ & 0 & \end{array}\right] = \left[\begin{array}{c|c} Residual\ part & \hat{X} \end{array}\right] \quad (1)$$

For each inequivalent residual code $Res_d(C)$, find all possible solutions for $\hat{X}$, such that all sets of 7 (or less) columns from G are linearly independent.

Algorithm EXTEND

Example of EXTEND in the case $[28, 14]^8 \implies [32, 15, 4]^8$

Definition

We call a set of columns $\hat{X}$ proper (relative the residual code $[28, 14, 8]^8$) if all sets of 7 (or less) columns from G (constructed as above) are linearly independent.

I.e., we want to find a proper set of $d - 1 = 3$ columns on the form $(1, x_2, ..., x_{15})^T$.

Let $V^* = \{(1, x_2, ...x_{15})^T : x_i \in \mathbb{F}_2\}$ and delete from V^* all even vectors and all linear combinations of $d^\perp - 2 = 6$ vectors (or less) from the residual part of G to obtain the searchspace

$$V = \{v_1, v_2, ..., v_{N-1}, v_N\}.$$

Algorithm EXTEND

The main idea for the algorithm EXTEND is similar to the strategy for finding the maximum clique in a graph, suggested by Patric Östergård.

Define the vector

$$a = (a_1, a_2, ..., a_{N-1}, a_N)$$

where a_i is the size of the largest proper set in $V_i = \{v_i, ..., v_N\}$.

Observe that $a_N = 1$ and that

$$a_i = \begin{cases} a_{i+1} + 1 & \text{if there is a proper set in } V_i \text{ containing } v_i \\ a_{i+1} & \text{otherwise} \end{cases}$$

Starting with $a_N = 1$ and going backwards through the indices, we look for proper sets in V_i containing v_i.

In the step i, add v_i to the residual part

$$G = \left[\begin{array}{ccc|c} 00\ldots0 & 1 & & 11 \\ & 0 & & \\ Res_d(C) & \vdots & v_i & \\ & 0 & & \end{array}\right] = \left[\begin{array}{c|c} \begin{array}{c} Residual \\ part \end{array} & \hat{X} \end{array}\right] \tag{2}$$

Delete from V_{i+1} all linear combinations of 7 columns from this new residual part, to get a set of possible additional extensions

$$U_i = \{v_{i+k_1}, v_{i+k_2}, ...\} \text{ for some positive } k_1 < k_2 < ... \tag{3}$$

Note that, if $a_{i+k_1} < 2$, we can parse the search here and set $a_i = a_{i+1}$.
If $a_{i+k_1} = 2$ we must investigate further and add, a_{i+k_1} to the residual part, and so on.
When we have gone through all the indices, the size of the largest proper set will be recorded in a_1.

Nonexistence of $[33, 18, 8]$ codes

There are exactly two inequivalent even codes with parameters $[32, 15]^8$.

$$\begin{pmatrix}
10000000000000000000000001111111\\
01000000000000001010101101100011\\
00100000000000000011100001010101\\
00010000000000000011010001011010\\
00001000000000001100010101110100\\
00000100000000011011101011111011\\
00000010000000010111111110111111\\
00000001000000010111110010110000\\
00000000100000010111110100001100\\
00000000010000011010010100101110\\
00000000001000011011000101011101\\
00000000000100011110101101010000\\
00000000000010000110011010011101\\
00000000000001001000110110010111\\
00000000000000100110101100111001
\end{pmatrix}
\text{ or }
\begin{pmatrix}
10000000000000000000000001111111\\
01000000000000001010101101110100\\
00100000000000000011100001010101\\
00010000000000011011100111001110\\
00001000000000010111101011111000\\
00000100000000011000111011000011\\
00000010000000011000111110100100\\
00000001000000011000110010101011\\
00000000100000011000110100010111\\
00000000010000010101010100101110\\
00000000001000011011000101101110\\
00000000000100010001101101100011\\
00000000000010000111110110110000\\
00000000000001000110011010001001\\
00000000000000100110101100101110
\end{pmatrix}$$

None of these can be extended to code with parameters $[33, 15]^8$.

Theorem

Codes with parameters $[33, 18, 8]$ *do not exist and* $n_2(18, 8) = 34$

Thank you for your attention!