Finite Fields and Their Applications 38 (2016) 72–92

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Two classes of two-weight linear codes [☆]

Ziling Heng [a,b], Qin Yue [a,b,*]

[a] *Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, PR China*
[b] *State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, PR China*

ARTICLE INFO

Article history:
Received 28 May 2015
Received in revised form 26 October 2015
Accepted 5 December 2015
Available online 7 January 2016
Communicated by Jacques Wolfmann

MSC:
94B05
68R01

Keywords:
Gauss period
Secret sharing scheme
Linear code
Hamming weight

ABSTRACT

Two-weight linear codes have many wide applications in authentication codes, association schemes, strongly regular graphs, and secret sharing schemes. In this paper, we present two classes of two-weight binary or ternary linear codes. In some cases, they are optimal or almost optimal. They can also be used to construct secret sharing schemes.

[☆] The paper is supported by NNSF of China (No. 11171150); Fundamental Research Funds for the Central Universities (No. NZ2015102); Funding of Jiangsu Innovation Program for Graduate Education (the Fundamental Research Funds for the Central Universities; No. KYZZ15_0086); Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-15-009).

[*] Corresponding author.
E-mail addresses: zilingheng@163.com (Z. Heng), yueqin@nuaa.edu.cn (Q. Yue).

http://dx.doi.org/10.1016/j.ffa.2015.12.002
1071-5797/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Throughout this paper, let p be a prime and r a power of p. Let $\mathbb{F}_r$ denote the finite field with r elements. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d. We call an $[n, k, d]$ linear code *optimal* if its parameters meet a bound on linear codes and *almost optimal* if $[n, k, d + 1]$ meets a bound on linear codes. Let A_i be the number of codewords with Hamming weight i in a code $\mathcal{C}$. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1 x + \cdots + A_n x^n.$$

The sequence $(1, A_1, \cdots, A_n)$ is called the weight distribution of $\mathcal{C}$. We can estimate the error correcting capability and the probability of error detection from the weight distribution of a code. Weight distributions were widely studied in [7,14,15,17,19,21].

Let $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_r$. Let $\mathbf{T}_r$ denote the trace function from $\mathbb{F}_r$ onto $\mathbb{F}_p$ throughout this paper. We define a p-ary linear code of length n by

$$\mathcal{C}_D = \{(\mathbf{T}_r(xd_1), \mathbf{T}_r(xd_2), \cdots, \mathbf{T}_r(xd_n)) : x \in \mathbb{F}_r\}.$$

We call D the *defining set* of this code $\mathcal{C}_D$. Note that different orderings of the elements of D can produce different codes $\mathcal{C}_D$, but these linear codes are permutation equivalent and have the same weight distribution. Hence, we do not consider the ordering of the elements in D. This construction was first introduced by Ding and Niederreiter in [5]. And it is generic in the sense that many classes of known codes [3,5,8,12] with a few weights could be produced by selecting the defining set.

Two-weight linear codes are interesting in the area of coding theory and have been studied intensively [1,3,4,8,9]. Two-weight codes are also closely related to objects in different areas of mathematics such as strongly regular graphs, partial geometries, and projective point-sets. Delsarte [10] was the first to study the connections between two-weight codes, strongly regular graphs, and projective point-sets. A survey of this relationship was given later by Calderbank and Kantor [1]. Two-weight codes can also be used to construct secret sharing schemes.

In this paper, we obtain two classes of two-weight binary or ternary linear codes. Our constructions can produce two-weight codes with new parameters. In some cases, they are optimal or almost optimal. They can also be used to construct secret sharing schemes.

In this correspondence, we use the following notations unless otherwise stated.

p	prime number,
m	positive integer such that $\gcd(m, p) = 1$,
h	positive integer which is no less than 2,
k	the least integer such that $p^k \equiv -1 \pmod{h}$,
$\mathbf{T}_r$	trace function from $\mathbb{F}_r$ onto $\mathbb{F}_p$,
$\mathfrak{Re}(x)$	real part of x,
ζ_p	primitive p-th root of complex unity,