A note on conditional expanders over prime fields

Mozhgan Mirzaei*

February 1, 2020

Abstract

Let $\mathbb{F}_p$ be a prime field of order p, and A be a set in $\mathbb{F}_p$ with $|A| \leq p^{1/2}$. In this note, we show that

$$\max\{|A+A|, |f(A,A)|\} \gtrsim |A|^{\frac{6}{5}+\frac{4}{305}},$$

where $f(x,y)$ is a *non-degenerate* quadratic polynomial in $\mathbb{F}_p[x,y]$. This improves a recent result given by Koh, Mojarrad, Pham, Valculescu (2018).

1 Introduction

Let A be a set of integers. The sum and product sets are defined as follows:

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

Throughout this paper, by $X \gg Y$, we mean $X \geq C_1 Y$ for some absolute constant C_1, and $X \sim Y$ means that $X \gg Y$ and $Y \gg X$, by $X \gtrsim Y$ we mean $X \gg (\log Y)^{-C_2} Y$ for some absolute constant C_2.

Erdős and Szemerédi [4] proved that for any finite set $A \subset \mathbb{Z}$, we have

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{1+\varepsilon}$$

for some positive constant ε. In the setting of finite fields, a similar result has been derived by Bourgain, Katz, and Tao [1]. They showed that for any set $A \subset \mathbb{F}_p$, where p is a prime and

*Department of Mathematics, University of California at San Diego, La Jolla, CA, 92093 USA. Supported by NSF grant DMS-1800746. Email: momirzae@ucsd.edu.

$p^\delta < |A| < p^{1-\delta}$ for some $\delta > 0$, one has

$$\max\{|A+A|, |A\cdot A|\} \geq C_\delta |A|^{1+\varepsilon},$$

for some $\varepsilon = \varepsilon(\delta) > 0$. We note here that in the result of Bourgain, Katz, and Tao [1], it is difficult to determine the relation between ε and δ.

Hart, Iosevich, and Solymosi [6] developed Fourier analysis tools to obtain a bound over arbitrary finite fields that gives an explicit dependence of ε on δ as follows.

Theorem 1.1 (**Hart-Iosevich-Solymosi,** [6])**.** *Let $\mathbb{F}_q$ be an arbitrary finite field of order q, and let $A \subset \mathbb{F}_q$. Suppose $|A+A| = m$ and $|A\cdot A| = n$, then we have*

$$|A|^3 \leq \frac{cm^2 n|A|}{q} + cq^{1/2}mn, \tag{1}$$

for some positive constant c.

By a direct computation, Theorem 1.1 is non-trivial when $|A| \gg q^{1/2}$. For $|A| \sim q^{7/10}$, we have the best growth

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{8/7}.$$

Using exponential sums, Garaev [5] obtained the following improvement.

Theorem 1.2 (**Garaev**, [5])**.** *Let $\mathbb{F}_p$ be a prime field of order p and A be a set in $\mathbb{F}_p$.*

1. *If $p^{1/2} \ll |A| \ll p^{2/3}$, then*

$$\max\{|A+A|, |A\cdot A|\} \gg \frac{|A|^2}{p^{1/2}}.$$

2. *If $|A| \gg p^{2/3}$, then*

$$\max\{|A+A|, |A\cdot A|\} \gg (p|A|)^{1/2}.$$

Hence, if $|A| = p^\alpha$, then we have

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+\alpha'},$$

where $\alpha' = \frac{1}{4} - \frac{1}{2}\left|\frac{1}{\alpha} - \frac{3}{2}\right|$. If α is very small, say $\alpha \leq 18/35$, then Rudnev, Shakan, and Shkredov [13] proved the following.

Theorem 1.3 (**Rudnev-Shakan-Shkredov**, [13])**.** *Let $\mathbb{F}_p$ be a prime field of order p. Let A be*

a set in $\mathbb{F}_p$. Suppose that $|A| \ll p^{\frac{18}{35}}$, then we have

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+\frac{2}{9}-o(1)}.$$

This theorem improves the earlier exponents 39/32 due to Chen, Kerr, and Mohammadi [3] and 6/5 due to Roche-Newton, Rudnev, and Shkredov [12].

Definition 1.4. *Let $\mathbb{F}_p$ be a prime field. A polynomial $f(x,y) \in \mathbb{F}_p[x,y]$ is degenerate if it is of the form $Q(L(x,y))$ where Q is a one-variable polynomial and L is a linear form in x and y.*

A more general statement of Theorem 1.2 has been established by Vu [19]. In particular, let $f(x,y)$ be a non-degenerate polynomial of degree d in $\mathbb{F}_p[x,y]$, and A a set in $\mathbb{F}_p$, we have

$$\max\{|A+A|, |f(A,A)|\} \gg \min\left\{\frac{|A|^{3/2}}{dp^{1/4}}, \frac{p^{1/3}|A|^{2/3}}{d^{1/3}}\right\}.$$

This statement tells us that if the size of $A+A$ is small, then the size of $f(A,A)$ is large. Note that the non-degenerate condition of f is necessary since otherwise we might have $\max\{|A+A|, |f(A,A)|\} \sim |A|$ when A is an arithmetic progression.

In the case $f(x,y) = xy$, this result is slight weaker than Theorem 1.2. This result is only non-trivial when $|A| \geq p^{1/2}$. When $|A| < p^{1/2}$, Bukh and Tsimerman [2] derived the following estimate for quadratic non-degenerate polynomials

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{1+\epsilon}, \tag{2}$$

for some $\epsilon > 0$.

This bound has been quantified and improved over the years. More precisely, Koh, Mojarrad, Pham, and Valculescu [9] proved the following theorem.

Theorem 1.5 (**Koh-Mojarrad-Pham-Valculescu**, [9])**.** *Let $\mathbb{F}_p$ be a prime field of order p, and let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. For $A \subset \mathbb{F}_p$ with $|A| \ll p^{5/8}$, we have*

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{6/5}.$$

Notice that the case $f(x,y) = x^2 + y^2$ was first proved by Pham, Vinh and De Zeeuw in [11]. We refer the interested reader to [14] for similar results in the setting of $\mathbb{R}$.

In this paper, we employ the theory of higher energies developed in [15, 16, 13, 17], namely *E_4-energy*, to give a better exponents as follows.

Theorem 1.6. *Let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. For $A \subset \mathbb{F}_p$ with $|A| \ll p^{1/2}$ we have*

$$\max\{|A+A|, |f(A,A)|\} \gtrsim |A|^{\frac{6}{5}+\frac{4}{305}}.$$

As in the Euclidean setting, it is expected that when A is not too large, then $\max\{|A+A|, |f(A,A)|\} \gg |A|^{2-\epsilon}$ for any $\epsilon > 0$. We will discuss about the limitations of methods in [13, 17] for our settings in Remarks 2.2 and 2.6. We also refer the interested reader to [7] for an application of E_4-*energy* in a variant of the distance problem over prime fields.

2 Proof of Theorem 1.6

For $A, B \subset \mathbb{F}_p$, let $E_4^+(A,B)$ be the number of tuples $(a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4) \in A^4 \times B^4$ such that

$$a_1 - b_1 = a_2 - b_2 = a_3 - b_3 = a_4 - b_4.$$

For $A \subset \mathbb{F}_p$, we define

$$d_4^+(A) := \sup_{B \neq \emptyset} \frac{E_4^+(A,B)}{|A||B|^3}.$$

Note that $d_4^+(A) \geq \frac{E_4^+(A,A)}{|A|^4} \geq \frac{|A|^4}{|A|^4} = 1$.

It has been observed in [17] that the sup is taken over all sets B with $|B| \leq |A|^{3/2}$. Indeed, if $|B| \geq |A|^{3/2}$, then

$$d_4^+(A) = \sup_{B \neq \emptyset} \frac{E_4^+(A,B)}{|A||B|^3} \leq \frac{|A|^4|B|}{|A||B|^3} \leq 1,$$

a contradiction.

In [17], Shakan and Shkredov proved that

$$d_4^+(A) \ll \frac{|A \cdot A|^2}{|A|^2} \tag{3}$$

whenever $|A| \leq p^{3/5}$. They also derived the following lemma, which says that small energy implies large sumset.

Lemma 2.1 ([17])**.** *For $A \subset \mathbb{F}_p$, we have*

$$d_4^+(A) \gtrsim \frac{|A|^{48/13}}{|A+A|^{35/13}}.$$

Remark 2.2. *It has been indicated in [17] that the best one can hope for the lower bound of* $d_4^+(A)$ *is as follows:*

$$d_4^+(A) \gtrsim \frac{|A|^3}{|A+A|^2}.$$

Combining this with the bound (3), one gets $\max\{|A+A|, |AA|\} \gg |A|^{5/4}$. *This is still far away from the conjecture.*

In this paper, we will give an upper bound of $d_4^+(A)$ in terms of $|f(A,A)|$ for any non-degenerate quadratic polynomial f as follows.

Lemma 2.3. *Let* $f(x,y) \in \mathbb{F}_p[x,y]$ *be a non-degenerate quadratic polynomial. For* $A \subset \mathbb{F}_p$ *with* $|A| \ll p^{1/2}$, *we have*

$$d_4^+(A) \lesssim \frac{|f(A,A)|^2}{|A|^2}.$$

To prove lemma 2.3, we use the following result in [8].

Theorem 2.4 ([8])**.** *Let* $f \in \mathbb{F}_p[x,y,z]$ *be a quadratic polynomial that depends on each variable and that does not have the form* $g(h(x)+k(y)+l(z))$. *For* $A,B,C \subset \mathbb{F}_p$ *with* $|A||B||C| \ll p^2$, *let* E *be the number of tuples* $(a,b,c,a',b',c') \in (A\times B\times C)^2$ *such that* $f(a,b,c) = f(a',b',c')$. *Then we have*

$$E \ll (|A||B||C|)^{3/2} + (|A|+|B|+|C|)(|A||B||C|) + |B|^2|C|^2.$$

Proof of Lemma 2.3: Let $B \subset \mathbb{F}_p$ be a set maximizing $d_4^+(A)$. By a dyadic decomposition, there exist a number $t > 0$ and a set $D_t := \{x\colon r_{A-B}(x) \geq t\}$ such that

$$E_4^+(A,B) \lesssim |D_t|t^4.$$

Without loss of generality, we assume that $f(x,y) = ax^2 + by^2 + cxy + dx + ey$ with $a \neq 0$. Let $f'(u,v,w) := f(u+v,w)$.

Since $f(x,y)$ is a non-degenerate polynomial, by an elementary calculation (similar to the proof of Lemma 5.1 in [9]), we have $f'(x,y,z)$ is not of the form $g'(h'(x)+k'(y)+l'(z))$ for some polynomials g', h', k', l'.

Consider the following equation

$$f'(u,v,w) = t', \tag{4}$$

with $u \in D_t, v \in B, w \in A, t' \in f(A,A)$.

It easy to check that the number of solutions of the equation (4) is at least $|D_t|t|A|$. Now by the

Cauchy-Schwarz inequality, we have

$$|D_t|t|A| \ll |f(A,A)|^{1/2}E^{1/2}, \tag{5}$$

where E is the number of tuples $(u,v,w,u',v',w') \in (D_t \times B \times A)^2$ such that

$$f'(u,v,w) = f'(u',v',w').$$

Suppose $|D_t||A||B| \ll p^2$. We now consider the following cases:

Case 1**:** If $|D_t| \leq |B|$, then Theorem 2.4 with $A := D_t, B := B, C := A$ gives

$$E \ll (|D_t||B||A|)^{3/2} + (|D_t| + |B| + |A|)(|D_t||B||A|) + |B|^2|A|^2.$$

Case 2**:** If $|D_t| \geq |B|$, then Theorem 2.4 with $A := B, B := D_t, C := A$ gives

$$E \ll (|B||D_t||A|)^{3/2} + (|B| + |D_t| + |A|)(|B||D_t||A|) + |D_t|^2|A|^2.$$

These cases can be handled in the same way. Therefore, without loss of generality, we assume that we are in the first case, i.e. $|D_t| \leq |B|$ (i. e. $|D_t|^2|A||B| \leq |D_t|^{3/2}|A||B|^{3/2}$).

We also can assume that $|B| \leq |D_t||A|$ (i. e. $|B|^2|D_t||A| \leq |B|^{3/2}(|D_t||A|)^{3/2}$), otherwise, using the fact that $|D_t|t \leq |D_t||A| \leq |B|$, we have

$$\frac{|D_t|t^4}{|A||B|^3} \leq \frac{|B|t^3}{|A||B|^3} \leq 1 \leq \frac{|f(A,A)|^2}{|A|^2}.$$

Similarly, we assume that $|A| \leq |D_t||B|$ (i. e. $|A|^2|D_t||B| \leq |A|^{3/2}(|D_t||B|)^{3/2}$). Furthermore, $|D_t| \leq |B|$ and $|B| \leq |A|^{3/2}$ implies that $|D_t|^5 \leq |B|^2|B|^3 \leq |A|^3|B|^3$. With these assumptions, we obtain

$$E \ll (|D_t||A||B|)^{3/2} + (|B||A|)^2.$$

Without loss of generality, let us assume $(|D_t||A||B|)^{3/2} \geq (|B||A|)^2$. (As otherwise, $|D_t|^3 \leq |B||A|$. Hence $\frac{|D_t|t^4}{|A||B|^3} \leq \frac{t^4}{|D_t|^2|B|^2} \leq \frac{t^4}{|D_t|^4} \leq 1 \leq \frac{|f(A,A)|^2}{|A|^2}$, and we are done.) Therefore,

$$|D_t|t^4 \ll \frac{|f(A,A)|^2|B|^3}{|A|},$$

and we are done by the definition of $d_4^+(A)$.

Now suppose $|D_t||A||B| \gg p^2$. We can use the point-plane incidence bound due to Vinh [18] for large sets in the proofs of Lemmas 2.2 and 2.3 in [11] to obtain an upper bound of E. More

precisely, we are able to obtain the following version of Lemma 5.1 in [9] for large sets.

Lemma 2.5. *Let $\mathbb{F}_p$ be a prime field. Let $f(x,y,z) \in \mathbb{F}_p[x,y,z]$ be a quadratic polynomial that depends on each variable and is not of the form $g(h(x)+k(y)+l(z))$. Let $A,B,C \subset \mathbb{F}_p$, then we have*

$$\left|\left\{(x,y,z,x',y',z') \in (A\times B\times C)^2 : f(x,y,z) = f\left(x',y',z'\right)\right\}\right| \leq \frac{(|A||B||C|)^2}{p} + p|A||B||C|.$$

Therefore, by Lemma 2.5 assuming $|D_t||A||B| \gg p^2$, we have the following upper bound on E

$$E \ll \frac{|D_t|^2|A|^2|B|^2}{p}.$$

Substituting this inequality to (5) we get

$$pt^2 \leq |f(A,A)||B|^2. \tag{6}$$

Since $|A| \leq p^{1/2}$ and $|B| \leq |A|^{3/2}$, we have

$$|B|^2|f(A,A)| \leq |A||B|^{4/3}|f(A,A)| \ll \frac{p}{|A|}\cdot|B|^{2/3}\cdot\frac{|f(A,A)|^{4/3}}{|A|1/3}.$$

Therefore, it follows from (6) that

$$\begin{aligned} pt^2 &\ll p\frac{|B|^{4/3}|f(A,A)|^{4/3}}{|A|^{4/3}} \\ \Rightarrow t^3 &\ll \frac{|B|^2|f(A,A)|^2}{|A|^2}. \end{aligned}$$

And, since $|D_t|t \leq |A||B|$,

$$E_4(A,B) \lesssim |D_t|t^4 = (|D_t|t).t^3 \ll |A||B|.\frac{|B|^2|f(A,A)|^2}{|A|^2} = \frac{|B|^3|f(A,A)|^2}{|A|}.$$

Theorem 1.6 follows by combining Lemma 2.1 and Lemma 2.3.

Remark 2.6. *It is clear that if $f(x,y) = xy$, then Theorem 1.6 is weaker than Theorem 1.3. In our general setting, the main difficulty arises when we want to give an upper bound for $E_2^+(A,A-A)$ in terms of $|f(A,A)|$, where $E_2^+(A,B)$ is the number of tuples $(a_1,a_2,b_1,b_2) \in A^2\times B^2$ such that $a_1-b_1 = a_2-b_2$. For all non-degenerate quadratic polynomials, it seems very difficult to give*

such an upper bound, but for some special families of polynomials it is possible. For instance, if $f(x,y) = g(x)(h(x)+y)$ is a function defined on $\mathbb{F}_p^* \times \mathbb{F}_p^*$, where $g, h\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ are arbitrary functions, then one can follow the proof of [10, Theorem 1.6*] to derive the following:*

$$E_2^+(B,C) \ll |A|^{-2}\left(|f(A,B)|^{3/2}|A|^{3/2}|C|^{3/2} + k|f(A,B)|A||C|\right),$$

where $k \leq \max\{|A|,|C|,|f(A,B)|\}$ under the assumption $|f(A,B)||A||C| \ll p^2$.

Acknowledgments. The author would like to thank Ben Lund for reading the manuscript carefully and for helpful comments, and also the referees for their valuable suggestions.

3 References

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

[2] B. Bukh, J. Tsimerman, *Sum–product estimates for rational functions*, Proceedings of the London Mathematical Society, **104**(1) (2012), 1-26.

[3] C. Chen, B. Kerr, A. Mohammadi, *A new sum-product estimate in prime fields*, arXiv:1807.10998, 2018.

[4] P. Erdős, E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics. To the memory of Paul Turan, Basel: Birkhäuser Verlag, pp. 213-218, 1983.

[5] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc., **136**(2008), 2735–2739.

[6] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. no. 5, (2007) Art. ID rnm007.

[7] A. Iosevich, D. Koh, T. Pham, *A new perspective on the distance problem over prime fields*, arXiv:1905.04179, 2019.

[8] D. Koh, M. Mirzaei, T. Pham, C. Shen, *Exponential sum estimates over prime fields*, `arXiv:1809.06837` (2018).

[9] D. Koh, H. Mojarrad, T. Pham, C. Valculescu, *Four-variable expanders over the prime fields*, Proceedings of the American Mathematical Society, **146**(12) (2018), 5025–5034.

[10] H. Mojarrad, T. Pham, *Conditional expanding bounds for two-variable functions over arbitrary fields*, Journal of Number Theory, **186** (2018): 137–146.

[11] T. Pham, L. A. Vinh, and F. De Zeeuw, *Three-variable expanding polynomials and higher-dimensional distinct distances*, Combinatorica, DOI: 10.1007/s00493-017-3773-y, 2018.

[12] O. Roche-Newton, M. Rudnev, and I.D. Shkredov, *New sum-product type estimates over finite fields*, Advances in Mathematics **293** (2016), 589–605.

[13] M. Rudnev, G. Shakan, I. Shkredov, *Stronger sum-product inequalities for small sets*, arXiv:1808.08465 (2018).

[14] C. Shen, *Algebraic methods in sum-product phenomena*, Israel J. Math. **188**(1) (2012), 123–130.

[15] I.D. Shkredov, *Some new results on higher energies*, Transactions of MMS, **74**(1) (2013), 35–73.

[16] I.D. Shkredov, *Energies and structure of additive sets*, Electronic Journal of Combinatorics, **21**(3) (2014), #P3.44, 1–53.

[17] G. Shakan, and I. D. Shkredov, *Breaking the* $6/5$ *threshold for sums and products modulo a prime*, arXiv:1806.07091 (2018).

[18] L. A. Vinh, *The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields*, Euro. J. Combin. **32** (2011), no. 8, 1177-1181.

[19] V. Vu, *Sum-product estimates via directed expanders*, Math. Res. Lett. **15** (2008), no. 2, 375-388.