Sum-Product type Estimates over Finite Fields

Esen Aksoy Yazici

March 25, 2019

Abstract

Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements where \( q = p^l \) is a prime power. Using Fourier analytic tools with a third moment method, we obtain sum-product type estimates for subsets of \( \mathbb{F}_q \).

In particular, we prove that if \( A \subset \mathbb{F}_q \), then

\[
|AA + A|, |A(A + A)| \gg \min \left\{ q, \frac{|A|^2}{q^2} \right\},
\]

so that if \( A \geq q^{\frac{3}{4}} \), then \( |AA + A|, |A(A + A)| \gg q \).

1 Introduction

Let \( R \) be a ring. For a finite subset \( A \) of \( R \) we define the sum set and the product set of \( A \) by

\[
A + A = \{ a + b : a, b \in A \} \quad \text{and} \quad AA = \{ a \cdot b : a, b \in A \},
\]

respectively. It is expected that, if \( A \) is not subring of \( R \), then either \( |A + A| \) or \( |AA| \) is large compared to \( |A| \).

In [4], Erdős and Szemeredi proved that that there exists an absolute constant \( \epsilon > 0 \) such that

\[
\max\{|A + A|, |AA|\} \gg |A|^{1+\epsilon}
\]

holds for any finite subset \( A \) of \( \mathbb{Z} \). They also conjectured that this bound should hold for any \( \epsilon < 1 \). The best known bound in this direction is due to Shakan [11, Theorem 1.2] which states that if \( A \) is a finite subset of \( \mathbb{R} \), then

\[
|A + A| + |AA| \gg |A|^{\frac{1}{3} + \frac{5}{2777}}
\]

The sum-product problem in the finite field context has been studied by various authors. In this setting, one generally works either on the small sets in terms of the
characteristic $p$ of $\mathbb{F}_q$ or for sufficiently large subsets of $\mathbb{F}_q$ to guarantee that the set itself is in fact not a proper subfield of $\mathbb{F}_q$. We refer the reader [1, 3, 5, 6, 7, 8, 9] and the references therein for an extensive exploration of the problem in this context.

In the present paper, we turn our attention to sum-product type estimates for the sets of the form $BA + C = \{ba + c : a \in A, b \in B, c \in C\}$ and $B(A + C) = \{b(a + c) : a \in A, b \in B, c \in C\}$ where $A, B,$ and $C$ are subsets of $\mathbb{F}_q$. To estimate a lower bound for these sets, we first consider an additive energy which we relate with a third moment method. Then we employ a lemma from [2] and prove the main result in the paper using the tools in Fourier analysis.

### 1.1 Preliminaries

Let $f : \mathbb{F}_q \rightarrow \mathbb{C}$. The Fourier transform of $f$ is defined as

$$\hat{f}(m) = q^{-1} \sum_{x \in \mathbb{F}_q} \chi(-xm)f(x)$$

where $\chi(z) = e^{\frac{2\pi i z}{q}}$. We will use the orthogonality relation

$$\sum_{x \in \mathbb{F}_q} \chi(xs) = \begin{cases} q, & \text{if } s = 0 \\ 0, & \text{otherwise} \end{cases}$$

and Plancherel identity

$$\sum_{m \in \mathbb{F}_q} |\hat{f}(m)|^2 = q^{-1} \sum_{x \in \mathbb{F}_q} |f(x)|^2.$$

The main result of the paper is the following theorem.

**Theorem 1.1.** If $A, B, C \subset \mathbb{F}_q$, then

$$|BA + C|, |B(A + C)| \gg \min \left\{ q, \frac{|B|^{\frac{1}{2}}|C|^{\frac{1}{2}}|A|}{q^{\frac{1}{2}}} \right\}.$$

In particular, taking $A = B = C$, we have

$$|AA + A|, |A(A + A)| \gg \min \left\{ q, \frac{|A|^2}{q^{\frac{1}{2}}} \right\}.$$

so that if $A \geq q^{\frac{3}{2}}$, then $|AA + A|, |A(A + A)| \gg q$. 

2
1.2 Proof of Theorem 1.1

Let $A \subset \mathbb{F}_q$ and $P$ be a set of points in $\mathbb{F}_q^2 \setminus \{(0,0)\}$. Define the set of lines pinned at $P$ as

$$L = L_P = \{l_{m,b} : (m,b) \in P\}$$

and also the image set of lines in $L$ as

$$L(A) = L_P(A) = \{l_{m,b}(a) = ma + b : (m,b) \in P, a \in A\}.$$

Similar to energy notion given in [1], define

$$E_3(L, A) = |\{m_1a_1 + b_1 = m_2a_2 + b_2 = m_3a_3 + b_3\}|$$

where $(m_1, b_1), (m_2, b_2), (m_3, b_3) \in P, a_i \in A$.

Lemma 1.2. With the notation above we have

$$\frac{|L|^3|A|^3}{|L(A)|^2} \leq E_3(L, A).$$

Proof. Let $r(x) = r_{L(A)}(x) = |\{(m,b), a \in P \times A : x = ma+b\}|$. Then, by Hölder inequality,

$$|L||A| = \sum r(x) \leq (\sum r(x)^3)^\frac{1}{3} (\sum 1^3)^\frac{2}{3} \leq E_3(L, A)^\frac{1}{3} L(A)^\frac{2}{3} \leq E_3(L, A).$$

We need the following lemma from [2].

Lemma 1.3. [2 Lemma 2.1]

$F$ a finite space, $f : F \to \mathbb{R}$.

$$\sum_{z \in F} f^n(z) \leq |F| \left(\frac{\|f\|_1}{|F|}\right)^n + \frac{n(n-1)}{2} \|f\|_\infty^{n-2} \sum_{z \in F} \left(f(z) - \frac{\|f\|_1}{|F|}\right)^2$$

where $\|f\|_1 = \sum_{z \in F} |f(z)|, \|f\|_\infty = \max_{z \in F} f(z)$.

Theorem 1.4. Let $L = L_P$ where $P \cong B \times C$.

$$L(A) \gg \min \left\{ q, \frac{|L|^\frac{1}{2}|A|}{q^\frac{2}{3}} \right\}$$
Proof. Now let
\[ f(z) := r_{L(A)}(z) = |\{z = a_1a_2 + a_3 : (a_1, a_3) \in P, a_2 \in A\}| \]
Then by taking \( n = 3, \ F = \mathbb{F}_q \) in Lemma 1.3, we have
\[ E_3(L, A) = \sum_z f(z)^3 \leq \frac{||f||_1^3}{q^2} + 3||f||_\infty \sum_{z \in F} \left( f(z) - \frac{||f||_1}{q} \right)^2. \]
Note that \( ||f||_1 = \sum f(z) = |L||A|, \ ||f||_\infty = \text{sup}_z f(z) \leq |L|, \) since when we fix \((a_1, a_3)\) in \( f(z) \) then \( a_2 \) is uniquely determined.
Therefore,
\[ E_3(L, A) \leq \frac{|L|^3|A|^3}{q^2} + 3|L| \sum_z (f(z) - \frac{|L||A|}{q})^2 \]
\[ = \frac{|L|^3|A|^3}{q^2} + 3|L|q \sum_{\xi \neq 0} |\hat{f}(\xi)|^2 \]
where we used the Plancherel in the last equality.
We can write
\[ f(z) = |\{z = a_1a_2 + a_3 : (a_1, a_3) \in P = B \times C, a_2 \in A\}| \]
\[ = q^{-1} \sum_{s,a_1,a_2,a_3} \chi((z - (a_1a_2 + a_3)s)B(a_1)C(a_3)A(a_2)) \]
\[ = q^{-1} \sum_{s,a_1,a_2,a_3} \chi(zs - a_1a_2s)\chi(-a_3s)C(a_3)B(a_1)A(a_2) \]
\[ = \sum_{s,a_1,a_2} \chi(zs - a_1a_2s)\hat{C}(s)B(a_1)A(a_2) \]
It follows that
\[ \hat{f}(\xi) = q^{-1} \sum_z \chi(z,\xi)f(z) \]
\[ = q^{-1} \sum_z \chi(-z,\xi) \sum_{s,a_1,a_2} \chi(zs - a_1a_2s)\hat{C}(s)B(a_1)A(a_2) \]
\[ = q^{-1} \sum_{s,a_1,a_2} \chi(-a_1a_2s)\hat{C}(s)B(a_1)A(a_2) \sum_{z \in \mathbb{F}_q} \chi(z(s-\xi)) \]
\[ = \sum_{a_1,a_2} \chi(-a_1a_2\xi)\hat{C}(\xi)B(a_1)A(a_2). \]
Therefore,

$$|\hat{f}(\xi)| \leq \sum_{a_1 \in B} \sum_{a_2 \in A} \chi(-a_1a_2\xi)\hat{C}(\xi)$$

By the Cauchy-Schwarz inequality, for $\xi \neq 0$,

$$|\hat{f}(\xi)|^2 \leq |B| \sum_{a_1 \in \mathbb{F}_q} \sum_{a_2, a'_2 \in A} \chi(-a_1a_2\xi)\hat{C}(\xi)\chi(a_1a'_2\xi)\hat{C}(\xi)$$

$$= |B| \sum_{a_1 \in \mathbb{F}_q} \sum_{a_2, a'_2 \in A} \chi(\xi(a'_2 - a_2))|\hat{C}(\xi)|^2$$

$$\leq |B| \sum_{a_1 \in \mathbb{F}_q} \sum_{a_2, a'_2 \in A} \chi(\xi(a'_2 - a_2))|\hat{C}(\xi)|^2$$

$$= |B|q \sum_{a_2, a'_2 \in A} \xi(a'_2 - a_2 = 0)$$

$$= |B|q \sum_{a'_2 = a_2 \in A} |\hat{C}(\xi)|^2$$

$$= |B|q|A||\hat{C}(\xi)|^2$$

It follows that

$$\sum_{\xi \neq 0} |\hat{f}(\xi)|^2 \leq |B|q|A|\sum_{\xi \neq 0} |\hat{C}(\xi)|^2$$

$$\leq |B|q|A|q^{-1} \sum_x |C(x)|^2$$

$$= |B||A||C|$$

$$= |L||A|$$

Plugging the last value in (1) and using Lemma 1.2 we have

$$\frac{|L|^3|A|^3}{|L(A)|^2} \leq E_3(L, A) \leq \frac{|L|^3|A|^3}{q^2} + 3|L|^2|A|q$$

Therefore

$$L(A) \gg \min \left\{ q, \frac{|L|^\frac{1}{2}|A|}{q^2} \right\}.$$
Proof of Theorem 1.1. Note that the set $BA + C = L_P(A)$ where $P = B \times C$. Hence, taking $|L| = |B||C|$ in Theorem 1.4 it follows that

$$|BA + C| \gg \min \left\{ q, \frac{|B|^\frac{1}{2}|C|^\frac{1}{2}|A|}{q^\frac{1}{2}} \right\}$$

Note that $B(A + C) = L_P(A)$ where $P \cong B \times C$, so the same argument applies. \qed

Acknowledgements

The author would like to thank Simon Macourt, Oliver Roche-Newton, Alex Iosevich, Jonathan Pakianathan and Ilya Shkredov for their valuable comments. The author is supported by TÜBİTAK-BİDEB 2218 Postdoctoral Research Fellowship.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, I. Shkredov, *Growth Estimates in Positive Characteristic via Collisions*, Int. Math. Res. Not. IMRN 2017, no. 23, 71487189.

[2] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, M. Rudnev, *Group actions and geometric combinatorics in $\mathbb{F}_q^d$*, Forum Math. 29 (2017), no. 1, 91110.

[3] J. Bourgain, N. H. Katz, T. Tao, *A sum-product estimate in finite fields, and applications*, Geometric & Functional Analysis GAFA 14, no 1 (2004), 27-57.

[4] P. Erdős, E. Szemerédi, *On sums and products of integers*. Studies in Pure Mathematics. To the memory of Paul Turán, Basel: Birkhäuser Verlag, pp. 213-218.

[5] N. Hegyvari, F. Hennecart, *Conditional expanding bounds for two-variable functions over prime fields*, European J. Combin., 34(2013), 1365-1382.

[6] B. Murphy, G. Petridis, *A second wave of expanders in finite fields*, Combinatorial and additive number theory. II, 215238, Springer Proc. Math. Stat., 220, Springer, Cham, 2017.

[7] B. Murphy, G. Petridis, *Products of difference over arbitrary finite fields*, Discrete Anal. 2018, Paper No. 18, 42 pp.

[8] O. Roche-Newton, M. Rudnev, I. D. Shkredov, *New sum-product type estimates over finite fields* Adv. Math. 293 (2016), 589605.
[9] M. Rudnev. An improved sum-product inequality in fields of prime order, Int. Math. Res. Not. IMRN, (16):3693-3705, 2012.

[10] M. Rudnev, G. Shakan, I. D. Shkredov, Stronger sumproduct inequalities for small sets, https://arxiv.org/pdf/1808.08465.pdf

[11] G. Shakan On Higher Energy Decompositions and the Sum-product Phenomena, https://arxiv.org/pdf/1803.04637.pdf