Regular Representations of Codes and Duality

Kôji UCHIDA

Graduate School of Information Sciences, Tohoku University,
Katahira, Aoba-Ku, 980-77, Sendai, Japan

Received March 5, 1995; final version accepted June 5, 1995

Let $K/F$ be finite fields with $[K:F] = m$. Let $\{u_1, \ldots, u_m\}$ be a basis of this extension. By the regular representation with this basis, every element of $K$ corresponds to an $m \times m$ matrix over $F$. Applying this representation, every linear code over $K$ induces a linear code over $F$. Another code may be induced by another basis. We study the condition of the basis which preserves duality, and also we show the existence of such a basis for any extension.

KEYWORDS: Linear code, Regular representation, Duality, Orthogonal basis

1. Introduction

Let $F$ be a finite field and let $K$ be an extension of $F$ of degree $m$. Let $C$ be a linear code defined over $K$. We know methods deriving codes over $F$ from $C$, i.e., concatenation and (as a special case of concatenation) subfield descent. Let $\{u_1, \ldots, u_m\}$ be a basis of $K$ over $F$. Then every element $\alpha$ of $K$ is uniquely represented as

$$\alpha = a_1 u_1 + \cdots + a_m u_m, \quad a_i \in F.$$

The subfield descent of $C$ is defined as the set of code words

$$\{ a_{11}, \ldots, a_{1m}, a_{21}, \ldots, a_{nm} \},$$

when $\{ \alpha_1, \ldots, \alpha_n \}$ are code words of $C$ such that $\alpha_i = a_1 u_1 + \cdots + a_m u_m$. Usually a basis of type $\{1, \beta_1, \ldots, \beta^{m-1}\}$ is chosen, but the choice of different bases may cause different codes as seen below, so it is worth studying the choice of the basis.

We fix a basis $\{ u_1, \ldots, u_m \}$ of $K/F$. Let $\alpha$ be any element of $K$. By the regular representation of $K$ with respect to this basis, $\alpha$ corresponds to an $m \times m$ matrix $A = (a_{ij})$ over $F$ such that $\alpha (u_1, \ldots, u_m) = (u_1, \ldots, u_m) A$, i.e.,

$$\alpha u_j = a_{ij} u_1 + \cdots + a_{mj} u_m, \quad a_{ij} \in F.$$

We can define an $F$-linear isomorphism $\phi$ of $K^n$ onto $F^m$ as follows. Let $v = (\alpha_1, \ldots, \alpha_n)$ be any element of $K^n$. Let $A_i$ be matrices corresponding to $\alpha_i$ by the regular representation. Then $\phi(v)$ is the first row of the $m \times mn$ matrix $(A_1, A_2, \cdots, A_n)$. As det $A_i \neq 0$ for $\alpha_i \neq 0$, the first row of such $A_i$ has at least one nonzero component. This shows the $F$-linear homomorphism $\phi$ is one-to-one, and $\phi$ maps $K^n$ onto $F^m$. For any linear code $C$ over $K$, we obtain a linear code $C_1 = \phi(C)$ over $F$. We call $C_1$ a (regular) representation of $C$ over $F$. If $C$ is an $(n, k)$ code, $C_1$ is an $(mn, mk)$ code. The minimal distance of $C_1$ is not smaller than the minimal distance of $C$.

Theorem 1. $C_1$ consists of all the rows of $(A_1 A_2 \cdots A_n)$ corresponding to code words $(\alpha_1, \ldots, \alpha_n)$ of $C$. If $(\alpha_{ij})$ is a generating $k \times n$ matrix of $C$, and if $A_{ij}$ correspond to $\alpha_{ij}$ by the representation, the $mk \times mn$ matrix $(A_{ij})$ is a generating matrix of $C_1$.

Proof. Let $v = (\alpha_1, \ldots, \alpha_n)$ be a non-zero element of $C$. Let $(A_1 A_2 \cdots A_n)$ be the corresponding matrix. Let $B$ be an element of $K$ which corresponds to the matrix $B$. Then the code word $\beta(\alpha_1, \ldots, \alpha_n)$ corresponds to the matrix $(A_1 B A_2 \cdots B A_n)$, whose first row is a linear combination over $F$ of rows of $(A_1 A_2 \cdots A_n)$. This shows that $\phi$ maps the $K$-subspace of $K^n$ generated by $v$ into the $F$-subspace generated by all rows of $(A_1 A_2 \cdots A_n)$. As they have the same dimension as $F$-space, this restriction of $\phi$ is surjective. We can assume that the $k \times k$ matrix consisting of the first $k$ columns of $(\alpha_{ij})$ has a non-zero determinant. Let $(\beta_{ij})$ be its inverse, and let $B_{ij}$ correspond to $\beta_{ij}$. Then $mk \times mk$ matrix $(B_{ij})$ is the inverse of $(A_{ij})$ $(1 \leq i, j \leq k)$. This shows $(A_{ij})$ has the rank $mk$ and it is a generating matrix of $C_1$.

One finds another code $C_2$ over $F$ if $(A_1 A_2 \cdots A_n)$ is substituted for $(A_1 A_2 \cdots A_n)$, where $A_j$ is the transpose of $A_j$. $C_2$ is called a transposed representation of $C$. A code word of $C_2$ consists of $(a_{11}^{(1)} a_{11}^{(2)} \cdots a_{1m}^{(1)} a_{1m}^{(2)} \cdots a_{mn}^{(m)})$, where $a_{1i} = a_{i1}^{(1)} u_1 + \cdots + a_{im}^{(m)} u_m$ for $(\alpha_1, \ldots, \alpha_n) \in C$. Hence the above word corresponds to $u_1 (\alpha_1, \ldots, \alpha_n)$ by the subfield descent. That is, $C_2$ is the subfield descent of $C$ by the basis $(u_1, \ldots, u_m)$. Let $C^\perp$ be the dual code of $C$ and let $\{ \beta_1, \ldots, \beta_n \}$ be any element of $C^\perp$. Then

$$\alpha_1 \beta_1 + \cdots + \alpha_n \beta_n = 0$$
for any \( \{ \alpha_1, \ldots, \alpha_n \} \in C \) shows
\[
A_1 B_1 + \cdots + A_n B_n = 0
\]
for representation matrices, which proves the next theorem.

**Theorem 2.** Let \( K \) be a finite field and let \( F \) be a subfield. We fix a basis \( \{ u_1, \ldots, u_m \} \). Let \( C \) be a linear code over \( K \) and \( C_1 \) the regular representation of \( C \) over \( F \). Then the dual code of \( C_1 \) is the transposed representation of \( C^\perp \).

**Remark.** One of the referees kindly pointed out to the author that he should refer to the book of MacWilliams and Sloane [M, S]. The companion matrix in p. 106 of this book may also be used to define the regular representation. The effect of changing the basis is also analyzed (pp. 298–301).

We call a regular representation symmetric if every representation matrix is symmetric. If \( \{ u_1, \ldots, u_m \} \) is a basis of \( K/F \) which causes a symmetric representation, \( C_1 = C_2 \) and the above theorem show that representations of dual codes are also duals. Especially the representation of a self dual code by such a basis is also a self dual code. We will use the notation \( C_0 \) instead of \( C_1 \) or \( C_2 \) in this case. We will see in the next section that every extension of the finite field has such a basis. In this section we see some examples.

**Example 1.** Let \( F = F_7 \) be the prime field of characteristic 2. Let \( K \) be generated over \( F \) by \( \alpha \) such that \( \alpha^3 + \alpha + 1 = 0 \). Let \( C \) be a \((3, 1, 3)\) code generated by \((1, \alpha, \alpha^2)\). If one chooses a basis \((1, \alpha, \alpha^2)\) of \( K/F \), representation matrices are
\[
\alpha \rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \alpha^2 \rightarrow \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}
\]
Hence \( C_1 \) is generated by the matrix
\[
\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix},
\]
whose weight distribution is \((1, 0, 0, 1, 2, 1, 1, 2, 0, 0)\). That is, \( C_1 \) is a \((9, 3, 3)\) code. We see \( C_2 \) has the same weight distribution. If one chooses another basis \((1, \alpha + 1, \alpha^2)\), the representation is symmetric and the generating matrix is
\[
\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},
\]
In this case, the weight distribution is \((1, 0, 0, 0, 2, 3, 1, 1, 0, 0)\). This code is a \((9, 3, 4)\) code.

**Example 2.** We can obtain the Golay \((24, 12, 8)\) code from the Reed-Solomon \((8, 4, 5)\) code \( C \) over the field \( F_8 \) with 8 elements. We can choose the basis in example 1, but we here choose another basis \((\alpha, \alpha^2, \alpha^3)\) for \( \alpha^3 + \alpha^2 + 1 = 0 \). For this choice of the basis, see section 3 below. A generating (and also a parity check) matrix of the RS code has \((i, j)\) components \( \alpha^{(i-1)(j-1)} \) for \( j \leq 7 \) and the last column is \((1, 0, 0, 0)\). We have \( \alpha^2 = \alpha^2 + 1, \alpha^3 = \alpha^2 + \alpha + 1, \alpha^j = \alpha + 1, \alpha^k = \alpha^2 + \alpha, \alpha^7 = 1 \). Representation matrices are
\[
\alpha \rightarrow A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \alpha^2 \rightarrow A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}
\]
Then the representation \( C_0 \) has the generating matrix
\[
G_0 = \begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\]
\[
\begin{array}{cccccccccccc}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
\end{array}
\]

\(C_8\) has the minimal weight not smaller than 5. As \(C\) is self dual, so is \(C_8\). As every row of \(G_0\) has a weight multiple of 4, the minimal weight of \(C_8\) is also a multiple of 4. Then it is not smaller than 8. This shows \(C_8\) is in fact the Golay code.

**Example 3.** In this and in the next examples, we obtain the Golay (12, 6, 6) code by representations from different fields. Let \(F\) be the prime field of characteristic 3. The extension field of degree 3 is generated by an element \(\alpha\) satisfying the equation \(X^3 + X^2 - 1 = 0\). Other roots of this equation are \(\alpha^2 = 1 - \alpha^2\) and \(\alpha^3 = 1 - \alpha + \alpha^2\), and \(\alpha\) is a 13th root of unity. The representation with the basis \(\{\alpha, \alpha^2, \alpha^3\}\) gives correspondence

\[
\alpha \rightarrow A = \begin{pmatrix}
-1 & 1 & -1 \\
1 & -1 & 0 \\
-1 & 0 & 1
\end{pmatrix}, \quad \alpha^2 \rightarrow A^2 = \begin{pmatrix}
0 & 1 & 0 \\
1 & -1 & -1 \\
0 & -1 & -1
\end{pmatrix}.
\]

Let \(C\) be a self dual code with a generating matrix

\[
G = (E_6 | B) = \begin{pmatrix}
1 & 0 & -\alpha & \alpha^0 \\
0 & 1 & \alpha^0 & \alpha
\end{pmatrix} = \begin{pmatrix}
1 & 0 & -\alpha & 1 + \alpha + \alpha^2 \\
0 & 1 & 1 + \alpha + \alpha^2 & \alpha
\end{pmatrix}.
\]

The representation \(C_8\) has the generating matrix \(G_0 = (E_6 | B_0)\) with

\[
B_0 = \begin{pmatrix}
1 & -1 & 1 & 0 & -1 & -1 \\
-1 & 1 & 0 & -1 & -1 & -1 \\
1 & 0 & -1 & -1 & -1 & 1 \\
0 & -1 & -1 & -1 & 1 & -1 \\
-1 & -1 & -1 & 1 & 1 & 0 \\
-1 & -1 & 1 & -1 & 0 & 1
\end{pmatrix}.
\]

As \(C_8\) is self-dual, its minimal weight is a multiple of 3. If we check it is not 3, the minimal weight is at least 6 and \(C_8\) is the Golay code. Every row of \(G_0\) has weight 6. Every linear combination of two rows has two nonzero components in the first 6 columns, and at least two nonzero components in the last 6 columns because \(B_0\) has one zero in every row in different columns. This shows the weight is at least 4 in this case. As \(B^{-1} = -B\), we know \(B_0^{-1} = -B_0\). Every linear combination of at least three rows of \(G_0\) has at least 3 nonzero components in the first 6 columns. As \(\det B_0 \neq 0\), at least one component of the last 6 columns is nonzero, i.e., the weight is at least 4. This shows \(C_8\) is in fact the Golay code.

**Example 4.** Let \(i^2 = -1\). Then \(i\) generates \(F_5\). A matrix

\[
G = \begin{pmatrix}
1 & 1 & i & -i & 0 & 0 \\
0 & 0 & 1 & 1 & i & -i \\
i & -i & 0 & 0 & 1 & 1
\end{pmatrix}
\]

generates a self-dual (6, 3, 4) code \(C\). We note that this matrix generates a self-dual code for any field of characteristic \(\neq 2\). Let \(C_0\) be the representation with the basis \((1, i - 1)\). Then \(C_0\) is a (12, 6) self-dual code with the minimal weight at least 4. As the minimal weight is a multiple of 3, it must be at least 6, and we obtain the Golay code.

2. Orthogonal basis for the extension of a finite field

We want to find the conditions when a basis of a field extension induces a symmetric regular representation.

**Definition.** Let \(F\) be a finite field and let \(K\) be an extension of \(F\) of degree \(m\). Let \(\{u_1, \ldots, u_m\}\) be a basis of \(K/F\). This basis is called an orthogonal basis if it is orthogonal with any conjugate basis, i.e.,

\[
u_i \sigma(u_i) + \cdots + u_m \sigma(u_m) = 0,
\]

for any element \(\sigma \neq id\) of the Galois group of \(K/F\). Then we obtain

\[
\sigma(u_1) \tau(u_1) + \cdots + \sigma(u_m) \tau(u_m) = 0,
\]

for any two elements \(\sigma \neq \tau\) of the Galois group.
The Galois group has $m$ elements. For any order of them, we use the notation $\alpha^{(i)}$ for the $i$-th conjugate of an element $\alpha$ of $K$. We usually assume that $\alpha^{(i)} = \alpha$. For any basis $\{u_1, \ldots, u_m\}$, we define a matrix $P$ with rows consisting of conjugate bases, i.e.,

$$
P = \begin{pmatrix}
\alpha^{(1)} \\
\alpha^{(2)} \\
\vdots \\
\alpha^{(m)}
\end{pmatrix}
\begin{pmatrix}
u_1^{(1)} & u_2^{(1)} & \cdots & u_m^{(1)} \\
u_1^{(2)} & u_2^{(2)} & \cdots & u_m^{(2)} \\
\vdots & \vdots & \ddots & \vdots \\
u_1^{(m)} & u_2^{(m)} & \cdots & u_m^{(m)}
\end{pmatrix}
$$

It is known that $\det P \neq 0$ [L]. For any element $\alpha$ of $K$, we define a diagonal matrix $Q(\alpha)$ by

$$
Q(\alpha) = \begin{pmatrix}
\alpha^{(1)} \\
\alpha^{(2)} \\
\vdots \\
\alpha^{(m)}
\end{pmatrix}
$$

**Theorem 3.** Let $K/F$ be finite fields and let $\{u_1, \ldots, u_m\}$ be a basis. The necessary and sufficient condition for $\{u_1, \ldots, u_m\}$ to give a symmetric regular representation is that $\{u_1, \ldots, u_m\}$ is an orthogonal basis.

**Proof.** Let $\{u_1, \ldots, u_m\}$ be orthogonal. Then the matrix $R = P^{-1}P$ is a diagonal matrix whose diagonal components are conjugates of $\alpha = u_1^t + \cdots + u_n^t$. As $\det R = (\det P)^2 \neq 0$, $\alpha$ is not zero. Matrices $A_k = P^tQ(u_k)P$ are symmetric matrices over $F$ because their components are $Tr(u_iu_ku_l)$. As the first rows of $R^tQ(u_k)P = PA_k$ are

$$
\alpha u_k(u_1, \ldots, u_m) = (u_1, \ldots, u_m)A_k,
$$

$\{\alpha u_1, \ldots, \alpha u_m\}$ correspond to symmetric matrices by the representation given by the basis $\{u_1, \ldots, u_m\}$. As $\{\alpha u_1, \ldots, \alpha u_m\}$ is also a basis of $K/F$, this representation is symmetric. We now assume the representation given by the basis $\{u_1, \ldots, u_m\}$ is symmetric. Let $\alpha$ be an element of $K$ which generates $K$ over $F$. Let $A$ be the matrix over $F$ corresponding to $\alpha$ by the regular representation with the basis $\{u_1, \ldots, u_m\}$. Then $A^tP = (P^tA) = t(Q(\alpha)P) = tPQ(\alpha)$, and this shows

$$
Q(\alpha)P^tP = PA^tP = P^tPQ(\alpha),
$$

i.e., $Q(\alpha)$ and $PP$ are commutative. As $Q(\alpha)$ is diagonal and diagonal components differ from each other, $PP$ also must be diagonal. This shows the basis $\{u_1, \ldots, u_m\}$ is orthogonal.

**Proposition 4.** Let $F \subset K \subset L$ be finite fields. Let $\{u_1, \ldots, u_m\}$ be an orthogonal basis of $L/K$, and let $\{v_1, \ldots, v_n\}$ be an orthogonal basis of $K/F$. Then

$$
\{u_1v_1, \ldots, u_1v_n, u_2v_1, \ldots, u_nv_n\}
$$

is an orthogonal basis of $L/F$.

**Proof.** Let $\sigma (\neq id)$ be any automorphism of $L/F$. If the restriction of $\sigma$ on $K$ is the identity, $\sigma$ is a non-identical automorphism of $L/K$. Then $\sigma(u_i) = 0$ and we have

$$
\sum_{ij} u_i v_j \sigma(u_i) \sigma(v_j) = \sum_j v_j \cdot \sum_i u_i \cdot \sigma(u_i) = 0.
$$

If $\sigma$ is not identical on $K$, we have $\sigma(v_j) = 0$ and

$$
\sum_{ij} u_i v_j \sigma(u_i) \sigma(v_j) = \sum_i u_i \sigma(u_i) \cdot \sum_j v_j \sigma(v_j) = 0.
$$

**Proposition 5.** Any extension of degree $2^m$ has an orthogonal basis.

**Proof.** Such an extension is obtained as a sequence of extensions of degree 2. Hence we only need to prove the existence of an orthogonal basis for every extension of degree 2. If the characteristic is 2, every extension of degree 2 is generated by a solution $\alpha$ of the Artin-Schreier equation $X^2 + X + a = 0$. Here $a \in F$ and $a \neq b^2 + b$ for any $b \in F$. The pair $(a, a + a)$ is a basis of this extension. As $\alpha^{(1)} + \alpha^{(2)} = 1$ and $\alpha^{(1)} + \alpha^{(2)} = a$, we have $a^2 + (\alpha^{(1)} + \alpha^{(2)} + a)^2 = 0$. That is, $(a, a + a)$ is an orthogonal basis. If the characteristic is not 2, every extension of degree 2 is a Kummer extension, i.e., generated by a solution $\alpha$ of an equation $X^2 - a = 0$, where $a \in F$ is not a square in $F$. As the set of the squares in $F$ is not additively closed, we can find two non-zero elements $b$ and $c$ such that $a = b^2 + c^2$. As

$$
b^2 + (\alpha^{(1)} + c)(\alpha^{(2)} + c) = b^2 - a + c^2 = 0,
$$
(b, α + c) is an orthogonal basis.

**Theorem 6.** There exists an orthogonal basis for any extension of finite field.

**Proof.** We first assume that the characteristic is not 2. By the above propositions we can assume \( m = [K:F] \) is odd. Let \( K \) be generated by an element \( α \). Then \( \{ 1, α, α^2, \ldots, α^{m-1} \} \) is a basis of this extension. Let

\[
Q = \begin{pmatrix}
1 & α^{(1)} & \cdots & α^{(1)(m-1)} \\
1 & α^{(2)} & \cdots & α^{(2)(m-1)} \\
\vdots & \vdots & \ddots & \vdots \\
1 & α^{(m)} & \cdots & α^{(m)(m-1)}
\end{pmatrix}
\]

be a matrix with rows conjugates of the above basis. Let \( ρ \) be a generator of the Galois group, and we assume \( ρ(α^{(i)}) = α^{(i+1)} \) for \( i = 1, \ldots, m - 1 \) and \( ρ(α^{(m)}) = α^{(0)} \). Then \( ρ(\det Q) = (-1)^{m-1} \det Q = \det Q \). This shows \( \det Q \) is an element of \( F \). Therefore the quadratic form with the matrix \( S = Q \cdot Q \) is a non-degenerate quadratic form over \( F \), and its discriminant is a square. Every non-degenerate quadratic form over a finite field is determined up to isomorphism by the dimension \( m \) and the fact the discriminant is square or not [W. Satz 12]. So our quadratic form is isomorphic to the quadratic form given by the identity matrix, i.e., there exists an invertible matrix \( A \) over \( F \) such that \( ASA = E \) (identity). We will see a direct proof of Witt's theorem in our case in the appendix below. Let \( P = QA \). As \( P \) has conjugate rows and as \( det P \neq 0 \), the first row is a basis of \( K/F \). As \( P \cdot P = E, P \cdot P \) is also the identity. This shows the first row of \( P \) is an orthogonal basis of \( K/F \). We next assume that the characteristic is 2. Let \( K/F \) be an extension of degree \( m \geq 2 \). In this case, \( m \) may be even. Let \( S = Q \cdot Q \) as above. We define \( S(x) = x^T S x \) for vectors \( x \in F^m \). Then we have \( S(x) = \sum s_{ij} x_i x_j \). As every element of \( F \) is a square, we can find \( t_i \) such that \( t_i^2 = s_{ii} \). Then we have \( S(x) = (\sum t_i x_i)^2 \). As \( K/F \) is separable, some \( s_{ii} = \text{Tr}(α^{-1})^T \) is non-zero [L]. Let \( H \) be the set of vectors which satisfy \( S(x) = 0 \). \( H \) is an \( m - 1 \) dimensional subspace because it is also the set of the solutions of a non-trivial equation \( \sum t_i x_i = 0 \). For any subspace \( V \) of \( F^m \), \( V^\perp \) denotes the orthogonal of \( V \) with respect to \( S \), i.e.,

\[
V^\perp = \{ x \in F^m : y^T S x = 0 \ \text{for any} \ y \in V \}.
\]

We will find vectors \( \{ c_i, \ldots, c_m \} \) satisfying the following three conditions:

1. They are orthogonal with respect to \( S \).
2. No \( c_i \) is contained in \( H \), i.e., \( S(c_i) \neq 0 \) for every \( i \).
3. Subspaces spanned by \( \{ c_1, \ldots, c_i \} \) do not include \( H^\perp \) if \( r < m \).

We proceed by induction. We assume \( \{ c_1, \ldots, c_{r-1} \} \) satisfies the conditions. This is trivially true for \( r = 1 \). The condition (3) shows \( \{ c_1, \ldots, c_{r-1} \}^\perp \) is not included in \( H \), i.e., there exists an element \( c_r \in \{ c_1, \ldots, c_{r-1} \}^\perp \) which is not in \( H \). This completes the proof if \( r = m \). If \( r < m \), the subspace \( \{ c_1, \ldots, c_{r-1} \}^\perp \) is at least 2 dimensional, and \( \{ c_1, \ldots, c_{r-1} \}^\perp \cap H \) contains a non-zero element \( d \). We show \( \{ c_1, \ldots, c_{r-1}, c_r, d \} \) are linearly independent over \( F \). Let

\[
x = a_1 c_1 + \cdots + a_{r-1} c_{r-1} + a_r c_r + b d_r,
\]

We see \( a_1 = \cdots = a_{r-1} = 0 \) because 0 = \( c_1 S x = c_1 S(c_1) \) for \( i = 1, \ldots, r - 1 \), and \( S(c_r) \neq 0 \). As \( c_r \) and \( d \) are linearly independent by their choice, all the coefficients of \( x \) are zero. We can find a vector \( h \) which generates \( H^\perp \) because \( \text{dim} H^\perp = 1 \). If there does not exist any relation

\[
h = a_1 c_1 + \cdots + a_{r-1} c_{r-1} + a_r c_r + b d_r,
\]

or if we obtain such a relation for \( a_r \neq 0 \), \( \{ c_1, \ldots, c_r \} \) satisfies the three conditions. If there exists such a relation for \( a_r \neq 0 \), we substitute \( c_r = c_r + a d_r, a \neq b/a \), for \( c_r \). Then \( \{ c_1, \ldots, c_r \} \) satisfies the three conditions. Now we have obtained \( \{ c_1, \ldots, c_m \} \) satisfying the three conditions. We can find non-zero \( a \) such that \( a_r^2 = S(c_r) \). Then the vectors \( d_i = a_i^{-1} c_i \) satisfies

\[
' d_i \cdot S \cdot d_j = \delta_{ij} \quad \text{(Kronecker's delta)}.
\]

If we put \( D = (d_1, \ldots, d_m) \) and \( P = QD \),

\[
E = 'DSD = 'P \cdot P.
\]

Then \( P \cdot P = E \) and the first row of \( P \) is an orthogonal basis.

3. **Orthogonal normal basis**

In some extensions, there exist normal bases which are orthogonal. Let \( \{ α^{(0)}, \ldots, α^{(m)} \} \) be the roots of an irreducible equation.
\[ P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0, \quad a_i \in F. \]

If \( \{\alpha^{(0)}, \ldots, \alpha^{(m)}\} \) is a basis of \( K/F \) and if it is an orthogonal basis, it is called an orthogonal normal basis. It should not be confused with the orthonormal basis in Linear Algebra. In this case \( r = \alpha^{(0)} + \cdots + \alpha^{(m)} \) is a non-zero element of \( F \), and \( r\alpha^{(p)} \) corresponds to the matrix \( A = P\Omega(\alpha^{(p)})P \) by the regular representation with the basis \( \{\alpha^{(0)}, \ldots, \alpha^{(m)}\} \) (See the proof of Theorem 3).

**Proposition 7.** Every extension of degree 3 has an orthogonal normal basis.

**Proof.** Let \( a \) be a non-zero element of \( F \). The mapping \( \phi(x) = x^2(x + a) \) is not a surjective mapping from \( F \) to \( F \), because \( \phi(0) = \phi(-a) = 0 \). Let \( -c \) be not in the image. Then \( X^3 + aX^2 + c = 0 \) is an irreducible equation over \( F \). The roots \( \{\alpha^{(0)}, \alpha^{(2)}, \alpha^{(3)}\} \) satisfy the relations \( \alpha^{(0)}\alpha^{(2)} = \alpha^{(2)}\alpha^{(3)} = \alpha^{(0)}\alpha^{(3)} = 0 \) and \( \alpha^{(0)} + \alpha^{(2)} + \alpha^{(3)} = a^2 \neq 0 \). These are the conditions for \( \{\alpha^{(0)}, \alpha^{(2)}, \alpha^{(3)}\} \) to be an orthogonal basis. In fact, \( a^2\alpha^{(1)} \) corresponds to the matrix

\[
A = \begin{pmatrix}
-a^3 - 3c & S & T \\
S & T & -3c \\
T & -3c & S
\end{pmatrix},
\]

where \( S = \alpha^{(0)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(0)} \) and \( T = \alpha^{(0)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(0)} \) are in \( F \), and they have the relations \( S + T = 3c, ST = a^2c + 9c^2 \).

When \( m = 2 \), the orthogonality condition for \( \{\alpha^{(0)}, \alpha^{(2)}\} \) means \( 2\alpha^{(0)}\alpha^{(2)} = 0 \). This shows that the constant term of \( P(X) \) is zero if the characteristic \( \neq 2 \). Hence there is no orthogonal normal basis of degree 2 for the characteristic \( \neq 2 \). When the characteristic is 2, the roots of any irreducible equation of the form \( X^2 + X + a = 0 \) are orthogonal normal bases; When \( m = 4 \), the orthogonality means \( \alpha^{(3)} = -\alpha^{(1)}, \alpha^{(4)} = -\alpha^{(2)} \). As this shows \( Tr(\alpha^{(3)}) = 0 \), there is no orthogonal normal basis.

Let \( F \) have \( q \) elements and let \( \rho(\alpha) = \alpha^k \) for \( \alpha \in K \). Then the conditions for orthogonality are equations given by symmetric polynomials of \( \{\alpha^{(0)}, \alpha^{(2)}, \ldots, \alpha^{(m)}\} \), i.e., they are represented by coefficients of \( P(X) \). As the two conditions

\[ \sum \alpha^{(i)} \rho^k(\alpha^{(i)}) = 0 \quad \text{and} \quad \sum \alpha^{(i)} \rho^{m-k}(\alpha^{(i)}) = 0 \]

are the same, we need \( [m/2] \) conditions for orthogonality. Then there is a large freedom of the coefficients for large \( m \), and we may expect an orthogonal normal basis for large \( m \).

4. **Appendix**

In this appendix, we give a direct proof of Witt’s theorem (in the finite field case).

**Theorem.** Let \( F \) be a finite field of characteristic \( \neq 2 \), and let \( S \) be an \( n \times n \) invertible symmetric matrix over \( F \). If the determinant \( \det S \) is a square in \( F \), we can find an invertible matrix \( A \) over \( F \) such that \( A^TSA = E \) (identity).

**Proof.** We first want to find an \( n \times n \) invertible matrix \( P \) over \( F \) such that \( P^TSP \) is diagonal. If \( s_{11} = 0 \), we can find \( s_{1j} \neq 0 \). Let \( P_1 \) be an \( n \times n \) matrix whose components are defined as follows: the \((j, j)\) component is 0, but other diagonal components are 1; the \((1, j)\) component is 1; the \((j, 1)\) component is \( \pm 1 \); and the other components are 0.

\[
P_1 = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & \cdot \\
0 & 1 & 0 & 0 & \cdot \\
\pm 1 & 0 & 0 & 0 & \cdot \\
0 & \cdot & 0 & 1 & 0 \\
\cdot & 0 & 0 & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & 0 & 1
\end{pmatrix}
\]

As

\[
\begin{pmatrix}
1 & \pm 1 \\
1 & 0
\end{pmatrix}
\begin{pmatrix}
a & b \\
b & c
\end{pmatrix}
\begin{pmatrix}
1 & 1 \\
\pm 1 & 0
\end{pmatrix}
= \begin{pmatrix}
a + c \pm 2b & a \pm b \\
a \pm b & a
\end{pmatrix},
\]

we can find the sign such that the \((1, 1)\) component of \( S_1 = P_1^TSP_1 \) is not 0. Let \( P_1 = E \) when the \((1, 1)\) component of \( S \) is not 0. Let \( s_{ij} \) (\( 1 \leq j \leq n \)) be the components of the first row of \( S_1 \). Let \( p_{ij} = -s_{ii}^{-1}s_{ij} \), and let
\[ P_2 = \begin{pmatrix}
1 & p_{12} & \cdots & \cdots & p_{1n} \\
0 & 1 & 0 & \cdots & 0 \\
\vdots & 0 & 1 & 0 & 0 \\
\vdots & 0 & 1 & 0 & \iddots \\
0 & \cdots & \cdots & \cdots & 0 & 1
\end{pmatrix} \]

Then it is easily seen that

\[ 'P_2S_1P_2 = \begin{pmatrix}
s_{11} & 0 & \cdots & 0 \\
0 & 0 & \cdots & T \\
\vdots & \ddots & \ddots & \ddots \\
0 & \cdots & T & 0
\end{pmatrix} \]

where \( T \) is an invertible symmetric matrix of size \( n - 1 \). Thus we can find an invertible matrix \( P \) such that \( U = P P_2 S P_2 \) is diagonal. As \( \text{det} S \) is a square in \( F \), the number of non-square diagonal components of \( U \) is even. Let \( u \) be such a component. Then other non-square components can be described as \( uv^2 \). As the squares are not additively closed in \( F \), we can find \( a \) and \( b \) in \( F \) such that \( a^2 + (bv)^2 = u^{-1} \). Then the equation

\[
\begin{pmatrix}
a & b \\
-bv & av^{-1}
\end{pmatrix}
\begin{pmatrix}
u & 0 \\
0 & u v^2
\end{pmatrix}
\begin{pmatrix}
a & -bv \\
b & av^{-1}
\end{pmatrix} = E
\]

shows that we can find an invertible matrix \( Q \) such that \( 'Q U Q = E \). Then \( AS A = E \) for \( A = PQ \) which proves Witt's theorem.

REFERENCES

[L] S. Lang, Algebra, Chapter 8-5, Addison-Wesley.