Serdica J. Computing **5** (2011), 199–206

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

NOTE ON AN IMPROVEMENT OF THE GRIESMER BOUND FOR q-ARY LINEAR CODES

Noboru Hamada, Tatsuya Maruta*

Abstract. Let $n_q(k,d)$ denote the smallest value of n for which an $[n,k,d]_q$ code exists for given integers k and d with $k \geq 3$, $1 \leq d \leq q^{k-1}$ and a prime or a prime power q. The purpose of this note is to show that there exists a series of the functions $h_{3,q}, h_{4,q}, \ldots, h_{k,q}$ such that $n_q(k,d)$ can be expressed as $n_q(k,d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil + \sum_{j=3}^{k} h_{j,q}(e_{k-j}, e_{k-j+1}, \ldots, e_{k-2})$ for some ordered $(k-1)$-tuple $(e_0, e_1, \ldots, e_{k-2})$ with $0 \leq e_0, e_1, \ldots, e_{k-2} \leq q-1$ satisfying $d = q^{k-1} - \sum_{i=0}^{k-2} e_i q^i$.

1. Introduction. Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements, where n is an integer ≥ 4 and q is a prime or a prime power. A q-ary linear code $\mathcal{C}$ of length n and dimension k, called an $[n,k]_q$ code, is a k-dimensional subspace of $\mathbb{F}_q^n$, where $n > k \geq 3$. An $[n,k]_q$ code $\mathcal{C}$ with minimum

ACM Computing Classification System (1998): E.4.
Key words: linear codes, Griesmer bound.
*This research was partially supported by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science under Contract Number 20540129.

Hamming distance d is referred to as an $[n,k,d]_q$ code. Let $G=[\boldsymbol{g}_1^{\mathrm{T}},\boldsymbol{g}_2^{\mathrm{T}},\cdots,\boldsymbol{g}_n^{\mathrm{T}}]$ be a $k\times n$ generator matrix of an $[n,k,d]_q$ code $\mathcal{C}$ with $\boldsymbol{g}_1,\cdots,\boldsymbol{g}_n\in\mathbb{F}_q^k$, where $\boldsymbol{g}^{\mathrm{T}}$ denotes the transpose of the vector $\boldsymbol{g}$. If there is no zero vector in $\{\boldsymbol{g}_1,\cdots,\boldsymbol{g}_n\}$, an $[n,k,d]_q$ code $\mathcal{C}$ is called a *nontrivial code*. A fundamental problem in coding theory is to solve the following problem.

Problem 1. *Find the smallest value of n, denoted by $n_q(k,d)$, for which an $[n,k,d]_q$ code exists for given integers q,k,d.*

An $[n,k,d]_q$ code is called *optimal* if $n=n_q(k,d)$. There is a lower bound on $n_q(k,d)$ called the Griesmer bound [2], [5]:

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

where $\lceil x\rceil$ denotes the smallest integer greater than or equal to x. A $[g_q(k,d),k,d]_q$ code is called a *Griesmer code*. In this note, we consider the case $k\geq 3$, $q\geq 3$ and $1\leq d\leq q^{k-1}$. In this case, d and $g_q(k,d)$ can be expressed as follows:

$$d = q^{k-1}-\sum_{i=0}^{k-2}e_iq^i, \tag{1.1}$$

$$g_q(k,d) = \theta_{k-1}-\sum_{i=0}^{k-2}e_i\theta_i \tag{1.2}$$

using some ordered $(k-1)$-tuple $(e_0,e_1,\ldots,e_{k-2})$ in $E(k,q)$, where $E(k,q)$ is the set of all ordered $(k-1)$-tuple $(e_0,e_1,\ldots,e_{k-2})$ such that $0\leq e_i\leq q-1$ and $\theta_i=(q^{i+1}-1)/(q-1)$ for $0\leq i\leq k-2$. In the special case $k=3$, d can be expressed as follows:

$$d=q^2-(e_0+e_1q).$$

Note that (1.2) shows that $g_q(k,d)$ is a function of $k,e_0,e_1,\ldots,e_{k-2}$ and q. Now, we define the *Hamada's function* $h_{k,q}(e_0,e_1,\ldots,e_{k-2})$ for $k\geq 3$ as follows:

$$h_{3,q}(e_0,e_1) = n_q(3,d)-g_q(3,d), \tag{1.3}$$

$$h_{k,q}(e_0,e_1,\cdots,e_{k-2}) = n_q(k,d)-g_q(k,d)-\sum_{j=3}^{k-1}h_{j,q}(e_{k-j},e_{k-j+1},\cdots,e_{k-2}) \tag{1.4}$$

for $k \geq 4$, where d is uniquely determined from k, q and $(e_0, e_1, \ldots, e_{k-2}) \in E(k, q)$ by (1.1).

Theorem 1.1 *For given $q \geq 3$, $k \geq 3$ and for any $(e_0, e_1, \cdots, e_{k-2}) \in E(k, q)$,*

$$h_{k,q}(e_0, e_1, \cdots, e_{k-2}) \geq 0 \tag{1.5}$$

holds and $n_q(k, d)$ for d satisfying (1.1) can be expressed as

$$n_q(k, d) = g_q(k, d) + \sum_{j=3}^{k} h_{j,q}(e_{k-j}, e_{k-j+1}, \cdots, e_{k-2}). \tag{1.6}$$

Remark 1.2. The formula (1.6), called the *Hamada's formula*, shows that there exists a series of Hamada's functions $h_{3,q}, h_{4,q}, \ldots, h_{k,q}$ such that $n_q(k, d)$ can be expressed as (1.6), where $h_{j,q} = h_{j,q}(e_{k-j}, e_{k-j+1}, \ldots, e_{k-2})$. Hence Problem 1 for $1 \leq d \leq q^{k-1}$ is equivalent to the following problem.

Problem 2. *Find the Hamada's function $h_{k,q} = h_{k,q}(e_0, e_1, \cdots, e_{k-2})$ such that $n_q(k, d)$ can be expressed as (1.6) for given integers $k \geq 3$ and $q \geq 3$.*

Example 1.3 [cf. Appendix]**.** *For $q = 3$ and $3 \leq k \leq 5$, $h_{k,3}(e_0, e_1, \ldots, e_{k-2})$ is given by*

(1) $h_{k,3}(e_0, e_1, \cdots, e_{k-2}) = 0$ *or* 1 *for all* $(e_0, e_1, \cdots, e_{k-2}) \in E(k, 3)$,

(2) $h_{3,3}(e_0, e_1) = 1$ *if and only if* $(e_0, e_1) = (0, 2)$,

(3) $h_{4,3}(e_0, e_1, e_2) = 1$ *if and only if* $(e_0, e_1, e_2) \in \{(0, 2, 2), (2, 1, 1), (1, 1, 1), (0, 1, 1)\}$,

(4) $h_{5,3}(e_0, e_1, e_2, e_3) = 1$ *if and only if* $(e_0, e_1, e_2, e_3) \in \{(0, 2, 2, 2),\ (2, 1, 1, 2),\ (1, 1, 1, 2),\ (0, 1, 1, 2),\ (2, 0, 1, 2),\ (1, 0, 1, 2),\ (0, 0, 1, 2),\ (2, 0, 0, 2),\ (1, 0, 0, 2),\ (0, 0, 0, 2),\ (1, 1, 2, 1),\ (0, 1, 2, 1),\ (2, 2, 0, 1),\ (1, 2, 0, 1),\ (0, 2, 0, 1),\ (2, 1, 0, 1),\ (1, 1, 0, 1),\ (0, 1, 0, 1),\ (2, 0, 2, 0),\ (1, 0, 2, 0),\ (0, 0, 2, 0)\}$.

Example 1.4. *In the case $q = 4$ and $3 \leq k \leq 4$, $h_{k,4}(e_0, e_1, \cdots, e_{k-2})$ is given by*

(1) $h_{k,4}(e_0, e_1, \cdots, e_{k-2}) = 0$ *or* 1 *for all* $(e_0, e_1, \cdots, e_{k-2}) \in E(k, 4)$,

(2) $h_{3,4}(e_0, e_1) = 1$ *if and only if* $(e_0, e_1) \in \{(1, 2), (0, 2)\}$,

(3) $h_{4,4}(e_0, e_1, e_2) = 1$ *if and only if* $(e_0, e_1, e_2) \in \{(1, 3, 3),\ (0, 3, 3),\ (1, 2, 3),\ (0, 2, 3),\ (3, 0, 3),\ (2, 0, 3),\ (1, 0, 3),\ (0, 0, 3),\ (1, 2, 2),\ (0, 2, 2),\ (3, 2, 1),\ (2, 2, 1),\ (1, 2, 1),\ (0, 2, 1),\ (3, 1, 1),\ (2, 1, 1),\ (1, 1, 1),\ (0, 1, 1)\}$.

Example 1.5. *In the case* $q = 5$ *and* $3 \le k \le 4$, $h_{k,5}(e_0, e_1, \cdots, e_{k-2})$ *is given by*

(1) $h_{k,5}(e_0, e_1, \cdots, e_{k-2}) = 0$ *or* 1 *for all* $(e_0, e_1, \cdots, e_{k-2}) \in E(k, 5)$,

(2) $h_{3,5}(e_0, e_1) = 1$ *if and only if* $(e_0, e_1) \in \{(0, 4), (1, 3), (0, 3), (2, 2), (1, 2), (0, 2)\}$,

(3) $h_{4,5}(e_0, e_1, e_2) = 1$ *if* $(e_0, e_1, e_2) \in \{(1, 4, 4),\ (0, 4, 4),\ (1, 3, 4),\ (0, 3, 4),\ (3, 2, 4),\ (2, 2, 4),\ (1, 2, 4),\ (0, 2, 4),\ (0, 0, 4),\ (4, 3, 3),\ (3, 3, 3),\ (2, 3, 3),\ (1, 3, 3),\ (0, 3, 3),\ (4, 2, 3),\ (3, 2, 3),\ (2, 2, 3),\ (1, 2, 3),\ (0, 2, 3),\ (2, 3, 1),\ (1, 3, 1),\ (0, 3, 1),\ (4, 2, 1),\ (3, 2, 1),\ (2, 2, 1),\ (1, 2, 1),\ (0, 2, 1),\ (4, 1, 1),\ (3, 1, 1),\ (2, 1, 1),\ (1, 1, 1),\ (0, 1, 1)\}$,

(4) $h_{4,5}(e_0, e_1, e_2) = 0$ *or* 1 *for* $(e_0, e_1, e_2) \in \{(4, 3, 1),\ (3, 3, 1)\}$ (still unknown).

Remark 1.6. (1) $n_3(6, d)$ for $1 \le d \le 243$ is not determined for 74 values of d (hence $h_{6,3}(e_0, e_1, e_2, e_3, e_4)$ is unknown for the 74 cases), see [4].
(2) It is known that $h_{6,3}(e_0, 0, 1, 2, 2) = 2$ for $e_0 = 0, 1, 2$ since $n_3(6, d) = g_3(6, d) + 2$ for $d = 16, 17, 18$ and since $n_3(5, 6) = g_3(5, 6)$. Thus, $h_{k,3}(e_0, e_1, \cdots, e_{k-2}) \ge 2$ could happen for $k \ge 6$.
(3) $h_{3,q}$ can be determined from the results on (n, r)-arcs in $\mathrm{PG}(2, q)$ since $(n, n - d)$-arcs and projective $[n, 3, d]_q$ codes are equivalent objects (recall that Griesmer $[n, k, d]_q$ codes with $d \le q^{k-1}$ are projective), see [1]. For example, $h_{3,q}(0, 2) = 1$ holds for $q \ge 3$ from the nonexistence of $(q^2 - q - 1, q - 1)$-arcs and the existence of $(q^2 - q, q)$-arcs in $\mathrm{PG}(2, q)$. But to find the largest n for which an (n, r)-arc exists in $\mathrm{PG}(2, q)$ for given r is a quite difficult problem in general, see [3].

Proof of Theorem 1.1.

Lemma 2.1. *For an* $[n, k, d]_q$ *code, it holds that* $n \ge g_q(k, d) + t$ *if* $n_q(k - 1, d') = g_q(k - 1, d') + t$ *for some integer* t, *where* $d' = \lceil d/q \rceil$.

P r o o f. Let $\mathcal{C}$ be an $[n, k, d]_q$ code with $d' = \lceil d/q \rceil$, and let $\mathcal{C}'$ be a residual $[n-d, k-1, d']_q$ code. From the assumption, we get

$$n - d \geq n_q(k-1, d') = g_q(k-1, d') + t. \tag{2.1}$$

Since $d' = \lceil d/q \rceil \geq d/q$, it holds that $d'/q^i \geq d/q^{i+1}$, so we have

$$g_q(k-1, d') = \sum_{i=0}^{k-2} \lceil d'/q^i \rceil \geq \sum_{i=0}^{k-2} \lceil d/q^{i+1} \rceil = \sum_{i=1}^{k-1} \lceil d/q^i \rceil.$$

Hence, from (2.1), we get

$$n - d \geq \sum_{i=1}^{k-1} \lceil d/q^i \rceil + t, \text{ i.e., } n \geq g_q(k, d) + t. \qquad \square$$

Remark 2.2. If d is an integer given by (1.1), then

$$d' = q^{k-2} - \sum_{i=1}^{k-2} e_i q^{i-1}. \tag{2.2}$$

P r o o f o f T h e o r e m 1.1. Since $n_q(k, d) \geq g_q(k, d)$, it is obvious from (1.3) that $h_{3,q}(e_0, e_1) \geq 0$. Hence (1.5) holds in the case and

$$n_q(3, d) = g_q(3, d) + h_{3,q}(e_0, e_1) \text{ for } d = q^2 - (e_0 + e_1 q).$$

In the case $k = 4$, $n_q(3, d')$ for

$$d = q^3 - (e_0 + e_1 q + e_2 q^2), \quad d' = \lceil d/q \rceil = q^2 - (e_1 + e_2 q) \tag{2.3}$$

is expressed as

$$n_q(3, d') = g_q(3, d') + h_{3,q}(e_1, e_2). \tag{2.4}$$

Hence it follows from (2.3), (2.4) and Lemma 2.1 that

$$n_q(4, d) \geq g_q(4, d) + h_{3,q}(e_1, e_2), \quad \text{i.e., } h_{4,q}(e_0, e_1, e_2) \geq 0.$$

In the case $k \geq 5$, we shall prove (1.5) using induction on k. In this case, d and d' can be expressed as (1.1) and (2.2), respectively. Since

$$n_q(k-1, d') = g_q(k-1, d') + \sum_{j=3}^{k-1} h_{j,q}(e_{k-j}, e_{k-j+1}, \ldots, e_{k-2}),$$

it follows from Lemma 2.1 that the following inequality holds:

$$n_q(k,d) \geq g_q(k,d) + \sum_{j=3}^{k-1} h_{j,q}(e_{k-j}, e_{k-j+1}, \ldots, e_{k-2}),$$

$$\text{i.e.,} \qquad h_{k,q}(e_0, e_1, \ldots, e_{k-2}) \geq 0. \qquad \square$$

Appendix. Tables of the values of d, $e = e_0e_1 \cdots e_{k-2}$, $g = g_3(k,d)$, $n = n_3(k,d)$ and $h_j = h_{j,3}(e_{k-j}, e_{k-j+1}, \cdots, e_{k-2})$ for $3 \leq j \leq k$, for $k = 3, 4, 5$.

Table 1. The values of $g_3(3,d)$, $n_3(3,d)$ and h_3 for $1 \leq d \leq 9$

d	e	g	n	h_3
1	22	3	3	0
2	12	4	4	0
3	02	5	6	1
4	21	7	7	0
5	11	8	8	0
6	01	9	9	0
7	20	11	11	0
8	10	12	12	0
9	00	13	13	0

Table 2. The values of $g_3(4,d)$, $n_3(4,d)$ and h_3, h_4 for $1 \leq d \leq 27$

d	e	g	n	h_3	h_4	d	e	g	n	h_3	h_4	d	e	g	n	h_3	h_4
1	222	4	4	0	0	10	221	17	17	0	0	19	220	30	30	0	0
2	122	5	5	0	0	11	121	18	18	0	0	20	120	31	31	0	0
3	022	6	7	0	1	12	021	19	19	0	0	21	020	32	32	0	0
4	212	8	8	0	0	13	211	21	22	0	1	22	210	34	34	0	0
5	112	9	9	0	0	14	111	22	23	0	1	23	110	35	35	0	0
6	012	10	10	0	0	15	011	23	24	0	1	24	010	36	36	0	0
7	202	12	13	1	0	16	201	25	25	0	0	25	200	38	38	0	0
8	102	13	14	1	0	17	201	26	26	0	0	26	100	39	39	0	0
9	002	14	15	1	0	18	201	27	27	0	0	27	000	40	40	0	0

Table 3. The values of $g_3(5,d)$, $n_3(5,d)$ and h_3, h_4, h_5 for $1 \le d \le 81$

d	e	g	n	h_3	h_4	h_5	d	e	g	n	h_3	h_4	h_5
1	2222	5	5	0	0	0	43	2011	66	67	0	1	0
2	1222	6	6	0	0	0	44	1011	67	68	0	1	0
3	0222	7	8	0	0	1	45	0011	68	69	0	1	0
4	2122	9	9	0	0	0	46	2201	71	72	0	0	1
5	1122	10	10	0	0	0	47	1201	72	73	0	0	1
6	0122	11	11	0	0	0	48	0201	73	74	0	0	1
7	2022	13	14	0	1	0	49	2101	75	76	0	0	1
8	1022	14	15	0	1	0	50	1101	76	77	0	0	1
9	0022	15	16	0	1	0	51	0101	77	78	0	0	1
10	2212	18	18	0	0	0	52	2001	79	79	0	0	0
11	1212	19	19	0	0	0	53	1001	80	80	0	0	0
12	0212	20	20	0	0	0	54	0001	81	81	0	0	0
13	2112	22	23	0	0	1	55	2220	85	85	0	0	0
14	1112	23	24	0	0	1	56	1220	86	86	0	0	0
15	0112	24	25	0	0	1	57	0220	87	87	0	0	0
16	2012	26	27	0	0	1	58	2120	89	89	0	0	0
17	1012	27	28	0	0	1	59	1120	90	90	0	0	0
18	0012	28	29	0	0	1	60	0120	91	91	0	0	0
19	2202	31	32	1	0	0	61	2020	93	94	0	0	1
20	1202	32	33	1	0	0	62	1020	94	95	0	0	1
21	0202	33	34	1	0	0	63	0020	95	96	0	0	1
22	2102	35	36	1	0	0	64	2210	98	98	0	0	0
23	1102	36	37	1	0	0	65	1210	99	99	0	0	0
24	0102	37	38	1	0	0	66	0210	100	100	0	0	0
25	2002	39	41	1	0	1	67	2110	102	102	0	0	0
26	1002	40	42	1	0	1	68	1110	103	103	0	0	0
27	0002	41	43	1	0	1	69	0110	104	104	0	0	0
28	2221	45	45	0	0	0	70	2010	106	106	0	0	0
29	1221	46	46	0	0	0	71	1010	107	107	0	0	0
30	0221	47	47	0	0	0	72	0010	108	108	0	0	0
31	2121	49	49	0	0	0	73	2200	111	111	0	0	0
32	1121	50	51	0	0	1	74	1200	112	112	0	0	0
33	0121	51	52	0	0	1	75	0200	113	113	0	0	0
34	2021	53	53	0	0	0	76	2100	115	115	0	0	0
35	1021	54	54	0	0	0	77	1100	116	116	0	0	0
36	0021	55	55	0	0	0	78	0100	117	117	0	0	0
37	2211	58	59	0	1	0	79	2000	119	119	0	0	0
38	1211	59	60	0	1	0	80	1000	120	120	0	0	0
39	0211	60	61	0	1	0	81	0000	121	121	0	0	0
40	2111	62	63	0	1	0							
41	1111	63	64	0	1	0							
42	0111	64	65	0	1	0							

REFERENCES

[1] Ball S. Table of bounds on three dimensional linear codes or (n, r) arcs in PG$(2, q)$. `http://www-ma4.upc.es/~simeon/codebounds.html`

[2] Griesmer J. H. A bound for error-correcting codes. *IBM J. Res. Develop.*, **4** (1960), 532–542.

[3] Hirschfeld J. W. P., L. Storme. The packing problem in statistics, coding theory and finite projective spaces. In: Finite Geometries, Proc. of the Fourth Isle of Thorns Conference, Kluwer, 2001(Eds A. Blokhuis et al.), 201–246.

[4] Maruta T. Griesmer bound for linear codes over finite fields. `http://www.geocities.jp/mars39geo/griesmer.htm`.

[5] Solomon G., J. J. Stiffler. Algebraically punctured cyclic codes. *Inform. Control*, **8** (1965), 170–179.

Noboru Hamada
Emeritus Professor at Osaka Women's University
e-mail: n-hamada@koala.odn.ne.jp

Tatsuya Maruta
Department of Mathematics and Information Sciences
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
e-mail: maruta@mi.s.osakafu-u.ac.jp

Received March 11, 2011
Final Accepted June 2, 2011