Partition, Construction, and Enumeration of M–P Invertible Matrices over Finite Fields

Zongduo Dai and Yufeng Zhang

State Key Laboratory of Information Security, Department of Mathematics, Graduate School, University of Science and Technology of China, 100039-08, Beijing, People’s Republic of China
E-mail: yangdai@mimi.cnc.ac.cn

Communicated by Zhe-Xian Wan

Received December 16, 1999; revised December 6, 2000; published online June 11, 2001

A necessary and sufficient condition for an \( m \times n \) matrix \( A \) over \( F \) having a Moor–Penrose generalized inverse (M–P inverse for short) was given in (C. K. Wu and E. Dawson, 1998, Finite Fields Appl. 4, 307–315). In the present paper further necessary and sufficient conditions are obtained, which make clear the set of \( m \times n \) matrices over \( F \) having an M–P inverse and reduce the problem of constructing M–P invertible matrices to that of constructing subspaces of certain type with respect to some classical groups. Moreover, an explicit formula for the M–P inverse of a matrix which is M–P invertible is also given. Based on this reduction, both the construction problem and the enumeration problem are solved by borrowing results in geometry of classical groups over finite fields (Z. X. Wan, 1993, “Geometry of Classical Groups over Finite Fields,” Studentlitteratur, Chatwell Bratt). © 2001 Academic Press

Key Words: Moor–Penrose generalized inverse; finite field; orthogonal group; pseudo-symplectic group

1. INTRODUCTION

The concept Moor–Penrose generalized inverse [1], which will be simply called the M–P inverse, of a matrix of order \( m \times n \) over a field \( F \) was proposed by Moor (in 1920, 1935) and Penrose (in 1955) for the case when \( F \) is the real field or the complex field, respectively. Penrose proved that every matrix over the real field or complex field does have an M–P inverse, and its M–P inverse is unique. Recently, the M–P inverses of matrices over a finite field \( F_q \) are considered in some cryptographic applications [2]. Unlike the case when \( F \) is the real or the complex field, it is not necessary that every matrix over an
arbitrary field has an M–P inverse. A matrix will be said to be M–P invertible if it has an M–P inverse. A necessary and sufficient condition for an \( m \times n \) matrix \( A \) over \( F_q \) having an M–P inverse was given in [3]. In the present paper further necessary and sufficient conditions are obtained, which make clear the set of \( m \times n \) matrices over \( F_q \) of rank \( r \) and having an M–P inverse and reduce the problem of constructing M–P invertible matrices to the problem of constructing vector subspaces of certain type with respect to the orthogonal groups or pseudo-symplectic groups, depending on \( q \) being odd or even. Moreover, an explicit formula for the M–P inverse of a matrix which is M–P invertible is also given. Based on this reduction, both the construction problem and the enumeration problem are solved by borrowing results in geometry of classical groups over finite fields [4].

2. CRITERIA AND PARTITION OF M-P INVERTIBLE MATRICES

Let \( M_{m,n}(F) \) denote the set of \( m \times n \) matrices over the field \( F \). A matrix \( X \) in \( M_{n,m}(F) \) is called as an M–P inverse of a matrix \( A \) in \( M_{m,n}(F) \) if it satisfies the following four conditions,

\[
\begin{align*}
AXA &= A \\
XAX &= X \\
(AX)^\dagger &= AX \\
(XA)^\dagger &= XA
\end{align*}
\]

where \( A^\dagger \) denotes the transpose of \( A \). The matrix \( A \) is called M–P invertible if \( A \) has an M–P inverse. From the definition we see if \( X \) is an M–P inverse of \( A \), then \( A \) is also an M–P inverse of \( X \), and \( X^\dagger \) is an M–P inverse of \( A^\dagger \) too.

We follow the notation of [4]. The set of \( n \times n \) nonsingular matrices over \( F \) is denoted by \( GL_n(F) \). We use

\[
F^{(n)} = \{(x_1, x_2, \ldots, x_n) | x_i \in F, i = 1, 2, \ldots, n\}
\]

to denote the \( n \)-dimensional row vector space over \( F \). Let \( R \) be an \( r \)-dimensional vector subspace of \( F^{(n)} \), and let \( v_1, v_2, \ldots, v_r \) be a basis of \( R \). We
use the $r \times n$ matrix

$$
\begin{pmatrix}
v_1 \\
v_2 \\
\vdots \\
v_r
\end{pmatrix}
$$

to represent the vector subspace $R$ and write

$$
R = \begin{pmatrix}
v_1 \\
v_2 \\
\vdots \\
v_r
\end{pmatrix}
$$

i.e., we use the same letter $R$ to denote a matrix which represents the vector subspace $R$ and call the matrix $R$ a matrix representation of the vector subspace $R$. It should be noted that a matrix representing an $r$-dimensional vector subspace in $F^{(n)}$ is an $r \times n$ matrix of rank $r$. It is clear that two $r \times n$ matrices $R$ and $T$ of rank $r$ represent the same $r$-dimensional vector subspace if and only if there is an $r \times r$ nonsingular matrix $b$ such that $R = bT$.

In this paper, for any matrix $A$ in $M_{m,n}(F)$, we denote by $L(A)$ the vector subspace spanned by all the rows of $A$ in $F^{(n)}$ and by $L(A^\top)$ the vector subspace spanned by the transpose of all the columns of $A$ in $F^{(m)}$. We always let $C$ be an $r$-dimensional vector subspace of $F^{(m)}$ and let $R$ be an $r$-dimensional vector subspace of $F^{(n)}$. We fix a matrix representation of the vector subspace $R$ and denote it also by $R$, as mentioned above. Similarly we fix a matrix representation of the vector subspace $C$ and denote it also by $C$. We denote by $M_{m,n}(F,r)$ the set of $m \times n$ matrices of rank $r$ over $F$ and denote by $M_{m,n}(F,r,C,R)$ the set of matrices $A$ in $M_{m,n}(F,r)$ with $L(A^\top) = C$ and $L(A) = R$. We denote by $F^{(n)}(r)$ the set of $r$-dimensional subspaces in $F^{(n)}$.

The following disjoint union is clear:

$$
M_{m,n}(F,r) = \bigcup_{(C,R) \in F^{(m)}(r) \times F^{(n)}(r)} M_{m,n}(F,r,C,R).
$$

**Lemma 2.1.** Let $A \in M_{m,n}(F)$. Then $A \in M_{m,n}(F,r,C,R)$ if and only if $A = C'aR$ for some $a \in GL_r(F)$; moreover, if this is the case, then the matrix $a$ is uniquely determined by $A$. In other words, the map $a \mapsto C'aR$ is a bijection from $GL_r(F)$ to $M_{m,n}(F,r,C,R)$. 
\textbf{Proof.} “Only if” part: There exist $Q \in GL_m(F)$ and $P \in GL_n(F)$ such that

$$A = Q \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} P.$$  

Here $I_r$ denotes the $r \times r$ identity matrix. Then

$$R = L(A) = L(Q^{-1}A) = L((I_r & 0)P);$$

hence $bR = (I_r & 0)P$ for some $b \in GL_r(F)$. We also have $A^t = P^t \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q^t$. Then

$$C = L(A^t) = L((I_r & 0)Q^t);$$

hence $dC = (I_r & 0)Q^t$ for some $d \in GL_r(F)$. Therefore

$$A = Q \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} P = Q \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} (I_r & 0)P = (dC)^t bR = C^t aR,$$

where $a = d^t b \in GL_r(F)$.

“If” part: There exist some $Q \in GL_m(F)$ and $P \in GL_n(F)$ such that

$$C = (I_r & 0)Q^t, \quad R = (I_r & 0)P,$$  

(6)

so we have

$$A = C^t aR = Q \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} a(I_r & 0)P = Q \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} P.$$  

(7)

Therefore

$$L(A) = L(Q^{-1}A) = L((a & 0)P) = L((I_r & 0)P) = L(R)$$

from (6) and (7). We also have

$$A^t = P^t \begin{pmatrix} a^t & 0 \\ 0 & 0 \end{pmatrix} Q^t$$

from (7), and therefore

$$L(A^t) = L((P^t)^{-1} A^t) = L((a^t & 0)Q^t) = L((I_r & 0)Q^t) = L(C);$$

thus $A \in M_{m,n}(F, r, C, R)$. 

“Uniqueness” part: Let $P$ and $Q$ be defined by (6); then $A = Q \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} P$ holds true whenever $A = C^i a R$. If $A = C^i a R = C^i b R$, then

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = Q^{-1} A P^{-1} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix};$$

hence $a = b$. ■

**Lemma 2.2.** Let $A \in M_{m,n}(F, r, C, R)$ be M–P invertible, and let $X$ be an M–P inverse of $A$. Then $X \in M_{n,m}(F, r, R, C)$.

**Proof.** Note that

$$L(A) = L(AXA) \subseteq L(XA) = L(A^t X^r) \subseteq L(X^r) \quad (8)$$

and

$$L(X) = L(XAX) \subseteq L(XA) = L(X^r A^t) \subseteq L(A^t), \quad (9)$$

Thus $\dim((L(A)) \leq \dim((L(X^r))) = \dim((L(X))) \leq \dim((L(A^t))) = \dim((L(A)))$. Therefore $\dim(L(A)) = \dim(L(X^r))$, and $\dim(L(A^t)) = \dim(L(X))$. The former together with (8) leads to $R = L(A) = L(X^r)$, and the latter together with (9) implies $L(X) = L(A^t) = C$; hence $X \in M_{n,m}(F, r, R, C)$. ■

**Theorem 2.1.** (Formula for M–P inverse). Let $A \in M_{m,n}(F, r, C, R)$. If $A$ is M–P invertible, then both $CC^r$ and $RR^r$ are nonsingular, and $R^r(CAR^r)^{-1} C$ is the unique M–P inverse of $A$.

**Proof.** We may assume $A = C^i a R$ for some $a \in GL_r(F)$ from Lemma 2.1. Let $X$ be an M–P inverse of $A$. We have $X \in M_{n,m}(F, r, R, C)$ from Lemma 2.2 and then $X = R^t b C$ for some $b \in GL_r(F)$ from Lemma 2.1. Note that

$$C^i a R = A = AXA = C^i a R R^t b C C^r a R;$$

we have $a = a R R^t b C C^r a$ from Lemma 2.1, and thus $a^{-1} = R R^t b C C^r$, which shows that both $R R^r$ and $C C^r$ are nonsingular. Then

$$X = R^t b C = R^t (R R^r)^{-1} a^{-1} (C C^r)^{-1} C$$

$$= R^t (C C^r a R R^t)^{-1} C = R^t (C A R^t)^{-1} C. \quad \Box$$

In the following, we will denote by $A^+$ the unique M–P inverse of $A$ when $A$ is M–P invertible. We denote by $L(A)^\perp$ the dual space of $L(A)$; i.e.,

$$L(A)^\perp = \{ x \in F^{(0)} \mid Ax^r = 0 \}. $$
**Lemma 2.3.** Let $A \in M_{m,n}(F,r,C,R)$. Then

1. $\text{rank}(AA^\tau) = \text{rank}(RR^\tau)$,
2. $\text{rank}(A^\tau A) = \text{rank}(CC^\tau)$,
3. $\text{dim}(L(A) \cap L(A)^\perp) + \text{rank}(RR^\tau) = r$,
4. $\text{dim}(L(A^\tau) \cap L(A^\perp)) + \text{rank}(CC^\tau) = r$.

**Proof.** We may assume $A = C^\tau aR$ for some $a \in GL_r(F)$ from Lemma 2.1.

1. Let $Q$ be defined by (6), then

$$AA^\tau = (C^\tau aR)(C^\tau aR)^\tau = C^\tau aRR^\tau a^\tau C$$

$$= Q \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} aRR^\tau a^\tau (I_r & 0)Q^\tau = Q \begin{pmatrix} aRR^\tau a^\tau & 0 \\ 0 & 0 \end{pmatrix}Q^\tau;$$

hence $\text{rank}(AA^\tau) = \text{rank}(Q^{-1}AA^\tau(Q^\tau)^{-1}) = \text{rank}(aRR^\tau a^\tau) = \text{rank}(RR^\tau)$.

2. Let $B = A^\tau$; then $B \in M_{n,m}(F,r,R,C)$. We have $\text{rank}(A^\tau A) = \text{rank}(BB^\tau) = \text{rank}(CC^\tau)$ from item 1.

3. We have

$$L(A) \cap L(A)^\perp = \{x \in L(A) = R | Rx^\tau = 0\}$$

$$= \{x = br | b \in F^{(r)}, RR^\tau b^x = 0\},$$

so

$$\text{dim}(L(A) \cap L(A)^\perp) = \text{dim}(\{x = br | b \in F^{(r)}, RR^\tau b^x = 0\})$$

$$= \text{dim}(\{b | b \in F^{(r)}, RR^\tau b^x = 0\})$$

$$= r - \text{rank}(RR^\tau).$$

4. Let $B = A^\tau$; then $B \in M_{n,m}(F,r,R,C)$. We have $\text{dim}(L(A^\tau) \cap L(A^\perp)) = \text{dim}(L(B) \cap L(B)^\perp) = r - \text{rank}(CC^\tau)$ from item 3. 

**Theorem 2.2 (Criteria).** Let $A \in M_{m,n}(F,r,C,R)$. Then the following conditions are equivalent:

1. The matrix $A$ is M–P invertible,
2. $\text{rank}(CC^\tau) = \text{rank}(RR^\tau) = r$,
3. $\text{rank}(A^\tau A) = \text{rank}(AA^\tau) = r$,
4. $L(A) \cap L(A)^\perp = (0)$ and $L(A^\tau) \cap L(A^\perp) = (0)$.

**Proof.** We may assume $A = C^\tau aR$ for some $a \in GL_r(F)$ from Lemma 2.1. From Theorem 2.1 we see item 1 implies item 2. If item 2 is true, we have $CAR^\tau = C(C^\tau aR)R^\tau = (CC^\tau)a(RR^\tau) \in GL_r(F)$. Take $X = R^\tau(CAR^\tau)^{-1}C$. It is easy to see $X$ is an M–P inverse of $A$ by checking the four conditions (1)–(4).
for \( A \) and \( X \); hence item 1 is true. Both the equivalence of items 2 and 3 and the equivalence of items 2 and 4 are easy consequences of Lemma 2.3.

**Corollary 2.1.**

1. If \( A \in M_{m,n}(F) \) and \( AA^t \) is nonsingular, then \( A \) is \( M-P \) invertible, and \( A^+ = A^t( AA^t)^{-1} \).
2. Assume both \( CC^t \) and \( RR^t \) to be nonsingular. Then for any \( A = C^t a R^t \), \( a \in GL_n(F) \), we have \( A^+ = R^+ a^{-1} (C^+)^t \).

**Proof.**

1. Take \( r = m, R = A, C = I_n, a = I_n \); we have \( A = C^t a R^t \), and then \( A \in M_{m,n}(F, r, C, R) \) from Lemma 2.1. Note that both \( CC^t = I_r \) and \( RR^t \) are nonsingular, so \( A \) is \( M-P \) invertible from Theorem 2.2. Moreover, \( A^+ = R^t (CAR^t)^{-1} C = A^t (AA^t)^{-1} \) from Theorem 2.1.

2. We see \( A \) is \( M-P \) invertible from Theorem 2.2. We have \( A^+ = R^t (CAR^t)^{-1} C \) and \( R^+ = R^t (RR^t)^{-1} \) and \( C^+ = C^t (CC^t)^{-1} \) from Theorem 2.1 and item 1, respectively. Note that the matrix \( CC^t \) is symmetric, we deduce that \( (CC^t)^{-1} \) is symmetric, and \( (C^+)^t = (C^t (CC^t)^{-1})^t = (CC^t)^{-1} C \). Then

\[
A^+ = R^t (CAR^t)^{-1} C = R^t [CC^t a R R^t ]^{-1} C = R^t (RR^t)^{-1} a^{-1} (CC^t)^{-1} C = R^+ a^{-1} (C^+)^t.
\]

We use the same letter \( A \) to denote the linear map \( x^t \mapsto Ax^t \) from \( F_{q^n}^{(m)_r} = \{ x^t | x \in F_{q^n}^{(m)} \} \) to \( F_{q^n}^{(m)_r} \), \( Im(A) \) to denote the image space of \( A \) and the symbol \( Ker(A) \) is used to denote the kernel space of \( A \), and for any subspace \( U \) of \( F^{(m)_r} \), the symbol \( U^\perp \) is used to denote the dual space of \( U \) in \( F^{(m)_r} \); i.e.,

\[
U^\perp = \{ x^t | x \in F^{(m)}, xu = 0 \ \forall u \in U \}.
\]

**Proposition 3.** Let \( A \in M_{m,n}(F_q) \). Then \( A \) is \( M-P \) invertible if and only if both \( F_{q^n}^{(m)_r} = Im(A) \oplus Im(A)^\perp \) and \( F_{q^n}^{(m)_r} = Ker(A) \oplus Ker(A)^\perp \) hold.

**Proof.** Note that \( L(A^t) = Im(A)^t \) and \( L(A) = Ker(A)^t \), we have \( L(A^t)^\perp = (Im(A)^t)^\perp = (Im(A))^{\perp t} \), and \( L(A) = (Ker(A)^\perp)^t = (Ker(A)^t)^\perp \). Then

\[
L(A^t) \cap L(A)^\perp = (0) \leftrightarrow Im(A)^t \cap [Im(A)]^t = (0) \\
\leftrightarrow Im(A) \cap Im(A)^\perp = (0) \\
\leftrightarrow F_{q^n}^{(m)_r} = Im(A) \oplus Im(A)^\perp, \text{ and}
\]

\[
L(A) \cap L(A)^\perp = (0) \leftrightarrow [Ker(A)^\perp]^t \cap Ker(A)^t = (0) \\
\leftrightarrow Ker(A)^\perp \cap Ker(A) = (0) \\
\leftrightarrow F_{q^n}^{(m)_r} = Ker(A) \oplus Ker(A);
\]

hence we get the desired result from Theorem 2.2.
In the following, we denote by \( F^{(n)}(r, \ast) \) the set of all possible \( r \)-dimensional subspaces \( R \) with \( RR^t \) being nonsingular in \( F^{(n)} \). For a finite set \( S \) we denote by \( |S| \) the cardinal number of \( S \).

**Theorem 2.3** (Partition). The set of all \( M-P \) invertible \( m \times n \) matrices of rank \( r \) over \( F \), denoted by \( M_{m,n}(F; r; \ast) \), is the following disjoint union:

\[
M_{m,n}(F; r; \ast) = \bigcup_{(C, R) \in F^{(m)}(r; \ast) \times F^{(n)}(r; \ast)} \{C^t aR | a \in GL_r(F)\}.
\]

Therefore

\[
|M_{m,n}(F_q; r; \ast)| = |GL_r(F_q)| \times |F_q^{(m)}(r; \ast)| \times |F_q^{(n)}(r; \ast)|.
\]

**Proof.** It is a consequence of Lemma 2.1 and Theorem 2.2. ■

### 3. Construction and Enumeration of M–P Invertible Matrices over Finite Fields with Odd Characteristic

In this section we let \( F_q \) be a finite field with odd characteristic. The problem of constructing and enumerating the \( m \times n \) \( M-P \) invertible matrices of rank \( r \) is reduced to that of constructing and enumerating the elements in \( GL_r(F_q) \), the elements in \( F_q^{(m)}(r; \ast) \), and the elements in \( F_q^{(n)}(r; \ast) \) by Theorem 2.3. It is known [4] how to construct matrices in \( GL_r(F_q) \) and it is also known [4] that \( |GL_r(F_q)| = \prod 0 \leq i < r(q^r - q^i) \), so we need consider only the problem of constructing and enumerating the elements in \( F_q^{(m)}(r; \ast) \) for any given \( n \). Our discussion will be based on geometry of the orthogonal groups. From Theorem 1.25 of [4] the following lemma follows immediately.

**Lemma 3.1.** Let \( F_q \) be of odd characteristic and let \( I^{(n)} \) be the \( n \times n \) identity matrix over \( F_q \). Then there exists an \( n \times n \) nonsingular matrix \( K \) over \( F_q \) such that \( KI^{(n)}K^t = S_{2v + \delta, \Delta} \), where

\[
S_{2v + \delta, \Delta} = \begin{pmatrix}
0 & I^{(v)}
\hline
I^{(v)} & 0
\end{pmatrix}, \quad n = 2v + \delta,
\]

and

\[
(\delta, \Delta) = \begin{cases}
(1, 1) & \text{if } n \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4},
(1, z) & \text{otherwise},
\end{cases}
\]

(10)
if $n$ is odd;

$$\delta = \begin{cases} 
(0,0) & \text{if $n \equiv 0 \pmod{4}$ or $q \equiv 1 \pmod{4}$,} \\
(2, (1 \ 0 \ -z)) & \text{otherwise,}
\end{cases}$$

(11)

if $n$ is even; and $z$ is an nonsquare element in $F_q$.

We also need the following lemma from [4].

**Lemma 3.2** [4]. *Keep the notation of Lemma 3.1. Let $R$ be an $r$-dimensional vector subspace of $F_q^{(2^v + \delta)}$. Then $RS_{2^v + \delta, \Delta} R^\tau$ is cogredient to one and only one of the following four normal forms:

$$M(r, 2s + \gamma, s, \Gamma) = \begin{pmatrix} 
0 & I(s) \\
I(s) & 0 \\
\Gamma & 0^{(r-2s-\gamma)}
\end{pmatrix},$$

(12)

where $0^{(r-2s-\gamma)}$ is a zero matrix of order $r - 2s - \gamma$ and

$$\gamma, \Gamma = \begin{cases} 
(0,0) & \text{or} \\
(1,1) & \text{or} \\
(1, z) & \text{or} \\
(2, (1 \ 0 \ -z));
\end{cases}$$

i.e., there exists a matrix representation $T$ ($T = bR$ for some $b \in GL_r(F_q)$) of the subspace $R$ such that

$$TS_{2^v + \delta, \Delta} T^\tau = M(r, 2s + \gamma, s, \Gamma).$$

(13)

$R$ is called a subspace of type $M(r, 2s + \gamma, s, \Gamma)$ with respect to the orthogonal group $O_{2^v + \delta, \Delta}(F_q, S_{2^v + \delta, \Delta})$ in $F_q^{(2^v + \delta)}$ if $RS_{2^v + \delta, \Delta} R^\tau$ is cogredient to $M(r, 2s + \gamma, s, \Gamma)$; and it is called an non-isotropic subspace if $r = 2s + \gamma$. It is clear that $R$ is nonisotropic if and only if $RS_{2^v + \delta, \Delta} R^\tau$ is nonsingular.

**Lemma 3.3.** *Keep the notation of Lemma 3.1. Let $R$ be an $r$-dimensional vector subspace of $F_q^{(2^v + \delta)}$, and let $R_1 = RK^{-1}$, where $K$ is the matrix mentioned in Lemma 3.1. Then the subspace $R$ belongs to $F_q^{(2^v + \delta)}(r, \ast)$ if and only if the subspace $R_1$ is nonisotropic with respect to the orthogonal group $O_{2^v + \delta, \Delta}(F_q)$ in $F_q^{(2^v + \delta)}$.***
Proof. Note that \( RR' = RK^{-1}S_q(K')^{-1}R' = R_1S_{2v+\delta,\Delta}R_1 \), we get the desired result. 

Construction of \( F_q^{(n)}(r;*) \). Keep the notation of Lemma 3.1. The problem of constructing the elements in \( F_q^{(n)}(r;*) \) is reduced to that of constructing the nonisotropic vector subspaces with respect to the orthogonal group \( O_{2v+\delta,\Delta}(F_q) \) in \( F_q^{(2v+\delta)} \) by Lemma 3.3, and it is reduced further to that of constructing the subspaces of each type \((r,2s + \gamma,s,\Gamma)\) with \( r = 2s + \gamma \), with respect to the orthogonal group \( O_{2v+\delta,\Delta}(F_q) \) in \( F_q^{(2v+\delta)} \) by Lemma 3.2 or, equivalently, to that of constructing the matrices \( T \) satisfying (13) for each type \((r,2s + \gamma,s,\Gamma)\) with \( r = 2s + \gamma \). A method for constructing these matrices is given in Section 6.2 [4]; see [4. pp. 266–280]. We also have

**Theorem 3.1 (Enumeration of \( F_q^{(n)}(r;*) \)).** Keep the notation of Lemma 3.1. The total number of the elements in \( F_q^{(n)}(r;*) \) is:

\[
|F_q^{(n)}(r;*)| = \begin{cases} 
\sum_{2t = 2s + \gamma,\gamma = 0,2} N(2t,2s + \gamma,s,\Gamma;2v + \delta,\Delta) & \text{if } r = 2t, \\
\sum_{x = 1,t} N(2t + 1,2t + 1,t,(x);2v + \delta,\Delta) & \text{if } r = 2t + 1,
\end{cases}
\]

where the formula for \( N(r,2s + \gamma,s,\Gamma;2v + \delta,\Delta) \), which is the total number of the vector subspaces of type \((r,2s + \gamma,s,\Gamma)\) with respect to \( O_{2v+\delta,\Delta}(F_q) \) in \( F_q^{(2v+\delta)} \) can be found in [4] (see also [5] or [6]).

Proof. It is a consequence of Lemma 3.3 and 3.2. 

4. CONSTRUCTION AND ENUMERATION OF M–P INVERTIBLE MATRICES OVER \( F_q \) WITH CHARACTERISTIC 2

In this section we let \( F_q \) be a finite field of characteristic 2. Similar to the case of odd characteristic, in order to construct and enumerate the \( m \times n \) M–P invertible matrices of rank \( r \), we need consider only the problem of constructing and enumerating the elements in \( F_q^{(n)}(r;*) \) for any given \( n \). Our discussion on the latter will be based on geometry of the pseudo-symplectic groups [4], and almost all concepts in discussion are quoted from [4]. We need the following lemmas which are shown in section 4 of [4].

**Lemma 4.1** [4]. Let \( F_q \) be of characteristic 2 and \( I^{(n)} \) be the \( n \times n \) identity matrix over \( F_q \). Then there exists an \( n \times n \) nonsingular matrix \( K \) such that
$K \ell^{(n)} K^r = S_{\delta}$, where

$$S_{\delta} = \begin{pmatrix} 0 & I^{(n)} \\ I^{(n)} & 0 \\ \Delta \end{pmatrix}, \quad n = 2v + \delta,$$

(14)

and

$$(\delta, \Delta) = \begin{cases} (1, (1)) & \text{if } n \text{ is odd}, \\ (2, (0, 1 \ 1)) & \text{if } n \text{ is even}. \end{cases} \quad \square$$

**Lemma 4.2.** [4]. *Keep the notation of Lemma 4.1. Let $R$ be an $r$-dimensional subspace of $F_q^{(n)}$. Then $R S_{\delta} R^r$ is cogredient to one and only one of the following three normal forms:

$$M(r, 2s + \tau, s) = \begin{pmatrix} 0 & I_r \\ I_r & 0 \\ \Gamma \\ 0^{(r-2s-\tau)} \end{pmatrix},$$

where

$$(\tau, \Gamma) = \begin{cases} (0, \emptyset), & \text{or} \\ (1, (1)), & \text{or} \\ (2, (0, 1 \ 1)), \end{cases}$$

i.e., there exists a matrix representation $T$ ($T = b R$ for some $b \in GL_r(F_q)$) of the subspace $R$ such that

$$T S_{\delta} T^r = M(r, 2s + \tau, s). \quad \square$$

$R$ is called a subspace of type $(r, 2s + \tau, s, \varepsilon)$, where $\varepsilon = 0$ or $1$, with respect to the pseudo-simplectic group $Ps_{2v + \delta}(F_q, S_{\delta})$ in $F_q^{(2v + \delta)}$ if $R S_{\delta} R^r$ is cogredient to $M(r, 2s + \tau, s)$ and

$$e_{2s+1} \notin R \text{ when } \varepsilon = 0; \quad e_{2s+1} \in R \text{ when } \varepsilon = 1,$$

(16)

where $e_{2v+1} = (0, 0, \cdots, 0, 1)$ and it is called a nonisotropic subspace if $r = 2s + \tau$. It is clear that $R$ is nonisotropic if and only if $R S_{2v + \delta, \Delta} R^r$ is nonsingular.
LEMMA 4.3. Keep the notation of Lemma 4.1. Let $R$ be an $r$-dimensional vector subspace of $F_q^{(2v+\delta)}$, and let $R_1 = RK^{-1}$, where $K$ is the matrix mentioned in Lemma 4.1. Then the subspace $R$ belongs to $F_q^{(2v+\delta)}(r;*)$ if and only if the subspace $R_1$ is nonisotropic with respect to the pseudo-symplectic group $P_{S_{2v+\delta}(F_q, S_\delta)}$ in $F_q^{(2v+\delta)}$.

Proof. Note that $RR^t = RK^{-1}S_\delta(K^t)^{-1}R = R_1S_\delta R_1^t$, we get the desired result. ■

Construction of $F_q^{(n)}(r;*)$. Keep the notation of Lemma 4.1. The problem of constructing the elements in $F_q^{(n)}(r;*)$ is reduced to that of constructing the nonisotropic subspaces with respect to $P_{S_{2v+\delta}(F_q, S_\delta)}$ in $F_q^{(2v+\delta)}$ by Lemma 4.3, and it is reduced further to that of constructing the vector subspaces of each type $(r, 2s + \tau, s, \varepsilon)$ with $r = 2s + \tau$, with respect to $P_{S_{2v+\delta}(F_q, S_\delta)}$ in $F_q^{(2v+\delta)}$ by Lemma 4.2 or, equivalently, to that of constructing the matrices satisfying both (15) and (16) for each type $(r, 2s + \tau, s, \varepsilon)$ with $r = 2s + \tau$. A method of constructing these matrices is given in an argument, which is given in Theorem 4.14 of [4] and is made for getting a formula for $N(r, 2s + \tau, s, \varepsilon; 2v + \delta)$ the number of vector subspaces of type $(r, 2s + \tau, s, \varepsilon)$ with respect to $P_{S_{2v+\delta}(F_q, S_\delta)}$ in $F_q^{(2v+\delta)}$. By Lemma 4.2 and 4.3 we have

**Theorem 4.1 (Enumeration of $F_q^{(n)}(r;*)$).** Keep the notation of Lemma 4.1. The total number of the elements in $F_q^{(n)}(r;*)$ is:

$$|F_q^{(n)}(r;*)| = \begin{cases} 
\sum_{\varepsilon=0,1} N(2t + 1, 2t + 1, t, \varepsilon; 2v + \delta), & \text{if } r = 2t + 1, \\
\sum_{\varepsilon=0,1} \sum_{2t=2s+\tau, t=0,2} N(2t, 2s + \tau, s, \varepsilon; 2v + \delta), & \text{if } r = 2t,
\end{cases}$$

where the formula for $N(2t, 2s + \tau, s, \varepsilon; 2v + \delta)$ can be found in [4]; see also [7].

ACKNOWLEDGMENTS

This work is supported by the 973 Science Foundation (No. G1999035804) and by the Chinese Natural Science Foundation (No. 69773015). The coauthors are grateful to the anonymous referees, whose comments and suggestions helped to considerably improve the presentation.

REFERENCES


