A generalization of the formulas for intersection numbers of dual polar association schemes and their applications

Jianmin Ma\textsuperscript{a}, Jun Guo\textsuperscript{b,\ast}, Fenggao Li\textsuperscript{c}, Kaishun Wang\textsuperscript{d}

\textsuperscript{a} Oxford College of Emory University, Oxford, GA 30054, USA
\textsuperscript{b} Math. and Inf. College, Langfang Teachers’ College, Langfang 065000, China
\textsuperscript{c} Dept. of Math., Hunan Institute of Science and Technology, Yueyang 414006, China
\textsuperscript{d} Sch. Math. Sci. & Lab. Math. Com. Sys., Beijing Normal University, Beijing 100875, China

A R T I C L E  I N F O

Article history:
Received 18 March 2010
Accepted 4 November 2010
Available online 4 December 2010
Submitted by R.A. Brualdi

AMS classification:
20G40
05E30
20B25
94A62
05C25

Keywords:
Dual polar scheme
Totally isotropic subspace
Pooling design
Cartesian authentication code
Vertex transitive graph

A B S T R A C T

Dual polar association schemes form an important family of association schemes, whose intersection numbers were computed in [Wan et al., Studies in Finite Geometry and the Construction of Incomplete Block Designs, Science Press, Beijing, 1966 (in Chinese)]. In this paper, we generalize the formulas for the intersection numbers, and introduce their applications to pooling designs, Cartesian authentication codes and vertex-transitive graphs.

© 2010 Published by Elsevier Inc.

1. Introduction

In this section we shall introduce the classical spaces, following notation and terminology from Wan’s book [19]. The classical spaces associated with the three types of forms (alternating bilinear, hermitian, and quadratic) are referred to by the same names as the groups associated with them:
symplectic, unitary, and orthogonal respectively. In this paper, we are concerned with those whose underlying vector spaces are of even dimension over a finite field.

Throughout this paper, we denote by $\mathbb{F}_q$ a finite field with $q$ elements and by $\mathbb{F}_q^{2\nu}$ the $2\nu$-dimensional row vector over $\mathbb{F}_q$ for a fixed a positive integer $\nu$. For an $m$-dimensional subspace $P$ in $\mathbb{F}_q^{2\nu}$, we mean by a matrix representation of $P$ an $m \times 2\nu$ matrix whose rows form a basis of $P$, denoted by the same symbol $P$. We shall work with partitioned matrices whose entries are themselves submatrices. For typographical convenience, we sometimes leave blank the zero submatrices. We write $I^{(r)}$ for the identity matrix of size $r$, and we omit $r$ if it is clear from the context. Let

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

The symplectic group of degree $2\nu$ over $\mathbb{F}_q$ with respect to $K$, denoted by $\text{Sp}_{2\nu}(\mathbb{F}_q)$, consists of all $2\nu \times 2\nu$ matrices $T$ over $\mathbb{F}_q$ satisfying $TKT^t = K$, where $T^t$ denotes the transpose of $T$. The space $\mathbb{F}_q^{2\nu}$ together with the right multiplication action of $\text{Sp}_{2\nu}(\mathbb{F}_q)$ is called the $2\nu$-dimensional symplectic space over $\mathbb{F}_q$. An $m$-dimensional subspace $P$ in $\mathbb{F}_q^{2\nu}$ is said to be of type $(m, s)$ if $PKP^t$ is of rank $2s$. In particular, subspaces of type $(m, 0)$ are called $m$-dimensional totally isotropic subspaces and $\nu$-dimensional totally isotropic subspaces are called maximal totally isotropic subspaces.

Let $q = p^2$, where $p$ is a prime power. Then $\mathbb{F}_q$ has an involutive automorphism $a \mapsto \overline{a} = a^p$. Let

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

The unitary group of degree $2\nu$ over $\mathbb{F}_q$, denoted by $\text{U}_{2\nu}(\mathbb{F}_q)$, consists of all $2\nu \times 2\nu$ matrices $T$ over $\mathbb{F}_q$ satisfying $HTH^t = H$. The vector space $\mathbb{F}_q^{2\nu}$ together with the right multiplication action of $\text{U}_{2\nu}(\mathbb{F}_q)$ is called the $2\nu$-dimensional unitary space over $\mathbb{F}_q$. An $m$-dimensional subspace $P$ in $\mathbb{F}_q^{2\nu}$ is said to be of type $(m, r)$ if $PKP^t$ is of rank $r$. Similarly, subspaces of type $(m, 0)$ are called $m$-dimensional totally isotropic subspaces and $\nu$-dimensional totally isotropic subspaces are called maximal totally isotropic subspaces.

It is more involved to define orthogonal spaces. Denote by $\mathcal{K}_{2\nu}$ the set of all $2\nu \times 2\nu$ alternate matrices over $\mathbb{F}_q$. Two $2\nu \times 2\nu$ matrices $A$ and $B$ over $\mathbb{F}_q$ are said to be congruent mod $\mathcal{K}_{2\nu}$, denoted by $A \equiv B \pmod{\mathcal{K}_{2\nu}}$, if $A - B \in \mathcal{K}_{2\nu}$. Clearly, $\equiv$ is an equivalence relation on the set of all $2\nu \times 2\nu$ matrices. Let $[A]$ denote the equivalence class containing $A$. Two matrix classes $[A]$ and $[B]$ are said to be coprime if there is a nonsingular $2\nu \times 2\nu$ matrix $Q$ over $\mathbb{F}_q$ such that $[QAQ^t] \equiv [B]$. Let

$$S_{2\nu} = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}$$

according the $q$ being odd or even, respectively. The orthogonal group of degree $2\nu$ over $\mathbb{F}_q$ with respect to $S_{2\nu}$, denoted by $\text{O}_{2\nu}(\mathbb{F}_q)$, consists of all $2\nu \times 2\nu$ matrices $T$ over $\mathbb{F}_q$ satisfying $[TS_{2\nu}T^t] \equiv [S_{2\nu}]$. The space $\mathbb{F}_q^{2\nu}$ together with the right multiplication action of $\text{O}_{2\nu}(\mathbb{F}_q)$ is called the $2\nu$-dimensional orthogonal space over $\mathbb{F}_q$. For $q$ being odd, let

$$S_{2\nu+\gamma} = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}, \quad \Gamma = \begin{cases} \emptyset, & \text{if } \gamma = 0, \\
(1) \text{ or } (z), & \text{if } \gamma = 1, \\
\text{diag}(1, -z), & \text{if } \gamma = 2, \end{cases}$$
where $z$ is a fixed non-square element of $\mathbb{F}_q$. For $q$ being even, let

$$S_{2s+\gamma}, \Gamma = \begin{pmatrix} 0 & 1^{(s)} \\ 0 & \Gamma \end{pmatrix}, \quad \Gamma = \begin{cases} \emptyset, & \text{if } \gamma = 0, \\
(1), & \text{if } \gamma = 1, \\
(\alpha, 1), & \text{if } \gamma = 2, \end{cases}$$

where $\alpha$ is a fixed element of $\mathbb{F}_q$ such that $\alpha \notin \{x^2 + x \mid x \in \mathbb{F}_q\}$. An $m$-dimensional subspace $P$ is a subspace of type $(m, 2s + \gamma, \alpha, \Gamma)$ if $PS_{2s+\gamma}, P^\Gamma$ is cogredient to $S_{2s+\gamma}$, $G$, $\alpha^{\dim(m-2s-\gamma)}$. If $\Gamma$ is the empty set, we omit the symbol. In particular, subspaces of type $(m, 0, 0)$ are called $m$-dimensional totally isotropic subspaces and $\nu$-dimensional totally isotropic subspaces are called maximal totally isotropic subspaces.

Let $G_2$, be one of the three classical groups acting on $\mathbb{P}^{2\nu}_q$. By [19, Theorems 3.7, 5.8, 6.4 and 7.6], the set of subspaces of the same type in $\mathbb{P}^{2\nu}_q$ forms an orbit under $G_2$. Denote by $\mathcal{M}(m, 0; 2\nu)$ the set of all $m$-dimensional totally isotropic subspaces of $\mathbb{P}^{2\nu}_q$. The action of $G_2$, on $\mathcal{M}(\nu, 0; 2\nu)$ gives rise to a dual polar association scheme (see [1]). Wan et al. [20] computed all intersection numbers of these dual polar schemes. As a generalization of dual polar schemes, we constructed association schemes from singular classical spaces (see [6–9]).

For $1 \leq m \leq \nu$, suppose $P, Q \in \mathcal{M}(\nu, 0; 2\nu)$, $U \in \mathcal{M}(m, 0; 2\nu)$ satisfying $\dim(P \cap Q) = \dim(P \cap U) = i$. Let

$$P^i_j(v, \nu; m) = \{R \in \mathcal{M}(m, 0; 2\nu) \mid \dim(P \cap R) = j, \dim(Q \cap R) = k\},
$$

$$P^i_j(v, m; \nu) = \{R \in \mathcal{M}(\nu, 0; 2\nu) \mid \dim(P \cap R) = j, \dim(U \cap R) = k\}.
$$

Note that the size of $P^i_j(v, \nu; m)$ is an intersection numbers of the dual polar scheme based on $\mathcal{M}(\nu, 0; 2\nu)$.

In this paper, we focus on the sizes of $P^i_j(v, \nu; m)$ and $P^i_j(v, m; \nu)$, and discuss their applications. In Section 2 we calculate the sizes of these two sets. In Section 3 we construct a family of error-correcting pooling designs, and exhibit its disjunct property. We construct a family of Cartesian authentication codes and vertex transitive graphs in Sections 4 or 5, respectively.

2. The cardinalities of $P^i_j(v, \nu; m)$ and $P^i_j(v, m; \nu)$

In this section we shall compute the sizes of $P^i_j(v, \nu; m)$ and $P^i_j(v, m; \nu)$. We begin with some useful lemmas.

**Lemma 2.1** [19, Theorems 3.30, 4.9, 5.31 and 6.37]. Let $S(t, m)$, $\mathcal{H}(t, m)$ and $\mathcal{K}(t, m)$ be the sets of all $m \times m$ symmetric, hermitian and alternate matrices of rank $t$ over $\mathbb{F}_q$, respectively. Then

$$|S(t, m)| = q^{t/2}(t/2 + 1) \prod_{l=t/2+1}^m (q^l - 1)/\left(\prod_{l=1}^{t/2} (q^{l} + 1) \prod_{l=1}^{m-t} (q^{l} - 1)\right),$$

$$|\mathcal{H}(t, m)| = q^{t(t+1)/4} \prod_{i=m-t+1}^m (q^i - 1)/\prod_{i=1}^t (q^{i/2} - (-1)^i),$$

$$|\mathcal{K}(t, m)| = q^{t/2(t-2) - 1} \prod_{l=m-t+1}^m (q^l - 1)/\prod_{l=1}^{t/2} (q^{2l} - 1).$$
Lemma 2.2 [20, Chapter 1, Theorem 5]. The number of \( m \times n \) matrices with rank \( i \) over \( \mathbb{F}_q \) is

\[
N(i; m \times n) = q^{(i-1)/2} \prod_{t=n-i+1}^{n} (q^t - 1),
\]

where \( \left[ \begin{array}{c} m \\ i \end{array} \right]_q = \prod_{t=m-i+1}^{m} (q^t - 1) / \prod_{t=1}^{i} (q^t - 1). \)

Lemma 2.3. Let \( 1 \leq m \leq n \). Then the number of all \( m \times n \) matrices \( (A \ B) \) of rank \( r \) over \( \mathbb{F}_q \), with \( A \) respectively symmetric, hermitian and alternate, is given by

\[
N^s(r; m \times n) = \sum_{t=r - \min(n-m, r)}^{r} q^{(n-m)} N(r-t; (m-t) \times (n-m)) \begin{cases} |S(t, m)|, & \text{in the symmetric case,} \\ |H(t, m)|, & \text{in the hermitian case,} \\ |K(t, m)|, & \text{in the alternate case.} \end{cases}
\]

Proof. For any \( m \times m \) matrix \( A \) of rank \( t \), let \( \mathcal{M}(A) \) denote the set of all \( m \times n \) matrices \( (A \ B) \) of rank \( r \) over \( \mathbb{F}_q \). For each \( (A \ B) \in \mathcal{M}(A) \), there exists a nonsingular \( m \times m \) matrix \( T \) such that

\[
T(A \ B) = (TA \ TB) = \begin{pmatrix} A_1 & B_1 \\ 0 & B_2 \end{pmatrix}^t_{m-t},
\]

and thus we have

\[
\text{rank } B_2 = r - t, \quad |\mathcal{M}(A)| = |\mathcal{M}(TA)|.
\]

By Lemma 2.2,

\[
|\mathcal{M}(A)| = |\mathcal{M}(TA)| = q^{(n-m)} N(r-t; (m-t) \times (n-m)).
\]

Since \( r - \min(n-m, r) \leq r \leq r \), the desired formula follows from Lemma 2.1.

Lemma 2.4. Let \( 1 \leq m \leq v, P_1, P_2 \in A(m, 0; 2v) \) and \( Q_1, Q_2 \in A(m, 0; 2v) \). Then \( \dim(P_1 \cap Q_1) = \dim(P_2 \cap Q_2) \) if and only if there exists a \( T \in G_{2v} \) such that \( P_1 T = P_2, Q_1 T = Q_2 \).

Proof. We illustrate with the symplectic case here. Suppose that \( P_1 \cap Q_1 = D_1, P_2 \cap Q_2 = D_2 \) and \( \dim(P_1 \cap Q_1) = \dim(P_2 \cap Q_2) = i \). Then \( P_1, Q_1, P_2, Q_2 \) have matrix representations of the forms

\[
P_1 = \begin{pmatrix} P_{11} \\ D_1 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} D_1 \\ Q_{11} \end{pmatrix}, \quad P_2 = \begin{pmatrix} P_{21} \\ D_2 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} D_2 \\ Q_{21} \end{pmatrix},
\]

respectively. Since \( \dim(P_1 + Q_1) = v + m - i \), by [19, Theorem 3.6], \( \text{rank } (P_{11}Q_{11}^t) \geq m - i \), which implies that \( \text{rank } (P_{11}Q_{11}^t) = m - i \). Similarly, \( \text{rank } (P_{21}Q_{21}^t) = m - i \). Hence, there exist two \( (v - i) \times (v - i) \) nonsingular matrices \( A_1, A_2 \) and two \( (m - i) \times (m - i) \) nonsingular matrices \( B_1, B_2 \).
such that

\[
\begin{pmatrix}
A_1 P_{11} \\
D_1 \\
B_1 Q_{11}
\end{pmatrix}
K
\begin{pmatrix}
A_1 P_{11} \\
D_1 \\
B_1 Q_{11}
\end{pmatrix}^t
=
\begin{pmatrix}
A_2 P_{21} \\
D_2 \\
B_2 Q_{21}
\end{pmatrix}
K
\begin{pmatrix}
A_2 P_{21} \\
D_2 \\
B_2 Q_{21}
\end{pmatrix}^t
= \begin{pmatrix}
0 & 0 \\
0 & 0 \\
-(I^{(m-i)} & 0)
\end{pmatrix}.
\]

By [19, Theorem 3.11], there exists a \( T \in \text{Sp}_{2v}(\mathbb{F}_q) \) such that \( P_1 T = P_2, Q_1 T = Q_2 \). The converse is obvious. \( \square \)

For \( 1 \leq m \leq v \), suppose that \( P, Q \in \mathcal{M}(v, 0; 2v) \) with \( \dim(P \cap Q) = i \). Recall that \( P_{jk}^i(v, v; m) \) is the set of all \( R \in \mathcal{M}(m, 0; 2v) \) satisfying \( \dim(P \cap R) = j \) and \( \dim(R \cap Q) = k \). By Lemma 2.4, \( P_{jk}^i(v, v; m) = |P_{jk}^i(v, v; m)| \) is independent of any particular choices of \( P \) and \( Q \) with \( \dim(P \cap Q) = i \).

**Theorem 2.5.** Let \( 1 \leq m \leq v \). Then \( P_{jk}^i(v, v; m) = \)

\[
\sum_{\alpha+\gamma \leq v-i, \beta+\rho \leq i, \beta+\gamma = k, \beta \leq \alpha+\gamma, \alpha+\beta = m} q^{(\alpha+\gamma)(i-\beta-\rho)+\rho(2v-i-m)} \begin{pmatrix} v-i & i \\ \alpha & \beta \end{pmatrix}^t \begin{pmatrix} v-i-\alpha & i-\beta \\ \rho & q \end{pmatrix}^t \times N_q^i(\alpha+\beta-j; \alpha \times (v-i-\gamma))
\]

\[
\begin{cases}
q^{\rho(\rho+1)/2}, & \text{the symplectic case}, \\
q^{\rho^2/2}, & \text{the unitary case}, \\
q^{\rho(\rho-1)/2}, & \text{the orthogonal case}.
\end{cases}
\]

**Proof.** By Lemma 2.4, we may take

\[
P = (I^{(v)} 0^{(v)}), \quad Q = (0^{(0,v-i)} I^{(v)} 0^{(v,i)}).
\]

For any \( R \in P_{jk}^i(v, v; m) \), write \( R \) in block form

\[
R = \begin{pmatrix}
R_1 & R_2 & R_3 & R_4
\end{pmatrix}.
\]

Suppose that \( \text{rank } R_4 = \rho, \text{rank } (R_1 R_4) = \rho + \alpha, \text{rank } (R_1 R_3 R_4) = \rho + \alpha + \gamma \) and \( \beta = m - (\rho + \alpha + \gamma) \). By suitable row elementary transformations, \( R \) may be reduced to the form

\[
\begin{pmatrix}
v-i & i & v-i & i \\
R_{11} & R_{12} & R_{13} & 0 \\
0 & R_{22} & 0 & 0 \\
0 & R_{32} & R_{33} & 0 \\
R_{41} & R_{42} & R_{43} & R_{44}
\end{pmatrix}
\]

\[
\begin{pmatrix}
\alpha \\
\beta \\
\gamma \\
\rho
\end{pmatrix},
\]

where \( \text{rank } R_{44} = \rho, \text{rank } R_{11} = \alpha, \text{rank } R_{33} = \gamma \) and \( \text{rank } R_{22} = \beta \). Note that there are \( \begin{pmatrix} v-i \\ \alpha \end{pmatrix} \) choices for subspace \( R_{11} \) and \( \begin{pmatrix} i \\ \beta \end{pmatrix} \) choices for \( R_{22} \). By the transitivity of \( G_{2v} \) on the set of subspaces with
the same type, the number of \( R \) does not depend on any particular choices for \( R_{11} \) and \( R_{22} \). Without loss of generality we may take

\[
R_{11} = (I^{(\alpha)} 0), \quad R_{22} = (I^{(\beta)} 0).
\]

Then \( R \) has a matrix representation of the form

\[
\begin{pmatrix}
\alpha & v-\alpha & \beta & i-\beta \\
\beta & i-\alpha & \alpha & v-\alpha \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

(1)

Since \( R \) is totally isotropic, we have \( R_{331} = 0 \) and \( R_{441} = 0 \). So rank \( R_{332} = \gamma \), rank \( R_{442} = \rho \) and \( \gamma \leq v-\alpha, \rho \leq i-\beta \). Note that there are \([v-\alpha-\gamma \gamma \rho q] \) choices for subspace \( R_{332} \) and \([i-\beta \rho q] \) choices for \( R_{442} \). Similarly, the number of \( R \) does not depend on any particular choices for \( R_{332} \) and \( R_{442} \). Without loss of generality we may take

\[
R_{332} = (I^{(\gamma)} 0), \quad R_{442} = (I^{(\rho)} 0).
\]

Then \( R \) must have the following unique matrix representation

\[
\begin{pmatrix}
\alpha & \gamma & v-\alpha-\gamma & \beta & i-\beta & \alpha & v-\alpha-\gamma & \beta & i-\beta-ho \\
\beta & \gamma & i-\alpha & \alpha & v-\alpha & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\]

(2)

For the symplectic case,

\[
R_{131}^{t} = R_{131}, \quad R_{132}^{t} R_{412}^{t} = R_{431}^{t} + R_{1221}
\]

(3)

for the unitary case,

\[
R_{131} + \tilde{R}_{131}^{t} = 0, \quad R_{132}^{t} \tilde{R}_{4122}^{t} + \tilde{R}_{431}^{t} + R_{1221} = 0,
\]

(4)

for the odd orthogonal case (i.e., the base field \( \mathbb{F}_q \) is of odd characteristic),

\[
R_{131} + R_{131}^{t} = 0, \quad R_{132}^{t} \tilde{R}_{4122}^{t} + R_{431}^{t} + R_{1221} = 0.
\]

(5)

for the even orthogonal case,

\[
R_{131} = 0, \quad R_{132} \tilde{R}_{4122}^{t} + \tilde{R}_{431} + R_{1221} = 0,
\]

(6)

From \( \dim(P \cap R) = j \) and \( \dim(Q \cap R) = k \) we deduce that \( j \leq \alpha + \beta, \beta + \gamma = k \) and rank \( (R_{131} R_{1322}) = \alpha + \beta - j \). By Lemma 2.3 and (3)–(6), the number of matrices \( (R_{131} R_{1322}) \) of rank \( \alpha + \beta - j \) is
\[ N_\alpha^*(\alpha + \beta - j; \alpha \times (v - i - \gamma)). \]

Once \( R_{131}, R_{1322}, R_{4121}, R_{431} \) and \( R_{4121} \) are fixed, the matrices \( R_{1221} \) and \( R_{3221} \) are uniquely determined; and there are

\[ q^{(\rho+1)/2}, q^{\rho^2/2}, q^{\rho(\rho-1)/2}, q^{\rho(\rho-1)/2} \]

choices for \( R_{4221} \) such that (3), (4), (5) and (6) hold, respectively. Since \( R_{1222}, R_{3222} \) and \( R_{4222} \) may be any \( \alpha \times (i - \beta - \rho), \gamma \times (i - \beta - \rho) \) and \( \rho \times (i - \beta - \rho) \) matrices over \( \mathbb{F}_q \), respectively, there are \( q^{(i-\beta-\rho)(\alpha+\gamma+\rho)} \) choices for \( R_{1222}, R_{3222} \) and \( R_{4222} \). Therefore, the number of subspaces of the form (2) is

\[ q^{(\alpha+\gamma)(i-\beta-\rho)+\rho(2v-i-m)} N_\alpha^*(\alpha + \beta - j; \alpha \times (v - i - \gamma)) \]

\[ \begin{cases} q^{\rho(\rho+1)/2}, & \text{the symplectic case,} \\ q^{\rho^2/2}, & \text{the unitary case,} \\ q^{\rho(\rho-1)/2}, & \text{the orthogonal case.} \end{cases} \]

Hence the desired assertion follows. \( \square \)

**Corollary 2.6.** Let \( 1 \leq m \leq v \). Then

\[ p_{i j}^v(v, v; m) = q^{(m-j)(v-m)} \begin{bmatrix} v \\ j \end{bmatrix}_q \begin{bmatrix} v - j \\ m - j \end{bmatrix}_q \begin{cases} q^{(m-j)(m-j+1)/2}, & \text{the symplectic case,} \\ q^{(m-j)^2/2}, & \text{the unitary case,} \\ q^{(m-j)(m-j-1)/2}, & \text{the orthogonal case.} \end{cases} \]

For \( 1 \leq m \leq v \), let \( P \in \mathcal{M}(v, 0; 2v), U \in \mathcal{M}(m, 0; 2v) \) with \( \dim(P \cup U) = i \). Recall that \( p_{i j}^v(v, m; v) \) consists of \( R \in \mathcal{M}(v, 0; 2v) \) with \( \dim(P \cap R) = j \) and \( \dim(U \cap R) = k \). By Lemma 2.4, \( p_{i j}^v(v, m; v) = |p_{i j}^v(v, m; v)| \) is independent of any particular choice for \( P \) and \( U \) with \( \dim(P \cap U) = i \).

**Corollary 2.7.** We have \( p_{i j}^v(v, m; v) = p_{i k}^v(v, v; m) \cdot p_{i j}^v(v, v; v) / p_{i j}^v(v, v; m) \).

**Proof.** Let

\[ M = \{(P, Q, R) \mid P, R \in \mathcal{M}(v, 0; 2v), Q \in \mathcal{M}(m, 0; 2v), \dim(P \cap Q) = i, \dim(P \cap R) = j, \dim(Q \cap R) = k \} \].

We count \( M \) in two different ways. For a fixed subspace \( P \in \mathcal{M}(v, 0; 2v) \), by Corollary 2.6, there are \( p_{i j}^v(v, v; m) \) subspaces \( Q \in \mathcal{M}(m, 0; 2v) \) satisfying \( \dim(P \cap Q) = i \). For two fixed subspaces \( P \in \mathcal{M}(v, 0; 2v), Q \in \mathcal{M}(m, 0; 2v) \) with \( \dim(P \cap Q) = i \), there are \( p_{i j}^v(v, m; v) \) subspaces \( R \in \mathcal{M}(v, 0; 2v) \) satisfying \( \dim(P \cap R) = j \) and \( \dim(Q \cap R) = k \). It follows that

\[ |M| = p_{i j}^v(v, m; v) \cdot p_{i j}^v(v, v; m) \cdot N(v, 0; 2v). \]

For a fixed subspace \( P \in \mathcal{M}(v, 0; 2v) \), by Corollary 2.6 again, there are \( p_{i j}^v(v, v; v) \) subspaces \( R \in \mathcal{M}(v, 0; 2v) \) satisfying \( \dim(P \cap R) = j \). For two fixed maximal totally isotropic subspaces \( P, R \) with \( \dim(P \cap R) = j \), there are \( p_{i k}^v(v, m; m) \) subspaces \( Q \in \mathcal{M}(m, 0; 2v) \) satisfying \( \dim(P \cap Q) = i \) and \( \dim(R \cap Q) = k \). By Theorem 2.5,

\[ |M| = p_{i j}^v(v, v; v) \cdot p_{i j}^v(v, v; v) \cdot N(v, 0; 2v). \]

Hence the desired assertion follows. \( \square \)
**Remark.** The action of $G_{2r}$ on $\mathcal{M}(m, 0; 2v) \cup \mathcal{M}(v, 0; 2v)$ defines a coherent configuration (see [10] for coherent configurations). The parameters $p_{jk}^v(v, v; m)$ and $p_{jj}^v(v, m; v)$ are intersection numbers of this configuration.

### 3. Pooling designs

A binary matrix is $d^e$-disjunct if for any column $C$ and any $d$ others columns, there exist at least $e$ rows such that each of them has value 1 at column $C$ and value 0 at all the other $d$ columns. A $d^1$-disjunct matrix is also called $d$-disjunct. $d^e$-disjunct matrices form the basis for error-tolerant nonadaptive group testing algorithms. These algorithms have applications in many areas such as DNA library screening [2]. There are several constructions of $d^e$-disjunct matrices in the literatures [3,5,12,14–16].

In this section, as an application of the theorems in Section 2, we shall construct a family of $d^e$-disjunct matrices and discuss their disjunct property.

For $1 \leq m < v$ and $0 \leq j \leq m$, let $M$ be the matrix with rows and columns respectively indexed by $\mathcal{M}(m, 0; 2v)$ and $\mathcal{M}(v, 0; 2v)$ in which $M(P, Q) = 1$ if $\dim(P \cap Q) = j$ and 0 otherwise.

**Lemma 3.1** [19, Corollaries 3.19, 5.20, 6.23 and 7.25]. Let $1 \leq m \leq v$. Then the number of $m$-dimensional totally isotropic subspaces in $\mathbb{F}_q^{2v}$ is

$$N(m, 0; 2v) = \begin{cases} \prod_{i=v-m+1}^{v} (q^{2i} - 1) / \prod_{i=1}^{m} (q^i - 1), & \text{the symplectic case,} \\ \prod_{i=v-m+1}^{v} (q^{i-1} - 1)(q^{i-1/2} + 1) / \prod_{i=1}^{m} (q^i - 1), & \text{the unitary case,} \\ \prod_{i=v-m+1}^{v} (q^{i-1} - 1)(q^{i-1} + 1) / \prod_{i=1}^{m} (q^i - 1), & \text{the orthogonal case.} \end{cases}$$

**Lemma 3.2.** Let $1 \leq m \leq v$ and $P \in \mathcal{M}(m, 0; 2v)$. Then the number of subspaces $Q \in \mathcal{M}(v, 0; 2v)$ with $\dim(P \cap Q) = j$ is $N(v, 0; 2v)p_{jj}^v(v, v; m)/N(m, 0; 2v)$.

**Proof.** Let \[ \mathcal{M} = \{(P, Q) \mid P \in \mathcal{M}(m, 0; 2v), Q \in \mathcal{M}(v, 0; 2v), \dim(P \cap Q) = j\}. \]

Now we count $\mathcal{M}$ in two different ways. For a fixed subspace $P$ of type $(m, 0)$, suppose that there are $\alpha$ maximal totally isotropic subspaces $Q$ satisfying $\dim(P \cap Q) = j$. By Lemma 3.1

$$|\mathcal{M}| = \alpha \cdot N(m, 0; 2v).$$

For a fixed maximal totally isotropic subspace $Q$, there are $p_{jj}^v(v, v; m)$ subspaces $P$ satisfying $\dim(P \cap Q) = j$. By Lemma 3.1 and Corollary 2.6,

$$|\mathcal{M}| = p_{jj}^v(v, v; m)N(v, 0; 2v).$$

Hence $\alpha = N(v, 0; 2v)p_{jj}^v(v, v; m)/N(m, 0; 2v)$, as desired. \( \square \)

By Lemmas 3.1, 3.2 and Corollary 2.6, $M$ is an $N(m, 0; 2v) \times N(v, 0; 2v)$ matrix, which has constant row weight $N(v, 0; 2v)p_{jj}^v(v, v; m)/N(m, 0; 2v)$ and constant column weight $p_{jj}^v(v, v; m)$.

**Theorem 3.3.** Let $1 \leq m < v$ and $0 \leq j \leq m$. If $1 \leq d \leq \lfloor p_{jj}^v(v, v; m)/\alpha \rfloor + 1$, then $M$ is $d^e$-disjunct, where $e = p_{jj}^v(v, v; m) - d\alpha$, $\alpha = \max\{p_{jj}^v(v, v; m) \mid 0 \leq l \leq v - 1\}$. 

Proof. Pick any \( d + 1 \) distinct columns \( C, C_1, C_2, \ldots, C_d \) of \( M \). By Theorem 2.5, we may assume that the number of subspaces \( P \in \mathcal{M}(m, 0; 2v) \) satisfying \( \dim(P \cap C) = j \) and \( \dim(P \cap C_i) = j \) is at most

\[
\alpha = \max\{p_{jj}(v, v; m) | 0 \leq l \leq v - 1\}.
\]

Hence the number of subspaces \( P \) of \( \mathcal{M}(m, 0; 2v) \) satisfying \( \dim(P \cap C) = j \) and \( \dim(P \cap C_1), \ldots, \dim(P \cap C_d) \neq j \) is at least

\[
e = p_{jj}(v, v; m) - d\alpha,
\]

from which follows that \( M \) is \( d^e \)-disjunct. Since \( e \geq 1 \), we obtain

\[
d \leq \left\lfloor \frac{p_{jj}(v, v; m)}{\alpha} \right\rfloor + 1,
\]

as desired. \( \Box \)

Remark. If \( j = m \), the disjunct matrices in Theorem 3.3 are the disjunct matrices based on pooling spaces in [11, Example 4.2].

4. Authentication codes

Authentication codes were invented in 1974 by Gilbert et al. [4] for protecting the integrity of information. For a survey of authentication codes, we recommend Simmons [17]. In 1992, Wan [18] constructed Cartesian authentication codes from the unitary space.

In this section we shall construct a family of authentication codes, following notation and terminology in [18]. As a by-product, we obtain some enumeration formulas in \( 2v \)-dimensional classical spaces.

Theorem 4.1. Let \( \mathbb{P}^{2v} \) be a \( 2v \)-dimensional classical spaces. Suppose that \( 2 \leq i \leq v - 1 \) and \( P_0 = (I^{(v)} 0^{(v)}) \). Define the source states to be all subspaces of dimension \( i \) contained in \( P_0 \), the encoding rules to be the maximal totally isotropic subspaces intersecting \( P_0 \) at \( \{0\} \), and the messages to be the subspaces of type \( \vartheta \) intersecting \( P_0 \) at \( i \)-dimensional subspaces, where \( \vartheta = (v + i, i), (v + i, 2i) \) or \( (v + i, 2i, i) \) according to the symplectic, unitary or orthogonal case, respectively. Denote the set of source states, the set of encoding rules, and the set of messages by \( S, E \) and \( \mathcal{M} \), respectively. Given any \( P \in S \) and any \( P_1 \in E \), \( P + P_1 \) is a message into which the source state \( P \) is encoded under the encoding rule \( P_1 \). The above construction yields a Cartesian authentication code, whose parameters are

\[
|S| = \begin{bmatrix} v \\ i \end{bmatrix}_q,
\]

\[
|E| = \begin{cases} q^{v(v+1)/2}, \text{ the symplectic case,} \\ q^{v^2/2}, \text{ the unitary case,} \\ q^{v(v-1)/2}, \text{ the orthogonal case,} \end{cases}
\]

\[
|M| = \begin{cases} q^{(v-i)(v+i+1)/2} \begin{bmatrix} v \\ i \end{bmatrix}_q, \text{ the symplectic case,} \\ q^{(v-i)(v+i)/2} \begin{bmatrix} v \\ i \end{bmatrix}_q, \text{ the unitary case,} \\ q^{(v-i)(v+i-1)/2} \begin{bmatrix} v \\ i \end{bmatrix}_q, \text{ the orthogonal case.} \end{cases}
\]
Suppose that the encoding rule is chosen according to a uniform probability distribution, and denote the probabilities of a successful impersonation attack and a successful substitution attack by $P_I$ and $P_S$, respectively. Then

$$P_I = \begin{cases} 
\frac{1}{q^{(\nu-i)(\nu+i+1)/2}}, & \text{the symplectic case,} 
\frac{1}{q^{(\nu-i)(\nu+i)/2}}, & \text{the unitary case,} 
\frac{1}{q^{(\nu-i)(\nu+i-1)/2}}, & \text{the orthogonal case,} 
\end{cases}$$

and $P_I$ is optimal.

**Proof.** Let $P$ be a source state and $P_1$ be an encoding rule. Since $P \subseteq P_0$ and $P_0 \cap P_1 = \{0\}$, $P + P_1$ is of type $\vartheta$. By

$$\dim((P + P_1) \cap P_0) = \dim(P + P_1) + \dim P_0 - \dim((P + P_1) + P_0) = i,$$

we have $(P + P_1) \cap P_0 = P$. It follows that $P + P_1$ is a message. So $P_1$ defines a map $f : S \mapsto \mathcal{M}$ by $f(P) = P + P_1$.

Next, let $Q$ be a message such that $P = P_0 \cap Q$. Then $P$ is a source state. We may take

$$Q = \begin{pmatrix} v & v \\ B & 0 \\ A & I \end{pmatrix}, \quad \text{where } P = (B \ 0).$$

Since rank $B = i$, that there exists a $v \times v$ nonsingular matrix $T_1$ such that $BT_1 = (I(I_0 \ 0^{(i,v-i)}))$. Let $T = \text{diag}(T_1, S_1^{-1}) \in G_{2v}$, where $S_1 = T_1^T, \overline{T}_1$ or $T_1^T$ according to the symplectic, unitary or orthogonal case, respectively, such that $P_0T = P_0$ and

$$QT = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & A_1 & I & 0 \\ 0 & A_2 & 0 & I \end{pmatrix}_{v-i}.$$ 

Since $QT$ is of type $\vartheta$, we have $A_2 - A_2^T = 0, A_2 + \overline{A}_2 = 0$ or $A_2 + A_2^T = 0$ according to the symplectic, unitary or orthogonal case, respectively. Take

$$P_1T^{-1} = \begin{pmatrix} I & 0 & 0 \\ 0 & A_1 & I \\ B_1 & A_2 & 0 \end{pmatrix}_{v-i}.$$ 

where $B_1 = A_1^T, -A_1^T$ or $-A_1^T$ according to the symplectic, unitary or orthogonal case, respectively. Then $P_1 \in \mathcal{E}$ satisfying $P + P_1 = Q$. Therefore, $f$ is a surjective map.
Suppose that there is another source state $P'$ encoded into the message $Q$. Then $P' \subseteq P_0$ and $P' \subseteq Q$; and so $P' \subseteq P_0 \cap Q = P$, which implies that $P = P'$. Hence the source state $P$ is uniquely determined by $Q$.

Clearly, $|S| = \begin{bmatrix} v \\ q \end{bmatrix}$. By Corollary 2.6, $|E| = p^{v_0}_0(v, v; v)$. Let $Q$ be a message. Without loss of generality, we may take

$$Q = \begin{pmatrix} I^{(i)} & 0^{(i, v-i)} & Q^{(i, v)} \\ 0 & 0 & I^{(v)} \end{pmatrix}.$$  

Then the encoding rules contained in $Q$ have a matrix representations of the form

$$\begin{pmatrix} A_1 & 0^{(v, v-i)} & I^{(i)} \\ A_2 & 0 & I^{(v-i)} \end{pmatrix}. \tag{7}$$

The subspaces of the form (7) are totally isotropic, so $A_2 = 0$ and $A_1 - A_1' = 0, A_1 + A_1' = 0$ or $A_2 + A_2' = 0$ according to the symplectic, unitary or orthogonal case, respectively. Hence, the number of encoding rules contained in $Q$ is $\alpha = q^{i+(i+1)/2}, q^{2i/2}$ or $q^{i-(i-1)/2}$ according to the symplectic, unitary or orthogonal case, respectively. So $|M| = |S| \cdot |E|/\alpha$.

Let $Q$, $Q'$ be two distinct messages containing a common encoding rule $P_1$, and let $P$, $P'$ be the unique source states contained in them, respectively. Then $P = Q \cap P_0$, $P' = Q' \cap P_0$ and

$$Q = P \oplus P_1, \quad Q' = P' \oplus P_1,$$

where $X \oplus Y$ denotes the direct sum of $X$ and $Y$.

We claim that $Q \cap Q' = (P \cap P') \oplus P_1$. For any $w \in Q \cap Q'$, we have $w = w + z_1 = x' + z_2$, where $x \in P, x' \in P'$ and $z_1, z_2 \in P_1$. Since $P + P' \subseteq P_0$, $x - x' = z_2 - z_1 \in P_0 \cap P_1$, which implies $z_1 = z_2$ and $x = x'$. Then $w \in (P \cap P') \oplus P_1$, and we prove the claim.

Let $d(P \cap P') = r$. Since $Q \neq Q'$, we have $\max\{2i - m, 0\} \leq r \leq i - 1$. We assert that the set of encoding rules contained in both $Q$ and $Q'$ coincides with the set of maximal totally isotropic subspaces $P_1$ contained in $Q \cap Q'$ such that $P_1 \cap (P \cap P') = \{0\}$. Indeed, let $P_1$ be the maximal totally isotropic subspace contained in $Q \cap Q'$ such that $P_1 \cap (P \cap P') = \{0\}$. Then

$$P_1 \cap P_0 \subseteq Q \cap Q' \cap P_0 \subseteq Q \cap P_0, \quad Q' \cap P_0.$$

Therefore, $P_1 \cap P_0 \subseteq P_1 \cap (P \cap P') = \{0\}$, which implies that $P_1$ is an encoding rule contained in both $Q$ and $Q'$. Conversely, let $P_1$ be an encoding rule contained in both $Q$ and $Q'$, that is, $P_1$ is a maximal totally isotropic subspace contained in both $Q$ and $Q'$ such that $P_1 \cap P = \{0\}$ and $P_1 \cap P' = \{0\}$. Then $P_1$ is a maximal totally isotropic subspace contained in $Q \cap Q'$ such that $P_1 \cap (P \cap P') = \{0\}$, and we prove the above assertion.

Hence the number of encoding rules contained in $Q$ and $Q'$ is $q^{r(r+1)/2}, q^{r/2}$ or $q^{r(r-1)/2}$ according to the symplectic, unitary or orthogonal case, respectively. Since $\max\{2i - m, 0\} \leq r \leq i - 1$, we obtain $P_1$ and $P_3$. It is obvious that $P_1$ is optimal. \(\square\)

**Corollary 4.2.** Let $\mathbb{F}_q^{2v}$ be a $2v$-dimensional classical space. Let $0 \leq i \leq v$ and $P_0$ be a fixed maximal totally isotropic subspace of $\mathbb{F}_q^{2v}$. Then the number of subspaces $Q$ of type $\mathfrak{g}$ satisfying $\dim(P_0 \cap Q) = i$ is

$$n_i(v; \mathfrak{g}) = \begin{cases} q^{(v-i)(v+i+1)/2} \begin{bmatrix} v \\ i \end{bmatrix}_q, & \text{the symplectic case,} \\
q^{(v-i)(v+i)/2} \begin{bmatrix} v \\ i \end{bmatrix}_q, & \text{the unitary case,} \\
q^{(v-i)(v+i-1)/2} \begin{bmatrix} v \\ i \end{bmatrix}_q, & \text{the orthogonal case,} \end{cases}$$
where \( \vartheta = (v + i, i) \), \((v + i, 2i)\) or \((v + i, 2i, i)\) according to the symplectic, unitary or orthogonal case, respectively.

**Corollary 4.3.** For \( 0 \leq i \leq v \), let \( Q_0 \) be a fixed subspace of type \( \vartheta \) in \( \mathbb{P}^2_{q,v} \), where \( \vartheta = (v + i, i) \), \((v + i, 2i)\) or \((v + i, 2i, i)\) according to the symplectic, unitary or orthogonal case, respectively. Then the number of maximal totally isotropic subspaces \( P \) satisfying \( \dim(P \cap Q_0) = i \) is

\[
N_i(v; \vartheta)N(v, 0; 2v) \frac{N(\vartheta; 2v)}{N(\vartheta; 2v)}
\]

where \( N(\vartheta; 2v) \) is the number of subspaces of \( \mathbb{P}^2_{q,v} \) of type \( \vartheta \) (see [19]).

**Proof.** The proof is similar to that of Lemma 3.2, and thus omitted. \( \square \)

## 5. Graphs

In this section we shall construct a family of vertex transitive graphs.

For \( 0 \leq i \leq m \leq v \), suppose that \( W_0 \) is a fixed \( m \)-dimensional totally isotropic subspace in \( \mathbb{P}^2_{q,v} \). Let \( X^{(i)} \) be the set of all the maximal totally isotropic subspaces \( P \) of \( \mathbb{P}^2_{q,v} \) satisfying \( \dim(P \cap W_0) = i \).

Define a graph \( \Gamma \) whose vertex set is the set \( X^{(i)} \), and two vertices \( P \) and \( Q \) are adjacent if and only if \( \dim(P \cap Q) = v - 1 \). Then \( \Gamma \) is a subgraph of the dual polar graph \( \Delta \) based on \( M(v, 0; 2v) \). If \( m = v \), then \( \Gamma \) is the \((v - i)\)-th subconstituent of \( \Delta \) (see [13, 21, 22]).

The stabilizer \( G_{2v}(W_0) \) of \( W_0 \) in \( G_{2v} \) is an automorphism group of \( \Gamma \), by Lemma 2.4 and Corollary 2.7. \( \Gamma \) is a vertex transitive graph of degree \( p^{n}_{v - 1,i}(v, m; v) \). Lemma 3.2 implies that \( \Gamma \) has \( N(v, 0; 2v)p^{n}_{v - 1,i}(v, v; m)/N(m, 0; 2v) \) vertices.

Let \( G_{2v}(W_0) \) act on the set \( X^{(i)} \times X^{(i)} \) in a natural way as

\[
(P, Q)T = (PT, QT), \quad \forall P, Q \in X^{(i)}, \quad \forall T \in G_{2v}(W_0).
\]

Let \( A_0, A_1, \ldots, A_t \) be the orbits of this action. Since \( G_{2v}(W_0) \) acts transitively on \( X^{(i)} \), the configuration \( (X^{(i)}, \{A_j\}_{0 \leq j \leq t}) \) forms a symmetric association scheme (see [1]). We will study these association schemes in a separate paper.

### Acknowledgment

We would like thank the referees for their valuable suggestions. This research is supported by NCET-08-0052, NSF of China (10971052, 10871027), Hunan Provincial Natural Science Foundation of China (09JJ3006), and the Fundamental Research Funds for the Central Universities of China.

### References