

# Finite Field Multiple Access for Sourced Massive Random Access with Finite Blocklength

Qi-yue Yu, *Senior Member, IEEE*, Shi-wen Lin, and Shu Lin, *Life Fellow, IEEE*

**Abstract**—For binary source transmission, this paper introduces the concept of element-pair (EP) and establishes that when the Cartesian product of  $J$  distinct EPs satisfies the unique sum-pattern mapping (USPM) structural property, these  $J$  EPs can form a uniquely-decodable EP (UD-EP) code. EPs are treated as virtual resources allocated to different users in finite fields, serving to distinguish users. This approach enables the reordering of multiplexing and channel encoding modules, effectively addressing the finite blocklength (FBL) challenge in multiuser reliable transmission. Next, we introduce an orthogonal EP code  $\Psi_{o,B}$  constructed over an extension field  $\text{GF}(2^m)$ . Using this EP code, we develop a time-division mode of finite-field multiple-access (FFMA) systems, consisting of sparse-form and diagonal-form structures. Based on the diagonal-form (DF) structure, we present a specific configuration, referred to as polarization-adjusted DF-FFMA, which can simultaneously obtain the power gain and coding gain from the entire blocklength. Simulation results demonstrate that the proposed FFMA systems significantly improve error performance over a Gaussian multiple-access channel, compared to a slotted ALOHA system.

**Index Terms**—Multiple access, sourced random access, slotted ALOHA, binary source transmission, element pair (EP), finite-field multi-access (FFMA), finite blocklength (FBL), polarization-adjusted, Gaussian multiple-access channel (GMAC).

## I. INTRODUCTION

For the next generation of wireless communication, ultra massive machine type communication (um-MTC) is required to serve a huge number of users (or devices) simultaneously, e.g., the connection density of an um-MTC system is around  $10^6 \sim 10^8$  devices/km<sup>2</sup> [1]–[3]. The required multiple-access (MA) technique should simultaneously support massive users with short packet traffic, and achieve an acceptable per-user probability of error (PUPE) [4].

In general, grant-free random access (RA) is considered as a promising MA scheme for supporting um-MTC communications [5], [6]. The grant-free random access technique can be classified into sourced and unsourced RA, which can be applied in different scenarios [7]. In this paper, we focus on the sourced RA, which is used to serve device-oriented scenarios, e.g., monitoring the status of sensors, enabling the base station (BS) to be aware of both the messages and users (or devices) identities [5]. For a sourced RA system, each user is assigned a unique signature to identify the active user(s) at the BS. Typically, we can use different resources, sequences and/or codebooks to identify different users. The classical sourced RA system utilizes time slots to distinguish users, operating in a slotted ALOHA scheme, which simplifies both the active user detection and multiuser detection algorithms [8].

Nevertheless, for the massive random access scenario, the reliable performance of the slotted ALOHA scheme is limited by the blocklength of each time slot [9], [10]. The blocklength or the number of degrees of freedom (DoF) is set to be  $N$ , which is also called *finite blocklength (FBL)* constraint. Suppose there are totally  $J$  users. To separate users without ambiguity, the number of time slots is set to be equal to the number of users  $J$ . Thus, the blocklength of each time slot is equal to  $N/J$ . According to [10], we know that the maximal rate of each time slot is equal to

$$C(P) - \sqrt{\frac{V(P)}{(N/J)}} Q^{-1}(\epsilon) + \frac{1}{2} \frac{\log(N/J)}{(N/J)} + \mathcal{O}\left(\frac{1}{(N/J)}\right)$$

where  $C(P)$  is the channel capacity,  $P$  is the maximum power constraint, and  $\epsilon$  is the average error probability.  $V(P) = \frac{P(P+2)}{2(1+P)^2}$  is the dispersion of the Gaussian channel. Obviously, the maximal rate of each time slot decreases with the increased number of users  $J$ , especially  $J$  is a large value. Hence, it is challenging to design suitable schemes for solving the FBL of massive users reliability transmission problem.

In this paper, an MA coding is devised based on the *element-pair (EP) code* constructed over finite fields (FFs) [15]. We refer the proposed MA technique based on EP-coding as *finite-field MA (FFMA)* technique (or coding). An MA communication system using FFMA-coding is referred to as an FFMA system for simplicity. Unlike the slotted ALOHA scheme, which operates with a blocklength of  $N/J$ , the proposed FFMA system leverages the entire blocklength  $N$  to achieve error correction capabilities across all DoF. The key distinction lies in the order of encoding and multiplexing (MUX) modules in the proposed FFMA system, which differs from conventional MA techniques. It is noted that the finite-field MUX is performed by the EP-coding. By performing multiplexing before channel coding, the system maximizes channel gains from all available DoF.

The rest of this paper is organized as follows. Section II introduces the concept of EP-coding and presents an orthogonal EP code constructed over  $\text{GF}(2^m)$ . The encoding of the orthogonal EP code is introduced in Section III. Section IV presents an FFMA system for a massive MA transmission. In Section V, simulations of the error performances of the proposed FFMA systems are given. Section VI concludes the paper with some remarks.

## II. ORTHOGONAL EP CODE OVER $\text{GF}(2^m)$

Suppose  $\text{GF}(q)$  is a finite-field with  $q$  elements, where  $q$  is a prime number or a power of the prime number. Let  $\alpha$  denote a primitive element of  $\text{GF}(q)$ , and the powers of  $\alpha$ , i.e.,

The work presented in this paper was supported by the National Natural Science Foundation of China under Grand No. 62071148.

$\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^{(q-2)}$ , give all the  $q$  elements of  $\text{GF}(q)$ . For binary source transmission, a transmit bit is either  $(0)_2$  or  $(1)_2$ . We utilize two different elements in a finite-field  $\text{GF}(q)$  to express the bit information, i.e.,  $(0)_2 \mapsto \alpha^{l_{j,0}}$  and  $(1)_2 \mapsto \alpha^{l_{j,1}}$ , where  $\alpha^{l_{j,0}}, \alpha^{l_{j,1}} \in \text{GF}(q)$  and  $l_{j,0} \neq l_{j,1}$ . We define the selected two elements  $(\alpha^{l_{j,0}}, \alpha^{l_{j,1}})$  as an *element pair (EP)*.

In this paper, we construct *orthogonal element pair (EP) codes* over  $\text{GF}(2^m)$ , where  $q = 2^m$  and  $m$  is a positive integer with  $m \geq 2$ . Then, each element  $\alpha^{l_j}$ , with  $l_j = 0, 1, \dots, 2^m - 2$ , in  $\text{GF}(2^m)$  can be expressed as a linear sum of  $\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^{(m-1)}$  with coefficients from  $\text{GF}(2)$  as

$$\alpha^{l_j} = a_{j,0} + a_{j,1}\alpha + a_{j,2}\alpha^2 + \dots + a_{j,m-1}\alpha^{(m-1)}. \quad (1)$$

From (1), we see that the element  $\alpha^{l_j}$  can be uniquely represented by the  $m$ -tuple  $(a_{j,0}, a_{j,1}, \dots, a_{j,m-1})$  over  $\text{GF}(2)$ , which is a linear combination of  $\alpha^0, \alpha^1, \dots, \alpha^{m-1}$ , i.e.,  $\alpha^{l_j} = \bigoplus_{i=0}^{m-1} a_{j,i}\alpha^i$ . For  $0 \leq i < m$ , it is known that  $\alpha^i = (0, 0, \dots, 1, 0, \dots, 0)$  is an  $m$ -tuple with a 1-component at the  $i$ -th location and 0s elsewhere.

Based on the finite-field  $\text{GF}(2^m)$ , we define  $m$  EPs as

$$\begin{aligned} C_1 &= (0, \alpha^0) &= \alpha^0 \cdot C_B = \{\mathbf{0}, (1, 0, \dots, 0)\}, \\ C_2 &= (0, \alpha^1) &= \alpha^1 \cdot C_B = \{\mathbf{0}, (0, 1, \dots, 0)\}, \\ &\vdots \\ C_m &= (0, \alpha^{m-1}) &= \alpha^{m-1} \cdot C_B = \{\mathbf{0}, (0, 0, \dots, 1)\}, \end{aligned}$$

where  $\mathbf{0}$  is an  $m$ -tuple of zeros, and  $C_B = (0, 1)$ . The subscript ‘‘B’’ stands for ‘‘binary’’. Hence, for  $1 \leq j \leq m$ , the  $j$ -th EP  $C_j$  is given as  $C_j = \alpha^{j-1} \cdot C_B$ . The  $m$  EPs together can form an EP set, defined by  $\Psi_{o,B}$ , i.e.,

$$\begin{aligned} \Psi_{o,B} &= \{C_1, C_2, \dots, C_m\}, \\ &= \{\alpha^0 \cdot C_B, \alpha^1 \cdot C_B, \dots, \alpha^{m-1} \cdot C_B\}. \end{aligned} \quad (2)$$

With  $0 \leq i < m$ , any two different EPs in  $\Psi_{o,B}$ , e.g.,  $C_j$  and  $C_{j'}$  where  $j \neq j'$ , are *orthogonal* to each other.

Let  $(u_1, u_2, \dots, u_j, \dots, u_J)$  be a  $J$ -tuple over  $\text{GF}(2^m)$  in which the  $j$ -th component  $u_j$  is an element from the EP  $C_j$ , where  $1 \leq j \leq J$  and  $J \leq m$ . The  $J$ -tuple  $(u_1, u_2, \dots, u_J)$  is an element in the *Cartesian product*  $C_1 \times C_2 \times \dots \times C_J$  of the EPs in the EP set  $\Psi_{o,B}$ . We view each  $J$ -tuple  $\mathbf{u} = (u_1, u_2, \dots, u_j, \dots, u_J)$  in  $C_1 \times C_2 \times \dots \times C_J$  as a  $J$ -user EP codeword. In our paper,  $\Psi_{o,B}$  stands for an EP set and also an EP code. Hence, the Cartesian product

$$\Psi_{o,B} \triangleq (\alpha^0 \cdot C_B) \times (\alpha^1 \cdot C_B) \times \dots \times (\alpha^{m-1} \cdot C_B),$$

of the  $m$  EPs in  $\Psi_{o,B}$  can form an  $m$ -user EP code over  $\text{GF}(2^m)$  with  $2^m$  codewords.

Let  $(u_1, u_2, \dots, u_J)$  and  $(u'_1, u'_2, \dots, u'_J)$  be any two  $J$ -tuples in  $C_1 \times C_2 \times \dots \times C_J$  of the EP code  $\Psi_{o,B}$ . If  $\bigoplus_{j=1}^J u_j \neq \bigoplus_{j=1}^J u'_j$ , then an *finite-field sum-pattern (FFSP)*  $w$  uniquely specifies a  $J$ -tuple in  $C_1 \times C_2 \times \dots \times C_J$ . That is to say the mapping

$$(u_1, u_2, \dots, u_J) \iff w = \bigoplus_{j=1}^J u_j, \quad (3)$$

is a one-to-one mapping. In this case, given the FFSP  $w = \bigoplus_{j=1}^J u_j$ , we can uniquely recover the  $J$ -tuple  $(u_1, u_2, \dots, u_J)$

without ambiguity. We say that the Cartesian product  $C_1 \times C_2 \times \dots \times C_J$  has a *unique sum-pattern mapping (USPM) structural property*, and form an *uniquely-decodable EP (UD-EP) code*.

Because of the orthogonality between any two EPs in  $\Psi_{o,B}$ , it is easy to know the EP codeword in  $\Psi_{o,B}$  has USPM structural property. We call  $\Psi_{o,B}$  a  $J$ -user *orthogonal uniquely decodable EP (UD-EP) code* over  $\text{GF}(2^m)$ . When this code is used for an MA communication system with  $J$  users, the  $j$ -th component  $u_j$  in a codeword  $(u_1, u_2, \dots, u_J)$  is the element to be transmitted by the  $j$ -th user.

### III. ENCODING OF ORTHOGONAL UD-EP CODES

In this section, we first introduce the encoder of an EP code  $\Psi_{o,B}$ . Then, we investigate the orthogonal UD-EP codes  $\Psi_{o,B}$  encoded by a channel encoder  $C_{gc}$ . The subscript ‘‘gc’’ of  $C_{gc}$  stands for ‘‘globe code’’, since the channel code  $C_{gc}$  is used through the MA transmission.

#### A. Binary to Finite-field $\text{GF}(q)$ Transform Function

Let the bit-sequence at the output of the  $j$ -th user be  $\mathbf{b}_j = (b_{j,0}, b_{j,1}, \dots, b_{j,k}, \dots, b_{j,K-1})$ , where  $K$  is a positive integer,  $1 \leq j \leq J$  and  $0 \leq k < K$ . The EP encoder is to map each bit-sequence  $\mathbf{b}_j$  uniquely into an element-sequence  $\mathbf{u}_j = (u_{j,0}, u_{j,1}, \dots, u_{j,k}, \dots, u_{j,K-1})$  by a *binary to finite-field  $\text{GF}(q)$  transform function*  $F_{B2q}$ , i.e.,  $u_{j,k} = F_{B2q}(b_{j,k})$ .

Assume each user is assigned an EP, e.g., the EP of  $C_j = (\alpha^{l_{j,0}}, \alpha^{l_{j,1}})$  is assigned to the  $j$ -th user for  $1 \leq j \leq J$ . The subscript ‘‘j’’ of ‘‘ $l_{j,0}$ ’’ and ‘‘ $l_{j,1}$ ’’ stands for the  $j$ -th EP, and the subscripts ‘‘0’’ and ‘‘1’’ of ‘‘ $l_{j,0}$ ’’ and ‘‘ $l_{j,1}$ ’’ represent the input bits are  $(0)_2$  and  $(1)_2$ , respectively. For  $1 \leq j \leq J$ , we can set the  $k$ -th component  $u_{j,k}$  of  $\mathbf{u}_j$  as

$$u_{j,k} = F_{B2q}(b_{j,k}) \triangleq b_{j,k} \odot C_j = \begin{cases} \alpha^{l_{j,0}}, & b_{j,k} = 0 \\ \alpha^{l_{j,1}}, & b_{j,k} = 1 \end{cases}, \quad (4)$$

where  $b_{j,k} \odot C_j$  is defined as a *switching function*. If the input bit is  $b_{j,k} = 0$ , the transformed element is  $u_{j,k} = \alpha^{l_{j,0}}$ ; otherwise,  $u_{j,k}$  is equal to  $u_{j,k} = \alpha^{l_{j,1}}$ .

Let the input *bit-block* of  $J$  users at the  $k$ -th component denote by  $\mathbf{b}[k]$ , i.e.,  $\mathbf{b}[k] = (b_{1,k}, b_{2,k}, \dots, b_{J,k})$ , where  $0 \leq k < K$ . We also call the EP codeword  $(u_{1,k}, u_{2,k}, \dots, u_{J,k})$  in  $\Psi_{o,B}$  as the output *element-block* of the  $k$ -th component of  $J$  users, i.e.,  $\mathbf{u}[k] = (u_{1,k}, u_{2,k}, \dots, u_{J,k})$ .

We assign the UD-EP  $C_j$  in  $\Psi_{o,B}$  to the  $j$ -th user for  $1 \leq j \leq J = m$ . Then, the multiplexing of the  $k$ -th components of  $m$  users, i.e.,  $u_{1,k}, u_{2,k}, \dots, u_{m,k}$ , is calculated as

$$\begin{aligned} w_k &= u_{1,k} + u_{2,k} + \dots + u_{m,k} \\ &\stackrel{(a)}{=} b_{1,k}\alpha^0 + b_{2,k}\alpha^1 + \dots + b_{m,k}\alpha^{m-1} = \mathbf{b}[k] \cdot \mathbf{G}_M^1, \end{aligned} \quad (5)$$

where (a) is deduced based on the orthogonal UD-EP code  $\Psi_{o,B}$  given by (2) and Eq. (4). We call  $\mathbf{G}_M^1$  the *full-one generator matrix*, given as

$$\mathbf{G}_M^1 = \begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \vdots \\ \alpha^{m-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix},$$

which is an  $m \times m$  identity matrix. Thus, based on the orthogonal UD-EP code  $\Psi_{o,B}$ , the proposed system is a *type of time division multiple-access in finite-field (FF-TDMA)*, in which the outputs of the  $m$  users completely occupy  $m$  locations in an  $m$ -tuple.

### B. Orthogonal Encoding of an Error-Correcting Code

For  $0 \leq j < m$ , we form the following element-sequence  $\mathbf{u}_j = (u_{j,0}, u_{j,1}, \dots, u_{j,k}, \dots, u_{j,K-1})$ , which is then multiplied  $\alpha^j$ , given by

$$\mathbf{u}_j \cdot \alpha^j \triangleq (u_{j,0}\alpha^j, u_{j,1}\alpha^j, \dots, u_{j,k}\alpha^j, \dots, u_{j,K-1}\alpha^j). \quad (6)$$

Next, the  $m$  element-sequences, i.e.,  $\mathbf{u}_0 \cdot \alpha^0, \mathbf{u}_1 \cdot \alpha^1, \dots, \mathbf{u}_{m-1} \cdot \alpha^{m-1}$ , can form an FFSP sequence as follows:

$$\mathbf{w} = \mathbf{u}_0 \cdot \alpha^0 + \mathbf{u}_1 \cdot \alpha^1 + \dots + \mathbf{u}_j \cdot \alpha^j + \dots + \mathbf{u}_{m-1} \cdot \alpha^{m-1}, \quad (7)$$

where  $\mathbf{w} = (w_0, w_1, \dots, w_{K-1})$ , and  $w_k$  is an  $m$ -tuple. It indicates that a sequence  $\mathbf{w}$  over  $\text{GF}(2^m)$  can be decomposed into  $m$  element-sequences  $\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_{m-1}$ .

Let  $\mathbf{G}_{gc}$  be the generator matrix of a binary  $(N, Km)$  linear block code  $C_{gc}$ . Then, we encode  $\mathbf{w}$  into a codeword  $\mathbf{v}$  in  $C_{gc}$  using the generator  $\mathbf{G}_{gc}$ , i.e.,  $\mathbf{v} = \mathbf{w} \cdot \mathbf{G}_{gc} = (v_0, v_1, v_2, \dots, v_{N-1})$ . It is able to derive that

$$\begin{aligned} \mathbf{v} &= \mathbf{w} \cdot \mathbf{G}_{gc} = (\mathbf{u}_0 \cdot \mathbf{G}_{gc})\alpha^0 \oplus \dots \oplus (\mathbf{u}_{m-1} \cdot \mathbf{G}_{gc})\alpha^{m-1} \\ &= \mathbf{v}_0\alpha^0 \oplus \mathbf{v}_1\alpha^1 \oplus \dots \oplus \mathbf{v}_{m-1}\alpha^{m-1}. \end{aligned}$$

where  $\mathbf{v}_j = \mathbf{u}_j \mathbf{G}_{gc}$  is the codeword of  $\mathbf{u}_j$  for  $0 \leq j < m$ . The codeword  $\mathbf{v}$  in orthogonal form is referred to as *orthogonal encoding* of the message  $\mathbf{w}$ , indicating the codeword  $\mathbf{v}$  is the FFSP of the codewords  $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{m-1}$ .

## IV. AN FFMA SYSTEM IN A GMAC

This section presents an FFMA system over a GMAC, based on the orthogonal UD-EP code  $\Psi_{o,B}$ , i.e.,  $\Psi_{o,B} = \{C_1, C_2, \dots, C_j, \dots, C_J\}$ , where  $C_j = \alpha^{j-1} \cdot C_B$  for  $1 \leq j \leq J \leq m$ . The UD-EP  $C_j$  is assigned to the  $j$ -th user.

At the transmitter, there are three modules, which are the EP code encoder denoted by  $F_{B2q}$ , the channel code encoder  $\mathbf{G}_{gc}$ , and the finite-field to complex-field transform function denoted by  $F_{F2C}$  which can be realized by modulation. In fact, the combination of EP code and channel code can be regarded as a *cascade code*, which is used to implement *multuser channel code*. At the receiving end, it explores the reverse operations, which are demodulation denoted by  $F_{C2F}$ , channel code decoder, and EP code decoder denoted by  $F_{q2B}$ .

### A. Transmitter of a Sparse-form FFMA System

The transmitter of the  $j$ -th user for  $1 \leq j \leq J$  maps each bit-sequence  $b_j$  uniquely into an element-sequence  $\mathbf{u}_j = (u_{j,0}, u_{j,1}, \dots, u_{j,k}, \dots, u_{j,K-1})$  by  $F_{B2q}$ , i.e.,  $u_{j,k} = F_{B2q}(b_{j,k})$ , which is determined by the EP  $C_j = \alpha^{j-1} \cdot C_B$ . For  $0 \leq k < K$ , the  $k$ -th element  $u_{j,k}$  of  $\mathbf{u}_j$  is represented by its corresponding  $m$ -tuple representation over  $\text{GF}(2)$ , i.e.,  $u_{j,k} = (u_{j,k,0}, u_{j,k,1}, \dots, u_{j,k,i}, \dots, u_{j,k,m-1})$ , where  $0 \leq i < m$ . Then, the  $m$ -tuple form of  $u_{j,k}$  is

$$u_{j,k} = F_{B2q}(b_{j,k}) = (0, \dots, 0, b_{j,k}, 0, \dots, 0), \quad (14)$$

and the  $i$ -th component of  $u_{j,k}$  is

$$u_{j,k,i} = \begin{cases} b_{j,k}, & i = j - 1 \\ 0, & i \neq j - 1 \end{cases} \quad (15)$$

For a large  $m$ ,  $u_{j,k}$  is a sparse vector with only one element at the  $(j-1)$ -th location, and the other locations are all 0s. For the binary form of the element-sequence  $\mathbf{u}$ , its length is equal to  $Km$ .

Next, the element-sequence  $\mathbf{u}_j$  of the  $j$ -th user is encoded into a codeword  $\mathbf{v}_j$  of a binary  $(N, mK)$  linear block code  $C_{gc}$ . Suppose the  $mK \times N$  generator matrix of  $C_{gc}$  is in systematic form, defined by  $\mathbf{G}_{gc,sysm}$ . Then, the codeword  $\mathbf{v}_j$  is of the following form

$$\mathbf{v}_j = \mathbf{u}_j \cdot \mathbf{G}_{gc,sysm} = (\mathbf{u}_j, \mathbf{v}_{j,red}),$$

where  $\mathbf{v}_{j,red}$  is the parity (or called redundancy) block, and the subscript ‘‘red’’ stands for ‘‘redundancy’’. In the systematic form, the codewords of  $m$  users can be arranged in an  $m \times N$  codeword matrix  $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_j, \dots, \mathbf{v}_m]^T$ , where  $1 \leq j \leq m$  and  $J = m$ . The codeword matrix  $\mathbf{V}$  can be divided into two sections, information section  $\mathbf{U}$  and parity section  $\mathbf{E}$ , given as

$$\mathbf{V} = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_m \end{bmatrix} = \begin{bmatrix} u_{1,0} & u_{1,1} & \dots & u_{1,K-1} & \mathbf{v}_{1,red} \\ u_{2,0} & u_{2,1} & \dots & u_{2,K-1} & \mathbf{v}_{2,red} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u_{m,0} & u_{m,1} & \dots & u_{m,K-1} & \mathbf{v}_{m,red} \end{bmatrix}. \quad (16)$$

The information section  $\mathbf{U}$  is a  $1 \times K$  array, i.e.,  $\mathbf{U} = [\mathbf{U}_0, \mathbf{U}_1, \dots, \mathbf{U}_k, \dots, \mathbf{U}_{K-1}]$ , and  $\mathbf{U}_k$  for  $0 \leq k < K$  is an  $m \times m$  matrix. For the information section  $\mathbf{U}$ ,  $J$  information bits  $b_{1,k}, b_{2,k}, \dots, b_{J,k}$  from the  $J$  users are lying on the main diagonal of  $\mathbf{U}_k$ . The parity section  $\mathbf{E}$  is an  $m \times (N - mK)$  matrix which consists of all the parity-check bits formed based on the generator matrix, i.e.,  $\mathbf{E} = [\mathbf{v}_{1,red}, \mathbf{v}_{2,red}, \dots, \mathbf{v}_{m,red}]^T$ .

To support massive users with short packet transmission scenario,  $m$  may be very large, indicating  $\mathbf{V}$  is a sparse matrix. In this case, we call  $\mathbf{V}$  a *sparse codeword matrix*, and the corresponding FFMA system is referred to as *sparse-form FFMA (SF-FFMA)*.

Then, each codeword  $\mathbf{v}_j$  is modulated by BPSK signaling and mapped to a complex-field signal sequence  $\mathbf{x}_j \in \mathbb{C}^{1 \times N}$ , i.e.,  $\mathbf{x}_j = (x_{j,0}, x_{j,1}, \dots, x_{j,n}, \dots, x_{j,N-1})$ . For  $0 \leq n < N$ , the  $n$ -th component  $x_{j,n}$  is given by

$$x_{j,n} = F_{F2C}(v_{j,n}) = 2v_{j,n} - 1, \quad (17)$$

where  $x_{j,n} \in \{-1, +1\}$ . The mapping from  $\mathbf{v}_j$  to  $\mathbf{x}_j$  is regarded as *finite-field to complex-field transform (F2C)*, denoted by  $F_{F2C}$ . Then  $\mathbf{x}_j$  is sent to a GMAC.

### B. Receiver of a Sparse-form FFMA System

At the receiving end, the received signal sequence  $\mathbf{y} \in \mathbb{C}^{1 \times N}$  is the combined outputs of the  $J$  users plus noise, i.e.,

$$\mathbf{y} = \sum_{j=1}^J \mathbf{x}_j + \mathbf{z} = \mathbf{r} + \mathbf{z}, \quad (18)$$

where  $\mathbf{z} \in \mathbb{C}^{1 \times N}$  is an AWGN vector with  $\mathcal{N}(0, N_0/2)$ . The sum in  $\mathbf{y}$  is called *complex-field sum-pattern (CFSP)* signal sequence, i.e.,  $\mathbf{r} = (r_0, r_1, \dots, r_n, \dots, r_{N-1}) \in \mathbb{C}^{1 \times N}$ , which is the sum of the  $J$  modulated signal sequences  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_J$ , i.e.,  $r_n = \sum_{j=1}^J x_{j,n}$ .

To separate the superposition signals, the classical method is to utilize *multiuser interference cancellation* algorithms. In our paper, we present another solution based on the USPM structural property of the orthogonal UD-EP code  $\Psi_{o,B}$ . We only need to map each CFSP signal  $r_n$  to an FFSP symbol  $v_n$ , i.e.,  $r_n \mapsto v_n$ , and then the bit-sequences of  $J$ -user can be recovered by decoding the EP codeword.

Thus, the first step of the detection process is to transform the received CFSP signal sequence  $\mathbf{r} = (r_0, r_1, \dots, r_n, \dots, r_{N-1})$  into its corresponding FFSP codeword sequence  $\mathbf{v} = (v_0, v_1, \dots, v_n, \dots, v_{N-1})$  by a *complex-field to finite-field (C2F)* transform function  $F_{C2F}$ , i.e.,  $v_n = F_{C2F}(r_n)$  for  $0 \leq n < N$ . We find the following facts of the CFSP  $r_n$  and FFSP  $v_n$ .

- 1) The value of CFSP  $r_n$  is determined by the number of users who send “+1” and the number of users who send “-1”. Thus, the set of  $r_n$ ’s values in ascendant order is  $\Omega_r = \{-J, -J+2, \dots, J-2, J\}$ , in which the difference between two adjacent values is 2. The total number of  $\Omega_r$  is equal to  $|\Omega_r| = J + 1$ .
- 2) The value of  $v_n$  is uniquely determined by the number of  $(1)_2$  bits coming from the  $J$  users. If there are odd number of bits  $(1)_2$  from the  $J$  users, then  $v_n = (1)_2$ ; otherwise,  $v_n = (0)_2$ . The corresponding FFSP set  $\Omega_v$  of  $\Omega_r$  is  $\Omega_v = \{0, 1, 0, 1, \dots\}$ , in which  $(0)_2$  and  $(1)_2$  appear alternatively.
- 3) Let  $C_j^\iota$  denote the number of users which send “+1”. The values of  $\iota$  are from 0 to  $J$ . When  $\iota = 0$ , it indicates that all the  $J$  users send  $(0)_2$ . If  $\iota$  increases by one, the number of  $(1)_2$  bits coming from  $J$  users increases by one accordingly. Hence, the probabilities of the elements in  $\Omega_r$  are  $\mathcal{P}_r = \{C_j^0/2^J, C_j^1/2^J, \dots, C_j^{J-1}/2^J, C_j^J/2^J\}$ .

Based on the relationship between  $r_n$  and  $v_n$ , we can calculate the posterior probabilities  $\Pr(v_n = 0|y_n)$  and  $\Pr(v_n = 1|y_n)$  for decoding  $\mathbf{y}$  [15].

When the generator matrix  $\mathbf{G}_{gc, sym}$  in systematic form is utilized, the decoded FFSP codeword sequence  $\hat{\mathbf{v}}$  can be expressed as  $\hat{\mathbf{v}} = (\hat{\mathbf{w}}, \hat{\mathbf{v}}_{red})$ , where  $\hat{\mathbf{w}}$  and  $\hat{\mathbf{v}}_{red}$  are the detected FFSP sequence and parity block, respectively.

After removing the parity block  $\hat{\mathbf{v}}_{red}$  from  $\hat{\mathbf{v}}$ , the detected FFSP sequence  $\hat{\mathbf{w}}$  can be divided into  $K$  FFSP blocks, and each block consists of  $m$  bits formed an  $m$ -tuple, i.e.,  $\hat{\mathbf{w}} = (\hat{w}_0, \hat{w}_1, \dots, \hat{w}_k, \dots, \hat{w}_{K-1})$ , where  $\hat{w}_k = (\hat{w}_{k,0}, \hat{w}_{k,1}, \dots, \hat{w}_{k,i}, \dots, \hat{w}_{k,m-1})$ , with  $0 \leq k < K$  and  $0 \leq i < m$ . Finally, we separate the detected FFSP block  $\hat{w}_k$  into  $J$  bits as  $\hat{b}_{1,k}, \hat{b}_{2,k}, \dots, \hat{b}_{j,k}, \dots, \hat{b}_{J,k}$  by using an inverse transform function  $F_{q2B}$ . According to (5), we know that the  $j$ -th user is assigned the EP  $C_j = \alpha^{j-1} \cdot C_B$ . Thus, to recover the transmit bit information of the  $j$ -th user, the inverse transform function  $F_{q2B}$  is given as

$$\hat{b}_{j,k} = F_{q2B}(\hat{w}_k) = \hat{w}_{k,j-1}, \quad (19)$$

where  $\hat{w}_{k,j-1}$  is the  $(j-1)$ -th component of  $\hat{w}_k$ .

After recovering the transmit bit information, we can directly obtain the active users’ information from the field-field. For instance, if  $\hat{b}_{j,k} = 0$  for  $0 \leq k < K$ , it can be inferred that the  $j$ -th user is not active. This phenomenon is appealing for the sourced RA, since it avoids the necessity of addressing the active user detection issue.

### C. A Diagonal-form FFMA System

Recall the *sparse form codeword matrix*  $\mathbf{V}$  given by (16), for the  $1 \times K$  information section  $\mathbf{U}$  of  $\mathbf{V}$ , each entry  $\mathbf{U}_k$  of  $\mathbf{U}$  is an  $m \times m$  matrix, and the  $m$  information bits  $b_{1,k}, b_{2,k}, \dots, b_{j,k}, \dots, b_{m,k}$  are located on the main diagonal of  $\mathbf{U}_k$ , and the other locations are all 0s, where  $0 \leq k < K$  and  $1 \leq j \leq J \leq m$ .

Permuting the columns of the  $1 \times K$  information array  $\mathbf{U}$  of  $\mathbf{V}$  and rearranging the bit sequences, we can obtain an  $m \times m$  information array  $\mathbf{U}_D$ , in which  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_j, \dots, \mathbf{b}_m$  are lying on the main diagonal of  $\mathbf{U}_D$  and the other entries are all 0s, given by

$$\mathbf{U}_D = \begin{bmatrix} \mathbf{u}_{1,D} \\ \mathbf{u}_{2,D} \\ \vdots \\ \mathbf{u}_{m,D} \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & & & \\ & \mathbf{b}_2 & & \\ & & \ddots & \\ & & & \mathbf{b}_m \end{bmatrix}, \quad (20)$$

where  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_j, \dots, \mathbf{b}_m$  are  $1 \times K$  vectors, and the subscript “D” stands for “diagonal”. Let  $\mathbf{u}_{j,D}$  denote as a  $1 \times mK$  information sequence of the  $j$ -th user, i.e.,  $\mathbf{u}_{j,D} = (\mathbf{0}, \dots, \mathbf{0}, \mathbf{b}_j, \mathbf{0}, \dots, \mathbf{0})$ , in which the  $1 \times K$  bit-sequence of the  $j$ -th user  $\mathbf{b}_j$  is located at the  $(j-1)$ -th entry of  $\mathbf{u}_{j,D}$  and  $\mathbf{0}$  is a  $1 \times K$  zero vector. Note that, if  $J < m$ , the  $(m-J)$  rightmost entries of  $\mathbf{U}_D$  are all zeros, forming an  $(m-J) \times (m-J)K$  zero matrix.

Then, we encode  $\mathbf{u}_{j,D}$  by the generator matrix  $\mathbf{G}_{gc, sym}$  in systemic form, and obtain the codeword  $\mathbf{v}_{j,D}$  of  $\mathbf{u}_{j,D}$ , i.e.,  $\mathbf{v}_{j,D} = (\mathbf{u}_{j,D}, \mathbf{v}_{j,D,red})$ , where  $\mathbf{v}_{j,D,red}$  is the parity block of  $\mathbf{v}_{j,D}$ , which is a  $(N - mK)$ -tuple. The codewords of  $\mathbf{v}_{1,D}, \mathbf{v}_{2,D}, \dots, \mathbf{v}_{J,D}$  together can form a *diagonal form codeword matrix*  $\mathbf{V}_D$ , given as follows:

$$\mathbf{V}_D = \begin{bmatrix} \mathbf{v}_{1,D} \\ \mathbf{v}_{2,D} \\ \vdots \\ \mathbf{v}_{m,D} \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & & & \mathbf{v}_{1,D,red} \\ & \mathbf{b}_2 & & \mathbf{v}_{2,D,red} \\ & & \ddots & \vdots \\ & & & \mathbf{b}_m & \mathbf{v}_{m,D,red} \end{bmatrix}, \quad (21)$$

consisting of an  $m \times m$  diagonal array  $\mathbf{U}_D = \text{diag}(\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m)$  and an  $m \times 1$  parity block  $\mathbf{E}_D$ , where  $\mathbf{E}_D = [\mathbf{v}_{1,D,red}, \mathbf{v}_{2,D,red}, \dots, \mathbf{v}_{m,D,red}]^T$ .

From the codeword  $\mathbf{v}_{j,D}$ , it is found that the useful vectors (i.e.,  $\mathbf{b}_j$  and  $\mathbf{v}_{j,D,red}$ ) are only located at the  $(j-1)$ -th entry of  $\mathbf{u}_{j,D}$  and the parity-check entry  $\mathbf{v}_{j,D,red}$ , and the other entries are all zeros. Thus, for the diagonal-form codeword  $\mathbf{v}_{j,D}$ , we can directly modulate and transmit the shorten codeword, defined by  $\mathbf{v}_{j,D,S} = (\mathbf{b}_j, \mathbf{v}_{j,D,red})$ , instead of  $\mathbf{v}_{j,D}$ , to reduce the transmit power. The subscript “S” indicates “shorten”. The codeword length of  $\mathbf{v}_{j,D,S}$  is equal to  $N - (m-1)K$ .

The FFMA system based on the shorten codeword  $\mathbf{v}_{j,D,S}$  is referred to as *diagonal-form FFMA (DF-FFMA)* system. For a short packet transmission, e.g.,  $K$  is an extremely small number, the length of  $\mathbf{v}_{j,D,S}$  is approximately equal to the length of parity block  $\mathbf{v}_{j,D,red}$ .

The permuting and rearranging operations do not affect the properties of FFMA system. Hence, the DF-FFMA system can be decoded like the aforementioned SF-FFMA system. For a DF-FFMA system, the bit-sequences of  $J$  users are transmitted in orthogonal mode and the  $J$  parity blocks are appended to them. Obviously, the DF-FFMA system is appealing for the

massive users with short data packet transmission scenario, which can obtain a large coding gain from all the massive users with a low-complexity decoder.

#### D. A Polarization-adjusted FFMA System

Now, we present a specific configuration of the DF-FFMA, referred to as *polarization-adjusted (or power allocation) DF-FFMA (PA-DF-FFMA)* or simply *PA-FFMA*.

Let  $P_{avg}$  denote the average transmit power per symbol. For an  $(N, mK)$  channel code  $C_{gc}$ , the total transmit power per user is  $NP_{avg}$ . In the SF-FFMA system, the entire transmit power of  $NP_{avg}$  is utilized. In contrast, the DF-FFMA system only utilizes a portion of this power, specifically  $(N - mK + K) \cdot P_{avg}$ , leaving  $(m - 1)K \cdot P_{avg}$  unused. The proposed PA-FFMA reallocates this unused power. By optimizing power allocation, the channel capacity is adjusted according to the assigned power, resulting in a form of *polarization* [11]–[13].

The shortened codeword  $\mathbf{v}_{j,D,S} = (\mathbf{b}_j, \mathbf{v}_{j,D,red})$  of the  $j$ -th user is consisted of an information block  $\mathbf{b}_j$  and a parity block  $\mathbf{v}_{j,D,red}$ . Assume that the power assigned to the information block per symbol is  $\mu_1 P_{avg}$ , while the power allocated to the parity block per symbol is  $\mu_2 P_{avg}$ . Then, the power allocation (or called polarization-adjusted) conditions are given as

$$\begin{aligned} C1 : NP_{avg} &= K \cdot (\mu_1 P_{avg}) + (N - mK) \cdot (\mu_2 P_{avg}), \\ C2 : 1 &\leq \left( \mu_{pas} = \frac{\mu_1}{\mu_2} \right) \leq m, \end{aligned} \quad (22)$$

where  $\mu_{pas} = \frac{\mu_1}{\mu_2}$  is defined as *polarization-adjusted scaling factor (PAS)*. Condition  $C1$  ensures that the total transmit power remains constant. Condition  $C2$  specifies that the information block receives more power than the parity block. Ideally, we aim to maximize the reliability of the information block by assigning as much power as possible to it. Additionally, considering the unused power is  $(m-1)K \cdot P_{avg}$ , the maximum power that can be assigned to the information block per symbol is  $m \cdot P_{avg}$ , which is equivalent to repeating the information block per symbol  $m$  times. With the increased power allocated to the information block, its reliability improves, leading to a higher degree of polarization. Nevertheless, the decoding (or detection) algorithm of PA-FFMA plays a critical role in influencing error performance. For a more detailed discussion, please refer to [15].

#### V. SIMULATION RESULTS

Now, we show the error performances over a GMAC. Suppose the frame size (or DoF) is  $N = 6000$ , each user transmits  $K = 10$  bits, and the numbers of total users are  $J = 1, 100$  and  $300$ , respectively. We set  $\mu_{pas} = 300$  for the PA-FFMA system.

For the SF-FFMA system, each user occupies the entire frame. In the the DF-FFMA systems, the frame structure consists of  $J$  information blocks and one parity block. For the slotted ALOHA scheme, we assume that the number of time slots is equal to the number of total users, and repetition code is used for error control. Hence, the blocklength of each time slot is  $\frac{N}{J}$ , and each bit is repeated  $\frac{N}{JK}$  times.

From Fig. 1, we observe that the BER decreases as the number of users increases. For the SF-FFMA systems, the BERs for cases where  $J = 100$  and  $J = 300$  are nearly

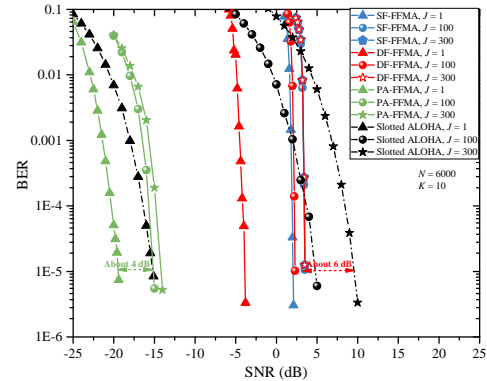


Fig. 1. BER performances of different systems over a GMAC. The proposed FFMA systems are used a binary (6000,3000) LDPC code  $C_{gc}$  for error control, and the slotted ALOHA utilizes repetition code for error control, where  $N = 6000$ ,  $K = 10$  bits,  $\mu_{pas} = 300$ , and  $J = 1, 100, 300$ .

identical. When the BER is  $P_b = 10^{-5}$ , the difference between the BERs of  $J = 1$  and  $J = 300$  is only 1.5 dB. We then compare the BER performance between the SF-FFMA and DF-FFMA systems. Under the same simulation conditions, the DF-FFMA system achieves a lower BER than the SF-FFMA, as the default bits, which are 0s, are available at the receiving end. However, as the number of users increases, the difference in BER between the SF-FFMA and DF-FFMA systems diminishes. For  $J = 300$ , both systems exhibit the same BER. Additionally, it is found that the PA-FFMA system provides significantly better BER performance than both the SF-FFMA and DF-FFMA systems. This improvement is attributed to a polarization gain of approximately  $10 \log_{10}(\mu_{pas}) \approx 24.77$  dB.

Next, we compare our proposed SF-FFMA and DF-FFMA systems with the slotted ALOHA system. When  $J = 1$ , slotted ALOHA with repetition coding outperforms both the SF-FFMA and DF-FFMA systems in terms of BER due to a coding gain of approximately  $10 \log_{10}(\frac{N}{JK}) \approx 27.78$  dB. Besides, the proposed PA-FFMA system offers an additional coding gain of approximately 4 dB over the slotted ALOHA system, as it combines both polarization gain from power and coding gain from the entire DoF.

For a large number of users, i.e.,  $J \geq 100$ , all three configurations of the proposed FFMA systems can offer much better BER performance than the slotted ALOHA system. Specifically, at  $P_b = 10^{-5}$  and  $J = 300$ , the SF-FFMA (or DF-FFMA) systems provide a coding gain of approximately 6 dB over the slotted ALOHA system, further validating the ability of the proposed FFMA systems to enhance BER performance in scenarios with massive user counts.

#### VI. CONCLUSIONS

In this paper, we propose a novel FFMA technique designed to support a massive number of users with short packet traffic, addressing the challenges of FBL in multiuser reliable transmission. Unlike traditional complex-field MA systems, we utilize EPs as virtual resources to distinguish between users. We introduce a type of orthogonal UD-EP code, denoted as  $\Psi_{o,B}$ , constructed over  $GF(2^m)$ , which can form TD-FFMA mode. Simulation results demonstrate that the proposed FFMA systems can support a large number of GMACs while maintaining favorable error performance in a GMAC.

## REFERENCES

- [1] C. -X. Wang et al., "On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905-974, Secondquarter 2023.
- [2] P. Fan et al., "Random access for massive Internet of things: current status, challenges and opportunities," *Journal on Communications*, vol. 42, no. 4, pp. 1-21, April 2021.
- [3] Y. Li et al., "Unsources multiple access for 6G massive machine type communications," *China Communications*, vol. 19, no. 3, pp. 70-87, March 2022.
- [4] Y. Polyanskiy, "A perspective on massive random-access," *IEEE International Symposium on Information Theory-Proceedings*, 2017, pp. 2523-2527.
- [5] M. Ke, Z. Gao, M. Zhou, D. Zheng, D. W. K. Ng and H. V. Poor, "Next-Generation URLLC With Massive Devices: A Unified Semi-Blind Detection Framework for Sourced and Unsourced Random Access," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 7, pp. 2223-2244, July 2023.
- [6] Qi-yue Yu, and Ke-xun Song, "Uniquely Decodable Multi-Amplitude Sequence for Grant-Free Multiple-Access Adder Channels," *IEEE Transactions on Wireless communications*, vol. 22, no. 12, pp. 8999-9012, Dec. 2023.
- [7] X. Shao, X. Chen, D. W. K. Ng, C. Zhong and Z. Zhang, "Cooperative Activity Detection: Sourced and Unsourced Massive Random Access Paradigms," *IEEE Transactions on Signal Processing*, vol. 68, pp. 6578-6593, 2020.
- [8] F. Schoute, "Dynamic Frame Length ALOHA," *IEEE Transactions on Communications*, vol. 31, no. 4, pp. 565-568, April 1983.
- [9] X. Chen, T.-Y. Chen and D. Guo, "Capacity of Gaussian many-access channels," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3516-3539, Jun. 2017.
- [10] R. C. Yavas, V. Kostina and M. Effros, "Gaussian Multiple and Random Access Channels: Finite-Block length Analysis," *IEEE Transactions on Information Theory*, vol. 67, no. 11, pp. 6983-7009, Nov. 2021.
- [11] E. Arıkan, "On the Origin of Polar Coding," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 2, pp. 209-223, Feb. 2016.
- [12] E. Arıkan, "From sequential decoding to channel polarization and back again," <https://arxiv.org/abs/1908.09594>.
- [13] M. Rowshan, A. Burg and E. Viterbo, "Polarization-Adjusted Convolutional (PAC) Codes: Sequential Decoding vs List Decoding," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1434-1447, Feb. 2021.
- [14] J. Li, S. Lin, K. Abdel-Ghaffar, W. E. Ryan, and D. J. Costello, "LDPC Code Designs, Constructions, and Unification," Cambridge University Press, 2017.
- [15] Qi-yue Yu, Jiang-xuan Li, and Shu Lin, "Finite Field Multiple Access," <https://arxiv.org/abs/2303.14086v2>.