NOTE

ON THE PROBABILITY THAT THE DETERMINANT OF AN \( n \times n \) MATRIX OVER A FINITE FIELD VANISHES

A. MUKHOPADHYAY

Department of Applied Mathematics, Indian Institute of Science, Bangalore 560012, India

Received 18 November 1982
Revised 23 January 1984

An expression is derived for the probability that the determinant of an \( n \times n \) matrix over a finite field vanishes; from this it is deduced that for a fixed field this probability tends to 1 as \( n \) tends to \( \infty \).

1. Introduction

Let \( p \) be a prime and \( \mathbb{Z}_p = \{0, 1, \ldots, p-1\} \). If addition (+) and multiplication (\( \cdot \)) are defined in \( \mathbb{Z}_p \) as being modulo \( p \), \( (\mathbb{Z}_p, +, \cdot) \) becomes a finite field of order \( p \); such a finite field is referred to as \( \text{GF}(p) \), a Galois field of order \( p \). Subsequently, by \( \mathbb{Z}_p \) we shall understand \( (\mathbb{Z}_p, +, \cdot) \).

Let \( A = [a_{ij}] \) be an \( n \times n \) matrix over \( \mathbb{Z}_p \). In the next section, we derive an expression for the probability that \( \det(A) \) vanishes. To do so, we find the probability distribution (p.d.) of the product \( X_1X_2 \cdots X_n \), where the \( X_i \)'s are independent and uniformly distributed with values in \( \mathbb{Z}_p \) and that of a finite sum of such products.

2. Analysis

Theorem 1. If \( Y = \prod_{i=1}^{n} X_i \), where \( X_1, X_2, \ldots, X_n \) are random variables, independent and uniformly distributed with values in \( \mathbb{Z}_p \), then the p.d. of \( Y \) is given by

\[
P(Y = 0) = 1 - k^n, \quad P(Y = i \neq 0) = k^{n-1}/p = k^n/(p - 1),
\]

where \( k = 1 - 1/p \) and \( P \) stands for 'the probability that'.

0012-365X/84/$3.00 \copyright 1984, Elsevier Science Publishers B.V. (North-Holland)
Proof.

\[ P(Y = 0) = 1 - P(X_1 \neq 0, X_2 \neq 0, \ldots, X_n \neq 0) \]
\[ = 1 - \prod_{i=1}^{n} P(X_i \neq 0) \quad \text{(the } X_i\text{'s are independent)} \]
\[ = 1 - \prod_{i=1}^{n} (1 - P(X_i = 0)) \]
\[ = 1 - \prod_{i=1}^{n} \left(1 - \frac{1}{p}\right), \quad \text{\(X_i\) is uniformly distributed} \]
\[ = 1 - \left(1 - \frac{1}{p}\right)^n. \]

By symmetry, it is equiprobable that \( Y \) assumes any non-zero value. Hence

\[ P(Y = i \neq 0) = \frac{(1 - P(Y = 0))/(p - 1)}{k^n/(p - 1)} = \frac{k^n}{(p - 1)}. \]

**Theorem 2.** If \( Z = Y_1 + Y_2 \), where \( Y_1 \) and \( Y_2 \) are random variables, independent and each distributed like \( Y \), then the p.d. of \( Z \) is given by

\[
P(Z = 0) = 1 + k^{2n-1} - 2k^n,
\]
\[
P(Z = i \neq 0) = \frac{(2k^n - k^{2n-1})/(p - 1)}{k^n/(p - 1)},
\]

where \( k = 1 - 1/p \).

Proof.

\[
P(Z = 0) = \sum_{i=0}^{p-1} P(Y_1 = i, Y_2 = p-i)
\]

\[
\text{(the events } Y_1 = i \text{ and } Y_2 = p-i \text{ are mutually exclusive and } (i + p - i) \bmod p = 0) \]
\[
= \sum_{i=0}^{p-1} P(Y_1 = i)P(Y_2 = p-i) \quad \text{\((Y_1 \text{ and } Y_2 \text{ are independent})\)} \]
\[
= P(Y_1 = 0)P(Y_2 = 0) + \sum_{i=1}^{p-1} P(Y_1 = i)P(Y_2 = p-i) \]
\[
= (1 - k^n)^2 + (p-1)k^{2n}/(p - 1)^2 \quad \text{(by Theorem 1)} \]
\[
= 1 + k^{2n-1} - 2k^n, \quad \text{on simplification.} \]

By symmetry again, it is equiprobable that \( Z \) assumes any non-zero value. Hence

\[
P(Z = i \neq 0) = (1 - P(Z = 0))/(p - 1) = (2k^n - k^{2n-1})/(p-1). \]

**Theorem 3.** If \( Z = \sum_{i=1}^{m} Y_i \), where \( Y_1, Y_2, \ldots, Y_m \) are random variables,
independent and distributed like \( Y \), then the p.d. of \( Z \) has the following form:

\[
P(Z = 0) = 1 - f(m, n),
\]

\[
P(Z = i \neq 0) = f(m, n)/(p - 1),
\]

where \( f(m, n) \) is some polynomial in \( k \).

**Proof.**

\[
P(Z = 0) = \sum_{i, j, \ldots, m \mod p = 0} P(Y_1 = j_1, Y_2 = j_2, \ldots, Y_m = j_m)
\]

(the events \( Y_1 = j_1, \ldots, Y_m = j_m \) are mutually exclusive)

\[
= P(Y_1 = 0, Y_2 = 0, \ldots, Y_m = 0) + \sum_{i, j, \ldots, m \neq 0} P(Y_1 = j_1, \ldots, Y_m = j_m)
\]

\[
= (1 - k^n)^m + \sum_{i, j, \ldots, m \neq 0} \prod_{i=1}^{m} P(Y_i = j_i)
\]

\[
= 1 - f(m, n),
\]

where \( f(m, n) \) is a polynomial in \( k \). By symmetry,

\[
P(Z = i \neq 0) = (1 - P(Z = 0))/(p - 1) = f(m, n)/(p - 1). \quad \square
\]

**Theorem 4.** For fixed \( n \), \( f(m + 1, n) = k^n - f(m, n)(k^{n-1} - 1) \).

**Proof.** If \( Y_1, Y_2, \ldots, Y_{m+1} \) are random variables, independent and distributed like \( Y \), then

\[
P\left( \sum_{i=1}^{m+1} Y_i = 0 \right) = \sum_{i=0}^{p-1} P\left( Y_i = i, \sum_{i=2}^{m+1} Y_i = p - i \right)
\]

(the events \( Y_1 = i \) and \( \sum_{i=2}^{m+1} Y_i = p - i \) are mutually exclusive)

\[
= P(Y_1 = 0, \sum_{i=2}^{m+1} Y_i = 0) + \sum_{i=1}^{p-1} P\left( Y_1 = i, \sum_{i=2}^{m+1} Y_i = p - i \right)
\]

\[
= P(Y_1 = 0)P\left( \sum_{i=2}^{m+1} Y_i = 0 \right) + \sum_{i=1}^{p-1} P(Y_1 = i)P\left( \sum_{i=2}^{m+1} Y_i = p - i \right)
\]

\( (Y_1 \text{ and } \sum_{i=2}^{m+1} Y_i \text{ are independent}) \)

\[
= (1 - k^n)(1 - f(m, n)) + (k^{n-1}/p)f(m, n)
\]

\[
= 1 - f(m + 1, n) \quad \text{(by Theorems 1, 2 and 3).}
\]

Therefore,

\[
f(m + 1, n) = k^n - f(m, n)(k^{n-1} - 1), \quad \text{on simplification.} \quad \square
\]
Theorems 1, 2 and 4 show
\[ f(1, n) = k^n \]
\[ f(2, n) = k^n(2 - k^{n-1}) \]
\[ \ldots \]
\[ f(m + 1, n) = k^n - f(m, n)(k^{n-1} - 1). \]
From there, it follows by induction on \( m \) that
\[ f(m, n) = O(k^n) \quad \text{and} \quad \deg f(m, n) = m(n - 1) + 1. \]
It can be verified by substitution in the above recurrence that
\[ f(m, n) = \sum_{i=0}^{m-1} m! C_i(-1)^{m-i} + 1 + k^{m-1}(n-1)+1, \]
a polynomial in \( k \) of degree \( m(n-1)+1 \).

Theorem 5.
\[ P\{\det(A) = 0\} = 1 + [f(m, n)]^2/k - 2f(m, n), \]
where \( m = n!/2 \).

Proof. The expansion of \( \det(A) \) in terms of its arguments consists of a sum of \( n! \) terms of the type \( \text{sign}(i_1, i_2, \ldots, i_n) \ a_{i_1} a_{i_2} \ldots a_{i_n} \), where \( (i_1, i_2, \ldots, i_n) \) is a permutation of \( (1, 2, \ldots, n) \) and \( \text{sign}(\cdot) \) is a function which takes the value \( +1 \) or \( -1 \) according as the permutation \( (i_1, i_2, \ldots, i_n) \) is even or odd. Each \( a_{i_j} \) can be treated as a uniformly distributed random variable and each product \( a_{i_1} a_{i_2} \ldots a_{i_n} \) as a random variable, distributed like \( Y \). Hence
\[ P\{\det(A) = 0\} = \sum_{i=0}^{n-1} P \left\{ \sum_{j=1}^{n} Z_i = i, \sum_{j=1}^{n} Z_i' = p - i \right\}, \]
where \( Z_i = a_{i_1} a_{i_2} \ldots a_{i_n}, \) \( (i_1, i_2, \ldots, i_n) \) being the \( j \)th even permutation of \( (1, 2, \ldots, n) \) and \( Z_i' = a_{i_1} a_{i_2} \ldots a_{i_n}, \) \( (i'_1, i'_2, \ldots, i'_n) \) being the \( j \)th odd permutation of \( (1, 2, \ldots, n) \), assuming a lexicographic order on all permutations of \( (1, 2, \ldots, n) \)
\[ = P \left\{ \sum_{j=1}^{n} Z_i = 0, \sum_{j=1}^{n} Z_i' = 0 \right\} + \sum_{i=1}^{n-1} P \left\{ \sum_{j=1}^{n} Z_i = i, \sum_{j=1}^{n} Z_i' = p - i \right\} \]
\[ = P \left\{ \sum_{j=1}^{n} Z_i = 0 \right\} P \left\{ \sum_{j=1}^{n} Z_i' = 0 \right\} + \sum_{i=1}^{n-1} P \left\{ \sum_{j=1}^{n} Z_i = i \right\} P \left\{ \sum_{j=1}^{n} Z_i' = p - i \right\} \]
\[ = (1 - f(m, n))^2 + [f(m, n)]^2/(p-1) \quad \text{by Theorem 4} \]
\[ = 1 + [f(m, n)]^2/k - 2f(m, n), \quad \text{on simplification.} \]
Corollary. Since \[ 1 + \left[ f(m, n) \right]^{2}/k - 2f(m, n) = 1 + O(k^n) \] and \( 0 < k < 1 \),

\[ P(\text{det}(A) = 0) \rightarrow 1 \quad \text{as} \quad n \rightarrow \infty. \]

Remark 1. We have taken some liberty in the use of the term random variable, since such a variable ought to be real-valued.

Remark 2. Though in many places in the above analysis we have appealed to symmetry, it is possible to give rigorous proofs, using induction and the properties of a finite field.

Acknowledgment

I thank the referee for his thoughtful suggestions and comments, which have greatly improved the quality of the paper.