PAPER

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

Tomoko K. MATSUSHIMA[†*a)], ***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 $q = p^m$, 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^2. 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 q^2 codewords with a length of q^2. For a GMPSC, $q = p^m$ 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.

Manuscript received January 29, 2021.
Manuscript revised March 24, 2021.
Manuscript publicized May 6, 2021.
[†]The authors are with Polytechnic University, Kodaira-shi, 187-0035 Japan.
[*]Presently, with Yokohama College of Commerce.
[**]Presently, with Hiroshima City University.
[***]Presently, with Japan Organization for Employment of the Elderly, Persons with Disabilities and Job Seekers.
a) E-mail: matsushima@shodai.ac.jp
DOI: 10.1587/transfun.2021EAP1015

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 2^2. 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(p^m) 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(p^m), where p is a prime number and m is a positive integer. F is represented as follows:

$$F = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{p^m-2}\}, \tag{1}$$

where α is a primitive element of GF(p^m) 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:

$$R = \{ (x, y) \mid x - y \in \{0, 1, \cdots, p-1\}\}. \tag{2}$$

Because R is an equivalence relation, the quotient set of F by R is

$$F/R = \{ [a] \mid a \in F\}, \tag{3}$$

where $[a] = \{x \mid (a, x) \in R\}$ is the equivalence class of a in F. In Appendix A, we show the proof that R defined by Eq. (2) is an equivalence relation.

For example,

$$F/R = \{\{0, 1\}, \{\alpha, \alpha^2\}\}$$

for GF(2^2) and $\pi(x) = x^2 + x + 1$,

$$F/R = \{\{0, 1\}, \{\alpha, \alpha^3\}, \{\alpha^2, \alpha^6\}, \{\alpha^4, \alpha^5\}\}$$

for GF(2^3) and $\pi(x) = x^3 + x + 1$, and

$$F/R = \{\{0, 1, \alpha^4\}, \{\alpha, \alpha^7, \alpha^6\}, \{\alpha^5, \alpha^2, \alpha^3\}\}$$

for GF(3^2) and $\pi(x) = x^2 + x + 2$.

2.2 Properties of GMPSC

MPSCs [3], [4] and GMPSCs [5], [6] are binary unipolar 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]:

$$\Gamma(\mathbf{c}_{i_1,j_1}, \mathbf{c}_{i_2,j_2}) = \begin{cases} p^m & \text{if } i_1 = i_2 \text{ and } j_1 = j_2 , \\ 0 & \text{if } i_1 = i_2 \text{ and } j_1 \neq j_2 , \\ 1 & \text{if } i_1 \neq i_2, \end{cases} \tag{4}$$

where $\mathbf{c}_{i,j}$ is the jth codeword in the ith group ($i, j = 0, 1, \cdots, p^m - 1$) and $\Gamma(\mathbf{a}, \mathbf{b})$ is the auto- or cross-correlation function between two sequences $\mathbf{a}$ and $\mathbf{b}$ 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.

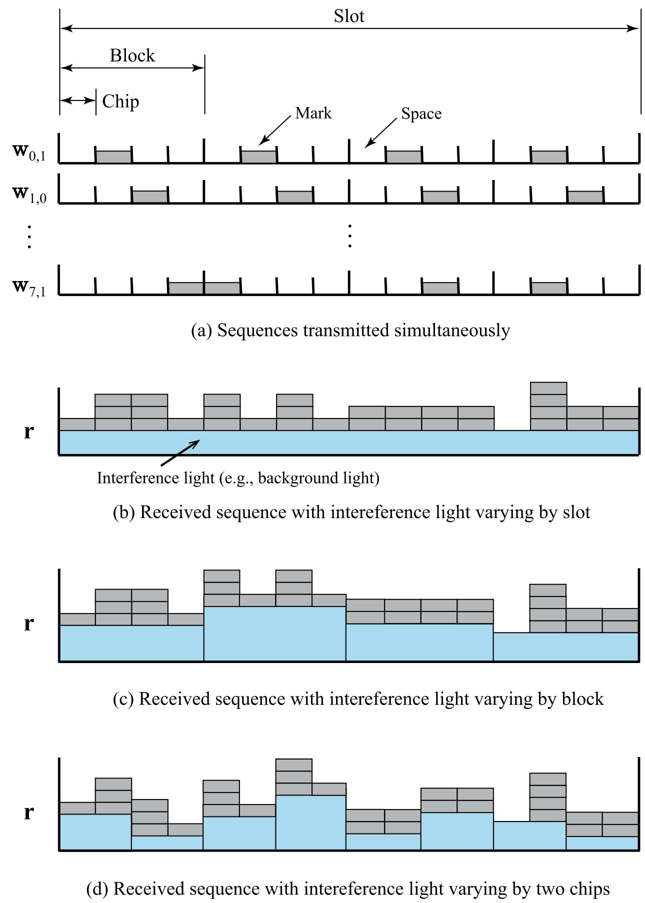


Fig. 1 Examples of multiplexed signals and interference light in optical CDMA system using GMPSC and the EWO scheme.

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

Table 1 $\boldsymbol{C}^*$ over GF(2^2) and its chip-pair code $\boldsymbol{C}$.

Gr.	User	$\boldsymbol{C}^*$	Chip-pair code $\boldsymbol{C}$
0	0	$\boldsymbol{c}^*_{0,0}$: $0\ 0\ 0\ 0$	$\boldsymbol{c}_{0,0}$: 1000 1000 1000 1000
		$\boldsymbol{c}^*_{0,1}$: $1\ 1\ 1\ 1$	$\boldsymbol{c}_{0,1}$: 0100 0100 0100 0100
	1	$\boldsymbol{c}^*_{0,2}$: $\alpha\ \alpha\ \alpha\ \alpha$	$\boldsymbol{c}_{0,2}$: 0010 0010 0010 0010
		$\boldsymbol{c}^*_{0,3}$: $\alpha^2\ \alpha^2\ \alpha^2\ \alpha^2$	$\boldsymbol{c}_{0,3}$: 0001 0001 0001 0001
1	2	$\boldsymbol{c}^*_{1,0}$: $0\ 1\ \alpha\ \alpha^2$	$\boldsymbol{c}_{1,0}$: 1000 0100 0010 0001
		$\boldsymbol{c}^*_{1,1}$: $1\ 0\ \alpha^2\ \alpha$	$\boldsymbol{c}_{1,1}$: 0100 1000 0001 0010
	3	$\boldsymbol{c}^*_{1,2}$: $\alpha\ \alpha^2\ 0\ 1$	$\boldsymbol{c}_{1,2}$: 0010 0001 1000 0100
		$\boldsymbol{c}^*_{1,3}$: $\alpha^2\ \alpha\ 1\ 0$	$\boldsymbol{c}_{1,3}$: 0001 0010 0100 1000
2	4	$\boldsymbol{c}^*_{2,0}$: $0\ \alpha\ \alpha^2\ 1$	$\boldsymbol{c}_{2,0}$: 1000 0010 0001 0100
		$\boldsymbol{c}^*_{2,1}$: $1\ \alpha^2\ \alpha\ 0$	$\boldsymbol{c}_{2,1}$: 0100 0001 0010 1000
	5	$\boldsymbol{c}^*_{2,2}$: $\alpha\ 0\ 1\ \alpha^2$	$\boldsymbol{c}_{2,2}$: 0010 1000 0100 0001
		$\boldsymbol{c}^*_{2,3}$: $\alpha^2\ 1\ 0\ \alpha$	$\boldsymbol{c}_{2,3}$: 0001 0100 1000 0010
3	6	$\boldsymbol{c}^*_{3,0}$: $0\ \alpha^2\ 1\ \alpha$	$\boldsymbol{c}_{3,0}$: 1000 0001 0100 0010
		$\boldsymbol{c}^*_{3,1}$: $1\ \alpha\ 0\ \alpha^2$	$\boldsymbol{c}_{3,1}$: 0100 0010 1000 0001
	7	$\boldsymbol{c}^*_{3,2}$: $\alpha\ 1\ \alpha^2\ 0$	$\boldsymbol{c}_{3,2}$: 0010 0100 0001 1000
		$\boldsymbol{c}^*_{3,3}$: $\alpha^2\ 0\ \alpha\ 1$	$\boldsymbol{c}_{3,3}$: 0001 1000 0010 0100

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

Equivalence class	Elements in $\boldsymbol{C}^*$	Subsequences in $\boldsymbol{C}$
$\{0, 1\}$	0	1000
	1	0100
$\{\alpha, \alpha^2\}$	α	0010
	$\alpha^2 = \alpha + 1$	0001

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

Gr.	$\boldsymbol{C}^*$	Gr.	$\boldsymbol{C}^*$
0	$0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$	4	$0\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1\ \alpha\ \alpha^2$
	$1\ 1\ 1\ 1\ 1\ 1\ 1\ 1$		$1\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2\ 0\ \alpha^3\ \alpha^6$
	$\alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha$		$\alpha\ 1\ \alpha^2\ \alpha^6\ \alpha^5\ \alpha^3\ 0\ \alpha^4$
	$\alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3$		$\alpha^3\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha\ 1\ \alpha^5$
	$\alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2$		$\alpha^2\ \alpha^5\ \alpha\ \alpha^3\ 1\ \alpha^6\ \alpha^4\ 0$
	$\alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6$		$\alpha^6\ \alpha^4\ \alpha^3\ \alpha\ 0\ \alpha^2\ \alpha^5\ 1$
	$\alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4$		$\alpha^4\ \alpha^6\ 0\ 1\ \alpha^3\ \alpha^5\ \alpha^2\ \alpha$
	$\alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5$		$\alpha^5\ \alpha^2\ 1\ 0\ \alpha\ \alpha^4\ \alpha^6\ \alpha^3$
1	$0\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6$	5	$0\ \alpha^4\ \alpha^5\ \alpha^6\ 1\ \alpha\ \alpha^2\ \alpha^3$
	$1\ 0\ \alpha^3\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2$		$1\ \alpha^5\ \alpha^4\ \alpha^2\ 0\ \alpha^3\ \alpha^6\ \alpha$
	$\alpha\ \alpha^3\ 0\ \alpha^4\ 1\ \alpha^2\ \alpha^6\ \alpha^5$		$\alpha\ \alpha^2\ \alpha^6\ \alpha^5\ \alpha^3\ 0\ \alpha^4\ 1$
	$\alpha^3\ \alpha\ 1\ \alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4$		$\alpha^3\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha\ 1\ \alpha^5\ 0$
	$\alpha^2\ \alpha^6\ \alpha^4\ 0\ \alpha^5\ \alpha\ \alpha^3\ 1$		$\alpha^2\ \alpha\ \alpha^3\ 1\ \alpha^6\ \alpha^4\ 0\ \alpha^5$
	$\alpha^6\ \alpha^2\ \alpha^5\ 1\ \alpha^4\ \alpha^3\ \alpha\ 0$		$\alpha^6\ \alpha^3\ \alpha\ 0\ \alpha^2\ \alpha^5\ 1\ \alpha^4$
	$\alpha^4\ \alpha^5\ \alpha^2\ \alpha\ \alpha^6\ 0\ 1\ \alpha^3$		$\alpha^4\ 0\ 1\ \alpha^3\ \alpha^5\ \alpha^2\ \alpha\ \alpha^6$
	$\alpha^5\ \alpha^4\ \alpha^6\ \alpha^3\ \alpha^2\ 1\ 0\ \alpha$		$\alpha^5\ 1\ 0\ \alpha\ \alpha^4\ \alpha^6\ \alpha^3\ \alpha^2$
2	$0\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1$	6	$0\ \alpha^5\ \alpha^6\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4$
	$1\ \alpha^3\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2\ 0$		$1\ \alpha^4\ \alpha^2\ 0\ \alpha^3\ \alpha^6\ \alpha\ \alpha^5$
	$\alpha\ 0\ \alpha^4\ 1\ \alpha^2\ \alpha^6\ \alpha^5\ \alpha^3$		$\alpha\ \alpha^6\ \alpha^5\ \alpha^3\ 0\ \alpha^4\ 1\ \alpha^2$
	$\alpha^3\ 1\ \alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha$		$\alpha^3\ \alpha^2\ \alpha^4\ \alpha\ 1\ \alpha^5\ 0\ \alpha^6$
	$\alpha^2\ \alpha^4\ 0\ \alpha^5\ \alpha\ \alpha^3\ 1\ \alpha^6$		$\alpha^2\ \alpha^3\ 1\ \alpha^6\ \alpha^4\ 0\ \alpha^5\ \alpha$
	$\alpha^6\ \alpha^5\ 1\ \alpha^4\ \alpha^3\ \alpha\ 0\ \alpha^2$		$\alpha^6\ \alpha\ 0\ \alpha^2\ \alpha^5\ 1\ \alpha^4\ \alpha^3$
	$\alpha^4\ \alpha^2\ \alpha\ \alpha^6\ 0\ 1\ \alpha^3\ \alpha^5$		$\alpha^4\ 1\ \alpha^3\ \alpha^5\ \alpha^2\ \alpha\ \alpha^6\ 0$
	$\alpha^5\ \alpha^6\ \alpha^3\ \alpha^2\ 1\ 0\ \alpha\ \alpha^4$		$\alpha^5\ 0\ \alpha\ \alpha^4\ \alpha^6\ \alpha^3\ \alpha^2\ 1$
3	$0\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1\ \alpha$	7	$0\ \alpha^6\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5$
	$1\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2\ 0\ \alpha^3$		$1\ \alpha^2\ 0\ \alpha^3\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4$
	$\alpha\ \alpha^4\ 1\ \alpha^2\ \alpha^6\ \alpha^5\ \alpha^3\ 0$		$\alpha\ \alpha^5\ \alpha^3\ 0\ \alpha^4\ 1\ \alpha^2\ \alpha^6$
	$\alpha^3\ \alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha\ 1$		$\alpha^3\ \alpha^4\ \alpha\ 1\ \alpha^5\ 0\ \alpha^6\ \alpha^2$
	$\alpha^2\ 0\ \alpha^5\ \alpha\ \alpha^3\ 1\ \alpha^6\ \alpha^4$		$\alpha^2\ 1\ \alpha^6\ \alpha^4\ 0\ \alpha^5\ \alpha\ \alpha^3$
	$\alpha^6\ 1\ \alpha^4\ \alpha^3\ \alpha\ 0\ \alpha^2\ \alpha^5$		$\alpha^6\ 0\ \alpha^2\ \alpha^5\ 1\ \alpha^4\ \alpha^3\ \alpha$
	$\alpha^4\ \alpha\ \alpha^6\ 0\ 1\ \alpha^3\ \alpha^5\ \alpha^2$		$\alpha^4\ \alpha^3\ \alpha^5\ \alpha^2\ \alpha\ \alpha^6\ 0\ 1$
	$\alpha^5\ \alpha^3\ \alpha^2\ 1\ 0\ \alpha\ \alpha^4\ \alpha^6$		$\alpha^5\ \alpha\ \alpha^4\ \alpha^6\ \alpha^3\ \alpha^2\ 1\ 0$

Table 4 Equivalence classes in GF(2^3) and binary subsequences.

Equivalence class	Elements in $\boldsymbol{C}^*$	Subsequences in $\boldsymbol{C}$
$\{0, 1\}$	0	10000000
	1	01000000
$\{\alpha, \alpha^3\}$	α	00100000
	$\alpha^3 = \alpha + 1$	00010000
$\{\alpha^2, \alpha^6\}$	α^2	00001000
	$\alpha^6 = \alpha^2 + 1$	00000100
$\{\alpha^4, \alpha^5\}$	$\alpha^4 = \alpha^2 + \alpha$	00000010
	$\alpha^5 = \alpha^2 + \alpha + 1$	00000001

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]. Reference [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 GMPSC 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 $\boldsymbol{C}^*$ over GF(p^m), and then we transform it into a binary p-chip code $\boldsymbol{C}$. The length of code $\boldsymbol{C}^*$ is p^m symbols, and the length of code $\boldsymbol{C}$ 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 codes is almost the same as that for GMPSCs. In the following procedure, the text in bold indicates actions that are required to construct p-chip codes but are not required to construct GMPSCs.

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

$$\boldsymbol{g} = (0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6).$$

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

$$x_0 = 0, \quad x_1 = 1, \quad x_2 = \alpha, \ \cdots, \ x_7 = \alpha^6.$$

(iii) Set up p^m constant vectors $\boldsymbol{y}_j$ ($j = 0, 1, \cdots, p^m - 1$) over GF($p^m$). The vectors $\boldsymbol{y}_j$ have a length p^m. All

Table 5 $\boldsymbol{C}^*$ over GF(3^2) for three-chip code $\boldsymbol{C}$.

Gr.	$\boldsymbol{C}^*$	Gr.	$\boldsymbol{C}^*$	Gr.	$\boldsymbol{C}^*$
0	$0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$	3	$0\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ 1\ \alpha$	6	$0\ \alpha^5\ \alpha^6\ \alpha^7\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4$
	$1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1$		$1\ \alpha^3\ \alpha^5\ 0\ \alpha^2\ \alpha\ \alpha^6\ \alpha^4\ \alpha^7$		$1\ \alpha^2\ \alpha\ \alpha^6\ \alpha^4\ \alpha^7\ \alpha^3\ \alpha^5\ 0$
	$\alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4$		$\alpha^4\ \alpha^5\ \alpha^2\ 1\ \alpha^3\ \alpha^7\ \alpha\ 0\ \alpha^6$		$\alpha^4\ \alpha^3\ \alpha^7\ \alpha\ 0\ \alpha^6\ \alpha^5\ \alpha^2\ 1$
	$\alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha$		$\alpha\ 1\ \alpha^4\ \alpha^6\ 0\ \alpha^3\ \alpha^2\ \alpha^7\ \alpha^5$		$\alpha\ 0\ \alpha^3\ \alpha^2\ \alpha^7\ \alpha^5\ 1\ \alpha^4\ \alpha^6$
	$\alpha^7\ \alpha^7\ \alpha^7\ \alpha^7\ \alpha^7\ \alpha^7\ \alpha^7\ \alpha^7\ \alpha^7$		$\alpha^7\ \alpha^4\ 0\ \alpha\ 1\ \alpha^5\ \alpha^3\ \alpha^6\ \alpha^2$		$\alpha^7\ 1\ \alpha^5\ \alpha^3\ \alpha^6\ \alpha^2\ \alpha^4\ 0\ \alpha$
	$\alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6$		$\alpha^6\ 0\ 1\ \alpha^7\ \alpha^4\ \alpha^2\ \alpha^5\ \alpha\ \alpha^3$		$\alpha^6\ \alpha^4\ \alpha^2\ \alpha^5\ \alpha\ \alpha^3\ 0\ 1\ \alpha^7$
	$\alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5$		$\alpha^5\ \alpha^7\ \alpha^6\ \alpha^3\ \alpha\ \alpha^4\ 1\ \alpha^2\ 0$		$\alpha^5\ \alpha\ \alpha^4\ 1\ \alpha^2\ 0\ \alpha^7\ \alpha^6\ \alpha^3$
	$\alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2$		$\alpha^2\ \alpha^6\ \alpha\ \alpha^5\ \alpha^7\ 0\ \alpha^4\ \alpha^3\ 1$		$\alpha^2\ \alpha^7\ 0\ \alpha^4\ \alpha^3\ 1\ \alpha^6\ \alpha\ \alpha^5$
	$\alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3$		$\alpha^3\ \alpha\ \alpha^7\ \alpha^2\ \alpha^6\ 1\ 0\ \alpha^5\ \alpha^4$		$\alpha^3\ \alpha^6\ 1\ 0\ \alpha^5\ \alpha^4\ \alpha\ \alpha^7\ \alpha^2$
1	$0\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7$	4	$0\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ 1\ \alpha\ \alpha^2$	7	$0\ \alpha^6\ \alpha^7\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5$
	$1\ \alpha^4\ \alpha^7\ \alpha^3\ \alpha^5\ 0\ \alpha^2\ \alpha\ \alpha^6$		$1\ \alpha^5\ 0\ \alpha^2\ \alpha\ \alpha^6\ \alpha^4\ \alpha^7\ \alpha^3$		$1\ \alpha\ \alpha^6\ \alpha^4\ \alpha^7\ \alpha^3\ \alpha^5\ 0\ \alpha^2$
	$\alpha^4\ 0\ \alpha^6\ \alpha^5\ \alpha^2\ 1\ \alpha^3\ \alpha^7\ \alpha$		$\alpha^4\ \alpha^2\ 1\ \alpha^3\ \alpha^7\ \alpha\ 0\ \alpha^6\ \alpha^5$		$\alpha^4\ \alpha^7\ \alpha\ 0\ \alpha^6\ \alpha^5\ \alpha^2\ 1\ \alpha^3$
	$\alpha\ \alpha^7\ \alpha^5\ 1\ \alpha^4\ \alpha^6\ 0\ \alpha^3\ \alpha^2$		$\alpha\ \alpha^4\ \alpha^6\ 0\ \alpha^3\ \alpha^2\ \alpha^7\ \alpha^5\ 1$		$\alpha\ \alpha^3\ \alpha^2\ \alpha^7\ \alpha^5\ 1\ \alpha^4\ \alpha^6\ 0$
	$\alpha^7\ \alpha^6\ \alpha^2\ \alpha^4\ 0\ \alpha\ 1\ \alpha^5\ \alpha^3$		$\alpha^7\ 0\ \alpha\ 1\ \alpha^5\ \alpha^3\ \alpha^6\ \alpha^2\ \alpha^4$		$\alpha^7\ \alpha^5\ \alpha^3\ \alpha^6\ \alpha^2\ \alpha^4\ 0\ \alpha\ 1$
	$\alpha^6\ \alpha\ \alpha^3\ 0\ 1\ \alpha^7\ \alpha^4\ \alpha^2\ \alpha^5$		$\alpha^6\ 1\ \alpha^7\ \alpha^4\ \alpha^2\ \alpha^5\ \alpha\ \alpha^3\ 0$		$\alpha^6\ \alpha^2\ \alpha^5\ \alpha\ \alpha^3\ 0\ 1\ \alpha^7\ \alpha^4$
	$\alpha^5\ \alpha^2\ 0\ \alpha^7\ \alpha^6\ \alpha^3\ \alpha\ \alpha^4\ 1$		$\alpha^5\ \alpha^6\ \alpha^3\ \alpha\ \alpha^4\ 1\ \alpha^2\ 0\ \alpha^7$		$\alpha^5\ \alpha^4\ 1\ \alpha^2\ 0\ \alpha^7\ \alpha^6\ \alpha^3\ \alpha$
	$\alpha^2\ \alpha^3\ 1\ \alpha^6\ \alpha\ \alpha^5\ \alpha^7\ 0\ \alpha^4$		$\alpha^2\ \alpha\ \alpha^5\ \alpha^7\ 0\ \alpha^4\ \alpha^3\ 1\ \alpha^6$		$\alpha^2\ 0\ \alpha^4\ \alpha^3\ 1\ \alpha^6\ \alpha\ \alpha^5\ \alpha^7$
	$\alpha^3\ \alpha^5\ \alpha^4\ \alpha\ \alpha^7\ \alpha^2\ \alpha^6\ 1\ 0$		$\alpha^3\ \alpha^7\ \alpha^2\ \alpha^6\ 1\ 0\ \alpha^5\ \alpha^4\ \alpha$		$\alpha^3\ 1\ 0\ \alpha^5\ \alpha^4\ \alpha\ \alpha^7\ \alpha^2\ \alpha^6$
2	$0\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ 1$	5	$0\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ 1\ \alpha\ \alpha^2\ \alpha^3$	8	$0\ \alpha^7\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6$
	$1\ \alpha^7\ \alpha^3\ \alpha^5\ 0\ \alpha^2\ \alpha\ \alpha^6\ \alpha^4$		$1\ 0\ \alpha^2\ \alpha\ \alpha^6\ \alpha^4\ \alpha^7\ \alpha^3\ \alpha^5$		$1\ \alpha^6\ \alpha^4\ \alpha^7\ \alpha^3\ \alpha^5\ 0\ \alpha^2\ \alpha$
	$\alpha^4\ \alpha^6\ \alpha^5\ \alpha^2\ 1\ \alpha^3\ \alpha^7\ \alpha\ 0$		$\alpha^4\ 1\ \alpha^3\ \alpha^7\ \alpha\ 0\ \alpha^6\ \alpha^5\ \alpha^2$		$\alpha^4\ \alpha\ 0\ \alpha^6\ \alpha^5\ \alpha^2\ 1\ \alpha^3\ \alpha^7$
	$\alpha\ \alpha^5\ 1\ \alpha^4\ \alpha^6\ 0\ \alpha^3\ \alpha^2\ \alpha^7$		$\alpha\ \alpha^6\ 0\ \alpha^3\ \alpha^2\ \alpha^7\ \alpha^5\ 1\ \alpha^4$		$\alpha\ \alpha^2\ \alpha^7\ \alpha^5\ 1\ \alpha^4\ \alpha^6\ 0\ \alpha^3$
	$\alpha^7\ \alpha^2\ \alpha^4\ 0\ \alpha\ 1\ \alpha^5\ \alpha^3\ \alpha^6$		$\alpha^7\ \alpha\ 1\ \alpha^5\ \alpha^3\ \alpha^6\ \alpha^2\ \alpha^4\ 0$		$\alpha^7\ \alpha^3\ \alpha^6\ \alpha^2\ \alpha^4\ 0\ \alpha\ 1\ \alpha^5$
	$\alpha^6\ \alpha^3\ 0\ 1\ \alpha^7\ \alpha^4\ \alpha^2\ \alpha^5\ \alpha$		$\alpha^6\ \alpha^7\ \alpha^4\ \alpha^2\ \alpha^5\ \alpha\ \alpha^3\ 0\ 1$		$\alpha^6\ \alpha^5\ \alpha\ \alpha^3\ 0\ 1\ \alpha^7\ \alpha^4\ \alpha^2$
	$\alpha^5\ 0\ \alpha^7\ \alpha^6\ \alpha^3\ \alpha\ \alpha^4\ 1\ \alpha^2$		$\alpha^5\ \alpha^3\ \alpha\ \alpha^4\ 1\ \alpha^2\ 0\ \alpha^7\ \alpha^6$		$\alpha^5\ 1\ \alpha^2\ 0\ \alpha^7\ \alpha^6\ \alpha^3\ \alpha\ \alpha^4$
	$\alpha^2\ 1\ \alpha^6\ \alpha\ \alpha^5\ \alpha^7\ 0\ \alpha^4\ \alpha^3$		$\alpha^2\ \alpha^5\ \alpha^7\ 0\ \alpha^4\ \alpha^3\ 1\ \alpha^6\ \alpha$		$\alpha^2\ \alpha^4\ \alpha^3\ 1\ \alpha^6\ \alpha\ \alpha^5\ \alpha^7\ 0$
	$\alpha^3\ \alpha^4\ \alpha\ \alpha^7\ \alpha^2\ \alpha^6\ 1\ 0\ \alpha^5$		$\alpha^3\ \alpha^2\ \alpha^6\ 1\ 0\ \alpha^5\ \alpha^4\ \alpha\ \alpha^7$		$\alpha^3\ 0\ \alpha^5\ \alpha^4\ \alpha\ \alpha^7\ \alpha^2\ \alpha^6\ 1$

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 $\boldsymbol{y}_{kp}, \boldsymbol{y}_{kp+1}, \cdots$, and $\boldsymbol{y}_{kp+p-1}$ ($k = 0, 1, \cdots, p^{m-1} - 1$) to be in an equivalence class of the relation R.** For example, we can choose the vectors for GF(2^3) as follows:

$$\begin{aligned}
\boldsymbol{y}_0 &= (0,0,0,0,0,0,0,0),\\
\boldsymbol{y}_1 &= (1,1,1,1,1,1,1,1),\\
\boldsymbol{y}_2 &= (\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha),\\
\boldsymbol{y}_3 &= (\alpha^3,\alpha^3,\alpha^3,\alpha^3,\alpha^3,\alpha^3,\alpha^3,\alpha^3),\\
\boldsymbol{y}_4 &= (\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2),\\
\boldsymbol{y}_5 &= (\alpha^6,\alpha^6,\alpha^6,\alpha^6,\alpha^6,\alpha^6,\alpha^6,\alpha^6),\\
\boldsymbol{y}_6 &= (\alpha^4,\alpha^4,\alpha^4,\alpha^4,\alpha^4,\alpha^4,\alpha^4,\alpha^4),\\
\boldsymbol{y}_7 &= (\alpha^5,\alpha^5,\alpha^5,\alpha^5,\alpha^5,\alpha^5,\alpha^5,\alpha^5).
\end{aligned}$$

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

$$\boldsymbol{c}^*_{i,j} = x_i\boldsymbol{g} + \boldsymbol{y}_j, \quad i, j = 0, 1, \cdots, p^m - 1. \tag{5}$$

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

$$\begin{aligned}
\boldsymbol{c}^*_{0,0} &= x_0\boldsymbol{g} + \boldsymbol{y}_0 = (0,0,0,0,0,0,0,0),\\
\boldsymbol{c}^*_{0,1} &= x_0\boldsymbol{g} + \boldsymbol{y}_1 = (1,1,1,1,1,1,1,1),\\
&\vdots\\
\boldsymbol{c}^*_{7,6} &= x_7\boldsymbol{g} + \boldsymbol{y}_6 = (\alpha^4,\alpha^3,\alpha^5,\alpha^2,\alpha,\alpha^6,0,1),\\
\boldsymbol{c}^*_{7,7} &= x_7\boldsymbol{g} + \boldsymbol{y}_7 = (\alpha^5,\alpha,\alpha^4,\alpha^6,\alpha^3,\alpha^2,1,0).
\end{aligned}$$

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

Equivalence class	Elements in $\boldsymbol{C}^*$	Subsequences in $\boldsymbol{C}$
$\{0, 1, \alpha^4\}$	0	100000000
	1	010000000
	$\alpha^4 = 2$	001000000
$\{\alpha, \alpha^7, \alpha^6\}$	α	000100000
	$\alpha^7 = \alpha + 1$	000010000
	$\alpha^6 = \alpha + 2$	000001000
$\{\alpha^5, \alpha^2, \alpha^3\}$	$\alpha^5 = 2\alpha$	000000100
	$\alpha^2 = 2\alpha + 1$	000000010
	$\alpha^3 = 2\alpha + 2$	000000001

(v) Finally, transform the codewords $\boldsymbol{c}^*_{i,j}$ ($i, j = 0, 1, \cdots, p^m - 1$) in the code $\boldsymbol{C}^*$ into binary codewords $\boldsymbol{c}_{i,j}$, which constitute the binary code $\boldsymbol{C}$. 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 $\boldsymbol{c}_{i,j}$ in the p-chip code $\boldsymbol{C}$, 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:

$$0 \rightarrow (\underline{1,0},0,0,0,0,0,0),$$

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

Gr.	User	C^*								Chip-pair code C							
0	0	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	10000000 01000000	10000000 01000000	10000000 01000000	10000000 01000000	10000000 01000000	10000000 01000000	10000000 01000000	10000000 01000000
	1	α α^3	α α^3	α α^3	α α^3	α α^3	α α^3	α α^3	α α^3	00100000 00010000	00100000 00010000	00100000 00010000	00100000 00010000	00100000 00010000	00100000 00010000	00100000 00010000	00100000 00010000
	2	α^2 α^6	α^2 α^6	α^2 α^6	α^2 α^6	α^2 α^6	α^2 α^6	α^2 α^6	α^2 α^6	00001000 00000100	00001000 00000100	00001000 00000100	00001000 00000100	00001000 00000100	00001000 00000100	00001000 00000100	00001000 00000100
	3	α^4 α^5	α^4 α^5	α^4 α^5	α^4 α^5	α^4 α^5	α^4 α^5	α^4 α^5	α^4 α^5	00000010 00000001	00000010 00000001	00000010 00000001	00000010 00000001	00000010 00000001	00000010 00000001	00000010 00000001	00000010 00000001
1	4	0 1	1 0	α α^3	α^2 α^6	α^3 α	α^4 α^5	α^5 α^4	α^6 α^2	10000000 01000000	01000000 10000000	00100000 00010000	00001000 00000100	00010000 00100000	00000010 00000001	00000001 00000010	00000100 00001000
	5	α α^3	α^3 α	0 1	α^4 α^5	1 0	α^2 α^6	α^6 α^2	α^5 α^4	00100000 00010000	00010000 00100000	10000000 01000000	00000010 00000001	01000000 10000000	00001000 00000100	00000100 00001000	00000001 00000010
	6	α^2 α^6	α^6 α^2	α^4 α^5	0 1	α^5 α^4	α α^3	α^3 α	1 0	00001000 00000100	00000100 00001000	00000010 00000001	10000000 01000000	00000001 00000010	00100000 00010000	00010000 00100000	01000000 10000000
	7	α^4 α^5	α^5 α^4	α^2 α^6	α α^3	α^6 α^2	0 1	1 0	α^3 α	00000010 00000001	00000001 00000010	00001000 00000100	00100000 00010000	00000100 00001000	10000000 01000000	01000000 10000000	00010000 00100000
2	8	0 1	α α^3	α^2 α^6	α^3 α	α^4 α^5	α^5 α^4	α^6 α^2	1 0	10000000 01000000	00100000 00010000	00001000 00000100	00010000 00100000	00000010 00000001	00000001 00000010	00000100 00001000	01000000 10000000
	9	α α^3	0 1	α^4 α^5	1 0	α^2 α^6	α^6 α^2	α^5 α^4	α^3 α	00100000 00010000	10000000 01000000	00000010 00000001	01000000 10000000	00001000 00000100	00000100 00001000	00000001 00000010	00010000 00100000
	10	α^2 α^6	α^4 α^5	0 1	α^5 α^4	α α^3	α^3 α	1 0	α^6 α^2	00001000 00000100	00000010 00000001	10000000 01000000	00000001 00000010	00100000 00010000	00010000 00100000	01000000 10000000	00000100 00001000
	11	α^4 α^5	α^2 α^6	α α^3	α^6 α^2	0 1	1 0	α^3 α	α^5 α^4	00000010 00000001	00001000 00000100	00100000 00010000	00000100 00001000	10000000 01000000	01000000 10000000	00010000 00100000	00000001 00000010
3	12	0 1	α^2 α^6	α^3 α	α^4 α^5	α^5 α^4	α^6 α^2	1 0	α α^3	10000000 01000000	00001000 00000100	00010000 00100000	00000010 00000001	00000001 00000010	00000100 00001000	01000000 10000000	00100000 00010000
	13	α α^3	α^4 α^5	1 0	α^2 α^6	α^6 α^2	α^5 α^4	α^3 α	0 1	00100000 00010000	00000010 00000001	01000000 10000000	00001000 00000100	00000100 00001000	00000001 00000010	00010000 00100000	10000000 01000000
	14	α^2 α^6	0 1	α^5 α^4	α α^3	α^3 α	1 0	α^6 α^2	α^4 α^5	00001000 00000100	10000000 01000000	00000001 00000010	00100000 00010000	00010000 00100000	01000000 10000000	00000100 00001000	00000010 00000001
	15	α^4 α^5	α α^3	α^6 α^2	0 1	1 0	α^3 α	α^5 α^4	α^2 α^6	00000010 00000001	00100000 00010000	00000100 00001000	10000000 01000000	01000000 10000000	00010000 00100000	00000001 00000010	00001000 00000100
⋮	⋮	⋮								⋮							

$$
\begin{aligned}
1 &\rightarrow (\underline{0, 1,}\, 0, 0, 0, 0, 0, 0),\\
\alpha &\rightarrow (0, 0, \underline{1, 0,}\, 0, 0, 0, 0),\\
\alpha^3 &\rightarrow (0, 0, \underline{0, 1,}\, 0, 0, 0, 0),\\
\alpha^2 &\rightarrow (0, 0, 0, 0, \underline{1, 0,}\, 0, 0),\\
\alpha^6 &\rightarrow (0, 0, 0, 0, \underline{0, 1,}\, 0, 0),\\
\alpha^4 &\rightarrow (0, 0, 0, 0, 0, 0, \underline{1, 0}),\\
\alpha^5 &\rightarrow (0, 0, 0, 0, 0, 0, \underline{0, 1}).
\end{aligned}
$$

(vi) When assigning p-chip codewords to each user in the EWO scheme, assign p consecutive codewords $\boldsymbol{c}_{i,kp}, \boldsymbol{c}_{i,kp+1}, \cdots, \boldsymbol{c}_{i,kp+p-1}$ $(i = 0, 1, \cdots, p^m - 1,\ k = 0, 1, \cdots, p^{m-1} - 1)$ **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 $\boldsymbol{c}_{0,0}$ and $\boldsymbol{c}_{0,1}$ to the 0th user, $\boldsymbol{c}_{0,2}$ and $\boldsymbol{c}_{0,3}$ to the 1st user, $\cdots$, and $\boldsymbol{c}_{7,6}$ and $\boldsymbol{c}_{7,7}$ 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 $\boldsymbol{C}^*$ over GF(2^2) and its chip-pair code $\boldsymbol{C}$. In Tables 1 and 2, α is a primitive element of GF(2^2) and $\pi(x) = x^2 + x + 1$. In the construction of $\boldsymbol{C}^*$, we suppose $\boldsymbol{g} = (0, 1, \alpha, \alpha^2)$, $x_0 = 0$, $x_1 = 1$, $x_2 = \alpha$, $x_2 = \alpha^2$, $\boldsymbol{y}_0 = (0, 0, 0, 0)$, $\boldsymbol{y}_1 = (1, 1, 1, 1)$, $\boldsymbol{y}_2 = (\alpha, \alpha, \alpha, \alpha)$, and $\boldsymbol{y}_3 = (\alpha^2, \alpha^2, \alpha^2, \alpha^2)$.

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 GF(2^2) and binary subsequences assigned to the GF(2^2) 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 shows the code $\boldsymbol{C}^*$ over GF(2^3) and its chip-pair code $\boldsymbol{C}$. Table 4 shows the equivalence classes in GF(2^3) and binary subsequences assigned to the GF(2^3) elements. In Tables 3 and 4, α is a primitive element of GF(2^3) and $\pi(x) = x^3 + x + 1$. In the construction of

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

Gr.	User	$\boldsymbol{C}^*$	GMPSC
0	0	$0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$ $1\ 1\ 1\ 1\ 1\ 1\ 1\ 1$	10000000 10000000 10000000 10000000 10000000 10000000 10000000 10000000 01000000 01000000 01000000 01000000 01000000 01000000 01000000 01000000
	1	$\alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha$ $\alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2$	00100000 00100000 00100000 00100000 00100000 00100000 00100000 00100000 00010000 00010000 00010000 00010000 00010000 00010000 00010000 00010000
	2	$\alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3$ $\alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4$	00001000 00001000 00001000 00001000 00001000 00001000 00001000 00001000 00000100 00000100 00000100 00000100 00000100 00000100 00000100 00000100
	3	$\alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5$ $\alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6$	00000010 00000010 00000010 00000010 00000010 00000010 00000010 00000010 00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001
1	4	$0\ 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6$ $1\ 0\ \alpha^3\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2$	10000000 01000000 00100000 00010000 00001000 00000100 00000010 00000001 01000000 10000000 00001000 00000001 00100000 00000010 00000100 00010000
	5	$\alpha\ \alpha^3\ 0\ \alpha^4\ 1\ \alpha^2\ \alpha^6\ \alpha^5$ $\alpha^2\ \alpha^6\ \alpha^4\ 0\ \alpha^5\ \alpha\ \alpha^3\ 1$	00100000 00001000 10000000 00000100 01000000 00010000 00000001 00000010 00010000 00000001 00000100 10000000 00000010 00100000 00001000 01000000
	6	$\alpha^3\ \alpha\ 1\ \alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4$ $\alpha^4\ \alpha^5\ \alpha^2\ \alpha\ \alpha^6\ 0\ 1\ \alpha^3$	00001000 00100000 01000000 00000010 10000000 00000001 00010000 00000100 00000100 00000010 00010000 00100000 00000001 10000000 01000000 00001000
	7	$\alpha^5\ \alpha^4\ \alpha^6\ \alpha^3\ \alpha^2\ 1\ 0\ \alpha$ $\alpha^6\ \alpha^2\ \alpha^5\ 1\ \alpha^4\ \alpha^3\ \alpha\ 0$	00000010 00000100 00000001 00001000 00010000 01000000 10000000 00100000 00000001 00010000 00000010 01000000 00000100 00001000 00100000 10000000
2	8	$0\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1$ $1\ \alpha^3\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2\ 0$	10000000 00100000 00010000 00001000 00000100 00000010 00000001 01000000 01000000 00001000 00000001 00100000 00000010 00000100 00010000 10000000
	9	$\alpha\ 0\ \alpha^4\ 1\ \alpha^2\ \alpha^6\ \alpha^5\ \alpha^3$ $\alpha^2\ \alpha^4\ 0\ \alpha^5\ \alpha\ \alpha^3\ 1\ \alpha^6$	00100000 10000000 00000100 01000000 00010000 00000001 00000010 00001000 00010000 00000100 10000000 00000010 00100000 00001000 01000000 00000001
	10	$\alpha^3\ 1\ \alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha$ $\alpha^4\ \alpha^2\ \alpha\ \alpha^6\ 0\ 1\ \alpha^3\ \alpha^5$	00001000 01000000 00000010 10000000 00000001 00010000 00000100 00100000 00000100 00010000 00100000 00000001 10000000 01000000 00001000 00000010
	11	$\alpha^5\ \alpha^6\ \alpha^3\ \alpha^2\ 1\ 0\ \alpha\ \alpha^4$ $\alpha^6\ \alpha^5\ 1\ \alpha^4\ \alpha^3\ \alpha\ 0\ \alpha^2$	00000010 00000001 00001000 00010000 01000000 10000000 00100000 00000100 00000001 00000010 01000000 00000100 00001000 00100000 10000000 00010000
3	12	$0\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1\ \alpha$ $1\ \alpha^6\ \alpha\ \alpha^5\ \alpha^4\ \alpha^2\ 0\ \alpha^3$	10000000 00010000 00001000 00000100 00000010 00000001 01000000 00100000 01000000 00000001 00100000 00000010 00000100 00010000 10000000 00001000
	13	$\alpha\ \alpha^4\ 1\ \alpha^2\ \alpha^6\ \alpha^5\ \alpha^3\ 0$ $\alpha^2\ 0\ \alpha^5\ \alpha\ \alpha^3\ 1\ \alpha^6\ \alpha^4$	00100000 00000100 01000000 00010000 00000001 00000010 00001000 10000000 00010000 10000000 00000010 00100000 00001000 01000000 00000001 00000100
	14	$\alpha^3\ \alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha\ 1$ $\alpha^4\ \alpha\ \alpha^6\ 0\ 1\ \alpha^3\ \alpha^5\ \alpha^2$	00001000 00000010 10000000 00000001 00010000 00000100 00100000 01000000 00000100 00100000 00000001 10000000 01000000 00001000 00000010 00010000
	15	$\alpha^5\ \alpha^3\ \alpha^2\ 1\ 0\ \alpha\ \alpha^4\ \alpha^6$ $\alpha^6\ 1\ \alpha^4\ \alpha^3\ \alpha\ 0\ \alpha^2\ \alpha^5$	00000010 00001000 00010000 01000000 10000000 00100000 00000100 00000001 00000001 01000000 00000100 00001000 00100000 10000000 00010000 00000010
⋮	⋮	⋮	⋮

$\boldsymbol{C}^*$, we suppose $\boldsymbol{g} = (0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$, $x_0 = 0$, $x_1 = 1$, $x_2 = \alpha$, $x_3 = \alpha^2$, $x_4 = \alpha^3$, $x_5 = \alpha^4$, $x_6 = \alpha^5$, $x_7 = \alpha^6$, $\boldsymbol{y}_0 = (0, 0, \cdots, 0)$, $\boldsymbol{y}_1 = (1, 1, \cdots, 1)$, $\boldsymbol{y}_2 = (\alpha, \alpha, \cdots, \alpha)$, $\boldsymbol{y}_3 = (\alpha^3, \alpha^3, \cdots, \alpha^3)$, $\boldsymbol{y}_4 = (\alpha^2, \alpha^2, \cdots, \alpha^2)$, $\boldsymbol{y}_5 = (\alpha^6, \alpha^6, \cdots, \alpha^6)$, $\boldsymbol{y}_6 = (\alpha^4, \alpha^4, \cdots, \alpha^4)$, and $\boldsymbol{y}_7 = (\alpha^5, \alpha^5, \cdots, \alpha^5)$. 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.

Table 5 shows an example of the code $\boldsymbol{C}^*$ over GF(3^2) and its three-chip code $\boldsymbol{C}$. Table 6 shows the equivalence classes in GF(3^2) and binary subsequences assigned to the GF(3^2) elements. In Tables 5 and 6, α is a primitive element of GF(3^2) and $\pi(x) = x^2 + x + 2$. In the construction of $\boldsymbol{C}^*$, we suppose $\boldsymbol{g} = (0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$, $x_0 = 0$, $x_1 = 1$, $x_2 = \alpha$, $x_3 = \alpha^2$, $x_4 = \alpha^3$, $x_5 = \alpha^4$, $x_6 = \alpha^5$, $x_7 = \alpha^6$, $x_8 = \alpha^7$, $\boldsymbol{y}_0 = (0, 0, \cdots, 0)$, $\boldsymbol{y}_1 = (1, 1, \cdots, 1)$, $\boldsymbol{y}_2 = (\alpha^4, \alpha^4, \cdots, \alpha^4)$, $\boldsymbol{y}_3 = (\alpha, \alpha, \cdots, \alpha)$, $\boldsymbol{y}_4 = (\alpha^7, \alpha^7, \cdots, \alpha^7)$, $\boldsymbol{y}_5 = (\alpha^6, \alpha^6, \cdots, \alpha^6)$, $\boldsymbol{y}_6 = (\alpha^5, \alpha^5, \cdots, \alpha^5)$, $\boldsymbol{y}_7 = (\alpha^2, \alpha^2, \cdots, \alpha^2)$, and $\boldsymbol{y}_8 = (\alpha^3, \alpha^3, \cdots, \alpha^3)$. Because p is equal to 3, three codewords are assigned to each user, as shown in Table 5. If we divide a codeword into 27 small blocks, each 3 chips long, nonzero chips of these 3 codewords 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 is small when q is 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 $\boldsymbol{C}^*$ over GF(2^3) in Table 3. The values of $\boldsymbol{g}$, x_i, and $\boldsymbol{y}_j$ for $\boldsymbol{C}^*$ in Table 7 are the same as those for $\boldsymbol{C}^*$ in Table 3. We can see that the codewords in this table have the chip-pair property. In contrast, Table 8 shows the binary codewords of the GMPSC presented in Ref. [21]. The values of $\boldsymbol{g}$ and x_i for $\boldsymbol{C}^*$ in Table 8 are the same as those for $\boldsymbol{C}^*$ in Table 3. However, the values of $\boldsymbol{y}_j$ are determined not considering the equivalent relation R, and they are supposed as follows: $\boldsymbol{y}_0 = (0, 0, \cdots, 0)$, $\boldsymbol{y}_1 = (1, 1, \cdots, 1)$, $\boldsymbol{y}_2 = (\alpha, \alpha, \cdots, \alpha)$, $\boldsymbol{y}_3 = (\alpha^2, \alpha^2, \cdots, \alpha^2)$, $\boldsymbol{y}_4 = (\alpha^3, \alpha^3, \cdots, \alpha^3)$, $\boldsymbol{y}_5 = (\alpha^4, \alpha^4, \cdots, \alpha^4)$, $\boldsymbol{y}_6 = (\alpha^5, \alpha^5, \cdots, \alpha^5)$, and $\boldsymbol{y}_7 = (\alpha^6, \alpha^6, \cdots, \alpha^6)$. Though both codes in Tables 7 and 8 are constructed from GF(2^3) and have the same code length, the codewords in Table 8 do not have the chip-pair property.

Because the class of p-chip codes is a subset of the class of GMPSCs, p-chip codes retain the properties of GMPSCs. For example, Eq. (4), which represents the correlation property of GMPSC, also represents that of p-chip codes.

In addition, any p-chip code generated from GF(p^m) has the p-chip property, that is, nonzero chips of p codewords assigned to a single user are always in the same sub-blocks. This property stems from the property of the code $\boldsymbol{C}^*$, 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 Sect. 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 $\beta + \gamma_0$, $\beta + \gamma_1, \cdots$, and $\beta + \gamma_{p-1}$ are in the equivalence class $[\beta + \gamma_0]$ for any element β in GF(p^m), if γ_0, γ_1, $\cdots$, and γ_{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, $\gamma_0, \gamma_1, \cdots$, and γ_{p-1} correspond to the elements in $\boldsymbol{y}_{kp}, \boldsymbol{y}_{kp+1}, \cdots$, and $\boldsymbol{y}_{kp+p-1}$, respectively, and β corresponds to each element in the vector $x_i\boldsymbol{g}$ in Eq. (5) for $i = 0, 1, \cdots, p^m - 1$ and $k = 0, 1, \cdots, p^{m-1} - 1$. In addition, the p elements in an equivalence class are always assigned to the binary subsequences whose locations of nonzero chips are in the same sub-block, when the codewords $\boldsymbol{c}^*_{i,j}$ $(i, j = 0, 1, \cdots, p^m - 1)$ in the code $\boldsymbol{C}^*$ are transformed into binary codewords $\boldsymbol{c}_{i,j}$ in the p-chip code $\boldsymbol{C}$. Hence the code $\boldsymbol{C}$ constructed by the procedure in Sect. 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 cancel 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, 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.

Acknowledgments

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

References

[1] P.R. Prucnal, Optical Code Division Multiple Access: Fundamentals and Applications, CRC Press, Boca Raton, FL, 2006.

[2] H. Ghafouri-Shiraz and M.M. Karbassian, Optical CDMA Networks: Principles, Analysis and Applications, John Wiley & Sons, Hoboken, NJ, 2012.

[3] W.C. Kwong, P.A. Perrier, and P.R. Prucnal, "Performance comparison of asynchronous and synchronous code-division multiple-access techniques for fiber-optic local area networks," IEEE Trans. Commun., vol.39, no.11, pp.1625–1634, Nov. 1991.

[4] G.-C. Yang and W.C. Kwong, Prime Codes with Applications to CDMA Optical and Wireless Networks, Artech House, Mobile communications series, Norwood, MA, 2002.

[5] T.K. Matsushima and Y. Teramachi, "Generalized MPSC and its performance in synchronous optical CDMA systems," Proc. Int. Symp. Information Theory and Its Applications, Seoul, Korea, Tue3-4-5, Oct. 2006.

[6] T.K. Matsushima, T. Nagao, N. Ochiai and Y. Teramachi, "Generalization of modified prime sequence codes and its properties," IEICE Trans. Fundamentals (Japanese Edition), vol.J91-A, no.5, pp.559–573, May 2008.

[7] H.M.H. Shalaby, M.A. Mangoud, and S.E. El-Khamy, "A new interference cancellation technique for synchronous CDMA communication systems using modified prime codes," Proc. 2nd IEEE Symposium on Computers and Communications, Alexandria, pp.556–560, July 1997.

[8] M.-Y. Liu and H.-W. Tsao, "Cochannel interference cancellation via employing a reference correlator for synchronous optical CDMA systems," Microwave and Optical Technology Letters, vol.25, no.6, June 2000.

[9] N. Ochiai, S. Kushibiki, T.K. Matsushima, and Y. Teramachi, "Performance analysis of synchronous optical CDMA systems with

EWO signaling," IEICE Trans. Fundamentals (Japanese Edition), vol.J86-A, no.9, pp.957–968, Sept. 2003.

[10] N. Ochiai, S. Kushibiki, T.K. Matsushima, and Y. Teramachi, "Performance analysis of synchronous optical CDMA systems with EWO signaling," Electron. Comm. Jpn. Pt. III, vol.87, no.12, pp.37–48, Dec. 2004.

[11] A. Kamikata, T.K. Matsushima, S. Yamasaki, S. Miyazaki, and K. Omura, "A study on synchronous optical CDMA systems canceling multi-user interference and background light simultaneously," IEICE Trans. Fundamentals (Japanese Edition), vol.J103-A, no.7, pp.126–141, July 2020.

[12] S. Rajagopal, R.D. Roberts, and S.K. Lim, "IEEE 802.15.7 visible light communication: Modulation schemes and dimming support," IEEE Commun. Mag., vol.50, no.3, pp.72–82, Oct. 2012.

[13] H. Miyakawa, Y. Iwadare, and H. Imai, Coding Theory, Shokodo, Tokyo, 1973 (in Japanese).

[14] K. Ono, S. Yamasaki, and T.K. Matsushima, "An optical CDMA scheme combining modified prime sequence codes and bi-orthogonal codes," IEICE Technical Report, WBS2019-65, March 2020 (in Japanese).

[15] K. Ono, S. Yamasaki, S. Miyazaki, and T.K. Matsushima, "Optical CDMA scheme using generalized modified prime sequence codes and extended bi-orthogonal codes," IEICE Trans. Fundamentals, vol.E104-A, no.9, pp.1329–1338, Sept. 2021.

[16] S. Yamasaki, T.K. Matsushima, and K. Ono, "A study on code construction method for optical CDMA with variable spreading factor," IEICE Technical Report, IT2020-9, May 2020 (in Japanese).

[17] T.K. Matsushima, S. Yamasaki, and K. Ono, "Study on construction method of generalized modified prime sequence codes — Proposal and applications of chip-pair codes —," IEICE Technical Report, WBS2020-2, July 2020 (in Japanese).

[18] T.K. Matsushima, S. Yamasaki, and K. Ono, "A study on chip-pair codes for synchronous optical CDMA systems," IEICE Technical Report, IT2020-19, Sept. 2020.

[19] R.E. Blahaut, Algebraic Methods for Signal Processing and Communications Coding, Section 3, Springer-Verlag, New York, NY, 1992.

[20] 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.

[21] T.K. Matsushima, N. Ochiai, T. Nagao, and Y. Teramachi, "On the construction of codes over GF(p^m) for synchronous optical CDMA systems," IEICE Technical Report, WBS2005-39, Oct. 2005.

[22] A.W. Lam and A.M. Hussain, "Performance analysis of direct-detection optical CDMA communication systems with avalanche photodiodes," IEEE Trans. Commun., vol.40, no.4, pp.810–820, April 1992.

[23] H. Habuchi and F. Ono, "Optical code shift keying with modified prime sequences," IEICE Technical Report, WBS2003-74, Oct. 2003 (in Japanese).

[24] S. Tanaka and S. Usami, "Consideration on multiplexing code shift keying on optical CDMA system," IEEJ Trans. EIS, vol.130, no.12, pp.2174–2175, Dec. 2010 (in Japanese).

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 Sect. 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 $xRy \wedge yRz \Rightarrow xRz$.

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 kth user, and the user uses $\mathbf{w}_{k,I}$ to spread a datum I ($I \in \{0, 1\}$) [9], [10]. The kth user's decoder computes $\mathit{\Gamma}_0$ and $\mathit{\Gamma}_1$, 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.

$\mathit{\Gamma}_0$ and $\mathit{\Gamma}_1$ are represented as follows:

$$\mathit{\Gamma}_0 = \Gamma(\mathbf{r}, \mathbf{w}_{k,0}), \tag{A·1}$$

$$\mathit{\Gamma}_1 = \Gamma(\mathbf{r}, \mathbf{w}_{k,1}). \tag{A·2}$$

Then the decoder calculates the difference $\mathit{\Gamma}_1 - \mathit{\Gamma}_0$. If the difference is greater than or equal to the threshold *zero*, the decoder outputs $\hat{I} = 1$ as a decoded datum. Otherwise, the decoder outputs $\hat{I} = 0$. 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 ith 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

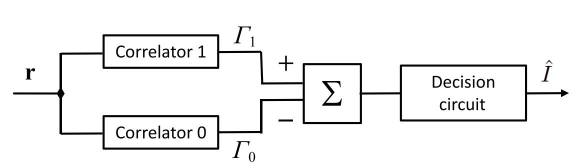


Fig. A·1 Block diagram of EWO decoder ($p = 2$).

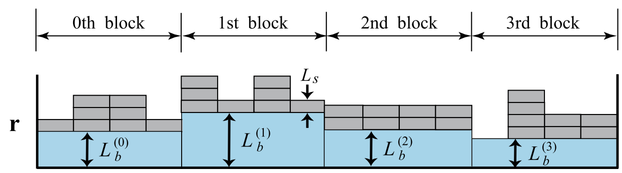


Fig. A·2 Example of received signals with interference light varying by block (p^m chips) and user sequences ($p = 2, q = 4$).

from the desired user and the interfering users. Figure A·2 shows an example of received signals that include interference light and users' sequences.

GMPSC codewords are assigned to $q^2/2$ users in total. From Eqs. (4), (A·1), and (A·2), the correlation values Γ_0 and Γ_1 calculated at each user's decoder are represented as follows:

$$\Gamma_0 = q(1-I)L_s + \frac{q^2-q}{2}L_s + \sum_{i=0}^{q-1} L_b^{(i)}, \qquad \text{(A·3)}$$

$$\Gamma_1 = qIL_s + \frac{q^2-q}{2}L_s + \sum_{i=0}^{q-1} L_b^{(i)}, \qquad \text{(A·4)}$$

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 $\Gamma_1 - \Gamma_0$, 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 $\mathbf{w}_{k,0}, \mathbf{w}_{k,1}, \cdots$, and $\mathbf{w}_{k,p-1}$ are assigned to the kth user and the user uses $\mathbf{w}_{k,I}$ to spread a datum I ($I \in \{0,1,\cdots,p-1\}$). Each user's decoder has p correlators and computes $\Gamma_0, \Gamma_1, \cdots$, and Γ_{p-1}, which are correlation values between the received sequence $\mathbf{r}$ and the codewords $\mathbf{w}_{k,0}, \mathbf{w}_{k,1}, \cdots$, and $\mathbf{w}_{k,p-1}$, respectively. Γ_ℓ is represented as follows:

$$\Gamma_\ell = \Gamma(\mathbf{r}, \mathbf{w}_{k,\ell}), \qquad \text{(A·5)}$$

for $\ell = 0, 1, \cdots, p-1$. Then, the decoder chooses the maximum value in $\Gamma_0, \Gamma_1, \cdots$, and Γ_{p-1}. If the maximum value is Γ_ℓ, 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 Γ_ℓ in Eq. (A·5) is represented as follows:

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

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.

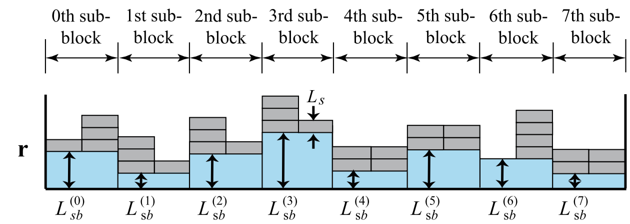


Fig. A·3 Example of received signals with interference light varying by sub-block (p chips) and user sequences ($p = 2, q = 4$).

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. 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 ith block is $L_{sb}^{(i)}$ 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 $\mathbf{w}_{k,0}, \mathbf{w}_{k,1}, \cdots$, and $\mathbf{w}_{k,p-1}$ are assigned to the kth user ($k = 0, 1, 2, \cdots, q^2/p - 1$), and that $\mathbf{w}_{k,I}$ 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 $\Phi_k = \{\phi_{k,0}, \phi_{k,1}, \cdots, \phi_{k,q-1}\}$, where the q marks in each codeword for the kth user are in the $\phi_{k,0}$th, $\phi_{k,1}$th, $\cdots$, and $\phi_{k,q-1}$th sub-blocks, respectively. For example, for the chip-pair code in Table 1, $\Phi_0 = \{0, 2, 4, 6\}$, $\Phi_1 = \{1, 3, 5, 7\}, \cdots$, and $\Phi_7 = \{1, 2, 5, 6\}$.

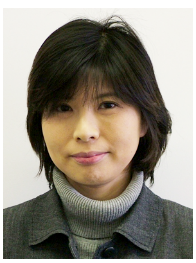
Each user's decoder has p correlators and computes $\Gamma_0, \Gamma_1, \cdots$, and Γ_{p-1}, which are correlation values between the received sequence $\mathbf{r}$ and the codewords $\mathbf{w}_{k,0}, \mathbf{w}_{k,1}, \cdots$, and $\mathbf{w}_{k,p-1}$, respectively. Γ_ℓ is represented as Eq. (A·5). Then, the decoder chooses the maximum value in $\Gamma_0, \Gamma_1, \cdots$, and Γ_{p-1}. If the maximum value is Γ_ℓ, 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 Γ_ℓ is represented as follows:

$$\Gamma_\ell = \begin{cases} qL_s + \frac{q^2-q}{p}L_s + \sum_{\phi\in\Phi_k} L_{sb}^{(\phi)} & \text{if } I = \ell, \\ \frac{q^2-q}{p}L_s + \sum_{\phi\in\Phi_k} L_{sb}^{(\phi)} & \text{if } I \neq \ell, \end{cases} \quad \text{(A·7)}$$

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 $\sum_{\phi\in\Phi_k} L_{sb}^{(\phi)}$ 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 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 an Emerita Professor. 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 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 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 wireless and multimedia communications. Dr. Yamasaki is a member of the IEEE.

Kyohei Ono received a B.S. degree in Manufacturing Technology and an M.S. degree in Manufacturing Engineering from National Institution for Academic Degrees and Quality Enhancement of Higher Education, Tokyo, Japan, in 2019 and 2021, respectively. He is currently with Japan Organization for Employment of the Elderly, Persons with Disabilities and Job Seekers. His research interests include optical communication systems, secret sharing and physical layer security.