Linear Algebra and its Applications 438 (2013) 549–558

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Association schemes based on singular symplectic geometry over finite fields and its application

You Gao *, Yifan He

College of Science, Civil Aviation University of China, Tianjin 300300, PR China

ARTICLE INFO

Article history:
Received 30 May 2012
Accepted 18 July 2012
Available online 1 September 2012

Submitted by R.A. Brualdi

Keywords:
Association scheme
Singular symplectic geometry
Authentication code

ABSTRACT

The paper provides the construction of association scheme on the subspaces of type$(\nu+k, 0, k)$ in singular symplectic geometry over finite fields. All intersection numbers of the scheme are computed. At last, an authentication code with perfect secrecy from the association scheme is construction.

1. Introduction

In this section, we shall introduce the concepts of singular symplectic geometry over finite fields, association scheme, and then introduce our main result. Notation and terminology will be adopted from [1,2]. We always assume that

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

and

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

[*] Corresponding author.
E-mail address: gao_you@263.net (Y. Gao).

0024-3795/$ - see front matter © 2012 Published by Elsevier Inc.
http://dx.doi.org/10.1016/j.laa.2012.07.030

where K_l is $(2\nu + l) \times (2\nu + l)$ alternate matrix, and K is $2\nu \times 2\nu$ alternate matrix. Let P be an m-dimensional vector subspace of $\mathbb{F}_q^{(n)}$, then we write dim P= m. Let $v_1, v_2, \ldots, v_m$ be a basis of P. We notice that $v_1, v_2, \ldots, v_m$ are vectors in $\mathbb{F}_q^{(n)}$. We usually use the $m \times n$ matrix

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

to represent the vector subspace spanned by the vectors $v_1, v_2, \ldots, v_m$, write

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

Denote the number of $m \times n$ matrices of rank r over $\mathbb{F}_q$ by $N(r, m \times n)$.

Singular symplectic geometry over finite fields is introduced in [1]. Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime, $n = 2\nu + l$. The set of all $(2\nu + l) \times (2\nu + l)$ nonsingular matrices T over $\mathbb{F}_q$ satisfying $TK_lT = K_l$ forms a group, called the singular symplectic group of degree $2\nu + l$ and index ν over $\mathbb{F}_q$, denoted by $Sp_{2\nu+l,\nu}(\mathbb{F}_q)$. We have an action of $Sp_{2\nu+l,\nu}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(2\nu+l)}$ defined as follows:

$$\mathbb{F}_q^{(2\nu+l)} \times Sp_{2\nu+l,\nu}(\mathbb{F}_q) \to \mathbb{F}_q^{(2\nu+l)}$$

$$((x_1 \cdots, x_\nu \cdots, x_{2\nu+l}), T) \mapsto (x_1 \cdots, x_\nu \cdots, x_{2\nu+l})T$$

The the vector space $\mathbb{F}_q^{(2\nu+l)}$ together with the above action of the group $S_{P_{2\nu+l,\nu}}(\mathbb{F}_q)$ is called the $2\nu + l$-dimensional singular symplectic space over $\mathbb{F}_q$.

Let $e_i (1 \leqslant i \leqslant 2\nu + l)$ be the row vector in $\mathbb{F}_q^{(2\nu+l)}$ whose i-th coordinate is 1 and all other coordinates are 0. Denote by E the l-dimensional subspace of $\mathbb{F}_q^{(2\nu+l)}$ generated by $e_{2\nu+1}, e_{2\nu+2}, \ldots, e_{2\nu+l}$. An m-dimensional subspace P of $\mathbb{F}_q^{(2\nu+l)}$ is called a subspace of type(m, s, k) if

(i) PK_lP^t is cogredient to $M(m, s)$, and
(ii) $\dim(P \cap E) = k$, where

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