Pacific Journal of Mathematics

SPECTRA OF PRODUCT GRAPHS AND PERMANENTS OF MATRICES OVER FINITE RINGS

LE ANH VINH

Volume 267 No. 2 February 2014

PACIFIC JOURNAL OF MATHEMATICS
Vol. 267, No. 2, 2014
dx.doi.org/10.2140/pjm.2014.267.479

SPECTRA OF PRODUCT GRAPHS AND PERMANENTS OF MATRICES OVER FINITE RINGS

LE ANH VINH

We study the spectra of product graphs over the finite cyclic ring $\mathbb{Z}_m$. Using this spectra, we show that if $\mathscr{E}$ is a sufficiently large subset of $\mathbb{Z}_m^k$ then the set of permanents of $k \times k$ matrices with rows in $\mathscr{E}$ contains all nonunits of $\mathbb{Z}_m$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements where q is an odd prime power. The prime base field $\mathbb{F}_p$ of $\mathbb{F}_q$ may then be naturally identified with $\mathbb{Z}_p$. Let M be an $k \times k$ matrix. Two basic parameters of M are its determinant

$$\mathrm{Det}(M) := \sum_{\sigma \in S_k} \mathrm{sgn}(\sigma) \prod_{i=1}^{k} a_{i\sigma(i)},$$

and its permanent

$$\mathrm{Per}(M) := \sum_{\sigma \in S_k} \prod_{i=1}^{k} a_{i\sigma(i)}.$$

The distribution of the determinants of matrices with entries in a finite field $\mathbb{F}_q$ has been studied by various researchers. Suppose that the ground field $\mathbb{F}_q$ is fixed and $M = M_k$ is a random $k \times k$ matrix with entries chosen independently from $\mathbb{F}_q$. If the entries are chosen uniformly from $\mathbb{F}_q$, then it is well known that

$$\text{(1-1)} \qquad \Pr(M_k \text{ is nonsingular}) \to \prod_{i \geqslant 1} (1 - q^{-i}) \quad \text{as } k \to \infty.$$

It is interesting that (1-1) is quite robust. Specifically, J. Kahn and J. Komlós [2001] proved a strong necessary and sufficient condition for (1-1).

Theorem 1.1 [Kahn and Komlós 2001]. *Let M_k be a random $k \times k$ matrix with entries chosen according to some fixed nondegenerate probability distribution μ on*

This research is supported by Vietnam National University, Hanoi, under project QG.12.43, “Some problems on matrices over finite fields”.
MSC2010: 05C50.
Keywords: permanent, finite ring, expander graph.

$\mathbb{F}_q$. *Then* (1-1) *holds if and only if the support of* μ *is not contained in any proper affine subfield of* $\mathbb{F}_q$.

An extension of the uniform limit to random matrices with μ depending on k was considered by Kovalenko, Levitskaya, and Savchuk [1986]. They proved the standard limit (1-1) under the condition that the entries m_{ij} of M are independent and $\Pr(m_{ij} = \alpha) > (\log k + \alpha(1))/n$ for all $\alpha \in \mathbb{F}_q$. The behavior of the nullity of M_k for $1 - \mu(0)$ close to $\log k/k$ and $\mu(\alpha) = (1 - \mu(0))/(q - 1)$ for $\alpha \neq 0$ was also studied by Blömer, Karp, and Welzl [1997].

Another direction is to fix the dimension k of matrices and view the size of the finite field as an asymptotic parameter. Note that the implied constants in the symbols O, o, $\lesssim$, and $\ll$ may depend on the integer parameter k. We recall that the notations $U = O(V)$ and $U \lesssim V$ are equivalent to the assertion that the inequality $|U| \leq c|V|$ holds for some constant $c > 0$. The notations $U = o(V)$ and $U \ll V$ are equivalent to the assertion that for any $\epsilon > 0$, the inequality $|U| \leq \epsilon|V|$ holds when the variables of U and V are sufficiently large. For an integer k and a subset $\mathscr{E} \subseteq \mathbb{F}_q^k$, let $M_k(\mathscr{E})$ denote the set of $k \times k$ matrices with rows in $\mathscr{E}$. For any $t \in \mathbb{F}_q$, let $D_k(\mathscr{E}; t)$ be the number of $k \times k$ matrices in $M_k(\mathscr{E})$ having determinant t. Ahmadi and Shparlinski [2007] studied some natural classes of matrices over finite fields $\mathbb{F}_p$ of p elements with components in a given subinterval $[-H, H] \subseteq [-(p-1)/2, (p-1)/2]$. They showed that

$$D_k([-H, H]^k; t) = (1 + o(1))\frac{(2H+1)^{k^2}}{p}, \tag{1-2}$$

if $t \in \mathbb{F}_p^*$ and $H \gtrsim p^{3/4+\varepsilon}$ for any constant $\varepsilon > 0$. In the case $k = 2$, the lower bound of the size of the interval can be improved to $H \gtrsim p^{1/2}$.

Using the geometry incidence machinery developed in [Covert et al. 2010], and some properties of nonsingular matrices, the author [Vinh 2009] obtained the following result for higher-dimensional cases ($k \geq 4$):

$$D_k(\mathscr{A}^k; t) = (1 + o(1))\frac{|\mathscr{A}|^{k^2}}{q},$$

if $t \in \mathbb{F}_q^*$ and $\mathscr{A} \subseteq \mathbb{F}_q$ of cardinality $|\mathscr{A}| \gg q^{k/(2k-1)}$. Covert et al. [2010] studied this problem in a more general setting. A subset $\mathscr{E} \subseteq \mathbb{F}_q^k$ is called a product-like set if $|\mathscr{H}_l \cap \mathscr{E}| \lesssim |\mathscr{E}|^{l/k}$ for any l-dimensional subspace $\mathscr{H}_l \subset \mathbb{F}_q^k$. Covert et al. showed that

$$D_3(\mathscr{E}; t) = (1 + o(1))\frac{|\mathscr{E}|^3}{q},$$

if $t \in \mathbb{F}_q^*$ and $\mathscr{E} \subset \mathbb{F}_q^3$ is a product-like set of cardinality $|\mathscr{E}| \gg q^{15/8}$. In the singular case, the author [Vinh 2012b] showed that for any subset $\mathscr{E} \subseteq \mathbb{F}_q^k$ with $|\mathscr{E}| \gg q^{k-1+2/k}$ then the number of singular matrices whose rows are in $\mathscr{E}$ is close to the expected number $(1+o(1))|\mathscr{E}|^k/q$. In the general case, the author [Vinh 2013a] showed that if $\mathscr{E}$ is a subset of the k-dimensional vector space over a finite field $\mathbb{F}_q$ ($k \geq 3$) of cardinality $|\mathscr{E}| \geq (k-1)q^{k-1}$, then the set of volumes of k-dimensional parallelepipeds determined by $\mathscr{E}$ covers $\mathbb{F}_q$. This bound is sharp up to a factor of $(k-1)$ as taking $\mathscr{E}$ to be a $(k-1)$-hyperplane through the origin shows.

On the other hand, little is known about the permanent. The only known uniform limit similar to (1-1) for the permanent is due to Lyapkov and Sevast′yanov [Lyapkov and Sevast'yanov 1996]. They proved that the permanent of a random $k \times l$ matrix M_{kl} with elements from $\mathbb{F}_p$ and independent rows has the limit distribution of the form

$$\lim_{k\to\infty} \Pr(\operatorname{Per}(M_{kl}) = \lambda) = \rho_l \delta_{\lambda 0} + (1-\rho_l)/p, \quad \lambda \in \mathbb{F}_p,$$

where $\delta_{\lambda 0}$ is Kronecker's symbol. In [Vinh 2012a], the author studied the distribution of the permanent when the dimension of matrices is fixed. We are interested in the set of all permanents, $P_k(\mathscr{E}) = \{\operatorname{Per}(M) : M \in M_k(\mathscr{E})\}$. Using Fourier analytic methods, the author [Vinh 2012a] proved the following result.

Theorem 1.2 [Vinh 2012a]. *Suppose that q is an odd prime power and* $\gcd(q,k)=1$. *If $\mathscr{E} \cap (\mathbb{F}_q^*)^k \neq \varnothing$, and $|\mathscr{E}| \gtrsim q^{(k+1/2)}$, then $\mathbb{F}_q^* \subseteq P_k(\mathscr{E})$.*

Note that if $|\mathscr{E}| > nq^{n-1}$ then $\mathscr{E} \cap (\mathbb{F}_q^*)^k \neq \varnothing$. Hence we have an immediate corollary of Theorem 1.2.

Corollary 1.3 [Vinh 2012a]. *Suppose that q is an odd prime power and* $\gcd(q,n)=1$.

(a) *If $\mathscr{E} \subset \mathbb{F}_q^n$ of cardinality $|\mathscr{E}| > nq^{n-1}$, then $\mathbb{F}_q^* \subseteq P_n(\mathscr{E})$.*

(b) *If $\mathscr{A} \subset \mathbb{F}_q$ of cardinality $|\mathscr{A}| \gg q^{1/2+1/(2n)}$, then $\mathbb{F}_q^* \subseteq P_n(\mathscr{A}^n)$.*

The bound in the first part of Corollary 1.3 is tight up to a factor of n. For example, $|\{\boldsymbol{x} \in \mathbb{F}_q^n : x_1 = 0\}| = q^{n-1}$ and $P_n(\{\boldsymbol{x} \in \mathbb{F}_q^n : x_1 = 0\}) = 0$. However, we conjecture that the bound in the second part of Corollary 1.3 can be further improved to $|\mathscr{A}| \gg q^{1/2+\epsilon}$ (for any $\epsilon > 0$) when n is sufficiently large.

Let m be a large nonprime integer and $\mathbb{Z}_m$ be the ring of residues modulo m. Let $\gamma(m)$ be the smallest prime divisor of m, $\omega(m)$ the number of prime divisors of m, and $\tau(m)$ the number of divisors of m. We identify $\mathbb{Z}_m$ with $\{0, 1, \ldots, m-1\}$. 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 $\mathbb{Z}_m^k$ consists of column vectors $\boldsymbol{x}$, with j-th entries $x_j \in \mathbb{Z}_m$. The main purpose of this paper is to extend Theorem 1.2 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 in the setting of rational points, one can ask questions for such sets and see how they compare to the answers in $\mathbb{R}^k$. By scale invariance of these questions, the problem for a subset $\mathscr{E}$ of $\mathbb{Q}^k$ would be the same as for subsets of $\mathbb{Z}_m^k$. More precisely, we have the following analog of Theorem 1.2 over the finite cyclic rings.

Theorem 1.4. *Suppose that m is a large integer and $\gcd(m, k) = 1$. If $\mathscr{E} \cap (\mathbb{Z}_m^\times)^k \neq \varnothing$, and*

$$|\mathscr{E}| \gtrsim \frac{\tau(m)m^k}{\gamma(m)^{(k-1)/2}},$$

then $\mathbb{Z}_m^\times \subseteq P_k(\mathscr{E})$.

Notice that if $|\mathscr{E}| > k(m - \phi(m))m^{k-1}$ then $\mathscr{E} \cap (\mathbb{Z}_m^\times)^k \neq \varnothing$. Hence, we have an immediate corollary of Theorem 1.4.

Corollary 1.5. *Suppose that m is a large integer and $\gcd(m, k) = 1$.*

(a) *Suppose that*

$$(m - \phi(m))\gamma(m)^{(k-1)/2} \gtrsim \tau(m)m$$

and

$$|\mathscr{E}| \gtrsim (m - \phi(m))m^{k-1},$$

then $\mathbb{Z}_m^\times \subseteq P_k(\mathscr{E})$.

(b) *Suppose that $\mathscr{A} \subset \mathbb{Z}_m$ of cardinality*

$$|\mathscr{A}| \gtrsim \frac{\tau(m)m}{\gamma(m)^{(k-1/2k)}},$$

then $\mathbb{Z}_m^\times \subseteq P_k(\mathscr{A}^k)$.

Note that the bound in Corollary 1.5 is sharp. For example, if $\mathscr{E} = \mathbb{Z}_m^0 \times \mathbb{Z}_m^{k-1}$ then $P_k(\mathscr{E}) \subset \mathbb{Z}_m^0$. Theorem 1.4 and Corollary 1.5 are most effective when m has only a few prime divisors. For example, if $m = p^r$, we have the following result.

Theorem 1.6. *Suppose that p^r is a large prime power and $\gcd(p, k) = 1$. If $\mathscr{E} \cap (\mathbb{Z}_{p^r}^\times)^k \neq \varnothing$, and*

$$|\mathscr{E}| \gtrsim (r + 1)p^{rk-(k-1/2)},$$

then $\mathbb{Z}_{p^r}^\times \subseteq P_k(\mathscr{E})$.

In particular, suppose that $k \geq 3$, $p \gg r$, and $|\mathscr{E}| \gtrsim p^{kr-1}$, then $\mathbb{Z}_{p^r}^\times \subset P_k(\mathscr{E})$. The lower bound of $|\mathscr{E}|$ in this case is sharp, as taking $\mathscr{E}$ to be the set $\mathbb{Z}_{p^r}^0 \times \mathbb{Z}_{p^r}^{k-1}$ shows.

Note that, the bounds in Corollary 1.5 and Theorem 1.6 are sharp in general cases. When $\mathscr{E} = \mathscr{A}^n$ is a product set, we conjecture that these bounds can be further improved when n is sufficiently large.

For any $t \in \mathbb{F}_q$ and $\mathscr{E} \subset \mathbb{F}_q^k$, let $P_k(\mathscr{E}; t)$ be the number of $k \times k$ matrices with rows in $\mathscr{E}$ having permanent t. In [Vinh 2012a], the author studied the distribution of $P_n(\mathscr{E}; t)$ when $\mathscr{E} = \mathscr{A}^k$ for a large subset $\mathscr{A} \subset \mathbb{F}_q$. It would be of interest to extend these results to the setting of finite rings.

2. Product graphs over rings

For a graph G, 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, 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 [Ahmadi and Shparlinski 2007, 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 well-known fact.

Theorem 2.1 [Ahmadi and Shparlinski 2007, Corollary 9.2.5]. *Let $G = (V, E)$ be an (n, d, λ)-graph. For any two sets $B, C \subset V$, we have*

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

For any $\lambda \in \mathbb{Z}_m$, the product graph $B_m(k, \lambda)$ is defined as follows. The vertex set of the product graph $B_m(k, \lambda)$ is the set $V(B_m(k, \lambda)) = \mathbb{Z}_m^k \backslash (\mathbb{Z}_m^0)^k$. Two vertices $\boldsymbol{a}$ and $\boldsymbol{b} \in V(B_m(k, \lambda))$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(B_m(k, \lambda))$, if and only if $\boldsymbol{a} \cdot \boldsymbol{b} = \lambda$. When $\lambda = 0$, the graph is a variant of the Erdős–Rényi graph, which has several interesting applications. We will study this case in a separate paper. We now study the product graph when $\lambda \in \mathbb{Z}_m^\times$.

Theorem 2.2 [Vinh 2013b]. *For any $k \geq 2$ and $\lambda \in \mathbb{Z}_m^\times$, the product graph $B_m(k, \lambda)$ is an*

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

Proof. This proof follows from the proof of [Vinh 2013b, Theorem 3.1]. We include its proof here for completeness. It follows from the definition of the product graph $B_m(k, \lambda)$ that $B_m(k, \lambda)$ is a graph of order $m^k - (m - \phi(m))^k$. The valency of the graph is also easy to compute. Given a vertex $\boldsymbol{x} \in V(B_m(k, \lambda))$, there exists an index $x_i \in \mathbb{Z}_m^\times$. We can assume that $x_1 \in \mathbb{Z}_m^\times$. We can choose $y_2, \dots, y_k \in \mathbb{Z}_m$ arbitrarily, then y_1 is determined uniquely such that $\boldsymbol{x} \cdot \boldsymbol{y} = \lambda$. Hence, $B_m(k, \lambda)$ is a regular graph of valency m^{d-1}. It remains to estimate the eigenvalues of this multigraph (that is, graph with loops). For any $\boldsymbol{a} \neq \boldsymbol{b} \in \mathbb{Z}_m^k \backslash (\mathbb{Z}_m^0)^k$, we count the number of solutions of the following system:

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv \boldsymbol{b} \cdot \boldsymbol{x} \equiv \lambda \bmod m, \quad \boldsymbol{x} \in \mathbb{Z}_m^k \backslash (\mathbb{Z}_m^0)^k. \tag{2-1}$$

There exist uniquely $n|m$ and $\boldsymbol{b}_1 \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k$ such that $\boldsymbol{b} = \boldsymbol{a} + n\boldsymbol{b}_1$. The system (2-1) becomes

$$\text{(2-2)} \qquad \boldsymbol{a} \cdot \boldsymbol{x} \equiv \lambda \bmod m, \quad n\boldsymbol{b}_1 \cdot \boldsymbol{x} \equiv 0 \bmod m, \quad \boldsymbol{x} \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k.$$

Let $\boldsymbol{a}_n \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k \equiv \boldsymbol{a} \bmod m/n$, $\boldsymbol{x}_n \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k \equiv \boldsymbol{x} \bmod m/n$, and $\lambda_n \equiv \lambda \bmod m/n$. To solve (2-2), we first solve the following system:

$$\text{(2-3)} \quad \boldsymbol{a}_n \cdot \boldsymbol{x}_n \equiv \lambda_n \bmod m/n, \ \boldsymbol{b}_1 \cdot \boldsymbol{x}_n \equiv 0 \bmod m/n, \quad \boldsymbol{x}_n \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k.$$

The system (2-3) has no solution when $\boldsymbol{a}_n \equiv t\boldsymbol{b}_1 \bmod p$ for some prime $p|(m/n)$ and $t \in \mathbb{Z}^\times_m$, and $(m/n)^{k-2}$ solutions otherwise. For each solution $\boldsymbol{x}_n$ of (2-3), putting back into the system

$$\text{(2-4)} \qquad \boldsymbol{a} \cdot \boldsymbol{x} \equiv \lambda \bmod m, \quad \boldsymbol{x} \equiv \boldsymbol{x}_n \bmod m/n,$$

gives us n^{k-1} solutions of the system (2-2). Hence, the system (2-2) has $m^{k-2}n$ solutions when $\boldsymbol{a}_n \not\equiv t\boldsymbol{b}_1 \bmod p$ and no solution otherwise. Let A be the adjacency matrix of $B_m(k, \lambda)$. It follows that

$$\text{(2-5)} \quad A^2 = m^{k-2}J + (m^{k-1} - m^{k-2})I - m^{k-2} \sum_{\substack{n|m \\ 1 \le n < m}} E_n + \sum_{\substack{n|m \\ 1 < n < m}} (m^{k-2}n - m^{k-2})F_n,$$

where J is the all-ones matrix; I is the identity matrix; E_n is the adjacency matrix of the graph $B_{E,n}$, where for any two vertices $\boldsymbol{a}, \boldsymbol{b} \in V(B_m(k, \lambda))$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{E,n}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + n\boldsymbol{b}_1$, $\boldsymbol{b}_1 \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k$ and $\boldsymbol{a}_n \equiv t\boldsymbol{b}_1 \bmod p$ for some prime $p|(m/n)$; and F_n is the adjacency matrix of the graph $B_{F,n}$, where for any two vertices $\boldsymbol{a}, \boldsymbol{b} \in V(B_m(k, \lambda))$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{F,n}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + n\boldsymbol{b}_1$, $\boldsymbol{b}_1 \in (\mathbb{Z}_{m/n})^k \backslash (\mathbb{Z}^0_{m/n})^k$, and $\boldsymbol{a}_n \not\equiv t\boldsymbol{b}_1 \bmod p$ for any prime $p|(m/n)$.

Therefore, $B_{E,n}$ is a regular graph of valency at most

$$\sum_{p|(m/n),\ p \in \mathcal{P}} (p-1)\Big(\frac{m}{np}\Big)^k < \omega(m)(m/n)^k \gamma(m)^{1-k}.$$

Hence all eigenvalues of E_n are at most $\omega(m)(m/n)^k\gamma(m)^{1-k}$. Besides, it is clear that all eigenvalues of F_n are at most $(m/n)^k$. Since $B_m(k, \lambda)$ is a m^{k-1}-regular graph, m^{k-1} is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $B_m(k, \lambda)$ is connected, therefore the eigenvalue m^{k-1} has multiplicity one. Since the graph $B_m(k, \lambda)$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ, $|\theta| < m^{k-1}$. 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 (2-5) that

$$(\theta^2 - m^{k-1} + m^{k-2})\boldsymbol{v}_\theta = \Big(m^{k-2} \sum_{\substack{n|m \\ 1 \le n < m}} E_n - \sum_{\substack{n|m \\ 1 < n < m}} (m^{k-2}n - m^{k-2})F_n\Big)\boldsymbol{v}_\theta.$$

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

$$m^{k-2}\sum_{\substack{n|m\\1\le n<m}} E_n - \sum_{\substack{n|m\\1<n<m}} (m^{k-2}n - m^{k-2})F_n.$$

Since the absolute values of the eigenvalues of a sum of matrices are bounded by the sums of the largest absolute values of eigenvalues of the summands, we have

$$\begin{aligned}\theta^2 &\le m^{k-1} - m^{k-2} + m^{k-2}\sum_{\substack{n|m\\1\le n<m}} \omega(m)(m/n)^k\gamma(m)^{1-k} + \sum_{\substack{n|m\\1<n<m}}(m^{k-2}n - m^{k-2})(m/n)^k\\ &< m^{k-1} + \omega(m)(\tau(m)-1)m^{2k-2}\gamma(m)^{1-k} + \sum_{\substack{n|m\\1<n<m}} m^{2k-2}n^{1-k}\\ &< (\omega(m)+1)(\tau(m)-1)m^{2k-2}\gamma(m)^{1-k} \le \tau(m)^2 m^{2k-2}\gamma(m)^{1-k}.\end{aligned}$$

The lemma follows. □

The following lemma is an immediate corollary of Theorems 2.1 and 2.2.

Lemma 2.3. *For any* $\mathscr{E}, \mathscr{F} \subset \mathbb{Z}_m^k \backslash (\mathbb{Z}_m^0)^k$ *and* $\lambda \in \mathbb{Z}_m^\times$, *let*

$$e_\lambda(\mathscr{E}, F) = |\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathscr{E}\times\mathscr{F} : \boldsymbol{x}\cdot\boldsymbol{y} = \lambda\}|.$$

Then

$$e_\lambda(\mathscr{E}, \mathscr{F}) = \frac{(1+o(1))|\mathscr{E}||\mathscr{F}|}{m} + O\left(\frac{\tau(m)m^{k-1}}{\gamma(m)^{(k-1)/2}}\sqrt{|\mathscr{E}||\mathscr{F}|}\right).$$

See also [Covert et al. 2012, Theorem 1.3.2] for another proof using character sums over finite rings of Lemma 2.3 in the case of $m = p^r$.

3. Proof of Theorem 1.4

Fix an $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathscr{E} \cap (\mathbb{Z}_m^\times)^k$. For any $\boldsymbol{x} = (x_1, \dots, x_k)$, and $\boldsymbol{y} = (y_1, \dots, y_k) \in \mathscr{E}$, let $M(\boldsymbol{a}; \boldsymbol{x}, \boldsymbol{y})$ denote the matrix whose rows are $\boldsymbol{x}$, $\boldsymbol{y}$, and $(k-2)$ $\boldsymbol{a}$'s. Let $\mathbf{1} := (1, \dots, 1)$, $\boldsymbol{x}/\boldsymbol{a} := (x_1/a_1, \dots, x_k/a_k)$, and $\boldsymbol{y}/\boldsymbol{a} := (y_1/a_1, \dots, y_k/a_k)$; we have

$$\operatorname{Per}(M(\boldsymbol{a}; \boldsymbol{x}, \boldsymbol{y})) = \prod_{i=1}^k a_i \operatorname{Per}(M(\mathbf{1}; \boldsymbol{x}/\boldsymbol{a}, \boldsymbol{y}/\boldsymbol{a})) = \left(\prod_{i=1}^k a_i\right)\sum_{i=1}^k \frac{x_i}{a_i}\sum_{j\ne i}\frac{y_j}{a_j}.$$

Set

$$\mathscr{E}_1 := \{(x_i/a_i)_{i=1}^k : (x_1, \dots, x_k) \in \mathscr{E}\}, \tag{3-1}$$

$$\mathscr{E}_2 := \left\{\left(\sum_{j\ne i} y_i/a_i\right)_{i=1}^k : (y_1, \dots, y_k) \in \mathscr{E}\right\}. \tag{3-2}$$

It is clear that $|\mathscr{E}_1| = |\mathscr{E}_2| = |\mathscr{E}|$ (as $\gcd(k, m) = 1$). For any $\lambda \in \mathbb{Z}_m^\times$, it follows from Lemma 2.3 that

$$
\begin{aligned}
e_\lambda(\mathscr{E}_1, \mathscr{E}_2) &= \frac{(1+o(1))|\mathscr{E}_1||\mathscr{E}_2|}{m} + O\left(\frac{\tau(m)m^{k-1}}{\gamma(m)^{(k-1)/2}}\sqrt{|\mathscr{E}_1||\mathscr{E}_2|}\right) \\
&= \frac{(1+o(1))|\mathscr{E}|^2}{m} + O\left(\frac{\tau(m)m^{k-1}}{\gamma(m)^{(k-1)/2}}|\mathscr{E}|\right).
\end{aligned}
\tag{3-3}
$$

Since

$$|\mathscr{E}| \gtrsim \frac{\tau(m)m^k}{\gamma(m)^{(k-1)/2}},$$

(3-3) implies that

$$\mathbb{Z}_m^\times \subset \{\mathrm{Per}(M(\boldsymbol{a}; \boldsymbol{x}, \boldsymbol{y})) : \boldsymbol{x}, \boldsymbol{y} \in \mathscr{E}\} \subset P_k(\mathscr{E}),$$

completing the proof of Theorem 1.4.

References

[Ahmadi and Shparlinski 2007] O. Ahmadi and I. E. Shparlinski, "Distribution of matrices with restricted entries over finite fields", *Indag. Math.* (*N.S.*) **18**:3 (2007), 327–337. MR 2008k:11127 Zbl 1181.11030

[Blömer et al. 1997] J. Blömer, R. Karp, and E. Welzl, "The rank of sparse random matrices over finite fields", *Random Structures Algorithms* **10**:4 (1997), 407–419. MR 99b:15028 Zbl 0877.15027

[Covert et al. 2010] D. Covert, D. Hart, A. Iosevich, D. Koh, and M. Rudnev, "Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields", *European J. Combin.* **31**:1 (2010), 306–319. MR 2010m:11014 Zbl 1243.11009

[Covert et al. 2012] D. Covert, A. Iosevich, and J. Pakianathan, "Geometric configurations in the ring of integers modulo p^ℓ", *Indiana Univ. Math. J.* **61**:5 (2012), 1949–1969. MR 3119606 Zbl 06236912

[Kahn and Komlós 2001] J. Kahn and J. Komlós, "Singularity probabilities for random matrices over finite fields", *Combin. Probab. Comput.* **10**:2 (2001), 137–157. MR 2002c:15043 Zbl 0979.15022

[Kovalenko et al. 1986] I. N. Kovalenko, A. A. Levitskaya, and M. N. Savchuk, *Izbrannye zadachi veroyatnostnoi kombinatoriki*, Naukova Dumka, Kiev, 1986. MR 88m:60022

[Lyapkov and Sevast'yanov 1996] L. A. Lyapkov and B. A. Sevast'yanov, "Limit distribution of the probabilities of the permanent of a random matrix in the field GF(p)", *Diskret. Mat.* **8**:2 (1996), 3–13. In Russian; translated in *Discrete Math. Appl.* **6**(2), 107–116 (1996). MR 97g:60017 Zbl 0869.15004

[Vinh 2009] L. A. Vinh, "Distribution of determinant of matrices with restricted entries over finite fields", *J. Comb. Number Theory* **1**:3 (2009), 203–212. MR 2011g:11056 Zbl 1234.11030

[Vinh 2012a] L. A. Vinh, "On the permanents of matrices with restricted entries over finite fields", *SIAM J. Discrete Math.* **26**:3 (2012), 997–1007. MR 3022119 Zbl 1260.15008

[Vinh 2012b] L. A. Vinh, "Singular matrices with restricted rows in vector spaces over finite fields", *Discrete Math.* **312**:2 (2012), 413–418. MR 2012h:15062 Zbl 1246.15035

[Vinh 2013a] L. A. Vinh, "On the volume set of point sets in vector spaces over finite fields", *Proc. Amer. Math. Soc.* **141**:9 (2013), 3067–3071. MR 3068960 Zbl 06203435

[Vinh 2013b] L. A. Vinh, "Product graphs, sum-product graphs and sum-product estimates over finite rings", *Forum Mathematicum* (2013).

Received December 18, 2011. Revised September 9, 2013.

LE ANH VINH
UNIVERSITY OF EDUCATION
VIETNAM NATIONAL UNIVERSITY, HANOI
144 XUAN THUY
CAU GIAY
HANOI 100000
VIETNAM
vinhla@vnu.edu.vn

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2014 is US $410/year for the electronic version, and $535/year for print and electronic.
Subscriptions, requests for back issues and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 267 No. 2 February 2014