Moderate Expanders Over Rings

Dao Nguyen Van Anh, Le Quang Ham, Doowon Koh
Mozhgan Mirzaei, Hossein Nassajian Mojarrad, and Thang Pham

Abstract

In this paper, 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. Using the same approach, we derive similar results in the setting of finite local and principal rings. In this general setting, we also obtain a new result on distance sets in the $p$-adic perspective.

1 Introduction

Let $\mathbb{F}$ be a field and $\mathcal{E}$ be a subset in $\mathbb{F}^\ell$. Given a function $f: \mathbb{F}^\ell \to \mathbb{F}$, define

$$f(\mathcal{E}) := \{f(\alpha) : \alpha \in \mathcal{E}\},$$

as the image of $\mathcal{E}$ under the function $f$. We say that $f$ is an $\ell$-variable expander with the exponent $\epsilon$ if $|f(\mathcal{E})| \geq C_\epsilon |\mathcal{E}|^{1+\epsilon}$ for any $\mathcal{E}$ possibly with some general conditions on $\mathcal{E}$. Over the last two decades, the study of various classical problems shows that several polynomials have expander property. For instance, the expander property will be described clearly in distance problems and sum-product topics as follows.

Over the real numbers, the breakthrough result of Guth and Katz [7] states that for any $\mathcal{E} \subset \mathbb{R}^2$, the number of distinct distances determined by points in $\mathcal{E}$ is at least $c|\mathcal{E}|/\log(|\mathcal{E}|)$ for some positive constant $c$. This result implies that the distance function in the plane $f(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||$ is a 4-variable expander with any exponent less than $\frac{1}{4}$.

Let $\mathbb{F}_q$ be a finite field of order $q$, where $q$ is a prime power. Given two points $\mathbf{x} = (x_1, \ldots, x_d)$
and \( y = (y_1, \ldots, y_d) \) in \( \mathbb{F}^d_q \), we define the distance between them as follows:

\[
||x - y|| := (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2.
\]

One can check that this distance function is not a metric, but it is invariant under rotations, reflections, and translations. Suppose \( \mathcal{E} \) is a set of points in \( \mathbb{F}^d_q \). Define

\[
\Delta_{\mathbb{F}_q}(\mathcal{E}) := \{||x - y||: x, y \in \mathcal{E}\},
\]

as the set of distances determined by points in \( \mathcal{E} \).

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 \( C' > 0 \).

The prime field version of the Erdős distinct distances problem was first considered in a remarkable work of Bourgain, Katz, and Tao [1].

**Theorem 1.1** ([1]). Let \( p \equiv 3 \mod 4 \) be a prime, and \( \mathcal{E} \) be a set in \( \mathbb{F}_p^2 \). Suppose that \( |\mathcal{E}| = p^\alpha \) with \( 0 < \alpha < 2 \), then

\[
|\Delta_{\mathbb{F}_p}(\mathcal{E})| \gg |\mathcal{E}|^{1+\epsilon},
\]

where \( \epsilon = \epsilon(\alpha) > 0 \).

This theorem tells us that over prime fields, the distance function is a 4-variable expander with the exponent \( \epsilon/2 \).

Over arbitrary finite fields \( \mathbb{F}_q \), where \( q \) is a prime power, Iosevich and Rudnev [14] showed that the conclusion of Theorem 1.1 does not hold in general since the whole plane over the sub-prime field only gives us the threshold \( |\mathcal{E}|^{1/2} \). In this general setting, using discrete Fourier analysis, Iosevich and Rudnev [14] showed that for \( \mathcal{E} \subset \mathbb{F}_q^d \), if the size of \( \mathcal{E} \) is sufficiently large, then the distance set \( \Delta_{\mathbb{F}_q}(\mathcal{E}) \) covers a positive proportion of all elements in \( \mathbb{F}_q \). The precise statement of their result is as follows.

**Theorem 1.2.** Let \( \mathbb{F}_q \) be an arbitrary finite field, and \( \mathcal{E} \) be a set in \( \mathbb{F}_q^d \) with \( |\mathcal{E}| \geq Cq^{d/2} \) for
sufficiently large. The distance set satisfies

$$|\Delta_{F_q}(E)| \gg \min \left\{ q, \frac{|E|}{q^{d+1}} \right\}.$$ 

It follows directly from this result that the distance function has expander property when \( q^{d+\delta} \leq |E| \leq q^{d-\delta} \) for any small \( \delta > 0 \).

Let \( \mathbb{Z}_{p^r} \) be the finite cyclic ring of order \( p^r \). Let \( \mathbb{Z}_{p^r}^\times \) be the set of units in \( \mathbb{Z}_{p^r} \). In the setting of \( \mathbb{Z}_{p^r} \), using the same techniques, Covert, Iosevich, and Pakianathan [3] obtained a similar result over \( \mathbb{Z}_{p^r}^d \), which also provides an example of expander property.

**Theorem 1.3.** Let \( E \) be a set in \( \mathbb{Z}_{p^r}^d \). Suppose that \( |E| \gg p^r d^{-\frac{d-1}{2}} \), then

$$\Delta_{\mathbb{Z}_{p^r}}(E) \supset \mathbb{Z}_{p^r}^\times \cup \{0\}.$$ 

If \( E \) has Cartesian product structure, then Hieu and Vinh [13] derived the following improvement.

**Theorem 1.4.** Let \( A \) be a set in \( \mathbb{Z}_{p^r} \). If \( |A| \gg p^\frac{d-1}{2} \), then \( |\Delta_{\mathbb{Z}_{p^r}}(A^d)| \gg p^r \).

Let \( A \) be a non-empty subset of a finite field \( \mathbb{F}_q \). We consider the sum set

$$A + A := \{a + b : a, b \in A\},$$

and the product set

$$A \cdot A := \{a \cdot b : a, b \in A\}.$$ 

The classical sum-product problem originated by Erdős and Szemerédi [4] states that for any \( A \subset \mathbb{R} \), we have

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

(1)

for some \( \epsilon > 0 \). This result can be viewed as a result on expanders in the sense that for a given set if one polynomial is non-expanding, then it may imply that another polynomial is an expander.
In the setting of arbitrary finite fields, Garaev [8] provided an optimal bound for large sets as follows.

**Theorem 1.5.** Let $\mathbb{F}_q$ be a finite field of order $q$ and $A$ be a set in $\mathbb{F}_q$.

1. If $q^{1/2} \ll |A| \ll q^{2/3}$, then
   \[
   \max \{|A + A|, |A \cdot A|\} \gg \frac{|A|^2}{q^{1/2}}.
   \]

2. If $|A| \gg q^{2/3}$, then
   \[
   \max \{|A + A|, |A \cdot A|\} \gg (q|A|)^{1/2}.
   \]

It follows from aforementioned results that it seems that expanders fall into one of the following three types.

**Definition 1.1 ([10]).** Let $f : \mathbb{F}_q^l \to \mathbb{F}_q$.

- The function $f$ is called a strong expander with the exponent $\epsilon$ if for all $A \subseteq \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A, \ldots, A)| \geq q - k$, for some fixed positive constant $k$.

- The function $f$ is called a moderate expander with the exponent $\epsilon$ if for all $A \subseteq \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A, \ldots, A)| \gg q$.

- The function $f$ is called a weak expander with parameters $0 < \epsilon < 1$ and $0 < \delta < 1$ if for all $A \subseteq \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A, \ldots, A)| \geq |A|^\delta q^{1-\delta}$.

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 $\frac{1}{3}$: $x + yz$ [24], $x + (y - z)^2$ and $x(y + z)$ [28], $(x - y)^2 + (z - t)^2$ [2], $xy + zt$ [6], $xy + z + t$ [23].

However, there are only few families in four variables with the exponent bigger than $\frac{1}{3}$. Murphy and Petridis [17] proved that the polynomial $(x - y)(z - t)$ is a moderate expander with $\alpha = \frac{1}{3} + \frac{1}{13542}$, and Vinh [28] 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 moderate expander with the exponent $\frac{3}{8}$ over arbitrary finite fields.

In the setting of prime fields, Rudnev, Shkredov, and Stevens [22] also proved that the function $\frac{y - z}{x - t}$ is a moderate expander with the exponent $\frac{17}{42} = \frac{1}{3} + \frac{1}{14}$ over prime fields.
The focus of this article

In this paper, 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. Using the same approach, we derive similar results in the setting of finite local and principal rings. In this general setting, we also obtain a new result on distance sets in the p-adic perspective.

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 1.6.** 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 $Q(u,v) := m(u) + u^n v^n$, 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 1.7.** The following 4-variable polynomials are moderate expanders with the exponent $\frac{3}{8}$ over arbitrary finite fields:

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

**Proof.** This follows directly from Theorem 1.6 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 1.6 are moderate expanders with bigger exponents.

**Theorem 1.8.** 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

\[
\]

**Corollary 1.9.** The following 4-variable polynomials are moderate expanders with the exponent \( \frac{5}{13} \) over prime fields:

\[
\begin{align*}
&u(u + v)y + z, \quad u(u + v) + yz, \quad u(u + v)(y + z) \\
y(u(u + v) + z), \quad (u(u + v) - y)^2 + z, \quad (y - z)^2 + u(u + v).
\end{align*}
\]

**Proof.** This follows directly from Theorem 1.8 with the following polynomials:

\[
\begin{align*}
&xy + z, \quad x + yz, \quad x(y + z), \quad (x - y)^2 + z, \quad (y - z)^2 + x,
\end{align*}
\]

respectively. \qed

**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, we refer the reader to [18].

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 1.6 to the setting of finite valuation rings. However, we are able to put Corollary 1.7 in this setting.

**Theorem 1.10.** 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 \( |A| \gg q^{\frac{8r^2}{8}} \), then, for each \( i \in \{1, \ldots, 6\} \), we have

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

**Distance result in the p-adic view over finite valuation rings:** We now have a deeper look into Theorems 1.3 and 1.4. In the p-adic aspect, namely, \( p \) is fixed and \( r \) goes to infinity, it is clear that Theorems 1.3 and 1.4 are trivial. With this perspective, Lichtin [16] recently used p-adic analytic and exponential sum estimates to improve Theorem 1.3 by removing the factor \( r(r+1) \) on the condition of \( E \) in Theorem 1.3 as follows.

**Theorem 1.11.** Let \( \mathcal{E} \) be a set in \( \mathbb{Z}_p^d \). Suppose that \( |\mathcal{E}| \gg p^{rd^{-\frac{3}{2}}} \), then

\[
\Delta_{\mathbb{Z}_p^d}(\mathcal{E}) \supset \mathbb{Z}_p^d \cup \{0\}.
\]

Motivated by this new perspective, as an application of a moderate expander (Lemma 4.4), in our next result, we improve Theorem 1.4 by removing the factor \( r^{\frac{d+1}{2d-1}} \) on the condition of \( |A| \), and extend it to a more general setting of finite valuation rings.

**Theorem 1.12.** Let \( \mathcal{R} \) be a finite valuation ring of order \( q^r \), and \( A \) be a set in \( \mathcal{R} \). Suppose that

\[
|A| \gg q^{\frac{(2r−1)(d−1)+r}{2d−1}},
\]

then we have \( |\Delta_\mathcal{R}(A^d)| \gg q^r \).
Acknowledgments

Doowon Koh was supported by Basic Science Research Programs through National Research Foundation of Korea (NRF) funded by the Ministry of Education (2018R1D1A1B07044469). Mozhgan Mirzaei was supported by NSF grant DMS-1800746. Hossein Mojarrad was supported by Swiss National Science Foundation grant P2ELP2-178313. Thang Pham was supported by Swiss National Science Foundation grant P400P2-183916.

Doowon Koh and Thang Pham would like to thank Vietnam Institute of Advanced Study in Mathematics (VIASM) for the hospitality, where this paper has been completed.

2 Moderate expanders over arbitrary finite fields (Theorem 1.6)

Using a point-plane incidence bound due to Rudnev [21], the third, fourth, sixth listed authors and Shen [15] proved the following general theorem on the energy of a polynomial in three variables over prime fields.

**Theorem 2.1** ([15]). 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 $U, V, W \subset \mathbb{F}_p^r$ 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 [15] identically and use Vinh’s point-plane incidence bound [27] in the place of Rudnev’s point-plane incidence bound and the Kővari-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 $U, V, W \subset \mathbb{F}_q^r$, 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

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

**Proof.** By the Cauchy-Schwarz inequality, we have

$$|f(U,V,W)| \geq \frac{|U|^2|V|^2|W|^2}{E},$$

where $E$ denotes the number of tuples $(u, v, w, u', v', w') \in (U \times V \times W)^2$ such that $f(u, v, w) = f(u', v', w')$. Hence, the corollary follows by applying Theorem 2.2 to the above inequality. 

Let $m(x)$ and $n(x)$ be affinely independent polynomials. Suppose that the degrees of $m$ and $n$ are bounded. In [12], 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 $\epsilon$.

Using the point-line incidence bound for large sets over arbitrary finite fields due to Vinh [27], and the point-line incidence bound for small Cartesian product sets over prime fields due to Stevens and De Zeeuw [26], the following is a consequence of [12, Theorem 4] due to Hegyvári and Hennecart.

**Lemma 2.4** ([12]). 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 note here that if $Q(u, v) = u^2 + uv$, then Lemma 2.4 (1) was first obtained by Shkredov in [25].

We are now ready to prove Theorem 1.6.

**Proof of Theorem 1.6.** Since $|A| > 2$, without loss of generality, we may assume that $0 \notin A$. We define $U := \{Q(a, b) : a, b \in A\}$. 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. 

\[\square\]

# 3 Moderate expanders over prime fields (Theorem 1.8)

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 $U, V, W \subset \mathbb{F}_p^*$ with
\[ |U||V||W| \ll p^2, \text{ we have} \]
\[
|f(U, V, W)| \gg \min \left\{ (|U||V||W|)^{1/2}, \ |U|^2, \ |V|^2, \ |W|^2 \right\} .
\]

We are now ready to prove Theorem 1.8.

**Proof of Theorem 1.8.** Since \(|A| > 2\), without loss of generality, we may assume that \(0 \notin A\). Set \(U := \{Q(a, b) : a, b \in A\}\). 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. \(\square\)

## 4 Moderate expanders over finite valuation rings (Theorem 1.10)

In order to prove Theorem 1.10, 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 [20], 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 $\mathbb{R}^2$ and $L$ be a set of lines in $\mathbb{R}^2$. The number of incidences between $P$ and $L$, denoted by $I(P, L)$, satisfies

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

The second result is due to Yazici in [29].

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

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

Our next two lemmas are consequences of Theorem 4.1.

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

$$|X(Y + Z)| \gg \min \left\{ q^r, \frac{|X||Y||Z|}{q^{2r-1}} \right\}. \quad (3)$$

Proof. Since $|X| \geq 2q^{r-1}$ and $|\mathbb{R}^0| = q^{r-1}$, without loss of generality we may assume that $X \subset \mathbb{R}^x$. 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

$$|X||Y||Z| \leq N. \quad (2)$$

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 $a \in \mathbb{R}^x$, 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

$$N \leq \frac{|X||Y||Z||T|}{q^r} + q^r - \frac{1}{2} \sqrt{|X||Y||Z||T|}. \quad (3)$$
Combining the above inequality with (2), 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 \( \varphi \) 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 \( \varphi \) 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

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

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 1.10.
Lemma 4.5. Let $A$ be a set in $\mathcal{R}$. Suppose that $|A| \geq 2q^{-1}$, then we have

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

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

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

By an elementary calculation, we have

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

which implies that

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

and the theorem follows. \qed
We are now ready to prove Theorem 1.10.

**Proof of Theorem 1.10.** 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 \(X = \{u(u + v) : u, v \in A\}, Y = Z = A\). It follows from Lemma 4.5 that

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

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

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

whenever \(|A| \gg q^{\frac{nr-3}{r}}\). This completes the proof in the case of \(F_1\).

For any \(F_i\) with \(2 \leq i \leq 6\), the proof is almost the same as that for \(F_1\) except that we have to use Lemma 4.3 or Lemma 4.4 instead of Lemma 4.2 with switching the roles of \(X, Y, Z\) if necessary. \(\square\)

5 Distance result in p-adic view (Theorem 1.12)

**Proof of Theorem 1.12.** Since \(|A| \geq 2q^{r-1}\), we have

\[
|A \cap \mathcal{R}^\times| \geq |A| - |\mathcal{R}^0| = |A| - q^{r-1} \geq \frac{|A|}{2}
\]

Thus we may assume that \(A\) is a subset of \(\mathcal{R}^\times\).

We now prove that the size of \(A^2 = \{y^2 | y \in A\}\) is at least \(\gg |A|\). Indeed, suppose \(x^2 = y^2\) with \(x, y \in A\), then we have \((x - y)(x + y) = 0\). Therefore, either \(x = y\), or \(x = -y\), or \(x - y \in (z)\) and \(x + y \in (z)\). Notice that if we are in the last case, then we can assume that
\(x - y = u_1 z^{k_1}\) and \(x + y = u_2 z^{k_2}\) with \(u_1, u_2 \in \mathcal{R}\) and some positive integers \(k_1, k_2\). Hence, we have \(2x = u_1 z^{k_1} + u_2 z^{k_2} \in (z)\), which is a contradiction as both \(2, x \in \mathcal{R}\). Therefore, we only need to consider case \(x = y\) or \(x = -y\). This means that \(|A^2| \gg |A|\).

This also gives us that \(|(A - A)^2| \gg |A|\).

It is enough to show the following inequality

\[
|\Delta_R(A^d)| \gg \min \left\{ q^r, \frac{|A|^{2d-1}}{q^{(2r-1)(d-1)}} \right\}.
\]

We now proceed by induction on \(d\). Set \(Z = (A - A)^2, X = Y = A\). Using Lemma 4.4, the base case \(d = 2\) can be proved by using the observation that

\[
|\Delta_R(A^2)| \gg |Z + (A - A)^2| \gg \min \left\{ q^r, \frac{|A|^3}{q^{2r-1}} \right\} \gg q^r,
\]

whenever \(|A| \gg q^{-\frac{1}{4}}\). Thus the base case follows.

Suppose that the statement holds for any \(d - 1 \geq 2\). We now show that the statement holds for any \(d\). Indeed, by induction hypothesis, we have

\[
|\Delta_R(A^{d-1})| \gg \min \left\{ q^r, \frac{|A|^{2d-3}}{q^{(2r-1)(d-2)}} \right\}
\]

Set \(Z = \Delta_R(A^{d-1}), X = Y = A\), and applying Lemma 4.4 one more time, we have

\[
|\Delta_R(A^d)| \gg \min \left\{ q^r, \frac{|A|^{2d-1}}{q^{(2r-1)(d-1)}} \right\}.
\]

This completes the proof of the theorem. \(\square\)

**References**


Dao Nguyen Van Anh  
The Olympia Schools Hanoi, and Hanoi University of Science  
Email: dao.anh.dnv@theolympiaschools.edu.vn

Le Quang Ham  
Hanoi University of Science, Vietnam  
E-mail: hamlaoshi@gmail.com

Doowon Koh  
Chungbuk National University, Korea  
E-mail: koh131@chungbuk.ac.kr

Mozhgan Mirzaei  
University of California San Diego, USA  
E-mail: momirzae@ucsd.edu

Hossein Nassajian Mojarrad  
New York University  
E-mail: hossein.mojarrad70@gmail.com, sn2854@nyu.edu

Thang Pham  
University of Rochester New York  
E-mail: vanthangpham@rochester.edu