Iranian Journal of Mathematical Sciences and Informatics
Vol. 14, No. 1 (2019), pp 21-34
DOI: 10.7508/ijmsi.2019.01.003

Isotropic Constant Dimension Subspace Codes

Fatemeh Bardestani [*,a] and S. Roghayeh Adhami [b]

[a] Mathematics and Informatics Research Group, ACECR at Tarbiat Modares University, B.O. Box: 14115-343, Tehran, Iran.
[b] Department of Mathematics, Faculty of Mathematical Sciences, Tarbiat Modares University, P.O.Box:14115-137,Tehran,Iran.

E-mail: fatemeh.bardestani@modares.ac.ir
E-mail: r.adhamy@gmail.com

Abstract. In network code setting, a constant dimension subspace code is a set of k-dimensional subspaces of $\mathbb{F}_q^n$. If $\mathbb{F}_q^n$ is a nondegenerate symplectic vector space with bilinear form f, an isotropic subspace $\mathcal{U}$ of $\mathbb{F}_q^n$ is a subspace for which $\mathcal{U} \subset \mathcal{U}^\perp$. We introduce isotropic subspace codes simply as a set of isotropic subspaces and show how the property of being isotropic is used in decoding process, then we demonstrate the structure of an isotropic spread code.

Keywords: Constant dimension subspace code, Isotropic subspace, Spread codes, Symplectic space.

2000 Mathematics subject classification: 20D20, 11T71.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and V be a vector space of dimension n over $\mathbb{F}_q$. The set of all subspaces of V is called projective space denoted by $\mathrm{PG}(n-1,q)$. A subspace code is defined simply as a subset of $\mathrm{PG}(n-1,q)$. The natural measure in $\mathrm{PG}(n-1,q)$ which is called subspace distance is a

*Corresponding Author

Received 06 February 2016; Accepted 25 January 2017
©2019 Academic Center for Education, Culture and Research TMU

[Downloaded from ijmsi.com on 2024-04-24]

metric on $\mathrm{PG}(n-1,q)$ and is given by

$$d_s(\mathcal{U},\mathcal{W}) = \dim(\mathcal{U}) + \dim(\mathcal{W}) - 2\dim(\mathcal{U}\cap\mathcal{W}),$$

for every $\mathcal{U},\mathcal{W} \in \mathrm{PG}(n-1,q)$.
The minimum distance $d_s(C)$ of a subspace code $C \subset \mathrm{PG}(n-1,q)$ is defined as:

$$d_s(C) = min\{d_s(\mathcal{U},\mathcal{W}) \mid \mathcal{U},\mathcal{W} \in C, \mathcal{U} \neq \mathcal{W}\}.$$

For every $0 \leq k \leq n$, the set of all $k-$dimensional subspaces of $\mathbb{F}_q^n$ is called Grassmannian denoted by $\mathcal{G}(k,n)$. Constant dimension subspace codes, which are defined as subsets of $\mathcal{G}(k,n)$, build up a subclass of subspace codes.

In 2008 Koetter and Kschischang in [9] demonstrated the application of subspace codes in random network coding to correct errors and erasures. This application of subspace codes leads a lot of research and interest to a wide variety of problems related to vector space and subspace codes (e.g. [4], [10] and [13]).

Trautmann et al. in [14] used the natural right action of a subgroup G of the general linear group $\mathrm{GL}_n(q)$ on Grassmannian $\mathcal{G}(k,n)$ and introduced a subclass of constant dimension codes called orbit codes. Particularly if G is a cyclic subgroup of $\mathrm{GL}_n(q)$, then related orbits are called cyclic orbit codes [14].

Spread codes are a class of constant dimension codes. These codes have maximal minimum distance and are optimal in the sense that they achieve the Singleton-like bound on the cardinality of network codes. For all parameters n,k which $k|n$, there exists a Spread code by an orbit structure [14].

Let V be a symplectic space with symplectic form f. A subspace $\mathcal{U}$ of V where $\mathcal{U} \subset \mathcal{U}^{\perp}$ is called an isotropic subspace. If $\mathcal{U} = \mathcal{U}^{\perp}$, subspace is called totally isotropic. If there exists a spread of totally isotropic subspaces, it is called symplectic spread. There exist a rich literature in the context of symplectic spreads (e.g. [1],[8]).

This paper focuses on symplectic vector space V which is endowed with a symplectic bilinear form f. We use isotropic subspaces to construct subspace codes and we show the properties of these codes.

In the next section we recall some preliminaries and definitions. In the third section we define the concept of isotropic subspace codes, and consider their decoding process. In the fourth section, We demonstrate the structure of an isotropic spread code.

Finally we conclude with the summary of the results of this paper and give some suggestions for further research.

[Downloaded from ijmsi.com on 2024-04-24]

2. Notation and Preliminaries

Let V be a vector space of dimension $2n$ over $\mathbb{F}_q$ and

$$f : V \times V \to \mathbb{F}_q$$

be a bilinear form on V such that for every $x \in V$, $f(x,x) = 0$, then f is called a symplectic form and V is called a symplectic vector space. To every symplectic form f and for a fixed basis of V corresponds a matrix $[f]$ such that for every $x, y \in V$, $f(x,y) = x[f]y^t$. A symplectic vector space V is called nondegenerate if for every $x \in \mathcal{V}$ such that $f(x,y) = 0$, for all $y \in V$, we conclude $x = 0$. It is well known that if V is a nondegenerate symplectic vector space, then $\dim(V) = 2n$ for some n.

For a subspace $\mathcal{W}$ of a a nondegenerate symplectic vector space V with symplectic form f

$$\mathcal{W}^{\perp} = \{x \in V | f(x,y) = 0, \forall y \in W\}.$$

A subspace $\mathcal{U}$ of a nondegenerate symplectic vectorspace V is called an isotropic subspace if $f(u,v) = 0$, for all $u, v \in \mathcal{U}$, which means $\mathcal{U} \subset \mathcal{U}^{\perp}$. It is well known that if $\mathcal{U}$ is an isotropic subspace then $\dim(\mathcal{U}) \leq \dim(V)/2$. The set of all r-dimensional isotropic subspaces of V is called isotropic Grassmannian, denoted by $\mathcal{GI}(n,r)$. Let V be a nondegenerate symplectic vector space of dimension $2n$, then

$$\mid \mathcal{GI}(2n,r) \mid = \prod_{i=1}^{i=r} \frac{q^{2(n-i+1)} - 1}{q^i - 1}.$$

Symplectic group $\mathrm{Sp}_{2n}(q) = \{A \in \mathrm{GL}_n(q) \mid A[f]A^{-1} = [f]\}$ is a subgroup of $\mathrm{GL}_n(q)$. It is well known that $\mathrm{Sp}_{2n}(q)$ acts naturally on $\mathcal{GI}(2n,r)$ and this action is doubly transitive. For more details about symplectic groups we refer to [2].

In the last section, we mentioned the definition of most basic concepts of subspace code setting which we need. We recall that a r–dimensional spread S in a vector space V is a partition of V by a set of r-dimensional subspaces in V. It is well known that spread S exists if and only if $r|\dim(\mathrm{V})$.

In this paper we assume that the ambient space V is a nondegenerate symplectic vector space of dimension $2n$ by symplectic form f. We denote a constant dimension subspace code by C, and the minimum distance of C is denoted by $d_s(C)$. It is clear that if $C \subset \mathcal{G}(k,n)$, then $d_s(C) \leq 2k$. By $\langle v_1, \cdots, v_r \rangle$ we denote the subspace generated by vectors $v_1, \cdots, v_r \in V$.

[Downloaded from ijmsi.com on 2024-04-24]

3. Isotropic subspace codes and decoding process

Let V be a symplectic vector space of dimension $2n$. We define an isotropic subspace code simply as a set of isotropic subspaces of V. Particularly we define an isotropic constant dimension subspace code as a subset of isotropic Grassmannian $\mathcal{GI}(2n, r)$. As we mentioned in second section symplectic group $\mathrm{Sp}_{2n}(q)$ has a doubly transitive action on isotropic Grassmannian $\mathcal{GI}(2n, r)$, so we can define an isotropic orbit code as the orbit of a symplectic subgroup of $\mathrm{Sp}_{2n}(q)$ on $\mathcal{GI}(2n, r)$.

Since the isotropic Grassmannian is a subset of Grassmannian, we may expect that in general, isotropic subspace codes are not as large as subspace codes. However we are interested in knowing if there is any benefit in considering isotropic subspace codes compared to subspace codes. To answer this question we need to focus on isotropic property of codewords.
We study isotropic subspace codes in two steps. first, in the rest of this section, we discuss how the isotropic property helps decoding process. If the received word is not isotropic we can find some error vectors and use a subspace of received word for decoding process. Since in this way we have reduced the dimension of received word, we expect to reduce computations by minimum distance decoder. Then in the next section, we consider the structure of isotropic spread codes which exist for suitable parameters. We guess that for all possible parameters there are isotropic cyclic orbit codes which are spread too. However the isotropic spreads we offer in that section do not take a cyclic isotropic orbit structure in general.

Decoding Process

Let $C \subset \mathcal{G}(n, r)$ be a constant dimension subspace code with $d_s(C) = d$. The decoding problem is how to efficiently find a codeword of $\mathcal{U}$ that is closest (respected to subspace distance) to a given subspace $\mathcal{R} \in \mathrm{PG}(n-1, q)$. Basically Closest codeword $\mathcal{U}$ to $\mathcal{R}$ has the maximum $\dim(\mathcal{R} \cap \mathcal{U})$ between all codewords. It is clear that the less the dimention of R is, the less computation we need to find the maximum $\dim(\mathcal{R} \cap \mathcal{U})$. We will continue by showing that for isotropic subspace codes, we can likely find a smaller subspace of R to be used in decoding process.
A minimum distance decoder $\mathrm{dec} : \mathrm{PG}(n-1, q) \to C \cup \{\epsilon\}$, for every $\mathcal{U} \in \mathrm{PG}(n-1, q)$, returns a codeword $\mathcal{V} \in C$ if $\mathcal{V}$ is the unique codeword that satisfies $d_s(\mathcal{V}, \mathcal{U}) \leq [(d-1)/2]$ and returns ϵ (failure indicator) otherwise.

Assume we use a constant dimension subspace code $C \subset \mathcal{G}(n, r)$ for transmission. Let $\mathcal{U}$ be transmitted and let $\mathcal{R} = \bar{\mathcal{U}} \oplus E$ be received, where E is the error space with $\dim(E) = t$ and $\bar{\mathcal{U}} \subset \mathcal{U}$ where $\dim(\bar{\mathcal{U}}) = r - \rho$ and ρ is the dimension of erasure space. If $2(t + \rho) < d(C)$ then a minimum distance decoder dec(.), returns the transmitted codeword $\mathcal{U}$ [9].

[Downloaded from ijmsi.com on 2024-04-24]

Now Let $C \subset \mathcal{GI}(2n, r)$ be an isotropic constant dimension subspace code. We recall that the ambient space is equipped with symplectic form f. As we mentioned before we are interested in knowing how isotropic property affect the minimum distance decoder dec(.).

Let $B = \{a_1, a_2, ..., a_s\}$ be a basis for $\mathcal{R}$. If there exists a pair $\{a_i, a_j\} \subset B$ such that $f(a_i, a_j) \neq 0$, then either a_i or a_j is an error vector. Now if we remove $\{a_i, a_j\}$ of B and consider the vectorspace $\mathcal{R}^{'} = \langle B - \{a_i, a_j\}\rangle$, then $\mathcal{R}^{'} = \mathcal{U}^{'} \oplus E^{'}$, where $\mathcal{U}^{'} = \mathcal{U} \cap \mathcal{R}^{'}$ and $E^{'} \subset E$ is the error space. Let $\dim(E^{'}) = t^{'}$ and $\dim(\mathcal{U}^{'}) = r - \rho^{'}$. If $2(t^{'} + \rho^{'}) < d_s(C)$, then the minimum distance decoder dec(.) returns $\mathcal{R}^{'}$ to $\mathcal{U}$. Since $a_i \in E$ or $a_j \in E$ there are two cases, $t^{'} = t - 1$ and $\rho^{'} = \rho + 1$ or $t^{'} = t - 2$ and $\rho^{'} = \rho$. Both cases lead to $2(t^{'} + \rho^{'}) < d_s(C)$. Notice that the existence of such pair is independent of the choice of the basis. Therefore the following theorem holds:

Theorem 3.1. *Assume we use an isotropic constant dimension subspace code $C \subset \mathcal{GI}(2n, r)$. Let codeword $\mathcal{U}$ be transmitted and $\mathcal{R} = \bar{\mathcal{U}} \oplus E$ be received, where $\dim(E) = t$, $\dim(\bar{\mathcal{U}}) = r - \rho$ and $2(t + \rho) < d_s(C)$. Let $B = \{a_1, a_2, ..., a_{r-\rho+t}\}$ be a basis for $\mathcal{R}$. If there exists a pair $\{a_i, a_j\} \subset B$ such that $f(a_i, a_j) \neq 0$, then the minimum distance decoder* dec(.) *returns $\mathcal{R}^{'} = \langle B - \{a_i, a_j\}\rangle$ to $\mathcal{U}$.*

We can even move further and generalize this result. By the same hypotheses, we can show more generally, if there are some disjoint pairs $\{a_i, a_j\} \subset B$ such that $f(a_i, a_j) \neq 0$, then we can remove all these disjoint pairs from basis B.

Theorem 3.2. *Assume we use an isotropic constant subspace code $C \subset \mathcal{GI}(2n, r)$, Let codeword $\mathcal{U}$ be transmitted and $\mathcal{R} = \bar{\mathcal{U}} \oplus E$ be received, where* $\dim(\mathrm{E}) = \mathrm{t}$, *$\dim(\bar{\mathcal{U}}) = r - \rho$ and $2(t + \rho) < d_s(C)$. Let $B = \{a_1, a_2, ..., a_{r-\rho+t}\}$ be a basis for $\mathcal{R}$. Let I be a set of disjoint pairs of the elements of B such that $f(a_i, a_j) \neq 0$, for all $\{a_i, a_j\} \in I$. Then* $\mathrm{dec}(\langle B - \bigcup_{\{i,j\} \in I} \{a_i, a_j\}\rangle) = \mathcal{U}$.

Proof. By the same argument as the one for Theorem 3.1, it is enough to prove that $\langle B - \bigcup_{\{i,j\} \in I} \{a_i, a_j\}\rangle \neq 0$. To show this, let $B = \bigcup_{\{i,j\} \in I} \{a_i, a_j\}$, then at least $|B|/2$ number of a_is are error vectors so $|B|/2 \leq t$. Since $|B| = \dim(\mathcal{R}) = r - \rho + t$, so $|B|/2 \geq r - \rho$. On the other hand $2(t + \rho) < d_s(C) \leq 2r$, therefore $|B|/2 \leq t < r - \rho$, a contradiction. □

According to this result if the received space is not isotropic, then we can consider a subspace of the received space for decoding process. Now a natural question is if we consider an isotropic subspace code and transmit a codeword $\mathcal{U}$, **what is the probability that the received subspace $\mathcal{R}$ is not isotropic.** In order to answer this question first we consider the number of all subspaces of

[Downloaded from ijmsi.com on 2024-04-24]

dimension $r-\rho+t$ which contains $\bar{\mathcal{U}}$, then we compute the number of $(r-\rho+t)$-dimensional isotropic subspaces that contains $\bar{\mathcal{U}}$. For our discussion we need the following fact:

Lemma 3.3. *Let V be a vector space of dimension n and $\mathcal{U}$ be a k-dimensional subspace of V. The number of m-dimensional subspaces $\mathcal{W}$ of V which include $\mathcal{U}$ is equal to $\begin{bmatrix} n-k \\ m-k \end{bmatrix}_q$, where $\begin{bmatrix} s \\ r \end{bmatrix}_q = \prod_{i=1}^{i=r} \frac{q^{s-i}-1}{q^i-1}$.*

Proof. Let V be a vector space of dimension n and $\mathcal{U}$ be a k-dimensional subspace of V, then $V = \mathcal{U} \oplus \mathcal{X}$, for a $n-k$-dimensional subspace $\mathcal{X}$ of V. Trivially the number of m-dimensional subspaces $\mathcal{W}$ of V, which contain $\mathcal{U}$ is the same as the number of $m-k$-dimensional subspaces of $\mathcal{X}$. □

Assume there exist $x_1, ..., x_i \in V$ such that $\langle \bar{\mathcal{U}}, x_1, ..., x_i \rangle$ is an isotropic subspace, then $x_1, ..., x_i \in \bar{\mathcal{U}}^{\perp}$. So every isotropic subspace which includes $\bar{\mathcal{U}}$ is a subspace of $\bar{\mathcal{U}}^{\perp}$. Assume p is the probability that $\mathcal{R} = \bar{\mathcal{U}} \oplus E$ is not isotropic. We know that in a symplectic space an isotropic subspace and its dual space are codimension. Therefore since $\dim(\bar{\mathcal{U}}) = r - \rho$, then $\dim(\bar{\mathcal{U}}^{\perp}) = n - r + \rho$ and according to Lemma 3.3 we have:

$$
\begin{aligned}
p &= 1 - \frac{\mid \{X \in \mathcal{GI}(n-r+\rho, r-\rho+t) \mid \bar{\mathcal{U}} \subset X\} \mid}{\mid \{X \in \mathcal{G}(n, r-\rho+t) \mid \bar{\mathcal{U}} \subset X\} \mid} \\
&\geq 1 - \frac{\begin{bmatrix} n-r+\rho-(r-\rho) \\ r-\rho+t-(r-\rho) \end{bmatrix}_q}{\begin{bmatrix} n-(r-\rho) \\ r-\rho+t-(r-\rho) \end{bmatrix}_q} \\
&= 1 - \frac{\begin{bmatrix} n-2r+2\rho \\ t \end{bmatrix}_q}{\begin{bmatrix} n-r+\rho \\ t \end{bmatrix}_q}.
\end{aligned}
$$

Let $q = 2$ and $r = \frac{n}{2}$, then

$$
p \geq 1 - \frac{\begin{bmatrix} 2\rho \\ t \end{bmatrix}_2}{\begin{bmatrix} \frac{n}{2}+\rho \\ t \end{bmatrix}_2}.
$$

So if the dimension of erasure space is low comparing to n or in other words the probability of errors is high, when n is increased then $p \to 1$. In the following table we calculate the probability p for some parameters:

[Downloaded from ijmsi.com on 2024-04-24]

n	r	ρ	t	$p \geq$
6	3	1	1	0.8
8	3	1	1	0.75
10	3	1	1	0.88
12	3	1	1	0.76
12	4	1	1	0.88

n	r	ρ	t	$p \geq$
8	4	1	2	0.99
10	5	1	2	0.99
10	5	2	2	0.997
12	6	2	3	0.999
14	7	2	3	0.999

4. Isotropic Spreads

In this section we study isotropic spread codes which exist for suitable parameters. Our conjecture is that for all possible parameters there are isotropic cyclic orbit codes which are spread too. However the isotropic spreads we offer in this section do not take a cyclic isotropic orbit structure in general. We give an explicit structure of isotropic spread codes by three steps. The main reference in this subsection is [3].

Step 1.

In this step we present a spread structure which we will show to be isotropic in the second and the third steps.

Let $\mathbb{F}_q^{2n}$ be a vector space and $r \mid n$, then $n = rN$ for some N. Let $L = \mathbb{F}_{q^r}$ and α be a root of primitive polynomial $p(x)$ over $\mathbb{F}_q$ in L, then $\{1, \alpha, \alpha^2, \cdots, \alpha^{r-1}\}$ is a basis for L over $\mathbb{F}_q$. Let $x = (x_1, \cdots, x_{2N}) \in L^{2N}$, then to every element $x_i \in L$ corresponds an element $(x_{i1}, \cdots, x_{ir}) \in \mathbb{F}_q^r$. Therefore we can define the following natural bijection:

$$\phi : L^{2N} \longrightarrow \mathbb{F}_q^{2n}$$

$$x \to (x_{11}, x_{21}, \cdots, x_{2N,1}, x_{12}, x_{22}, \cdots, x_{2N,2}, \cdots, x_{1,r}, \cdots, x_{2N,r}).$$

Thus to an element $x \in L^{2N}$ corresponds a $\phi(x) \in \mathbb{F}_q^{2n}$. We emphasize that $\phi(x) = (X_1, \cdots, X_r)$, where every

$$X_i = (x_{1,i}, x_{2,i}, \cdots, x_{2N,i})$$

is a vector of length $2N$. This way to define ϕ will be useful in the third step.

We use the fact that ϕ is an $\mathbb{F}_q$-linear map to prove the following lemma:

Lemma 4.1. *Let $\langle x \rangle \subset L^{2N}$, be a 1-dimensional subspace, then $\langle \phi(x), \phi(x\alpha), \cdots, \phi(x\alpha^{r-1}) \rangle$ is an r-dimensional subspace of $\mathbb{F}_q^{2n}$.*

Proof. Let $\sum_0^{r-1} \beta_i \phi(x\alpha^i) = 0$, where $\beta_i \in \mathbb{F}_q$, then $\sum_0^{r-1} \phi(\beta_i x \alpha^i) = 0$. So $\phi(\sum_0^{r-1} \beta_i x \alpha^i) = 0$. Therefore $\sum_0^{r-1} \beta_i x \alpha^i = 0$, but then $(\sum_0^{r-1} \beta_i \alpha^i)x = 0$. Thus $\sum_0^{r-1} \beta_i \alpha^i = 0$. This implies that $\beta_i = 0$, for every i. □

[Downloaded from ijmsi.com on 2024-04-24]

There are $\frac{q^{2Nr}-1}{q^r-1}$ number of 1-dimensional subspaces in L^{2N}. By Lemma 4.1, these subspaces induce a set of r-dimensional subspaces in $\mathbb{F}_q^{2n}$ over $\mathbb{F}_q$ which we denote by ζ_r.

The following example clarifies the construction of ζ_r.

EXAMPLE 4.2. Let $n = 6$ and $r = 3$, then $N = 2$. Consider $L = \mathbb{F}_{2^3}$, primitive polynomial $p(x) = 1 + x + x^3$ over $\mathbb{F}_2$ and α, where $p(\alpha) = 0$. There are 585 subspaces of dimension 1 in L^4 which are generated by the following vectors:

- $(1, 0, 0, 0)$
- $(x, 1, 0, 0),\ x \in L$
- $(x, y, 1, 0),\ x, y \in L$
- $(x, y, z, 1),\ x, y, z \in L$

Consider $e = (1, 0, 0, 0)$, then $\langle e\rangle$ is a 1-dimensional subspace of L^4 and

- $\phi(e) = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$,
- $\phi(e\alpha) = \phi(\alpha, 0, 0, 0) = (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$,
- $\phi(e\alpha^2) = \phi(\alpha^2, 0, 0, 0) = (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$.

$\mathcal{U} = \langle\phi(e), \phi(e\alpha), \phi(e\alpha^2)\rangle$ is a 3-dimensional subspace of $\mathbb{F}_2^{12}$.

Notice that in general,

$$|\zeta_r| = \frac{q^{2Nr} - 1}{q^r - 1} = \frac{q^{2n} - 1}{q^r - 1},$$

which is the size of an r-dimensional spread in $\mathbb{F}_q^{2n}$. The following lemma shows that ζ_r is always a spread in $\mathbb{F}_q^{2n}$:

Lemma 4.3. *Let r divides n, then ζ_r is an r-dimensional spread in $\mathbb{F}_q^{2n}$.*

Proof. Let $x, y \in L^{2N}$, $\langle x\rangle \neq \langle y\rangle$, $\mathcal{U}_1 = \langle\phi(x), \phi(x\alpha), \cdots, \phi(x\alpha^{r-1})\rangle$ and $\mathcal{U}_2 = \langle\phi(y), \phi(y\alpha), \cdots, \phi(y\alpha^{r-1})\rangle$ belong to ζ_r. If there are $\beta_i, \gamma_i \in F_q$ such that:

$$\sum_0^{r-1} \beta_i\phi(x\alpha^i) = \sum_0^{r-1} \gamma_i\phi(y\alpha^i).$$

Then we will have:

$$\phi(\sum_0^{r-1} \beta_i\alpha^i x) = \phi(\sum_0^{r-1} \gamma_i\alpha^i y).$$

[Downloaded from ijmsi.com on 2024-04-24]

So

$$\sum_{0}^{r-1}(\beta_i\alpha^i)x = \sum_{0}^{r-1}(\gamma_i\alpha^i)y.$$

But we have $\langle x\rangle \neq \langle y\rangle$, therefore

$$\sum_{0}^{r-1}(\beta_i\alpha^i)x = \sum_{0}^{r-1}(\gamma_i\alpha^i)y = 0.$$

Then $\sum_{0}^{r-1}(\beta_i\alpha^i) = \sum_{0}^{r-1}(\gamma_i\alpha^i) = 0$, so $\beta_i = \gamma_i = 0$, for all i. And the proof is complete. □

EXAMPLE 4.4. In Example 4.2 consider $e^{'} = (\alpha, 1, 0, 0)$, then

- $\phi(e^{'}) = (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$,
- $\phi(e^{'}\alpha) = \phi(\alpha^2, \alpha, 0, 0) = (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$,
- $\phi(e^{'}\alpha^2) = \phi(\alpha^3, \alpha^2, 0, 0) = (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$.

$\mathcal{V} = \langle\phi(e^{'}), \phi(e^{'}\alpha), \phi(e^{'}\alpha^2)\rangle$ is a 3-dimensional subspace of $\mathbb{F}_2^{12}$. If $x \in \mathcal{U} \cap \mathcal{V}$, then

$$\begin{aligned} x &= x_1\phi(e) + x_2\phi(e\alpha) + x_3\phi(e\alpha^2) \\ &= y_1\phi(e^{'}) + y_2\phi(e^{'}\alpha) + y_3\phi(e^{'}\alpha^2), \end{aligned}$$

where $x_i, y_i \in F_2$, for $i = 1, 2, 3$. Therefore

$$\begin{aligned} x &= (x_1, 0, 0, 0, x_2, 0, 0, 0, x_3, 0, 0, 0) \\ &= (y_3, y_1, 0, 0, y_1 + y_3, y_2, 0, 0, y_2, y_3, 0, 0) \end{aligned}$$

This implies $x_i = y_i = 0$, for all $1 \leq i \leq 3$. So $x = 0$.

Step 2.
In this step we begin to give an isotropic structure to spread ζ_r. To do this we need to define a nondegenerate symplectic form on $\mathbb{F}_q^{2n}$ and show that ζ_r is isotropic with this form.

Let $v = (v_1, \cdots, v_{2N}), w = (w_1, \cdots, w_{2N}) \in L^{2N}$ and consider a symplectic form f on L^{2N} as follows:

$$f(v, w) = (v_1w_2 - v_2w_1) + (v_3w_4 - v_4w_3) + \cdots + (v_{2N}w_{2N-1} - v_{2N-1}w_{2N}).$$

[Downloaded from ijmsi.com on 2024-04-24]

We denote the corresponding matrix to f by J and we have:

$$J = \begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \end{pmatrix}.$$

If we consider every v_i and w_i as an $\mathbb{F}_q$-linear combination of α^is, then $f(v,w) = \sum_{0}^{r-1} \alpha^i f_i(\phi(v), \phi(w))$, where f_i is a bilinear form over $\mathbb{F}_q^{2n}$, for every i.

Let study f_is in more details. For every i, $v_i = \sum_{1}^{r} v_{ij}\alpha^{j-1}$ and $w_i = \sum_{1}^{r} w_{ij}\alpha^{j-1}$, where $v_{ij}, w_{ij} \in \mathbb{F}_q$. Therefore we have:

$$\begin{aligned} v &= (v_1, v_2, \cdots, v_{2N}) \\ &= (\sum_{1}^{r} v_{1j}\alpha^{j-1}, \sum_{1}^{r} v_{2j}\alpha^{j-1}, \cdots, \sum_{1}^{r} v_{2N,j}\alpha^{j-1}) \\ &= \sum_{1}^{r} V_j \alpha^{j-1}, \end{aligned}$$

where $V_j = (v_{1j}, v_{2j}, \cdots, v_{2N,j})$. By the same notations for w, we have:

$$\begin{aligned} f(v,w) &= f(\sum_{1}^{r} V_j\alpha^{j-1}, \sum_{1}^{r} W_j\alpha^{j-1}) \\ &= (\sum_{1}^{r} V_j\alpha^{j-1}) J (\sum_{1}^{r} W_j\alpha^{j-1})^t. \end{aligned} \tag{1}$$

Every f_i is a symplectic form on $\mathbb{F}_q^{2n}$. In general the symplectic forms f_i depend on primitive polynomial $p(x)$, and we are able to formulate them if we fix $p(x)$. However if we fix n, r and the field extension, then we are able to formulate f_is as symplectic forms on $\mathbb{F}_q^{2n}$, where we are not sure if they are nondegenerate. But for the special case f_0 we are able to formulate f_0 exactly when $q = 2$.

We continue with formulating f_0, then we prove that f_0 is a nondegenerate symplectic form on $\mathbb{F}_q^{2n}$. If we consider the constant coefficient of summation in the right side of (1), then we have:

$$f_0(\phi(v), \phi(w)) = \sum_{1}^{r-1} \beta_i V_{i+1} J W_{r-i+1}^t + V_1 J W_1^t,$$

for some $\beta_i \in \mathbb{F}_q$. Particularly if $q = 2$, then symplectic form f_0 is independent of $p(x)$:

$$f_0(\phi(v), \phi(w)) = \sum_{1}^{r-1} V_{i+1} J W_{r-i}^t + V_1 J W_1^t.$$

[Downloaded from ijmsi.com on 2024-04-24]

Let $J^* = \mathrm{Diag}(J, \cdots, J)$ be a $2Nr \times 2Nr(2n \times 2n)$ matrix, then

$$f_0(\phi(v), \phi(w)) = \sum_{1}^{r-1} V_{i+1} J W_{r-i+1}^t + V_1 J W_1^t$$
$$= (V_1, V_2, V_3, \cdots, V_r) J^* (W_1, W_r, W_{r-1}, \cdots, W_2)^t.$$

Therefore $[f_0] = J^*$. It follows that $\det([\mathrm{f_0}]) = \det(\mathrm{J})^{\mathrm{r}} = 1 \neq 0$ and consequently f_0 is a nondegenerate symplectic form. Therefore f_0 is a nondegenerate symplectic form on $\mathbb{F}_q^{2n}$ obtained from f.

Example 4.5. Assume the hypothesis of Example 4.2, and consider bilinear form f on L^4 as in the first step. For every elements $v, w \in L^4$ where $v = (v_1, \cdots, v_4)$, $w = (w_1, \cdots, w_4)$ there exist $v_{ij}, w_{ij} \in F_2$ such that $v_i = \sum_{1}^{3} v_{ij}\alpha^{j-1}$ and $w_i = \sum_{1}^{3} w_{ij}\alpha^{j-1}$. Put $V_j = (v_{1j}, v_{2j}, v_{3j}, v_{4j})$, for every $j \in \{1, 2, 3\}$. Then

$$f(v, w) = (v_1, v_2, v_3, v_4) J (w_1, w_2, w_3, w_4)^t = (\sum_{1}^{3} V_j \alpha^j) J (\sum_{1}^{3} W_j \alpha^j)^t.$$

Since $1 + \alpha + \alpha^3 = 0$, if we consider the constant coefficient in the right hand of the formulation f we have:

$$f_0(\phi(v), \phi(w)) = f_0((V_1, V_2, V_3), (W_1, W_2, W_3))$$
$$= V_1 J W_1^t + V_2 J W_3 + V_3 J W_2$$
$$= (V_1, V_2, V_3)\ \mathrm{Diag}(J, J, J)\ (W_1, W_3, W_2)^t.$$

Step 3.
Finally in this step we prove that respect to symplectic form f_0, ζ_r is an isotropic spread.

By Lemma 4.3 ζ_r is a spread in $\mathbb{F}_q^{2n}$. In the following theorem we prove that in fact ζ_r is a set of isotropic subspaces:

Theorem 4.6. *Let r divide n, then there is an r-dimensional spread in $\mathbb{F}_q^{2n}$, where its elements are isotropic subspaces.*

Proof. Let ζ_r be constructed as in the first step and $\mathcal{U} \in \zeta_r$, then for every $x, y \in \mathcal{U}$, there is a $\lambda \in L$ such that for corresponding elements $\phi^{-1}(x)$ and $\phi^{-1}(y)$ in L^{2N}, we have $\phi^{-1}(x) = \lambda\phi^{-1}(y)$. Since $f(\phi^{-1}(x), \lambda\phi^{-1}(y)) = 0$, then $f(\phi^{-1}(x), \phi^{-1}(y)) = 0$, so for every i, $f_i(x, y) = 0$ particularly $f_0(x, y) = 0$ and the proof is complete. □

Example 4.7. According to our method to construct 2-dimensional isotropic spread in $\mathbb{F}_2^4$, let $L = \mathbb{F}_2^2$, then L^2 has five 1-dimensional subspaces and each one induces a 2-dimensional subspace of $\mathbb{F}_2^4$:

[Downloaded from ijmsi.com on 2024-04-24]

$$\langle(1,0)\rangle \Rightarrow \mathcal{S}_1 = \langle(1,0,0,0),(0,0,1,0)\rangle,$$
$$\langle(0,1)\rangle \Rightarrow \mathcal{S}_2 = \langle(0,1,0,0),(0,0,0,1)\rangle,$$
$$\langle(\alpha,1)\rangle \Rightarrow \mathcal{S}_3 = \langle(0,1,1,0),(1,0,1,1)\rangle,$$
$$\langle(1,\alpha)\rangle \Rightarrow \mathcal{S}_4 = \langle(1,0,0,1),(0,1,1,1)\rangle,$$
$$\langle(1,1)\rangle \Rightarrow \mathcal{S}_5 = \langle(1,1,0,0),(0,0,1,1)\rangle.$$

The corresponding matrix J to the bilinear form on $\mathbb{F}_2^4$ is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Therefore $S = \{S_1, S_2, \cdots, S_5\}$ is the isotropic spread.

As we mentioned in section 1 there is a cyclic orbit structure for spread codes, therefore naturally we are interested in knowing whether there is an orbit structure for isotropic spread codes.

Computing with GAP2015 [6] we see that the structure in above example is not a cyclic isotropic orbit code. We emphasize that according to Example 4.2 an element of our isotropic spread structure is the subspace with the following basis:

$$\{\underbrace{(1,0,\cdots,0)}_{2Nr},\cdots,\underbrace{(0,\cdots,0}_{2N(i-1)},1,0,\cdots,0),\cdots,\underbrace{(0,\cdots,0}_{2N(r-1)},1,0,\cdots,0)\}$$

Therefore we searched isotropic cyclic orbits with this fixed starting point.

Nevertheless there are several isotropic spreads as cyclic isotropic orbit code in $\mathbb{F}_2^4$. Assume S_1 as in Example 4.7:

Example 4.8. Let

$$G = \langle \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \rangle.$$

Then the cyclic isotropic orbit of G with starting point S_1 is an isotropic spread.

The following example is another case that shows isotropic spread ζ_r is not an isotropic orbit code in general.

Example 4.9. Consider $\mathbb{F}_2^6$ and primitive polynomial $p(x) = x^3 + x + 1$. According to our method the 3-dimensional isotropic spread has the following elements:

$$\langle(1,0)\rangle \Rightarrow \mathcal{S}_1 = \langle(1,0,0,0,0,0),(0,0,1,0,0,0),(0,0,0,0,1,0)\rangle,$$
$$\langle(0,1)\rangle \Rightarrow \mathcal{S}_2 = \langle(0,1,0,0,0,0),(0,0,0,1,0,0),(0,0,0,0,0,1)\rangle,$$
$$\langle(\alpha,1)\rangle \Rightarrow \mathcal{S}_3 = \langle(0,1,1,0,0,0),(0,0,0,1,1,0),(1,0,1,0,0,1)\rangle,$$

[Downloaded from ijmsi.com on 2024-04-24]

$\langle(1,\alpha)\rangle \Rightarrow \mathcal{S}_4 = \langle(1,0,0,1,0,0),(0,0,1,0,0,1),(0,1,0,1,1,0)\rangle$,
$\langle(1,1)\rangle \Rightarrow \mathcal{S}_5 = \langle(1,1,0,0,0,0),(0,0,1,1,0,0),(0,0,0,0,1,1)\rangle$.
$\langle(1,\alpha^2)\rangle \Rightarrow \mathcal{S}_6 = \langle(1,0,0,0,0,1),(0,1,1,1,0,0),(0,0,0,1,1,1)\rangle$.
$\langle(\alpha^2,1)\rangle \Rightarrow \mathcal{S}_7 = \langle(0,1,0,0,1,0),(1,0,1,1,0,0),(0,0,1,0,1,1)\rangle$.
$\langle(1,\alpha+\alpha^2)\rangle \Rightarrow \mathcal{S}_8 = \langle(1,0,0,1,0,1),(0,1,1,1,0,1),(0,1,0,0,1,1)\rangle$.
$\langle(1,1+\alpha)\rangle \Rightarrow \mathcal{S}_9 = \langle(1,1,0,1,0,0),(0,0,1,1,0,1),(0,1,0,1,1,1)\rangle$.

Checking by GAP2015, we found out this spread is not a cyclic isotropic orbit either. While if we consider symplectic subgroup

$$G = \langle \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \rangle,$$

then the isotropic orbit with starting point S_1 is an isotropic spread code.

In these steps we showed there exists an r-dimensional isotropic spread in $\mathbb{F}_q^{2n}$ respect to symplectic form f_0, where $r \mid n$.

5. Conclusion

We have defined an isotropic subspace code as a set of isotropic subspaces in an ambient symplectic vector space. We have described several properties of these codes. If error occurs during transmission, with a high probability the received space will not be isotropic. Therefore we can consider a smaller subspace of received vector space in decoding process. Also we explicitly mentioned a structure of isotropic spreads for suitable parameters. Finally with some examples we have showed our structure does not form a cyclic isotropic orbit code in general. While we guess that for all parameters r and n such that $r|n$, there exist an r-dimensional isotropic spread with an isotropic cyclic orbit structure. We are interested in finding a systematic method for isotropic spreads as isotropic orbit codes. Studying isotropic orbit codes generally and searching for large isotropic subspace codes to derive more properties of these codes may be further research interest.

Acknowledgments

The authors wish to thank referees for their valuable comments.

References

1. S. Ball, J. Bamberg, M. Lavrauw, T. Penttila, Symplectic spreads, *Designs, Codes and Cryptography*, **32**(1), 9–14, (2004).

[Downloaded from ijmsi.com on 2024-04-24]

2. R. W. Carter, Simple Groups of Lie Type, John Wiley and sons, London, (1972).
3. R. H. Dye, Partitions and their stabilizers for line complexes and quadrics, *Annali di Matematica pura ed applicata*, **114**(1) 173–194, (1977).
4. T. Etzion, Problems on q-analogs in coding theory, arXiv:13056126 [cs.IT], (2013).
5. T. Etzion, A. Vardy, Error-correcting codes in projective geometry, *IEEE Trans. Inform. Theory*, IT-57, 1165–1173, (2011).
6. The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.8; 2015. (http://www.gap-system.org)
7. H. Gluesing-Luerssen, K. Morrison, C. Troha, Cyclic orbit codes and stabilizer subfields, arXiv:1403.1218, (2014).
8. N. L. Johnson, O. Vega, Symplectic spreads and symplectically paired spreads, *Note di Matematica*, **26**(2), 119–134, (2006).
9. R. Kötter , F.R Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theor.*, **54**(8), 3579–3591, (2008).
10. W. J. Martin, X. J. Zhu, Anticodes for the Grassman and bilinear forms graphs, *Designs, Codes and Cryptography,* **6**, 73–79 (1995).
11. F. Manganiello, A.-L. Trautmann, J. Rosenthal, On conjugacy classes of subgroups of the general linear group and cyclic orbit codes, *In Proceedings of the 2011 IEEE International Symposium on Information Theory,* **31**(5) 1916–1920, (2011).
12. J. Rosenthal, A.-L. Trautman, A complete characterization of irreducible cyclic orbit codes and their Plücker embedding, *Des. Codes Cryptogr.,* 275–289, (2013).
13. M. Schwartz, T. Etzion, Codes and anticodes in the Grassman graph, *J. Combinatorial Theory, Series A*, **97**, 27-42, (2002).
14. A. L. Trautmann, F. Manganiello, M. Braun, J. Rosenthal, Cyclic orbit codes, *IEEE Trans. Inf. Theor.*, IT-59, 7386-7404, (2013).

[Downloaded from ijmsi.com on 2024-04-24]