

*Pacific  
Journal of  
Mathematics*

**SPECTRA OF PRODUCT GRAPHS AND  
PERMANENTS OF MATRICES OVER FINITE RINGS**

LE ANH VINH

Volume 267 No. 2

February 2014



## 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  $\mathcal{E}$  is a sufficiently large subset of  $\mathbb{Z}_m^k$  then the set of permanents of  $k \times k$  matrices with rows in  $\mathcal{E}$  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

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

and its permanent

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

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

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

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  $\mu$  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  $\mu$  is not contained in any proper affine subfield of  $\mathbb{F}_q$ .

An extension of the uniform limit to random matrices with  $\mu$  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  $\mathcal{E} \subseteq \mathbb{F}_q^k$ , let  $M_k(\mathcal{E})$  denote the set of  $k \times k$  matrices with rows in  $\mathcal{E}$ . For any  $t \in \mathbb{F}_q$ , let  $D_k(\mathcal{E}; t)$  be the number of  $k \times k$  matrices in  $M_k(\mathcal{E})$  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

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

if  $t \in \mathbb{F}_p^*$  and  $H \gtrsim p^{3/4+\epsilon}$  for any constant  $\epsilon > 0$ . 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 ( $k \geq 4$ ):

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

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

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

if  $t \in \mathbb{F}_q^*$  and  $\mathcal{E} \subset \mathbb{F}_q^3$  is a product-like set of cardinality  $|\mathcal{E}| \gg q^{15/8}$ . In the singular case, the author [Vinh 2012b] showed that for any subset  $\mathcal{E} \subseteq \mathbb{F}_q^k$  with  $|\mathcal{E}| \gg q^{k-1+2/k}$  then the number of singular matrices whose rows are in  $\mathcal{E}$  is close to

the expected number  $(1 + o(1))|\mathcal{E}|^k/q$ . In the general case, the author [Vinh 2013a] showed that if  $\mathcal{E}$  is a subset of the  $k$ -dimensional vector space over a finite field  $\mathbb{F}_q$  ( $k \geq 3$ ) of cardinality  $|\mathcal{E}| \geq (k-1)q^{k-1}$ , then the set of volumes of  $k$ -dimensional parallelepipeds determined by  $\mathcal{E}$  covers  $\mathbb{F}_q$ . This bound is sharp up to a factor of  $(k-1)$  as taking  $\mathcal{E}$  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

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

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,  $P_k(\mathcal{E}) = \{\text{Per}(M) : M \in M_k(\mathcal{E})\}$ . 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  $\mathcal{E} \cap (\mathbb{F}_q^*)^k \neq \emptyset$ , and  $|\mathcal{E}| \gtrsim q^{(k+1/2)}$ , then  $\mathbb{F}_q^* \subseteq P_k(\mathcal{E})$ .*

Note that if  $|\mathcal{E}| > nq^{n-1}$  then  $\mathcal{E} \cap (\mathbb{F}_q^*)^k \neq \emptyset$ . 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  $\mathcal{E} \subset \mathbb{F}_q^n$  of cardinality  $|\mathcal{E}| > nq^{n-1}$ , then  $\mathbb{F}_q^* \subseteq P_n(\mathcal{E})$ .*
- (b) *If  $\mathcal{A} \subset \mathbb{F}_q$  of cardinality  $|\mathcal{A}| \gg q^{1/2+1/(2n)}$ , then  $\mathbb{F}_q^* \subseteq P_n(\mathcal{A}^n)$ .*

The bound in the first part of Corollary 1.3 is tight up to a factor of  $n$ . For example,  $|\{\mathbf{x} \in \mathbb{F}_q^n : x_1 = 0\}| = q^{n-1}$  and  $P_n(\{\mathbf{x} \in \mathbb{F}_q^n : x_1 = 0\}) = 0$ . However, we conjecture that the bound in the second part of Corollary 1.3 can be further improved to  $|\mathcal{A}| \gg q^{1/2+\epsilon}$  (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  $\{0, 1, \dots, m-1\}$ . 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  $\mathbf{x}$ , 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  $\mathcal{E}$  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  $\mathcal{E} \cap (\mathbb{Z}_m^\times)^k \neq \emptyset$ , and*

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

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

Notice that if  $|\mathcal{E}| > k(m - \phi(m))m^{k-1}$  then  $\mathcal{E} \cap (\mathbb{Z}_m^\times)^k \neq \emptyset$ . 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

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

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

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

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

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

Note that the bound in Corollary 1.5 is sharp. For example, if  $\mathcal{E} = \mathbb{Z}_m^0 \times \mathbb{Z}_m^{k-1}$  then  $P_k(\mathcal{E}) \subset \mathbb{Z}_m^0$ . 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  $\mathcal{E} \cap (\mathbb{Z}_{p^r}^\times)^k \neq \emptyset$ , and*

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

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

*In particular, suppose that  $k \geq 3$ ,  $p \gg r$ , and  $|\mathcal{E}| \gtrsim p^{kr-1}$ , then  $\mathbb{Z}_{p^r}^\times \subset P_k(\mathcal{E})$ . The lower bound of  $|\mathcal{E}|$  in this case is sharp, as taking  $\mathcal{E}$  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  $\mathcal{E} = \mathcal{A}^n$  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  $\mathcal{E} \subset \mathbb{F}_q^k$ , let  $P_k(\mathcal{E}; t)$  be the number of  $k \times k$  matrices with rows in  $\mathcal{E}$  having permanent  $t$ . In [Vinh 2012a], the author studied the distribution of  $P_n(\mathcal{E}; t)$  when  $\mathcal{E} = \mathcal{A}^k$  for a large subset  $\mathcal{A} \subset \mathbb{F}_q$ . 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  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  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 [Ahmadi and Shparlinski 2007, 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 well-known fact.

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

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

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  $V(B_m(k, \lambda)) = \mathbb{Z}_m^k \setminus (\mathbb{Z}_m^0)^k$ . Two vertices  $\mathbf{a}$  and  $\mathbf{b} \in V(B_m(k, \lambda))$  are connected by an edge,  $(\mathbf{a}, \mathbf{b}) \in E(B_m(k, \lambda))$ , if and only if  $\mathbf{a} \cdot \mathbf{b} = \lambda$ . 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  $\mathbf{x} \in V(B_m(k, \lambda))$ , 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  $\mathbf{x} \cdot \mathbf{y} = \lambda$ . 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  $\mathbf{a} \neq \mathbf{b} \in \mathbb{Z}_m^k \setminus (\mathbb{Z}_m^0)^k$ , we count the number of solutions of the following system:

$$(2-1) \quad \mathbf{a} \cdot \mathbf{x} \equiv \mathbf{b} \cdot \mathbf{x} \equiv \lambda \pmod{m}, \quad \mathbf{x} \in \mathbb{Z}_m^k \setminus (\mathbb{Z}_m^0)^k.$$

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

$$(2-2) \quad \mathbf{a} \cdot \mathbf{x} \equiv \lambda \pmod{m}, \quad n\mathbf{b}_1 \cdot \mathbf{x} \equiv 0 \pmod{m}, \quad \mathbf{x} \in (\mathbb{Z}_{m/n})^k \setminus (\mathbb{Z}_{m/n}^0)^k.$$

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

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

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

$$(2-4) \quad \mathbf{a} \cdot \mathbf{x} \equiv \lambda \pmod{m}, \quad \mathbf{x} \equiv \mathbf{x}_n \pmod{m/n},$$

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

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

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

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

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

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  $\theta$ ,  $|\theta| < m^{k-1}$ . Let  $\mathbf{v}_\theta$  denote the corresponding eigenvector of  $\theta$ . Note that  $\mathbf{v}_\theta \in \mathbf{1}^\perp$ , so  $J\mathbf{v}_\theta = 0$ . It follows from (2-5) that

$$(\theta^2 - m^{k-1} + m^{k-2})\mathbf{v}_\theta = \left(m^{k-2} \sum_{\substack{n|m \\ 1 \leq n < m}} E_n - \sum_{\substack{n|m \\ 1 < n < m}} (m^{k-2}n - m^{k-2})F_n\right)\mathbf{v}_\theta.$$



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

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

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

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

The lemma follows. □

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

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

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

Then

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

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

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

Set

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

$$(3-2) \quad \mathcal{E}_2 := \left\{ \left( \sum_{j \neq i} y_j/a_j \right)_{i=1}^k : (y_1, \dots, y_k) \in \mathcal{E} \right\}.$$

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

from Lemma 2.3 that

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

Since

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

(3-3) implies that

$$\mathbb{Z}_m^\times \subset \{\text{Per}(M(\mathbf{a}; \mathbf{x}, \mathbf{y})) : \mathbf{x}, \mathbf{y} \in \mathcal{E}\} \subset P_k(\mathcal{E}),$$

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  $p^\ell$ ”, *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, *Izbrannyye 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  $\text{GF}(p)$ ”, *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](mailto: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)

## EDITORS

V. S. Varadarajan (Managing Editor)  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
pacific@math.ucla.edu

Paul Balmer  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
balmer@math.ucla.edu

Don Blasius  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
blasius@math.ucla.edu

Vyjayanthi Chari  
Department of Mathematics  
University of California  
Riverside, CA 92521-0135  
chari@math.ucr.edu

Daryl Cooper  
Department of Mathematics  
University of California  
Santa Barbara, CA 93106-3080  
cooper@math.ucsb.edu

Robert Finn  
Department of Mathematics  
Stanford University  
Stanford, CA 94305-2125  
finn@math.stanford.edu

Kefeng Liu  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
liu@math.ucla.edu

Jiang-Hua Lu  
Department of Mathematics  
The University of Hong Kong  
Pokfulam Rd., Hong Kong  
jhlu@maths.hku.hk

Sorin Popa  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
popa@math.ucla.edu

Jie Qing  
Department of Mathematics  
University of California  
Santa Cruz, CA 95064  
qing@cats.ucsc.edu

Paul Yang  
Department of Mathematics  
Princeton University  
Princeton NJ 08544-1000  
yang@math.princeton.edu

## PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

## SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI  
CALIFORNIA INST. OF TECHNOLOGY  
INST. DE MATEMÁTICA PURA E APLICADA  
KEIO UNIVERSITY  
MATH. SCIENCES RESEARCH INSTITUTE  
NEW MEXICO STATE UNIV.  
OREGON STATE UNIV.

STANFORD UNIVERSITY  
UNIV. OF BRITISH COLUMBIA  
UNIV. OF CALIFORNIA, BERKELEY  
UNIV. OF CALIFORNIA, DAVIS  
UNIV. OF CALIFORNIA, LOS ANGELES  
UNIV. OF CALIFORNIA, RIVERSIDE  
UNIV. OF CALIFORNIA, SAN DIEGO  
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ  
UNIV. OF MONTANA  
UNIV. OF OREGON  
UNIV. OF SOUTHERN CALIFORNIA  
UNIV. OF UTAH  
UNIV. OF WASHINGTON  
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.

---

See inside back cover or [msp.org/pjm](http://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/>

© 2014 Mathematical Sciences Publishers

# PACIFIC JOURNAL OF MATHEMATICS

Volume 267    No. 2    February 2014

---

Sums of squares in algebraic function fields over a complete discretely valued field	257
KARIM JOHANNES BECHER, DAVID GRIMM and JAN VAN GEEL	
On the equivalence problem for toric contact structures on $S^3$ -bundles over $S^2$	277
CHARLES P. BOYER and JUSTIN PATI	
An almost-Schur type lemma for symmetric $(2,0)$ tensors and applications	325
XU CHENG	
Algebraic invariants, mutation, and commensurability of link complements	341
ERIC CHESEBRO and JASON DEBLOIS	
Taut foliations and the action of the fundamental group on leaf spaces and universal circles	399
YOSUKE KANO	
A new monotone quantity along the inverse mean curvature flow in $\mathbb{R}^n$	417
KWOK-KUN KWONG and PENGZI MIAO	
Nonfibered L-space knots	423
TYE LIDMAN and LIAM WATSON	
Families and Springer's correspondence	431
GEORGE LUSZTIG	
Reflexive operator algebras on Banach spaces	451
FLORENCE MERLEVÈDE, COSTEL PELIGRAD and MAGDA PELIGRAD	
Harer stability and orbifold cohomology	465
NICOLA PAGANI	
Spectra of product graphs and permanents of matrices over finite rings	479
LE ANH VINH	
The concavity of the Gaussian curvature of the convex level sets of minimal surfaces with respect to the height	489
PEI-HE WANG	



0030-8730(2014)267:2;1-6