INCIDENCES AND THE SPECTRA OF GRAPHS

JÓZSEF SOLYMOSI

Abstract. In this paper we give incidence bounds for arrangements of curves in $\mathbb{F}_q^2$. As an application, we prove a new result that if $(x, f(x))$ is a Sidon set then either $A + A$ or $f(A) + f(A)$ should be large. The main goal of the paper is to illustrate the use of graph spectral techniques in additive combinatorics. This is an extended version of the talks I gave in the Additive Combinatorics DocCourse held at the CRM in Barcelona and at the conference "Fete of Combinatorics" held in Keszthely.

1. Introduction

The main goal of the paper is to illustrate the use of graph spectral techniques in additive combinatorics. The problem of finding non-trivial incidence bounds on lines and curves in $\mathbb{F}_q^2$ is closely related to sum-product estimates. In the first section we will prove Garaev's sum-product bound [14] using combinatorial arguments. Such techniques were used in similar context by Vu [27] and by Vinh [26]. Vu gave incidence bounds on polynomial curves and Vinh reproved Garaev's result, an improvement on the Bourgain-Katz-Tao incidence bound for large (larger than q) sets of points and lines in $\mathbb{F}_q^2$.

In Section 3 we sketch a spectral proof for Roth's theorem, that every dense set of integers contains three-term arithmetic progressions. There are several examples where one can choose between the Fourier method or a proof based on eigenvalues. A classical example is a discrepancy theorem for arithmetic progressions by Roth [23], who used the Fourier transform. Later, Lovász and Sós proved the theorem using eigenvalues. (see in [3] or in [8] on page 20.)

In the third part of the paper we present new results. We partially answer a question of Bourgain [6], giving incidence bounds similar to Garaev's, but for a more general family of curves. It is a finite field extension of a theorem of Elekes, Nathanson, and Ruzsa. Applying Elekes' incidence method [11], Elekes, Nathanson, and Ruzsa proved in [13] the following. Let $f : \mathbb{R} \to \mathbb{R}$ be a convex function. Then for any finite set $A \subset \mathbb{R}$,

$$\max\{|A + A|, |f(A) + f(A)|\} \geq c|A|^{5/4} \tag{1}$$

The research was conducted while the author was member of the Institute for Advanced Study. Funding provided by The Charles Simonyi Endowment.

The research was supported by NSERC and OTKA grants and by Sloan Research Fellowship.

In the inequality $A+A$ denotes the set of pairwise sums, $A+A=\{a+b : a,b \in A\}$ and $f(A)=\{f(a) : a \in A\}$. We don't have the notion of a convex function in $\mathbb{F}_q$, so we will use a weaker condition on f to get results in $\mathbb{F}_q$ similar to (1).

2. The Sum-Product problem

An old conjecture of Erdős and Szemerédi states that if A is a finite set of integers then the sumset or the productset should be large. The sumset of A was defined earlier and the productset is defined in a similar way,

$$A \cdot A = \{ab | a,b \in A\}.$$

Erdős and Szemerédi conjectured that the sumset or the productset is almost quadratic in the size of A, i.e.

$$\max(|A+A|, |A \cdot A|) \geq c|A|^{2-\delta}$$

for any positive δ.

Bourgain, Katz, and Tao proved a nontrivial, $|A|^{1+\varepsilon}$, lower bound for the finite field case [5]. Let $A \subset \mathbb{F}_p$ and $p^\alpha \leq |A| \leq p^{1-\alpha}$. Then there is an $\varepsilon > 0$ depending on α only, such that

$$\max(|A+A|, |A \cdot A|) \geq c|A|^{1+\varepsilon}$$

It is important that p is prime, otherwise one could select A being a subring in which case both the product set and the sum set are small, equal to $|A|$. For the case, $\mathbb{F}_q$, where q is a power of an odd prime, the best known bound is due to Garaev [14]. It follows from a construction of Ruzsa, that his bound is asymptotically the best possible in the range $|A| \geq q^{2/3}$. Garaev's proof uses bounds on exponential sums. We are going to derive similar sum-product estimates using spectral bounds for graphs.

Sum-product bounds have important applications , not only to number theory, but to computer science, Ramsey theory, and cryptography.

2.1. **The Sum-Product graph.** The vertex set of the sum-product graph G_{SP} is the Cartesian product of the multiplicative subgroup and the field, $V(G_{SP}) = \mathbb{F}_q^* \times \mathbb{F}_q$ (as before, q is a power of an odd prime). Two vertices, $u=(a,b)$ and $v=(c,d) \in V(G_{SP})$, are connected by and edge, $(u,v) \in E(G_{SP})$, iff $ac=b+d$. This multigraph (there are a few loops) has a very special structure which makes it easy to compute the second largest eigenvalue of the graph. The set of eigenvalues are given by the eigenvalues of the adjacency matrix of the graph. The matrix is symmetric, so all $q(q-1)$ eigenvalues are real, we can order them, $\mu_0 \geq \mu_1 \geq \ldots \geq \mu_{q^2-q-1}$. The second largest eigenvalue, λ, is defined as $\lambda = \max(\mu_1, |\mu_{q^2-q-1}|)$. Using λ, one can write isoperimetric inequalities on the graph. In order to do so, we give a bound on λ. First, observe that for any two vertices, $u=(a,b)$ and

$v = (c, d) \in V(G_{SP})$, if $a \neq c$ and $b \neq d$, then the vertices have exactly one common neighbor, $N(u, v) = (x, y) \in V(G_{SP})$.

The unique solution of the system

$$\left.\begin{array}{l} ax = b + y \\ cx = d + y \end{array}\right\} \qquad \text{is given by} \qquad \begin{array}{c} x = (b - d)(a - c)^{-1} \\ 2y = x(a + c) - b - d. \end{array} \tag{2}$$

If $a = c$ or $b = d$, then the vertices, u, v, have no common neighbors. Let M denote the adjacency matrix of G_{SP}, that is $a_{ij} = 1$ if $(v_i, v_j) \in E(G_{SP})$, and $a_{ij} = 0$ otherwise. M is a symmetric matrix, moreover

$$M^2 = J + (q - 2)I - E,$$

where J is the all-one matrix, I is the identity matrix, and E is the "error matrix", the adjacency matrix of the graph, G_E, where for any two vertices, $v_i = (a, b)$ and $v_j = (c, d) \in V(G_{SP})$, $(v_i, v_j) \in E(G_E)$ iff $a = c$ or $b = d$. As G_{SP} is a $(q - 1)$-regular graph, $q - 1$ is an eigenvalue of M with the all-one eigenvector, $\overrightarrow{\mathbf{1}}$. The matrix M is symmetric, so that eigenvectors of other eigenvalues are orthogonal to $\overrightarrow{\mathbf{1}}$. It is a corollary of the Spectral Theorem, that there is an orthonormal basis, V, consisting of eigenvectors of M. Let θ denote the second largest eigenvalue of M. The graph, G_{SP}, is connected so the eigenvalue $q - 1$ has multiplicity one, and the graph is not bipartite, so for any other eigenvalue, θ, $|\theta| < q - 1$. A corresponding eigenvector is denoted by $\overrightarrow{v_\theta}$. Let us multiply both sides of the matrix equation above by $\overrightarrow{v_\theta}$. The "trick" is that $J\overrightarrow{v_\theta} = 0$, as the eigenvectors are orthogonal to the all-one vector, so we get:

$$(\theta^2 - q + 2)\overrightarrow{v_\theta} = E\overrightarrow{v_\theta}.$$

Note that E has the same set of eigenvectors as M has. G_E is a $2q - 3$-regular graph, so any eigenvalue of E is at most $2q - 3$ in absolute value.

$$\theta^2 - q + 2 \leq 2q,$$

$$|\theta| < \sqrt{3q}.$$

For illustration we show the matrices M, M^2, and E for the case when $q = 5$.

$$M = \begin{bmatrix}
0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1\\
1&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&1&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0\\
0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0\\
1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0
\end{bmatrix}$$

$$M^2 = \begin{bmatrix}
4&0&0&0&0&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1\\
0&4&0&0&0&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
0&0&4&0&0&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1\\
0&0&0&4&0&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1\\
0&0&0&0&4&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0\\
0&1&1&1&1&4&0&0&0&0&0&1&1&1&1&0&1&1&1&1\\
1&0&1&1&1&0&4&0&0&0&1&0&1&1&1&1&0&1&1&1\\
1&1&0&1&1&0&0&4&0&0&1&1&0&1&1&1&1&0&1&1\\
1&1&1&0&1&0&0&0&4&0&1&1&1&0&1&1&1&1&0&1\\
1&1&1&1&0&0&0&0&0&4&1&1&1&1&0&1&1&1&1&0\\
0&1&1&1&1&0&1&1&1&1&4&0&0&0&0&0&1&1&1&1\\
1&0&1&1&1&1&0&1&1&1&0&4&0&0&0&1&0&1&1&1\\
1&1&0&1&1&1&1&0&1&1&0&0&4&0&0&1&1&0&1&1\\
1&1&1&0&1&1&1&1&0&1&0&0&0&4&0&1&1&1&0&1\\
1&1&1&1&0&1&1&1&1&0&0&0&0&0&4&1&1&1&1&0\\
0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&4&0&0&0&0\\
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&0&4&0&0&0\\
1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&0&0&4&0&0\\
1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&0&0&0&4&0\\
1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&0&0&0&0&4
\end{bmatrix}$$

$$E = \begin{bmatrix}
0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
1&0&1&1&1&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0\\
1&1&0&1&1&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0\\
1&1&1&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
1&1&1&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&0&1&1&1&1&1&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&1&0&1&1&1&0&1&0&0&0&0&1&0&0&0\\
0&0&1&0&0&1&1&0&1&1&0&0&1&0&0&0&0&1&0&0\\
0&0&0&1&0&1&1&1&0&1&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&1&1&1&1&1&0&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&0&1&1&1&1&1&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&1&0&1&1&1&0&1&0&0&0\\
0&0&1&0&0&0&0&1&0&0&1&1&0&1&1&0&0&1&0&0\\
0&0&0&1&0&0&0&0&1&0&1&1&1&0&1&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&1&1&1\\
0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&1&1&1\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1&1&0&1&1\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&1&1&1&0&1\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0
\end{bmatrix}$$

2.2. **The spectral bound.** The small value of the second largest eigenvalue shows us that G_{SP} is a quasirandom graph and we can bound the number of edges between large vertex sets efficiently. We are going to use following Cheeger-type discrepancy bound; For any two sets of vertices, $S, T \subset V(G_{SP})$,

$$\left| e(S,T) - \frac{|S||T|}{q} \right| \leq \lambda \sqrt{|S||T|}, \tag{3}$$

where $e(S,T)$ is the number of edges between S and T. (see e.g. in [10] or [1].) Inequality (3) and the bound on λ imply that

$$e(S,T) \leq \frac{|S||T|}{q} + \sqrt{3q|S||T|}. \tag{4}$$

From (4) we can deduct Garaev's sum-product bound [14]. We can suppose that $0 \notin A$, WLOG. Set $S = (AA) \times (-A)$ and $T = (A^{-1}) \times (A + A)$. There is an edge between any two vertices $(ab, -c) \in S$ and $(b^{-1}, a + c) \in T$, therefore the number of edges between S and T is at least $|A|^3$. On the other hand

$$|A|^3 \leq e(S,T) \leq \frac{|S||T|}{q} + \sqrt{3q|S||T|} = \frac{|AA||A+A||A|^2}{q} + \sqrt{3q|AA||A+A||A|^2}.$$

After rearranging the inequality we get the desired sum-product bound.

$$|A + A||AA| \gg \min\left\{ q|A|, \frac{|A|^4}{q} \right\}.$$

In particular, if $|A| \approx q^{2/3}$, then $\max\{|AA|, |A + A|\} \gg |A|^{5/4}$.

3. 3-term arithmetic progressions

In the previous example it was enough to show that the second largest eigenvalue is small. There are cases where we can not guarantee that the second eigenvalue is small; however when it is large then we might find some structure in the graph. To illustrate this, we will sketch one of the several possible proofs of Roth's theorem [22].

Theorem 3.1 (Roth's Theorem)**.** *For any $N \geq 3$ if $S \subset [1, \dots, N]$ and $|S| \gg N/\log\log N$ then S contains a 3-term arithmetic progression.*

Note, that it is enough to prove Roth's theorem modulo a prime p. For any $p \geq 3$ if $S \subset \mathbb{F}_p$ and $|S| \gg p/\log\log p$ then S contains a 3-term arithmetic progression. Indeed, choose p that $p \geq 3N$ and translate S that it is in the middle third of the interval $[1, \dots, p]$. In this way any arithmetic progression modulo q is also a "regular" arithmetic progression.

3.2. **The 3-AP graph.** To prove the "mod p" variant, we define a graph, G_{3AP}, on $2p-1$ vertices. We label the vertices by $v_0, v_1, \dots v_{p-1}$, and $v_{-1}, v_{-2}, \dots, v_{-p+1}$., A way to think of the vertices if they were the $(2p-1)$-th roots of unity, assigning v_j to $\exp(\frac{2\pi\imath}{2p-1}j)$. The neighbors of v_0 are defined by the set S in the following way; v_i is connected to v_0 by an edge iff $|i| \in S$. (Suppose that $0 \notin S$.) Extend the graph by adding the edges necessary that the mapping, $i \mapsto i+1 \pmod{2p-1}$, is an automorphism of G_{3AP}. Using the roots of unity notation, it means that multiplying the vertices by $\exp(\frac{2\pi\imath}{2p-1}j)$ is an automorphism of the graph for any integer j. (It is the Cayley graph of $\mathbb{Z}/(2p-1)\mathbb{Z}$ with respect to S.)

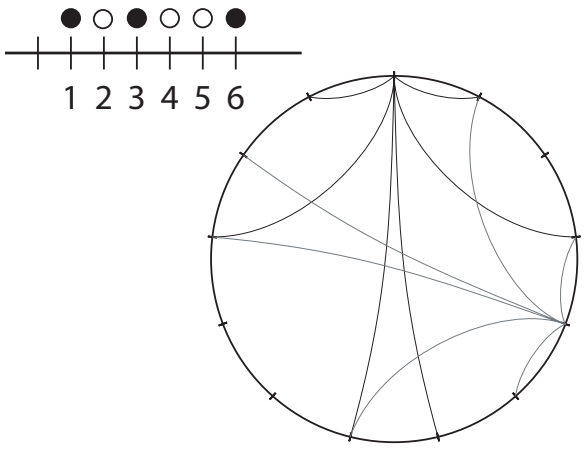

FIGURE 1. A partial drawing of G_{3AP} for the set shown.

For graphs with a "nice" automorphism group, finding the eigenvectors and eigenvalues is not a hard task. (see Exercise 8. in [18], Chapter 16 in [4], or [19] for a more detailed description) In our case it is easy to check that for this circulant

graph, $2p-1$ linearly independent eigenvectors are given by the vectors

$$\left[\exp\left(\frac{2\pi\imath k}{2p-1}\right), \exp\left(\frac{4\pi\imath k}{2p-1}\right), \exp\left(\frac{6\pi\imath k}{2p-1}\right), \dots, \exp\left(\frac{2(2p-1)\pi\imath k}{2p-1}\right)\right]^T,$$

where $0 \le k \le 2p-2$. Then the eigenvalues of G_{3AP} are given by the sums

$$\theta_k = \sum_{s\in S} \exp\left(\frac{2\pi\imath sk}{n}\right) + \sum_{s\in S} \exp\left(\frac{-2\pi\imath sk}{n}\right).$$

There are two possibilities. Either the second largest eigenvalue is large or all eigenvalues but the largest, $\mu_0 = 2|S|$, are small. In the former case, most of the summands have large positive real part. It implies that there is a long arithmetic progression having a very large intersection with S. We won't explore this case here, instead we show that if all eigenvalues are small then there is a 3-term arithmetic progression in S. The interested reader will find the details for the density increment case in Roth's original paper [22], or in one of the many books discussing Roth's theorem, like [15],[25], or [16]. Our moderate plan here is to show that if $|S|^2/(2p-1) > \lambda$ then S contains a 3AP.

We can find a relation between the assumption that S has no 3-term arithmetic progressions (it is *3AP-free*) and the structure of the graph G_{3AP}. We show that if S is 3AP-free then there are large vertex sets spanning less than expected edges. For every edge we can define its halving point. Consider the edges as arcs between points on the unit circle. The points are the vertices, represented by the roots of unity and the edges are the shorter circular arcs. The halving point of the edge is the geometric halving point of the circular arc. The number of possible halving points is $4p-2$. The number of edges is $|S|(2p-1)$, so there is a point which is the halving point of at least $\lceil |S|/2 \rceil$ edges. Note that if we had two edges sharing the same halving point, such that there is another edge between the two-two endvertices separated by the halving point, that would imply that there is a 3AP in S. (See fig. 2.)

If S is 3AP-free then between the two $\lceil |S|/2 \rceil$-size sets of endvertices, A and B, there are exactly $\lceil |S|/2 \rceil$ edges. Inequality (3) implies that

$$\left| e(A,B) - \frac{2|S| \left\lceil |S|/2 \right\rceil^2}{2p-1} \right| \le \lambda l \left\lceil |S|/2 \right\rceil,$$

from where we get that

$$\frac{|S|^2}{2p-1} \le \lambda,$$

as we wanted to show.

4. Sidon functions

In this section we extend a result of Elekes, Nathanson, and Ruzsa [13] to the finite field case.

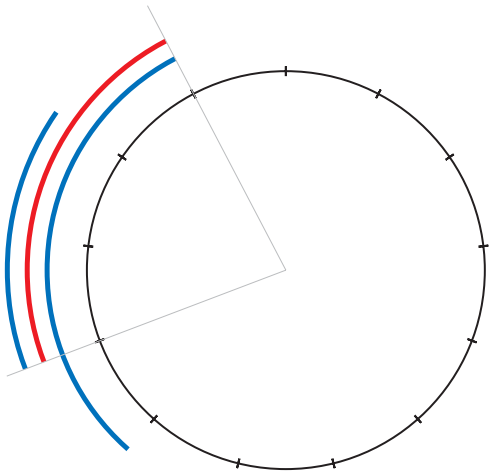

FIGURE 2. If there are two edges sharing the same halving point, h, then the endpoints of the edges can be written as $h+d_1, h-d_1$ and $h+d_2, h-d_2$. If $h+d_2$ and $h-d_1$ are connected by an edge, it means that d_1+d_2 is in S with $2d_1$ and $2d_2$, forming a 3AP.

Theorem 4.1 (Elekes, Nathanson, and Ruzsa)**.** *Let $f:\mathbb{R}\to\mathbb{R}$ be a convex function. Then for any finite set $A\subset\mathbb{R}$,*

$$\max\{|A+A|,|f(A)+f(A)|\}\geq c|A|^{5/4}$$

4.2. **Sidon functions.** We need a notation which substitutes convexity in finite fields. The graph of a convex function is a Sidon set in $\mathbb{R}^2$, this is the property we are going to use for finite fields. A set $H\subset\mathbb{F}_q\times\mathbb{F}_q$ is a *Sidon set* if for any $h_i,h_j,h_k,h_l\in H$ the equation

$$h_i-h_j\equiv h_k-h_l \pmod q$$

implies $i=k$ and $j=l$. A function, $f:S\to\mathbb{F}_q$ for some $S\subset\mathbb{F}_q$, is said to be a *Sidon function* if its graph $H=\{(x,f(x)):x\in S\}$ is a Sidon set. Note that the graph of any convex function in $\mathbb{R}^2$ forms a Sidon set.

Theorem 4.3. *For any integer, k, and for any $S\subset\mathbb{F}_q, |S|\geq q-k$, if $f:S\to\mathbb{F}_q$ is a Sidon function, then for any set $A\subset S$, and sets $B,C\subset\mathbb{F}_q$,*

$$|A+B||f(A)+C|\geq\min\left\{\frac{q|A|}{2},\frac{|A|^2|B||C|}{8(k+1)q}\right\}.$$

Using the right substitution for C and D, Theorem 4.3 gives the following corollaries.

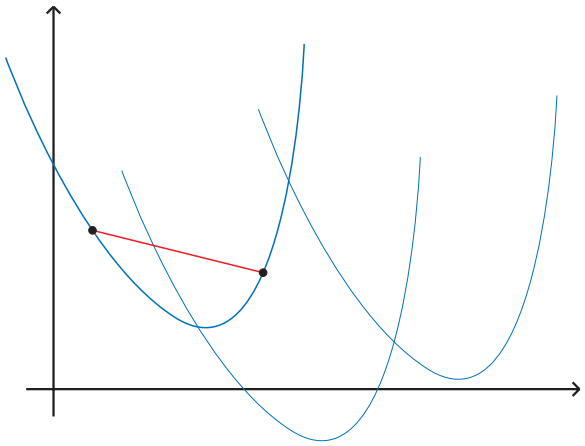

FIGURE 3. The graph of any convex function in $\mathbb{R}^2$ forms a Sidon set.

Corollary 4.4. *For any integer, k, there is a constant, $c = c(k)$, such that for any $S \subset \mathbb{F}_q, |S| \geq q - k$, if $f : S \to \mathbb{F}_q$ is a Sidon function, then for any set $A \subset S$,*

$$|A + A||f(A) + f(A)| \geq c \min \left\{ q|A|, \frac{|A|^4}{q} \right\}.$$

It is remarkable that the inequality above matches to the Elekes-Nathanson-Ruzsa bound for sets A such that $|A| \approx q^{2/3}$. It has a single term variant, which we state in a separate statement.

Corollary 4.5. *For any integer, k, there is a constant, $c = c(k)$, such that for any $S \subset \mathbb{F}_q, |S| \geq q - k$, if $f : S \to \mathbb{F}_q$ is a Sidon function, then for any set $A \subset S$,*

$$|A + f(A)| \geq c \min \left\{ \sqrt{q|A|}, \frac{|A|^2}{\sqrt{q}} \right\}.$$

4.6. **A bipartite incidence graph.** The proof of Theorem 4.3 is based on the following incidence bound. Let f be a function, $S \to \mathbb{F}_q$, for some $S \subset \mathbb{F}_q$. The *graph of* f is the set of points $\{(x, f(x)) \in \mathbb{F}_q \times \mathbb{F}_q : x \in S\}$. A translate of f by a vector $u = (u', u'') \in \mathbb{F}_q \times \mathbb{F}_q$, is the set $T_u(f) = \{(x + u', f(x) + u'') : x \in S\}$. The translate of the *mirror graph of* f is defined as $T_u(f)^\tau = \{(u' - x, u'' - f(x)) : x \in S\}$.

Lemma 4.7. *For any integer, k, and for any $S \subset \mathbb{F}_q, |S| = q - k$ if $f : S \to \mathbb{F}_q$ is a Sidon function, then for any set $P \subset \mathbb{F}_q \times \mathbb{F}_q$, the number of incidences between P and s translates of f, the set $\{T_{u_i}(f)\}_{i=1}^s, u_i = (u_i', u_i'')$, is bounded as follows;*

$$\sum_{i=1}^{s} |\{x \in S : (x + u_i', f(x) + u_i'') \in P\}| \leq \frac{|P|s}{q} + \sqrt{2(k+1)q|P|s}.$$

Proof: Define a bipartite graph, $G(A, B)$, as follows. The vertex set of G consists of two copies of $\mathbb{F}_q \times \mathbb{F}_q$.

The edges of $G(A,B)$ are given by the graph of f. Two vertices, $u=(u',u'')\in A=\mathbb{F}_q\times\mathbb{F}_q$, and $v=(v',v'')\in B=\mathbb{F}_q\times\mathbb{F}_q$, are connected by an edge in G if

$$f(v'-u')=v''-u''. \tag{5}$$

The neighborhood of a vertex $u\in A$ is given by $N(u)=T_u(f)\subset B$, and neighborhood of a vertex $u\in B$ is described by $N(v)=T_v(f)^\tau\subset A$. The graph, $G(A,B)$, is a $(q-k)$-regular bipartite graph. The spectra of $G(A,B)$ is symmetric. For this graph the second largest eigenvalue is defined as $\lambda=\mu_1$. As the graph is $(q-k)$-regular, the largest and the smallest eigenvalues are $q-k$ and $k-q$. Similarly as we did in the sum-product example, we can bound λ by examining the $q^2\times q^2$ adjacency matrix of $G(A,B)$, denoted by M. The function f is a Sidon function, therefore the neighborhoods of two vertices in A or in B intersect in at most one vertex. A translate, $T_u(f)$, covers $\binom{q-k}{2}$ vertex pairs. All translates (the neighborhoods of vertices) cover $2\binom{q-k}{2}q^2$ pairs out of the $2\binom{q^2}{2}$ vertex pairs in A and in B. Let us define an error graph, H, which has two components, one in A and one in B, and two vertices, u and v are connected by an edge iff there is no vertex connected to both in $G(A,B)$. The error graph, H, has $2(\binom{q^2}{2}-q^2\binom{q-k}{2})$ edges and it is regular of degree $q^2-1-(q-k)(q-k-1)$. Its adjacency matrix is denoted by E.

$$M^2=\begin{bmatrix} J & 0\\ 0 & J\end{bmatrix}+(q-k-1)I-E.$$

As in the first example, we can multiply the equation by an eigenvector of M, which belongs to the second largest eigenvalue.

$$E\overrightarrow{v_\lambda}=(q-k-1-\lambda^2)\overrightarrow{v_\lambda}.$$

We know that H is $(2kq+q-k^2-k-1)$-regular, therefore any eigenvalue of E is less or equal to $2kq+q-k^2-k-1$.

$$|q-k-1-\lambda^2|\le 2kq+q-k^2-k-1,$$

so

$$\lambda<\sqrt{2(k+1)q}.$$

4.8. **The spectral bound.** For bipartite graphs, like $G(A,B)$, inequality (3) is slightly different. If $G(A,B)$ is a r-regular bipartite graph on n vertices, then for any subsets $A'\subset A$ and $B'\subset B$,

$$\left|e(A',B')-\frac{2r|A'||B'|}{n}\right|\le\lambda\sqrt{|A'||B'|}.$$

Now we are ready to complete the proof of Lemma 4.7, to state a bound on incidences between a set of points, P, and s translates, $\{T_{u_i}(f)\}_{i=1}^s, u_i=(u_i',u_i'')$. An edge in the graph $G(A,B)$ represents an incidence between a point and a translate.

$$\sum_{i=1}^{s}|\{x\in S:(x+u_i',f(x)+u_i'')\in P\}|\le\frac{|P|s}{q}+\sqrt{2(k+1)q|P|s}.$$

□

Proof of Theorem 4.3: Let us consider the Cartesian product $(A+B)\times(f(A)+C)$. It has $|B||C|$ translates of the smaller product $A\times f(A)$, which contains an $|A|$-element subset of the graph of f. The $|B||C|$ translates determine $|A||B||C|$ incidences in $(A+B)\times(f(A)+C)$. Now we apply Lemma 4.7 with substitutions $s=|B||C|$, $|P|=|A+B||f(A)+C|$, and with $|A||B||C|$ incidences. □

Note that Theorem 4.3 generalizes Garaev's point-line incidence bound, since the mapping $(x,y)\mapsto(x,y+x^2)$ maps any line, $ax+by=c, a\neq 0$, to a translate of the parabola, $y=x^2$, which is a Sidon function.

For any set $P\subset\mathbb{F}_q\times\mathbb{F}_q$, the number of incidences between P and s lines is bounded by

$$O\left(\frac{|P|s}{q}+\sqrt{q|P|s}\right). \tag{6}$$

5. Incidence Bounds on Pseudolines

Incidence bounds in geometries have various applications. The celebrated theorem of Szemerédi and Trotter [24] gives sharp incidence bound for the number of point-line incidences in the Euclidean plane. The Szemerédi-Trotter Theorem was extended to pseudolines. For the details about variants of the planar Szemerédi-Trotter theorem we refer to [21].

Our goal here is finding non-trivial incidence bounds for pseudolines in $\mathbb{F}_q^2$. First we give a definition of pseudolines which form a partial geometry in $\mathbb{F}_q^2$. The incidence graph will be a strongly regular graph, therefore we can use standard spectral bounds to estimate incidences.

5.1. **The incidence bound.**

The following is a standard, (however not the only) definition of pseudolines in the Eucledean plane, see in e.g. [2].

A collection $\mathcal{L}$ of x-monotone unbounded Jordan curves in the plane is called a family of pseudolines if every pair of curves intersects in at most one point.

To find a proper definition of pseudolines in finite fields isn't so straightforward. We are going to use one possible definition which has interesting applications. Instead of x-monotone unbounded Jordan curves we consider "lines", $l_i=\{(x,f(x)) : x\in\mathbb{F}_q\}$, where $f:\mathbb{F}_q\to\mathbb{F}_q$.

Definition 5.2. A collection $\mathcal{L}$ of subsets of $\mathbb{F}_q^2$, $\mathcal{L}=\{l_1,l_2,\dots,l_k\}$ is called a family of pseudolines if the following conditions hold

a, For every $a\in\mathbb{F}_q$, any set, l_i, has exactly one point with x-coordinate a.
b, Every pair of sets, l_i and l_j, intersects in at most one point.
c, If $l_i\in\mathcal{L}$, then its y-translates are also in the arrangement, $l_i+(0,a)\in\mathcal{L}$ for any $a\in\mathbb{F}_q$.

The last condition implies that the size of a family of pseudolines is divisible by q.

Theorem 5.3. *Let a family of pseudolines, $\mathcal{L}$, and a family of points, P, in $\mathbb{F}_q^2$ be given. Suppose that $|\mathcal{L}| = kq$, and $|P| = n$. Then the number of incidences between m pseudolines and n points is bounded by*

$$I(m,n) \leq n\sqrt{km/q} + \sqrt{qnm}.$$

The incidence bound for pseudolines implies a new bound on point line incidences. It is better than inequality 6 in line arrangements with a few distinct slopes only.

Corollary 5.4. *Let a family of pseudolines, $\mathcal{L}$, and a family of points, P, in $\mathbb{F}_q^2$ be given. Suppose that the lines have no more than k different slopes. Then the number of incidences between the s lines and points of P is bounded by*

$$I(s,|P|) \leq |P|\sqrt{ks/q} + \sqrt{q|P|s}.$$

The bound is better than inequality (6) if $k < s/q$. To see how Theorem 5.3 implies Corollary 5.4, observe that the set all lines with slopes from a given set, forms a family of pseudolines.

The incidence bound in Theorem 5.3 is a corollary of the following statement which is proved in the next subsection.

Theorem 5.5. *Given a family of pseudolines, $\mathcal{L}$, and two sets of points, P_1 and P_2 in $\mathbb{F}_q^2$. Suppose that $|\mathcal{L}| = kq$, $|P_1| = n_1$, and $|P_2| = n_2$. Then the number of collinear pairs in $P_1 \times P_2$ is bounded as*

$$|\{(p_i,p_j) : p_i \in P_1, p_j \in P_2, \exists \ell \in \mathcal{L} : p_i, p_j \in \ell\}| \leq \frac{kn_1n_2}{q} + q\sqrt{n_1n_2}.$$

Proof of Theorem 5.3: Suppose that the m pseudodolines are incident to $t_1, t_2, \dots, t_m$ points in P. Then, the number of copseudolinear pairs in P is at least $\sum_{i=1}^m \binom{t_i}{2}$. On the other hand, $I(m,n) = \sum_{i=1}^m t_i$, so the number of copseudolinear pairs is at least $m\binom{I(m,n)/m}{2} \sim I(m,n)^2/m$. Using the inequality from Theorem 5.5 we have

$$\frac{I(m,n)^2}{m} \leq \frac{kn^2}{q} + qn,$$

concluding the proof of Theorem 5.3. □

5.6. **Strongly regular graphs.** In [7] Bose introduced the notation of partial geometries. A set of points and lines is a finite partial geometry if there are integers such that:

i For each two different points p and q, there is at most one line incident with both of them.
ii Each line is incident with $r+1$ points.
iii Each point is incident with $s+1$ lines.
iv If a point p and a line L are not incident, then there are exactly t points on L collinear to p.

Lemma 5.7. *Any family of pseudolines is a partial geometry.*

The easy proof is left to the reader.

Proof of Theorem 5.5: The incidence graph, $G(\mathcal{L})$, of a family of pseudolines is defined as follows. G has q^2 vertices, the elements of $\mathbb{F}_q^2$. Two vertices v and u are connected iff the points are collinear, i.e. there is a line, $l \in \mathcal{L}$, such that $v, u \in l$. As we observed earlier, the number of lines is divisible by q. There is an integer, k, $1 \leq k \leq q$, such that $|\mathcal{L}| = kq$.

$G(\mathcal{L})$ is a strongly regular graph, where each vertex has degree $k(q-1)$. Two collinear (adjacent) vertices have $q - 2 + (k-1)(k-2) = q + k^2 - 3k$ common neighbors and non-adjacent vertices have $k^2 - k$ common neighbors. The adjacency matrix of the graph is denoted by A.

$$A^2 = (q + k^2 - 3k)A + (k^2 - k)(J - A - I) + k(q-1)I.$$

The usual trick - multiplying both sides by an eigenvector - helps us to find the eigenvalues. The adjacency matrix of this graph has only three distinct eigenvalues. The largest is $k(q-1)$ and the other two are $q-k$ and $-k$. (For more details about such graphs we refer to [17].) In our applications $q \gg k$, so the second largest eigenvalue is $q-k$. From this, Theorem 5.5 follows immediately by applying inequality (3). □

6. Acknowledgement

I am indebted to the anonymous referee for his valuable comments on my previous draft.

References

[1] N. Alon and J. Spencer, The Probabilistic Method, Wiley, 3rd. ed. 2008.
[2] P.K. Agarwal and M. Sharir, Pseudoline Arrangements: Duality, Algorithms, and Applications, 2001
[3] J. Beck and V.T. Sós, Discrepancy theory, in Handbook of Combinatorics, Chapter 26, eds., Graham, Grötschel, Lovász, North-Holland, 1995, 1405–1446.
[4] N. Biggs, Algebraic Graph Theory, Cambridge University Press, 1974, 1993.
[5] J. Bourgain,N. Katz, and T. Tao, A sumproduct estimate in finite fields and applications, GAFA 14 (2004), 27-57.
[6] J. Bourgain, (personal communication, October 10, 2007)
[7] R.C. Bose, Strongly regular graphs, partial geometries and partially balanced designs. Pacific J. Math. Volume 13, Number 2 (1963), 389–419.
[8] B. Chazelle, The Discrepancy Method: Randomness and Complexity, Cambridge University Press, 2000.
[9] J. Cheeger, A lower bound for the smallest eigenvalue of the Laplacian, Problems in Analysis, Papers dedicated to Salomon Bochner, 1969, Princeton University Press, Princeton, 195-199.
[10] F.R.K. Chung, Spectral Graph Theory. Providence, RI: American Mathematical Society. no 92. (1997).

[11] Gy. Elekes, On the Number of Sums and Products, Acta Arithmetica LXXXI.4, (1997) 365–367.
[12] P. Erdős and E. Szemerédi, On sums and products of integers, *Studies in pure mathematics,* 213–218, Birkhuser, Basel, 1983.
[13] Gy. Elekes, M. B. Nathanson, and I. Z. Ruzsa, Convexity and Sumsets, Journal of Number Theory 83, 194–201 (1999)
[14] M.Z. Garaev, An Explicit Sum-Product Estimate in $\mathbb{F}_q$, International Mathematics Research Notices (2007) Vol. 2007, 1–11.
[15] R. Graham, B. Rothschild, and J. Spencer, Ramsey Theory, Wiley-Interscience Series in Discrete Mathematics, second ed. (1990),
[16] A. Granville, M.B. Nathanson, and J. Solymosi, Additive Combinatorics, CRM Proceedings & Lecture Notes, AMS, vol 43 (2007)
[17] C. Godsil and G. Royle, Algebraic Graph Theory, §10 Strongly Regular Graphs, Springer, Graduate Text in Mathematics, 207. (2001)
[18] L. Lovász, Combinatorial problems and exercises, AMS Chelsea Publishing, 1979; 639 pp;
[19] L. Lovász, Spectra of graphs with transitive groups, Periodica Mathematica Hungarica Vol. 6 (2), (1975), 191–195.
[20] L. Lovász, J. Spencer, and K. Vesztergombi, Discrepancy of set systems and matrices, European J. Combinatorics 7 (1986), 151–160.
[21] J. Pach and P. Agarwal, Combinatorial Geometry, Wiley, New York, 1995.
[22] K.F. Roth, On certain sets of integers, I, *Journal of the London Mathematical Society* 28, (1953), 104-109.
[23] K.F. Roth, Remark concerning integer sequences, Acta Arithmetica 9, (1964) 257–260.
[24] E Szemerédi and W.T Trotter, Extremal problems in discrete geometry, Combinatorica 3 (1983), 381–392.
[25] T. Tao and V. Vu, Additive Combinatorics, Series: Cambridge Studies in Advanced Mathematics (No. 105) Cambridge University Press (2006).
[26] L.A. Vinh, Szemeredi-Trotter type theorem and sum-product estimate in finite fields, preprint. arXiv:0711.4427v1 [math.CO]
[27] V.H. Vu, Sum-product estimates via directed expanders, Math. Res. Lett. 15 (2008), no. 2, 375-388.

Department of Mathematics, UBC, 1984 Mathematics Road, Vancourver, BC, Canada V6T 1Z2

E-mail address: solymosi@math.ubc.ca