Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 20-25*

Minimum lengths for codes with given minimal primal and dual distance

Iliya Bouyukliev iliya@moi.math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
5000 Veliko Tarnovo, BULGARIA
Eric Jacobsson
Department of Mathematical Sciences, University of Gothenburg and
Chalmers University of Technology, S-412 96 Gothenburg, SWEDEN

Abstract. In this paper we study the function $N(d, d^\perp)$. More precisely, we give results for classification and construction of codes which reach, or give upper bounds on $N(d, d^\perp)$.

1 Introduction

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the Galois field $\mathbb{F}_q$. The *Hamming distance* $d(x, y)$ between two vectors $x, y \in \mathbb{F}_q^n$ is defined to be the number of coordinates in which they differ, and accordingly we define the *weight* of a vector $x \in \mathbb{F}_q^n$ to be $wt(x) = d(x, 0)$. A linear q-ary $[n, k, d]$-code is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. We say that the code C has *length* n, *dimension* k and *minimum (primal) distance* d.

Let $(u, v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in the linear space $\mathbb{F}_q^n$. Then $C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \text{ for all } v \in C\}$ is called the *dual code* of the linear code C. It is known that $C^\perp$ is an $[n, n-k, d^\perp]$ code. Also, $d^\perp$ is called the *dual distance* of the code C. If $C \subseteq C^\perp$, C is termed *self-orthogonal* and if $C = C^\perp$, the code is *self-dual*.

Let C_1 and C_2 be two linear $[n, k]_q$ codes. They are said to be *equivalent* if the codewords of C_2 can be obtained from the codewords of C_1 via a sequence of transformations of the following types: (1) permutation on the set of coordinate positions; (2) multiplication of the elements in a given position by a non-zero element of $\mathbb{F}_q$; (3) application of a field automorphism to the elements in all coordinate positions.

One of the main concerns in coding theory is the problem of finding codes with largest possible minimum distance. Many papers study the function $n_q(k, d)$ (the minimum length of linear codes for the given minimum distance d and dimension k) and construction and classification of codes with parameters $[n_q(k, d), k, d]$. A variant of this problem is given by Matsumoto et al. [9]. They

define the function $N(d, d^\perp)$ as the minimal n such that there exist a linear binary code of length n with minimum distance d and dual distance $d^\perp$. They also present some general bounds on the function $N(d, d^\perp)$ and some examples. This problem is directly related to the design method of cryptographic Boolean functions suggested by Kurosawa and Satoh [8].

In this paper we continue to study $N(d, d^\perp)$. More precisely, we give results for classification and construction of codes which reach, or give upper bounds on, $N(d, d^\perp)$. Notice that there are many classification results for $[n_q(k, d), k, d]$ and tables with such results (see for example [6], [7]). But only in some cases they coincide with the codes that achieve $N(d, d^\perp)$.

In this research, we use some theoretical and software tools. These tools are discussed in Section 2. In Section 3, we consider a particular example of classification of codes. In Section 4, we present a table for $N(d, d^\perp)$ when $d \leq 12, d^\perp \leq 12$.

2 Preliminaries and tools

In our methods for construction and classification we use punctured, shortened and residual codes of a given code C.

Proposition 1 *Let C be a linear code with minimum distance d and dual distance $d^\perp$, and C' be the punctured code of C. Then C' has minimum distance at least $d-1$ and dual distance at least $d^\perp$.*

Definition 1 *Let G be a generator matrix of a linear binary $[n, k, d]$ code C. Then the* residual code *$Res(C, c)$ of C with respect to a codeword c is the code generated by the restriction of G to the columns where c has a zero entry.*

If $w = wt(c)$ we will also use the notation $Res_w(C)$. A lower bound on the minimum distance of the residual code is given by

Lemma 2 *([11], Lemma 3.9): Suppose C is a binary $[n, k, d]$-code and suppose $c \in C$ has weight w, where $d > w/2$. Then $Res(C, c)$ is an $[n-w, k-1, d']$-code with $d' \geq d - w + \lceil w/2 \rceil$.*

Proposition 3 *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 also $d^\perp$.*

Let C be a binary $[n, k, d]$ code and B_i denote the number of codewords of weight i in its dual code $C^\perp$.

Lemma 4 *[4]: For a binary $[n, k, d]$ code $B_i = 0$ for each value of i (where $1 \leq i \leq k$) such that there does not exist a binary $[n - i, k - i + 1, d]$ code.*

One of our tools is Q-Extension. We use this program to construct all inequivalent linear codes with length n, dimension k, and minimum distance d, from their residual or shortening codes. In practice, this program gives us options for two types of extensions in the case of codes with fixed dual distance (according to the statements 1-4).

The first approach uses results for the parameters of residuals of codes. Let $\mathbf{G}$ be a generator matrix of a linear $[n, k, d]$ code C. In addition to constructing $[n, k, d]$ codes from their $[n - w, k - 1, d']$ residual codes, one may also start from $[n - i, k, d']$ codes. On the bottom of this hierarchy of extensions is the trivial $[k, k, 1]$ code. In the second approach, $[n, k, d]$ codes are constructed by extending $[n-i, k-i, d]$ or $[n - i - 1, k - i, d]$ codes. If $\mathbf{G}$ is a generator matrix for an $[n - i, k - i, d]$ or an $[n - i - 1, k - i, d]$ code, we extend it (in all possible ways) to

$$\left(\begin{array}{c|c} * & \mathbf{I}_i \\ \hline \mathbf{G} & \mathbf{0} \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} * & \mathbf{1}\ \mathbf{I}_i \\ \hline \mathbf{G} & \mathbf{0} \end{array}\right), \tag{1}$$

respectively, where $\mathbf{I}_i$ is the $i \times i$ identity matrix, $\mathbf{1}$ is an all-1 column vector, and the starred submatrix is to be determined. If we let the matrix $\mathbf{G}$ be in systematic form, we can fix k more columns to get

$$\left(\begin{array}{c|c|c} * & \mathbf{0} & \mathbf{I}_i \\ \hline \mathbf{G}_1 & \mathbf{I}_k & \mathbf{0} \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c|c} * & \mathbf{0} & \mathbf{1}\ \mathbf{I}_i \\ \hline \mathbf{G}_1 & \mathbf{I}_k & \mathbf{0} \end{array}\right). \tag{2}$$

More information on this topic can be found in [1] and in http://www.moi.math.bas.bg/~ iliya/Q_ext.htm.

3 Classification of codes which reach $N(9, 6)$, $N(10, 6)$, $N(12, 6)$ and related results

According to Brouwer's table [28,10,10] and [27,10,9] linear codes with dual distance 5 could exist [2] (there are [27,10,9] and [27,17,5] codes but no [26,17,5] codes exist).

Let C_{27} be a [27,10,9] linear code with dual distance 5. Then we can consider

a generator matrix of C_{27} in the form:

$$G_{27} = \left(\begin{array}{ll} 00000 & \\ \ldots & G_{22} \\ 00000 & \\ \hline 11000 & \\ 10100 & A \\ 10010 & \\ 10001 & \end{array}\right)$$

Adding a parity check bit to this matrix we obtain a generator matrix of a code C_{28} with parameters $[28, 10, 10]$. This generator matrix is:

$$G_{28} = \left(\begin{array}{lll} 00000 & & \\ \ldots & G_{23} & \\ 00000 & & \\ \hline 11000 & & b_7 \\ 10100 & A & b_8 \\ 10010 & & b_9 \\ 10001 & & b_{10} \end{array}\right)$$

where G_{23} generates a [23,6,10] code.

Obviously, if we know all inequivalent codes C_{28} with generator matrix of the form G_{28} we can obtain, after exhaustive search and deleting each coordinate, all inequivalent C_{27}. We can make the following extensions: from [23,6,10] to [25,7,10] and then $[25, 7, 10] \rightarrow [26, 8, 10] \rightarrow [27, 9, 10] \rightarrow [28, 10, 10]$. It is easy to find that there are 29 inequivalent [23,6,10] codes. Using these codes and extension by dimension, we obtain 30522 [25,7,10], 507533 [26,8,10] and 30481 inequivalent [27,9,10] codes. In the end, we construct exactly ten inequivalent codes with parameters [28,10,10] - five with dual distance 5 and five with dual distance 4. One of these was obtained in [10] as a quasi-cyclic code. The number of inequivalent codes with parameters [27,10,9] and dual distance 5 is 137.

Let us consider optimal codes with minimum distance 12. Starting from 91 inequivalent $[15, 5, \geq 6]$ codes, we make the following extensions:

$[15, 5, \geq 6] \rightarrow [27, 6, 12]178 \rightarrow [28, 7, 12]129 \rightarrow [29, 8, 12]73 \rightarrow [30, 9, 12]9 \rightarrow [31, 10, 12]2 \rightarrow [32, 11, 12]2$.

We can conclude that there are exactly two inequivalent $[31, 10, 12]$ codes which have dual distance 5 and transitive automorphism group of order 155 and exactly two inequivalent $[32, 11, 12]$ which have dual distance 6 and transitive automorphism group of order 4960. The codes of dimension 11 have the following spectrum $1 + 496z^{12} + 1054z^{16} + 496z^{20} + z^{32}$.

From Proposition 1 and the results for optimal codes with minimum distance 12, we have: $N(12,6) = 32, N(11,6) = 31, N(10,6) = 30$ and $N(9,6) = 29$. Also $N(12,5) = 31, N(11,5) = 30, N(10,5) \leq 29$ and $N(9,5) \leq 28$. Moreover, there are exactly two inequivalent codes which reach N(11,6), and exactly two inequivalent codes which reach N(11,5).

4 Table of $N(d, d^{\perp})$

The table contains bounds and exact values for $N(d, d^{\perp})$. In the brackets we put the number of inequivalent codes.

$d/d^{\perp}$	3	4	5	6	7	8	9	10	11	12
3	6(1)	-	-	-	-	-	-	-	-	-
4	7(1)	8(1)	-	-	-	-	-	-	-	-
5	11(1)	13(1)	16(1)	-	-	-	-	-	-	-
6	12(1)	14(1)	17(1)	18(1)	-	-	-	-	-	-
7	14(1)	15(1)	20(1)	21(1)	22*(1)	-	-	-	-	-
8	15(1)	16(1)	21(1)	22*(1)	23*(1)	24*(1)	-	-	-	-
9	20(3)	22(1)	27(137)	29($\geq$ 2)	32-37[3]	33-41	38-42	-	-	-
10	21(2)	24(2)	28(5)	30($\geq$ 2)	33-41	34-42	39-43	40-44	-	-
11	23(1)	26(1)	30(2)	31(2)	36-42	37-43	41-44	43-45	46*(1)	-
12	24(1)	28(7)	31(2)	32(2)	37-43	38-44	42-45	44-46	47*(1)	48*(1)

Keynotes:

1. In most of the cases, the lower bounds on $N(d, d^{\perp})$ coincide with the minimum length n_m, for which codes with parameters $[n_m, k, d]$ and $[n_m, n-k, d^{\perp}]$ exist. $N(11,4)$ and $N(12,4)$ are exceptions.

2. The results noted by * are related with the unique [48,24,12] code (see [5]) and the unique [24,12,8] code (see [3]).

3. We have constructed [37,16,9] code with dual distance 7.

Open problem: A binary formally self-dual (f.s.d.) code is a code which has the same weight distribution as its dual code. It is not known whether there is an extremal f.s.d. [40,20,10] code. Existence of a code with such parameters directly leads to an exact value of $N(d, d^{\perp})$.

References

[1] I. Bouyukliev, J. Simonis, Some new results for optimal ternary linear codes, *IEEE Trans. Inform. Theory* 48, 2002, 981-985.

[2] A. E. Brouwer, *Bounds on the size of linear codes*, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam, 1998, 295-461.

[3] S.M. Dodunekov, S.B. Encheva, Uniqueness of some linear subcodes of the extended binary Golay code, *Probl. Pered. Inform.* 29 (1993), 45-51; English transl. in *Probl. Inform. Transm.* 29, 1993, 38-43.

[4] R. Hill, D. E. Newton, Optimal ternary linear codes, *Des., Codes Crypt.* 2, 1992, 137-157.

[5] S. K. Houghten, C. W. H. Lam, L.H. Thiel, J.A. Parker, The extended quadratic residue code is the only (48,24,12) self-dual doubly-even code, *IEEE Trans. Inform. Theory* 49, 2003, 53-59.

[6] D. B. Jaffe, Binary linear codes: new results on nonexistence, http://www.math.unl.edu/ djaffe, 1997, Dept. Math. Stat., Univ. Nebraska, Lincoln.

[7] P. Kaski, P. R. Ostergard, Classification Algorithms for Codes and Designs, Springer, 2006.

[8] K. Kurosawa, T. Satoh, Design of SAC/PC(l) of order k boolean functions and three other cryptographic criteria, in *Adv. Cryptology EUROCRYPTO97*, ser. Lect. Notes Comp. Sci. 1233. Springer-Verlag, 1997, 434-449.

[9] Matsumoto et al., Primal-dual distance bounds of linear codes with application to cryptography, *IEEE Trans. Inform. Theory* 52, 2006, 42514256.

[10] P. Piret, Good linear codes of length 27 and 28, *IEEE Trans. Inform. Theory* 26, 1980, 227.

[11] V. Pless, W. C. Huffman, R. Brualdi, An Introduction to Algebraic Codes, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998, 177-294.