Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

Note

A new class of optimal linear codes with flexible parameters[☆]

Gaojun Luo[a], Xiwang Cao[a,b,*], Guangkui Xu[c], Shanding Xu[a]

[a] School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[b] State Key Laboratory of Information Security Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[c] Department of Mathematics, Huainan Normal University, Huainan 232038, China

ARTICLE INFO

Article history:
Received 29 June 2017
Received in revised form 7 November 2017
Accepted 15 November 2017
Available online xxxx

Keywords:
Linear code
Griesmer bound
Two-weight code

ABSTRACT

In this paper, we construct a class of linear codes over the local ring $R = \mathbb{F}_q + u\mathbb{F}_q$ and determine the Lee distribution by employing character sums. Using the Gray map, we obtain a class of linear codes with two weights over $\mathbb{F}_q$. These linear codes are proved to be optimal with respect to the Griesmer bound. Notably, the parameters of these linear codes are flexible and new. As an application, we employ these linear codes to construct association schemes.

1. Introduction

Linear codes have wide utilization in association schemes, authentication codes, data storage systems and some other fields. In particular, linear codes with two weights are closely related to strongly regular graphs, partial difference sets and finite geometry [2]. The construction of linear codes is a hot topic in coding theory. During the past decade, a great deal of effort has been devoted to the study of linear codes [5,6,9–12,19]. Let q be a power of a prime p and $\mathbb{F}_q$ the finite field with q elements. A q-ary $[n, k, d]$ linear code is a k-dimensional linear subspace of the vector space $\mathbb{F}_q^n$ with minimum Hamming distance d. Denote by A_i the number of codewords with weight i in a linear code $\mathcal{C}$ of length n. Then the weight enumerator of $\mathcal{C}$ is defined by the polynomial $A_0 + A_1x + A_2x^2 + \cdots + A_nx^n$. The coefficient A_i $(0 \le i \le n)$ of this polynomial is called the weight distribution of the code $\mathcal{C}$. Obviously, we can obtain the minimum distance of the code $\mathcal{C}$ from its weight distribution. We call $\mathcal{C}$ a t-weight linear code if the number of nonzero A_i in the sequence $(A_1, A_2, \ldots, A_n)$ is equal to t.

For an $[n, k, d]$ code $\mathcal{C}$, there exists some trade-offs among these parameters of $\mathcal{C}$ such as the Sphere Packing bound, the Singleton bound and so on. It is desirable to construct a linear code achieving one bound. Next, we introduce an upper bound which generalizes the Singleton Bound known as the Griesmer Bound. Remarkably, it is only applicable to linear codes. Let us recall it in the following lemma [7].

Lemma 1.1 ([7] Griesmer Bound). *For any $[n, k, d]$ linear code over $\mathbb{F}_q$, we have*

$$n \ge \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil \cdot \rceil$ is the ceiling function.

☆ This work was supported by the National Natural Science Foundation of China (Grant Nos. 11371011, 11771007, 61572027 and 11601177), the Funding for Outstanding Doctoral Dissertation in NUAA (Grant No. BCXJ16-08), Anhui Provincial Natural Science Foundation (1608085QA05), the Foundation for Distinguished Young Talents in Higher Education of Anhui Province of China (gxyqZD2016258).

* Corresponding author at: School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China.
E-mail addresses: gjluo1990@nuaa.edu.cn (G. Luo), xwcao@nuaa.edu.cn (X. Cao).

https://doi.org/10.1016/j.dam.2017.11.020

An $[n, k, d]$ linear code $\mathcal{C}$ is optimal if the parameters n, k and d achieve this bound with equality [7] and $\mathcal{C}$ is called distance-optimal if there is no $[n, k, d+1]$ code [8]. For simplicity, we call such a code optimal.

In [5,6], Ding et al. proposed a generic construction of linear codes over $\mathbb{F}_q$. Inspired by this idea, one can construct linear codes over finite rings as follows. Let $R = \mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = 0$. It is easy to check that R is a local ring with the maximal ideal (u). Let m be a positive integer and $\mathcal{R} = \mathbb{F}_{q^m} + u\mathbb{F}_{q^m}$ with $u^2 = 0$ an extension ring of R. Denote by $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$. A linear code over R with a defining set $K \subseteq \mathcal{R}^*$ is given by

$$\mathcal{C}_K = \{(\mathrm{Tr}(ak))_{k\in K} : a \in \mathcal{R}\}, \tag{1}$$

where $\mathrm{Tr}(\cdot)$ is the trace function from $\mathcal{R}$ to R (see Section 2) and $\mathcal{R}^* = \mathbb{F}_{q^m}^* + u\mathbb{F}_{q^m}$ is the group of units of $\mathcal{R}$. Clearly, $\mathcal{C}_K$ can be viewed as an R^n-module. Proceeding as in the proof of Theorem 6 in [6], the rank of $\mathcal{C}_K$ is equal to that of the R-module spanned by K. Using the Gray map on $\mathcal{C}_K$, we can obtain a corresponding linear code over $\mathbb{F}_q$ from $\mathcal{C}_K$. Employing this technique, Shi et al. [16–18] and Liu et al. [14] got some optimal linear codes with few weights.

The main purpose of this paper is to construct a class of linear codes over R by the approach mentioned above. By the Gray map, we can obtain a class of linear codes over $\mathbb{F}_q$ and these linear codes are optimal with respect to the Griesmer bound. Notably, to our best knowledge, the parameters of these optimal linear codes are new.

An outline of this paper is as follows. In Section 2, we introduce some basic definitions. In Section 3, we present our main results. In Section 4, we use the linear codes obtained to construct association schemes. In Section 5, we make a conclusion.

2. Preliminaries

In this section, we present some notations and definitions on rings and characters over the finite fields, which will be needed in our discussion.

Let m be a positive integer and $r = q^m$. The trace function from $\mathbb{F}_r$ to $\mathbb{F}_q$ is

$$\mathrm{tr}_{r/q}(x) = x + x^q + \cdots + x^{q^{m-1}},$$

where $x \in \mathbb{F}_r$.

For each $a \in \mathbb{F}_r$, we define the additive character of $\mathbb{F}_r$ by the function $\chi_a(x) = e^{2\pi\sqrt{-1}\mathrm{tr}_{r/p}(ax)/p}$. When $a = 1$, $\chi_1(x)$ is the canonical additive character of $\mathbb{F}_r$. Throughout this paper, we write the canonical additive character of $\mathbb{F}_r$ and $\mathbb{F}_q$ simply as χ and μ, respectively.

Note that $R = \mathbb{F}_q + u\mathbb{F}_q$ and its extension ring $\mathcal{R} = \mathbb{F}_r + u\mathbb{F}_r$, where $u^2 = 0$. There exists a Frobenius transformation f mapping $a+ub$ to a^q+ub^q for every $a, b \in \mathbb{F}_r$. Then the trace function from $\mathcal{R}$ to R is defined by $\mathrm{Tr}(a+ub) = \sum_{i=0}^{m-1} f^i(a+ub)$. It is simple to show that $\mathrm{Tr}(a+ub) = \mathrm{tr}_{r/q}(a) + u\mathrm{tr}_{r/q}(b)$.

Define the Gray map φ from R to $\mathbb{F}_q^2$ by $\varphi(x+uy) = (y, x+y)$, where $x, y \in \mathbb{F}_q$. It is a bijection and it can extend naturally to a map from R^n to $\mathbb{F}_q^{2n}$. Let $\mathcal{C}$ be a linear code of length n over R and $\mathbf{c} = X + uY$ a codeword of $\mathcal{C}$, where $X, Y \in \mathbb{F}_q^n$. Denote by $w_H(X)$ the Hamming weight of X. Then the Lee weight of $\mathbf{c}$ is defined as

$$w_L(\mathbf{c}) = w_H(Y) + w_H(X+Y).$$

Denote the number of codewords with Lee weight i in $\mathcal{C}$ by L_i. Then the Lee weight enumerator is given by the polynomial $1 + L_1 z + L_2 z^2 + \cdots + L_{2n} z^{2n}$. The coefficient L_i $(0 < i \le 2n)$ of this polynomial is called the Lee weight distribution of the code $\mathcal{C}$.

For a codeword $\mathbf{c}$ of $\mathcal{C}$, in order to determine the Lee weight of $\mathbf{c}$, we should compute its corresponding Hamming weight after Gray mapping. The following lemma provides a method to determine the Hamming weight of a given vector. Using the same method as in [15, p. 411–412], we can carry out the proof of this lemma.

Lemma 2.1. *Let n be a positive integer. For $Z = (z_1, z_2, \ldots, z_n) \in \mathbb{F}_q^n$, we have*

$$\sum_{x\in\mathbb{F}_q^*} \Psi(xZ) = (q-1)n - q w_H(Z),$$

where $\Psi(xZ) = \sum_{i=1}^{N} \mu(xz_i)$.

3. Main results

In this section, we firstly construct a class of linear codes defined by (1) and present its Lee weight distribution. Throughout this section, we set $r = q^m$, where q is a power of a prime p and m is a positive integer.

Theorem 3.1. *Let D_l be an l-subset of $\mathbb{F}_q^*$, where $0 < l < q$. Assume that $K = D_l + u\mathbb{F}_r$ with $u^2 = 0$. Then $\mathcal{C}_K$ defined by (1) is a linear code of length lr over $\mathbb{F}_q + u\mathbb{F}_q$ and the Lee weight distribution is listed in Table 1.*

Please cite this article in press as: G. Luo, et al., A new class of optimal linear codes with flexible parameters, Discrete Applied Mathematics (2017), https://doi.org/10.1016/j.dam.2017.11.020.