Wan Zhexian

Geometry of Classical Groups over Finite Fields

Second Edition

(有限域上典型群的几何学（第二版))

Science Press
Beijing/New York

(O-1647.1101)　Responsible Editor: Lu Hong (吕虹)

ISBN 7-03-010595-8

9 787030 105950 >

Wan Zhexian

Geometry of Classical Groups over Finite Fields

Second Edition

(有限域上典型群的几何学(第二版))

SCIENCE PRESS
Beijing/New York

Responsible Editor: Lü Hong

Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, China

Printed in Beijing

ISBN 7 - 03 - 010595 - 8

Preface to the Second Edition

As applications of the Anzahl theorems in the geometry of classical groups over finite fields some critical problems of finite vector spaces, Moor-Penrose generalized inverses of matrices over a finite field, and the representation of a form (bilinear, alternate, hermitian, or quadratic, etc.) by another form of the same kind over a finite field are added in this edition.

Wan Zhexian

Beijing, 2002

Preface

This monograph is a comprehensive survey of the results obtained on the geometry of classical groups over finite fields mainly in the 1960s and early 1990s.

For the convenience of the readers I start with the affine geometry and projective geometry over finite fields in Chapters 1 and 2, respectively. Among other things, the affine classification of quadrics is included in Chapter 1, and conics and ovals are studied in detail in Chapter 2. From Chapter 3 and onwards the geometries of symplectic, pseudo-symplectic, unitary, and orthogonal groups are studied in succession. The book ends with two appendices, on the axiomatic projective geometry, and on polar spaces and finite generalized quadrangles, respectively.

Now I shall say a few words about the problems we are going to study in Chapters 3–7, and in addition give some historical remarks.

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime, $\mathbb{F}_q^{(n)}$ be the n-dimensional row vector space over $\mathbb{F}_q$, and $GL_n(\mathbb{F}_q)$ be the general linear group of degree n over $\mathbb{F}_q$. It is well-known that $GL_n(\mathbb{F}_q)$ has an action on $\mathbb{F}_q^{(n)}$ and an induced action on the subspaces of $\mathbb{F}_q^{(n)}$, which are thus subdivided into orbits under the action of $GL_n(\mathbb{F}_q)$. It is natural to ask:

(i) How should the orbits be described?

(ii) How many orbits are there?

(iii) What are the lengths of the orbits?

(iv) What is the number of subspaces in any orbit contained in a given subspace?

The answers to these questions are classical and well-known for $GL_n(\mathbb{F}_q)$, but a natural question arises: If $GL_n(\mathbb{F}_q)$ is replaced by any one of the other classical groups: the symplectic group $Sp_{2\nu}(\mathbb{F}_q)$ (where $n = 2\nu$), the pseudo-symplectic group $Ps_{2\nu+\delta}(\mathbb{F}_q)$ (where q is even, $n = 2\nu + \delta$, and $\delta = 1$ or 2), the unitary group $U_n(\mathbb{F}_q)$ (where q is a square), and the orthogonal group $O_{2\nu+\delta}(\mathbb{F}_q)$ (where $n = 2\nu + \delta$ and $\delta = 0, 1,$ or 2), then what will the answers of the four problems mentioned above be? This is what we shall analyse in Chapters 3–7.

In 1937 E. Witt studied problem (i) for the orthogonal group $O_n(F, S)$ defined by an $n \times n$ nonsingular symmetric matrix S over any field F of characterstic $\neq 2$. His famous theorem asserts that two subspaces P_1 and P_2 of $F^{(n)}$ belong to the same orbit under the action of $O_n(F, S)$ if and only if they have the same dimension and $P_1 S\, {}^tP_1$ and $P_2 S\, {}^tP_2$ are cogredient, where P_1 and P_2 also denote matrix representations of the subspaces P_1 and P_2, respectively. Later C. Arf, J. Dieudonné, L. K. Hua, et al. extended Witt's theorem to other classical groups.

In 1958 B. Segre studied problem (iii) for orthogonal groups over any finite field $\mathbb{F}_q$ but he restricted himself to consider only totally isotropic and totally singular subspaces where q is odd and even, respectively. He used the geometrical method and geometrical language. In his address at the International Congress of Mathematicians, Edinburgh, 1958, he announced his formula for the number of subspaces of a given dimension lying on a non-degenerate quadratic in the projective space over any finite field without any restriction on its characteristic.

In the mid-1960s problem (iii) was attacked by three of my students at that time, Z. Dai, X. Feng, and B. Yang, and myself. We obtained the closed formulas for the lengths of all the orbits of subspaces under the action of the symplectic, unitary, and orthogonal groups over finite fields. Our method is algebraic. Closed formulas for problem (iv), i.e., for the number of subspaces in any orbit contained in a given subspace were also obtained by myself in 1966.

In the early 1990s I studied problems (i) and (ii). Conditions satisfied by the numerical invariants characterizing the orbits of subspaces under the symplectic, unitary, and orthogonal groups over finite fields were obtained and then the number of orbits was computed. Problems (i) – (iii) for the pseudo-symplectic groups over finite fields of characteristic 2 were studied together with Y. Liu. Moreover, I also studied problem (iv) for the pseudo-symplectic group and problems (i) – (iv) for the singular symplectic, pseudo-symplectic, unitary, and orthogonal groups.

My interest in the geometry of classical groups over finite fields was arisen by block designs in the mid-1960s and by authentication codes in the early 1990s. By using it, many interesting block designs and authentication codes can be constructed. However, due to the limitation of the thickness of the book only some simple authentication codes constructed from the geometry of classical groups over finite fields are included in this monograph as examples. Using the geometry of classical groups over finite fields one can also construct projective codes with a few distinct weights and study the weight hierarchies of them; they are, however, not included in this monograph.

A large portion of the book is adopted from the lecture notes of a course entitled "Finite Geometry" which I gave at the Department of Information Theory, Lund University. I would like to express my sincere gratitude to Professor Rolf Johannesson who invited me to visit Lund and to give the course and encouraged me to write the present book. My visit in Lund is most fruitful and many of the results on the geometry of classical groups over finite fields that I obtained in Lund are compiled in the present book. The author is also deeply indebted to Mrs. Lena Månsson for her beautiful typesetting, careful and hard work, and most of all her patience and cooperation.

Lund, 1993 Wan Zhexian (Zhe-Xian Wan)

Contents

Chapter 1
Affine Geometry over Finite Fields

1.1 Vector Spaces and Matrices over Finite Fields

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime, and n a positive integer. We use

$$\mathbb{F}_q^{(n)} = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{F}_q,\ i = 1, 2, \ldots, n\}$$

to denote the n-dimensional *row vector space* over $\mathbb{F}_q$ formed by the set of all n-tuples (or n-dimensional row vectors)

$$(x_1, x_2, \ldots, x_n), \quad x_i \in \mathbb{F}_q,\ i = 1, 2, \ldots, n,$$

over $\mathbb{F}_q$ with addition and scalar multiplication defined by

$$\begin{aligned}(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &= (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n), \\ x(x_1, x_2, \ldots, x_n) &= (xx_1, xx_2, \ldots, xx_n),\end{aligned}$$

where $x, x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in \mathbb{F}_q$. Let

$$e_1 = (1, 0, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0), \ldots,\ e_n = (0, 0, \ldots, 0, 1),$$

then $e_1, e_2, \ldots, e_n$ form a *basis* of $\mathbb{F}_q^{(n)}$, i.e., any vector $(x_1, x_2, \ldots, x_n)$ of $\mathbb{F}_q^{(n)}$ can be written as a linear combination of $e_1, e_2, \ldots, e_n$ with coefficients in $\mathbb{F}_q$:

$$(x_1, x_2, \ldots, x_n) = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n,$$

and the expression is unique. Of course, any n linearly independent vectors in $\mathbb{F}_q^{(n)}$ form a basis of $\mathbb{F}_q^{(n)}$. Clearly, $\mathbb{F}_q^{(n)}$ has altogether q^n vectors.

Now let P be an m-dimensional vector subspace of $\mathbb{F}_q^{(n)}$, then we write $\dim P = m$. Let $v_1, v_2, \ldots, v_m$ be a basis of P. We notice that $v_1, v_2, \ldots, v_m$ are vectors in $\mathbb{F}_q^{(n)}$. We usually use the $m \times n$ matrix

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

to represent the vector subspace P, write

$$P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix},$$

i.e., we use the same letter P to denote a matrix which represents the vector subspace P, and call the matrix P a *matrix representation* of the vector subspace P. It should be noted that a matrix representing an m-dimensional vector subspace is an $m \times n$ matrix of rank m. Of course, two $m \times n$ matrices P and Q both of rank m represent the same m-dimensional vector subspace, if and only if there is an $m \times m$ nonsingular matrix A such that

$$P = AQ.$$

Obviously, any m-dimensional vector subspace contains exactly q^m vectors.

Let P_1 and P_2 be two vector subspaces of $\mathbb{F}_q^{(n)}$. The set of vectors belonging to both P_1 and P_2 is a vector subspace of $\mathbb{F}_q^{(n)}$, called the *intersection* of P_1 and P_2 and denoted by $P_1 \cap P_2$. The set of vectors which can be written as sums of a vector of P_1 and a vector of P_2 is also a vector subspace of $\mathbb{F}_q^{(n)}$, called the *join* of P_1 and P_2 and denoted by $P_1 + P_2$. We have the *dimension formula*

$$\dim P_1 + \dim P_2 = \dim (P_1 \cap P_2) + \dim (P_1 + P_2).$$

The set of $n \times n$ nonsingular matrices over $\mathbb{F}_q$ forms a group under matrix multiplication, called the *general linear group* of degree n over $\mathbb{F}_q$ and denoted by $GL_n(\mathbb{F}_q)$. Elements of $GL_n(\mathbb{F}_q)$ can be regarded as linear transformations of $\mathbb{F}_q^{(n)}$. In fact, let $T \in GL_n(\mathbb{F}_q)$, then T carries (or transforms) the vector $(x_1, x_2, \ldots, x_n)$ of $\mathbb{F}_q^{(n)}$ into $(x_1, x_2, \ldots, x_n)T$. That is, we have a map

$$\begin{gathered}\mathbb{F}_q^{(n)} \times GL_n(\mathbb{F}_q) \to \mathbb{F}_q^{(n)} \\ ((x_1, x_2, \ldots, x_n), T) \mapsto (x_1, x_2, \ldots, x_n)T.\end{gathered}$$

We also say that there is an *action* of $GL_n(\mathbb{F}_q)$ on $\mathbb{F}_q^{(n)}$, or $GL_n(\mathbb{F}_q)$ *acts* on $\mathbb{F}_q^{(n)}$. This action induces an action of $GL_n(\mathbb{F}_q)$ on the set of $m \times n$ matrices over $\mathbb{F}_q$ and also on the set of m-dimensional vector subspaces of $\mathbb{F}_q^{(n)}$: if $T \in GL_n(\mathbb{F}_q)$ and P is an $m \times n$ matrix over $\mathbb{F}_q$ or an m-dimensional vector subspace of $\mathbb{F}_q^{(n)}$, then T carries P into PT.

Theorem 1.1. If $T \in GL_n(\mathbb{F}_q)$ and P is an $m \times n$ matrix of rank m over $\mathbb{F}_q$, then PT is also an $m \times n$ matrix of rank m. Furthermore, if P and Q are both $m \times n$ matrices of rank m over $\mathbb{F}_q$, then there is an element $T \in GL_n(\mathbb{F}_q)$ such that $P = QT$.

Proof. The first statement is clear from linear algebra. We prove the second statement only. Write

$$P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} \qquad \text{and} \qquad Q = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix},$$

where $v_1, v_2, \ldots, v_m$ are the m rows of P and $u_1, u_2, \ldots, u_m$ are the m rows of Q. Since P is of rank m, $v_1, v_2, \ldots, v_m$ are linearly independent. Thus there exist $n - m$ vectors $v_{m+1}, v_{m+2}, \ldots, v_n$ such that the n vectors $v_1, v_2, \ldots, v_m, v_{m+1}, v_{m+2}, \ldots, v_n$ are linearly independent. Then

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

is an $n \times n$ nonsingular matrix. Similarly, since Q is also of rank m, there exist $n - m$ vectors $u_{m+1}, u_{m+2}, \ldots, u_n$ such that

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

is also an $n \times n$ nonsingular matrix. Let

$$T = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}^{-1} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

then $T \in GL_n(\mathbb{F}_q)$ and $P = QT$. □

Corollary 1.2. The set of all non-zero vectors of $\mathbb{F}_q^{(n)}$ forms an *orbit*, i.e., a *transitive set*, under $GL_n(\mathbb{F}_q)$. The zero vector $(0, 0, \ldots, 0)$ is left fixed by every element of $GL_n(\mathbb{F}_q)$. □

Theorem 1.3. The set of all m-dimensional vector subspaces of $\mathbb{F}_q^{(n)}$ forms an orbit under $GL_n(\mathbb{F}_q)$.

Proof. Use matrix representations of vector subspaces of $\mathbb{F}_q^{(n)}$. □

Theorem 1.4. The number of orbits of subspaces of $\mathbb{F}_q^{(n)}$ is $n + 1$. □

Now let us prove some Anzahl theorems in $\mathbb{F}_q^{(n)}$.

Let $N(m, n)$ be the number of m-dimensional vector subspaces in $\mathbb{F}_q^{(n)}$. Our goal is to compute $N(m, n)$. Let $n(m, n)$ be the number of $m \times n$ matrices of rank m over $\mathbb{F}_q$. We know that two $m \times n$ matrices P and Q both of rank m represent the same m-dimensional subspace if and only if there is an $m \times m$ nonsingular matrix A such that $P = AQ$, thus

$$n(m, n) = \mid GL_m(\mathbb{F}_q) \mid N(m, n),$$

where $\mid GL_m(\mathbb{F}_q) \mid$ is the order of $GL_m(\mathbb{F}_q)$. Clearly

$$\mid GL_m(\mathbb{F}_q) \mid = n(m, m).$$

Thus to compute $N(m, n)$ it is sufficient to compute $n(m, n)$.

Lemma 1.5. Let $m \leq n$. Then the number of $m \times n$ matrices of rank m over $\mathbb{F}_q$ is

$$n(m, n) = q^{m(m-1)/2} \prod_{i=n-m+1}^{n} (q^i - 1).$$

Proof. Let P be an $m \times n$ matrix of rank m. Write

$$P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix},$$

where $v_1, v_2, \ldots, v_m$ are the m rows of P. If we want to enumerate how many possible P's there are, it is sufficient to enumerate how many possible v_1's there are, and once a v_1 is chosen to enumerate how many possible v_2's there are, etc. Now, v_1 can be any non-zero vector of $\mathbb{F}_q^{(n)}$, thus there are $q^n - 1$ possible choices for v_1. Once v_1 is chosen, v_2 can be any vector of $\mathbb{F}_q^{(n)}$ which is linearly independent with v_1, thus there are $q^n - q$ possible choices of v_2. After v_1 and v_2 are chosen, v_3 can be any vector of $\mathbb{F}_q^{(n)}$ which is linearly independent with v_1 and v_2; since v_1 and v_2 are linearly independent, there are $q^n - q^2$ possible choices of v_3. Proceeding in this way, finally after $v_1, v_2, \ldots, v_{m-1}$ are chosen, v_m can be any vector of $\mathbb{F}_q^{(n)}$ which is linearly independent with $v_1, v_2, \ldots, v_{m-1}$; but since $v_1, v_2, \ldots, v_{m-1}$ are linearly independent, there are $q^n - q^{m-1}$ possible choices of v_m. Therefore

$$\begin{aligned} n(m,n) &= (q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{m-1}) \\ &= q^{m(m-1)/2} \prod_{i=n-m+1}^{n} (q^i - 1). \end{aligned}$$

□

From Lemma 1.5 follows immediately

Theorem 1.6.

$$\mid GL_n(\mathbb{F}_q) \mid = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1).$$

Proof. In fact,

$$\mid GL_n(\mathbb{F}_q) \mid = n(n,n).$$

□