Communications
in
Mathematical
Research
31(4)(2015), 345–350

Self-dual Codes with Symplectic Inner Product

Nan Ji-zhu and Yu Xue-min
(*School of Mathematical Sciences, Dalian University of Technology, Dalian, Liaoning, 116024*)

Communicated by Du Xian-kun

Abstract: In this paper, we discuss a kind of Hermitian inner product — symplectic inner product, which is different from the original inner product — Euclidean inner product. According to the definition of symplectic inner product, the codes under the symplectic inner product have better properties than those under the general Hermitian inner product. Here we present the necessary and sufficient condition for judging whether a linear code C over F_p with a generator matrix in the standard form is a symplectic self-dual code. In addition, we give a method for constructing a new symplectic self-dual codes over F_p, which is simpler than others.

Key words: symplectic inner product, symplectic self-dual code, symplectic circulant code
2010 MR subject classification: 94B05, 51A50
Document code: A
Article ID: 1674-5647(2015)04-0345-06
DOI: 10.13447/j.1674-5647.2015.04.06

1 Introduction

Let F_p be a field, where p is a prime number. Self-dual codes over F_p are an important class of linear codes, as described in [1]. Kim and Lee[2] have discussed self-dual codes under Euclidean inner product or Hermitian inner product.

Now, we give a brief introduction to several basic definitions and facts in coding theory. A linear $[n, k]$ code C over F_p is a k-dimensional vector subspace of F_p^n. The element c of C is called codeword. The value n is called the length of C.

There are two normal inner products – Euclidean and Hermitian inner products. For two vectors $\boldsymbol{x} = (x_1, \cdots, x_n)$, $\boldsymbol{y} = (y_1, \cdots, y_n) \in F_p^n$, the Euclidean inner product over finite field F_p is defined as

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_n y_n.$$

Received date: March 28, 2014.
Foundation item: The NSF (11371343) of China.
E-mail address: jznan@163.com (Nan J Z).

When p is an even power of any prime, we can also consider the Hermitian inner product which is defined as

$$\boldsymbol{x} * \boldsymbol{y} = x_1\overline{y_1} + \cdots + x_n\overline{y_n},$$

where $\overline{y_i} = {y_i}^{\sqrt{p}}$.

The Euclidean dual code $C^{\perp E}$ of C is defined as

$$C^{\perp E} = \{\boldsymbol{x} \in F_p^n \mid \boldsymbol{x} \cdot \boldsymbol{y} = 0 \ \text{ for all } \boldsymbol{y} \in C\}.$$

Similarly the Hermitian dual code $C^{\perp H}$ is defined as

$$C^{\perp H} = \{\boldsymbol{x} \in F_p^n \mid \boldsymbol{x} * \boldsymbol{y} = 0 \ \text{ for all } \boldsymbol{y} \in C\}.$$

If $C \subseteq C^{\perp E}$ (resp. $C^{\perp H}$), then C is called a Euclidean (resp. Hermitian) self-orthogonal code. If $C = C^{\perp E}$ (resp. $C^{\perp H}$), then C is called a Euclidean (resp. Hermitian) self-dual code.

We know that

$$Sp_{2n} = \left\{ \boldsymbol{A} \in GL_{2n}(F_p) \mid \boldsymbol{A} \begin{pmatrix} 0 & \boldsymbol{I}_n \\ -\boldsymbol{I}_n & 0 \end{pmatrix} \boldsymbol{A}^{\perp} = \begin{pmatrix} 0 & \boldsymbol{I}_n \\ -\boldsymbol{I}_n & 0 \end{pmatrix} \right\}$$

is the symplectic group with respect to $\begin{pmatrix} 0 & \boldsymbol{I}_n \\ -\boldsymbol{I}_n & 0 \end{pmatrix}$ over F_p, and the element in Sp_{2n} is called symplectic matrix. Let us define a new inner product.

Definition 1.1 *Let C be a code over F_p. The lengths of the codewords are all $2n$. For two codewords $\boldsymbol{x} = (x_1, \cdots, x_{2n})$, $\boldsymbol{y} = (y_1, \cdots, y_{2n}) \in C$, we define the symplectic inner product of $\boldsymbol{x}, \boldsymbol{y}$ as follows*:

$$\boldsymbol{x} \bullet \boldsymbol{y} = \boldsymbol{x} \begin{pmatrix} 0 & \boldsymbol{I}_n \\ -\boldsymbol{I}_n & 0 \end{pmatrix} \boldsymbol{y}^{\mathrm{T}} = -x_{n+1}y_1 - \cdots - x_{2n}y_n + x_1y_{n+1} + \cdots + x_ny_{2n},$$

where $\boldsymbol{y}^{\mathrm{T}}$ denotes transposed vector of $\boldsymbol{y}$ and $\boldsymbol{I}_n$ is the identity matrix of order n.

Remark 1.1 The length of any codeword $\boldsymbol{x} \in C$ is $2n$, since we discuss the self-dual code under symplectic inner product.

Definition 1.2 *The symplectic dual code $C^{\perp S}$ of C is defined as*

$$C^{\perp S} = \{\ \boldsymbol{x} \in F_p^{2n} \mid \boldsymbol{x} \bullet \boldsymbol{y} = 0 \text{ for all } \boldsymbol{y} \in C\ \}.$$

If $C \subseteq C^{\perp S}$, then C is called a symplectic self-orthogonal code. If $C = C^{\perp S}$, then C is called a symplectic self-dual code. The necessary condition for C to be a symplectic self-dual code is that $k = n$ (i.e., C is a linear $[2n, n]$ code).

In this paper, we consider the linear $[2n, n]$ code over F_p with a generator matrix in the standard form: $\boldsymbol{G} = \begin{pmatrix} \boldsymbol{I}_n & \boldsymbol{A} \end{pmatrix}$, where $\boldsymbol{A}$ is an $n \times n$ matrix over F_p.

Now we give several basic definitions (see [3]). The matrix $\boldsymbol{A}$ is called a circulant matrix, if

$$\boldsymbol{A} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}.$$