New 6-Dimensional Linear Codes over GF(8) and GF(9)[1]

Rumen N. Daskalov
Department of Mathematics,
Technical University,
5300 Gabrovo, Bulgaria
daskalov@tugab.bg

T. Aaron Gulliver
Department of Electrical and Computer Engeneering,
University of Victoria,
P.O. Box 3055, STN CSC, Victoria,
BC, Canada V8W 3P6
agullive@ece.uvic.ca

Abstract

Let $[n,k,d]_q$ codes be linear codes of length n, dimension k and minimum Hamming distance d over $GF(q)$. In this paper, the existence of the following codes is proven: $[42,6,30]_8$, $[49,6,36]_8$, $[78,6,60]_8$, $[84,6,65]_8$, $[91,6,71]_8$, $[96,6,75]_8$, $[102,6,80]_8$, $[108,6,85]_8$, $[114,6,90]_8$, and $[48,6,35]_9$, $[54,6,40]_9$, $[60,6,45]_9$, $[96,6,75]_9$, $[102,6,81]_9$, $[108,6,85]_9$, $[114,6,90]_9$, $[126,6,100]_9$, $[132,6,105]_9$. The nonexistence of five codes over $GF(9)$ is also proven. All of these results improve the respective upper and lower bounds in Brouwer's table [2].

1 Introduction

Let $GF(q)$ denote the Galois field of q elements, and let $V(n,q)$ denote the vector space of all ordered n-tuples over $GF(q)$. A linear code C of length n and dimension k over $GF(q)$ is a k-dimensional subspace of $V(n,q)$. Such a code is called an $[n,k,d]_q$-code if its minimum Hamming distance is d.

A central problem in coding theory is that of optimizing one of the parameters n, k and d for given values of the other two and q fixed. Two versions are:

Problem 1: Find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d]_q$-code.

Problem 2: Find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d]_q$-code.

A code which achieves one of these two values is called optimal.

[1]This work was supported in part by the Bulgarian National Science Fund and the Natural Sciences and Engineering Research Council of Canada.

For the case of linear codes over $GF(8)$, Problem 2 has been solved for $k \leq 3$ (see [6]). In addition Gulliver and Bhargava [5] constructed many new codes in dimensions $k = 4$ and 5. New codes are also given in [4] and [10]. In this paper we consider $k = 6$, and present nine new quasi-cyclic (QC) linear codes.

For the case of linear codes over $GF(9)$, much less is known. Bierbrauer and Gulliver [1] constructed many new codes in dimensions $k = 4$ and 5. In this paper we consider $k = 6$, and present nine new QC linear codes. In addition, the nonexistence of five codes is proven.

All of these results improve the respective lower and upper bounds in Brouwer's tables [2].

2 Preliminary results

Definition 1 *The dual code $C^{\perp}$ of C is the set of words of length n that are orthogonal to all codewords in C, with respect to the standard inner product.*

Given an $[n, k, d]_q$ code C, we denote by A_i the number of codewords of weight i in C. The ordered $(n+1)$-tuple of integers $\{A_i\}_{i=0}^{n}$ is called the *weight distribution* or *weight enumerator* of C.

Theorem 1 *[8] (MacWilliams' identities)*

Let an $[n, k, d]_q$-code and its dual code have weight enumerators $\{A_i\}_{i=0}^{n}$ and $\{B_i\}_{i=0}^{n}$, respectively. Then

$$\sum_{i=0}^{n} K_t(i) A_i = q^k B_t, \qquad \text{for } 0 \leq t \leq n,$$

where

$$K_t(i) = \sum_{j=0}^{t} (-1)^j \binom{n-i}{t-j} \binom{i}{j} (q-1)^{t-j},$$

are the Krawtchouk polynomials.

Theorem 2 *[7] For an $[n, k, d]_q$-code $B_i = 0$ for each value of i (where $1 \leq i \leq k$) such that there does not exist an $[n-i, k-i+1, d]_q$-code.*

The Linear Programming Bound.

The weight enumerator of an $[n, k, d]_q$-code C is a feasible solution of the following linear program **(LP)**

$$\text{maximize: } L = 1 + \sum_{i=d}^{n} A_i,$$

subject to:

$$\begin{array}{rcll} \sum_{i=d}^{n} K_t(i).A_i & = & -K_t(0) & t = 1,\ldots,d^{\perp}-1 \\ \sum_{i=d}^{n} K_t(i).A_i & \geq & -K_t(0) & t = d^{\perp},\ldots,n \\ A_i & \geq & 0 & i = d,\ldots,n \\ A_i & = & 0 & i \in I \text{ (the set of absent weights).} \end{array}$$

It is clear that if $L_{max} < q^k$, then the code C does not exist.

Quasi-Cyclic Codes.

A code C is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword in C. A cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = mp$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $(m \times m)$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0;\ R_1;\ R_2;\ \ldots;\ R_{p-1}], \tag{1}$$

where $R_i, i = 0, 1, \ldots, p-1$ is a circulant matrix of the form

$$R = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ r_{m-2} & r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{bmatrix}. \tag{2}$$

The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - 1)$ if R is mapped onto the polynomial, $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{m-1} x^{m-1}$, formed from the entries in the first row of R [8]. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [3].

If the defining polynomials $r_i(x)$ contain a common factor which is also a factor of $x^m - 1$, then the QC code is called *degenerate* [3]. Define the *order* of this QC code as [9]

$$h(x) = \frac{x^m - 1}{\gcd\{x^m - 1, r_0(x), r_1(x), \cdots, r_{p-1}(x)\}}. \tag{3}$$

The dimension of the QC code, k, is equal to the degree of $h(x)$. If $h(x)$ has degree m, the dimension of the code is m, and (1) is a generator matrix. If $\deg(h(x)) = k < m$, a generator matrix for the code can be constructed by deleting $m - k$ rows of (1).

For convenience, the coefficients of the defining polynomials are given as integers. For GF(8), $2 = \alpha, 3 = \alpha^2, \ldots, 7 = \alpha^6$, where α is a root of the binary primitive polynomial x^3+x+1. For GF(9), $2=\alpha, 3=\alpha^2, \ldots, 8=\alpha^7$, where α is a root of the ternary primitive polynomial x^2+x+2. The defining polynomials are listed with the lowest degree coefficient on the left, i.e., 4321 corresponds to the polynomial x^3+2x^2+3x+4.

3 Bounds on minimum distance

Theorem 3 *There exist quasi-cyclic codes with parameters:*

$$[42,6,30]_8, [49,6,36]_8, [78,6,60]_8, [84,6,65]_8,$$

$$[91,6,71]_8, [96,6,75]_8, [102,6,80]_8, [108,6,85]_8, [114,6,90]_8.$$

Proof: The coefficients of the defining polynomials of these codes are as follows:

1. A $[42,6,30]_8$-code:
000166, 014246, 014765, 001475, 111616, 111246, 011317;

2. A $[49,6,36]_8$-code:
0114273, 0127353, 0104376, 0126117, 0145662, 0001251, 0001433;

3. A $[78,6,60]_8$-code:
001141, 111246, 011317, 113342, 001077, 116756, 013724, 113255, 015737, 014246, 014765, 001475, 111616;

4. A $[84,6,65]_8$-code:
001247, 111145, 113342, 001077, 116756, 013724, 113255, 015737, 014246, 014765, 001475, 111616, 111246, 011317;

5. A $[91,6,71]_8$-code:
0140453, 0014531, 0166455, 1134632, 0101033, 1232413, 0123157, 0127353, 0104376, 0126117, 0145662, 0001251, 0001433;

6. A $[96,6,75]_8$-code:
001132, 015625, 013373, 111145, 113342, 001077, 116756, 013724, 113255, 015737, 014246, 014765, 001475, 111616, 111246, 011317;

7. A $[102,6,80]_8$-code:
001217, 113133, 015625, 013373, 111145, 113342, 001077, 116756, 013724, 113255, 015737, 014246, 014765, 001475, 111616, 111246, 011317;

8. A $[108,6,85]_8$-code:
001504, 116756, 013724, 001225, 113133, 015625, 013373, 111246, 011317, 111145, 113342, 001077, 113255, 015737, 014246, 014765, 001475, 111616,;

9. A $[114,6,90]_8$-code:
001035, 015452, 001225, 113133, 015625, 013373, 111145, 113342, 001077, 116756, 013724, 113255, 015737, 014246, 014765, 001475, 111616, 111246, 011317;

Table 1: New quasi-cyclic codes over GF(8).

N:	code	d	d_{br}	N:	code	d	d_{br}
1	[42,6]	30	29	6	[96,6]	75	71
2	[49,6]	36	34	7	[102,6]	80	76
3	[78,6]	60	58	8	[108,6]	85	81
4	[84,6]	65	63	9	[114,6]	90	86
5	[90,6]	70	67				

Theorem 4 *There exist quasi-cyclic codes with parameters:*

$$[48,6,35]_9, [54,6,40]_9, [60,6,45]_9, [96,6,75]_9,$$

$$[102,6,81]_9, [108,6,85]_9, [114,6,90]_9, [126,6,100]_9, [132,6,105]_9.$$

Proof: The coefficients of the defining polynomials of these codes are as follows:

1. A $[48,6,35]_9$-code:
000013, 001143, 001144, 013517, 112587, 014857, 128745, 001206;

2. A $[54,6,40]_9$-code:
001538, 127135, 001131, 123685, 112233, 000013, 001041, 123185, 015448;

3. A $[60,6,45]_9$-code:
000013, 123238, 010107, 010832, 001267, 016648, 112367, 016165, 128545, 018754;

4. A $[96,6,75]_9$-code:
016018, 113838, 000105, 112245, 014056, 013673, 112743, 116254, 018158, 116367, 126463, 117345, 016258, 113828, 112185, 138385;

5. A $[102,6,81]_9$-code:
012252, 000017, 111657, 121683, 123823, 113636, 125365, 118535, 014113, 010775, 113743, 113445, 015128, 016883, 015756, 015446, 134647;

6. A $[108,6,85]_9$-code:
112757, 112548, 000113, 010612, 124834, 015881, 017234, 015528, 015661, 131747, 016784, 016572, 017187, 001363, 131628, 121345, 018743, 018838;

7. A $[114,6,90]_9$-code:
000118, 000124, 142746, 146717, 011034, 113182, 018872, 014516, 016884, 111143, 013052, 113176, 113152, 010467, 018878, 123128, 001407, 015887, 124683;

8. A $[126,6,100]_9$-code:
000154, 112434, 113564, 011828, 013252, 012274, 012878, 010311, 016114, 018124, 011525, 014668, 127476, 001482, 001681, 113287, 010726, 017521, 018785, 010331, 014661;

9. A $[132,6,105]_9$-code:
010126, 000011, 001177, 116465, 000001, 117343, 111764, 113643, 111254, 113714, 010247, 001874, 124234, 118638, 011578, 114823, 131464, 113462, 121748, 001351, 117466, 016263;

Table 2: New quasi-cyclic codes over GF(9).

N:	code	d	d_{br}	N:	code	d	d_{br}
1	[48,6]	35	34	6	[108,6]	85	82
2	[54,6]	40	39	7	[114,6]	90	87
3	[60,6]	45	44	8	[126,6]	100	97
4	[99,6]	75	74	9	[132,6]	105	
5	[102,6]	81	79				

Theorem 5 *There do not exist codes with parameters:*

$$[75,6,63]_9, [84,6,71]_9, [93,6,79]_9, [101,6,86]_9, [110,6,94]_9.$$

Proof:

N:	code	source
1	$[75,6,63]_5$	$L_{max} = 503480.10 < 9^6 = 531441$
2	$[84,6,71]_5$	$L_{max} = 448067.56 < 9^6$
3	$[93,6,79]_5$	$L_{max} = 445021.36 < 9^6$
4	$[101,6,86]_5$	$L_{max} = 489425.06 < 9^6$
5	$[110,6,94]_5$	$L_{max} = 472754.51 < 9^6$

Remark: It is very difficult to check the results obtained via the LP bound. However, for every code in Theorem 5 it can be shown explicitly that the MacWilliams' identities have no solution in nonnegative integers.

For example: Let C be a $[75,6,63]_9$ code. By Theorem 2 and [2] $B_1 = B_2 = 0$. Denote the first five MacWilliams' identities by e_0, e_1, e_2, e_3, e_4. Calculating the next linear combination

$$(-5350.e_0 - 5690.e_1/3 - 171.e_2 - 13.e_3 - 4.e_4/9)/243,$$

gives

$$110.A_{64} + 120.A_{65} + 81.A_{66} + 35.A_{70} + 96.A_{71} + 162.A_{72} + 200.A_{73}$$
$$+165.A_{74} + 28431.B_3 + 972.B_4 = -615600,$$

which is a contradiction. Therefore $[75,6,63]_9$ codes do not exist.

References

[1] J. Bierbrauer and T.A. Gulliver, "New linear codes over GF(9)," *Austral. J. Comb.*, **21** (2000), 131–140.

[2] A.E. BROUWER, Linear code bound [electronic table; online], `http://www.win.tue.nl/~aeb/voorlincod.html`.

[3] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs, Codes and Cryptography*, **2** (1992), 81–91.

[4] T.A. Gulliver, "New linear codes of dimensions 5 and 6 over GF(8)," *Ars Combinatoria*, **46**, (2002), 91–96.

[5] T.A. Gulliver and V.K. Bhargava, "New linear codes over GF(8)," *Appl. Math. Lett.*, **13** (2000), 17–19.

[6] R. Hill, "Optimal linear codes," *Cryptography and Coding II*, C. Mitchel, Ed. Oxford, UK: Oxford Univ. Press, (1992), 75–104.

[7] R. Hill and D. E. Newton, "Optimal ternary linear codes," *Designs, Codes & Crypt.*, **2** (1992), 137–157.

[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., New York, NY, 1977.

[9] G.E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes", Technical Report, Royal Military College of Canada, Kingston, ON, 1991.

[10] I. Siap, "New linear codes over $GF(8)$ and improvements on minimum distance," (see references in [2]).