Erdős–Rényi graph, Szemerédi–Trotter type theorem, and sum-product estimates over finite rings

Pham Van Thang and Le Anh Vinh

Communicated by Jörg Brüdern

Abstract. We study a variant of Erdős–Rényi graph over finite rings. We then use this graph to obtain a Szemerédi–Trotter type theorem and a sum-product estimate in finite rings.

Keywords. Erdős–Rényi graphs, Szemerédi–Trotter theorem, sum-product estimate.

2010 Mathematics Subject Classification. 05C55, 05C35.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of $q$ elements where $q$ is a large odd prime power. Let $\mathcal{A}$ be a non-empty subset of a finite field $\mathbb{F}_q$. We consider the sum set

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

and the product set

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

Let $|\mathcal{A}|$ denote the cardinality of $\mathcal{A}$. Here, and throughout, $X \leq Y$ means that there exists $C > 0$ such that $X \leq CY$, and $X \ll Y$ means that $X = o(Y)$. Bourgain, Katz and Tao ([3]) 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 $\epsilon > 0$; this improves the trivial bound $|\mathcal{A} + \mathcal{A}| \cdot |\mathcal{A} \cdot \mathcal{A}| \gtrsim |\mathcal{A}|$. The precise statement of the sum-product estimate is as follows.

Theorem 1.1 ([3]). Let $\delta > 0$, and let $\mathbb{F}_q$ be a finite field of $q$ elements where $q$ is an odd prime. Then, there exists a number $\epsilon > 0$ such that for any set $\mathcal{A}$ be a subset of $\mathbb{F}_q$ with

$$q^\delta < |\mathcal{A}| < q^{1-\delta}$$

one has

$$\max(|\mathcal{A} + \mathcal{A}|, |\mathcal{A} \cdot \mathcal{A}|) \gtrsim |\mathcal{A}|^{1+\epsilon}.$$
Using Theorem 1.1, Bourgain, Katz and Tao proved a theorem of Szemerédi–Trotter type in two-dimensional finite field geometries. Roughly speaking, this theorem asserts that if we are in the finite plane $\mathbb{F}_q^2$ and one has $N$ lines and $N$ points in that plane for some $1 \ll N \ll q^2$, then there are at most $O(N^{3/2 - \varepsilon})$ incidences; this improves the standard bound of $O(N^{3/2})$ obtained from extremal graph theory. The precise statement of the theorem is as follows.

**Theorem 1.2 ([3]).** Let $\mathcal{P}$ be a collection of points and $\mathcal{L}$ be a collection of lines in $\mathbb{F}_q^2$. For any $0 < \alpha < 2$, if $|\mathcal{P}|, |\mathcal{L}| \leq N = q^\alpha$, then we have

$$|\{(p, l) \in \mathcal{P} \times \mathcal{L} : p \in l\}| \lesssim N^{3/2 - \varepsilon},$$

for some $\varepsilon = \varepsilon(\alpha) > 0$ depending only on the exponent $\alpha$.

In [13], the second author proceeded in an opposite direction: he first proved a theorem of Szemerédi–Trotter type about the number of incidences between points and lines in finite field geometries and then applied this result to obtain a different proof of a result of Garaev on sum-product estimate for large subsets of finite fields. This estimate is the best known bound in the finite field problem. More precisely, we have the following results.

**Theorem 1.3 ([13, Theorem 3]).** Let $\mathcal{P}$ be a collection of points and $\mathcal{L}$ be a collection of lines in $\mathbb{F}_q^2$. Then we have

$$|\{(p, l) \in \mathcal{P} \times \mathcal{L} : p \in l\}| \leq \frac{|\mathcal{P}| |\mathcal{L}|}{q} + q^{1/2} \sqrt{|\mathcal{P}| |\mathcal{L}|}. \quad (1.1)$$

Note that the analog of Theorem 1.3 for the case $\mathcal{P} \equiv \mathcal{L}$ (in $P\mathbb{F}_q^d$) is obtained by Alon and Krivelevich ([1]) via a similar approach and by Hart, Iosevich, Koh and Rudnev ([6]) via Fourier analysis. Note that going from one set formulation in Theorem 2.1 in [6] and Lemma 2.2 in [1] to a two set formulation is just a matter of inserting a different letter in a couple of places. Furthermore, the proof of [13, Theorem 3] shows that in order to deal with large sets in the finite projective plane the only axiom one needs is regularity: every line has $q + 1$ points. More involved properties of $P\mathbb{F}_q^3$, such as the Desargues or Pappus axioms, are not needed (this is not clear with the Fourier approach.) The latter two axioms enable the field arithmetic on the lines in $P\mathbb{F}_q^3$, but the proof in [13] shows that, in fact, it has nothing to do with the arithmetics in large sets. Presumably, to extend the theorem to smaller sets shall require the use of the Desargues and/or Pappus axioms, and that is why it seems much more difficult.

In the spirit of Bourgain–Katz–Tao’s result, one can derive from Theorem 1.3 a reasonably good estimate when $d = 2$ and $1 < \alpha < 2$. 


Corollary 1.4 ([13, Corollary 1]). Let $\mathcal{P}$ be a collection of points and $\mathcal{L}$ be a collection of lines in $\mathbb{F}_q^2$. Suppose that $|\mathcal{P}|, |\mathcal{L}| \leq N = q^\alpha$ with $1 + \epsilon \leq \alpha \leq 2 - \epsilon$ for some $\epsilon > 0$. Then we have

$$|\{(p, l) \in \mathcal{P} \times \mathcal{L} : p \in l\}| \leq 2N^{\frac{3}{2} - \frac{\epsilon}{4}}. \quad (1.2)$$

Corollary 1.4 has applications in several combinatorial problems (see for example [8,9]). In [13], the second author also used the incidence bound in Theorem 1.3 to obtain a sum-product estimate.

Theorem 1.5 ([13, Theorem 5, Corollary 2]). Let $\mathcal{A} \subset \mathbb{F}_q$ with $q$ is an odd prime power. Suppose that

$$|\mathcal{A} + \mathcal{A}| = u, |\mathcal{A}A| = v. \quad \text{Then}$$

$$|\mathcal{A}|^2 \leq \frac{uv|\mathcal{A}|}{q} + q^{1/2}\sqrt{uv}. \quad (1.3)$$

In particular, we have

$$\max(|\mathcal{A} + \mathcal{A}|, |\mathcal{A}A|) \geq \frac{2|\mathcal{A}|^2}{q^{1/2} + \sqrt{q + \frac{4|\mathcal{A}|^3}{q}}}. \quad (1.3)$$

We note the following trivial consequence of Theorem 1.5.

Corollary 1.6. Let $A \subset \mathbb{F}_q$ where $q$ is an odd prime power.

(i) Suppose that $q^{1/2} \lesssim |A| \lesssim q^{2/3}$. Then

$$\max(|A + A|, |AA|) \gtrsim \frac{|A|^2}{q^{1/2}}.$$

(ii) Suppose that $q^{2/3} \lesssim |A| \lesssim q$. Then

$$\max(|A + A|, |AA|) \gtrsim (q|A|)^{1/2}.$$
Besides, the bound in Theorem 1.5 is stronger than those established in [7, Theorem 1.1]. We also call the reader’s attention to the fact that the application of the spectral method from graph theory in sum-product estimates was independently used by Vu in [14]. The bound in Corollary 1.6 is stronger than those in [14, Remark 1.4] (which is also implicit from [7, Theorem 1.1]).

Let \( m \) be a large non-prime integer and \( \mathbb{Z}_m \) be the ring of residues mod \( m \). Let \( \gamma(m) \) be the smallest prime divisor of \( m \), \( \alpha(m) \) be the number of prime divisors of \( m \), and \( \tau(m) \) be the number of divisors of \( m \). We identify \( \mathbb{Z}_m \) with the set \( \{0, 1, \ldots, m - 1\} \). Define the set of units and the set of nonunits in \( \mathbb{Z}_m \) by \( \mathbb{Z}_m^\times \) and \( \mathbb{Z}_m^0 \) respectively. The finite Euclidean space \( \mathbb{Z}_m^d \) consists of column vectors \( x \), with \( j \) th entry \( x_j \in \mathbb{Z}_m \). In this paper, we will extended the aforementioned results to the setting of finite cyclic rings \( \mathbb{Z}_m \). One reason for considering this situation is that if one is interested in answering similar questions on the setting of rational points, one can ask questions for such sets and how they compare to the answers in \( \mathbb{R}^d \). By scale invariance of these questions, the problem for a subset \( E \) of \( \mathbb{Q}^d \) would be the same as for subsets of \( \mathbb{Z}_m^d \).

The rest of this paper is organized as follows. In Section 2, we study a variant of Erdős–Rényi graphs over the finite ring \( \mathbb{Z}_m \). We then use this graph to obtain a Szemerédi–Trotter type theorem over \( \mathbb{Z}_m \). More precisely, we will prove the following theorem in Section 3.

**Theorem 1.7.** Let \( \mathcal{P} \) be a collection of points and \( \mathcal{L} \) be a collection of lines in \( \mathbb{Z}_m^2 \). Then we have

\[
|\{(p, l) \in \mathcal{P} \times \mathcal{L} : p \in l\}| \leq \frac{|\mathcal{P}||\mathcal{L}|}{m} + \frac{2\tau(m)m^2}{\phi(m)\gamma(m)^{1/2}} \sqrt{|\mathcal{P}||\mathcal{L}|}. \tag{1.4}
\]

Notice that Theorem 1.7 is most effective when \( m \) has only few prime divisors. For example, if \( m = p^r \), in the spirit of Bourgain–Katz–Tao’s result, one can obtain a reasonably good estimate when \( p^{2r-1+\epsilon} \lesssim N \lesssim p^{2r-\epsilon} \).

**Corollary 1.8.** Let \( \mathcal{P} \) be a collection of points and \( \mathcal{L} \) be a collection of lines in \( \mathbb{Z}_p^2 \). Suppose that \( |\mathcal{P}|, |\mathcal{L}| \lesssim N = p^\alpha \) with \( 2r - 1 + \epsilon \leq \alpha \leq 2r - \epsilon \) for some \( \epsilon > 0 \). Then we have

\[
|\{(p, l) \in \mathcal{P} \times \mathcal{L} : p \in l\}| \lesssim N^\frac{3}{2} \frac{\epsilon}{\alpha^\epsilon}. \tag{1.5}
\]

Finally, we will derive a sum-product estimate in finite rings from Theorem 1.7 (which is of the same order as [5, Theorem 1.4]).

**Theorem 1.9.** Let \( A \subset \mathbb{Z}_m \). Suppose that

\[
|A + A| = u, \quad |A.A| = v.
\]
Then
\[ |A| \leq \frac{uv|A|}{m} + \frac{2\tau(m)m^2}{\phi(m)\gamma(m)^{1/2}} \sqrt{uv}, \]
which implies that
\[ \max(|A + A|, |AA|) \geq \min \left( \frac{|A|^2 \phi(m)\gamma(m)^{1/2}}{\tau(m)m^2}, (m|A|)^{1/2} \right). \]

2 Erdős–Rényi graphs over rings

2.1 Pseudorandom graphs

For a graph $G$ of order $n$, let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ 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 $(n, d, \lambda)$-graph if it is $d$-regular, has $n$ vertices, and the second eigenvalue of $G$ is at most $\lambda$. It is well known (see [2, Chapter 9] for more details) that if $\lambda$ 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 first recall the following two well-known facts (see, for example, [2]).

**Theorem 2.1** ([2, Theorem 9.2.4]). Let $G = (V, E)$ be an $(n, d, \lambda)$-graph. For any subset $U$ of $V$, we have
\[ \sum_{v \in V} (d_U(v) - d|U|/n)^2 < \lambda^2 |U|. \]

The following result is an easy corollary of Theorem 2.1.

**Corollary 2.2** ([2, Corollary 9.2.5]). Let $G = (V, E)$ be an $(n, d, \lambda)$-graph. For any two sets $B, C \subset V$, we have
\[ \left| e(B, C) - \frac{d|B||C|}{n} \right| \leq \lambda \sqrt{|B||C|}. \]

2.2 Zero-product graphs

For any integers $m, d \geq 2$, the zero-product graph $\mathbb{ZP}_{m,d}$ is defined as follows. The vertex set of the zero-product graph $\mathbb{ZP}_{m,d}$ is the set
\[ V(\mathbb{ZP}_{m,d}) = \mathbb{Z}_m^d \setminus (\mathbb{Z}_m^0)^d. \]
Two vertices \( a, b \in V(\mathcal{P}_{m,d}) \) are connected by an edge, \((a, b) \in E(\mathcal{P}_{m,d})\), if and only if \( a \cdot b = 0 \in \mathbb{Z}_m \). We have the following pseudo-randomness of the zero-product graph \( \mathcal{P}_{m,d} \).

**Theorem 2.3.** For any \( m, d \geq 2 \), the zero-product graph \( \mathcal{P}_{m,d} \) is an

\[
\left( m^d - (m - \phi(m))^d, m^{d-1} - (m - \phi(m))^{d-1}, \frac{2\tau(m)m^{d-1}}{\gamma(m)(d-2)/2} \right) \text{-graph.}
\]

**Proof.** It follows from the definition of the zero-product graph that \( \mathcal{P}_{m,d} \) is a graph of order \( m^d - (m - \phi(m))^d \). The valency of the graph is also easy to compute. Given a vertex \( x \in V(\mathcal{P}_{m,d}) \), there exists an index \( x_i \in \mathbb{Z}_m^\times \). We can assume that \( x_1 \in \mathbb{Z}_m^\times \). For any choice of \( y_2, \ldots, y_d \in \mathbb{Z}_m \) where not all \( y_j \) are non-units, the equation \( x \cdot y = 0 \) determines \( y_1 \) uniquely (note that, if \( y_2, \ldots, y_d \in \mathbb{Z}_m^0 \), then so is \( y_1 \)). Hence, \( \mathcal{P}_{m,d} \) is a regular graph of valency \( m^{d-1} - (m - \phi(m))^{d-1} \).

It remains to estimate the eigenvalues of this multigraph (i.e. graph with loops). For any \( a \neq b \in \mathbb{Z}_m \setminus (\mathbb{Z}_m^0)^d \), we count the number of solutions of the following system:

\[
a \cdot x \equiv b \cdot x \equiv 0 \mod m, \quad x \in \mathbb{Z}_m \setminus (\mathbb{Z}_m^0)^d. \tag{2.1}
\]

There exist uniquely \( n \mid m \) and \( b_1 \in (\mathbb{Z}_{m/n})^d \setminus (\mathbb{Z}_{m/n}^0)^d \) such that \( b = a + nb_1 \). The system (2.1) above becomes

\[
a \cdot x \equiv nb_1 \cdot x \equiv 0 \mod m, \quad x \in (\mathbb{Z}_m)^d \setminus (\mathbb{Z}_m^0)^d. \tag{2.2}
\]

Let \( a_n \in (\mathbb{Z}_{m/n})^d \setminus (\mathbb{Z}_{m/n}^0)^d \), \( a_n \equiv a \mod m/n \) and \( x_n \in (\mathbb{Z}_{m/n})^d \setminus (\mathbb{Z}_{m/n}^0)^d \), \( x_n \equiv x \mod m/n \). To solve (2.2), we first solve the following system:

\[
a_n \cdot x_n \equiv b_1 \cdot x_n \equiv 0 \mod m/n, \quad x_n \in (\mathbb{Z}_{m/n})^d \setminus (\mathbb{Z}_{m/n}^0)^d. \tag{2.3}
\]

Let \( a_n = (a_1, \ldots, a_d) \) and \( b_1 = (b_1, \ldots, b_d) \). Since \( a_n \in (\mathbb{Z}_{m/n})^d \setminus (\mathbb{Z}_{m/n}^0)^d \), there exists \( a_i \in \mathbb{Z}_m^\times \). W.l.o.g., we can assume that \( a_1 \in \mathbb{Z}_m^\times \). Let

\[
k_1 = a_2x_2 + \cdots + a_dx_d \quad \text{and} \quad k_2 = b_2x_2 + \cdots + b_dx_d.
\]

System (2.3) is equivalent to the following system:

\[
a_1x_1 + k_1 \equiv 0 \mod m/n, \quad b_1x_1 + k_2 \equiv 0 \mod m/n, \tag{2.4}
\]

which implies that

\[
a_1k_2 - b_1k_1 \equiv 0 \mod m/n. \tag{2.5}
\]

Therefore, if \( x \) is a solution of (2.1), then \((x_2, \ldots, x_d)\) satisfies equation (2.5). We now count the number of solutions of this equation. Note that equation (2.5) can
be written as
\[(a_1 b_2 - a_2 b_1)x_2 + \cdots + (a_1 b_d - a_d b_1)x_d \equiv 0 \mod m/n. \tag{2.6}\]

Let \(h\) be the greatest common divisor of \(a_1 b_2 - a_2 b_1, \ldots, a_1 b_d - a_d b_1,\) and \(m/n.\) Note that, it is equivalent to \(a_n \equiv tb_1 \mod h\) for some \(t \in \mathbb{Z}_h^n.\) Set \(t_i = (a_1 b_i - a_i b_1)/h.\) Then equation (2.6) becomes
\[h(t_2 x_2 + \ldots t_d x_d) \equiv 0 \mod m/n. \tag{2.7}\]

By the way of choosing \(h,\) there exists an index \(t_i \in \mathbb{Z}^0_{m/n}.\) We can assume that \(t_i \in \mathbb{Z}^0_{m/n}.\) For any choice of \(x_3, \ldots, x_d \in \mathbb{Z}_m\) where not all \(x_j\) are non-units, equation (2.7) determines \(x_2\) uniquely. (Note that, if \(x_3, \ldots, x_d \in \mathbb{Z}^0_m,\) then we have \(x_2 \in \mathbb{Z}^0_m.\)) Hence, equation (2.7) has
\[(m/n)^{d-1} - (m/n - \phi(m/n))^{d-1}\]
solutions if \(h = m/n\) and
\[( (m/n)^{d-2} - (m/n - \phi(m/n))^{d-2})h\]
solutions otherwise.

For each solution \((x_2, \ldots, x_d,\) since \(a_1 \in \mathbb{Z}^\times_m,\) we have an uniquely choice of \(x_1.\) Given a solution \(x_n\) of (2.3), putting back into the system
\[a \cdot x \equiv 0 \mod m, \quad x \equiv x_n \mod m/n, \tag{2.8}\]
gives us \(n^{d-1}\) solutions of system (2.2). Therefore, for any \(n \mid m\) and \(h \mid (m/n),\) set
\[v_{n,h} = \begin{cases} ((m/n)^{d-1} - (m/n - \phi(m/n))^{d-1})n^{d-1} & \text{if } h = m/n, \\ ((m/n)^{d-2} - (m/n - \phi(m/n))^{d-2})hn^{d-1} & \text{if } h < m/n, \end{cases}\]
then the system (2.1) has \(v_{n,h}\) solutions.

For any \(n, h\) with \(n \mid m\) and \(h \mid (m/n),\) let \(B_{E_{n,h}}\) be a graph with the vertex set \(V(B_{E_{n,h}}) = V(\mathbb{Z}P_{m,d}).\) For any two vertices \(a, b \in \mathbb{Z}_m^d \setminus (\mathbb{Z}_m^0)^d, (a, b)\) is an edge of \(B_{E_{n,h}},\) if and only if \(b = a + nb_1\) for some \(b_1 \in (\mathbb{Z}_m/m)^d \setminus (\mathbb{Z}_m^0/m)^d,\) and let \(a_n \in (\mathbb{Z}_m/m)^d \setminus (\mathbb{Z}_m^0/m)^d = a \mod m/n,\) then we have \(a_n \equiv tb_1 \mod h\) for some \(t \in \mathbb{Z}_h^n.\) It is easy to see that \(B_{E_{n,h}}\) is a regular graph of valency
\[\phi(h)\left(\left(\frac{m}{nh}\right)^d - \left(m - \phi\left(\frac{m}{nh}\right)\right)^d\right) < \phi(h)\left(\frac{m}{nh}\right)^d.\]

Let \(E_{n,h}\) be the adjacency matrix of \(B_{E_{n,h}},\) then absolute values of eigenvalues of \(E_{n,h}\) are bounded by \(\phi(h)(\frac{m}{nh})^d.\)
Let $A$ be the adjacency matrix of $\mathbb{Z}_P^{m,d}$. It follows that

$$A^2 = (m^{d-1} - (m - \phi(m))^{d-1}I + \sum_{\substack{n|m \\
h|m/n}} v_{n,h}E_{n,h}$$

$$= (m^{d-1} - (m - \phi(m))^{d-1} - v_{1,1})I + v_{1,1}J$$

$$+ \sum_{\substack{n|m \\
h|m/n}} (v_{n,h} - v_{1,1})E_{n,h}, \quad (2.9)$$

where $I$ is the identity matrix and $J$ is the all-one matrix.

As $\mathbb{Z}_P^{m,d}$ is an $m^{d-1} - (m - \phi(m))^{d-1}$-regular graph, $m^{d-1} - (m - \phi(m))^{d-1}$ is an eigenvalue of $A$ with the all-one eigenvector $\mathbf{1}$. The graph $\mathbb{Z}_P^{m,d}$ is connected therefore the eigenvalue $m^{d-1} - (m - \phi(m))^{d-1}$ has multiplicity one. Since the graph $\mathbb{Z}_P^{m,d}$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue $\theta$ then $|\theta| < m^{d-1} - (m - \phi(m))^{d-1}$. Let $v_{\theta}$ denote the corresponding eigenvector of $\theta$. Note that $v_{\theta} \in \mathbf{1}^\perp$, so $Jv_{\theta} = 0$. It follows from (2.9) that

$$(\theta^2 - m^{d-1} + (m - \phi(m))^{d-1} + v_{1,1})v_{\theta} = \left( \sum_{\substack{n|m \\
h|m/n}} (v_{n,h} - v_{1,1})E_{n,h} \right)v_{\theta}.$$ 

Hence, $v_{\theta}$ is also an eigenvalue of

$$\sum_{\substack{n|m \\
h|m/n}} (v_{n,h} - v_{1,1})E_{n,h}.$$ 

Since eigenvalues of sum of matrices are bounded by sum of largest eigenvalues of the summands, we have

$$\theta^2 \leq m^{d-1} - (m - \phi(m))^{d-1} - v_{1,1} + \sum_{\substack{n|m \\
1<n<m \\
h=1}} (v_{n,1} - v_{1,1})\phi(1) \left( \frac{m}{n} \right)^d$$

$$+ \sum_{\substack{n|m \\
1<n<m \\
h=m/n}} (v_{n,m/n} - v_{1,1})\phi \left( \frac{m}{n} \right)$$

$$+ \sum_{\substack{n|m \\
1\leq n<m \\
2\leq h<m/n}} (v_{n,h} - v_{1,1})\phi(h) \left( \frac{m}{nh} \right)^d. \quad (2.10)$$
Next, we estimate each term of (2.10). We have

\[
\sum_{\substack{n|m \\
1<n<m \\
h=1}} (v_{n,1} - v_{1,1}) \phi(1) \left( \frac{m}{n} \right)^d \leq \sum_{\substack{n|m \\
1<n<m \\
h=1}} (m/n)^{d-2} n^{d-1} \left( \frac{m}{n} \right)^d < \tau(m) \frac{m^{2d-2}}{\gamma(m)^{d-1}} \tag{2.11}
\]

\[
\sum_{\substack{n|m \\
1\leq n<m \\
h=m/n}} (v_{n,m/n} - v_{1,1}) \phi \left( \frac{m}{n} \right)^d \leq \sum_{\substack{n|m \\
1\leq n<m \\
h=m/n}} \left( \frac{m}{n} \right)^{d-1} n^{d-1} \phi \left( \frac{m}{n} \right) < \tau(m) m^d \tag{2.12}
\]

\[
\sum_{\substack{n|m \\
1\leq n<m \\
2\leq h<m/n}} (v_{n,h} - v_{1,1}) \phi(h) \left( \frac{m}{nh} \right)^d \leq \sum_{\substack{n|m \\
1\leq n<m \\
2\leq h<m/n}} (m/n)^{d-2} n^{d-1} h \phi(h) \left( \frac{m}{nh} \right)^d < (\tau(m))^2 \frac{m^{2d-2}}{n^{d-1} h^{d-2}} \leq (\tau(m))^2 \frac{m^{2d-2}}{\gamma(m)^{d-2}}. \tag{2.13}
\]

Putting (2.10), (2.11), (2.12), and (2.13) together, the theorem follows. □

### 2.3 Erdős–Rényi graph

In this subsection, we study a variant of the Erdős–Rényi graph over the ring \( \mathbb{Z}_m \). For any \( x \in \mathbb{Z}_m^d \setminus (\mathbb{Z}_m^0)^d \), denote by \([x]\) the equivalence class of \( x \) in \( \mathbb{Z}_m^d \setminus (\mathbb{Z}_m^0)^d \), where \( x, y \in \mathbb{Z}_m^d \setminus (\mathbb{Z}_m^0)^d \) are equivalent if and only if \( x = ty \) for some \( t \in \mathbb{Z}_m^x \). Let \( \mathcal{E}R_{m,d} \) denote the Erdős–Rényi graph whose vertices are the points of the projective space over \( \mathbb{Z}_m \), where two vertices \([x]\) and \([y]\) are connected if and only if \( x \cdot y = 0 \). One can follow exactly the proof of Theorem 2.3 above to obtain the following result.

**Theorem 2.4.** For any \( m, d \geq 2 \), the Erdős–Rényi graph \( \mathcal{E}P_{m,d} \) is an

\[
\left( \frac{m^d - (m - \phi(m))^d}{\phi(m)}, \frac{m^d - (m - \phi(m))^d}{\phi(m)}, \frac{2\tau(m)m^{d-1}}{\phi(m)\gamma(m)(d-2)/2} \right)-graph.
\]

Alternatively, the product-graph can be obtained from the Erdős–Rényi graph by blowing it up (which means replacing each vertex by an independent set of size
\( \phi(m) \) and connecting two vertices in the new graph if and only if the corresponding vertices of the Erdős–Rényi graph are connected by an edge. The bound in Theorem 2.4 now can be derived from Theorem 2.3 by using well-known results on the eigenvalues of the tensor product of two matrices (see [10] for more details).

3 A Szemerédi–Trotter type theorem over rings

We give a proof of Theorem 1.7 in this section. We can embed the space \( \mathbb{Z}_m^2 \) into \( P\mathbb{Z}_m^3 \) by identifying \((x_1, x_2)\) with the equivalence class of \((x_1, x_2, 1)\). Any line in \( \mathbb{Z}_m^2 \) also can be represented uniquely as an equivalence class in \( P\mathbb{Z}_m^3 \) of some element \( h \in \mathbb{Z}_m^3 \setminus (\mathbb{Z}_m^3)^3 \).

Let \( \mathcal{B} \) be the set of vertices of the Erdős–Rényi graph \( \mathcal{E} \mathcal{R}_{m,3} \) that represents the collection \( \mathcal{P} \) of points in \( \mathbb{Z}_m^2 \) and \( \mathcal{C} \) be the set of vertices of \( \mathcal{E} \mathcal{R}_{m,3} \) that represents the collection \( \mathcal{L} \) of lines in \( \mathbb{Z}_m^2 \). It follows from Corollary 2.2 and Theorem 2.4 that

\[
|\{(p, h) \in \mathcal{P} \times \mathcal{L} : p \in h\}| = e_{\mathcal{E} \mathcal{R}_{m,3}}(\mathcal{B}, \mathcal{C}) \leq \frac{|\mathcal{B}||\mathcal{C}|}{m} + \frac{2\tau(m)m^2}{\phi(m)\gamma(m)^{1/2}} \sqrt{|\mathcal{B}||\mathcal{C}|} = \frac{|\mathcal{P}||\mathcal{L}|}{m} + \frac{2\tau(m)m^2}{\phi(m)\gamma(m)^{1/2}} \sqrt{|\mathcal{P}||\mathcal{L}|}.
\]

This concludes the proof of Theorem 1.7.

We also have an analog of Theorem 1.7 in higher dimension.

**Theorem 3.1.** Let \( \mathcal{P} \) be a collection of points in \( \mathbb{Z}_m^d \) and \( \mathcal{H} \) be a collection of hyperplanes in \( \mathbb{Z}_m^d \) with \( d \geq 2 \). Then we have

\[
|\{(p, h) \in \mathcal{P} \times \mathcal{H} : p \in h\}| \leq \frac{|\mathcal{P}||\mathcal{L}|}{m} + \frac{2\tau(m)m^{d-1}}{\phi(m)\gamma(m)^{(d-2)/2}} \sqrt{|\mathcal{P}||\mathcal{L}|}. \tag{3.1}
\]

The proof of this theorem is similar to the proof of Theorem 1.7.

4 A sum-product estimate for large sets over rings

Elekes ([4]) observed that there is a connection between the incidence problem and the sum-product problem. The statement and the proof here follow the presentation in [3].

**Lemma 4.1** ([4]). Let \( \mathcal{A} \) be a subset of \( \mathbb{Z}_m^2 \). Then there is a collection of points \( \mathcal{P} \) and lines \( \mathcal{L} \) with \( |\mathcal{P}| = |\mathcal{A} + \mathcal{A}| \) and \( |\mathcal{L}| = |\mathcal{A}|^2 \) which has at least \( |\mathcal{A}|^3 \) incidences.
Proof. Take $\mathcal{P} = (\mathcal{A} + \mathcal{A}) \times (\mathcal{A} \cdot \mathcal{A})$, and let $\mathcal{L}$ be the collection of all lines of form $l(a, b) := \{(x, y) : y = b(x-a)\}$ where $a, b \in \mathcal{A}$. The claim follows since $(a + c, bc) \in \mathcal{P}$ is incident to $l(a, b)$ whenever $a, b, c \in \mathcal{A}$.

Theorem 1.9 follows from Theorem 1.7 and Lemma 4.1. Let $\mathcal{P}$ and $\mathcal{L}$ be collections of points and lines as in the proof of Lemma 4.1. Then from Theorem 1.7, we have

$$|\mathcal{A}|^3 \leq \frac{uv|\mathcal{A}|^2}{m} + \frac{2\tau(m)m^2}{\phi(m)\gamma(m)^{1/2}}|\mathcal{A}|\sqrt{uv}.$$ 

This implies that

$$|\mathcal{A}|^2 \leq \frac{uv|\mathcal{A}|}{m} + \frac{2\tau(m)m^2}{\phi(m)\gamma(m)^{1/2}}\sqrt{uv}. \quad (4.1)$$

Let $x = \max(|\mathcal{A} + \mathcal{A}|, |\mathcal{A} \cdot \mathcal{A}|)$, we have

$$|\mathcal{A}|x^2 + \frac{2\tau(m)m^3}{\phi(m)\gamma(m)^{1/2}}x - m|\mathcal{A}|^2 \geq 0.$$ 

Solving this inequality gives us the desired lower bound for $x$, concluding the proof of Theorem 1.9.

Bibliography


Received December 30, 2011; revised May 16, 2012.

**Author information**

Pham Van Thang, Faculty of Mathematics, Mechanics and Informatics, Hanoi University of Science, Vietnam National University, Hanoi, Vietnam.  
E-mail: phmanhthang@gmail.com

E-mail: vinhla@vnu.edu.vn