Nonexistence of some Griesmer codes of dimension 4 over $\mathbb{F}_8$

MAYA FUJI \quad sxb01161@edu.osakafu-u.ac.jp
TATSUYA MARUTA\footnote{This research of this author was partially supported by JSPS KAKENHI Grant Number JP16K05256.} \quad maruta@mi.s.osakafu-u.ac.jp

Department of Mathematics and Information Sciences
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

Abstract. We prove the nonexistence of $[g_8(4,d),4,d]_8$ code for $d = 173, 574, 693, 697, 810$ using the geometric method, where $g_q(k,d) = \sum_{i=0}^{k-1} \lfloor d/q^i \rfloor$.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of $n$-tuples over $\mathbb{F}_q$, the field of $q$ elements. An $[n,k,d]_q$ code $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming weight $d = \min \{ \text{wt}(c) \mid c \in C, c \neq (0,\ldots,0) \}$, where $\text{wt}(c)$ is the number of non-zero entries in $c$. The weight distribution of $C$ is the list of numbers $A_i$ which is the number of codewords of $C$ with weight $i$. 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 (\cite{3}). There is a natural lower bound on $n_q(k,d)$, the Griesmer bound: $n_q(k,d) \geq g_q(k,d) = \sum_{i=0}^{k-1} \lfloor d/q^i \rfloor$, where $\lfloor x \rfloor$ denotes the smallest integer greater than or equal to $x$. The values of $n_q(k,d)$ are determined for all $d$ only for some small values of $q$ and $k$. The problem to determine $n_q(4,d)$ for all $d$ has been solved for $q = 2, 3, 4$ but not for $q \geq 5$. For $k = 3$, $n_q(3,d)$ is known for all $d$ for $q \leq 9$. In this paper, we tackle the problem to determine $n_q(4,d)$ for all $d$. See \cite{13} for the updated table of $n_q(k,d)$ for some small $q$ and $k$. The following results are already known for $n_q(k,d)$ with $k = 3, 4$, see \cite{1,2,4-6,10,12,13}.

Theorem 1. $n_8(3,d) = g_8(3,d) + 1$ for $d = 13-16, 29-32, 37-40, 43-48$ and $n_8(3,d) = g_8(3,d)$ for any other $d$.

Theorem 2. (a) $n_8(4,d) = g_8(4,d)$ for $d = 1-6, 9-12, 17-20, 49-56, 65-68, 257, 258, 265-272, 385-392, 441-568, 577-608, 705-728, 769-784$ and for $d \geq 833$. (b) $n_8(4,d) = g_8(4,d) + 1$ for $d = 7, 8, 13-16, 22-24, 29-32, 37, 43-48, 57-64, 80, 87, 88, 95-120, 286-288, 377-384, 399, 400, 407, 408, 414-440, 575, 576, 639, 640, 702-704, 750-768, 813-832.

(d) \(g_8(4, d) + 1 \leq n_8(4, d) \leq g_8(4, d) + 2\) for \(d = 38-40, 121-128, 177, 185-192, 225-227, 233-236, 241-246, 249-256, 289-320, 337-376.

(e) \(n_8(4, d) \geq g_8(4, d) + 1\) for \(d = 178-184, 221-224, 228-232, 237-240, 247, 248.

(f) \(n_8(4, d) \leq g_8(4, d) + 2\) for \(d = 133-176, 194-206, 209-220, 329-336.

We prove the following.

**Theorem 3.** There exists no \([g_8(4, d), 4, d]_8\) code for \(d = 173, 574, 693, 697, 810.

**Corollary 4.** (a) \(n_8(4, d) = g_8(4, d) + 1\) for \(d = 574, 693-701, 810-812.

(b) \(g_8(4, d) + 1 \leq n_8(4, d) \leq g_8(4, d) + 2\) for \(173 \leq d \leq 176.

**Remark.** The nonexistence of a \([g_q(4, d), 4, d]_q\) code for \(d = 2q^3 - rq^2 - q + 1\) for \(3 \leq r \leq q - q/p\), \(q = p^h\) with \(p\) prime, is proved in [6]. We conjecture that a \([g_q(4, d), 4, d]_q\) code for \(d = 2q^3 - rq^2 - q + 1\) with \(r = q - q/p - 1\) does not exist for non-prime \(q \geq 8\), which is valid for \(q = 8, 9\) by Theorem 3 and [7].

## 2 Preliminary results

We denote by PG\((r, q)\) the projective geometry of dimension \(r\) over \(F_q\). A \(j\)-flat is a projective subspace of dimension \(j\) in PG\((r, q)\). 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 \(\theta_j\) the number of points in a \(j\)-flat, i.e., \(\theta_j = (q^{3-j} - 1)/(q - 1)\).

Let \(C\) be an \([n, k, d]_q\) code having no coordinate which is identically zero. The columns of a generator matrix of \(C\) can be considered as a multiset of \(n\) points in \(\Sigma = \text{PG}(k - 1, q)\) denoted by \(\mathcal{M}_C\). An \(i\)-point is a point of \(\Sigma\) which has multiplicity \(i\) in \(\mathcal{M}_C\). Denote by \(\gamma_0\) the maximum multiplicity of a point from \(\Sigma\) in \(\mathcal{M}_C\) and let \(C_i\) be the set of \(i\)-points in \(\Sigma\), \(0 \leq i \leq \gamma_0\). We denote by \(\Delta_1 + \cdots + \Delta_s\) the multiset consisting of the \(s\) sets \(\Delta_1, \ldots, \Delta_s\) in \(\Sigma\). We write \(s\Delta_1\) for \(\Delta_1 + \cdots + \Delta_s\) when \(\Delta_1 = \cdots = \Delta_s\). Then, \(\mathcal{M}_C = \sum_{i=1}^{\gamma_0} iC_i\). For any subset \(S\) of \(\Sigma\), we denote by \(\mathcal{M}_C(S)\) the multiset \(\{P \in \mathcal{M}_C \mid P \in S\}\). The multiplicity of \(S\) with respect to \(C\), denoted by \(m_C(S)\), is defined as the cardinality of \(\mathcal{M}_C(S)\), i.e., \(m_C(S) = \sum_{i=1}^{\gamma_0} i|S \cap C_i|\), where \(|T|\) denotes the number of elements in a set \(T\). Then we obtain the partition \(\Sigma = \bigcup_{i=0}^{\gamma_0} C_i\) such that \(n = m_C(\Sigma)\) and \(n - d = \max\{m_C(\pi) \mid \pi \in F_{k-2}\}\), where \(F_j\) denotes the set of \(j\)-flats in \(\Sigma\). Such a partition of \(\Sigma\) is called an \((n, n - d)\)-arc of \(\Sigma\). Conversely an \((n, n - d)\)-arc of \(\Sigma\) gives an \([n, k, d]_q\) code in the natural manner. A line \(l\) with \(t = m_C(l)\) is
called a t-line. A t-plane, a t-hyperplane and so on are defined similarly. For an m-flat \( \Pi \) in \( \Sigma \) we define

\[
\gamma_j(\Pi) = \max\{m \ell(\Delta) \mid \Delta \subset \Pi, \Delta \in \mathcal{F}_j\}, \quad 0 \leq j \leq k - 2.
\]

Let \( \lambda_s(\Pi) \) be the number of s-points in \( \Pi \). We denote simply by \( \gamma_j \) and by \( \lambda_s \) instead of \( \gamma_j(\Sigma) \) and \( \lambda_s(\Sigma) \), respectively. It holds that \( \gamma_{k-2} = n - d \), \( \gamma_{k-1} = n \).

When \( C \) is Griesmer, the values \( \gamma_0, \gamma_1, \ldots, \gamma_{k-3} \) are also uniquely determined as \( \gamma_j = \sum_{u=0}^{\lfloor d/q^k - 1 - u \rfloor} \) for \( 0 \leq j \leq k - 1 \) [11]. So, every Griesmer \([n, k, d]_q \) code is projective if \( d \leq q^{k-1} \). Denote by \( a_i \) the number of \( i \)-hyperplanes in \( \Sigma \). The list of \( a_i \)'s is called the spectrum of \( C \). We usually use \( \tau_j \)'s for the spectrum of a hyperplane \( \Delta \) to distinguish from the spectrum of \( C \). Simple counting arguments yield the following.

**Lemma 5** ([8]).

(a) \( \sum_{i=0}^{n-d} a_i = \theta_{k-1} \).

(b) \( \sum_{i=1}^{n-d} ia_i = n \theta_{k-2} \).

(c) \( \sum_{i=2}^{n-d} i(i-1)a_i = n(n-1)\theta_{k-3} + q^{k-2} \sum_{s=2}^{j_0} s(s-1)\lambda_s \).

When \( \gamma_0 \leq 2 \), the three equalities in Lemma 5 yield the following:

\[
\sum_{i=0}^{n-d-2} \binom{n-d-i}{2} a_i = \binom{n-d}{2} \theta_{k-1} - n(n-d-1)\theta_{k-2} + \binom{n}{2} \theta_{k-3} + q^{k-2}\lambda_2. \tag{1}
\]

When \( \gamma_0 = 2 \), we have

\[
\lambda_2 = \lambda_0 + n - \theta_{k-1} \tag{2}
\]

from \( \lambda_0 + \lambda_1 + \lambda_2 = \theta_{k-1} \) and \( \lambda_1 + 2\lambda_2 = n \).

**Lemma 6** ([14]). Let \( \Pi \) be an \( w \)-hyperplane through a \( t \)-secundum \( \delta \). Then

(a) \( t \leq \gamma_{k-2} = (n - w)/q = (w + q\gamma_{k-2} - n)/q \).

(b) \( a_w = 0 \) if a \([w, k-1, d_0]_q \) code with \( d_0 \geq \lfloor (w + q\gamma_{k-2} - n)/q \rfloor \) does not exist, where \( \lfloor x \rfloor \) denotes the largest integer less than or equal to \( x \).

(c) \( \gamma_{k-3}(\Pi) = \lfloor (w + q\gamma_{k-2} - n)/q \rfloor \) if there exists no \([w, k-1, d_1]_q \) code with \( d_1 \geq \lfloor (w + q\gamma_{k-2} - n)/q \rfloor + 1 \).

(d) Let \( c_j \) be the number of \( j \)-hyperplanes through \( \delta \) other than \( \Pi \). Then

\[
\sum_j c_j = q \text{ and } \sum_j (jw - j)c_j = w + q\gamma_{k-2} - n - qt.
\]

(e) A \( \gamma_{k-2} \)-hyperplane \( \Pi_0 \) with spectrum \( (\tau_0, \ldots, \tau_{k-3}) \) satisfies \( \tau_i > 0 \) if \( w + q\gamma_{k-2} - n - qt < q \).

A set of \( s \) lines in \( \text{PG}(2, q) \) is called an \( s \)-arc of lines if no three of which are concurrent. An \( f \)-multiset \( \mathcal{F} \) in \( \text{PG}(2, q) \) is an \((f, m)\)-minihyper if every line meets \( \mathcal{F} \) in at least \( m \) points and if some line meets \( \mathcal{F} \) in exactly \( m \) points with multiplicity.
Lemma 7 ([9]). For $x = \frac{q}{2} + 1$ with $q$ even, every $(x(q + 1), x)$-minihyper in $PG(2, q)$ is either the sum of $x$ lines or the union of $(q + 2)$-arc of lines.

Lemma 8. Let $C$ be a $[101, 3, 88]_8$ code and let $\Sigma = PG(2, 8)$. Then,
(a) $C$ has spectrum $(a_5, a_{13}) = (5, 68)$ with $\lambda_0 = 10$ and $M_C = 2\Sigma - (l_1 + \cdots + l_5)$, where $\{l_1, \ldots, l_5\}$ is a 5-arc of lines; or
(b) $C$ has spectrum $(a_9, a_{13}) = (10, 63)$ with $\lambda_0 = 0$ and $M_C = 2\Sigma - L$, where $L$ is the union of a 10-arc of lines.

Lemma 9. Every $[100, 3, 87]_8$ code is extendable.

3 Proof of Theorem 3

We prove Theorem 3 only for $d = 697$. Let $C$ be a putative Griesmer $[798, 4, 697]_8$ code. By Lemma 8, the spectrum of a $\gamma_2$-plane $\Delta_1$ is either (A) $(\tau_5, \tau_{13}) = (5, 68)$ or (B) $(\tau_9, \tau_{13}) = (10, 63)$. An $i$-plane with a $t$-line satisfies

\[ t \leq \frac{i + 10}{8} \quad (3) \]

by Lemma 6. From Theorem 1 and Lemma 6, one can get $a_i = 0$ for all $i \notin \{30-33, 62-73, 94-101\}$. It follows from (1) that

\[ \sum_{i \leq 99} \binom{101 - i}{2} a_i = 64\lambda_2 - 9123. \quad (4) \]

Lemma 6(d) gives $\sum_j c_j = 8$ and

\[ \sum_j (101 - j)c_j = w + 10 - qt. \quad (5) \]

Suppose $a_{73} > 0$. Since a 73-plane has spectrum $\tau_9 = 73$, $\Delta_1$ has spectrum (B). It follows from (5) that $a_{73} > 0$ implies $a_{73} = 1$ and $a_j = 0$ for other $j < 94$. Setting $w = 73$, the maximum possible contribution of $c_j$'s in (5) to the LHS of (4) is $(c_{94}, c_{97}, c_{101}) = (1, 1, 6)$ for $t = 9$. Hence we get (LHS of (4)) $\leq (21 + 6)73 + 378 = 2349$, giving $\lambda_2 \leq 179$, which contradicts (3): $\lambda_2 = \lambda_0 + 213 \geq 213$. In this proof, we often obtain a contradiction to rule out the existence of some $i$-plane by eliminating the value of $\lambda_2$ using (4), (5) and the possible spectra for a fixed $w$-plane. We refer to this proof technique as "(\(\lambda_2, w\))-ruling out method ((\(\lambda_2, w\))-ROM)" in what follows. One can deduce that $a_w = 0$ by $(\lambda_2, w)$-ROM for $70 \leq w \leq 72$ using the possible spectra of the $[73 - j, 3, 64 - j]_8$ codes for $1 \leq j \leq 3$.

Suppose $a_{30} > 0$ and let $\delta_{30}$ be a 30-plane. It follows from (5) that $a_{30} > 0$ implies $a_{30} = 1$ and $a_j = 0$ for other $j < 94$. Since $\gamma_1(\delta_{30}) = 5$, one can
find a 101-plane $\Delta$ of spectrum (A) meeting $\delta_{30}$ in a 5-line. Take another 5-line $l_5$ on $\Delta$. Then, every plane through $l_5$ has multiplicity at least 94, which is impossible from (5) with $(w, t) = (101, 5)$. Hence $a_{30} = 0$. One can get $a_{31} = a_{32} = a_{33} = 0$, similarly. Using the possible spectra of the $[70-j, 3, 61-j]_8$ codes, we can also prove that $a_{70-j} = 0$ by $(\lambda_2, 70-j)$-ROM for $1 \leq j \leq 3$.

Now, we have $a_i = 0$ for all $i \not\in \{62-66, 94-101\}$. Note that a $(62+e)$-plane with $0 \leq e \leq 3$ could have a 2-point because it corresponds to a $[62+e, 3, 53+e]_8$ code which is not Griesmer. Suppose a $(62+e)$-plane $\delta$ with $0 \leq e \leq 3$ has a 2-point. Then, one can find a 9-line $l_9$ through the 2-point on $\delta$ and a 101-plane through $l_9$ from (5) with $(w, t) = (62+e, 9)$. This contradicts that a 9-line in a 101-plane with spectrum (B) has no 2-point by Lemma 8. Thus, a $(62+e)$-plane with $0 \leq e \leq 4$ has no 2-point since a 66-plane corresponds to a Griesmer code.

Suppose $a_{62} > 0$ and let $\delta_{62}$ be a 62-plane and let $l$ be a 9-line on $\delta_{62}$. Then, the other planes through $l$ are 101-planes, say $\Delta_1, \ldots, \Delta_8$. For a fixed 1-point $P$ on $l$, one can take a 9-line $l_j(\neq l)$ on $\Delta_j$ for $1 \leq j \leq 8$ from the geometric structure described in Lemma 8. Suppose that the plane $\delta = \langle l_1, l_2 \rangle$ is a $(62+e)$-plane with $0 \leq e \leq 3$ and let $\delta \cap \delta_{62}$ be an $\alpha$-line. Since $\gamma_1(\delta) = 9$, $\delta$ contains all of $l_1, \ldots, l_8$, and we have $m_\delta(\delta) = 64 + \alpha$. One can rule out such cases by $(\lambda_2, 64 + \alpha)$-ROM. Hence, $a_{62} > 0$ implies that $a_{62} = 1$ and $a_1 = 0$ for other $j < 94$. Setting $w = 101$, the maximum possible contributions of $c_j$'s in (5) to the LHS of (4) are $(c_{62}, c_{101}) = (1, 7)$ for $t = 9$ with $c_{62} > 0$; $(c_{94}, c_{95}, c_{101}) = (5, 1, 2)$ for $t = 9$ with $c_{62} = 0$; $(c_{94}, c_{101}) = (1, 7)$ for $t = 13$. Using the spectrum of a 101-plane of spectrum (B), one can get a contradiction by $(\lambda_2, 101)$-ROM. Hence $a_{62} = 0$. One can similarly prove $a_{63} = 0$.

To rule out a 101-plane of spectrum (A), let $\Delta_1$ be such a plane. From (5) with $(w, t) = (101, 5)$, there exists a $(64+e)$-plane with $0 \leq e \leq 2$ through each of the 5-lines on $\Delta_1$. One can rule out such a 66-plane by $(\lambda_2, 66)$-ROM using all possible spectra of a 66-plane with a 5-line. Hence $a_{66} = 0$. Note that $\lambda_0 \geq 8 - 4 + 10 = 14$ since a 101-plane of spectrum (A) has ten 0-points. Setting $w = 101$, the maximum possible contributions of $c_j$'s in (5) to the LHS of (4) are $(c_{64}, c_{94}, c_{95}, c_{101}) = (1, 4, 1, 2)$ for $t = 5$; $(c_{94}, c_{101}) = (1, 7)$ for $t = 13$. Using the spectrum of a 101-plane of spectrum (A), one can get a contradiction by $(\lambda_2, 101)$-ROM. Hence every 101-plane has spectrum (B).

Suppose $a_{66} > 0$ and let $\delta_{66}$ be a 66-plane with spectrum $(\tau_2, \ldots, \tau_9)$. Then, from the three equalities in Lemma 5, we obtain $\tau_2 + \tau_3 + \tau_4 \leq 2$ and $\tau_5 + \tau_6 + \tau_7 \leq 21$. Setting $w = 66$, the maximum possible contributions of $c_j$'s in (5) to the LHS of (4) are $(c_{64}, c_{94}, c_{95}, c_{99}) = (1, 1, 1, 5)$ for $t = 2$ since a 100-plane has no 2-line by Lemma 9; $(c_{94}, c_{96}, c_{100}) = (4, 1, 3)$ for $t = 5$ since $c_{101} = 0$; $(c_{96}, c_{100}) = (1, 7)$ for $t = 8$; $(c_{97}, c_{101}) = (1, 7)$ for $t = 9$. Using $(\tau_2, \tau_5, \tau_8, \tau_9) = (2, 21, 49, 1)$ instead of all possible spectra of a 66-plane, one can get a contradiction by $(\lambda_2, 66)$-ROM. Hence $a_{66} = 0$. We can prove $a_{65} = a_{64} = 0$ similarly.

Hence, we have ruled out all possible $i$-planes with $i < 94$. Finally, using the spectrum (B) of a 101-plane, one can get a contradiction by $(\lambda_2, 101)$-ROM. This completes the proof of Theorem 3 for $d = 697$. 

References


