数理解析研究所講究録
第 840 巻 1993 年 124-140

Survey on Geometry of Classical Groups over Finite Fields and Its Applications

Dedicated to Professor Hsiao-Fu Tuan on His Eightieth Birthday

Zhe-xian Wan

The Chinese Academy of Sciences

1. The Germ of Our Study

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power, $\mathbb{F}_q^{(n)}$ 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 $\mathbb{F}_q$. $GL_n(\mathbb{F}_q)$ acts on $\mathbb{F}_q^{(n)}$ in the following way:

$$\begin{array}{rcl} \mathbb{F}_q^{(n)} \times GL_n(\mathbb{F}_q) & \to & \mathbb{F}_q^{(n)}, \\ ((x_1, x_2, \cdots, x_n), T) & \mapsto & (x_1, x_2, \cdots, x_n)T. \end{array} \qquad (1)$$

Let P be an m-dimensional subspace of $\mathbb{F}_q^{(n)}$ and $v_1, v_2, \cdots, v_m$ be a basis of P, then

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} \qquad (2)$$

is an $m \times n$ matrix over $\mathbb{F}_q$ of rank m. We call the matrix (2) a *matrix representation* of the subspace P and use also the same letter P to denote the matrix (2) if no ambiguity arises. The action (1) of $GL_n(\mathbb{F}_q)$ on $\mathbb{F}_q^{(n)}$ induces an action on the set of subspaces of $\mathbb{F}_q^{(n)}$ such that $T \in GL_n(\mathbb{F}_q)$ carries the subspace P into PT. We may propose the following problems:

(i) What are the orbits of subspaces of $\mathbb{F}_q^{(n)}$ under the action of $GL_n(\mathbb{F}_q)$?

(ii) How many orbits are there ?

(iii) What are the lengths of the orbits ?

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

The answers to these four problems are well-known; they are:

i) Two subspaces belong to the same orbit if and only if their dimensions are equal.

ii) There are altogether $n+1$ orbits.

iii) Denote the length of the orbit of m-dimensional subspaces ($0 \leq m \leq n$) by $N(m,n)$, then

$$N(m,n) = \frac{\prod\limits_{i=n-m+1}^{n} (q^i - 1)}{\prod\limits_{i=1}^{m} (q^i - 1)}. \tag{3}$$

iv) The number of k-dimensional subspaces contained in a given m-dimensional subspace ($0 \leq k \leq m \leq n$) is $N(k,m)$.

2. The Problems We Are Interested in

It is natural to propose the following problem.

Use any one of the other classical groups, such as the symplectic group $Sp_n(\mathbb{F}_q)$ (where $n = 2\nu$), the unitary group $U_n(\mathbb{F}_q)$ (where q is a square), or the orthogonal group $O_n(\mathbb{F}_q)$ (where $n = 2\nu + \delta$ and $\delta = 0, 1,$ or 2) to replace $GL_n(\mathbb{F}_q)$, then study Problems (i)–(iv).

Now let us introduce the definition of the other classical groups.

Let $n = 2\nu$. It is well-known that the cogredience normal form of $2\nu \times 2\nu$ nonsingular alternate matrices is

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}. \tag{4}$$

Let

$$Sp_{2\nu}(\mathbb{F}_q) = \{T \in GL_{2\nu}(\mathbb{F}_q) | TK\,{}^tT = K\}. \tag{5}$$

Then $Sp_{2\nu}(\mathbb{F}_q)$ is a group with respect to the matrix multiplication, called the *symplectic group* of degree 2ν over $\mathbb{F}_q$.

Let $q = q_0^2$, where q_0 is a prime power. $\mathbb{F}_q$=$\mathbb{F}_{q_0^2}$ has an involutive automorphism

$$- : a \longrightarrow \bar{a}, \tag{6}$$

whose fixed field is $\mathbb{F}_{q_0}$. Let

$$U_n(\mathbb{F}_q) = \{T \in GL_n(\mathbb{F}_q) | T\,{}^t\bar{T} = I^{(n)}\}. \tag{7}$$

Then $U_n(\mathbb{F}_q)$ is a group with respect to the matrix multiplication, called the *unitary group* of degree n over $\mathbb{F}_q$.

Let q be a power of an odd prime and z be a non-square element of $\mathbb{F}_q$. The cogredience normal forms of $n \times n$ nonsingular symmetric matrices over $\mathbb{F}_q$ are

$$S_0 = \begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \tag{8}$$

$$S_{1,d} = \begin{pmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & d \end{pmatrix}, \tag{9}$$

where $d = 1$ or z, and

$$S_2 = \begin{pmatrix} 0 & I^{(\nu)} & & \\ I^{(\nu)} & 0 & & \\ & & 1 & \\ & & & -z \end{pmatrix}. \tag{10}$$

Corresponding to these four cases, n is equal to 2ν, $2\nu+1$, $2\nu+1$, and $2\nu+2$, respectively. We use $n = 2\nu+\delta$ and $S_{\delta,d}$ to cover these four cases, where $\delta = 0, 1$, or 2, $d = 1$ or z when $\delta = 1$, and d disappears when $\delta = 0$ or 2. Let

$$O_{2\nu+\delta,d}(\mathbb{F}_q) = \{T \in GL_{2\nu+\delta}(\mathbb{F}_q) | TS_{\delta,d}\,{}^tT = S_{\delta,d}\}. \tag{11}$$

Then $O_{2\nu+\delta,d}(\mathbb{F}_q)$ is a group with respect to the matrix multiplication, called the *orthogonal group* of degree $2\nu+\delta$ over $\mathbb{F}_q$. It is easy to prove that $O_{2\nu+1,1}(\mathbb{F}_q)$ and $O_{2\nu+1,z}(\mathbb{F}_q)$ are isomorphic. Thus it is enough to consider the three orthogonal groups $O_{2\nu}(\mathbb{F}_q)$, $O_{2\nu+1,1}(\mathbb{F}_q)$, and $O_{2\nu+2}(\mathbb{F}_q)$. We write $O_{2\nu+1}(\mathbb{F}_q)$ simply for $O_{2\nu+1,1}(\mathbb{F}_q)$.

When $\mathbb{F}_q$ is of characteristic 2, there are also three types of orthogonal groups $O_{2\nu+\delta}(\mathbb{F}_q)$, where $\delta = 0, 1$, or 2, but their definitions are omitted.

3. The History of the Problems

In 1937 E. Witt [1] studied problem (i) for the orthogonal group over any field F of characteristic $\neq 2$. Let S be an $n \times n$ nonsingular symmetric matrix over F. The *orthogonal group* of degree n over F relative to S, denoted by $O_n(F,S)$, is defined to be

$$O_n(F,S) = \{T \in GL_n(F) | TS{}^tT = S\} \tag{12}$$

The famous Witt's Theorem asserts that two subspaces P_1 and P_2 of $\mathbb{F}_q^{(n)}$ belong to the same orbit of $O_n(F,S)$ if and only if $\dim P_1 = \dim P_2$ and $P_1 S{}^tP_1$ and $P_2 S{}^tP_2$ are cogredient. Later Witt's theorem was generalized to other classical groups by C. Arf [2], J, Dieudonné [3, 4], L. K. Hua [5], and V. Pless [6]. It is worth to mention that Hua [5] gave also a simple matrix proof of the generalized Witt's theorem.

In 1948 B. Segre [7] studied problem (iii) for the orthogonal group over $\mathbb{F}_q$, but he restricted himself to consider only totally isotropic or totally singular subspaces corresponding to cases when q is odd or even, respectively. For simplicity we follow the notation of the previous paragraph, thus assume that $\mathbb{F}_q$ is characteristic $\neq 2$. A subspace P of $F^{(n)}$ is called *totally isotropic*, if $PS{}^tP = 0$. By Witt's theorem totally isotropic subspaces of the same dimension of $F^{(n)}$ form an orbit under $O_n(F,S)$. Segre determined the lengths of the orbits of totally isotropic subspaces of the same dimension of $\mathbb{F}_q^{(2\nu+\delta)}$ under $O_{2\nu+\delta}(\mathbb{F}_q)$. He used geometric language to state his results as follows. The number of m-dimensional flats lying on a nondegenerate quadric in an $(n-1)$-dimensional projective space over $\mathbb{F}_q$, $PG(n-1, \mathbb{F}_q)$, is equal to

$$\frac{\prod\limits_{i=\nu-m}^{\nu} (q^i - 1)(q^{i+\delta-1} - 1)}{\prod\limits_{i=1}^{m+1} (q^i - 1)}, \tag{13}$$

where $-1 \leq m \leq \nu - 1$, $\nu = \frac{n-1}{2}$ when n is odd, and $\nu = \frac{n}{2}$ or $\frac{n}{2} - 1$ when n is even and the quadric is of the hyperbolic type or the elliptic type, respectively. He used geometric method to deduce this formula which holds also for the case of characteristic 2.

In 1964 three students of mine at that time and myself [8–11] studied problem (iii) for the groups $Sp_{2\nu}(\mathbb{F}_q)$, $U_n(\mathbb{F}_q)$ (where q is a square), and $O_{2\nu+\delta}(\mathbb{F}_q)$ (where $\delta = 0, 1$, or 2). We determined not only the lengths of those orbits of totally isotropic or totally singular subspaces but also the lengths of all the orbits. Our methods is algebraic and our results were compiled in our monograph [12].

In 1965 V. Pless [13] computed the lengths of those orbits of totally isotropic subspaces of $\mathbb{F}_q^{(2\nu)}$ under the group $Sp_{2\nu}(\mathbb{F}_q)$ and the number of totally isotropic subspaces of the same dimension of $\mathbb{F}_q^{(2\nu+\delta)}$ (where $\delta = 1$ or 2) with respect to a $(2\nu + \delta) \times (2\nu + \delta)$ nonsingular non-alternate symmetric matrix over $\mathbb{F}_q$ when q is even.

In 1966 R. C. Bose and I. M. Chakravarti [14] determined the lengths of those orbits of totally isotropic subspaces of $\mathbb{F}_q^{(n)}$ under the group $U_n(\mathbb{F}_q)$ (where q is a squre of a prime power).

In 1966 the author studied problem (iv) for the group $Sp_{2\nu}(\mathbb{F}_q)$, $U_n(\mathbb{F}_q)$ (q is a square), and $O_{2\nu+\delta}(\mathbb{F}_q)$ (where $\delta = 0, 1$, or 2) and obtained closed formulas for the number of subspaces in an orbit under each of these group contained in a given subspace. These results were also compiled in [12].

4. Recent Results

In the early nineties I returned to the study of the geometry of classical groups over finite fields and obtained the following results.

1) Problems (i) and (ii) for the symplectic, unitary, and orthogonal groups over finite fields are studied [15–18]. Of course, Witt's theorem and its generalizations give a solution of problem (i), but we would like to use a set of numerical invariants to characterize an orbit and to derive the conditions satisfied by them that such an orbit exists, then the number of orbits can be computed.

Take the symplectic case as an example. Let (4)

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

Then the symplectic group of degree 2ν is defined as (5)

$$Sp_{2\nu}(\mathbb{F}_q) = \{T \in GL_{2\nu}(\mathbb{F}_q) | TK\,{}^tT = K\}.$$

Let P be an m-dimensional subspace of $\mathbb{F}_q^{(2\nu)}$. Clearly $PK\,{}^tP$ is alternate, hence rank $PK\,{}^tP$ is even. Assume that rank $PK\,{}^tP = 2s$, then P is said to be of *type* (m, s). From Dieudonné's generalization [3] of Witt's theorem it follows that two subspaces belong to the same orbit under $Sp_{2\nu}(\mathbb{F}_q)$ if and only if they are of the same type. It can be proved [15] that type (m, s) of a subspace satisfies the inequality

$$2s \leq m \leq \nu + s \tag{14}$$

and for any pair of non-negative integers (m, s) satisfying (14) there exist subspaces of type (m, s). Thus the number of orbits of subspaces under $Sp_{2\nu}(\mathbb{F}_q)$ is equal to the number of pairs of non-negative integers (m, s) satisfying (14). We computed that the latter is equal to

$$\frac{1}{2}(\nu + 1)(\nu + 2). \tag{15}$$

By the way we mention that the length $N(m, s; 2\nu)$ of the orbit of subspaces of type (m, s) of $\mathbb{F}_q^{(2\nu)}$ given in [8] is

$$N(m, s; 2\nu) = q^{2s(\nu+s-m)} \frac{\prod\limits_{i=\nu+s-m+1}^{\nu} (q^{2i} - 1)}{\prod\limits_{i=1}^{s} (q^{2i} - 1)} \prod_{i=1}^{m-2s} (q^{i} - 1) \tag{16}$$

This is the solution of problem (iii) for the symplectic group.

2) The singular symplectic, unitary, and orthogonal groups are introduced and the problems (i)–(iv) are studied [19, 20].

Take the singular symplectic case as an example. Let

$$K_l = \begin{pmatrix} K & \\ & 0^{(l)} \end{pmatrix} \tag{17}$$

where K is the nonsingular alternate matrix (4). Define

$$Sp_{2\nu+l,\nu}(\mathbb{F}_q) = \{T \in GL_{2\nu+l}(\mathbb{F}_q) | TK_l{}^tT = K_l\}, \tag{18}$$

which is called the *singular symplectic group* over $\mathbb{F}_q$. Clearly, $Sp_{2\nu+l,\nu}(\mathbb{F}_q)$ acts on $\mathbb{F}_q^{(2\nu+l)}$ in an obvious way. Then problems (i)–(iv) can be studied for $Sp_{2\nu+l,\nu}(\mathbb{F}_q)$, and complete results are obtained.

Similarly, singular unitary and orthogonal groups over $\mathbb{F}_q$ can be defined, and complete results for problems (i)–(iv) are obtained.

A natural question arises. Why do we study the geometry of singular symplectic, unitary, and orthogonal groups over finite fields ?

The answer to problem (iv) for the general linear group $GL_n(\mathbb{F}_q)$ is easy. The number of k-dimensional subspaces contained in a given m-dimensional subspace $(0 \le k \le m \le n)$ of $\mathbb{F}_q^{(n)}$ is $N(k, m)$. However, problem (iv) for the other classical groups is not so easy.

Take again the symplectic case as an example. Now assume that $Sp_{2\nu}(\mathbb{F}_q)$ acts on $\mathbb{F}_q^{(2\nu)}$. Given a subspace P of type (m, s), where (m, s) satisfies (14), we would like to compute the number of subspaces of type (m_1, s_1), where $2s_1 \le m_1 \le \nu + s_1$, contained in P. Denote this number by $N(m_1, s_1; m, s; 2\nu)$. We may choose a matrix representation of P, denoted by P again, so that

$$PK\,{}^tP = \begin{pmatrix} 0 & I^{(s)} & \\ -I^{(s)} & 0 & \\ & & 0^{(m-2s)} \end{pmatrix}. \tag{19}$$

Let P_1 be a subspace of type (m_1, s_1) contained in P. As an m_1-dimensional subspace of the m-dimensional space P, P_1 has a matrix representation, denoted by P_1 again, which is a $m_1 \times m$ matrix of rank m_1. Then as a subspace of $\mathbb{F}_q^{(2\nu)}$, the subspace P_1 has P_1P as a matrix representation. Similarly, we can choose the matrix P_1 so that

$$(P_1P)K\,{}^t(P_1P) = \begin{pmatrix} 0 & I^{(s_1)} & \\ -I^{(s_1)} & 0 & \\ & & 0^{(m_1-2s_1)} \end{pmatrix}. \tag{20}$$

Then

$$P_1 \begin{pmatrix} 0 & I^{(s)} & \\ -I^{(s)} & 0 & \\ & & 0^{(m-2s)} \end{pmatrix} {}^tP_1 = \begin{pmatrix} 0 & I^{(s_1)} & \\ -I^{(s_1)} & 0 & \\ & & 0^{(m_1-2s_1)} \end{pmatrix}. \tag{21}$$

Thus for any $T \in Sp_{2s+(m-2s),s}(\mathbb{F}_q)$, P_1TP is also a matrix representation of a subspace of type (m_1, s_1) and contained in P and as a subspace of P it is represented by the matrix P_1T. Therefore it is natural to introduce the singular symplectic group $Sp_{2s+(m-2s),s}(\mathbb{F}_q)$ and study how the subspaces of $\mathbb{F}_q^{(m)}$ are subdivided into orbits under $Sp_{2s+(m-2s),s}(\mathbb{F}_q)$, the length of each orbit, and what orbits are contained in P.

3) For pseudo-symplectic groups over finite fields of characteristic 2 problems (i)–(iv) are also studied [21, 22].

Now let $\mathbb{F}_q$ be a finite field of characteristic 2, then any $n \times n$ nonsingular non-alternate symmetric matrix over $\mathbb{F}_q$ is cogredient to either

$$S_1 = \begin{pmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & 1 \end{pmatrix}, \quad \text{when } n = 2\nu + 1 \quad \text{is odd} \tag{22}$$

or

$$S_2 = \begin{pmatrix} 0 & I^{(\nu)} & & \\ I^{(\nu)} & 0 & & \\ & & 0 & 1 \\ & & 1 & 1 \end{pmatrix}, \quad \text{when } n = 2\nu + 2 \text{ is even.} \tag{23}$$

We use S_δ ($\delta = 1$ or 2) to cover these two cases. Define the *pseudo symplectic group* of degree $2\nu + \delta$ over $\mathbb{F}_q$ to be

$$Ps_{2\nu+\delta}(\mathbb{F}_q) = \{T \in GL_{2\nu+\delta}(\mathbb{F}_q) | TS_\delta {}^tT = S_\delta\}. \tag{24}$$

It was proved by Dieudonné [3] that $Ps_{2\nu+1}(\mathbb{F}_q) \simeq Sp_{2\nu}(\mathbb{F}_q)$ and $Ps_{2\nu+2}(\mathbb{F}_q)$ has a normal series with $Sp_{2\nu}(\mathbb{F}_q)$ as one of its factors and $\mathbb{F}_q$ as all the other factors. Thus from a group theory point of view the pseudo symplectic group $Ps_{2\nu+\delta}(\mathbb{F}_q)$ is less interesting. However, its geometry is very peculiar. Let P be an m-dimensional subspace of $\mathbb{F}_q^{(2\nu+\delta)}$, then $PS_\delta {}^tP$ is a symmetric matrix and is cogredient to one of the following normal forms.

$$\begin{pmatrix} 0 & I^{(s)} & \\ I^{(s)} & 0 & \\ & & 0^{(m-2s)} \end{pmatrix}, \tag{25}$$

$$\begin{pmatrix} 0 & I^{(s)} & & \\ I^{(s)} & 0 & & \\ & & 1 & \\ & & & 0^{(m-2s-1)} \end{pmatrix}, \tag{26}$$

and

$$\begin{pmatrix} 0 & I^{(s)} & & & \\ I^{(s)} & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 1 & \\ & & & & 0^{(m-2s-2)} \end{pmatrix}. \tag{27}$$

P is called a subspace of *type* $(m, 2s+\tau, s, \varepsilon)$ where $\tau = 0, 1$, or 2 corresponding to the above three normal forms (25), (26), or (27), respectively, and $\varepsilon = 0$ or

1 corresponding to the cases $e_{2\nu+1} \notin P$ or $e_{2\nu+1} \in P$, respectively, $e_{2\nu+1}$ is the $(2\nu+\delta)$-dimensional row vector whose $(2\nu+1)$-th component is 1 and other components are all 0. It is proved that two subspaces of $\mathbb{F}_q^{(2\nu+\delta)}$ belong to the same orbit under $Ps_{2\nu+\delta}(\mathbb{F}_q)$ if and only if they are of the same type. It is also proved that subspaces of type $(m, 2s+\tau, s, \varepsilon)$ exist if and only if

$$(\tau,\varepsilon) = \begin{cases} (0,0),(1,0),(1,1), \text{ or } (2,0), & \text{when } \delta = 1, \\ (0,0),(0,1),(1,0),(2,0), \text{ or } (2,1), & \text{when } \delta = 2 \end{cases} \tag{28}$$

and

$$2s + \max\{\tau,\varepsilon\} \leq m \leq \nu + s + [(\tau+\delta-1)/2] + \varepsilon. \tag{29}$$

Using conditions (28) and (29) we can compute the number of orbits of subspaces under $Ps_{2\nu+\delta}(\mathbb{F}_q)$, which is equal to

$$\frac{1}{2}(\nu+1)((\nu+4)\delta+3\nu). \tag{30}$$

Denote the length of the orbit of subspaces of type $(m, 2s+\tau, s, \varepsilon)$ by $N(m, 2s+\tau, s, \varepsilon; 2\nu+\delta)$. Then

$$N(m, 2s+\tau, s, \varepsilon; 2\nu+\delta) = q^{n_0+2(s+(2-\delta)[\tau/2])(\nu+s-m+\delta[(\tau+1)/2]+(\delta-1)(\tau-1)(\tau-2)\varepsilon/2)}$$

$$\times \frac{\prod_{i=\nu+s-m+[(\tau+\delta-1)/2]+\epsilon+1}^{\nu} (q^{2i}-1)}{\prod_{i=1}^{s}(q^{2i}-1) \prod_{i=1}^{m-2s-\max(\tau,\epsilon)} (q^i-1)}, \tag{31}$$

where $n_0 = 1$ when $\delta = 1$, and $n_0 = m, 0, 2(\nu+1)-m$, $2(\nu+1)-m$, or $2(\nu+1)-m$ corresponding to the cases $(\tau,\varepsilon) = (0,0),(0,1),(1,0),(2,0)$, or $(2,1)$, respectively, when $\delta = 2$.

In order to study problem (iv) for the pseudo symplectic group $Ps_{2\nu+\delta}(\mathbb{F}_q)$ the singular pseudo symplectic group is introduced and for which problems (i)-(iii) are studied [22].

4) The affine classification of quadrics over finite fields is obtained [23, 24].

The foregoing results together with our results obtained in the mid sixties are compiled in the monograph [25].

5. Applications

Why do we study problems (i)–(iv) for the classical groups over finite fields ? Of course, they are well-posed mathematical problems and were studied by several famous mathematicians before us. However, we have been interested in these problems mainly because they have interesting applications. In the sixties the geometry of classical groups over finite fields was used to construct association schemes and PBIB designs. I came back to this field in the early nineties because I found that it could be used to construct authentication codes.

In 1954 W.H.Clatworthy [26] showed that a geometric configuration in $PG(3,\mathbb{F}_q)$ may be interpreted as a PBIB design. In our terminology, he took the set of 1-dimensional subspaces of the 4-dimensional symplectic space over $\mathbb{F}_q$ as the set of treatments and set of 2-dimensional totally isotropic subspaces as the set of blocks. Two treatments are said to be the first associates (or second associates) if they span a 2-dimensional totally isotropic subspace (or non-isotropic subspace), respectively. A treatment is defined to be set in a block if the 1-dimensional subspace as the treatment is contained in the 2-dimensional totally isotropic subspace as the block. Then a PBIB(2) design is obtained. Clatworthy also computed the parameters of the design.

In 1962 D.K.Ray-Chaudhuri [27] used the geometry of orthogonal groups, which was called the geometry of quadrics by him, to construct PBIB designs. He constructed several PBIB(2) designs with 1-dimensional or 2-dimensional totally isotropic (or singular) subspaces of the geometry of orthogonal groups over finite fields as treatments or blocks and computed their parameters. At that time only the number of totally isotropic (or singular) subspaces of a given dimension is known, so he naturally restrict himself to take only totally isotropic (or singular) subspaces as treatments and blocks in order to compute the parameters of the designs he constructed.

In the mid sixties after we had found the closed formulas of the number of subspaces in any orbit under the symplectic, unitary, and orthogonal groups over finite fields, we [28, 9, 29, 30] constructed many asssociation schemes and PBIB designs by taking the 1-dimensional, 2-dimensional, or ν-dimensional totally isotropic subspaces as treatments and subspaces of any given type as blocks and computed their parameters. These results were also compiled in the monograph [12] and sketched in [31]. They will not be repeated here.

However, we would like to mention that when we take the 2-dimensional totally isotropic (or singular) subspaces as treatments to construct association schemes and PBIB designs, we consider only the symplectic, unitary, and orthogonal space of low dimensions. Because in the higher dimensional case if we take the 2-dimensional totally isotropic (or singular) subspaces as treatments, the computation of intersection numbers is not so immediate.

Of course, we can take any orbit of subspaces under the symplectic, unitary, or orthogonal group over finite fields as the set of treatments and define the associate relation according to the orbit of pairs of treatments under that group, then an association scheme is obtained. Moreover, if we take any orbit of subspaces as the set of blocks and define a treatment to be set in a block in a certain way, then a PBIB design is obtained. To compute the parameters of the association scheme and the PBIB design thus obtained the computation of intersection numbers is usually not so immediate. In a short note [32] published in 1965 some association schemes and PBIB designs were constructed by taking the 1-dimensionsl non-isotropic (or non-singular) subspaces in the unitary or orthogonal geometry over some small fields as treatments and their parameters were computed. In the eighties the idea of taking the 1-dimensional non-isotropic (or non-singular) subspaces or taking the 2-dimensional totally isotropic (or singular) subspaces as treatments were carried out by several Chinese mathematicians and their works were sketched in [31] and will not be repeated.

In the following we shall mention how to use the geometry of classical groups over finite fields to construct authentication code, since it is rather new and more work could be done.

Let $\mathcal{S}, \mathcal{E}$, and $\mathcal{M}$ be three nonempty finite sets and let $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ be a map, the four tuple $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is called an *authentication code* [33], if

1) The map $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ is surjective and
2) For any $m \in \mathcal{M}$ and $e \in \mathcal{E}$, if there is an $s \in \mathcal{S}$ satisfying $f(s, e) = m$, then such an s is uniquely determined by the given m and e.

Suppose that $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is an authentication code, then $\mathcal{S}, \mathcal{E}$, and $\mathcal{M}$ are called the set of *source states*, the set of *encoding rules*, and the set of *messages*, respectively, and f is called the *encoding map.* Let $s \in \mathcal{S}, e \in \mathcal{E}$, and $m \in \mathcal{M}$ be such that $m = f(s, e)$, then we say that the source state s is encoded into the message m under the encoding rule e, and for convenience we say that the message m contains the encoding rule e. The cardinals $|\mathcal{S}|, |\mathcal{E}|, |\mathcal{M}|$ are called the *size parameters* of the code . Moreover if the authentication code satisfies the further requirement that given any message m there is a unique source state s such that $m = f(s, e)$ for every encoding rule e contained in m, then the code is called a *Cartesian* authentication code.

Authentication codes are used in communication channels where besides the transmitter and the receiver there is an opponent who may play either the impersonation attack or the substitution attack. By an *impersonation attack* we mean that the opponent sends a message through the channel to the receiver and hopes the receiver will accept it as authentic. i.e., as a message sent by the transmitter. By a *substitution attack* we mean that after the opponent intercepts a message sent by the transmitter to the receiver, he sends another message instead and hopes the receiver will accept it as authentic. To protect against these attacks the transmitter-receiver may use an authentication code which is publicly known and choose a fixed encoding rule e in secret. The set of information which the transmitter would like to be able to transmit to the receiver should be identified with the set of source states of the code. Suppose that the transmitter wants to send a source state s to the receiver, he first encodes s into a message m under the encoding rule e, i.e., $m = f(s, e)$, and then sends m to the receiver. Once the receiver receives a message m', he first has to judge whether m' is authentic, i.e., whether the encoding rule e is contained in m'. If $e \in m'$. then he regards m' as authentic and decodes m' by e to get a source state s', where $m' = f(s', e)$. If $e \notin m'$ then he regards m' as a false message. The object of the component is to choose a message and send it to the receiver so that the probability of deceiving the receiver, i.e., of causing him to accept as authentic a message not sent by the transmitter is as large as possible. We denote by P_I and P_S, respectively, the largest probabilities that he could deceive the receiver when he plays an impersonation attack and a substitution attack and call them the probabilities of a successful impersonation attack and of a successful substitution attack, respectively.

In [34] some authentication codes based on projective geometry over finite fields were constructed. Projective geometry, according to Klein's Erlangen Program, is the geometry of the projective general linear group. Then it is natural to propose the problem whether it is possible to construct authentication codes from the geometry of symplectic, unitary, or orthogonal groups over finite fields. The answer is of course positive and some authentication codes have been so constructed [35–38]. To illustrate we give a construction [38] below.

Consider the 2ν-dimensional symplectic space over $\mathbb{F}_q$, i.e., the 2ν-dimensional row vector space $\mathbb{F}_q^{(2\nu)}$ on which the symplectic group $Sp_{2\nu}(\mathbb{F}_q)$ acts. Assume that $\nu \geq 2$ and let s be an integer such that $1 \leq s < \nu$. Let P_0 be a fixed subspace of type $(s, 0)$. Take the set of subspces of type $(2s, s)$ containing P_0 to be the set $\mathcal{S}$ of source states, the set of s-dimensional subspaces whose joins with P_0 are subspaces of type $(2s, s)$ to be the set $\mathcal{E}$ of encoding rules and also the set $\mathcal{M}$ of messages. For any source state s and encoding rule e, let $f(s, e) = s \cap e^{\perp}$, where

$$e^{\perp} = \{x \in \mathbb{F}_q^{(2\nu)} | xK\,{}^t e = 0\}.$$

It can be proved that $s \cap e^{\perp}$ is an s-dimensional subspace whose join with P_0 is of type $(2s, s)$. Thus we may define $f(s, e) = s \cap e^{\perp}$ to be the message into which the source state s is encoded using the encoding rule e. Then a Cartesian authentication code is obtained and its size parameters are

$$|\mathcal{S}| = q^{2s(\nu-s)}, \quad |\mathcal{E}| = |\mathcal{M}| = q^{s(2\nu-s)}.$$

Now assume that the encoding rules are chosen according to a uniform probability distribution. Then the probabilities of a successful impersonation attack and a successful substitution attack are, respectively,

$$P_I = \frac{1}{q^{s^2}}, \quad P_S = \frac{1}{q^s}$$

In virtue of the combinatorial lower bounds $P_I \geq |\mathcal{S}|/|\mathcal{M}|$ and $P_S \geq (|\mathcal{S}| - 1)/(|\mathcal{M}| - 1)$, for the authentication code constructed above P_I is optimal. If we require the order of magnitude of P_S as a function of q to be optimal, then for the code, P_S is nearly optimal when and only when $s = 1$.

Similar constructions can be done for the unitary and orthogonal cases.

Finally, it should be added that the geometry of classical groups was also used in the study of correlation properties of binary $m-$sequences [39–41, 20] and in the construction of projective codes with few weights [42–46].

References

[1] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, *J. Reine Angew. Math.*, **176**(1937), 31–44.

[2] C. Arf, Untersuchungen iiber quadratischen Formen in Körpern der Charakteristik 2, Teil I, *J. Reine Angqw. Math.*, **183** (1941), 148–167.

[3] J. Dieudonné, *Sur les groupes classiques*, Hermann, Paris, 1948.

[4] J. Dieudonné, On the structure of unitary groups, *Trans. Amer. Math. Soc.*, **72**(1952), 367–385.

[5] L. K. Hua, A generalization of Hermitian matrices, *Acta Scientia Sinica*, 2(1953), 1–58.

[6] V. Pless, On Witt's theorem for nonalternating symmetric bilinear forms over a field of characteristic 2, *Proc. Amer. Math. Sco.*, **15**(1964), 979–983.

[7] B. Segre, On Galois geometries, *Proc. Intern. Congress Math.* 1958, Cambridge, 1960, 488–499.

[8] Z, Wan, Notes on finite geometries and the construction of PBIB designs I, Some "Anzahl" theorems in symplectic geometry over finite fields, *Acta Scientia Sinica*, **13**, (1964), 515–516.

[9] Z. Wan and B. Yang, Notes on finite geometries and the construction of PBIB designs III, Some "Anzahl" theorems in unitary geometry over finite fields and their applications, *Acta Scientia Sinica*, **13** (1964), 1006–1007.

[10] Z. Dai and X. Feng, Notes on finite geometries and the construction of PBIB designs IV, Some "Anzahl" theorems in orthogonal geometry over finite fields of characteristic not 2, *Acta Scientia Sinica*, **13** (1964), 2001–2004.

[11] X. Feng and Z. Dai, Notes on finite geometries and the construction of PBIB designs V, Some "Anzahl" theorems in orthogonal geometry over finite fields of characteristic 2, *Acta Scientia Sinica*, **13** (1964), 2005–2008.

[12] Z. Wan, Z. Dai, X. Feng, and B. Yang, *Studies on Finite Geometry and the Construction of Incomplete Block Designs,* Science Press, Beijing, 1966. (In Chinese.)

[13] V. Pless, The number of isotropic subspaces in a finite geometry, *Atti Accad. Naz. Lincei. Rend.*, **39** (1965), 418–421.

[14] R. C. Bose and I. M. Chakravati, Hermitian varieties in a finite projective space PG(N, q^2), *Canad. J. Math.*, **18** (1966), 1161–1182.

[15] Z. Wan, On the symplectic invariants of a subspace of a vector space, *Acta Mathematica Scientia*, **11**(1991), 251–253.

[16] Z. Wan, On the unitary invariants of a subspace of a vector space over a finite field, Chinese Science Bulletin, **37**(1992), 705–707.

[17] Z. Wan, On the orthogonal invariants of a subspace of a vector space over a finite field of odd characteristic, accepted for publication in *Linear Algebra and Its Applications.*

[18] Z. Wan, On the orthogonal invariants of a subspace of a vector space over a finite field of even characteristic, accepted for publication in *Linear Algebra and Its Applications.*

[19] Z. Wan, Some Anzahl theorems in finite singular symplectic, unitary and orthogonal geometries, accepted for publication in *Discrete Mathematics.*

[20] Z. Wan, Further studies on singular symplectic, unitary, and orthogonal geometries over finite fields, preprint.

[21] Y. Liu and Z. Wan, Pseudo symplectic geometries over finite fields of characteristic two, *Recent Advances on Finite Geometries and Designs,* ed. by J. Hirschfeld et al., Oxford University Press, 1991, 265–288.

[22] Z. Wan, Singular pseudo symplectic geometry over finite fields of characteristic 2, accepted for publication in *Northeastern Mathematical Journal.*

[23] Z. Wan, Quadrics in $AG(n,\mathbb{F}_q)$ for q odd, *Chinese Science Bulletin,* **36**(1991), 2014–2015.

[24] Z. Wan, Quadrics in $AG(n, \mathbb{F}_q)$ for q even, *Chinese Science Bulletin,* **36** (1991), 2016–2017.

[25] Z. Wan, *Geometry of Classical Groups over Finite Fields*, studentlitteratur, Lund, 1993.

[26] W. H. Clatworthy, A geometrical configuration which is a partially

balanced incomplete block design, *Proc. Amer. Math. Soc*, **5**(1954), 47–55.

[27] D. K. Ray-Chaudhuri, Application of the geometry of quadrics for constructing PBIB designs, *Annals of Mathematical Statistics*, **33** (1962), 1175–1186.

[28] Z. Wan, Notes on finite geometries and the construction of PBIB designs II, Some PBIB designs with two associate classes based on the symplectic geometry over finite fields, *Scientia Sinica*, **13** (1964), 516–517.

[29] B. Yang, Finite geometries and the construction of incomplete block designs, VII Association schemes with several associate classes by taking the maximal totally isotropic subspaces in the symplectic geometry over finite fields as treatments, *Acta Mathematica Sinica*, **15**(1955), 812–825. (In Chinese.)

[30] B. Yang, Finite geometries and the construction of incomplete block designs, VIII Association schemes with several associate classes by taking the maximal totally isotropic subspaces in the unitary geometry over finite fields as treatments, *Acta Mathematica Sinica*, **15**(1965), 826–841. (In Chinese.)

[31] Z. Wan, Finite geometries and block designs, *Sankhya: The Indian Journal of Statistics, Senes A,* **54**(1991).

[32] Z. Wan, Notes on finite geometries and the construction of PBIB designs VI, Some association schemes and PBIB designs based on finite geometries, *Scientia Sinica*, **14**(1965), 1872–1876.

[33] G. Simmons, Authentication theory/secrecy theory, *Advances in Cryptography, Proc. of Crypto* 84, *Lecture Notes in Computer Science*, No. 196, Springer, 1985, 411–431.

[34] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, *Bell System Technical Journal* **53**(1974), 405–424.

[35] Z. Wan, B. Smeets and P. Vanroose, On the construction of authentication codes over symplectic spaces, preprint.

[36] Z. Wan, Further constructions of Cartesian authentication codes from symplectic geometry, *Northeastern Mathematical Journal*, 8(1992), 4–20.

[37] Z. Wan, Constructions of Cartesian authentication codes from unitary geometry, *Designs, Codes and Cryptography*, 2(1992), 335–356.

[38] R. Feng and Z. Wan, A new construction of Cartesian authentication codes from geometry of classical groups, preprint.

[39] T. Hϕholdt and J. Justeen, Tenary sequences with perfect periodic autocorrelation, *IEEE Transactions on Information Theory*, **IT–19**(1983) 597-600.

[40] R. A. Games, The geometry quadrics and correlations of sequences, *IEEE Transactions on Information Theory*, **IT–32**(1986), 423–426.

[41] R. A. Games, The geometry of m-sequences: three-valued crosscorrelations and quadrics in finite projective geometry, *SIAM J. Alg. Disc. Math.*, **7**(1986), 43–52.

[42] J. Wolfman, Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie, *Discrete Math.*, **13**(1975), 185–211.

[43] J. Wolfman, Codes projectifs à deux poids, " caps" complets et ensembles de differences, *J. Comb. Theory.,* Series A, **23**(1977), 208–222.

[44] I. M. Chakravarti, Families of codes with few distinct weights from singular and non-singular Hermitian varieties and quadrics in projective geometries and Hadamard difference sets and designs associated with two-weight codes, *IMA Volumes in Math. and Its Applications.*, **20**, Springer, 1990, 35–50.

[45] J. W. P. Hirschfeld, M. A. Tafasman, and S. G. Vladut, The weight hierachy of higher-dimensional Hermitian codes, preprint.

[46] Z. Wan, The weight hierachies of the projective codes from nondegenerate quadrics, preprints.