Sum and shifted-product subsets of product-sets over finite rings

Le Anh Vinh

University of Education
Vietnam National University, Hanoi

vinhla@vnu.edu.vn

Submitted: Jan 6, 2012; Accepted: May 25, 2012; Published: Jun 6, 2012
Mathematics Subject Classification: 05C35, 05C38

Abstract

For sufficiently large subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ of $\mathbb{F}_q$, Gyarmati and Sárközy (2008) showed the solvability of the equations $a+b = cd$ and $ab+1 = cd$ with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$. They asked whether one can extend these results to every $k \in \mathbb{N}$ in the following way: for large subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ of $\mathbb{F}_q$, there are $a_1, \dots, a_k, a'_1, \dots, a'_k \in \mathcal{A}$, $b_1, \dots, b_k, b'_1, \dots, b'_k \in \mathcal{B}$ with $a_i + b_j, a'_i b'_j + 1 \in \mathcal{CD}$ (for $1 \leqslant i, j \leqslant k$). The author (2010) gave an affirmative answer to this question using Fourier analytic methods. In this paper, we will extend this result to the setting of finite cyclic rings using tools from spectral graph theory.

1 Introduction

In [6] and [7], Sárközy proved that if $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ are "large" subsets of $\mathbb{Z}_p$, more precisely, $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg p^3$, then the equation

$$ab + 1 = cd, \tag{1.1}$$

resp.

$$a + b = cd, \tag{1.2}$$

can be solved with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$ and $d \in \mathcal{D}$. Here, and throughout, $X \gg Y$ means that there exists $C > 0$ such that $X \geqslant CY$. Gyarmati and Sárközy [4] generalized the results on the solvability of equation (1.2) to arbitrarily finite fields $\mathbb{F}_q$, where q be a large odd prime power. Hegyvári [5] and Shparlinski [8] also studied these problems in the imbalanced cases. Furthermore, Garaev [2, 3] considered the equations (1.2) and (1.1) over some special sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ to obtain new results on the sum-product problem in finite fields. The author reproved these results using graph theory methods in [10].

At the end of [4], Gyarmati and Sárközy proposed some open problems related to the above equations. They asked whether one can extend the solvability of the equations (1.2) and (1.1) in the following way: for every $k \in \mathbb{N}$, there are $c = c(k) > 0$ and $q_0 = q_0(k)$ such that if $q > q_0$, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q$, $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > q^{4-c}$ then there are $a_1, \dots, a_k, a'_1, \dots, a'_k \in \mathcal{A}$, $b_1, \dots, b_k, b'_1, \dots, b'_k \in \mathcal{B}$ with $a_i + b_j$, $a'_i b'_j + 1 \in \mathcal{CD}$ for $1 \leqslant i, j \leqslant k$. In [11], the author gave an affirmative answer to this question. More precisely, the author proved the following results.

Theorem 1.1 *([11]) For every $k \in \mathbb{N}$. If $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg q^{4-\frac{1}{2(k+1)}}$, then there are $a_1, \dots, a_k \in \mathcal{A}$, $b_1, \dots, b_k \in \mathcal{B}$ with $a_i + b_j \in \mathcal{CD}$ for $1 \leqslant i, j \leqslant k$.*

Theorem 1.2 *([11]) For every $k \in \mathbb{N}$. If $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg q^{4-\frac{1}{2(k+1)}}$, then there are $a_1, \dots, a_k \in \mathcal{A}$, $b_1, \dots, b_k \in \mathcal{B}$ with $a_i b_j + 1 \in \mathcal{CD}$ for $1 \leqslant i, j \leqslant k$.*

Let p be a large prime and $r \geqslant 2$. Let $\mathbb{Z}_{p^r}$ be the ring of residues mod p^r. We identify $\mathbb{Z}_{p^r}$ with $\{0, 1, \dots, p^r - 1\}$. Define the set of units and the set of nonunits in $\mathbb{Z}_{p^r}$ by $\mathbb{Z}_{p^r}^\times$ and $\mathbb{Z}_{p^r}^0$ respectively. It is natural to extend these results to the setting of finite cyclic rings. Our main results of this paper are the following theorems.

Theorem 1.3 *For every $k \in \mathbb{N}$. If $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_{p^r}$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg p^{4r-\frac{1}{2(k+1)}}$, then there are $a_1, \dots, a_k \in \mathcal{A}$, $b_1, \dots, b_k \in \mathcal{B}$ with $a_i + b_j \in \mathcal{CD}$ for $1 \leqslant i, j \leqslant k$.*

Theorem 1.4 *For every $k \in \mathbb{N}$. If $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_{p^r}$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg p^{4r-\frac{1}{2(k+1)}}$, then there are $a_1, \dots, a_k \in \mathcal{A}$, $b_1, \dots, b_k \in \mathcal{B}$ with $a_i b_j + 1 \in \mathcal{CD}$ for $1 \leqslant i, j \leqslant k$.*

The rest of this paper is organized as follows. In Section 2 we study spectrums of product graphs and sum-product graphs over finite rings. Proofs of Theorem 1.3 and Theorem 1.4 are given in Section 3 and Section 4, respectively.

2 Product graphs and sum-product graphs

For a graph G, let $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$ 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 first recall the following two well-known facts (see, for example, [1]).

Theorem 2.1 *([1, Theorem 9.2.4]) Let $G = (V, E)$ be an (n, d, λ)-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 *([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*

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

2.1 Sum-product graphs over rings

Suppose that $q = p^r$ for some odd prime p and $r \geqslant 2$. The sum-product graph SP_q is defined as follows. The vertex set of the sum-product graph $\mathcal{SP}_q$ is the set $V(\mathcal{SP}_q) = \mathbb{Z}_q \times \mathbb{Z}_q$. Two vertices (a, b) and $(c, d) \in V(\mathcal{SP}_q)$ are connected by an edge in $E(\mathcal{SP}_q)$, if and only if $a + c = bd$. Our construction is similar to that of Solymosi in [9] in the finite field setting.

Theorem 2.3 *The sum-product graph $\mathcal{SP}_q$ is a*

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

Proof It is easy to see that $\mathcal{SP}_q$ is a regular graph of order p^{2r} and valency p^r. We now compute the eigenvalues of this multigraph. For any $a, c \in \mathbb{Z}_{p^r}$, $b, d \in \mathbb{Z}_{p^r}$ and $b \neq d$, we count the number of solutions of the following system

$$a + u = bv, \ c + u = dv, \ \ u, v \in \mathbb{Z}_{p^r}. \tag{2.1}$$

For each solution v of

$$(b - d)v = a - c, \tag{2.2}$$

there exists a unique u satisfying the system (2.1). Therefore, we only need to count the number of solutions of (2.2).

Let $1 \leqslant \alpha \leqslant r - 1$ be the largest power such that $b - d$ is divisible by p^α. Suppose that $p^\alpha | (a - c)$. Let $\gamma = (a - c)/p^\alpha$ and $\beta = (b - d)/p^\alpha$. Since $\beta \in \mathbb{Z}^\times_{p^{r-\alpha}}$, there exists an unique solution $v \in \mathbb{Z}_{p^{r-\alpha}}$ of $\beta v = \gamma$. Putting back in to (2.2) gives us p^α solutions. Hence, (2.1) has p^α solutions if $p^\alpha | (a - c)$, and no solution otherwise.

Therefore, for any two vertices (a, b) and $(c, d) \in V(\mathcal{SP}_q)$, let $p^\alpha = \gcd(b - d, p^r)$, then (a, b) and (c, d) have p^α common neighbors if $p^\alpha \mid c - a$ and no common neighbors otherwise. Let A be the adjacency matrix of $\mathcal{SP}_q$. It follows that

$$A^2 = J + (p^r - 1)I - \sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha, \tag{2.3}$$

where J is the all-one matrix, I is the identity matrix, E_α is the adjacency matrix of the graph $B_{E,\alpha}$, where the vertex set of $B_{E,\alpha}$ is $\mathbb{Z}_q \times \mathbb{Z}_q$ and for any two vertices $U = (a, b)$ and $V = (c, d) \in V(B_{E,\alpha})$, (U, V) is an edge of $B_{E,\alpha}$ if and only if $p^\alpha = \gcd(b - d, p^r) > \gcd(a - c, p^r)$; and F_α is the adjacency matrix of the graph $B_{F,\alpha}$, where the vertex set of $B_{F,\alpha}$ is $\mathbb{Z}_q \times \mathbb{Z}_q$ and for any two vertices $U = (a, b)$ and $V = (c, d) \in V(B_{F,\alpha})$, (U, V) is an edge of $B_{F,\alpha}$ if and only if $p^\alpha = \gcd(b - d, p^r) \leqslant \gcd(a - c, p^r)$. For any $\alpha > 0$ then $B_{E,\alpha}$ is a regular graph of order less than $p^{2r-\alpha}$ and $B_{F,\alpha}$ is a regular graph of order less than $p^{2(r-\alpha)}$. Hence, all eigenvalues of E_α are at most $p^{2r-\alpha}$, and all eigenvalues of F_α are at most $p^{2(r-\alpha)}$. Note that E_0 is a zero matrix.

Since $\mathcal{SP}_q$ is a p^r-regular graph, p^r is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{SP}_q$ is connected; therefore, the eigenvalue p^r has multiplicity one. Since the graph $\mathcal{SP}_q$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ then $|\theta| < p^r$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of θ. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It follows from (2.3) that

$$(\theta^2 - p^r + 1)\boldsymbol{v}_\theta = \left(-\sum_{\alpha=1}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha \right) \boldsymbol{v}_\theta.$$

Hence, $\boldsymbol{v}_\theta$ is also an eigenvalue of

$$\sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha - \sum_{\alpha=1}^{r-1} E_\alpha.$$

Since eigenvalues of the sum of matrices are bounded by sum of the largest eigenvalues of summands. We have

$$\begin{aligned} \theta^2 &\leqslant p^r - 1 + \sum_{\alpha=1}^{r-1} p^{2r-\alpha} + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)p^{2(r-\alpha)} \\ &< 2rp^{2r-1}. \end{aligned}$$

The lemma follows. □

2.2 Product graphs over rings

Suppose that $q = p^r$ for some odd prime p and $r \geqslant 2$. We identify $\mathbb{Z}_q$ with $\{0, 1, \ldots, q-1\}$, then $p\mathbb{Z}_{p^{r-1}}$ is the set of nonunits in $\mathbb{Z}_q$. The product graph $\mathcal{PG}_q$ is defined as follows. The vertex set of the product graph $\mathcal{PG}_q$ is the set $V(\mathcal{PG}_q) = \mathbb{Z}_{p^r}^2 \setminus (p\mathbb{Z}_{p^{r-1}})^2$. Two vertices $\boldsymbol{a} = (a_1, a_2), \boldsymbol{b} = (b_1, b_2) \in V(\mathcal{PG}_q)$ are connected by an edge $(\boldsymbol{a}, \boldsymbol{b}) \in E(\mathcal{PG}_q)$, if and only if $\boldsymbol{a} \cdot \boldsymbol{b} = a_1b_1 + a_2b_2 = 1$.

Theorem 2.4 *The product graph $\mathcal{PG}_q$ is an*

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

Proof It follows from the definition of the product graph that $\mathcal{PG}_q$ is a graph of order $p^{2r} - p^{2(r-1)}$. The valency of the graph is also easy to compute. Given a vertex $\boldsymbol{x} = (x_1, x_2) \in V(\mathcal{PG}_q)$, there exists an index $x_i \in \mathbb{Z}_q^\times$. We can assume that $x_1 \in \mathbb{Z}_q^\times$. Then we can choose $y_2 \in \mathbb{Z}_q$ arbitrarily, and y_1 is determined uniquely such that $x_1y_1 + x_2y_2 = 1$. Hence, $\mathcal{PG}_q$ is a regular graph of valency p^r. It remains to estimate the eigenvalues of this multigraph (i.e. graph with loops). For any $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_{p^r}^2 \backslash (p\mathbb{Z}_{p^{r-1}})^2$ and $\boldsymbol{a} \neq \boldsymbol{b}$, we count the number of solutions of the following system

$$\boldsymbol{a} \cdot \boldsymbol{x} = \boldsymbol{b} \cdot \boldsymbol{x} = 1,\ \boldsymbol{x} \in \mathbb{Z}_{p^r}^2 \backslash (p\mathbb{Z}_{p^{r-1}})^2. \tag{2.4}$$

There exist uniquely $0 \leqslant \alpha \leqslant r-1$ and $\boldsymbol{b}_1 \in (\mathbb{Z}_{p^{r-\alpha}})^2 \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^2$ such that $\boldsymbol{b} = \boldsymbol{a} + p^\alpha \boldsymbol{b}_1$. The system (2.4) above becomes

$$\boldsymbol{a} \cdot \boldsymbol{x} = 1,\ p^\alpha \boldsymbol{b}_1 \cdot \boldsymbol{x} = \boldsymbol{0},\ \boldsymbol{x} \in \mathbb{Z}_{p^r}^2 \backslash (p\mathbb{Z}_{p^{r-1}})^2. \tag{2.5}$$

Let $\boldsymbol{a}_\alpha \in \mathbb{Z}_{p^{r-\alpha}}^2 \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^2 \equiv \boldsymbol{a} \mod p^{r-\alpha}$, $\boldsymbol{x}_\alpha \in \mathbb{Z}_{p^{r-\alpha}}^2 \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^2 \equiv \boldsymbol{x} \mod p^{r-\alpha}$. To solve (2.5), we first solve the following system

$$\boldsymbol{a}_\alpha \cdot \boldsymbol{x}_\alpha = 1,\ \boldsymbol{b}_1 \cdot \boldsymbol{x}_\alpha = \boldsymbol{0},\ \boldsymbol{x}_\alpha \in \mathbb{Z}_{p^{r-\alpha}}^2 \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^2. \tag{2.6}$$

The system (2.6) has an unique solution when $\boldsymbol{a}_\alpha \not\equiv t\boldsymbol{b}_1 \mod p$ for some $t \in \mathbb{Z}_p^\times$ and no solution otherwise. For each solution $\boldsymbol{x}_\alpha$ of (2.6), putting back into the system

$$\boldsymbol{a} \cdot \boldsymbol{x} = \lambda,\ \boldsymbol{x} \equiv \boldsymbol{x}_\alpha \mod p^{r-\alpha}, \tag{2.7}$$

gives us p^α solutions of the system (2.5). Hence, the system (2.5) has p^α solutions when $\boldsymbol{a}_\alpha \not\equiv t\boldsymbol{b}_1 \mod p$, and no solution otherwise. Let A be the adjacency matrix of $\mathcal{PG}_q$, it follows that

$$A^2 = J + (p^r - 1)I - \sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha, \tag{2.8}$$

where J is the all-one matrix; I is the identity matrix; E_α is the adjacency matrix of the graph $B_{E,\alpha}$, where the vertex set of $B_{E,\alpha}$ is $\mathbb{Z}_{p^r}^2 \backslash (p\mathbb{Z}_{p^{r-1}})^2$, and for any two vertices $\boldsymbol{a}, \boldsymbol{b} \in V(B_{E,\alpha})$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{E,\alpha}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + p^\alpha \boldsymbol{b}_1$, $\boldsymbol{b}_1 \in (\mathbb{Z}_{p^{r-\alpha}})^2 \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^2$ and $\boldsymbol{a}_\alpha \equiv t\boldsymbol{b}_1 \mod p$; and F_α is the adjacency matrix of the graph $B_{F,\alpha}$, where where the vertex set of $B_{F,\alpha}$ is $\mathbb{Z}_{p^r}^2 \backslash (p\mathbb{Z}_{p^{r-1}})^2$, for any two vertices $\boldsymbol{a}, \boldsymbol{b} \in V(B_{F,\alpha})$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{F,\alpha}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + p^\alpha \boldsymbol{b}_1$, $\boldsymbol{b}_1 \in (\mathbb{Z}_{p^{r-\alpha}})^2 \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^2$ and $\boldsymbol{a}_\alpha \not\equiv t\boldsymbol{b}_1 \mod p$. Therefore, $B_{E,\alpha}$ is a regular graph of valency $(p-1)p^{2(r-\alpha-1)}$ and all eigenvalues of E_α are at most $(p-1)p^{2(r-\alpha-1)}$. It also implies that all eigenvalues of F_α are at most $p^{2(r-\alpha)}$.

Since $\mathcal{PG}_q$ is a p^r-regular graph, p^r is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{PG}_q$ is connected; therefore, the eigenvalue p^r has multiplicity one. Since the graph $\mathcal{PG}_q$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ, $|\theta| < p^r$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of θ. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It follows from (2.8) that

$$(\theta^2 - p^r + 1)\boldsymbol{v}_\theta = \left(\sum_{\alpha=0}^{r-1} E_\alpha - \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha \right) \boldsymbol{v}_\theta.$$

Hence, $\boldsymbol{v}_\theta$ is also an eigenvalue of $\sum_{\alpha=0}^{r-1} E_\alpha - \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha$. Since eigenvalue of sum of matrices is bounded by the sum of largest eigenvalues of summands. We have

$$\begin{aligned}\theta^2 &\leqslant p^r - 1 + \sum_{\alpha=0}^{r-1}(p-1)p^{2(r-\alpha-1)} + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)p^{2(r-\alpha)} \\ &< p^r + rp^{2(r-1)+1} + (r-1)p^{2(r-1)+1} \\ &< 2rp^{2r-1}.\end{aligned}$$

The lemma follows. □

3 Pseudo-randomness of sum-product graphs - Proof of Theorem 1.3

Suppose that $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_{p^r}$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg p^{4r-c}$ for some $0 < c < \frac{1}{2(k+1)}$. It follows that $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}| \gg p^{r-c}$, and we can assume $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{Z}_{p^r}^\times$. Denote $N^{\mathcal{C},\mathcal{D}}(\mathcal{A}, \mathcal{B})$ be the set of pairs $(a, b) \in \mathcal{A} \times \mathcal{B}$ such that $a + b \in \mathcal{C}\mathcal{D}$. We first show that for any two large subsets $\mathcal{A}, \mathcal{B}$ of $\mathbb{F}_q$, there are many pairs $(a, b) \in \mathcal{A} \times \mathcal{B}$ with $a + b \in \mathcal{C}\mathcal{D}$. More precisely, we have the following lemma.

Lemma 3.1 *Suppose that $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{Z}_{p^r}^\times$. We have*

$$N^{\mathcal{C},\mathcal{D}}(\mathcal{A}, \mathcal{B}) \geqslant \frac{|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}| - \sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\sqrt{|\mathcal{A}||\mathcal{B}|}.$$

Proof For any $a \in \mathcal{A}$, $c \in \mathcal{C}$, denote $N^{c,\mathcal{D}}(a)$ be the set of all $b \in \mathbb{Z}_{p^r}$ such that $a+b \in c\mathcal{D}$, and let $N^{c,\mathcal{D}}(a, \mathcal{B}) = N^{c,\mathcal{D}}(a) \cap \mathcal{B}$. Applying Theorem 2.1 and Theorem 2.3 for the product graph $\mathcal{PG}_q$ and the set $\mathcal{B} \times \mathcal{D}$, we have

$$\sum_{(a,c)\in\mathbb{Z}_{p^r}^2} \left(\left|N^{c,\mathcal{D}}(a, \mathcal{B})\right| - \frac{|\mathcal{B}||\mathcal{D}|}{p^r}\right)^2 < 2rp^{2r-1}|\mathcal{B}||\mathcal{D}|.$$

This estimate says that the cardinalities of $N^{c,\mathcal{D}}(a, \mathcal{B})$'s are close to $\frac{|\mathcal{B}||\mathcal{D}|}{p^r}$ when $|\mathcal{B}|, |\mathcal{D}|$ are large.

By the pigeon-hole principle, there exists $c_0 \in \mathcal{C}$ such that

$$\sum_{a\in\mathcal{A}} \left(\left|N^{c_0,\mathcal{D}}(a, \mathcal{B})\right| - \frac{|\mathcal{B}||\mathcal{D}|}{p^r}\right)^2 \leqslant \frac{1}{|\mathcal{C}|}\sum_{a\in\mathcal{A},c\in\mathcal{C}} \left(\left|N^{c,\mathcal{D}}(a, \mathcal{B})\right| - \frac{|\mathcal{B}||\mathcal{D}|}{p^r}\right)^2 < \frac{2rp^{2r-1}|\mathcal{D}||\mathcal{B}|}{|\mathcal{C}|}.$$

By the Cauchy-Schwartz inequality,

$$\begin{aligned}\left|N^{c_0,\mathcal{D}}(\mathcal{A},\mathcal{B})-\frac{|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}|\right| &\leqslant \sum_{a\in\mathcal{A}}\left||N^{c_0,\mathcal{D}}(a,\mathcal{B})|-\frac{|\mathcal{B}||\mathcal{D}|}{p^r}\right| \\ &\leqslant \sqrt{|\mathcal{A}|}\sqrt{\sum_{a\in\mathcal{A}}\left(|N^{c_0,\mathcal{D}}(a,\mathcal{B})|-\frac{|\mathcal{B}||\mathcal{D}|}{p^r}\right)^2} \\ &\leqslant \sqrt{\frac{2rp^{2r-1}|\mathcal{D}}{|\mathcal{C}|}}\sqrt{|\mathcal{A}||\mathcal{B}|}.\end{aligned}$$

The lemma now follows from the fact that $N^{\mathcal{C},\mathcal{D}}(\mathcal{A},\mathcal{B})\geqslant N^{c_0,\mathcal{D}}(\mathcal{A},\mathcal{B})$. □

We also need the following key lemma.

Lemma 3.2 *Suppose that $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D}\subset\mathbb{Z}_{p^r}^{\times}$ with*

$$|\mathcal{A}|,|B|\gg\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\left(\frac{p^r}{|\mathcal{D}|}\right)^k.$$

Then there are $a_1,\ldots,a_k\in\mathcal{A}$, $b_1,\ldots,b_k\in\mathcal{B}$ such that $a_i+b_j\in\mathcal{C}\mathcal{D}$ for all $1\leqslant i,j\leqslant k$.

Proof The proof proceeds by induction on k. The base case $k=1$ follows immediately from Lemma 3.1. Suppose that the theorem hold for all $l<k$. From Lemma 3.1, we have

$$N^{\mathcal{C},\mathcal{D}}(\mathcal{A},\mathcal{B})\geqslant\frac{|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}|-\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\sqrt{|\mathcal{A}||\mathcal{B}|}=(1+o(1))\frac{|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}|.$$

By the pigeon-hole principle, there exists $a_1\in\mathcal{A}$ such that

$$N^{\mathcal{C},\mathcal{D}}(a_1,\mathcal{B})\geqslant(1+o(1))\frac{|\mathcal{D}|}{p^r}|\mathcal{B}|\gg\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\left(\frac{p^r}{|\mathcal{D}|}\right)^{k-1}. \tag{3.1}$$

Let $\mathcal{B}_1$ be the set of all $b\in\mathcal{B}$ such that $a_1+b\in\mathcal{C}\mathcal{D}$. From Lemma 3.1 again, we have

$$N^{\mathcal{C},\mathcal{D}}(\mathcal{A},\mathcal{B}_1)\geqslant\frac{|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}_1|-\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\sqrt{|\mathcal{A}||\mathcal{B}_1|}=(1+o(1))\frac{|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}_1|.$$

By the pigeon-hole principle, there exists $b_1\in\mathcal{B}_1$ such that

$$N^{\mathcal{C},\mathcal{D}}(\mathcal{A},b_1)\geqslant(1+o(1))\frac{|\mathcal{D}|}{p^r}|\mathcal{A}|\gg\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\left(\frac{p^r}{|\mathcal{D}|}\right)^{k-1}. \tag{3.2}$$

Let $\mathcal{A}_1$ be the set of all $a\in\mathcal{A}$ such that $a+b_1\in\mathcal{C}\mathcal{D}$. Set $\mathcal{A}^*=\mathcal{A}\backslash\{a_1\}$ and $\mathcal{B}^*=\mathcal{B}_1\backslash\{b_1\}$, it follows from (3.1) and (3.2) that

$$|\mathcal{A}^*|,|\mathcal{B}^*|\gg\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\left(\frac{p^r}{|\mathcal{D}|}\right)^{k-1}.$$

Thus, by the induction hypothesis, there are $a_2, \ldots, a_k \in \mathcal{A}^*$, $b_2, \ldots, b_k \in \mathcal{B}^*$ such that $a_i + b_j \in \mathcal{CD}$ for all $2 \leqslant i, j \leqslant k$. We also have $a_1 + b_i, a_j + b_1 \in \mathcal{CD}$ for all $i, j = 1, \ldots, k$. This completes the proof of the lemma. □

Let $c = c(k) < \frac{1}{2(k+1)}$ and $q \gg 1$, then $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}| \gg q^{1-c}$. It follows that

$$\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}} \left(\frac{p^r}{|\mathcal{D}|}\right)^k \ll p^{r-\frac{1}{2}+ck} \ll p^{r-c} \ll |\mathcal{A}|, |\mathcal{B}|. \tag{3.3}$$

Theorem 1.3 now follows immediately from Lemma 3.2.

4 Pseudo-randomness of product graphs - Proof of Theorem 1.4

Suppose that $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_{p^r}$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg p^{4r-c}$ for some $0 < c < \frac{1}{2(k+1)}$. It follows that $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}| \gg p^{r-c}$, and we can assume $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{Z}_{p^r}^\times$. Denote $T^{\mathcal{C},\mathcal{D}}(\mathcal{A}, \mathcal{B})$ be the set of pairs $(a, b) \in \mathcal{A} \times \mathcal{B}$ such that $ab + 1 \in \mathcal{CD}$. Similar to the previous section, we can show that for any two large subsets $\mathcal{A}, \mathcal{B}$ of $\mathbb{Z}_{p^r}^\times$, there are many pairs $(a, b) \in \mathcal{A} \times \mathcal{B}$ with $ab + 1 \in \mathcal{CD}$. More precisely, we have the following lemma.

Lemma 4.1 *For every subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{Z}_{p^r}^\times$, then*

$$T^{\mathcal{C},\mathcal{D}}(\mathcal{A}, \mathcal{B}) \geqslant \frac{(1 + o(1))|\mathcal{D}|}{p^r}|\mathcal{A}||\mathcal{B}| - \sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}}\sqrt{|\mathcal{A}||\mathcal{B}|}.$$

Similar to the proof of Lemma 3.2, using Lemma 4.1 instead of Lemma 3.1, we have the following result.

Lemma 4.2 *Suppose that $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D} \subset \mathbb{Z}_{p^r}^\times$ with*

$$|\mathcal{A}|, |B| \gg \sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}} \left(\frac{p^r}{|\mathcal{D}|}\right)^k.$$

Then there are $a_1, \ldots, a_k \in \mathcal{A}$, $b_1, \ldots, b_k \in \mathcal{B}$ such that $a_i b_j + 1 \in \mathcal{CD}$ for all $1 \leqslant i, j \leqslant k$.

Let $c < \frac{1}{2(k+1)}$ and $q \gg 1$, then $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}| \gg q^{1-c}$. It follows that

$$\sqrt{\frac{2rp^{2r-1}|\mathcal{D}|}{|\mathcal{C}|}} \left(\frac{p^r}{|\mathcal{D}|}\right)^k \ll p^{r-\frac{1}{2}+ck} \ll p^{r-c} \ll |\mathcal{A}|, |\mathcal{B}|. \tag{4.1}$$

Theorem 1.4 now follows from Lemma 4.2.

References

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

[2] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* **136** (2008), 2735–2739.

[3] M. Z. Garaev and V. Garcia, The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications, *Journal of Number Theory* **128**(9) (2008), 2520–2537.

[4] K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets, II (algebraic equations), *Acta Math. Hungar.* **119** (2008), 259–280.

[5] N. Hegyvári, Some remarks on multilinear exponential sums with an application, *Journal of Number Theory* **132** (2012), 94–102.

[6] A. Sárközy, On sums and products of residues modulo p, *Acta. Arith.* **118** (2005), 403–409.

[7] A. Sárközy, On products and shifted products of residues modulo p, *Integers: Electronic Journal of Combinatorial Number Theory*, **8**(2) (2008), A9.

[8] I. E. Shparlinski, On the solvability of bilinear equations in finite fields, *Glassgow Mathematical Journal* **50** (2008), 523–529.

[9] J. Solymosi, Incidences and the Spectra of Graphs, *Building Bridges between Mathematics and Computer Science.* Vol. **19**. Ed. Martin Groetschel and Gyula Katona. Series: Bolyai Society Mathematical Studies. Springer, 2008. 499–513.

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

[11] L. A. Vinh, On some problems of Gyarmati and Sárközy, *INTEGERS: The Electronic Journal of Combinatorial Number Theory*, to appear.