On Determinants of Random Symmetric Matrices over $\mathbf{Z}_m$

Richard P. Brent
Computer Sciences Laboratory
Australian National University

Brendan D. McKay
Computer Science Department
Australian National University

Report TR-CS-88-03

February 1988
Republished October 1998

Abstract

We determine the probability that a random n by n symmetric matrix over $\{1, 2, \ldots, m\}$ has determinant divisible by m.

1 Introduction

Let m be an integer. The *m-rank* of an integer matrix A is the greatest integer k such that A has a k by k submatrix (not necessarily contiguous) whose determinant is nonzero mod m, or 0 if there is no such matrix. If m is a prime, the m-rank is equivalent to the usual rank over the field $GF(m)$. In this paper we assume that the elements a_{ij} of A are chosen at random, independently and uniformly, from $\mathbf{Z}_m = \{1, 2, \ldots, m\}$, subject to the condition that $a_{ij} = a_{ji}$, i.e., that A is symmetric. For corresponding results without the symmetry constraint, see [1].

Let $P(n,m)$ denote the probability that a random n by n symmetric matrix A over $\mathbf{Z}_m$ has m-rank n, and define $Q(n,m) = 1 - P(n,m)$. Thus, $Q(n,m)$ is the probability that $\det(A) = 0 \pmod{m}$. As in Lemma 1.1 of [1], we have

Lemma 1.1 *Suppose $m = p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}$, where $p_1, p_2, \ldots, p_k$ are distinctive primes. Then*

$$Q(n,m) = \prod_{i=1}^{k} Q(n, p_i^{\mu_i}).$$

In view of Lemma 1.1, we restrict our attention to the case that m is a prime power, say $m = p^\mu$. It is useful to define $q = 1/p$.

As in [1], our principal tool is Gaussian elimination, but in this case we have to use forms of Gaussian elimination which preserve symmetry. This is discussed in Section 2. Then, in Section 3, we use symmetric Gaussian elimination to show that $P(n, p^\mu)$ satisfies a five-term recurrence relation. In Section 4 we show that the five-term recurrence can be reduced to a three-term recurrence. Finally, in Section 5 we show that the three-term recurrence can be solved explicitly.

The solution depends on the parity of n and μ, and is well-known for $\mu = 1$, but appears to be new for $\mu > 1$. To conclude Section 5, we deduce some inequalities from the explicit solution.

TR-CS-88-03 retyped by Frances Page at Oxford University Computing Laboratory, October 1998.
Revision © 1988 Charles Babbage Research Centre appeared in *Ars Combinatoria* 26A(1988), 57–64.
 rpb101tr typeset using LaTeX.

An interesting problem is to determine the probability that a random n by n symmetric matrix A over $\mathbf{Z}_m$ has given m-rank r, where $r < n$. The case $\mu = 1$ has been solved by Carlitz [2] (provided $p \neq 2$), and the unsymmetric case has been considered in [1], but the general symmetric case remains open.

Another open problem is to determine the probability that $\det(A) \bmod m$ takes a given (nonzero) value d. Small examples show that this probability depends on d. For example, if $\mu = 1, k = \lceil n/2 \rceil, (d|p)$ is the Legendre symbol,

$$s = \begin{cases} 0, & \text{if } p = 2 \text{ or } n \text{ is odd,} \\ (d|p)(-1)^{k(p-1)/2}, & \text{otherwise,} \end{cases}$$

and Π is defined as in Section 5, then the probability is

$$\left(\frac{q}{1-q}\right) \frac{\Pi_{2k}(q)}{\Pi_k(q^2)} (1 + sq^k).$$

2 Symmetric Gaussian Elimination

Suppose that $A, n, m = p^\mu$ and $P(n, m)$ are as in Section 1. Lemmas 2.1 and 2.2 describe symmetric versions of Gaussian elimination.

Lemma 2.1 *Suppose that $n > 1$ and $a_{11} \neq 0 \pmod p$. Then there is a matrix U such that*

$$UAU^T = \left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \pmod{p^\mu} \tag{2.1}$$

where A' is a random $n-1$ by $n-1$ symmetric matrix.

Proof. Define

$$U = \begin{pmatrix} 1 & & & & \\ \lambda_2 & 1 & & 0 & \\ \lambda_3 & & \ddots & & \\ \vdots & & 0 & \ddots & \\ \lambda_n & & & & 1 \end{pmatrix}$$

where

$$a_{11}\lambda_j = -a_{1j} \pmod m \quad \text{for } j = 2, 3, \ldots, n. \tag{2.2}$$

Observe that $\lambda_2, \ldots, \lambda_n$ exist (since $a_{11} \neq 0 \pmod p$) and (2.1) clearly holds. Also, A' depends linearly on the random symmetric matrix

$$\begin{pmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{pmatrix},$$

and thus is random over $\mathbf{Z}_m$. □

Lemma 2.2 *Suppose that $n > 2, a_{11} = 0 \pmod p$, and $a_{12} \neq 0 \pmod p$. Then there is a matrix V such that*

$$VAV^T = \left(\begin{array}{cc|c} a_{11} & a_{12} & \multirow{2}{*}{0} \\ a_{21} & a_{22} & \\ \hline \multicolumn{2}{c|}{0} & A'' \end{array}\right) \pmod{p^\mu} \tag{2.3}$$

where A'' is a random $n-2$ by $n-2$ symmetric matrix.

Proof. Define

$$V = \begin{pmatrix} 1 & & & & \\ 0 & 1 & & 0 & \\ \lambda_3 & \mu_3 & 1 & & \\ \vdots & \vdots & & \ddots & \\ \lambda_n & \mu_n & 0 & & 1 \end{pmatrix},$$

where

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} \lambda_j \\ \mu_j \end{pmatrix} = -\begin{pmatrix} a_{1j} \\ a_{2j} \end{pmatrix} \pmod m$$

for $j = 3, \ldots, n$. Observe that μ_j and λ_j exist ($j = 3, \ldots, n$) since

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \neq 0 \pmod p.$$

It is easy to see that (2.3) holds. Also, A'' depends linearly on the random symmetric matrix

$$\begin{pmatrix} a_{33} & \cdots & a_{3n} \\ \vdots & \ddots & \vdots \\ a_{n3} & \cdots & a_{nn} \end{pmatrix}$$

and thus is random over $\mathbf{Z}_m$. □

3 A five-term recurrence for $P(n, p^\mu)$

It is convenient to define

$$P(0, p^\mu) = 1 \quad \text{for } \mu > 0$$

and

$$P(n, p^\mu) = 0 \quad \text{for } \mu \leq 0. \tag{3.1}$$

Theorem 3.1 *If $n > 0, \mu > 0$, and boundary conditions are given by (3.1), then*

$$\begin{aligned} P(n, p^\mu) = {} & (1-q)P(n-1, p^\mu) + q(1-q^{n-1})P(n-2, p^\mu) \\ & + q^n(1-q)P(n-1, p^{\mu-1}) + q^{n+1}P(n, p^{\mu-2}). \end{aligned} \tag{3.2}$$

Proof. Let A be a random symmetric $n \times n$ matrix over $\mathbf{Z}_m, m = p^\mu$. The four terms on the right side of (3.2) arise from four mutually exclusive cases:

1. $a_{11} \neq 0 \pmod p$.

2. $a_{11} = 0 \pmod p$ and some $a_{1j} \neq 0 \pmod p$.

3. $a_{1j} = 0 \pmod p$ for $j = 1, \ldots, n$ and $a_{11} \neq 0 \pmod{p^2}$.

4. $a_{1j} = 0 \pmod p$ for $j = 1, \ldots, n$ and $a_{11} = 0 \pmod{p^2}$.

In case 1, which occurs with probability $1-q$, we apply Lemma 2.1; since $\det(A) = a_{11}\det(A') \pmod{p^\mu}$ we have $\det(A) \neq 0 \pmod{p^\mu}$ iff $\det(A') \neq 0 \pmod{p^\mu}$, which occurs with conditional probability $P(n-1, p^\mu)$.

In case 2, which occurs with probability $q(1-q^{n-1})$, we can assume that $a_{12} \neq 0 \pmod p$ by making a suitable permutation of rows and columns, if necessary. We then apply Lemma 2.2, obtaining $\det(A) = (a_{11}a_{22} - a_{12}^2)\det(A'') \pmod{p^\mu}$, so $\det(A) \neq 0 \pmod{p^\mu}$ iff $\det(A'') \neq 0 \pmod{p^\mu}$, which occurs with conditional probability $P(n-2, p^\mu)$.

In case 3, which occurs with probability $q^n(1-q)$, we can reduce A to the form (2.1) because (2.2) is solvable. Thus $\det(A) = a_{11}\det(A') \pmod{p^\mu}$ and $\det(A) \neq 0 \pmod{p^\mu}$ iff $\det(A') \neq 0 \pmod{p^{\mu-1}}$, which occurs with conditional probability $P(n-1, p^{\mu-1})$.

Finally, in case 4, which occurs with probability q^{n+1}, we can divide the first row and column of A by p, add random multiples of $p^{\mu-1}$ to elements in the first row (and to corresponding elements in the first column), add a random multiple of $p^{\mu-2}$ to the (1,1) element, and obtain a new random symmetric matrix $\bar{A}$ such that

$$\det(A) = p^2 \det(\bar{A}) \pmod{p^\mu},$$

so $\det(A) \neq 0 \pmod{p^\mu}$ with conditional probability $P(n, p^{\mu-2})$. □

4 A three-term recurrence

The five-term recurrence (3.2) with boundary conditions (3.1) can be used to calculate $P(n, p^\mu)$ in $O(n\mu)$ arithmetic operations. However, to obtain inequalities and asymptotic results it is useful to have an explicit solution. To obtain such a solution, we first reduce (3.2) to a three-term recurrence for $P(n, p^\mu)$ (n odd).

Theorem 4.1 *If $\mu > 0$ and boundary conditions are given by (3.1), then for odd $n \geq 3$,*

$$P(n, p^\mu) = (1-q^n)P(n-2, p^\mu) + q^n P(n, p^{\mu-2}) \tag{4.1}$$

and for odd $n \geq 1$,

$$P(n-1, p^\mu) = \frac{P(n, p^\mu) - q^n P(n, p^{\mu-1})}{1-q^n}. \tag{4.2}$$

Remarks. Equation (4.1) is a three-term recurrence from which $P(n, p^\mu)$ can be calculated for odd n. Equation (4.2) then determines $P(n, p^\mu)$ for even n. Equations (4.1) and (4.2) do not hold for all $n \geq 3$; for example, (4.2) fails if n is even and μ is odd. In the unsymmetric case [1], (4.2) holds for both even and odd n.

Proof (of Theorem 4.1) Let

$$\mathcal{P}_n = \mathcal{P}_n(x) = \sum_{\mu=1}^{\infty} P(n, p^{\mu}) x^{\mu} \tag{4.3}$$

be a generating function for $P(n, p^{\mu})$. From the boundary conditions (3.1) we have

$$\mathcal{P}_0 = x/(1-x). \tag{4.4}$$

Theorem 3.1 gives

$$(1 - q^{n+1}x^2)\mathcal{P}_n = (1-q)(1+q^n x)\mathcal{P}_{n-1} + q(1-q^{n-1})\mathcal{P}_{n-2} \tag{4.5}$$

for $n \geq 1$. Thus, for odd $n = 2k+1 \geq 1$ we have

$$(1 - q^{2k+2}x^2)\mathcal{P}_{2k+1} = (1-q)(1+q^{2k+1}x)\mathcal{P}_{2k} + q(1-q^{2k})\mathcal{P}_{2k-1} \tag{4.6}$$

and for even $n = 2k+2 \geq 2$ we have

$$(1 - q^{2k+3}x^2)\mathcal{P}_{2k+2} = (1-q)(1+q^{2k+2}x)\mathcal{P}_{2k+1} + q(1-q^{2k+1})\mathcal{P}_{2k}. \tag{4.7}$$

Both (4.6) and (4.7) hold for $k \geq 0$, and with the boundary condition (4.4) they define $\mathcal{P}_n$ for all $n \geq 0$.

Assume for the moment that (4.1) and (4.2) are correct. From (4.1) with $n = 2k+3$ we have

$$\mathcal{P}_{2k+3} = \left(\frac{1 - q^{2k+3}}{1 - q^{2k+3}x^2} \right) \mathcal{P}_{2k+1} \tag{4.8}$$

and from (4.2) with $n = 2k+1$ we have

$$\mathcal{P}_{2k} = \left(\frac{1 - q^{2k+1}x}{1 - q^{2k+1}} \right) \mathcal{P}_{2k+1}. \tag{4.9}$$

Clearly (4.8) and (4.9) for $k \geq 0$ and (4.4) define $\mathcal{P}_n$ for all $n \geq 0$. Thus, it is sufficient to show that (4.8) and (4.9) for $k \geq 0$ imply (4.6) and (4.7) for $k \geq 0$.

From (4.8) and (4.9) we have

$$\mathcal{P}_1 = \left(\frac{1-q}{1-qx} \right) \mathcal{P}_0 \tag{4.10}$$

$$\mathcal{P}_2 = \left(\frac{1-q^3 x}{1-q^3 x^2} \right) \mathcal{P}_1, \tag{4.11}$$

which satisfy (4.6) and (4.7) with $k = 0$. Thus, we may assume $k \geq 1$. Equation (4.8) with k replaced by $k-1$ gives

$$\mathcal{P}_{2k-1} = \left(\frac{1 - q^{2k+1}x^2}{1 - q^{2k+1}} \right) \mathcal{P}_{2k+1}. \tag{4.12}$$

Substituting (4.9) and (4.12) in the right side of (4.8) and simplifying, we obtain $(1-q^{2k+2}x^2)\mathcal{P}_{2k+1}$, so (4.6) holds. Similarly, some algebra shows that (4.8) and (4.9) imply (4.7).

Thus, the same generating function $\mathcal{P}_n, n \geq 0$, is defined by (4.1) and (4.2) as by (4.5). $\square$

We can now give an explicit formula for the generating function $\mathcal{P}_n$.

Theorem 4.2 *If $k \geq 0$, then*

$$\mathcal{P}_{2k+1}(x) = \left(\frac{x}{1-x}\right)\left(\frac{1-qx^2}{1-qx}\right)\prod_{j=0}^{k}\left(\frac{1-q^{2j+1}}{1-q^{2j+1}x^2}\right) \tag{4.13}$$

and

$$\mathcal{P}_{2k}(x) = \left(\frac{1-q^{2k+1}x}{1-q^{2k+1}}\right)\mathcal{P}_{2k+1}(x). \tag{4.14}$$

Proof. Equation (4.13) follows by induction from (4.8), using (4.4) and (4.10). Equation (4.14) is just (4.9). □

5 An explicit solution and some bounds

From Theorem 4.2 we can obtain an explicit solution for $P(n, p^\mu)$, and hence for $Q(n, p^\mu)$. Define

$$\Pi_n(q) = \prod_{j=1}^{n}(1-q^j)$$

and

$$T_\beta(k,s) = \begin{cases} 1, & \text{if } k = 0, \\ \displaystyle\sum_{j=0}^{s} q^{\beta j}\frac{\Pi_{k+j-1}(q^2)}{\Pi_j(q^2)\Pi_{k-1}(q^2)}, & \text{if } k \geq 1. \end{cases} \tag{5.1}$$

Our explicit solution may be written in terms of T_1 and T_3:

Theorem 5.1 *If $n \geq 1, \mu \geq 1, k = \lfloor n/2 \rfloor$, and $s = \lfloor(\mu-1)/2\rfloor$ then*

$$P(n,p^\mu) = \frac{\Pi_{2k}(q)}{(1-q)\Pi_k(q^2)}\Big((1-q^{2k+1})T_3(k,s) - q^\mu(1-q^n)T_1(k,s)\Big). \tag{5.2}$$

Proof. We may show by induction on k from (4.1) that

$$P(2k+1,p^\mu) = \frac{\Pi_{2k+1}(q)}{(1-q)\Pi_k(q^2)}\left(T_3(k,s) - q^\mu T_1(k,s)\right). \tag{5.3}$$

Considering the cases $\mu = 2s+1$ and $\mu = 2s+2$ separately, it follows from (4.2) that

$$P(2k,p^\mu) = P(2k+1,p^\mu) + q^{2k+\mu}\frac{\Pi_{2k}(q)}{\Pi_k(q^2)}T_1(k,s). \tag{5.4}$$

After some simplification we see that (5.2) holds both for $n = 2k$ and $n = 2k+1$. □

Equation (5.2) is inconvenient for numerical computation as $P(n, p^\mu)$ is close to 1 unless p^μ is small. In order to deduce a convenient expression for $Q(n,p^\mu) = 1 - P(n,p^\mu)$, we use the following identities for T_1 and T_3.

Lemma 5.1 *If $k \geq 0$ and $s \geq 0$ then*

$$T_1(k,s) = \frac{\Pi_k(q^2)}{\Pi_{2k}(q)} \left(1 - q^{s+1} \sum_{j=0}^{k-1} q^{2j} \frac{\Pi_{2j}(q)\Pi_{j+s}(q^2)}{\Pi_j(q^2)^2 \Pi_s(q^2)} \right). \tag{5.5}$$

and

$$T_3(k,s) = \frac{\Pi_k(q^2)}{\Pi_{2k+1}(q)} \left(1 - q - q^{3s+3} \sum_{j=0}^{k-1} q^{2j} \frac{\Pi_{2j+1}(q)\Pi_{j+s}(q^2)}{\Pi_j(q^2)^2 \Pi_s(q^2)} \right). \tag{5.6}$$

Proof. (5.5) and (5.6) may be proved by induction on k. The proof is similar to the proof of Theorem 2.1 of [1], so details are omitted. □

If we substitute (5.5) into (5.2) the factor $\Pi_k(q^2)/\Pi_{2k}(q)$ cancels. This gives a convenient explicit solution for $Q(n, p^\mu)$.

Theorem 5.2 *If $n \geq 1, \mu \geq 1, k = \lfloor n/2 \rfloor$, and $s = \lfloor (\mu-1)/2 \rfloor$ then*

$$Q(n, p^\mu) = \frac{q^\mu(1-q^n) - R}{1-q} \tag{5.7}$$

where

$$R = q^{s+1} \sum_{j=0}^{k-1} \left(q^\mu(1-q^n) - q^{2s+2}(1-q^{2j+1}) \right) q^{2j} \frac{\Pi_{2j}(q)\Pi_{j+s}(q^2)}{\Pi_j(q^2)^2 \Pi_s(q^2)} \tag{5.8}$$

and

$$0 \leq R < q^{3\mu/2}. \tag{5.9}$$

Proof. Equations (5.7) and (5.8) follow from Theorem 5.1 and Lemma 5.1 after some simplification. Since $\mu \leq 2s+2$ and $n \geq 2k$, we have $q^\mu(1-q^n) > q^{2s+2}(1-q^{2j+1})$ for $0 \leq j \leq k-1$, so $R \geq 0$ (with equality only when $k = 0$). It is clear from (5.8) that $R = O(q^{\mu+s+1}) = O(q^{3\mu/2})$, and computation shows that $R < q^{3\mu/2}$ (the worst case is n large, $\mu = 2s+1$ large and $q = 1/2$). □

We now show that $P(n, p^\mu)$ has the expected monotonicity properties.

Theorem 5.3 *For $n \geq 0$ and $\mu \geq 0$,*

$$P(n+1, p^\mu) \leq P(n, p^\mu) \leq P(n, p^{\mu+1}). \tag{5.10}$$

Proof. The inequality $P(n, p^\mu) \leq P(n, p^{\mu+1})$ follows by induction on $n+\mu$ from the recurrence (3.2), since the coefficients on the right side of (3.2) are independent of μ.

To prove $P(n+1, p^\mu) \leq P(n, p^\mu)$ we consider several cases. If n is even the inequality follows from (5.4). If $n = 2k+1$ is odd and $\mu = 2s+2$ is even then, from Theorem 5.1,

$$P(2k+1, p^{2s+2}) - P(2k+2, p^{2s+2}) = q^{2k+2s+3}(1+q) \frac{\Pi_{2k+1}(q)}{\Pi_k(q^2)} T_1(k+1, s) \geq 0.$$

Finally, if $n = 2k+1$ and $\mu = 2s+1$ are odd then, from Theorem 5.1,

$$\begin{aligned} &P(2k+1, p^{2s+1}) - P(2k+2, p^{2s+1}) \\ &= q^{2k+2s+2} \frac{\Pi_{2k+1}(q)}{\Pi_k(q^2)} \left(T_1(k+1, s) - q^s \frac{\Pi_{k+s}(q^2)}{\Pi_s(q^2)} \right) \\ &\geq 0. \end{aligned}$$

□

Corollary 5.1 *$\lim_{n\to\infty} Q(n, p^\mu)$ exists and lies in the interval $[q^\mu, q^\mu/(1-q)]$. Moreover,*

$$\lim_{n\to\infty} P(n, p^\mu) = \frac{\Pi_\infty(q)}{(1-q)\Pi_\infty(q^2)} \sum_{j=0}^{s} \frac{q^{3j} - q^{\mu+j}}{\Pi_j(q^2)}$$

and

$$\lim_{n\to\infty} Q(n, p^\mu) = \left(q^\mu - \frac{\Pi_\infty(q)}{\Pi_\infty(q^2)} \sum_{j=s+1}^{\infty} \frac{q^{\mu+j} - q^{3j}}{\Pi_j(q^2)} \right) \Big/ (1-q),$$

where $s = \lfloor (\mu - 1)/2 \rfloor$.

Proof. The limit exists by monotonicity in n, and the bounds follow from this monotonicity and Theorem 5.2. The explicit limits follow from Theorem 5.1 and Lemma 5.1 respectively. □

References

[1] R. P. Brent and B. D. McKay, Determinants and ranks of random matrices over $\mathbf{Z}_m$, *Discrete Math.* **66** (1987) 35-49.

[2] L. Carlitz, Representations by quadratic forms in a finite field, *Duke Math. J.* **21** (1954) 123-137.