PAPER

Orthogonal Variable Spreading Factor Codes over Finite Fields***

Shoichiro YAMASAKI[†*a)], ***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 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 arbitrary field [12]. Row or column components of the DFT matrix yield the orthogonal sequences. The tree structure combining the sequences generates OVSF codes over finite fields when the DFT matrix is designed over prime fields or extension fields. The design method for the proposed codes is shown and examples of such codes are demonstrated.

Manuscript received January 8, 2021.
Manuscript revised May 13, 2021.
Manuscript publicized June 24, 2021.

[†]The authors are with Polytechnic University, Kodaira-shi, 187-0035 Japan.
[*]Presently, the author is with Hiroshima City University.
[**]Presently, the author is with Yokohama College of Commerce.

[***]The present study was presented in part in the IEICE Technical Report, vol.119, no.376, IT2019-66, pp.173–178, Jan. 2020.

a) E-mail: syamasa@uitec.ac.jp

DOI: 10.1587/transfun.2021EAP1001

The remainder of the present paper is organized as follows. The conventional OVSF codes are shown in Sect. 2, the properties of the DFT are shown in Sect. 3, and the proposed OVSF codes over finite fields are shown in Sect. 4.

2. Conventional OVSF Codes

2.1 Binary OVSF Codes

OVSF codes have been used in DS-CDMA wireless systems that support multi-rate communication services [6]–[9]. These codes are binary codes having elements in $\{+1, -1\}$. The two-point Hadamard matrix $S_{H,2}^{(2)}$ is shown as

$$S_{H,2}^{(2)} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} s_{H,2,0}^{(2)}{}^{T} & s_{H,2,1}^{(2)}{}^{T} \end{bmatrix}^{T}, \tag{1}$$

where $s_{H,2,0}^{(2)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$ and $s_{H,2,1}^{(2)} = \begin{bmatrix} 1 & -1 \end{bmatrix}$. $s_{H,2,i}^{(2)}$ corresponds to a Walsh code sequence of length 2 for $i = 0, 1$.

We define $r_{H,2,h}^{(2)}$ which is equal to $s_{H,2,h}^{(2)}$ for $h = 0, 1$. The inner product of $s_{H,2,i}^{(2)}$ and $r_{H,2,h}^{(2)}$ yields

$$s_{H,2,i}^{(2)} r_{H,2,h}^{(2)}{}^{T} = \begin{cases} 2 & (h = i), \\ 0 & (\text{otherwise}), \end{cases} \tag{2}$$

then $s_{H,2,i}^{(2)}$ and $r_{H,2,h}^{(2)}$ are orthogonal to each other for $h \neq i$.

We define an $M_1 \times M_1$ square matrix X and an $M_2 \times M_2$ square matrix Y respectively, then the Kronecker product [1] of X and Y generates the $M_1M_2 \times M_1M_2$ matrix Z as

$$\begin{aligned} Z &= X \otimes Y \\ &= \begin{bmatrix} x_{0,0}Y & x_{0,1}Y & \cdots & x_{0,M_1-1}Y \\ x_{1,0}Y & x_{1,1}Y & \cdots & x_{1,M_1-1}Y \\ \vdots & \vdots & \ddots & \vdots \\ x_{M_1-1,0}Y & x_{M_1-1,1}Y & \cdots & x_{M_1-1,M_1-1}Y \end{bmatrix}, \end{aligned} \tag{3}$$

where

$$X = \begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,M_1-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,M_1-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{M_1-1,0} & x_{M_1-1,1} & \cdots & x_{M_1-1,M_1-1} \end{bmatrix}. \tag{4}$$

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

$$S_{H,4}^{(2,2)} = S_{H,2}^{(2)} \otimes S_{H,2}^{(2)} = \begin{bmatrix} S_{H,2}^{(2)} & S_{H,2}^{(2)} \\ S_{H,2}^{(2)} & -S_{H,2}^{(2)} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} {s_{H,4,0}^{(2,2)}}^T & {s_{H,4,1}^{(2,2)}}^T & {s_{H,4,2}^{(2,2)}}^T & {s_{H,4,3}^{(2,2)}}^T \end{bmatrix}^T, \quad (5)$$

where $s_{H,4,i}^{(2,2)}$ is the ith row of $S_{H,4}^{(2,2)}$ for $i = 0, 1, 2, 3$. In addition, $s_{H,4,0}^{(2,2)}$, $s_{H,4,1}^{(2,2)}$, $s_{H,4,2}^{(2,2)}$ and $s_{H,4,3}^{(2,2)}$ correspond to Walsh sequences of length 4.

Next, we describe the superscripts attached to the matrices and sequences. The matrix $S_{H,n_1n_2}^{(n_1,n_2)}$ and the sequence $s_{H,n_1n_2,i}^{(n_1,n_2)}$ have superscripts of (n_1, n_2), which indicates that the Kronecker product of the n_2-point matrix $S_{H,n_2}^{(n_2)}$ and the n_1-point matrix $S_{H,n_1}^{(n_1)}$ generates the n_1n_2-point matrix $S_{H,n_1n_2}^{(n_1,n_2)}$ and the sequence $s_{H,n_1n_2,i}^{(n_1,n_2)}$ of length n_1n_2 for $i = 0, 1, \ldots, n_1n_2 - 1$. Furthermore, the Kronecker product of $S_{H,n_3}^{(n_3)}$ and $S_{H,n_1n_2}^{(n_1,n_2)}$ generates the $n_1n_2n_3$-point matrix $S_{H,n_1n_2n_3}^{(n_1,n_2,n_3)}$ and the sequence $s_{H,n_1n_2n_3,i}^{(n_1,n_2,n_3)}$ of length $n_1n_2n_3$ for $i = 0, 1, \ldots, n_1n_2n_3 - 1$.

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

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

$$= \begin{bmatrix} s_{H,8,0}^{(2,2,2)T} & s_{H,8,1}^{(2,2,2)T} & \cdots & s_{H,8,7}^{(2,2,2)T} \end{bmatrix}^T, \quad (6)$$

where $s_{H,8,i}^{(2,2,2)}$ is the ith row of $S_{H,8}^{(2,2,2)}$ for $i = 0, 1, \ldots, 7$ and $s_{H,8,0}^{(2,2,2)}, s_{H,8,1}^{(2,2,2)}, \ldots, s_{H,8,7}^{(2,2,2)}$ 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 halves of $s_{H,4,i}^{(2,2)}$ and orthogonal to the second halves of $s_{H,4,i}^{(2,2)}$ for $i = 1$ and 3. $s_{H,4,0}^{(2,2)}$ is orthogonal to the first halves of $s_{H,8,i}^{(2,2,2)}$ and orthogonal to the second halves of $s_{H,8,i}^{(2,2,2)}$ 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

$$S_{C,n} = \begin{bmatrix} \omega^0 & \omega^0 & \cdots & \omega^0 \\ \omega^0 & \omega^1 & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^0 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{bmatrix}, \quad (7)$$

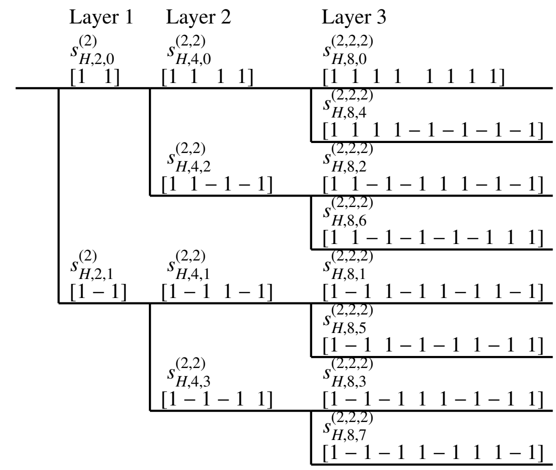

Fig. 1 Conventional binary OVSF codes.

where n is a positive integer. The complex number ω is a primitive nth root of unity and is represented by

$$\omega = e^{-j2\pi/n}, \quad (8)$$

where $j = \sqrt{-1}$. The n different nth 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 $s_{C,n,i} = \begin{bmatrix} \omega^0 & \omega^i & \cdots & \omega^{(n-1)i} \end{bmatrix}$ 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 ${r_{C,n,h}}^H$, where ${r_{C,n,h}}^H$ corresponds to a conjugate transpose of $r_{C,n,h}$, yields

$$s_{C,n,i}{r_{C,n,h}}^H = \begin{cases} n & (h = i), \\ 0 & \text{(otherwise)}. \end{cases} \quad (9)$$

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

$$S_{C,2}^{(2)} = \begin{bmatrix} \omega^0 & \omega^0 \\ \omega^0 & \omega^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} {s_{C,2,0}^{(2)}}^T & {s_{C,2,1}^{(2)}}^T \end{bmatrix}^T, \quad (10)$$

where $\omega = e^{-j2\pi/2} = -1$, $s_{C,2,0}^{(2)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$ and $s_{C,2,1}^{(2)} = \begin{bmatrix} 1 & -1 \end{bmatrix}$. 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

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

$$= \begin{bmatrix} {s_{C,4,0}^{(4)}}^T & {s_{C,4,1}^{(4)}}^T & {s_{C,4,2}^{(4)}}^T & {s_{C,4,3}^{(4)}}^T \end{bmatrix}^T, \quad (11)$$

where $\omega = e^{-j2\pi/4} = -j$ and $s_{C,4,i}^{(4)} = \begin{bmatrix} \omega^0 & \omega^i & \omega^{2i} & \omega^{3i} \end{bmatrix}$ for $i = 0, 1, 2, 3$. In addition, $s_{C,4,0}^{(4)}$, $s_{C,4,1}^{(4)}$, $s_{C,4,2}^{(4)}$ and $s_{C,4,3}^{(4)}$ 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

$$S_{C,8}^{(4,2)} = S_{C,2}^{(2)} \otimes S_{C,4}^{(4)} = \begin{bmatrix} S_{C,4}^{(4)} & S_{C,4}^{(4)} \\ S_{C,4}^{(4)} & -S_{C,4}^{(4)} \end{bmatrix}$$

$$= \begin{bmatrix} s_{C,8,0}^{(4,2)\,T} & s_{C,8,1}^{(4,2)\,T} & \cdots & s_{C,8,7}^{(4,2)\,T} \end{bmatrix}^T, \tag{12}$$

where $s_{C,8,i}^{(4,2)} = \begin{bmatrix} \omega^0 & \omega^i & \omega^{2i} & \omega^{3i} & \omega^0 & \omega^i & \omega^{2i} & \omega^{3i} \end{bmatrix}$ and $s_{C,8,i+4}^{(4,2)} = \begin{bmatrix} \omega^0 & \omega^i & \omega^{2i} & \omega^{3i} & -\omega^0 & -\omega^i & -\omega^{2i} & -\omega^{3i} \end{bmatrix}$ 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 subscript in this paper. Moreover, a is an element in the finite field and n is a positive integer that satisfies $a^n = 1$ and $a^i \neq 1$ for $i = 1, 2, \ldots, n-1$. In the finite field, we define $V = \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-1} \end{bmatrix}^T$ of length n. When referring to the notation shown in [12], the DFT operation of V generates $U = \begin{bmatrix} u_0 & u_1 & \cdots & u_{n-1} \end{bmatrix}^T$ as

$$U = S_{F,n} V, \tag{13}$$

$$S_{F,n} = \begin{bmatrix} a^0 & a^0 & \cdots & a^0 \\ a^0 & a^1 & \cdots & a^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a^0 & a^{n-1} & \cdots & a^{(n-1)^2} \end{bmatrix}$$
$$= \begin{bmatrix} s_{F,n,0}{}^T & s_{F,n,2}{}^T & \cdots & s_{F,n,n-1}{}^T \end{bmatrix}^T, \tag{14}$$

where $S_{F,n}$ is defined as an n-point DFT matrix and $S_{F,n} = S_{F,n}{}^T$. In addition, $s_{F,n,i}$ is the ith row of $S_{F,n}$ and is defined as

$$s_{F,n,i} = \begin{bmatrix} a^0 & a^i & a^{2i} & \cdots & a^{(n-1)i} \end{bmatrix}, \tag{15}$$

for $i = 0, 1, \ldots, n-1$. Each $s_{F,n,i}$ corresponds to a spreading code sequence of length n for data multiplexing.

We define the inverse element of a as a^{-1} such that $a \cdot a^{-1} = 1$ over the finite field. The n-point inverse DFT (IDFT) matrix is defined as

$$R_{F,n} = \begin{bmatrix} a^0 & a^0 & \cdots & a^0 \\ a^0 & a^{-1} & \cdots & a^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a^0 & a^{-(n-1)} & \cdots & a^{-(n-1)^2} \end{bmatrix}$$
$$= \begin{bmatrix} r_{F,n,0}{}^T & r_{F,n,1}{}^T & r_{F,n,2}{}^T & \cdots & r_{F,n,n-1}{}^T \end{bmatrix}^T, \tag{16}$$

where $R_{F,n} = R_{F,n}{}^T$, and $r_{F,n,h}$ is the hth row of $R_{F,n}$ for $h = 0, 1, \ldots, n-1$ and is defined as

$$r_{F,n,h} = \begin{bmatrix} a^0 & a^{-h} & a^{-2h} & \cdots & a^{-(n-1)h} \end{bmatrix}. \tag{17}$$

Each $r_{F,n,h}$ corresponds to a despreading code sequence of length n for data demultiplexing.

The inner product of $s_{F,n,i}$ and $r_{F,n,h}$, which is calculated by multiplying $s_{F,n,i}$ and $r_{F,n,h}{}^T$ over the finite field, yields

$$s_{F,n,i} r_{F,n,h}{}^T = \begin{cases} n_F & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \tag{18}$$

Therefore, $s_{F,n,i}$ 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 $s_{F,n,i} r_{F,n,h}{}^T = 1$ for $h = i$, the definition of $r_{F,n,h}$ in Eq. (17) is replaced with

$$r_{F,n,h} = n_F^{-1} \begin{bmatrix} a^0 & a^{-h} & a^{-2h} & \cdots & a^{-(n-1)h} \end{bmatrix}, \tag{19}$$

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 $p \geq 2$, 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

$$q - 1 = p_1^{e_1} p_2^{e_2} \cdots p_i^{e_i}, \tag{20}$$

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

$$d = (e_1 + 1)(e_2 + 1) \cdots (e_i + 1) - 1. \tag{21}$$

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 $q - 1 = 5 - 1 = 4 = 2^2$. The four-point DFT matrix $S_{F_5,4}^{(4)}$ over GF(5) is given as

$$S_{F_5,4}^{(4)} = \begin{bmatrix} a^0 & a^0 & a^0 & a^0 \\ a^0 & a^1 & a^2 & a^3 \\ a^0 & a^2 & a^4 & a^6 \\ a^0 & a^3 & a^6 & a^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$
$$= \begin{bmatrix} s_{F_5,4,0}^{(4)\,T} & s_{F_5,4,1}^{(4)\,T} & s_{F_5,4,2}^{(4)\,T} & s_{F_5,4,3}^{(4)\,T} \end{bmatrix}^T, \tag{22}$$

where $s_{F_5,4,i}^{(4)}$ is the ith row of $S_{F_5,4}^{(4)}$ for $i = 0, 1, 2, 3$.

The four-point IDFT matrix $R_{F_5,4}^{(4)}$ is given as

$$R^{(4)}_{F_5,4} = \begin{bmatrix} a^0 & a^0 & a^0 & a^0 \\ a^0 & a^{-1} & a^{-2} & a^{-3} \\ a^0 & a^{-2} & a^{-4} & a^{-6} \\ a^0 & a^{-3} & a^{-6} & a^{-9} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}$$
$$= \begin{bmatrix} r^{(4)\,T}_{F_5,4,0} & r^{(4)\,T}_{F_5,4,1} & r^{(4)\,T}_{F_5,4,2} & r^{(4)\,T}_{F_5,4,3} \end{bmatrix}^T, \quad (23)$$

where $r^{(4)}_{F_5,4,h}$ is the hth row of $R^{(4)}_{F_5,4}$ for $h = 0, 1, 2, 3$.

Multiplying $s^{(4)}_{F_5,4,i}$ and $r^{(4)\,T}_{F_5,4,h}$ over GF(5) yields

$$s^{(4)}_{F_5,4,i} r^{(4)\,T}_{F_5,4,h} = \begin{cases} 4 & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \quad (24)$$

Next, we focus on other 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 $S^{(2)}_{F_5,2}$ over GF(5) is written as

$$S^{(2)}_{F_5,2} = \begin{bmatrix} a^0 & a^0 \\ a^0 & a^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} s^{(2)\,T}_{F_5,2,0} & s^{(2)\,T}_{F_5,2,1} \end{bmatrix}^T, \quad (25)$$

where $s^{(2)}_{F_5,2,i}$ is the ith row of $S^{(2)}_{F_5,2}$ for $i = 0, 1$.

The two-point IDFT matrix $R^{(2)}_{F_5,2}$ is written as

$$R^{(2)}_{F_5,2} = \begin{bmatrix} a^0 & a^0 \\ a^0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} r^{(2)\,T}_{F_5,2,0} & r^{(2)\,T}_{F_5,2,1} \end{bmatrix}^T, \quad (26)$$

where $r^{(2)}_{F_5,2,h}$ is the hth row of $R^{(2)}_{F_5,2}$ for $h = 0, 1$.

Multiplying $s^{(2)}_{F_5,2,i}$ and $r^{(2)\,T}_{F_5,2,h}$ over GF(5) yields

$$s^{(2)}_{F_5,2,i} r^{(2)\,T}_{F_5,2,h} = \begin{cases} 2 & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \quad (27)$$

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 $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{254}\}$ in GF(2^8), where α is a primitive root of the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. In this case, $\alpha^{255} = 1$ and $\alpha^i \neq 1$ 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(2^8) [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 $a = \alpha$ in the n-point DFT, then the 255-point DFT matrix is given as

$$S^{(255)}_{F_{2^8},255} = \begin{bmatrix} \alpha^0 & \alpha^0 & \cdots & \alpha^0 \\ \alpha^0 & \alpha^1 & \cdots & \alpha^{254} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & \alpha^{254} & \cdots & \alpha^{254^2} \end{bmatrix}$$
$$= \begin{bmatrix} s^{(255)\,T}_{F_{2^8},255,0} & s^{(255)\,T}_{F_{2^8},255,1} & \cdots & s^{(255)\,T}_{F_{2^8},255,254} \end{bmatrix}^T, \quad (28)$$

$$s^{(255)}_{F_{2^8},255,i} = \begin{bmatrix} \alpha^0 & \alpha^i & \alpha^{2i} & \cdots & \alpha^{254i} \end{bmatrix}, \quad (29)$$

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

The 255-point IDFT matrix is given as

$$R^{(255)}_{F_{2^8},255} = \begin{bmatrix} \alpha^0 & \alpha^0 & \cdots & \alpha^0 \\ \alpha^0 & \alpha^{-1} & \cdots & \alpha^{-254} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & \alpha^{-254} & \cdots & \alpha^{-254^2} \end{bmatrix}$$
$$= \begin{bmatrix} r^{(255)\,T}_{F_{2^8},255,0} & r^{(255)\,T}_{F_{2^8},255,1} & \cdots & r^{(255)\,T}_{F_{2^8},255,254} \end{bmatrix}^T, \quad (30)$$
$$r^{(255)}_{F_{2^8},255,h} = \begin{bmatrix} \alpha^0 & \alpha^{-h} & \alpha^{-2h} & \cdots & \alpha^{-254h} \end{bmatrix}, \quad (31)$$

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

Multiplying $s^{(255)}_{F_{2^8},255,i}$ and $r^{(255)\,T}_{F_{2^8},255,h}$ over GF(2^8) yields

$$s^{(255)}_{F_{2^8},255,i} r^{(255)\,T}_{F_{2^8},255,h} = \begin{cases} 1 & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \quad (32)$$

For $h = i$, $s^{(255)}_{F_{2^8},255,i} r^{(255)\,T}_{F_{2^8},255,h} = 1$, 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 $a = \alpha^{85}$ in GF(2^8). Then $a^3 = 1$. The three-point DFT matrix $S^{(3)}_{F_{2^8},3}$ over GF(2^8) is given as

$$S^{(3)}_{F_{2^8},3} = \begin{bmatrix} a^0 & a^0 & a^0 \\ a^0 & a^1 & a^2 \\ a^0 & a^2 & a^4 \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^{85} & \alpha^{170} \\ \alpha^0 & \alpha^{170} & \alpha^{85} \end{bmatrix}$$
$$= \begin{bmatrix} s^{(3)\,T}_{F_{2^8},3,0} & s^{(3)\,T}_{F_{2^8},3,1} & s^{(3)\,T}_{F_{2^8},3,2} \end{bmatrix}^T, \quad (33)$$

where $s^{(3)}_{F_{2^8},3,i}$ is the ith row of $S^{(3)}_{F_{2^8},3}$ for $i = 0, 1, 2$.

The three-point IDFT matrix $R^{(3)}_{F_{2^8},3}$ is given as

$$R^{(3)}_{F_{2^8},3} = \begin{bmatrix} a^0 & a^0 & a^0 \\ a^0 & a^{-1} & a^{-2} \\ a^0 & a^{-2} & a^{-4} \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^{-85} & \alpha^{-170} \\ \alpha^0 & \alpha^{-170} & \alpha^{-85} \end{bmatrix}$$
$$= \begin{bmatrix} r^{(3)\,T}_{F_{2^8},3,0} & r^{(3)\,T}_{F_{2^8},3,1} & r^{(3)\,T}_{F_{2^8},3,2} \end{bmatrix}^T, \quad (34)$$

where $r^{(3)}_{F_{2^8},3,h}$ is the hth row of $R^{(3)}_{F_{2^8},3}$ for $h = 0, 1, 2$.

Multiplying $s^{(3)}_{F_{2^8},3,i}$ and $r^{(3)\,T}_{F_{2^8},3,h}$ over GF(2^8) yields

$$s^{(3)}_{F_{2^8},3,i} r^{(3)\,T}_{F_{2^8},3,h} = \begin{cases} 1 & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \quad (35)$$

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

$$S^{(5)}_{F_{2^8},5} = \begin{bmatrix} a^0 & a^0 & a^0 & a^0 & a^0 \\ a^0 & a^1 & a^2 & a^3 & a^4 \\ a^0 & a^2 & a^4 & a^6 & a^8 \\ a^0 & a^3 & a^6 & a^9 & a^{12} \\ a^0 & a^4 & a^8 & a^{12} & a^{16} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^{51} & \alpha^{102} & \alpha^{153} & \alpha^{204} \\ \alpha^0 & \alpha^{102} & \alpha^{204} & \alpha^{51} & \alpha^{153} \\ \alpha^0 & \alpha^{153} & \alpha^{51} & \alpha^{204} & \alpha^{102} \\ \alpha^0 & \alpha^{204} & \alpha^{153} & \alpha^{102} & \alpha^{51} \end{bmatrix}$$
$$= \begin{bmatrix} s^{(5)}_{F_{2^8},5,0}{}^T & s^{(5)}_{F_{2^8},5,1}{}^T & \cdots & s^{(5)}_{F_{2^8},5,4}{}^T \end{bmatrix}^T, \tag{36}$$

where $s^{(5)}_{F_{2^8},5,i}$ is the ith row of $S^{(5)}_{F_{2^8},5}$ for $i = 0, 1, 2, 3, 4$.

The five-point IDFT matrix $R^{(5)}_{F_{2^8},5}$ is written as

$$R^{(5)}_{F_{2^8},5} = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^{-51} & \alpha^{-102} & \alpha^{-153} & \alpha^{-204} \\ \alpha^0 & \alpha^{-102} & \alpha^{-204} & \alpha^{-51} & \alpha^{-153} \\ \alpha^0 & \alpha^{-153} & \alpha^{-51} & \alpha^{-204} & \alpha^{-102} \\ \alpha^0 & \alpha^{-204} & \alpha^{-153} & \alpha^{-102} & \alpha^{-51} \end{bmatrix}$$
$$= \begin{bmatrix} r^{(5)}_{F_{2^8},5,0}{}^T & r^{(5)}_{F_{2^8},5,1}{}^T & \cdots & r^{(5)}_{F_{2^8},5,4}{}^T \end{bmatrix}^T, \tag{37}$$

where $r^{(5)}_{F_{2^8},5,h}$ is the hth row of $R^{(5)}_{F_{2^8},5}$ for $h = 0, 1, 2, 3, 4$.

Multiplying $s^{(5)}_{F_{2^8},5,i}$ and $r^{(5)}_{F_{2^8},5,h}{}^T$ over GF(2^8) yields

$$s^{(5)}_{F_{2^8},5,i} r^{(5)}_{F_{2^8},5,h}{}^T = \begin{cases} 1 & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \tag{38}$$

4. Proposed OVSF Codes over Finite Fields

The multiplication of the ith row of the n-point DFT matrix and the hth 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), $q-1$ 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_l-point DFT matrix $S^{(n_l)}_{F_q,n_l}$ is applied to construct the codes for $l = 1, 2, \ldots, L$. Each n_l is selected from $f_1, f_2, \ldots, f_d$ arbitrarily. Therefore, there exist d^L kinds of code tree. The code length in Layer l is defined as k_l and is decided as $k_l = \prod_{i=1}^{l} n_i$.

Next, we present examples. In the case of GF(q) for $q = p = 7$, $q-1$ is factorized as $q - 1 = 6 = 2 \cdot 3$, then the divisors of $q-1$ are $f_1 = 2$, $f_2 = 3$ and $f_3 = 6$, and the number of divisors is $d = 3$. For $L = 3$, there exist $27 (= d^L = 3^3)$ kinds of code tree. Table 1 shows 27 kinds of (n_1, n_2, n_3), where each n_l 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).

Table 1 DFT-points (n_1, n_2, n_3) and code lengths (k_1, k_2, k_3) for $L = 3$ and GF(7).

n_1	2	2	2	2	2	2	2	2	2
n_2	2	2	2	3	3	3	6	6	6
n_3	2	3	6	2	3	6	2	3	6
k_1	2	2	2	2	2	2	2	2	2
k_2	4	4	4	6	6	6	12	12	12
k_3	8	12	24	12	18	36	24	36	72
n_1	3	3	3	3	3	3	3	3	3
n_2	2	2	2	3	3	3	6	6	6
n_3	2	3	6	2	3	6	2	3	6
k_1	3	3	3	3	3	3	3	3	3
k_2	6	6	6	9	9	9	18	18	18
k_3	12	18	36	18	27	54	36	54	108
n_1	6	6	6	6	6	6	6	6	6
n_2	2	2	2	3	3	3	6	6	6
n_3	2	3	6	2	3	6	2	3	6
k_1	6	6	6	6	6	6	6	6	6
k_2	12	12	12	18	18	18	36	36	36
k_3	24	36	72	36	54	108	72	108	216

In the case of GF(q) for $q = 2^8$, $q-1$ is factorized as $q - 1 = 3 \cdot 5 \cdot 17$. Then, the number of divisors is $d = 7$, as shown in Eq. (21). For $L = 3$, there exist $343 (= d^L = 7^3)$ 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 $a^i \neq 1$ for $i = 1, 2, \ldots, q-2$, then the n_1-point DFT matrix $S^{(n_1)}_{F_q,n_1}$ for Layer 1 is written as

$$S^{(n_1)}_{F_q,n_1} = \begin{bmatrix} s^{(n_1)}_{F_q,n_1,0}{}^T & s^{(n_1)}_{F_q,n_1,1}{}^T & \cdots & s^{(n_1)}_{F_q,n_1,n_1-1}{}^T \end{bmatrix}^T, \tag{39}$$

where $s^{(n_1)}_{F_q,n_1,i_1} = \begin{bmatrix} b_1^0 & b_1^{i_1} & b_1^{2i_1} & \cdots & b_1^{(n_1-1)i_1} \end{bmatrix}$ is the i_1th row of $S^{(n_1)}_{F_q,n_1}$ and corresponds to the code sequence of length n_1 in Layer 1 for $b_1 = a^{(q-1)/n_1}$ and $i_1 = 0, 1, \ldots, n_1 - 1$. In addition, the n_2-point DFT matrix $S^{(n_2)}_{F_q,n_2}$ is written as

$$S^{(n_2)}_{F_q,n_2} = \begin{bmatrix} s^{(n_2)}_{F_q,n_2,0}{}^T & s^{(n_2)}_{F_q,n_2,1}{}^T & \cdots & s^{(n_2)}_{F_q,n_2,n_2-1}{}^T \end{bmatrix}^T, \tag{40}$$

where $s^{(n_2)}_{F_q,n_2,i} = \begin{bmatrix} b_2^0 & b_2^{i} & b_2^{2i} & \cdots & b_2^{(n_2-1)i} \end{bmatrix}$ is the ith row of $S^{(n_2)}_{F_q,n_2}$ for $b_2 = a^{(q-1)/n_2}$ and $i = 0, 1, \ldots, n_2 - 1$.

The Kronecker product of $S^{(n_2)}_{F_q,n_2}$ and $S^{(n_1)}_{F_q,n_1}$ generates the $n_1 n_2$-point matrix $S^{(n_1,n_2)}_{F_q,n_1 n_2}$ for Layer 2 as

$$S^{(n_1,n_2)}_{F_q,n_1 n_2} = S^{(n_2)}_{F_q,n_2} \otimes S^{(n_1)}_{F_q,n_1}$$
$$= \begin{bmatrix} s^{(n_1,n_2)}_{F_q,n_1 n_2,0}{}^T & s^{(n_1,n_2)}_{F_q,n_1 n_2,1}{}^T & \cdots & s^{(n_1,n_2)}_{F_q,n_1 n_2,n_1 n_2-1}{}^T \end{bmatrix}^T, \tag{41}$$

where $s^{(n_1,n_2)}_{F_q,n_1 n_2,i_2}$ is the i_2th row of $S^{(n_1,n_2)}_{F_q,n_1 n_2}$ and corresponds to the code sequence of length $n_1 n_2$ in Layer 2 for $i_2 = 0, 1, \ldots, n_1 n_2 - 1$. Then, the n_2 code sequences $s^{(n_1,n_2)}_{F_q,n_1 n_2,i_1}$, $s^{(n_1,n_2)}_{F_q,n_1 n_2,i_1+n_1}$, $s^{(n_1,n_2)}_{F_q,n_1 n_2,i_1+2n_1}$, $\ldots$, $s^{(n_1,n_2)}_{F_q,n_1 n_2,i_1+(n_2-1)n_1}$ of Layer 2 are the descendants of $s^{(n_1)}_{F_q,n_1,i_1}$ of Layer 1 for $i_1 =$

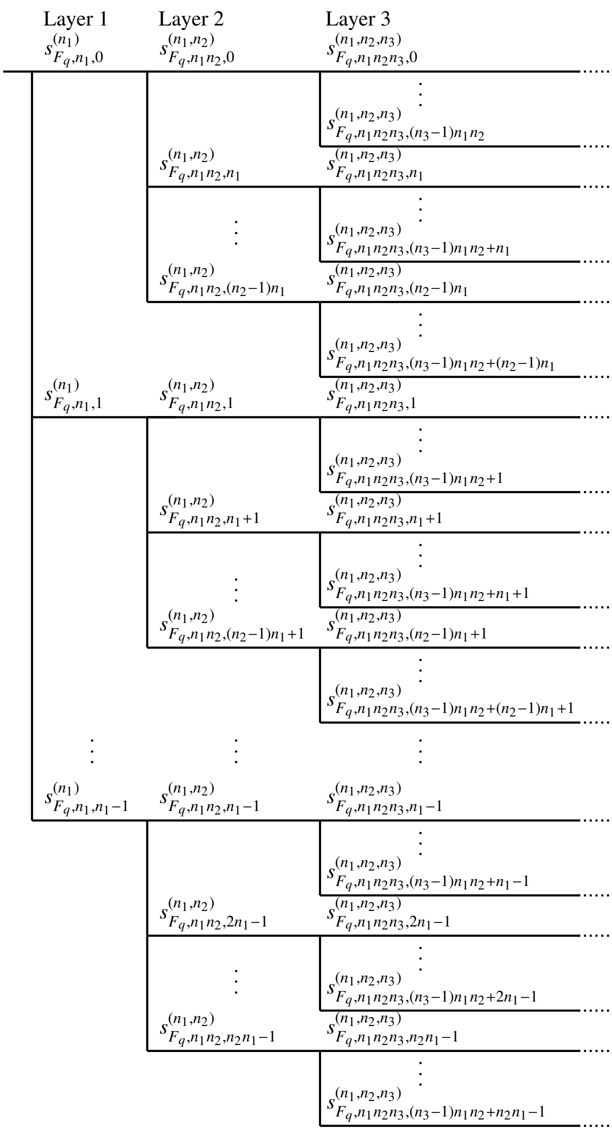

Fig. 2 The proposed OVSF codes based on DFT over GF(q), which are used as spreading sequences for data multiplexing.

$0, 1, \ldots, n_1 - 1$ in the code tree shown in Fig. 2.

For $l = 2, 3, \ldots, L$, the Kronecker product of the n_l-point DFT matrix $S^{(n_l)}_{F_q,n_l}$ and the $n_1n_2\cdots n_{l-1}$-point matrix $S^{(n_1,n_2,\ldots,n_{l-1})}_{F_q,n_1n_2\cdots n_{l-1}}$ generates the $n_1n_2\cdots n_l$-point matrix $S^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l}$ for Layer l as

$$\begin{aligned} S^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l} &= S^{(n_l)}_{F_q,n_l} \otimes S^{(n_1,n_2,\ldots,n_{l-1})}_{F_q,n_1n_2\cdots n_{l-1}} \\ &= \left[\, s^{(n_1,n_2,\ldots,n_l)\,T}_{F_q,n_1n_2\cdots n_l,0} \quad s^{(n_1,n_2,\ldots,n_l)\,T}_{F_q,n_1n_2\cdots n_l,1} \quad \cdots \quad s^{(n_1,n_2,\ldots,n_l)\,T}_{F_q,n_1n_2\cdots n_l,n_1n_2\cdots n_l-1} \right]^T, \end{aligned} \tag{42}$$

where $s^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l,i_l}$ is the i_lth row of $S^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l}$ and corresponds to the code sequence of length $n_1n_2\cdots n_l$ in Layer l for $i_l = 0, 1, \ldots, n_1n_2\cdots n_l - 1$. Then, the n_l code sequences $s^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l,i_{l-1}}$, $s^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l,i_{l-1}+n_1n_2\cdots n_{l-1}}$, $s^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l,i_{l-1}+2n_1n_2\cdots n_{l-1}}$, $\ldots$, $s^{(n_1,n_2,\ldots,n_l)}_{F_q,n_1n_2\cdots n_l,i_{l-1}+(n_l-1)n_1n_2\cdots n_{l-1}}$ of Layer l are the descendants of $s^{(n_1,n_2,\ldots,n_{l-1})}_{F_q,n_1n_2\cdots n_{l-1},i_{l-1}}$ of Layer $l-1$ for $i_{l-1} = 0, 1, \ldots, n_1n_2\cdots n_{l-1} - 1$ in the code tree.

The code sequences 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 $S^{(2)}_{F_5,2}$ and $S^{(4)}_{F_5,4}$ generates $S^{(4,2)}_{F_5,8}$ as

$$\begin{aligned} S^{(4,2)}_{F_5,8} &= S^{(2)}_{F_5,2} \otimes S^{(4)}_{F_5,4} = \begin{bmatrix} 1\cdot S^{(4)}_{F_5,4} & 1\cdot S^{(4)}_{F_5,4} \\ 1\cdot S^{(4)}_{F_5,4} & 4\cdot S^{(4)}_{F_5,4} \end{bmatrix} \\ &= \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&2&4&3&1&2&4&3 \\ 1&4&1&4&1&4&1&4 \\ 1&3&4&2&1&3&4&2 \\ 1&1&1&1&4&4&4&4 \\ 1&2&4&3&4&3&1&2 \\ 1&4&1&4&4&1&4&1 \\ 1&3&4&2&4&2&1&3 \end{bmatrix} \\ &= \left[\, s^{(4,2)\,T}_{F_5,8,0} \quad s^{(4,2)\,T}_{F_5,8,1} \quad \cdots \quad s^{(4,2)\,T}_{F_5,8,7} \right]^T, \end{aligned} \tag{43}$$

where $s^{(4,2)}_{F_5,8,i}$ of length 8 is the ith row of $S^{(4,2)}_{F_5,8}$ for $i = 0, 1, \ldots, 7$.

The inverse matrix of $S^{(4,2)}_{F_5,8}$ is obtained as

$$\begin{aligned} R^{(4,2)}_{F_5,8} &= R^{(2)}_{F_5,2} \otimes R^{(4)}_{F_5,4} = \begin{bmatrix} 1\cdot R^{(4)}_{F_5,4} & 1\cdot R^{(4)}_{F_5,4} \\ 1\cdot R^{(4)}_{F_5,4} & 4\cdot R^{(4)}_{F_5,4} \end{bmatrix} \\ &= \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&3&4&2&1&3&4&2 \\ 1&4&1&4&1&4&1&4 \\ 1&2&4&3&1&2&4&3 \\ 1&1&1&1&4&4&4&4 \\ 1&3&4&2&4&2&1&3 \\ 1&4&1&4&4&1&4&1 \\ 1&2&4&3&4&3&1&2 \end{bmatrix} \\ &= \left[\, r^{(4,2)\,T}_{F_5,8,0} \quad r^{(4,2)\,T}_{F_5,8,1} \quad \cdots \quad r^{(4,2)\,T}_{F_5,8,7} \right]^T, \end{aligned} \tag{44}$$

where $r^{(4,2)}_{F_5,8,h}$ of length 8 is the hth row of $R^{(4,2)}_{F_5,8}$ for $h = 0, 1, \ldots, 7$.

Multiplying $s^{(4,2)}_{F_5,8,i}$ and $r^{(4,2)\,T}_{F_5,8,h}$ over GF(5) yields

$$s^{(4,2)}_{F_5,8,i} r^{(4,2)\,T}_{F_5,8,h} = \begin{cases} 3 & (h = i), \\ 0 & (\text{otherwise}). \end{cases} \tag{45}$$

When we refer to Eq. (42), the Kronecker product of $S^{(2)}_{F_5,2}$ and $S^{(4,2)}_{F_5,8}$ generates $S^{(4,2,2)}_{F_5,16}$ over GF(5) as

$$\begin{aligned} S^{(4,2,2)}_{F_5,16} &= S^{(2)}_{F_5,2} \otimes S^{(4,2)}_{F_5,8} = \begin{bmatrix} 1\cdot S^{(4,2)}_{F_5,8} & 1\cdot S^{(4,2)}_{F_5,8} \\ 1\cdot S^{(4,2)}_{F_5,8} & 4\cdot S^{(4,2)}_{F_5,8} \end{bmatrix} \\ &= \left[\, s^{(4,2,2)\,T}_{F_5,16,0} \quad s^{(4,2,2)\,T}_{F_5,16,1} \quad \cdots \quad s^{(4,2,2)\,T}_{F_5,16,15} \right]^T, \end{aligned} \tag{46}$$

where $s^{(4,2,2)}_{F_5,16,i}$ of length 16 is the ith row of $S^{(4,2,2)}_{F_5,16}$ for $i =$

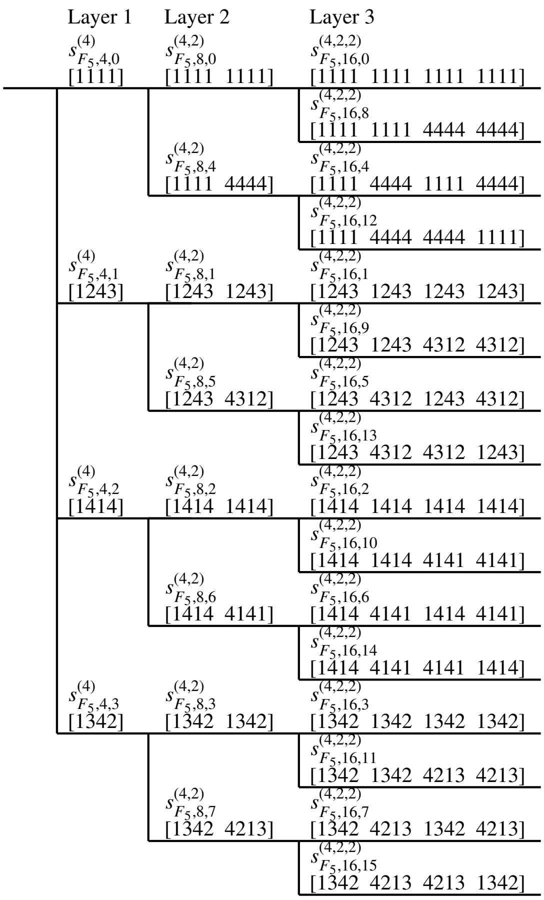

Fig. 3 Example of the proposed three-layer OVSF codes based on DFT over GF(5), which are used as spreading sequences for data multiplexing.

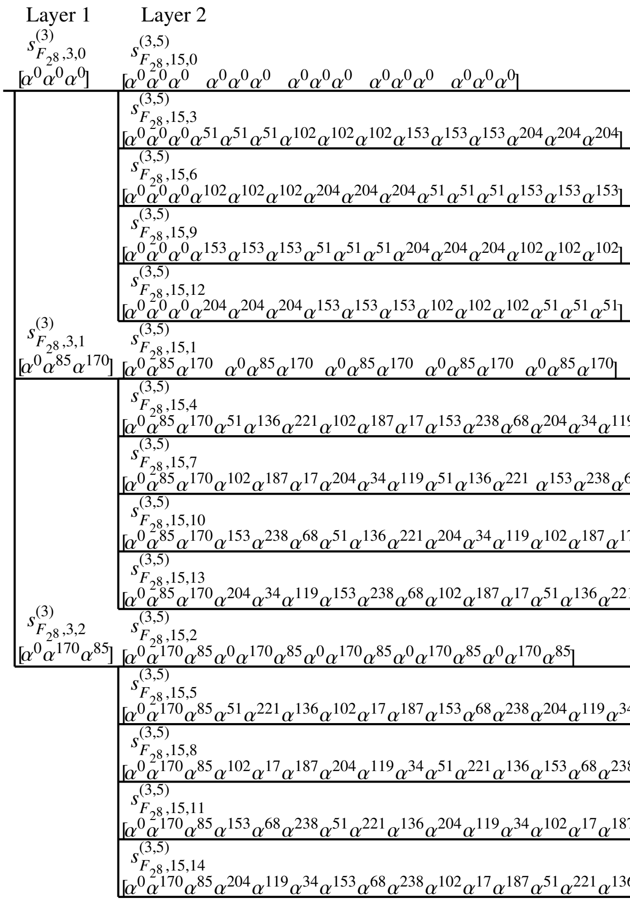

Fig. 4 Example of the proposed two-layer OVSF codes based on DFT over GF(2^8), which are used as spreading sequences for data multiplexing.

$0, 1, \ldots, 15$.

The inverse matrix of $S^{(4,2,2)}_{F_5,16}$ is derived as

$$R^{(4,2,2)}_{F_5,16} = R^{(2)}_{F_5,2} \otimes R^{(4,2)}_{F_5,8} = \begin{bmatrix} 1 \cdot R^{(4,2)}_{F_5,8} & 1 \cdot R^{(4,2)}_{F_5,8} \\ 1 \cdot R^{(4,2)}_{F_5,8} & 4 \cdot R^{(4,2)}_{F_5,8} \end{bmatrix}$$
$$= \begin{bmatrix} r^{(4,2,2)\,T}_{F_5,16,0} & r^{(4,2,2)\,T}_{F_5,16,1} & \cdots & r^{(4,2,2)\,T}_{F_5,16,15} \end{bmatrix}^T, \quad (47)$$

where $r^{(4,2,2)}_{F_5,16,h}$ of length 16 is the hth row of $R^{(4,2,2)}_{F_5,16}$ for $h = 0, 1, \ldots, 15$.

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 $s^{(4,2)}_{F_5,8,5}$, or the sequence [4 3 1 2], which is the second half of $s^{(4,2)}_{F_5,8,5}$, is not orthogonal to $r^{(4)}_{F_5,4,1} = [1\ 3\ 4\ 2]$. Moreover, the sequence [1 2 4 3 4 3 1 2], which is the first half of $s^{(4,2,2)}_{F_5,16,13}$, or the sequence [4 3 1 2 1 2 4 3], which is the second half of $s^{(4,2,2)}_{F_5,16,13}$, is not orthogonal to $r^{(4,2)}_{F_5,8,5} = [1\ 3\ 4\ 2\ 4\ 2\ 1\ 3]$. 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(2^8), the Kronecker product of $S^{(5)}_{F_{2^8},5}$ and $S^{(3)}_{F_{2^8},3}$ generates $S^{(3,5)}_{F_{2^8},15}$ as

$$S^{(3,5)}_{F_{2^8},15} = S^{(5)}_{F_{2^8},5} \otimes S^{(3)}_{F_{2^8},3}$$
$$= \begin{bmatrix} S^{(3)}_{F_{2^8},3} & S^{(3)}_{F_{2^8},3} & S^{(3)}_{F_{2^8},3} & \cdots & S^{(3)}_{F_{2^8},3} \\ S^{(3)}_{F_{2^8},3} & \alpha^{51} S^{(3)}_{F_{2^8},3} & \alpha^{102} S^{(3)}_{F_{2^8},3} & \cdots & \alpha^{204} S^{(3)}_{F_{2^8},3} \\ S^{(3)}_{F_{2^8},3} & \alpha^{102} S^{(3)}_{F_{2^8},3} & \alpha^{204} S^{(3)}_{F_{2^8},3} & \cdots & \alpha^{153} S^{(3)}_{F_{2^8},3} \\ S^{(3)}_{F_{2^8},3} & \alpha^{153} S^{(3)}_{F_{2^8},3} & \alpha^{51} S^{(3)}_{F_{2^8},3} & \cdots & \alpha^{102} S^{(3)}_{F_{2^8},3} \\ S^{(3)}_{F_{2^8},3} & \alpha^{204} S^{(3)}_{F_{2^8},3} & \alpha^{153} S^{(3)}_{F_{2^8},3} & \cdots & \alpha^{51} S^{(3)}_{F_{2^8},3} \end{bmatrix},$$
$$= \begin{bmatrix} s^{(3,5)\,T}_{F_{2^8},15,0} & s^{(3,5)\,T}_{F_{2^8},15,1} & \cdots & s^{(3,5)\,T}_{F_{2^8},15,14} \end{bmatrix}^T, \quad (48)$$

where $s^{(3,5)}_{F_{2^8},15,i}$ of length 15 is the ith row of $S^{(3,5)}_{F_{2^8},15}$ for $i = 0, 1, \ldots, 14$. These sequences construct the code tree of the OVSF codes over GF(2^8), as shown in Fig. 4. Since the DFTs of lengths 3, 5, 15, 17, 51, 85, and 255 exist over GF(2^8), combining these DFTs in multiple layers realizes the various OVSF codes over GF(2^8).

4.3 Advantages of the Proposed Codes

We investigate the advantages of the proposed codes. Any

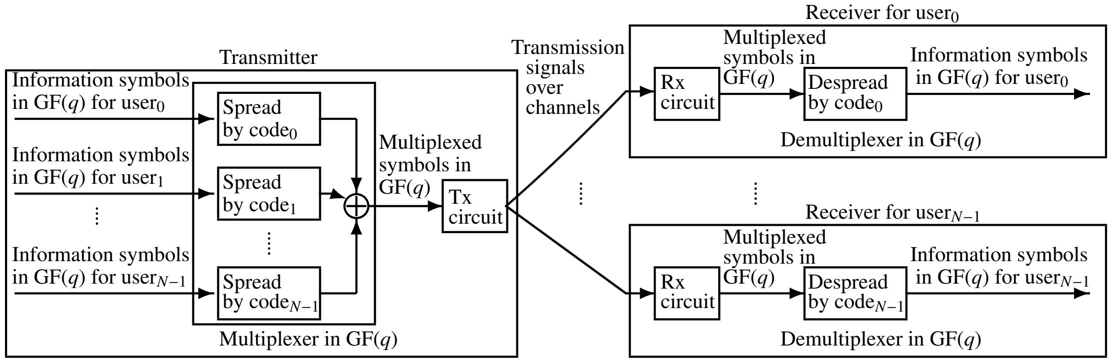

Fig. 5 Downlink system configuration for the proposed codes.

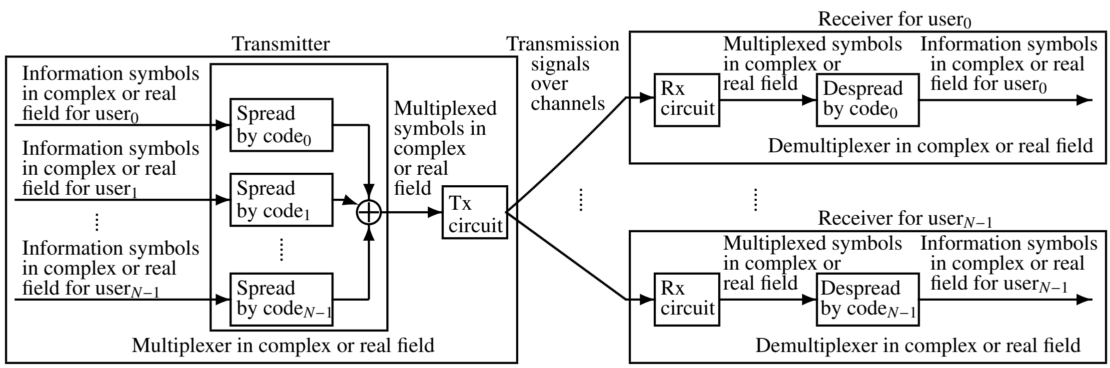

Fig. 6 Downlink system configuration for the conventional codes.

of the proposed OVSF codes has a layered structure with L Layers for $L \geq 2$. Combining the DFT matrices of points $n_1, n_2, \ldots, n_l$ over GF(q) generates the code sequence of Layer l for $l = 1, 2, \ldots, L$. The value n_l is selected from the d divisors of $q-1$, except for one. These d divisors are defined as $f_1, f_2, \ldots, f_d$ and are decided by the factorization of $q-1$ using prime numbers, as shown in Eq. (20). Therefore, d^L kinds of code tree exist and the various code lengths are obtained, because the code length on Layer l is decided as $\prod_{i=1}^{l} n_i$. The proposed codes realize multi-rate communications with various code lengths.

The conventional OVSF code [6]–[9] also has a layered structure with L Layers for $L \geq 2$. Combining the Hadamard matrices of points $n_1, n_2, \ldots, n_l$ generates 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 α is a primitive root of the primitive polynomial $p(x) = x^2+x+1$. 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(2^2). 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(2^2) 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$_i$ for $i = 0, 1, \cdots, N-1$, 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 each user are spread by an assigned code sequence, and the spread sequence symbols for N users are multiplexed over the real or the complex field operation. Multiplexing causes expansion of the range for symbol values.

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 transforms 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.

Acknowledgments

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

[1] A. Goldsmith, Wireless Communications, Cambridge University Press, NY, Oct. 2005.
[2] E.H. Dinan and B. Jabbar, "Spreading codes for direct sequence CDMA and wideband CDMA cellular networks," IEEE Commun. Mag., vol.36, no.9, pp.48–54, Sept. 1998.
[3] F. Adachi, M. Sawahashi, and H. Suda, "Wideband DS-CDMA for next-generation mobile communications systems," IEEE Commun. Mag., vol.36, no.9, pp.56–69, Sept. 1998.
[4] R.L. Frank, "Polyphase complementary codes," IEEE Trans. Inf. Theory, vol.26, no.6, pp.641–647, Nov. 1980.
[5] T. Kojima, "Hadamard-type matrices on finite fields and complete complementary codes," IEICE Trans. Fundamentals, vol.E102-A, no.12, pp.1651–1658, Dec. 2019.
[6] F. Adachi, M. Sawahashi, and K. Okawa, "Tree structured generation of orthogonal spreading codes with different lengths for forward link of DS-CDMA mobile radio," Electron. Lett., vol.33, no.1, pp.27–28, Jan. 1997.
[7] K. Okawa and F. Adachi, "Orthogonal forward link using orthogonal multi-spreading factor codes for coherent DS-CDMA mobile radio," IEICE Trans. Commun., vol.E81-B, no.4, pp.777–784, April 1998.
[8] T. Inoue, D. Garg, and F. Adachi, "Study on the OVSF code selection for downlink MC-CDMA," IEICE Trans. Commun., vol.E88-B, no.2, pp.499–508, Feb. 2005.
[9] Q. Yu, F. Adachi, and W. Meng, "Adaptive code assignment algorithm for a multi-user/multi-rate CDMA system," IEICE Trans. Commun., vol.E92-B, no.5, pp.1600–1607, May 2009.
[10] T.K. Matsushima and S. Yamasaki, "Construction method of orthogonal variable spreading factor codes over the complex number field," Proc. 42nd Symposium on Information Theory and Its Applications (SITA2019), 1.4.3, pp.72–77, Nov. 2019.
[11] T.K. Matsushima and S. Yamasaki, "Complex orthogonal variable spreading factor codes based on polyphase sequences," IEICE Trans. Fundamentals, vol.E103-A, no.10, pp.1218–1226, Oct. 2020.
[12] R.E. Blahut, Algebraic Methods for Signal Processing and Communications Coding, Chapter 3, Sringer-Verlag, 1992.

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 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.