Finite Fields and Their Applications 54 (2018) 176–196

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Minimal linear codes over finite fields

Ziling Heng [a], Cunsheng Ding [b], Zhengchun Zhou [c,d,*]

[a] School of Science, Chang'an University, Xi'an 710064, China
[b] Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China
[c] School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China
[d] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China

ARTICLE INFO

Article history:
Received 27 March 2018
Received in revised form 9 August 2018
Accepted 10 August 2018
Available online xxxx
Communicated by Wang Qiang

MSC:
94C10
94B05
94A60

Keywords:
Linear code
Minimal code
Minimal vector
Secret sharing

ABSTRACT

As a special class of linear codes, minimal linear codes have important applications in secret sharing and secure two-party computation. Constructing minimal linear codes with new and desirable parameters has been an interesting research topic in coding theory and cryptography. Ashikhmin and Barg showed that $w_{\min}/w_{\max} > (q-1)/q$ is a sufficient condition for a linear code over the finite field GF(q) to be minimal, where q is a prime power, $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weights in the code, respectively. The first objective of this paper is to present a sufficient and necessary condition for linear codes over finite fields to be minimal. The second objective of this paper is to construct an infinite family of ternary minimal linear codes satisfying $w_{\min}/w_{\max} \leq 2/3$. To the best of our knowledge, this is the first infinite family of nonbinary minimal linear codes violating Ashikhmin and Barg's condition.

* Corresponding author at: School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China.
E-mail addresses: zilingheng@163.com (Z. Heng), cding@ust.hk (C. Ding), zzc@home.swjtu.edu.cn (Z. Zhou).

https://doi.org/10.1016/j.ffa.2018.08.010
1071-5797/

1. Introduction

Let q be a prime power and $\mathrm{GF}(q)$ denote the finite field with q elements. An $[n, k, d]$ code $\mathcal{C}$ over $\mathrm{GF}(q)$ is a k-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$. The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$.

The support of a vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathrm{GF}(q)^n$, denoted by $\mathrm{Suppt}(\mathbf{v})$, is defined by

$$\mathrm{Suppt}(\mathbf{v}) = \{1 \le i \le n : v_i \neq 0\}.$$

The vector $\mathbf{v}$ is called the characteristic vector or the incidence vector of the set $\mathrm{Suppt}(\mathbf{v})$. A vector $\mathbf{u} \in \mathrm{GF}(q)^n$ covers another vector $\mathbf{v} \in \mathrm{GF}(q)^n$ if $\mathrm{Suppt}(\mathbf{u})$ contains $\mathrm{Suppt}(\mathbf{v})$. We write $\mathbf{v} \preceq \mathbf{u}$ if $\mathbf{v}$ is covered by $\mathbf{u}$, and $\mathbf{v} \prec \mathbf{u}$ if $\mathrm{Suppt}(\mathbf{v})$ is a proper subset of $\mathrm{Suppt}(\mathbf{u})$. A codeword $\mathbf{u}$ in a linear code $\mathcal{C}$ is said to be *minimal* if $\mathbf{u}$ covers only the codeword $a\mathbf{u}$ for all $a \in \mathrm{GF}(q)$, but no other codewords in $\mathcal{C}$. A linear code $\mathcal{C}$ is said to be *minimal* if every codeword in $\mathcal{C}$ is minimal.

Minimal linear codes have interesting applications in secret sharing [4,15,16] and secure two-party computation [2,7], and could be decoded with a minimum distance decoding method [1]. Searching for minimal linear codes has been an interesting research topic in coding theory and cryptography. The following sufficient condition for a linear code to be minimal is due to Ashikhmin and Barg [1].

Lemma 1 *(Ashikhmin–Barg). A linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ is minimal if*

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q},$$

where $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero Hamming weights in the code $\mathcal{C}$, respectively.

With the help of Lemma 1, a number of families of minimal linear codes with $w_{\min}/w_{\max} > (q-1)/q$ have been reported in the literature (see, [4], [8], [10], [16], for example). Sporadic examples in [7] show that Ashikhmin–Barg's condition is not necessary for linear codes to be minimal. However, no infinite family of minimal linear codes with $w_{\min}/w_{\max} \le (q-1)/q$ was found until the breakthrough in [6], where an infinite family of such binary codes was discovered. Inspired by the work in [6], the authors of the present paper gave a further study of binary minimal linear codes [9]. Specifically, a necessary and sufficient condition for binary linear codes to be minimal was derived in [9]. With this new condition, three infinite families of minimal binary linear codes with $w_{\min}/w_{\max} \le 1/2$ were obtained from a general construction in [9].