Construction of new Griesmer codes of dimension 5

Construction of new Griesmer codes of dimension 5

Yuto Inoue, Tatsuya Maruta [1]

Department of Mathematical Sciences, Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

Keywords: linear codes, divisible codes, projective dual, projective geometry

Abstract. We construct Griesmer $[n, 5, d]_q$ codes for $2q^4 - 3q^3 + 1 \leq d \leq 2q^4 - 3q^3 + q^2$ and for $3q^4 - 5q^3 + q^2 + 1 \leq d \leq 3q^4 - 5q^3 + 2q^2$ for every $q \geq 3$ using some geometric methods such as projective dual and geometric puncturing.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements. The *weight* of a vector $\boldsymbol{x} \in \mathbb{F}_q^n$, denoted by $wt(\boldsymbol{x})$, is the number of nonzero coordinate positions in $\boldsymbol{x}$. An $[n, k, d]_q$ code $\mathcal{C}$ is a k dimensional subspace of $\mathbb{F}_q^n$ with minimum weight $d = \min\{wt(\boldsymbol{c}) > 0 \mid \boldsymbol{c} \in \mathcal{C}\}$ over $\mathbb{F}_q$. The weight distribution of $\mathcal{C}$ is the list of numbers A_i which is the number of codewords of $\mathcal{C}$ 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 for given q, k, d, see [5, 6]. The Griesmer bound is a well-known lower bound on the length n:

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

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. $\mathcal{C}$ is called *Griesmer* if it attains the Griesmer bound, i.e., $n = g_q(k, d)$. The values of $n_q(k, d)$ are determined for all d only for some small values of q and k [4, 14]. For the case $k = 5$, it is known that $n_q(5, d) = g_q(5, d)$ for $q^4 - 2q^2 + 1 \leq d \leq q^4$, $2q^4 - 2q^3 - q^2 + 1 \leq d \leq 2q^4 + q^2 - q$ and $d \geq 3q^4 - 4q^3 + 1$ for all q [9, 12], see also [3]. The main aim of this paper is to construct new Griesmer codes of dimension 5, which are already known for $q \leq 4$ but not for $q \geq 5$, as follows.

Theorem 1.1. *There exist $[g_q(5, d), 5, d]_q$ codes for $2q^4 - 3q^3 + 1 \leq d \leq 2q^4 - 3q^3 + q^2$ for all q.*

Theorem 1.2. *There exist $[g_q(5, d), 5, d]_q$ codes for $3q^4 - 5q^3 + q^2 + 1 \leq d \leq 3q^4 - 5q^3 + 2q^2$ for all q.*

Corollary 1.3. *$n_q(5, d) = g_q(5, d)$ for $2q^4 - 3q^3 + 1 \leq d \leq 2q^4 - 3q^3 + q^2$ for all q.*

Corollary 1.4. *$n_q(5, d) = g_q(5, d)$ for $3q^4 - 5q^3 + q^2 + 1 \leq d \leq 3q^4 - 5q^3 + 2q^2$ for all q.*

[1] Corresponding author.

E-mail addresses: syb01016@edu.osakafu-u.ac.jp (Y. Inoue), maruta@mi.s.osakafu-u.ac.jp (T. Maruta)

2 Construction methods through projective geometry

We denote by $\mathrm{PG}(r,q)$ the projective geometry of dimension r over $\mathbb{F}_q$. The 0-flats, 1-flats, 2-flats, 3-flats and $(r-1)$-flats are called *points, lines, planes, solids* 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. Then, 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 by $\mathcal{M}_{\mathcal{C}}$. We see linear codes from this geometrical point of view. An *i-point* is a point of Σ which has multiplicity i in $\mathcal{M}_{\mathcal{C}}$. Denote by γ_0 the maximum multiplicity of a point from Σ in $\mathcal{M}_{\mathcal{C}}$. Let C_i be the set of i-points in Σ, $0 \le i \le \gamma_0$, and let $\lambda_i = |C_i|$, where $|C_i|$ denotes the number of elements in a set C_i. For any subset S of Σ, *the multiplicity of S*, denoted by $m_{\mathcal{C}}(S)$, is defined as $m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|$. 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. A hyperplane H with $t = m_{\mathcal{C}}(H)$ is called a *t-hyperplane*. A *t-line*, a *t-plane* and *t-solid* are defined similarly. Denote by a_i the number of i-hyperplanes in Σ. The list of the values a_i is called the *spectrum* of $\mathcal{C}$, which can be calculated from the weight distribution by $a_i = A_{n-i}/(q-1)$ for $0 \le i \le n-d$. An $[n,k,d]_q$ code is called *m-divisible* if all codewords have weights divisible by an integer $m > 1$.

Lemma 2.1 ([16]). *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 $\lambda_0 > 0$ and

$$\bigcap_{H \in \mathcal{F}_{k-2},\ m_{\mathcal{C}}(H) < n-d} H = \emptyset.$$

Then there exists a t-divisible $[n^*,k,d^*]_q$ code $\mathcal{C}^*$ with $t = q^{k-2}/m$, $n^* = \sum_{j=0}^{w-1} j\alpha_j = ntq - \frac{d}{m}\theta_{k-1}$, $d^* = ((n-d)q - n)t$ whose spectrum is

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

The condition "$\bigcap_{H \in \mathcal{F}_{k-2},\ m_{\mathcal{C}}(H) < n-d} H = \emptyset$" is needed to guarantee that $\mathcal{C}^*$ has dimension k although it was missing in Lemma 5.1 of [16]. Note that a generator matrix for $\mathcal{C}^*$ is given by considering $(n-d-jm)$-hyperplanes as j-points in the dual space Σ^* of Σ for $0 \le j \le w-1$ [16]. $\mathcal{C}^*$ is called a *projective dual* of $\mathcal{C}$, see also [2] and [6].

Lemma 2.2 ([13, 15]). *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 $\cup_{i\ge 1} C_i$ contains a t-flat Δ and if $d > q^t$, then there exists an $[n-\theta_t, k, d']_q$ code $\mathcal{C}'$ with $d' \ge d - q^t$.*

The code $\mathcal{C}'$ in Lemma 2.2 can be constructed from $\mathcal{C}$ by removing the t-flat Δ from the multiset $\mathcal{M}_{\mathcal{C}}$. In general, the method for constructing new codes from a given $[n,k,d]_q$ code by deleting the coordinates corresponding to some geometric object in $\mathrm{PG}(k-1,q)$ is called *geometric puncturing* [13].

3 Proof of Theorems

A set S of s points in $\mathrm{PG}(r,q)$, $r \geq 2$, is called an *s-arc* if no $r+1$ points are on the same hyperplane, see [7] and [8] for arcs. When $q \geq r$, one can take a normal rational curve as a $(q+1)$-arc, see Theorem 27.5.1 in [8]. We first assume $k \geq 4$ and $q \geq k-2$. Let H be a hyperplane of $\Sigma = \mathrm{PG}(k-1,q)$. Take a $(q+1)$-arc $K = \{P_0, P_1, \ldots, P_q\}$ in H and a line $l_0 = \{P_0, Q_1, \ldots, Q_q\}$ of Σ not contained in H meeting H at the point P_0. Let l_i be the line joining P_i and Q_i for $1 \leq i \leq q$. Setting $C_1 = (\cup_{i=1}^q l_i) \setminus l_0$, $C_{q-1} = \{P_0\}$, $C_0 = \Sigma \setminus (C_1 \cup C_{q-1})$, we get the following.

Lemma 3.1. *For $k \geq 4$, $q \geq k-2$, a q-divisible $[q^2+q-1, k, q^2-(k-3)q]_q$ code exists.*

From now on, let $k=5$ and take a normal rational curve as K with

$$P_0(1,0,0,0,0),\ P_i(1,\alpha^i,\alpha^{2i},\alpha^{3i},0),\ P_q(0,0,0,1,0)$$

in $H = [0,0,0,0,1]$ and the line l_0 with

$$Q_i(1,0,0,0,\alpha^i) \text{ for } 1 \leq i \leq q-1,\ Q_q(0,0,0,0,1),$$

where $[a_0, a_1, \ldots, a_4]$ stands for the hyperplane in $\mathrm{PG}(4,q)$ defined by the equation $a_0x_0 + a_1x_1 + \cdots + a_4x_4 = 0$ and α is a primitive element of $\mathbb{F}_q$. Let H_{ij} be the solid containing l_i and l_j for $1 \leq i < j \leq q$. Take the point $Q(0,1,0,0,1)$ and the plane $\delta_0 = \langle l_0, Q\rangle$, where $\langle \chi_1, \chi_2, \cdots \rangle$ denotes the smallest flat containing $\chi_1, \chi_2, \cdots$. For any point $P(a,b,0,0,c) \in \delta_0$, the solid $H_{iq} = [0, -\alpha^i, 1, 0, 0]$ contains P if and only if $b = 0$, i.e., $P \in l_0$ for $1 \leq i \leq q-1$. Similarly, the solid $H_{ij} = [0, \alpha^{i+j}, -\alpha^i - \alpha^j, 1, 0]$ contains P if and only if $P \in l_0$ for $1 \leq i < j \leq q-1$. Thus, $H_{ij} \cap \delta_0 = l_0$ for $1 \leq i < j \leq q$, and no $(3q-1)$-solid contains Q. Hence, adding Q as a q-point, we get a q-divisible $[q^2+2q-1, 5, q^2-q]_q$ code, say $\mathcal{C}_1$. The spectrum of $\mathcal{C}_1$ can be derived as follows. The $(3q-1)$-solids consist of the $\binom{q}{2}$ solids H_{ij}, $1 \leq i < j \leq q$, the q solids $\langle \delta_0, l_i \rangle$, $1 \leq i \leq q$, the q^2 solids through one of the planes $\langle Q, l_i \rangle$ other than $\langle \delta_0, l_i \rangle$, $1 \leq i \leq q$, and the q^2 solids through the line $\langle Q, P_0 \rangle$ not containing δ_0. Hence $a_{3q-1} = \binom{q}{2} + 2q^2 + q$. From two equalities $a_{q-1} + a_{2q-1} + a_{3q-1} = \theta_4$ and $2a_{q-1} + a_{2q-1} = 2q^4 - q^3 + 1$, we get the spectrum of $\mathcal{C}_1$ as follows.

Lemma 3.2. *There exists a q-divisible $[q^2+2q-1, 5, q^2-q]_q$ code $\mathcal{C}_1$ with spectrum*

$$(a_{q-1}, a_{2q-1}, a_{3q-1}) = (\binom{q}{2} + q^4 - 2q^3 + q^2, 3q^3 - 3q^2 + q + 1, \binom{q}{2} + 2q^2 + q).$$

For a geometrical object S in Σ, we denote by S^* the corresponding object in the dual space Σ^* of Σ. Considering the $(q-1)$-solids, $(2q-1)$-solids and $(3q-1)$-solids in Σ as 2-points, 1-points and 0-points in Σ^* respectively, we get the following q^2-divisible code $\mathcal{C}_1^*$ as a projective dual of $\mathcal{C}_1$.

Lemma 3.3. *There exists a q^2-divisible $[2q^4 - q^3 + 1, 5, 2q^4 - 3q^3 + q^2]_q$ code $\mathcal{C}_1^*$.*

Lemma 3.4. *The multiset $\mathcal{M}_{\mathcal{C}_1^*}$ contains $q-1$ skew lines.*

Proof. Recall that the 0-points for $\mathcal{C}_1^*$ are the $(3q-1)$-solids for $\mathcal{C}_1$. Since l_0 is contained in H_{ij} and δ_0 in Σ, the plane l_0^* contains exactly $\binom{q}{2}+q$ 0-points in Σ^* corresponding to the solids H_{ij}, $1 \le i < j \le q$, and the solids $\langle \delta_0, l_i \rangle$, $1 \le i \le q$. Hence the number of i-points with $i \ge 1$ on l_0^* is $\theta_2 - \binom{q}{2} - q \ge q-1$. On the other hand, the plane l_0^* is contained in the solids P_0^* and $Q_1^*, \dots, Q_q^*$ in Σ^*, and the 0-points in Σ^* corresponding to the q^2 solids through the line $\langle Q, P_0 \rangle$ not containing δ_0 in Σ are contained in P_0^*. Since the set of 0-points in Σ^* corresponding to the q^2 solids through one of the planes $\langle Q, l_i \rangle$ other than $\langle \delta_0, l_i \rangle$, $1 \le i \le q$, in Σ meets Q_i^* in a line on the plane l_i^*, one can take $q-1$ skew lines in the solid Q_1^* containing no 0-point in Σ^*. □

Next, we construct another q-divisible code from the first assumption: H is a hyperplane of $\Sigma = \mathrm{PG}(k-1,q)$ with $k \ge 4$, $q \ge k-2$, $K = \{P_0, P_1, \dots, P_q\}$ is a $(q+1)$-arc in H, $l_0 = \{P_0, Q_1, \dots, Q_q\}$ is a line of Σ not contained in H meeting H at the point P_0, and $l_i = \langle P_i, Q_i \rangle$, $1 \le i \le q$. Setting $C_1 = (\cup_{i=1}^{q-1} l_i) \setminus l_0$, $C_{q-1} = \{P_0, Q_q\}$, $C_q = \{P_q\}$,$C_0 = \Sigma \setminus (C_1 \cup C_{q-1} \cup C_q)$, we get the following.

Lemma 3.5. *For $k \ge 4$, $q \ge k-2$, a q-divisible $[q^2+2q-2, k, q^2-(k-3)q]_q$ code exists.*

Let $k=5$ again and take the $(q+1)$-arc and the line l_0 as for $\mathcal{C}_1$. Similarly to the situation for constructing $\mathcal{C}_1$, no $(4q-2)$-solid contains δ_0. Hence, we get a q-divisible $[q^2+3q-2, 5, q^2-q]_q$ code by adding Q as a q-point, say $\mathcal{C}_2$. The $(4q-2)$-solids consist of the $\binom{q}{2}$ solids H_{ij}, $1 \le i < j \le q$, the q solids $\langle \delta_0, l_i \rangle$, $1 \le i \le q$, the $q-1$ solids $\langle P_q, Q, l_i \rangle$ with $1 \le i \le q-1$, the q solids through the plane $\langle Q, l_q \rangle$ not containing l_0, and the q solids through the plane $\langle Q, P_0, P_q \rangle$ not containing l_0. Hence $a_{4q-2} = \binom{q}{2} + 4q - 1$. The $(3q-2)$-solids consist of the q solids through the plane $\langle l_0, l_i \rangle$ not containing Q and any other $l_j \ne l_i$ for $1 \le i \le q$, the solid through δ_0 not containing l_i, $1 \le i \le q$, the q^2-q solids through the line $\langle P_0, P_q \rangle$ not containing Q and Q_q, the q^2-q solids through the line $\langle P_0, Q \rangle$ not containing l_0 and P_q, the q^2-q solids through the line l_q not containing Q and P_0, the q^2-q solids through the line $\langle Q, Q_q \rangle$ not containing l_0 and P_q, the $(q-1)^2$ solids through the plane $\langle P_q, l_i \rangle$ not containing Q and Q_q, $1 \le i \le q-1$, the $(q-1)^2$ solids through the plane $\langle Q, l_i \rangle$ not containing l_0 and P_q, $1 \le i \le q-1$, and the $(q-1)^2$ solids through the plane $\langle Q, P_q, Q_i \rangle$ not containing l_0 and l_i, $1 \le i \le q-1$. Hence $a_{3q-2} = 7q^2 - 9q + 4$. From two equalities $a_{q-2} + a_{2q-2} + a_{3q-2} + a_{4q-2} = \theta_4$ and $3a_{q-2} + 2a_{2q-2} + a_{3q-2} = 3q^4 - 2q^3 + 1$, we get the following.

Lemma 3.6. *There exists a q-divisible $[q^2+3q-2, 5, q^2-q]_q$ code $\mathcal{C}_2$ with spectrum*

$$(a_{q-2}, a_{2q-2}, a_{3q-2}, a_{4q-2}) = (q^4 - 4q^3 + 6q^2 - 4q + 1,$$
$$5q^3 - 12q^2 + 10q - 3 - \binom{q}{2}, 7q^2 - 9q + 4, \binom{q}{2} + 4q - 1).$$

Considering the $((4-j)q-2)$-solids in Σ as j-points in Σ^* for $j = 0,1,2,3$, we get the following q^2-divisible code $\mathcal{C}_2^*$ as a projective dual of $\mathcal{C}_2$.

Lemma 3.7. *There exists a q^2-divisible $[3q^4 - 2q^3 + 1, 5, 3q^4 - 5q^3 + 2q^2]_q$ code $\mathcal{C}_2^*$.*

Lemma 3.8. *The multiset $\mathcal{M}_{\mathcal{C}_2^*}$ contains $q-1$ skew lines.*

Proof. Note that the 0-points for $\mathcal{C}_2^*$ are the $(4q-2)$-solids for $\mathcal{C}_2$. From the same argument with that in the proof of Lemma 3.4, the plane l_0^* contains exactly $\binom{q}{2}+q$ 0-points in Σ^*, and the number of i-points with $i \geq 1$ on l_0^* is $\theta_2 - \binom{q}{2} - q \geq q-1$. Recall that the plane l_0^* is contained in the solids P_0^* and $Q_1^*, \ldots, Q_q^*$ in Σ^*. The 0-points in Σ^* corresponding to the q solids through the plane $\langle Q, P_0, P_q \rangle$ not containing l_0 in Σ are contained in P_0^*, and the 0-points in Σ^* corresponding to the q solids through the plane $\langle Q, l_q \rangle$ not containing l_0 in Σ are contained in Q_q^*. Since the set of 0-points in Σ^* corresponding to the $q-1$ solids $\langle P_q, Q, l_i \rangle$ with $1 \leq i \leq q-1$ in Σ meets Q_i^* in a point on the plane l_i^*, one can take $q-1$ skew lines in the solid Q_1^* containing no 0-point in Σ^*. $\square$

It follows from Lemmas 3.4 and 3.8 that applying Lemma 2.2 repeatedly (for $t=1$), starting with the code $\mathcal{C}_1^*$ or $\mathcal{C}_2^*$, we get the following.

Lemma 3.9. *There exist* $[2q^4-q^3+1-s(q+1), 5, 2q^4-3q^3+q^2-sq]_q$ *codes for* $1 \leq s \leq q-1$.

Lemma 3.10. *There exist* $[3q^4-2q^3+1-s(q+1), 5, 3q^4-5q^3+2q^2-sq]_q$ *codes for* $1 \leq s \leq q-1$.

Lemmas 3.9 and 3.10 provide the codes needed in Theorems 1.1 and 1.2 respectively, when d is divisible by q. The rest of the codes required for the theorem can be obtained by puncturing these divisible codes.

Remark 1. As the projective duals of the q-divisible codes in Lemmas 3.1 and 3.5, one can obtain q^{k-3}-divisible Griesmer codes of dimension k with minimum weights $d = (k-3)q^{k-1} - 2q^{k-2} + q^{k-3}$ and $(k-2)q^{k-1} - 4q^{k-2} + 2q^{k-3}$. Griesmer codes with the same parameters are known to exist, see [1], [11] for $k=4$ and [10] for $k \geq 5$.

Acknowledgments

The research of the second author is partially supported by JSPS KAKENHI Grant Number JP16K05256.

References

[1] N. Bono, T. Maruta, Some new 4-dimensional linear codes, in: Proc. 8th Intern. Workshop on Optimal Codes and Related Topics, Sofia, Bulgaria, 2017, pp. 37–42.

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

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

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

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

[6] 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.

[7] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Second edition, Clarendon Press, Oxford, 1998.

[8] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Clarendon Press, Oxford, 1991.

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

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

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

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

[13] T. Maruta, Construction of optimal linear codes by geometric puncturing, Serdica J. Computing **7** (2013) 73–80.

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

[15] T. Maruta, Y. Oya, On optimal ternary linear codes of dimension 6, Adv. Math. Commun. **5** (2011) 505–520.

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