A point-plane incidence theorem in matrix rings

Nguyen Van The * Le Anh Vinh †

Abstract

In this paper, we study a point-hyper plane incidence theorem in matrix rings, which generalizes all previous works in literature of this direction.

1 Introduction

Let \( \mathbb{F}_q \) be a finite field of order \( q \) where \( q \) is an odd prime power. Let \( M_n(\mathbb{F}_q) \) be the set of \( n \times n \) matrices with entries in \( \mathbb{F}_q \) and \( GL_n(\mathbb{F}_q) \) be the set of invertible matrices in \( M_n(\mathbb{F}_q) \). For \( A_1, A_2, \ldots, A_d, B \in M_n(\mathbb{F}_q) \), we define a hyper-plane in \( M_n(\mathbb{F}_q)^{d+1} = M_n(\mathbb{F}_q) \times \ldots \times M_n(\mathbb{F}_q) \) as the set of points \((X_1, \ldots, X_d, Y) \in M_n(\mathbb{F}_q)^{d+1}\) satisfying

\[
A_1X_1 + \ldots A_dX_d + B = Y. \tag{1}
\]

Note that, this definition is a formal definition, however, it is associated to an \( d \)-dimensional affine plane over the module \( M_n(\mathbb{F}_q)^{d+1} \). When \( d = 1 \), we say the set of points satisfying (1) is a line in \( M_n(\mathbb{F}_q)^2 \) formed by \( A_1 \) and \( B \). In the first version of this note, we prove the following point-line incidence with \( d = 1 \) and \( n = 2 \).

**Theorem 1.1.** Let \( \mathcal{P} \) be a set of points and \( \mathcal{L} \) be a set of lines in \( M_2(\mathbb{F}_q) \times M_2(\mathbb{F}_q) \), then we have

\[
I(\mathcal{P}, \mathcal{L}) \leq \frac{|\mathcal{P}||\mathcal{L}|}{q^4} + \sqrt{2}q^{7/2}\sqrt{|\mathcal{P}||\mathcal{L}|}.
\]

During revision process, Xie and Ge [5] extended this results by considering the equation \( AX + BY = C + D \) where \( A, B, C, D, X, Y \in M_n(\mathbb{F}_q) \), which also generalizes the work of

\*University of Science, Vietnam National University - Hanoi, Email: nguyenvanthe@hus.edu.vn

†Vietnam National University - Hanoi, Email: vinhla@vnu.edu.vn. Vietnam Institute of Educational Sciences. Email: vinhle@vnies.edu.vn
Mohammadi, Pham and Wang [2] for \( n = 2 \). Some similar results could be found in [1, 3], in which they consider the sum-product equation.

In this note, we prove a generalization of all above mentioned results in [1, 2, 3, 5]. Particularly, we consider the equation (1) for all \( d \geq 1 \) and \( n \geq 2 \).

**Theorem 1.2.** For \( d \geq 1 \), \( n \geq 2 \), let \( A_1, \ldots, A_d, B_1, \ldots, B_d, E, F \subset M_n(\mathbb{F}_q) \) and \( N \) be the number of solutions to the sum-product equation

\[
A_1B_1 + A_2B_2 + \cdots + A_dB_d = E + F, \quad A_i \in A_i, B_i \in B_i, E \in E, F \in F.
\]

Then we have

\[
\left| \left| N - \frac{|E||F| |A_1||B_1| \cdots |A_n||B_n|}{q^{n^2}} \right| \right| \ll q^{dn^2 - (d-1)n/2 - 1/2} \sqrt{|E||F| \prod_{i=1}^{n} |A_i||B_i|}.
\]

Theorem 1.2 will be proved via spectral graph theory, in particular, the expander mixing lemma of regular directed graph given by Vu [4]. Firstly, we recall some definitions from graph theory as the following subsection, which is extracted from Section 4 in [3].

## 2 Tools from spectral graph theory

Let \( G \) be a directed graph (digraph) on \( n \) vertices where the in-degree and out-degree of each vertex are both \( d \).

Let \( A_G \) be the adjacency matrix of \( G \), i.e., \( a_{ij} = 1 \) if there is a directed edge from \( i \) to \( j \) and zero otherwise. Suppose that \( \lambda_1 = d, \lambda_2, \ldots, \lambda_n \) are the eigenvalues of \( A_G \). These eigenvalues can be complex, so we cannot order them, but it is known that \( |\lambda_i| \leq d \) for all \( 1 \leq i \leq n \). Define \( \lambda(G) := \max_{i \neq 0} |\lambda_i| \). This value is called the second largest eigenvalue of \( A_G \). We say that the \( n \times n \) matrix \( A \) is normal if \( A^tA = AA^t \) where \( A^t \) is the transpose of \( A \). The graph \( G \) is normal if \( A_G \) is normal. There is a simple way to check whenever \( G \) is normal or not. Indeed, for any two vertices \( x \) and \( y \), let \( N^+(x, y) \) be the set of vertices \( z \) such that \( x \rightarrow z \) and \( y \rightarrow z \) are edges, and \( N^-(x, y) \) be the set of vertices \( z \) such that \( z \rightarrow x \) and \( z \rightarrow y \) are edges. By a direct computation, we have \( A_G \) is normal if and only if \( |N^+(x, y)| = |N^-(x, y)| \) for any two vertices \( x \) and \( y \).
A digraph $G$ is called an $(n, d, \lambda) - digraph$ if $G$ has $n$ vertices, the in-degree and out-degree of each vertex are both $d$, and $\lambda(G) \leq \lambda$. Let $G$ be an $(n, d, \lambda) - digraph$. We have the following expander mixing lemma given by Vu [4].

**Lemma 2.1** (Expander Mixing Lemma, [4]). Let $G = (V, E)$ be an $(n, d, \lambda)$ - digraph. For any two sets $B, C \subseteq V$, we have

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

where $e(B, C)$ be the number of ordered pairs $(u, w)$ such that $u \in B$, $w \in C$, and $\vec{uw} \in e(G)$.

As $d|B||C|/n$ is the expected number of edges from $B$ to $C$, the above lemma gives us a bound for the gap between this number and the number of edges between $B$ and $C$.

### 3 Proof of Theorem 1.2

To prove Theorem 1.2, we define the sum-product digraph $G = (V, E)$ with the vertex set

$$V = M_n(\mathbb{F}_q)^{d+1} = M_n(\mathbb{F}_q) \times M_n(\mathbb{F}_q) \times \cdots \times M_n(\mathbb{F}_q)$$

. There exists a directed edge from $(A_1, \ldots, A_d, E)$ to $(B_1, \ldots, B_d, F)$ if

$$A_1 B_1 + A_2 B_2 + \cdots + A_d B_d = E + F.$$

Theorem 1.2 will be directly followed from Lemma 2.1 and the following proposition.

**Proposition 3.1.** The sum-product digraph $G = (V, E)$ is an $(q^{(d+1)n^2}, q^{dn^2}, C q^{dn^2 - (d-1)n/2 - 1/2}) - digraph$ for some positive constant $C$.

To prove Proposition 3.1, we need some basic facts from linear algebra via the following lemmas.

**Lemma 3.2.** Denote $M_{n \times t}(\mathbb{F}_q)$ be the set of $n \times t$ matrices with entries restricted in $\mathbb{F}_q$ with $n < t$. Then the number of matrices of rank $k \leq n$ is less than

$$\binom{t}{k} (q^n - 1) (q^n - q) \cdots (q^n - q^{k-1}) q^{(t-k)k} \leq C_{t,k} q^{nk+k(t-k)}$$

for some positive constant $C_{t,k}$. 

---

3
Proof. It is observed that the number of $k$ independent column vectors $c_1, \ldots, c_k$ in $F_q^n$ is

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{k-1}).$$

For each matrix $A \in M_{n \times t}(F_q)$ of rank $k$, there exist $k$ independent column vectors $c_1, \ldots, c_k$ in $A$. Furthermore, the $t - k$ other columns can be written as a linear combination of $\{c_i\}_{i=1}^k$, each has $q^k$ possibilities. We can choose $k$ of $t$ column vectors, which are linearly independent. Since two different ways can be just one matrix, the number of matrices of rank $k \leq n$ is bounded by

$$\binom{t}{k} (q^n - 1)(q^n - q^2) \ldots (q^n - q^{k-1}) q^{k(t-k)} \leq C q^{nk + k(t-k)}$$

for some positive constant $C$. \qed

Lemma 3.3. For $n \geq m \geq k \geq 0$, let $T_{m,k}$ be the number of pair $(M, C)$ with $M \in M_{n \times t}(F_q), C \in M_n(F_q)$ satisfying $\text{rank}(M) = m, \text{rank}(C) = k$, and the system $MZ = C$ has solution. We have

$$T_{m,k} \ll q^{nm + m(t-m) + mk + k(n-k)}$$

Proof. For each matrix $M \in M_{n \times t}$ of rank $m$, we will bound the number of matrices $C \in M_n(F_q)$ of rank $k$ that satisfy the equation $MZ = C$ has solution. It follows from Kronecker-Capelli theorem that the equation $MZ = C$ has solution if and only if $\text{rank}(M) = \text{rank}((M C))$ where $(M C)$ is the matrix obtained by adding $C$ to $M$ on the right.

Let $r_{M_1}, \ldots, r_{M_n}$ be row vectors of $M$ and $r_{C_1}, \ldots, r_{C_n}$ be row vectors of $C$, respectively. Without loss of generality, we assume that $r_{M_1}, \ldots, r_{M_k}$ are linearly independent and

$$r_{M_i} = \alpha_1 r_{M_1} + \alpha_2 r_{M_2} + \cdots + \alpha_m r_{M_m}, i = m + 1, m + 2, \ldots, n$$

for some $\alpha_j \in F_q$ for all $j = 1, \ldots, m$. Since $\text{rank}(M) = \text{rank}((M C))$, we have

$$r_{C_i} = \alpha_1 r_{C_1} + \alpha_2 r_{C_2} + \cdots + \alpha_m r_{C_m}, i = m + 1, m + 2, \ldots, n.$$

This means the $n - m$ later row vectors of $C$ are uniquely determined by first $m$ row vectors $r_{C_1}, \ldots, r_{C_m}$ for a given matrix $M$. Therefore, we only need to count number of $m$ row vectors $r_{c_1}, \ldots, r_{c_m}$ satisfying $\text{rank}(r_{c_1}, \ldots, r_{c_m}) = k$, or equivalently, the number of $m \times n$
matrices of rank $k$. Hence, it follows from Lemma 3.2 that the number of matrices $C$ satisfying $MZ = C$ has solution is bounded by $dq^{mk+k(n-k)}$ for some positive constant $d$.

Again, applying Lemma 3.2 there are at most $dq^{nm+m(t-m)}$ matrices $M$ of rank $m$ in $\mathbb{M}_{n \times t}$. Thus, we obtain

$$T_{m,k} \ll q^{nm+m(t-m)+mk+k(n-k)},$$

which completes the proof of Lemma 3.3.

We are now ready to prove Proposition 3.1.

**Proof of Proposition 3.1.** It is obvious that the order of $G$ is $q^{(d+1)n^2}$, because $|M_n(\mathbb{F}_q)| = q^{n^2}$ and so $|M_d(\mathbb{F}_q)^{d+1}| = q^{(d+1)n^2}$. Next, we observe that $G$ is a regular digraph of in-degree and out-degree $q^{dn^2}$. Indeed, for any vertex $(A_1, \ldots, A_d, E) \in V$, if we choose each $d$-tuple $(B_1, \ldots, B_d) \in M_n(\mathbb{F}_q)^d$, there exists a unique $F = A_1B_1 + \cdots + A_dB_d - E$ such that

$$A_1B_1 + \cdots + A_dB_d = E + F.$$

Hence, the out-degree of any vertex in $G$ is $|M_n(\mathbb{F}_q)^d|$, which is $q^{dn^2}$. The same holds for the in-degree of each vertex. Therefore, to prove Proposition 3.1 we only need to bound the second largest eigenvalue of $G$.

To this end, we first need to show that $G$ is a normal digraph. Let $A_G$ be the adjacency matrix of $G$. It is known that if $A_G$ is a normal matrix and $\beta$ is an eigenvalue of $A_G$, then the complex conjugate $\overline{\beta}$ is an eigenvalue of $A_G'$. Hence, $|\beta|^2$ is an eigenvalue of $A_GA_G'$ and $A_G'A_G$. In other words, in order to bound $\beta$, it is enough to bound the second largest eigenvalue of $A_GA_G'$.

Firstly, we will show that $G$ is a normal graph. Let $(A_1, A_2, \ldots, A_d, E)$ and $(A'_1, A'_2, \ldots, A'_d, E')$ be two different vertices, we now count the of the neighbors $(B_1, \ldots, B_d, F)$ such that there are directed edges from $(A_1, \ldots, A_d, E)$ and $(A'_1, \ldots, A'_d, E')$ to $(B_1, \ldots, B_d, F)$. This number is $N^+((A_1, \ldots, A_d, E), (A'_1, \ldots, A'_d, E'))$. We have

$$A_1B_1 + \cdots + A_dB_d = E + F \text{ and } A'_1B_1 + \cdots + A'_dB_d = E' + F.$$  \hfill (2)
which implies

\[(A_1 - A'_1)B_1 + \cdots + (A_d - A'_d)B_d = A - A'. \quad (3)\]

Note that if we fix a solution \((B_1, \ldots, B_d)\) to the equation (3), then \(F\) in (2) is uniquely determined. Let \(M = (A_1 - A'_1 \ A_1 - A'_1 \ \ldots \ A_d - A'_d)\), \(X = (B_1 \ B_2 \ \ldots \ B_d)\) and \(Y = E - E'\), then the equation can be rewritten as the following matrix equation.

\[MX = Y\] \quad (4)

with \(M \in M_{n \times dn}(F_q), Y \in M_n(F_q)\) and \(X \in M_{dn \times n}(F_q)\). We now fall into the following cases.

- **Case 1.** If \(\text{rank}(M) = n\), then there exists unique \(X\) such that \(MX = Y\). Thus the system (2) has only one solution in this case.

- **Case 2.** If \(\text{rank}(M) = m\) and \(\text{rank}(Y) = k\) with \(m < k \leq n\), then the equation \(MX = Y\) has no solution.

- **Case 3.** If \(\text{rank}(M) = m\) and \(\text{rank}(Y) = k\) with \(n > m \geq k\), we need to further consider different situations as follows.
  - **Case 3.1.** If \(\text{rank}(M) = \text{rank}(Y) = 0\), then \(E = E', A_i = A'_i\) for all \(i = 1, \ldots, d\), which contracts with our assumption that \((A_1, A_2, \ldots, A_d, E)\) and \((A'_1, A'_2, \ldots, A'_d, E')\) are two different vertices. Thus, we can rule out this case.
  - **Case 3.2.** If \(\text{rank}(M) > m\) where \(\overline{M} = (M \ Y)\), it follows from Kronecker-Capelli theorem that the equation \(MX = E\) has no solution.
  - **Case 3.3.** Suppose that \(\text{rank}(\overline{M}) = m\) where \(\overline{M} = (M \ Y)\), we have known that the equation \(MX = Y\) has solution by the Kronecker Capelli theorem. Moreover, the number of its solutions is equal to the number of solutions of \(MX = 0\). Now, we are ready to count the number of solutions of \(MX = 0\).

Put \(X = [x_1 \ x_2 \ \ldots \ x_n]\) for some column vectors \(x_1, x_2, \ldots, x_n \in \mathbb{F}_q^{dn}\), we just need to estimate the number of solutions of \(MX = 0\) because the number of solutions of \(MX = 0\) is equal to \(n^{th}\) power of the number of solutions of \(Mx_1 = 0\). It is known that the set \(L\) of all solutions of \(Ax_1 = 0\) is a vector subspace of \(\mathbb{F}_q^{dn}\) and
has the dimension \( \dim L = dn - \text{rank}(M) = dn - m \). Hence, we have

\[ |L| = q^{dn-m}. \]

Therefore, the equation \( MX = 0 \) has \( q^{dn-m} \) solutions if this equation has solutions.

Since the same argument works for the case of \( N^-((A_1, \ldots, A_d, E), (A'_1, \ldots, A'_d, E')) \), we obtain the same value for \( N^-((A_1, \ldots, A_d, e), (A'_1, \ldots, A'_d, E')) \). In short, \( A_G \) is normal.

As we discussed above, in order to bound the second largest eigenvalue of \( M \), it is enough to bound the second largest value of \( MM^t \). Note that each entry of \( A_G A_G^t \) can be interpreted as counting the number of common outgoing neighbors between two vertices. Based on previous calculations, we have

\[
A_G A_G^t = \left( q^{dn^2} - 1 \right) I + J - \sum_{0 \leq m < k \leq n} F_{m,k} - \sum_{0 \leq k \leq m < n: (m, k) \neq (0,0)} H_{m,k} + \left( q^{n(n-m)} - 1 \right) \sum_{0 \leq k \leq m < n: (m, k) \neq (0,0)} E_{m,k}
\]

where \( I \) is the identity matrix, \( J \) denotes the all-one matrix and the others defined as follows.

\( F_{m,k} \) is the adjacency matrix of the graph \( G_{m,k}, 0 \leq m < k \leq n \) with the vertex set \( V(F_{m,k}) = M_n(\mathbb{F}_q)^{d+1} \) and there is an edge between \((A_1, \ldots, A_d, E)\) and \((A'_1, \ldots, A'_d, E')\) if \( \text{rank} (A_1 - A'_1 \ldots A_d - A'_d) = m \) and \( \text{rank} (E - E') = k \).

\( H_{m,k} \) is the adjacency matrix of the graph \( G_{m,k}, 0 \leq k \leq m < n, (m, k) \neq (0,0) \) with the vertex set \( V(H_{m,k}) = M_n(\mathbb{F}_q)^{d+1} \) and there is an edge between \((A_1, \ldots, A_d, E)\) and \((A'_1, \ldots, A'_d, E')\) if \( \text{rank} (A_1 - A'_1 \ldots A_d - A'_d) = m \), \( \text{rank} (E - E') = k \) and

\[
\text{rank} (A_1 - A'_1 \ldots A_d - A'_d E - E') > m.
\]

\( E_{m,k} \) is the adjacency matrix of the graph \( G\mathcal{P}_{m,k}, 0 \leq k \leq m < n, (m, k) \neq (0,0) \) with the vertex set \( V(E_{m,k}) = M_n(\mathbb{F}_q)^{d+1} \) and there is an edge between \((A_1, \ldots, A_d, E)\) and \((A'_1, \ldots, A'_d, E')\) if \( \text{rank} (A_1 - A'_1 \ldots A_d - A'_d) = m \), \( \text{rank} (E - E') = k \) and

\[
\text{rank} (A_1 - A'_1 \ldots A_d - A'_d E - E') = m.
\]
Using the Lemma 3.2, one can easily check that for any \(0 \leq k \leq n, 0 \leq m < n\) and \((m, k) \neq (0, 0)\), the graph \(G_{mk}\) is \(d_{mk}\) regular for some \(d_{mk}\) where
\[
d_{mk} \ll q^{nm+m(dn-m)}q^{nk+k(n-k)} = q^{(d+1)nm+2nk-m^2-k^2} \leq q^{(d+1)n^2-(d-1)n-1}.
\]

For the graph \(G_{P_{m,k}}, 0 \leq k \leq m < n, (m, k) \neq (0, 0)\), it follows directly from Lemma 3.3 that \(G_{mk}\) is \(y_{mk}\) regular for some \(y_{mk}\) where
\[
y_{m,k} \ll q^{nm+m(dn-m)+mk+k(n-k)}.
\]

Suppose \(\lambda_2\) is the second largest eigenvalue of \(A_G\) and \(\vec{v}_2^2\) is the corresponding eigenvector. Since \(G\) is a regular graph, we have \(J \cdot \vec{v}_2 = 0\). (Indeed, since \(G\) is regular, it always has \((1, 1, \ldots, 1)\) as an eigenvector with eigenvalue being its regular-degree. Moreover, since the graph \(G\) is connected, this eigenvalue has multiplicity one. Thus any other eigenvectors will be orthogonal to \((1, 1, \ldots, 1)\) which in turns gives us \(J \cdot \vec{v}_2 = 0\). Since \(A_GA_G^t \vec{v}_2 = |\lambda_2|^2 \vec{v}_2\), we get
\[
|\lambda_2|^2 \vec{v}_2 = \left[ q^{dn^2} - 1 \right] - \sum_{0 \leq k \leq m \leq n} F_{m,k} - \sum_{0 \leq k \leq m < n; (m, k) \neq (0, 0)} H_{m,k} + \left( q^{n(n-m)} - 1 \right) \sum_{0 \leq k \leq m < n; (m, k) \neq (0, 0)} E_{m,k} \vec{v}_2.
\]
(5)

One easily to check that \(y_{m,k}q^{n(dn-m)} \ll q^{2dn^2-(d-1)n-1}\) for all \(0 \leq k \leq m < n, (m, k) \neq 0\). Therefore, all previous calculations and the equation (5) give us
\[
|\lambda_2|^2 \ll q^{2dn^2-(d-1)n-1},
\]

since eigenvalues of a sum of matrices are bounded by the sum of largest eigenvalue of the summands. We complete the proof of Proposition 3.1.

\[\Box\]

References

[1] Y. D. Karabulut, D. Koh, T. Pham, C.-Y. Shen, and L. A. Vinh. Expanding phenomena over matrix rings. Forum Mathematicum, 31(4):951–970, 2019
[2] A. Mohammadi, T. Pham, and Y. Wang. An energy decomposition theorem for matrices and related questions. \textit{arXiv:2106.07328}, 2021.

[3] N. V. The and L. A. Vinh. Expanding phenomena over higher dimensional matrix rings. \textit{Journal of Number Theory}, 216:174–191, 2020.

[4] V. Vu. Sum-product estimates via directed expanders. \textit{Mathematical Research Letters}, 15:375–388, 2008.

[5] C. Xie and G. Ge. Some sum-product estimates in matrix rings over finite fields. \textit{Finite Fields and Their Applications}, 79:101997, 2022.