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].

In this paper, we improve Gilbert-Varshamov bound by analysing the spectrum of $G_{q,n,d}$ and bounding its independence number. In Section 2, we use properties of Cayley graph to calculate the closed form of the eigenvalues and eigenvectors of $G_{q,n,d}$, and get an upper bound and a lower bound using the minimum eigenvalue. The improvement of Gilbert-Varshamov bound is given in Section 3. Section 4 concludes the results and gives some open problems.

2 The spectrum of the Gilbert graph

A graph G is a set of N vertices $V(G)=\{v_1,\ldots,v_N\}$ and a set of edges $E(G)\subseteq V(G)\times V(G)$. For $v_i,v_j\in V(G)$, we say v_i and v_j are adjacent if $(v_i,v_j)\in E(G)$. The neighbourhood of $v\in V(G)$ is the set of all vertices adjacent to v and denoted by $N(v)$. The number of edges that are incident to v is the degree of v. A graph is called a D-regular graph if each vertex has degree D. The adjacent matrix for G is a $N\times N$ matrix A where A_{ij} is 1 if v_i and v_j are adjacent, and 0 otherwise.

A subset of V is called an independent set if none of vertices in the set are adjacent. The independence number of G is the size of the largest independent set in G and denoted by $\alpha(G)$.

The spectrum of a graph is the eigenvalues of its adjacent matrix, which has a strong relationship with the structure of the graph [3], including independence number we study in this paper.

It is clear that $G_{q,n,d}$ is a $(V_q(n,d-1)-1)$-regular graph. More exactly, $G_{q,n,d}$ is vertex-transitive [7, 12]. Then Gilbert-Varshamov bound is the direct consequence of following facts:

Proposition 2.1.

$$\alpha(G_{q,n,d})=A_q(n,d).$$

Lemma 2.1.

$$\alpha(G)\geq\frac{|V(G)|}{\Delta(G)+1},$$

where $\Delta(G)$ is the maximal degree of G.

Here, Proposition 2.1 is from that a q-ary code of length n has minimum distance d if and only if it is an independent set in $G_{q,n,d}$. Lemma 2.1 holds since if some vertex v is in an independent set I of graph G, it forbids at most $\Delta(G)+1$ vertices (including v itself) to be added into I.

Definition 2.1 ([7]). *A group $(H,\cdot)$ is a set H together with a binary operation $\cdot$ on $H\times H\to H$ such that the following properties hold:*

1. *For all $a,b,c\in G$, $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.*
2. *There exists an identity element $e\in H$ such that for every $a\in H$, $a\cdot e=e\cdot a=a$.*

3. For each $a\in H$, there exists a unique inverse element $a^{-1}\in H$ of a such that $a\cdot a^{-1}=a^{-1}\cdot a=e$.

Moreover, if a group $(H,\cdot)$ also satisfies $a\cdot b=b\cdot a$ for all $a,b\in H$, it is called an Abelian group.

Definition 2.2 ([1,3,7]). *Denote that content $(H,\cdot)$ is a finite group and $S\subseteq H$ satisfies $\{s^{-1}\,|\,s\in S\}=S$ and identity element $e\notin S$. The (finite and undirected) Cayley graph on H with difference set S is denoted as Γ with vertex set H and edge set $E=\{(x,y)\,|\,yx^{-1}\in S\}$.*

In this paper, we always assume H is an Abelian group.

Example 2.1. $(\mathbb{F}_q^n,+)$ is an Abelian group with

$$(u_1,u_2,\ldots,u_n)+(v_1,v_2,\ldots,v_n)=(u_1+v_1,u_2+v_2,\ldots,u_n+v_n),$$

where '+' is the addition operation of integers mod q. The identity element is $(0,0,\ldots,0)$ and the inverse element of $u=(u_1,u_2,\ldots,u_n)$ is $-u=(-u_1,-u_2,\ldots,-u_n)$.

Since $w(u)$=$w(-u)$, $G_{q,n,d}$ can be regarded as a Cayley graph on $H=\mathbb{F}_q^n$ with $S=\{u\in\mathbb{F}_q^n\,|\,1\leq w(u)\leq d-1\}$.

To compute the spectrum of a Cayley graph Γ, let us define a character of H to be a map $\chi:H\to\mathbb{C}^*$ satisfying $\chi(xy)=\chi(x)\chi(y)$, where $\mathbb{C}$ is the set of complex numbers and $\mathbb{C}^*=\mathbb{C}-\{0\}$. Then

$$\sum_{y\in N(x)}\chi(y)=\left(\sum_{s\in S}\chi(s)\right)\chi(x),$$

so the vector $(\chi(x))_{x\in H}$ is an eigenvector of the adjacency matrix of Γ with eigenvalue $\sum_{s\in S}\chi(s)$.

To calculate the closed form of the spectrum for $G_{q,n,d}$, we need to use Krawtchouk polynomials.

Definition 2.3 ([10]). *For positive integers q,k,n, Krawtchouk polynomials are defined as*

$$K_k(x;n,q)=\sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j},\tag{2.1}$$

where

$$\binom{x}{j}=\frac{x(x-1)\ldots(x-j+1)}{j!}.$$

Specially, $\binom{x}{0}=1$.

Lemma 2.2 ([10]). *When $x=1,\ldots,n$,*

$$\sum_{k=0}^{d-1}K_k(x;n,q)=K_{d-1}(x-1;n-1,q).\tag{2.2}$$

It is well-known that Delsarte [4] has used Krawtchouk polynomials to prove an upper bound of $A_q(n,d)$ by linear programming. We now want to use them to prove a lower bound by spectral graph theory.

Write $u=(u_1,\ldots,u_n),v=(v_1,\ldots,v_n)\in\mathbb{F}_q^n$ and define $\langle u,v\rangle=\sum_{i=1}^n u_iv_i\in\mathbb{F}_q$. Now we have the following theorem on the spectrum of $G_{q,n,d}$.

Theorem 2.1. *Denote $z=\exp\{2\pi i/q\}\in\mathbb{C}$. The q^n orthogonal eigenvectors of $G_{q,n,d}$ are*

$$a_v=\left(z^{\langle u,v\rangle}\right)_{u\in V(G_{q,n,d})} \tag{2.3}$$

for all $v\in\mathbb{F}_q^n$. The corresponding eigenvalue λ_v of a_v is $K_{d-1}(w(v)-1,n-1,q)-1$ if $w(v)\neq 0$ and $V_q(n,d-1)-1$ if $w(v)=0$.

Proof. Recall that $G_{q,n,d}$ is a Cayley graph on $H=\mathbb{F}_q^n$ with difference set $S=\{u\in\mathbb{F}_q^n\,|\,1\leq w(u)\leq d-1\}$. Let χ be a character of $(\mathbb{F}_q^n,+)$ and e_i be the vector in $\mathbb{F}_q^n$ with 1 on i-th position and 0 otherwise. For any $u=(u_1,\ldots,u_n)\in\mathbb{F}_q^n$,

$$\chi(u)=\chi\left(\sum_{i=1}^n u_ie_i\right)=\prod_{i=1}^n\chi(e_i)^{u_i},$$

so $\chi(u)$ can be determined by $\chi(e_1),\ldots,\chi(e_n)$. Since $\chi(qe_i)=\chi(e_i)^q=1$, $\chi(e_i)$ must be a q-th root of unity. For all $v=(v_1,\ldots,v_n)\in\mathbb{F}_q^n$, define χ_v to be a character satisfying $\chi_v(e_i)=z^{v_i}$. The q^n eigenvectors of $G_{q,n,d}$ are

$$a_v=\left(\chi_v(u)\right)_{u\in V(G_{q,n,d})}=\left(\prod_{i=1}^n\chi_v(e_i)^{u_i}\right)_{u\in V(G_{q,n,d})}=\left(z^{\langle u,v\rangle}\right)_{u\in V(G_{q,n,d})}.$$

For any $v,v'\in\mathbb{F}_q^n$ and $v\neq v'$,

$$\sum_{u\in\mathbb{F}_q^n}\chi_v(u)\overline{\chi_{v'}(u)}=\sum_{u\in\mathbb{F}_q^n}z^{\langle u,v-v'\rangle}=\prod_{i=1}^n\sum_{j=0}^{q-1}z^{j(v_i-v_i')}=0,$$

where $\overline{\chi_{v'}(u)}$ is the complex conjugate of $\chi_{v'}(u)$. Therefore, these q^n eigenvectors are orthogonal with each other, and hence linearly independent.

The eigenvalues of a_v are $\lambda_v=\sum_{u\in S}\chi_v(u)$. Let $\mathrm{supp}(v)=\{i\,|\,v_i\neq 0\}$. If $w(v)\neq 0$, for any integers $k,j\in\mathbb{Z}$, denote

$$\mathcal{A}_{k,j}=\left\{A\subseteq\{1,\ldots,n\}\,\middle|\,|A|=k\text{ and }|A\cap\mathrm{supp}(v)|=j\right\},$$

then $|\mathcal{A}_{k,j}|=\binom{n-w(v)}{k-j}\binom{w(v)}{j}$ and $S=\bigcup_{k=1}^{d-1}\bigcup_{j=0}^{k}\mathcal{A}_{k,j}$. For any $A\in\mathcal{A}_{k,j}$,

$$\begin{aligned}\sum_{\mathrm{supp}(u)=A}\chi_v(u)&=\sum_{\mathrm{supp}(u)=A}z^{\langle u,v\rangle}\\&=\prod_{i\in A}\left(z^{v_i}+z^{2v_i}+\ldots+z^{(q-1)v_i}\right)=(q-1)^{k-j}(-1)^j.\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{u\in S}\chi_v(u)&=\sum_{k=1}^{d-1}\sum_{j=0}^{k}\sum_{A\in\mathcal{A}_{k,j}}\sum_{\mathrm{supp}(u)=A}\chi_v(u)\\&=\sum_{k=1}^{d-1}\sum_{j=0}^{k}\binom{n-w(v)}{k-j}\binom{w(v)}{j}(q-1)^{k-j}(-1)^j\\&=\sum_{k=1}^{d-1}K_k\big(w(v);n,q\big)=K_{d-1}\big(w(v)-1;n-1,q\big)-1.\end{aligned}$$

Here the last equation is from Lemma 2.2.

If $w(v)=0$, $\chi_v(u)=1$ for all $u\in\mathbb{F}_q^n$, so

$$\lambda_v=\sum_{u\in S}\chi_v(u)=V_q(n,d-1)-1,$$

which is the degree of $G_{q,n,d}$. □

From the proof, we see the maximum eigenvalue of $G_{q,n,d}$ is $V_q(n,d-1)-1$ and the corresponding eigenvector is all-one vector $\mathbf{1}$. Let $\lambda_{\min}(G)$ be the minimum eigenvalue of G, then

$$\lambda_{\min}(G_{q,n,d})=\min_{1\le x\le n}K_{d-1}(x-1;n-1,q)-1.$$

It seems not easy to find the closed form of x which minimize $K_{d-1}(x-1;n-1,q)$, but we can compute the accurate value of $\lambda_{\min}(G_{q,n,d})$ in polynomial time for given n,q and d by Theorem 2.1.

Now we can apply two bounds on independence number to bound $\alpha(G_{q,n,d})$.

Proposition 2.2 (Hoffman's Bound)**.**

$$\alpha(G_{q,n,d})\le\frac{-q^n\lambda_{\min}(G_{q,n,d})}{V_q(n,d-1)-1+\lambda_{\min}(G_{q,n,d})}.\tag{2.4}$$

Proposition 2.3 ([17])**.** *Let G be a D-regular graph of N vertices, then*

$$\alpha(G)\ge\frac{N}{D+1+M(\lambda_{\min}(G)+1)/N},$$

where

$$M=\max\{M_+^2,M_-^2\},$$

and

$$M_+=\min_{b(G)_i>0}\frac{1}{b(G)_i},\quad M_-=\min_{b(G)_i<0}-\frac{1}{b(G)_i},$$

and $b(G)$ is one of normalized real eigenvectors of the minimum eigenvalue, $b(G)_i$ is the i-th component of $b(G)$.

To apply Proposition 2.3, we need real eigenvectors of $G_{q,n,d}$, but when $q \geq 3$, the eigenvectors given from Theorem 2.1 are complex. By our knowledge now, we can only get part of real eigenvectors from the following idea.

Given a nonempty set $A \subseteq \{1,\ldots,n\}$, for $j=1,\ldots,n-1$, define $v^{(j)} \in \mathbb{C}^n$ by

$$(v^{(j)})_i = \begin{cases} z^j, & \text{if} \quad i \in A, \\ 0, & \text{otherwise.} \end{cases}$$

Define $b_A = \sum_{j=1}^{n-1} v^{(j)}$. Notice that the value of λ_v is determined by $w(v)$ and $w(v^{(j)}) = |A|$ for all j, then b_A is an eigenvector of $G_{q,n,d}$ with eigenvalue $K_{d-1}(|A|-1;n-1,q)-1$. Since the entries of b_A are only -1 and $q-1$ and $b_A^T \mathbf{1} = 0$, we know that $\|b_A\|_2 = \sqrt{q^n(q-1)}$.

There exists some $A \subseteq \{1,\ldots,n\}$ such that $b(G_{q,n,d}) = b_A / \|b_A\|_2$ and $M = q^n(q-1)$ in Proposition 2.3. Therefore,

Corollary 2.1.

$$\alpha(G_{q,n,d}) \geq \frac{q^n}{V_q(n,d-1)+(q-1)\lambda_{\min}(G_{q,n,d})+q}. \tag{2.5}$$

We notice that Corollary 2.1 is an improvement of Gilbert-Varshamov bound since $\lambda_{\min}(G_{q,n,d}) < -1$. Proposition 2.2 and Corollary 2.1 can be calculated in polynomial time for given n,q and d by Theorem 2.1.

3 Improved lower bound

In this section, we will improve the lower bound further. Let $G_0 = G_{q,n,d}$. $\lambda_{\min}^{(0)}$ is the minimum eigenvalue of G_0 and $a_{v^{(0)}}$ is one of corresponding eigenvectors. By induction, assume we already have a series of orthogonal vectors $v^{(0)},\ldots,v^{(t-1)}$. Define G_t to be the induced graph of G_0 with vertex set $V_t = \bigcup_{i=0}^{t-1} \{u \in \mathbb{F}_q^n | \langle u, v^{(i)} \rangle = 0\}$ and edge set $E_t = E(G_0) \cap (V_t \times V_t)$. Notice that V_t is a subspace of $\mathbb{F}_q^n$.

Lemma 3.1. *For $0 \leq t < n$, G_t is Cayley graph with q^{n-t} vertices and difference set $S_t = V_t \cap \{u \in \mathbb{F}_q^n | 1 \leq w(u) \leq d-1\}$. Then the q^{n-t} orthogonal eigenvectors of G_t are*

$$a_v^{(t)} = (\chi_v(u))_{u \in V_t} = \left(z^{\langle u,v \rangle}\right)_{u \in V_t}, \tag{3.1}$$

where v is orthogonal to $v^{(0)},\ldots,v^{(t-1)}$ and χ_v is defined in Theorem 2.1.

Proof. Notice that $a_v^{(t)} = (z^{\langle u,v \rangle})_{u \in V_t}$ and $a_{v'}^{(t)} = (z^{\langle u,v' \rangle})_{u \in V_t}$ are the same vector if and only if $v - v'$ is a linear combination of $v^{(0)},\ldots,v^{(t-1)}$, so we only need to consider q^{n-t} eigenvectors $\{a_v^{(t)} \mid v \text{ is orthogonal to } v^{(0)},\ldots,v^{(t-1)}\}$. Now we need to prove that these q^{n-t}

eigenvectors are orthogonal with each other. Suppose $v-v'$ is not a linear combination of $v^{(0)},\ldots,v^{(t-1)}$, then there must be some $w\in V_t$ which is not orthogonal to $v-v'$. Therefore,

$$\sum_{u\in V_t} z^{\langle u,v-v'\rangle}=\prod_{i=t}^{n-1}\sum_{j=0}^{q-1} z^{j\langle w,v-v'\rangle}=0.$$

The proof is complete. □

Let $\lambda_{\min}^{(t)}$ denote the minimum eigenvalue of G_t and $D^{(t)}$ denote the degree of vertices in G_t. Note that the dimension of the eigenspace of $\lambda_{\min}^{(t)}$ may be larger than one. For convenience, we can sort the vectors in $\mathbb{F}_q^n$ by lexicographic order on components and choose $v^{(t)}$ as the smallest one such that $a_{v^{(t)}}^{(t)}$ is the eigenvector of $\lambda_{\min}^{(t)}$. Now let

$$V_{t+1}:=V_t\cup\Big\{u\in\mathbb{F}_q^n\,|\,(a_{v^{(t)}})_u=1\Big\}=\bigcup_{i=0}^{t}\Big\{u\in\mathbb{F}_q^n\,|\,\langle u,v^{(i)}\rangle=0\Big\}$$

and G_{t+1} is the induced graph from V_{t+1}.

Lemma 3.2. *The degree of every vertex in G_{t+1} is*

$$D^{(t+1)}=\frac{1}{q}\Big(D^{(t)}+(q-1)\lambda_{\min}^{(t)}\Big).$$

Proof. Recall $z=\exp\{2\pi i/q\}\in\mathbb{C}$. To see the degree of G_{t+1}, we notice that for any $j=1,\ldots,q-1$, $u\in S_t$ if and only if $iu\in S_t$. Also,

$$\sum_{j=1}^{q-1} z^{\langle ju,v^{(t)}\rangle}=\begin{cases}q-1, & \text{if}\quad \langle u,v^{(t)}\rangle=0,\\ -1, & \text{otherwise.}\end{cases}$$

Therefore,

$$\begin{aligned}\lambda_{\min}^{(t)}&=\sum_{u\in S_t} z^{\langle u,v^{(t)}\rangle}=|S_{t+1}|-\frac{1}{q-1}\big(|S_t|-|S_{t+1}|\big)\\&=D^{(t+1)}-\frac{1}{q-1}\big(D^{(t)}-D^{(t+1)}\big),\end{aligned}$$

where the second equality follows from

$$S_{t+1}=S_t\cap V_{t+1}=S_t\cap\Big\{u\in V_t\,|\,\langle u,v^{(t)}\rangle=0\Big\}.$$

The proof is complete. □

Remark 3.1. From Lemmas 3.1 and 3.2, we can say that G_{t+1} is sparser than G_t. In explicit language, the ratio of vertex number to degree of G_{t+1} is larger than that of G_t, since

$$\frac{|V_{t+1}|}{D^{(t+1)}+1}=\frac{|V_t|}{D^{(t)}+(q-1)\lambda_{\min}^{(t)}+q}\geq\frac{|V_t|}{D^{(t)}+1},$$

if $\lambda_{\min}^{(t)}\leq -1$, which holds for any graph with at least one edge. This means that the lower bound in Lemma 2.1 for G_{t+1} is better than that for G_t. In fact, among all subgraphs of G_t whose vertex set is a subgroup with $|V_t|/q$ elements, G_{t+1} is the sparsest one.

Due to Remark 3.1, we can improve the Gilbert-Varshamov bound.

Theorem 3.1. *If G_{t+1} has at least one edge, then*

$$A_q(n,d)=\alpha(G_{q,n,d})\geq\frac{q^n}{V_q(n,d-1)+\sum_{i=0}^{t}(q-1)q^i\lambda_{\min}^{(i)}+q^{t+1}}. \tag{3.2}$$

Proof. From Lemma 3.2,

$$D^{(t+1)}=\frac{D^{(t)}+(q-1)\lambda_{\min}^{(t)}}{q}=\frac{V_q(n,d-1)+\sum_{i=0}^{t}(q-1)q^i\lambda_{\min}^{(i)}}{q^{t+1}},$$

then

$$\alpha(G_{q,n,d})\geq\alpha(G_{t+1})\geq\frac{|V(G_{t+1})|}{D^{(t+1)}}=\frac{q^n}{V_q(n,d-1)+\sum_{i=0}^{t}(q-1)q^i\lambda_{\min}^{(i)}+q^{t+1}}.$$

The proof is complete. □

Theorem 3.1 is exactly Corollary 2.1 when $t=0$, and improves Corollary 2.1 when $t\geq 1$.

We can repeat the above procedures to get new subgraphs and improve the bound until for some integer s the graph G_s has no edges, so $\lambda_{\min}^{(s)}=0$. Now V_s is an independent set of $G_{q,n,d}$ and a subspace of $\mathbb{F}_q^n$, so V_s is a $[n,n-s,d]_q$ linear code. Therefore,

Theorem 3.2. *If $\lambda_{\min}^{(s)}=0$, then there is a $[n,n-s,d]_q$ linear code.*

This implies that Theorem 3.1 also holds for linear codes. In other words, $\lambda_{\min}^{(s)}=0$ is equal to $D^{(s)}=0$, which implies

$$V_q(n,d-1)+\sum_{t=0}^{s-1}(q-1)q^t\lambda_{\min}^{(t)}=0,$$

then

Theorem 3.3. *For any sequence* $\{b_t\}$ *with* $b_t \geq \lambda_{\min}^{(t)}$ *and* $0 \leq t \leq s-1$, *there exists a* $[n,k,d]_q$ *linear code if*

$$V_q(n,d-1)+\sum_{t=0}^{n-k-1}(q-1)q^t b_t \geq 0.$$

Since $V_s=\bigcup_{i=0}^{s-1}\{u\in\mathbb{F}_q^n \mid \langle u,v^{(i-1)}\rangle=0\}$, the code with parity check matrix $(v^{(0)},\ldots,v^{(s-1)})$ satisfies Theorem 3.2.

Now the last problem is how to calculate $\lambda_{\min}^{(t)}$. For any $v\in\mathbb{F}_q^n$, the eigenvector of G_t is $a_v^{(t)}=(z^{\langle u,v\rangle})_{u\in V_t}$, and the eigenvalue is $\lambda_v^{(t)}=\sum_{u\in S_t} z^{\langle u,v\rangle}$. Now define

$$v_r = v + r v^{(t-1)}.$$

Then

$$\sum_{r=0}^{q-1}\chi_{v_r}(u) = z^{\langle u,v\rangle}\sum_{r=0}^{q-1} z^{r\langle u,v^{(t)}\rangle} = q\chi_v(u)\mathbf{1}_{\langle u,v^{(t-1)}\rangle=0}.$$

Thus,

$$\lambda_v^{(t)} = \sum_{u\in S_t}\chi_v(u) = \sum_{u\in S_{t-1}}\chi_v(u)\mathbf{1}_{\langle u,v^{(t-1)}\rangle=0} = \frac{1}{q}\sum_{r=0}^{q-1}\sum_{u\in S_{t-1}}\chi_{v_r}(u) = \frac{1}{q}\sum_{r=0}^{q-1}\lambda_{v_r}^{(t-1)}.$$

Since $\lambda_v^{(0)}$ is known by Theorem 2.1, all eigenvalues of G_t (including the minimum eigenvalue $\lambda_{\min}^{(t)}$) can be obtained. Now we can complete the whole procedures. Algorithm 1 describes the whole process briefly.

Algorithm 1 Framework of Generating Subgraph and Linear Code.

$G=G_{q,n,d}$, $t=0$;
repeat
  Calculate the minimum eigenvalue $\lambda_{\min}^{(t)}$ of G and choose one of the corresponding eigenvector $a_{v^{(t)}}^{(t)}$;
  $G \Leftarrow$ the induced graph with vertex set $\{u\in V(G) \mid \langle u,v^{(t)}\rangle=0\}$;
  $t \Leftarrow t+1$;
until $\lambda_{\min}^{(t)}=0$
return the code with check matrix $(v^{(0)},\ldots,v^{(t-1)})$.

Remark 3.2. Our results hold when q is a prime number. In fact, when q is a prime power, the results still hold with little difference. The only difficult part is that the closed form for eigenvalues of $G_{q,n,d}$ will be much more complicated.

4 Conclusions and open problems

In this paper we use graph spectral method to improve Gilbert-Varshamov bound. The improvement is non-asymptotic. A natural question is to ask

Problem 4.1. What is the asymptotic form of Theorem 3.1 or 3.2?

We also design Algorithm 1 to give codes satisfying our improved bound. The time complexity of the algorithm is $\mathcal{O}(nq^n)$.

Problem 4.2. Could it be possible to find algorithms with lower complexity?

In the algorithm, we use the minimum eigenvalue and the corresponding eigenvector of G_t to construct G_{t+1}. It is possible to use other eigenvalues and eigenvectors instead of $\lambda_{\min}^{(t)}$ and $a_{v^{(t)}}^{(t)}$ in Algorithm 1.

Conjecture 4.1. For all vectors v such that $a_v^{(t)}$ is the eigenvector with eigenvalue $\lambda_{\min}^{(t)}$ in G_t, the graphs induced by $\{u \in V_t \mid \langle u,v\rangle = 0\}$ are isomorphic.

The conjecture is from the symmetry of the graphs. However, we also want to know

Problem 4.3. Is there a rule to choose $v^{(t)}$ such that $(v^{(0)},\ldots,v^{(s-1)})$ has a good structure which is helpful for encoding and decoding?

However, if people choose other eigenvalues rather than the minimum one to construct G_t, we believe the result can be improved.

Problem 4.4. Which eigenvalue is much better than the minimum one?

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer Science & Business Media, 2013.

[2] A. Barg, S. Guritman, and J. Simonis, *Strengthening the Gilbert-Varshamov bound. Linear algebra and its applications*, 307(1-3):119–129, 2000.

[3] A.E. Brouwer and W.H. Haemers, *Spectra of Graphs*, Springer Science & Business Media, 2011.

[4] P. Delsarte, *An Algebraic Approach to the Association Schemes of Coding Theory*, Philips Res. Rep. Suppl., vi+-97, 1973.

[5] M. Elia, *Some results on the existence of binary linear codes (Corresp.)*, IEEE Trans. Inf. Theory, 29(6):933–934, 1983.

[6] E.N. Gilbert, *A comparison of signalling alphabets*, Bell Syst. Tech. J., 31(3):504–522, 1952.

[7] C. Godsil and G.F. Royle, *Algebraic Graph Theory*, Vol. 207, Springer Science & Business Media, 2013.

[8] J. Hao, H. Huang, G. Livshyts, and K. Tikhomirov, *Distribution of the minimum distance of random linear codes*, in: 2020 IEEE International Symposium on Information Theory (ISIT), IEEE, 114–119, 2020.

[9] T. Jiang and A. Vardy, *Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes*, IEEE Trans. Inf. Theory, 50(8):1655–1664, 2004.
[10] V.I. Levenshtein, *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*, IEEE Trans. Inf. Theory, 41(5):1303–1321, 1995.
[11] K.M. O'Brien and P. Fitzpatrick, *Bounds on codes derived by counting components in Varshamov graphs*, Des. Codes Cryptogr., 39(3):387–396, 2006.
[12] S.El. Rouayheb and C.N. Georghiades, *Graph theoretic methods in coding theory*, in: Classical, Semi-Classical and Quantum Noise, Springer, 53–62, 2012.
[13] N.J.A. Sloane,*Unsolved problems in graph theory arising from the study of codes*, Graph theory notes N. Y., 18:11–20, 1989.
[14] A. Trachtenberg, *Designing lexicographic codes with a given trellis complexity*, IEEE Trans. Inf. Theory, 48(1):89–100, 2002.
[15] M.A. Tsfasman, S.G. Vlădutx, and Th. Zink, *Modular curves, shimura curves, and goppa codes, better than Varshamov-Gilbert bound*, Mathematische Nachrichten, 109(1):21–28, 1982.
[16] R.R. Varshamov, *Estimate of the number of signals in error correcting codes*, Docklady Akad. Nauk, SSSR, 117:739–741, 1957.
[17] H.S. Wilf, *Spectral bounds for the clique and independence numbers of graphs*, J. Comb. Theory. Ser. B, 40(1):113–117, 1986.