

Title	The submanifold of self-dual codes in a Grassmann manifold
Author(s)	Kobayashi, Shigeru
Citation	Osaka Journal of Mathematics. 32(4) p1001-p.1012
Issue Date	1995
oaire:version	VoR
URL	<a href="https://doi.org/10.18910/10141">https://doi.org/10.18910/10141</a>
DOI	
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

## THE SUBMANIFOLD OF SELF-DUAL CODES IN A GRASSMANN MANIFOLD

SHIGERU KOBAYASHI AND ICHIRO TAKADA

(Received May 16, 1994)

### 1. Introduction

By a  $[N, m]$ -linear code over a finite field  $F$ , we mean an  $m$ -dimensional vector subspace of an  $N$ -dimensional vector space  $V$  over  $F$ . Let  $C^\perp$  be the orthogonal complement of a  $[N, m]$ -linear code  $C$  in  $V$ , that is  $C^\perp = \{v \in V \mid \langle v, c \rangle = 0 \text{ for any } c \in C\}$ , where  $\langle \cdot, \cdot \rangle$  denotes a fixed inner product of  $V$ . This is called the dual code of  $C$  which is a  $[N, N-m]$ -linear code.  $C$  is called self-orthogonal (resp. self-dual) if and only if  $C \subset C^\perp$  (resp.  $C = C^\perp$ ). For any linear code, it may be known that there exists a self-dual embedding, and so every linear code can be made from a self-dual code. Therefore we are interested in self-dual codes. Since a linear code  $C$  is a vector space,  $C$  can be thought as an element of the Grassmann manifold  $GM(m, V)$ . Similarly,  $C^\perp$  can be thought as an element of  $GM(N-m, V)$ . As a set,  $GM(m, V)$  and  $GM(N-m, V)$  are isomorphic so that  $C$  and  $C^\perp$  correspond each other as elements of the Grassmann manifolds. In this paper, we shall study the self-orthogonality and the self-duality of linear codes through the Grassmann manifolds. In section 1, we shall give a constructive proof of self-dual embedding of linear codes. In section 2, we shall summarize about the Grassmann manifolds and give an elementary result about the self-duality using a projective embedding. In section 3, we shall give our main theorem on self-orthogonality and self-duality of linear codes. This theorem shows that self-orthogonal codes and self-dual codes are on a quadratic surface in the projective space. Combining our results, we can see that every linear code can be obtained from a self-dual code, and every self-dual code is a special case of a self-orthogonal code.

### 2. Self-dual embedding of linear codes

In this section, we assume  $N = n + m$ . Let  $C$  be a  $[N, m]$ -linear code over a finite field  $F$ . We shall construct a self-dual code which contains  $C$  as an embedding image. It may be known, but this is a motive for studying self-dual codes and so we shall give the proof. Since  $C$  can be thought as a subspace of

$F^N$ , we can write

$$C = \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \begin{matrix} \uparrow \\ m \\ \downarrow \end{matrix} \\ \leftarrow N \rightarrow$$

where  $\xi^{(i)}$  ( $i=0, \dots, m-1$ ) are column vectors of  $F^N$ . First assume that  $ch(F)=2$  and consider the equation

$$\langle \xi^{(0)}, \xi^{(0)} \rangle + X^2 = 0. \tag{2.1}$$

where  $\langle , \rangle$  means the inner product of  $F^N$ . Since the Frobenius map  $x \rightarrow x^2$  is an automorphism of  $F$ , the equation (2.1) has solution, say  $X=a_{0,0}$ . Further consider the equations

$$\langle \xi^{(i)}, \xi^{(0)} \rangle + a_{0,0}X_i = 0 \quad (i=0, \dots, m-1).$$

Since these equations are linear, they has solutions, say  $X_i=a_{0,i}$  ( $i=0, \dots, m-1$ ). Now the following matrix

$$\begin{pmatrix} \xi^{(0)} & a_{0,0} \\ \xi^{(1)} & a_{0,1} \\ \vdots & \vdots \\ \xi^{(m-1)} & a_{0,m-1} \end{pmatrix} = \begin{pmatrix} \xi_1^{(0)} \\ \xi_1^{(1)} \\ \vdots \\ \xi_1^{(m-1)} \end{pmatrix} \begin{matrix} \uparrow \\ m \\ \downarrow \end{matrix} \\ \leftarrow N \rightarrow$$

satisfies  $\langle \xi_1^{(0)}, \xi_1^{(j)} \rangle = 0$  ( $j=0, \dots, m-1$ ), where  $\xi_1^{(j)} = (\xi^{(j)}, a_{0,j})$  are column vectors in  $F^N$ . Next consider the equation

$$\langle \xi^{(1)}, \xi^{(1)} \rangle + X^2 = 0.$$

We can obtain the solution as above, say  $X=a_{1,1}$ . Further consider equations

$$\langle \xi^{(1)}, \xi^{(i)} \rangle + a_{1,1}X_i = 0 \quad (i=1, \dots, m-1).$$

Clearly we have solutions, say  $X_i=a_{1,i}$  ( $i=1, \dots, m-1$ ). Hence the following matrix

$$\begin{pmatrix} \xi_1^{(0)} & 0 \\ \xi_1^{(1)} & a_{1,1} \\ \vdots & \vdots \\ \xi_1^{(m-1)} & a_{1,m-1} \end{pmatrix} = \begin{pmatrix} \xi_2^{(0)} \\ \xi_2^{(1)} \\ \vdots \\ \xi_2^{(m-1)} \end{pmatrix} \begin{matrix} \uparrow \\ m \\ \downarrow \end{matrix}$$

$\leftarrow N \rightarrow$

satisfies

$$\begin{aligned} \langle \xi_2^{(0)}, \xi_2^{(j)} \rangle &= 0 \quad (j=0, 1, \dots, m-1) \\ \langle \xi_2^{(1)}, \xi_2^{(k)} \rangle &= 0 \quad (k=1, 2, \dots, m-1) \end{aligned}$$

where  $\xi_2^{(0)} = (\xi_1^{(0)}, 0)$  and  $\xi_2^{(i)} = (\xi_1^{(i)}, a_{1,i})$  ( $i=1, \dots, m-1$ ). We continue this process, so that we have the following matrix

$$C \begin{pmatrix} a_{0,0} & \cdots & \cdots & \mathbf{0} \\ a_{0,1} & a_{1,1} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,m-1} & a_{1,m-1} & \cdots & a_{m-1,m-1} \end{pmatrix} = \begin{pmatrix} \xi_{m-1}^{(0)} \\ \xi_{m-1}^{(1)} \\ \vdots \\ \xi_{m-1}^{(m-1)} \end{pmatrix}$$

$\leftarrow N+m \rightarrow$

We can express this matrix in the form

$$\begin{pmatrix} C & A \end{pmatrix} = \begin{pmatrix} \xi_{m-1}^{(0)} \\ \xi_{m-1}^{(1)} \\ \vdots \\ \xi_{m-1}^{(m-1)} \end{pmatrix}$$

$\leftarrow N+m \rightarrow$

where  $A$  is the following  $m \times m$  matrix

$$\begin{pmatrix} a_{0,0} & \cdots & \cdots & \mathbf{0} \\ a_{0,1} & a_{1,1} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,m-1} & a_{1,m-1} & \cdots & a_{m-1,m-1} \end{pmatrix}. \tag{2.2}$$

Clearly the matrix (2.2) satisfies

$$\langle \xi_{m-1}^{(i)}, \xi_{m-1}^{(j)} \rangle = 0 \quad (i, j=0, 1, \dots, m-1).$$

Thus this matrix gives a self-orthogonal code. On the other hand, consider

the dual code  $C^\perp$ . Then the same argument can be applied to the dual code  $C^\perp$ . Since  $N=m+n$ , we can express  $C^\perp$  in the form

$$C^\perp = \begin{pmatrix} \eta^{(0)} \\ \eta^{(1)} \\ \vdots \\ \eta^{(n-1)} \end{pmatrix} \begin{matrix} \uparrow \\ n \\ \downarrow \end{matrix} \cdot \\ \leftarrow N \rightarrow$$

We can also obtain a self-orthogonal code from  $C^\perp$  and express in the form

$$(C^\perp \ B)$$

where  $B$  is an  $n \times n$  matrix obtained from  $C^\perp$  as well as  $A$ . To make a self-dual code, we take the following matrix

$$\hat{C} = \begin{pmatrix} C & A & 0 \\ C^\perp & 0 & B \end{pmatrix} \begin{matrix} \uparrow \\ m+n \\ \downarrow \end{matrix} \cdot \\ \leftarrow N+m+n \rightarrow$$

This is a self-dual  $[2N, N]$ -code because  $C^\perp$  is a dual vector space of  $F^N / C$ . Next we assume  $ch(F)=p>2$  and consider an equation

$$X_1^2 + X_2^2 + X_3^2 + \langle \xi^{(0)}, \xi^{(0)} \rangle = 0.$$

Then a theorem of Chevalley-Waring (cf.[3]) shows that this equation have a solution, say  $(a_{0,0}^{(1)}, a_{0,0}^{(2)}, a_{0,0}^{(3)})$ . Further we consider following equations

$$\langle \xi^{(0)}, \xi^{(i)} \rangle + a_{0,0}^{(1)} X_i = 0 \quad (i=1, \dots, m-1).$$

These equations have a solution since the equations are linear. We set a solution as

$$(x_1, \dots, x_{m-1}) = (a_{0,1}, a_{0,2}, \dots, a_{0,m-1}).$$

Then the following matrix

$$\begin{pmatrix} C & \begin{matrix} a_{0,0}^{(1)} & a_{0,0}^{(2)} & a_{0,0}^{(3)} \\ a_{0,1} & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ a_{0,m-1} & \cdots & \mathbf{0} \end{matrix} \end{pmatrix} = \begin{pmatrix} \xi_1^{(0)} \\ \xi_1^{(1)} \\ \vdots \\ \xi_1^{(m-1)} \end{pmatrix} \cdot$$

satisfies

$$\langle \xi_1^{(0)}, \xi_1^{(i)} \rangle = 0 \quad (i=0, 1, \dots, m-1).$$

Next consider

$$X_1^2 + X_2^2 + X_3^2 + \langle \xi_5^{(1)}, \xi_5^{(1)} \rangle = 0.$$

Let  $(a_{1,1}^{(1)}, a_{1,1}^{(2)}, a_{1,1}^{(3)})$  and  $a_{1,j}$  be a solution of

$$\langle \xi_5^{(1)}, \xi_5^{(j)} \rangle + a_{1,1}^{(1)} x_j = 0 \quad (j=1, 2, \dots, m-1).$$

Then the following matrix

$$\begin{pmatrix} \xi_1^{(1)} \\ \xi_1^{(2)} \\ \vdots \\ \xi_1^{(m-1)} \end{pmatrix} \begin{pmatrix} a_{1,1}^{(1)} & a_{1,1}^{(2)} & a_{1,1}^{(3)} \\ a_{1,2} & 0 & 0 \\ a_{1,2} & \ddots & \vdots \\ a_{1,m-1} & \cdots & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \xi_2^{(1)} \\ \xi_2^{(2)} \\ \vdots \\ \xi_2^{(m-1)} \end{pmatrix},$$

satisfies

$$\langle \xi_2^{(1)}, \xi_2^{(j)} \rangle = 0 \quad (j=1, 2, \dots, m-1).$$

We continue this process, so that we have the following matrix

$$(C \ A) = \begin{pmatrix} \xi_{m-1}^{(0)} \\ \xi_{m-1}^{(1)} \\ \vdots \\ \xi_{m-1}^{(m-1)} \end{pmatrix},$$

where  $A$  is the following  $m \times 3m$  matrix

$$A = \begin{pmatrix} a_{0,0}^{(1)} & a_{0,0}^{(2)} & a_{0,0}^{(3)} & \cdots & \cdots & \mathbf{0} \\ a_{0,1} & 0 & 0 & \cdots & \cdots & \vdots \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{0,m-1} & \cdots & \mathbf{0} & a_{m-1,m-1}^{(1)} & a_{m-1,m-1}^{(2)} & a_{m-1,m-1}^{(3)} \end{pmatrix},$$

which satisfies:

$$\langle \xi_{m-1}^{(i)}, \xi_{m-1}^{(j)} \rangle = 0 \quad (i, j=0, 1, \dots, m-1).$$

Thus this matrix gives a self-orthogonal code. Further we can apply the same method to the dual code  $C^\perp$ . By using the same notation as above, we have a self-orthogonal code for  $C^\perp$

$$\left( \begin{pmatrix} \eta^{(0)} \\ \eta^{(1)} \\ \vdots \\ \eta^{(n-1)} \end{pmatrix} B \right)$$

where  $B$  is an  $n \times 3n$  matrix obtained from  $C^\perp$  as well as  $A$ . For  $k \geq 5$ , consider the following equations

$$f_1(X_1, \dots, X_k) = \sum_{i=1}^k X_i^2 = 0$$

$$f_2(X_1, \dots, X_k) = \sum_{i=1}^{k-1} X_i X_{i+1} = 0$$

Since  $\sum_{i=1}^2 \deg f_i = 4 < k$ , we can use a theorem of Chevalley-Waring again, so that there exists a non-trivial solution

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k).$$

Since  $\alpha$  is non-trivial, we may assume that  $\alpha_1 \neq 0$ . We set

$$M = \begin{pmatrix} \alpha_1 & \cdots & \alpha_k & & \mathbf{0} \\ 0 & \alpha_1 & \cdots & & \\ & & & \ddots & \vdots \\ & & & & \alpha_1 & \cdots & \alpha_k \end{pmatrix} \begin{matrix} \uparrow \\ (k+1)N \\ \downarrow \end{matrix}$$

$\leftarrow \quad 2kN \quad \rightarrow$

Then the following matrix

$$\begin{pmatrix} C & A & 0 & \mathbf{0} \\ C^\perp & 0 & B & \\ \mathbf{0} & & & M \end{pmatrix}$$

gives a self-dual  $[(2k+4)N, (k+2)N]$ -linear code.

Therefore we obtain the following theorem.

**Theorem 1.** *Let  $C$  be a  $[N, m]$ -linear code over a finite field  $F$ . Then there exist a self-dual code  $\hat{C}$  such that  $C$  is embedded in  $\hat{C}$ . More precisely, we can take  $\hat{C}$  as follows:*

- (1) if  $ch(F) = 2$ ,  $\hat{C}$  is self-dual  $[2N, N]$ -linear code.
- (2) if  $ch(F) = p > 2$ , then for any integer  $k \geq 5$ ,  $\hat{C}$  is a self-dual  $[(2k+4)N, (k+2)N]$ -linear code.

3. Grassmann Manifold

In this section, we summarize about Grassmanian manifolds. Let  $N=n+m$  and  $V=V(N)$  be an  $N$ -dimensional vector space over a field  $F$ . Put  $GM(m,V)=\{m\text{-dimensional subspace of } V\}$ . Take a basis  $\{e_0, e_1, \dots, e_{N-1}\}$  of  $V$ . Then  $V=Fe_0 \oplus Fe_1 \oplus Fe_2 \dots \oplus Fe_{N-1}$ . Let  $V^*$  be the dual space of  $V$  and  $\{f_0, f_1, \dots, f_{N-1}\}$  be a dual basis with  $\langle e_i, f_j \rangle = \delta_{i,j}$ , where  $\delta_{ij}$  denotes Kronecker'delta. Let  $V^*=Ff_0 \oplus Ff_1 \oplus \dots \oplus Ff_{N-1}$ . For a subspace  $V_0 \subseteq V$ , define  $V_0^\perp = \{f \in V^* \mid f(V_0) = 0\}$ . Then there is a one to one correspondence between  $V_0$  and  $V_0^\perp$ , so that  $GM(m,V)$  is isomorphic to  $GM(n,V^*)$  as a set. Let  $\wedge^m V$  be the space of  $m$ -th exterior products of  $V$ .  $\wedge^m V$  is the  $\binom{N}{m}$ -dimensional vector space over  $F$  with basis  $\{e_{i_0} \wedge e_{i_1} \wedge \dots \wedge e_{i_{m-1}}; 0 \leq i_0 \leq i_1 \leq \dots \leq i_{m-1} \leq N\}$ . We define the projective embedding of  $GM(m,V)$  as follows:

$$GM(m,V) \rightarrow P(\wedge^m V)$$

$$\xi = \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \mapsto \xi^{(0)} \wedge \dots \wedge \xi^{(m-1)}.$$

For  $\xi \in GM(m,V)$ , we can write  $\xi^{(j)} = \sum_{0 \leq i \leq N} \xi_{ji}^{(j)} e_i$ . Then

$$\xi^{(0)} \wedge \dots \wedge \xi^{(m-1)} = \sum_{0 \leq l_0 < \dots < l_{m-1} \leq N} \xi_{l_0, \dots, l_{m-1}} e_{l_0} \wedge \dots \wedge e_{l_{m-1}}$$

where  $\xi_{l_0, \dots, l_{m-1}}$  is the determinant of the matrix obtained by picking out the  $l_0, \dots, l_{m-1}$  columns of  $\xi$ .

The above projective embedding can be translated as follows:

$$GM(m,V) \rightarrow P^{\binom{N}{m}-1}(F)$$

$$\xi = \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \mapsto (\xi_{l_0, \dots, l_{m-1}})_{0 \leq l_0 < \dots < l_{m-1} \leq N}. \tag{3.1}$$

Further, this projective embedding satisfies the *Plücker* relation

$$\sum_{0 \leq i \leq N} (-1)^i \xi_{k_0, \dots, k_{m-2}, i} \xi_{l_0, \dots, \check{l}_i, \dots, l_m} = 0$$

for

$$0 \leq k_0 < \dots < k_{m-2} < N, 0 \leq l_0 < \dots < l_m \leq N$$



where  $\bar{I}_i$  means removing  $I_i$ .

Let  $C$  be a  $[N, m]$ -linear code which is an element of  $GM(m, V)$  and write

$$C = \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} .$$

Likewise, let

$$C^\perp = \begin{pmatrix} \eta^{(0)} \\ \vdots \\ \eta^{(n-1)} \end{pmatrix} ,$$

which is an element of  $GM(n, V)$ . According to (3.1),  $GM(m, V)$  has a projective embedding into  $\mathbf{P}^{\binom{N}{m}-1}(F)$  and similarly  $GM(n, V)$  has a projective embedding into  $\mathbf{P}^{\binom{N}{n}-1}(F)$ . Since  $\mathbf{P}^{\binom{N}{m}-1}(F) = \mathbf{P}^{\binom{N}{n}-1}(F)$ , we have an easy criterion of self-duality of  $C$  as follows:

**Theorem 2.** *Let  $C$  be a  $[N, m]$ -linear code over a finite field  $F$  and let  $C^\perp$  be the dual code of  $C$ . Assume that  $C$  and  $C^\perp$  are as above. Then  $C$  is self-dual if and only if  $(\xi_{I_0, \dots, I_{m-1}})_{0 \leq I_0 < \dots < I_{m-1} \leq N} = (\eta_{s_0, \dots, s_{n-1}})_{0 \leq s_0 < \dots < s_{n-1} \leq N}$  in  $\mathbf{P}^{\binom{N}{m}-1}$  and  $N = 2m$ .*

*Proof.* First assume that  $C$  is a self-dual code. Then since  $C = C^\perp$ , the theorem is clear. Conversely, assume that  $(\xi_{I_0, \dots, I_{m-1}})_{0 \leq I_0 < \dots < I_{m-1} \leq N} = (\eta_{s_0, \dots, s_{n-1}})_{0 \leq s_0 < \dots < s_{n-1} \leq N}$  in  $\mathbf{P}^{\binom{N}{m}-1}$  and  $N = 2m$ . Then clearly  $(\xi^{(0)} \wedge \dots \wedge \xi^{(m-1)}) = (\eta^{(0)} \wedge \dots \wedge \eta^{(n-1)})$  and  $\xi^{(0)} \wedge \dots \wedge \xi^{(m-1)} = a\eta^{(0)} \wedge \dots \wedge \eta^{(n-1)}$  for some non zero element  $a$  of  $F$ . Hence  $\xi^{(0)} \wedge \dots \wedge \xi^{(m-1)} \wedge \eta^{(i)} = a\eta^{(0)} \wedge \dots \wedge \eta^{(i)} \wedge \eta^{(n-1)} \wedge \eta^{(i)} = 0$  ( $i = 0, \dots, m-1$ ), that is  $\eta^{(i)} \in F\xi^{(0)} \oplus \dots \oplus F\xi^{(m-1)}$ . Similarly, we have  $\xi^{(i)} \in F\eta^{(0)} \oplus \dots \oplus F\eta^{(n-1)}$ . This implies that  $F\xi^{(0)} \oplus \dots \oplus F\xi^{(m-1)} = F\eta^{(0)} \oplus \dots \oplus \eta^{(n-1)}$  and we have  $C = C^\perp$ .

#### 4. Self-duality of linear codes

In this section, we shall study self-orthogonal (resp. self-dual) codes in the Grassmann manifolds.

**Theorem 3.** *Let  $C = F\xi^{(0)} \oplus \dots \oplus F\xi^{(m-1)}$  be a  $[N, m]$ -linear code over a finite field  $F$ . Then  $C$  is a self-orthogonal (resp. self-dual) code if and only if  $C$  is a point of the Grassmann manifolds which satisfies the Plücker's relations and is on the quadratic surface defined by*

$$\sum_{0 \leq I_0 < \dots < I_{m-1} \leq N} \xi_{I_0, \dots, I_{m-1}}^2 = 0 \quad (\text{resp. further } N = 2m),$$

where  $\xi_{l_0, \dots, l_{m-1}}$  is the determinant of the matrix obtained by picking out the  $m$  columns  $l_0, \dots, l_{m-1}$  of  $C$ .

Proof. As explained in the previous section,  $C$  can be thought as a point of the Grassmann manifolds which satisfies the *Plücker's* relations. So we must prove that  $C$  is self-orthogonal if and only if  $C$  is on the quadratic surface defined as above. First assume that  $C$  is a self-orthogonal code. Let

$$C = \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \begin{matrix} \uparrow \\ m \\ \downarrow \end{matrix} \\ \leftarrow N \rightarrow$$

Since  $C$  is contained in  $C^\perp$ , we have

$$\begin{matrix} \uparrow \\ m \\ \downarrow \end{matrix} \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \begin{pmatrix} {}^t\xi^{(0)} & \dots & {}^t\xi^{(m-1)} \end{pmatrix} \begin{matrix} \uparrow \\ N \\ \downarrow \end{matrix} = 0, \\ \leftarrow N \rightarrow \qquad \leftarrow m \rightarrow$$

where  ${}^t\xi^{(i)}$  is the transpose of  $\xi^{(i)}$ . Then we have

$$\det \left\{ \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \begin{pmatrix} {}^t\xi^{(0)} & \dots & {}^t\xi^{(m-1)} \end{pmatrix} \right\} = 0.$$

In this case, Binet-Cauchy formula (cf.[1]) implies

$$\begin{aligned} & \det \left\{ \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{pmatrix} \begin{pmatrix} {}^t\xi^{(0)} & \dots & {}^t\xi^{(m-1)} \end{pmatrix} \right\} \\ &= \sum_{\square} \det(\square) \det(\square) \\ &= \sum_{\square} \det \square \square \\ &= \sum \xi_{l_0, \dots, l_{m-1}}^2 = 0 \end{aligned}$$

where  $\square$  is an  $m \times m$  matrix obtained by picking out  $m$  columns of  $C$  and summation is taken over all  $m \times m$  matrices.

Conversely, we assume that

$$\sum \xi_{i_0 \dots i_{m-1}}^2 = 0.$$

Then Binet-Cauchy formula implies

$$\det \left\{ \left( \begin{array}{c} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{array} \right) \left( \begin{array}{ccc} {}_t\xi^{(0)} & \dots & {}_t\xi^{(m-1)} \end{array} \right) \right\} = 0$$

since

$$\begin{aligned} & \det \left\{ \left( \begin{array}{c} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{array} \right) \left( \begin{array}{ccc} {}_t\xi^{(0)} & \dots & {}_t\xi^{(m-1)} \end{array} \right) \right\} \\ &= \det \left( \begin{array}{ccc} \langle \xi^{(0)}, \xi^{(0)} \rangle, & \dots, & \langle \xi^{(0)}, \xi^{(m-1)} \rangle \\ \vdots & \dots & \vdots \\ \langle \xi^{(m-1)}, \xi^{(0)} \rangle, & \dots, & \langle \xi^{(m-1)}, \xi^{(m-1)} \rangle \end{array} \right) = 0 \end{aligned}$$

where  $\langle \cdot, \cdot \rangle$  means canonical inner product in  $F^N$ .

This shows that for any  $i$  ( $i=0, \dots, m-1$ ),

$$X_0 \langle \xi^{(0)}, \xi^{(i)} \rangle + \dots + X_{m-1} \langle \xi^{(m-1)}, \xi^{(i)} \rangle = 0$$

has a non-trivial solution  $(\lambda_0, \dots, \lambda_{m-1})$ . In particular,

$$\langle \lambda_0 \xi^{(0)} + \dots + \lambda_{m-1} \xi^{(m-1)}, \xi^{(i)} \rangle = 0$$

so that

$$\lambda_0 \xi^{(0)} + \dots + \lambda_{m-1} \xi^{(m-1)}$$

is contained in  $C \cap C^\perp$ . We set

$$\eta^{(m-1)} = \lambda_0 \xi^{(0)} + \dots + \lambda_{m-1} \xi^{(m-1)}$$

which satisfies

$$\langle \xi^{(i)}, \eta^{(m-1)} \rangle = 0 \quad (i=0, \dots, m-1).$$

By renumbering  $\lambda_0, \dots, \lambda_{m-1}$ , we may assume that  $\lambda_{m-1} \neq 0$ . We claim that

$$\xi^{(0)}, \dots, \xi^{(m-2)}, \eta^{(m-1)}$$

are linearly independent over  $F$ . Assume that

$$a_0 \xi^{(0)} + \dots + a_{m-2} \xi^{(m-2)} + a_{m-1} \eta^{(m-1)} = 0$$

for  $a_0, \dots, a_{m-1} \in F$ . Then

$$a_0 \xi^{(0)} + \dots + a_{m-2} \xi^{(m-2)} + a_{m-1} (\lambda_0 \xi^{(0)} + \dots + \lambda_{m-1} \xi^{(m-1)}) = 0.$$

Since  $\xi^{(0)}, \dots, \xi^{(m-1)}$  are linearly independent, we have

$$a_i + a_{m-1} \lambda_i = 0 \quad (i=0, \dots, m-1), \quad a_{m-1} \lambda_{m-1} = 0.$$

Since  $\lambda_{m-1} \neq 0$ , we have that  $a_{m-1} = 0$ . Thus we obtain

$$a_0 \xi^{(0)} + \dots + a_{m-2} \xi^{(m-2)} = 0.$$

Since  $\xi^{(0)}, \dots, \xi^{(m-2)}$  are linearly independent, we have

$$a_0 = \dots = a_{m-2} = 0.$$

This shows that  $\xi^{(0)}, \dots, \xi^{(m-2)}, \eta^{(m-1)}$  are linearly independent.

Now  $\{\xi^{(0)}, \dots, \xi^{(m-2)}, \eta^{(m-1)}\}$  becomes a basis of  $C$ . Since

$$\langle \eta^{(m-1)}, \xi^{(i)} \rangle = 0 \quad (i=0, \dots, m-1),$$

we know

$$\det \left\{ \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-2)} \\ \eta^{(m-1)} \end{pmatrix} \left( {}^t \xi^{(0)}, \dots, {}^t \xi^{(m-2)}, {}^t \eta^{(m-1)} \right) \right\} = 0$$

which implies

$$\begin{aligned} & \det \left\{ \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-2)} \\ \eta^{(m-1)} \end{pmatrix} \left( {}^t \xi^{(0)}, \dots, {}^t \xi^{(m-2)}, {}^t \eta^{(m-1)} \right) \right\} \\ &= \det \left\{ \begin{pmatrix} \xi^{(0)} \\ \vdots \\ \xi^{(m-2)} \end{pmatrix} \left( {}^t \xi^{(0)} \dots {}^t \xi^{(m-1)} \right) \right\} = 0. \end{aligned}$$

By the same argument, we see that there exists a non-trivial solution

$$(\mu_0, \dots, \mu_{m-2}) \in F^{m-1}$$

such that

$$\langle \mu_0 \xi^{(0)} + \dots + \mu_{m-2} \xi^{(m-2)}, \xi^{(i)} \rangle = 0 \quad (i=0, \dots, m-2).$$

We set

$$\eta^{(m-2)} = \mu_0 \xi^{(0)} + \cdots + \mu_{m-2} \xi^{(m-2)}$$

which satisfies

$$\langle \xi^{(i)}, \eta^{(m-2)} \rangle = 0 \quad (i=0, \dots, m-2), \quad \langle \eta^{(m-1)}, \eta^{(m-2)} \rangle = 0.$$

Similarly,

$$\{\xi^{(0)}, \dots, \xi^{(m-3)}, \eta^{(m-2)}, \eta^{(m-1)}\}$$

becomes a basis of  $C$ . We proceed this process. Then we obtain a basis

$$\{\eta^{(0)}, \dots, \eta^{(m-1)}\}$$

which satisfies

$$\langle \eta^{(i)}, \eta^{(j)} \rangle = 0 \quad (i, j=0, \dots, m-1).$$

Now  $C$  becomes a self-orthogonal code. Since the case of a self-dual code is clear, the proof is complete.

---

#### References

- [1] S. Lang: Linear Algebra, Springer, New York, 1987.
- [2] J.H. van Lint, G. van der Geer: Introduction to Coding Theory and Algebraic Geometry, Birkhäuser, Basel, 1988.
- [3] J.-P. Serre: Cours d'Arithmétique, P. U. France, 1970.

Department of Mathematics  
 Naruto University of Education  
 Takashima, Naruto, 772, Japan  
 e-mail address: skoba@naruto-u.ac.jp  
 and  
 Department of Mathematics  
 Tokushima University  
 Tokushima, 770, JAPAN  
 e-mail address: g01536@sinet.ad.jp