Some nonexistence results for 7-dimensional ternary linear codes *

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

Abstract

Let $d_3(n,k)$ be the maximum possible minimum Hamming distance of a ternary linear $[n,k,d;3]$-code for given values of n and k. The nonexistence of [142,7,92;3], [162,7,106;3], [165,7,108;3] and [191,7,125;3] codes is proved.

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 central 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 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.

The problem of finding $n_3(k,d)$ has been solved for $k \leq 5$ for all d. A table of the bounds for $n_3(6,d)$ was given by Hamada [7] and Daskalov [2] and Hamada and Watamori [8]. Recently a table with improved bounds for $d_3(7,d)$ was published by Gulliver and Östergård [6]. In this paper we improve some upper bounds in table [6] and in table [1].

*This work was partially supported by the Bulgarian Science Fund under Grant I-618/96.

2 Preliminary results

The well-known lower bound for $n_q(k,d)$ is the Griesmer bound

$$n_q(k,d) \geq g_q(k,d) = \sum_{j=0}^{k-1} \lceil \frac{d}{q^j} \rceil$$

($\lceil x \rceil$ denotes the smallest integer $\geq$x).

Lemma 1: *(the MacWilliams' identities)*
Let C be an $[n,k,d;3]$-code and A_i and B_i denote the number of codewords of weight i in the code C and in its dual code $C^{\perp}$ respectively. Then

$$\sum_{i=0}^{n} K_t(i)A_i = 3^k B_t, \qquad \text{for } 0 \leq t \leq n,$$

where

$$K_t(i) = \sum_{j=0}^{t} (-1)^j \binom{n-i}{t-j} \binom{i}{j} 2^{t-j}$$

are the Krawtchouk polynomials.

Lemma 2: [9] For an $[n,k,d;3]$-code $B_i = 0$ for each value of i (where $1 \leq i \leq k$) such that there does not exist $[n-i, k-i+1, d;3]$-code.

Lemma 3: [4] Let C be an $[n,k,d;3]$-code and $x \in C$, $wt(x) = w$ and $w < d + \lceil \frac{w}{3} \rceil$. Then $Res(C,w)$ has parameters $[n-w, k-1, d^{\circ}]$, where $d^{\circ} \geq d - w + \lceil \frac{w}{3} \rceil$.

Lemma 4: [9] Let C be an $[n,k,d;3]$-code with $k \geq 2$. Then:
a) $A_i = 0$ or 2 for $i > (3n-2d)/2$
b) If $A_i = 2$, then $A_j = 0$ for $j + i > 3n - 2d$ and $i \neq j$.

Lemma 5: [9] Let C be a $[g_3(k,d), k, d;3]$-code. Then: $B_1 = 0$ for all d and $B_i = 0$ if $1 < i < k+1$ and if $d \leq 3^{k-i+1}$.
Corollary 5.1: If $k = 7$, then $B_1 = 0$ for all d, $B_2 = 0$ for $d \leq 729$ and $B_3 = 0$ for $d \leq 243$.

Lemma 6: [5] Let C be an $[n,k,d;3]$-code. If $d \equiv 2$ (*mod* 3) and no codeword of C is of weight 1 *mod* 3, then C can be extended to a self-orthogonal $[n+1, k, d+1;3]$-code.

Let S_1 denote the number of codewords in an $[n, k, d; 3]$-code of weight 1 *mod* 3.

Lemma 7: [3] Let C be an $[n, k, d; 3]$-code with $d \ mod \ 3 \neq 1$ and $B_1 = 0$. Let also $A_i = 0$ if $i \ mod \ 3 = 1$ and $i \leq 3n + d - \frac{9}{2}d + \frac{d}{2.3^{k-2}}$. Then $S_1 = 0$.

3 The new results

If we prove the non-existence of [142,7,92;3] codes, then it follows immediately that [143,7,93;3] codes do not exist either. But it is very difficult to prove directly the non-existence of [142,7,92;3] codes. For this reason we will first prove the non-existence of [143,7,93;3] codes and after that, by Lemma 7 and Lemma 6 it follows easily that [142,7,92;3] codes do not exist.

By [6] $90 \leq d_3(143, 7) \leq 93$.

Theorem 1: $d_3(143, 7) \leq 92$.

Proof: Suppose there exists a $[g_3(7, 93)$=143,7,93;3]-code C. By Corollary 5.1 it follows that $B_1 = B_2 = B_3 = 0$. By Lemma 3 and [8] or [1] and [10] it follows that $A_i \neq 0$ for $i \in \{93, 99, 108, 117, 131, 132, 138, 139, 140, 141, 142, 143\}$.

The first four MacWilliams identities are:

$$\begin{aligned}
e_0: \ & A_{93} + A_{99} + A_{108} + A_{117} + A_{131} + A_{132} + A_{138} + A_{139} + A_{140} \\
& + A_{141} + A_{142} + A_{143} = 2186 \\
e_1: \ & 7.A_{93} - 11.A_{99} - 38.A_{108} - 65.A_{117} - 107.A_{131} - 110.A_{132} \\
& - 128.A_{138} - 131.A_{139} - 134.A_{140} - 137.A_{141} - 140.A_{142} \\
& - 143.A_{143} = -286 \\
e_2: \ & -122.A_{93} - 77.A_{99} + 598.A_{108} + 2002.A_{117} + 5635.A_{131} \\
& + 5962.A_{132} + 8113.A_{138} + 8503.A_{139} + 8902.A_{140} + 9310.A_{141} \\
& + 9727.A_{142} + 10153.A_{143} = -40612 \\
e_3: \ & -866.A_{93} + 1375.A_{99} - 4376.A_{108} - 38558.A_{117} - 194609.A_{131} \\
& - 212168.A_{132} - 339446.A_{138} - 364565.A_{139} - 390872.A_{140} \\
& - 418394.A_{141} - 447158.A_{142} - 477191.A_{143} = -3817528
\end{aligned}$$

Calculating the next linear combination

$$(-1562.e_0 - 162.e_1 - 15.e_2 - 1.e_3)/9,$$

we get

$$(a): \quad 1944.A_{117} + 13984.A_{131} + 15444.A_{132} + 26325.A_{138} + 28520.A_{139} + 30832.A_{140} + 33264.A_{141} + 35819.A_{142} + 38500.A_{143} = 117612.$$

It follows by Lemma 4 that $A_i \in \{0, 2\}$ for $i = 131, 132, 138, 139, 140, 141, 142, 143$. If $A_{143} = 2$ then by Lemma 4 $A_{117} = A_{131} = A_{132} = A_{138} = A_{139} = A_{140} = A_{141} = A_{142} = 0$ and equation (a) gives a contradiction. Thus $A_{158} = 0$. Similarly $A_{142} = A_{141} = A_{140} = A_{139} = A_{138} = A_{132} = A_{131} = 0$.

Now the first four MacWilliams identities are:

$$\begin{aligned} e_0: &\quad A_{93} + A_{99} + A_{108} + A_{117} = 2186 \\ e_1: &\quad 7.A_{93} - 11.A_{99} - 38.A_{108} - 65.A_{117} = -286 \\ e_2: &\quad -122.A_{93} - 77.A_{99} + 598.A_{108} + 2002.A_{117} = -40612 \\ e_3: &\quad -866.A_{93} + 1375.A_{99} - 4376.A_{108} - 38558.A_{117} = -3817528 \end{aligned}$$

There is no solution of the MacWilliams identities in non-negative integer, because the unique solution of the above system is:

$$10.A_{93} = 16731, \quad A_{99} = 338, \quad 5.A_{108} = 572, \quad 2.A_{117} = 121.$$

Theorem 2: $d_3(142, 7) \leq 91$.

Proof: Suppose there exists a $[g_3(7, 92) = 142, 7, 92; 3]$-code C. By [1] or [6] a [141,7,92;3]-code does not exist and it follows by Lemma 2 that $B_1 = 0$. For code C $3n + d - \frac{9}{2}d + \frac{d}{2.3^{k-2}} = 104, 19$. By Lemma 3 $Res(C, 94)$ = [48,6,30;3]-code, $Res(C, 97)$ = [45,6,28;3]-code, $Res(C, 100)$ = [42,6,26;3]-code, $Res(C, 103)$ = [39,6,24;3]-code. By [1] these codes do not exist and it follows by Lemma 7 that $S_1 = 0$. Then by Lemma 6 a [142,7,92;3]-code can be extended to a self-orthogonal [143,7,93;3]-code, which contradicts Theorem 1. So [142,7,92;3]-codes do not exist.

By [6] $102 \leq d_3(162, 7) \leq 106$.

Theorem 3: $d_3(162, 7) \leq 105$.

Proof: Suppose there exists a $[g_3(7, 106)$=162,7,106;3]-code C. By Corollary 5.1 it follows that $B_1 = B_2 = B_3 = 0$. By Lemma 3 and [8] or [1] it follows that $A_i \neq 0$ for $i \in \{106, 107, 108, 114, 150, 157, 158, 159, 160, 161, 162\}$.

The first four MacWilliams identities are:

$$\begin{aligned}
e_0: &\ A_{106}+A_{107}+A_{108}+A_{114}+A_{150}+A_{157}+A_{158}+A_{159}\\
&+A_{160}+A_{161}+A_{162}=2186\\
e_1: &\ 6.A_{106}+3.A_{107}-18.A_{114}-126.A_{150}-147.A_{157}-150.A_{158}\\
&-153.A_{159}-156.A_{160}-159.A_{161}-162.A_{162}=-324\\
e_2: &\ -147.A_{106}-159.A_{107}-162.A_{108}+9.A_{114}+7839.A_{150}\\
&+10716.A_{157}+11163.A_{158}+11619.A_{159}+12084.A_{160}\\
&+12558.A_{161}+13041.A_{162}=-52164\\
e_3: &\ -840.A_{106}-375.A_{107}+108.A_{108}+1872.A_{114}-320940.A_{150}\\
&-516450.A_{157}-549492.A_{158}-583893.A_{159}-619680.A_{160}\\
&-656880.A_{161}-695520.A_{162}=-5564160
\end{aligned}$$

Calculating the next linear combination

$$(-3492.e_0-279.e_1-94.e_2/3-2.e_3/3)/3,$$

we get

$$\begin{aligned}
&301.A_{107}+504.A_{108}+15351.A_{157}+18304.A_{158}+21465.A_{159}\\
&+24840.A_{160}+28435.A_{161}+32256.A_{162}=-733068,
\end{aligned}$$

a contradiction.

By [6], [1] $105 \le d_3(165,7) \le 108$.

Theorem 4: $d_3(165,7) \le 107$.

Proof: Suppose there exists a $[g_3(7,108)+1{=}165,7,108;3]$-code C. By [1] [164,7,108;3] and [163,6,108;3] codes do not exist and by Lemma 2 it follows that $B_1 = B_2 = 0$. By Lemma 3 and [8] or [1] it follows that $A_i \neq 0$ for $i \in \{108,109,110,111,117,153,160,161,162,163,164,165\}$.

Although only the first three MacWilliams' identities are free of B_i terms, we will use now the first four identities.

$$\begin{aligned}
e_0: &\ A_{108}+A_{109}+A_{110}+A_{111}+A_{117}+A_{153}+A_{160}+A_{161}\\
&+A_{162}+A_{163}+A_{164}+A_{165}=2186\\
e_1: &\ 6.A_{108}+3.A_{109}-3.A_{111}-21.A_{117}-129.A_{153}-150.A_{160}\\
&-153.A_{161}-156.A_{162}-159.A_{163}-162.A_{164}-165.A_{165}=-330\\
e_2: &\ -150.A_{108}-162.A_{109}-165.A_{110}-159.A_{111}+66.A_{117}\\
&+8220.A_{153}+11160.A_{160}+11616.A_{161}+12081.A_{162}\\
&+12555.A_{163}+13038.A_{164}\\
&+13530.A_{165}=-54120\\
e_3: &\ -856.A_{108}-382.A_{109}+110.A_{110}+593.A_{111}+1790.A_{117}\\
&-344836.A_{153}-549040.A_{160}-583432.A_{161}-619210.A_{162}\\
&-656401.A_{163}-695032.A_{164}-735130.A_{165}-2187.B_3\\
&=-5881040
\end{aligned}$$

Calculating the next linear combination

$$(-5266.e_0 - 490.e_1 - 49.e_2 - e_3)/9$$

we get

$$176.A_{109} + 301.A_{110} + 378.A_{111} + 7826.A_{160} + 9328.A_{161} + 10935.A_{162} \\ +12650.A_{163} + 14476.A_{164} + 16416.A_{165} + 243.B_3 = -312984,$$

a contradiction.

By [6] $123 \leq d_3(192,7) \leq 126$.

Theorem 5: $d_3(192,7) \leq 125$.

Proof: Suppose there exists a $[g_3(7,126)+1=192,7,126;3]$-code C. By [1] [190,6,126;3] and [191,7,126;3] codes do not exist and by Lemma 2 it follows that $B_1 = B_2 = 0$. By Lemma 3 and [8] or [1] and [10] it follows that $A_i \neq 0$ for $i \in \{126, 135, 136, 137, 138, 180, 187, 188, 189, 190, 191, 192\}$.

The first four MacWilliams identities are:

$$\begin{aligned}
e_0: \quad & A_{126} + A_{135} + A_{136} + A_{137} + A_{138} + A_{180} + A_{187} + A_{188} + A_{189} \\
& + A_{190} + A_{191} + A_{192} = 2186 \\
e_1: \quad & 6.A_{126} - 21.A_{135} - 24.A_{136} - 27.A_{137} - 30.A_{138} - 156.A_{180} \\
& - 177.A_{187} - 180.A_{188} - 183.A_{189} - 186.A_{190} \\
& - 189.A_{191} - 192.A_{192} = -384 \\
e_2: \quad & -177.A_{126} + 39.A_{135} + 108.A_{136} + 186.A_{137} + 273.A_{138} \\
& + 12054.A_{180} + 15561.A_{187} + 16098.A_{188} + 16644.A_{189} \\
& + 17199.A_{190} + 17763.A_{191} + 18336.A_{192} = -73344 \\
e_3: \quad & -1000.A_{126} + 2375.A_{135} + 2120.A_{136} + 1640.A_{137} + 908.A_{138} \\
& - 614980.A_{180} - 905935.A_{187} - 953692.A_{188} - 1003078.A_{189} \\
& - 1054120.A_{190} - 1106845.A_{191} - 1161280.A_{192} - 2187.B_3 \\
& = -9290240
\end{aligned}$$

Calculating the next linear combination

$$(-13808.e_0 - 1631.e_1 - 122.e_2 - 2.e_3)/9,$$

we get

$$1215.A_{135} + 880.A_{136} + 473.A_{137} + 20923.A_{187} + 24800.A_{188} + 28917.A_{189} \\ +33280.A_{190} + 37895.A_{191} + 42768.A_{192} + 486.B_3 = -225504,$$

a contradiction.

Theorem 6: $d_3(191,7) \leq 124$.

Proof: Suppose there exists a $[g_3(7,92)+1 = 191,7,125;3]$-code C. By [1] a [190,7,125;3]-code does not exist and it follows by Lemma 2 that $B_1 = 0$. For code C $3n + d - \frac{9}{2}d + \frac{d}{2.3^{k-2}} = 135,76$. By Lemma 3 $Res(C,127)$ = [64,6,41;3]-code, $Res(C,130)$ = [61,6,39;3]-code, $Res(C,133)$ = [58,6,37;3]-code. By [1] these codes do not exist and it follows by Lemma 7 that $S_1 = 0$. Then by Lemma 6 a [191,7,125;3]-code can be extended to a self-orthogonal [192,7,126;3]-code, which contradicts Theorem 5. So [191,7,125;3]-codes do not exist.

Table: Improved bounds on $d_3(n,7)$

n	$d_3(n,7)$ in [6]	$d_3(n,7)$	Source
133	84-86	84-85	[10]
134	84-87	84-86	
142	89-92	89-91	Th. 2
143	90-93	90-92	
156	99-102	99-101	
159	100-104	100-103	[3]
160	101-105	101-104	
162	102-106	102-105	Th. 3
163	103-107	103-106	
164	104-108	104-107	Th. 4
165	105-108	105-107	
191	122-125	122-124	Th. 6
192	123-126	123-125	

References

[1] A.E. Brouwer, Minimum distance bounds for linear codes over GF(3), lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, the Netherlands.

[2] R.N. Daskalov, Bounds on the minimum length for ternary linear codes of dimension six, *Mathematics and Education in Mathematics*, Sofia, (1993), 15–22.

[3] R.N. Daskalov, The nonexistence of ternary linear [158,6,104] and [203,6,134] codes, *In Proc. Inter. Workshop ACCT-V*, Sozopol, Bulgaria, June 1–7, (1996), 111–116.

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

[5] M. van Eupen, An extension theorem for ternary linear codes, *In Proc. Inter. Workshop Optimal Codes and Related Topics*, Sozopol, Bulgaria, May 26 – June 1, (1995), 137–140.

[6] T.A.Gulliver and P.R.J.Östergård, Improved bounds for ternary linear codes of dimension 7, *IEEE Trans. Inf. Theory*, vol.43, no.5, (1997), 1377–1381.

[7] N. Hamada, A survey of recent work on characterization of minihypers in $PG(t,q)$ and nonbinary linear codes meeting the Griesmer bound, *J. Combin. Inform. Syst. Sci.* vol. 18, (1993), 161–191.

[8] N. Hamada and Y. Watamori, The nonexistence of some ternary linear codes of dimension 6 and the bound for $n_3(6,d)$, $1 \leq d \leq 243$, *Math. Japonica* 43, no.3 (1996), 577–593.

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

[10] R. Hill and C. Jones, The non-existence of ternary [47,6,29] codes, *In Proc. II Intern. Workshop OC'98*, Sozopol, Bulgaria, June 9–15, (1998), 90–96.