Some Anzahl Theorems in Symmetric Matrices over Finite
Local Rings (I)

LIU Yan¹, NAN Ji-zhu²
(1. Dept. of Math., Beijing Jiaotong University, Beijing 100044, China;
2. Dept. of Math., Dalian University of Technology, Liaoning 116024, China)
(E-mail: jznan@163.com)

Abstract: Let \( A_n(R) \) be the set of symmetric matrices over \( \mathbb{Z}/p^k\mathbb{Z} \) with order \( n \), where \( n \geq 2 \), \( p \) is a prime, \( p > 2 \) and \( p \equiv 1(\mod 4) \), \( k > 1 \). By determining the normal form of \( n \) by \( n \) symmetric matrices over \( \mathbb{Z}/p^k\mathbb{Z} \), we compute the number of the orbits of \( A_n(R) \) and then compute the order of the orthogonal group determined by the special symmetric matrix. Finally we get the number of the symmetric matrices which are in the same orbit with the special symmetric matrix.

Key words: congruent transformation; normal form of symmetric matrix; orthogonal group.
MSC(2000): 20H25, 15A21
CLC number: O152

1. Introduction

Mr WAN Zhe-xian etc.\(^1\) determined the normal form of symmetric matrices over a finite field \( F \) with char\( F \neq 2 \) and figured out the order of the orthogonal group determined by every kind of normal form of symmetric matrices. The order of

\[ O_{2n}(R) = \{ A \in \text{GL}_{2n}(R) | AHA' = H, \text{ for every column vector } v = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \in A, \sum_{i=1}^{n} x_i x_{i+1} = 0 \} \]

has been obtained in [3]. In this paper, the normal form of symmetric matrices over finite local ring \( \mathbb{Z}/p^k\mathbb{Z} \) is determined. The number of orbits that linear group \( \text{GL}_n(R) \) acts on \( A_n(R) \) is computed and the order of the orthogonal group which is determined by \( H \) and the number of the symmetric matrices which are congruent to \( H \) are also computed.

Let \( R \) denote finite local ring \( \mathbb{Z}/p^k\mathbb{Z} \), \( p \) be a prime, \( p > 2 \) and \( p \equiv 1(\mod 4) \). \( M \) denotes the maximal ideal of \( R \). Then \( M = \langle \bar{p} \rangle \). \( K \) denotes the quotient field and \( R^* \) is the set of all invertible elements in \( R \). We have \( \bar{a} = \bar{\bar{a}} \times \bar{p}^f \) for any \( \bar{a} \in R \) (\( \bar{\bar{a}} \in R - \langle \bar{p} \rangle, 0 \leq f \leq k \)). Let \( \pi : R \rightarrow K \) denote the natural homomorphism from \( R \) to \( K \), then it induces homomorphism \( \pi \) from \( M_{m \times n}(R) \) to \( M_{m \times n}(K) \). \( A_m(R) \) is the set of \( m \) by \( m \) symmetric matrices over \( R \). If rank(\( \pi P \)) = \( r \) for any \( P \) in \( A_m(R) \), then we say that \( P \) has real rank \( r \).

Received date: 2004-06-11
Foundation item: the Key Project of Chinese Ministry of Education (03060)
Lemma 1\[2\] If \( p \equiv 1 (\text{mod} 4) \), then \(-1\) is a quadratic residue (mod\( p^k \)), i.e., the equation \(-1 \equiv x^2 (\text{mod} p^k)\) has solutions.

Lemma 2\[2\] \( a_1 x_1 + \cdots + a_n x_n + b \equiv 0 (\text{mod} p^k) \) has solutions \((x_1, \cdots, x_n)\) if and only if \((a_1, \cdots, a_n, p^k) | b\). Then the number of solutions is \( p^{k(n-1)} (a_1, \cdots, a_n, p^k) \).

Lemma 3\[3\] Let \( \text{GL}_n(R) \) be general linear group over \( R \), then
\[
|\text{GL}_n(R)| = p^{kn^2} \prod_{i=0}^{n-1} (1 - \frac{1}{p^{n-i}}), \quad |\text{SL}_n(R)| = p^{k(n^2-1)} \prod_{i=0}^{n-2} (1 - p^{i-n}).
\]

Lemma 4\[4\] If \( R \) is a finite local ring, then \(|R| = p^k\), \(|M| = \langle \bar{p} \rangle = p^{k-1}\), \(|K| = |R/M| = p\), \(|R^*| = p^k - p^{k-1} = p^{k-1}(p-1)\).

Lemma 5 If \( \bar{a} \bar{p}^r = \bar{b} \bar{p}^s, 0 \leq r \leq s \leq k \), then \( \bar{a} \in \langle \bar{p} \rangle \) and \( \bar{a} = \bar{c} \bar{p}^{s-r} \), \( \bar{c} \in R^* \).

2. The number of orbits of \( A_n(R) \)

Suppose that \( A \) is an \( n \) by \( n \) symmetric matrix over \( R \). Call \( A \) symmetric if \( A' = A \). The matrices that are congruent to a symmetric matrix must be symmetric. \( R^* \) that consists of all invertible elements in \( R \) is a cyclic group with multiplication. If \( \bar{z} \) denotes some nonsquare invertible element in \( R^* \), then any nonsquare invertible element in \( R^* \) can be written as \( \bar{z} \bar{y}^2 \).

Theorem 1 Let \( A \) be an \( n \) by \( n \) symmetric matrix over \( R \). If there exists \( P \in \text{GL}_n(K) \) such that \( P \pi AP' = \begin{pmatrix} 0 & I(r) \\ I(r) & 0 \end{pmatrix} \), then \( A \) is congruent to the normal form
\[
\begin{pmatrix} 0 & I(r) \\ I(r) & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & D_1(s_1) \\ D_1(s_1) & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & D_2(s_2) \\ D_2(s_2) & \bar{p}^{l_2} \end{pmatrix} \oplus \ldots \oplus \begin{pmatrix} 0 & D_5(s_5) \\ D_5(s_5) & \bar{p}^{l_5} \end{pmatrix} \oplus \begin{pmatrix} 0 & \bar{p}^{l_5} \\ \bar{p}^{l_5} & 0 \end{pmatrix},
\]
where \( 2r \) is the real rank of \( A \), \( l_2, l_4 \) are even and \( l_3, l_5 \) are odd, \( D_1 = [\bar{p}^{t_1}, \cdots, \bar{p}^{t_1}] \),
\[
1 \leq r_1 \leq r_2 \leq \ldots \leq r_{s_1} \leq k-1, \quad 0 \leq s_1 \leq n,
\]
\[
\begin{pmatrix} 0 & D_1(s_1) \\ D_1(s_1) & \bar{p}^{l_1} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \bar{p}^{l_1} & \bar{p}^{l_1} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \bar{p}^{l_1-k} & 0 \\ 0 & \cdots & 0 & \bar{p}^{l_1-k} \end{pmatrix},
\]
where \( 0 < l_1 < l_2 < \cdots < l_1 < k \).

Proof Let
\[
A = \begin{pmatrix} \bar{a}_{11} & \bar{a}_{12} & \cdots & \bar{a}_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \bar{a}_{n1} & \bar{a}_{n2} & \cdots & \bar{a}_{nn} \end{pmatrix} \bar{a}_{ij} \in R.
\]
We select $\bar{a}_{ii} \neq 0$ and $\bar{a}_{ii} \in A$ which has the smallest power of $\bar{p}$. If it is not in $(1,1)$, then we can use elementary congruent transformation to do it. So we may assume that $\bar{a}_{11}$ is the element with the smallest power of $\bar{p}$. Let the element in $(i, j)$ be $\bar{a}_{ij}\bar{p}^{r_{ij}}(i \neq j)$; the element in $(i, i)$ be $\bar{a}_{ii}\bar{p}^{r_i}(\bar{a}_{ij} \in R^*0 \leq r_{ij} \leq k)$ and $\bar{a}_{ij}\bar{a}_{ij} = \bar{1}$. Let

$$P_1 = \begin{pmatrix}
    1 \\
    -\bar{a}_{11}\bar{a}_{12}\bar{p}^{r_{12} - r_1} \\
    \vdots \\
    -\bar{a}_{11}\bar{a}_{1n}\bar{p}^{r_{1n} - r_1} \\
    1
\end{pmatrix},$$

then

$$P_1AP_1' = \begin{pmatrix}
    \bar{a}_{11}\bar{p}^{r_1} & 0 & \cdots & 0 \\
    0 & A_1 & \cdots & 0 \\
    \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & 1
\end{pmatrix}.$$

Since $P_1AP_1'$ is still a symmetric matrix, $A_1$ is a $(n-1) \times (n-1)$ symmetric matrix. We can proceed in this fashion to show the existence of invertible matrices $P_2, \cdots, P_s$, such that

$$P_s \cdots P_1AP_1' \cdots P_1' = B = \begin{pmatrix}
    \bar{a}_{11}\bar{p}^{r_1} \\
    \vdots \\
    \bar{a}_{mmp}^{r_m} \\
    0 \\
    \ddots \\
    0 \\
    0
\end{pmatrix},$$

where $0 \leq r_1 \leq r_2 \leq \cdots \leq m < k$. If rank($\pi A$) = 2r, then $r_i = 0, 1 \leq i \leq 2r$. We will rearrange $\bar{a}_{11} \cdots \bar{a}_{2s,2s}$ and let $\bar{a}_{12} \cdots \bar{a}_{ss} \in R^{*2}$ and $\bar{a}_{s+1s+1} \cdots \bar{a}_{2r,2r}$ not in $R^{*2}$. $s$ is even since $P_\pi AP' = \begin{pmatrix}
    0 & I^{(r)} \\
    I^{(r)} & 0 \\
    0 & 0
\end{pmatrix}$.

Denote $Q_1 = [\bar{a}_{11}^{-1} \cdots \bar{a}_{ss}^{-1}, (\bar{a}_{s+1s+1}\bar{z}^{-1})^{-\frac{1}{2}} \cdots (\bar{a}_{2r,2r}\bar{z}^{-1})^{-\frac{1}{2}} \bar{1} \cdots \bar{1}]$, then

$$Q_1BQ_1' = [\bar{1}, \cdots, \bar{1}, \bar{z}, \cdots, \bar{z}, \bar{a}_{s+1s+1}\bar{z}^{r_{s+1s+1}} \cdots \bar{a}_{2r,2r}\bar{z}^{r_{2r,2r}} 0 \cdots 0].$$

By Lemma 1, we have $-1 \in R^{*2}$ and let $-1 \equiv x^2 (mod \bar{p}^k)$, then

$$\begin{pmatrix}
x \\
-2^{-1}x \\
\bar{1} \\
-2^{-1}x \\
\bar{1}
\end{pmatrix} \begin{pmatrix}
\bar{1} & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix},$$

and

$$\begin{pmatrix}
x \\
-(2\bar{z})^{-1}x \\
\bar{1} \\
-(2\bar{z})^{-1}x \\
\bar{1}
\end{pmatrix} \begin{pmatrix}
\bar{1} & 0 & 0 \\
0 & \bar{1} & 0 \\
0 & 0 & \bar{1}
\end{pmatrix} = \begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix}.$$
So there exists $Q_2 \in \text{GL}_n(R)$ such that
\[
Q_2Q_1BQ_1'Q_2' = \begin{pmatrix} 0 & I^{(r)} \\ I^{(r)} & 0 \end{pmatrix} \oplus \begin{pmatrix} \tilde{a}_{2r+1,2r+1} \tilde{p}^{r_1} \\ & \ddots \\ & & \tilde{a}_{mm} \tilde{p}^{m-2r} \\ & & & 0 \end{pmatrix} = B_1.
\]

We will rearrange $\tilde{a}_{2r+1,2r+1} \tilde{p}^{r_1} \cdots \tilde{a}_{mm} \tilde{p}^{m-2r}$, and let $\tilde{a}_{2r+1,2r+1} \cdots \tilde{a}_{2r+s_1+s_2+3r+s_1+s_2+s_3} \in R^2$, $\tilde{a}_{2r+s_1+s_2+3r+s_1+s_2+s_3+1} \cdots \tilde{a}_{mm}$ not in $R^2$ and
\[
Q_3 = [\tilde{a}_{2r+1} \cdots \tilde{a}_{2r+s_1+s_2+3r+s_1+s_2+s_3} (\tilde{a}_{2r+s_1+s_2+3r+s_1+s_2+s_3+1} \cdots (\tilde{a}_{mm} \tilde{z}^{-1}))^{-\frac{1}{2}} 1 \cdots 1].
\]

Then
\[
B_2 = Q_3B_1Q_3' = \begin{pmatrix} 0 & I^{(r)} \\ I^{(r)} & 0 \end{pmatrix} \oplus \begin{pmatrix} \tilde{p}^{r_1} \\ & \ddots \\ & & \tilde{p}^{r_{s_1+s_2+s_3}} \\ & & & \tilde{p}^{m-2r} \\ & & & & 0 \end{pmatrix}
\]

Since
\[
\begin{pmatrix} \tilde{p}^{r_1} & 0 \\ 0 & \tilde{p}^{r_1} \end{pmatrix} = \tilde{p}^{r_1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},
\]
\[
\begin{pmatrix} \tilde{p}^{r_{s_1+s_2+s_3}} & 0 \\ 0 & \tilde{p}^{r_{s_1+s_2+s_3}} \end{pmatrix} = \tilde{p}^{r_{s_1+s_2+s_3}} \begin{pmatrix} \tilde{z} & 0 \\ 0 & \tilde{z} \end{pmatrix},
\]
as (2),(3) using the same argument with changing $Q_1BQ_1'$, there exists $Q_4 \in \text{GL}_n(R)$ such that
\[
B_3 = Q_4B_2Q_4' = \begin{pmatrix} 0 & I^{(r)} \\ I^{(r)} & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & D_1^{(s_1)} \\ D_1^{(s_1)} & 0 \end{pmatrix} \oplus \\
\begin{pmatrix} \tilde{p}^{t_1} \\ & \ddots \\ & & \tilde{p}^{t_2+t_3} \end{pmatrix} \oplus \begin{pmatrix} \tilde{z} \tilde{p}^{t_2+t_3+1} \\ & \ddots \\ & & \tilde{z} \tilde{p}^{m-2r} \\ & & & 0 \end{pmatrix},
\]
where $D_1 = [p^{r_1}, \cdots, p^{r_{s_1}}]$. Suppose that $-1 \equiv x^2 (\text{mod} p^k)$, that $t_1$ and $t_2$ are both even or odd, and that $t_2 < t_1$, then
\[
\begin{pmatrix} 1 & xp^{t_1-t_2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{p}^{t_1} & 0 \\ 0 & \tilde{p}^{t_2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ xp^{t_1-t_2} & 1 \end{pmatrix} = \begin{pmatrix} 0 & xp^{t_2} \\ xp^{t_1-t_2} & \tilde{p}^{t_2} \end{pmatrix}.
\]
\[ Q_5 \left( \begin{array}{ccc} 0 & x^{p_{t_2+2}} & 0 \\ x^{p_{t_2+2}} & 0 & 0 \\ 0 & 0 & 0 \end{array} \right) \] 

where \( Q_5 = \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & x^{t_2-t_3} \\ 0 & 0 & 1 \end{array} \right) \), and \( t_2 > t_3 \) that are both even or odd, then

\[ Q_6 \left( \begin{array}{ccc} 0 & x^{p_{t_2+2}} & 0 \\ x^{p_{t_2+2}} & 0 & 0 \\ 0 & 0 & 0 \end{array} \right) \] 

where \( Q_6 = \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & x^{-1} & 0 \\ 0 & 0 & 1 \end{array} \right) \). Using elementary congruent transformations we can part \( t_1 \cdots t_2 + t_3, t_2 + t_3 + 1 \cdots t_{m-2r} \) into two parts such that one is even and the other is odd, then there exists \( Q_7 \in \text{GL}_n(R) \) such that \( Q_7 B_3 Q_7^t \) is equal to (1).

\[ \square \]

**Corollary 1** Let \( A, B \in A_n(R) \), then they are congruent if and only if there exist \( P, Q \in \text{GL}_n(R) \) such that \( PAP' \) and \( QBQ' \) have the same form (1).

**Corollary 2** Let \( A \in A_n(R) \) and there exists \( P \in \text{GL}_n(K) \) such that \( P \pi M P' = \left( \begin{array}{cc} 0 & I^{(r)} \\ I^{(r)} & 0 \end{array} \right) \), then \( n = 2r \) and \( M \) is congruent to \( \left( \begin{array}{cc} 0 & I^{(r)} \\ I^{(r)} & 0 \end{array} \right) \).

**Theorem 2** Let \( \omega \) be the number of orbits that linear group \( \text{GL}_n(R) \) acts on \( A_n(R) \).

(i) If \( m \) is odd and \( k \) is odd, then

\[ \omega = (m - \frac{1}{2} + 1) + \sum_{s_1 \neq 0, \text{ or } s_i' \neq 0, \text{ or } 3i} (m - \frac{1}{2} - s_1 - \frac{s_2' + s_3' + s_4' + s_5'}{2} + 1) \]

\[ \left\{ \left( \begin{array}{c} k-1 \\ 1 \end{array} \right) + \left( \begin{array}{c} k-1 \\ 2 \end{array} \right) \left( \begin{array}{c} s_1-1 \\ 1 \end{array} \right) + \cdots + \left( \begin{array}{c} k-1 \\ s_1 \end{array} \right) \right\} \]

\[ \left( \begin{array}{c} k-1 \\ s_2' \end{array} \right) \left( \begin{array}{c} k+1 \\ s_3' \end{array} \right) \left( \begin{array}{c} k-1 \\ s_4' \end{array} \right) \left( \begin{array}{c} k+1 \\ s_5' \end{array} \right) \]

(ii) If \( m \) is odd and \( k \) is even, then

\[ \omega = (m - \frac{1}{2} + 1) + \sum_{s_1 \neq 0, \text{ or } s_i' \neq 0, \text{ or } 3i} (m - \frac{1}{2} - s_1 - \frac{s_2' + s_3' + s_4' + s_5'}{2} + 1) \]

\[ \left\{ \left( \begin{array}{c} k-1 \\ 1 \end{array} \right) + \left( \begin{array}{c} k-1 \\ 2 \end{array} \right) \left( \begin{array}{c} s_1-1 \\ 1 \end{array} \right) + \cdots + \left( \begin{array}{c} k-1 \\ s_1 \end{array} \right) \right\} \]

\[ \left( \begin{array}{c} k \\ s_2' \end{array} \right) \left( \begin{array}{c} k \\ s_3' \end{array} \right) \left( \begin{array}{c} k \\ s_4' \end{array} \right) \left( \begin{array}{c} k \\ s_5' \end{array} \right) \]
(iii) If \( m \) is even and \( k \) is odd, then

\[
\omega = \left( \frac{m}{2} + 1 \right) + \sum_{s_1 \neq 0, \text{ or } s_1' \neq 0, \exists i} \left( \frac{m}{2} - s_1 - \frac{s_2' + s_3' + s_4' + s_5' + \varepsilon}{2} \right) + 1
\]

\[
\left[ \left( \begin{array}{c} k_1 - 1 \\ 1 \end{array} \right) + \left( \begin{array}{c} k - 1 \\ 2 \end{array} \right) \left( \begin{array}{c} s_1 - 1 \\ 1 \end{array} \right) + \cdots + \left( \begin{array}{c} k - 1 \\ s_1 \end{array} \right) \right]
\]

\[
\left( \frac{k-1}{s_2'} \right) \left( \frac{k+1}{s_3'} \right) \left( \frac{k-1}{s_4'} \right) \left( \frac{k+1}{s_5'} \right);
\]

(iv) If \( m \) is even and \( k \) is even, then

\[
\omega = \left( \frac{m}{2} + 1 \right) + \sum_{s_1 \neq 0, \text{ or } s_1' \neq 0, \exists i} \left( \frac{m}{2} - s_1 - \frac{s_2' + s_3' + s_4' + s_5' + \varepsilon}{2} \right) + 1
\]

\[
\left[ \left( \begin{array}{c} k_1 - 1 \\ 1 \end{array} \right) + \left( \begin{array}{c} k - 1 \\ 2 \end{array} \right) \left( \begin{array}{c} s_1 - 1 \\ 1 \end{array} \right) + \cdots + \left( \begin{array}{c} k - 1 \\ s_1 \end{array} \right) \right]
\]

\[
\left( \frac{k}{s_2'} \right) \left( \frac{k}{s_3'} \right) \left( \frac{k}{s_4'} \right) \left( \frac{k}{s_5'} \right),
\]

where \( s_2', s_3', s_4', s_5' \) are orders of the third, the fourth, the fifth and the sixth matrices in (1), respectively. When \( s_2' + s_3' + s_4' + s_5' \) is odd, let \( \varepsilon = 1 \); when \( s_2' + s_3' + s_4' + s_5' \) is even, let \( \varepsilon = 0 \).

**Proof** (i) When \( m \) is odd, \( k \) is odd and \( s_1 = s_2' = s_3 = s_4' = s_5' = 0 \), since \( 2r \leq m \Rightarrow 2r \leq m - 1 \Rightarrow r \leq \frac{m-1}{2} \), the number of \( r' \)'s is \( \frac{m-1}{2} + 1 \); When \( s_1, s_2', s_3, s_4', s_5' \) are not all zero, the number of \( r' \)'s is \( \frac{m-1}{2} - s_1 - \frac{s_2' + s_3' + s_4' + s_5' + \varepsilon}{2} + 1 \); The second matrix in (1) has \( \left( \begin{array}{c} k - 1 \\ 1 \end{array} \right) + \left( \begin{array}{c} k - 1 \\ 2 \end{array} \right) \left( \begin{array}{c} s_1 - 1 \\ 1 \end{array} \right) + \cdots + \left( \begin{array}{c} k - 1 \\ s_1 \end{array} \right) \) possible choices. The number of \( (t_1^i \cdots t_s^i)^{\prime} \)'s is \( \left( \frac{k-1}{s_1} \right) \) if \( i = 2, 4 \), and \( \left( \frac{k+1}{s_1} \right) \) if \( i = 3, 5 \), then \( \omega \) has the form in Theorem 2. By a similar argument we can conclude that there are (ii),(iii),(iv).

3. The orders of the orthogonal groups determined by \( H \) and \( \bar{H} \)

Let \( H = \left( \begin{array}{cc} 0 & I^{(r)} \\ I^{(r)} & 0 \end{array} \right), \bar{H} = \left( \begin{array}{cc} 0 & D^{(s)} \\ D^{(s)} & 0 \end{array} \right) \), where

\( D^{(s)} = [\bar{p}^{l_1}, \cdots, \bar{p}^{l_s}] \) \( 1 \leq l_1 \leq l_2 \leq \cdots \leq l_s \leq k - 1 \),

\( O_{2r}(R) = \{ A \in \text{GL}_n(R) | AH^A = H \}, O_{2r+2s}(R) = \{ B \in \text{GL}_n(R) | BHB' = \bar{H} \} \).

Let \( M(m, s, t, r_1, \cdots, r_t) = \left( \begin{array}{cc} 0 & I^{(s)} \\ I^{(s)} & 0 \end{array} \right) \otimes R^{(2t)} \), \( R^{(2t)} = \left( \begin{array}{cc} 0 & \bar{p}^{r_1} \\ \bar{p}^{r_1} & 0 \end{array} \right) \otimes \cdots \otimes \left( \begin{array}{cc} 0 & \bar{p}^{(r_t)} \\ \bar{p}^{(r_t)} & 0 \end{array} \right), 1 \leq r_1 \leq \cdots \leq r_t \leq k - 1 \),

\( 0 \leq 2t \leq m \).
Lemma 6\textsuperscript{[1,5]} Let $n(P)$ and $n(P_1)$ denote the numbers of $(r_1 + r_2)$ by $2v$ matrix $P'$s whose rank is $(r_1 + r_2)$ and $r_1$ by $2v$ matrix $P_1'$s whose rank is $r_1$. The number of $PHP'$ and $P_1HP_1'$ are, respectively, the same with that of $(r_1 + r_2)$ by $(r_1 + r_2)$ matrix and $r_1$ by $r_1$ matrix in left upper position in $M(m, s, t, r_1, \cdots, r_1)$. Let $n(P_2)$ denote the number of $P_2$'s $(r_2 \times 2v)$ which satisfies $\text{rank } P(= \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}) = r_1 + r_2$ and the number of $PHP'$ is the same with $(r_1 + r_2)$ matrix in left upper position in $M(m, s, t, r_1, \cdots, r_1)$. Hence $n(P_2)$ has no relation with the selection of $P_1$ and $n(P) = n(P_1) \times n(P_2)$.

Lemma 7 Let $n(1, 0; 2r)$ denote the number of nonzero solutions to $xHx' = 0$, then $n(1, 0; 2r) = p^{kr} - 1 - (p^{k-1})^{2rk-kr} - 1$.

Proof Let $x = (x_1 \cdots x_{2r})$, and let $n(1, 0; 2r)$ be the number of nonzero solutions to $xHx' = 0$, i.e. the number of nonzero solutions to $\sum_{i=1}^{r} x_jx_{r+j} = 0$. When $(x_1 \cdots x_r) = (0 \cdots 0)$, the number of nonzero solutions is $p^{kr} - 1$; When $(x_1 \cdots x_r) \neq (0 \cdots 0)$, let $x_j = x_j', j = 1, \cdots, k - 1$, equation $\sum_{j=1}^{r} x_jx_{r+j} = 0$ is equal to $p^i \sum_{j=1}^{r} x_{r+j}' = 0$. Then at least one of $x_{r+j}'' \cdots x_{2r-1}''$ in $R^r$. Without loss of generality, let $x''_1 \in R^r$ and $x''_{r+i} = Y, Y \in \{0 < x' x = 0\}$. We may change $\sum_{j=1}^{r} x''_{r+j} = 0$ to $x''_{r+i} = \sum_{j \neq i} x''_{r+j} + Y$. By Lemma 2 the number of solutions is $\sum_{i=0}^{k-1} (p^k - p^{k-1})^{p^{k(2r-2)-1}/p^i}$ when $(x_1 \cdots x_r) \neq (0 \cdots 0)$. Then Lemma 7 is proved. □

Lemma 8 Let $n(s, 0; 2r)$ denote the number of solutions to $PHP' = 0^{(s)}$ with rank $P_s \times 2r = s(s \leq r)$, then $n(s, 0; 2r) = \prod_{i=1}^{s} (p^k - p^{k-1})^{p^{(2r-i-1)}}$.

Proof Suppose that $P = \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix}$, where $v_i(1 \leq i \leq s)$ is a unitary vector in $P$, then $v_iHv' = 0$.

By Lemma 7 the number of $v'_i$'s is $(p^k - p^{k-1})^{p^{(2r-2)}}$. By Lemma 6, let $v_1 = (1 0 \cdots 0)$, then $v_2 = (x_1, \cdots, x_r, 0, x_{r+2}, \cdots x_{2r})$ since $v_2Hv'_1 = 0$. And since $v_2Hv'_2 = 0$, we have

$$\sum_{i=2}^{r} x_ix_{r+i} = 0, \quad (4)$$

where $x_1$ is any element in $R$. Then the number of unitary vector $v'_i$'s that satisfies (4) and is independent with $v_1$ is $p^{k}p^{k(2r-2)-4}(p^k - p^{k-1})$. By induction the number of $v'_i$'s is $(p^k - p^{k-1})^{p^{(2r-s-1)}}$. □

Lemma 9 Let $s \leq r$, then $n(2s, s; 2r) = n(s, 0; 2r) \times p^{s(k-1)}$.

Proof $n(2s, s; 2r)$ is the number of solutions to $PHP' = \begin{pmatrix} 0 \\ I^{(s)} \end{pmatrix}$, where rank $P_{2s \times 2r} = 2s$. Let $P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$, where $P_1$ and $P_2$ are $s$ by $2r$ matrices

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \begin{pmatrix} 0 & I^{(s)} \\ I^{(r)} & 0 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}' = \begin{pmatrix} 0 & I^{(s)} \\ I^{(r)} & 0 \end{pmatrix}.$$
Then
\[ P_1 HP_1' = 0, \quad P_2 HP_2' = 0, \quad P_3 HP_3' = I(s). \]
The number of \( P_1' \) is \( n(s; 0; 2r) \). Since the number of \( P_2' \) is independent with \( P_1 \), we denote \( P_1 = \begin{pmatrix} I(s) & 0 \end{pmatrix} (s, 2r-s) \), and continue to calculate the number of \( P_2' \). Set \( P_2 = \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} \), where
\[ v_1 \cdots v_s \] are unitary row vectors in \( P_2 \). First we calculate the number of \( v_1' \)s. Since \( e_1 Hv_1' = 1, e_2 Hv_1' = \cdots = e_s Hv_1' = 0 \), \( v_1 = (x_1 \cdots x_r, 1, 0 \cdots 0, x_{r+s+1} \cdots x_{2r}) \) and \( v_1 Hv_1' = 0 \), we have
\[ x_1 + \sum_{i=s+1}^{r} x_i x_{r+i} = 0. \] (5)
Therefore, \( x_2 \cdots x_s \) are any elements in \( R \) and \( x_1, x_{s+1}, \cdots x_r, x_{r+s+1} \cdots x_{2r} \) must satisfy Equation (5). Then the number of \( v_1' \) is \( p^{k(s-1)} p^{k(r-s)} = p^{k(r-1)} \). Similarly, we have \( v_2 = (x_1 \cdots x_r, 0, 1 \cdots 0, x_{r+s+1} \cdots x_{2r}) \) and clearly it is linear independent of \( v_1 \). Following \( v_2 Hv_2' = 0 \), then the number of \( v_2' \) is equal to that of \( v_1' \). By induction the number of \( v_2' \) is \( p^{k(r-1)} \). Then Lemma 9 is proved.

**Theorem 3** \( |O_{2r}(R)| = n(2r, r; 2r) = n(r, 0; 2r) \times p^{r(k(r-1))} \).

**Lemma 10** Let \( R = Z/\overline{p}^k Z, P_t \in GL_{2s_i}(R), D_t = \begin{pmatrix} 0 & D_{i} \\ D_{i} & 0 \end{pmatrix} = \overline{p}^{r_i} H_{i}, D_{i} = \text{diag}(\overline{p}^{r_i}, \cdots, \overline{p}^{r_i}) \),
\[ H_{i} = \begin{pmatrix} 0 & I(s_i) \\ I(s_i) & 0 \end{pmatrix} (0 < r_i < k), \] then the number of solutions to
\[ P_t D_t P_t' - D_t = 0 \] (6)
is
\[ p^{r_i (2s_i^2 + s_i)}|O_{2s_i}(R)|, \] (7)
where \( P_t \) is a \( 2s_i \) by \( 2s_i \) matrix over \( R \).

**Proof** First for symmetric matrix \( B \) over \( R(\pi B = 0, b_{ij} \in < \overline{p} >) \), we have \( B = \overline{p}^{r_i} B, B \in A_{2s_i}(R)(0 < l \leq k) \) and there exists \( 2s_i \) by \( 2s_i \) invertible matrix \( P_t \) over \( R \) that satisfies \( P_t H_{i} P_t' - H_i = B \). Since \( B \) is a noninvertible matrix over \( R \) and \( H_i \) is an invertible matrix over \( R \) with the same order of \( B, H_i + B \) is an invertible matrix over \( R \). By Corollary 2 there exists \( \overline{p} \in GL_{2s_i}(R) \) that satisfies \( P(H_i + B)P' = H_i, H_i + B = P^{-1} H_i P' \), i.e., equation \( P(H_i P' - H_i = B \) has at least one solution \( P_t = P^{-1} \). Secondly, we will change (6) to
\[ \overline{p}^{r_i} [P_t H_i P_t' - H_i] = 0 \] (8)
By Theorem 3 there exists \( P_t \) that satisfies \( P_t H_i P_t' - H_i = 0 \) and the number of solutions to the equation is \( |O_{2s_i}(R)| \), where \( P_t \) is a \( 2s_i \) by \( 2s_i \) invertible matrix. Clearly, the solutions to this equation are the solutions to equation (8). Let
\[ M = \{ P_t \in GL_{2s_i}(R) | \overline{p}^{r_i} [P_t H_i P_t' - H_i] = 0 \}, \]
$M_1 = \{P_iH_iP_i' - H_i|\forall P_i \in M\}$, \(M_2 = \{W \in A_{2s_i}(R)|\bar{p}^rW = 0\}\).

For any \(P_i \in M, P_iH_iP_i' - H_i = D \in A_{2s_i}(R)\) and \(\bar{p}^rH = 0, M_1 \subseteq M_2\). Homomorphism \(\varphi : P \rightarrow PH_iP_i' - H_i\) for any \(P \in M\) maps \(M\) to \(M_2\). On the other hand, \(\bar{p}^rW = 0\) for any \(W \in M_2\).

Then \(W = \bar{p}^{k-r}W\), \(W \in A_{2s_i}(R)\). Since \(0 < r_i < k, 0 < k - r_i < k\), by Lemma 10 equation \(XH_iX' - H_i = \bar{p}^{k-r}W\) i.e. \(XH_iX' - H_i = W\) has at least one solution \(X = P_i \in GL_{2s_i}(R)\), i.e. \(\varphi(P_i) = W\). Hence \(\varphi\) is surjective, i.e. \(M_1 = M_2\) and \(\ker\varphi = \{P|PH_iP_i' - H_i = 0\} = O_{2s_i}(R)\).

Since \(2s_i\) by \(2s_i\) symmetric matrix \(W\) over \(R\) is determined by \(2s_i^2 + s_i\) elements and \(\bar{p}^rW = 0\) for any \(W \in M_2\), by Lemma 2

\[
|M_2| = p^{r_s(2s_i^2 + s_i)}.
\]

By first isomorphism theorem, we know \(M/\ker\varphi \cong M_2\), then \(|M| = |\ker\varphi||M_2|\). So Lemma 10 is proved.

**Lemma 11** Suppose that \(P = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix}\), \((2r)\) \((2s_1)\) in \(GL_n(R)\) can be decomposed to

\[
P = LU, \text{ where } L = \begin{pmatrix} I & 0 & 0 \\ X & I & 0 \\ Y & Z & I \end{pmatrix}, U = \begin{pmatrix} a & u & v \\ 0 & b & w \\ 0 & 0 & c \end{pmatrix}, \text{ and } n = 2r + 2(s_1 + s_2), \text{ then this } \text{LU decomposition is unique.}
\]

**Proof** If \(P\) has another \(LU\) decomposition that \(P = L_0U_0\), where \(L_0 = \begin{pmatrix} I_1 & 0 & 0 \\ X_0 & I_2 & 0 \\ Y_0 & Z_0 & I_3 \end{pmatrix}\), \(U_0 = \begin{pmatrix} a_0 & u_0 & v_0 \\ 0 & b_0 & w_0 \\ 0 & 0 & c_0 \end{pmatrix}\), \(n = 2r + 2(s_1 + s_2)\), then \(LU = L_0U_0L_0^{-1}L = U_0U^{-1} = I\), i.e.

\[
\begin{pmatrix} I_1 & 0 & 0 \\ X_1 & I_2 & 0 \\ Y_1 & Z_1 & I_3 \end{pmatrix} = \begin{pmatrix} a_{0a}^{-1} & u_1 & v_1 \\ 0 & b_{0b}^{-1} & w_1 \\ 0 & 0 & c_{0c}^{-1} \end{pmatrix}.
\]

So \(a_{0a}^{-1} = I_1, b_{0b}^{-1} = I_2, c_{0c}^{-1} = I_3, u_1 = v_1 = w_1 = X_1 = Y_1 = Z_1 = 0; \text{then } a = a_0, b = b_0, c = c_0, L_0^{-1}L = U_0U^{-1} = I = \text{diag}\{I_1, I_2, I_3\}\). Therefore \(P\) has the unique \(LU\) decomposition.

**Theorem 4** Let \(R = Z/\bar{p}^rZ, \mathcal{D}_i = \text{diag}\{C_{(1)}, C_{(2)}, \ldots, C_{(i+1)}\}\) = \(\text{diag}\{\bar{D}_i, \bar{D}_i, \ldots, \bar{D}_i\}\), where \(C_1 = \bar{U}^{(2r)}, C_2 = \bar{D}_1, \ldots, C_{l+1} = \bar{D}_l, \bar{U}^{(2r)} = \begin{pmatrix} 0 & I^{(r)} \\ I^{(r)} & 0 \end{pmatrix}\), \(\bar{D}_i = \begin{pmatrix} 0 & D_i \\ D_i & 0 \end{pmatrix}\). \(D_i = \text{diag}\{\bar{p}^r, \ldots, \bar{p}^r\} = \bar{p}^rI^{(s_i)}\), \(\sum_{i=1}^{t} s_i = t, 1 \leq r_1 < r_2 < \cdots < r_t \leq k - 1\). Suppose that \(n\) by \(n\) matrix \(P(n = 2r + 2t) \in GL_n(R)\) is partitioned into blocks:

\[
P = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1,t+1} \\ P_{21} & P_{22} & \cdots & P_{2,t+1} \\ \cdots & \cdots & \cdots & \cdots \\ P_{t+1,1} & P_{t+1,2} & \cdots & P_{t+1,t+1} \end{pmatrix} \begin{pmatrix} (2r) \\ (2s_1) \\ \vdots \\ (2s_t) \end{pmatrix}
\]

\(2r\) \((2s_t)\) \(\cdots\) \((2s_t)\)
Then the number of solutions to $\overline{P\overline{H}}P' = \overline{H}$, where $P \in \text{GL}_n(R)$, is

$$O_{2r+2\ell}(R) = \prod_{j=2}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}| \prod_{j=3}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}| \cdots$$

$$= \prod_{j=1}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}| \prod_{i=2}^{l+1} |\{P_{ij}|P_{ij}C_i = 0\}|$$  \hspace{1cm} (12)

$$= \prod_{i=1}^{l+1} |\{P_{ii}|P_{ii}C_{i}P_{i}' = C_{i}\}| = p^E \prod_{i=2}^{l+1} \prod_{j=1}^{2s_{i-1}+r_{i-1}} |O_{2s_{i-1}}(R)||O_{2r}(R)|,$$

where

$$E = 4[r \sum_{i=1}^{l} r_i s_i + s_1 \sum_{i=2}^{l} r_i s_i + \cdots + s_{l-1} r_i s_i] + 4[r_1 s_1 \sum_{i=2}^{l} s_i + \cdots + r_{j-1} s_{j-1} \sum_{i=j}^{l} s_i + \cdots + r_{l-1} s_{l-1} s_l],$$

where the orders of rows and columns of $P_{ij}$ in (12) and $P_{ij}$ in $P$ that satisfies $\overline{P\overline{H}}P' = \overline{H}$ with form (11) are equal, but the entries in them may not be equal.

**Proof** Clearly, there exists at least one solution to $\overline{P\overline{H}}P' = \overline{H}$ ($P = I$ is a solution ). Let $P$ denote a solution to $\overline{P\overline{H}}P' = \overline{H}$ and $O_{2r+2\ell}(R)$ is the number of solutions to $\overline{P\overline{H}}P' = \overline{H}$.

Partition matrix $(P')^{-1} = B$ following $P$ is $B = (B_{ij})$. First since $\overline{P\overline{H}}P' = \overline{H}$, $\overline{P\overline{H}} = \overline{H}B$, i.e.,

$$\begin{pmatrix} P_{11} \bar{U} & P_{12} \bar{B}_1 & \cdots & P_{1{l+1}} \bar{B}_l \\ P_{21} \bar{U} & P_{22} \bar{B}_1 & \cdots & P_{2{l+1}} \bar{B}_l \\ \vdots & \vdots & \ddots & \vdots \\ P_{l+1,1} \bar{U} & P_{l+1,2} \bar{B}_1 & \cdots & P_{l+1,l+1} \bar{B}_l \end{pmatrix} = \begin{pmatrix} \bar{U} B_{11} & \bar{U} B_{12} & \cdots & \bar{U} B_{1{l+1}} \\ \bar{B}_1 B_{21} & \bar{B}_1 B_{22} & \cdots & \bar{B}_1 B_{2{l+1}} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{B}_{l+1,1} B_{l+1,2} & \bar{B}_{l+1,2} B_{l+1,2} & \cdots & \bar{B}_{l+1,l+1} \end{pmatrix}.$$  \hspace{1cm} (13)

Following (13), there exists equation

$$P_{ij} \bar{D}_{j-1} = \bar{D}_{i-1} B_{ij} (i > j),$$  \hspace{1cm} (14)

where $\bar{D}_{j-1} = \bar{p}^{r_{j-1}} \begin{pmatrix} 0 & I_{(s_{j-1})} \\ I_{(s_{j-1})} & 0 \end{pmatrix}$, and $\bar{D}_0 = \bar{U}$ when $j = 1$. Since $1 \leq r_1 < r_2 < \cdots < r_l \leq k - 1$, by Lemma 6 every element in $P_{ij} (i > j)$ is in $(\bar{p})$. Then $P_{ii} (i = 1, 2, \cdots, l + 1)$ is invertible since $P$ is invertible. Therefore $P$, the solution to $\overline{P\overline{H}}P' = \overline{H}$, has $LU$ decomposition by Lemma 11.
Secondly, we will calculate $O_{2r+2t}(R)$. Without loss of generality we only prove for $3 \times 3$ partitioned matrix $((\mathcal{P} = \text{diag}\{C_1, C_2, C_3\}))$. Let the $n$ by $n$ invertible matrix ($n = 2r + 2t$, $t = s_1 + s_2$)

$$P = \begin{pmatrix}
P_{11} & P_{12} & P_{13} \\
P_{21} & P_{22} & P_{23} \\
P_{31} & P_{32} & P_{33}
\end{pmatrix} \begin{pmatrix}
(2r) \\
(2s_1) \\
(2s_2)
\end{pmatrix}$$

(15)

be one solution to $P\mathcal{P}P' = \mathcal{P}$, where $C_1 = \bar{U}^{(2r)}$, $C_2 = \bar{D}_1, C_3 = \bar{D}_2, \bar{D}_1, \bar{D}_2$ are respectively $2s_1$ by $2s_1$ and $2s_2$ by $2s_2$ matrices that satisfy Theorem 4.

Let

$$G_P = \{ P \in \text{GL}_n(R) | P\mathcal{P}P' = \mathcal{P} \},$$

$$A = \left\{ \bar{P} \in \text{GL}_n(R) \left| \begin{array}{c}
P\mathcal{P}P' = \mathcal{P}, P' = \begin{pmatrix}
I & 0 & 0 \\
A_{21} & I & 0 \\
A_{31} & A_{32} & I
\end{pmatrix}
\end{array} \right. \right\},$$

$$H' = \left\{ \bar{P} \in \text{GL}_n(R) \left| \begin{array}{c}
P\mathcal{P}P' = \mathcal{P}, P' = \begin{pmatrix}
H_{11} & H_{12} & H_{13} \\
0 & H_{22} & H_{23} \\
0 & 0 & H_{33}
\end{pmatrix}
\end{array} \right. \right\}.$$ 

By Lemma 11 since $G_P \subseteq \text{GL}_n(R)$,

$$P = LU$$

(16)

for any $P \in G_P$, where

$$L = \begin{pmatrix}
I & 0 & 0 \\
X & I & 0 \\
Y & Z & I
\end{pmatrix}, U = \begin{pmatrix}
a & u & v \\
b & w & 0 \\
c & 0 & 0
\end{pmatrix}.$$ 

Note that $L$ may be not in $A$ and $U$ may be not in $H$.

Since $LU$ decomposition (16) is unique, we will calculate the number of $L$ and $U$ for any $P \in G_P$, i.e. $n(P)$ the number of $P \in G_P$. Let

$$\bar{L} = \left\{ \begin{array}{c}
\begin{pmatrix}
I & 0 & 0 \\
\Delta_{21} & I & 0 \\
\Delta_{31} & \Delta_{32} & I
\end{pmatrix} \left| \Delta_{21}, \Delta_{31}, \Delta_{32} \text{(the elements in them are in } R) \right.
\end{array} \right\},$$

$$\bar{U} = \left\{ \begin{array}{c}
\begin{pmatrix}
\bar{a} & \alpha_1 & \alpha_2 \\
0 & \bar{b} & \alpha_3 \\
0 & 0 & \bar{c}
\end{pmatrix} \left| \alpha_1, \alpha_2, \alpha_3 \text{(the elements in them are in } R), \text{ and } \bar{a}, \bar{b}, \bar{c} \text{(the elements in them are in } R^* \right.
\end{array} \right\}.$$ 

Clearly, $\bar{L}$ and $\bar{U}$ are groups, and $A$ and $H'$ are respectively their subgroups. Then there exist the coset decompositions of $\bar{L}$ and $\bar{U}(L \in \bar{L}, U \in \bar{U})$

$$\bar{L} = \bigcup_{t \in \bar{L}} tA, \bar{U} = \bigcup_{u \in \bar{U}} H'u.$$ 

So $LU$ decomposition (16) can be rewritten as

$$P = l_P\mathcal{P}u_P,$$  

(17)
where $L \in A, \hat{U} \in H', l_P \in \hat{L}$ and $u_P \in \hat{U}$. Then $n(P)$ is determined by the elements in $A$ and $H'$, i.e. $|G_P| \leq |A||H'|$. On the other hand, $A, H' \subseteq G_p$ and $A \cap H' = \{1\}$, then $|G_P| \geq |A||H'|$. So

$$|G_P| = |A||H'|. \quad (18)$$

For the convenience let $P_{ij}$ denote $A_{ij}(i > j)$ in $A$ and $P_{ij}$ denote $H_{ij}(i < j)$ in $H$.

We will calculate $|H'|$ at first. For any $\bar{P} = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ 0 & P_{22} & P_{23} \\ 0 & 0 & P_{33} \end{pmatrix} \in H'$, $\bar{P}$ can be decomposed uniquely into

$$\bar{P} = \begin{pmatrix} I & P_{12}P_{22}^{-1} & (P_{13} - P_{12}P_{22}^{-1}P_{23})P_{33}^{-1} \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix} \begin{pmatrix} P_{11} & 0 & 0 \\ 0 & P_{22} & P_{23} \\ 0 & 0 & P_{33} \end{pmatrix} = \hat{P}_1\hat{P}_2. \quad (19)$$

Let $H_1 = \left\{ \begin{pmatrix} I & \omega_1 & \omega_2 \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix} | \, \omega_1, \omega_2 \text{(the elements in them are in } R) \right\},$

$$H_2 = \left\{ \begin{pmatrix} P_{11} & 0 & 0 \\ 0 & P_{22} & \omega_3 \\ 0 & 0 & P_{33} \end{pmatrix} | \, \omega_3 \text{(the elements in it are in } R) \right\}.$$}

It is easy to prove that $H_1$ and $H_2$ are groups and $\overline{H}_1 = \{ P \in H_1 | P\overline{H}P' = \overline{H} \}$ and $\overline{H}_2 = \{ P \in H_2 | P\overline{H}P' = \overline{H} \}$ are respectively the subgroups of $H_1$ and $H_2$. Then there exist the coset decompositions of $H_1$ and $H_2(\hat{P}_1 \in H_1, \hat{P}_2 \in H_2)$, i.e. $H_1 = \cup_{h_1 \in H_1} h_1\overline{H}_1, H_2 = \cup_{h_2 \in H_2} h_2\overline{H}_2$. So by an argument similar to the preceding there exists the following equation

$$|H'| = |\overline{H}_1||\overline{H}_2|. \quad (20)$$

Since $P\overline{H}P' = \overline{H}$ for any $P = \begin{pmatrix} I & P_{12} & P_{13} \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix} \in \overline{H}_1$, $P_{12}C_2 = 0, P_{13}C_3 = 0$. Then

$$|\overline{H}_1| = |\{(P_{12}, P_{13})| P_{12}C_2 = 0, P_{13}C_3 = 0\}| = |\{(P_{12}| P_{12}C_2 = 0\})||\{P_{13}| P_{13}C_3 = 0\}|. \quad (21)$$

For any $P = \begin{pmatrix} P_{11} & 0 & 0 \\ 0 & P_{22} & P_{23} \\ 0 & 0 & P_{33} \end{pmatrix} \in \overline{H}_2$, $P$ can be decomposed uniquely into

$$P = \begin{pmatrix} I & 0 & 0 \\ 0 & I & P_{23}P_{33}^{-1} \\ 0 & 0 & I \end{pmatrix} \begin{pmatrix} P_{11} & 0 & 0 \\ 0 & P_{22} & 0 \\ 0 & 0 & P_{33} \end{pmatrix}.$$}

Set

$$\tilde{H}_2 = \left\{ \begin{pmatrix} I & 0 & 0 \\ 0 & I & * \\ 0 & 0 & I \end{pmatrix} | \, * \text{ (the elements in it are in } R) \right\},$$

$$\tilde{\overline{H}}_2 = \left\{ \begin{pmatrix} P_{11} & 0 & 0 \\ 0 & P_{22} & 0 \\ 0 & 0 & P_{33} \end{pmatrix} | \, P_{11}, P_{22}, P_{33} \text{(the elements in them are in } R^*) \right\}.$$
Similarly, for any 

\[ H_2^{(1)} = \{ P \in \overline{H}_2 | P \overline{H} P' = \overline{H} \}, \]

\[ H_2^{(2)} = \{ P \in \overline{H}_2 | P \overline{H} P' = \overline{H} \}, \]

where \( H_2^{(1)}, H_2^{(2)} \) are the subgroups of \( \overline{H}_2, \overline{H}_2 \). Then \( |\overline{H}_2| = |H_2^{(1)}||H_2^{(2)}| \).

For any \( P = \begin{pmatrix} I & 0 & 0 \\ 0 & I & P_{23} \\ 0 & 0 & I \end{pmatrix} \) \in H_2^{(1)} \), since \( P \overline{H} P' = \overline{H} \), \( P_{23} C_3 = 0 \). So

\[ |H_2^{(1)}| = \{ P_{23} P_{23} C_3 = 0 \}. \]

Similarly, for any \( P = \begin{pmatrix} P_{11} & 0 & 0 \\ 0 & P_{22} & 0 \\ 0 & 0 & P_{33} \end{pmatrix} \) \in H_2^{(2)} \), since \( P \overline{H} P' = \overline{H} \),

\[ |H_2^{(2)}| = \{ P_{11} P_{11} C_1 P_{33} = C_1 \}|\{ P_{22} P_{22} C_2 P_{22} = C_2 \}|\{ P_{33} P_{33} C_3 P_{33} = C_3 \}. \]

Then

\[ |\overline{H}_2| = \{ P_{23} P_{23} C_3 = 0 \}\prod_{i=1}^{3} \{ P_{ii} P_{ii} C_i P_{ii} = C_i \}. \tag{22} \]

Combining (21), (22) and (20), we have

\[ |H| = \prod_{j=2}^{3} \{ P_{ij} P_{ij} C_j = 0 \} \prod_{j=3}^{3} \{ P_{ij} P_{ij} C_j = 0 \} \prod_{i=1}^{3} \{ P_{ii} P_{ii} C_i P_{ii} = C_i \}. \tag{23} \]

Next we will count \(|A|\) in (18). For any \( \overline{P} = \begin{pmatrix} I & 0 & 0 \\ P_{21} & I & 0 \\ P_{31} & P_{32} & I \end{pmatrix} \in A, \overline{P} \) can be decomposed uniquely into

\[ \overline{P} = \begin{pmatrix} I & 0 & 0 \\ P_{21} & I & 0 \\ P_{31} & P_{32} & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & P_{32} & I \end{pmatrix} = \overline{P}_1 \overline{P}_2. \]

Set \( A_1 = \left\{ \begin{pmatrix} I & 0 & 0 \\ X & I & 0 \\ Y & 0 & I \end{pmatrix} \mid X, Y \text{ (the elements in them are in } R \text{)} \right\}, \]

\[ A_2 = \left\{ \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & Z & I \end{pmatrix} \mid Z \text{ (the elements in it are in } R \text{)} \right\}, \]

\( \overline{A}_1 = \{ P \in A_1 | P \overline{H} P' = \overline{H} \}, \overline{A}_2 = \{ P \in A_2 | P \overline{H} P' = \overline{H} \}. \) Then \( \overline{A}_1 \) and \( \overline{A}_2 \) are respectively the subgroups of \( A_1 \) and \( A_2 \) and \( \overline{P}_1 \in A_1, \overline{P}_2 \in A_2 \). By an argument similar to the preceding we get

\[ |A| = |\overline{A}_1||\overline{A}_2|. \tag{24} \]

Since \( P \overline{H} P' = \overline{H} \), for \( P = \begin{pmatrix} I & 0 & 0 \\ P_{21} & I & 0 \\ P_{31} & P_{32} & I \end{pmatrix} \) \in \overline{A}_1, P_{21} C_1 = 0, P_{31} C_1 = 0. Therefore,

\[ |\overline{A}_1| = \{ P_{21} P_{21} C_1 = 0 \}|\{ P_{31} P_{31} C_1 = 0 \}. \]
Similarly, \(|\overline{\mathcal{A}}_2| = \left\{ P = \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & P_{32} \end{pmatrix} \in \overline{\mathcal{A}}_2 | P\mathbf{P}' = \mathbf{P} \right\} = \{|P_{32}|P_{32}C_2 = 0\}|.

So

\[|A| = \prod_{i=2}^{3} \left( |\{P_{ij}|P_{ij}C_1 = 0\}| \prod_{j=3}^{3} |\{P_{2j}|P_{2j}C_j = 0\}| \prod_{i=2}^{3} |\{P_{ij}|P_{ij}C_1 = 0\}| \right)

\tag{25}\]

Combining (23), (25) and (18), we have

\[|G_P| = \prod_{j=2}^{3} |\{P_{ij}|P_{ij}C_j = 0\}| \prod_{j=3}^{3} |\{P_{2j}|P_{2j}C_j = 0\}| \prod_{i=2}^{3} |\{P_{ij}|P_{ij}C_1 = 0\}| \prod_{j=2}^{3} \left( \prod_{i=1}^{3} |\{P_{ij}|P_{ij}C_iP'_{ji} = C_i\}| \right).

\tag{26}\]

By induction the number of solutions to \(P\mathbf{P}' = \mathbf{P}\), where \(P\) is invertible, is

\[O_{2r+2l}(R) = \left( \prod_{j=2}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}| \prod_{j=3}^{l+1} |\{P_{2j}|P_{2j}C_j = 0\}| \right) \cdots
\]

\[\prod_{j=l+1}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}| \prod_{i=2}^{l+1} |\{P_{ij}|P_{ij}C_1 = 0\}| \cdots
\]

\[\prod_{i=l+1}^{l+1} |\{P_{ij}|P_{ij}C_i = 0\}| \prod_{i=1}^{l+1} |\{P_{ij}|P_{ij}C_iP'_{ji} = C_i\}|.
\]

\tag{27}\]

Since \(C_1 = \overline{\mathbf{U}}^{(2r)}\) is invertible,

\[|\{P_{ij}|P_{ij}C_1 = 0\}| = 1, i = 2, \cdots, l + 1.
\]

Note that \(C_j = \overline{\mathbf{U}}_{j-1} = \overline{\mathbf{P}}r_{j-1}H_{j-1}(j = 2, \cdots, l + 1)\). Hence when \(i \neq j, j \neq 1\), by Lemma 2 we have

\[|\{P_{ij}|P_{ij}C_j = \overline{\mathbf{P}}r_{j-1}P_{ij} = 0\}| = pr_{j-1}(2^{s_j-1} \times 2^{s_{j-1}}),\]

\tag{29}\]

where \(2s_{i-1}, 2s_{j-1}\) are respectively the orders of rows and columns in \(P_{ij}\). \(2s_{i-1} = 2s_0 = 2r\) when \(i = 1\). Since \(C_1 = \overline{\mathbf{U}}^{(2r)}\), by Theorem 3, we have

\[|\{P_{ij}|P_{ij}C_1P'_{ji} = C_i\}| = n(r, s; 0; 2r) \times pr^{k(r-1)},\]

\tag{30}\]

where when \(i = 2, \cdots, l + 1, P_{ij}C_iP'_{ji} = P_{ii}\overline{\mathbf{U}}_{i-1}P_{ij} = C_i = \overline{\mathbf{U}}_{i-1}.\) By Lemma 10 we have

\[|\{P_{ii}|P_{ii}C_iP'_{ji} = C_i\}| = pr_{i-1}^{(2^{s_{i-1}}+s_i)}|O_{2s_{i-1}}(R)|.
\]

\tag{31}\]

Furthermore, by (29), we have

\[N_1 = \prod_{j=2}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}| \prod_{j=3}^{l+1} |\{P_{2j}|P_{2j}C_j = 0\}| \prod_{i=2}^{l+1} |\{P_{ij}|P_{ij}C_j = 0\}|
\]

\[= pr_{1}(2r \times 2s_1) \cdots + \cdots + r_l(2r \times 2s_l) + r_1(2s_1 \times 2s_1) + \cdots + r_l(2s_{l-1} \times 2s_l)
\]

\[= p^{4[r \sum_{i=1}^{l} s_i + s_1 - \sum_{j=2}^{l} s_i + s_1 - 1]}.\]

\tag{32}\]
By (28) and (29),
\[ N_2 = \left( \prod_{i=1}^{l+1} |\{P_{j1}|P_{j1}C_1 = 0\}| \cdots \prod_{i=1}^{l+1} |\{P_{i0}|P_{i0}C_0 = 0\}| \right) \]
\[ = p \sum_{i=2}^{4+1} (r_i s_i + r_{j-1} s_{j-1}) \sum_{i=2}^{4+1} (r_i s_i + r_{j-1} s_{j-1}) \]
\[ = p. \tag{33} \]

By (30) and (31),
\[ N_3 = \left( \prod_{i=1}^{l+1} |\{P_{j1}|P_{j1}C_1 = C_i\}| \right) = \left( \prod_{i=2}^{l+1} p^{r_i - 1(2^j - 1 + s_i - 1)} |O_{2s_i - 1}(R)||O_{2r}(R)|. \tag{34} \]

Then by (32), (33), (34) and (27), \(O_{2r+2l}(R)\) is equal to (12).

\[ \square \]

**Theorem 5** If the normal form of \( A (A \in A_m(R)) \) is \( \bar{H} \oplus (0) \), then the number of symmetric matrices (in \( A_m(R) \)) that are in the same orbit with \( A \) is

\[ p^{km} \prod_{i=1}^{m-1} \left( 1 - \frac{1}{m^{i-1}} \right). \tag{35} \]

**Proof** Let \( M = \{ PAP' | P \in GL_m(R) \} \) be the set that the elements in it are in the same orbit with \( A \). Then \( |M| = \frac{|GL_m(R)|}{|G_A|} \), where \( G_A = \{ P \in GL_m(R) | PAP' = A \} \). By Theorem 1 there exists \( P_0 \in GL_m(R), \) such that \( P_0A P_0^t = \bar{H} \oplus (0) = Q = \text{diag}(U^{2r}, D^{2t}, 0^{m-2r-2t}) \), where \( U^{2r} = \left( \begin{array}{cc} I^{(r)} & 0 \\ 0 & D \end{array} \right), \)

\[ D = \left( \begin{array}{cc} 0 & D_i \\ D_i & 0 \end{array} \right) \].

Set \( M_1 = \{ P_0 P P_0^{-1} | P \in G_A \}, M_2 = \{ \bar{P} \in GL_m(R) | \bar{P} Q \bar{P}' = Q \}, M_2 = \{ P_0^{-1} \bar{P} P_0 | \bar{P} \in M_2 \}. \]

Clearly, \( |G_A| = |M_1|, |M_2| = |M_2| \).

Since \( A = P_0^{-1} Q (P_0^{-1}) \), for any \( P \in G_A, PAP' = A, PP_0^{-1} Q (P_0^{-1}) \), and \( P_0 P_0^{-1} Q (P_0^{-1}) \), i.e. \( P_0 P_0^{-1} \in M_2, |G_A| \leq |M_2| \); similarly, we have \( |M_2| \leq |G_A| = |M_1| \), so \( |G_A| = |M_2| \). Then \( |G_A| = |G_Q| (G_Q = \{ \bar{P} Q \bar{P}' = Q \}). \)

Since equation \( \bar{P} Q \bar{P}' = Q \)

has at least one solution (\( P = I \)), each block \( P_{ij} \) exists when \( P \) is partitioned into blocks. We partition \( P, (P')^{-1} = B, \) and \( P, \bar{P}, (P')^{-1} \) following partitioned matrix \( Q \):

\[ \bar{P} = \begin{pmatrix} \bar{P}_{11} & \bar{P}_{12} & \bar{P}_{13} \\ \bar{P}_{21} & \bar{P}_{22} & \bar{P}_{23} \\ \bar{P}_{31} & \bar{P}_{32} & \bar{P}_{33} \end{pmatrix} \quad \begin{pmatrix} 2r \\ 2t \end{pmatrix} \quad \begin{pmatrix} 2r \\ 2t \end{pmatrix} \quad (m-2r-2t) \]

\[ \bar{P}' = \begin{pmatrix} \bar{P}'_{11} & \bar{P}'_{12} & \bar{P}'_{13} \\ \bar{P}'_{21} & \bar{P}'_{22} & \bar{P}'_{23} \\ \bar{P}'_{31} & \bar{P}'_{32} & \bar{P}'_{33} \end{pmatrix} \quad \begin{pmatrix} 2r \\ 2t \end{pmatrix} \quad \begin{pmatrix} 2r \\ 2t \end{pmatrix} \quad (m-2r-2t) \]

\[ (P')^{-1} = B = \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{pmatrix}, \]
Since $PQP' = Q$, 
\[
\begin{align*}
P_{11}U'P_{11}' + P_{12}DP'_{12} &= \bar{U} \\
P_{11}U'P_{21}' + P_{12}DP'_{22} &= 0 \\
P_{11}U'P_{31}' + P_{12}DP'_{32} &= 0 \\
P_{21}U'P_{11}' + P_{22}DP'_{12} &= 0 \\
P_{21}U'P_{21}' + P_{22}DP'_{22} &= \bar{D} .
\end{align*}
\]
(38)

Then it is easily seen that $\tilde{P}_{13}, \tilde{P}_{23}$ and $\tilde{P}_{33}$ are not in Equation (38). Hence $\tilde{P}_{13}$ and $\tilde{P}_{23}$ are any $(2r) \times (m - 2r - 2t)$ and $(2t) \times (m - 2r - 2t)$ matrices respectively and $P_{31}$ is any matrix in $\text{GL}_{(m - 2r - 2t)}(R)$. So

the number of possible choices of $\tilde{P}_{13} = p^{2kr(m - 2r - 2t)}$, \hspace{1cm} (39)

the number of possible choices of $\tilde{P}_{23} = p^{2kt(m - 2r - 2t)}$, \hspace{1cm} (40)

the number of possible choices of $\tilde{P}_{33} = p^{k(m - 2r - 2t)^2 - \frac{m - 2r - 2t}{i=0} (1 - \frac{1}{p^{m - 2r - 2t - 1}})}$. \hspace{1cm} (41)

Since $\bar{P} = Q(\bar{P})^{-1}$ and $Q \bar{P}' = \bar{P}^{-1} Q$, $\bar{P}_{31}\bar{U} = 0, \bar{P}_{32}\bar{D} = 0, \bar{U}\bar{P}_{31}' = 0, \bar{D}\bar{P}_{32}' = 0, \bar{P}_{21}\bar{U} = \bar{D}\bar{B}_{21}$. $\bar{U}$ is invertible so $\bar{P}_{31} = 0, \bar{P}_{31}' = 0$. By Lemma 6 we know that all of the elements in $\tilde{P}_{21}, \tilde{P}_{32}$ and $\tilde{P}_{32}'$ are in $\langle \tilde{p} \rangle$. Since $\bar{P}$ is invertible, $\tilde{P}_{11}, \tilde{P}_{22}, \tilde{P}_{33}$ are invertible in $R$. By $\tilde{P}_{31}\tilde{U} = 0, \tilde{P}_{32}\tilde{D} = 0, \tilde{U}\tilde{P}_{31}' = 0$ and $\tilde{D}\tilde{P}_{32}' = 0$, (38) is equivalent with

\[
\begin{align*}
P_{11}U'P_{11}' + P_{12}DP'_{12} &= \bar{U} \\
P_{11}U'P_{21}' + P_{12}DP'_{22} &= 0 \\
P_{21}U'P_{11}' + P_{22}DP'_{12} &= 0 \\
P_{21}U'P_{21}' + P_{22}DP'_{22} &= \bar{D} \\
\Rightarrow \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix} \begin{pmatrix} \bar{U} & 0 \\ 0 & \bar{D} \end{pmatrix} = \begin{pmatrix} P_{11}' & P_{12}' \\ P_{21}' & P_{22}' \end{pmatrix}
\end{align*}
\]
(42)

Put $P = \begin{pmatrix} \tilde{P}_{11} & \tilde{P}_{12} \\ \tilde{P}_{21} & \tilde{P}_{22} \end{pmatrix}$, $D = \begin{pmatrix} \bar{U} & 0 \\ 0 & \bar{D} \end{pmatrix}$, hence the number of solutions to (42) is equivalent with that of $P\bar{P}\bar{P}' = \bar{H}$ in Theorem 4. So by Theorem 4 we have the number of solutions to (42). Since $\tilde{P}_{32}\bar{D} = 0$, we partition $\tilde{P}_{32}$ into blocks: $(V_1V_2\cdots V_l)$, where $V_i(i = 1, 2, \cdots, l)$ is $(m - 2r - 2t) \times (2s_i)$ matrix and

\[
\bar{D} = \text{diag}\{\bar{D}_1, \cdots, \bar{D}_t\}, \bar{D}_i = \begin{pmatrix} 0 & D_i \\ D_i & 0 \end{pmatrix}, \sum_{i=1}^{l} s_i = t.
\]

Hence $V_i\bar{D}_i = 0(i = 1, \cdots, l)$. By Lemma 2 the number of possible choices of $\tilde{P}_{32}$ is

\[
p^{r_1(m - 2r - 2t)/2s_1 + \cdots + r_l(m - 2r - 2t)/2s_l} = p^{2(m - 2r - 2t)\sum_{i=1}^{l} r_is_i}.
\]
(43)
By combining (12), (39), (40), (41), (43) and (36), Theorem 5 is proved.

References:


有限局部环上对称矩阵的计数定理 (I)

刘岩 1, 南基洙 2

(1. 北京交通大学数学系，北京 100044；2. 大连理工大学应用数学系，辽宁 大连 116024)

摘要：设 $A_n(R)$ 是有限局部环 $\mathbb{Z}/p^k\mathbb{Z}$ 上 $n$ 阶对称矩阵的集合，这里 $n \geq 2$, $p$ 是大于 2 素数，
$p \equiv 1(\text{mod} 4)$ 和 $k > 1$. 通过确定有限局部环 $\mathbb{Z}/p^k\mathbb{Z}$ 上对称矩阵的标准型，计算出 $A_n(R)$ 在线性群 $GL_n(R)$ 作用下的轨道数。从而计算出由特定对称矩阵确定的正交群的阶以及与特定对称矩阵在同一轨道的对称矩阵的阶。

关键词：合同变换，对称矩阵标准型，正交群，轨道。