mathematics

MDPI

Article

On the Maximum Probability of Full Rank of Random Matrices over Finite Fields

Marija Delić and Jelena Ivetić *

Faculty of Technical Sciences, University of Novi Sad, 21000 Novi Sad, Serbia; marijadelic@uns.ac.rs
* Correspondence: jelenaivetic@uns.ac.rs; Tel.: +381-214852280

Abstract: The problem of determining the conditions under which a random rectangular matrix is of full rank is a fundamental question in random matrix theory, with significant implications for coding theory, cryptography, and combinatorics. In this paper, we study the probability of full rank for a $K \times N$ random matrix over the finite field $\mathbb{F}_q$, where q is a prime power, under the assumption that the rows of the matrix are sampled independently from a probability distribution $\mathcal{P}$ over $\mathbb{F}_q^N$. We demonstrate that the probability of full rank attains a local maximum when the distribution $\mathcal{P}$ is uniform over $\mathbb{F}_q^N \setminus \{0\}$, for any $K \leqslant N$ and prime power q. Moreover, we establish that this local maximum is also a global maximum in the special case where $K = 2$. These results highlight the optimality of the uniform distribution in maximizing full rank and represent a significant step toward solving the broader problem of maximizing the probability of full rank for random matrices over finite fields.

Keywords: random matrices; probability of full rank; linear independence; finite fields; uniform distribution; local maximum

MSC: 15B52; 15A03; 60B20

1. Introduction

Random matrices have long been a cornerstone of mathematical research, offering a rich interplay between theoretical challenges and practical applications across various disciplines, including mathematical physics, theoretical computer science, and communication engineering. One of the most studied problems in this domain is the probability of non-singularity for square matrices, or, more generally, the probability of full rank for rectangular matrices. This is a question intimately tied to the structural properties of matrices and their utility in fields such as coding theory and cryptography. Closely related is the rank distribution of random matrices, particularly over finite fields, which plays a crucial role in understanding matrix behavior and designing applications in combinatorics and number theory. The study of random matrices over finite fields has its roots in foundational work such as Balakin's investigation of rank distributions [1], which provided an early probabilistic framework for analyzing these matrices. This was followed by significant contributions exploring various properties, including the rank of sparse random matrices [2], asymptotic probabilities of invertibility [3], and combinatorial methods for assessing distributions over finite fields [4,5]. Additionally, works like those by Blake and Studholme [6] have examined practical applications of these matrices, broadening their relevance to engineering and computer science.

Further advancements have refined these ideas, with key studies addressing singularity probabilities [7,8] and their asymptotic behaviors [9]. Significant contributions to

check for updates

Academic Editor: Alexander Tikhomirov

Received: 30 December 2024
Revised: 24 January 2025
Accepted: 29 January 2025
Published: 6 February 2025

Citation: Delić, M.; Ivetić, J. On the Maximum Probability of Full Rank of Random Matrices over Finite Fields. *Mathematics* **2025**, *13*, 540. https://doi.org/10.3390/math13030540

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

the study of discrete integer matrices have included [10], which introduces advanced techniques for singularity analysis, and [11–13], which analyzed singularity probabilities of Bernoulli matrices. The use of Stein's method for rank analysis [14] and combinatorial approaches to restricted random matrices [9,15] has deepened the theoretical understanding of structural properties. Meanwhile, recent studies have focused on sparse and binary matrices [16,17] and the universality of characteristic polynomials [18–20]. These results not only provide critical insights into the underlying properties of random matrices, but also extend their applicability to practical challenges in coding theory, combinatorial optimization, and secure communications.

One of the central questions in the study of random matrices over finite fields is understanding the conditions under which a matrix is most likely to be of full rank. As this property of a matrix is equivalent to the linear independence of its row vectors, identifying the row vector distributions that maximize this probability remains an important and open problem. In this paper, we create two key contributions to this problem. First, we demonstrate that the probability of full rank reaches a local maximum when the row vectors follow a discrete uniform distribution. Second, we prove that this local maximum is, in fact, a global maximum in the special case where the matrix consists of only two rows. These findings not only provide a deeper understanding of the relationship between row distributions and matrix invertibility, but also represent a step forward in addressing the broader problem of maximizing the probability of full rank of random matrices over finite fields.

2. Preliminaries

Let q be a prime power, i.e., $q = p^n$ for some prime p and positive integers n.

Definition 1 ([21]). *For a prime p, let $\mathbb{F}_p$ be the set $\{0, 1, \ldots, p-1\}$ of integers, and let $\varphi : \mathbb{Z}/(p) \to \mathbb{F}_p$ be the mapping defined by $\varphi([a]) = a$ for $a = 0, 1, \ldots, p-1$. Then, $\mathbb{F}_p$, endowed with the field structure induced by φ, is a finite field, called the Galois field of order p.*

For any prime power $q = p^n$, where $n \geq 1$, the finite field $\mathbb{F}_q$ is defined as a field with q elements. It is the unique (up to isomorphism) splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$, meaning every element of $\mathbb{F}_q$ is a root of $x^q - x$, and the field has dimension n as a vector space over its prime subfield $\mathbb{F}_p$.

If the rank of a matrix is the same as its smaller dimension, we say the matrix is of full rank. If a matrix is not of full rank, we say it is rank deficient. A full rank matrix that is square is called non-singular [22].

Let $M^*_{q;K,N} \subseteq \mathbb{F}_q^{K \times N}$ denote the set of all full rank $K \times N$ matrices over $\mathbb{F}_q$.

For notational simplicity, we will sometimes refer to it by M^*, understanding that K, N, and q are fixed. The cardinality of $M^*_{q;K,N}$ is given in [23] as:

$$\left|M^*_{q;K,N}\right| = \binom{N}{K}_q \cdot \sum_{j=0}^{K} (-1)^{K-j} \binom{K}{j}_q q^{jN+\binom{K-j}{2}} \tag{1}$$

where

$$\binom{N}{K}_q = \frac{(q^N-1)(q^{N-1}-1)\cdots(q^{N-K+1}-1)}{(q^K-1)(q^{K-1}-1)\cdots(q-1)} \tag{2}$$

are Gaussian numbers (or q-binomial coefficients).

Let $\mathbb{F}_q^N$ denote the set of vectors with a length of N over the field $\mathbb{F}_q$ and let $\mathcal{P}$ be some probability distribution over $\mathbb{F}_q^N \setminus \{0\}$. We exclude the zero vector at the very beginning, i.e., fix its probability to zero, because that will clearly increase the probability of a matrix

being full rank. Now, consider a random matrix obtained by choosing K vectors, $K \leq N$, from $\mathbb{F}_q^N \setminus \{0\}$ independently and according to $\mathcal{P}$. Then, the probability that the obtained matrix is of full rank can be defined as

$$f_{q;K,N}(\mathcal{P}) \triangleq \sum_{(v_1,\ldots,v_K)\in M^*_{q;K,N}} \mathcal{P}(v_1)\cdots\mathcal{P}(v_K) \tag{3}$$

where $v_i \in \mathbb{F}_q^N \setminus \{0\}$. As with M^*, we will sometimes drop the indices q, K, N from the notation and simply write $f(\mathcal{P})$.

In the following section, we will prove that $f_{q;K,N}(\mathcal{P})$ is locally maximized when $\mathcal{P}$ is uniform, and that this is also a global maximum when $K = 2$.

3. Results

3.1. Ordering of Vectors in $\mathbb{F}_q^N \setminus \{0\}$

To facilitate the derivation, we impose an ordering on the set of $q^N - 1$ vectors in $\mathbb{F}_q^N \setminus \{0\}$ based on their equivalence classes under scalar multiplication. Specifically, consider a vector v and all its nonzero scalar multiples, of which there are exactly $q - 1$. If the probability distribution $\mathcal{P}$ assigns a total probability p to this equivalence class, then the value of $f(\mathcal{P})$ remains invariant, regardless of how p is distributed among the individual vectors within the class. This invariance arises from the fact that scalar multiples of row vectors do not influence the rank of the corresponding matrix.

For simplicity in the subsequent analysis, we assume that the probability distributions under consideration assign a probability of zero to all but one vector in each equivalence class. Consequently, we are left with $(q^N - 1)/(q - 1)$ linearly independent representatives, which we order as follows.

First, select any vector as v_0. Next, choose another vector, v_1, such that it is not a scalar multiple of v_0. Following this, consider the equivalence class of vectors within the $\text{span}(v_0, v_1) = \{av_0 + bv_1 \mid a, b \in \mathbb{F}_q\}$, excluding v_0 and v_1 themselves. This span contributes $q - 1$ linearly independent vectors. There are $q^2 - 1$ nonzero linear combinations of v_0 and v_1. Since we select one vector from each equivalence class, we divide by $q - 1$, which gives $(q^2 - 1)/(q - 1) - 2 = q - 1$. Here, we subtract 2 because v_0 and v_1 are excluded. These vectors are labeled as $v_2, \ldots, v_q$. Subsequently, select a vector v_{q+1} from outside $\text{span}(v_0, v_1)$, and repeat the process: identify the equivalence class of $q - 1$ vectors within $\text{span}(v_0, v_{q+1})$, label them, and proceed iteratively.

This procedure results in an ordered sequence: v_0, followed by clusters of q vectors corresponding to equivalence classes within spans involving v_0 and one additional vector, such as $\text{span}(v_0, v_1)$ and $\text{span}(v_0, v_{q+1})$, and so on. At the end, the total number of such clusters is $((q^N - 1)/(q - 1) - 1)/q = q^{N-2} + q^{N-3} + \cdots + q + 1$.

From this point forward, we assumed that $\mathcal{P} = (p_0, \ldots, p_{L-1})$ represents a probability distribution over the set of L equivalence classes of nonzero vectors under scalar multiplication. The number of these classes is given by

$$L = \frac{q^N - 1}{q - 1} = q^{N-1} + \ldots + q + 1, \tag{4}$$

and the representatives of these classes are pairwise linearly independent, and ordered in the described way.

3.2. Properties of $M^*_{q;K,N}$

We now present two statements regarding the set of all full rank $K \times N$ matrices over $\mathbb{F}_q$, which will be used in the proof of the main result.

Lemma 1. *Let $v_{i_1}, \ldots, v_{i_r} \in \mathbb{F}_q^N$. Let $M^*_{q;K,N}$ denote the set of all full rank $K \times N$ matrices over $\mathbb{F}_q$ and $M^*_{q;K,N}(v_{i_1}, \ldots, v_{i_r})$ the set of all full rank $K \times N$ matrices over $\mathbb{F}_q$ with the first r row vectors fixed to $v_{i_1}, \ldots, v_{i_r}$. Then,*

$$\left|M^*_{q;K,N}(v_{i_1}, \ldots, v_{i_r})\right| = \begin{cases} \frac{|M^*_{q;K,N}|}{|M^*_{q;r,N}|}, & \text{if } v_{i_1}, \ldots, v_{i_r} \text{ are linearly independent} \\ 0, & \text{otherwise.} \end{cases}$$

In particular, $|M^*_{q;K,N}(v_{i_1}, \ldots, v_{i_r})|$ does not depend on $v_{i_1}, \ldots, v_{i_r}$ as long as they are linearly independent.

Proof. If $v_{i_1}, \ldots, v_{i_r}$ are linearly dependent, then there are no full rank matrices with these row vectors and $|M^*_{q;K,N}(v_{i_1}, \ldots, v_{i_r})| = 0$. Suppose now that $v_{i_1}, \ldots, v_{i_r}$ are linearly independent, and let $w_{i_1}, \ldots, w_{i_r}$ be another set of linearly independent vectors over $\mathbb{F}_q$. We can complement both sets to obtain two bases of $\mathbb{F}_q^N$, $\mathcal{B}_1$ and $\mathcal{B}_2$. Consider a linear map from $\mathbb{F}_q^N$ to itself such that $\mathcal{B}_1$ is mapped to $\mathcal{B}_2$, and, in particular, v_{i_j} is mapped to w_{i_j}, $j \in \{1, \ldots, r\}$. This map can also be seen as a bijection between the space of all $K \times N$ full rank matrices with $v_{i_1}, \ldots, v_{i_r}$ as their first r row vectors and the space of all $K \times N$ full rank matrices with $w_{i_1}, \ldots, w_{i_r}$ as their first r row vectors. This implies that $|M^*_{q;K,N}(v_1, \ldots, v_r)| = |M^*_{q;K,N}(w_1, \ldots, w_r)|$. As the number of ways to choose the first r linearly independent row vectors is $|M^*_{q;r,N}|$, the claim follows. □

From (1) and Lemma 1 we have

$$\left|M^*_{q;K,N}(v_{i_1}, \ldots, v_{i_r})\right| = \frac{\sum_{j=0}^{K} (-1)^{K-j} \binom{K}{j}_q q^{jN+\binom{K-j}{2}}}{\sum_{j=0}^{r} (-1)^{r-j} \binom{r}{j}_q q^{jN+\binom{r-j}{2}}}, \tag{5}$$

whenever $v_{i_1}, \ldots, v_{i_r}$ are linearly independent.

Lemma 2. *$M^*_{q;K,N}$ is permutation invariant, that is, if $(v_{i_1}, \ldots, v_{i_K})^{\mathrm{T}} \in M^*_{q;K,N}$, then the matrices obtained by permuting the row vectors of $(v_{i_1}, \ldots, v_{i_K})^{\mathrm{T}}$ are also in $M^*_{q;K,N}$.*

Proof. This is straightforward—interchanging row vectors do not affect the rank. □

3.3. Local and Global Optimality of the Uniform Distribution

Our main result, which establishes the optimality of the uniform distribution for maximizing the probability of full rank for random matrices over the finite field, is stated in the following theorems. In the subsequent proofs, we use partitioning of vectors into L classes as described in Section 3.1, and the standard abbreviated notation p_i for $\mathcal{P}(v_i)$.

Theorem 1. *The function $f_{q;K,N}(\mathcal{P})$ is locally maximized when $\mathcal{P} = (p_0, \ldots, p_{L-1})$ is the uniform distribution over L classes of pairwise linearly independent vectors.*

Proof. Let us express the probability $f_{q;K,N}(\mathcal{P})$ from (3) in a more convenient form. Permutation invariance, together with the constraint $\sum_{i=0}^{L-1} p_i = 1$, gives

$$\begin{aligned} f(\mathcal{P}) &= \sum_{(v_{i_1}, v_{i_2}, \ldots, v_{i_K})^{\mathrm{T}} \in M^*} p_{i_1} \cdots p_{i_K} \\ &= K \cdot \sum_{(v_0, v_{i_2}, \ldots, v_{i_K})^{\mathrm{T}} \in M^*} \left(1 - \sum_{j=1}^{L-1} p_j\right) p_{i_2} \cdots p_{i_K} \quad + \sum_{\substack{(v_{i_1}, \ldots, v_{i_K})^{\mathrm{T}} \in M^* \\ i_s \neq 0}} p_{i_1} \cdots p_{i_K}. \end{aligned} \tag{6}$$

This is now a function of $L-1$ variables, $p_1, \ldots, p_{L-1}$. Its partial derivatives are:

$$\begin{aligned}\frac{\partial f(\mathcal{P})}{\partial p_\ell} = &- K \cdot \sum_{(v_0, v_{i_2}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_2} \cdots p_{i_K} \\ &+ K\left(1 - \sum_{j=1}^{L-1} p_j\right)(K-1) \cdot \sum_{(v_0, v_\ell, v_{i_3}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_3} \cdots p_{i_K} \\ &+ K \cdot \sum_{\substack{(v_\ell, v_{i_2}, \ldots, v_{i_K})^\intercal \in M^* \\ i_s \neq 0}} p_{i_2} \cdots p_{i_K}\end{aligned} \tag{7}$$

for $\ell \in \{1, \ldots, L-1\}$, where we again used permutation invariance of M^*.

Now let us check that $p_1 = \ldots = p_{L-1} = \frac{1}{L}$ is a stationary point. To this end, write the third summand in (7) as

$$\begin{aligned}&\sum_{\substack{(v_\ell, v_{i_2}, \ldots, v_{i_K})^\intercal \in M^* \\ i_s \neq 0}} p_{i_2} \cdots p_{i_K} \\ &= \sum_{(v_\ell, v_{i_2}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_2} \cdots p_{i_K} - (K-1) \cdot \sum_{(v_\ell, v_0, v_{i_3}, \ldots, v_{i_K})^\intercal \in M^*} \left(1 - \sum_{j=1}^{L-1} p_j\right) p_{i_3} \cdots p_{i_K}.\end{aligned} \tag{8}$$

By substituting (8) into (7), we obtain:

$$\frac{\partial f(\mathcal{P})}{\partial p_\ell} = K \cdot \left(\sum_{(v_\ell, v_{i_2}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_2} \cdots p_{i_K} - \sum_{(v_0, v_{i_2}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_2} \cdots p_{i_K} \right). \tag{9}$$

For $p_1 = \ldots = p_{L-1} = \frac{1}{L}$ this reduces to

$$\frac{\partial f(\mathcal{P})}{\partial p_\ell}\Big|_{p_1 = \ldots = p_{L-1} = \frac{1}{L}} = K \cdot L^{-(K-1)} \cdot (q-1)^{-(K-1)} \cdot \left(|M^*(v_\ell)| - |M^*(v_0)| \right) = 0 \tag{10}$$

where the last equality follows from Lemma 1. The factor $(q-1)^{-(K-1)}$ comes from the fact that only one out of $q-1$ vectors from each class is taken, so only a fraction of $(q-1)^{-(K-1)}$ of all full rank matrices have nonzero probability. Based on (9), one might think that any point with $p_1 = \ldots = p_{L-1}$ is stationary, but note that in the first summand in (9), the variable p_0 appears implicitly when $(v_\ell, v_0, v_{i_3}, \ldots, v_{i_K}) \in M^*$ and, therefore, its value must also be taken into consideration.

Now, to show that this stationary point in fact a maximum, we need to establish that the Hessian matrix of $f(\mathcal{P})$ is negative definite at $p_1 = \ldots = p_{L-1} = \frac{1}{L}$. We have

$$\begin{aligned}\frac{\partial^2 f(\mathcal{P})}{\partial p_\ell \, \partial p_r} = &- K(K-1) \cdot \sum_{(v_0, v_r, v_{i_3}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_3} \cdots p_{i_K} \\ &- K(K-1) \cdot \sum_{(v_0, v_\ell, v_{i_3}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_3} \cdots p_{i_K} \\ &+ K(K-1)\left(1 - \sum_{j=1}^{L-1} p_j\right)(K-2) \cdot \sum_{(v_0, v_\ell, v_r, v_{i_4}, \ldots, v_{i_K})^\intercal \in M^*} p_{i_4} \cdots p_{i_K} \\ &+ K(K-1) \cdot \sum_{\substack{(v_\ell, v_r, v_{i_3}, \ldots, v_{i_K})^\intercal \in M^* \\ i_s \neq 0}} p_{i_3} \cdots p_{i_K},\end{aligned} \tag{11}$$

for $\ell, r \in \{1, \ldots, L-1\}$. Writing the last term in a different form, similar to (8), this becomes

$$\frac{\partial^2 f(\mathcal{P})}{\partial p_\ell \, \partial p_r} = -K(K-1) \cdot \left(\sum_{(v_0, v_r, v_{i_3}, \ldots, v_{i_K})^{\mathrm{T}} \in M^*} p_{i_3} \cdots p_{i_K} + \sum_{(v_0, v_\ell, v_{i_3}, \ldots, v_{i_K})^{\mathrm{T}} \in M^*} p_{i_3} \cdots p_{i_K} - \sum_{(v_\ell, v_r, v_{i_3}, \ldots, v_{i_K})^{\mathrm{T}} \in M^*} p_{i_3} \cdots p_{i_K} \right). \tag{12}$$

Let $\mathbf{H}_{f(\mathcal{P})} = \left(\frac{\partial^2 f(\mathcal{P})}{\partial p_\ell \, \partial p_r} \right)\Big|_{p_1 = \ldots = p_{L-1} = \frac{1}{L}}$ denote the Hessian matrix of $f(\mathcal{P})$ evaluated at $p_1 = \ldots = p_{L-1} = \frac{1}{L}$. The evaluated elements of the matrix are:

$$H_{f(\mathcal{P})}(\ell, r) = -K(K-1) L^{-(K-2)} (q-1)^{-(K-2)} \cdot \left(|M^*(v_0, v_\ell)| + |M^*(v_0, v_r)| - |M^*(v_\ell, v_r)| \right). \tag{13}$$

Showing negative definiteness of the matrix $\mathbf{H}_{f(\mathcal{P})}$ is equivalent to showing positive definiteness of $\mathbf{T} = -\frac{L^{(K-2)}(q-1)^{(K-2)}}{K(K-1)} \mathbf{H}_{f(\mathcal{P})}$, with elements

$$T(\ell, r) = \left(|M^*(v_0, v_\ell)| + |M^*(v_0, v_r)| - |M^*(v_\ell, v_r)| \right)$$

from (13).

Now, let us analyze the values of $T(\ell, r)$. We distinguish two cases: $\ell = r$ and $\ell \neq r$. The first case entails that $|M^*(v_\ell, v_r)| = 0$ from Lemma 1, because the vectors are equal, thus linearly dependent. In the second case, vectors v_0, v_ℓ, and v_r are pairwise linearly independent, and from Lemma 1, we have that $|M^*(v_0, v_\ell)| = |M^*(v_0, v_r)| = |M^*(v_\ell, v_r)|$. Let us denote $|M^*(v_\ell, v_r)| = a$, then

$$T(\ell, r) = \begin{cases} 2a, & \ell = r \\ a, & \ell \neq r. \end{cases} \tag{14}$$

and

$$\mathbf{T} = \begin{bmatrix} 2a & a & a & \cdots & a \\ a & 2a & a & \cdots & a \\ a & a & 2a & \cdots & a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a & a & a & \cdots & 2a \end{bmatrix}. \tag{15}$$

Therefore, $\mathbf{T}$ is a sum of a constant matrix and a diagonal matrix, both with positive entries; therefore, it is positive definite (the first one is positive semi-definite and the second one is positive definite). This proves that $f(\mathcal{P})$ attains a local maximum when uniformly distributed, i.e., for $p_0 = p_1 = \ldots = p_{L-1} = \frac{1}{L}$. □

Corollary 1. *The function $f_{q;K,N}(\mathcal{P})$ is locally maximized when $\mathcal{P}$ is the uniform distribution over $\mathbb{F}_q^N \setminus \{0\}$.*

Proof. If $\mathcal{P}$ is uniformly distributed over the set of vectors from $\mathbb{F}_q^N \setminus \{0\}$, then it is also uniformly distributed over the set of L classes of vectors (see Section 3.1). Thus, we obtain the result using Theorem 1. □

Theorem 2. *The function $f_{q;2,N}(\mathcal{P})$ reaches the maximum when $\mathcal{P}$ is uniformly distributed over $\mathbb{F}_q^N \setminus \{0\}$. Consequently,*

$$\max_{\mathcal{P}} f_{q;2,N}(\mathcal{P}) = f(\mathcal{U}) = \frac{q^N - q}{q^N - 1}. \tag{16}$$

Proof. This is a special case of Theorem 1, for $K = 2$. In this case, using the partitioning of vectors into L classes, we can write

$$f(\mathcal{P}) = \sum_{(v_{i_1}, v_{i_2})^{\mathrm{T}} \in M^*} p_{i_1} p_{i_2} = \sum_{i=0}^{L-1} \sum_{\substack{j=0 \\ j \neq i}}^{L-1} p_i p_j = 2 \sum_{i=0}^{L-1} p_i \sum_{j=i+1}^{L-1} p_j. \tag{17}$$

The second equality is again due to the fact that we are considering only pairwise independent vectors without loss of generality, see Section 3.1. Note that the quantity on the right end of (17) is a symmetric polynomial of degree 2 in L variables, which is known to be a concave function [24]. Therefore, the local maximum obtained for $\mathcal{U} = \left(\frac{1}{L}, \ldots, \frac{1}{L}\right)$ is also a global maximum. Furthermore, from (17), we have

$$\begin{aligned} f(\mathcal{U}) &= 2 \sum_{i=0}^{L-1} p_i \sum_{j=i+1}^{L-1} p_j = 2 \sum_{i=0}^{L-1} \frac{1}{L} \sum_{j=i+1}^{L-1} \frac{1}{L} \\ &= \frac{2}{L^2} \sum_{i=0}^{L-1} \sum_{j=i+1}^{L-1} 1 = \frac{2}{L^2} \sum_{i=0}^{L-1} (L-1-i) \\ &= \frac{2}{L^2} \left(\sum_{i=0}^{L-1} (L-1) - \sum_{i=0}^{L-1} i \right) \\ &= \frac{2}{L^2} \left((L-1)L - \frac{(L-1)L}{2} \right) \\ &= \frac{2}{L^2} \cdot \frac{(L-1)L}{2} = \frac{L-1}{L} = \frac{q^N - q}{q^N - 1}, \end{aligned}$$

where L is defined in (4). □

4. Concluding Remarks

This paper is focused on one of the central questions in studying random matrices over finite fields—identifying the row vector distributions that maximize the probability of full rank. We have shown that this probability achieves a local maximum when the probability $\mathcal{P}$ is uniform over $\mathbb{F}_q^N \setminus \{0\}$, and further it is proved that this maximum is global in the case of matrices with two rows.

Building upon these findings, our future work will aim to generalize this result by proving that the uniform distribution achieves the global maximum for matrices of an arbitrary size. To this end, we will investigate the quasi-concavity of the probability function of full rank. Demonstrating quasi-concavity would allow us to confirm that the uniform distribution maximizes the probability by showing that any deviation from uniformity decreases the likelihood of full rank. This approach leverages the structural properties of the function, providing a systematic method to analyze and optimize row vector distributions beyond the specific case proved in this paper. Another interesting line of research would be to explore the geometric structure of the space of distributions as a manifold and its connection to the probability of full rank, drawing inspiration from foundational works such as [25,26].

Author Contributions: Conceptualization: M.D.; Methodology: M.D.; Validation: M.D. and J.I.; Formal Analysis: M.D. and J.I.; Writing—Original Draft: M.D.; Writing—Review and Editing: M.D. and J.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Ministry of Science, Technological Development and Innovation (Contract No. 451-03-65/2024-03/200156) and the Faculty of Technical Sciences, University

of Novi Sad through project "Scientific and Artistic Research Work of Researchers in Teaching and Associate Positions at the Faculty of Technical Sciences, University of Novi Sad" (No. 01-3394/1).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest within this paper.

References

1. Balakin, G.V. The distribution of the rank of random matrices over a finite field. *Theory Probab. Appl.* **1968**, *13*, 594–605. [CrossRef]
2. Blömer, J.; Karp, R.; Welzl, E. The rank of sparse random matrices over finite fields. *Random Struct. Algorithms* **1997**, *10*, 407–419. [CrossRef]
3. Charlap, L.S.; Rees, H.D.; Robbins, D.P. The asymptotic probability that a random biased matrix is invertible. *Discret. Math.* **1990**, *82*, 153–163. [CrossRef]
4. Cooper, C. On the rank of a random matrices. *Random Struct. Algorithms* **2000**, *16*, 209–232. [CrossRef]
5. Cooper, C. On the distribution of rank of a random matrix over a finite field. *Random Struct. Algorithms* **2000**, *17*, 197–212. [CrossRef]
6. Blake, I.F.; Studholme, C. Properties of Random Matrices and Applications. Available online: http://www.cs.toronto.edu/~cvs/coding/random_report.pdf (accessed on 28 December 2024).
7. Kahn, J.; Komlos, J. Singularity probabilities for random matrices over finite fields. *Singul. Probab. Random Matrices Over Finite Fields* **2001**, *10*, 137–157. [CrossRef]
8. Maples, K. Singularity of random matrices over finite fields. *arXiv* **2013**, arXiv:1012.2372.
9. Vinh, L.A. Singular matrices with restricted rows in vector spaces over finite fields. *Discret. Math.* **2012**, *312*, 413–418. [CrossRef]
10. Bourgain, J.; Vu, V.H.; Wood, P.M. On the singularity probability of discrete random matrices. *J. Funct. Anal.* **2010**, *258*, 559–603. [CrossRef]
11. Litvak, A.E.; Tikhomirov, K.E. Singularity of sparse Bernoulli matrices. *Duke Math. J.* **2022**, *171*, 1135–1233. [CrossRef]
12. Tao, T.; Vu, V.H. On the singularity probability of random Bernoulli matrices. *J. Am. Math. Soc.* **2007**, *20*, 603–628. [CrossRef]
13. Tikhomirov, K. Singularity of random Bernoulli matrices. *Ann. Math.* **2020**, *191*, 593–634. [CrossRef]
14. Fulman, J.; Goldstein, L. Stein's method and the rank distribution of random matrices over finite fields. *Ann. Probab.* **2015**, *43*, 1274–1314. [CrossRef]
15. Kovalenko, I.N.; Levitskaya, A.A. Stochastic properties of systems of random linear equations over finite algebraic structures. In *Probabilistic Methods in Discrete Mathematics*; Kolchin, V.F., Kozlov, V.Y., Pavlov, Y.L., Prokhorov, Y.V., Eds.; TVP/VSP: Utrecht, The Netherlands, 1993; pp. 64–70.
16. Cooper, C.; Frieze, A.; Pegden, W. On the rank of a random binary matrix. *Electron. J. Combin.* **2019**, *26*, #P4.12. [CrossRef] [PubMed]
17. Luh, K.; Meehan, S.; Nguyen, H.H. Some new results in random matrices over finite fields. *J. Lond. Math. Soc.* **2021**, *103*, 1209–1252. [CrossRef]
18. Eberhard, S. The characteristic polynomial of a random matrix. *Combinatorica* **2022**, *42*, 491–527. [CrossRef]
19. Fulman, J. Random matrix theory over finite fields. *Bull. Am. Math. Soc.* **2002**, *39*, 51–85. [CrossRef]
20. He, J.; Pham, H.T.; Xu, M.W. Universality for low-degree factors of random polynomials over finite fields. *Int. Math. Res. Not.* **2023**, *2023*, 14752–14794. [CrossRef]
21. Lidl, R.; Niederreiter, H. *Finite Fields*, 2nd ed.; Encyclopedia of Mathematics and Its Applications, Volume 20; Cambridge University Press: Cambridge, UK, 1997.
22. Gentle, J.E. *Matrix Algebra: Theory, Computations, and Applications in Statistics*; Springer: Berlin/Heidelberg, Germany, 2007.
23. van Lint, J.H.; Wilson, R.M. *A Course in Combinatorics*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2001.
24. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.
25. Demmel, J.W. The Probability that a Numerical Analysis Problem is Difficult. *Math. Comput.* **1988**, *50*, 449–480. [CrossRef]
26. Bürgisser, P.; Cucker, F. *Condition: The Geometry of Numerical Algorithms*; Springer: Berlin/Heidelberg, Germany, 2013.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.