Nonexistence of some Griesmer codes of dimension 4 over \mathbb{F}_q^{-1}

KAZUKI KUMEGAWAsu301015@edu.osakafu-u.ac.jpTATSUYA MARUTAmaruta@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 $[g_q(4, d), 4, d]_q$ codes for (a) $d = q^3/2 - q^2 - 2q + 1$ for $q = 2^h, h \ge 3$, (b) $d = 2q^3 - 3q^2 - 2q + 1$ for $q \ge 7$, and (c) $d = 2q^3 - rq^2 - q + 1$ for $3 \le r \le q - q/p, q = p^h$ with p prime, where $g_q(k, d) = \sum_{i=0}^{k-1} \left[d/q^i \right]$.

1 Introduction

An $[n, k, d]_q$ code C is a linear code of length n, dimension k and minimum Hamming weight d over \mathbb{F}_q , the field of q elements. 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. The Griesmer bound gives a lower bound on $n_q(k, d)$ as $n_q(k, d) \ge g_q(k, d) = \sum_{i=0}^{k-1} \left\lceil d/q^i \right\rceil$, where $\lceil x \rceil$ denotes the smallest integer $\ge x$. An $[n, k, d]_q$ code is called *Griesmer* if $n = g_q(k, d)$. The values of $n_q(k, d)$ are determined for all d only for some small values of q and k. For k = 4, $n_q(4, d)$ is known for all d only for q = 2, 3, 4. It is known that $n_q(4, d) \ge g_q(4, d) + 1$ for $q^3/2 - q^2 - q + 1 \le d \le q^3/2 - q^2$ for even $q \ge 4$ [4] and for $2q^3 - rq^2 - q + 1 \le d \le 2q^3 - rq^2$ for q > r, r = 3, 4 and for $q > 2(r-1), r \ge 5$ [5]. It is also known that $n_q(4, d) = g_q(4, d) + 1$ for $2q^3 - 3q^2 - q + 1 \le d \le 2q^3 - 3q^2$ for $q \ge 4$ [5]. Our main result is following.

Theorem 1. There exist no $[g_q(4, d), 4, d]_q$ codes for (a) $d = q^3/2 - q^2 - 2q + 1$ for $q = 2^h$, $h \ge 3$, (b) $d = 2q^3 - 3q^2 - 2q + 1$ for $q \ge 7$, and (c) $d = 2q^3 - rq^2 - q + 1$ for $3 \le r \le q - q/p$, $q = p^h$ with p prime.

Note that a $[g_q(4, d)+1, 4, d]_q$ code with $d = 2q^3 - 3q^2 - q$ can be constructed, see Lemma 8 in [3]. 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 results (combining the previously known results).

Corollary 2. $n_q(4,d) = g_q(4,d) + 1$ for $2q^3 - 3q^2 - 2q + 1 \le d \le 2q^3 - 3q^2$ for $q \ge 5$.

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

Corollary 3. $n_q(4,d) \ge g_q(4,d) + 1$ for (a) $q^3/2 - q^2 - 2q + 1 \le d \le q^3/2 - q^2$ for $q = 2^h$, $h \ge 3$, (b) $2q^3 - rq^2 - q + 1 \le d \le 2q^3 - rq^2$ for $4 \le r \le q - q/p$, $q = p^h$ with p prime.

2 Preliminary results

We denote by 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 in PG(r, q) are called *points*, lines, planes, secundums and hyperplanes, respectively. We denote by \mathcal{F}_j the set of j-flats of 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 $\Sigma = PG(k-1,q)$ denoted also by C. We see linear codes from this geometrical point of view. An *i*-point is a point of Σ which has multiplicity i in 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 , $0 \leq i \leq \gamma_0$. For any subset S of Σ , the multiplicity of S with respect to C, denoted by $m_{\mathcal{C}}(S)$, is defined 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. A line l with $t = m_{\mathcal{C}}(l)$ is called a *t*-line. A *t*-plane 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_i instead of $\gamma_i(\Sigma)$. Then $\gamma_{k-2} = n - d$, $\gamma_{k-1} = n$. For a Griesmer $[n, k, d]_q$ code, it is known (see [6]) that

$$\gamma_j = \sum_{u=0}^{j} \lceil d/q^{k-1-u} \rceil \quad \text{for } 0 \le j \le k-1.$$
(1)

So, every Griesmer $[n, k, d]_q$ code is projective if $d \leq q^{k-1}$. 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 4. (a)
$$\sum_{i=0}^{n-d} a_i = \theta_{k-1}$$
. (b) $\sum_{i=1}^{n-d} ia_i = n\theta_{k-2}$.
(c) $\sum_{i=2}^{n-d} i(i-1)a_i = n(n-1)\theta_{k-3} + q^{k-2} \sum_{s=2}^{\gamma_0} s(s-1)\lambda_s$.

When $\gamma_0 \leq 2$, the above three equalities yield the following:

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

Kumegawa, Maruta

Lemma 5 ([7]). Let Π be an *i*-hyperplane through a *t*-secundum δ . Then (a) $t \leq \gamma_{k-2} - (n-i)/q = (i+q\gamma_{k-2}-n)/q$.

(b) $a_i = 0$ 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. (c) $\gamma_{i-1} = \lfloor (i + q\gamma_{k-2} - n)/q \rfloor$ if $an [i, k-1, d_1]$ code with $d_1 \ge i - q$

(c) $\gamma_{k-3}(\Pi) = \lfloor (i+q\gamma_{k-2}-n)/q \rfloor$ if an $[i,k-1,d_1]_q$ code with $d_1 \geq i - \lfloor (i+q\gamma_{k-2}-n)/q \rfloor + 1$ does not exist.

(d) Let c_j be the number of *j*-hyperplanes through δ other than Π . Then

$$\sum_{j} (\gamma_{k-2} - j)c_j = i + q\gamma_{k-2} - n - qt.$$
(3)

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

Lemma 6 ([4]). For even $q \ge 4$, the spectrum of a $[q(q-1)/2 - 1, 3, q(q-2)/2 - 1]_q$ code is $(a_0, a_{q/2-1}, a_{q/2}) = (q+2, q+1, q^2 - q - 2)$.

Lemma 7 ([4]). For $q \ge 7$, the spectrum of a $[2q^2 - q - 2, 3, 2q^2 - 3q - 1]_q$ code is either $(a_{q-2}, a_{q-1}, a_{2q-2}, a_{2q-1}) = (1, 2, q, q^2 - 2)$ or $(a_{q-1}, a_{2q-2}, a_{2q-1}) = (3, q + 1, q^2 - 3)$.

An *n*-set K in PG(2,q) is an (n,r)-arc if every line meets K in at most r points and if some line meets K in exactly r points. Let $m_r(2,q)$ denote the largest value of n for which an (n,r)-arc exists in PG(2,q).

Lemma 8 ([2]). (a) $m_r(2,q) \leq (r-1)q + r$. (b) $m_r(2,q) \leq (r-1)q + r - 3$ for $4 \leq q < q$ with $r \not| q$. (c) $m_r(2,q) \leq (r-1)q + r - 4$ for $9 \leq q < q$ with $r \not| q$.

An f-multiset F in PG(2,q) is an (f,m)-minihyper if every line meets F in at least m points and if some line meets F in exactly m points with multiplicity.

Lemma 9 ([1]). Every (x(q+1), x)-minihyper in PG(2, q), $q = p^h$, p prime, with $x \leq q - q/p$ is a sum of x lines.

3 Proof of Theorem 1

To prove (a) of Theorem 1, let C_1 be a putative $[g_q(4,d), 4, d]_q$ codes for $d = q^3/2 - q^2 - 2q + 1$ for $q = 2^h$, $h \ge 4$ (see [4] for q = 8). By Lemma 6, the spectrum of a γ_2 -plane Δ_1 is $(\tau_0, \tau_{\frac{q}{2}-1}, \tau_{\frac{q}{2}}) = (q+2, q+1, q^2 - q - 2)$. For any integer *i* with $1 \le i \le (q^2 - 5q - 2)/2$, we have

$$t \le \frac{i}{q} + \frac{3}{2} \tag{4}$$

by Lemma 5. Let $C_1^{(i)}$ be the $[i,3]_q$ code corresponding to an *i*-plane δ_1 . For $1 \leq i \leq \frac{q}{2} - 1$, we get $t \leq 1$ from (4). Since δ_1 has no 1-line, we have t = 0 by Lemma 5(e), which is impossible. For $(s-\frac{1}{2})q \leq i \leq (s+\frac{1}{2})q-1$ $(1 \leq s \leq \frac{q}{2}-3)$, we get $t \leq s+1$ from (4). Since δ_1 has no (s+1)-line, we have $t \leq s$ and $C_1^{(i)}$ is an $[i,3,d_0]_q$ code with $d_0 \geq i-s$ by Lemma 5(e), which does not exist by the Griesmer bound. Hence $a_i = 0$ for all $i \notin \{0, (q^2 - 5q)/2, \cdots, (q^2 - q - 2)/2\}$. It follows from (2) with $\lambda_2 = 0$ that

$$\binom{\gamma_2}{2}a_0 + \sum_{j=0}^{2q-1} \binom{2q-1-j}{2}a_{\alpha+j} = \frac{q^5+q^4}{8} - \frac{3}{2}q^2 - 2q + 1, \tag{5}$$

where $\alpha = \frac{q^2 - 5q}{2}$. Lemma 5(d) gives $\sum_j c_j = q$ and

$$\sum_{j} \left(\frac{q^2 - q - 2}{2} - j\right)c_j = i + \frac{3}{2}q - qt.$$
(6)

Suppose $a_0 > 0$. It follows from (6) that $a_0 = 1$ and $a_j = 0$ for $1 \le j \le \frac{q^2 - 4q - 4}{2}$. Setting $i = n - d = \frac{q^2 - q - 2}{2}$, RHS of (6) is $\frac{q^2 + 2q - 2}{2}$ for t = 0; 2q - 1 for $t = \frac{q}{2} - 1$; q - 1 for $t = \frac{q}{2}$. If $q \equiv 2$ mod 3, the maximum possible contributions of c_j 's in (6) to the LHS of (5) are $(c_0, c_{\frac{q^2 - 4q - 2}{2}}, c_{n-d}) = (1, 1, q - 2)$ if $c_0 > 0$ for t = 0 and $(c_{\frac{q^2 - 4q - 2}{2}}, c_{\frac{q^2 - 2q}{2}}, c_{n-d}) = (\frac{q+1}{3}, 1, \frac{2q-4}{3})$ if $c_0 = 0$ for t = 0; $(c_{\frac{q^2 - 4q - 2}{2}}, c_{\frac{q^2 - 2q}{2}}, c_{n-d}) = (1, 1, q - 2)$ for $t = \frac{q}{2} - 1$; $(c_{\frac{q^2 - 3q}{2}}, c_{n-d}) = (1, q - 1)$ for $t = \frac{q}{2}$. Hence we get (LHS of (5)) $\le (\binom{\gamma_2}{2} + \binom{\frac{3}{2}q}{2} + 0 \cdot (q - 2)) + (\binom{\frac{3}{2}q}{2} \cdot \frac{q+1}{3} + \binom{\frac{q}{2}-1}{2}) + 0 \cdot \frac{2q-4}{3} \cdot (\tau_0 - 1) + (\binom{\frac{3}{2}q}{2}) + \binom{\frac{q}{2}-1}{2} + 0 \cdot (q - 2)) \cdot \tau_{\frac{q}{2}-1} + (\binom{q-1}{2}) + 0 \cdot (q - 1)) \cdot \tau_{\frac{q}{2}} = q^4 - \frac{3}{8}q^3 + q^2 + \frac{3}{2}q + 1 < \frac{q^5 + q^4}{8} - \frac{3}{2}q^2 - 2q + 1$, a contradiction. One can get a contradiction for $q \equiv 1 \pmod{3}$ similarly. Thus $a_0 = 0$. Setting i = n - d, the maximum possible contributions of c_j 's in (6) to the LHS of (5) are $(c_{\frac{q^2 - 5q}{2}}, c_{n-d}) = (\frac{q}{4}, 1, \frac{3}{4}q - 1)$ for $t = \frac{q}{2}$. So, (LHS of (5)) $\le (\binom{2q-1}{2} + \binom{q}{4} + \binom{5}{2} - 1) + 0 \cdot \binom{2q-1}{4} + \binom{5}{4} - \frac{1}{2} + 0 \cdot \binom{2q-1}{2} + 0 \cdot (q - 1)) \cdot \tau_{\frac{q}{2}-1} + (\binom{q-1}{2}) + 0 \cdot \binom{q-1}{2} + 0 \cdot$

Next, to prove (b) of Theorem 1, let C be a putative $[g_q(4, d), 4, d]_q$ codes for $d = 2q^3 - 3q^2 - 2q + 1$ for $q \ge 7$. We have $\gamma_0 = 2$, $\gamma_1 = 2q - 1$ from (1). By Lemma 7, the spectrum of a γ_2 -plane Δ is (A) $(\tau_{q-2}, \tau_{q-1}, \tau_{2q-2}, \tau_{2q-1}) = (1, 2, q, q^2 - 2)$ or (B) $(\tau_{q-1}, \tau_{2q-2}, \tau_{2q-1}) = (3, q + 1, q^2 - 3)$. By Lemma 5, an *i*-plane satisfies

Kumegawa, Maruta

$$\begin{split} i &\geq (q-2)q - (q+1) = q^2 - 3q - 1. \text{ Hence } a_i = 0 \text{ for any } i < q^2 - 3q - 1. \\ \text{Assume that an } i\text{-plane contains a 2-point. Since } (\gamma_1 - 2)\theta_2 + 2 = n + 2q, \text{ we} \\ \text{have } i &\geq (\gamma_1 - 2)\theta_1 + 2 - 2q = (2q-3)\theta_1 + 2 - 2q = 2q^2 - 3q - 1 > \theta_2 \text{ for } q \geq 7. \\ \text{Thus, } a_i = 0 \text{ if } i < q^2 - 3q - 1 \text{ or } \theta_2 < i < 2q^2 - 3q - 1. \\ \text{Furthermore, using Lemmas 5 and 8, it can be proved that } a_i > 0 \text{ implies } i \in \{q^2 - 3q - 1, \cdots, q^2 - 2q - 5, q^2 - 2q - 1, \cdots, q^2 - q - 5, q^2 - 1, q^2 + q - 1, 2q^2 - 3q - 1, \cdots, 2q^2 - q - 2\}. \\ \text{From (2), we get} \end{split}$$

$$\sum_{i=q^2-3q-1}^{2q^2-q-4} \binom{2q^2-q-2-i}{2} a_i = q^2\lambda_2 + \left(-q^5 + \frac{7}{2}q^4 + 2q^3 - \frac{11}{2}q^2 - 2q + 1\right).$$
(7)

For any *i*-plane through a *t*-line, Lemma 5(d) gives $\sum_{j} c_{j} = q$ and

$$\sum_{j} (2q^2 - q - 2 - j)c_j = i + q + 1 - qt.$$
(8)

Suppose $a_i > 0$ for $i = q^2 - 3q - 1 + e$ with $0 \le e \le q - 4$ and let δ be an *i*-plane. We may assume that Δ has spectrum (A). It follows from Lemma 8 and known results on $m_{q-2}(2,q)$ for small q that we have $i \le q^2 - 2q - 6$ for $q \ge 7$. So, we have $e \le q - 5$. Note that $a_i > 0$ implies $a_i = 1$ and $a_j = 0$ for $q^2 - 3q - 1 \le j \le q^2 - 2q - 6$, $j \ne i$. Now, we set i = n - d in (8). If q is odd, the maximum possible contributions of c_j 's in (8) to the LHS of (7) are $(c_{q^2-3q-1+e}, c_{n-d-e}, c_{n-d}) = (1, 1, q-2)$ for t = q-2; $(c_{2q^2-3q-1}, c_{2q^2-\frac{3}{2}q-\frac{3}{2}}, c_{n-d}) = (\frac{q+1}{2}, 1, \frac{q-3}{2})$ for t = q-1; $(c_{2q^2-3q-1}, c_{n-d}) = (1, q - 1)$ for t = 2q - 2; $(c_{2q^2-2q-1}, c_{n-d}) = (1, q - 1)$ for t = 2q - 1. Hence we get (LHS of (7)) $\le (\binom{q^2+2q-1-e}{2} + \binom{e}{2})\tau_{q-2} + (\frac{q+1}{2}\binom{2q-1}{2} + \binom{\frac{q-1}{2}}{2})\tau_{q-1} + \binom{2q-1}{2}\tau_{2q-2} + \binom{q-1}{2}\tau_{2q-1}$, giving $\lambda_2 < q^3 - \frac{5}{2}q^2 + \frac{5}{2}q + \frac{15}{4}$. On the other hand, we have $\lambda_2 = n - \theta_3 + \lambda_0 \ge (2q^3 - q^2 - 3q - 1) - (q^3 + q^2 + q + 1) + ((q^2 + q + 1) - (q^2 - 2q - 6)) = q^3 - 2q^2 - q + 5$, giving a contradiction for $q \ge 7$. One can also get a contradiction when q is even. Thus, $a_i = 0$ for $q^2 - 3q - 1 \le i \le q^2 - 2q - 5$. Similarly, we can get $a_i = 0$ for all $i < 2q^2 - 3q - 1$ using Lemma 5 and (7). Finally, we investigate (7) and (8) with i = n - d again. Assume q is odd. The maximum possible contributions of c_j 's in (8) to the LHS of (7) on Δ are $(c_{2q^2-3q-1}, c_{2q^2-\frac{5}{2}q-\frac{3}{2}}, c_{n-d}) = (\frac{q+1}{2}, 1, \frac{q-3}{2})$ for t = q - 2; $(c_{2q^2-3q-1}, c_{2q^2-\frac{5}{2}q-\frac{3}{2}}, c_{n-d}) = (\frac{q+1}{2}, 1, \frac{q-3}{2})$ for t = q - 2; $(c_{2q^2-3q-1}, c_{2q^2-\frac{5}{2}q-\frac{3}{2}}, c_{n-d}) = (\frac{q+1}{2}, \frac{q-1}{2})$ for t = 2q - 1. Hence we get (LHS of (7)) $\leq (\frac{q+1}{2}\binom{2q-1}{2} + \binom{\frac{q+1}{2}\binom{2q-1}{2}} + \binom{\frac{q+1}{2}\binom{2q-1}{2}} + \binom{\frac{q+1}{2}\binom{2q-1}{2}} + \binom{\frac{q+1}{2}\binom{2q-1}{2}} + \binom{\frac{q+1}{2}\binom{2q-1}{2}} + \binom{\frac{q+1}{2}\binom{2q-1}{2}} + \binom{\frac{q+1}{2}\binom{2q$

 $n-\theta_3+\lambda_0 \ge (2q^3-q^2-3q-1)-(q^3+q^2+q+1)=q^3-2q^2-4q-2$, giving a contradiction for $q \ge 7$. One can get a contradiction similarly when q is even. This completes the proof of (b).

Finally, we give a sketch of the proof of (c) in Theorem 1. Let \mathcal{C} be a putative $[g_q(4,d), 4, d]_q$ codes for $d = 2q^3 - rq^2 - q + 1$ for $3 \leq r \leq q - q/p$, $q = p^h$ with p prime. Let Δ be a γ_2 -plane. Then we can prove the following.

Lemma 10 (Cf. [5]). (a) On Δ , every line through a 2-point is a γ_1 -line. (b) Every *i*-line through a 2-point satisfies $\theta_2 < \gamma_2 - (q-1) \le i \le \gamma_2$. (c) The multiset for Δ consists of two copies of the plane with an (r, 2)-arc of lines deleted.

Since the multiset given by two copies of Δ with the multiset for Δ deleted forms an $(r\theta_1, r; 2, q)$ -minihyper and since $\gamma_0 = 2$, we can employ Lemma 9 to prove the part (c) of Lemma 10. Lemma 10 yields that Lemma 4.1 in [5] holds under our assumption " $5 \leq r \leq q - q/p$, $q = p^h$ with p prime" instead of " $q > 2(r-1), r \geq 5$ ". From a similar argument as in the proof for (a), we can show that $a_i > 0$ implies $q^2 - (r-1)q - (r-3) \leq i \leq q^2 - (r-2)q - (r-2)$ or $\gamma_2 - (q-1) \leq i \leq \gamma_2$. Then, one can get a contradiction as in the proof of Theorem 1.4 in [5]. This completes the proof of (c).

References

- R. Hill and H. Ward, A geometric approach to classifying Griesmer codes, Des. Codes Cryptogr., 44, 169–196, 2007.
- [2] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, in: A. Blokhuis et al. (Eds.), Finite Geometries, Developments in Mathematics Vol. 3, Kluwer, 2001, 201-246.
- [3] Y. Kageyama and T. Maruta, On the construction of optimal codes over \mathbb{F}_q , preprint.
- [4] R. Kanazawa and T. Maruta, On optimal linear codes over F₈, *Electron. J. Combin.*, 18, #P34, 27pp., 2011.
- [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, On the nonexistence of q-ary linear codes of dimension five, Des. Codes Cryptogr., 22, 165-177, 2001.
- [7] M. Takenaka, K. Okamoto and T. Maruta, On optimal non-projective ternary linear codes, *Discrete Math.*, 308, 842–854, 2008.