PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 2, February 2013, Pages 461–473
S 0002-9939(2012)11338-3
Article electronically published on June 19, 2012

FOURIER ANALYSIS AND EXPANDING PHENOMENA IN FINITE FIELDS

DERRICK HART, LIANGPAN LI, AND CHUN-YEN SHEN

(Communicated by Matthew A. Papanikolas)

Abstract. In this paper we study set expansion in finite fields. Fourier analytic proofs are given for several results recently obtained by other authors using spectral graph theory. In addition, several generalizations of these results are given.

In the case that A is a subset of a prime field $\mathbb{F}_p$ of size less than $p^{1/2}$ it is shown that $|\{a^2+b : a, b \in A\}| \geq C_1|A|^{147/146}$ and $|\{\frac{b+1}{a} : a, b \in A\}| \geq C_2|A|^{110/109}$, where $|\cdot|$ denotes the cardinality of a set and C_1 and C_2 are absolute constants.

1. Introduction

Given a finite set Θ of maps $\{f_i : X^d \to Y\}_{i=1}^m$, we say that Θ is a d-dimensional expander from X^d to Y with expansion index $\kappa > 1$ if

$$\max_{1\leq i\leq m} \left|f_i(A^d)\right| \geq C_\kappa |A|^\kappa$$

for all finite subsets $A \subset X$ possibly under some structural or density assumptions. Several classical problems in additive and geometric combinatorics deal with showing that certain sets of polynomials have the expander property. For example, Erdős and Szemerédi [8] conjectured in 1983 that given a set $A \subset \mathbb{Z}$ that either the size of the sum-set $A + A$ or the size of of the product-set $A \cdot A$ is essentially quadratically large, that is

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

and proved that

$$\max(|A+A|,\ |A\cdot A|) \geq C_\kappa |A|^{\kappa},$$

for some $\kappa \in (1, 2)$, which means in the expansion language that $\{x_1 + x_2, x_1x_2\}$ is a two-dimensional expander from $\mathbb{Z}^2$ to $\mathbb{Z}$. Explicit bounds on the expansion index κ later were given by Nathanson ([19]), Ford ([9]), Elekes ([6]) and Solymosi ([26]). The best-known bound, due to Solymosi ([28]), is given by

$$\max(|A+A|,\ |A\cdot A|) \geq \frac{|A|^{4/3}}{2\lceil\log_2|A|\rceil^{1/3}}.$$

A similar sum-division estimate obtained by Shen and the second author ([17]) states that $\max(|A+A|, |A/A|) \geq \frac{|A|^{4/3}}{2}$.

Received by the editors April 10, 2011 and, in revised form, July 4, 2011.
2010 *Mathematics Subject Classification.* Primary 11B75.
Key words and phrases. Sums, products, expanding maps, character sums.

The sum-product problems also have been explored in the context of a variety of rings. In the case of finite fields $\mathbb{F}_q$, the problem becomes more complicated due to the fact that one may not rely on the topological properties of the real numbers. It is known, however, via ground breaking work in [3] that in a prime field $\mathbb{F}_p$, for any $\epsilon \in (0, 1)$, there exists a $\kappa > 1$ such that for all $A \subset \mathbb{F}_p$ with $|A| \leq p^{1-\epsilon}$,

$$\max(|A + A|,\ |A \cdot A|) \geq C_\epsilon |A|^\kappa.$$

This bound was given via combinatorial means and did not yield a precise relationship between κ and ϵ. In [14] the first author, along with Iosevich and Solymosi, used Fourier analysis to develop incidence theory between points and hyperbolas in $\mathbb{F}_q^2$, the two-dimensional vector space over $\mathbb{F}_q$. This led to, for the first time, a concrete value of κ, for $|A| > q^{1/2}$. This bound on $|A|$ is natural in finite fields which are not necessarily prime fields where subfields of size $q^{1/2}$ give the trivial bound. Later a pioneering work by Garaev ([10]) gives explicit bounds for all ranges of $|A|$ in prime fields.

For a variant of sum-product problems, Solymosi ([27]) applied spectral graph theory to obtain the following bounds:

$$\max(|A + B|,\ |f(A) + C|) \geq M \cdot \min(|A|^{1/2}q^{1/2},\ |A||B|^{1/2}|C|^{1/2}q^{-1/2}),$$

for a class of functions f, where A, B, C are subsets of $\mathbb{F}_q$ and M is a universal constant depending only on the degree of f. Setting $B = f(A)$ and $C = A$ immediately gives a Garaev-type ([11]) estimate $|A + f(A)| \geq \widetilde{M} \cdot \min(|A|^{1/2}q^{1/2}, |A|^2q^{-1/2})$, which in turn implies that $x_1 + f(x_2)$ is a two-dimensional expander for "large subsets"; here and afterwards, a subset of a finite field is called large or small if the square of its size is greater than or less than that of the finite field. This result is analogous to the work done by Elekes, Nathanson and Ruzsa ([7]) in the real numbers. However it was shown later in [4] that the class of functions f in the above estimates only contains quadratic polynomials.

In [31] Vu used spectral graph theory to classify the polynomials $f(x_1, x_2)$ for which if $|A + A|$ is small, then $|f(A, A)|$ is large. Specifically, it was shown that if f is a "nondegenerate" polynomial, then

$$\max(|A + A|,\ |f(A, A)|) \geq M \cdot \min(|A|^{2/3}q^{1/3},\ |A|^{3/2}q^{-1/4});$$

as before, M is a universal constant depending only on the degree of f. This result means that $\{x_1 + x_2, f(x_1, x_2)\}$ is a two-dimensional expander for large subsets (also see [23] for the same problem in a real setting).

In this paper, we shall mainly use Fourier analytic methods to study set expansion phenomena for large subsets in finite fields. In particular, we develop an incidence bound between points and polynomial curves in finite fields which is analogous to the main result in ([7]). Our incidence bounds not only give us nontrivial results on the sum-product problems for a very general class of functions, but also give us nontrivial lower bounds on the mixed-operations sum-product problems (see section 2.2 for details). We also use Fourier analytic methods to give a new proof for the generalized Erdős distance problem studied by Vu ([31]).

In prime fields it follows from the result of Glibichuk and Konyagin ([13]) that for $|A| \leq p^{1/2}$ one has that $|A \cdot A + A| \geq C|A|^{7/6}$. This shows that $x_1x_2 + x_3$ is a three-dimensional expander for small subsets. Bourgain ([1]) answered Widgerson's two-variable expander construction problem, especially showing that $x_1(x_1 + x_2)$ and $x_1(x_2 + 1)$ are two-variable expanders. However, Bourgain did not give explicit expansion indexes. In the latter case, Garaev and the third listed author ([12]) showed that the expansion index could be taken to be $106/105+o(1)$. On the other hand, from the work of Pudlák ([21]) or a private communication with Croot ([5]), we know that when $|A| \le p^{1/2}$ with p prime, then $|\{x+y^2 : x, y \in A\}| \ge C_\kappa |A|^\kappa$ for some $\kappa > 1$. Pudlák's proof relied on the finite field Szemerédi-Trotter incidence theorem while Croot's one relied on the classical version of the Balog-Szemerédi-Gowers theorem; thus no explicit expansion index has been determined yet. In this paper we shall for the first time provide a concrete expansion index for $x+y^2$.

Throughout this paper we will write $X \lesssim Y$ to mean $X \le CY$, where C is a universal constant, which may vary from line to line but is always universal. We will use $X \lessapprox Y$ to mean $X \lesssim C(\log|A|)^\alpha Y$. It is also clear that when the quantities X, Y have $f(A)$ involved for some polynomial f, the implied constant may also depend on the degree of f.

2. Sum-product estimates for large sets

Let $\mathbb{G}^d = G_1 \times \cdots \times G_d$, where $G_i \in \{\mathbb{F}_q, \mathbb{F}_q^*\}$ and the group operation $\odot$ is inherited from each coordinate group. Define the Fourier transform of any given function $f : \mathbb{G}^d \to \mathbb{C}$ by

$$\widehat{f}(\chi) = |\mathbb{G}^d|^{-1} \sum_{x \in \mathbb{G}^d} f(x)\overline{\chi}(x),$$

where $\chi = (\chi_1, \ldots, \chi_d)$ and χ_j denotes the additive or multiplicative character corresponding to G_j and by the function $\chi(x)$ we mean $\chi_1(x_1)\cdots\chi_d(x_d)$.

We also define the convolution of functions f, g by

$$(f * g)(x) = \sum_{y \in \mathbb{G}^d} f(y) g(x \odot y^{-1}),$$

where y^{-1} is the inverse of y in $\mathbb{G}^d$. Then the following are easy to verify:

$$f(x) = \sum_\chi \chi(x)\widehat{f}(\chi), \tag{2.1}$$

$$\widehat{f * g}(\chi) = |\mathbb{G}^d|\widehat{f}(\chi)\widehat{g}(\chi), \tag{2.2}$$

$$\sum_x f(x)\overline{g(x)} = |\mathbb{G}^d| \sum_\chi \widehat{f}(\chi)\overline{\widehat{g}(\chi)}. \tag{2.3}$$

Define ([29]) the uniformity norm (or *Fourier bias*) of f by

$$\|f\|_u = \max_{\chi \ne \chi^0} |\widehat{f}(\chi)|,$$

where by χ^0 we mean $(\chi_1^0, \ldots, \chi_d^0)$ for χ_j^0 the trivial character of the coordinate group. We first give a modified version of a lemma of Solymosi ([27]).

Lemma 2.1. *Suppose that $X, Y, P \subset \mathbb{G}^d$. Then*

$$\big||\{(x,y) \in X \times Y : x \odot y \in P\}| - |X||Y||P||\mathbb{G}^d|^{-1}\big| \le \|X\|_u \sqrt{|Y||P|}|\mathbb{G}^d|.$$

Proof. Since

$$\begin{aligned}|\{(x,y)\in X\times Y : x\odot y\in P\}| &= \sum_z (X*Y)(z)P(z)\\ &= |\mathbb{G}^d|\sum_\chi \widehat{X*Y}(\chi)\overline{\widehat{P}(\chi)}\\ &= |\mathbb{G}^d|^2\sum_\chi \widehat{X}(\chi)\widehat{Y}(\chi)\overline{\widehat{P}(\chi)},\end{aligned}$$

we have

$$\begin{aligned}\big||\{(x,y)\in X\times Y : x\odot y\in P\}| - |X||Y||P||\mathbb{G}^d|^{-1}\big| &\le |\mathbb{G}^d|^2\sum_{\chi\neq\chi^0}|\widehat{X}(\chi)\widehat{Y}(\chi)\overline{\widehat{P}(\chi)}|\\ &\le |\mathbb{G}^d|^2\|X\|_u\sum_{\chi\neq\chi^0}|\widehat{Y}(\chi)||\widehat{P}(\chi)|,\end{aligned}$$

which in turn by Cauchy-Schwarz and Plancherel is $\le |\mathbb{G}^d|\|X\|_u\sqrt{|Y||P|}$. □

We say that a set F is Salem with constant C if

$$\|F\|_u \le C\sqrt{|F|}|\mathbb{G}^d|^{-1}.$$

Let $P = X\odot Y$, where X is a subset of a Salem set $\tilde{X}$ with constant C. Then one has that

$$|X||Y| \le |\{(x,y)\in \widetilde{X}\times Y : x\odot y\in P\}| \le |\tilde{X}||Y||X\odot Y||\mathbb{G}^d|^{-1} + C\sqrt{|\tilde{X}||Y||X\odot Y|}.$$

This gives the following theorem.

Theorem 2.2. *Suppose $X\subset\mathbb{G}^d$ is a subset of a Salem set $\tilde{X}$ with constant C. Then for any $Y\subset\mathbb{G}^d$ one has that*

$$|X\odot Y| \ge \min(|\mathbb{G}^d||X||\tilde{X}|^{-1},\ C^{-2}|X|^2|Y||\tilde{X}|^{-1}).$$

Remark 2.3. This theorem can be viewed as a finite field version of the main theorem in [7] by Elekes, Nathanson and Ruzsa, in which the authors investigated the incidences between points and convex curves in the real plane, and applied the incidence bound to show that $|S+T| \gtrsim \min(|S||T|, |S|^{3/2}|T|^{1/2})$ for any finite subset S of a strictly convex curve in $\mathbb{R}^2$, while T is arbitrary.

2.1. **Salem sets.** Let $\mathbb{F}_q$ be a finite field with characteristic p, and $Tr : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function. It is well known ([18]) that the function $\widetilde{\chi}$ defined by

$$\widetilde{\chi}(c) = \exp(2\pi i Tr(c)/p) \quad (c\in\mathbb{F}_q)$$

is a character of the additive group of $\mathbb{F}_q$, and every additive character χ of $\mathbb{F}_q$ is of the form $\chi(c) = \widetilde{\chi}(bc)$ for some $b\in\mathbb{F}_q$. Note also that the group of multiplicative characters of $\mathbb{F}_q$ is a cyclic group. Denote by $N(f)$ the number of distinct roots of $f\in\mathbb{F}_q[x]$ in its splitting field over $\mathbb{F}_q$. Then it is easy to see that $N(f^ig^j)\le N(f)+N(g)$ for any $i,j\ge 0$.

The classical bound due to Weil as well as its generalization for mixed character sums may be used to show that certain sets $\tilde{X}$ defined by polynomials are Salem.

Theorem 2.4 (Weil's Bound [18, 20])**.** *Let χ be a nontrivial additive character of $\mathbb{F}_q$ and ψ be a nontrivial multiplicative character of $\mathbb{F}_q$ of order s.*

(1) *Suppose that* $f \in \mathbb{F}_q[x]$ *satisfies* $gcd(deg(f), q) = 1$. *Then we have*

$$\Big| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \Big| \le (deg(f) - 1)\sqrt{q}.$$

(2) *Suppose that* $g \in \mathbb{F}_q[x]$ *is not, up to a nonzero multiplicative constant, an* s*-th power of a polynomial in* $\mathbb{F}_q[x]$. *Then for any* $f \in \mathbb{F}_q[x]$ *we have*

$$\Big| \sum_{x \in \mathbb{F}_q} \chi(f(x))\psi(g(x)) \Big| \le (deg(f) + d - 1)\sqrt{q},$$

where d *is the number of distinct roots of* g *in its splitting field over* $\mathbb{F}_q$. *Particularly, taking* f *to be some constant function, we get*

$$\Big| \sum_{x \in \mathbb{F}_q} \psi(g(x)) \Big| \le (d - 1)\sqrt{q}.$$

Corollary 2.5. *Let* p *be the characteristic of* $\mathbb{F}_q$. *Suppose* $f, g \in \mathbb{F}_q[x]$ *with* $M \doteq deg(f) + deg(g) < p$ *and define* $F = \{(f(x), g(x)) \in \mathbb{G}^2\}$.

(1) *Let* $\mathbb{G}^2 = \mathbb{F}_q \times \mathbb{F}_q$ *and suppose* $1 \le deg(f) < deg(g)$. *Or,*
(2) *Let* $\mathbb{G}^2 = \mathbb{F}_q \times \mathbb{F}_q^*$ *and suppose* $gcd(deg(g), q - 1) = 1$. *Or,*
(3) *Let* $\mathbb{G}^2 = \mathbb{F}_q^* \times \mathbb{F}_q^*$. *Suppose* f *contains some irreducible factors that are not factors of* g *such that the great common divisor of the powers of these factors in the canonical factorization of* f *is* 1, *and vice versa.*

Then F *is a Salem set with constant* M.

Proof.

Case 1. Suppose $(\chi_1, \chi_2) \neq (\chi^0, \chi^0)$. There exist $b_1, b_2 \in \mathbb{F}_q$, not all b_i equal to zero, such that

$$\chi_1(c) = \widetilde{\chi}(b_1 c), \quad \chi_2(c) = \widetilde{\chi}(b_2 c).$$

Thus

$$\widehat{F}(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(f(x))\chi_2(g(x)) = \sum_{x \in \mathbb{F}_q} \widetilde{\chi}(b_1 f(x) + b_2 g(x)).$$

Since $(b_1, b_2) \neq (0, 0)$ and $1 \le deg(f) < deg(g)$, we have that $b_1 f(x) + b_2 g(x)$ is a polynomial of positive degree $\le \max\{deg(f), deg(g)\} \le M$. By Theorem 2.4(1), F is a Salem set with constant M.

Case 2. Suppose $(\chi, \psi) \neq (\chi^0, \psi^0)$ and let $\widetilde{\psi}$ be one of its generators of the group of multiplicative characters of $\mathbb{F}_q$. If $\psi = \psi^0$, then by Theorem 2.4(2) we are done since $M < p$. Next suppose $\psi \neq \psi^0$. Thus there exists $1 \le k \le q - 2$ such that $\psi = (\widetilde{\psi})^k$. Thus

$$\widehat{F}(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(f(x))\psi(g(x)) = \sum_{x \in \mathbb{F}_q} \chi(f(x))\widetilde{\psi}(g^k(x)).$$

Since $1 \le k \le q - 2$ and $gcd(deg(g), q - 1) = 1$, g^k could not be a $(q-1)$-th power of a polynomial. By Theorem 2.4(2), F is a Salem set with constant M.

Case 3. By assumption, we may write

$$f = Q_1^{a_1} Q_2^{a_2} \cdots Q_s^{a_s} P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n},$$
$$g = R_1^{b_1} R_2^{b_2} \cdots R_t^{b_t} P_1^{f_1} P_2^{f_2} \cdots P_n^{f_n},$$

where $Q_1, \cdots, Q_s$, $P_1, \cdots, P_n$, $R_1, \cdots, R_t$ all are distinct irreducible polynomials, $e_i, f_i \geq 0$, $gcd(a_1, \cdots, a_s) = gcd(b_1, \cdots, b_m) = 1$. Now suppose $(\psi_1, \psi_2) \neq (\psi^0, \psi^0)$. Following the notation used in Case (2), we may write $\psi_1 = (\widetilde{\psi})^k$, $\psi_2 = (\widetilde{\psi})^j$, $0 \leq k, j \leq q-2$, $k + j > 0$. Thus

$$\widehat{F}(\psi_1, \psi_2) = \sum_{x \in F_q} \psi_1(f(x))\psi_2(g(x)) = \sum_{x \in F_q} \widetilde{\psi}(f(x)^k g(x)^j).$$

Suppose $f^k g^j$ could be a $(q-1)$-th power of a polynomial. Then for all $i \leq s, m \leq t$ we have

$$(q-1)|ka_i, \quad (q-1)|jb_m.$$

Thus

$$(q-1)|gcd(ka_1, \cdots, ka_s) = k, \quad (q-1)|gcd(jb_1, \cdots, jb_m) = j,$$

which implies $j = k = 0$, a contradiction. Therefore by Theorem 2.4(3), F is a Salem set with constant M. □

2.2. **Sum-product estimates.** Let p be the characteristic of $\mathbb{F}_q$ and $f, g \in \mathbb{F}_q[x]$. Let $F = \{(f(x), g(x)) \in \mathbb{G}^2\}$. For A, B, C subsets of $\mathbb{F}_q$ we let $X = \{(f(x), g(x)) \in \mathbb{G}^2 : x \in A\}$, $\tilde{X} = F$ and $Y = B \times C$. Then combining Theorem 2.2 with Corollary 2.5 gives the following generalization (at least if one's attention is restricted to polynomials of integer coefficients) of Solymosi ([27]).

Theorem 2.6. *Let p be the characteristic of $\mathbb{F}_q$ and $f, g \in \mathbb{F}_q[x]$.*

(1) *If $1 \leq deg(f) < deg(g) < p$, then*

$$|f(A) + B||g(A) + C| \gtrsim \min(|A|q, |A|^2|B||C|q^{-1}).$$

Particularly, one has

$$|f(A) + g(A)| \gtrsim \min(|A|^{1/2}q^{1/2}, |A|^2q^{-1/2}).$$

(2) *Suppose $gcd(deg(g), q-1) = 1$ and $deg(f) \geq 1, deg(f) + deg(g) < p$. Then*

$$|f(A) + B||g(A)C| \gtrsim \min(|A|q, |A|^2|B||C|q^{-1}).$$

(3) *Suppose f contains some irreducible factors that are not factors of g such that the greatest common divisor of the powers of these factors in the canonical factorization of f is 1, and vice versa. Suppose $deg(f) + deg(g) < p$. Then*

$$|f(A)B||g(A)C| \gtrsim \min(|A|q, |A|^2|B||C|q^{-1}).$$

Particularly, one has

$$|f(A)g(A)| \gtrsim \min(|A|^{1/2}q^{1/2}, |A|^2q^{-1/2}).$$

2.3. **Vu's nondegenerate polynomials.** We give a generalization of Vu's result ([31]) using Theorem 2.2. Following Vu, a polynomial $P \in \mathbb{F}_q[x_1, x_2]$ is said to be *degenerate* if it is of the form $Q \circ L$, where $Q \in \mathbb{F}_q[x]$ and L is a linear form in x_1, x_2. We first recall the Schwarz-Zipple lemma ([29]) and the Katz theorem in [15].

Lemma 2.7 (Schwarz-Zipple). *Let $f \in \mathbb{F}_q[x_1, ..., x_n]$ be a nonzero polynomial with degree $\leq k$. Then*

$$|\{x \in \mathbb{F}_q^n : f(x) = 0\}| \leq kq^{n-1}.$$

Theorem 2.8 (Katz). *Let $P(x_1, x_2)$ be a polynomial of degree k in $\mathbb{F}_q^2$ which does not contain a linear factor. Let $P^{-1} = \{(x, y) \in \mathbb{F}_q^2 : P(x, y) = 0\}$. Then*

$$\|P^{-1}\|_u \lesssim k^2 q^{-3/2},$$

that is to say, P^{-1} is a Salem set with respect to $\mathbb{F}_q^2$.

Theorem 2.9. *Let P be a nondegenerate polynomial of degree k in $\mathbb{F}_q[x_1, x_2]$. Then for any $E, F \subset \mathbb{F}_q^2$ with $|E| \geq Ck^2 q$, $C > 1$ is a fixed constant, we have*

$$|P(E)| \gtrsim \min\left(\frac{|E|q}{|E+F|}, \frac{|E||F|^{1/2}}{|E+F|^{1/2} q^{1/2}}\right).$$

Proof. For each $a \in \mathbb{F}_q$, let

$$P^{-1}(a) = \{(x_1, x_2) \in \mathbb{F}_q^2 : \ P(x_1, x_2) = a\}.$$

By Vu's Lemma 5.1 ([31]), there are at least $q - (k-1)$ elements a_i such that $P - a_i$ does not contain a linear factor. We first call such a_i *good* and the others remaining *bad*, then form the *bad* elements into a set Δ. With these definitions, $|\Delta| \leq k - 1$. By Lemma 2.7, for each $z \in \Delta$ one has $|P^{-1}(z)| \leq kq$. Hence $\sum_{z\in\Delta} |P^{-1}(z)| \leq (k-1)kq$, and considering that $|E| \geq Ck^2 q$ we get

$$\left|E \backslash \bigcup_{z\in\Delta} P^{-1}(z)\right| \sim |E|.$$

Therefore,

$$|P(E)| \geq \frac{\left|E \backslash \bigcup_{z\in\Delta} P^{-1}(z)\right|}{M} \sim \frac{|E|}{M},$$

where $M \doteq \max_{a\in\mathbb{F}_q\backslash\Delta} |E \cap P^{-1}(a)|$. Now choose a *good* element $a \in \mathbb{F}_q \backslash \Delta$ which achieves the above maximum and define

$$X = E \cap P^{-1}(a), \quad \tilde{X} = P^{-1}(a), \quad Y = F.$$

Combining Lemma 2.7, Theorem 2.8 with the deduction of Theorem 2.2 gives

$$\min\left(qM, \frac{M^2|F|}{q}\right) \lesssim |X + Y| \leq |E + F|.$$

Consequently,

$$M \lesssim \max\left(\frac{|E+F|}{q}, \sqrt{q}\frac{|E+F|^{1/2}}{|F|^{1/2}}\right),$$

which in turn gives

$$|P(E)| \gtrsim \min\left(\frac{|E|q}{|E+F|}, \frac{|E||F|^{1/2}}{|E+F|^{1/2} q^{1/2}}\right).$$

□

Remark 2.10. Applying Theorem 2.9 to $E = F = A \times A$ with $|A| \geq Ckq^{1/2}$, $C > 1$, gives Vu's estimate:

$$\max(|A + A|, |P(A, A)|) \gtrsim \min(|A|^{2/3} q^{1/3}, |A|^{3/2} q^{-1/4}).$$

Theorem 2.11. *Let $f \in \mathbb{F}_q[x_1, x_2]$ be a nondegenerate polynomial of degree k and define $g(x_1, x_2, y_1, y_2) = f(x_1 - y_1, x_2 - y_2)$. Then the following two propositions are equivalent:*
(1) $f - b$ does not contain a linear factor for any $b \in \mathbb{F}_q$.
(2) $|g(E, F)| \gtrsim \min(k^{-1}q,\ k^{-2}\sqrt{|E||F|}q^{-1/2})$ holds for all $E, F \subset \mathbb{F}_q^2$.

Proof. (1)⇒(2): Suppose (1) holds true. For any $b \in \mathbb{F}_q$, apply Lemma 2.1 with $\mathbb{G}^2 = \mathbb{F}_q^2, X = E, Y = -F, P = f_b$ to get

$$M_b \doteq |\{(x, y) \in E \times F : f(x_1 - y_1, x_2 - y_2) = b\}| \le \frac{|E||F||f_b|}{q^2} + \|f_b\|_u \sqrt{|E||F|}q^2,$$

where $f_b \doteq \{(z_1, z_2) \in \mathbb{F}_q^2 : f(z_1, z_2) = b\}$. By Lemma 2.7 and Theorem 2.8 we get

$$M \doteq \max_b M_b \lesssim \max(\frac{k|E||F|}{q},\ k^2\sqrt{|E||F|q}),$$

which in turn gives

$$|g(E, F)| \ge \frac{|E||F|}{M} \gtrsim \min(k^{-1}q,\ k^{-2}\sqrt{|E||F|}q^{-1/2}).$$

(2)⇒(1): Suppose (2) holds true. We are trying to prove that (1) also holds true and argue it by contradiction. Suppose there exists $\widetilde{b} \in \mathbb{F}_q$ such that $f - \widetilde{b}$ contains a linear factor. Thus $(f - \widetilde{b})^{-1}(0)$ must contain a straight line, say for example $\widetilde{L}$, as a subset. Now we choose two straight lines E, F in $\mathbb{F}_q^2$ such that $E - F = \widetilde{L}$. Consequently, $g(E, F) = \{\widetilde{b}\}$, a contradiction to (2). We are done. □

2.4. **Multi-fold sums and products.**

Theorem 2.12. *Given $A \subset \mathbb{F}_q$ and $\oplus \in \{+, \times\}$, suppose there exist $a, b > 0$ such that for all $B \subset \mathbb{F}_q$,*

$$|A \oplus B| \ge \min(a, b|B|).$$

Then for all $d \ge 2$ we have

$$|d^{\oplus} A| \ge \min(a, b^{d-1}|A|),$$

where $d^{\oplus}A$ is the d-fold $\oplus$-set of A.

Proof. Define a function $\varphi : (0, \infty) \to (0, \infty)$ by $\varphi(x) = \min(a, \widetilde{b}x)$, where $\widetilde{b} \doteq \max(b, 1) \ge 1$. It is easy to verify that $\varphi^{(s)}(x) = \min(a, \widetilde{b}^s x)$, where $\varphi^{(1)} = \varphi, \varphi^{(s)} = \varphi^{(s-1)} \circ \varphi$. By the given assumption, for all $B \subset \mathbb{F}_q$ we have $|A \oplus B| \ge \varphi(|B|)$. Since φ is nondecreasing, we have

$$|d^{\oplus}A| \ge \varphi(|(d-1)^{\oplus}A|) \ge \cdots \ge \varphi^{(d-1)}(|A|) = \min(a, \widetilde{b}^{d-1}|A|) \ge \min(a, b^{d-1}|A|).$$

This finishes the proof. □

Combining Theorem 2.6 with the preceding theorem naturally gives the following estimate, which improves the relevant results in [14, 30].

Theorem 2.13. *Let A be a subset of $\mathbb{F}_q$ and $f \in \mathbb{F}_q[x]$.*

(1) *If $1 < deg(f) < p$, then*

$$|dA| \gtrsim \min\Big(\frac{q|A|}{|f(A)+A|},\ |A|\cdot\big(\frac{|A|^3}{q|f(A)+A|}\big)^{d-1}\Big),$$

$$|df(A)| \gtrsim \min\Big(\frac{q|A|}{|A+A|},\ |A|\cdot\big(\frac{|A|^3}{q|A+A|}\big)^{d-1}\Big).$$

If $1 \le deg(f) < p$, then

$$|A^d| \gtrsim \min\Big(\frac{q|A|}{|f(A)+A|},\ |A|\cdot\big(\frac{|A|^3}{q|f(A)+A|}\big)^{d-1}\Big)$$

and

$$|df(A)| \gtrsim \min\Big(\frac{q|A|}{|AA|},\ |A|\cdot\big(\frac{|A|^3}{q|AA|}\big)^{d-1}\Big).$$

(2) *If f contains a simple root not equal to zero, then*

$$|A^d| \gtrsim \min\Big(\frac{q|A|}{|f(A)A|},\ |A|\cdot\big(\frac{|A|^3}{q|f(A)A|}\big)^{d-1}\Big)$$

and

$$|f(A)^d| \gtrsim \min\Big(\frac{q|A|}{|AA|},\ |A|\cdot\big(\frac{|A|^3}{q|AA|}\big)^{d-1}\Big),$$

where dB and B^d denote the d-fold sum-set and product-set of B respectively.

3. Expanding phenomena for small sets in prime fields

Theorem 3.1. *Suppose $A \subset \mathbb{F}_p$ with p prime and $|A| \le p^{1/2}$. Then one has*

$$|A + A^2| \gtrsim |A|^{147/146},$$

where $A^2 \doteq \{a^2 : a \in A\}$.

Theorem 3.2. *Suppose $A \subset \mathbb{F}_p^*$ with p prime and $|A| \le p^{1/2}$. Then one has*

$$\Big|\frac{A+1}{A}\Big| \gtrsim |A|^{110/109}.$$

The authors believe the above three expanding indexes are far from optimal. Before proceeding to prove the theorems, we recall two results. The first one is a variant of the Balog-Szemerédi-Gowers theorem established by Bourgain and Garaev ([2]). The second one is a Garaev-type sum-product estimate, which is a slight variant of a theorem obtained by the second author ([16]), improving upon the one obtained by Bourgain and Garaev ([2]) and the third author ([24, 25]).[1]

Lemma 3.3 ([2], Lemma 2.2). *Let A, B be two sets in an abelian group G, and E be a subset of $A \times B$. Then there exists a subset $D \subset A$ with $|D| \gtrsim |E|/|B|$ such that*

$$|A \overset{E}{-} B|^4 \gtrsim \frac{|D-D|\cdot|E|^5}{|A|^4\cdot|B|^3},$$

where $A \overset{E}{-} B \triangleq \{a-b : (a,b) \in E\}$.

Lemma 3.4. *Suppose $A \subset \mathbb{F}_p^*$ with p prime and $|A| \le p^{12/23}$. Then for any $\oplus \in \{+,-\}$, $\otimes \in \{\times, \div\}$, one has $|A \oplus A|^8 \cdot |A \otimes A|^4 \gtrsim |A|^{13}$.*

[1] We note that a recent preprint of Rudnev ([22]) gives $\max\{|A+A|, |AA|\} \gtrsim |A|^{12/11}$.

Proof of Lemma 3.4. Let $E^{\otimes}(A,A)$ be the $\otimes$-energy of A, that is,

$$E^{\otimes}(A,A)=\sum_{x\in A}\sum_{y\in A}|(x\otimes A)\cap(y\otimes A)|.$$

It is very easy to observe that $E^{\times}(A,A)=E^{\div}(A,A)$ ($\clubsuit$), and from the Cauchy-Schwarz inequality one has $E^{\otimes}(A,A)\geq\frac{|A|^4}{|A\otimes A|}$ ($\spadesuit$). Tracing back the proof of Theorem 1.1 in [16], we have $E^{\times}(A,A)^4\lesssim|A|^3\cdot|A\oplus A|^8$, which in turn yields $E^{\otimes}(A,A)^4\lesssim|A|^3\cdot|A\oplus A|^8$ (due to $\clubsuit$), and $|A|^{13}\lesssim|A\otimes A|^4\cdot|A\oplus A|^8$ (due to $\spadesuit$). This finishes the proof. □

Proof of Theorem 3.1. Denote

$$E=\{(x+y,\frac{1}{x-y}):x,y\in A,x\neq y,x\neq -y\}\subset\big((A+A)\backslash\{0\}\big)\times\Big(\frac{1}{(A-A)\backslash\{0\}}\Big).$$

Obviously, $|E|\sim|A|^2$ and $((A+A)\backslash\{0\})\overset{E}{\div}(\frac{1}{(A-A)\backslash\{0\}})\subset A^2-A^2$. Applying Lemma 3.3 with the ambient group $\mathbb{F}_p^*$, one can find a subset $D\subset A+A$ with $|D|\gtrsim\frac{|A|^2}{|A-A|}$ so that

$$|A^2-A^2|^4\cdot|A+A|^4\cdot|A-A|^3\gtrsim|D/D|\cdot|A|^{10}.$$

There are two cases to consider.

Case 1. Suppose $|D|\leq p^{12/23}$. Noticing the fact that $D\subset A+A$ and that a lower bound for $|D/D|$ can be simply established from Lemma 3.4, we have

$$|A+A+A+A|^2\cdot|A^2-A^2|^4\cdot|A+A|^4\cdot|A-A|^3\gtrsim|D|^{3.25}\cdot|A|^{10}\gtrsim\frac{|A|^{16.5}}{|A-A|^{3.25}},$$

which gives

$$|A+A+A+A|^8\cdot|A^2-A^2|^{16}\cdot|A+A|^{16}\cdot|A-A|^{25}\gtrsim|A|^{66}.$$

Noting $\frac{|A|}{2}\leq|A^2|\leq|A|$, we apply the Plünnecke-Ruzsa inequality several times as follows:

$$\begin{aligned}|A+A+A+A|&\leq\frac{|A+A^2|^4}{|A^2|^3}\sim\frac{|A+A^2|^4}{|A|^3},\\ |A^2-A^2|&\leq\frac{|A^2-(-A)|\cdot|(-A)-A^2|}{|A|}=\frac{|A+A^2|^2}{|A|},\\ |A+A|&\leq\frac{|A+A^2|^2}{|A^2|}\sim\frac{|A+A^2|^2}{|A|},\\ |A-A|&\leq\frac{|A-(-A^2)|\cdot|(-A^2)-A|}{|A^2|}\sim\frac{|A+A^2|^2}{|A|},\end{aligned}$$

to get $|A+A^2|\gtrsim|A|^{147/146}$.

Case 2. Suppose $|D|\geq p^{12/23}$. Then $|A+A|\geq|D|\geq p^{12/23}\geq|A|^{24/23}$. From Ruzsa's inequality, we also have

$$|A+A|\leq\frac{|A+A^2|^2}{|A^2|}\sim\frac{|A+A^2|^2}{|A|}.$$

Therefore $|A+A^2|^2\gtrsim|A+A|\cdot|A|\geq|A|^{47/23}$, which yields $|A+A^2|\gtrsim|A|^{47/46}$.

□

Proof of Theorem 3.2. Without loss of generality we may assume $-1 \notin A$. Denote $B = \frac{A+1}{A}$ and

$$E = \{(\frac{1}{x}, \frac{y+1}{x}) : x, y \in A\} \subset (1/A) \times B.$$

Then $|E| = |A|^2$ and $-A/A = (1/A) \overset{E}{-} B$. Applying Theorem 3.3 with the ambient group $\mathbb{F}_p$, there exists a subset $D \subset 1/A$ with $|D| \gtrsim \frac{|A|^2}{|B|}$ so that

$$|A/A|^4 \gtrsim \frac{|D-D| \cdot |A|^6}{|B|^3},$$

which gives

$$|A/A|^{32} \cdot |B|^{24} \gtrsim |D-D|^8 \cdot |A|^{48}. \tag{3.1}$$

By Theorem 3.4,

$$|D-D|^8 \cdot |D/D|^4 \gtrsim |D|^{13} \gtrsim \frac{|A|^{26}}{|B|^{13}}. \tag{3.2}$$

We notice that $D \subset 1/A$; thus

$$|A/A|^4 \geq |D/D|^4. \tag{3.3}$$

Combining (3.1), (3.2) and (3.3) we get $|A/A|^{36} \cdot |B|^{37} \gtrsim |A|^{74}$. Thus by applying the Ruzsa inequality

$$|A/A| \leq \frac{|A/(A+1)| \cdot |(A+1)/A|}{|A+1|} = \frac{|B|^2}{|A|},$$

we get $|B|^{109} \gtrsim |A|^{110}$. This finishes the proof. □

Remark 3.5. One may notice that from Theorem 2.6 we have

$$|A + A^2| \gtrsim \min(|A|^{1/2}p^{1/2}, |A|^2 p^{-1/2}).$$

Therefore combining Theorem 3.1, one has that $x + y^2$ is an expander for all sizes of $|A|$. In addition, we notice that if $|A| > p^{2/3}$, then

$$|A + A^2| \gtrsim \sqrt{p\,|A|}.$$

Let us show by adopting the Garaev-Shen example ([12]) that this is optimal up to the implied constant. Let $N < 0.01p$ be a positive integer, $M = [2\sqrt{Np}]$ and let X be the set of x so that x^2 modulo p belongs to the interval $[1, M]$. Then it is known that $|X| \gtrsim M$. From the pigeonhole principle, there is a number L such that

$$|X \cap \{L+1, \ldots, L+M\}| \gtrsim \frac{M^2}{2p} \sim N.$$

Take $A = X \cap \{L+1, \ldots, L+M\}$. Then we have $|A| \gtrsim N$ and $|A + A^2| \leq 2M \lesssim \sqrt{pN}$.

Acknowledgments

The second author was supported by the NSF of China (11001174) and the Texas Higher Education Coordinating Board (ARP 003615-0039-2007). He also thanks Chunlei Liu and Jian Shen for helpful discussions. The authors thank the anonymous referee for carefully reading the manuscript.

References

[1] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory **1** (2005), 1–32. MR2172328 (2006g:11041)

[2] J. Bourgain, M. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields,* Math. Proc. Cambridge Philos. Soc. **146** (2009), 1–21. MR2461864 (2009k:11019)

[3] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27–57. MR2053599 (2005d:11028)

[4] J. Cilleruelo, *Combinatorial problems in finite fields and Sidon sets*, arXiv:1003.3576, 2010. Combinatorica, to appear.

[5] E. Croot, Private communication, 2009.

[6] Gy. Elekes, *On the number of sums and products*, Acta Arith. **81** (1997), 365–367. MR1472816 (98h:11026)

[7] Gy. Elekes, M. B. Nathanson, I. Z. Ruzsa, *Convexity and sumsets*, J. Number Theory **83** (2000), 194–201. MR1772612 (2001e:11020)

[8] P. Erdős, E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics, pages 213-218, Birkhäuser, Basel, 1983. MR820223 (86m:11011)

[9] K. Ford, *Sums and products from a finite set of real numbers*, Ramanujan J. **2** (1998), 59–66. MR1642873 (99i:11014)

[10] M. Garaev, *An explicit sum-product estimate in $\mathbb{F}_p$*, Int. Math. Res. Notices **11** (2007), Art. ID rnm035. MR2344270 (2008g:11038)

[11] M. Garaev, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc. **136** (2008), 2735–2739. MR2399035 (2009e:11043)

[12] M. Garaev, C.-Y. Shen, *On the size of the set $A(A+1)$*, Math. Z. **265** (2010), 125–132. MR2606952 (2011b:11022)

[13] A. Glibichuk, S. Konyagin. *Additive properties of product sets in fields of prime order*, CRM Proc. Lecture Notes, **43**, Additive combinatorics, 279–286, Amer. Math. Soc., Providence, RI, 2007. MR2359478 (2009a:11054)

[14] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices **5** (2007), Art. ID rmn007. MR2341599 (2008i:11037)

[15] N. M. Katz, *Sommes exponentielles*, Astérisque **79**, Société Mathématique de France, Paris, 1980. MR617009 (82m:10059)

[16] L. Li, *Slightly improved sum-product estimates in fields of prime order*, Acta. Arith. **147** (2011), 153–160. MR2771659

[17] L. Li, J. Shen, *A sum-division estimate of reals*, Proc. Amer. Math. Soc. **138** (2010), 101–104. MR2550173 (2010m:11033)

[18] R. Lidl, H. Niederreiter, Finite Fields, second edition, Cambridge University Press, 1997. MR1429394 (97i:11115)

[19] M. B. Nathanson, *On sums and products of integers*, Proc. Amer. Math. Soc. **125** (1997), 9–16. MR1343715 (97c:11010)

[20] H. Niederreiter, *Incomplete character sums and polynomial interpolation of the discrete logarithm*, Finite Fields Appl. **8** (2002), 184–192. MR1894512 (2003a:11155)

[21] P. Pudlák, *On explicit Ramsey graphs and estimates of the number of sums and products*, Topics in discrete mathematics, 169–175, Algorithms Combin., 26, Springer, Berlin, 2006. MR2249270 (2007h:05107)

[22] M. Rudnev, *An improved sum-product inequality in fields of prime order*, arXiv:1011.2738, 2010. IMRN, to appear.

[23] C.-Y. Shen, *Algebraic methods in sum-product phenomena*, Israel J. Math. **188** (2012), no. 1.

[24] C.-Y. Shen, *An extension of Bourgain and Garaev's sum-product estimates*, Acta Arith. **135** (2008), 351–356. MR2465717 (2009i:11028)

[25] C.-Y. Shen, *On the sum product estimates and two variables expanders*, Publ. Math. **54** (2010), 149–157. MR2603593 (2011b:11023)

[26] J. Solymosi, *On the number of sums and products*, Bull. London Math. Soc. **37** (2005), 491–494. MR2143727 (2006c:11021)

[27] J. Solymosi, *Incidences and the spectra of graphs*, Building Bridges, 499–513, Bolyai Soc. Math. Stud., 19, Springer, Berlin, 2008. MR2484652 (2010e:05189)

[28] J. Solymosi, *Bounding multiplicative energy by the sumset*, Adv. Math. **222** (2009), 402–408. MR2538014 (2010h:11014)

[29] T. Tao, V. Vu, Additive Combinatorics, Cambridge University Press, 2006. MR2289012 (2008a:11002)

[30] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs*, arXiv:0904.0441, 2009.

[31] V. Vu, *Sum-product estimates via directed expanders*, Math. Res. Lett. **15** (2008), 375–388. MR2385648 (2009e:11023)

Department of Mathematics, Rutgers University, Piscataway, New Jersey 08854
E-mail address: dnhart@math.rutgers.edu

Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China – and – Department of Mathematical Sciences, Loughborough University, Leicestershire LE11 3TU, United Kingdom
E-mail address: liliangpan@gmail.com

Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario L8S 4K1, Canada
E-mail address: shenc@umail.iu.edu
Current address: Department of Mathematics, Michigan State University, East Lansing, Michigan 48824