CSIAM Trans. Appl. Math.
doi: 10.4208/csiam-am.SO-2021-0024

Vol. **4**, No. 1, pp. 1-12
March 2023

Improving the Gilbert-Varshamov Bound by Graph Spectral Method

Zicheng Ye[1,2], Huazi Zhang[3], Rong Li[3], Jun Wang[3], Guiying Yan[1,2,*] and Zhiming Ma[1,2]

[1] *Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China.*
[2] *University of Chinese Academy of Sciences, Beijing 100049, China.*
[3] *Hangzhou Research Center, Huawei Technologies Co., Ltd., Hangzhou 310052, Zhejiang Province, China.*

Received 6 April 2021; Accepted 9 February 2022

Abstract. We improve Gilbert-Varshamov bound by graph spectral method. Gilbert graph $G_{q,n,d}$ is a graph with all vectors in $\mathbb{F}_q^n$ as vertices where two vertices are adjacent if their Hamming distance is less than d. In this paper, we calculate the eigenvalues and eigenvectors of $G_{q,n,d}$ using the properties of Cayley graph. The improved bound is associated with the minimum eigenvalue of the graph. Finally we give an algorithm to calculate the bound and linear codes which satisfy the bound.

AMS subject classifications: 05C50, 05C69, 68P30

Key words: Gilbert–Varshamov bound, independence number, graph spectral method, Cayley graph, linear codes.

1 Introduction

Let q be a prime number and $\mathbb{F}_q$ be the finite field given by the integers mod q. $\mathbb{F}_q^n$ is the n-dimension vector space over $\mathbb{F}_q$. A subset C of $\mathbb{F}_q^n$ is called a q-ary code with length n. C is said to be linear if C is a subspace. The vectors in C are called codewords. The dimension of C is given by $k=\log_q|C|$, and the rate is given by k/n.

Let $c=(c_1,\ldots,c_n)$ be a vector in $\mathbb{F}_q^n$. The Hamming weight of c is $w(c)=|\{i\,|\,c_i\neq 0\}|$. The Hamming distance between two vectors $c,c'\in\mathbb{F}_q^n$ is $d(c,c')=|\{i\,|\,c_i\neq c_i'\}|$. C is called a code with minimum distance d if the distance of any two distinct codewords in C are

*Corresponding author. *Email addresses:* yezicheng@amss.ac.cn (Z. Ye), zhanghuazi@huawei.com (H. Zhang), lirongone.li@huawei.com (R. Li), wangjun@huawei.com (J. Wang), yangy@amss.ac.cn (G. Yan), mazm@amt.ac.cn (Z. Mang)

greater or equal to d. The relative distance of C is then given by d/n. A code in $\mathbb{F}_q^n$ with dimension k and minimum distance d is called an $[n,k,d]_q$ code.

Let $A_q(n,d)$ be the maximum number of codewords in a q-ary code with length n and minimum Hamming distance d. Finding the value of $A_q(n,d)$ is a very fundamental and difficult problem in coding theory [13]. The first and most important lower bound of $A_q(n,d)$ is Gilbert-Varshamov bound.

Proposition 1.1 (Gilbert-Varshamov Bound [6]). *Let*

$$V_q(n,d)=\sum_{i=0}^{d}\binom{n}{i}(q-1)^i$$

be the number of vectors with Hamming weight less than d, then

$$A_q(n,d)\geq\frac{q^n}{V_q(n,d-1)}. \tag{1.1}$$

Proposition 1.1 has been improved variously in [2, 4, 5, 8, 9, 11, 14, 16]. Among them, the best improvement on the order of magnitude is from Jiang and Vardy [9] by studying the independence number of the graph $G_{q,n,d}$ defined as follows:

Definition 1.1 ([9]). *Gilbert graph $G_{q,n,d}$ is a graph whose $V(G_{q,n,d})=\mathbb{F}_q^n$ and $\forall u,v\in V(G_{q,n,d})$, $(u,v)\in E(G_{q,n,d})$ if and only if $1\leq d(u,v)\leq d-1$.*

People are also interested to the asymptotic form of Gilbert-Varshamov bound as n goes to infinity. The maximum rate of code families with relative distance δ is defined as

$$\beta_q(\delta)=\lim_{n\to\infty}\frac{1}{n}A_q(n,n\delta).$$

Notice that

$$\frac{1}{n}\log_q V_q(n,d)=h_q\left(\frac{d}{n}\right)+o(1)$$

as $n\to\infty$ where

$$h_q(x)=x\log_q(q-1)-x\log_q x-(1-x)\log_q(1-x).$$

This implies the asymptotic form of Proposition 1.1.

Proposition 1.2 (Asymptotic Gilbert-Varshamov Bound [6]). *For every $0\leq\delta<1-1/q$,*

$$\beta_q(\delta)\geq 1-h_q(\delta). \tag{1.2}$$

Tsfasman *et al.* [15] have proved that $\beta_q(\delta)>1-h_q(\delta)$ for some $q\geq 49$. However, when $q=2$, some people conjecture that there does not exist any binary code with relative distance δ and rate $R>1-h_2(\delta)$ as $n\to\infty$ [9].