Journal of Number Theory 218 (2021) 223–233

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Moderate expanders over rings

Dao Nguyen Van Anh [a], Le Quang Ham [b], Doowon Koh [c], Mozhgan Mirzaei [d], Hossein Mojarrad [e], Thang Pham [f,*]

[a] *The Olympia Schools Hanoi, Hanoi, Viet Nam*
[b] *Hanoi University of Science, Viet Nam*
[c] *Chungbuk National University, Republic of Korea*
[d] *University of California San Diego, USA*
[e] *New York University, USA*
[f] *University of Rochester New York, USA*

ARTICLE INFO

Article history:
Received 14 February 2020
Received in revised form 22 July 2020
Accepted 30 July 2020
Available online 13 August 2020
Communicated by A. Pal

Keywords:
Finite fields
Expanders
Local rings
Polynomials

ABSTRACT

In this note, we provide a large class of *moderate expanders* with the exponents $\frac{3}{8}$ and $\frac{5}{13}$ over arbitrary finite fields and prime fields, respectively. Our main ingredients are an energy result due to the third, fourth, sixth listed authors and Shen (2019) and a theorem on two-variable expanding functions given by Hegyvári and Hennecart (2009). Using the same approach, we derive similar results in the setting of finite local and principal rings.

© 2020 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_q$ be an arbitrary finite field of order q, where q is a prime power. We first recall the following definition from [5].

* Corresponding author.
E-mail addresses: anh.dnv@theolympiaschools.edu.vn (D.N.V. Anh), hamlaoshi@gmail.com (L.Q. Ham), koh131@chungbuk.ac.kr (D. Koh), momirzae@ucsd.edu (M. Mirzaei), hossein.mojarrad70@gmail.com (H. Mojarrad), vanthangpham@rochester.edu (T. Pham).

https://doi.org/10.1016/j.jnt.2020.07.009
0022-314X/© 2020 Elsevier Inc. All rights reserved.

Definition 1.1. Let $f: \mathbb{F}_q^l \to \mathbb{F}_q$.

- The function f is called a strong expander with the exponent ϵ if for all $A \subset \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A,\dots,A)| \geq q-k$, for some fixed positive constant k.
- The function f is called a moderate expander with the exponent ϵ if for all $A \subset \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A,\dots,A)| \gg q$.
- The function f is called a weak expander with parameters $0<\epsilon<1$ and $0<\delta<1$ if for all $A \subset \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A,\dots,A)| \geq |A|^{\delta} q^{1-\delta}$.

Throughout this paper, we use $X \ll Y$ if $X \leq CY$ for some constant $C>0$ independent of the parameters related to X and Y, and write $X \gg Y$ for $Y \ll X$. The notation $X \sim Y$ means that both $X \ll Y$ and $Y \ll X$ hold. In addition, we use $X \lesssim Y$ to indicate that $X \ll (\log Y)^{C'} Y$ for some constant $C'>0$.

Over the past 10 years, there has been an intensive progress on seeking moderate expanders with biggest exponents. For instance, the followings are moderate expanders with the exponent $\frac{1}{3}$: $x+yz$ [15], $x+(y-z)^2$ and $x(y+z)$ [19], $(x-y)^2+(z-t)^2$ [2,4], $xy+zt$ [3], $xy+z+t$ [14]. We also know that $(x-y)(z-t)$ is a moderate expander with the exponent $\frac{1}{3}$ in [1], which has been slightly improved to $\frac{1}{3}+\frac{1}{13542}$ in [9].

Using spectral graph theory techniques, Vinh [19] proved that the polynomial $xy+(z-t)^2$ is a moderate expander with the exponent $\frac{3}{8}=\frac{1}{3}+\frac{1}{24}$. To the best knowledge of the authors, this is the only known polynomial moderate expander with the exponent $\frac{3}{8}$ over arbitrary finite fields in the literature. In the setting of prime fields, Rudnev, Shkredov, and Stevens [13] also proved that the function $\frac{xy-z}{x-t}$ is a moderate expander with the exponent $\frac{17}{42}=\frac{1}{3}+\frac{1}{14}$ over prime fields.

In the case of two-variable polynomial expanders, Tao [17] proved that any polynomial in two variables which is not of the form $Q(F(x)+G(y))$ or $Q(F(x)G(y))$, for some polynomials Q,F,G, is a moderate expander over $\mathbb{F}_q$ with the exponent $\frac{1}{16}$.

In this note, we provide a large class of polynomial moderate expanders with the exponents $\frac{3}{8}$ and $\frac{5}{13}$ over arbitrary finite fields and prime fields, respectively. Our main ingredients are an energy result due to the third, fourth, sixth listed authors and Shen (2019) and a theorem on two-variable expanding functions given by Hegyvári and Hennecart (2009). Using the same approach, we derive similar results in the setting of finite local and principal rings.

We will see in our first result that there are actually many moderate expanders with the exponent $\frac{3}{8}$ over arbitrary finite fields.

Let $m(x)$ and $n(x)$ be polynomials with integer coefficients. We say that $m(x)$ and $n(x)$ are affinely independent if there is no $(\lambda,\beta) \in \mathbb{Z}\times\mathbb{Z}$ such that $m(x)=\lambda\cdot n(x)+\beta$ or $n(x)=\lambda\cdot m(x)+\beta$. Our first result is as follows.

Theorem 1.1. *Let $\mathbb{F}_q$ be an arbitrary finite field. Let $f \in \mathbb{F}_q[x,y,z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x)+k(y)+l(z))$. Let $m(x)$ and $n(x)$ be affinely independent polynomials with bounded degrees. Define*

$Q(u,v) := m(u)+u^k n(v)$, and $F(u,v,y,z) := f\,(Q(u,v),y,z)$, where k is a fixed positive integer. For $A \subset \mathbb{F}_q$ with $|A| \gg q^{\frac{5}{8}}$, we have

$$|F(A,A,A,A)| \gg q.$$

Corollary 1.2. *The following 4-variable polynomials are moderate expanders with the exponent $\frac{3}{8}$ over arbitrary finite fields:*

$$u(u+v)y+z, \quad u(u+v)+yz, \quad u(u+v)(y+z)$$
$$y\,(u(u+v)+z)\,, \quad (u(u+v)-y)^2+z, \quad (y-z)^2+u(u+v).$$

Proof. This follows directly from Theorem 1.1 with the following polynomials: $xy+z,\ x+yz,\ x(y+z),\ y(x+z),\ (x-y)^2+z,\ (y-z)^2+x$, respectively. □

In the setting of prime fields, using recent new results in incidence geometry, one can prove that polynomials in Theorem 1.1 are moderate expanders with bigger exponents.

Theorem 1.3. *Let $\mathbb{F}_p$ be a prime field. 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 $g(h(x)+k(y)+l(z))$. Let $m(x)$ and $n(x)$ be affinely independent polynomials with bounded degrees. Define $Q(u,v) := m(u)+u^k n(v)$, and $F(u,v,y,z) := f\,(Q(u,v),y,z)$, where k is a fixed positive integer. For $A \subset \mathbb{F}_p$ with $|A| \gg p^{\frac{8}{13}}$, we have*

$$|F(A,A,A,A)| \gg p.$$

Corollary 1.4. *The following 4-variable polynomials are moderate expanders with the exponent $\frac{5}{13}$ over prime fields:*

$$u(u+v)y+z, \quad u(u+v)+yz, \quad u(u+v)(y+z)$$
$$y\,(u(u+v)+z)\,, \quad (u(u+v)-y)^2+z, \quad (y-z)^2+u(u+v).$$

Proof. This follows directly from Theorem 1.3 with the following polynomials: $xy+z,\ x+yz,\ x(y+z),\ y(x+z),\ (x-y)^2+z,\ (y-z)^2+x$, respectively. □

An extension to finite local and principal rings A ring $\mathcal{R}$ is *local* if $\mathcal{R}$ has a unique maximal ideal that contains every proper ideal of $\mathcal{R}$. A finite valuation ring $\mathcal{R}$ is a finite ring that is local and principle.

Let $\mathcal{R}$ be a finite valuation ring of order q^r, where $q = p^n$ is an odd prime number. Throughout this paper, we assume $\mathcal{R}$ is commutative, and also it has an identity. Let $\mathcal{R}^\times$ denote the set of units in $\mathcal{R}$. Likewise, let $\mathcal{R}^0$ denote the set of non-units in $\mathcal{R}$. Since $\mathcal{R}$ has a unique maximal ideal that contains every proper ideals of $\mathcal{R}$, we have a non-unit $z \in \mathcal{R}$ so that the maximal ideal is generated by z. Let (z) denote the maximal ideal of

$\mathcal{R}$. Throughout, q and r will denote the structural parameters associated to $\mathcal{R}$. For the maximal ideal (z), r is the smallest positive integer such that $z^r = 0$, and also q is the size of the residue field $\mathcal{R}/(z)$. We assume q is an odd prime number. Hence, 2 is a unit in $\mathcal{R}$.

For more details on finite valuation rings and earlier sum-product results over $\mathcal{R}$, we refer the interested reader to [8,10,11] and references therein.

Here are some examples of finite valuation rings.

(1) Finite fields $\mathbb{F}_q, q = p^n$ for some $n > 0$.
(2) Finite rings $\mathbb{Z}/p^r\mathbb{Z}$, where p is a prime.
(3) $\mathbb{F}_q[x]/(f^r)$, where $f \in \mathbb{F}_q[x]$ is an irreducible polynomial.
(4) $\mathcal{O}/(p^r)$ where $\mathcal{O}$ is the ring of integers in a number field and $p \in \mathcal{O}$ is a prime.

In general, there are many zero divisors in $\mathcal{R}$, so it seems difficult to extend Theorem 1.1 to the setting of finite valuation rings. However, we are able to put Corollary 1.2 in this setting.

Theorem 1.5. *Let $\mathcal{R}$ be a finite valuation ring of order q^r, and A be a set in $\mathcal{R}$.*

Let $F_1(u,v,y,z) = u(u+v)y + z$, $F_2(u,v,y,z) = u(u+v) + yz$, $F_3(u,v,y,z) = u(u+v)(y+z)$, $F_4(u,v,y,z) = y\,(u(u+v)+z)$, $F_5(u,v,y,z) = (u(u+v)-y)^2+z$, and $F_6(u,v,y,z) = (y-z)^2+u(u+v)$. Suppose that $|A| \gg q^{\frac{8r-3}{8}}$, then, for each $i \in \{1,\dots,6\}$, we have

$$|F_i(A,A,A,A)| \gg q^r.$$

2. Moderate expanders over arbitrary finite fields (Theorem 1.1)

Using a point-plane incidence bound due to Rudnev [12], the third, fourth, sixth listed authors and Shen [7] proved the following general theorem on the energy of a polynomial in three variables over prime fields.

Theorem 2.1 *([7], Lemma 2.5). Suppose that $f \in \mathbb{F}_p[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. For $U,V,W \subset \mathbb{F}_p^\times$ with $|U||V||W| \ll p^2$, let E be the number of tuples $(u,v,w,u',v',w') \in (U\times V\times W)^2$ such that $f(u,v,w) = f(u',v',w')$. Then we have*

$$E \ll (|U||V||W|)^{3/2} + \max\{|V|^2|W|^2, |V|^2|U|^2, |U|^2|W|^2\}.$$

One can follow the proof of this theorem in [7] identically and use Vinh's point-plane incidence bound [18] in the place of Rudnev's point-plane incidence bound and the Kövari-Sós-Turán theorem to obtain a version over arbitrary finite fields. For simplicity, we omit the proof.

Theorem 2.2. *Suppose that $f \in \mathbb{F}_q[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. For $U,V,W \subset \mathbb{F}_q^\times$, let E be the number of tuples $(u,v,w,u',v',w') \in (U\times V\times W)^2$ such that $f(u,v,w) = f(u',v',w')$. If $|U||V||W| \geq q^2$, then*

$$E \ll \frac{|U|^2|V|^2|W|^2}{q} + \max\{|V|^2|W|^2, |V|^2|U|^2, |U|^2|W|^2\}.$$

The next corollary is a direct application of the Cauchy-Schwarz inequality and Theorem 2.2.

Corollary 2.3. *Suppose that $f \in \mathbb{F}_q[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. If $U,V,W \subset \mathbb{F}_q^\times$ with $|U||V||W| \gg q^2$, then*

$$|f(U,V,W)| \gg \min\left\{q,\ |U|^2,\ |V|^2,\ |W|^2\right\}.$$

Let $m(x)$ and $n(x)$ be affinely independent polynomials. Suppose that the degrees of m and n are bounded. In [6], Hegyvári and Hennecart proved that the polynomial $Q(u,v) = m(u) + u^k n(v)$ is an expander. More precisely, for $A \subset \mathbb{F}_p$ with $|A| \leq p^{1-\epsilon}$ for some $0 < \epsilon < 1$, we have

$$|Q(A,A)| \gg |A|^{1+\epsilon'},$$

where $\epsilon' > 0$ depending on ϵ.

Using the point-line incidence bound for large sets over arbitrary finite fields due to Vinh [18], and the point-line incidence bound for small Cartesian product sets over prime fields due to Stevens and De Zeeuw [16], the following is a consequence of [6, Theorem 4] due to Hegyvári and Hennecart.

Lemma 2.4 *([6]). Let $m(x)$ and $n(x)$ be affinely independent polynomials. Suppose that the degrees of m and n are bounded. Define $Q(u,v) := m(u) + u^k n(v)$.*

1. *For $A \subset \mathbb{F}_q$, we have*

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

2. *For $A \subset \mathbb{F}_p$ with $|A| \leq p^{2/3}$, we have*

$$|Q(A,A)| \gg |A|^{5/4}.$$

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Since $|A| > 2$, without loss of generality, we may assume that $0 \notin A$. We define $U := \{Q(a,b)\colon a,b \in A\}$. It follows from Lemma 2.4 that

$$|U| \gg \min\left\{q, \frac{|A|^2}{q^{1/2}}\right\}.$$

Let $U^* = U \setminus \{0\}$. We also have

$$|U^*| \gg \min\left\{q, \frac{|A|^2}{q^{1/2}}\right\}.$$

When $|A| \gg q^{5/8}$, this inequality implies that $|A||A||U^*| \gg q^2$. Thus we can apply Corollary 2.3 so that

$$|F(A,A,A,A)| = |f(U,A,A)| \geq |f(U^*,A,A)| \gg \min\left\{q,\ |U^*|^2,\ |A|^2\right\} \gg q,$$

under the assumption $|A| \gg q^{5/8}$. This completes the proof of the theorem. □

3. Moderate expanders over prime fields (Theorem 1.3)

As in the previous section, the following corollary is a direct application of Theorem 2.1 and the Cauchy-Schwarz inequality.

Corollary 3.1. *Suppose that $f \in \mathbb{F}_p[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. For $U,V,W \subset \mathbb{F}_p^\times$ with $|U||V||W| \ll p^2$, we have*

$$|f(U,V,W)| \gg \min\left\{(|U||V||W|)^{1/2},\ |U|^2,\ |V|^2,\ |W|^2\right\}.$$

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Since $|A| > 2$, without loss of generality, we may assume that $0 \notin A$.

Set $U := \{Q(a,b)\colon a,b \in A\}$. It follows from Lemma 2.4 that

$$|U| \gg |A|^{5/4},$$

under the condition $|A| \leq p^{2/3}$.

Since $\frac{8}{13} \leq \frac{2}{3}$, for our purpose, there is no harm to assume that $|A| \leq p^{\frac{2}{3}}$ in the rest of the proof.

Let $U^* = U \setminus \{0\}$. We also have $|U^*| \gg |A|^{5/4}$.

Set $V = W = A$. It is not hard to see that $F(A,A,A,A) = f(U,V,W)$.

If $|U||A|^2 \gg p^2$, then it follows from Corollary 2.3 that $|F(A,A,A,A)| \gg p$ and we are done.

Therefore, we assume that $|U||A|^2 \ll p^2$, and apply Corollary 3.1 to get

$$|F(A,A,A,A)| = |f(U,V,W)| \geq |f(U^*,V,W)| \gg \min\left\{(|U^*||A|^2)^{1/2},\ |A|^2,\ |U^*|^2\right\}.$$

Using the fact that $|U^*| \gg |A|^{5/4}$, the theorem follows. □

4. Moderate expanders over finite valuation rings (Theorem 1.5)

In order to prove Theorem 1.5, the following results play crucial roles. Recall that $\mathcal{R}$ denotes the finite valuation ring of order q^r.

The first result is a point-line incidence bound over finite valuation rings due to Pham and Vinh [11], where a line over $\mathcal{R}$ is defined of the form $ax + by + c = 0$ with $(a,b,c) \notin (\mathcal{R}^0)^3$.

Theorem 4.1. *Let P be a set of points in $\mathcal{R}^2$ and L be a set of lines in $\mathcal{R}^2$. The number of incidences between P and L, denoted by $I(P,L)$, satisfies*

$$I(P,L) \leq \frac{|P||L|}{q^r} + q^{r-\frac{1}{2}}\sqrt{|P||L|}.$$

The second result is due to Yazici in [20].

Lemma 4.2. *Let X, Y, Z be sets in $\mathcal{R}$. We have*

$$|XY + Z| \gg \min\left\{q^r, \frac{|X||Y||Z|}{q^{2r-1}}\right\}.$$

Our next two lemmas are consequences of Theorem 4.1.

Lemma 4.3. *Let X, Y, Z be sets in $\mathcal{R}$. If $|X| \geq 2q^{r-1}$, then*

$$|X(Y + Z)| \gg \min\left\{q^r,\ \frac{|X||Y||Z|}{q^{2r-1}}\right\}.$$

Proof. We recall that $\mathcal{R}^0$ is the set of non-units in $\mathcal{R}$. Since $|X| \geq 2q^{r-1}$ and $|\mathcal{R}^0| = q^{r-1}$, without loss of generality we may assume that $X \subset \mathcal{R}^\times$. Let $T = X(Y + Z)$ and let us consider the following equation

$$y = a(x + c)$$

with $a \in X, x \in Y, c \in Z$, and $y \in T$. Let N denote the number of solutions of the above equation. It is clear that

$$|X||Y||Z| \leq N. \tag{1}$$

We now find an upper bound of N. Let L be a collection of lines of the form $y = a(x+c)$ with $a \in X$ and $c \in Z$. In addition, define P as the set of points (x, y) with $x \in Y$ and $y \in T$. Since $a \in \mathcal{R}^\times$, the lines in L are distinct. It is clear that $|L| = |X||Z|$ and $|P| = |Y||T|$. It is not hard to see that $N = I(P, L)$ which is the number of incidences between L and P. Hence, using Theorem 4.1, we have

$$N \leq \frac{|X||Y||Z||T|}{q^r} + q^{r-\frac{1}{2}}\sqrt{|X||Y||Z||T|}.$$

Combining the above inequality with (1), we have

$$|T| = |X(Y+Z)| \gg \min\left\{q^r, \frac{|X||Y||Z|}{q^{2r-1}}\right\},$$

as required. □

Lemma 4.4. *Let X, Y, Z be sets in $\mathcal{R}$. We have*

$$|(X-Y)^2 + Z| \gg \min\left\{q^r, \frac{|X||Y||Z|}{q^{2r-1}}\right\}.$$

Notice that Lemma 4.4 will also be used to give a new distance result in the p-adic perspective in the next section.

Proof. We consider the following equation

$$(x-y)^2 + z = t,$$

where $x \in X, y \in Y, z \in Z, t \in T := (X-Y)^2 + Z$.

Let N be the number of solutions of this equation. We can see that $N \geq |X||Y||Z|$.

Define $P := X \times T$ and C being the set of curves of the form $t = (x-a)^2 + c$ with $a \in Y$ and $c \in Z$. It is clear that N is bounded by the number of incidences between points in P and curves in C.

Let φ be a map from $\mathcal{R}^2$ to $\mathcal{R}^2$, which maps the point (x, t) to $(x, t - x^2)$. It is clear that φ is a bijection. Under this map, the curve $t = (x-a)^2 + c$ in C will be sent to the line $t' = -2xa + c + a^2$. Furthermore, we also have that the number of incidences between P and C is equal to the number of incidences between the point set $\varphi(P)$ and the line set $\varphi(C)$.

Applying Theorem 4.1, we have

$$N \leq \frac{|P||C|}{q^r} + q^{\frac{2r-1}{2}}\sqrt{|P||C|},$$

where we have used the fact that $|\varphi(P)| = |P|, |\varphi(C)| = |C|$.

By using $|P| = |X||T|, |C| = |Y||Z|$, and $N \geq |X||Y||Z|$, we obtain the desired estimate. □

The following result is very important in the proof of Theorem 1.5.

Lemma 4.5. *Let A be a set in $\mathcal{R}$. Suppose that $|A| \geq 2q^{r-1}$, then we have*

$$|\{a(a+b)\colon a,b \in A\}| \gg \min\left\{q^r, \frac{|A|^2}{q^{\frac{2r-1}{2}}}\right\}.$$

Proof. Since $|A| \gg q^{r-1} = |(z)|$, we may assume that $A \subset \mathcal{R}^\times$. Let N be the size of the set $\{a^2+ab\colon a,b \in A\}$. By the Cauchy-Schwarz inequality, we have

$$N \geq \frac{|A|^4}{E},$$

where E is the number of quadruples $(a,b,a',b') \in A^4$ such that

$$a^2+ab = a'^2+a'b'.$$

Let L be the set of lines of the form $ax-a'y = a'^2-a^2$ with $a,a' \in A$, and P be the set of points (b,b') with $b,b' \in A$. It is not hard to see that $|L| = |P| = |A|^2$. We have $E = I(P,L)$.

Let L' be the subset of L that contains lines $ax-a'y = a'^2-a^2$ with $a'^2-a^2 \in \mathcal{R}^0$. Since $|\mathcal{R}^0| = q^{r-1}$ and $A \subset R^\times$, we have the number of pairs $(a,a') \in A^2$ such that $a'^2-a^2 \in \mathcal{R}^0$ is bounded by $2q^{r-1}|A|$. On the other hand, for each such pair (a,a') and each $b \in A$, the number of $b' \in A$ satisfying $a^2+ab = a'^2+a'b'$ is at most one. Thus, $I(P,L') \leq 2|A|^2q^{r-1}$.

It is not hard to check that the lines in $L \setminus L'$ are distinct.

Applying Theorem 4.1 we have

$$I(P,L\setminus L') \leq \frac{|P||L|}{q^r} + q^{r-\frac{1}{2}}\sqrt{|P||L|} = \frac{|A|^4}{q^r} + q^{r-\frac{1}{2}}|A|^2.$$

By an elementary calculation, we have

$$E = I(P,L\setminus L') + I(P,L') \ll \frac{|A|^4}{q^r} + q^{r-\frac{1}{2}}|A|^2,$$

which implies that

$$N \gg \min\left\{q^r, \frac{|A|^2}{q^{\frac{2r-1}{2}}}\right\},$$

and the theorem follows. □

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. Since $|A| \gg q^{r-\frac{3}{8}} > |(z)| = q^{r-1}$, without loss of generality, we assume that A is a subset of $\mathcal{R}^\times$.

We now start with the case of $F_1 = u(u+v)y + z$.

Set $X = \{u(u+v)\colon u, v \in A\}, Y = Z = A$. It follows from Lemma 4.5 that

$$|X| \gg \min\left\{q^r, \frac{|A|^2}{q^{\frac{2r-1}{2}}}\right\}.$$

On the other hand, it is not hard to see that

$$|F_1(A,A,A,A)| = |XA + A|.$$

Lemma 4.2 tells us that

$$|XA + A| \gg \min\left\{q^r, \frac{|A|^2}{q^{r-1}}, \frac{|A|^4}{q^{\frac{6r-3}{2}}}\right\} \gg q^r,$$

whenever $|A| \gg q^{\frac{8r-3}{8}}$. This completes the proof in the case of F_1. The same proof holds for the case of F_2 by switching the roles of X, Y, and Z if necessary.

For any F_i with $3 \leq i \leq 6$, the proof is almost the same as that for F_1 except that we have to use Lemma 4.3 (for F_3 and F_4) or Lemma 4.4 (for F_5 and F_6) instead of Lemma 4.2 □

Acknowledgments

The authors are grateful to Ilya Shkredov and the referee for useful comments and suggestions.

D. Koh was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology, Grant number NRF-2018R1D1A1B07044469. M. Mirzaei was supported by NSF grant DMS-1800736. H. Mojarrad was supported by Swiss National Science Foundation grant P2ELP2-178313. T. Pham was supported by Swiss National Science Foundation grant P400P2-183916.

References

[1] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, M. Rudnev, Group actions and geometric combinatorics in $\mathbb{F}_q^d$, Forum Math. 29 (1) (2017) 91–110.

[2] J. Chapman, M.B. Erdogan, D. Hart, A. Iosevich, D. Koh, Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates, Math. Z. 271 (1–2) (2012) 63–93.

[3] D. Hart, A. Iosevich, Sums and products in finite fields: an integral geometric viewpoint, in: Radon Transforms, Geometry, and Wavelets, in: AMS Contemporary Mathematics, vol. 464, AMS, RI, 2008, pp. 129–136.

[4] D. Hart, A. Iosevich, D. Koh, M. Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture, Trans. Am. Math. Soc. 363 (2011) 3255–3275.

[5] D. Hart, L. Li, C-Y. Shen, Fourier analysis and expanding phenomena in finite fields, Proc. Am. Math. Soc. 141 (2) (2013) 461–473.
[6] N. Hegyvári, F. Hennecart, Explicit constructions of extractors and expanders, Acta Arith. 140 (2009) 233–249.
[7] D. Koh, M. Miraei, T. Pham, C-Y. Shen, Exponential sum estimates over prime fields, Int. J. Number Theory 16 (2020) 291–308.
[8] H. Le, T. Pham, V. Le, Conditional expanding bounds for two-variable functions over finite valuation rings, Eur. J. Comb. 60 (2017) 114–123.
[9] B. Murphy, G. Petridis, Products of differences over arbitrary finite fields, arXiv:1705.06581, 2017.
[10] B. Nica, Unimodular graphs and Eisenstein sums, J. Algebraic Comb. 45 (2) (2017) 423–454.
[11] T. Pham, Le Anh Vinh, Some combinatorial number theory problems over finite valuation rings, Ill. J. Math. 61 (1–2) (2017) 243–257.
[12] M. Rudnev, On the number of incidences between points and planes in three dimensions, Combinatorica 38 (1) (2018) 219–254.
[13] M. Rudnev, I. Shkredov, S. Stevens, On the energy variant of the sum-product conjecture, Rev. Mat. Iberoam. (2018), in press.
[14] A. Sárközy, On sums and products of residues modulo p, Acta Arith. 118 (4) (2005) 403–409.
[15] I.E. Shparlinski, On the solvability of bilinear equations in finite fields, Glasg. Math. J. 50 (3) (2008) 523–529.
[16] S. Stevens, F. De Zeeuw, An improved point-line incidence bound over arbitrary fields, Bull. Lond. Math. Soc. 49 (5) (2017) 842–858.
[17] T. Tao, Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets, Contrib. Discrete Math. 10 (1) (2015).
[18] L.A. Vinh, A Szemerédi-Trotter type theorem and sum-product estimate over finite fields, Eur. J. Comb. 32 (8) (2011) 1177–1181.
[19] L.A. Vinh, On four-variable expanders in finite fields, SIAM J. Discrete Math. 27 (4) (2013) 2038–2048.
[20] E. Yazici, Sum-product type estimates for subsets of finite valuation rings, Acta Arith. 185 (1) (2018).