Research Article

Le Quang Ham, Nguyen Van The, Phuc D. Tran and Le Anh Vinh*

On three-variable expanders over finite valuation rings

https://doi.org/10.1515/forum-2020-0203
Received August 2, 2020; revised August 17, 2020

Abstract: Let \( R \) be a finite valuation ring of order \( q^r \). In this paper, we prove that for any quadratic polynomial \( f(x, y, z) \in R[x, y, z] \) that is of the form \( axy + R(x) + S(y) + T(z) \) for some one-variable polynomials \( R, S, T \), we have
\[
|f(A, B, C)| \gg \min\left\{ q^r, \frac{|A||B||C|}{q^{2r-1}} \right\}
\]
for any \( A, B, C \subset R \). We also study the sum-product type problems over finite valuation ring \( R \). More precisely, we show that for any \( A \subset R \) with \( |A| \gg q^{-r} \), then \( \max(|AA|, |A^d + A^d|), \max(|A + A|, |A^2 + A^2|), \max(|A - A|, |AA + AA|) \gg |A|^\frac{3}{2} q^2 \), and \( |f(A) + A| \gg |A|^\frac{5}{2} q^5 \) for any one variable quadratic polynomial \( f \).

Keywords: Expanders, finite valuation rings, sum product estimates

MSC 2010: 05D99

Communicated by: Christopher D. Sogge

1 Introduction

Let \( \mathbb{F}_q \) be a finite field of order \( q \), where \( q \) is an odd prime power. Given a function \( f: \mathbb{F}_q^d \rightarrow \mathbb{F}_q \), the set
\[
f(A, \ldots, A) = \{ f(a_1, \ldots, a_d) : a_1, \ldots, a_d \in A \}
\]
is called the image of the set \( A^d \subset \mathbb{F}_q^d \) under the function \( f \). We will use the following definition of expander polynomials, which can be found in [11].

Definition 1.1. Let \( f \) be a function from \( \mathbb{F}_q^d \) to \( \mathbb{F}_q \).
1. The function \( f \) is called a strong expander with the exponent \( \varepsilon > 0 \) if for all \( A \subset \mathbb{F}_q \) with \( |A| \gg q^{1-\varepsilon} \), one has \( |f(A, \ldots, A)| \gg q - k \) for some fixed constant \( k \).
2. The function \( f \) is called a moderate expander with the exponent \( \varepsilon > 0 \) if for all \( A \subset \mathbb{F}_q \) with \( |A| \gg q^{1-\varepsilon} \), one has \( |f(A, \ldots, A)| \gg q \).

Here and throughout, \( X \ll Y \) means that there exists some absolute constant \( C_1 > 0 \) such that \( X \leq C_1 Y, X \geq Y \) means \( X \gg (\log Y)^{-C_2} Y \) for some absolute constant \( C_2 > 0 \), and \( X \sim Y \) means \( X \ll Y \ll X \).

The study of expander polynomials over finite fields has been of much research interest in recent years. For two variable expanders, Tao [19] gave a general result that for any polynomial \( P(x, y) \in \mathbb{F}_q[x, y] \) that is not
one of the forms $Q(F_1(x) + F_2(y))$ and $Q(F_1(x)F_2(y))$ for some one variable polynomials $Q, F_1, F_2$, we have

$$|P(A, A)| \gg q,$$

under the assumption $|A| \gg q^{1 - \epsilon}$. This implies that such polynomials $P(x, y)$ are moderate expanders with the exponent $\epsilon = \frac{1}{15}$.

For three variable expanders over prime fields, Pham, de Zeeuw and the fourth listed author [16] showed that any quadratic polynomial in three variables $P \in \mathbb{F}_p[x, y, z]$ that is not independent on any variable and that does not have the form $G(H(x) + K(y) + L(z))$ for some one variable polynomials $G, H, K, L$ is a moderate expander with the exponent $\epsilon = \frac{1}{3}$. Note that the exponent $\frac{1}{3}$ can be improved in the case of rational function expanders. More precisely, Rudnev, Shkredov and Stevens [17] showed that the function $(xy - z)(x - t)^{-1}$ is a moderate expander with the exponent $\epsilon = \frac{17}{22}$ over prime fields.

Over general finite fields, for three and four variable expanders, there are several known families of moderate expanders with the exponent $\epsilon = \frac{1}{4}$ constructed by various authors. For example, the expander $(x - y)(z - t)$ is constructed by Bennett, Hart, Iosevich, Pakianathan and Rudnev [4], the expander $x + yz$ is constructed by Hart and Iosevich [10], the expander $x + y + z$ is constructed by Shparlinski [18], and the expanders $x(y + z)$ and $x + (y - z)^2$ are constructed by the fourth listed author [20]. Using methods from spectral graph theory, one can break the exponent $\frac{1}{4}$ by showing that $(x - y)^2 + z$ is a moderate expander with $\epsilon = \frac{2}{5}$, see [20]. Until now, there is no constructed moderate expander with a better exponent.

Let $\mathcal{R}$ be a finite valuation ring of order $q^r$. Throughout, $\mathcal{R}$ is assumed to be commutative, and to have an identity. Let us denote the set of units, non-units in $\mathcal{R}$ by $\mathcal{R}^*, \mathcal{R}^0$, respectively.

In the setting of finite valuation ring, the study of expanding polynomials have been of great interest and was considered in many different context by various authors in the literature. In [9], Pham, the first and the fourth listed authors concluded a result for two-variable polynomials. More precise, they showed that for any set $A \subset \mathcal{R} \setminus \{q^0, \mathcal{R}^0 - 1\}$ we have

$$|A(A + 1)| \gg \min\left\{\sqrt{q^3|A|}, \frac{|A|^2}{\sqrt{q^{2r-1}}}\right\}.$$

For three-variable polynomials, Yazici [1] developed a point-plane incidence estimate over finite valuation ring and showed that the function $xy + z$ is a moderate expander over $\mathcal{R}$ with the exponent $\frac{1}{3}$. More precisely, they proved the following result.

**Theorem 1.2** ([1, Theorem 1.1]). Let $\mathcal{R}$ be a finite valuation ring of order $q^r$ and let $A, B, C$ be the subsets of $\mathcal{R}$. Then

$$|AB + C| \gg \min\left\{q^r, \frac{|A||B||C|}{q^{2r-1}}\right\}.$$ 

In [2], Anh and her colleagues proved the following result.

**Theorem 1.3** ([2, Lemma 4.4]). Let $X, Y, Z$ be sets in $\mathcal{R}$. We have

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

As a direct consequence, the polynomial $(x - y)^2 + z$ is a moderate expander with the exponent $\frac{1}{4}$. They also provided a family of four variable moderate expanding polynomials over finite valuation rings with the exponent $\frac{1}{4}$. More precisely, they showed that $x(x + t)y + z, x(x + t) + yz, x(x + t)(y + z), y(x(x + t) + z), (x(x + t) - y)^2 + z$ and $(y - z)^2 + x(x + t)$ are moderate expanders over $\mathcal{R}$ with the exponents $\frac{1}{5}$.

For more background about this problem and an extensive exploration of the subject over finite valuation rings, we refer the reader [6, 7, 13, 15, 17, 19] and the references therein.

In this paper, following the spirit of Yazici’s point-plane incidence, we will present several results for large sets. Our first result is the finite valuation ring version of a previous result over prime field by Pham, De Zeeuw and the forth listed author [16]. Note that, the result of Pham, De Zeeuw and the forth listed author is for any quadratic polynomial $f \in \mathbb{F}[x, y, z]$, which is not of the form $g(h(x) + k(y) + l(z))$. In Section 7, we give a remark that the same arguments in the proof of Theorem 1.4 do not apply for more general cases.
Theorem 1.4. Let \( \mathcal{R} \) be a finite valuation ring of order \( q^r \). Consider a polynomial
\[
f(x, y, z) = axy + R(x) + S(y) + T(z),
\]
where \( R, S, T \in \mathcal{R}[u] \) are polynomials of degree at most two, \( a \neq 0 \), and \( T(z) \) is not a constant with the highest coefficient \( m \in \mathcal{R}^* \). Suppose that \( A, B, C \subseteq \mathcal{R} \) and we further assume that \( |C| \geq 2q^{r-1} \) if \( T \) has degree two. We have the following estimation:
\[
|f(A, B, C)| \geq \frac{1}{8} \min\left\{ q^r, \frac{|A||B||C|}{q^{2r-1}} \right\}.
\]

Note that Theorem 1.2 and Theorem 1.3 are special cases of Theorem 1.4.

In [1], Yazici obtained the following sum-product type estimate over an arbitrary finite valuation ring \( \mathcal{R} \).

Theorem 1.5 ([1, Theorem 1.2]). For any subset \( A \) of \( \mathcal{R} \) with \( |A + A||A|^2 > q^{3r-1} \), we have
\[
|A^2 + A^2||A + A| \gg q^{\frac{r}{2}}|A|^{\frac{3}{2}}.
\]

Using methods from spectral graph theory, Hiep [12] proved the following improvement of Theorem 1.5.

Theorem 1.6 ([12, Theorem 1.5]). Let \( A \) be a subset of \( \mathcal{R} \). Suppose that \( |A + A||A|^2 \geq q^{3r-1} \). Then we have
\[
|A^2 + A^2||A + A| \geq \frac{1}{2}|A|^2 q^r.
\]
This implies that
\[
\max\{|A + A|, |A^2 + A^2|\} \geq 2^{-\frac{1}{2}}|A|^\frac{3}{2} q^\frac{r}{2}.
\]

In this paper, we give another proof of Theorem 1.6 using point-plane incidences. By a slightly different technique, we also give a lower bound in term of \( A^3 + A^3 \) in Theorem 1.6.

Theorem 1.7. For \( A \subseteq \mathcal{R} \) with \( \frac{|A^3 + A^3|}{|A|^3} \geq q^{3r-1} \), we have
\[
\max\{|A + A|, |A^3 + A^3|\} \gg q^{r/10}|A|^{9/10}.
\]

The idea of Theorem 1.4 also leads to the following results.

Theorem 1.8. Let \( f \) be a one-variable quadratic polynomial with coefficients over \( \mathcal{R} \). If \( |A + f(A)||A|^2 \geq q^{3r-1} \), then
\[
|f(A) + A| \geq 2^{-\frac{1}{2}}|A|^\frac{3}{2} q^\frac{r}{2}.
\]

Theorem 1.9. For \( A \subseteq \mathcal{R} \) with \( |A| \geq q^{r-\frac{1}{2}} \), we have
\[
\max\{|A - A|, |AA + AA|\} \geq 2^{-\frac{1}{2}}|A|^\frac{1}{2} q^\frac{r}{2}.
\]

We also develop a weighted version of Yazici’s incidence to prove the sum-product estimates over finite valuation ring. More precisely, we have the following theorems.

Theorem 1.10. Let \( d \) be an integer with \( d \geq 1 \) and let \( A \) be a subset of \( \mathcal{R} \). Suppose that \( |AA||A|^2 \geq q^{3r-1} \). Then we have
\[
|A^d + A^d||AA|^2 \gg q^r|A|^2
\]
or
\[
\max\{|A^d + A^d|, |AA||\} \gg q^r|A|^\frac{1}{2}.
\]

Note that the condition \( |A| \gg q^{r-\frac{1}{2}} \) implies the conditions in previous theorems. Therefore, we can replace all conditions in previous theorems by the condition \( |A| \gg q^{r-\frac{1}{2}} \).

2 Preliminaries

We start this section by recalling the definition of finite valuation rings.

Definition 2.1. Finite valuation rings are finite rings that are local and principal.
Throughout, rings are assumed to be commutative, and to have an identity. Let \( \mathcal{R} \) be a finite valuation ring, then \( \mathcal{R} \) has a unique maximal ideal that contains every proper ideals of \( \mathcal{R} \). This implies that there exists a non-unit \( z \) called uniformizer in \( \mathcal{R} \) such that the maximal ideal is generated by \( z \). Moreover, we also note that the uniformizer \( z \) is defined up to a unit of \( \mathcal{R} \).

There are two structural parameters associated to \( \mathcal{R} \) as follows: the cardinality of the residue field \( F = \mathcal{R}/(z) \), and the nilpotency degree of \( z \), where the nilpotency degree of \( z \) is the smallest integer \( r \) such that \( z^r = 0 \). Let us denote the cardinality of \( F \) by \( q \). In this note, \( q \) is assumed to be odd, then \( 2 \) is a unit in \( \mathcal{R} \).

If \( \mathcal{R} \) is a finite valuation ring, and \( r \) is the nilpotency degree of \( z \), then we have a natural valuation

\[
\nu : \mathcal{R} \rightarrow \{0, 1, \ldots, r\}
\]
defined as follows: \( \nu(0) = r \), for \( x \neq 0 \), \( \nu(x) = k \) if \( x \in (z^k) \setminus (z^{k+1}) \). We also note that \( \nu(x) = k \) if and only if \( x = uz^k \) for some unit \( u \) in \( \mathcal{R} \). Each abelian group \((z^k)/(z^{k+1})\) is a one-dimensional linear space over the residue field \( F = \mathcal{R}/(z) \), thus its size is \( q \). This implies that \( |(z^k)| = q^{r-k} \), \( |\mathcal{R}| = q^r \) and \( |\mathcal{R}^k| = |\mathcal{R}| - |(z)| = q^r - q^{r-1} \) (for more details about valuation rings, see [3, 5, 8, 14]). The following are some examples of finite valuation rings:

(i) Finite fields \( \mathbb{F}_q \), \( q = p^n \) for some \( n > 0 \).

(ii) Finite rings \( \mathbb{Z}_{p'} \), where \( p \) is a prime.

(iii) \( \mathbb{O}/(p') \) where \( \mathbb{O} \) is the ring of integers in a number field and \( p \in \mathbb{O} \) is a prime.

(iv) \( \mathbb{F}_q[x]/(f') \), where \( f \in \mathbb{F}_q[x] \) is an irreducible polynomial.

For the proofs of Theorem 1.4, Theorem 1.8, and Theorem 1.9, we use the following incidence theorem between points and planes in \( \mathbb{R}^3 \), which given by Yazici [1].

**Theorem 2.2 ([1, Theorem 2.3]).** Let \( \mathcal{R} \) be a finite valuation ring of order \( q' \). Let \( Q \) be a set of point in \( \mathbb{R}^3 \) and let \( \Pi \) be a set of planes in \( \mathbb{R}^3 \). Then the number of incidences \( I(Q, \Pi) \) satisfies

\[
\left| I(Q, \Pi) - \frac{1}{q'^{r-1}} q^2 + q + 1 \right| Q||\Pi| \leq q^{2r-1}|Q|^\frac{3}{2}|\Pi|^{\frac{5}{2}}.
\]

Hence,

\[
|I(Q, \Pi)| \leq \frac{1}{q'}|Q||\Pi| + q^{2r-1}|Q|^\frac{3}{2}|\Pi|^{\frac{5}{2}}.
\]

To prove Theorem 1.10, we will need the following weighted version of the point-plane incidences over finite valuation rings.

**Theorem 2.3 (Point-plane incidences – weighted version).** Let \( Q, \Pi \) be weighted set of points and planes in \( \mathbb{R}^3 \) with the weighted integer function \( \omega \), both total weight \( W \). Suppose that maximum weights are bounded by \( \omega_0 \geq 1 \). Define the number of weighted incidences is

\[
I_\omega = \sum_{q \in Q, \pi \in \Pi} \omega(q) \omega(\pi) \delta_{q, \pi},
\]

where

\[
\delta_{q, \pi} = \begin{cases} 
1 & \text{if } q \in \pi, \\
0 & \text{if } q \notin \pi.
\end{cases}
\]

Then the number \( I_\omega \) of weighted incidences is bounded as follows:

\[
I_\omega = \sum_{q \in Q} \omega(q) \omega(\pi) \ll \frac{1}{q'} W^2 + q^{2r-1} W.
\]

**Proof.** In this proof, we will use a weight rearrangement argument. Firstly, we rewrite the number of weighted incidences as

\[
I_\omega = \sum_{q \in Q} \omega(q) \left( \sum_{\pi \in \Pi} \omega(\pi) \right) = \sum_{q \in Q} \omega(q) W(q),
\]

where

\[
W(q) = \sum_{\pi \in \Pi : q \in \pi} \omega(\pi).
\]
Since no weight is larger than $\omega_0$, we always can pick a subset $Q' \subset Q$, containing $n = \lceil \frac{\log q}{\log 2} \rceil$ ‘richest’ points $q_1, q_2, \ldots, q_n$ in terms of $W(q)$. We replace $Q$ by $Q'$ by assign to each one of the points in $Q'$ the weight $\omega_0$ and deleting the rest of points in $Q$. Without loss of generality, we can assume that $W(q_n)$ is minimum of $W(q_k)$ for $1 \leq k \leq n$. Note that

$$I_\omega(Q, \Pi) = \sum_{q \in Q'} \omega(q) W(q) + \sum_{q \in Q \setminus Q'} \omega(q) W(q) \leq \sum_{q \in Q'} \omega(q) W(q) + \left( W - \sum_{q \in Q'} \omega(q) \right) W(q_n) \leq \sum_{q \in Q'} \omega(q) W(q) - W(q_n) + n \omega_0 W(q_n) \leq \sum_{k=1}^n \omega_0 W(q_k).$$

The number of weighted incidences $I_\omega$ will thereby not decrease. Similarly, we can pick a subset $\Pi'$ of the plane set $\Pi$, containing $n$ richest planes in terms of their non-weighted incidences with $Q'$. We also assign the weight $\omega_0$ to each plane in $\Pi'$. We now replace $Q, \Pi$ by $Q', \Pi'$.

Applying Theorem 2.2, we obtain

$$I_\omega(Q, \Pi) \leq I_{\omega_0}(Q', \Pi') \leq \left( \frac{1}{q^r} \right) W^2 + q^{2r-1} \omega_0 n \approx \left( \frac{1}{q^r} \right) W^2 + q^{2r-1} W,$$

which completes the proof of Theorem 2.3.

## 3 Proof of Theorem 1.4

Let $N$ be the number of tuples $(x, y, z, x', y', z') \in (A \times B \times C)^2$ such that $f(x, y, z) = f(x', y', z')$. We rewrite this equation as

$$(ay)x - (ax')y + (R(x) - S(y') + T(z)) = R(x') - S(y) + T(z').$$

We define the point set $Q$ and the plane set $\Pi$ as following:

$$Q := \{(x, y', R(x) - S(y') + T(z)) : (x, y', z) \in A \times B \times C\},$$
$$\Pi := \{(ay) \cdot X - (ax') \cdot Y + Z = R(x') - S(y) + T(z') : (x', y', z') \in A \times B \times C\}.$$  

For each choice of $x, y'$, and $n$, we count the number of solutions of the equation $T(z) = n$. If $\deg(T) = 1$, it is clear that the equation has exactly one solution since its highest coefficient $m$ is a unit of $\mathbb{R}$. If $\deg(T) = 2$, we rewrite the equation as follows:

$$(z - u)^2 = n',$$

where $u$ is a fixed number and does not depend on $x, y', n$. If there does not exist $z_1$ such that $z_1^2 = n'$, then (3.1) has no solution. Otherwise, we have

$$(z - u - z_1)(z - u + z_1) = 0,$$  

where $\mu$ is uniformizer in $\mathbb{R}$. It follows that $z - u = 2^{-1}(u_1 \mu a_1 + u_2 \mu a_2)$ is non-unit. Since $|C| \geq 2q^{r-1}$, without loss of generality, we can assume that $z - u$ is unit so equation (3.2) has at most two solutions. This implies that $T(z) = n$ has at most two solutions. Therefore, each point $(u, v, w) \in Q$ corresponds to at most two points $(x, y', z) \in A \times B \times C$.
Apply the same argument to the set of planes $\Pi$, we have

$$|Q|_\Pi \leq |A||B||C|$$

and

$$N \leq 4 \cdot I(Q, \Pi),$$

where $I(Q, \Pi)$ is number of incidences between $Q$ and $\Pi$. Now applying the Cauchy–Schwarz inequality and Theorem 2.2, we get

$$(|A||B||C|)^2 \leq |f(A, B, C)| \cdot N$$

$$\leq 4|f(A, B, C)| \cdot I(Q, \Pi)$$

$$\leq 4|f(A, B, C)| \left( \frac{1}{q} |Q|_\Pi + q^{2r-1} |Q|_{\Pi}^{1/2} \right)$$

$$\leq 4|f(A, B, C)| \left( \frac{|A|^2|B|^2|C|^2}{q^r} + q^{2r-1}|A||B||C| \right).$$

This implies that

$$|f(A, B, C)| \geq \frac{1}{8} \min \left\{ q^r, \frac{|A||B||C|}{q^{2r-1}} \right\},$$

completing the proof of Theorem 1.4.

## 4 Proofs of Theorem 1.6 and Theorem 1.7

**Proof of Theorem 1.6.** Let $f(x, y, z) = (x - z)^2 + y^2$, we consider the following equation:

$$f(x, y, z) = t,$$  \hspace{1cm} (4.1)

where $x \in A + A$, $y, z \in A$, $t \in A^2 + A^2$. For any triple $(u, v, w) \in A$, a solution of equation (4.1) is given by $x = u + w \in A + A$, $y = v \in A$, $z = u \in A$, $t = w^2 + v^2 \in A^2 + A^2$. Thus, there are at least $|A|^3$ solutions of equation (4.1). Now applying the Cauchy–Schwarz inequality, we get

$$|A|^6 \leq |A^2 + A^2| : \ |(x, y, z, x', y', z') \in (A + A) \times A \times A^2 : f(x, y, z) = f(x', y', z')|.$$  \hspace{1cm} (4.2)

We proceed similarly as in the proof of Theorem 1.4 for the specific function

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

with $|A| = |B|, |C| = |A + A|$. It follows from (4.2) that

$$|A|^6 \leq |A^2 + A^2| : \left( \frac{|A + A||A|^6}{q^r} + q^{2r-1}|A + A||A|^2 \right).$$

Hence,

$$|A|^2q^r \leq |A^2 + A^2||A + A|^2 \left( 1 + \frac{q^{2r-1}}{|A + A||A|^2} \right).$$

Thus, under the our assumption $|A + A| \cdot |A|^2 \geq q^{3r-1}$, we have

$$|A + A|^2|A^2 + A^2| \geq \frac{1}{2}|A|^2q^r,$$

which completes the proof of Theorem 1.6.

For the proof of Theorem 1.7, we will need the following Plunnecke–Ruzsa inequality.

**Lemma 4.1.** Let $A$ and $B$ be finite subsets of an abelian group such that $|A + B| \leq K|A|$. Then, for an arbitrary $0 < \delta < 1$, there is a nonempty set $X \subset A$ such that $|X| \geq (1 - \delta)|A|$, and for any integer $k$, one has

$$|X + kB| \leq \left( \frac{K}{\delta} \right)^k |X|.$$
Proof of Theorem 1.7. Let \( b = d - a \), where \( a, b \in A \), \( d \in A + A \). We have
\[
a^3 + (d - a)^3 = d[a^2 - a(d - a) + (d - a)^2]
= d(3a^2 - 3ad + d^2)
= 3d \left( a - \frac{d}{2} \right)^2 + \frac{d^2}{12}
= 3d \left( s^2 + \frac{d^2}{12} \right),
\]
where \( s = a - \frac{d}{2} \).

Let \( E \) be the number of solutions of the following equation:
\[
c^3 + b^3 + a^3 = c'^3 + b'^3 + a'^3, \quad (a, b, c, c', b', a') \in A^6. \tag{4.3}
\]
By the Plunnecke–Ruzsa inequality, we can choose a large subset \( A' \subset A \) such that
\[
|A'^3 + A'^3 + A'^3| \ll \frac{|A^3 + A^3|^2}{|A|}. \tag{4.4}
\]
Putting (4.3) and (4.4) together with the Cauchy–Schwarz inequality, we have
\[
\frac{|A^3 + A^3|^2}{|A|} \ll |A|^6. \tag{4.5}
\]
Besides, we can rewrite equation (4.3) as \( 3ds^2 + \frac{d^3}{4} + c^3 = 3d's'^2 + \frac{d'^3}{4} + c'^3 \). This is equivalent to
\[
s^2 \cdot (3d) - 3d's'^2 - \frac{d^3}{4} - c^3 = -\frac{d^3}{4} - c^3.
\]
Define the point set \( Q \) and the plane set \( \Pi \) as follows;
\[
Q := \left\{ (s^2, 3d', -\frac{d^3}{4} - c^3) : s \in A - \frac{A + A}{2}, \quad d' \in A + A, \quad c' \in A \right\},
\]
\[
\Pi := \left\{ 3d \cdot X - s'^2, \quad Y + Z = -\frac{d^3}{4} - c^3 : s' \in A - \frac{A + A}{2}, \quad d \in A + A, \quad c \in A \right\}.
\]
For each \((u, v, w) \in Q\), there are at most six triples \((s, d', c') \in (A - \frac{A + A}{2}) \times A + A \times A\) such that \(u = s^2, v = 3d', w = -\frac{d^3}{4} - c^3\).

Apply the same argument to the plane set \( \Pi \), we have
\[
|Q|, |\Pi| \leq \left| A - \frac{A + A}{2} \right| |A + A||A| \tag{4.6}
\]
and
\[
E \leq 36 \cdot I(Q, \Pi),
\]
where \( I(Q, \Pi) \) is the number of incidences between \( Q \) and \( \Pi \). Applying the Theorem 2.2, we obtain
\[
E \leq 36 \left( \frac{1}{q^r} |Q||\Pi| + q^{2r-1} |Q|^{\frac{3}{2}}|\Pi|^{\frac{1}{2}} \right). \tag{4.7}
\]
Now, we bound the number of values of \( s \). Note that
\[
\left| A - \frac{A + A}{2} \right| = 2A - A \cdot A \leq |A + A - A| \leq \frac{|A + A|^3}{|A|^2}. \tag{4.8}
\]
The last inequality is obtained by applying the Plunnecke–Ruzsa inequality twice.

From (4.6) and (4.8), we have
\[
|Q|, |\Pi| \leq \frac{|A + A|^4}{|A|}. \tag{4.9}
\]
From (4.7) and (4.9), we have
\[
E \leq 36 \left( \frac{1}{q^r} \left| A + A \right|^8 \left| A \right|^2 + q^{2r-1} \cdot \frac{|A + A|^4}{|A|} \right). \tag{4.10}
\]
Putting (4.5) and (4.10) together, we have
\[
|A|^7 \ll |A^3 + A^3|^2, \quad E \ll |A^3 + A^3|^2 \left( \frac{1}{q^r} \left| A + A \right|^8 \left| A \right|^2 + q^{2r-1} \cdot \frac{|A + A|^4}{|A|} \right).
\]
Hence
\[ q' |A|^9 \ll |A^3 + A^3|^2 |A + A|^8 \left( 1 + \frac{q^{3r-1}|A|}{|A + A|^4} \right). \]
Therefore, if \( q^{3r-1} \ll \frac{|A^3 + A^3|^2}{|A + A|^4} \), then
\[ \max(|A + A|, |A^3 + A^3|) \gg q^{\frac{8r}{3}} |A|^2, \]
which completes the proof of Theorem 1.7.

4.1 Proof of Theorem 1.8

Without loss of generality, we can assume that \( f(x) = ax^2 + bx \) with \( a \neq 0 \). We consider the equation
\[ a(x - y)^2 + b(x - y) + z = t, \quad (4.11) \]
where \( x \in A + f(A) \), \( y \in f(A) \), \( z \in A \), and \( t \in A + f(A) \). Note that for any \( u, v, w \in A \), a solution of equation (4.11) is given by \( x = u + f(v) \in A + f(A) \), \( y = f(v) \in f(A) \), \( z = w \in A \), and \( t = w + f(u) \in A + f(A) \). Therefore, let \( N \) be the number of solutions of equation (4.11), we have \( N \geq |A|^3 \). On the other hand, by using the Cauchy–Schwarz inequality, one has
\[ N^2 \leq |f(A) + A| \cdot |(x, y, z, z', y') \in ((A + f(A)) \times f(A) \times A)^2 : f(x - y) + z = f(x' - y') + z'| \]
\[ = |f(A) + A| \cdot |E|. \]
Hence,
\[ |A|^6 \leq |A + f(A)| \cdot |E|. \quad (4.12) \]

Similarly, to bound \( |E| \), we apply Theorem 2.2 for the following set of points and set of planes:
\[ Q := \{(ax, y', ax^2 + bx - z - ay'^2 + by') : (x, y', z) \in (A + f(A)) \times f(A) \times A\}, \]
\[ \Pi := \{-2y \cdot X + 2ax' \cdot Y + Z = ax^2 + bx' + z' - ay^2 + by : (x', y', z') \in (A + f(A)) \times f(A) \times A\}. \]

Note that \( |Q| = |\Pi| \leq |A + f(A)||f(A)||A| \leq |A + f(A)||A|^2 \) and \( |E| \leq \|I(Q, \Pi) \| \), where \( I(Q, \Pi) \) is number of incidences between \( Q \) and \( \Pi \). Therefore, it follows from (4.12) and applying Theorem 2.2, one gets
\[ |A|^6 \leq |A + f(A)||I(Q, \Pi) | \leq |A + f(A)| \left( \frac{|A + f(A)||A|^4}{q^r} + q^{3r-1}|A + f(A)||A|^2 \right). \]

Hence
\[ |A|^2 q^r \leq |A + f(A)|^3 \left( 1 + \frac{q^{3r-1}}{|A + f(A)||A|^2} \right). \]

Therefore, if \( |A + f(A)||A|^{3q^{3r-1}} \), then we have
\[ |f(A) + A| \geq 2^{-\frac{1}{3}} |A|^{\frac{2}{3}} q^{\frac{2}{3}} , \]
which completes the proof of Theorem 1.8.

5 Proof of Theorem 1.9

For each \( m \in \mathbb{R} \), consider the equation
\[ xy + zt = m, \quad \text{where } x, y, z, t \in A. \]
It follows from the Cauchy–Schwarz inequality that
\[ |A|^8 \leq |AA + AA| \cdot |(x, y, z, t, x', y', z', t') \in A^8 : xy + zt = x'y' + z't'| | \]
\[ \leq |AA + AA| \cdot |A - A|^2 \cdot |(x, y, t, x', t, y', z') \in A^6 : xy + xt + at = x'y' + x't' + \beta t'|, \]
where \((a, \beta) \in (A - A) \times (A - A)\) is any chosen pair, and \((x, y, t, x', y', t') \in A^6\).
Define the point set $Q$ and the plane set $\Pi$ as follows:

\[ Q := \{(x, y', xt + at) : (x, y', t) \in A^3 \}, \]
\[ \Pi := \{y \cdot X - x' \cdot Y + Z = x't' + \beta t' : (y, x', t') \in A^3 \}. \]

Note that $|Q|, |\Pi| \leq |A|^3$, and the number of incidences between $Q$ and $\Pi$ satisfies

\[ |\{(x, y, t, x', l', y', \alpha, \beta) : xy + xt = x'y' + x't' + \beta t'\}| \leq I(Q, \Pi). \]

Then, applying Theorem 2.2, we obtain

\[ |A|^8 \leq |AA + AA||A - A|^2 \cdot I(Q, \Pi) \leq |AA + AA||A - A|^2 \cdot \left(\frac{|A|^6}{q^r} + q^{2r-1}|A|^3 \right). \]

Therefore, if $|A|^3 \geq q^{3r-1}$, then

\[ \frac{1}{2}|A|^2q^r \leq |AA + AA||A - A|^2, \]

or equivalently,

\[ \max(|A - A|, |AA + AA|) \geq 2^{-\frac{1}{2}}|A|^\frac{1}{2}q^{\frac{r}{2}}. \]

This completes the proof of the theorem.

### 6 Proof of Theorem 1.10

We first observe that if $|A| \ll q^{r-\frac{1}{2}}$, then

\[ |A^d + A^d||AA|^2 \gg |A||AA|^2 \gg \frac{q^{6r-2}}{|A|^3} \gg q'|A|^2. \]

Therefore, we only need to consider the case of $|A| \gg q^{r-\frac{1}{2}}$. Since $|\mathbb{R}^0| = q^{r-1}$, without loss of generality, we can assume that $A \subset \mathbb{R}^*$. We define the $d$-power energy of $A$ by

\[ E_d(A) = |\{a^d + b^d = c^d + e^d : a, b, c, d \in A\}|. \]

For $f, g \in A$, we have

\[ E_d(A) = |A|^{-2}\left\{ a^d + \frac{(bf)^d}{f^d} = c^d + \frac{(eg)^d}{g^d} \right\} \leq |A|^{-2}\left\{ a^d + \frac{h^d}{f^d} = c^d + \frac{k^d}{g^d} : a, f, c, g \in A, h, k \in AA \right\}. \]

We define the multi-set of points with coordinates $(a^d, \frac{1}{f^d}, k^d)$ and the multi-set of planes with equation $X + h^d \cdot Y - \left(\frac{1}{f^d}\right) \cdot Z = c^d$. Since $A \subset \mathbb{R}^*$, the number of solutions of the equation $x^d = t$ for $x, t \in A$ is at most $d$. Therefore, these points and planes may have weights up to $d^3$, implying that $\omega \leq d^3$, and $W = 2|A|^2|AA|$.

From the point-plane weighted incidences (Theorem 2.3) and using the Cauchy–Schwarz inequality, we have

\[ |A|^6 \ll E_d(A)|A^d + A^d|. \]

Hence

\[ |A|^6 \ll |A^d + A^d| \left(\frac{1}{q^r}|A|^6|AA|^2 + q^{2r-1}|A|^2|AA| \right). \]

In other words,

\[ q'|A|^2 \ll |A^d + A^d||AA|^2 \left(1 + \frac{q^{3r-1}}{|AA||AA|^2} \right). \]

Therefore, if $|AA||A|^2 \geq q^{3r-1}$, then

\[ |A^d + A^d||AA|^2 \gg q'|A|^2, \]

which completes the proof of Theorem 1.10.
7 Further remarks

Note that, using the same arguments as in the proof of Theorem 1.4, we cannot extend the theorem for more general quadratic polynomials

\[ f(x, y, z) = axy + bxz + R(s) + S(y) + T(z) \quad \text{and} \quad f(x, y, z) = axy + bxz + czy + R(s) + S(y) + T(z). \]

The main reason is that we cannot control the number of solutions of the equations \( T(z) + bxz = n \) and \( T(z) + bxz + czy = n \) as these equations may have up to \( q^{r-1} \) solutions.

Given the commutative ring \( R \) and its units \( R^* \), we can define its ring of fraction \( \mathbb{Q} = (R^*)^{-1}R \). This ring of fraction defines an equivalence relation on \( R \times R^* \) that \((m, m') \sim (r, r') \) if and only if \( mr' = m'r \). We write \( \frac{m}{m'} = \frac{r}{r'} \) if \((m, m') \sim (r, r') \).

We can define the collinearity property in \( R \times R \): three points \((a, a'), (b, b'), (c, c') \in R \times R \) are collinear if there exists a number \( k \in \mathbb{Q} \) such that \((a - b) = k(c - b) \) and \((a' - b') = k(c' - b') \). The set of points, which are collinear to an initial point \((u, v) \) via a fixed number \( k \in \mathbb{Q} \), is a line.

By applying Theorem 2.3 and proceeding similarly to the arguments as in the previous sections, we also have the following geometric type result.

**Theorem 7.1.** Let \( T(P) \) be the number of collinear triples in the point set \( P = A \times A \subset R \times R \) and let \( L(P) \) be the set of lines connecting pairs of distinct points of \( P = A \times A \). Then

\[ T(P) \leq q^{2r-1}|A|^3 + \frac{|A|^6}{q^r} + 2 \cdot |A|^6, \]

and

\[ |L(P)| \geq \min\left\{q^{2r}, \frac{|A|^6}{q^{r-2}}\right\}. \]

**Funding:** The research is funded by the National Foundation for Science and Technology Development Project 101.99-2019.318.

References

[1] E. Aksoy Yazici, Sum-product type estimates for subsets of finite valuation rings, *Acta Arith.* **185** (2018), no. 1, 9–18.

[2] D. N. V. Anh, L. Q. Ham, D. Koh, M. Mirzaie, H. Mojarrad and T. Pham, Moderate expanders over rings, *J. Number Theory* (2020), DOI 10.1016/j.jnt.2020.07.009.

[3] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*. Vol. 2, Addison-Wesley, Reading, 1969.

[4] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*, Kluwer Int. Ser. Eng. Comput. Sci. 680, Kluwer Academic, Boston, 2002.

[5] J. Bourgain, The sum-product theorem in \( \mathbb{Z}_q \) with \( q \) arbitrary, *J. Anal. Math.* **106** (2008), 1–93.

[7] P. Erdős and E. Szemerédi, On sums and products of integers, in: *Studies in Pure Mathematics*, Birkhäuser, Basel (1983), 213–218.

[8] W. Fulton, *Algebraic Curves*, Adv. Book Class., Addison-Wesley, Redwood City, 1989.

[9] L. Q. Ham, P. V. Thang and L. A. Vinh, Conditional expanding bounds for two-variable functions over finite valuation rings, *European J. Combin.* **50** (2015), 114–123.

[10] D. Hart and A. Iosevich, Sums and products in finite fields: An integral geometric viewpoint, in: *Radon Transforms, Geometry, and Wavelets*, Contemp. Math. 464, American Mathematical Society, Providence (2008), 129–135.

[11] D. Hart, L. Li and C.-Y. Shen, Fourier analysis and expanding phenomena in finite fields, *Proc. Amer. Math. Soc.* **141** (2013), no. 2, 461–473.

[12] P. D. Hiep, A note on sum-product estimates over finite valuation rings, preprint (2020), https://arxiv.org/abs/2005.05564.

[13] B. Murphy, O. Rocha-Newton and I. Shkredov, Variations on the sum-product problem, *SIAM J. Discrete Math.* **29** (2015), no. 1, 514–540.

[14] B. Nica, Unimodular graphs and Eisenstein sums, *J. Algebraic Combin.* **45** (2017), no. 2, 423–454.
[15] T. Pham and L. A. Vinh, Some combinatorial number theory problems over finite valuation rings, *Illinois J. Math.* 61 (2017), no. 1–2, 243–257.

[16] T. Pham, L. A. Vinh and F. de Zeeuw, Three-variable expanding polynomials and higher-dimensional distinct distances, *Combinatorica* 39 (2019), no. 2, 411–426.

[17] M. Rudnev, I. Shkredov and S. Stevens, On the energy variant of the sum-product conjecture, *Rev. Mat. Iberoam.* 36 (2020), no. 1, 207–232.

[18] I. E. Shparlinski, On the solvability of bilinear equations in finite fields, *Glasg. Math. J.* 50 (2008), no. 3, 523–529.

[19] T. Tao, The sum-product phenomenon in arbitrary rings, *Contrib. Discrete Math.* 4 (2009), no. 2, 59–82.

[20] L. A. Vinh, On four-variable expanders in finite fields, *SIAM J. Discrete Math.* 27 (2013), no. 4, 2038–2048.