МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2003
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2003
Proceedings of the Thirty Second Spring Conference of
the Union of Bulgarian Mathematicians
Sunny Beach, April 5–8, 2003

IMPROVED MINIMUM DISTANCE BOUNDS FOR LINEAR CODES OVER GF(5)*

Rumen Daskalov, Elena Metodieva

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, nine new codes over $GF(5)$ are constructed and the nonexistence of fifty codes is proved. All of these results improve the respective known lower and upper bounds on the minimum distance in [2].

1. Introduction and preliminary results. 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 $GF(q)$. The Hamming weight of a vector x, denoted by $wt(x)$, is the number of nonzero entries in x. 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 $[n, k, d]_q$-code if its minimum Hamming distance is d. For a linear code, the minimum distance is equal to the smallest of the weights of the nonzero codewords.

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.

For the case of linear codes over $GF(5)$, Problem 2 has been solved for $k \leq 3$ (see [6]). In addition, $n_5(4, d)$ has been found for all but 22 values of d in [1]. Now there are only eight unsolved cases (see [8]) in this dimension. In [4], fourty-four new linear codes over $GF(5)$ were constructed, the nonexistence of twenty linear codes was proven and a table of $d_5(n, k), k \leq 8, n \leq 100$ was presented. Eight new quasi-cyclic (QC) linear codes are constructed and the nonexistence of six codes is proved in [3]. New codes are also given in [10], [11].

In this paper, new QC codes (for the definition and the properties of QC codes see e. g. [3], [4]) are constructed, using a nonexhaustive algebraic-combinatorial computer search. The parameters of these codes are given in Table 1. The minimum distances, d_{br} [2], of the previously best known codes are given for comparison. The nonexistence of many linear codes is also proven.

*2000 Math. Subject Classification: 94B05, 94B65.

This work was partially supported by the Ministry of Education and Science under contract in TU-Gabrovo.

Definition. *The dual code $C^{\perp}$ of C is the set of words of length n that are orthogonal to all codewords in C, w. r. t. the ordinary 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 [9] (the MacWilliams' identities)**.** *Let an $[n,k,d]_5$-code and its dual code have weight enumerators $\{A_i\}_{i=0}^{n}$ and $\{B_i\}_{i=0}^{n}$ respectively. Then*

$$\sum_{i=0}^{n} K_t(i)A_i = 5^k B_t, \qquad \text{for } 0 \le t \le n,$$

where

$$K_t(i) = \sum_{j=0}^{t} (-1)^j \binom{n-i}{t-j}\binom{i}{j} 4^{t-j}$$

are the Krawtchouk polynomials.

Lemma 1 [7]**.** *For an $[n,k,d]_5$-code, $B_i = 0$ for each value of i (where $1 \le i \le k$) such that there does not exist an $[n-i, k-i+1, d]_5$-code.*

Definition. *A $k \times n$ matrix G having as rows the vectors of a basis of a linear code C is called a generator matrix for C.*

Definition. *Let C be an $[n,k,d]_q$-code with generator matrix G and let c be a row of G. The residual code of C with respect to c is the code generated by the restriction of G to the columns where c has a zero entry. The residual code of C with respect to c is denoted $Res(C,c)$ or $Res(C,w)$ if the weight of c is w ($wt(c) = w$).*

Lemma 2 [5]**.** *Let C be an $[n,k,d]_5$-code and $c \in C$, $wt(c) = w$ and $w < d + \lceil \frac{w}{5} \rceil$. Then $Res(C,w)$ has parameters $[n-w, k-1, d^{\circ}]_5$, where $d^{\circ} \ge d - w + \lceil \frac{w}{5} \rceil$.*

Lemma 3 [7]**.** *Let C be an $[n,k,d]_5$-code with $k \ge 2$. Then:*
a) $A_i = 0$ or 4 for $i > (5n-4d)/2$
b) If $A_i = 4$, then $A_j = 0$ for $j + i > 5n - 4d$ and $i \ne j$.

The Linear Programming Bound. The weight enumerator of an $[n,k,d]_5$-code C is a feasible solution of the following linear program **(LP)**

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

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

It is clear now that if $L_{max} < 5^k$, then the code C does not exist.

2. Bounds on minimum distance.

2.1. Lower bounds.

Theorem 2. *There exists an optimal* $[54, 5, 40]_5$*-code.*

Proof. The generator matrix and the weight enumerator are as follows:

$$G = \begin{pmatrix} 000000000111111111111111111111111111111111111111111111111111 \\ 000111111000000111111111112222222222233333333333444444 \\ 011000222001144122233334441111222233400011123334223444 \\ 002014123230203111401242230112113333402313421124043223 \\ 111303133010313002424240430241241411411013341231324401 4 \end{pmatrix},$$

$0^1 40^{580} 41^{720} 42^{420} 45^{520} 46^{780} 50^{24} 52^{80}$.

Theorem 3. *There exist QC codes with parameters:*

$$[33, 11, 15]_5, [44, 11, 23]_5, [55, 11, 30]_5, [77, 11, 46]_5,$$

$$[88, 11, 53]_5, [99, 11, 61]_5, [52, 13, 26]_5, [65, 13, 35]_5.$$

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

1. **A** $[33, 11, 15]_5$**-code:** 00010112142, 00001112123, 00000000001;

2. **A** $[44, 11, 23]_5$**-code:** 00102414424, 00010121423, 00001112123, 00000000001;

3. **A** $[55, 11, 30]_5$**-code:** 00001121322, 00110212114, 00010121423, 00001112123, 00000000001;

4. **A** $[77, 11, 46]_5$**-code:** 00101241113, 00014311142, 00001333412, 00110212114, 00010121423, 00001112123, 00000000001;

5. **An** $[88, 11, 53]_5$**-code:** 00001131232, 00101241113, 00014311142, 00001333412, 00110212114, 00010121423, 00001112123, 00000000001;

6. **A** $[99, 11, 61]_5$**-code:** 00114234011, 00001141434, 00101241113, 00014311142, 00001333412, 00110212114, 00010121423, 00001112123, 00000000001;

7. **A** $[52, 13, 26]_5$**-code:** 0001020332010, 0010322333012, 0001244224421, 0000000000001;

8. **A** $[65, 13, 35]_5$**-code:** 0001111431431, 0001020332043, 0010322333012, 0001244224421, 0000000000001.

Table 1. Minimum distances of the new linear codes over $GF(5)$.

code	d	$d_{br}[2]$	code	d	$d_{br}[2]$
[33,11]	15	14	[88,11]	53	52
[44,11]	23	22	[99,11]	61	60
[55,11]	30	29	[52,13]	26	25
[77,11]	46	45	[65,13]	35	34

2.2. Upper bounds.

Theorem 4. *We have* $d_5(106,5) \leq 82$.

Proof. Suppose there exists a $[106,5,83]_5$-code C. By [2] $[103,3,83]_5$, $[104,4,83]_5$ and $[105,5,83]_5$ codes do not exist. So by Lemma 1 it follows that $B_1 = B_2 = B_3 = 0$. For codewords with weights 86, 87, 88, 89, 91, 92, 93, 96, 97, 98, 99, 101 and 102 we calculate the parameters of the respective residual codes, using Lemma 2. From [2] these residual codes do not exist and so A_{86}, A_{87}, A_{88}, A_{89}, A_{91}, A_{92}, A_{93}, A_{96}, A_{97}, A_{98}, A_{99}, A_{101} and A_{102} are equal to zero.

By Lemma 3 A_{100}, A_{103}, A_{104}, A_{105}, A_{106} are either 0 or 4.

The first four MacWilliams identities are:

$$e_0 : A_{83} + A_{84} + A_{85} + A_{90} + A_{94} + A_{95} + A_{100} + A_{103} + A_{104} + A_{105} + A_{106} = 3124$$

$$e_1 : 9.A_{83} + 4.A_{84} - A_{85} - 26.A_{90} - 46.A_{94} - 51.A_{95} - 76.A_{100} - 91.A_{103} - 96.A_{104} - 101.A_{105} - 106.A_{106} = -424$$

$$e_2 : -185.A_{83} - 210.A_{84} - 210.A_{85} + 165.A_{90} + 915.A_{94} + 1165.A_{95} + 2790.A_{100} + 4065.A_{103} + 4540.A_{104} + 5040.A_{105} + 5565.A_{106} = -89040$$

$$e_3 : -1445.A_{83} - 420.A_{84} + 630.A_{85} + 1880.A_{90} - 9420.A_{94} - 14995.A_{95} - 65620.A_{100} - 118695.A_{103} - 140920.A_{104} - 165620.A_{105} - 192920.A_{106} = -12346880.$$

Calculating the linear combination $(772.e_0 + 101.e_1 + 22.e_2/5 + 3.e_3/5)/25$ we get

$$a_1 : 5.A_{85} - 220.A_{94} - 330.A_{95} - 1360.A_{100} - 2470.A_{103}$$

$$-2940.A_{104} - 3465.A_{105} - 4048.A_{106} = -217240.$$

By Lemma 3 a) A_{106} and A_{105} are either 0 or 4. If A_{106} or A_{105} equals 4 then using Lemma 3 b) and equation a_1 we obtain that $A_{85} < 0$, a contradiction.
So $A_{106} = A_{105} = 0$.

Calculating the next two linear combinations $(1092.e_0 + 126.e_1 + 32.e_2/5 + 3.e_3/5)/25$ and $(126.e_0 - 42.e_1 + 1.e_2/5 - 1.e_3/5)/125$ we get respectively:

$$a_2 : 7.A_{83} - 180.A_{94} - 275.A_{95} - 1200.A_{100} - 2223.A_{103} - 2660.A_{104} = -184800$$
$$a_3 : 7.A_{90} + 33.A_{94} + 44.A_{95} + 136.A_{100} + 228.A_{103} + 266.A_{104} = 22904.$$

If $A_{104} = 4$ then by Lemma 3 $A_{103} = A_{100} = A_{95} = 0$ and equation $a_2 + 7.a_3$ gives a contradiction. So $A_{104} = 0$. Analoguosly $A_{103} = 0$ and $A_{100} = 0$. Now the equation $a_2 + 7.a_3$ gives $7.A_{83} + 49.A90 + 51.A94 + 33.A_{95} = 160328 - 184800 < 0$, a contradiction. So a $[106,5,83]_5$-code does not exist.

Theorem 5. *We have* $d_5(102,5) \leq 79$.

Proof. Suppose there exists a $[102,5,80]_5$-code C. By Lemma 1 and [2] $B_1 = B_2 = B_3 = 0$. Using Lemma 2 and the respective upper bounds in [2] we find that the only nonzero weights that may occur in C are A_{80}, A_{90}, A_{99}, A_{100}, A_{101} and A_{102}. Since $q = 5$ divides $d = 80$, it follows by the remarkable result of Ward [12] that all weights are divisilbe by $q = 5$ and so only A_{80}, A_{90} and A_{100} are not equal zero.

The first three MacWilliams identities are:

$$e_0 : A_{80} + A_{90} + A_{100} = 3124$$
$$e_1 : 8.A_{80} - 42.A_{90} - 92.A_{100} = -408$$
$$e_2 : -184.A_{80} + 741.A_{90} + 4166.A_{100} = -82416.$$

This system has the unique solution

$$A_{80} = 2625, \quad A_{90} = 490, \qquad A_{100} = 9,$$

but by Lemma 3 $A_{100} = 0$ or 4, a contradiction. So a $[102, 5, 80]_5$-code does not exist.

Theorem 6. *There do not exist codes with parameters:*

$[104, 6, 80]_5$,	$[109, 6, 84]_5$,	$[114, 6, 88]_5$,	$[119, 6, 92]_5$,	$[124, 6, 96]_5$,	$[129, 6, 100]_5$,
$[109, 7, 83]_5$,	$[114, 7, 87]_5$,	$[124, 7, 95]_5$,	$[128, 7, 98]_5$,	$[75, 8, 55]_5$,	$[80, 8, 59]_5$,
$[124, 8, 94]_5$,	$[75, 9, 54]_5$,	$[80, 9, 58]_5$,	$[103, 9, 76]_5$,	$[107, 9, 79]_5$,	$[112, 9, 83]_5$,
$[117, 9, 87]_5$,	$[122, 9, 91]_5$,	$[127, 9, 95]_5$,	$[76, 10, 54]_5$,	$[80, 10, 57]_5$,	$[89, 10, 64]_5$,
$[94, 10, 68]_5$,	$[103, 10, 75]_5$,	$[107, 10, 78]_5$,	$[112, 10, 82]_5$,	$[116, 10, 85]_5$,	$[121, 10, 89]_5$,
$[126, 10, 93]_5$,	$[130, 10, 96]_5$,	$[71, 11, 49]_5$,	$[76, 11, 53]_5$,	$[80, 11, 56]_5$,	$[85, 11, 60]_5$,
$[76, 12, 52]_5$,	$[80, 12, 55]_5$,	$[84, 12, 58]_5$,	$[89, 12, 62]_5$,	$[93, 12, 65]_5$,	$[98, 12, 69]_5$,
$[102, 12, 72]_5$,	$[107, 12, 76]_5$,	$[112, 12, 80]_5$,	$[117, 12, 84]_5$,	$[122, 12, 88]_5$,	$[126, 12, 91]_5$.

Proof. For every of the above codes we solve the respective linear program with the aid of the well-known simplex method. In all of the cases we obtain $L_{max} < 5^k$ and so the codes do not exist.

REFERENCES

[1] I. Boukliev, S. Kapralov, T. Maruta, M. Fukui. Optimal linear codes of dimension 4 over GF(5). *IEEE Trans. Inform. Theory*, **43**, (1997), 308–313.

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

[3] R. N. Daskalov. New bounds on minimum distance for 9-dimensional linear codes over GF(5). In: Proc. of Seventh International Workshop on Algebraic and Combinatorial Coding Theory, Bansko, Bulgaria, June 18–24, 2000, 112–116.

[4] R. N. Daskalov, T. A. Gulliver. Bounds on Minimum Distance for Linear Codes over GF(5). *Appl. Algebra in Engin. Comm. and Computing*, **9**, No 6 (1999), 547–558.

[5] S. M. Dodunekov. Minimum block length of a linear q-ary code with specified dimension and code distance. *Probl. Inform. Transm.*, **20** (1984), 239–249.

[6] R. Hill. Optimal Linear Codes. In: Cryptography and Coding II, (Ed. C. Mitchel) Oxford, UK, Oxford Univ. Press, 1992, 75–104.

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

[8] I. Landjev, A. Rousseva, T. Maruta, R. Hill. On optimal codes over the field with five elements, preprint.

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

[10] I. Siap, D. Ray-Chaudhury. New codes over F_3 and F_5 and improvements on bounds. *Designs, Codes and Cryptography*, **21** (2000), 223–233.

[11] I. Siap, D. Ray-Chaudhury. New codes over F_5 obtained by tripling method and improvements on their bounds. *IEEE Trans. Inform. Theory*, **48**, No 10 (2002), 2764–2768.

[12] H. N. Ward. Divisibility of codes meeting the Griesmer bound. *J. Combin. Theory*, Ser. A, **83**, No 1 (1998), 79–93.

Rumen Daskalov
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria
e-mail: daskalov@tugab.bg

Elena Metodieva
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria
e-mail: metodieva@tugab.bg

ПОДОБРЕНИ ГРАНИЦИ ЗА МИНИМАЛНОТО РАЗСТОЯНИЕ НА ЛИНЕЙНИ КОДОВЕ НАД GF(5)

Румен Даскалов, Елена Методиева

Нека $[n, k, d]_q$-код е линеен код с дължина n, размерност k и минимално Хемингово разстояние d над $GF(q)$. В тази статия са конструирани девет нови кода и е доказано несъществуването на петдесет кода над поле с пет елемента. Получените резултати подобряват съответните познати до момента долни и горни граници за минималното разстояние в таблицата на Брауер [2].