Signature Codes to Remove Interference Light in Synchronous Optical Code-Division Multiple Access Systems

Tomoko K. MATSUSHIMA†, Member, Shoichiro YAMASAKI†, Senior Member, and Kyohei ONO†, Nonmember

SUMMARY This paper proposes a new class of signature codes for synchronous optical code-division multiple access (CDMA) and describes a general method for construction of the codes. The proposed codes can be obtained from generalized modified prime sequence codes (GMPSCs) based on extension fields GF(q), where q = pm, p is a prime number, and m is a positive integer. It has been reported that optical CDMA systems using GMPSCs remove not only multi-user interference but also optical interference (e.g., background light) with a constant intensity during a slot of length q. Recently, the authors have reported that optical CDMA systems using GMPSCs also remove optical interference with intensity varying by blocks with a length of q. The proposed codes, referred to as p-chip codes in general and chip-pair codes in particular for the case of p = 2, have the property of removing interference light with an intensity varying by shorter blocks with a length of p without requiring additional equipment. The present paper also investigates the algebraic properties and applications of the proposed codes.

key words: optical CDMA, generalized modified prime sequence code, p-chip code, chip-pair code, interference cancellation, background light

1. Introduction

The optical code-division multiple access (CDMA) technique has been studied to realize multiple-user transmission and reception in optical communication systems [1],[2]. Modified prime sequence codes (MPSCs) [3],[4] and generalized MPSCs (GMPSCs) [5],[6] are signature codes proposed for synchronous optical CDMA. An MPSC is generated from a prime field and a GMPSC is generated from an extension field. If the field has q elements and is represented as GF(q), both codes are composed of q² codewords with a length of q². For a GMPSC, q = pm where p is a prime number and m is a positive integer, while q is a prime number for an MPSC. Although MPSCs and GMPSCs are non-orthogonal codes, it has been shown that multi-user interference (MUI) is completely canceled when they are used with appropriate MUI cancellation schemes, such as Shalaby’s scheme [7], Liu’s scheme [8], or the equal-weight orthogonal (EWO) scheme [9],[10], in synchronous optical CDMA systems.

Recently, it was reported that optical CDMA systems using MPSCs or GMPSCs have the ability to remove interference light, such as background light and other optical signals, simultaneously with MUI at each user’s decoder. In Ref. [11], it is shown that interference light with a constant intensity within a code length is canceled at the decoder completely when the system adopts the EWO scheme, Shalaby’s scheme, or a modified Liu’s scheme for MUI cancellation. In general, ambient light interference mostly exists in the spectrum up to around 60 Hz [12], and the intensity of such interference light can be considered to be constant over the length of the signature code. Furthermore, it has been reported that interference light is removed even if its intensity varies by blocks with a length of q chips. Using this property, an optical CDMA system employing both an extended bi-orthogonal code [13] and a GMPSC has been proposed [14],[15]. In addition, in Ref. [16], the authors showed that there exists a GMPSC that has the property of removing interference light with an intensity that varies by a shorter block two chips long when q is equal to 2². However, they also recognized that not every GMPSC has this property.

In this paper, we propose a new class of GMPSCs that has the property of removing interference light whose intensity varies by p chips. The proposed codes are referred to as p-chip codes in general and chip-pair codes in particular for the case of p = 2 in this paper. We describe a general construction method for the proposed codes, which can be constructed from any extension field GF(pᵐ) by adding some actions to the conventional method for constructing GMPSCs. Furthermore, this paper investigates the algebraic properties and applications of the proposed p-chip and chip-pair codes.

This work was partially presented in Refs. [16],[17], and [18].

2. p-chip codes and chip-pair codes

2.1 Preliminaries

The mathematical concept of finite fields provides an important framework for designing signal sequences [19],[20]. The codes proposed in this paper are based on the arithmetic properties of finite fields.

Let F be the set of all elements in GF(pm), where p is a prime number and m is a positive integer. F is represented as follows:

\[ F = \{ 0, 1, \alpha, \alpha^2, \cdots, \alpha^{m-2} \}, \]

where \( \alpha \) is a primitive element of GF(pm) satisfying \( \pi(\alpha) = 0 \) for an m-degree primitive polynomial \( \pi(x) \) over GF(p). Then, we define a relation R on F as follows:
codes proposed for synchronous optical CDMA. GMPSCs are a generalized version of MPSCs and have the same correlation property as MPSCs. Although MPSCs are generated only from prime fields, GMPSCs are generated from extension fields GF($p^m$).

A GMPSC consists of $p^{2m}$ codewords, which can be divided into $p^m$ groups of $p^m$ codewords each. Every codeword has a code length of $p^{2m}$ and a Hamming weight of $p^m$. Every GMPSC has a special correlation property in a synchronous system, as shown in the following equation [5],[6]:

$$\Gamma(c_{i,j}, c_{i,j}) = \begin{cases} p^m & \text{if } i_1 = i_2 \text{ and } j_1 = j_2, \\ 0 & \text{if } i_1 = i_2 \text{ and } j_1 \neq j_2, \\ 1 & \text{if } i_1 \neq i_2. \end{cases} \quad (4)$$

where $c_{i,j}$ is the $j$th codeword in the $i$th group ($i, j = 0, 1, \ldots, p^m - 1$) and $\Gamma(a, b)$ is the auto- or cross-correlation function between two sequences $a$ and $b$ at zero shift.

Equation (4) shows that GMPSCs have the same correlation property as the original MPSCs. Therefore, the conventional MUI cancellation schemes [7]–[10] can be applied to optical CDMA systems using GMPSCs instead of the original MPSCs. The EWO scheme is one such MUI cancellation scheme [9],[10]. In the EWO scheme, multiple equal-weight and orthogonal codewords are assigned to each user. The transmitter for each user chooses one of the assigned codewords according to the transmission data and transmits the chosen codeword as an optical sequence. The optical sequences from all the users are multiplexed over the channel, and the multiplexed sequence is received by all receivers. At each receiver, MUI is removed and the transmission data are estimated by each user’s decoder.

In practical wireless optical communication, the received sequence includes not only the multiplexed sequence of transmitted codewords but also interference light (e.g., background light) at the receiver. Figure 1 illustrates some examples of the multiplexed sequence and the interference light received at the optical CDMA system using a GMPSC of $p^m = 4$ and the EWO scheme. Figure 1(a) shows the sequences transmitted from eight users simultaneously. Each GMPSC codeword consists of positive chips, called marks and denoted by 1s, and null chips, called spaces and denoted by 0s. In this paper, a slot represents a time period during which one codeword consisting of $p^{2m}$ chips is transmitted, and a block represents a set of $p^m$ chips when one slot is divided into $p^m$ parts of equal length, as shown in Fig. 1(a). If the main component of the interference light is sunlight, the intensity of the interference light is considered to be constant within each slot, as shown in Fig. 1(b). It has been reported that an optical CDMA system using an MPSC or GMPSC removes MUI and interference light simultaneously at the decoder, when the interference light intensity is constant within a slot and an adequate MUI cancellation scheme is adopted [11]. Ref. [11] presents three different schemes for canceling interference light and MUI simultaneously, and one of these is the EWO scheme. Through the discussion in [11], we have obtained a further result that the interference light can be removed at the decoder, when its
 intensity varies by block as shown in Fig. 1(c). In Appendix B, we explain how the decoder removes interference light that varies by block when a GMPC is used as a signature code.

2.3 Procedure for construction of \( p \)-chip codes

The proposed \( p \)-chip codes are codes having the ability to remove interference light with an intensity that varies by \( p \) chips, as shown in Fig. 1(d), when they are used with the EWO scheme. In particular, we referred to the \( p \)-chip codes as chip-pair codes when \( p = 2 \). In the construction procedure of a \( p \)-chip code, we first generate a code \( C^* \) over GF\((p^m)\), and then we transform it into a binary \( p \)-chip code \( C \). The length of code \( C^* \) is \( p^m \) symbols, and the length of code \( C \) is \( p^{2m} \) chips. Each code consists of \( p^{2m} \) codewords, which can be divided into \( p^m \) groups of \( p^m \) codewords each. The construction procedure for the \( p \)-chip code is almost the same as that for GMPCs. In the following procedure, the text in bold indicates actions that are required to construct \( p \)-chip codes but are not required to construct GMPCs.

(i) First, set up a generator vector \( g = (g_0, g_1, \ldots, g_{p^m-1}) \), where \( g_i \in \text{GF}(p^m) \) and no two elements \( g_i \) and \( g_j \) (\( i \neq j \)) are equal for \( i, j = 0, 1, \ldots, p^m - 1 \). For example, we can choose the vector for GF\((2^3)\) and \( \pi(x) = x^3 + x + 1 \) as follows:

\[
g = (0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6).
\]

(ii) Select a group coefficient \( x_i \) (\( x_i \in \text{GF}(p^m) \), \( i = 0, 1, \ldots, p^m - 1 \)) for each group. No two group coefficients are equal. For example, we can choose the coefficients for GF\((2^3)\) as follows:

\[
x_0 = 0, \quad x_1 = 1, \quad x_2 = \alpha, \ldots, x_7 = \alpha^6.
\]

(iii) Set up \( p^m \) constant vectors \( y_j \) (\( j = 0, 1, \ldots, p^m - 1 \)) over GF\((p^m)\). The vectors \( y_j \) have a length \( p^m \) elements. All elements of a single vector are identical, and no two vectors are the same. In addition, we have to set the \( p \) elements consisting of \( y_{kp}, y_{kp+1}, \ldots, y_{kp+p-1} \) \((k = 0, 1, \ldots, p^{m-1} - 1)\) to be in an equivalence class of the relation \( R \). For example, we can choose the vectors for GF\((2^3)\) as follows:

\[
y_0 = (0, 0, 0, 0, 0, 0, 0),
\]

\[
y_1 = (1, 1, 1, 1, 1, 1, 1),
\]

\[
y_2 = (\alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha),
\]

\[
y_3 = (\alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3),
\]

\[
y_4 = (\alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2),
\]

\[
y_5 = (\alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6),
\]

\[
y_6 = (\alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4),
\]

\[
y_7 = (\alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5),
\]

(iv) Then, generate the codewords \( c^*_{ij} \) in the code \( C^* \) over GF\((p^m)\) with the following equation:

\[
c^*_{ij} = xg + y_j, \quad i, j = 0, 1, \ldots, p^m - 1.
\]

Multiplication and addition in Eq. (5) are performed over GF\((p^m)\). The \( p^m \) codewords in the \( i \)th group are \( c_{i,0}, c_{i,1}, \ldots, c_{i,p^m-1} \). For example, the codewords for GF\((2^3)\) are obtained as follows:

\[
c^*_{0,0} = x_0g + y_0 = (0, 0, 0, 0, 0, 0, 0),
\]

\[
c^*_{0,1} = x_0g + y_1 = (1, 1, 1, 1, 1, 1, 1),
\]

\[
\vdots
\]

\[
c^*_{7,6} = x_7g + y_6 = (\alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4),
\]

\[
c^*_{7,7} = x_7g + y_7 = (\alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5).
\]

(v) Finally, transform the codewords \( c^*_{ij} \) \((i, j = 0, 1, \ldots, p^m - 1)\) in the code \( C^* \) into binary codewords \( c_{ij} \), which constitute the binary code \( C \). In this transformation, each GF\((p^m)\) element is assigned to a different binary vector with a length of \( p^m \) and a weight of 1. These vectors are subsequences of a binary codeword \( c_{ij} \) in the \( p \)-chip code \( C \), and every codeword consists of \( p^m \) subsequences. Note that the \( p \) elements in an equivalence class have to be assigned to the vectors whose locations of nonzero chips are in the same small block when we divide a subsequence into \( p^{m-1} \) small blocks whose lengths are \( p \) chips. For example, the assignment of GF\((2^3)\) elements to binary vectors can be given as follows:

\[
0 \rightarrow (1, 0, 0, 0, 0, 0, 0, 0),
\]

\[
1 \rightarrow (0, 1, 0, 0, 0, 0, 0, 0),
\]

\[
\alpha \rightarrow (0, 0, 1, 0, 0, 0, 0, 0),
\]

\[
\alpha^3 \rightarrow (0, 0, 0, 1, 0, 0, 0, 0),
\]

\[
\alpha^2 \rightarrow (0, 0, 0, 0, 1, 0, 0, 0),
\]

\[
\alpha^6 \rightarrow (0, 0, 0, 0, 0, 1, 0, 0),
\]

\[
\alpha^4 \rightarrow (0, 0, 0, 0, 0, 0, 1, 0),
\]

\[
\alpha^5 \rightarrow (0, 0, 0, 0, 0, 0, 0, 1).
\]

(vi) When assigning \( p \)-chip codewords to each user in the EWO scheme, assign \( p \) consecutive codewords \( e_{ijkp}, e_{ijkp+1}, \ldots, e_{ijkp+p-1} \) \((i = 0, 1, \ldots, p^m - 1, \quad k = 0, 1, \ldots, p^{m-1} - 1)\) in the same group to a single user. In total, \( p^{2m} \) codewords are assigned to \( p^{2m-1} \) users. For example, we can assign \( e_{0,0} \) to the 0th user, \( e_{0,2} \) and \( e_{0,3} \) to the 1st user, \( \ldots \), and \( e_{7,6} \) and \( e_{7,7} \) to the 31st user, respectively, for the chip-pair code generated from GF\((2^3)\).

2.4 Examples of \( p \)-chip codes and chip-pair codes

Table 1 shows the code \( C^* \) over GF\((2^3)\) and its chip-pair code \( C \). In Tables 1 and 2, \( \alpha \) is a primitive element of GF\((2^3)\)...
Table 1: $C^*$ over $\text{GF}(2^3)$ and its chip-pair code $C$.  

<table>
<thead>
<tr>
<th>Gr.</th>
<th>User</th>
<th>$C^*$</th>
<th>Chip-pair code $C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>$e_{0,0}$</td>
<td>$0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$e_{0,1}$</td>
<td>$1 \ 1 \ 1 \ 1$</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>$e_{2,0}$</td>
<td>$0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$e_{2,1}$</td>
<td>$1 \ 0 \ 1 \ 0$</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$e_{4,0}$</td>
<td>$0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$e_{4,1}$</td>
<td>$1 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>$e_{6,0}$</td>
<td>$0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$e_{6,1}$</td>
<td>$1 \ 0 \ 0 \ 0$</td>
</tr>
</tbody>
</table>

and $\pi(x) = x^2 + x + 1$. In the construction of $C^*$, we suppose $g = (0, 1, \alpha, \alpha^2)$, $x_0 = 0$, $x_1 = 1$, $x_2 = \alpha$, $x_3 = \alpha^2$, $y_0 = (0, 0, 0, 0)$, $y_1 = (1, 1, 1, 1)$, $y_2 = (\alpha, \alpha, \alpha, \alpha)$, and $y_3 = (\alpha^2, \alpha^2, \alpha^2, \alpha^2)$.

Each user uses two codewords in the same group ("Gr.") in the table of the chip-pair code. Table 2 shows the equivalence classes in $\text{GF}(2^3)$ and binary subsequences assigned to the $\text{GF}(2^3)$ elements. Two codewords assigned to a single user have equal weight and are orthogonal, as shown in Table 1. In addition, for each pair of codewords assigned to a single user, every nonzero chip position in each codeword is adjacent to that in the other codeword. In other words, when we divide a codeword into eight small blocks, each having a length of two chips, nonzero chips of these two codewords are always in the same small blocks. It is this feature that gives the chip-pair code the ability to remove interference light with an intensity that varies by two chips.

Table 3: $C^*$ over $\text{GF}(2^3)$ for chip-pair code $C$.  

<table>
<thead>
<tr>
<th>Gr.</th>
<th>$C^*$</th>
<th>$C^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
<td>$4 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0$</td>
</tr>
<tr>
<td>1</td>
<td>$1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1$</td>
<td>$1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td>2</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td>3</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
</tr>
</tbody>
</table>

Table 4: Equivalence classes in $\text{GF}(2^3)$ and binary subsequences.  

<table>
<thead>
<tr>
<th>Equivalence class</th>
<th>Elements in $C^*$</th>
<th>Subsequences in $C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0, 1]$</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
</tr>
<tr>
<td>$[\alpha, \alpha^2]$</td>
<td>$\alpha \ \alpha^2 = \alpha + 1$</td>
<td>$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$</td>
</tr>
</tbody>
</table>

Table 5 shows an example of the code $C^*$ over $\text{GF}(2^3)$ and its three-chip code $C$. Table 6 shows the equivalence classes in $\text{GF}(2^3)$ and binary subsequences assigned to the $\text{GF}(3^2)$ elements. In Tables 5 and 6, $\alpha$ is a primitive element of $\text{GF}(2^3)$ and $\pi(x) = x^2 + x + 1$. In the construction of $C^*$, we suppose $g = (0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$, $x_0 = 0$, $x_1 = 1$, $x_2 = \alpha$, $x_3 = \alpha^2$, $x_4 = \alpha^3$, $x_5 = \alpha^4$, $y_0 = (0, 0, 0, 0, 0, 0, 0, 0)$, $y_1 = (1, 1, 1, 1, 1, 1, 1, 1)$, $y_2 = (\alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha)$, $y_3 = (\alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2)$, $y_4 = (\alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3, \alpha^3)$, $y_5 = (\alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4, \alpha^4)$, $y_6 = (\alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5, \alpha^5)$, $y_7 = (\alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6, \alpha^6)$, $y_8 = (\alpha^7, \alpha^7, \alpha^7, \alpha^7, \alpha^7, \alpha^7, \alpha^7, \alpha^7)$. Because $p$ is equal to 2, the chip-pair code has the ability to remove interference light with an intensity that varies by two chips.
chip-pair property of GMPSCs. In other words, though some GMPSCs are p-chip codes, many other GMPSCs are not p-chip codes. For example, the GMPSC constructed from GF(2^2), which was introduced in Ref. [5], is identical with the chip-pair code shown in Table 1. However, the probability that a randomly chosen GMPSC happens to be a p-chip code is a subset of the large. In fact, the other GMPSCs introduced in Refs. [5] and [21] are not p-chip codes. Table 7 shows the binary codewords of the chip-pair code generated from C* over GF(2^3) in Table 3. The values of p, q, and the small blocks are always in the same small blocks. Then this three-chip code has the ability to remove interference light with an intensity that varies by three chips.

3. Algebraic properties and applications

In this section, we investigate algebraic properties and applications of the proposed p-chip codes.

The proposed p-chip codes have a unique property: marks in the p codewords assigned to a single user always exist in the same q small blocks when we divide a codeword into q^2/p small blocks whose lengths are p chips. We refer to this property as the p-chip property and the small blocks as sub-blocks. In particular, we refer to the property as the chip-pair property for the case of p = 2.

The class of p-chip codes is a proper subset of the class of GMPSCs. In other words, though some GMPSCs are p-chip codes, many other GMPSCs are not p-chip codes. For example, the GMPSC constructed from GF(2^2), which was introduced in Ref. [5], is identical with the chip-pair code shown in Table 1. However, the probability that a randomly chosen GMPSC happens to be a p-chip code is a subset of the large. In fact, the other GMPSCs introduced in Refs. [5] and [21] are not p-chip codes. Table 7 shows the binary codewords of the chip-pair code generated from C* over GF(2^3) in Table 3. The values of p, q, and the small blocks are always in the same small blocks. Then this three-chip code has the ability to remove interference light with an intensity that varies by three chips.

Table 6: Equivalence classes in GF(3^2) and binary subsequences.

<table>
<thead>
<tr>
<th>Equivalence class</th>
<th>Elements in C*</th>
<th>Subsequences in C*</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0, 1, α]</td>
<td>0</td>
<td>1000000000</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>010000000</td>
</tr>
<tr>
<td></td>
<td>α^2 = 2</td>
<td>001000000</td>
</tr>
<tr>
<td>[α, α', α^2]</td>
<td>α^2 = α + 1</td>
<td>000100000</td>
</tr>
<tr>
<td></td>
<td>α^2 = α + 2</td>
<td>000010000</td>
</tr>
<tr>
<td>[α^2, α^3, α^4]</td>
<td>α^2 = 2α</td>
<td>000000100</td>
</tr>
<tr>
<td></td>
<td>α^2 = 2α + 1</td>
<td>000000010</td>
</tr>
<tr>
<td></td>
<td>α^3 = 2α + 2</td>
<td>000000001</td>
</tr>
</tbody>
</table>
blocks. This property stems from the property of the code $C^*$, in which all the elements at the same location in $p$ codewords assigned to a single user are in the same equivalence class of the relation $R$. The code construction procedure in Section 2.3 guarantees that all the elements at the same location in $p$ codewords assigned to a single user are in the same equivalence class of the relation $R$. The reason is that $\beta + \gamma_0, \beta + \gamma_1, \cdots, \beta + \gamma_{p-1}$ are in the equivalence class $[\beta + \gamma_0]$ for any element $\beta$ in $GF(p^m)$. If $\gamma_0, \gamma_1, \cdots, \gamma_{p-1}$ are in the equivalence class $[\gamma_0]$ in $GF(p^m)$. This fact can be proved easily by Eq. (2). In the code construction procedure, $\gamma_0, \gamma_1, \cdots, \gamma_{p-1}$ correspond to the elements in $y_{kp}, y_{kp+1}, \cdots, y_{kp+p-1}$, respectively, and $\beta$ corresponds to each element in the vector $x_g$ in Eq. (5) for $i = 0, 1, \cdots, p^m - 1$ and $k = 0, 1, \cdots, p^m - 1$. In addition, the $p$ elements in an equivalence class are always assigned to the binary sub-sequences whose locations of nonzero chips are in the same sub-block, when the codewords $e_i^j$ $(i, j = 0, 1, \cdots, p^m - 1)$ in the code $C^*$ are transformed into binary codewords $c_{ij}$ in the $p$-chip code $C$. Hence the code $C$ constructed by the procedure in Section 2.3 certainly possesses $p$-chip property.

For example, in Table 7, the red boxes show the equivalence classes of $R$ on $GF(2^3)$ and sub-blocks in the green boxes have the chip-pair property. As a consequence, any $p$-chip code generated from $GF(p^m)$ has the ability to remove interference light with an intensity that varies by $p$ chips when each user transmits $p$-ary data and the EWO scheme is adopted. Optical CDMA systems using $p$-chip codes instead of MPSCs or GMPSCs can not only MUI but also interference light without requiring additional equipment. In Appendix C, we explain how the EWO decoder using a $p$-chip code removes interference light and MUI simultaneously, even if the intensity of interference light varies by sub-block.

The value $p$ can be set to any arbitrary prime number, such as two or three. Although the optical CDMA systems using conventional codes do not cancel interference light with intensity varying by sub-blocks with a length of two or three chips, the systems using the proposed $p$-chip codes do cancel such interference light. Therefore, the $p$-chip codes including chip-pair codes have the capability to remove interference light that cannot be removed by other coding schemes. Using this property, the proposed system can be used simultaneously with dimming-controlled illumination that is realized by the pulse-width modulation (PWM) technique [12], when the PWM pulses are synchronized with a duration of sub-blocks in each GMPSC slot.

4. Conclusion

This paper proposes a new GMPSC, referred to as a $p$-chip code, for synchronous optical CDMA. A general method for constructing the proposed code for an arbitrary extension field $GF(p^m)$ is presented. This paper also shows that the optical CDMA system using a $p$-chip code as a signature code and the EWO MUI cancellation scheme removes interference light with an intensity that varies by $p$ chips. In particular, chip-pair codes, which are $p$-chip codes for $p = 2$, remove interference light with an intensity that varies by two chips.

Acknowledgment

This work was supported by the Japan Society for the Promotion of Science, KAKENHI Grants 19K04403 and 19K04402.

References


Table 7: Codewords in chip-pair code constructed from $\text{GF}(2^3)$. The two elements in each red box are in an equivalence class of the relation $R$ on $\text{GF}(2^3)$. The two sub-blocks of length two in each green box have the chip-pair property.

<table>
<thead>
<tr>
<th>Gr.</th>
<th>User</th>
<th>$C^*$</th>
<th>Chip-pair code $C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$C_0$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$\alpha$</td>
<td>$C_1$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$\alpha^2$</td>
<td>$C_2$</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>$\alpha + 1$</td>
<td>$C_3$</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>$C_4$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>$\alpha$</td>
<td>$C_5$</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>$\alpha^2$</td>
<td>$C_6$</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>$\alpha + 1$</td>
<td>$C_7$</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>0</td>
<td>$C_8$</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>$\alpha$</td>
<td>$C_9$</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>$\alpha^2$</td>
<td>$C_{10}$</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>$\alpha + 1$</td>
<td>$C_{11}$</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>0</td>
<td>$C_{12}$</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>$\alpha$</td>
<td>$C_{13}$</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>$\alpha^2$</td>
<td>$C_{14}$</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>$\alpha + 1$</td>
<td>$C_{15}$</td>
</tr>
</tbody>
</table>


**Appendix A: Proof that the relation $R$ is an equivalence relation**

A relation is an equivalence relation if it is reflexive, symmetric, and transitive. The relation $R$ on $F$ in Section 2.1 is an equivalence relation because $R$ has the following three properties:

**Reflexive:** For every $x \in F$, $x - x = 0 \in \{0, 1, \cdots, p - 1\}$. Hence $\forall x \in F$, $xRx$.

**Symmetric:** If $x - y \in \{0, 1, \cdots, p - 1\}$, then $y - x \in \{0, 1, \cdots, p - 1\}$. Hence $xRy \Rightarrow yRx$.

**Transitive:** If $x-y \in \{0, 1, \cdots, p-1\}$ and $y-z \in \{0, 1, \cdots, p-1\}$, then $x-z \in \{0, 1, \cdots, p-1\}$. Hence $xRy \land yRz \Rightarrow xRz$. 
Appendix B: Cancellation of interference light varying by block for GMPSCs

It has been reported that the EWO scheme cancels interference light and MUI simultaneously, when the interference light intensity is constant within a slot and a GMPSC, including MPSC, is employed as the signature code [11]. In this appendix, we provide a theoretical explanation of how the EWO decoder using a GMPSC removes interference light and MUI simultaneously, even if the intensity of interference light varies by block as shown in Fig. 1(c).

The EWO scheme for optical CDMA was originally introduced in Ref. [22]. Later, it was reported that the EWO scheme using an MPSC cancels MUI completely [9],[10]. The EWO scheme employs code shift keying as a signaling method [23],[24]. Figure A-1 illustrates a block diagram of the EWO decoder for \( p = 2 \). In the EWO scheme, two equal-weight and orthogonal codewords \( \mathbf{w}_k,0 \) and \( \mathbf{w}_k,1 \) are assigned to the \( k \)th user, and the user uses \( \mathbf{w}_k,l \) to spread a datum \( l \in \{0, 1\} \) [9],[10]. The \( k \)th user’s decoder computes \( \Gamma_0 \) and \( \Gamma_1 \), which are correlation values between the received sequence \( \mathbf{r} \), which is a multiplexed sequence of all the sequences transmitted synchronously, and the two codewords \( \mathbf{w}_k,0 \) and \( \mathbf{w}_k,1 \), respectively.

Table 8: Codewords in GMPSC constructed from GF(\( 2^3 \)).

<table>
<thead>
<tr>
<th>Gr.</th>
<th>User</th>
<th>( C^* )</th>
<th>GMPSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0</td>
<td>1 1 1 1 1 1 1 1 1</td>
</tr>
<tr>
<td>1</td>
<td>( a, a, a, a, a, a, a, a, a, a, a, a, a, a, a, a )</td>
<td>( a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 )</td>
<td>0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>2</td>
<td>( a^3 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 )</td>
<td>0 0 0 0 0 0 0 0 0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>( a^3 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 a^2 )</td>
<td>0 0 0 0 0 0 0 0 0</td>
<td></td>
</tr>
</tbody>
</table>

... continues...

\[ \Gamma_0 \] and \( \Gamma_1 \) are represented as follows:

\[ \Gamma_0 = \Gamma(r, \mathbf{w}_k,0), \]  
\[ \Gamma_1 = \Gamma(r, \mathbf{w}_k,1). \]  

Then the decoder calculates the difference \( \Gamma_1 - \Gamma_0 \). If the difference is greater than or equal to the threshold zero, the decoder outputs \( \hat{l} = 1 \) as a decoded datum. Otherwise, the decoder outputs \( \hat{l} = 0 \). Because the threshold in the EWO decoder is always zero, this scheme cancels MUI without needing to estimate the received light intensity.

Now we consider an optical CDMA employing a GMPSC with \( q = 2^m \) and the EWO scheme. We suppose a link where MUI and interference light are the primary performance-degrading factors, and other factors are negligible. We also suppose that the intensity of interference light is constant during a single block, and the intensity at the \( i \)th
block is $L_b^{(i)}$ for $i = 0, 1, \cdots, q - 1$. The interference light is received at the receiver together with the optical sequences from the desired user and the interfering users. Figure A-2 shows an example of received signals that include interference light and users’ sequences.

GMSPC codewords are assigned to $q^2/2$ users in total. From Eqs. (4), (A-1), and (A-2), the correlation values $I_0$ and $I_1$ calculated at each user’s decoder are represented as follows:

$$I_0 = q(1 - 1)L_s + \frac{q^2 - q}{2} L_s + \sum_{i=0}^{q-1} L_b^{(i)},$$  \hspace{1cm} (A-3)

$$I_1 = qI_s + \frac{q^2 - q}{2} L_s + \sum_{i=0}^{q-1} L_b^{(i)},$$  \hspace{1cm} (A-4)

where $I$ ($I \in \{0, 1\}$) is a transmitted datum and $L_s$ is the received light intensity of each mark. In Eqs. (A-3) and (A-4), $((q^2 - q)/2) L_s$ and $\sum_{i=0}^{q-1} L_b^{(i)}$ are the terms representing MUI and interference light, respectively. When the decoder calculates the difference $I_1 - I_0$, these two terms are eliminated completely. Thus, the EWO decoder removes interference light and MUI simultaneously, even if the intensity of interference light varies by block.

In the cases of $p \neq 2$ and $q = p^m$, each of $q^2/p$ users transmits $p$-ary data. The $p$ codewords $w_{k,0}, w_{k,1}, \cdots$, and $w_{k,p-1}$ are assigned to the $k$th user and the user uses $w_{k,I}$ to spread a datum $I$ ($I \in \{0, 1, \cdots, p - 1\}$). Each user’s decoder has $p$ correlators and computes $I_0, I_1, \cdots,$ and $I_{p-1}$, which are correlation values between the received sequence $r$ and the codewords $w_{k,0}, w_{k,1}, \cdots$, and $w_{k,p-1}$, respectively. $I_\ell$ is represented as follows:

$$I_\ell = \Gamma(r, w_{k,\ell}),$$  \hspace{1cm} (A-5)

for $\ell = 0, 1, \cdots, p - 1$. Then, the decoder chooses the maximum value in $I_0, I_1, \cdots,$ and $I_{p-1}$. If the maximum value is $I_\ell$, the decoder outputs $\hat{I} = \ell$ as the decoded datum.

When we suppose a link where other performance-degrading factors are negligible except for MUI and interference light, the correlation value $I_\ell$ in Eq. (A-5) is represented as follows:

$$I_\ell = \begin{cases} qL_s + \frac{q^2 - q}{p} L_s + \sum_{i=0}^{q-1} L_b^{(i)} & \text{if } I = \ell, \\ \frac{q^2 - q}{p} L_s + \sum_{i=0}^{q-1} L_b^{(i)} & \text{if } I \neq \ell. \end{cases}$$  \hspace{1cm} (A-6)

In Eq. (A-6), $((q^2 - q)/p) L_s$ and $\sum_{i=0}^{q-1} L_b^{(i)}$ are the terms representing MUI and interference light, respectively. When the decoder chooses the maximum among the $p$ correlation values, these two terms are eliminated completely. Thus, when $p \neq 2$, the EWO decoder also removes interference light and MUI simultaneously, even if the intensity of interference light varies by block.

Appendix C: Cancellation of interference light varying by sub-block for p-chip codes

In this appendix, we provide a theoretical explanation of how the EWO decoder using a $p$-chip code removes interference light and MUI simultaneously, even if the intensity of interference light varies by sub-block as shown in Fig. I-1(d).

We consider an optical CDMA employing a $p$-chip code with $q = p^m$ and the EWO scheme. We also suppose that the intensity of interference light is constant during a single sub-block, which consists of $p$ chips, and the intensity at the $i$th block is $L_b^{(i)}$ for $i = 0, 1, \cdots, q^2/p - 1$. The interference light is received at the receiver together with the optical sequences from the desired user and the interfering users. Figure A-3 shows an example of received signals that include interference light and user sequences.

There are $q^2$ codewords in a $p$-chip code. Each of $q^2/p$ users transmits a $p$-ary datum $I$ in each slot ($I \in \{0, 1, \cdots, p - 1\}$). Suppose that the $p$ codewords $w_{k,0}, w_{k,1}, \cdots$, and $w_{k,p-1}$ are assigned to the $k$th user ($k = 0, 1, 2, \cdots, q^2/p - 1$), and that $w_{k,I}$ is used to spread a datum $I$. Because of the $p$-chip property, the locations of the marks in the $p$ codewords for a single user are in the same $q$ sub-blocks. We define the set $\Phi_k = \{\phi_{k,0}, \phi_{k,1}, \cdots, \phi_{k,q^2/p - 1}\}$, where the $q$ marks in each codeword for the $k$th user are in the $\phi_{k,0}$th, $\phi_{k,1}$th, $\cdots$, and $\phi_{k,q^2/p - 1}$th sub-blocks, respectively. For example, for the chip-pair code in Table 1, $\Phi_0 = \{0, 2, 4, 6\}$, $\Phi_1 = \{1, 3, 5, 7\}$, $\Phi_2 = \{1, 2, 5, 6\}$.

Each user’s decoder has $p$ correlators and computes $I_0, I_1, \cdots,$ and $I_{p-1}$, which are correlation values between the received sequence $r$ and the codewords $w_{k,0}, w_{k,1}, \cdots$, and $w_{k,p-1}$, respectively. $I_\ell$ is represented as Eq. (A-5). Then, the decoder chooses the maximum value in $I_0, I_1, \cdots,$ and $I_{p-1}$. If the maximum value is $I_\ell$, the decoder outputs $\hat{I} = \ell$ as the decoded datum ($\ell \in \{0, 1, \cdots, p - 1\}$).

When we consider a link in which performance-degrading factors other than MUI and interference light are negligible, the correlation value $I_\ell$ is represented as follows:

$$I_\ell = \begin{cases} qL_s + \frac{q^2 - q}{p} L_s + \sum_{\phi_k \in \Phi_k} L_b^{(\phi_k)} & \text{if } I = \ell, \\ \frac{q^2 - q}{p} L_s + \sum_{\phi_k \in \Phi_k} L_b^{(\phi_k)} & \text{if } I \neq \ell. \end{cases}$$  \hspace{1cm} (A-7)

where $L_s$ is the received light intensity for each mark.

In Eq. (A-7), $((q^2 - q)/p) L_s$ is the term representing MUI, and $\sum_{\phi_k \in \Phi_k} L_b^{(\phi_k)}$ is the term representing interference light varying by sub-block. When the decoder chooses the maximum among the $p$ correlation values, these two terms are eliminated completely. Thus, the decoder removes interference light and MUI simultaneously, even if the intensity
Fig. A.3: Example of received signals with interference light varying by sub-block ($p$ chips) and user sequences ($p = 2, q = 4$).

of interference light varies by sub-block.

Tomoko K. Matsushima received B.E., M.E. and Dr.E. degrees from Waseda University, Tokyo, Japan, in 1985, 1987 and 1999, respectively. She was with Toshiba Corporate R & D Center from 1987 to 1994. She has been with Polytechnic University, Japan, since 1994, where she is currently a Professor. 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 the IEEE.

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 has been a Professor at Polytechnic University, Japan, since 2004. His research interests include coding, signal processing, and security in wireless and multimedia communications. Dr. Yamasaki is a member of the IEEE.

Kyohei Ono received a B.S. degree in Manufacturing Technology from Polytechnic University, Tokyo, Japan, in 2019. He is currently a student in the Graduate Course of Master of Science in Manufacturing Engineering at Polytechnic University. His research interests include optical communication systems, secret sharing and physical layer security.