Orthogonal Variable Spreading Factor Codes over Finite Fields∗∗∗

Shoichiro YAMASAKI†, Senior Member and Tomoko K. MATSUSHIMA†++, Member

SUMMARY The present paper proposes orthogonal variable spreading factor codes over finite fields for multi-rate communications. The proposed codes have layered structures that combine sequences generated by discrete Fourier transforms over finite fields, and have various code lengths. The design method for the proposed codes and examples of the codes are shown.

key words: orthogonal variable spreading factor codes, multi-rate communications, finite fields, discrete Fourier transform

1. Introduction

Orthogonal spreading codes have been applied to wireless communication systems using direct sequence code division multiple access (DS-CDMA) [1]-[3]. Various orthogonal codes have been studied. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.

The present study proposes OVSF codes over finite fields. The discrete Fourier transform (DFT) exists over an extension field. The discrete Fourier transform (DFT) exists over an extension field. Walsh codes that are derived from Hadamard matrices are one example of such codes [1]. Polyphase orthogonal codes over the complex field have been studied [4]. Recently, Hadamard-type matrices on finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes and complete complementary codes have been derived by introducing the concept of the GF-conjugate [5].

Tree-structured generation of orthogonal spreading codes with different code lengths has been proposed, and these codes, called orthogonal variable spreading factor (OVSF) codes, have been used in DS-CDMA systems realizing multi-rate communications, which support a wide data rate range [6]-[9]. These OVSF codes are based on Walsh codes and are binary codes. The authors have proposed non-binary OVSF codes over the complex field [10], [11]. The tree structure combining polyphase orthogonal codes realizes the codes, and the binary OVSF codes are represented as a special case of non-binary OVSF codes.
complex field \( S \), \([10],[11]\). A polyphase orthogonal code over

\[ \mathbf{H} = \begin{bmatrix} H_{1,0} & H_{1,1} & \cdots & H_{1,n} \\ H_{2,0} & H_{2,1} & \cdots & H_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ H_{n,0} & H_{n,1} & \cdots & H_{n,n} \end{bmatrix}, \]  

(5)

where \( H_{i,j} \) is the \( j \)th row of \( S_{H,i,j} \) for \( i = 0, 1, 2, 3 \). In addition, \( S_{H,i,j} \) and \( S_{H,i,j}^T \) correspond to Walsh sequences of length 4.

Next, we describe the superscripts attached to the matrices and sequences. The matrix \( S_{H,n_{i,j}} \) and the sequence \( s_{H,n_{i,j}} \) have superscripts of \( (n_1,n_2) \), which indicates that the Kronecker product of the \( n_2 \)-point matrix \( S_{H,n_1} \) and the \( n_1 \)-point matrix \( S_{H,n_2} \) generates the \( n_1n_2 \)-point matrix \( S_{H,n_{i,j}} \) and the sequence \( s_{H,n_{i,j}} \) of length \( n_1n_2 \) for \( i = 0, 1, \ldots, n_1n_2-1 \). Furthermore, the Kronecker product of \( S_{n_1} \) and \( S_{n_2} \) generates the \( n_1n_2 \)-point matrix \( S_{H,n_{i,j}} \) and the sequence \( s_{H,n_{i,j}} \) of length \( n_1n_2 \) for \( i = 0, 1, \ldots, n_1n_2-1 \).

The Kronecker product of \( S_{H,2} \) and \( S_{H,4} \) generates \( S_{H,8} \) as

\[ S_{H,8}^{(2,2)} = S_{H,2} \otimes S_{H,4} = \begin{bmatrix} S_{H,4}^{(2,2)} & S_{H,4}^{(2,2)} \\ S_{H,4}^{(2,2)} & S_{H,4}^{(2,2)} \end{bmatrix} \]

(6)

where \( S_{H,8}^{(2,2)} \) is the \( i \)th row of \( S_{H,8}^{(2,2)} \) for \( i = 0, 1, \ldots, 7 \) and \( S_{H,8}^{(2,2)} \) correspond to Walsh sequences of length 8.

The tree-structured code generation constructs the three-layer code sequences shown in Fig. 1. In multi-rate DS-CDMA systems, each Layer 1 code sequence of length 2 is used for the high-rate data, each Layer 2 code sequence of length 4 is used for the middle-rate data and each Layer 3 code sequence of length 8 is used for the low-rate data. When a code sequence is selected in the tree, code sequences other than its descendant or ancestor code sequences are selected in order to realize the orthogonality of the sequences. Examples exhibit the following properties: \( s_{H,2,0}^{(2)} \) is orthogonal to the first halve of \( s_{H,2,2}^{(2)} \) and orthogonal to the second halves of \( s_{H,2,2}^{(2)} \) for \( i = 1 \) and 3. \( s_{H,4,0}^{(2)} \) is orthogonal to the first half of \( s_{H,4,2}^{(2)} \) and orthogonal to the second halves of \( s_{H,4,2}^{(2)} \) for \( i = 1, 2, 3, 5, 6 \) and 7.

2.2 Polyphase OVSF codes

The authors have proposed non-binary OVSF codes over the complex field \([10],[11]\). A polyphase orthogonal code over the complex field is given by the \( n \times n \) matrix

\[ S_{C,n} = \begin{bmatrix} \omega^0 & \omega^0 & \cdots & \omega^0 \\ \omega^0 & \omega^1 & \cdots & \omega^1 \\ \vdots & \vdots & \ddots & \vdots \\ \omega^0 & \omega^{n-1} & \cdots & \omega^{n-1} \end{bmatrix}, \]

(7)

where \( n \) is a positive integer. The complex number \( \omega \) is a primitive \( n \)th root of unity and is represented by

\[ \omega = e^{-j2\pi/n}, \]

(8)

where \( j = \sqrt{-1} \). The \( n \) different \( n \)th roots of unity are denoted as \( \omega^0, \omega^1, \omega^2, \ldots, \omega^{n-1} \). Polyphase orthogonal code sequences of length \( n \) are presented as the rows of \( S_{C,n} \), which are defined as \( S_{C,n} = [ \omega^0 \omega^1 \cdots \omega^{(n-1)} ] \) for \( i = 0, 1, \ldots, n-1 \).

We define \( r_{C,n,h} \) which is equal to \( s_{C,n,h} \) for \( h = 0, 1, \ldots, n-1 \). Multiplying \( s_{C,n,i} \) and \( s_{C,n,h}^T \), where \( r_{C,n,h}^T \) corresponds to a conjugate transpose of \( r_{C,n,h} \), yields

\[ S_{C,n} \cdot C_{n,h} \]

(9)

For \( n = 2, S_{C,2}^{(2)} \) is shown as

\[ S_{C,2}^{(2)} = \begin{bmatrix} \omega^0 & \omega^0 \\ \omega^0 & \omega^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} S_{C,2,0}^T & S_{C,2,1}^T \end{bmatrix}, \]

(10)

where \( \omega = e^{-j2\pi/2} = -1 \). \( s_{C,2}^{(2)} = [ 1 1 ] \) and \( s_{C,2,1}^{(2)} = [ 1 -1 ] \). In addition, \( s_{C,2,0}^{(2)} \) and \( s_{C,2,1}^{(2)} \) correspond to polyphase sequences of length 2.

For \( n = 4, S_{C,4}^{(4)} \) over the complex field is shown as

\[ S_{C,4}^{(4)} = \begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \omega^3 \\ \omega^0 & \omega^2 & \omega^4 & \omega^6 \\ \omega^0 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & -1 & 1 \\ 1 & j & -1 & -j \end{bmatrix}, \]

(11)

where \( \omega = e^{-j2\pi/4} = -j \) and \( s_{C,4}^{(4)} = [ \omega^0 \omega^j \omega^{2j} \omega^{3j} ] \) for \( i = 0, 1, 2, 3 \). In addition, \( s_{C,4,0}^{(4)} \) and \( s_{C,4,2}^{(4)} \) correspond to polyphase sequences of length 4. The Kronecker product of \( S_{C,2}^{(2)} \) and \( S_{C,4}^{(4)} \) generates \( S_{C,8}^{(4,2)} \) as

\[ S_{C,8}^{(4,2)} = S_{C,2}^{(2)} \otimes S_{C,4}^{(4)} = \begin{bmatrix} S_{C,4,0}^{(4,2)} & S_{C,4,1}^{(4,2)} \\ S_{C,4,2}^{(4,2)} & S_{C,4,3}^{(4,2)} \end{bmatrix} \]

(12)

where \( s_{C,8,0}^{(4,2)} = [ \omega^0 \omega^j \omega^{2j} \omega^{3j} ] \) and \( s_{C,8,i+4}^{(4,2)} = [ \omega^0 \omega^j \omega^{2j} \omega^{3j} - \omega^0 - \omega^j - \omega^{2j} - \omega^{3j} ] \) for \( i = 0, 1, 2, 3 \). These sequences of length 8 construct the code tree of the polyphase OVSF codes over the complex field. The matrix \( S_{C,n} \) generating the polyphase sequence is closely related to the DFT matrix.

3. Properties of DFT

3.1 DFT over a finite field

We introduce the DFT operation over arbitrary finite fields GF(q), including prime fields and extension fields. \( F \) is added to a matrix or a sequence over the finite field as a
Each code sequence of length \( n \) for the finite field and additional \( -1 \) for \( i \). In addition, we define the inverse element of \( S \) as \( S^{-1} \).

We define the inverse element of \( S \) as \( S^{-1} \).

Let \( S_{F,n} \) be the \( i \)-th row of \( S_{F,n} \). In addition, \( S_{F,n,t} \) is the \( t \)-th row of \( S_{F,n} \) and is defined as

\[
s_{F,n,t} = \begin{bmatrix} a_0^t & a_1^t & \cdots & a_{(n-1)^t} \\
end{bmatrix},
\]

for \( t = 0, 1, \ldots, n-1 \). Each \( s_{F,n,t} \) corresponds to a spreading code sequence of length \( n \) for data demultiplexing.

The inner product of \( s_{F,n,t} \) and \( r_{F,n,h} \), which is calculated by multiplying \( s_{F,n,t} \) and \( r_{F,n,h} \) over the finite field, yields

\[
s_{F,n,t} r_{F,n,h} = \begin{cases} n_F (h = i), \\
0 \text{ (otherwise)}.
\end{cases}
\]

Therefore, \( s_{F,n,t} \) and \( r_{F,n,h} \) are orthogonal to each other for \( h \neq i \). In Eq. (18), \( n_F \) is equal to a value obtained by adding 1 \( n \) times over the finite field. In order to normalize the transform as \( s_{F,n,t} r_{F,n,h} = 1 \) for \( h = i \), the definition of \( r_{F,n,h} \) in Eq. (17) is replaced with

\[
r_{F,n,h} = n_F^{-1} \begin{bmatrix} a_0^h & a_2^h & \cdots & a_{-1}^{(n-1)h} \\
end{bmatrix},
\]

where the normalization factor \( n_F^{-1} \) is the inverse of \( n_F \) such that \( n_F \cdot n_F^{-1} = 1 \) over the finite field. However, in this paper, the normalization factor is not used for easy understanding.

### 3.2 Number of points for DFT

In this section, we consider the DFT over a finite field denoted as \( GF(q) \). Then, \( q \) is set to \( q = p \) for a prime field, where \( p \) is a prime number of \( p \geq 3 \). In addition, \( q \) is set to \( q = p^m \) for an extension field, where \( p \) is a prime number of \( p \geq 3 \), and \( m \) is an integer of \( m \geq 2 \). Therefore, the proposed code cannot be constructed over \( GF(2) \).

A prime factorization of \( q - 1 \) is represented as

\[
a - 1 = p_1^{e_1} p_2^{e_2} \cdots p_i^{e_i},
\]

where \( p_1, p_2, \ldots, p_i \) for \( i \geq 1 \) are prime numbers that are different from each other, and \( e_1, e_2, \ldots, e_i \) are positive integers. We define \( d \) as the number of divisors except for one, and \( d \) is given by

\[
d = (e_1 + 1)(e_2 + 1) \cdots (e_i + 1) - 1.
\]

Each divisor except for the value of one corresponds to the number of points for the DFT. Next, we show some examples. \( F_q \) is added to a matrix or a sequence over \( GF(q) \) as a subscript in this paper.

### 3.3 DFT over prime fields

When \( q = p = 5 \), the elements of \( GF(5) \) are included in the set \{0, 1, 2, 3, 4\}. Let \( a = 2 \). Then \( a^4 = 1 \) and \( a^i \neq 1 \) for \( i = 1, 2, 3 \).

A four-point DFT and a two-point DFT exist over \( GF(5) \), because \( q - 1 = 5 - 1 = 4 = 4^2 \). The four-point DFT matrix \( S_{F_4,4} \) over \( GF(5) \) is given as

\[
S_{F_4,4} = \begin{bmatrix} a_0^0 & a_0^0 & a_0^0 & a_0^0 \\
end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 3 \\
1 & 4 & 1 & 4 \\
1 & 3 & 4 & 2 \\
end{bmatrix},
\]

where \( s_{F_4,4,i}^{(4)} \) is the \( i \)-th row of \( S_{F_4,4} \) for \( i = 0, 1, 2, 3 \).
The four-point IDFT matrix $R_{F_{i,4}}^{(4)}$ is given as

$$R_{F_{i,4}}^{(4)} = \begin{bmatrix} a^0 & a^0 & a^0 & a^0 \\ a^0 & a^{-1} & a^{-2} & a^{-3} \\ a^0 & a^{-2} & a^{-4} & a^{-6} \\ a^0 & a^{-3} & a^{-6} & a^{-9} \end{bmatrix} = \begin{bmatrix} r_{F_{i,4,0}}^{(4)} & r_{F_{i,4,1}}^{(4)} & r_{F_{i,4,2}}^{(4)} & r_{F_{i,4,3}}^{(4)} \end{bmatrix}^T,$$

where $r_{F_{i,4,h}}^{(4)}$ is the $h$th row of $R_{F_{i,4}}^{(4)}$ for $h = 0, 1, 2, 3$.

Multiplying $s_{F_{i,4}}^{(4)}$ and $r_{F_{i,4,h}}^{(4)}$ over GF(5) yields

$$s_{F_{i,4,h}}^{(4)} = \begin{cases} 4 & (h = i), \\ 0 & \text{(otherwise)}. \end{cases}$$

Next, we focus on another element of GF(5) to explain other matrix size. Let $a = 4$. Then, $a^2 = 1$ and there exists the DFT of matrix size two. The two-point DFT matrix $S_{F_{i,2}}$ over GF(5) is written as

$$S_{F_{i,2}}^{(2)} = \begin{bmatrix} a^0 & a^0 \\ a^0 & a^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} s_{F_{i,2,0}}^{(2)} & s_{F_{i,2,1}}^{(2)} \end{bmatrix}^T,$$

where $s_{F_{i,2,h}}^{(2)}$ is the $h$th row of $S_{F_{i,2}}^{(2)}$ for $h = 0, 1$.

The two-point IDFT matrix $R_{F_{i,2}}^{(2)}$ is written as

$$R_{F_{i,2}}^{(2)} = \begin{bmatrix} a^0 & a^0 \\ a^0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} r_{F_{i,2,0}}^{(2)} & r_{F_{i,2,1}}^{(2)} \end{bmatrix}^T,$$

where $r_{F_{i,2,h}}^{(2)}$ is the $h$th row of $R_{F_{i,2}}^{(2)}$ for $h = 0, 1$.

Multiplying $s_{F_{i,2,h}}^{(2)}$ and $r_{F_{i,2,h}}^{(2)}$ over GF(5) yields

$$s_{F_{i,2,h}}^{(2)} = \begin{cases} 2 & (h = i), \\ 0 & \text{(otherwise)}. \end{cases}$$

3.4 DFT over extension fields

For $p = 2$ and $m = 8$, $q$ is equal to $p^m = 2^8$. Then, there are 256 elements of $\{0, 1, a, a^2, \ldots, a^{254}\}$ in GF($2^8$), where $a$ is a primitive root of the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. In this case, $a^{255} = 1$ and $a^i \neq 1$ for $i = 1, 2, \ldots, 254$. $q - 1 = 2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$, then 255 has divisors of 3, 5, 15, 17, 51, 85, and 255, except for one. Each divisor corresponds to the number of points for the DFT over GF($2^h$) [12].

The 255-point DFT over GF($2^8$) maps a vector of 255 eight-bit bytes into a vector of 255 eight-bit bytes. Let $n = 255$ and $a = a$ in the $n$-point DFT, then the 255-point DFT matrix is given as

$$S_{F_{255}}^{(255)} = \begin{bmatrix} a^0 & a^0 & \cdots & a^0 \\ a^0 & a^1 & \cdots & a^{254} \\ \vdots & \vdots & \ddots & \vdots \\ a^0 & a^{254} & \cdots & a^{254} \end{bmatrix}$$

$$= \begin{bmatrix} S_{F_{255,0}}^{(255)} & S_{F_{255,1}}^{(255)} & \cdots & S_{F_{255,254}}^{(255)} \end{bmatrix},$$

for $i = 0, 1, \ldots, 254$.

The 255-point IDFT matrix is given as

$$R_{F_{255}}^{(255)} = \begin{bmatrix} a^0 & a^0 & \cdots & a^0 \\ a^0 & a^{-1} & \cdots & a^{-254} \\ \vdots & \vdots & \ddots & \vdots \\ a^0 & a^{-254} & \cdots & a^{-254} \end{bmatrix}$$

$$= \begin{bmatrix} r_{F_{255,0}}^{(255)} & r_{F_{255,1}}^{(255)} & \cdots & r_{F_{255,254}}^{(255)} \end{bmatrix},$$

for $h = 0, 1, \ldots, 254$.

Multiplying $s_{F_{255}}^{(255)}$ and $r_{F_{255,h}}^{(255)}$ over GF($2^8$) yields

$$s_{F_{255,h}}^{(255)} = \begin{cases} 1 & (h = i), \\ 0 & \text{(otherwise)}. \end{cases}$$

For $h = i$, $s_{F_{255,i}}^{(255)} = 1$, because the number of points for the DFT over GF($2^m$) is odd and adding 1 an odd number of times equals 1 in the case of GF($2^m$) calculation. We define $a = a^{85}$ in GF($2^8$). Then $a^3 = 1$. The three-point DFT matrix $S_{F_{3,3}}$ over GF($2^8$) is given as

$$S_{F_{3,3}}^{(3)} = \begin{bmatrix} a^0 & a^0 & a^0 \\ a^0 & a^1 & a^2 \\ a^0 & a^3 & a^4 \end{bmatrix} = \begin{bmatrix} a^0 & a^{85} & a^{170} \\ a^0 & a^{-85} & a^{-170} \\ a^0 & a^{-170} & a^{-85} \end{bmatrix}$$

$$= \begin{bmatrix} S_{F_{3,3,0}}^{(3)} & S_{F_{3,3,1}}^{(3)} & S_{F_{3,3,2}}^{(3)} \end{bmatrix},$$

where $s_{F_{3,3,h}}^{(3)}$ is the $h$th row of $S_{F_{3,3}}^{(3)}$ for $i = 0, 1, 2$.

The three-point IDFT matrix $R_{F_{3,3}}^{(3)}$ is given as

$$R_{F_{3,3}}^{(3)} = \begin{bmatrix} a^0 & a^0 & a^0 \\ a^0 & a^{-1} & a^{-2} \\ a^0 & a^{-2} & a^{-4} \end{bmatrix} = \begin{bmatrix} a^0 & a^{85} & a^{170} \\ a^0 & a^{-85} & a^{-170} \\ a^0 & a^{-170} & a^{-85} \end{bmatrix}$$

$$= \begin{bmatrix} r_{F_{3,3,0}}^{(3)} & r_{F_{3,3,1}}^{(3)} & r_{F_{3,3,2}}^{(3)} \end{bmatrix},$$

where $r_{F_{3,3,h}}^{(3)}$ is the $h$th row of $R_{F_{3,3}}^{(3)}$, for $h = 0, 1, 2$.

Multiplying $s_{F_{3,3,h}}^{(3)}$ and $r_{F_{3,3,h}}^{(3)}$ over GF($2^8$) yields

$$s_{F_{3,3,h}}^{(3)} = \begin{cases} 1 & (h = i), \\ 0 & \text{(otherwise)}. \end{cases}$$

We define $a = a^{51}$ in GF($2^8$). Then $a^3 = 1$. The five-point DFT matrix $S_{F_{5,5}}^{(5)}$ in GF($2^8$) is written as

$$S_{F_{5,5}}^{(5)} = \begin{bmatrix} a^0 & a^0 & a^0 & a^0 & a^0 \\ a^0 & a^1 & a^2 & a^3 & a^4 \\ a^0 & a^2 & a^4 & a^6 & a^8 \\ a^0 & a^3 & a^6 & a^9 & a^{12} \\ a^0 & a^4 & a^8 & a^{12} & a^{16} \end{bmatrix}$$
\[ R_{F_{q,5}}^{(5)} = \begin{bmatrix} a_0 & a_0 & a_0 & a_0 & a_0 \\ a_0 & a_0 & a_{102} & a_{153} & a_{204} \\ a_0 & a_{102} & a_{204} & a_{51} & a_{153} \\ a_0 & a_{153} & a_{204} & a_{51} & a_{102} \\ a_0 & a_{204} & a_{153} & a_{51} & a_{102} \end{bmatrix} \]

where \( S_{F_{q,5},5}^{(5)} \) is the \( i \)th row of \( S_{F_{q,5}}^{(5)} \) for \( i = 0, 1, 2, 3, 4 \).

The five-point IDFT matrix \( R_{F_{q,5}}^{(5)} \) is written as

\[ R_{F_{q,5}}^{(5)} = \begin{bmatrix} a_0 & a_0 & a_0 & a_0 & a_0 \\ a_0 & a_0 & a_{102} & a_{153} & a_{204} \\ a_0 & a_{102} & a_{204} & a_{51} & a_{153} \\ a_0 & a_{153} & a_{204} & a_{51} & a_{102} \\ a_0 & a_{204} & a_{153} & a_{51} & a_{102} \end{bmatrix} \]

where \( r_{F_{q,5},5}^{(5)} \) is the \( h \)th row of \( S_{F_{q,5}}^{(5)} \) for \( h = 0, 1, 2, 3, 4 \).

Multiplying \( S_{F_{q,5}}^{(5)} \) and \( r_{F_{q,5},5}^{(5)} \) over GF(28) yields

\[ S_{F_{q,5},5}^{(5)} \cdot r_{F_{q,5},5}^{(5)} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \]

\[ (h = i), \quad (\text{otherwise}). \]

4. Proposed OVSF codes over finite fields

The multiplication of the \( i \)th row of the \( n \)-point DFT matrix and the \( h \)th column of the \( n \)-point IDFT matrix gives 0 over finite fields for \( i \neq h \), where \( i = 0, 1, \ldots, n-1 \) and \( h = 0, 1, \ldots, n-1 \), as shown in Eq. (18). Using this fact, we propose tree-structured OVSF codes over finite fields.

4.1 Construction of the proposed codes

We generalize the construction of the proposed codes over GF(q). Then, \( q \) is set to \( q = p \) for a prime field, where \( p \) is a prime number of \( p \geq 3 \). In addition, \( q \) is set to \( q = p^m \) for an extension field, where \( p \) is a prime number of \( p \geq 2 \) and \( m \) is an integer of \( m \geq 2 \).

We assume that the number of layers is \( L \) for \( L \geq 2 \). When \( q = 1 \) is factorized using prime numbers \( p_1, p_2, \ldots, p_i \) for \( i \geq 1 \), as shown in Eq. (20), \( q \geq 1 \) has \( d \) divisors, except for the divisor of value one, as shown in Eq. (21). We define these \( d \) divisors as \( f_1, f_2, \ldots, f_d \). The \( n \)-point DFT matrix \( S_{n}^{(n)} \) is applied to construct the codes for \( l = 1, 2, \ldots, L \). Each \( n_i \) is selected from \( f_1, f_2, \ldots, f_d \) arbitrarily. Therefore, there exist \( d^k \) kinds of code tree. The code length in Layer \( l \) is defined as \( k_i \) and is decided as \( k_i = \prod_{i=1}^{l} n_i \).

Next, we present examples. In the case of GF(q) for \( q = p = 7 \), \( q \geq 1 \) is factorized as \( q = 1 \) = \( 6 = 2 \cdot 3 \), then the divisors of \( q \) are \( f_1 = 2, f_2 = 3 \) and \( f_3 = 6 \). Then Table 1 shows 27 kinds of \( (n_1, n_2, n_3) \), where each \( n_i \) is selected from \( f_1 = 2, f_2 = 3 \) and \( f_3 = 6 \) for \( l = 1, 2, 3 \). Then Table 1 also shows 27 kinds of code lengths \((k_1, k_2, k_3)\) corresponding to \((n_1, n_2, n_3)\).

In the case of GF(q) for \( q = 2^s \), \( q \geq 1 \) is factorized as \( q = 1 \) = \( 2 \cdot 3 \cdot 5 \cdot 17 \). Then, the number of divisors is \( d = 7 \), as shown in Eq. (21). For \( L = 3 \), there exist \( 343 = (d^7) \) kinds of code tree.

We show a generalized construction method for the proposed codes over GF(q) of both prime and extension fields. Let \( a \) be an element in GF(q) which satisfies \( a^{q-1} = 1 \) and \( a \neq 1 \) for \( i = 1, 2, \ldots, q-2 \), then the \( n \)-point DFT matrix \( S_{F_{q,n}}^{(n)} \) for Layer 1 is written as

\[ S_{F_{q,n}}^{(n)} = \begin{bmatrix} s_{F_{q,n},0}^{(n)} & s_{F_{q,n},1}^{(n)} & \cdots & s_{F_{q,n},n-1}^{(n)} \end{bmatrix}^T, \]

where \( s_{F_{q,n},i}^{(n)} = \begin{bmatrix} b_{i0} & b_{i1} & \cdots & b_{i(n-1)} \end{bmatrix} \) is the \( i \)th row of \( S_{F_{q,n}}^{(n)} \) and \( b_{i0}, b_{i1}, \ldots, b_{i(n-1)} \) are written as

\[ S_{F_{q,n},i}^{(n)} = \begin{bmatrix} b_{i0} & b_{i1} & b_{i2} & \cdots & b_{i(n-1)} \end{bmatrix} \]

where \( b_{i0}, b_{i1}, b_{i2}, \ldots, b_{i(n-1)} \) is the \( i \)th row of \( S_{F_{q,n}}^{(n)} \) for \( b_{i0}, b_{i1}, \ldots, b_{i(n-1)} \) and \( i = 0, 1, \ldots, n-2 \). The Kronecker product of \( S_{F_{q,n}}^{(n)} \) and \( S_{F_{q,n}}^{(n)} \) generates the \( n \)-2-point matrix \( S_{F_{q,n},n-2}^{(n)} \) for Layer 2 as

\[ S_{F_{q,n},n-2}^{(n)} = \begin{bmatrix} s_{F_{q,n},0}^{(n)} \cdots s_{F_{q,n},n-2}^{(n)} \end{bmatrix}^T, \]

where \( s_{F_{q,n},i}^{(n)} \) is the \( i \)th row of \( S_{F_{q,n},i}^{(n)} \) and corresponds to the code sequence of length \( n \)-2 in Layer 2 for \( i \) = \( 0, 1, n_1 - 2 \). Then, the \( n \)-2 code sequences \( s_{F_{q,n},i}^{(n)} \) of Layer 2 are the descendants of \( s_{F_{q,n},i}^{(n)} \) of Layer 1 for \( i_1 = \)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Code Points</th>
<th>Code Lengths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1</td>
<td>(n1, n2, n3)</td>
<td>(k1, k2, k3)</td>
</tr>
<tr>
<td>n1</td>
<td>2 2 2 2 2 2 2 2</td>
<td>2 2 2 2 2 2 2 2</td>
</tr>
<tr>
<td>n2</td>
<td>2 2 2 3 3 3 6 6</td>
<td>2 2 2 2 2 2 2 2</td>
</tr>
<tr>
<td>n3</td>
<td>2 3 6 2 3 6 2 3</td>
<td>2 2 2 2 2 2 2 2</td>
</tr>
<tr>
<td>k1</td>
<td>2 2 2 2 2 2 2 2</td>
<td>2 2 2 2 2 2 2 2</td>
</tr>
<tr>
<td>k2</td>
<td>4 4 4 4 6 6 6 12</td>
<td>12 12 12 12 12 12 12 12</td>
</tr>
<tr>
<td>k3</td>
<td>8 8 12 24 12 18 36 24 36 108 72 108 216</td>
<td>216</td>
</tr>
</tbody>
</table>
When we design the sequences over GF(5), the Kronecker product of the \( n \)-point DFT matrix \( S_{F_{n}^{q}} \) and the \( n_{1}n_{2} \cdots n_{l-1} \)-point matrix \( S_{F_{n_{1}n_{2} \cdots n_{l-1}}} \) generates the \( n_{1}n_{2} \cdots n_{l} \)-point matrix \( S_{F_{n_{1}n_{2} \cdots n_{l}}} \) for Layer \( l \) as

\[
S_{F_{n_{1}n_{2} \cdots n_{l}}} = S_{F_{n_{1}n_{2} \cdots n_{l-1}}} \otimes S_{F_{n_{l}}},
\]

where \( S_{F_{n}} \) is the \( n \)-th row of \( S_{F_{n_{1}n_{2} \cdots n_{l-1}}} \) and corresponds to the code sequence of length \( n_{1}n_{2} \cdots n_{l} \) in Layer \( l \) for \( i = 0, 1, \ldots, n_{1}n_{2} \cdots n_{l} \). Then, the \( n \)-th code sequence \( S_{F_{n_{1}n_{2} \cdots n_{l}}} \) is generated by \( i \)-th layer of \( n_{1}n_{2} \cdots n_{l} \)-point code sequence \( S_{F_{n_{1}n_{2} \cdots n_{l-1}}} \). The code sequence obtained from the IDFT matrix over GF(q) are derived by the same procedure.

4.2 Examples of the proposed codes

When we design the sequences over GF(5), the Kronecker product of \( S_{F_{5}}^{(2)} \) and \( S_{F_{3}}^{(4)} \) generates \( S_{F_{8}}^{(4,2)} \) as

\[
S_{F_{8}}^{(4,2)} = S_{F_{5}}^{(2)} \otimes S_{F_{3}}^{(4)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

where \( S_{F_{8}}^{(4,2)} \) of length 8 is the \( i \)-th row of \( S_{F_{8}}^{(4,2)} \) for \( i = 0, 1, \ldots, 7 \).

The inverse matrix of \( S_{F_{8}}^{(4,2)} \) is obtained as

\[
R_{F_{8}}^{(4,2)} = R_{F_{5}}^{(2)} \otimes R_{F_{3}}^{(4)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

where \( R_{F_{8}}^{(4,2)} \) of length 8 is the \( i \)-th row of \( R_{F_{8}}^{(4,2)} \) for \( i = 0, 1, \ldots, 7 \).

When we refer to Eq. (42), the Kronecker product of \( S_{F_{5,2}}^{(2)} \) and \( S_{F_{8}}^{(4,2)} \) generates \( S_{F_{16}}^{(4,2,8)} \) over GF(5) as

\[
S_{F_{16}}^{(4,2,8)} = S_{F_{5,2}}^{(2)} \otimes S_{F_{8}}^{(4,2)} = \begin{bmatrix}
1 & S_{F_{8,8}}^{(2)} & 1 & S_{F_{8,8}}^{(2)}
\end{bmatrix}
\begin{bmatrix}
1 & S_{F_{8,8}}^{(2)} & 4 & S_{F_{8,8}}^{(2)}
\end{bmatrix}
\]

where \( S_{F_{8,8}}^{(2)} \) of length 16 is the \( i \)-th row of \( S_{F_{16}}^{(4,2,8)} \) for \( i = 0, 1, \ldots, 15 \).

The obtained sequences construct the code tree of the OVSF codes depending on the DFT matrices over GF(5), as shown in Fig. 3, which is used in data multiplexing. For example, the sequence [1 2 4 3], which is the first half of \( S_{F_{8,8}}^{(2)} \), is not orthogonal to \( R_{F_{8,8}}^{(4,2,8)} = [1 3 4 2] \). Moreover, the sequence [1 2 4 3 4 1 2 3], which is the first half of \( S_{F_{16,13,8}}^{(2,4,8)} \), or the sequence [1 3 4 2 1 3 4 2], which is the second half of \( S_{F_{16,13,8}}^{(2,4,8)} \), is not orthogonal to \( R_{F_{8,8}}^{(4,2,8)} = [1 3 4 2 1 3 4 2] \). Therefore, if one sequence is selected as the spreading code in the system, then the sequences, which are located as its ancestors or its descendants in the code tree, cannot be selected as the spreading codes.

When we design the sequences over GF(2^5), the Kronecker product of \( S_{F_{5,2}}^{(5)} \) and \( S_{F_{8,3}}^{(3)} \) generates \( S_{F_{15,15}}^{(3,5)} \) as

\[
S_{F_{15,15}}^{(3,5)} = S_{F_{5,2}}^{(5)} \otimes S_{F_{8,3}}^{(3)} = \begin{bmatrix}
S_{F_{5,2}}^{(5)} & S_{F_{8,3}}^{(3)} & S_{F_{8,3}}^{(3)} & \cdots & S_{F_{8,3}}^{(3)}
\end{bmatrix}
\begin{bmatrix}
S_{F_{5,2}}^{(5)} & S_{F_{8,3}}^{(3)} & S_{F_{8,3}}^{(3)} & \cdots & S_{F_{8,3}}^{(3)}
\end{bmatrix}
\]

where \( S_{F_{15,15}}^{(3,5)} \) of length 15 is the \( i \)-th row of \( S_{F_{15,15}}^{(3,5)} \) for \( i = 0, 1, \ldots, 14 \). These sequences construct the code tree of the OVSF codes over GF(2^5), as shown in Fig. 4. Since the
The proposed OVSF codes based on DFT over GF($q$) obtained, because the code length on Layer $d$ of the proposed OVSF codes has a layered structure with

$$d^f$$

of the code sequence of Layer $l$ for $l = 1, 2, \ldots, L$. Then, the code lengths of the code sequences are restricted to powers of 2.

A system configuration when the proposed codes are applied to synchronous code division multiplexing system for the downlink transmission between a transmitter at an access point and receivers for $N$ users is illustrated in Fig. 5. At the transmitter, $\oplus$ denotes an addition circuit in GF($q$). Every element in information symbols, spread sequence symbols and multiplexed sequence symbols is in GF($q$). This means that the symbols are spread and multiplexed by the calculation over GF($q$). Multiplexing causes no expansion of the range for symbol values.

We show the case of $q = 2^2$ as an example. There are four elements of $\{0, 1, \alpha, \alpha^2\}$ in GF($2^2$), where $\alpha$ is a primitive root of the primitive polynomial $\rho(x) = x^2 + x + 1$. Then, $\alpha^3 = 1$ and $\alpha^i \neq 1$ for $i = 1, 2$. Since $q - 1$ has divisor of 3, the three-point DFT exists over GF($2^2$). The proposed codes of length $k_l = 3^l$ are used as the spread sequences in Layer $l$ for $l \geq 1$. Multiplexing the user information symbols over GF($2^2$) by using these sequences generates the multiplexed sequence symbols over GF($2^8$). Both the information symbols and the multiplexed sequence symbols are elements in the set $\{0, 1, \alpha, \alpha^2\}$, which is mapped in a one-to-one way onto the set $\{00, 01, 10, 11\}$.

At a transmission circuit, which is denoted as Tx circuit in Fig. 5, the multiplexed sequence symbols in GF($2^8$) are converted to continuous-time transmission signals fed to the channel such as a radio channel, a cable channel and an optical channel. At each receiver for user, for $i = 0, 1, \ldots, N - 1$, signals from the channel are fed to a receiving circuit, which is denoted as Rx circuit in Fig. 5, and are converted to discrete-time symbols in GF($2^2$). Demultiplexing the symbols reconstructs the information symbols in GF($2^2$).

Several methods transmitting the multiplexed sequence symbols in GF($2^2$) can be supposed. These symbols, which consist of two-bit patterns in $\{00, 01, 10, 11\}$, are transmitted by on-off keying signals. And they are also transmitted by 4-phase-shift keying signals. In addition, the multiplexed sequence symbols can be error correction coded to increase error resilience of transmission signals through an erroneous channel. For example, they are transmitted by coded modulation signals combined with error correction coding of code rate 2/3 and 8-phase-shift keying mapping.

In the case of GF($2^2$) as an example, we have shown that the proposed scheme has several transmission methods. The other cases will be studied in future work.

At the end of this section, we illustrate a system configuration when the conventional codes [6]-[9] are applied to synchronous code division multiplexing for the downlink transmission in Fig. 6, where $\oplus$ denotes an addition circuit over the real or the complex field. Information symbols of

<table>
<thead>
<tr>
<th>Layer 1</th>
<th>Layer 2</th>
<th>Layer 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{F}_l(n_1)$</td>
<td>$\mathcal{F}_l(n_2)$</td>
<td>$\mathcal{F}_l(n_3)$</td>
</tr>
<tr>
<td>$\mathcal{F}_l(n_1, n_2)$</td>
<td>$\mathcal{F}_l(n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
</tr>
<tr>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_2, n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
</tr>
<tr>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_2, n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
</tr>
<tr>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_2, n_2, n_3)$</td>
<td>$\mathcal{F}_l(n_1, n_2, n_3)$</td>
</tr>
</tbody>
</table>

Fig. 2 The proposed OVSF codes based on DFT over GF($q$), which are used as spreading sequences for data multiplexing.
The present paper proposed tree-structured orthogonal spreading codes with different code lengths over finite fields including prime fields and extension fields. Combining the sequences generated by the discrete Fourier transform over finite fields realizes various lengths of the codes. The design method for the proposed codes was shown and examples of the codes were demonstrated. The proposed scheme multiplexing symbols over finite fields would have potential of low peak-to-average power ratio (PAPR) characteristics of the transmission signal and a discussion of the PAPR is future work.

5. Conclusion

The present paper proposed tree-structured orthogonal spreading codes with different code lengths over finite fields including prime fields and extension fields. Combining the sequences generated by the discrete Fourier transform over finite fields realizes various lengths of the codes. The design method for the proposed codes was shown and examples of the codes were demonstrated. The proposed scheme multiplexing symbols over finite fields would have potential of low peak-to-average power ratio (PAPR) characteristics of the transmission signal and a discussion of the PAPR is future work.

Acknowledgment

The present study was supported by JSPS KAKENHI Grant Numbers 19K04403 and 19K04402. The authors would like to thank the anonymous reviewers for their careful reviews and valuable comments.

References


Shoichiro YAMASAKI received B.E., M.E., and Dr.Eng. Degrees in Electrical Engineering from Keio University, Yokohama, Japan, in 1980, 1982, and 1985, respectively. He was with Toshiba Corporation from 1985 to 2004. He was a Professor at Polytechnic University, Japan, from 2004 to 2021, and is currently an Emeritus Professor there. He is also a Visiting Researcher at Hiroshima City University from 2021. His research interests include coding, signal processing, and security in communications. He received the 1987 Shinohara Memorial Young Engineer Award from IEICE. Dr. Yamasaki is a member of the Information Processing Society of Japan and IEEE.

Tomoko K. Matsushima received B.E., M.E. and Dr.E. degrees from Waseda University, Tokyo, Japan, in 1985, 1987, and 1999, respectively. From 1987 to 1994, she was with the Toshiba Corporate R & D Center, Kanagawa, Japan. She has been with Polytechnic University, Japan, since 1994, and is currently an Emerita Professor there. She is also a Professor at Yokohama College of Commerce from 2021. From 2001 to 2002, she was a Visiting Researcher at the University of Hawaii, U.S.A. Her research interests are coding theory and its applications. She received the 1991 Shinohara Memorial Young Engineer Award, and the 2008 Best Paper Award from IEICE. Dr. Matsushima is a member of the Information Processing Society of Japan and IEEE.