Journal of Mathematical Research & Exposition
Nov., 2008, Vol. 28, No. 4, pp. 1021–1026
DOI:10.3770/j.issn:1000-341X.2008.04.038
Http://jmre.dlut.edu.cn

The Subspace Representations of Finite Field and Its Applications

LIU Shuxia[1], *ZHANG Chunhua*[2], *MENG Guifen*[3], *WANG Mei*[1]
(1. College of Mathematics and Information Science, Hebei Normal University, Hebei 050016, China;
2. Hengshui Radio and TV University, Hebei 053000, China;
3. Chengde Vocational Institute, Hebei 067000, China)
(E-mail: liu_shuxia2005@126.com)

Abstract In this paper, some problems on representations of subspace in a finite field are discussed, a result in [3] is generalized, and a new proof about Singer Difference Sets is given. Finally, a class of association schemes are constructed by all affine hyperplanes in a finite field and the parameters are computed.

Keywords finite field; association schemes.

Document code A
MR(2000) Subject Classification 05E30
Chinese Library Classification O153

1. Introduction

The theory of finite fields plays an important role in theoretical mathematics and also finds various applications in computer science, coding theory, cryptography, algebraic geometry, number theory, group theory, and many branches in discrete mathematics. Therefore, it is very important to study the theory of finite field.

In this paper, some problems on representations of subspace in a finite field are discussed, a result in [3] is generalized in Sections 2, and a new proof about Singer Difference Sets is given in Section 3. Finally, in Section 4 a class of association schemes are constructed by all affine hyperplanes in a finite field, and the parameters are computed.

2. Representations of subspace in a finite field

Let F_q be a finite field with q elements, where q is a power of the prime p. F_{q^n} is an n degree extension field of F_q. Let $N=\{x^q-x|x\in F_{q^n}\}$ be a subset of F_{q^n}. When $q=2$, we have

Lemma 2.1[3] *Suppose that F_{2^n} is a finite field of characteristic 2, where $n\geq 2$. Then*

$$|(a_1N+b_1)\cap(a_2N+b_2)\cap\cdots\cap(a_mN+b_m)|=2^{n-m}$$

if and only if $a_1^{-1},a_2^{-1},\ldots,a_m^{-1}$ are linearly independent over F_2, where $a_i,b_i\in F_{2^n},a_i\neq 0,i=1,2,\ldots,m$.

Received date: 2006-09-11; **Accepted date**: 2007-01-19
Foundation item: the Natural Science Foundation of Hebei Province (No. A2008000135).

In this section, we discuss some problems on representations of subspace in a finite field F_{q^n} over F_q, and generalize a result in Lemma 2.1. At first, we introduce some properties of a finite field and some counting results on subspaces of vector space over a finite field. More information can be found in [2] and [5].

For $\alpha \in F = F_{q^n}$, we define the trace of α on $K = F_q$ as

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

Lemma 2.2[2] *If F is a finite extension field on a field K, then for $\alpha \in F$, we have $Tr_{F/K}(\alpha) = 0$ if and only if $\alpha \in N$.*

Lemma 2.3[5] *If $0 \leq m \leq n$, F is a vector space with dimension n on K, then the number of m dimensional subspace of F, denoted by $N(m, n)$, is*

$$\frac{\Pi_{i=n-m+1}^{n}(q^i - 1)}{\Pi_{i=1}^{m}(q^i - 1)}.$$

Considering F as a vector space of dimension n over K, we define a symmetric inner product over F as follows：

$$(a, b) = Tr_{F/K}(ab), \quad \forall a, b \in F.$$

Obviously, this inner product is non-degenerate. Notice that the map $\varphi : F \to N$ given by

$$\varphi : x \mapsto x^q - x, \forall x \in F$$

is a group epimorphism, where $N = \{x^q - x \mid \ x \in F\}$ is subgroup of additive group F, and the kernel of φ is just K. So $|N| = q^{n-1}$, and N is an $(n-1)$-dimensional subspace over K of F. For an arbitrary $a \in F, a \neq 0$, aN is an $(n-1)$-dimensional subspace of F, and has the orthogonal complement $(aN)^{\perp} = \langle a^{-1} \rangle$. Therefore, $aN = bN$, $\forall a, b \in F^*$ if and only if $ab^{-1} \in K^*$, where F^* and K^* denote respectively the multiplication groups of F and K. Thus, the number of these $n-1$-dimensional subspaces of F with the form aN is $\frac{q^n-1}{q-1}$. By Lemma 2.3, $\{aN | a \in F^*\}$ presents all the subspaces of dimension $n-1$ in F. So each affine hyperplane of F is of the form $aN + b$, where $a \in F^*, b \in F$. By linear algebra, we have the following theorem.

Theorem 2.4 *Suppose that K is a finite field with q elements of characteristic p, and F is an n degree extension field of K, where $n \geq 2$. If $N = \{x^q - x | x \in F\}$, then*

$$|(a_1N + b_1) \cap (a_2N + b_2) \cap \cdots \cap (a_mN + b_m)| = q^{n-m}$$

if and only if $a_1^{-1}, a_2^{-1}, \ldots, a_m^{-1}$ are linearly independent over K, where $a_i, b_i \in F_q, a_i \neq 0, i = 1, 2, \ldots, m$.

3. Singer differece set

In this section, we apply Theorem 2.4 to give another proof of Singer difference sets.

Definition 3.1 *Let G be an additively written group of order v. A k-subset D of G is called a $(v, k, \lambda; n)$-difference set, if every nonzero element g of G has exactly λ representations as a* *difference $x-y$ with elements from D. In particular, the difference set is cyclic if the group G is cyclic.*

Theorem 3.2[4] *Suppose that q is a power of a prime, $n \geq 3$ an integer, then there exists a (v,k,λ)-cyclic difference set with the parameters*

$$v=\frac{q^n-1}{q-1}, k=\frac{q^{n-1}-1}{q-1}, \lambda=\frac{q^{n-2}-1}{q-1}.$$

Proof Suppose that K is a finite field with q elements of characteristic p, and F is an n degree extension field of K, $n \geq 3$. We know that the multiplicative group of a finite field is cyclic. Denote by M the quotient group F^* modulo K^*. Obviously, M is a cyclic group of order $\frac{q^n-1}{q-1}$. Let $D=\{xK^*|x \in N^*\}$, where N^* denotes the set of all nonzero elements in the set $N=\{x^q-x|x \in F\}$. Notice that for any $x,y \in F^*$, $xK^*=yK^*$ if and only if $y^{-1}x \in K^*$. Furthermore, since $x^q=x, \forall x \in K^*$, $a \in N^*$ if and only if $ax \in N^*, \forall x \in K^*$. Therefore, the subset D of M has $\frac{q^{n-1}-1}{q-1}$ elements. For any nonidentity tK^* of M, $aK^*, bK^* \in D$ such that $aK^*(b^{-1})K^*=tK^*$ if and only if $aK^*=tbK^*$. Obviously,$a \in N^* \cap tN^*$. Since $tK^* \neq K^*, t^{-1} \notin K^*$, by Theorem 2.4, there are $q^{n-2}-1$ possible choices for a. Notice that $a \in N^*$ if and only if $ax \in N^*, \forall x \in K^*$. So there are $\frac{q^{n-2}-1}{q-1}$ possible choices for aK^*. Once aK^* is chosen, bK^* is unique, that is, $bK^*=t^{-1}aK^*$. Thus, we obtain a (v,k,λ)-cyclic difference set, where

$$v=\frac{q^n-1}{q-1}, k=\frac{q^{n-1}-1}{q-1}, \lambda=\frac{q^{n-2}-1}{q-1}.$$

4. A class of association schemes

Association schemes have close connections with coding theory, design theory and finite group theory, etc. It has become an important and basic part of algebraic combinatorics. We refer to [1] for more about association schemes.

Let X be the finite set with n elements and $R_0, R_1, \ldots, R_d$ be subsets of $X \times X$, which satisfy the following conditions

(1) $R_0=\{(x,x)|x \in X\}$;

(2) $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$, $R_i \cap R_j = \phi$ $(i \neq j)$;

(3) For any i, there is some $i' \in \{0,1,\ldots,d\}$ such that

$${}^tR_i=\{(x,y)|(y,x) \in R_i\}=R_{i'};$$

(4) For any $i,j,k \in \{0,1,\ldots,d\}$, $|\{z \in X|(x,z) \in R_i,(z,y) \in R_j\}|$ is a constant whenever $(x,y) \in R_k$, which is denoted by p_{ij}^k, called the intersection number.

The configuration $\mathcal{X}=(X,\{R_i\}_{0 \leq i \leq d})$ is called an association scheme on X. Moreover, an association scheme with the following additional condition;

(5) $p_{ij}^k=p_{ji}^k$, $\forall i,j$, is called a commutative association scheme. And an association scheme with the following additional condition;

(6) $i'=i$, $\forall i$, is called a symmetric association scheme. Obviously, a symmetric association

scheme is necessarily commutative. n and p_{ij}^k are called parameters of an association scheme. $k_i = p_{ii'}^0$ is called the valency of R_i.

It is known that the parameters of an association scheme of class d have the following basic relations

$$k_i = p_{ii'}^0, k_0 = 1, |X| = k_0 + k_1 + \cdots + k_d,$$

$$p_{0j}^i = \delta_{ij}, \quad p_{j0}^i = \delta_{ij}, \quad p_{ij}^0 = k_i\delta_{ij'}, \quad p_{jk}^i = p_{j'k'}^{i'},$$

$$\sum_{k=0}^d p_{jk}^i = k_j, \quad k_i p_{jk}^i = k_j p_{ik'}^j, \quad \sum_{m=0}^d p_{ij}^m p_{km}^l = \sum_{n=0}^d p_{ki}^n p_{nj}^l.$$

Example Suppose that G is a finite group, and acts transitively on the finite set $\Omega(|\Omega| = n > 1)$. It deduces a natural action on the set $\Omega \times \Omega$, that is, for any $(x, y) \in \Omega \times \Omega$, $\sigma \in G$,

$$(x, y)^\sigma = (x^\sigma, y^\sigma).$$

Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_d$ be the orbits of G on $\Omega \times \Omega$, where $\Lambda_0 = \{(x, x)|x \in \Omega\}$. Then $\mathcal{X} = (\Omega, \{\Lambda_i\}_{0\le i\le d})$ is an association scheme.

Let $K = F_q$ be a finite field with q elements of characteristic p, $F = F_{q^n}$ be an n $(n \ge 2)$ degree extension field of K, $N = \{x^q - x|x \in F\}$, $\Omega = \{aN + b|a \in F^*, b \in F\}$, that is, the set of all affine superplanes of F over K and $G = \{(x, y)|x \in F^*, y \in F\}$. Define a binary operation $*_i, (i = 1, 2)$ on G, called multiplication,

$$(x_1, y_1) *_1 (x_2, y_2) = (x_1x_2, x_1y_2 + y_1),$$

$$(x_1, y_1) *_2 (x_2, y_2) = (x_1x_2, y_2 + x_2^{-1}y_1).$$

It is easy to verify that G is a group with order $q^n(q^n - 1)$ for $*_i, (i = 1, 2)$.

Define the action of $(G, *_1)$ on the set Ω

$$(x, y)(aN + b) = (axN + bx + y), \forall(x, y) \in G, aN + b \in \Omega.$$

Obviously, it is transitive. Thus, we obtain a class of association schemes by this action. Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_d$ be the orbits of $(G, *_1)$ on $\Omega \times \Omega$. By the transitivity, we have that every orbit contains an element of the form $(N, aN + b)$. The orbit containing the element $(N, aN + b)$ is denoted by $[a, b]$. $(N, aN + b)$ and $(N, cN + d)$ are in an orbit if and only if there exists $(x, y) \in (G, *_1)$ such that $(x, y)((N, aN + b)) = (N, cN + d)$, that is,

$$x \in K^*, y \in N, ac^{-1} \in K^*, bx + y - d \in aN.$$

(i) Whence $a \in K^*$, $aN = N$. By Theorem 2.4, $(N, N + b)$ and $(N, cN + d)$ belong to the same orbit if and only if there exists $x \in K^*$ such that $c \in K^*, bx - d \in N$. Notice that, if $b \in N$, then $bx \in N$ by $x \in K^*$, so $d \in N$. Contrarily, if $d \in N$, then $b \in N$. Furthermore, if $b \notin N$, then $d \notin N$. Consider N as an $(n - 1)$-dimension subspace of F over K and let $\alpha_i, i = 1, \ldots, n - 1$, be a base of N. Since $b \notin N$, $b, \alpha_i, i = 1, \ldots, n - 1$, are a base of F over K. So there exists a group of elements $\lambda, \mu_i \in K, i = 1, \ldots, n - 1$ such that

$$-d = \lambda b + \mu_1\alpha_1 + \cdots + \mu_{n-1}\alpha_{n-1}.$$

Let $x = -\lambda \in K^*$. From $d \notin N$ and $\lambda \neq 0$ it follows $bx - d \in N$. From the above argument, we have that, when $a \in K^*$, $(N, aN + b)$ and $(N, cN + d)$ belong to the same orbit if and only if $c \in K^*, b, d \in N$ or $c \in K^*, b, d \notin N$;

(ii) When $a \notin K^*$, by Theorem 2.4, $|(N + bx - d) \cap aN| = q^{n-2} \geq 1$. $(N, aN + b)$ and $(N, cN + d)$ belong to the same orbit if and only if $ac^{-1} \in K^*$.

From above, we have

Theorem 4.1 *With the definition of the group $(G, *_1)$ and the set Ω as above, the action of $(G, *_1)$ on Ω is transitive. Define an association scheme with $\frac{q^n-1}{q-1}$ classes by this action, denoted by $\mathcal{X}_1$. Suppose that α is a fixed element in F and not in N, and $K^*, a_1K^*, \ldots, a_{\frac{(q^n-1)}{q-1}-1}K^*$ are all cosets of K^* in $F*$. Then*

$$[1,0], [1,\alpha], [a_j, 0], j = 1, \ldots, \frac{(q^n-1)}{q-1} - 1$$

are all classes of $\mathcal{X}_1$.

Theorem 4.2 *The parameters of $\mathcal{X}_1$ are the following:*

$$n = \frac{q(q^n-1)}{q-1}; k_0 = k_{[1,0]} = 1, k_{[1,\alpha]} = q - 1,$$

$$k_{[a_j,0]} = q, j = 1, \ldots, \frac{(q^n-1)}{q-1} - 1,$$

$$k^{[1,\alpha]}_{[1,\alpha],[1,\alpha]} = q - 2, \quad k^{[1,\alpha]}_{[1,\alpha],[a_j,0]} = 0, \quad k^{[1,\alpha]}_{[a_i,0],[1,\alpha]} = 0,$$

$$k^{[1,\alpha]}_{[a_i,0],[a_j,0]} = \begin{cases} q & a_ia_j = 1 \\ 0 & a_ia_j \neq 1 \end{cases}, \quad k^{[a_k,0]}_{[1,\alpha],[1,\alpha]} = 0,$$

$$k^{[a_k,0]}_{[1,\alpha],[a_j,0]} = \begin{cases} q-1 & a_k = a_j \\ 0 & a_k \neq a_j \end{cases}, \quad k^{[a_k,0]}_{[a_i,0],[1,\alpha_t]} = \begin{cases} q-1 & a_k = a_i \\ 0 & a_k \neq a_i \end{cases},$$

$$k^{[a_k,0]}_{[a_i,0],[a_j,0]} = \begin{cases} q & a_k = a_ia_j \\ 0 & a_k \neq a_ia_j \end{cases}.$$

Proof We only compute $k^{[1,\alpha]}_{[a_i,0],[a_j,0]}$ as example, and the others are similar.

Now that the element $(N, N + \alpha) \in [1, \alpha]$ is chosen, then

$$k^{[1,\alpha]}_{[a_i,0],[a_j,0]} = |\{xN + y \in \Omega | (N, xN + y) \in [a_i, 0], (xN + y, N + \alpha) \in [a_j, 0]\}|.$$

Since $(N, xN + y)$ and (N, a_iN) belong to the same orbit if and only if $x{a_i}^{-1} \in K^*$. Therefore, $x = a_i, y \in F$. Furthermore, $(xN + y, N + \alpha)$ and (N, a_jN) belong to the same orbit if and only if $x = {a_j}^{-1}$. So, if $a_ia_j = 1$, then there are q possible choices for $xN + y$. Otherwise, there are 0 possible choices for $xN + y$.

Notice that $[a_i, 0] = [a_i, 0]'$ if and only if $a_i^2 \in K^*$, that is, the order of a_iK^* is 2 in the quotient group of F^* modulo K^*. Since this quotient group is cyclic, for any i, $a_i^2 \in K^*$ if and only if the order of the quotient group is 2. By calculation, the equation $\frac{q^n-1}{q-1} = 2$ has no solution. Therefore, $\mathcal{X}_1$ is not symmetric. By the parameters in Theorem 4.2, $\mathcal{X}_1$ is a commutative association scheme. Thus, we have

Corollary 4.3 *The association scheme $\mathcal{X}_1$ is commutative and nonsymmetric.*

Suppose that $\mathcal{X} = (X, \{R_i\}_{0\leq i\leq d})$ and $\mathcal{Y} = (Y, \{\Lambda_i\}_{0\leq i\leq d})$ are two association schemes, and their classes are equal. Let $|X| = |Y|$, f be a bijective map from X to Y, and a permutation $\sigma(f)$ be induced on the set $\{0, 1, \ldots, d\}$, that is, for any elements u and v in X, $(u, v) \in R_i$ if and only if $(f(u), f(v)) \in \Lambda_{i^{\sigma(f)}}$. Then f is called an isomorphism between $\mathcal{X}$ and $\mathcal{Y}$. Whence $\mathcal{X}$ is isomorphic to $\mathcal{Y}$.

Define the action of $(G, *_2)$ on Ω

$$(x, y)(aN + b) = (axN + bx + yx), \quad \forall (x, y) \in G, aN + b \in \Omega.$$

Obviously, this action is transitive. Thus, it induces a class of association schemes, denoted by $\mathcal{X}_2$.

Let φ be a map from the group $(G, *_1)$ to the group $(G, *_2)$, such that $\varphi(x, y) = (x, xy), \forall (x, y) \in (G, *_1)$. It is easy to verify that φ is an isomorphism between $(G, *_1)$ and $(G, *_2)$, and satisfies that for any $aN + b \in \Omega$,

$$(x, y)(aN + b) = \varphi(x, y)(aN + b), \quad \forall (x, y) \in (G, *_1).$$

Therefore, the orbits of $(G, *_1)$ on $\Omega \times \Omega$ are the same as $(G, *_2)$ $\Omega \times \Omega$. So, we have

Theorem 4.4 *$\mathcal{X}_1$ is isomorphic to $\mathcal{X}_2$.*

References

[1] BANNAI E, ITO T. *Algebraic combinatorics. I. Association Schemes* [M]. The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.

[2] LIDL R, NIEDERREITER H. *Finite Fields* [M]. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[3] MA Changli, WANG Yangxian. *Automorphisms of association schemes of quadratic forms over a finite field of characteristic two* [J]. Algebra Colloq., 2003, **10**(1): 63–74.

[4] SINGER J. *A theorem in finite projective geometry and some applications to number theory* [J]. Trans. Amer. Math. Soc., 1938, **43**(3): 377–385.

[5] WAN Zhexian. *Geometry of Classical Groups over Finite Fields* [M]. Studentlitteratur, Lund; Chartwell-Bratt Ltd., Bromley, 1993.