Title	Optimal linear codes over GF(5)(Semigroups, Formal Languages and Combinatorics on Words)
Author(s)	Fukui, Masaharu; Maruta, Tatsuya
Citation	数理解析研究所講究録 (1995), 910: 5-13
Issue Date	1995-05
URL	http://hdl.handle.net/2433/59545
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
910巻 1995年 5-13

Optimal linear codes over $GF(5)$

Masaharu Fukui (福井 雅晴)
The Graduate School of Mathematics
Meijo University
and
Tatsuya Maruta (丸田 辰哉)
Meijo University, Junior College Division

1 Introduction

Let $GF(q)$ denote the Galois field of q elements and let $V(n,q)$ denote the row vector space of ordered n-tuples with entries in $GF(q)$. The (*Hamming*) *distance* $d(x,y)$ between two row vectors x and y is definded to be the number of co-ordinate places in which they differ. The *weight* $wt(x)$ of a row vector x is definded to be the number of non-zero entries of x. Note that

$$wt(x) = d(x,0).$$

A *linear* $[n,k]_q$*-code* C is a k-dimensional subspace of $V(n,q)$. The row vectors of C are called *codewords*. The *minimum distance* of C is the smallest value of the distances between distinct codewords. A linear $[n,k]_q$-code with the minimum distance d is called linear $[n,k,d]_q$-code. We deal with only linear codes, so that is called simply an $[n,k]_q$-code or an $[n,k,d]_q$-code. A *generator matrix* of an $[n,k]_q$-code C is a $k \times n$ matrix whose k row vectors form a basis of C.

Next we explain about the error correcting of codewords. Suppose that some noises invade to a codeword c, transmitted as a message, and that c changed c'. Then the following is well known: c' can be corrected to c if at most $\lfloor \frac{d-1}{2} \rfloor$ errors occur, where $\lfloor x \rfloor$ denotes the largest integer smaller than or equal to x.

A good code will have small n (for fast transmission of messages), large k (to enable transmission of a wide variety of messages) and large d (to correct many errors). Now we consider the following Problem:

Problem.

Optimize one of the parameters n, k and d for given values of the other two.

In particular, the problem of optimizing n, i.e. finding the smallest value of n for which there exists an $[n, k, d]_q$-code for given k, d (we denote the value by $n_q(k, d)$), is the most natural, because later the Griesmer bound provides an important lower bound on $n_q(k, d)$. An $[n_q(k, d), k, d]_q$-code is called *optimal*.

Set $g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer larger than or equal to x. The following theorem is well known:

Theorem 1.1. (The Griesmer bound)

$$n_q(k, d) \geq g_q(k, d).$$

Theorem 1.2. (R.Hill [4])

For given q and k, the Griesmer bound is attaind if $d \geq (k-2)q^{k-1} + 1$.

By Theorem 1.2, for a fixed dimension k, $n_q(k, d)$ is equal to $g_q(k, d)$ for all sufficiently large values of d. So the problem of finding $n_q(k, d)$ is a finite one. The values of $n_q(k, d)$ are already known for the following $k(\leq 4)$, q:

(i) $k \leq 2$ for all q and d,

(ii) $k = 3$, $q \leq 9$ for all d,

(iii) $k = 4$, $q \leq 4$ for all d,

(iv) $k = 4$, $q = 5$ for all but 54 values of d (c.f. I.G.Boukliev and S.N.Kapralov [1]).

We resolved eight of these fifty four cases in (iv), and we improved one of the remaining ones. Table 1 is arranged to put contents of [1] and updated values or bounds together. Details are in Section 3.

In Section 3 we only consider optimal codes for $q = 5$ and $k = 4$. Note that for $k \leq 2$, $n_5(k, d) = g_5(k, d)$ for all d by Theorem 1.2. For $k = 3$, the values of $n_5(3, d)$ are as follows (c.f. R.Hill [4]):

$$n_5(3, d) = \begin{cases} g_5(3, d) + 1 & \text{for} \quad d = 5, 9, 10, 13, 14, 15, \\ g_5(3, d) & \text{for other values of } d. \end{cases}$$

In Section 2 we give some preliminary results.

2 Preriminaries

Theorem 2.1. (T.Maruta [7])
For $q \geq 4$ there dose not exist an $[n, 4, n+1-q^2]_q$-code with $n = \lceil q^3 - q - \sqrt{q} - 2 \rceil$.

Lemma 2.2. (P.P.Greenough and R.Hill [3])
(i) $n_q(k,d) \leq n_q(k,d+1) - 1$, (ii) $n_q(k,d) \geq n_q(k,d-1) + 1$.

Definition.
Let C be an $[n,k]_q$-code. The *dual* code of C, denoted by $C^\perp$, is given by

$$C^\perp = \{v \in V(n,q) \mid (v,c) = 0 \text{ for all } c \in C\},$$

where (x,y) is the inner product as usual.

Theorem 2.3. (The MacWilliams identities)
Let C be an $[n,k]_q$-code. Let A_i and B_i denote the number of codewords of weight i in C and in the dual code $C^\perp$ respectively. Then the A_i's and B_i's satisfy

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

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

Definition.
Let G be a generator matrix of a linear $[n,k,d]_q$-code C. Then the *residual* code of C with respect to a codeword c, denoted by $\mathrm{Res}(C,c)$, is the code generated by the restriction of G to the columns where c has a zero entry.

Theorem 2.4. (R.Hill [4])
Suppose C is an $[n,k,d]_q$-code and suppose $c \in C$ has weight w , where $d > \frac{w(q-1)}{q}$. Then $\mathrm{Res}(C,c)$ is an $[n-w, k-1, d^\circ]_q$-code with $d^\circ \geq d - w + \lceil \frac{w}{q} \rceil$.

Definition.
A linear code is called *projective* if no two columns of a generator matrix are linearly dependent.

Theorem 2.5. (R.Hill [4])
Suppose $d \leq q^{k-1}$ and that C is an $[n,k,d]_q$-code which attains the Griesmer bound. Then C is projective.

Note that the columns of a generator matrix of a projective $[n, k]_q$-code may be regarded as distinct points of the projective space $PG(k-1, q)$.

Lemma 2.6. (R.Hill [4])
There exists a projective $[n, k, d]_q$-code if and only if there exists an n-set L of $PG(k-1, q)$ such that $|L \cap \Pi| \leq n - d$ for any hyperplane Π of $PG(k-1, q)$ and that equality holds for some hyperplane.

In Lemma 2.6, take the n columns of a generator matrix as an n-set L , then it is easy to verify that this set satisfies the condition in Lemma 2.6. Consequently when we consider problems with respect to a code, we may regard the column vectors of a generator matrix of the code as points of the corresponding projective space.

Definition.
For a given $[n, k, d]_q$-code C, an i-line (resp. an i-plane) is a line (resp. a plane) containing exactly i points of C. Denoted by a_i the number of planes Π_i of $PG(k-1, q)$ with $|C \cap \Pi_i| = i$.

Let C be an $[n, k, d]_q$-code which attains the Griesmer bound with $d \leq q^{k-1}$. By Theorem 2.5 C is projective. Then, by Theorem 2.3 We have the following equalities:

$$\sum_{i=0}^{n-d} a_i = \frac{q^k - 1}{q - 1},$$

$$\sum_{i=1}^{n-d} i\, a_i = n\, \frac{q^{k-1} - 1}{q - 1},$$

$$\sum_{i=2}^{n-d} i\,(i-1)\, a_i = n\,(n-1)\, \frac{q^{k-2} - 1}{q - 1}.$$

At the following two lemmas we set $k = 4$, and we assume that any plane Π of $PG(3, q)$ meets C in at most m points.

Lemma 2.7.
If there is a t-line, then we have $t \leq \frac{1}{q}\{m(q+1) - |C|\}$.

Lemma 2.8.
$a_i > 1$ implies $i \geq \frac{1}{2}\{|C| - m(q-1)\}$.

3 Optimal linear codes over $GF(5)$ with k=4

In this section, we explain about Table 1 and our new results. Table 1 is the updated best bounds or values of $n_5(4,d)$. For comparison, we also list the values of $g_5(4,d)$. For all d not listed, in Table 1, it is already known that the Griesmer bound is attained. In the table, the values labeled a are due to I.G.Boukliev [2], labeled b are our new results, and others are given by I.G.Boukliev and S.N.Kapralov [1]. Note that the lower bounds are given either by the Griesmer bound (Theorem 1.1) or by proving the nonexistence of codes attaining the Griesmer bound and applying Lemma 2.2. On the other hand, the upper bounds are given by constructing codes with suitable parameters.

Next we prove some of our new results.

Theorem 3.1.

There exist no codes which have the following parameters:

(i) $[44,4,34]_5$, (ii) $[50,4,39]_5$, (iii) $[106,4,84]_5$, (iv) $[110,4,87]_5$, (v) $[115,4,91]_5$.

Proof. (v) follows from Theorem 2.1. We only prove (ii) here, because the proof of (ii) is comparatively easy. The other results are also proved similarly making use of the concept of projective geometry.

Let C be a $[50,4,39]_5$-code. By Theorem 2.5 C is projective. By Theorem 2.4 $A_i > 0$ implies $i \in \{0,39,40,44,45,49,50\}$. So, $a_i > 0$ implies $i \in \{11,10,6,5,1,0\}$. Now we have the following Lemma:

Lemma 3.2.

(i) $|C \cap \Pi| \leq 11$, for any plane Π of $PG(3,5)$,

(ii) There are no 4-, 5- and 6-line,

(iii) $a_0 = 0$,

(iv) $a_1 = 0$.

Proof. (i): This follows from Lemma 2.6.

(ii): This follows from Lemma 2.7.

(iii): By Lemma 2.8, note that $a_0 > 0$ implies $a_0 = 1$. Suppose $a_0 = 1$. Let L be a line containd in the 0-plane, and consider the six planes containing L. Then from (i) and $|C| = 11 \times 4 + 6$, we cannot have a 1- and 5-plane. Hence $a_1 = a_5 = 0$. Then we have the unique solution

$$a_0 = 1, \quad a_6 = \frac{75}{2}, \quad a_{10} = -\frac{65}{2}, \quad a_{11} = 150,$$

which contradicts that a_i's must be non-negative integers.
(iv): Note that $a_1 > 0$ implies $a_1 = 1$. Suppose $a_1 = 1$, then we have the unique solution

$$a_1 = 1, \quad a_5 = 25, \quad a_6 = 1, \quad a_{10} = 1, \quad a_{11} = 128.$$

Let Π_5 and Π_{10} be a 5-plane and the 10-plane respectively, and let L' be the intersection of Π_5 and Π_{10}. Set $C' = C \setminus L'$. Consider the six planes containing L'. If L' is an i-line, then we have $|C'| = 35 + i$ for $i = 0, 1, 2, 3$, from (ii). But we cannot find the remaining four planes containing L' from the unique solution. □

By Lemma 3.2(iii),(iv), $a_i > 0$ implies $i \in \{11, 10, 6, 5\}$. Then the MacWilliams identities yield a contradiction. □

Remark

Note that there exist no $[45, 4, 35]_5$-, $[51, 4, 40]_5$-, $[111, 4, 88]_5$- and $[116, 4, 92]_5$-codes by Lemma 2.2 and Theorem 3.1.

For the unresolved cases of $k = 4$ and $q = 5$, we can show that optimal codes with the following parameters, if they exist, must have the unique weight distributions indicated:

$$\text{a } [39, 4, 30]_5\text{-code:} \quad A_{30} = 468, \quad A_{35} = 156.$$

$$\text{a } [70, 4, 55]_5\text{-code:} \quad A_{55} = 512, \quad A_{60} = 88, \quad A_{65} = 24.$$

If there exist both codes with above parameters, then we can result $n_5(4, 28) = 37$, $n_5(4, 29) = 38$, $n_5(4, 52) = 67$, $n_5(4, 53) = 68$, and $n_5(4, 54) = 69$.

Table 1. Values and bounds for $n_5(4,d)$.

d	$g_5(4,d)$	$n_5(4,d)$	d	$g_5(4,d)$	$n_5(4,d)$
1	4	4	32	42	42—43
2	5	5	33	43	43—44
3	6	6	34	44	45^b
4	7	8	35	45	46^b–47
5	8	9	36	47	47—48
6	10	10	37	48	48—49
7	11	11	38	49	49—50
8	12	12	39	50	51^b
9	13	14	40	51	52^b
10	14	15	41	53	54
11	16	16	42	54	55
12	17	18	43	55	56^a
13	18	19	44	56	57^a
14	19	20	45	57	58^a
15	20	21	46	59	60
16	22	22	47	60	61
17	23	23	48	61	62
18	24	24	49	62	63
19	25	25	50	63	64
20	26	26	51	66	66
21	28	29	52	67	67—68
22	29	30	53	68	68—69
23	30	31	54	69	69—70
24	31	32	55	70	70—71
25	32	33—34	56	72	72
26	35	35	57	73	73
27	36	36^a	58	74	74
28	37	37—38	59	75	75
29	38	38—39	60	76	76
30	39	39—40	61	78	79
31	41	41—42	62	79	80

63	80	81	97	122	122
64	81	82	98	123	123
65	82	83			
66	84	85			
67	85	86	146	184	184—185[a]
68	86	87[a]	147	185	185—186[a]
69	87	88[a]	148	186	186—187[a]
70	88	89[a]	149	187	187—188[a]
71	90	91	150	188	188—189[a]
72	91	92	151	191	191
73	92	93	152	192	192
74	93	94	153	193	193
75	94	95	154	194	194
76	97	97	155	195	195
77	98	98	156	197	197
78	99	99	157	198	198
79	100	100	158	199	199
80	101	101	159	200	200
81	103	103—104	160	201	201
82	104	104—105	161	203	203—204
83	105	105—106	162	204	204—205
84	106	107[b]	163	205	205—206
85	107	108	164	206	206—207
86	109	109—110	165	207	207—208
87	110	111[b]	166	209	209—210
88	111	112[b]	167	210	210—211
89	112	113	168	211	211—212
90	113	114	169	212	212—213
91	115	116[b]	170	213	213—214
92	116	117[b]	171	215	215—216
93	117	118	172	216	216—217
94	118	119	173	217	217—218
95	119	120	174	218	218—219
96	121	121	175	219	219—220

References

[1] I.G.Boukliev and S.N.Kapralov: Optimal linear codes of dimension 4 over F_5, preprint.

[2] I.G.Boukliev: private communication.

[3] P.P.Greenough and R.Hill: Optimal linear codes over $GF(4)$, *Discrete Math.* 125, 187-199.

[4] R.Hill: Optimal linear codes, in: C.Mitchell ed., Proc. 2nd IMA Conf. on Cryptography and Coding, Oxford Univ. Press, Oxford 1992, 75-104.

[5] I.Landgev, T.Maruta and R.Hill: On the nonexistence of quaternary [51,4,34] codes, preprint.

[6] F.J.MacWilliams and N.J.A.Sloane: The Theory of Error-Correcting Codes, North-Holland Mathematical Library Vol.16, Amsterdam, 1977.

[7] T.Maruta: On the non-existence of linear codes attaining the Griesmer bound, preprint.