Linear Algebra and its Applications 655 (2022) 302–313

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Lovász theta approach to eventown problem

Mikhaylo Antipov [a], Danila Cherkashin [b,*]

[a] *National Research University Higher School of Economics, Soyuza Pechatnikov str., 16, St. Petersburg, Russia*
[b] *St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, 27 Fontanka, St. Petersburg, Russia*

ARTICLE INFO

Article history:
Received 20 January 2022
Accepted 30 June 2022
Available online 28 July 2022
Submitted by R.A. Brualdi

Keywords:
Graph coloring
Lovász theta function
Eventown problem

MSC:
05C15
05C50
05D05

ABSTRACT

We apply the bound on independence number via Lovász theta function to eventown problem and its generalizations over $\mathbb{Z}_n$.
© 2022 Published by Elsevier Inc.

1. Introduction

The following bound was introduced by Lovász in his celebrated paper on Shannon capacity. In particular it implies famous Hoffman bound [8].

* Corresponding author.
E-mail address: jiocb.orlangyr@gmail.com (D. Cherkashin).

https://doi.org/10.1016/j.laa.2022.06.029
0024-3795/© 2022 Published by Elsevier Inc.

Theorem 1 *(Lovász, [12]). Let $G = (V, E)$ be a simple graph. Consider a symmetric real matrix A such that $A_{ij} = 1$ for every pair $\{i, j\} \notin E(G)$. Then*

$$\alpha(G) \leqslant \lambda_{max}(A),$$

where $\alpha(G)$ is the size of a maximal independent set of G and $\lambda_{max}(A)$ is the maximal eigenvalue of A.

The minimum of $\lambda_{max}(A)$ over the appropriate A is called *Lovász number* or *Lovász theta function* of a graph.

Also we need the following corollaries. Suppose that A and G satisfy the conditions of Theorem 1. Let c, λ_{max} and sp stand for the minimal entry, the maximal eigenvalue and the spectral radius of A, respectively.

Corollary 1. *Let I be a set with at most $\varepsilon|I|^2/2$ edges inside. Suppose that $(1-c)\varepsilon < 1$. Then*

$$|I| \leqslant \frac{\lambda_{max}}{1-(1-c)\varepsilon}.$$

Corollary 2. *Let I and J be subsets of $V(G)$ with at most $\varepsilon|I| \cdot |J|$ edges between I and J (edges in $I \cap J$ are counted twice here). Suppose that $(1-c)\varepsilon < 1$. Then*

$$|I| \cdot |J| \leqslant \left(\frac{\mathrm{sp}}{1-(1-c)\varepsilon}\right)^2.$$

For the bounds on *disjoint* I and J one can make the class of appropriate matrices slightly wider, i.e. not demand $A_{ii} = 1$. Then one may combine the proof of Corollary 2 with Proposition 4.1 in the paper of Haemers [7].

Structure of the paper Subsections 1.1 and 1.2 contain our results. Section 2 is devoted to proofs; we also provide the proof of Theorem 1 in the interest of completeness. We discuss relation to several subjects and propose some further questions in Section 3.

1.1. A straightforward application to the eventown problem

Let F be a family of subsets of $[n]$ is *eventown* if the intersection of any two members is even (in particular all sets have even size). Berlekamp [2] and Graver [6] independently proved F has at most $2^{\lfloor n/2 \rfloor}$ members, which is also best possible. The proof is very short up to general linear algebra. Note that every maximal eventown F is a linear subspace of $\mathbb{F}_2^n$; otherwise one can replace F with span F. Since F lies in the orthogonal complement $F^\perp$ and $\dim F + \dim F^\perp = n$, $|F|$ has the dimension at most $\lfloor n/2 \rfloor$.

Consider the following Hadamard matrix

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Its spectrum is $\{\pm\sqrt{2}\}$. Then the spectrum of $M = A^{\otimes n}$ is $\{\pm 2^{\frac{n}{2}}\}$. Let us consider $G = (2^{[n]}, E)$ and $(X, Y) \in E$ iff $|X \cap Y|$ is odd. Then we identify elements of $2^{[n]}$ with $\{0,1\}^n$ by usual way as well as indices for rows and columns of matrix M (where we mean that $A = (a_{ij})_{i,j\in\{0,1\}}$). Let $M = (m_{st})_{s,t\in\{0,1\}^n}$. Then for each $X, Y \in 2^{[n]}$ we have

$$m_{\chi(X),\chi(Y)} = \prod_{r=1}^{n} a_{(\chi(X))_r,(\chi(Y))_r} = (-1)^{|\{r\in\{1,\dots,n\}|a_{(\chi(X))_r,(\chi(Y))_r}=-1\}|} = (-1)^{|X\cap Y|}.$$

Thus we see that graph G and matrix M satisfy the conditions of Theorem 1.

Applying Theorem 1 one has $|F| \leqslant 2^{n/2}$. For even n we already get another proof of the eventown theorem. For even n we should also recall that F is a linear subspace, so $|F| \leqslant 2^{\lfloor n/2\rfloor}$.

Let $op(F)$ denote the number of distinct pairs $f_1, f_2 \in F$ for which $|f_1 \cap f_2|$ is odd. O'Neill [13] showed that for $1 \leqslant s \leqslant 2^{\lfloor n/2\rfloor} - 2^{\lfloor n/4\rfloor}$ there is a family F with $|F| = 2^{\lfloor n/2\rfloor} + s$ and $op(F) = s \cdot 2^{\lfloor n/2\rfloor - 1}$. Also he conjectured that this example is tight and proved the conjecture for $s = 1, 2$. The application of Corollary 1 gives twice weaker bound for even n (and much weaker bound for odd n).

Theorem 2. *Let $|F| = 2^{n/2} + s$ for some integer s. Then*

$$op(F) \geqslant s \cdot 2^{\lfloor \frac{n}{2}\rfloor - 2}.$$

1.2. An application to k-town problem

Let F be a family of vectors from $\{0, \dots, k-1\}^n$, such that $(f_1, f_2) = 0 \pmod k$ for any $f_1, f_2 \in F$ (in particular for $f_1 = f_2$); such F is further called a *k-town family.*

First, for prime k the classical argument gives the tight upper bound $k^{\lfloor n/2\rfloor}$.

If k is square free we can obtain the same bound from the prime k case in the following way. Let us see that the case $k = pq$ is a formal consequence of the cases $k = p$, $k = q$ if p, q are coprime. Indeed let $F \subset (\mathbb{Z}/pq\mathbb{Z})^n$ such that $(f_1, f_2) = 0$ for each $f_1, f_2 \in F$. Then by assumption the number of residues modulo p for elements F does not exceed $p^{\frac{n}{2}}$ and number of residues modulo q for elements F does not exceed $q^{\frac{n}{2}}$. Then by the Chinese remainder theorem $|F| \leqslant p^{\frac{n}{2}} q^{\frac{n}{2}}$.

The observations above should be folklore, meanwhile we do not know how to prove the first inequality in the following theorem without spectral graph theory for an arbitrary k.

Theorem 3. *If F is a k-town family then*

$$|F| \leqslant k^{\frac{n}{2}}.$$

Moreover suppose that k is prime, and $(f_1, f_2) \neq 0 \pmod k$ for at most $\varepsilon|F|^2$ pairs $f_1, f_2 \in F$. If $\varepsilon < \frac{k-1}{k}$ then

$$|F| \leqslant \frac{k^{\frac{n}{2}}}{1 - \frac{k}{k-1}\varepsilon}.$$

Obtaining an example of k-town F with $|F| = k^{\frac{n}{2}}$ in the case of prime k and even n is equivalent to finding a set of $\frac{n}{2}$ pairwise (and-self) orthogonal linear independent vectors in $(\mathbb{Z}/k\mathbb{Z})^n$. There are lots of such sets; for example for a prime $k = 4t + 1$ one can consider vectors of the form $v_j = e_{2j-1} + \varepsilon^t e_{2j}$ for $1 \leqslant j \leqslant \frac{n}{2}$ (here $\{e_j\}$ — is the standard basis in $(\mathbb{Z}/k\mathbb{Z})^n$, ε is a primitive root in $\mathbb{Z}/k\mathbb{Z}$).

For a general prime k one can choose $v_1, v_2, \dots$ inductively and almost arbitrarily such that $v_j \in \langle v_1, \dots, v_{j-1}\rangle^\perp \setminus \langle v_1, \dots, v_{j-1}\rangle$ and $(v_j, v_j) = 0$. This can be done: indeed, for $j < \frac{n}{2} - 2$ we can choose arbitrary $4 < \dim\langle v_1, \dots, v_{j-1}\rangle^\perp - \dim\langle v_1, \dots, v_{j-1}\rangle$ linearly independent vectors and find v_j in their span (as any quadratic form with $\geqslant 3$ variables over finite field has an isotropic vector). When $j = [\frac{n}{2}] - 2$, we can choose 4-dimensional $V \subset (\langle v_1, \dots, v_{j-1}\rangle^\perp \setminus \langle v_1, \dots, v_{j-1}\rangle) \cup 0$ as well, and it is also well-known that there exists $v_{\frac{n}{2}-1}, v_{\frac{n}{2}} \in V$ such that $(v_{\frac{n}{2}-1}, v_{\frac{n}{2}-1}) = (v_{\frac{n}{2}-1}, v_{\frac{n}{2}}) = (v_{\frac{n}{2}}, v_{\frac{n}{2}}) = 0$.

In some cases where k is non-prime we can obtain examples of different nature. For example, when $k = m^2$ for some integer m one can consider the set of vectors of the form $(mx_1, \dots, mx_n)$. This example shows that in the case of k being a perfect square the first inequality of Theorem 3 is also tight for an odd n.

Suppose that we are interested in the scalar product t instead of 0. Then the statement of Theorem 3 can be slightly improved.

Corollary 3. *Let F be a family of vectors from $\{0, \dots, k-1\}^n$, and $(f_1, f_2) = t \pmod k$ for every $f_1, f_2 \in F$. Then*

$$|F| \leqslant c(t, k) \cdot k^{\frac{n}{2}}$$

for some $\frac{1}{\sqrt{2}} < c(t, k) \leqslant 1$. Moreover if $\frac{k}{\gcd(k,t)}$ tends to infinity $c(t, k)$ tends to $\frac{1}{\sqrt{2}}$ (gcd stands for the greatest common divisor).

Assume also that k is prime and $(f_1, f_2) \neq t \pmod k$ for at most $\varepsilon|F|^2$ pairs $f_1, f_2 \in F$ for some $t \neq 0$. If $\varepsilon < \frac{k-1}{k}$ then

$$|F| \leqslant c(k)\frac{k^{\frac{n}{2}}}{1 - \frac{k}{k-1}\varepsilon},$$

where $c(k) < 1$ and $c(k) \to \frac{2\sqrt{2}}{\pi}$ with $k \to \infty$.

2. Proofs

Proof of Theorem 1. Let I be an independent set, denote by χ_I its characteristic vector. Then

$$(A\chi_I, \chi_I) = |I|^2.$$

From the other hand, one has

$$(A\chi_I, \chi_I) = \sum c_i^2 \lambda_i \leqslant \left(\sum c_i^2\right) \lambda_{max} = |I| \cdot \lambda_{max},$$

where $\chi_I = \sum c_i v_i$ is the decomposition of χ_I via orthonormal eigenbasis $\{v_i\}$ of A. (We use that symmetric matrix has real spectrum and the length of χ_I is the same in the standard basis and in $\{v_i\}$, i.e. $\sum c_i^2 = |I|$.) $\square$

Proof of Corollary 1. Denote by χ_I the characteristic vector of I. Then

$$(A\chi_I, \chi_I) \geqslant |I|^2 \cdot (1 - (1-c)\varepsilon).$$

From the other hand, one has

$$(A\chi_I, \chi_I) = \sum c_i^2 \lambda_i \leqslant \left(\sum c_i^2\right) \lambda_{max} = |I| \cdot \lambda_{max},$$

where $\chi_I = \sum c_i v_i$ is the decomposition of χ_I via orthonormal eigenbasis $\{v_i\}$ of A. $\square$

Proof of Corollary 2. Denote by χ_I and χ_J the characteristic vectors of I and J respectively. Then

$$(A\chi_I, \chi_J) \geqslant |I| \cdot |J| \cdot (1 - (1-c)\varepsilon).$$

From the other hand, one has

$$(A\chi_I, \chi_I) = \sum c_i d_i \lambda_i \leqslant \left(\sum |c_i| \cdot |d_i|\right) \mathrm{sp} \leqslant \sqrt{\left(\sum c_i^2\right)\left(\sum d_i^2\right)} \cdot \mathrm{sp} = \sqrt{|I| \cdot |J|} \cdot \mathrm{sp},$$

where $\chi_I = \sum c_i v_i$ and $\chi_J = \sum d_i v_i$ are the decompositions of χ_I and χ_J via orthonormal eigenbasis $\{v_i\}$ of A. $\square$

Proof of Theorem 3. Consider the following $k \times k$ matrix:

$$a_{jl} = \phi^{jl},$$

where ϕ is a primitive k-th root of unity and $0 \leqslant j, l \leqslant k-1$ and the matrix $M = A^{\otimes n}$. Then we have $A^4 = k^2 E$, therefore $|\lambda| = (k^{\frac{1}{2}})^n = k^{\frac{n}{2}}$ for each eigenvalue λ of M, i.e., $\mathrm{sp}(M) = k^{\frac{n}{2}}$.

Let us see that A (and, as a consequence, M) has an eigenbasis in $\mathbb{R}^n$. Let $\{e_i\}$ be a standard basis. Then moving to the basis $\{e_1, \frac{1}{\sqrt{2}}(e_j \pm e_{k+2-j})\}$ or to $\{e_1, e_{\frac{k}{2}}, \frac{1}{\sqrt{2}}(e_j \pm e_{k+2-j})\}$ for even k (note that it is a unitary transformation) we obtain a block matrix with two blocks of the form A_1, iA_2, where A_1, A_2 are the real symmetric matrices (they have the sizes $\frac{k+1}{2}$ and $\frac{k-1}{2}$ respectively for odd k and $\frac{k}{2}+1$, $\frac{k}{2}+1$ for even k). As a matter of fact, for each $2 \leqslant j \leqslant k$ we have

$$\begin{aligned} A(e_j + e_{k+2-j}) &= \sum_{l=1}^{k} \phi^{(j-1)(l-1)} e_l + \sum_{l=1}^{k} \phi^{(k+1-j)(l-1)} e_l \\ &= 2 + \sum_{l=2}^{k} (\phi^{(j-1)(l-1)} + \overline{\phi^{(j-1)(l-1)}}) e_l \\ &= 2 + \sum_{l=2}^{[\frac{k}{2}]} 2 \cdot \mathrm{Re}(\phi^{(j-1)(l-1)})(e_l + e_{k+2-l}) \end{aligned}$$

and for each $2 \leqslant j \leqslant k$, $j \neq \frac{k}{2}$

$$\begin{aligned} A(e_j - e_{k+2-j}) &= \sum_{l=1}^{k} \phi^{(j-1)(l-1)} e_l - \sum_{l=1}^{k} \phi^{(k+1-j)(l-1)} e_l \\ &= \sum_{l=2}^{k} (\phi^{(j-1)(l-1)} - \overline{\phi^{(j-1)(l-1)}}) e_l \\ &= i \cdot \sum_{l=2}^{[\frac{k}{2}]} 2 \cdot \mathrm{Im}(\phi^{(j-1)(l-1)})(e_l - e_{k+2-l}). \end{aligned}$$

Thus we see that this change of the base (over $\mathbb{R}$) leads to real symmetric matrix and to pure imaginary symmetric matrix, which both have real eigenbasis, therefore A has real eigenbasis as well. Hence $N := \mathrm{Re}\, M$ has the same real eigenbasis with M. Obviously, all eigenvalues of N lie in $\{\pm k^{n/2}, 0\}$.

Let us consider $G = ((\mathbb{Z}/k\mathbb{Z})^n, E)$, where $(X, Y) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in E$ iff $\sum_{r=1}^{n} x_r y_r \neq 0$. Then we also identify $(\mathbb{Z}/k\mathbb{Z})^n$ as indices for rows and columns of matrix M (taking all indices in A modulo k). Let $M = (m_{st})_{s,t \in \{0,\ldots,k-1\}^n}$. Now for each $X, Y \in (\mathbb{Z}/k\mathbb{Z})^n, (X, Y) \notin E$ we have

$$m_{X,Y} = \prod_{r=1}^{n} a_{x_r, y_r} = \phi^{\sum_{r=1}^{n} x_r y_r} = \phi^0 = 1.$$

Thus graph G and matrix M (and also N) satisfy the conditions of Theorem 1, so the first statement of the theorem is proved.

Now let k be a prime number. An immediate application of Corollary 1 gives

$$|F| \leqslant \frac{k^{\frac{n}{2}}}{1-t\varepsilon},$$

where $t = 1 - \cos\left(\left\lfloor \frac{k}{2} \right\rfloor \frac{2\pi}{k}\right)$, which tends to 2 with $k \to \infty$. So we modify the proof of Corollary 1 in the following way.

For every root ϕ the matrix $N = N(\phi)$ satisfies

$$(N(\phi)\chi_F, \chi_F) = \sum_{i,j \in F} N_{ij}(\phi)$$

and

$$(N(\phi)\chi_F, \chi_F) \leqslant |F| \cdot k^{\frac{n}{2}}.$$

Summing up these inequalities for all k-th roots except 1 one has

$$(k-1) \cdot |F|^2 \cdot (1-\varepsilon) - \varepsilon \cdot |F|^2 \leqslant (k-1) \cdot |F| \cdot k^{\frac{n}{2}} \tag{1}$$

since for every i, j that corresponds to sets with nonzero scalar product

$$\sum_{\phi \neq 1} N_{ij}(\phi) = -1,$$

and for i, j that corresponds to sets with zero scalar product

$$\sum_{\phi \neq 1} N_{ij}(\phi) = k - 1.$$

Rewriting (1) finishes the proof. □

Proof of Corollary 3. Fix a primitive k-th root of unity ϕ and consider the same matrices A and M as in the previous proof. Let us consider $G = ((\mathbb{Z}/k\mathbb{Z})^n, E)$, where $(X, Y) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in E$ iff $\sum_{r=1}^n x_r y_r \neq t$. Then G and $N := \mathrm{Re}(\phi^t M)$ satisfy the conditions of Theorem 1. Note that N and M shares a real eigenbasis, so all eigenvalues of N lie in $\mathrm{Re}\{\pm\phi^t k^{n/2}, \pm\phi^t k^{n/2} i\}$. Hence the spectral radius of N lies between $\frac{1}{\sqrt{2}} k^{n/2}$ and $k^{n/2}$.

Let us check the second part of the first proposition. Note that for any coprime x, y we have $\frac{xy}{\gcd(xy,t)} = \frac{x}{\gcd(x,t)} \cdot \frac{y}{\gcd(y,t)}$ and $c(t, xy) \leqslant c(t, x)c(t, y)$ — this follows from remarks before Theorem 3. Therefore we need only treat the case $k = p^s$ for prime p.

Note that any upper bound for $|F|$ with some $t = t_0$ is also an upper bound for $t = t_0 r^2, r \in (\mathbb{Z}/k\mathbb{Z})^*$. Indeed, if $(f_1, f_2) = t_0 r^2$ for each $f_1, f_2 \in F$, then $(\frac{1}{r} f_1, \frac{1}{r} f_2) = t_0$ and we can apply a bound for $t = t_0$. Now we are to show that we can choose $r = r(k, t)$

such that $|\operatorname{Re}(\phi^{tr^2})|$ tends to $\frac{1}{\sqrt{2}}$ if $\frac{k}{\gcd(k,t)}$ tends to infinity — in this case $|\operatorname{Re}(\phi^{tr^2} i^l)|$ tends to $\frac{1}{\sqrt{2}}$ as well. To obtain this, it's sufficient to choose r such that $|\frac{tr^2}{k/8}|$ tends to 1 (with suitable choice of representative of tr^2 modulo k).

Any $t \in \mathbb{Z}/p^s\mathbb{Z}$ we can consider as $t = p^m t', r \in \mathbb{Z}/p^{s-m}\mathbb{Z}$ and replacing (t, p^s) with (r, p^{s-m}) (this doesn't change both ratios in question) we can assume that $t \in (\mathbb{Z}/p^s\mathbb{Z})^*$ (and $\frac{k}{\gcd(k,t)} = k$).

Let $p > 2$. Let's prove that we can choose l such that $|l| < k^{\frac{1}{2}}$ and $t = lw^2$ modulo k for some w. Suppose that t is non-square modulo k (else we can take $l = 1$). If $p = 2$, then all non-squares are known to be of the form $3w^2, 5w^2$ or $7w^2$ for some w, so we can take $l \in \{1, 3, 5, 7\}$ (when $s > 5$). If $p > 2$ we can take l_1, l_2 with $|l_i| < \sqrt{p}$ such that $l_1 = l_2 t$ modulo p by Thues lemma. Then for some i l_i is a non-square modulo m and therefore modulo $k = p^s$. As t is non square as well we can write $t = l_i w^2$ and take $l = l_i$.

Now take $x \in \mathbb{Z}$ such that $x^2 \in \left(\frac{k}{8|l|} - \left(\frac{k}{|l|}\right)^{\frac{1}{2}}, \frac{k}{8|l|} + \left(\frac{k}{|l|}\right)^{\frac{1}{2}}\right)$, then $||lx^2| - \frac{k}{8}| \leqslant (kl)^{\frac{1}{2}} < k^{\frac{3}{4}}$ and $|\frac{lx^2}{\frac{k}{8}}|$ tends to 1 when k tends to infinity, as desired (we put $r = \frac{x}{w}$ modulo k).

Now we prove the second part of Corollary. Repeat the proof of the corresponding part of Theorem 3. Then the right part of (1) is replaced with

$$\sum_{a=1}^{k-1} \operatorname{sp} \operatorname{Re}(\phi^{ta} M).$$

Note that for every a

$$\operatorname{sp} \operatorname{Re}(\phi^{ta} M) = \max(\operatorname{Re}(\phi^{ta}), \operatorname{Re}(\phi^{ta} \cdot i), -\operatorname{Re}(\phi^{ta}), -\operatorname{Re}(\phi^{ta} \cdot i)) \cdot k^{n/2} =$$
$$\max\left(\left|\cos\frac{2\pi ta}{k}\right|, \left|\cos\left(\frac{2\pi ta}{k} + \frac{\pi}{2}\right)\right|, \left|\cos\left(\frac{2\pi ta}{k} + \pi\right)\right|, \left|\cos\left(\frac{2\pi ta}{k} + \frac{3\pi}{2}\right)\right|\right) k^{n/2}.$$

After summation over $1 \leqslant a \leqslant k-1$ and taking $k^{n/2}$ out of the brackets and dividing by $k-1$, one has a Riemann sum for the following integral

$$\frac{\int_0^{\pi/4} \cos(x) dx}{\pi/4} = \frac{2\sqrt{2}}{\pi}. \quad \square$$

3. Discussion

3.1. Related subjects

It turns out that Theorem 3 is closely related with several well-studied themes.

Erdős distance problem over a finite field Let $\mathbb{F}_q$ be a finite field. Hart and Iosevich [9] proved that if $t \neq 0$ and $E \subset \mathbb{F}_q^n$, then

$$|\{(x,y) \in E \times E : x \cdot y = t\}| = \frac{|E|^2}{q} + R(E),$$

where

$$|R(E)| \leqslant q^{\frac{n-1}{2}}|E|.$$

In the notation of Theorem 3 (for this part we assume k to be prime) it implies inequality

$$|F| \leqslant \frac{k^{\frac{n-1}{2}}}{\frac{k-1}{k} - \varepsilon}.$$

This bound is better than Theorem 3 for a large prime k, but it essentially requires the condition $t \neq 0$. The bound for $t = 0$ is obtained in [10] and is slightly weaker than Theorem 3.

Define the distance in an n-dimensional vector space over a finite field as

$$\mathrm{dist}(\bar{x}, \bar{y}) = (x_1 - y_1)^2 + \ldots (x_n - y_n)^2,$$

i.e. we omit the square root in the standard formula. Let $\Delta(E)$ be the set of all distances between points in E. The Erdős distance problem is to determine the smallest possible cardinality of the set $\Delta(E)$ over all sets E of a given size.

In the case of prime $k > 2$ Theorem 3 gives the following elementary bound which is far from the Iosevich–Rudnev estimate [11]. Let E be a set with $|\Delta(E)| = s$. Without loss of generality $(0, \ldots, 0) \in E$; otherwise one may shift E. Then E lies on s spheres centered at $(0, \ldots, 0)$. By a pigeon-hole principle there is a sphere containing a subset $E' \subset E$ of size at least $(|E| - 1)/s$. Since k is odd and E' lie on a sphere, there are at most s different scalar products between vectors of E'. Let t be a most popular scalar product in $E' \times E'$. Then one may apply Theorem 3 with $\varepsilon = \frac{s-1}{s}$ and receive that

$$|E'| \leqslant \frac{k^{n/2}}{1 - \frac{k}{k-1}\frac{s-1}{s}} = \frac{s(k-1)k^{n/2}}{k-s}.$$

Hence

$$|E| \leqslant \frac{s^2(k-1)k^{n/2}}{k-s} + 1.$$

For instance, $s = k - 1$ means that we evaluate the size of a set without a single distance r by $k^{\frac{n+6}{2}}$, meanwhile Iosevich–Rudnev estimate is $Ck^{\frac{n+1}{2}}$ with an absolute constant $C > 0$.

A bound via singular numbers Let $G = (V, E)$ be a simple graph. Suppose that A is a complex matrix such that $A_{ij} = 1$ for every pair $\{i, j\} \notin E(G)$. Then

$$\alpha(G) \leqslant \sigma_{max}(A),$$

where $\alpha(G)$ is the size of a maximal independent set of G and $\sigma_{max}(A)$ is the maximal singular value of A (i.e. the square root of a maximal eigenvalue of a self-adjoint operator A^*A, where A^* denotes the adjoint of A). The proof immediately follows from the main theorem of [3].

For matrix A in the proof of Theorem 3 one has

$$A^*A = kE,$$

so every singular number of matrix A is equal to $\sqrt{k}$. Hence every singular number of $M = A^{\otimes n}$ is equal to $k^{n/2}$. This implies the first inequality of Theorem 3.

Hypergraph discrepancy and asymptotic precision of Theorem 2 when ε is close to $1/2$ A hypergraph is a pair (V, E), where V is a finite set whose elements are called vertices and E is a family of subsets of V, called edges. A vertex 2-coloring of a hypergraph (V, E) is a map $\pi : V \to \{\pm 1\}$. A *discrepancy* of a coloring π is the largest value of $|\sum_{v \in e} \pi(v)|$ over $e \in E$.

Consider an explicit hypergraph $H = (V, E)$, where $V = [N] \times [N]$ and edges have form $I \times J$ for $I, J \subset [N]$. Note that every $\{\pm 1\}$ matrix of size N produces a 2-coloring of H. Let $N = 2^n$ and χ be the coloring from $A^{\otimes n}$ (recall that A is 2×2 Hadamard matrix). Let $I \times J$ be an edge of H providing the discrepancy disc of χ; without loss of generality let disc be positive. Then

$$\text{disc} = (A^{\otimes n}\chi_I, \chi_J) = (1 - 2\varepsilon) \cdot |I| \cdot |J|,$$

where ε satisfies the conditions of Theorem 2. Theorem 2 implies

$$\text{disc}^2 = |I|^2 \cdot |J|^2 (1 - 2\varepsilon)^2 \leqslant 2^n |I| \cdot |J| \leqslant 2^{3n} = N^3. \tag{2}$$

Astashkin proved [1] that H has the discrepancy at least $cN^{3/2}$ for *every* coloring χ and some absolute constant $c > 0$, i.e. inequality (2) is precise up to an absolute constant. It means that Theorem 2 is precise up to an absolute constant in the case when $|I|$ and $|J|$ are close to N and $\frac{1}{2} - \varepsilon$ is of order $2^{-n/2}$.

3.2. Further questions

Generalization on k-eventown We say that $F \subset 2^{[n]}$ is k-eventown if the size of the intersection of any (not necessarily different) $f_1, f_2 \in F$ is zero modulo k. The problem of determining the maximal size of k-eventown was studied by Frankl and Odlyzko [4].

They found a nice construction based on Hadamard matrices of k-eventowns of size at least $(ck)^{\lfloor n/(4k)\rfloor}$, where $c > 0$ is an absolute constant. In addition, they showed that any k-eventown has size at most $2^{O(\log k/k)n}$ as n tends to ∞.

In particular, for $k = 3$ the best known lower and upper bounds are $24^{\lfloor n/12\rfloor}$ and $2^{\lfloor n/2\rfloor}$ respectively.

Generalization on t-wise k-eventown We say that $F \subset 2^{[n]}$ is t-wise k-eventown if the size of the intersection of any different $f_1, \dots, f_t \in F$ is zero modulo k. Note that a 2-wise k-eventown is not the same as an k-eventown, since in the former we do not require that the sets themselves have size zero modulo k.

Sudakov and Vieira [14] show that a t-wise eventown has for $t \geqslant 3$ a unique extremal configuration and obtain a stability result for this problem. Gishboliner, Sudakov and Tomon [5] show that for every k there is $t = t(k)$ that the size of any t-wise k-eventown is bounded by

$$|F| \leqslant 2^{[n/k]} + const(k, t).$$

A generalization of the methods of the paper, if it exists, will have a deal with some tensor analysis.

Declaration of competing interest

There is no competing interest.

Acknowledgements

The authors are grateful to Fedor Petrov, Andrey Kupavskii and Pavel Prozorov for useful discussions. The reviewer's remarks were extremely helpful. The work of Danila Cherkashin was supported by the Russian Science Foundation grant 21-11-00040.

References

[1] Sergey V. Astashkin, Rademacher functions in symmetric spaces, J. Math. Sci. 169 (6) (2010) 725–886.
[2] E.R. Berlekamp, On subsets with intersections of even cardinality, Can. Math. Bull. 12 (4) (1969) 471–474.
[3] Jeffrey Danciger, A min–max theorem for complex symmetric matrices, Linear Algebra Appl. 412 (1) (2006) 22–29.
[4] Peter Frankl, Andrew M. Odlyzko, On subsets with cardinalities of intersections divisible by a fixed integer, Eur. J. Comb. 4 (3) (1983) 215–220.
[5] Lior Gishboliner, Benny Sudakov, István Tomon, Small doubling, atomic structure and ℓ-divisible set families, arXiv preprint arXiv:2103.16479, 2021.
[6] Jack E. Graver, Boolean designs and self-dual matroids, Linear Algebra Appl. 10 (2) (1975) 111–128.
[7] Willem H. Haemers, Bicliques and eigenvalues, J. Comb. Theory, Ser. B 82 (1) (2001) 56–66.
[8] Willem H. Haemers, Hoffman's ratio bound, Linear Algebra Appl. 617 (2021) 215–219.
[9] Derrick Hart, Alex Iosevich, Sums and products in finite fields: an integral geometric viewpoint, Radon Transform. Geom. Wavel. 464 (2008) 129–135.

[10] Derrick Hart, Alex Iosevich, Doowon Koh, Misha Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős–Falconer distance conjecture, Trans. Am. Math. Soc. 363 (6) (2011) 3255–3275.
[11] Alex Iosevich, Misha Rudnev, Erdős distance problem in vector spaces over finite fields, Trans. Am. Math. Soc. 359 (12) (2007) 6127–6142.
[12] László Lovász, On the Shannon capacity of a graph, IEEE Trans. Inf. Theory 25 (1) (1979) 1–7.
[13] Jason O'Neill, Towards supersaturation for oddtown and eventown, arXiv preprint arXiv:2109.09925, 2021.
[14] Benny Sudakov, Pedro Vieira, Two remarks on eventown and oddtown problems, SIAM J. Discrete Math. 32 (1) (2018) 280–295.