Nonexistence of some Griesmer codes of dimension 5 *

Wataru Kuranaka, Tatsuya Maruta †
Department of Mathematical Sciences
Osaka Prefecture University

1 Introduction

A linear code over $\mathbb{F}_q$, the field of q elements, of length n, dimension k is a k-dimensional subspace $\mathcal{C}$ of the vector space $\mathbb{F}_q^n$ of n-tuples over $\mathbb{F}_q$. $\mathcal{C}$ is called an $[n,k,d]_q$ code if it has minimum Hamming weight d. A $k \times n$ matrix G whose rows form a basis of $\mathcal{C}$ is a *generator matrix* of $\mathcal{C}$. 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 for given q,k,d [6, 7]. A natural lower bound on $n_q(k,d)$ is the Griesmer bound:

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

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x, see [1]. A linear 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 [5, 16]. Note that $n_q(k,d) = g_q(k,d)$ for all d when $k = 1$ or 2 [6]. The problem to determine $n_q(k,d)$ for all d has been solved for $k \leq 8$ when $q = 2$, for $k \leq 5$ when $q = 3$, for $k \leq 4$ when $q = 4$ and only for $k = 3$ when $5 \leq q \leq 9$, see [16]. For the case $k = 5$, the following results are known.

Theorem 1.1 ([2, 9, 10, 15]). *For any prime power q, $n_q(5,d) = g_q(5,d)$ for*

(1) $q^4 - q^3 - q + 1 \leq d \leq q^4 - q^3 + q^2 - q$,

(2) $q^4 - 2q^2 + 1 \leq d \leq q^4 + q$,

(3) $2q^4 - 3q^3 + 1 \leq d \leq 2q^4 - 3q^3 + q^2$,

(4) $2q^4 - 2q^3 - q^2 + 1 \leq d \leq 2q^4 + q^2 - q$,

*This paper is a preliminary version and the final version will be submitted to elsewhere.
†Corresponding author. E-mail address: maruta@mi.s.osakafu-u.ac.jp

(5) $3q^4 - 5q^3 + q^2 + 1 \le d \le 3q^4 - 5q^3 + 2q^2$,

(6) $d \ge 3q^4 - 4q^3 + 1$.

Theorem 1.2 ([3, 4, 11, 15, 16]). $n_q(5, d) = g_q(5, d) + 1$ *for*

(1) $q^4 - q^3 - q^2 + 1 < d \le q^4 - q^3 - q$ *for* $q \ge 3$,

(2) $q^4 - 2q^2 - 2q + 1 \le d \le q^4 - 2q^2 - q$ *for* $q \ge 4$,

(3) $q^4 - 2q^2 - q + 1 \le d \le q^4 - 2q^2$ *for* $q \ge 3$,

(4) $2q^4 - 2q^3 - q^2 - 2q + 1 \le d \le 2q^4 - 2q^3 - q^2$ *for* $q \ge 3$,

(5) $3q^4 - 4q^3 - 2q + 1 \le d \le 3q^4 - 4q^3 - q$ *for* $q \ge 11$,

(6) $3q^4 - 4q^3 - q + 1 \le d \le 3q^4 - 4q^3$ *for* $q \ge 5$.

Our main result is the following.

Theorem 1.3. $n_q(5, d) = g_q(5, d) + 1$ *for* $3q^4 - 4q^3 - 4q + 1 \le d \le 3q^4 - 4q^3 - q$ *for* $q \ge 5$.

2 Preliminaries

In this section, we give the geometric method through $\mathrm{PG}(r, q)$, the projective geometry of dimension r over $\mathbb{F}_q$, and preliminary results to prove the main result. The 0-flats, 1-flats, 2-flats, 3-flats, $(r-2)$-flats and $(r-1)$-flats in $\mathrm{PG}(r, q)$ are called *points, lines, planes, solids, secundums* and *hyperplanes*, respectively.

Let $\mathcal{C}$ be an $[n, k, d]_q$ code having no coordinate which is identically zero. The columns of a generator matrix G of $\mathcal{C}$ can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1, q)$, denoted by $\mathcal{M}_\mathcal{C}$. A point P of Σ is an *i-point* if it has multiplicity $m_\mathcal{C}(P) = i$ in $\mathcal{M}_\mathcal{C}$. In other words, $m_\mathcal{C}(P)$ is the number of times which P appears as columns of G. Denote by γ_0 the maximum multiplicity of a point from Σ in $\mathcal{M}_\mathcal{C}$. For any subset S of Σ, *the multiplicity of S with respect to $\mathcal{M}_\mathcal{C}$*, denoted by $m_\mathcal{C}(S)$, is defined as $m_\mathcal{C}(S) = \sum_{P \in S} m_\mathcal{C}(P)$. Then $m_\mathcal{C}$ satisfies $n = m_\mathcal{C}(\Sigma)$ and

$$n - d = \max\{m_\mathcal{C}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}, \tag{2.1}$$

where $\mathcal{F}_j$ denotes the set of j-flats of Σ. Conversely, such a mapping $m_\mathcal{C} : \Sigma \to \mathbb{N}_0 = \{0, 1, 2, \dots\}$ as above gives an $[n, k, d]_q$ code in the natural manner, see [1]. For an m-flat Π in Σ, we define

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

We denote simply by γ_j instead of $\gamma_j(\Sigma)$. Then $\gamma_{k-2} = n - d$, $\gamma_{k-1} = n$. For a Griesmer $[n, k, d]_q$ code, it is known (see [15]) that

$$\gamma_j = \sum_{u=0}^{j} \left\lceil \frac{d}{q^{k-1-u}} \right\rceil \ \text{ for } \ 0 \le j \le k-1. \tag{2.2}$$

A line l with $t = m_{\mathcal{C}}(l)$ is called a *t-line*. A *t-plane* and so on are defined similarly. Denote by a_i the number of i-hyperplanes 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 Π of Σ to distinguish from the spectrum of $\mathcal{C}$ (τ_j is the number of j-secundums contained in Π). Let θ_j be the number of points in a j-flat, i.e., $\theta_j = (q^{j+1} - 1)/(q - 1)$. Simple counting arguments yield the following.

Lemma 2.1 ([17]). *Let Π be a w-hyperplane through a t-secundum δ. Then*

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

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

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

(d) *Let c_j be the number of j-hyperplanes through δ other than Π. Then* $\sum_j c_j = q$ *and*

$$\sum_j (\gamma_{k-2} - j)c_j = w + q\gamma_{k-2} - n - qt. \tag{2.3}$$

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

Lemma 2.2 ([12]). *Let Π be an i-hyperplane and let $\mathcal{C}_\Pi$ be an $[i, k-1, d_0]$ code generated by $\mathcal{M}_{\mathcal{C}}(\Pi)$. If any γ_{k-2}-hyperplane has no t-secundum with* $t = \left\lfloor \frac{i+q\gamma_{k-2}-n}{q} \right\rfloor$, *then* $d_0 \geq i - t + 1$.

Lemma 2.3. *The spectrum of an $[n, k, d]_q$ code satisfies* $\sum_{i \leq u} a_i \leq 1$, *where*

$$u = \left\lfloor \frac{n - (n-d)(q-1) - 1}{2} \right\rfloor.$$

Proof. Assume $a_i > 0$ for an $i \leq u$. Then, the right hand side of (2.3) is at most $u + (n-d)q - n$. Since $u < (n - (n-d)(q-1))/2$, we have $n - d - u > u + (n-d)q - n$, which implies that $c_j = 0$ for any $j \leq u$. Hence, $a_i = 1$ and $a_j = 0$ for other $j \leq u$. □

An f-multiset $\mathcal{F}$ on PG(r, q) satisfying

$$m = \min\{m_{\mathcal{F}}(\pi) \mid \pi \in \mathcal{F}_{r-1}\}$$

is called an (f, m)-*minihyper*. When an $[n, k, d]_q$ code is projective (i.e. $\gamma_0 = 1$), the set of 0-points forms a $(\theta_{k-1} - n, \theta_{k-2} - (n-d))$-minihyper in PG$(k-1, q)$, and vice versa.

Lemma 2.4 ([8]). *Every $(x(q+1), x)$-minihyper in PG$(2, q)$ with $q = p^m$, p prime, $m \geq 1$, $1 \leq x \leq q - q/p$, is a sum of x lines.*

3 A sketch of the proof of Theorem 1.3

Lemma 3.1. *Let $q \geq 3$ be a prime power.*

(a) *A $[2q^2, 3, 2q^2 - 2q]_q$ code has spectrum $(a_0, a_{2q}) = (1, q^2 + q)$.*

(b) *A $[2q^2 + q + 1, 3, 2q^2 - q]_q$ code has spectrum $(a_{q+1}, a_{2q+1}) = (1, q^2 + q)$.*

(c) *A $[2q^2 + 2q + 1, 3, 2q^2 - 1]_q$ code has spectrum $(a_{2q+1}, a_{2q+2}) = (q + 1, q^2)$.*

(d) *A $[2q^2 + 2q + 2, 3, 2q^2 - 2q]_q$ code has spectrum $a_{2q+2} = q^2 + q + 1$.*

Lemma 3.2. *Let $\mathcal{C}_1$ be a Griesmer $[3q^2 - q - 1, 3, 3q^2 - 4q]_q$ code with $q \geq 5$. Then, the spectrum of $\mathcal{C}_1$ is $(a_{2q-1}, a_{3q-1}) = (4, \theta_2 - 4)$ and $\mathcal{M}_{\mathcal{C}_1} = 3\Sigma - (l_1 + l_2 + l_3 + l_4)$, where $\Sigma = \mathrm{PG}(2, q)$ and $l_1, \ldots, l_4$ are four non-concurrent lines.*

Proof. Since $\gamma_0 = 3$ from (2.2), the multiset $\mathcal{F} = 3\Sigma - \mathcal{M}_{\mathcal{C}_1}$ forms a $(4\theta_1, 4)$-minihyper. Hence $\mathcal{F}$ is a sum of four lines, say $l_1, \ldots, l_4$, by Lemma 2.4, which are non-concurrent because of $\gamma_0 = 3$. □

Using Lemmas 3.1 and 3.2, one can prove the following.

Lemma 3.3. *Let $\mathcal{C}_2$ be a Griesmer $[3q^3 - q^2 - q - a, 4, 3q^3 - 4q^2 - a + 1]_q$ code with $q \geq 5$ and $2 \leq a \leq 4$. Then, the spectrum of $\mathcal{C}_2$ satisfies that $a_i > 0$ implies $2q^2 - q - a \leq i \leq 2q^2 - q - 1$ or $3q^2 - q - a \leq i \leq 3q^2 - q - 1$ and that*

$$\sum_{i \leq 2q^2 - q - 1} a_i = 4. \tag{3.1}$$

Lemma 3.4 ([14])**.** *$n_q(4, d) = g_q(4, d) + 1$ for $2q^3 - 3q^2 - q + 1 \leq d \leq 2q^3 - 3q^2$ for $q \geq 4$.*

It is known that $[g_q(5, d) + 1, 5, d]_q$ codes exist for $3q^4 - 4q^3 - 4q + 1 \leq d \leq 3q^4 - 4q^3 - q$ for $q \geq 5$, see [11]. Hence, it suffices to show the following to prove Theorem 1.3.

Lemma 3.5. *There exists no $[g_q(5, d), 5, d]_q$ code for $d = 3q^4 - 4q^3 - aq + 1$ with $2 \leq a \leq 4$ for $q \geq 5$.*

Proof. We prove the lemma only for $a = 3$. One can prove the lemma similarly for $a = 2, 4$. Let $\mathcal{C}$ be a putative $[g_q(5, d), 5, d = 3q^4 - 4q^3 - 3q + 1]_q$ code with $q \geq 5$. Then, a γ_3-solid Δ_0 gives a Griesmer $[3q^3 - q^2 - q - 3, 4, 3q^3 - 4q^2 - 2]_q$ code. Since an i-solid through a t-plane satisfies

$$t \leq \frac{i + q + 2}{q} \tag{3.2}$$

by Lemma 2.1, we have

$$i \geq (2q^2 - q - 3)q - (q + 2) = 2q^3 - q^2 - 4q - 2.$$

Hence, $a_i = 0$ for all $i < 2q^3 - q^2 - 4q - 2$. Applying Lemma 2.1(d), we have $\sum_j c_j = q$ and

$$\sum_j (3q^3 - q^2 - q - 3 - j)c_j = i - qt + q + 2. \tag{3.3}$$

Suppose an i-solid Δ exists for $i = 2q^3 - q^2 - q - 2 + y$ with $0 \le y \le q - 1$. Then, we have $t \le 2q^2 - q - 1$ by (3.2) and Lemma 3.3. Hence, Δ gives an $[i, 4, 2q^3 - 3q^2 - 1 + y]_q$ code, which does not exist for $y > 1$ by the Griesmer bound. For $y = 0, 1$, Δ gives a Griesmer code, which does not exist by Lemma 3.4. Hence $a_i = 0$ for $2q^3 - q^2 - q - 2 \le i \le 2q^3 - q^2 - 3$.
Next, suppose an i-solid Δ exists for $i = 2q^3 - q^2 + xq - 2 + y$ with $0 \le x \le q^2 - 5$, $0 \le y \le q - 1$. Then, we have $t \le 2q^2 - q + 1 + x$ by (3.2). Since (3.3) satisfies $c_{n-d} = 0$ for $t = 2q^2 - q + 1 + x$ and $c_{n-d} = c_{n-d-1} = 0$ for $t = 2q^2 - q + x$ by Lemma 3.3, we have $t \le 2q^2 - q - 1 + x$. Hence, Δ gives an $[i, 4, 2q^3 - 3q^2 + (x+1)q - 1 - x + y]_q$ code, which does not exist by the Griesmer bound. Hence, $a_i = 0$ for $2q^3 - q^2 - 2 \le i \le 3q^3 - q^2 - 4q - 3$. Now, the spectrum of $\mathcal{C}$ satisfies that $a_i > 0$ implies

$$sq^3 - q^2 - 4q - 2 \le i \le sq^3 - q^2 - q - 3 \text{ with } s = 2 \text{ or } 3.$$

Setting $(i, t) = (3q^3 - q^2 - q - 3, 2q^2 - q - 3 + e)$ with $0 \le e \le 2$, the RHS of (3.3) is equal to $q^3 + (3 - e)q - 1$. Hence

$$\sum_{i \le 2q^3 - q^2 - q - 3} a_i = 4 \tag{3.4}$$

by (3.1). Setting $i = 2q^3 - q^2 - q - 3$ in (3.3), (RHS of (3.3))$= 2q^3 - q^2 - 1 - qt$. When $\sum_{j \le 2q^3 - q^2 - q - 3} c_j > 0$, we have $t \le q^2 - q - 1$ from (3.3). It follows from Lemma 2.3 with length $n = i$ and $n - d = 2q^2 - q - 1$ that $u = \lfloor q^2 - \frac{q+5}{2} \rfloor > q^2 - q - 1$. Hence, $\sum_{i \le 2q^3 - q^2 - q - 3} a_i \le 2$, which contradicts (3.4). Similarly, we get $\sum_{i \le 2q^3 - q^2 - q - 3} a_i \le 2$ for $2q^3 - q^2 - 4q - 2 \le i \le 2q^3 - q^2 - q - 4$, which contradicts (3.4) again. Thus, there exists no $[g_q(5, d), 5, d]_q$ code for $d = 3q^4 - 4q^3 - 3q + 1$. $\square$

References

[1] J. Bierbrauer, Introduction to Coding Theory, Chapman & Hall/CRC, 2005.

[2] E.J. Cheon, Y. Kageyama, S.J. Kim, N. Lee, T. Maruta, Construction of two-weight codes over finite fields and its applications, Bull. Korean Math. Soc. **54** (2017) 731–736.

[3] E.J. Cheon, T. Kato, S.J. Kim, On the minimum length of some linear codes of dimension 5, Design Codes Cryptogr. **37** (2005) 421–434.

[4] E.J. Cheon, T. Kato, S.J. Kim, Nonexistence of a $[g_q(5, d), 5, d]_q$ code for $3q^4 - 4q^3 - 2q + 1 \le d \le 3q^4 - 4q^3 - q$, Discrete Math. **308** (2008) 3082–3089.

[5] M. Grassl, Tables of linear codes and quantum codes (electronic table, online). `http://www.codetables.de/`.

[6] R. Hill, Optimal linear codes, in: Mitchell C. (ed.) Cryptography and Coding II, pp. 75–104. Oxford Univ. Press, Oxford, 1992.

[7] R. Hill, E. Kolev, A survey of recent results on optimal linear codes, in: Holroyd F.C. et al (ed.) Combinatorial Designs and their Applications, pp.127–152. Chapman and Hall/CRC Press Research Notes in Mathematics CRC Press. Boca Raton, 1999.

[8] R. Hill, H. Ward, A geometric approach to classifying Griesmer codes, Des. Codes Cryptogr. **44** (2007) 169-196.

[9] Y. Inoue, T. Maruta, Construction of new Griesmer codes of dimension 5, Finite Fields Appl. **55** (2019), 231–237.

[10] Y. Kageyama, T. Maruta, On the construction of Griesmer codes of dimension 5, Des. Codes Cryptogr. **75** (2015) 277–280.

[11] Y. Kageyama, T. Maruta, On the geometric constructions of optimal linear codes, Des. Codes Cryptogr. **81** (2016) 469–480.

[12] K. Kumegawa, T. Okazaki, T. Maruta, On the minimum length of linear codes over the field of 9 elements, *Electronic J. Combin.* **24**(1) (2017), #P1.50.

[13] I.N. Landjev, T. Maruta, On the minimum length of quaternary linear codes of dimension five, *Discrete Math.* **202** (1999) 145–161.

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

[15] T. Maruta, On the nonexistence of q-ary linear codes of dimension five, Des. Codes Cryptogr. **22** (2001) 165–177.

[16] T. Maruta, Griesmer bound for linear codes over finite fields, `http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer/`.

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