Discrete Mathematics 341 (2018) 2676–2685

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Nonexistence of some linear codes over the field of order four

Hitoshi Kanda, Tatsuya Maruta *

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

ARTICLE INFO

Article history:
Received 15 November 2017
Received in revised form 12 April 2018
Accepted 14 June 2018
Available online 14 July 2018

Keywords:
Optimal linear code
Griesmer bound
Geometric method

ABSTRACT

We consider the problem of determining $n_4(5, d)$, the smallest possible length n for which an $[n, 5, d]_4$ code of minimum distance d over the field of order 4 exists. We prove the nonexistence of $[g_4(5, d) + 1, 5, d]_4$ codes for $d = 31, 47, 48, 59, 60, 61, 62$ and the nonexistence of a $[g_4(5, d), 5, d]_4$ code for $d = 138$ using the geometric method through projective geometries, where $g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. This yields to determine the exact values of $n_4(5, d)$ for these values of d. We also give the updated table for $n_4(5, d)$ for all d except some known cases.

1. Introduction

We denote by $\mathbb{F}_q^n$ the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements. An $[n, k, d]_q$ *code* $\mathcal{C}$ is a linear code of length n, dimension k and minimum Hamming weight d over $\mathbb{F}_q$. 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 $\boldsymbol{x}$. 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. We only consider *non-degenerate* codes having no coordinate which is identically zero. 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. This problem is sometimes called the optimal linear codes problem, see [5,6]. A well-known lower bound on $n_q(k, d)$, called the Griesmer bound, says:

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

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. The values of $n_q(k, d)$ are determined for all d only for some small values of q and k. The optimal linear codes problem for $q = 4$ is solved for $k \leq 4$ for all d, see [8,15].

Theorem 1.1. *$n_4(4, d) = g_4(4, d) + 1$ for $d = 3, 4, 7, 8, 13–16, 23–32, 37–44, 77–80$ and $n_4(4, d) = g_4(4, d)$ for any other d.*

As for the case $k = 5$, the value of $n_4(5, d)$ is unknown for 107 values of d, and the remaining cases look quite difficult because the only progress after the computer-aided research [1] was the nonexistence of Griesmer codes for $d = 287, 288$ [9], see also [15]. It is known that $n_4(5, d)$ is equal to $g_4(5, d)+1$ or $g_4(5, d)+2$ for $d = 31, 47, 48, 59, 60, 61, 62$ and that $n_4(5, d)$ is equal to $g_4(5, d)$ or $g_4(5, d) + 1$ for $d = 138$. Our purpose is to prove the following theorems to determine $n_4(5, d)$ for these values of d.

Theorem 1.2. *There exists no $[g_4(5, d) + 1, 5, d]_4$ code for $d = 31, 47, 48, 59, 60, 61, 62$.*

Theorem 1.3. *There exists no $[g_4(5, d), 5, d]_4$ code for $d = 138$.*

* Corresponding author.
E-mail addresses: jinza80kirisame@gmail.com (H. Kanda), maruta@mi.s.osakafu-u.ac.jp (T. Maruta).

https://doi.org/10.1016/j.disc.2018.06.024

We note that our proofs would heavily depend on the extension theorems which are valid only for linear codes over $\mathbb{F}_4$. So, generalizing the nonexistence results to $q \geq 5$ seems hopeless. The above theorems determine $n_4(5, d)$ for some d as follows.

Corollary 1.4. *$n_4(5, d) = g_4(5, d) + 2$ for $d = 31, 47, 48, 59, 60, 61, 62$.*

Corollary 1.5. *$n_4(5, d) = g_4(5, d) + 1$ for $d = 138$.*

For $k \geq 6$, we get the following by shortening since $g_q(k, d) = g_q(5, d) + k - 5$ for $k \geq 6$ if $d \leq q^5$.

Corollary 1.6. *$n_4(k, d) \geq g_4(k, d) + 2$ for $d = 31, 47, 48, 59, 60, 61, 62$ for $k \geq 6$.*

Corollary 1.7. *$n_4(k, d) \geq g_4(k, d) + 1$ for $d = 138$ for $k \geq 6$.*

We also give the updated table for $n_4(5, d)$ as Table 2. We give the values and bounds of $g = g_4(5, d)$ and $n = n_4(5, d)$ for all d except for $249 \leq d \leq 256$ and for $d \geq 369$ which are the cases satisfying $n_4(5, d) = g_4(5, d)$. Entries in boldface are given in this paper.

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 results. 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 of $\mathcal{C}$ can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1, q)$, denoted by $\mathcal{M}_\mathcal{C}$. 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 $\mathcal{M}_\mathcal{C}$ 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 $\mathcal{M}_\mathcal{C}$*, 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

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

where $\mathcal{F}_j$ denotes the set of j-flats of Σ. 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

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

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 [13]) that

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

Let θ_j be the number of points in a j-flat, i.e., $\theta_j = (q^{j+1} - 1)/(q - 1)$. An $[n, k, d]_q$ code, which is not necessarily Griesmer, satisfies the following:

$$\gamma_j \leq \gamma_{j+1} - \frac{n - \gamma_{j+1}}{\theta_{k-2-j} - 1}, \tag{2.3}$$

see [8]. We denote by λ_s the number of s-points in Σ. When $\gamma_0 = 2$, we have

$$\lambda_2 = \lambda_0 + n - \theta_{k-1}. \tag{2.4}$$

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 of Σ to distinguish from the spectrum of $\mathcal{C}$. Simple counting arguments yield the following.

Lemma 2.1 (*[10]*). (a) $\sum_{i=0}^{n-d} a_i = \theta_{k-1}$. (b) $\sum_{i=1}^{n-d} i a_i = n\theta_{k-2}$.
(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:

$$\sum_{i=0}^{n-d-2} \binom{n-d-i}{2} a_i = \binom{n-d}{2} \theta_{k-1} - n(n-d-1)\theta_{k-2} + \binom{n}{2} \theta_{k-3} + q^{k-2}\lambda_2. \tag{2.5}$$