POLITECNICO DI TORINO
Repository ISTITUZIONALE

On the distribution of the entries of a fixed-rank random matrix over a finite field

Original
On the distribution of the entries of a fixed-rank random matrix over a finite field / Sanna, Carlo. - In: FINITE FIELDS AND THEIR APPLICATIONS. - ISSN 1071-5797. - 93:(2024), pp. 1-15. [10.1016/j.ffa.2023.102333]

Availability:
This version is available at: 11583/2983809 since: 2023-11-13T14:57:55Z

Publisher:
Elsevier

Published
DOI:10.1016/j.ffa.2023.102333

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
Elsevier preprint/submitted version

Preprint (submitted version) of an article published in FINITE FIELDS AND THEIR APPLICATIONS © 2024, http://doi.org/10.1016/j.ffa.2023.102333

(Article begins on next page)

12 October 2024

arXiv:2307.14172v1 [math.CO] 26 Jul 2023

ON THE DISTRIBUTION OF THE ENTRIES OF A FIXED-RANK RANDOM MATRIX OVER A FINITE FIELD

CARLO SANNA†

Abstract. Let $r > 0$ be an integer, let $\mathbb{F}_q$ be a finite field of q elements, and let $\mathcal{A}$ be a nonempty proper subset of $\mathbb{F}_q$. Moreover, let $\mathbf{M}$ be a random $m \times n$ rank-r matrix over $\mathbb{F}_q$ taken with uniform distribution. We prove, in a precise sense, that, as $m, n \to +\infty$ and $r, q, \mathcal{A}$ are fixed, the number of entries of $\mathbf{M}$ that belong to $\mathcal{A}$ approaches a normal distribution.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q element. For every matrix $\mathbf{M}$ over $\mathbb{F}_q$, let $\mathrm{wt}(\mathbf{M})$ be the *weight* of $\mathbb{F}_q$, that is, the number of nonzero entries of $\mathbf{M}$.

Migler, Morrison, and Ogle [3] proved a formula for the expected value of $\mathrm{wt}(\mathbf{M})$ when $\mathbf{M}$ is taken at random, with uniform distribution, from the set of $m \times n$ rank-r matrices over $\mathbb{F}_q$. Furthermore, they suggested that, as $m, n \to +\infty$ and r, q are fixed, an appropriate scaling of $\mathrm{wt}(\mathbf{M})$ approaches a normal distribution. Sanna [6] proved this last claim for $q = 2$ and assuming that m/n converges to a positive real number.

For every $\mathcal{A} \subseteq \mathbb{F}_q$ and for every matrix $\mathbf{M}$ over $\mathbb{F}_q$, let $\mathrm{ct}_{\mathcal{A}}(\mathbf{M})$ be the number of entries of $\mathbf{M}$ that belong to $\mathcal{A}$. Moreover, put $\gamma_{\mathcal{A}}(q) := \sum_{a \in \mathcal{A}} \gamma_a(q)$, where $\gamma_0(q) := q^{-1} - 1$ and $\gamma_a(q) := q^{-1}$ for each $a \in \mathbb{F}_q^*$, and let

$$\mu_{\mathcal{A}}(q, m, n) := \left(|\mathcal{A}|q^{-1} - \gamma_{\mathcal{A}}(q)q^{-r}\right)mn,$$
$$\sigma^2_{\mathcal{A}}(q, m, n) := \gamma_{\mathcal{A}}(q)^2 q^{-r}(1 - q^{-r})(m + n)mn,$$

for all integers $m, n > 0$. Note that $\gamma_{\mathcal{A}}(q) \neq 0$ unless $\mathcal{A} = \varnothing$ or $\mathcal{A} = \mathbb{F}_q$.

Our result is the following.

Theorem 1.1. *Fix an integer $r > 0$ and a nonempty set $\mathcal{A} \subsetneq \mathbb{F}_q$. Let $\mathbf{M}$ be taken at random, with uniform distribution, from the set of $m \times n$ rank-r matrices over $\mathbb{F}_q$. Then, as $m, n \to +\infty$, we have that*

$$\frac{\mathrm{ct}_{\mathcal{A}}(\mathbf{M}) - \mu_{\mathcal{A}}(q, m, n)}{\sqrt{\sigma^2_{\mathcal{A}}(q, m, n)}} \tag{1}$$

converges in distribution to a standard normal random variable.

Roughly speaking, Theorem 1.1 asserts that, as m and n both grow, $\mathrm{ct}_{\mathcal{A}}(\mathbf{M})$ approaches a normal random variable with expected value $\mu_{\mathcal{A}}(q, m, n)$ and variance $\sigma^2_{\mathcal{A}}(q, m, n)$. Note that, if the condition on the rank is dropped, that is, if $\mathbf{M}$ is taken at random with uniform distribution from the set of $m \times n$ matrices over $\mathbb{F}_q$, then an easy application of the central limit theorem yields that $\mathrm{ct}_{\mathcal{A}}(\mathbf{M})$ approaches a normal random variable with expected value $|\mathcal{A}|q^{-1}mn$ and variance $|\mathcal{A}|q^{-1}\left(1 - |\mathcal{A}|q^{-1}\right)mn$.

Before we proceed, let us outline the main ideas of the proof of Theorem 1.1. First, using full-rank factorization and the well-known formula for the number of $m \times n$ rank-r matrices over $\mathbb{F}_q$, it is shown that, for the sake of proving Theorem 1.1, we can assume that $\mathbf{M} = \mathbf{XY}$, where $\mathbf{X}$ and $\mathbf{Y}$ are $m \times r$ and $r \times n$ independent random matrices taken with uniform distribution

2010 *Mathematics Subject Classification.* Primary: 15B52, Secondary: 11T99, 11B33, 05A16.

Key words and phrases. Finite field, Hamming weight, normal distribution, random matrix, rank.

† C. Sanna is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.

from their respective spaces. Second, the event that the product of a row of $\mathbf{X}$ and a column of $\mathbf{Y}$ is equal to a prescribed element of $\mathbb{F}_q$ is handled via the Fourier transform of $\mathbb{F}_q$ respect to multiplicative characters. The use of multiplicative characters is necessary to conveniently "separate" the entries of $\mathbf{X}$ by the entries of $\mathbf{Y}$ in two factors of a product. However, it introduces some complications (essentially because the Fourier inversion formula holds only for functions $\mathbb{F}_q^t \to \mathbb{C}$ that are supported on $(\mathbb{F}_q^*)^t$), which are dealt with by a kind of Möbius transform. Finally, all of this makes possible to write (1) as a main term, which converges in distribution to a standard normal random variable, plus an error term, which is shown to be negligible.

It might be interesting to strenghten Theorem 1.1 by letting also r goes to infinity, but in a way controlled by m and n (see Remark 5.1).

2. General notations and definitions

For every finite set $\mathcal{A}$, we let $|\mathcal{A}|$ be the number of elements of $\mathcal{A}$. For each statement S, we let $\mathbb{1}[S]$ be equal to 1 if S is true, and to 0 if S is false. For every event E, we let $\mathbb{P}[E]$ be the probability that E occurs. For each real or complex random variable X, we write $\mathbb{E}[X]$ and $\mathbb{V}[X]$ for the expected value and the variance of X. For every sequence (X_n) of random variables, we write $X_n \xrightarrow{d} X$ to denote that (X_n) converges in distribution to X. For a complex random variable $Z = X + \boldsymbol{i}Y$, where X and Y are real random variables and $\boldsymbol{i}$ is the imaginary unity, the *covariance matrix* of Z is the covariance matrix of the random vector (X, Y). Also, we say that Z is a *complex normal random variable* if the random vector (X, Y) follows a bivariate normal distribution. For each integer $r > 0$, we set $[r] := \{1, \dots, r\}$. We say that a function $f \colon \mathcal{X} \to \mathbb{C}$ is *supported* on a set $\mathcal{Y}$ if $f(x) = 0$ for every $x \in \mathcal{X} \setminus \mathcal{Y}$. We adopt the usual convention that the empty sum and the empty product are equal to 0 and 1, respectively.

3. Preliminaries on the Fourier transform

3.1. **Characters of finite fields.** We recall some basics facts about characters of finite fields (see, e.g., [2, Chapter 5, Section 1] and [4, Chapter 10, Section 1]).

Given a finite abelian group G, a *character* of G is a group homomorphism $G \to \mathbb{C}^*$. The set of characters of G is denoted by $\widehat{G}$ and is a finite abelian group respect to the pointwise product of functions. The identity of $\widehat{G}$ is the *trivial character*, which sends each element of G to 1, while the inverse of each $\chi \in \widehat{G}$ is the pointwise complex conjugation of χ, which is denoted by $\overline{\chi}$.

The *additive characters* of $\mathbb{F}_q$ are the characters of $\mathbb{F}_q$ as an additive group. We let ψ_0 denote the trivial additive character of $\mathbb{F}_q$. The *multiplicative characters* of $\mathbb{F}_q$ are the characters of $\mathbb{F}_q^*$ as a multiplicative group. We let χ_0 denote the trivial multiplicative character of $\mathbb{F}_q$. Moreover, we extend each multiplicative character χ of $\mathbb{F}_q$ to a function $\mathbb{F}_q \to \mathbb{C}$ by setting $\chi(0) := 0$.

The additive and multiplicative characters of $\mathbb{F}_q$ satisfy the orthogonality relations:

$$\frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} \psi(a) = \mathbb{1}[a = 0] \tag{2}$$

$$\frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(a) = \mathbb{1}[a = 1] \tag{3}$$

for every $a \in \mathbb{F}_q$, and

$$\frac{1}{q} \sum_{a \in \mathbb{F}_q} \psi(a) = \mathbb{1}[\psi = \psi_0] \tag{4}$$

$$\frac{1}{q-1} \sum_{a \in \mathbb{F}_q} \chi(a) = \mathbb{1}[\chi = \chi_0] \tag{5}$$

for every $\psi \in \widehat{\mathbb{F}_q}$ and $\chi \in \widehat{\mathbb{F}_q^*}$.

For every function $f \colon \mathbb{F}_q^t \to \mathbb{C}$ that is supported on $(\mathbb{F}_q^*)^t$, the *Fourier transform* of f is the function $\widehat{f} \colon \widehat{\mathbb{F}_q}^t \to \mathbb{C}$ defined by

$$\widehat{f}(\chi_1, \dots, \chi_t) := \frac{1}{(q-1)^t} \sum_{a_1, \dots, a_t \in \mathbb{F}_q} f(a_1, \dots, a_t) \overline{\chi_1}(a_1) \cdots \overline{\chi_t}(a_t) \tag{6}$$

for every $\chi_1, \dots, \chi_t \in \widehat{\mathbb{F}_q^*}$.[1] From the orthogonality relation (3), it easily follows that

$$f(a_1, \dots, a_t) = \sum_{\chi_1, \dots, \chi_t \in \widehat{\mathbb{F}_q^*}} \widehat{f}(\chi_1, \cdots, \chi_t)\chi_1(a_1) \cdots \chi_t(a_t) \tag{7}$$

for every $a_1, \dots, a_t \in \mathbb{F}_q$, which is the *Fourier inversion formula*.

3.2. **Möbius transform.** We need a kind of *Möbius transform* and its corresponding inversion formula, which is essentially a consequence of the inclusion-exclusion principle (see, e.g., [7, Example 3.8.3]).

First, note that from the binomial theorem it easily follows that

$$\sum_{\mathcal{A} \subseteq \mathcal{B}} (-1)^{|\mathcal{A}|} = \mathbb{1}[\mathcal{B} = \varnothing], \tag{8}$$

for every finite set $\mathcal{B}$.

Throughout the rest of Section 3, let $r > 0$ be a fixed integer. For every $\mathcal{S} \subseteq [r]$, we write $a_{\mathcal{S}}$ to denote the $|\mathcal{S}|$-tuple $(a_{k_1}, \dots, a_{k_{|\mathcal{S}|}})$, where $k_1 < \cdots < k_{|\mathcal{S}|}$ are the elements of $\mathcal{S}$. (If $\mathcal{S}$ is empty, then $a_{\mathcal{S}}$ is the empty tuple). Moreover, we write $a_{(\mathcal{S})}$ to denote the r-tuple $(b_1, \dots, b_r)$, where $b_k := 0$ if $k \notin \mathcal{S}$, and $b_k := a_k$ if $k \in \mathcal{S}$.

For every function $f \colon \mathbb{F}_q^r \to \mathbb{C}$ and for every $\mathcal{S} \subseteq [r]$, we define the function $f_{\mathcal{S}} \colon \mathbb{F}_q^{|\mathcal{S}|} \to \mathbb{C}$ by

$$f_{\mathcal{S}}(a_{\mathcal{S}}) := \sum_{\mathcal{T} \subseteq \mathcal{S}} (-1)^{|\mathcal{S} \setminus \mathcal{T}|} f(a_{(\mathcal{T})}), \tag{9}$$

for every $a_{\mathcal{S}} \in \mathbb{F}_q^{|\mathcal{S}|}$.

Lemma 3.1. *Let $f \colon \mathbb{F}_q^r \to \mathbb{C}$. Then, for every $\mathcal{S} \subseteq [r]$, the function $f_{\mathcal{S}}$ is supported on $(\mathbb{F}_q^*)^{|\mathcal{S}|}$. Moreover, we have that*

$$f(a_1, \dots, a_r) = \sum_{\mathcal{S} \subseteq [r]} f_{\mathcal{S}}(a_{\mathcal{S}}) \tag{10}$$

for every $a_1, \dots, a_r \in \mathbb{F}_q$.

Proof. First, let us prove that for every $\mathcal{S} \subseteq [r]$ the function $f_{\mathcal{S}}$ is supported on $(\mathbb{F}_q^*)^{|\mathcal{S}|}$. Pick any $a_{\mathcal{S}} \in \mathbb{F}_q^{|\mathcal{S}|} \setminus (\mathbb{F}_q^*)^{|\mathcal{S}|}$. Hence, there exists $k_0 \in \mathcal{S}$ such that $a_{k_0} = 0$. Therefore, by (9) we have that

$$\begin{aligned} f_{\mathcal{S}}(a_{\mathcal{S}}) &= \sum_{\mathcal{T} \subseteq \mathcal{S} \setminus \{k_0\}} (-1)^{|\mathcal{S} \setminus \mathcal{T}|} f(a_{(\mathcal{T})}) + \sum_{\{k_0\} \subseteq \mathcal{T} \subseteq \mathcal{S}} (-1)^{|\mathcal{S} \setminus \mathcal{T}|} f(a_{(\mathcal{T})}) \\ &= \sum_{\mathcal{T} \subseteq \mathcal{S} \setminus \{k_0\}} (-1)^{|\mathcal{S} \setminus \mathcal{T}|} f(a_{(\mathcal{T})}) - \sum_{\mathcal{T}' \subseteq \mathcal{S} \setminus \{k_0\}} (-1)^{|\mathcal{S} \setminus \mathcal{T}'|} f(a_{(\mathcal{T}')}) = 0, \end{aligned}$$

where we used the fact that each set $\mathcal{T}$ satisfying $\{k_0\} \subseteq \mathcal{T} \subseteq \mathcal{S}$ can be written in a unique way as $\mathcal{T} = \mathcal{T}' \cup \{k_0\}$ with $\mathcal{T}' \subseteq \mathcal{S} \setminus \{k_0\}$. The claim is proven.

Let us prove (10). From (9) and (8), we get that

$$\begin{aligned} \sum_{\mathcal{S} \subseteq [r]} f_{\mathcal{S}}(a_{\mathcal{S}}) &= \sum_{\mathcal{S} \subseteq [r]} \sum_{\mathcal{T} \subseteq \mathcal{S}} (-1)^{|\mathcal{S} \setminus \mathcal{T}|} f(a_{(\mathcal{T})}) = \sum_{\mathcal{T} \subseteq [r]} f(a_{(\mathcal{T})}) \sum_{\mathcal{T} \subseteq \mathcal{S} \subseteq [r]} (-1)^{|\mathcal{S} \setminus \mathcal{T}|} \\ &= \sum_{\mathcal{T} \subseteq [r]} f(a_{(\mathcal{T})}) \sum_{\mathcal{S}' \subseteq [r] \setminus \mathcal{T}} (-1)^{|\mathcal{S}'|} = f(a_1, \dots, a_r), \end{aligned}$$

where we wrote $\mathcal{S} = \mathcal{S}' \cup \mathcal{T}$. The proof is complete. □

[1] We normalize the Fourier transform by the factor $(q-1)^{-t}$ because later this simplifies some formulas.

3.3. **Möbius–Fourier inversion formula.** We can combine the results of Sections 3.1 and 3.2 to obtain a *Möbius–Fourier inversion formula*.

Lemma 3.2. *Let $f\colon \mathbb{F}_q^r \to \mathbb{C}$. Then we have that*

$$f(a_1,\dots,a_r) = \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}}(\chi_{\mathcal{S}}) \prod_{k\in\mathcal{S}} \chi_k(a_k),$$

for every $a_1,\dots,a_r \in \mathbb{F}_q$.

Proof. The claim easily follows from the Fourier inversion formula (7) and Lemma 3.1. □

For every function $f\colon \mathbb{F}_q^r \to \mathbb{C}$ and for every $\mathcal{S}\subseteq[r]$, let $f_{(\mathcal{S})}\colon \mathbb{F}_q^{|\mathcal{S}|} \to \mathbb{C}$ be the function defined by $f_{(\mathcal{S})}(a_{\mathcal{S}}) := f(a_{(\mathcal{S})})$ for each $a_{\mathcal{S}} \in \mathbb{F}_q^{|\mathcal{S}|}$.

Lemma 3.3. *Let $f\colon \mathbb{F}_q^r \to \mathbb{C}$ and $\mathcal{S}\subseteq[r]$. Then we have that*

$$\widehat{f_{\mathcal{S}}}(\chi_{\mathcal{S}}) = \sum_{\{\chi_k\neq\chi_0 : k\in\mathcal{S}\}\subseteq\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}\setminus\mathcal{T}|} \widehat{f_{(\mathcal{T})}}(\chi_{\mathcal{T}}),$$

for every $\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}$.

Proof. From (6) and (9), we get that

$$\begin{aligned}
\widehat{f_{\mathcal{S}}}(\chi_{\mathcal{S}}) &= \frac{1}{(q-1)^{|\mathcal{S}|}} \sum_{a_{\mathcal{S}}\in\mathbb{F}_q^{|\mathcal{S}|}} f_{\mathcal{S}}(a_{\mathcal{S}}) \prod_{k\in\mathcal{S}} \overline{\chi_k}(a_k) \\
&= \frac{1}{(q-1)^{|\mathcal{S}|}} \sum_{a_{\mathcal{S}}\in\mathbb{F}_q^{|\mathcal{S}|}} \sum_{\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}\setminus\mathcal{T}|} f(a_{(\mathcal{T})}) \prod_{k\in\mathcal{S}} \overline{\chi_k}(a_k) \\
&= \sum_{\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}\setminus\mathcal{T}|} \left(\frac{1}{(q-1)^{|\mathcal{T}|}} \sum_{a_{\mathcal{T}}\in\mathbb{F}_q^{|\mathcal{T}|}} f_{(\mathcal{T})}(a_{\mathcal{T}}) \prod_{k\in\mathcal{T}} \overline{\chi_k}(a_k) \right) \\
&\qquad \cdot \left(\frac{1}{(q-1)^{|\mathcal{S}\setminus\mathcal{T}|}} \sum_{a_{\mathcal{S}\setminus\mathcal{T}}\in\mathbb{F}_q^{|\mathcal{S}\setminus\mathcal{T}|}} \prod_{k\in\mathcal{S}\setminus\mathcal{T}} \overline{\chi_k}(a_k) \right).
\end{aligned} \tag{11}$$

Furthermore, for every $\mathcal{U}\subseteq[r]$, we have that

$$\sum_{a_U\in\mathbb{F}_q^{|\mathcal{U}|}} \prod_{k\in\mathcal{U}} \overline{\chi_k}(a_k) = \prod_{k\in\mathcal{U}} \left(\sum_{a\in\mathbb{F}_q} \overline{\chi_k}(a) \right) = (q-1)^{|\mathcal{U}|}\, \mathbb{1}[\chi_k = \chi_0 \text{ for each } k\in\mathcal{U}], \tag{12}$$

where we employed the orthogonality relation (5). At this point, the claim follows by combining (6), (11), and (12). □

3.4. **Some Fourier transforms.** For every $a\in\mathbb{F}_q$, define the function $f^{(a)}\colon \mathbb{F}_q^r \to \mathbb{C}$ by

$$f^{(a)}(a_1,\dots,a_r) = \mathbb{1}\left[\sum_{k=1}^r a_k = a \right],$$

for every $a_1,\dots,a_r \in \mathbb{F}_q^r$.

Furthermore, let $\chi_{\mathbf{0}}$ denote a tuple $(\chi_0,\dots,\chi_0)$, where the length will be always clear from the context.

Lemma 3.4. *For every $a\in\mathbb{F}_q$ and $\mathcal{T}\subseteq[r]$, we have that*

$$\widehat{f^{(a)}_{(\mathcal{T})}}(\chi_{\mathbf{0}}) = \frac{1}{q} - \frac{\gamma_a(q)}{(1-q)^{|\mathcal{T}|}}.$$

Proof. This is essentially the evaluation of a generalized Jacobi sum of trivial characters, which is a well-known subject (see, e.g., [4, Theorem 6.1.35]), but we include the details for completeness.

First, from (4) it follows that

$$\sum_{a_{\mathcal{T}}\in(\mathbb{F}_q^*)^{|\mathcal{T}|}}\prod_{k\in\mathcal{T}}\psi(a_k)=\prod_{k\in\mathcal{T}}\left(\sum_{a\in\mathbb{F}_q^*}\psi(a)\right)=\begin{cases}(q-1)^{|\mathcal{T}|} & \text{if } \psi=\psi_0;\\ (-1)^{|\mathcal{T}|} & \text{if } \psi\neq\psi_0;\end{cases} \tag{13}$$

for every $\psi\in\widehat{\mathbb{F}_q}$. Then, from (6), (2), and (13), we get that

$$\begin{aligned}\widehat{f_{(\mathcal{T})}^{(a)}}(\chi_{\mathbf{0}})&=\frac{1}{(q-1)^{|\mathcal{T}|}}\sum_{a_{\mathcal{T}}\in\mathbb{F}_q^{|\mathcal{T}|}}f_{(\mathcal{T})}^{(a)}(a_{\mathcal{T}})\prod_{k\in\mathcal{T}}\overline{\chi_0}(a_k)=\frac{1}{(q-1)^{|\mathcal{T}|}}\sum_{a_{\mathcal{T}}\in(\mathbb{F}_q^*)^{|\mathcal{T}|}}f_{(\mathcal{T})}^{(a)}(a_{\mathcal{T}})\\
&=\frac{1}{(q-1)^{|\mathcal{T}|}}\sum_{a_{\mathcal{T}}\in(\mathbb{F}_q^*)^{|\mathcal{T}|}}\mathbb{1}\left[\sum_{k\in\mathcal{T}}a_k=a\right]=\frac{1}{(q-1)^{|\mathcal{T}|}}\sum_{a_{\mathcal{T}}\in(\mathbb{F}_q^*)^{|\mathcal{T}|}}\frac{1}{q}\sum_{\psi\in\widehat{\mathbb{F}_q}}\psi\left(\sum_{k\in\mathcal{T}}a_k-a\right)\\
&=\frac{1}{q(q-1)^{|\mathcal{T}|}}\sum_{\psi\in\widehat{\mathbb{F}_q}}\sum_{a_{\mathcal{T}}\in(\mathbb{F}_q^*)^{|\mathcal{T}|}}\prod_{k\in\mathcal{T}}\psi(a_k)\,\overline{\psi}(a)=\frac{1}{q}+\frac{1}{q(1-q)^{|\mathcal{T}|}}\sum_{\psi\in\widehat{\mathbb{F}_q}\setminus\{\psi_0\}}\overline{\psi}(a)\\
&=\frac{1}{q}+\frac{1}{q(1-q)^{|\mathcal{T}|}}\left(\sum_{\psi\in\widehat{\mathbb{F}_q}}\overline{\psi}(a)-1\right)=\frac{1}{q}-\frac{\gamma_a(q)}{(1-q)^{|\mathcal{T}|}},\end{aligned}$$

since $\gamma_a(q)=q^{-1}-\mathbb{1}[a=0]$. The proof is complete. □

Lemma 3.5. *For every $a\in\mathbb{F}_q$ and $\mathcal{S}\subseteq[r]$, we have that*

$$\widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathbf{0}})=\frac{\mathbb{1}[\mathcal{S}=\varnothing]}{q}-\gamma_a(q)\left(\frac{1}{q}-1\right)^{-|\mathcal{S}|}.$$

Proof. By Lemma 3.3 and Lemma 3.4, we have that

$$\begin{aligned}\widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathbf{0}})&=\sum_{\mathcal{T}\subseteq\mathcal{S}}(-1)^{|\mathcal{S}\setminus\mathcal{T}|}\widehat{f_{(\mathcal{T})}^{(a)}}(\chi_{\mathbf{0}})=\sum_{\mathcal{T}\subseteq\mathcal{S}}(-1)^{|\mathcal{S}\setminus\mathcal{T}|}\left(\frac{1}{q}-\frac{\gamma_a(q)}{(1-q)^{|\mathcal{T}|}}\right)\\
&=\frac{1}{q}\sum_{\mathcal{T}\subseteq\mathcal{S}}(-1)^{|\mathcal{S}\setminus\mathcal{T}|}-\gamma_a(q)\sum_{\mathcal{T}\subseteq\mathcal{S}}(-1)^{|\mathcal{S}\setminus\mathcal{T}|}(1-q)^{-|\mathcal{T}|}\\
&=\frac{\mathbb{1}[\mathcal{S}=\varnothing]}{q}-\gamma_a(q)\left(\frac{1}{q}-1\right)^{-|\mathcal{S}|},\end{aligned}$$

where we used (8) and the more general fact that

$$\sum_{\mathcal{A}\subseteq\mathcal{B}}s^{|\mathcal{B}\setminus\mathcal{A}|}\,t^{|\mathcal{A}|}=(s+t)^{|\mathcal{B}|}$$

for every finite set $\mathcal{B}$ and for all real numbers s and t. □

4. Further preliminaries

For every field $\mathbb{K}$, let $\mathbb{K}^{m\times n}$ be the vector space of $m\times n$ matrices over $\mathbb{K}$, and let $\mathbb{K}^{m\times n,r}$ be the set of $m\times n$ rank-r matrices over $\mathbb{K}$. The next lemma regards the *full-rank factorization* of matrices and it is well known (cf. [5, Theorem 2]).

Lemma 4.1. *Let $\mathbb{K}$ be a field. For every $\mathbf{N}\in\mathbb{K}^{m\times n,r}$ there exist $\mathbf{X}_0\in\mathbb{K}^{m\times r,r}$ and $\mathbf{Y}_0\in\mathbb{K}^{r\times n,r}$ such that $\mathbf{N}=\mathbf{X}_0\mathbf{Y}_0$. Moreover, if $\mathbf{N}=\mathbf{X}\mathbf{Y}$ for some $\mathbf{X}\in\mathbb{K}^{m\times r}$ and $\mathbf{Y}\in\mathbb{K}^{r\times n}$, then there exists $\mathbf{R}\in\mathbb{K}^{r\times r,r}$ such that $\mathbf{X}=\mathbf{X}_0\mathbf{R}$ and $\mathbf{Y}=\mathbf{R}^{-1}\mathbf{Y}_0$.*

Proof. See, e.g., [6, Lemma 2.1]. There the second part of the lemma is stated with $\mathbf{X} \in \mathbb{K}^{m\times r,r}$ and $\mathbf{Y} \in \mathbb{K}^{r\times n,r}$ instead of $\mathbf{X} \in \mathbb{K}^{m\times r}$ and $\mathbf{Y} \in \mathbb{K}^{r\times n}$. However, if $\mathbf{X} \in \mathbb{K}^{m\times r}$ and $\mathbf{Y} \in \mathbb{K}^{r\times n}$ satisfy $\mathbf{XY} \in \mathbb{K}^{m\times n,r}$, then $\mathbf{X} \in \mathbb{K}^{m\times r,r}$ and $\mathbf{Y} \in \mathbb{K}^{r\times n,r}$. Therefore, the two versions are equivalent. □

Lemma 4.2. *Let $\mathbf{M} \in \mathbb{F}_q^{m\times n,r}$, $\mathbf{X} \in \mathbb{F}_q^{m\times r}$, and $\mathbf{Y} \in \mathbb{F}_q^{r\times n}$ be independent random matrices uniformly distributed in their respective spaces. Then we have that*

$$\sum_{\mathbf{N}\in\mathbb{F}_q^{m\times n}} \big|\mathbb{P}\big[\mathbf{XY}=\mathbf{N}\big]-\mathbb{P}\big[\mathbf{M}=\mathbf{N}\big]\big| \to 0, \tag{14}$$

as $m,n\to+\infty$ and r is fixed.

Proof. It is well-known (see, e.g., [3, Formula 3]) that

$$|\mathbb{F}_q^{s\times t,r}| = \prod_{i=0}^{r-1}\frac{(q^s-q^i)(q^t-q^i)}{q^r-q^i}, \tag{15}$$

for all integers $s,t,r>0$ with $r\le\min(s,t)$.

Furthermore, we have that

$$\frac{\prod_{i=0}^{r-1}(q^m-q^i)(q^n-q^i)}{q^{mr}\cdot q^{rn}} = \prod_{i=0}^{r-1}\frac{(q^m-q^i)(q^n-q^i)}{q^m\cdot q^n} = \prod_{i=0}^{r-1}(1-q^{i-m})(1-q^{i-n}) \to 1. \tag{16}$$

as $m,n\to+\infty$ and r is fixed.

Let us split the sum in (14) into three sums $\Sigma_{(<)}$, $\Sigma_{(=)}$, $\Sigma_{(>)}$ according to the rank of $\mathbf{N}$ being less than, equal to, or greater than r, respectively. We have to prove that, in the aforementioned limit, each of these sums goes to zero.

For every matrix $\mathbf{Z}$ over $\mathbb{F}_q$, let $\mathrm{rk}(\mathbf{Z})$ denote the rank of $\mathbf{Z}$. From (15) and (16), we get that

$$\begin{aligned}\Sigma_{(<)} &= \sum_{\substack{\mathbf{N}\in\mathbb{F}_q^{m\times n}\\ \mathrm{rk}(\mathbf{N})<r}} \mathbb{P}\big[\mathbf{XY}=\mathbf{N}\big] = \mathbb{P}\big[\mathrm{rk}(\mathbf{XY})<r\big] = 1-\mathbb{P}[\mathbf{X}\in\mathbb{F}_q^{m\times r,r}]\,\mathbb{P}[\mathbf{Y}\in\mathbb{F}_q^{r\times n,r}]\\ &= 1-\frac{|\mathbb{F}_q^{m\times r,r}||\mathbb{F}_q^{r\times n,r}|}{|\mathbb{F}_q^{m\times r}||\mathbb{F}_q^{r\times n}|} = 1-\frac{\prod_{i=0}^{r-1}(q^m-q^i)(q^n-q^i)}{q^{mr}\cdot q^{rn}} \to 0,\end{aligned}$$

where we used the fact that $\mathrm{rk}(\mathbf{XY})\le r$ with equality if and only if $\mathrm{rk}(\mathbf{X})=\mathrm{rk}(\mathbf{Y})=r$.

If $\mathbf{N}\in\mathbb{F}_q^{m\times n,r}$ then, by Lemma 4.1, there exist matrices $\mathbf{X}_0\in\mathbb{F}_q^{m\times r,r}$ and $\mathbf{Y}_0\in\mathbb{F}_q^{r\times n,r}$ such that $\mathbf{N}=\mathbf{X}_0\mathbf{Y}_0$. Moreover, again by Lemma 4.1, we have that $\mathbf{XY}=\mathbf{N}$ if and only if there exists $\mathbf{R}\in\mathbb{F}_q^{r\times r,r}$ such that $\mathbf{X}=\mathbf{X}_0\mathbf{R}$ and $\mathbf{Y}=\mathbf{R}^{-1}\mathbf{Y}_0$. Consequently, we have that

$$\mathbb{P}\big[\mathbf{XY}=\mathbf{N}\big] = \sum_{\mathbf{R}\in\mathbb{F}_q^{r\times r,r}} \mathbb{P}\big[\mathbf{X}=\mathbf{X}_0\mathbf{R}\big]\,\mathbb{P}\big[\mathbf{Y}=\mathbf{R}^{-1}\mathbf{Y}_0\big] = \frac{|\mathbb{F}_q^{r\times r,r}|}{|\mathbb{F}_q^{m\times r}||\mathbb{F}_q^{r\times n}|}.$$

Therefore, we get that

$$\begin{aligned}\Sigma_{(=)} &= \sum_{\mathbf{N}\in\mathbb{F}_q^{m\times n,r}} \big|\mathbb{P}\big[\mathbf{XY}=\mathbf{N}\big]-\mathbb{P}\big[\mathbf{M}=\mathbf{N}\big]\big| = \sum_{\mathbf{N}\in\mathbb{F}_q^{m\times n,r}} \left|\frac{|\mathbb{F}_q^{r\times r,r}|}{|\mathbb{F}_q^{m\times r}||\mathbb{F}_q^{r\times n}|}-\frac{1}{|\mathbb{F}_q^{m\times n,r}|}\right|\\ &= \left|\frac{|\mathbb{F}_q^{r\times r,r}||\mathbb{F}_q^{m\times n,r}|}{|\mathbb{F}_q^{m\times r}||\mathbb{F}_q^{r\times n}|}-1\right| = \left|\frac{\prod_{i=0}^{r-1}(q^m-q^i)(q^n-q^i)}{q^{mr}\cdot q^{rn}}-1\right| \to 0,\end{aligned}$$

where we employed (15) and (16).

Finally, since $\mathbf{XY}$ and $\mathbf{M}$ have rank not exceeding r, it follows that $\Sigma_{(>)}=0$. Thus all the three sums go to zero and the proof is complete. □

The next result is a version of Slutsky's lemma (cf. [9, Lemma 2.8]).

Lemma 4.3. *Let (U_n) and (V_n) be sequences of complex random variables such that $U_n \xrightarrow{d} U$ and $V_n \xrightarrow{d} c$ as $n \to +\infty$, where U is a random variable and c is a constant. Then we have that:*

(i) $U_n + V_n \xrightarrow{d} U + c$; and

(ii) $U_n V_n \xrightarrow{d} Uc$;

as $n \to +\infty$.

Proof. In [9, Lemma 2.8] the result is stated for real random variables. However, the proof can be easily adapted by identifying $\mathbb{C}$ with $\mathbb{R}^2$ and applying [9, Theorem 2.7] accordingly; noting that, with this identification, the addition and the multiplication of two complex numbers are continuous functions $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$. □

Lemma 4.4. *Let c_1, c_2 be real numbers, and let N_1, N_2 be independent normal random variables of expected values μ_1, μ_2 and variances σ_1^2, σ_2^2, respectively. Then $c_1 N_1 + c_2 N_2$ is a normal random variable of expected value $c_1\mu_1 + c_2\mu_2$ and variance $c_1^2\sigma_1^2 + c_2^2\sigma_2^2$.*

Proof. This fact is well known (cf. [8, Exercise 2.1.9]). □

5. Proof of Theorem 1.1

Let $m, n, r > 0$ be integers with $r \leq \min(m, n)$. Let $\mathbf{X} \in \mathbb{F}_q^{m\times r}$ and $\mathbf{Y} \in \mathbb{F}_q^{r\times n}$ be independent random matrices taken with uniform distribution from their respective spaces.

For every $\mathcal{S} \subseteq [r]$ and $\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}$, define the complex random variables

$$X_{\mathcal{S},\chi} := \sum_{i=1}^{m} \prod_{k\in\mathcal{S}} \chi_k(x_{i,k}) \quad \text{and} \quad Y_{\mathcal{S},\chi} := \sum_{j=1}^{n} \prod_{k\in\mathcal{S}} \chi_k(y_{k,j}), \tag{17}$$

and also the real random variables

$$Z := \sum_{i=1}^{m} \prod_{k=1}^{r} \big(1 - \chi_0(x_{i,k})\big) \quad \text{and} \quad W := \sum_{i=1}^{n} \prod_{k=1}^{r} \big(1 - \chi_0(y_{k,j})\big),$$

where $x_{i,j}$ and $y_{i,j}$ denote the entries of $\mathbf{X}$ and $\mathbf{Y}$, respectively.

The next two lemmas provide the expected values of $X_{\mathcal{S},\chi}$ and $Y_{\mathcal{S},\chi}$, and the expected values and the variances of Z and W.

Lemma 5.1. *For all $\mathcal{S} \subseteq [r]$ and $\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}$, we have that*

$$\mathbb{E}[X_{\mathcal{S},\chi}] = C(\chi_{\mathcal{S}}) \left(1 - \frac{1}{q}\right)^{|\mathcal{S}|} m \quad \textit{and} \quad \mathbb{E}[Y_{\mathcal{S},\chi}] = C(\chi_{\mathcal{S}}) \left(1 - \frac{1}{q}\right)^{|\mathcal{S}|} n,$$

where

$$C(\chi_{\mathcal{S}}) := \mathbb{1}[\,\chi_k = \chi_0 \textit{ for each } k \in \mathcal{S}\,].$$

Proof. Fix $\chi \in \widehat{\mathbb{F}_q^*}$ and let $c \in \mathbb{F}_q$ be taken at random with uniform distribution. From (5) it follows that

$$\mathbb{E}[\chi(c)] = \frac{1}{q} \sum_{a\in\mathbb{F}_q} \chi(a) = \left(1 - \frac{1}{q}\right) \mathbb{1}[\chi = \chi_0].$$

Consequently, if $c_{\mathcal{S}} \in \mathbb{F}_q^{|\mathcal{S}|}$ is a random tuple taken with uniform distribution, then

$$\mathbb{E}\left[\prod_{k\in\mathcal{S}} \chi_k(c_k)\right] = \prod_{k\in\mathcal{S}} \mathbb{E}[\chi_k(c_k)] = C(\chi_{\mathcal{S}}) \left(1 - \frac{1}{q}\right)^{|\mathcal{S}|}.$$

At this point, the formulas for the expected values of $X_{\mathcal{S},\chi}$ and $Y_{\mathcal{S},\chi}$ follow by linearity. □

Lemma 5.2. *We have that*

$$\mathbb{E}[Z] = \frac{1}{q^r}m, \quad \mathbb{V}[Z] = \frac{1}{q^r}\left(1-\frac{1}{q^r}\right)m, \quad \mathbb{E}[W] = \frac{1}{q^r}n, \quad \mathbb{V}[W] = \frac{1}{q^r}\left(1-\frac{1}{q^r}\right)n.$$

Proof. The claim follows easily by noticing that Z and W are binomial random variables of m and n trials, respectively, and probability of success equal to q^{-r}. □

We can now prove a formula for $\mathrm{ct}_{\mathcal{A}}(\mathbf{XY})$, for every $\mathcal{A} \subseteq \mathbb{F}_q$.

Lemma 5.3. *For every $a \in \mathbb{F}_q$, we have that*

$$\sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \mathbb{E}[Y_{\mathcal{S},\chi}] X_{\mathcal{S},\chi} = \frac{1}{q}mn - \gamma_a(q)nZ, \tag{18}$$

$$\sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \mathbb{E}[X_{\mathcal{S},\chi}] Y_{\mathcal{S},\chi} = \frac{1}{q}mn - \gamma_a(q)mW, \tag{19}$$

$$\sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \mathbb{E}[X_{\mathcal{S},\chi}] \mathbb{E}[Y_{\mathcal{S},\chi}] = \left(\frac{1}{q} - \frac{\gamma_a(q)}{q^r}\right)mn. \tag{20}$$

Proof. From Lemma 5.1 and Lemma 3.5, it follows that

$$\begin{aligned}
\sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \mathbb{E}[Y_{\mathcal{S},\chi}] X_{\mathcal{S},\chi} &= n \sum_{\mathcal{S}\subseteq[r]} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathbf{0}}) \left(1-\frac{1}{q}\right)^{|\mathcal{S}|} X_{\mathcal{S},\chi_{\mathbf{0}}} \\
&= n \sum_{\mathcal{S}\subseteq[r]} \left(\frac{\mathbb{1}[\mathcal{S}=\varnothing]}{q} - \gamma_a(q)\left(\frac{1}{q}-1\right)^{-|\mathcal{S}|}\right)\left(1-\frac{1}{q}\right)^{|\mathcal{S}|} X_{\mathcal{S},\chi_{\mathbf{0}}} \\
&= \frac{1}{q}mn - \gamma_a(q)n \sum_{\mathcal{S}\subseteq[r]} (-1)^{|\mathcal{S}|} X_{\mathcal{S},\chi_{\mathbf{0}}},
\end{aligned}$$

since $X_{\varnothing,\chi_{\mathbf{0}}} = m$. Furthermore, from (17), we have that

$$\begin{aligned}
\sum_{\mathcal{S}\subseteq[r]} (-1)^{|\mathcal{S}|} X_{\mathcal{S},\chi_{\mathbf{0}}} &= \sum_{\mathcal{S}\subseteq[r]} (-1)^{|\mathcal{S}|} \sum_{i=1}^{m} \prod_{k\in\mathcal{S}} \chi_0(x_{i,k}) = \sum_{i=1}^{m} \sum_{\mathcal{S}\subseteq[r]} \prod_{k\in\mathcal{S}} \big(-\chi_0(x_{i,k})\big) \\
&= \sum_{i=1}^{m} \prod_{k=1}^{r} \big(1-\chi_0(x_{i,k})\big) = Z,
\end{aligned}$$

and (18) follows. The proof of (19) proceeds similarly.

Finally, taking the expected value of both sides of (18), and employing Lemma 5.2, we obtain (20). □

Lemma 5.4. *For every $\mathcal{A} \subseteq \mathbb{F}_q$, we have that*

$$\begin{aligned}
\mathrm{ct}_{\mathcal{A}}(\mathbf{XY}) = \mu_{\mathcal{A}}(q,m,n) &+ \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \sum_{a\in\mathcal{A}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \big(X_{\mathcal{S},\chi} - \mathbb{E}[X_{\mathcal{S},\chi}]\big)\big(Y_{\mathcal{S},\chi} - \mathbb{E}[Y_{\mathcal{S},\chi}]\big) \\
&- \gamma_{\mathcal{A}}(q)n\big(Z - \mathbb{E}[Z]\big) - \gamma_{\mathcal{A}}(q)m\big(W - \mathbb{E}[W]\big).
\end{aligned}$$

Proof. Let $a \in \mathbb{F}_q$. From Lemma 3.2 and (17), we have that

$$\begin{aligned}
\mathrm{ct}_{\{a\}}(\mathbf{XY}) &= \sum_{i=1}^{m}\sum_{j=1}^{n} \mathbb{1}\left[\sum_{k=1}^{r} x_{i,k}y_{k,j} = a\right] = \sum_{i=1}^{m}\sum_{j=1}^{n} f^{(a)}(x_{i,1}y_{1,j},\dots,x_{i,r}y_{r,j}) \\
&= \sum_{i=1}^{m}\sum_{j=1}^{n} \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}} \in \widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \prod_{k\in\mathcal{S}} \chi_k(x_{i,k}y_{k,j})
\end{aligned}$$

$$= \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) \left(\sum_{i=1}^{m}\prod_{k\in\mathcal{S}}\chi_k(x_{i,k})\right)\left(\sum_{j=1}^{n}\prod_{k\in\mathcal{S}}\chi_k(y_{k,j})\right)$$

$$= \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}}) X_{\mathcal{S},\chi} Y_{\mathcal{S},\chi}.$$

Then, from the identity

$$X_{\mathcal{S},\chi}Y_{\mathcal{S},\chi} = \big(X_{\mathcal{S},\chi}-\mathbb{E}[X_{\mathcal{S},\chi}]\big)\big(Y_{\mathcal{S},\chi}-\mathbb{E}[Y_{\mathcal{S},\chi}]\big) + \mathbb{E}[Y_{\mathcal{S},\chi}]X_{\mathcal{S},\chi} + \mathbb{E}[X_{\mathcal{S},\chi}]Y_{\mathcal{S},\chi} - \mathbb{E}[Y_{\mathcal{S},\chi}]\mathbb{E}[X_{\mathcal{S},\chi}],$$

we get that

$$\begin{aligned}\mathrm{ct}_{\{a\}}(\mathbf{XY}) &= \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}})\big(X_{\mathcal{S},\chi}-\mathbb{E}[X_{\mathcal{S},\chi}]\big)\big(Y_{\mathcal{S},\chi}-\mathbb{E}[Y_{\mathcal{S},\chi}]\big)\\ &\quad+\sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}})\mathbb{E}[Y_{\mathcal{S},\chi}]X_{\mathcal{S},\chi} + \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}})\mathbb{E}[X_{\mathcal{S},\chi}]Y_{\mathcal{S},\chi}\\ &\quad-\sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \widehat{f_{\mathcal{S}}^{(a)}}(\chi_{\mathcal{S}})\mathbb{E}[Y_{\mathcal{S},\chi}]\mathbb{E}[X_{\mathcal{S},\chi}].\end{aligned}$$

At this point, the claim follows easily by applying Lemma 5.3 and Lemma 5.2, and by summing over all $a\in\mathcal{A}$. □

Fix a nonempty $\mathcal{A}\subsetneq\mathbb{F}_q$ and, for the sake of brevity, let

$$\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{N}) := \frac{\mathrm{ct}_{\mathcal{A}}(\mathbf{N})-\mu_{\mathcal{A}}(q,m,n)}{\sqrt{\sigma^2_{\mathcal{A}}(q,m,n)}}$$

for every $\mathbf{N}\in\mathbb{F}_q^{m\times n}$. Moreover, hereafter, let $m,n\to+\infty$.

Note that each of the complex random variables $X_{\mathcal{S},\chi}$ and $Y_{\mathcal{S},\chi}$ is the sum of independent identically distributed random variables with finite covariance matrices. Therefore, by the Central Limit Theorem in $\mathbb{R}^2$ (see, e.g., [1, Theorem 3.9.6]), we have that $\big(X_{\mathcal{S},\chi}-\mathbb{E}[X_{\mathcal{S},\chi}]\big)/\sqrt{m}$ and $\big(Y_{\mathcal{S},\chi}-\mathbb{E}[Y_{\mathcal{S},\chi}]\big)/\sqrt{n}$ converge in distribution to some complex normal random variables, which we call $X'_{\mathcal{S},\chi}$ and $Y'_{\mathcal{S},\chi}$, respectively.

Similarly, each of the real random variables Z and W is the sum of independent identically distributed random variables. Hence, it follows from the Central Limit Theorem (in $\mathbb{R}$) that $\big(Z-\mathbb{E}[Z]\big)/\sqrt{\mathbb{V}[Z]}$ and $\big(W-\mathbb{E}[W]\big)/\sqrt{\mathbb{V}[W]}$ converge in distribution to standard normal random variables, which we call Z' and W', respectively.

From Lemma 5.4 and Lemma 5.2, it follows that

$$\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{XY}) = \sum_{\mathcal{S}\subseteq[r]} \sum_{\chi_{\mathcal{S}}\in\widehat{\mathbb{F}_q^*}^{|\mathcal{S}|}} \frac{c_{\mathcal{A},\mathcal{S},\chi}(q)}{\sqrt{m+n}} X'_{\mathcal{S},\chi}Y'_{\mathcal{S},\chi} - \frac{Z'}{\sqrt{1+m/n}} - \frac{W'}{\sqrt{1+n/m}}, \tag{21}$$

where each $c_{\mathcal{A},\mathcal{S},\chi}(q)$ depends only on $\mathcal{A}$, $\mathcal{S}$, $\chi_{\mathcal{S}}$, q, r, and not on m and n.

Since $X'_{\mathcal{S},\chi}$ and $Y'_{\mathcal{S},\chi}$ are independent, their product converges in distribution to $\widetilde{X}_{\mathcal{S},\chi}\widetilde{Y}_{\mathcal{S},\chi}$. Therefore, from Lemma 4.3(ii), we get that each term of the double sum in (21) converges in distribution to the constant 0. Consequently, by Lemma 4.3(i), the double sum in (21) converges in distribution to the constant 0.

Since $\widetilde{Z}$ and $\widetilde{W}$ are independent, from Lemma 4.4 it follows that

$$U := -\frac{\widetilde{Z}}{\sqrt{1+m/n}} - \frac{\widetilde{W}}{\sqrt{1+n/m}}$$

is a standard normal random variable.

Moreover, from $Z' \xrightarrow{d} \widetilde{Z}$, $W' \xrightarrow{d} \widetilde{W}$, and the fact that $1/\sqrt{1+m/n}$ and $1/\sqrt{1+n/m}$ belong to $(0,1)$, we get easily that

$$\frac{\widetilde{Z}-Z'}{\sqrt{1+m/n}} \xrightarrow{d} 0 \quad \text{and} \quad \frac{\widetilde{W}-W'}{\sqrt{1+n/m}} \xrightarrow{d} 0.$$

Therefore, Lemma 4.3(i) yields that

$$-\frac{Z'}{\sqrt{1+m/n}} - \frac{W'}{\sqrt{1+n/m}} = U + \frac{\widetilde{Z}-Z'}{\sqrt{1+m/n}} + \frac{\widetilde{W}-W'}{\sqrt{1+n/m}} \xrightarrow{d} U.$$

From a last application of Lemma 4.3(i) we get that $\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{XY})$ converges in distribution to U.

Let $\mathbf{M}$ be a random matrix taken with uniform distribution from $\mathbb{F}_q^{m\times n,r}$. Thanks to Lemma 4.2, for every real number t, we have that

$$\begin{aligned}\big|\mathbb{P}[\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{M}) \le t] - \mathbb{P}[\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{XY}) \le t]\big| &= \Big| \sum_{\substack{\mathbf{N}\in\mathbb{F}_q^{m\times n}\\ \widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{N})\le t}} \big(\mathbb{P}[\mathbf{M}=\mathbf{N}] - \mathbb{P}[\mathbf{XY}=\mathbf{N}]\big)\Big| \\ &\le \sum_{\mathbf{N}\in\mathbb{F}_q^{m\times n}} \big|\mathbb{P}[\mathbf{XY}=\mathbf{N}] - \mathbb{P}[\mathbf{M}=\mathbf{N}]\big| \to 0.\end{aligned}$$

Consequently, we get that $\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{M})$ and $\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{XY})$ have the same limiting distribution (if it exists). Since we already proved that $\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{XY})$ converges in distribution to a standard normal random variable, we get that $\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{M})$ also converges in distribution to a standard normal random variable.

The proof of Theorem 1.1 is complete.

Remark 5.1. A crucial part of the proof is the fact that, since r is fixed, the double sum in (21) has a fixed number of terms, and so it is possible to prove that it converges in distribution to the constant 0 without having to closely inspect its terms. If one let $r \to +\infty$, in a way controlled by m and n, then it seems likely that understanding the behavior of $\widetilde{\mathrm{ct}}_{\mathcal{A}}(\mathbf{XY})$ would require a more detailed study of the terms of the double sum in (21), since the number of such terms grows with r.

References

[1] R. Durrett, *Probability—theory and examples*, fifth ed., Cambridge Series in Statistical and Probabilistic Mathematics, vol. 49, Cambridge University Press, Cambridge, 2019.

[2] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994.

[3] T. Migler, K. E. Morrison, and M. Ogle, *How much does a matrix of rank k weigh?*, Math. Mag. **79** (2006), no. 4, 262–271.

[4] G. L. Mullen and D. Panario (eds.), *Handbook of finite fields*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, 2013.

[5] R. Piziak and P. L. Odell, *Full Rank Factorization of Matrices*, Math. Mag. **72** (1999), no. 3, 193–201.

[6] C. Sanna, *A note on the distribution of weights of fixed-rank matrices over the binary field*, Finite Fields Appl. **87** (2023), Paper No. 102157, 7.

[7] R. P. Stanley, *Enumerative combinatorics. Volume 1*, second ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.

[8] T. Tao, *Topics in random matrix theory*, Graduate Studies in Mathematics, vol. 132, American Mathematical Society, Providence, RI, 2012.

[9] A. W. van der Vaart, *Asymptotic statistics*, Cambridge Series in Statistical and Probabilistic Mathematics, vol. 3, Cambridge University Press, Cambridge, 1998.

Department of Mathematical Sciences, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
Email address: carlo.sanna@polito.it