On two-variable Expanders over finite rings

Do Duy Hieu
Institute of Mathematics
Vietnam Academy of Science and Technology
ddhieu@math.ac.vn

Abstract

In this short note, we will give the finite ring versions of some results on two-variable expanders, which were studied over finite fields by Balog et al. and Hart et al.

Data availability: Not applicable.

1 Introduction

Let $q = p^r$ be an odd prime power, and let $\mathbb{F}_q$ be a finite field of q elements. Bourgain, Katz, and Tao ([3]) made the first investigation on the finite field analogs of the sum-product problem. They showed that when $1 \ll |\mathcal{A}| \ll q$, then $\max\{|\mathcal{A}+\mathcal{A}|, |\mathcal{A}\cdot\mathcal{A}|\} \gtrsim |\mathcal{A}|^{1+\epsilon}$, for some $\epsilon > 0$, where $X \gg Y$ means that $Y = o(X)$, and $X \gtrsim Y$ means that $X \geq CY$ for some large constant C, with X, Y are viewed as functions of the parameter q. This improves the trivial bound $|\mathcal{A}+\mathcal{A}||\mathcal{A}\cdot\mathcal{A}| \gtrsim |\mathcal{A}|$. The precise statement of their result is as follows.

Theorem 1.1 (**Bourgain-Katz-Tao**, [3]). *Let $\mathcal{A}$ be a subset of $\mathbb{F}_q$ such that $q^\delta < |\mathcal{A}| < q^{1-\delta}$ for some $\delta > 0$. Then one has a bound of the form*

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

for some $\epsilon = \epsilon(\delta) > 0$.

The relationship between ϵ and δ in their result is difficult to determine. The explicit bounds on ϵ can be found in [16, 19].

The Bourgain-Katz-Tao theorem has stimulated a lot of research on finite field analogs of sum-product estimates in recent years, see for example [4, 5, 6, 8, 9, 12, 13, 14, 16, 19], and references therein.

The main purpose of this short note is to study some two-variable expanders over finite cyclic rings $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$. Our first result is the finite ring analog of a result due to A. Balog, A. Broughan, and E. Shparlinski [2].

Theorem 1.2. *For arbitrary set $A \subseteq \mathbb{Z}_q^\times$, of cardinality $|A| \gtrsim q^{\frac{1}{2}}$, with p be an odd prime, $q = p^r$. We have*

$$|A + A^{-1}| \gtrsim \min\left\{\sqrt{p^r|A|}, \frac{|A|^2}{\sqrt{rp^{2r-1}}}\right\}.$$

Our second result is the finite ring version of a result established by D. Hart, L. Li, and C-Y. Shen [9].

Theorem 1.3. *Let $A \subseteq \mathbb{Z}_q$, of cardinality $|A| \gtrsim q^{\frac{1}{2}}$, with p be an odd prime, $q = p^r$. We have*

$$|A + A^2| \gtrsim \min\left\{\sqrt{p^r|A|}, \frac{|A|^2}{\sqrt{2rp^{2r-1}}}\right\}.$$

To evaluate cardinality of the set $A(A+1)$ in the next theorem, we will use the product graph $B_q(d, \lambda)$ in [17]. The author needs to use division operations in this graph construction, so we must avoid the non-invertible elements in the ring $\mathbb{Z}_q$. Therefore, here we only consider the case of the set $A \subseteq \mathbb{Z}_q \setminus \{p\mathbb{Z}_{p^{r-1}}, p\mathbb{Z}_{p^{r-1}} - 1\}$. We also obtain the following theorem using the same techniques as proof of the Theorem 1.3.

Theorem 1.4. *Let $A \subseteq \mathbb{Z}_q \setminus \{p\mathbb{Z}_{p^{r-1}}, p\mathbb{Z}_{p^{r-1}} - 1\}$, of cardinality $|A| \gtrsim q^{\frac{1}{2}}$, with p be an odd prime, $q = p^r$. We have*

$$|A(A+1)| \gtrsim \min\left\{\sqrt{p^r|A|}, \frac{|A|^2}{\sqrt{2rp^{2r-1}}}\right\}.$$

2 Graphs over finite rings

For a graph G, let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. The quantity $\lambda(G) = \max\{\lambda_2, -\lambda_n\}$ is called the second eigenvalue of G. A graph $G = (V, E)$ is called an (n, d, λ)-graph if it is d-regular, has n vertices and the second eigenvalue of G is at most λ. It is well known (see [1, Chapter 9] for more details) that if λ is much smaller than the degree d, then G has certain random-like properties. For two (not necessarily) disjoint subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs (u, w) such that $u \in U$, $w \in W$, and (u, w) is an edge of G. For a vertex v of G, let $N(v)$ denote the set of vertices of G adjacent to v and let $d(v)$ denote its degree. Similarly, for a subset U of the vertex set, let $N_U(v) = N(v) \cap U$ and $d_U(v) = |N_U(v)|$. We will need the following well-known fact.

Lemma 2.1. *([1, Corollary 9.2.5]) Let $G = (V, E)$ be an (n, d, λ)-graph. For any two sets $B, C \subset V$, we have*

$$\left|e(B, C) - \frac{d|B||C|}{n}\right| \leq \lambda\sqrt{|B||C|}.$$

2.1 Product graphs over finite rings

Suppose that $q = p^r$ for some odd prime p and $r \geq 2$. We identify $\mathbb{Z}_q$ with $\{0, 1, \ldots, q-1\}$, then $p\mathbb{Z}_{p^{r-1}}$ is the set of nonunits in $\mathbb{Z}_q$. For any $\lambda \in \mathbb{Z}_q$, the product graph $B_q(d, \lambda)$ is defined as follows. The vertex set of the product graph $B_q(d, \lambda)$ is the set $V(B_q(d, \lambda)) = \mathbb{Z}_{p^r}^d \backslash (p\mathbb{Z}_{p^{r-1}})^d$. Two vertices $\boldsymbol{a}$ and $\boldsymbol{b} \in V(B_q(d, \lambda))$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(B_q(d, \lambda))$, if and only if $\boldsymbol{a} \cdot \boldsymbol{b} = \lambda$. When $\lambda = 0$, the graph is a variant of Erdős-Rényi graph, which has many interesting applications (see [18]) . We now study the product graph when $\lambda \in \mathbb{Z}_q^\times$.

Lemma 2.2. *([17, Theorem 2.4]) For any $d \geq 2$ and $\lambda \in \mathbb{Z}_{p^r}^\times$, the product graph $B_q(d, \lambda)$ is an*

$$(p^{rd} - p^{(r-1)d}, p^{r(d-1)}, \sqrt{2rp^{(d-1)(2r-1)}}) - graph.$$

2.2 Sum-square graphs over finite rings

Suppose that $q = p^r$ for a sufficiently large prime p. The sum-square the graph $\mathcal{SR}_q$ is defined as follows. The vertex set of the sum-product graph $\mathcal{SR}_q$ is the set $V(\mathcal{SR}_q) = \mathbb{Z}_q \times \mathbb{Z}_q$. Two vertices (a, b) and $(c, d) \in V(\mathcal{SR}_q)$ are connected by an edge in $E(\mathcal{SR}_q)$, if and only if $a+c = (b+d)^2$. We have the following pseudo-randomness of the sum-product graph $\mathcal{SR}_q$.

Theorem 2.3. *([7, Theorem 3.4]) The sum-square graph $\mathcal{SR}_q$ is a*

$$\left(p^{2r}, p^r, \sqrt{2rp^{2r-1}}\right) - graph.$$

3 Proof of Theorem 1.2

In this section, we will need the following Fourier-analytic result, which is an easy variant of the corresponding estimate from [10] and [11]. Define the Fourier transform $\widehat{f}$ of $f(x)$ as

$$\widehat{f}(\boldsymbol{m}) = q^{-2} \sum_{\boldsymbol{x} \in \mathbb{Z}_q^2} f(\boldsymbol{x}) \cdot \chi(-\boldsymbol{x} \cdot \boldsymbol{m}),$$

where $\chi(x) = exp(2\pi ix/q)$.

Firstly, we will need the following additional Lemmas.

Lemma 3.1. *Let p be an odd prime, $q = p^r$ and $j \in \mathbb{Z}_q^\times$. Let $S_j = \{\boldsymbol{x} \in \mathbb{Z}_q^2 : x_1 \cdot x_2 = j\}$. Then,*

$$|S_j| = p^r - p^{r-1}.$$

Proof. Since $x_1 \cdot x_2 = j \in \mathbb{Z}_q^\times$, hence for every $x_1 \in \mathbb{Z}_q^\times$ there exists a unique x_2, this completes the proof of Lemma 3.1. □

Lemma 3.2. *Identify S_j with its indicator function. For $j \in \mathbb{Z}_q^\times$ with $q = p^r$, we have*

$$\sup_{\boldsymbol{m} \neq (0,0)} |\widehat{S}_j(\boldsymbol{m})| \leq r p^{-r-\frac{1}{2}}.$$

Proof. We write

$$\begin{aligned}
\widehat{S}_j(\boldsymbol{m}) &= q^{-2} \sum_{\boldsymbol{x} \in \mathbb{Z}_q^2} S_j(\boldsymbol{x}) \chi(-\boldsymbol{m} \cdot \boldsymbol{x}), \\
&= q^{-2} \sum_{x_1 \cdot x_2 = j} \chi(-\boldsymbol{m} \cdot \boldsymbol{x}), \\
&= q^{-2} \sum_{x_1 \cdot x_2 = j} \chi(-x_1 \cdot m_1 - x_2 \cdot m_2), \\
&= q^{-2} \sum_{x_1 \in \mathbb{Z}_q^\times} \chi(-x_1 \cdot m_1 - m_2 j x_1^{-1}).
\end{aligned}$$

By Kloosterman sums [20], we have

$$|\widehat{S}_j(\boldsymbol{m})| \leq q^{-2} \tau(q) \sqrt{gcd(m_1, j m_2, q)}\, q^{1/2} \leq r p^{-r-\frac{1}{2}}.$$

This completes the proof of Lemma 3.2. □

Lemma 3.3. *Let $\mathcal{E}, \mathcal{F} \in \mathbb{Z}_q^2$. Then*

$$|\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{E} \times \mathcal{F} \,:\, (x_1 - y_1) \cdot (x_2 - y_2) = j\}| \leq |\mathcal{E}||\mathcal{F}| q^{-1} + r p^{r-\frac{1}{2}} \sqrt{|\mathcal{E}||\mathcal{F}|}.$$

Proof. Let

$$S_j = \{\boldsymbol{x} \in \mathbb{Z}_q^2 \,:\, x_1 \cdot x_2 = j\}.$$

We have

$$\begin{aligned}
&|\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{E} \times \mathcal{F} \,:\, (x_1 - y_1) \cdot (x_2 - y_2) = j\}| \\
&= \sum_{\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^2} E(\boldsymbol{x}) F(\boldsymbol{y}) S_j(\boldsymbol{x} - \boldsymbol{y}), \qquad (3.1)
\end{aligned}$$

where E and F are characteristic functions of $\mathcal{E}$ and $\mathcal{F}$ respectively.
Using Fourier transform, (3.1) equals

$$\begin{aligned}
&\sum_{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{m} \in \mathbb{Z}_q^2} \chi(\boldsymbol{m} \cdot (\boldsymbol{x} - \boldsymbol{y})) E(\boldsymbol{x}) F(\boldsymbol{y}) \widehat{S}_j(\boldsymbol{m}), \\
&= q^4 \sum_{\boldsymbol{m} \in \mathbb{Z}_q^2} \widehat{E}(\boldsymbol{m}) \overline{\widehat{F}(\boldsymbol{m})} \widehat{S}_j(\boldsymbol{m}), \\
&= q^{-2} |\mathcal{E}||\mathcal{F}||S_j| + q^4 \sum_{\boldsymbol{m} \neq \boldsymbol{0}} \widehat{E}(\boldsymbol{m}) \overline{\widehat{F}(\boldsymbol{m})} \widehat{S}_j(\boldsymbol{m}) = A + B,
\end{aligned}$$

By Lemma 3.1 we have

$$|A| = q^{-2}|\mathcal{E}||\mathcal{F}||S_j| = q^{-2}(p^r - p^{r-1})|\mathcal{E}||\mathcal{F}| \leq q^{-1}|\mathcal{E}||\mathcal{F}|. \tag{3.2}$$

Using Cauchy- Schwartz we see that

$$|B| \leq q^4 \left(\sum_{\boldsymbol{m}\in\mathbb{Z}_q^2} |\widehat{E}(\boldsymbol{m})|^2 \right)^{\frac{1}{2}} \left(\sum_{\boldsymbol{m}\in\mathbb{Z}_q^2} |\widehat{F}(\boldsymbol{m})|^2 \right)^{\frac{1}{2}} \cdot \sup_{\boldsymbol{m}\neq(0,0)} |\widehat{S}_j(\boldsymbol{m})| \tag{3.3}$$

By Parseval identity [15], we have

$$\sum_{\boldsymbol{m}\in\mathbb{Z}_q^2} |\widehat{E}(\boldsymbol{m})|^2 = q^{-2} \sum_{\boldsymbol{x}\in\mathbb{Z}_q^2} |E(\boldsymbol{x})|^2 = q^{-2}|\mathcal{E}|, \tag{3.4}$$

$$\sum_{\boldsymbol{m}\in\mathbb{Z}_q^2} |\widehat{F}(\boldsymbol{m})|^2 = q^{-2} \sum_{\boldsymbol{x}\in\mathbb{Z}_q^2} |F(\boldsymbol{x})|^2 = q^{-2}|\mathcal{F}|. \tag{3.5}$$

Plugging (3.4) and (3.5) into (3.3) we get

$$|B| \leq q^2\sqrt{|\mathcal{E}||\mathcal{F}|} \sup_{\boldsymbol{m}\neq(0,0)} |\widehat{S}_j(\boldsymbol{m})|.$$

By Lemma 3.2, we have

$$|B| \leq q^2\sqrt{|\mathcal{E}||\mathcal{F}|}rp^{-r-\frac{1}{2}} = rp^{r-\frac{1}{2}}\sqrt{|\mathcal{E}||\mathcal{F}|}. \tag{3.6}$$

Combining (3.6) and (3.2) estimates. This completes the proof of Lemma 3.3. □

We are now ready to give a proof of Theorem 1.2. Let N be the number of solutions of equation

$$c + (s-b)^{-1} = t,\ (s, b, c, t) \in S \times B \times C \times T,$$

where

$$S = A + B,\ T = A^{-1} + C.$$

It is clear that $N \geq |A||B||C|$. Let $\mathcal{E} = T \times S$, $\mathcal{F} = C \times B$, from Lemma 3.3, we have

$$|A||B||C| \leq N \leq \frac{|S||B||C||T|}{p^r} + \sqrt{rp^{2r-1}|S||B||C||T|},$$

Let $t = \sqrt{|S||T|} \geq 0$, then

$$\frac{\sqrt{|B||C|}}{p^r}t^2 + \sqrt{rp^{2r-1}}t - |A|\sqrt{|B||C|} \geq 0,$$

which implies that

$$
\begin{aligned}
\sqrt{|S||T|} &\geq \frac{-\sqrt{rp^{2r-1}} + \sqrt{rp^{2r-1} + 4|A||B||C|/p^r}}{2\sqrt{|B||C|}/p^r} \\
&= \frac{2|A|\sqrt{|B||C|}}{\sqrt{rp^{2r-1}} + \sqrt{rp^{2r-1} + 4|A||B||C|/p^r}} \\
&\gtrsim \min\left\{\sqrt{p^r|A|}, \sqrt{\frac{|A|^2|B||C|}{rp^{2r-1}}}\right\}.
\end{aligned}
$$

We replace B by A^{-1} and C by A. This concludes the proof of the Theorem 1.2.

4 Proof of Theorem 1.3

Let N be the number of solutions of equation

$$(s-d)^2 + c = t, \ (s, d, c, t) \in S \times D \times C \times T,$$

where

$$S = A + B^2, \ D = B^2, \ T = A^2 + C.$$

It is clear that $N \geq |A||B||C|/2$. Besides, N is the number of edges between $(-C)\times(-B)$ and $T \times S$ of the sum-square graph $\mathcal{SR}_q$. From Lemma 2.1 and Lemma 2.3, we have

$$\left| N - \frac{|S||B^2||C||T|}{q} \right| \leq \sqrt{q|S||B^2||C||T|},$$

Similar to the previous section, we have

$$\sqrt{|S||T|} \gtrsim \min\left\{\sqrt{p^r|A|}, \sqrt{\frac{|A|^2|D||C|}{2rp^{2r-1}}}\right\}.$$

We replace B and C by A. This concludes the proof of the Theorem 1.3.

5 Proof of Theorem 1.4

Let N be the number of solutions of equation

$$(sb^{-1} + 1)c = t, \ (s, b, c, t) \in S \times B \times C \times T,$$

where

$$S = A(D+1), \ B = D+1, \ T = C(A+1).$$

It is clear that $N \geq |A||B||C|$. Besides, N is the number of edges between $C^{-1} \times B^{-1}$ and $T \times (-S)$ of the product graph $B_q(2,1)$. From Lemma 2.1 and Lemma 2.2, we have

$$\left| N - \frac{|S||B||C||T|}{p^r(1-1/p^2)} \right| \leq \sqrt{2rp^{2r-1}|S||B||C||T|},$$

Similar to the previous section, we have

$$\sqrt{|S||T|} \quad \gtrsim \quad \min \left\{ \sqrt{p^r|A|}, \sqrt{\frac{|A|^2|D||C|}{2rp^{2r-1}}} \right\}.$$

We replace C and D by A. This concludes the proof of the Theorem 1.4.

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.

[2] A. Balog, K. A. Broughan, I. E. Shparlinski, *Sum-products estimates with several sets and applications*, Integers, **12**(5) (2010), 895–906.

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

[4] J. Cilleruelo, Combinatorial problems in finite fields and Sidon sets, Combinatorica, 32(5) (2012), 497–511.

[5] M. Garaev, *The sum-product estimate for large subsets of prime fields*, Proceedings of the American Mathematical Society, **136**(8) (2008), 2735–2739.

[6] M. Garaev, C.-Y. Shen, *On the size of the set* $A(A+1)$, Math. Z. **263**(2009), no. 94.

[7] D. D. Hieu and L. A. Vinh, On distance sets and product sets in vector spaces over finite rings, *Michigan Math. J.,* **62** (2013), 14p.

[8] 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.

[9] D. Hart, L. Li, C-Y. Shen, *Fourier analysis and expanding phenomena in finite fields*, Proceedings of the American Mathematical Society, **141**(2)(2013), 461–473.

[10] D. Hart, A. Iosevich. *Sums and products in finite fields: an integral geometric viewpoint.* Radon transforms, geometry, and wavelets, pp. 129–135. Contemp. Math., 464, Amer. Math. Soc., Providence, RI (2008).

[11] 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. Amer. Math. Soc. 363 (2011), no. 6, 3255–3275.

[12] N. Hegyvári, F. Hennecart, *Explicit construction of extractors and expanders*, Acta Arith. **140**(2009), 233–249.

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

[14] D. Hart, A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Contemp. Math. **464**(2008).

[15] A. Terras, Fourier Analysis on Finite Groups and Applications. London Mathematical Society, Student Texts 43, 1999.

[16] L.A. Vinh, *A Szemerédi-Trotter type theorem and sum-product estimate over finite fields*, Eur. J. Comb. **32**(8) (2011), 1177–1181.

[17] L. A. Vinh, Sum and shifted-product subsets of product-sets over finite rings, *The Electronic Journal of Combinatorics* **19**(2) (2012), P33.

[18] L. A. Vinh and P. V. Thang, Erdős - Rényi graph, Szemerédi - Trotter type theorem, and sum-product estimates over finite rings, *Forum Mathematicum*, DOI:10.1515/forum-2011-0161 (published online).

[19] H. V. Vu, *Sum-product estimates via directed expanders*, Mathematical research letters **15**(2) (2008), 375–388.

[20] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. 34 (1948), 204–207.