

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

(O-1647.0102)

Responsible Editor: Lu Hong (吕虹)

ISBN 7-03-010595-8



9 787030 105950 >

ISBN 7-03-010595-8

定价: 76.00 元



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))



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

Responsible Editor : Lü Hong

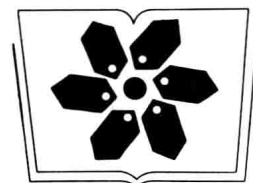
Copyright © 2002 by Science Press
Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, China

Printed in Beijing

Second Printed in 2006

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the copyright owner.

ISBN 7-03-010595-8



中国科学院科学出版基金资助出版

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, Moore-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 characteristic $\neq 2$. 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 $P_1 S^t P_1$ and $P_2 S^t P_2$ 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

Preface to the Second Edition	i
Preface	iii
Chapter 1 Affine Geometry over Finite Fields	1
1.1 Vector Spaces and Matrices over Finite Fields	1
1.2 Affine Spaces and Affine Groups over Finite Fields	8
1.3 Quadrics in $AG(n, \mathbb{F}_q)$ for q Odd	21
1.4 Quadrics in $AG(n, \mathbb{F}_q)$ for q Even	41
1.5 Comments	57
1.6 Exercises	58
Chapter 2 Projective Geometry over Finite Fields	61
2.1 Projective Spaces and Projective Groups over Finite Fields	61
2.2 Quadrics in $PG(n, \mathbb{F}_q)$	78
2.3 Conics in $PG(2, \mathbb{F}_q)$	84
2.4 Ovals in $PG(2, \mathbb{F}_q)$	92
2.5 Comments	103
2.6 Exercises	104
Chapter 3 Geometry of Symplectic Groups over Finite Fields	107
3.1 Symplectic Groups and Symplectic Spaces over Finite Fields	107

3.2 Anzahl Theorems in Symplectic Geometry over Finite Fields 119

3.3 Singular Symplectic Geometry over Finite Fields 127

3.4 Symplectic Polarities and Polar Spaces Arising from Them 140

3.5 Comments 151

3.6 Exercises 152

Chapter 4 Geometry of Pseudo-symplectic Groups over Finite Fields of Characteristic 2 154

4.1 Pseudo-symplectic Groups over Finite Fields of Characteristic 2 154

4.2 Pseudo-symplectic Geometry over Finite Fields of Characteristic 2 164

4.3 Singular Pseudo-symplectic Geometry over Finite Fields of Characteristic 2 190

4.4 Pseudo-symplectic Geometry over Finite Fields of Characteristic 2 Again 197

4.5 Pseudo-symplectic Polarities 213

4.6 Comments 218

4.7 Exercises 218

Chapter 5 Geometry of Unitary Groups over Finite Fields 220

5.1 Unitary Geometry over Finite Fields 220

5.2 Anzahl Theorems in Unitary Geometry over Finite Fields 231

5.3 Singular Unitary Geometry over Finite Fields 238

5.4 Unitary Polarities and Polar Spaces Arising from Them . . . 243

5.5 Hermitian varieties in $PG(n, \mathbb{F}_{q^2})$ and $AG(n, \mathbb{F}_{q^2})$ 246

5.6 Comments 248

5.7 Exercises 249

Chapter 6 Geometry of Orthogonal Groups over Finite Fields of Odd Characteristic 251

6.1	Orthogonal Geometry over Finite Fields of Odd Characteristic	251
6.2	Anzahl Theorems in Orthogonal Geometry over Finite Fields of Odd Characteristic	267
6.3	Singular Orthogonal Geometry over Finite Fields of Odd Characteristic	282
6.4	Orthogonal Polarities and Polar Spaces Arising from Them	290
6.5	Comments	292
6.6	Exercises	292
Chapter 7 Geometry of Orthogonal Groups over Finite Fields of Characteristic 2		294
7.1	Orthogonal Geometry over Finite Fields of Characteristic 2	294
7.2	Anzahl Theorems in Orthogonal Geometry over Finite Fields of Characteristic 2	316
7.3	Singular Orthogonal Geometry over Finite Fields of Characteristic 2	328
7.4	Polar Spaces Arising from Orthogonal Geometry over Finite Fields of Characteristic 2	344
7.5	Comments	345
7.6	Exercises	345
Appendix A Axiomatic Projective Geometry		347
A.1	Incidence Structures	347
A.2	Axioms of Projective Planes and the Principle of Duality	348
A.3	Finite Projective Planes	350
A.4	Collineations in Projective Planes	353
A.5	Desargues Planes	356
A.6	Projective Spaces	357
Appendix B Polar Spaces and Generalized Quadrangles		364
B.1	Polar Spaces	364
B.2	Generalized Quadrangles	366

Appendix C Critical Problems	380
C.1 A Critical Problem in Finite Vector Spaces	380
C.2 Critical Problems in Finite Unitary Spaces	385
C.3 A Critical Problem in Finite Symplectic Spaces	390
C.4 Comments	394
Appendix D Moor-Penrose Generalized Inverses of Matrices over Finite Fields	395
D.1 Definition and Properties	395
D.2 Construction of Enumeration of M-P Invertible Matrices . .	400
D.3 Generalization to Matrices over \mathbb{F}_{q^2}	403
D.4 Comments	406
Appendix E Representations of Forms by Forms in a Finite Field	407
E.1 Representations of Bilinear Forms	407
E.2 Representations of Alternate Forms	412
E.3 Representations of Hermitian Forms	416
E.4 Representations of Quadratic Forms (Odd Characteristic Case)	418
E.5 Representations of Quadratic Forms (Even Characteristic Case)	421
E.6 Representations of Symmetric Bilinear Forms over Finite Fields of Even Characteristic	427
E.7 Comments	430
E.8 Exercises	430
Bibliography	431
Notation	437
Index.....	442