THE NONEXISTENCE OF TERNARY [231, 6, 153] CODES

NOBORU HAMADA

Department of Applied Mathematics, Osaka Women's University, Daisen-cho, Sakai, Osaka 590, Japan

Abstract. It is known (cf. Hamada [12] and Brouwer and van Eupen [2]) that (1) there is no ternary [230, 6, 153] code meeting the Griesmer bound but (2) there exists a ternary [232, 6, 153] code. This implies that $n_3(6, 153) = 231$ or 232, where $n_3(k, d)$ denotes the smallest value of n for which there exists a ternary $[n, k, d]$ code. The purpose of this paper is to prove that $n_3(6, 153) = 232$ by proving the nonexistence of ternary [231, 6, 153] codes.

1. Introduction

Let $V(n, q)$ be an n-dimensional vector space consisting of row vectors over the Galois field GF(q) of order q, where $n > 3$ and q is a prime power. A k-dimensional subspace C of $V(n, q)$ is called an $[n, k, d; q]$-code (or a q-ary linear code with length n, dimension k, and minimum distance d) if the minimum Hamming distance of the code C is equal to d. In the special case $q = 3$, an $[n, k, d; 3]$-code is also called a ternary $[n, k, d]$ code.

Let $n_q(k, d)$ denote the smallest value of n for which there exists an $[n, k, d; q]$-code. In the case $q = 3$, the value of $n_3(k, d)$ is known for $k \leq 5$ and for all d (cf. References). But in the case $q = 3$ and $k = 6$, the value of $n_3(6, d)$ is unknown for many integer d and a table of the bounds for $n_3(6, d)$, $1 \leq d \leq 243$, was given by Hamada [13]. Recently the table has been updated by Hamada and Watamori [16] using recent result. In the special case $q = 3$, $k = 6$ and $d = 153$, it is known (cf. Hamada [12] and Brouwer and van Eupen [2]) that $n_3(6, 153) = 231$ or 232. The purpose of this paper is to prove the following theorem.

Theorem 1.1. *There is no ternary* [231, 6, 153] *code and* $n_3(6, 153) = 232$.

In Section 2, we shall give the proof of Theorem 1.1. In Section 3, we shall give the proof of the following theorem which was written in Hamada and Watamori [16] as Theorem 6.3 without proof.

Theorem 1.2. *There is no ternary* $[204, 6, 135]$ *code.*

2. The proof of Theorem 1.1

In order to prove Theorems 1.1 and 1.2, we use the following two lemmas due to Hill and Newton [18] and the MacWilliams identities.

Lemma 2.1. *Suppose* C *is an* $[n, k, d; q]$*-code and suppose* $c \in C$ *has weight* w*, where* $w < dq/(q-1)$*. Then the residual code of* C *with respect to a codeword* c *is an* $[n-w, k-1, d_0; q]$*-code with* $d_0 \geq d - w + \lceil w/q \rceil$.

Lemma 2.2. *Let* C *be an* $[n, k, d; 3]$*-code with* $k \geq 2$*. Then:*
(1) $A_i = 0$ *or* 2 *for* $i > (3n-2d)/2$,
(2) if $A_i \geq 2$*, then* $A_j = 0$ *for* $j > 3n - 2d - i$ *and* $j \neq i$,
where A_i *denotes the number of codewords of weight* i *in the code* C.

Lemma 2.3. *Let* C *be an* $[n, k, d; q]$*-code and let* A_i *and* B_i *denote the number of codewords of weight* i *in the code* C *and in its dual code, respectively. Then*

$$\sum_{j=0}^{n-t} \binom{n-j}{t} A_j = q^{k-t} \sum_{j=0}^{t} \binom{n-j}{n-t} B_j \tag{2.1}$$

for $t = 0, 1, \cdots, n$.

Lemma 2.4. *If there exists a ternary* $[231, 6, 153]$ *code* C*, then* $w(c) =$ 153, 162, 176, 177, 230 *or* 231 *for any codeword* c *in* C*, where* $w(c)$ *denotes weight of the codeword* c.

Proof. Suppose there exists a ternary $[231, 6, 153]$ code C and suppose $c \in C$ has weight w, where $153 \leq w \leq 229$.

In the case $w = 154$, it follows from Lemma 2.1 that the residual code of C with respect to a codeword c is a ternary $[77, 5, d_0]$ code with $d_0 \geq 51$. This implies that there exists a ternary $[77, 5, d]$ code for some integer $d \geq 51$, which is contradictory to Table A.1 in Appendix A. Hence there is no codeword c in C such that $w(c) = 154$.

Similarly, it can be shown using Lemma 2.1 and Table A.1 that there is no codeword c in C such that $155 \leq w(c) \leq 161$, $163 \leq w(c) \leq 175$ or $178 \leq w(c) \leq 229$. This completes the proof.

From Lemma 2.2, we have the following lemma.

Lemma 2.5. *If there exists a ternary* $[231, 6, 153]$ *code* C, *then:*

(1) $A_i = 0$ *or* 2 *for* $i > 193$.

(2) If $A_{231} = 2$, *then* $A_j = 0$ *for* $j > 156$ *and* $j \neq 231$.

(3) If $A_{230} = 2$, *then* $A_j = 0$ *for* $j > 157$ *and* $j \neq 230$.

Lemma 2.6. *If there exists a ternary* $[231, 6, 153]$ *code* C, *then* $w(\mathrm{c}) = 153$, 162 *or* 177 *for any codeword* c *in* C *and* $(A_{153}, A_{162}, A_{177}) = (690, 2, 36)$ *and* $B_2 = 38$.

Proof. Let C be a ternary $[231, 6, 153]$ code. It follows from Lemmas 2.4 and 2.5 that $w(\mathrm{c}) = 153$, 162, 176, 177, 230 or 231 for any codeword c in C and $A_i = 0$ or 2 for $i = 230, 231$.

(A) In the case $A_{231} = 2$, it follows from Lemmas 2.5 and 2.3 ($n = 231, k = 6, q = 3, t = 1$) that $78A_{153} = 231(3^5 - 1) = 55902$, i.e., $A_{153} = 716.69\cdots$. This is a contradiction.

(B) In the case $A_{230} = 2$, it follows from Lemmas 2.5 and 2.3 that $78A_{153} + A_{230} = 55902$, i.e., $A_{153} = 55900/78 = 716.66\cdots$. This is a contradiction.

(C) In the case $A_{230} = A_{231} = 0$, it follows from (2.1) that

$$A_{153} + A_{162} + A_{176} + A_{177} = 728, \tag{2.2}$$

$$78A_{153} + 69A_{162} + 55A_{176} + 54A_{177} = 55902, \tag{2.3}$$

$$\binom{78}{2}A_{153} + \binom{69}{2}A_{162} + \binom{55}{2}A_{176} + \binom{54}{2}A_{177} = 2125200 + 81B_2. \tag{2.4}$$

Since A_{153}, A_{162}, A_{176}, A_{177} and B_2 are even, there exist nonnegative integers a, b, c, d and β such that $A_{153} = 2a$, $A_{162} = 2b$, $A_{176} = 2c$, $A_{177} = 2d$ and $B_2 = 2\beta$. It follows from (2.2) $\times$ 2691 $-$ (2.3) $\times$ 73 + (2.4) and (2.2) $\times$ 78 $-$ (2.3) that

$$161c = 9(189 + 9\beta - 20d), \tag{2.5}$$

$$9b + 23c + 24d = 441, \tag{2.6}$$

respectively. It follows from (2.5) and (2.6) that c must be a multiple of 27 and d must be a multiple of 3. Hence there exist two nonnegative integers c_0 and d_0 such that $c = 27c_0$, $d = 3d_0$, $161c_0 = 63 + 3\beta - 20d_0$ and $b + 69c_0 + 8d_0 = 49$. Since b and β are nonnegative integers, this implies that $c_0 = 0$, $d_0 = 6$, $\beta = 19$ and $b = 1$. Hence $A_{162} = 2b = 2$, $A_{176} = 54c_0 = 0$, $A_{177} = 6d_0 = 36$, $B_2 = 2\beta = 38$ and $A_{153} = 690$. This completes the proof.

Proof of Theorem 1.1. Suppose there exists a ternary $[231, 6, 153]$ code C. Then it follows from Lemma 2.6 that $w(\mathrm{c}) = 153$, 162 or 177 for any codeword c in C and $(A_{153}, A_{162}, A_{177}) = (690, 2, 36)$ and $B_2 = 38$. Hence there exists a ternary $[229, 5, 153]$ code $\overline{C}$ such that $w(\mathrm{c}) = 153$, 162 or 177 for any codeword c in $\overline{C}$ and $\overline{A}_{162} = 0$ or 2, where $\overline{A}_i$ denotes the number of codewords c in $\overline{C}$ such that $w(\mathrm{c}) = i$. It follows from (2.1) that

$$\overline{A}_{153} + \overline{A}_{162} + \overline{A}_{177} = 242, \tag{2.7}$$

$$76\overline{A}_{153} + 67\overline{A}_{162} + 52\overline{A}_{177} = 18320. \tag{2.8}$$

Hence it follows from (2.7) $\times$ 76 $-$ (2.8) that $3\overline{A}_{162} + 8\overline{A}_{177} = 24$.

(A) In the case $\overline{A}_{162} = 0$, it follows that $\overline{A}_{177} = 3$. Since $\overline{A}_{177}$ must be even, this is a contradiction.

(B) In the case $\overline{A}_{162} = 2$, it follows that $\overline{A}_{177} = 18/8 = 2.25$. This is a contradiction.

It follows from (A) and (B) that there is no ternary $[231, 6, 153]$ code. This completes the proof.

3. The proof of Theorem 1.2

Using Lemmas 2.1, 2.2 and Table A.1, we have the following two lemmas.

Lemma 3.1. *If there exists a ternary* $[204, 6, 135]$ *code* C, *then* $w(\mathrm{c}) =$ 135, 149, 150, 203 *or* 204 *for any codeword* c *in* C.

Lemma 3.2. *If there exists a ternary* $[204, 6, 135]$ *code* C, *then:*

(1) $A_i = 0$ *or* 2 *for* $i > 171$.

(2) if $A_{204} = 2$, *then* $A_j = 0$ *for* $j > 138$ *and* $j \neq i$.

(3) if $A_{203} = 2$, *then* $A_j = 0$ *for* $j > 139$ *and* $j \neq i$.

Proof of Theorem 1.2. Suppose there exists a ternary $[204, 6, 135]$ code C. It follows from Lemmas 3.1 and 3.2 that $A_{203} = 0$ or 2 and $A_{204} = 0$ or 2.

(A) In the case $A_{204} = 2$, it follows from Lemmas 3.1, 3.2 and 2.3 ($n = 204, k = 6, q = 3, t = 1$) that $69A_{135} = 204(3^5 - 1)$, i.e., $A_{135} = 49368/69 = 715.47\cdots$. This is a contradiction.

(B) In the case $A_{203} = 2$, it follows from Lemmas 3.1, 3.2 and 2.3 ($t = 1$) that $69A_{135} + A_{203} = 49368$. This implies that $A_{135} = 49366/69 = 715.44\cdots$, a contradiction.

(C) In the case $A_{203} = A_{204} = 0$, it follows from Lemmas 3.1 and 2.3 $(t = 0, 1, 2)$ that

(3.1) $$A_{135} + A_{149} + A_{150} = 728,$$

(3.2) $$69A_{135} + 55A_{149} + 54A_{150} = 49368,$$

(3.3) $$\binom{69}{2}A_{135} + \binom{55}{2}A_{149} + \binom{54}{2}A_{150} = 1656480 + 81B_2.$$

It follows from (3.1)×3795−(3.2)×123+(3.3)×2 and (3.1)×69−(3.2) that $15A_{150} = 3456 + 162B_2$ and $14A_{149} + 15A_{150} = 864$. Since $B_2 \geq 0$, it follows that $A_{150} > 230$ and $14A_{149} = 864 - 15A_{150} < -2586$, a contradiction. This completes the proof.

Acknowledgements. This research was partially supported by Grant-in-Aid for Scientific Research of the Ministry of Education, Science and Culture under Contract Numbers 304-3508-07640326.

Appendix A. Table of the values of $n_3(5, d)$, $1 \leq d \leq 81$

Let $d = 3^4 - \sum_{i=0}^{3} \epsilon_i 3^i$, $g = v_5 - \sum_{i=0}^{3} \epsilon_i v_{i+1}$ and $\epsilon = (\epsilon_0, \epsilon_1, \epsilon_2, \epsilon_3)$, where $\epsilon_i = 0$, 1 or 2 for $i = 0, 1, 2, 3$. Let $n = n_3(5, d)$ denote the smallest length of codes of dimension 5 and minimum distance d over the Galois field $GF(3)$. The value of $n_3(5, d)$, $1 \leq d \leq 81$, is given in Table A.1.

Table A.1. The values of $n_3(5,d)$ for $1 \leq d \leq 81$.

d	ϵ	g	n	d	ϵ	g	n	d	ϵ	g	n
1	2222	5	5	28	2221	45	45	55	2220	85	85
2	1222	6	6	29	1221	46	46	56	1220	86	86
3	0222	7	8	30	0221	47	47	57	0220	87	87
4	2122	9	9	31	2121	49	49	58	2120	89	89
5	1122	10	10	32	1121	50	51	59	1120	90	90
6	0122	11	11	33	0121	51	52	60	0120	91	91
7	2022	13	14	34	2021	53	53	61	2020	93	94
8	1022	14	15	35	1021	54	54	62	1020	94	95
9	0022	15	16	36	0021	55	55	63	0020	95	96
10	2212	18	18	37	2211	58	59	64	2210	98	98
11	1212	19	19	38	1211	59	60	65	1210	99	99
12	0212	20	20	39	0211	60	61	66	0210	100	100
13	2112	22	23	40	2111	62	63	67	2110	102	102
14	1112	23	24	41	1111	63	64	68	1110	103	103
15	0112	24	25	42	0111	64	65	69	0110	104	104
16	2012	26	27	43	2011	66	67	70	2010	106	106
17	1012	27	28	44	1011	67	68	71	1010	107	107
18	0012	28	29	45	0011	68	69	72	0010	108	108
19	2202	31	32	46	2201	71	72	73	2200	111	111
20	1202	32	33	47	1201	72	73	74	1200	112	112
21	0202	33	34	48	0201	73	74	75	0200	113	113
22	2102	35	36	49	2101	75	76	76	2100	115	115
23	1102	36	37	50	1101	76	77	77	1100	116	116
24	0102	37	38	51	0101	77	78	78	0100	117	117
25	2002	39	41	52	2001	79	79	79	2000	119	119
26	1002	40	42	53	1001	80	80	80	1000	120	120
27	0002	41	43	54	0001	81	81	81	0000	121	121

References

1. G. T. Bogdanova and I. G. Boukliev, New linear codes of dimension 5 over GF(3), Proceedings of the Fourth International Workshop on Algebraic and Combinatorial Coding Theory, Novgorod, Russia, September 1994, 41–43.
2. A. E. Brouwer and M. van Eupen, The correspondence between projective codes and 2–weight codes, to appear in Designs, Codes and Cryptography.
3. A. E. Brouwer and N. J. A. Sloane, "Tables of Codes", in "Handbook of Coding Theory", edited by R. Brualdi, W. C. Huffman and V. Pless, North–Holland, Amsterdam, to appear.
4. M. van Eupen, Some new results for ternary linear codes of dimension 5 and 6, to appear in IEEE Trans. Inform. Theory.
5. M. van Eupen, N. Hamada and Y. Watamori, The nonexistence of ternary $[50,5,32]$ codes, Designs, Codes and Cryptography 7 (1995), 235–237.
6. M. van Eupen and R. Hill, An optimal ternary $[69,5,45]$ code and related codes, Designs, Codes and Cryptography 4 (1994), 271–282.
7. T. A. Gulliver, Two new optimal ternary two-weight codes and strongly regular graphs, to appear in Discrete Math..
8. T. A. Gulliver, New optimal ternary linear codes of dimension 6, Ars Combin. 40 (1995), 97–108.
9. T. A. Gulliver, New optimal ternary linear codes, IEEE Tran. Inform. Theory 41 (1995), 1182–1185.
10. T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and $(p-1)/p$ quasi–cyclic codes over $GF(3)$ and $GF(4)$, IEEE Trans. Inform. Theory 38 (1992), 1369–1374.
11. T. A. Gulliver and V. K. Bhargava, New good rate $(m-1)/pm$ ternary and quaternary quasi–cyclic codes, to appear in Designs, Codes and Cryptography.
12. N. Hamada, A characterization of some $[n,k,d;q]$–codes meeting the Griesmer bound using a minihyper in a finite projective geometry, Discrete Math. 116 (1993a), 229–268.
13. N. Hamada, A survey of recent work on characterization of minihypers in $\mathrm{PG}(t,q)$ and nonbinary linear codes meeting the Griesmer bound, J. Combin. Inform. Syst. Sci. 18 (1993b), 161–191.
14. N. Hamada, A necessary and sufficient condition for the existence of some ternary $[n,k,d]$ codes meeting the Griesmer bound, to appear in Designs, Codes and Cryptography.
15. N. Hamada and T. Helleseth, Construction of some optimal ternary codes and the uniqueness of $[294,6,195;3]$–codes meeting the Griesmer bound, Finite Fields and Their Applications 1 (1995), 458–468.
16. N. Hamada and Y. Watamori, The nonexistence of some ternary linear codes of dimension 6 and the bounds for $n_3(6,d)$, $1 \leq d \leq 243$, Math. Japonica 43 (1996). (in press)
17. N. Hamada and Y. Watamori, The nonexistence of $[71,5,46;3]$–codes, to appear in J. Statist. Plann. Inference.
18. R. Hill and D. E. Newton, Optimal ternary linear codes, Designs, Codes and Cryptography 2 (1992), 137–157.