ACTA ARITHMETICA
Online First version

Note on a result of Shparlinski and related results

by

Norbert Hegyvári and Máté Pálfy (Budapest)

1. Introduction. Let $\mathbb{F}_q$ be the finite field of q elements. Denote by $\mathbb{F}_q^n$ the vector space over the field $\mathbb{F}_q$. Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$. The *additive energy* $E(\mathcal{A}, \mathcal{B})$ is defined by

$$E(\mathcal{A}, \mathcal{B}) = |\{(\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4) \in \mathcal{A} \times \mathcal{A} \times \mathcal{B} \times \mathcal{B} : \underline{x}_1 + \underline{x}_2 = \underline{x}_3 + \underline{x}_4\}|.$$

When $\mathcal{A} = \mathcal{B}$ we briefly write $E(\mathcal{A})$.

For $\underline{x}, \underline{y} \in \mathbb{F}_q^n$ define their *distance* in the usual way:

$$d(\underline{x}, \underline{y}) := \sum_{i=1}^{n} (x_i - y_i)^2, \quad \underline{x} = (x_1, \dots, x_n),\ \underline{y} = (y_1, \dots, y_n),$$

and write $D(\mathcal{X}, \mathcal{Y}) = \{d(\underline{x}, \underline{y}) : \underline{x}, \underline{y} \in \mathcal{X} \times \mathcal{Y}\}$. For two sets $\mathcal{X}$ and $\mathcal{Y}$ the *energy* of the distance set is

$$E_D(\mathcal{X}, \mathcal{Y}) := E(D(\mathcal{X}, \mathcal{Y})).$$

Denote by $\mathrm{Span}(\underline{x}_1, \dots, \underline{x}_k)$ the subspace spanned by the vectors $\underline{x}_1, \dots, \underline{x}_k$.

In [S] Shparlinski proved the following result:

Theorem 1.1. *For every odd q and arbitrary sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_q^n$,*

$$\left| E_D(\mathcal{X}, \mathcal{Y}) - \frac{|\mathcal{X}|^4 |\mathcal{Y}|^4}{q} \right| \le |\mathcal{X}|^3 |\mathcal{Y}|^3 q^{n-1} + |\mathcal{X}|^3 |\mathcal{Y}|^2 q^{3n/2}.$$

One of the main tools of the proof was the following nice result:

Proposition 1.2. *For every q and arbitrary sets $\mathcal{S}, \mathcal{T} \subseteq \mathbb{F}_q^n$ we have*

$$\left| N(\mathcal{S}, \mathcal{T}) - \frac{|\mathcal{S}|\,|\mathcal{T}|}{q} \right| \le \sqrt{|\mathcal{S}|\,|\mathcal{T}| q^n}$$

where $N(\mathcal{S}, \mathcal{T})$ counts the number of pairs $(\underline{s}, \underline{t}) \in \mathcal{S} \times \mathcal{T}$ which are perpendicular.

2020 *Mathematics Subject Classification*: Primary 11B30, 11L03; Secondary 11B75.
Key words and phrases: additive energy, distance sets, graph spectra, character sums.
Received 18 October 2018; revised 24 January 2019 and 5 January 2020.
Published online 16 January 2020.

DOI: 10.4064/aa181018-8-4 © Instytut Matematyczny PAN, 2020

The proof of this statement uses discrete Fourier transforms. In Section 2 we give a new proof of this statement (in a little stronger form for $n \geq 3$) using the technique of graph spectra, and we derive a consequence of this result. Many nice results can be proved via this technique (see e.g. [SO], [P2], [V], [HH]). We have learnt that Thang Pham [P1] also recently proved the proposition above in a different way (using the sum-product graph).

From Proposition 1.2 we will derive some structural theorem for 'dense' sets.

DEFINITION 1.3. Let $\mathcal{S} \subseteq \mathbb{F}_q^n$ be an arbitrary set and let $\mathcal{X} \subseteq \mathrm{Span}(\mathcal{S})$ be a set of independent vectors. This set is said to be an *independent-normal corner* or briefly a *normal corner* if $\|\underline{x}\| = \|\underline{y}\|$ for any $\underline{x}, \underline{y} \in \mathcal{X}$. Let

$$I_k := \{\mathcal{X} \subseteq \mathrm{Span}(\mathcal{S}) : \mathcal{X} \text{ is a normal corner and } |\mathcal{X}| \leq k\}.$$

THEOREM 1.4. *Let $n \geq 3$, let $\mathcal{S} \subseteq \mathbb{F}_q^n$ be an arbitrary set of vectors and let*

$$k = \left\lfloor \frac{\log\left(\frac{|\mathcal{S}|}{2q^{n/2+2}}\right)}{\log(2q)} \right\rfloor. \tag{1.1}$$

For every $\mathcal{X} \in I_k$, there is a $\lambda \in \mathbb{F}_q$ such that $\lambda\mathcal{X} \subseteq \mathcal{S}$.

Roughly speaking this result says that every possible normal configuration occurs in $\mathcal{S}$, provided its size is bounded by (1.1). Note that the theorem is nontrivial when $n \geq 6$ and $|S| \geq 4q^{n/2+3}$. (For a related result see [IR].)

2. Proofs of Proposition 1.2 and Theorem 1.4

Proof of Proposition 1.2. For a graph G let $\lambda_1 \geq \cdots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. Then $\lambda = \lambda(G) = \max\{|\lambda_2|, |\lambda_n|\}$ is said to be the *second eigenvalue* of G. If G is d-regular and λ is much smaller than d then G looks like a *random* graph.

In the proof we will use the following Cheeger-type bound (see [AS]):

LEMMA 2.1. *Let $G = (V, E)$ be a d-regular graph with n vertices. Let $\lambda_1 \geq \cdots \geq \lambda_n$ be the sequence of eigenvalues of its adjacency matrix M. Let $\lambda(G) = \max\{|\lambda_2|, |\lambda_n|\}$. Then for any $S, T \subseteq V$ (not necessarily disjoint),*

$$\left| e(S,T) - \frac{d}{n}|S|\,|T| \right| \leq \lambda\sqrt{|S|\,|T|}$$

where $e(S,T)$ is the number of ordered pairs of edges between S and T.

We construct the following graph: The vertices will be the elements of $\mathbb{F}_q^n \setminus \{0\}$. Two vertices $\underline{i}$ and $\underline{j}$ are connected by an edge if and only if they are perpendicular. We can easily see that it is a $q^{n-1} - 1$-regular graph. Indeed, the orthogonal complement of a given nonzero vector (minus the zero vector) has cardinality $q^{n-1} - 1$. It is known that if G is connected and nonbipartite,

then the eigenvalue $q^{n-1}-1$ has multiplicity 1 (i.e. $|\lambda_i| < \lambda_1 = d = q^{n-1}-1$ for all $i = 2, 3, \dots, n$)

Since $n \geq 3$, we can see that the vertices $(1,0,0,\dots)$, $(0,1,0,\dots)$, $(0,0,1,\dots)$ form a triangle, so the graph is not bipartite, and trivially it is connected, because if we pick two vectors $\underline{a}$ and $\underline{b}$ then the subspace orthogonal to $\mathrm{Span}(\underline{a}, \underline{b})$, which has dimension at least 1, gives the set of vertices for a path of length two between them.

Let M be the adjacency matrix of G and write

$$M^2 = (q^{n-2}-1)J + (q^{n-1}-q^{n-2})I + (q^{n-1}-q^{n-2})E \tag{2.1}$$

where J is the all-one matrix, I is the identity matrix and E is the 'error' matrix.

It is easy to see that the $(\underline{i}, \underline{j})$ entry of M^2 gives the number of paths of length two between vertices $\underline{i}$ and $\underline{j}$, in particular for $\underline{i} = \underline{j}$ it gives the degree of vertex $\underline{i}$.

We will show that E is a matrix of a regular graph, so we can give an estimate for λ of M.

In the matrix M^2, on the diagonal, there are $q^{n-1}-1$, as discussed before, hence in E the diagonal entries are 0. Furthermore if $(\underline{i}, \underline{j}) \in M^2$, and they are not parallel, then their orthogonal subspace (without $\underline{0}$) has cardinality $q^{n-2}-1$. If $\underline{i}$ and $\underline{j}$ are parallel (which means that there exists a $\lambda \in \mathbb{F}_p$ such that $\lambda\underline{i} = \underline{j}$), then their orthogonal complement has cardinality $q^{n-1}-1$.

Hence by (2.1) we find that E is the matrix of a $q-1$-regular graph.

Now pick an eigenvector $\underline{v}$ of M with eigenvalue $\lambda \neq q^{n-1}-1$. It is also an eigenvector of M^2, and so of E. Thus

$$M^2\underline{v} = (q^{n-2}-1)J\underline{v} + (q^{n-1}-q^{n-2})I\underline{v} + (q^{n-1}-q^{n-2})E\underline{v}.$$

Note that $\underline{v} \in \underline{1}^{\perp}$, where $\underline{1}$ is the all-one eigenvector, thus $J\underline{v} = \underline{0}$. Reducing $M^2\underline{v}$ to $(q^{n-1}-q^{n-2})I\underline{v} + (q^{n-1}-q^{n-2})E\underline{v}$, and since λ^2 is an eigenvalue of the sum of matrices with eigenvector $\underline{v}$, we obtain

$$|\lambda^2|\,|\underline{v}| = |\lambda^2\underline{v}| \leq (q^{n-1}-q^{n-2})|\underline{v}| + (q-1)(q^{n-1}-q^{n-2})|\underline{v}|,$$

which gives

$$\lambda \leq \sqrt{q^n - q^{n-1}}.$$

Finally, since $e(\mathcal{S}, \mathcal{T}) = N(\mathcal{S}, \mathcal{T})$, using Lemma 2.1 we obtain the statement. ∎

Proof of Theorem 1.4. Since the length of a vector is at most q, we can select a subset $\mathcal{S}^*$ of $\mathcal{S}$ such that $\|\underline{s}\| = \|\underline{s}'\|$ for all $\underline{s}, \underline{s}' \in \mathcal{S}^*$ and $|\mathcal{S}^*| \geq |\mathcal{S}|/q$. Let $\mathcal{X} \in I_k$. Since $\mathcal{X}$ is a set of independent vectors, there is an invertible matrix M for which the set $M(\mathcal{X}) := \{M \cdot x : x \in \mathcal{X}\}$ consists of pairwise perpendicular vectors. We can also assume that $\det(M) = 1$, hence M is an isometry too (for this it is enough to assume that p is large enough).

So let $\mathcal{S}' := M(\mathcal{S}^*)$. We follow an iteration process. Let $\mathcal{S}' =: \mathcal{S}_0$. Then by Proposition 1.2,

$$N(\mathcal{S}_0, \mathcal{S}_0) > \frac{|\mathcal{S}_0|^2}{q} - |\mathcal{S}_0|\sqrt{q^n} > \frac{|\mathcal{S}_0|^2}{2q}$$

provided $|\mathcal{S}_0| > 2q^{n/2+1}$. By an averaging argument we get an $\underline{s}_1 \in \mathcal{S}_0$ and an $\mathcal{S}_1 \subseteq \mathcal{S}_0$ for which $|\mathcal{S}_1| \geq |\mathcal{S}_0|/(2q)$ and each vector of $\mathcal{S}_1$ is perpendicular to $\underline{s}_1$.

Assume now that sets $\mathcal{S}_0 \supseteq \mathcal{S}_1 \supseteq \cdots \supseteq \mathcal{S}_i$ and vectors $\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_i$ have been defined such that

$$|\mathcal{S}_i| \geq \frac{|\mathcal{S}_{i-1}|}{2q}, \tag{2.2}$$

and for all $1 \leq r \neq t \leq i$, $\underline{s}_t$ and $\underline{s}_r$ are perpendicular and each vector of $\mathcal{S}_i$ is perpendicular to $\underline{s}_r$. From (2.2), $|\mathcal{S}_i| \geq |\mathcal{S}_0|/(2q)^i$ and if $|\mathcal{S}_0|/(2q)^i > 2q^{n/2+1} > 2q^{(n-i)/2+1}$ then we can define a set $\mathcal{S}_i \supseteq \mathcal{S}_{i+1}$ and a vector $\underline{s}_{i+1}$ in a similar way. Our iteration terminates at some $\mathcal{S}_k$ and $\underline{s}_k$ with

$$k \leq \frac{\log\left(\frac{|\mathcal{S}_0|}{2q^{n/2+2}}\right)}{\log(2q)}$$

since $|\mathcal{S}^*| \geq |\mathcal{S}|/q$. Now $X = M^{-1}(\{\underline{s}_i\}_{i=1}^k)$ is of the form $\lambda\mathcal{X}$ and is contained in $\mathcal{S}$.

3. Analogue of Theorem 1.1 for some 'additive' sets. In this section we additionally assume that the usual additive energy of the set $\mathcal{Y}$ is 'small'. We will use a modified version of Proposition 1.2. Instead of the bound $\sqrt{|\mathcal{S}|\,|\mathcal{T}|q^n}$ we will get the bound $\sqrt{\mathcal{S}\mathcal{T}}\,q^{n/8}(E(\mathcal{S})E(\mathcal{T}))^{1/8}$, which is less than the previous one when $E(\mathcal{S})E(\mathcal{T}) < q^{3n}$. Since $E(\mathcal{S}) < |\mathcal{S}|^3$ and $E(\mathcal{T}) < |\mathcal{T}|^3$, in this range the bound $|\mathcal{S}|\,|\mathcal{T}| < q^n$ is nontrivial. Shparlinski [S] also obtained a result for small sets. He introduced the largest projection size of a set as follows:

$$w(\mathcal{Y}) := \max_{1\leq i\leq n} |\{(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n) : (y_1, \ldots, y_n) \in \mathcal{Y}\}|.$$

For the 'error' term in [S, Theorem 3] the bound is $2w(\mathcal{Y})|\mathcal{X}|^3|\mathcal{Y}|^2q^n$. Clearly $w(\mathcal{Y}) \geq |\mathcal{Y}|/q$. Now assuming that the additive energy of $\mathcal{Y}$ is $E(\mathcal{Y}) = |\mathcal{Y}|^{3-c}$ for some $c > 0$, an easy calculation shows that the next theorem is new in the range $q^{(n+16)/(2+2c)} < |\mathcal{Y}| < q^{n/2}$.

We will prove

THEOREM 3.1. *For every odd q and arbitrary sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_q^n$,*

$$\left|E_D(\mathcal{X}, \mathcal{Y}) - \frac{|\mathcal{X}|^4|\mathcal{Y}|^4}{q}\right| \leq |\mathcal{X}|^3|\mathcal{Y}|^3q^{n-1} + |\mathcal{X}|^3|\mathcal{Y}|^2q^{(9n+8)/8}E(\mathcal{Y})^{1/4}.$$

Proof. We follow the idea of [S, Theorem 1]. Let Ψ be a nontrivial character of $\mathbb{F}_q$. It is easy to see that by orthogonality of characters we have

$$E_D(\mathcal{X},\mathcal{Y}) = \frac{1}{q}\sum_{r\in\mathbb{F}_q}\Big|\sum_{\underline{x}\in\mathcal{X},\,\underline{y}\in\mathcal{Y}}\Psi(rd(\underline{x},\underline{y}))\Big|^4,$$

and separating the $r=0$ term we get

$$E_D(\mathcal{X},\mathcal{Y}) = \frac{|\mathcal{X}|^4|\mathcal{Y}|^4}{q} + \frac{1}{q}\sum_{r\in\mathbb{F}_q^*}\Big|\sum_{\underline{x}\in\mathcal{X},\,\underline{y}\in\mathcal{Y}}\Psi(rd(\underline{x},\underline{y}))\Big|^4. \tag{3.1}$$

LEMMA 3.2. *We have*

$$\sum_{r\in\mathbb{F}_q^*}\Big|\sum_{\underline{x},\underline{y}\in\mathcal{Y}}\Psi(rd(\underline{x},\underline{y}))\Big|^4 = N|\mathcal{X}|^3q^{n+1} \tag{3.2}$$

where N is the maximum number of solutions $(\underline{s},\underline{t})$ of the equation

$$\sum_{i=1}^n s_it_i = 0$$

with $\underline{s},\underline{t}\in\mathcal{Y}-\underline{y}$ with any fixed $\underline{y}\in\mathcal{Y}$.

This bound is equation (7) in [S].

Now we express $N(\mathcal{S},\mathcal{T})$ using Fourier transforms. It is easy to check that

$$N(\mathcal{S},\mathcal{T}) = \frac{|\mathcal{S}|\,|\mathcal{T}|}{q} + \frac{1}{q}\sum_{r\in\mathbb{F}_q^*}\Big|\sum_{\underline{s}\in\mathcal{S}}\sum_{\underline{t}\in\mathcal{T}}\Psi(r\underline{s}\,\underline{t})\Big|,$$

where the first term relates to $r=0$. In the rest of the proof we use another bound for the character sum than in [S]. We have

LEMMA 3.3. *Let $\mathcal{S},\mathcal{T}\subseteq\mathbb{F}_q^n$, $r\in\mathbb{F}_q^*$ and $H = |\sum_{\underline{s}\in\mathcal{S}}\sum_{\underline{t}\in\mathcal{T}}\Psi(r\underline{s}\,\underline{t})|$. Then*

$$H \le \sqrt{|\mathcal{S}|\,|\mathcal{T}|}\,q^{n/8}(E(\mathcal{S})E(\mathcal{T}))^{1/8}.$$

A similar bound can be found e.g. in [H] and in [L]. For the sake of completeness we include the short proof.

Proof of Lemma 3.3. Using the triangle inequality and the Cauchy inequality with respect to $\mathcal{S}$ we have

$$H^2 \le |\mathcal{S}|\sum_{\underline{s}\in\mathcal{S}}\Big|\sum_{\underline{t}\in\mathcal{T}}\Psi(r\underline{s}\,\underline{t})\Big|^2 = |\mathcal{S}|\sum_{\underline{s}\in\mathcal{S}}\sum_{\underline{t},\underline{t}'\in\mathcal{T}}\Psi(r\underline{s}(\underline{t}-\underline{t}')).$$

Changing the order of summation and using again the Cauchy inequality with respect to $\mathcal{T}^2$ yields

$$H^4 \le |\mathcal{S}|^2|\mathcal{T}|^2\sum_{\underline{z}\in\mathbb{F}_q^n}d_{\mathcal{T}}(\underline{z})\Big|\sum_{\underline{s}\in\mathcal{S}}\Psi(r\underline{s}\,\underline{z})\Big|^2$$

where $d_{\mathcal{T}}(\underline{z}) = |\{(\underline{t},\underline{t}')\in\mathcal{T}^2 : \underline{z} = \underline{t}-\underline{t}'\}|$.

Finally again by the Cauchy inequality with respect to $\underline{z}$ we get

$$H^8 \le |\mathcal{S}|^4|\mathcal{T}|^4 \sum_{\underline{z}\in\mathbb{F}_q^n} d_{\mathcal{T}}^2(\underline{z}) \sum_{\underline{z}\in\mathbb{F}_q^n} \Big|\sum_{\underline{s}\in\mathcal{S}} \Psi(r\underline{s}\,\underline{z})\Big|^4.$$

An easy calculation shows that $\sum_{\underline{z}\in\mathbb{F}_q^n} d_{\mathcal{T}}^2(\underline{z}) = E(\mathcal{T})$ and by orthogonality

$$\sum_{\underline{z}\in\mathbb{F}_q^n} \Big|\sum_{\underline{s}\in\mathcal{S}} \Psi(r\underline{s}\,\underline{z})\Big|^4 = q^n E(\mathcal{S}).$$

Taking the 8th root we obtain the desired bound. ∎

Now by Lemmas 3.2 and 3.3 we have

$$N \le |\mathcal{Y}|\Big(\frac{|\mathcal{Y}|^2}{q} + |\mathcal{Y}|q^{n/8}E(\mathcal{Y})^{1/4}\Big). \tag{3.3}$$

By (3.1)–(3.3) we complete the proof.

4. Concluding remarks. The energy of any given set is the same as the number of some affine cubes, called *Hilbert cubes* in the literature.

A Hilbert cube H is defined by

$$H(\underline{x}_0, \underline{a}_1, \dots, \underline{a}_d) = \Big\{\underline{x}_0 + \sum_{1\le i\le d} \varepsilon_i \underline{a}_i : \varepsilon_i \in \{0,1\}\Big\},$$

where $\underline{x}_0, \underline{a}_1, \dots, \underline{a}_d$ are any elements in $\mathbb{F}_q^n$. We say that $\dim(H) := d$ is the dimension of H.

Since $H(\underline{x}_0, \underline{a}_1, \underline{a}_2) = \{\underline{x}_0, \underline{x}_0 + \underline{a}_1, \underline{x}_0 + \underline{a}_2, \underline{x}_0 + \underline{a}_1 + \underline{a}_2\}$, we have $\underline{x}_0 + (\underline{x}_0 + \underline{a}_1 + \underline{a}_2) = (\underline{x}_0 + \underline{a}_1) + (\underline{x}_0 + \underline{a}_2)$ and thus $|\{H(\underline{x}_0, \underline{a}_1, \underline{a}_2) \subseteq \mathcal{A}\}| = E(\mathcal{A})$.

So one can ask the following

Problem 4.1. *For a given set $\mathcal{S} \subseteq \mathbb{F}_q^n$, estimate the number of Hilbert cubes with dimension d in the distance set of $\mathcal{S}$.*

We plan to investigate this question elsewhere.

Acknowledgements. The first author is supported by NKFIH (OTKA) grant K-129335, the second author is supported by the European Union, co-financed by the European Social Fund (EFOP-3.6.3-VEKOP-16-2017-00002).

References

[AS] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd ed., Wiley-Interscience, 2000.

[H] N. Hegyvári, *Some remarks on multilinear exponential sums with an application*, J. Number Theory 132 (2012), 94–102.

[HH] N. Hegyvári and F. Hennecart, *Conditional expanding bounds for two-variable functions over prime fields*, Eur. J. Combin. 34 (2013), 1365–1382.

[IR] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. 359 (2007), 6127–6142.

[L] M. Lewko, *An explicit two-source extractor with min-entropy rate near* 4/9, arXiv: 1804.05451, (2018).

[P1] T. Pham, personal communication.

[P2] T. Pham, M. Tait, L. A. Vinh and R. Won, *A structure theorem for product sets in extra special groups*, J. Number Theory 184 (2018), 461–472.

[S] I. Shparlinski, *On the additive energy of the distance set in finite fields*, Finite Fields Appl. 42 (2016), 187–199.

[SO] J. Solymosi, *Incidences and the spectra of graphs*, in: Combinatorial Number Theory and Additive Group Theory, Adv. Courses Math. CRM Barcelona, Birkhäuser, Basel, 2009, 299–314.

[V] L. A. Vinh, *Graphs generated by Sidon sets and algebraic equations over finite fields*, J. Combin. Theory Ser. B 103 (2013), 651–657.

Norbert Hegyvári, Máté Pálfy
Institute of Mathematics
Eötvös University
Pázmány St. 1/c
H-1117 Budapest, Hungary
E-mail: hegyvari@elte.hu
palfymateandras@gmail.com