

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,

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

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  $\delta$ .

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  $\alpha$  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 an 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,  $\mu_0 \geq \mu_1 \geq \dots \geq \mu_{q^2-q-1}$ . The second largest eigenvalue,  $\lambda$ , is defined as  $\lambda = \max(\mu_1, |\mu_{q^2-q-1}|)$ . Using  $\lambda$ , one can write isoperimetric inequalities on the graph. In order to do so, we give a bound on  $\lambda$ . 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

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

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,  $\vec{\mathbf{1}}$ . The matrix  $M$  is symmetric, so that eigenvectors of other eigenvalues are orthogonal to  $\vec{\mathbf{1}}$ . It is a corollary of the Spectral Theorem, that there is an orthonormal basis,  $V$ , consisting of eigenvectors of  $M$ . Let  $\theta$  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,  $\theta$ ,  $|\theta| < q - 1$ . A corresponding eigenvector is denoted by  $\vec{v}_\theta$ . Let us multiply both sides of the matrix equation above by  $\vec{v}_\theta$ . The "trick" is that  $J\vec{v}_\theta = 0$ , as the eigenvectors are orthogonal to the all-one vector, so we get:

$$(\theta^2 - q + 2)\vec{v}_\theta = E\vec{v}_\theta.$$

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.

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

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



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

**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,  $S, T \subset V(G_{SP})$ ,

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

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  $\lambda$  imply that

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

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  $\max\{|AA|, |A + A|\} \gg |A|^{5/4}$ .