Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 257–262*

Optimal 4-dimensional linear codes over $\mathbb{F}_8$

Tatsuya Maruta[1] maruta@mi.s.osakafu-u.ac.jp
Department of Mathematics and Information Sciences,
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

Abstract. We construct new linear codes over $\mathbb{F}_8$ with parameters $[368, 4, 320]_8$, $[436, 4, 380]_8$, $[669, 4, 584]_8$, $[678, 4, 592]_8$, $[687, 4, 600]_8$, $[696, 4, 608]_8$, $[733, 4, 640]_8$. We also prove the nonexistence of $[658, 4, 575]_8$ codes attaining the Griesmer bound.

1 Introduction

An $[n, k, d]_q$ code $\mathcal{C}$ is a linear code of length n, dimension k and minimum weight d over $\mathbb{F}_q$, the field of q elements. The *weight* of a vector $\boldsymbol{x} \in \mathbb{F}_q^n$, denoted by $\mathrm{wt}(\boldsymbol{x})$, is the number of nonzero coordinate positions in $\boldsymbol{x}$.

A fundamental problem in coding theory is to find $n_q(k, d)$, the minimum length n for which an $[n, k, d]_q$ code exists. See [6] for the updated tables of $n_q(k, d)$ for some small q and k. The Griesmer bound gives a natural lower bound on $n_q(k, d)$: $n_q(k, d) \geq g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer $\geq x$. An $[n, k, d]_q$ code attaining the Griesmer bound is called a *Griesmer code*. The values of $n_q(k, d)$ are determined for all d only for some small values of q and k. For linear codes over $\mathbb{F}_8$, $n_8(k, d)$ is known for $k \leq 3$ for all d, but the value of $n_8(4, d)$ is unknown for many integers d although the Griesmer bound is attained for all $d \geq 833$. It is known that $n_8(4, d) = g_8(4, d)$ or $g_8(4, d) + 1$ for $575 \leq d \leq 608$, $g_8(4, d) + 1 \leq n_8(4, d) \leq g_8(4, d) + 3$ for $317 \leq d \leq 320$, and $n_8(4, d) = g_8(4, d) + 1$ or $g_8(4, d) + 2$ for $d = 379, 380, 639, 640$, see [3]. Our purpose is to prove the following theorems.

Theorem 1.1. *There exist codes with parameters* $[368, 4, 320]_8$, $[436, 4, 380]_8$, $[669, 4, 584]_8$, $[678, 4, 592]_8$, $[687, 4, 600]_8$, $[696, 4, 608]_8$, $[733, 4, 640]_8$.

Theorem 1.2. *There exists no* $[658, 4, 575]_8$ *code.*

Since the existence of an $[n, k, d]_q$ code implies the existence of an $[n-1, k, d-1]_q$ code, we get the following.

Corollary 1.3. (1) $n_8(4, d) = g_8(4, d)$ *for* $581 \leq d \leq 608$.
(2) $n_8(4, d) = g_8(4, d) + 1$ *for* $d = 379, 380, 575, 576, 639, 640$.
(3) $n_8(4, d) = g_8(4, d) + 1$ *or* $g_8(4, d) + 2$ *for* $317 \leq d \leq 320$.

[1]This research is partially supported by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science under Contract Number 24540138.

2 Preliminary results

We denote by $\mathrm{PG}(r,q)$ the projective geometry of dimension r over $\mathbb{F}_q$. The 0-flats, 1-flats, 2-flats, $(r-2)$-flats and $(r-1)$-flats are called *points, lines, planes, secundums* and *hyperplanes* respectively. We denote by $\mathcal{F}_j$ the set of j-flats of $\mathrm{PG}(r,q)$ and by θ_j the number of points in a j-flat, i.e. $\theta_j = (q^{j+1}-1)/(q-1)$.

Let $\mathcal{C}$ be an $[n,k,d]_q$ code having no coordinate which is identically zero. The columns of a generator matrix of $\mathcal{C}$ can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1,q)$ denoted also by $\mathcal{C}$. We see linear codes from this geometrical point of view. An *i-point* is a point of Σ which has multiplicity i in $\mathcal{C}$. Denote by γ_0 the maximum multiplicity of a point from Σ in $\mathcal{C}$ and let C_i be the set of i-points in Σ, $0 \le i \le \gamma_0$. For any subset S of Σ we define *the multiplicity of S with respect to $\mathcal{C}$*, denoted by $m_{\mathcal{C}}(S)$, as $m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|$, where $|T|$ denotes the number of elements in a set T. When the code is projective, i.e. when $\gamma_0 = 1$, the multiset $\mathcal{C}$ forms an n-set in Σ and the above $m_{\mathcal{C}}(S)$ is equal to $|\mathcal{C} \cap S|$. A line l with $t = m_{\mathcal{C}}(l)$ is called a *t-line*. A *t-plane*, a *t-hyperplane* and so on are defined similarly. Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ such that $n = m_{\mathcal{C}}(\Sigma)$ and $n-d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}$. Conversely such a partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ as above gives an $[n,k,d]_q$ code in the natural manner. For an m-flat Π in Σ we define

$$\gamma_j(\Pi) = \max\{m_{\mathcal{C}}(\Delta) \mid \Delta \subset \Pi,\ \Delta \in \mathcal{F}_j\},\ 0 \le j \le m.$$

We denote simply by γ_j instead of $\gamma_j(\Sigma)$. It holds that $\gamma_{k-2} = n-d$, $\gamma_{k-1} = n$. When $\mathcal{C}$ attains the Griesmer bound, γ_j's are uniquely determined. Every $[n,k,d]_q$ code attaining the Griesmer bound is projective if $d \le q^{k-1}$. Denote by a_i the number of hyperplanes Π in Σ with $m_{\mathcal{C}}(\Pi) = i$ and by λ_s the number of s-points in Σ. The list of a_i's is called the *spectrum* of $\mathcal{C}$. We usually use τ_j's for the spectrum of a hyperplane of Σ to distinguish from the spectrum of $\mathcal{C}$. Simple counting arguments yield the following.

Lemma 2.1. (1) $\sum_{i=0}^{n-d} a_i = \theta_{k-1}$. (2) $\sum_{i=1}^{n-d} i a_i = n\theta_{k-2}$.
(3) $\sum_{i=2}^{n-d} i(i-1)a_i = n(n-1)\theta_{k-3} + q^{k-2}\sum_{s=2}^{\gamma_0} s(s-1)\lambda_s$.

Lemma 2.2 ([8])**.** *Let Π be an i-hyperplane through a t-secundum δ. Then*
(1) *$t \le \gamma_{k-2} - (n-i)/q = (i + q\gamma_{k-2} - n)/q$.*
(2) *$a_i = 0$ if an $[i,k-1,d_0]_q$ code with $d_0 \ge i - \lfloor (i+q\gamma_{k-2}-n)/q \rfloor$ does not exist, where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x.*
(3) *$\gamma_{k-3}(\Pi) = \lfloor (i+q\gamma_{k-2}-n)/q \rfloor$ if an $[i,k-1,d_1]_q$ code with $d_1 \ge i - \lfloor (i+q\gamma_{k-2}-n)/q \rfloor + 1$ does not exist.*
(4) *Let c_j be the number of j-hyperplanes through δ other than Π. Then*

$$\sum_j (\gamma_{k-2} - j)c_j = i + q\gamma_{k-2} - n - qt. \tag{2.1}$$

(5) *For a* γ_{k-2}*-hyperplane* Π_0 *with spectrum* $(\tau_0, \cdots, \tau_{\gamma_{k-3}})$*,* $\tau_t > 0$ *holds if* $i + q\gamma_{k-2} - n - qt < q$.

An f-set F in $\mathrm{PG}(r, q)$ satisfying $m = \min\{|F \cap \pi| \mid \pi \in \mathcal{F}_{r-1}\}$ is called an $\{f, m; r, q\}$*-minihyper*. When $\gamma_0 = 1$, the set of 0-points C_0 forms a $\{\theta_{k-1} - n, \theta_{k-2} - (n - d); k - 1, q\}$-minihyper, and vice versa.

We also use the following theorems to prove Theorem 1.2.

Theorem 2.3 ([2])**.** *Let* $\mathcal{C}$ *be an* $[n, k, d]_q$ *code with* $gcd(d, q) = 1$ *whose spectrum satisfies* $a_i = 0$ *for all* $i \not\equiv n, n - d \pmod 3$*. Then* $\mathcal{C}$ *is extendable.*

Theorem 2.4 ([9])**.** *Let* $\mathcal{C}$ *be a Griesmer* $[n, k, d]_8$ *code. If* 8 *divides* d*, then* $\mathcal{C}$ *is* 2*-divisible.*

3 Proof of Theorem 1.1

Let $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$, with $\alpha^3 = \alpha + 1$. For simplicity, we denote $\alpha, \alpha^2, \cdots, \alpha^6$ by $2, 3, \cdots, 7$ so that $\mathbb{F}_8 = \{0, 1, 2, 3, \cdots, 7\}$.

Lemma 3.1 ([4])**.** *Let* $\mathcal{C}_0$ *be the linear code over* $\mathbb{F}_8$ *with generator matrix*

$$G_0 = \begin{bmatrix} 1&1&1&1&1&1&0&0&1&1&1&1&0&1&1&1&1&1&1&1&1 \\ 6&6&7&4&5&1&1&1&6&6&3&5&1&0&4&4&3&5&2&6&3 \\ 0&6&0&7&0&0&3&3&2&1&7&4&2&5&7&2&1&2&0&3&1 \\ 2&6&3&6&4&7&3&1&2&5&2&3&0&4&0&6&0&5&6&7&2 \end{bmatrix}.$$

Then $\mathcal{C}_0$ *is a* $[21, 4, 16]_8$ *code with spectrum* $(a_1, a_3, a_5) = (228, 240, 117)$*.*

Lemma 3.2 ([4])**.** (1) *There exists a* $[76, 4, 64]_8$ *code with spectrum* $(a_4, a_8, a_{12}) = (72, 224, 289)$*.*
(2) *A* $[28, 4, 22]_8$ *code with spectrum* $(a_0, a_2, a_4, a_6) = (25, 231, 196, 133)$ *exists.*

As a method to construct good codes, we first introduce the projective dual. An $[n, k, d]_q$ code is called m*-divisible* if all codewords have weights divisible by an integer $m > 1$.

Lemma 3.3 ([8])**.** *Let* $\mathcal{C}$ *be an* m*-divisible* $[n, k, d]_q$ *code with* $q = p^h$*,* p *prime, whose spectrum is*

$$(a_{n-d-(w-1)m}, a_{n-d-(w-2)m}, \cdots, a_{n-d-m}, a_{n-d}) = (\alpha_{w-1}, \alpha_{w-2}, \cdots, \alpha_1, \alpha_0),$$

where $m = p^r$ *for some* $1 \le r < h(k-2)$ *satisfying* $\lambda_0 > 0$*. Then there exists a* t*-divisible* $[n^*, k, d^*]_q$ *code* $\mathcal{C}^*$ *with* $t = q^{k-2}/m$*,* $n^* = \sum_{j=0}^{w-1} j\alpha_j = ntq - \frac{d}{m}\theta_{k-1}$*,* $d^* = n^* - nt + \frac{d}{m}\theta_{k-2} = ((n-d)q - n)t$ *whose spectrum is*

$$(a_{n^*-d^*-\gamma_0 t}, a_{n^*-d^*-(\gamma_0-1)t}, \cdots, a_{n^*-d^*-t}, a_{n^*-d^*}) = (\lambda_{\gamma_0}, \lambda_{\gamma_0-1}, \cdots, \lambda_1, \lambda_0).$$

$\mathcal{C}^*$ is called the *projective dual* of $\mathcal{C}$, see [1]. Applying Lemma 3.3 to the codes in Lemmas 3.1 and 3.2, we obtain the following codes.

Corollary 3.4. (1) *There exists a* $[368, 4, 320]_8$ *code with spectrum* $(a_{48}, a_{32}, a_{16}) = (511, 72, 2)$.
(2) *There exists a* $[696, 4, 608]_8$ *code with spectrum* $(a_{56}, a_{88}) = (21, 564)$.
(3) *There exists a* $[733, 4, 640]_8$ *code with spectrum* $(a_{61}, a_{93}) = (28, 557)$.

We apply the following "geometric puncturing" to obtain other codes.

Lemma 3.5 ([7])**.** *Let $\mathcal{C}$ be an $[n, k, d]_q$ code and let $\cup_{i=0}^{\gamma_0} C_i$ be the partition of $\Sigma = \mathrm{PG}(k-1, q)$ obtained from $\mathcal{C}$. If $\cup_{i=1}^{\gamma_0} C_i$ contains a t-flat and if $d > q^t$, then an $[n - \theta_t, k, d - q^t]_q$ code exists.*

The above lemma can be generalized as follows.

Lemma 3.6. *Let $\mathcal{C}$ and $\cup_{i=0}^{\gamma_0} C_i$ be as in Lemma 3.5. If $\cup_{i=1}^{\gamma_0} C_i$ contains an $\{f, m; k-1, q\}$-minihyper $\mathcal{F}$ such that $(C_1 \setminus \mathcal{F}) \cup (\cup_{i \geq 2} C_i)$ spans Σ, then there exists an $[n - f, k, d + m - f]_q$ code.*

Proof. Let $C_i' = (C_i \setminus \mathcal{F}) \cup (C_{i+1} \cap \mathcal{F})$ for all i. Then $\cup_{i=0}^{\gamma_0} C_i'$ forms a partition of Σ giving an $[n' = n - f, k, d']_q$ code, say $\mathcal{C}'$. For any hyperplane π of Σ, π meets $\mathcal{F}$ in at least m points. So, $m_{\mathcal{C}'}(\pi) \leq n' - d' \leq n - d - m$, giving $d' \geq d - f + m$. □

Let $\mathcal{C}$ be the 2^5-divisible $[696, 4, 608]_8$ code found in Corollary 3.4 and let $C_0 \cup C_1 \cup C_2$ be the partition of $\Sigma = \mathrm{PG}(3, 8)$ obtained from $\mathcal{C}$. Then it follows from Lemmas 3.2 and 3.3 that $(\lambda_0, \lambda_1, \lambda_2) = (117, 240, 228)$, where $\lambda_i = |C_i|$. Actually, the sets C_i for $\mathcal{C}$ are constructed from G_0 in Lemma 3.1 as follows:

$$C_i = \{\mathbf{P}(p_0, p_1, p_2, p_3) \in \mathrm{PG}(3, 8) \mid wt(p_0 g_0 + \cdots + p_3 g_3) = 16 + 2i\} \quad \text{for } 0 \leq i \leq 2,$$

where g_i is the $(i+1)$-th row of G_0 for $0 \leq i \leq 3$. It can be checked with the aid of a computer that the set $C_1 \cup C_2$ contains three skew lines $l_1 = \langle 1523, 0152 \rangle$, $l_2 = \langle 2342, 7220 \rangle$ and $l_3 = \langle 3545, 5352 \rangle$, where $x_0 x_1 x_2 x_3$ stands for the point $\mathbf{P}(x_0, \cdots, x_3)$ of Σ represented by a vector $(x_0, \cdots, x_3)$. Applying Lemma 3.5 with $\Pi = l_1$ to $\mathcal{C}$ gives a $[687, 4, 600]_8$ code $\mathcal{C}_1$ with spectrum

$$(a_{55}, a_{79}, a_{87}) = (21, 9, 555)$$

and applying Lemma 3.5 with $\Pi = l_2$ to $\mathcal{C}_1$ gives a $[678, 4, 592]_8$ code $\mathcal{C}_2$ with spectrum

$$(a_{54}, a_{78}, a_{86}) = (21, 18, 546).$$

Furthermore, applying Lemma 3.5 with $\Pi = l_3$ to $\mathcal{C}_2$ gives a $[669, 4, 584]_8$ code with spectrum

$$(a_{53}, a_{77}, a_{85}) = (21, 27, 537).$$

Next, we construct a $[436, 4, 380]_8$ code from a $[449, 4, 392]_8$ code by the projective puncturing Lemma 3.6. Let $\mathcal{H} = \mathbf{V}(x_0x_1 + x_2x_3)$ be a hyperbolic quadric in $\Sigma = \mathrm{PG}(3, 8)$. Take $P(0010) \in \mathcal{H}$ and $\pi = \mathbf{V}(x_3)$, the tangent plane at P. Putting $C_0 = (\mathcal{H} \cup \pi) \setminus \{P\}$ and $C_1 = \Sigma \setminus C_0$, one can get a Griesmer $[449, 4, 392]_8$ code $\mathcal{C}$ [5]. We cannot find a line to apply Lemma 3.5 since C_1 contains no line, for $\gamma_1 = 8$. Instead, we take a blocking 13-set in a plane through P as $\mathcal{F}$ in Lemma 3.6. Let $\delta = \mathbf{V}(x_0 + x_1)$ and take a blocking 13-set in δ:

$$\mathcal{B} = \{P, 0011, 0012, 0014, 0017, 1101, 1121, 1161, 1171, 1112, 1132, 1142, 1152\}.$$

Applying Lemma 3.6 with $\mathcal{B}$ to $\mathcal{F}$ gives a $[436, 4, 380]_8$ code with spectrum

$$(a_0, a_{44}, a_{46}, a_{48}, a_{52}, a_{54}, a_{56}) = (1, 1, 10, 54, 24, 118, 377).$$

This completes the proof of Theorem 1.1. □

4 Proof of Theorem 1.2

Lemma 4.1. *The spectrum of a* $[83, 3, 72]_8$ *code satisfies* $a_i = 0$ *for all* $i \notin \{3, 5, 7, 9, 11\}$.

Proof. Let l be a t-line through a 1-point P in $\Sigma = \mathrm{PG}(2, 8)$. Then we have $n = 83 \le (\gamma_1 - 1)8 + t$, giving $t \ge 3$. Since there is no line with even multiplicity by Theorem 2.4, our assertion follows. □

Now, let $\mathcal{C}_0$ be a putative $[659, 4, 576]_8$ code and let δ_0 be a γ_2-plane in $\Sigma = \mathrm{PG}(3, 8)$. Then δ_0 satisfies $\tau_i = 0$ for all $i \notin \{3, 5, 7, 9, 11\}$ by Lemmas 4.1, so $a_i = 0$ for all $i < 19$ by Lemma 2.2. Hence $a_i = 0$ for all $i \notin \{67, 69, 71, 73, 83\}$ by Lemma 2.2, Theorem 2.4 and the known $n_8(3, d)$-table.

Suppose $a_{73} > 0$ and let π be a 73-plane. Then π gives a projective $[73, 3, 64]_8$ code consisting of the points in π. Hence π has a 9-line. Since (2.1) for $(i, t) = (73, 9)$ has no solution, a contradiction. Hence $a_{73} = 0$. We can prove $a_{71} = a_{69} = 0$ similarly. Then we have $(a_{67}, a_{83}) = (28, 557)$ by Lemma 2.1. Let δ be a 67-plane. Then, δ corresponds to a projective Griesmer $[67, 3, 58]_8$ code. So, δ has exactly six 0-points, and has a 8-line, say ℓ. Let x be the number of 67-planes through ℓ. Then we have $(67 - 8)x + (83 - 8)(9 - x) + 8 = 659$, i.e., $y = 15/2$, a contradiction. Thus we get the following.

Lemma 4.2. *There exists no* $[659, 4, 576]_8$ *code.*

Next, let $\mathcal{C}$ be a putative $[658, 4, 575]_8$ code and let δ_0 be a γ_2-plane in $\Sigma = \mathrm{PG}(3, 8)$. Then we have $a_i = 0$ for all $i \notin \{66, 67, 68, 69, 70, 71, 72, 73, 82, 83\}$ by Lemma 2.2 and the known $n_8(3, d)$-table.

Suppose $a_{66+e} > 0$ and let π be a $(66+e)$-plane for $0 \le e \le 7$. Then π gives a projective code, and π has a 8-line. Since it follows from Lemma 4.1 that $c_{83} = 0$ in (2.1) for $(i,t) = (66+e, 8)$, (2.1) has no solution for $1 \le e \le 6$. Hence $a_i = 0$ for $67 \le i \le 72$. For $(i,t) = (73,9)$, (2.1) has the unique solution $(c_{82}, c_{83}) = (7,1)$. Then we have the spectrum $(a_{73}, a_{82}, a_{83}) = (1, 511, 73)$, which gives $\lambda_2 = 3001/64$ from (3) in Lemma 2.1, a contradiction. Hence $a_{73} = 0$. Thus, we have $a_i = 0$ for all $i \notin \{66, 82, 83\}$, which implies that $\mathcal{C}$ is extendable by Theorem 2.3. But there exists no $[659, 4, 576]_8$ code by Lemma 4.2, a contradiction. This completes the proof. □

References

[1] A.E. Brouwer, M. van Eupen, The correspondence between projective codes and 2-weight codes, *Des. Codes Cryptogr.* **11**, 261–266, 1997.

[2] R. Hill, An extension theorem for linear codes, *Des. Codes Cryptogr.* **17** (1999) 151–157.

[3] R. Kanazawa, T. Maruta, On optimal linear codes over $\mathbb{F}_8$, *Electron. J. Combin.* **18**, #P34, 27pp, 2011.

[4] A. Kohnert, Best linear codes, http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/Linear_Codes_BKW/

[5] T. Maruta, On the minimum length of q-ary linear codes of dimension four, *Discrete Math.* **208/209**, 427–435, 1999.

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

[7] T. Maruta, Y. Oya, On optimal ternary linear codes of dimension 6, Advances in Mathematics of Communications **5**, 505–520, 2011.

[8] M. Takenaka, K. Okamoto, T. Maruta, On optimal non-projective ternary linear codes, *Discrete Math.* **308**, 842–854, 2008.

[9] H.N. Ward, Divisible codes - a survey, *Serdica Math. J.* **27**, 263-278, 2001.