

The submanifold of self-dual codes in a Grassmann manifold

Shigeru Kobayashi (小林 滋)

Naruto University of Education

1 Introduction

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

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 . In this section we shall construct a self-dual code which contains C . It may be well known, but this is a motive for studying self-dual code, so we shall give a proof. Since C can be thought as a subspace of F^N , we can write

$$C = \left(\begin{array}{c} \xi^{(0)} \\ \vdots \\ \xi^{(m-1)} \end{array} \right) \begin{array}{c} \uparrow \\ m \\ \downarrow \end{array} \\ \leftarrow N \rightarrow$$

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

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

where $\langle \cdot, \cdot \rangle$ means the inner product of F^N . Since the Frobenius map $x \rightarrow x^2$ is an automorphism of F , the equation (1) has solution, say $X = a_{00}$. 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 have solutions, say $X_i = a_{0,i}$ ($i = 0, \dots, m-1$). Now the following matrix

$$\left(\begin{array}{cc} \xi^{(0)} & a_{0,0} \\ \xi^{(1)} & a_{0,1} \\ \vdots & \vdots \\ \xi^{(m-1)} & a_{0,m-1} \end{array} \right) = \left(\begin{array}{c} \xi_1^{(0)} \\ \xi_1^{(1)} \\ \vdots \\ \xi_1^{(m-1)} \end{array} \right) \begin{array}{c} \uparrow \\ m \\ \downarrow \end{array} \\ \leftarrow N \rightarrow$$

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

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

$\longleftarrow N \longrightarrow$

satisfies

$$\begin{aligned} \langle \xi_2^{(0)}, \xi_2^{(j)} \rangle &= 0 \quad (j = 0, 1, \dots, m-1) \\ \langle \xi_2^{(1)}, \xi_2^{(k)} \rangle &= 0 \quad (k = 1, 2, \dots, m-1) \end{aligned} \quad (2.9)$$

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

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

$\longleftarrow N+m \longrightarrow$

We can express this matrix in the form

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

$\longleftarrow N+m \longrightarrow$

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

$$\begin{pmatrix} a_{0,0} & \cdots & \cdots & 0 \\ a_{0,1} & a_{1,1} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,m-1} & a_{1,m-1} & \cdots & a_{m-1,m-1} \end{pmatrix} \quad (2)$$

Clearly matrix (2) satisfies

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

Thus this matrix become self-orthogonal code. On the other hand, consider the dual code $C^\perp$, then the same argument can apply to the dual code $C^\perp$. Since $N = m + n$, We can express $C^\perp$ in the form

$$C^\perp = \left(\begin{array}{c} \eta^{(0)} \\ \eta^{(1)} \\ \vdots \\ \eta^{(n-1)} \end{array} \right) \begin{array}{c} \uparrow \\ n \\ \downarrow \end{array}$$

$\leftarrow N \rightarrow$

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

$$\left(\begin{array}{cc} C^\perp & B \end{array} \right)$$

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

$$\hat{C} = \left(\begin{array}{ccc} C & A & 0 \\ C^\perp & 0 & B \end{array} \right) \begin{array}{c} \uparrow \\ m+n \\ \downarrow \end{array}$$

$\leftarrow N + m + n \rightarrow$

This is a self-dual $[2N, N]$ code because that C and $C^\perp$ are linearly independent.

Similarly, we can obtain a self-dual code in the case $vh(F) = p > 0$, so 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 contained in $\hat{C}$. More precisely,*

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

3 Self-duality of linear codes

Let $N = n + m$ and $V = V(N)$ be a N - dimensional vector space over a field F . Put $GM(m, V) = \{m\text{-dimensional subspace of } V\} / \sim$. $\xi \sim \xi'$ (where ξ and ξ' are m - dimensional vector subspace of V) means $\xi = h\xi'$ for some $h \in GL(m, F)$. Take basis $\{e_0, e_1, \dots, e_{N-1}\}$ of V , then $V = Fe_0 \oplus Fe_1 \oplus Fe_2 \oplus \dots \oplus Fe_{N-1}$. Let V^* be the dual space of V and $\{f_0, f_1, \dots, f_{N-1}\}$ be an dual basis, then $V^* = Kf_0 \oplus Kf_1 \oplus Kf_{N-1}$. We have an canonical map $\langle e_i, f_j \rangle = \delta_{ij}$, where δ_{ij} means Kronecker'delta. For a subspace $V_0 \subseteq V$, define $V_0^\perp = \{\eta \in V, \eta = \sum b_i f_i \mid \sum a_i b_i = 0 \text{ for all } \sum a_i b_i \in V_0\}$, then there is a one to one correspondence between V_0 and $V_0^\perp$, so $GM(m, V)$ is isomorphic to $GM(n, V^*)$ as a vector space. 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 $\{e_{i_0} \wedge e_{i_1} \wedge \dots \wedge e_{i_{m-1}}; \ 0 \leq i_0 \leq i_1 \leq \dots \leq i_{m-1} \leq N\}$. Now we can define the projective embedding of $GM(m, V)$ as follows,

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

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

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 matrix obtained by picking out $l_0, \dots, l_{m-1}$ columns of ξ .

Now above projective embedding can translate as follows

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

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

Further, this projective embedding satisfies the *Plücker* relation.

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

for

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

where $\check{l}_i$ means removing l_i .

Let C be a $[N, m]$ -linear code and write

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

then C can be an element of $GM(m, V)$. Likewise, let

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

then $C^\perp$ also can be an element of $GM(n, V)$. Since $\wedge^m V$ and $\wedge^n V$ are isomorphic as a vector space, $\mathbf{P}(\wedge^m V)$ and $\mathbf{P}(\wedge^n V)$ are isomorphic, so we can identify C and $C^\perp$ as an element of Projective space. Thus we assume that $C = (\xi^{(0)} \wedge \dots \wedge \xi^{(m-1)})$ and $C^\perp = (\eta^{(0)} \wedge \dots \wedge \eta^{(n-1)})$. We shall give a self-orthogonality (resp. self-duality) of linear codes.

Theorem 2 *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 self-orthogonal (resp. self-dual) code if and only if C is a point of Grassmann manifold satisfies the Plücker's relations and is on the quadratic surface defined by*

$$\sum_{0 \leq l_0 < \dots < l_{m-1} \leq N} \xi_{l_0, \dots, l_{m-1}}^2 = 0 \quad (\text{resp. further } N = 2m)$$

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

References

- [1] S.Kobayashi, I.Takada, *The submanifold of self-dual codes in a Grassmann manifold*, Osaka J. Math. **32** (1995), 1001-1012
- [2] S. Lang. Linear Algebra, Springer, New York, 1987
- [3] J.H. van Lint, G. van der Geer, Introduction to Coding Theory and Algebraic Geometry, Birkhäuser, Basel, 1988
- [4] J.-P. Serre. Cours d'Arithmetique, P. U. France., 1970