NUMBER OF RANK r SYMMETRIC MATRICES OVER FINITE FIELDS

Abstract. We determine the number of $n \times n$ symmetric matrices over $GF(p^k)$ that have rank r for $0 \leq r \leq n$.

In [BM2] Brent and McKay determine the number of $n \times n$ symmetric matrices over $\mathbb{Z}_p$ that have determinant zero. Thus they determine the number of $n \times n$ symmetric matrices over $\mathbb{Z}_p$ that have rank n. We extend their result to symmetric matrices over $GF(p^k)$ and we determine the number of matrices that have rank r for any r.

The problem when the matrix is not required to be symmetric was treated in [BM1] and in [GR]. In these papers the number of $(n+\Delta) \times n$ matrices over $\mathbb{Z}_p$ with rank r is determined for all r and $\Delta \geq 0$.

Let $I(n, r, p^k)$ be the number of $n \times n$ symmetric matrices over $GF(p^k)$ with rank r. Furthermore, let $q(n, p^k)$ be the probability that an $n \times n$ symmetric matrix over $GF(p^k)$ is invertible. Define $q(0, p^k)$ to be 1. Also note that $q(1, p^k) = (1 - \frac{1}{p^k})$.

Theorem 0.1. *In the notation given above, $q(n, p^k)$ satisfies the recurrence*

$$q(n,p^k) = \left(1 - \left(\frac{1}{p^k}\right)\right) q(n-1,p^k) + \left(\frac{1}{p^k}\right)\left(1 - \left(\frac{1}{p^k}\right)^{n-1}\right) q(n-2,p^k) \tag{0.1}$$

for all $n \geq 2$. Furthermore, this recurrence gives

$$q(n,p^k) = \prod_{j=0}^{s}\left(1 - \left(\frac{1}{p^k}\right)^{2j-1}\right),$$

where $s = \lfloor \frac{n}{2} \rfloor$.

In particular, the number of invertible symmetric $n \times n$ matrices over $GF(p^k)$ is

$$I(n,n,p^k) = \left(p^k\right)^{\binom{n}{2}} q(n,p^k) = \left(p^k\right)^{\binom{n}{2}} \prod_{j=0}^{s}\left(1 - \left(\frac{1}{p^k}\right)^{2j-1}\right). \tag{0.2}$$

Before we prove this result we will give a couple of Lemmas.

Lemma 0.2. *Suppose $A = (a_{ij})_{1 \leq i,j \leq n}$ is a symmetric $n \times n$ matrix over $GF(p^k)$ and that $a_{11} \neq 0$. Additionally, define the $n \times n$ matrix $\Lambda = (\lambda_{ij})_{1 \leq i,j \leq n}$ with*

$$\lambda_{ij} = \begin{cases} 1 & \textit{if } i = j \neq 1 \\ -a_{11}^{-1}a_{1j} & \textit{if } i = 1 \\ 0 & \textit{otherwise} \end{cases}.$$

Date: August 8, 2004.

Then

$$\Lambda^T A \Lambda = \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & b_{11} & b_{12} & \dots & b_{1(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & b_{(n-1)1} & b_{(n-1)2} & \cdots & b_{(n-1)(n-1)} \end{pmatrix}$$

where the matrix $B = (b_{ij})_{1 \le i,j \le (n-1)}$ *is a symmetric* $(n-1) \times (n-1)$ *matrix. Furthermore, if* A *is random then so is* B.

Proof. By doing the multiplication we see that $\Lambda A \Lambda^T$ has the desired form. Furthermore, $b_{ij} = -a_{11} a_{1(i+1)} a_{1(j+1)} + a_{(i+1)(j+1)}$. Thus $b_{ij} = b_{ji}$. So B is symmetric. Furthermore, if A is a random matrix, then matrix B is random. □

Lemma 0.3. *Suppose* $A = (a_{ij})_{1 \le i,j \le n}$ *is a symmetric* $n \times n$ *matrix over* $GF(p^k)$, $a_{11} = 0$ *and* $a_{12} \neq 0$. *Additionally, let* $n \times n$ *matrix* $\Gamma = (\gamma_{ij})_{1 \le i,j \le n}$ *with*

$$\gamma_{ij} = \begin{cases} 1 & \text{if } i = j \\ -a_{12}^{-1} a_{1j} & \text{if } i = 2 \text{ and } j \ge 3 \\ a_{12}^{-2} a_{22} a_{1j} - a_{12}^{-1} a_{2j} & \text{if } i = 1 \text{ and } j \ge 3 \\ 0 & \text{otherwise} \end{cases}.$$

Then

$$\Gamma^T A \Gamma = \begin{pmatrix} 0 & a_{12} & 0 & \dots & 0 \\ a_{12} & a_{22} & 0 & \dots 0 & \\ 0 & 0 & c_{11} & \dots & c_{1(n-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & c_{(n-2)1} & \cdots & c_{(n-2)(n-2)} \end{pmatrix}$$

where the matrix $C = (c_{ij})_{1 \le i,j \le (n-2)}$ *is a symmetric* $(n-2) \times (n-2)$ *matrix. Furthermore, if* A *is random then so is* C.

Proof. The proof is similar to the proof of the previous Lemma. Doing the multiplication we see that the matrix has the desired form and that $c_{ij} =??$. So C is a symmetric matrix. As in the previous Lemma C will be random if A is random. □

We are now prepared to prove the first of our two main theorems.

Proof. Proof of Theorem 0.1 We begin by deriving 0.1. Let A be a random symmetric $n \times n$ matrix over $GF(p^k)$ with $n \ge 2$. Throughout the proof we use the fact that A is invertible if and only if $det(A) \neq 0$. We derive the recursion by considering the two cases when $a_{11} \neq 0$ and when $a_{11} = 0$.

First suppose $a_{11} \neq 0$ this happens with probability $1 - 1/p^k$. With the notation of Lemma 0.2 and using the fact $det(\Lambda) = det(\Lambda^T) = 1$, we see that $det(A) = det(\Lambda) det(A) det(\Lambda^T) = det(\Lambda A \Lambda^T) = a_{11} det(B)$. Since A was random B is a random symmetric $(n-1) \times (n-1)$ matrix. Hence, if $a_{11} \neq 0$ then the probability that A is invertible is $\left(1 - \frac{1}{p^k}\right) q(n-1, p^k)$.

Next suppose that $a_{11} = 0$. If $a_{1j} = 0$ for all j, then $det(A) = 0$. So, A is not invertible. Suppose that there exists at least one $j \neq 1$ such that $a_{1j} \neq 0$. This happens with probability $\frac{1}{p^k}\left(1 - \left(\frac{1}{p^k}\right)^{n-1}\right)$. Switching the j^{th} column with the 2^{nd} column and switching the j^{th} row with the 2^{nd} row keeps A a symmetric matrix. Furthermore, whether or not the determinant is 0 is not changed. Thus we may assume without loss of generality that $a_{12} \neq 0$.

With the notation of Lemma 0.3 and using the fact $det(\Gamma) = det(\Gamma^T) = 1$, we see that $det(A) = det(\Gamma)det(A)det(\Gamma^T) = det(\Gamma A \Gamma^T) = a_{12}a_{22}det(C)$. Since A was random C is a random symmetric $(n-2) \times (n-2)$ matrix. Hence, if $a_{11} = 0$ then the probability that A is invertible is $\frac{1}{p^k}\left(1 - \left(\frac{1}{p^k}\right)^{n-1}\right) q(n-2, p^k)$. Summing the two probabilities gives 0.1.

From this recursion it is easy to deduce that

$$q(n, p^k) = \prod_{j=0}^{s} \left(1 - \left(\frac{1}{p^k}\right)^{2j-1}\right),$$

where $s = \lfloor \frac{n}{2} \rfloor$. □

We are will give a couple of Lemmas before stating and proving the main result.

Proposition 0.4. *An $n \times n$ matrix M is symmetric if and only if $v^T M = (Mv)^T$ for all vectors v.*

Lemma 0.5. *Let A be a symmetric $n \times n$ matrix and let B be an $n \times n$ matrix. Then $B^T AB$ is a symmetric matrix.*

Proof. To prove this we will show that for all $\vec{v} \in Z_2^n$, $v^T B^T AB = (B^T ABv)^T$. If we establish this, then the result follows from Proposition 0.4.

It is well known that $v^T B^T = (Bv)^T$. Using this twice and Proposition 0.4 we have

$$v^T B^T AB = (Bv)^T AB = (ABv)^T (B^T)^T = (B^T ABv)^T,$$

as desired. □

Let $d(n, j, p^k)$ be the number of j dimensional subspaces of $GF(p^k)^n$. Define $\prod_n(q) = (1-q)(1-q^2)\dots(1-q^n)$. It is well known, see [BM1], that

$$d(n, j, p^k) = \frac{\prod_n(p^k)}{\prod_{n-j}(p^k)\prod_j(p^k)}.$$

Theorem 0.6. *In the notation above,*

$$\begin{aligned} I(n, n-j, p^k) =& d(n, j, p^k) I(n-j, n-j, p^k) \\ =& \frac{\prod_n(p^k)}{\prod_{n-j}(p^k)\prod_j(p^k)} I(n-j, n-j, p^k). \end{aligned}$$

Proof. We will prove this theorem in three steps. Say that e_j is the n dimensional vector over $GF(p^k)^n$ that has a 0 in each entry except for the j^{textth} entry.

Step 1. Let $E = \text{span}\ \{e_1, \dots, e_j\}$. Then there are $I(n-j, n-j, p^k)$ rank $n-j$ $n \times n$ matrices that take exactly E to zero.

To see this we begin by noting that Me_m is the mth column of the matrix M. Therefore, if A is a symmetric matrix with $Ae_m = \vec{0}$ then the mth column and mth row of A must be zero. Furthermore, A has rank $n-j$ if and only if $n-j$ of the column vectors are independent.

Let A be a symmetric $n \times n$ matrix with rank $n-j$ that takes E to zero. Since the first j columns of A are zero, if A has rank $n-j$ we must have that the final $n-j$ column vectors of A are linearly independent. Since the first j rows of A are also the zero, A will send

$e_1, \ldots, e_j$ to $\vec{0}$ and have rank $n-j$ if and only if the symmetric $(n-j)\times(n-j)$ submatrix $A^* = (a_{ij})_{(j+1)\leq i,j\leq n}$ has linearly independent column vectors. That is if and only if A^* is invertible.

Therefore, there are $I(n-j, n-j, p^k)$ symmetric $n \times n$ matrices of rank $n-j$ that send $e_1, \ldots, e_j$ to $\vec{0}$.

Step 2. Let S be any j dimensional subspace of $GF(p^k)^n$ with basis $\{v_1, \cdots, v_j\}$. Also let $\mathcal{S} = \{$ all $n \times n$ symmetric matrices of rank $n-j$ that take S to zero$\}$ and let $\mathcal{E} = \{$ all $n \times n$ symmetric matrices of rank $n-j$ that take E to zero$\}$. I will show that there is a 1-1 onto map from $\mathcal{S}$ to $\mathcal{E}$, thus these sets have the same size. The result follows, since the subspace S was arbitrarily chosen and there are $I(n-j, n-j)$ elements in $\mathcal{E}$.

It remains to demonstrate the 1-1 onto map. There exists $k_1, \ldots, k_{n-j}$ such that $\{v_1, \ldots, v_j, e_{k_1}, \ldots, e_{k_{n-j}}\}$ is a basis for $GF(p^k)^n$. Let B be the change of basis matrix such that $e_s \mapsto v_s$ for $1 \leq s \leq j$ and $e_{j+t} \mapsto e_{k_t}$ for $1 \leq t \leq (n-j)$.

Define the map $\phi : \mathcal{S} \to \mathcal{E}$ by $\phi(A) = B^T AB$. Since B is invertible so is B^T. Thus, $B^T ABv = \vec{0}$ if and only if $ABv = \vec{0}$. But $ABv = \vec{0}$ if and only if $Bv \in S$. Since B is the change of basis matrix from $\{e_1, \ldots, e_j\}$ and $\{v_1, \ldots, v_j\}$ we have $B^T ABv = \vec{0}$ if and only if $v \in E$. Therefore, the map is well defined onto the spaces indicated.

Furthermore, ϕ is 1-1, since B and B^T are both invertible. To show that ϕ is onto let $X \in \mathcal{E}$ be arbitrary and $Y = (B^T)^{-1} X B^{-1}$. Since $\phi(Y) = B^T Y B = B^T (B^T)^{-1} X B^{-1} B = X$, it is enough to show that $Y \in \mathcal{S}$. Since B^T is invertible $Yv = \vec{0}$ if and only if $XB^{-1}v = \vec{0}$. Furthermore, since $X \in \mathcal{E}$, $XB^{-1}v = \vec{0}$ if and only if $B^{-1}v \in E$. But B^{-1} is the change of basis matrix from $\{v_1, \ldots, v_j\}$ to $\{e_1, \ldots, e_j\}$, thus $Yv = \vec{0}$ if and only if $v \in S$. So $Y \in \mathcal{S}$.

This completes the proof that $I(n, n-j, p^k) = d(n, j, p^k) I(n-j, n-j, p^k)$. To finish the proof we use the well known result about $d(n, j, p^k)$ discussed above.

□

References

[BM1] R. P. Brent and B. D. McKay, *Determinants of and rank of random matrices over $\mathbb{Z}_m$*, *Discrete Math.*, **66** (1987) 35 - 49.

[BM2] R. P. Brent and B. D. McKay, *On determinants of random symmetric matrices over $\mathbb{Z}_m$*, *ARS Combinatoria*, **26A** (1988) 57 - 64.

[GR] J. Goldman and G.-C. Rota, *On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions*, *Stud. Appl. Math.* 49(3) (1970) 239 - 258.