МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2002
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2002
Proceedings of Thirty First Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 3–6, 2002

THE LINEAR PROGRAMMING BOUND FOR TERNARY AND QUATERNARY LINEAR CODES*

Rumen Daskalov, Elena Daskalova

The linear programming bound for ternary and quaternary linear codes of word length between 201 and 250 is determined.

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 $[n,k,d]_q$-code if its minimum Hamming distance is d.

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

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

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

Many upper bounds for $d_3(n,k)$ and $d_4(n,k)$ are determined in [2–9]. All of the results obtained in these papers are included in Brouwers online tables [1]. We continue these investigations for word lenght between 201 and 250.

2. Preliminary results. The Hamming weight of a vector x, denoted by $wt(x)$, is the number of nonzero entries in x. For a linear code, the minimum distance is equal to the smallest of the weights of the nonzero codewords.

Let G be a *generator matrix* of an $[n,k,d]_q$-code C.

Definition. *The residual code of C with respect to $c \in C$ is the code generated by the restriction of G to the columns where c has a zero. The residual code of C with respect to $c \in C$ is denoted by $Res(C,c)$ or $Res(C,w)$ if the Hamming weight of c is w.*

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.*

Lemma 1 (the MacWilliams' identities (cf. [12]). *Suppose that linear code $C = [n,k,d]_q$ and its dual code $C^{\perp}$ have weight enumerators $\{A_i\}$ and $\{B_i\}$ $(0 \le i \le n)$, respectively. Then:*

$$\sum_{i=0}^{n} K_t(i).A_i = q^k B_t \qquad for \quad t = 0,1,\ldots,n$$

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

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 polinomials of degree t.

Lemma 2 [11]**.** *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.*

By this Lemma we find a lower bound $d^{\perp}$ for the minimum distance of $C^{\perp}$ and so $B_1 = 0, \ldots, B_{d^{\perp}-1} = 0$.

Lemma 3 [10]**.** *Let* C *be an* $[n,k,d]_q$*-code and* $x \in C$, $wt(x) = w$ *and* $w < d + \lceil \frac{w}{3} \rceil$. *Then* $Res(C,w)$ *is an* $[n-w, k-1, d^{\circ}]_q$*-code, where* $d^{\circ} \geq d - w + \lceil \frac{w}{q} \rceil$. *(*$\lceil x \rceil$ *denotes the smallest integer* $\geq x$*).*

If no such code exists then it follows that C has no words of weight w, and so $A_w = 0$.

Thus, the weight enumerator of an $[n,k,d]_q$-code C is a feasible solution of the linear program,

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

subject to

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

Solving this linear programming problem, by the well–known simplex method, we find the upper bounds on $d_q(n,k)$ which are given in the next two sections.

3. New upper bounds on $\boldsymbol{d_3(n,k)}$**.** The next ternary linear codes do not exist:

$[201,18,119]_3$	$[202,18,121]_3$	$[206,18,122]_3$	$[209,18,124]_3$	$[212,18,126]_3$
$[215,18,128]_3$	$[218,18,130]_3$	$[221,18,132]_3$	$[223,18,133]_3$	$[225,18,135]_3$
$[229,18,137]_3$	$[232,18,139]_3$	$[235,18,141]_3$	$[238,18,143]_3$	$[241,18,145]_3$
$[244,18,147]_3$	$[246,18,148]_3$	$[218,19,129]_3$	$[221,19,131]_3$	$[229,19,136]_3$
$[232,19,138]_3$	$[235,19,140]_3$	$[238,19,142]_3$	$[241,19,144]_3$	$[243,19,145]_3$
$[242,20,144]_3$	$[204,21,118]_3$	$[208,21,121]_3$	$[214,21,125]_3$	$[216,21,126]_3$
$[219,21,128]_3$	$[222,21,130]_3$	$[225,21,132]_3$	$[228,21,134]_3$	$[236,21,139]_3$
$[239,21,141]_3$	$[207,22,119]_3$	$[210,22,121]_3$	$[213,22,123]_3$	$[215,22,124]_3$
$[218,21,126]_3$	$[221,22,128]_3$	$[224,22,130]_3$	$[227,22,132]_3$	$[229,22,133]_3$
$[232,21,135]_3$	$[235,22,137]_3$	$[209,23,119]_3$	$[213,23,122]_3$	$[224,23,129]_3$
$[227,23,131]_3$	$[232,23,134]_3$	$[209,25,118]_3$	$[214,25,121]_3$	$[217,25,123]_3$
$[220,25,125]_3$	$[223,25,127]_3$			

4. New upper bounds on $d_4(n,k)$. The following quaternary linear codes do not exist:

	$[202,8,146]_4$	$[206,8,149]_4$	$[209,8,151]_4$	$[213,8,154]_4$
$[217,8,157]_4$	$[221,8,160]_4$	$[225,8,163]_4$	$[229,8,166]_4$	$[233,8,169]_4$
$[237,8,172]_4$	$[241,8,175]_4$	$[245,8,178]_4$	$[249,8,181]_4$	$[245,9,177]_4$
$[203,10,145]_4$	$[207,10,148]_4$	$[201,11,142]_4$	$[205,11,145]_4$	$[208,11,147]_4$
$[211,11,149]_4$	$[215,11,152]_4$	$[219,11,155]_4$	$[223,11,158]_4$	$[227,11,161]_4$
$[231,11,164]_4$	$[235,11,167]_4$	$[239,11,170]_4$	$[243,11,173]_4$	$[247,11,176]_4$
$[202,12,141]_4$	$[206,12,144]_4$	$[209,12,146]_4$	$[213,12,149]_4$	$[217,12,152]_4$
$[221,12,155]_4$	$[224,12,157]_4$	$[228,12,160]_4$	$[232,12,163]_4$	$[236,12,166]_4$
$[239,12,168]_4$	$[243,12,171]_4$	$[247,12,174]_4$	$[201,14,139]_4$	$[203,14,140]_4$
$[207,14,143]_4$	$[222,14,154]_4$	$[201,15,137]_4$	$[204,15,139]_4$	$[208,15,142]_4$
$[212,15,145]_4$	$[216,15,148]_4$	$[219,15,150]_4$	$[223,15,153]_4$	$[227,15,156]_4$
$[231,15,159]_4$	$[235,15,162]_4$	$[239,15,165]_4$	$[242,15,167]_4$	$[246,15,170]_4$
$[250,15,173]_4$	$[201,16,136]_4$	$[204,16,138]_4$	$[208,16,141]_4$	$[212,16,144]_4$
$[215,16,146]_4$	$[219,16,149]_4$	$[223,16,152]_4$	$[226,16,154]_4$	$[230,16,157]_4$
$[233,16,159]_4$	$[237,16,162]_4$	$[241,16,165]_4$	$[244,16,167]_4$	$[248,16,170]_4$
$[201,18,134]_4$	$[205,18,137]_4$	$[208,18,139]_4$	$[212,18,142]_4$	$[216,18,145]_4$
$[220,18,148]_4$	$[223,18,150]_4$	$[227,18,153]_4$	$[231,18,156]_4$	$[235,18,159]_4$
$[242,18,164]_4$	$[246,18,167]_4$	$[250,18,170]_4$	$[201,19,133]_4$	$[203,19,134]_4$
$[207,19,137]_4$	$[211,19,140]_4$	$[214,19,142]_4$	$[218,19,145]_4$	$[222,19,148]_4$
$[225,19,150]_4$	$[229,19,153]_4$	$[233,19,156]_4$	$[236,19,158]_4$	$[240,19,161]_4$
$[244,19,164]_4$	$[248,19,167]_4$	$[201,20,132]_4$	$[233,20,155]_4$	$[240,20,160]_4$
$[244,20,163]_4$	$[248,20,166]_4$	$[201,21,131]_4$	$[248,21,165]_4$	$[201,22,130]_4$
$[204,22,132]_4$	$[207,22,134]_4$	$[211,22,137]_4$	$[215,22,140]_4$	$[218,22,142]_4$
$[222,22,145]_4$	$[226,22,148]_4$	$[229,22,150]_4$	$[233,22,153]_4$	$[237,22,156]_4$
$[241,22,159]_4$	$[244,22,161]_4$	$[248,22,164]_4$	$[201,23,129]_4$	$[215,23,139]_4$
$[222,23,144]_4$	$[226,23,147]_4$	$[229,23,149]_4$	$[233,23,152]_4$	$[236,23,154]_4$
$[240,23,157]_4$	$[243,23,159]_4$	$[247,23,162]_4$	$[250,23,164]_4$	

REFERENCES

[1] A.E. Brouwer. Linear code bounds [electronic table; online], `www.win.tue.nl/math/dw/personalpages/aeb/voorlincod.html`.

[2] A. E. Brouwer, R. N. Daskalov, D. Berntzen, P. Kemper. The linear programming bound for ternary and quaternary linear codes. March 1993, (preprint).

[3] R. N. Daskalov. The linear programming bound for ternary linear codes. In: Proc. 1994 IEEE International Symposium on Information Theory. Trondheim, Norway, June 27–July 01, 1994, 423.

[4] R. N. Daskalov. Minimum distance bounds for quaternary linear codes, *Mathematics and Education in Mathematics*, **23** (1994), 143–155.

[5] R. N. Daskalov, E. Metodieva. Bounds on minimum length for quaternary linear codes in dimensions six and seven. *Mathematics and Education in Mathematics*, **23** (1994), 156–161.

[6] R. N. Daskalov. The linear programming bound for quaternary linear codes. In: Proceedings of Fourth International Workshop on Algebraic and Combinatorial Coding Theory. Novgorod, Russia, September 11–17, 1994, 74–77.

[7] R. N. Daskalov. The sharpened linear programming bound for ternary linear codes. *Mathematics and Education in Mathematics*, **24** (1995), 158–166.
[8] R. N. Daskalov, E. Metodieva. Minimum distance bounds for quaternary linear codes in dimension five. *Mathematics and Education in Mathematics* **24** (1995), 167–176.
[9] S. Guritman. Restrictions on the Weight Distribution of Linear Codes. Ph. D. Dissertation, Delft University of Technology, The Netherlands, 2000.
[10] 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.
[11] R. Hill, D. E. Newton. Optimal ternary linear codes. *Designs, Codes and Cryptography*, **2** (1992), 137–157.
[12] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error–Correcting Codes. Amsterdam, North-Holland, 1977.

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

ГРАНИЦА НА ЛИНЕЙНОТО ПРОГРАМИРАНЕ ЗА ЛИНЕЙНИ КОДОВЕ НАД $GF(3)$ И $GF(4)$

Румен Даскалов, Елена Даскалова

Пресметната е границата на линейното програмиране за линейни кодове с дължина между 201 и 250 над $GF(3)$ и $GF(4)$.