THREE CLASSES OF PARTITIONED DIFFERENCE FAMILIES
AND THEIR OPTIMAL CONSTANT COMPOSITION CODES

SHANDING XU
College of Liberal Arts and Science
National University of Defense Technology
Changsha 410073, China

LONGJIANG QU
College of Liberal Arts and Science
National University of Defense Technology
Changsha 410073, China

XIWANG CAO
Department of Mathematics
Nanjing University of Aeronautics and Astronautics
Nanjing 210016, China

(Communicated by Sihem Mesnager)

Abstract. Cyclotomy, firstly introduced by Gauss, is an important topic in Mathematics since it has a number of applications in number theory, combinatorics, coding theory and cryptography. Depending on $v$ prime or composite, cyclotomy on a residue class ring $\mathbb{Z}_v$ can be divided into classical cyclotomy or generalized cyclotomy. Inspired by a foregoing work of Zeng et al. [40], we introduce a generalized cyclotomy of order $e$ on the ring $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$, where $q_i$ and $q_j$ ($i \neq j$) may not be co-prime, which includes classical cyclotomy as a special case. Here, $q_1, q_2, \cdots, q_k$ are powers of primes with an integer $e|\text{lcm}(q_i - 1)$ for any $1 \leq i \leq k$. Then we obtain some basic properties of the corresponding generalized cyclotomic numbers. Furthermore, we propose three classes of partitioned difference families by means of the generalized cyclotomy above and $d$-form functions with difference balanced property. Afterwards, three families of optimal constant composition codes from these partitioned difference families are obtained, and their parameters are also summarized.

1. Introduction

For a positive integer $v$, let $\mathbb{Z}_v$ be the residue class ring module $v$ and $\mathbb{Z}_v^*$ be the set of all invertible elements of $\mathbb{Z}_v$. A partition $\{D_0, D_1, \cdots, D_{d-1}\}$ of $\mathbb{Z}_v^*$ is a collection of some subsets with

$$D_i \cap D_j = \emptyset \text{ for any } i \neq j, \text{ and } \bigcup_{i=0}^{d-1} D_i = \mathbb{Z}_v^*.$$
If \( D_0 \) is a multiplicative subgroup of \( \mathbb{Z}_v \), and there exist elements \( a_1, \ldots, a_{d-1} \) in \( \mathbb{Z}_v^* \) such that \( D_i = a_i D_0 \) for any \( 1 \leq i < d \), then these cosets \( D_i \) are called \textit{generalized cyclotomic classes} of order \( d \) when \( v \) is composite, and \textit{classical cyclotomic classes} of order \( d \) when \( v \) is prime. The \textit{(generalized) cyclotomic numbers} of order \( d \) are defined by \((i,j) = |(D_i + 1) \cap D_j|\) with \( 0 \leq i, j < d \).

The theory of cyclotomy can date back to Gauss and has some important applications in number theory. In the beginning, cyclotomy means “circle-division” and refers to the problem of dividing the circumference of the unit circle into a given number, \( v \), of arcs of equal lengths. We refer the reader to the classical book by Storer [32] for an exposition. Note that different subgroups \( D \) of the ring \( \mathbb{Z}_v \) could give different generalized cyclotomics and cyclotomic numbers. Nowadays, to the knowledge of ours, there are mainly five classes of cyclotomy: Classical cyclotomy [19], Whiteman generalized cyclotomy [35], Ding-Helleseth generalized cyclotomy [15], Zeng-Cai-Tang-Yang generalized cyclotomy [40] and Fan-Ge generalized cyclotomy [17]. Specifically speaking, classical cyclotomy was firstly dealt to a good extent by Gauss in his book “Disquisitiones Arithmeticae” [19], where he introduced the so-called Gaussian periods and cyclotomic numbers. Later, it was extended to finite fields as well and the properties of cyclotomic numbers were extensively investigated in [32]. For searching for residue difference sets, a generalized cyclotomy of order \( d \) with respect to \( pq \) was introduced by Whiteman [35] and was applied to design of sequences with good autocorrelation, where \( p \) and \( q \) are distinct odd primes with \( \gcd(p - 1, q - 1) = d \). Obviously, this generalized cyclotomy is not consistent with classical cyclotomy. Later, Ding and Helleseth proposed a new generalized cyclotomy of order 2 with respect to \( v = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \) [15] and gave error-correcting codes derived from this generalized cyclotomy [16], where odd primes \( p_i \) and \( p_j \) satisfy \( \gcd(p_i - 1, p_j - 1) = 2 \) for any \( 1 \leq i \neq j \leq k \). It includes classical cyclotomy of order 2 and Whiteman generalized cyclotomy of order 2 as special cases. In 2013, Zeng et al. [40] introduced the generalized cyclotomy of order \( \phi(v)/e \) with respect to \( v = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \) and presented a construction of optimal frequency-hopping sequences sets and two constructions of optimal frequency-hopping sequences, where \( \phi(x) \) denotes the Euler function and \( e > 1 \) is a common factor of \( p_1 - 1, p_2 - 1, \ldots, p_k - 1 \). In 2015, Zha and Hu [41] introduced cyclotomic cosets of the set \( \mathbb{Z}_v \), which may help the reader to have a better understanding of generalized cyclotomy proposed by Zeng et al. [40]. Moreover, Fan and Ge [17] introduced the generalized cyclotomy order \( e \) with respect to \( v \), where they constructed an infinite series of near-optimal codebooks over \( \mathbb{Z}_{pq} \) and asymptotically optimal difference systems of sets over \( \mathbb{Z}_v \). Especially, Fan-Ge generalized cyclotomy includes Whiteman and Ding-Helleseth generalized cyclotomics as special cases. More recently, the cyclotomy has proved to be valuable in other applied fields such as sequences [40, 15, 8, 22, 9], coding theory [15, 17, 16, 10, 25] and cryptography [15]. The combinatorics has also benefited from the use of cyclotomy, which can be applied for constructing difference sets, difference families, and so on [32, 35, 17, 41, 36, 7, 39, 34, 37, 6, 29].

Let \( A \) be an additive group of order \( n \) and \( \mathcal{P} = \{ B_i : 0 \leq i < m \} \) be a collection of nonempty subsets (blocks) of \( A \). \( \mathcal{P} \) is called a \textit{difference family} (DF) in \( A \), if every nonzero element of \( A \) occurs exactly \( \lambda \) times in the multiset

\[
\Delta \mathcal{P} = \bigcup_{i=0}^{m-1} \Delta B_i,
\]
where the multiset $\Delta(B_i) = \{ b - b' : b, b' \in B_i, \ b \neq b' \}$. Let $K$ be the multiset
$\{ |B_i| : 0 \leq i < m \}$. In brief, one says that $P$ is an $(A, K, \lambda)$ DF. In particular,
if $A$ is a cyclic group of order $n$, we also denote $P$ as an $(n, K, \lambda)$ DF. A difference
family is called disjoint (DDF) if its blocks are pairwise disjoint. Let $P$ be an
$(A, K, \lambda)$ DF, if $P$ forms a partition of $A$, then it is called a partitioned difference
family (PDF) and denoted as an $(A, K, \lambda)$ PDF. In the sequel, we sometimes use
a more informative notation to describe the multiset $K$: an $(A, [k_1^{u_1} k_2^{u_2} \ldots k_s^{u_s}], \lambda)$
DF is a difference family in which there are $u_i$ blocks of size $k_i$ for $1 \leq i \leq s$.

In 2005, PDFs were explicitly introduced by Ding and Yin in [14] to construct
optimal constant composition codes. As a matter of fact, PDFs were implicitly
studied in the literature concerning DFs, such as [36]. There are various methods
of constructing PDFs, which have been presented in [36, 7, 39, 14, 18, 20, 5,
27, 2, 3, 4]. Recently, PDFs have been investigated intensively under the notion of
zero-difference balanced function [41, 37, 6, 29, 11, 12, 42, 33, 38, 13]. Let $f$ be a
function from an additive group $A$ onto a set $B$, where $|A| = n$ and $|B| = m$. $f$
is called an $(n, m, \lambda)$ zero-difference balanced (ZDB) function if for any nonzero
$a \in A$, we have $|\{ x \in A : f(a+x) = f(x) \}| = \lambda$ for some constant $\lambda$. In recent years, it was
proved that ZDB functions have played an important role in the constructions of
optimal constant composition codes [41, 37, 6, 29, 14, 11, 42, 38], optimal constant
weight codes [42, 33, 38], optimal frequency-hopping sequences [6, 18, 20, 33, 38],
optimal and perfect difference systems of sets [41, 6, 29, 12, 42, 38]. Due to the
widespread applications of ZDB functions, many researchers have been occupied
in constructing ZDB functions. For a recent survey of ZDB functions and their
applications, please refer to [13].

It is meaningful to point out that ZDB functions and PDFs are two equivalent
objects as follows.

**Lemma 1.1.** [42] Let $A$ be an additive group with $|A| = n$ and $B$ be a set with
$|B| = m$, where $B = \{ b_0, b_1, \ldots, b_{m-1} \}$. Let $f$ be a function from $A$ onto $B$. For
each $i$ with $0 \leq i < m$, denote $B_i = \{ x \in A : f(x) = b_i \}$ and $P = \{ B_i : 0 \leq i < m \}$. Then $f$
is an $(n, m, \lambda)$ ZDB function if and only if $P$ is an $(A, K, \lambda)$ PDF, where
the multiset $K = \{ |B_i| : 0 \leq i < m \}$. In 2019, Buratti and Jungnickel [4] made a comparison between the equivalent
notions of a PDF and a ZDB function, raising four reasons for which they prefer
to use the terminology and notation of PDFs. It was pointed out that some papers
published in the last decade on ZDB functions may be repetitive and of little value
since they rediscovered simple results on DFs which were known since the 90s or
even earlier. This problem deserves our full attention. Hence, in the present paper,
we use the terminology of PDFs.

The main contribution of the present paper consists of the following three parts:

(1) This paper builds a general bridge between the generalized cyclotomy over
the ring $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$ and the generalized cyclotomy over the product ring
$R = \text{GF}(q_1) \times \text{GF}(q_2) \times \cdots \times \text{GF}(q_k)$ of finite fields, see Section 2.1. More specifically,
we present the generalized cyclotomy of order $\prod_{i=1}^{k} (q_i - 1)/e$ on the ring $R$, which is
a generalization of the classical cyclotomy. Here, $q_1, q_2, \ldots, q_k$ are powers of primes
with an integer $e|q_i - 1$ for any $1 \leq i \leq k$, where $q_i$ and $q_j$ ($i \neq j$) may not
be co-prime. Whereafter, some basic properties of the corresponding generalized
cyclotomic numbers are derived. Compared to the Zeng-Cai-Tang-Yang generalized
cyclotomy, we have essentially replaced the requirement \( e \mid (p_i - 1) \) by \( e \mid (p_i^{m_i} - 1) \), where \( p_i, 1 \leq i \leq k \), are primes. In 2011, Chung and Yang \cite{9} introduced the \( k \)-fold cyclotomy of order \( (v - 1)/e \) over the ring \( R \), where \( v = q_1 q_2 \cdots q_k \) and the set of its cyclotomic classes is a partition of \( R \setminus \{0\} \). In comparison, our method is quite neat and more clear to understand. And above all, by virtue of the generalized cyclotomy in this paper, we can construct more PDFs and optimal constant composition codes. It seems that these constructions can not be obtained by the other cyclotomies or generalized cyclotomies, such as the classical cyclotomy, the Zeng-Cai-Tang-Yang generalized cyclotomy and so on.

(2) In this paper, we present three constructions of PDFs based on the generalized cyclotomy above and \( d \)-form functions with difference balanced property, see Theorems 3.4, 3.6 and 3.9. Firstly, compared with Construction 1 in \cite{6} and Construction 1 in \cite{29} respectively, Construction 1 and Construction 2 in this paper provide new parameters since the requirement \( e \mid (p_i^{m_i} - 1) \) gives more flexibility. Furthermore, compared with the recursive constructions of PDFs in \cite{27, Theorem 18} and \cite[Chapter 3]{4}, our constructions are direct. Secondly, Construction 3 in this paper not only includes \cite[Theorem 13]{37} as a special case, but also gives flexible parameters due to the free choice of \( k \) and \( e \). In particular, Construction 3 works for every \( d \)-form function with difference-balanced property and the parameters of Theorem 3.9 are new when \( k \neq 1 \) or \( e \neq q - 1 \).

(3) According to \cite[Construction 6]{14}, every PDF leads to an optimal constant composition code. Employing our newly constructed PDFs, three classes of optimal constant composition codes with new parameters are obtained.

The outline of the paper is organized as follows. In Section 2, we introduce the generalized cyclotomy on product ring of finite fields and difference balanced functions. In Section 3, we construct three classes of PDFs by means of the generalized cyclotomy and \( d \)-form functions with difference balanced property of Section 2. In Section 4, we give an application of such PDFs. Finally, Section 5 concludes this paper.

2. Preliminaries

In this section we introduce some properties of the generalized cyclotomy on product ring of finite fields and difference balanced functions. These will be used to construct more PDFs in Section 3.

2.1. The generalized cyclotomy on product ring of finite fields and its properties. Let an integer \( v = q_1 q_2 \cdots q_k \), where \( q_1, q_2, \ldots, q_k \) are powers of primes. For each \( i \), let \( GF(q_i) \) be a finite field of order \( q_i \) and \( g_i \) be a generator of the multiplicative group \( GF(q_i)^* = GF(q_i) \setminus \{0\} \). Consider the commutative ring \( R = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \) with the identity \( \overline{I}_R = \{1_R, 1_{R_2}, \cdots, 1_{R_k}\} \), where \( R_i = GF(q_i) \) and \( 1_{R_i} \) is the identity of \( R_i \), \( 1 \leq i \leq k \). For any element \( \overline{x} = (x_1, x_2, \cdots, x_k) \) and \( \overline{y} = (y_1, y_2, \cdots, y_k) \) in \( R \), we define an addition and a multiplication in \( R \) as follows:

\[
\overline{x} + \overline{y} = (x_1 + y_1, x_2 + y_2, \cdots, x_k + y_k)
\]
\[
\overline{x} \cdot \overline{y} = (x_1 y_1, x_2 y_2, \cdots, x_k y_k)
\]

where \( x_i + y_i \) and \( x_i y_i \) are operated in \( GF(q_i) \). Further, we have

\[
R^* = R_1^* \times R_2^* \times \cdots \times R_k^*.
\]
where \( R^* \) denotes the set of all invertible elements in \((R, \cdot)\). Obviously,

\[
|R^*| = \prod_{i=1}^{k} |R_i^*| = \prod_{i=1}^{k} (q_i - 1).
\]

For a subset \( H \) of \( R \) and an element \( \vec{x} \) in \( R \), define \( \vec{x} + H \) and \( \vec{x} \cdot H \) as

\[
\vec{x} + H = \{ \vec{x} + \vec{h} : \vec{h} \in H \}, \quad \vec{x} \cdot H = \{ \vec{x} \cdot \vec{h} : \vec{h} \in H \}.
\]

Let \( e > 1 \) be a common factor of \( q_1 - 1, q_2 - 1, \ldots, q_k - 1 \), i.e.

\[
g_i - 1 = ef_i
\]

for \( k \) positive integers \( f_i \) with \( 1 \leq i \leq k \). Let \( \vec{g}(K,e) \in R \) be defined by \( \vec{g}(K,e) = (g_1^{i_1}, g_2^{i_2}, \ldots, g_k^{i_k}) \) with \( K = \{1,2,\cdots,k\} \). Since the order of \( g_i \) is \( q_i - 1 \) for any \( i \), the order of \( \vec{g}(K,e) \) in \( R \) is \( e \) and thus the set

\[
D^{(K,e)} = \{(\vec{g}(K,e))^s : 0 \leq s < e\}
\]

is a cyclic subgroup of order \( e \) of \( R^* \).

In the sequel, we will employ the subgroup \( D^{(K,e)} \) and its cosets to give a partition of \( R^* \). Let

\[
\Omega^{(e)}_K = \mathbb{Z}_{f_1} \times \mathbb{Z}_{q_2-1} \times \cdots \times \mathbb{Z}_{q_k-1}
\]

and define \( D^{(K,e)}_I \) as

\[
D^{(K,e)}_I = \langle g_1^{i_1}, g_2^{i_2}, \ldots, g_k^{i_k} \rangle \cdot D^{(K,e)}
\]

for any \( I_K = (i_1, i_2, \ldots, i_k) \in \Omega^{(e)}_K \). In particular, if \( I_K = (0,0,\cdots,0) \in \Omega^{(e)}_K \), then \( D^{(K,e)}_I = D^{(K,e)} \). Furthermore, for any two \( k \)-dimensional vectors \( I_K = (i_1, i_2, \ldots, i_k) \) and \( J_K = (j_1, j_2, \ldots, j_k) \) in \( \Omega^{(e)}_K \), the addition is defined as the following

\[
I_K + J_K = (i_1 + j_1, i_2 + j_2, \ldots, i_k + j_k)
\]

where the operation \( i_1 + j_1 \) is performed in the ring \( \mathbb{Z}_{f_1} \), and the operations \( i_r + j_r \) \((2 \leq r \leq k)\) are performed in the ring \( \mathbb{Z}_{q_r-1} \), respectively. By a similar analysis as in [40], it can be proved that \( \{ D^{(K,e)}_I : I_K \in \Omega^{(e)}_K \} \) is a partition of \( R^* \). In accordance with the notation of [15], we call \( D^{(K,e)}_I, I_K \in \Omega^{(e)}_K \), generalized cyclotomic classes of order \( \prod_{i=1}^{k} (q_i - 1)/e \) with respect to the ring \( R \). For fixed \( I_K \) and \( J_K \) with \( I_K, J_K \in \Omega^{(e)}_K \), the corresponding generalized cyclotomic numbers of order \( \prod_{i=1}^{k} (q_i - 1)/e \) are defined by

\[
(I_K, J_K) = |(D^{(K,e)}_I + J_K) \cap D^{(K,e)}_J|.
\]

**Remark 1.** In 2013, Zeng et al. introduced the Zeng-Cai-Tang-Yang cyclotomy [40] for constructing frequency-hopping sequences with optimal Hamming correlation. On one hand, the group \( \mathbb{Z}_p \) in [40] is cyclic and the group \((R, +)\) in our paper is not cyclic in general; on the other hand, compared with [40], the parameter \( e \) is more flexible, since we replace \( e!(p_i - 1) \) with \( e!(p_i^{m_i} - 1) \), where \( p_i, 1 \leq i \leq k, \) are primes.
In the next section, we will employ this generalized cyclotomy to construct more PDFs. To this end, we study some necessary properties of the generalized cyclotomic classes and generalized cyclotomic numbers above. From now on, we always assume that \( v \) is an odd integer unless particularly stated. The following lemma can be easily verified, we omit its proof.

**Lemma 2.1.** If \( \vec{x} \in D_{I_K}^{(K,e)} \) for some \( I_K \in \Omega_K^{(e)} \), then \( \vec{x} \cdot D_{J_K}^{(K,e)} = D_{I_K+J_K}^{(K,e)} \) for any \( J_K \in \Omega_K^{(e)} \).

**Lemma 2.2.** \( -\vec{1}_R \in D^{(K,e)} \) if \( e \) is even and \( -\vec{1}_R \in D_{E_K}^{(K,e)} \) if \( e \) is odd, where
\[
E_K = \left( \frac{f_1}{2}, \frac{f_2}{2}, \cdots, \frac{f_k}{2} \right).
\]

**Proof.** See Appendix A.

Similar to Proposition 1 in [40], the following proposition can be proved by virtue of the definitions of generalized cyclotomic classes and generalized cyclotomic numbers.

**Proposition 2.3.** For \( I_K = (i_1, i_2, \cdots, i_k) \in \Omega_K^{(e)} \) and \( J_K = (j_1, j_2, \cdots, j_k) \in \Omega_K^{(e)} \), the generalized cyclotomic numbers defined in equality (2) have the following properties:

1. \((I_K, J_K) = (-I_K, J_K - I_K)\).
2. \[
(I_K, J_K) = \begin{cases} (J_K, I_K), & \text{if } e \text{ is even} \\
(J_K + E_K, I_K + E_K), & \text{if } e \text{ is odd} \end{cases}
\]
where \( E_K \) is defined as Lemma 2.2.

(3) Let
\[
N_{I_K} = \left\{ \frac{i_r}{f_r} \pmod{e} : i_r \equiv 0 \pmod{f_r}, 1 \leq r \leq k \right\}
\]
and
\[
N_{I_K}' = \left\{ \frac{i_r}{f_r} - \frac{1}{2} \pmod{e} : i_r \equiv \frac{f_r}{2} \pmod{f_r}, 1 \leq r \leq k \right\}.
\]
Then
\[
\sum_{J_K \in \Omega_K^{(e)}} (I_K, J_K) = \begin{cases} e - |N_{I_K}'|, & \text{if } e \text{ is even} \\
\frac{e}{2} - |N_{I_K}|, & \text{if } e \text{ is odd} \end{cases}
\]

(4) Let
\[
N_{J_K} = \left\{ \frac{j_r}{f_r} \pmod{e} : j_r \equiv 0 \pmod{f_r}, 1 \leq r \leq k \right\}.
\]
Then
\[
\sum_{I_K \in \Omega_K^{(e)}} (I_K, J_K) = e - |N_{J_K}|.
\]

**Corollary 2.4.** Let \( e \geq 2 \) be an integer. Then

(1) \[
\sum_{I_K \in \Omega_K^{(e)}} (I_K, I_K) = e - 1.
\]
(2) For any element \( \vec{a} \in R^* \),
\[
\sum_{I_K \in \Omega_K^{(e)}} |(D_{I_K}^{(K,e)} + \vec{a}) \cap D_{I_K}^{(K,e)}| = e - 1.
\]
Proof. See Appendix B.

**Corollary 2.5.** Let \( e \geq 2 \) be an odd integer and \( \Lambda_K \) be any fixed element with \( 0 \leq \Lambda_K < f_1 \). Then
\[
\sum_{I_K = (i_1, i_2, \ldots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + f_1 / 2} (I_K, I_K) = \frac{e - 1}{2}.
\]

(2) For each \( J_K \in \Omega^{(e)}_K \),
\[
\sum_{I_K = (i_1, i_2, \ldots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + f_1 / 2} (I_K - J_K, I_K - J_K) = \frac{e - 1}{2}.
\]

(3) For any \( J_K \in \Omega^{(e)}_K \) and \( \vec{a} \in R^* \),
\[
\sum_{I_K = (i_1, i_2, \ldots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + f_1 / 2} |(D_{I_K}^{(K,e)} + \vec{a}) \cap D_{I_K}^{(K,e)}| = \frac{e - 1}{2}.
\]

Proof. See Appendix C.

**Remark 2.** Compared with [29, Lemma 2], Corollary 2.5 is more general due to the flexible choice of \( \Lambda_K \). In other words, if we replace “\( 0 \leq i_1 < (F_n)_1 \)" by "\( \Lambda_1 \leq i_1 < \Lambda_1 + (F_n)_1 \)" where \( (F_n)_1 = \phi \left( p_{t_1}^{m_{t_1}} \right) \) and \( \Lambda_1 \) is any fixed element with \( 0 \leq \Lambda_1 < (F_n)_1 \), then [29, Lemma 2] still holds. Hence, Construction 2 in Section 3 can obtain more PDFs with new parameters than Construction 1 in [29].

### 2.2. Difference Balanced Functions

Let \( q = p^l \), where \( p \) is a prime and \( l \) is a positive integer. Let \( m \) and \( r \) be two positive integers with \( r | m \). And let \( \text{Tr}_{q^m/q^r}(x) = \sum_{i=0}^{r-1} x^{q^i} \), \( x \in \text{GF}(q^m) \), be the trace mapping from \( \text{GF}(q^m) \) to its subfield \( \text{GF}(q^r) \).

**Definition 2.6.** A function \( f(x) \) from \( \text{GF}(q^m) \) onto \( \text{GF}(q^r) \) is said to be balanced if any element of \( \text{GF}(q^r) \) appears \( q^m - r \) times with \( x \) ranging over \( \text{GF}(q^m) \). It is said to be difference balanced, if for any \( \delta \in \text{GF}(q^m) \setminus \{0, 1\} \), the difference function \( f(\delta x) - f(x) \) is balanced.

As you know, \( d \)-form functions give a rich source of functions with difference balanced property, which were first defined in [26].

**Definition 2.7.** Let \( d \) be an integer with \( \gcd(d, q^r - 1) = 1 \). A function \( h(x) \) from \( \text{GF}(q^m) \) onto \( \text{GF}(q^r) \) is a \( d \)-form function if
\[
h(yx) = y^d h(x)
\]
for any \( y \in \text{GF}(q^r) \) and \( x \in \text{GF}(q^m) \).

In the literature, there are only a few constructions of difference balanced functions from \( \text{GF}(q^m) \) onto \( \text{GF}(q^r) \):
(1) The single trace function \( f(x) = \text{Tr}_{q^m/q^r}(x^d) \) taken from \( m \)-sequence, where \( d \) is a positive integer with \( \gcd(d, q^m - 1) = 1 \).

(2) The Helleseth-Gong (HG) function extracted from non-binary HG sequence [23];

(3) The Lin function in characteristic 3 [28, 24, 1];

(4) The cascaded composition of the functions above by means of the Gordon–Mills–Welch method [21].

It is observed that all currently known difference balanced functions listed above are \( d \)-form functions for some \( d \). In 2004, No derived the following lemma:

**Lemma 2.8.** [31] If \( f(x) \) is a \( d \)-form function from \( \text{GF}(q^m) \) onto \( \text{GF}(q^r) \) with difference balanced property, then \( f(x) \) is balanced.

### 3. Three Classes of PDFs

In this section, we will construct three classes of PDFs based on the generalized cyclotomy and \( d \)-form functions with difference balanced property introduced in Section 2. Before proposing our constructions, we give some necessary definitions and notation.

For each non-empty subset \( K' \subseteq K \), let

\[
R_{K'} = \{ \bar{x} = (x_1, x_2, \ldots, x_k) \in R : x_i \in \text{GF}(q_i)^*, \text{ if } i \in K'; x_i = 0, \text{ if } i \notin K' \}
\]

Without confusion we may identify \( R_{K'} \) with \( \bigotimes_{i \in K'} \text{GF}(q_i)^* \). Assume that \( K' = \{ t_1, t_2, \ldots, t_{|K'|} \} \subseteq K \) and define \( \bar{g}(K', e) = (g_{t_1}^{f_1}, g_{t_2}^{f_2}, \ldots, g_{t_{|K'|}}^{f_{|K'|}}) \in R_{K'} \). Thus the set \( D(K', e) = \{ (g_i^{t_1})^s : 0 \leq s < e \} \) is a cyclic subgroup of \( R_{K'} \) of order \( e \). Let

\[
\Omega_{K'}^{(e)} = \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_{|K'|}}
\]

and define \( D_{K'}^{(K', e)} \) as

\[
D_{K'}^{(K', e)} = (g_{t_1}^{f_1}, g_{t_2}^{f_2}, \ldots, g_{t_{|K'|}}^{f_{|K'|}}) \cdot D(K', e)
\]

for each \( I_{K'} = (i_1, i_2, \ldots, i_{|K'|}) \in \Omega_{K'}^{(e)} \).

The assertion in the following lemma is obvious.

**Lemma 3.1.** Let an integer \( v = q_1q_2\cdots q_k \) and \( R = \text{GF}(q_1) \times \text{GF}(q_2) \times \cdots \times \text{GF}(q_k) \), where \( q_1, q_2, \ldots, q_k \) are powers of primes. Then we have

\[
R \setminus \{ \bar{0} \} = \bigcup_{\emptyset \neq K' \subseteq K} \bigcup_{I_{K'} \in \Omega_{K'}^{(e)}} D_{K'}^{(K', e)}.
\]

The following lemma can be used to analyze the difference property of the PDFs generated by Construction 1 and Construction 2.

**Lemma 3.2.** Let \( \emptyset \neq K' \subseteq K \), \( I_{K'} \in \Omega_{K'}^{(e)} \) and \( \bar{a} \in \bigotimes_{i \in K''} \text{GF}(q_i)^* \) with \( \emptyset \neq K'' \subseteq K' \).

Then we have

\[
|D_{K'}^{(K', e)} + \bar{a}) \cap D_{K'}^{(K', e)}| = \begin{cases} (I_{K'} + J_{K'}, I_{K'} + J_{K'}), \text{ if } K' = K'' \\
0, \text{ otherwise}
\end{cases}
\]

where \( \bar{a}^{-1} \in D_{K''}^{(K'', e)} \) for some \( |K''| \)-dimensional vector \( J_{K''} \).
Proof. Firstly, if $K' = K''$, then
$$|D_i^{(K', e)} + a\rangle \cap D_i^{(K', e)} = |(\langle a \rangle^{-1} \cdot D_i^{(K', e)} + I_{R_{K'}}) \cap (\langle a \rangle^{-1} \cdot D_i^{(K', e)} | = (I_{K'} + J_{K'}, I_{K'} + J_{K'})$$
where the last equality is from Lemma 2.1.

Secondly, if $K' \neq K''$, we need to show that $|\langle \langle D_i^{(K', e)} + a \rangle \cap D_i^{(K', e)} | | = 0$. Now we prove it by contradiction. In this case, the discussion is divided into two cases.

Case 1: There exists an integer $1 \leq t_d \leq k$ such that $t_d \in K''$ and $t_d \notin K'$, where $1 \leq d \leq |K''|$. Let $K'' = \{t_1, \ldots, t_d, \ldots, t_{|K''|}\} \subseteq K$, $J_{K''} = (-j_1, \ldots, -j_d, \ldots, -j_{|K''|})$, and use the corresponding generalized cyclotomies to construct PDFs. In $R$, where $1 \leq s < e$, one can get different partitions of $\bar{K}$, where we define an addition and a multiplication in $R$. Let $K' = \{1\} \subseteq K$. Then there exist two integers $s_1$ and $s_2$, with $0 \leq s_1, s_2 < e$, such that
$$g_{i_1}^{s_1f_{i_1}} + 0 = g_{i_1}^{s_2f_{i_1}}$$
in $R$, which leads to $s_1 = s_2$. Thus, $\bar{a} = \bar{0}$, which is in contradiction with $\bar{a} \in \prod_{i \in K'} \{0\}$. 

Case 2: There exists an integer $1 \leq t_l \leq l \leq |K'|$ such that $t_l \in K'$ and $t_l \notin K''$, where $1 \leq l \leq |K'|$. Let $K' = \{t_1, \ldots, t_l, \ldots, t_{|K'|}\} \subseteq K$ and $I_{K'} = (i_1, \ldots, i_l, \ldots, i_{|K'|}) \subseteq \Omega_K^{(e)}$. Then there exist two integers $s_1$ and $s_2$, with $0 \leq s_1, s_2 < e$, such that
$$g_{i_1}^{s_1f_{i_1}} + 0 = g_{i_1}^{s_2f_{i_1}}$$
in $R$, which leads to $s_1 = s_2$. Thus, $\bar{a} = \bar{0}$, which is in contradiction with $\bar{a} \in \prod_{i \in K'} \{0\}$.

Based on the previous discussion, we know that for different choice of the number $e$, one can get different partitions of $R$. In what follows, we consider two choices of $e$ and use the corresponding generalized cyclotomies to construct PDFs. In Construction 1, we always assume that $e$ and $e-1$ are divisors of $(q_i-1)$, $i = 1, \ldots, k$.

Then $D_i^{(K', e)}$, $I_{K'} \subseteq \Omega_K^{(e)}$, and $D_i^{(K', e-1)}$, $J_{K'} \subseteq \Omega_K^{(e-1)}$, are two different partitions of $\bar{R} \setminus \emptyset$, where $\emptyset \neq K' \subseteq K$. Therefore,
$$\mathcal{A}_e = \{D_i^{(K', e)} : \emptyset \neq K' \subseteq K, I_{K'} \subseteq \Omega_K^{(e)} \} \cup \{\emptyset\}$$
and
$$\mathcal{A}_{e-1} = \{D_i^{(K', e-1)} : \emptyset \neq K' \subseteq K, J_{K'} \subseteq \Omega_K^{(e-1)} \} \cup \{\emptyset\}$$
are two different partitions of $R$. From now on, we will combine these two partitions to generate the first class of PDFs.

Hereafter, $(a)_b$ denotes the least nonnegative residue of $a$ modulo $b$, where $a$ and $b$ are two positive integers. Let $\varphi$ be a bijection from the set $\mathcal{A}_e$ to $\mathbb{Z}_{e^{-1}+1}$ with $\varphi(\emptyset) = e^{-1}$. And let $\psi$ be a bijection from the set $\mathcal{A}_{e-1}$ to $\mathbb{Z}_{e^{-1}+1}$ with $\psi(\emptyset) = e^{-1}$.

Define a function $\eta$ from $R \setminus \emptyset$ to $\mathbb{Z}_e$ by $\eta(\bar{x}) = \{s\}_e$ if
$$\bar{x} = (g_{i_1}^{s_1f_{i_1}}, g_{i_2}^{s_2f_{i_2}}, \ldots, g_{i_{|K'|}}^{s_{|K'|}}) \cdot (\bar{y})^s \in R \setminus \emptyset$$
where $K' = \{t_1, t_2, \ldots, t_{|K'|}\} \subseteq K$ and $(i_1, i_2, \ldots, i_{|K'|}) \subseteq \Omega_K^{(e)}$. Consider the commutative ring $R \times \mathbb{Z}_e$, where we define an addition and a multiplication in $R \times \mathbb{Z}_e$ as follows: for any element $(\bar{x}, s)$ and $(\bar{y}, t)$ in $R \times \mathbb{Z}_e$,
$$(\bar{x}, s) + (\bar{y}, t) = (\bar{x} + \bar{y}, (s + t)_e)$$
$$(\bar{x}, s) \cdot (\bar{y}, t) = (\bar{x} \cdot \bar{y}, (st)_e)$$
where $\vec{x} + \vec{y}$ and $\vec{x} \cdot \vec{y}$ are operated in $R$. The following result on the function $\eta$ will be useful in the sequel.

**Lemma 3.3.** Let the function $\eta$ be defined as above. Then for any given $(\vec{a}_1, a_2) \in R \times Z_e$ with $\vec{a}_1 \neq \vec{0}$ and $a_2 \neq 0$, there exists a unique $\vec{x}_1$ in $\bigcup_{A \in A_c \setminus \{\vec{0}\}} \{ \vec{x} \in A : \vec{x} + \vec{a}_1 \in A \}$ such that

$$a_2 + \eta(\vec{x}_1 + \vec{a}_1) \equiv \eta(\vec{x}_1) \pmod{e}.$$  

**Proof.** Suppose there exist $K' = \{t_1, t_2, \cdots, t_{|K'|}\} \subseteq K$ and $(i_1, i_2, \cdots, i_{|K'|}) \in \Omega_K^{(e)}$ such that

$$\vec{x}_1 = (g_{i_1}^{t_1}, g_{i_2}^{t_2}, \cdots, g_{i_{|K'|}}^{t_{|K'|}}) \cdot (\vec{g}(K', e)),$$

and

$$\vec{x}_1 + \vec{a}_1 = (g_{i_1}^{t_1}, g_{i_2}^{t_2}, \cdots, g_{i_{|K'|}}^{t_{|K'|}}) \cdot (\vec{g}(K', e))(s-a_2),$$

which is equivalent to

$$[(\vec{g}(K', e))^{(s-a_2)} - 1]^{-1} \cdot \vec{a}_1 = (g_{i_1}^{t_1}, g_{i_2}^{t_2}, \cdots, g_{i_{|K'|}}^{t_{|K'|}}) \cdot (\vec{g}(K', e)).$$

Note that $\{D_{I_{K'}}^{(K', e)} : \emptyset \neq K' \subseteq K, I_{K'} \in \Omega_{K'}^{(e)}\}$ is a partition of $R \setminus \{\vec{0}\}$. Hence, the assertion is proved. \hfill $\square$

We are now in a position to propose our constructions of PDFs. The first construction of PDFs is presented as follows.

**Construction 1:** Let the notation be defined as above and $c \in Z_e^*$. Generate a function $f$ over $R \times Z_e$ as

$$f(\vec{x}_1, x_2) = \begin{cases} e \varphi(D_{I_{K'}}^{(K', e)}) + (\eta(\vec{x}_1)) + cx_2, & \text{if } \vec{x}_1 \in D_{I_{K'}}^{(K', e)} \text{ and } x_2 \neq 0 \\ e \varphi(\{\vec{0}\}), & \text{if } \vec{x}_1 = \vec{0} \text{ and } x_2 \neq 0 \\ v \psi(D_{I_{K'}}^{(K', e-1)}), & \text{if } \vec{x}_1 \in D_{I_{K'}}^{(K', e-1)} \text{ and } x_2 = 0 \\ v \psi(\{\vec{0}\}), & \text{if } \vec{x}_1 = \vec{0} \text{ and } x_2 = 0 \\ 
\end{cases}$$

where $(\vec{x}_1, x_2) \in R \times Z_e$, $\emptyset \neq K' \subseteq K$, $I_{K'} \in \Omega_{K'}^{(e)}$, and $J_{K'} \in \Omega_{K'}^{(e-1)}$. For each $i$ with $0 \leq i \leq \frac{e-1}{e-1}$, define

$$B_i = \{ (\vec{x}_1, x_2) \in R \times Z_e : f(\vec{x}_1, x_2) = i \}$$

and

$$\mathcal{P} = \{ B_i : 0 \leq i \leq \frac{e-1}{e-1} \}.$$

For the above construction, we have the first main result.

**Theorem 3.4.** The set $\mathcal{P}$ generated by Construction 1 is an $(R \times Z_e, [(e-1) \frac{e-1}{e-1}, 1])$-PDF.

**Proof.** For any given nonzero $(\vec{a}_1, a_2) \in R \times Z_e$, we have

$$|\{(\vec{x}_1, x_2) \in R \times Z_e : f(\vec{x}_1 + \vec{a}_1, x_2 + a_2) = f(\vec{x}_1, x_2)\}| = \Delta_1(\vec{a}_1, a_2) + \Delta_2(\vec{a}_1, a_2) + \Delta_3(\vec{a}_1, a_2)$$

where

$$\Delta_1(\vec{a}_1, a_2) = |\{(\vec{x}_1, x_2) \in R \times Z_e : f(\vec{x}_1 + \vec{a}_1, x_2 + a_2) = f(\vec{x}_1, x_2) = v - 1\}|,$$

$$\Delta_2(\vec{a}_1, a_2) = |\{(\vec{x}_1, x_2) \in R \times Z_e : v \leq f(\vec{x}_1 + \vec{a}_1, x_2 + a_2) = f(\vec{x}_1, x_2) < v + \frac{v-1}{e-1}\}|$$

and

$$\Delta_3(\vec{a}_1, a_2) = \cdots$$
and
\[ \Delta_3(\vec{a}_1, a_2) = |\{(\vec{x}_1, x_2) \in R \times \mathbb{Z}_e : 0 \leq f(\vec{x}_1 + \vec{a}_1, x_2 + a_2) = f(\vec{x}_1, x_2) < v - 1\}|. \]

If \( f(\vec{x}_1 + \vec{a}_1, x_2 + a_2) = f(\vec{x}_1, x_2) = v - 1 \), then \( \vec{x}_1 = 0 \), \( x_2 \neq 0 \), \( \vec{x}_1 + \vec{a}_1 = \vec{0} \) and \( \langle x_2 + a_2 \rangle_\epsilon \neq 0 \). Therefore, \( \Delta_1(\vec{a}_1, a_2) = 0 \) if \( \vec{a}_1 \neq \vec{0} \) and otherwise
\[ \Delta_1(\vec{0}, a_2) = |\{(\vec{x}_1, x_2) \in R \times \mathbb{Z}_e : \vec{x}_1 = \vec{0} \text{ and } x_2 \in \mathbb{Z}_e \setminus \{0, -a_2\}\}| = e - 2 \]
for any given \( a_2 \neq 0 \). Hence, we have
\[
\Delta_1(\vec{a}_1, a_2) = \begin{cases} 
0, & \text{if } \vec{a}_1 \neq \vec{0} \\
e - 2, & \text{if } \vec{a}_1 = \vec{0} \text{ and } a_2 \neq 0
\end{cases}
\]

When \( a_2 \neq 0 \), it follows from the definition of the function \( f \) that \( \Delta_2(\vec{a}_1, a_2) = 0 \). When \( \vec{a}_1 \neq 0 \) and \( a_2 = 0 \), it follows from the definitions of the functions \( f \) and \( \psi \) that
\[
\Delta_2(\vec{a}_1, 0) = \sum_{\vec{x}_1 \in \mathbb{Z}_e \setminus \{\vec{0}\}} |\{x_1 \in D^{(K', e-1)}_J : \vec{x}_1 + \vec{a}_1 \in D^{(K', e-1)}_J\}|
\]
\[
= \sum_{\vec{x}_1 \in \mathbb{Z}_e \setminus \{\vec{0}\}} |(D^{(K', e-1)}_J + \vec{a}_1) \cap D^{(K', e-1)}_J|
\]
\[
e - 2
\]
where the last identity followed from Corollary 2.4-(2). Hence, we have
\[
\Delta_2(\vec{a}_1, a_2) = \begin{cases} 
0, & \text{if } a_2 \neq 0 \\
e - 2, & \text{if } \vec{a}_1 \neq \vec{0} \text{ and } a_2 = 0
\end{cases}
\]

If \( 0 \leq f(\vec{x}_1 + \vec{a}_1, x_2 + a_2) = f(\vec{x}_1, x_2) < v - 1 \), then there exist \( I_{K'} \in \Omega_{K', e}^{(e)} \) and \( I_{K''} \in \Omega_{K'', e}^{(e)} \), where \( \emptyset \neq K' \subseteq K \) and \( \emptyset \neq K'' \subseteq K \), such that \( \vec{x}_1 \in D^{(K', e)}_I \) and \( \vec{x}_1 + \vec{a}_1 \in D^{(K'', e)}_I \). Furthermore, \( x_2 \neq 0 \), \( \langle x_2 + a_2 \rangle_\epsilon \neq 0 \) and
\[
h[f(\vec{x}_1, x_2), f(\vec{x}_1 + \vec{a}_1, x_2 + a_2)] = h[e \varphi(D^{(K', e)}_{I_{K'}}) + (\eta(\vec{x}_1) + cx_2)_e, e \varphi(D^{(K'', e)}_{I_{K''}}) + (\eta(\vec{x}_1 + \vec{a}_1) + c(x_2 + a_2))_e]
\]
\[
= h[\varphi(D^{(K', e)}_{I_{K'}}), \varphi(D^{(K'', e)}_{I_{K''}})]h[(\eta(\vec{x}_1) + cx_2)_e, (\eta(\vec{x}_1 + \vec{a}_1) + c(x_2 + a_2))_e]
\]
where
\[
h[a, b] = \begin{cases} 
1, & \text{if } a = b \\
0, & \text{otherwise}
\end{cases}
\]
If \( h[f(\vec{x}_1, x_2), f(\vec{x}_1 + \vec{a}_1, x_2 + a_2)] = 1 \), then \( D^{(K', e)}_{I_{K'}} = D^{(K'', e)}_{I_{K''}} \) and \( ca_2 + \eta(\vec{x}_1 + \vec{a}_1) \equiv \eta(\vec{x}_1) \pmod{e} \), which lead to \( K' = K'' \) and \( I_{K'} = I_{K''} \). Hence, \( \Delta_3(\vec{a}_1, a_2) \) is equal to \( (e - 2)|\mathcal{T}| \), where
\[
\mathcal{T} = \{\vec{x}_1 \in \bigcup_{A \in \mathcal{A}_I \setminus \{\vec{0}\}} \{\vec{x} \in A : \vec{x} + \vec{a}_1 \in A\} : ca_2 + \eta(\vec{x}_1 + \vec{a}_1) \equiv \eta(\vec{x}_1) \pmod{e}\}.
\]
Now we distinguish the following three cases to discuss \( |\mathcal{T}| \).

Case 1: \( \vec{a}_1 = 0 \) and \( a_2 \neq 0 \). If \( ca_2 + \eta(\vec{x}_1 + \vec{a}_1) \equiv \eta(\vec{x}_1) \pmod{e} \), then \( a_2 = 0 \) since \( c \in \mathbb{Z}_e^* \). This is a contradiction with \( a_2 \neq 0 \). Hence, \( |\mathcal{T}| = 0 \) in this case.
\[ \Delta_3(a_1, a_2) = \begin{cases} 0, & \text{if } a_1 = 0 \text{ or } a_2 = 0 \\ e - 2, & \text{if } a_1 \neq 0 \text{ and } a_2 \neq 0. \end{cases} \]

It then follows from equalities (9), (10), (11) and (12) that

\[ |\{ (\vec{x}_1, x_2) \in R \times \mathbb{Z}_e : f(\vec{x}_1 + a_1, x_2 + a_2) = f(\vec{x}_1, x_2) = 0 \}| = e - 2. \]

Hence, the function \( f \) generated by Construction 1 is an \((ev, \frac{ev-1}{e-1}, 1, e - 2)\) ZDB function from \( R \times \mathbb{Z}_e \) onto \( \mathbb{Z}_{\frac{ev-1}{e-1} + 1} \). According to Lemma 1.1 and equality (8), we conclude that \( \mathcal{P} \) is a \((R \times \mathbb{Z}_e, [(e - 1)^{\frac{ev-1}{e-1}} 1], e - 2)\) PDF. 

In the following, an example of PDF generated by Construction 1 is given.

**Example 3.5.** Let \( v = p^2 = 5^2 \) and \( e = 4 \). Then \( e(e - 1) | (p^2 - 1) \). The set \( \mathcal{A}_4 \) in Construction 1 is given by listing its elements as

\[ \{1, 2, 4, 3\}, \{3, 4, 1, 2\}, \{5, 6, 1, 4\}, \{6, 5, 1, 4\}, \{7, 0, 1, 3\} \]

and the set \( \mathcal{A}_3 \) in Construction 1 is given by listing its elements as

\[ \{1, 0, 9\}, \{0, 1, 9\}, \{1, 9, 0\}, \{9, 0, 1\}, \{0, 9, 1\}, \{9, 1, 0\} \]

where \( \alpha \) is a generator of the multiplicative group \( GF(5^2)^* \) and the superscript numbers denote the indices of the sets in \( \mathcal{A}_4 \) and \( \mathcal{A}_3 \) respectively. For any \( x \in GF(5^2) \), define \( \varphi(x) = i - 1 \) if \( x \) belongs to the \( i \)th set \((1 \leq i \leq 7) \) in \( \mathcal{A}_4 \) and \( \psi(x) = j - 1 \) if \( x \) belongs to the \( j \)th set \((1 \leq j \leq 9) \) in \( \mathcal{A}_3 \). Then by Construction 1 we can generate a function \( f \) from \( GF(5^2) \times \mathbb{Z}_4 \) onto \( \mathbb{Z}_{33} \) as

\[ (f(0, 0), f(0, 1), f(0, 2), f(0, 3), f(1, 0), f(1, 1), f(1, 2), f(1, 3), f(0, 0), \cdots, f(0, 2), f(2, 3), 3, 4, 24, 24, 24, 25, 1, 2, 3, 26, 5, 6, 7, 27, 9, 10, 11, 28, 13, 14, 15, 29, 17, 18, 19, 30, 21, 22, 31, 2, 3, 0, 32, 6, 7, 4, 25, 10, 11, 8, 26, 14, 15, 12, 27, 18, 19, 6, 16, 22, 23, 20, 29, 3, 0, 1, 30, 7, 4, 5, 31, 11, 8, 9, 32, 15, 12, 13, 25, 19, 16, 17, 26, 23, 20, 21, 27, 0, 1, 2, 28, 4, 5, 6, 29, 8, 9, 10, 30, 12, 13, 14, 31, 16, 17, 18, 32, 20, 21, 22). \]

With a simple calculation by using a computer, we can check that \( \mathcal{P} = \{ B_i : 0 \leq i \leq 33 \} \) is a \((GF(5^2) \times \mathbb{Z}_4, [33^{33} 1], 2)\) PDF, where \( B_i = \{(x_1, x_2) \in GF(5^2) \times \mathbb{Z}_4 : f(x_1, x_2) = i \} \) with \( 0 \leq i \leq 33 \). This is consistent with the result of Theorem 3.4.

**Construction 2:** Suppose \( v = q_1 q_2 \cdots q_k \) is an odd integer and \( K = \{1, 2, \cdots, k\} \), where \( q_1, q_2, \cdots, q_k \) are powers of odd primes. Let \( K', \Omega^e_K \) and \( D_{K'}^{(K', e)} \) be defined as above. Let \( e \geq 3 \) be odd such that \( q_i = ef_i + 1 \). Denote

\[ S_1 = \{ D_{K'}^{(K', e)} : 0 \neq K' = \{i_1, i_2, \cdots, i_{|K'|}\} \subseteq K, \ I_{K'} = \{i_1, i_2, \cdots, i_{|K'|}\} \in \Omega^e_K, \ \Lambda_{K'} \leq i_1 < \Lambda_{K'} + \frac{f_i}{2} \} \]
and

\[
S = S_1 \bigcup \left\{ \{\vec{x} \in R \setminus \bigcup_{D_i^{(K',e)} \in S_1} D_i^{(K',e)} \} \right\},
\]

where \(\Lambda_{K'}\) is any fixed element with \(0 \leq \Lambda_{K'} < f_{t_1}\).

For Construction 2, we have the second main result.

**Theorem 3.6.** The set \(S\) generated by Construction 2 is an \((R, [e^{\frac{x+1}{2}}, \frac{x+1}{2}])\) PDF.

**Proof.** For any \(\vec{a} \in R \setminus \{0\}\), there exists a unique nonempty set \(K'' = \{t_1', t_2', \ldots, t_{|K'|}''\} \subseteq K\) such that \(\vec{a} \in \prod_{i \in K''} \text{GF}(q_i)^\ast\). Let \((\vec{a})^{-1} \in D_{I_{K''}^{(e)}}^{(K'',e)}\), where \(J_{K''} \in \Omega_{(e)}^{(e)}\).

By equality (13), we need to prove that the number of \(\vec{x} \in R\) such that \(\vec{x} + \vec{a} \in S_1\) belong to some same set in \(S\) is always \(\frac{e - 1}{2}\). Hence, we have

\[
|\{\vec{x} \in R : \vec{x} \in S_1 \text{ and } \vec{x} + \vec{a} \in S_1\}| = \sum_{\emptyset \neq K' = \{t_1, t_2, \ldots, t_{|K'|}''\} \subseteq K} |\sum_{\Lambda_{K'} \leq 1 < \Lambda_{K''} + \frac{f_{t_1}'}{I_{K''}^{(e)}}} (D_{I_{K''}^{(e)}}^{(K'',e)} + \vec{a}) \cap D_{I_{K''}^{(e)}}^{(K'',e)}| = \sum_{\Lambda_{K'} \leq 1 < \Lambda_{K''} + \frac{f_{t_1}'}{I_{K''}^{(e)}}} (D_{I_{K''}^{(e)}}^{(K'',e)} + \vec{a}) \cap D_{I_{K''}^{(e)}}^{(K'',e)}| = \frac{e - 1}{2}
\]

where the second and last equalities follow from Lemma 3.2 and Corollary 2.5-(3) respectively. This completes the proof. \(\Box\)

Here we employ the following example to illustrate Construction 2 and Theorem 3.6.

**Example 3.7.** Let \(v = 5^2 \times 7, e = 3, f_1 = 8\) and \(f_2 = 2\). And let \(\Lambda_{K'} = 0\) for any \(K' \subseteq \{0, 1\}\). The set \(S_1\) in Construction 2 is given by listing its elements as

\[
\{ (1, 1), (\alpha^8, 2), (\alpha^{16}, 4), (1, 2), (\alpha^8, 4), (\alpha^{16}, 1), (1, 3), (\alpha^8, 6), (\alpha^{16}, 5), \}
\{ (1, 4), (\alpha^8, 1), (\alpha^{16}, 2), (1, 5), (\alpha^8, 3), (\alpha^{16}, 6), (1, 6), (\alpha^8, 5), (\alpha^{16}, 3), \}
\{ (1, 7), (\alpha^8, 2), (\alpha^{16}, 4), (1, 8), (\alpha^8, 4), (\alpha^{16}, 1), (1, 9), (\alpha^8, 6), (\alpha^{16}, 5), \}
\{ (1, 10), (\alpha^8, 1), (\alpha^{16}, 2), (1, 11), (\alpha^8, 3), (\alpha^{16}, 6), (1, 12), (\alpha^8, 5), (\alpha^{16}, 3), \}
\{ (1, 13), (\alpha^8, 2), (\alpha^{16}, 4), (1, 14), (\alpha^8, 4), (\alpha^{16}, 1), (1, 15), (\alpha^8, 6), (\alpha^{16}, 5), \}
\{ (1, 16), (\alpha^8, 1), (\alpha^{16}, 2), (1, 17), (\alpha^8, 3), (\alpha^{16}, 6), (1, 18), (\alpha^8, 5), (\alpha^{16}, 3), \}
\]
where $\alpha$ is a generator of the multiplicative group $GF(5^2)^\ast$. We can check that the set $S = S_1 \cup \{ \bar{x} \in (GF(5^2) \times GF(7)) \setminus \bigcup_{A \in S_1} A \}$ is a $(GF(5^2) \times GF(7), [32^{91} 188])$, 1) PDF by using a computer, which is consistent with the result of Theorem 3.6.

The following result is useful for the construction of the third class of PDFs.

**Lemma 3.8.** [42] Let $e$ be a positive integer such that $e | (q - 1)$ and $\text{gcd}(e, m) = 1$. Let $\alpha$ be a generator of the multiplicative group $GF(q^m)^\ast$ and $C_0^{(e, q^m)}, C_1^{(e, q^m)}, \cdots, C_{e-1}^{(e, q^m)}$ be the cyclotomic classes of order $e$ in $GF(q^m)$, where $C_i^{(e, q^m)} = \alpha^i \langle \alpha^e \rangle$ for $i = 0, 1, \cdots, e - 1$. Suppose that $h(x)$ is a $d$-form function from $GF(q^m)$ onto $GF(q)$ with difference balanced property. Then for each $0 \leq i < e$ and any $\delta \in GF(q^m) \setminus \{0, 1\}$,

$$|\{x \in C_i^{(e, q^m)} : h(x) = 0\}| = \frac{q^{m-1} - 1}{e}$$

and

$$|\{x \in C_i^{(e, q^m)} : h(\delta x) = h(x)\}| = \frac{q^{m-1} - 1}{e}.$$

The third construction of PDFs is presented as the following.

**Construction 3:** Let $e$ be a positive integer such that $e | (q - 1)$ and $\text{gcd}(e, m) = 1$. Let $\alpha$ be a generator of the multiplicative group $GF(q^m)^\ast$. Suppose that $h(x)$ is a $d$-form function from $GF(q^m)$ onto $GF(q)$ with difference balanced property. For any $1 \leq k \leq e$, define

$$D = \{(s, i) : h(\alpha^{sk+i}) = 0, \ 0 \leq s < \frac{q^m - 1}{e}, \ 0 \leq i < k\}$$

and

$$\mathcal{J} = \{D\} \cup \left\{ \{x \in (\mathbb{Z}_{q^m-1} \times \mathbb{Z}_k) \setminus D\right\}.$$

**Theorem 3.9.** For any $1 \leq a < k\frac{q^m - 1}{e}$, we have

$$|D + a \cap D| = k \frac{q^{m-2} - 1}{e}$$

and the set $\mathcal{J}$ defined by Construction 3 is a $(\mathbb{Z}_{q^m-1} \times \mathbb{Z}_k, [k\frac{q^{m-1} - 1}{e}, 1\frac{q^{m-1} - 1}{e}])$ PDF.

**Proof.** Firstly, we have by Lemma 3.8

$$|D| = |\{(s, i) : h(\alpha^{sk+i}) = 0, \ 0 \leq s < \frac{q^m - 1}{e}, \ 0 \leq i < k\}|$$

$$= \sum_{i=0}^{k-1} |\{x \in C_i^{(e, q^m)} : h(x) = 0\}|$$

$$= k \frac{q^{m-1} - 1}{e}.$$
Secondly, for any $1 < a < k^{\frac{m-1}{e}}$, there exists only one $(t, j)$ such that $a = tk + j$ with $t \in \mathbb{Z}_{\frac{m-1}{e}}$ and $j \in \mathbb{Z}_k$. Let $\delta = \alpha^{tk+j}$. Hence, we have by Lemma 3.8

$$|(D + a) \cap D| = |\{(s, i) : h(\alpha^{s+i}) = 0, h(\alpha^{(s+i)k+i+j}) = 0, 0 \leq s < \frac{q^m-1}{e}, 0 \leq i < k\}|$$

$$= |\{(s, i) : h(\alpha^{s+i}) = 0, h(\alpha^{tk+j}\alpha^{s+i}) = 0, 0 \leq s < \frac{q^m-1}{e}, 0 \leq i < k\}|$$

$$= |\{x \in \bigcup_{i=0}^{k-1} C_i^{(e, q^m)} : h(x) = 0, h(\delta x) = 0\}|$$

$$= k\frac{q^m-2}{e} - 1.$$ 

This completes the proof of Theorem 3.9.

**Remark 3.** In this paper, we propose three constructions of PDFs by virtue of the generalized cyclotomy and difference balanced functions in Section 2. It can be easily checked that Theorem 3.4 still holds for even $v$. We summarize these PDFs in Table 1, where $q_1, q_2, \cdots, q_k$ are powers of primes and $R = \text{GF}(q_1) \times \text{GF}(q_2) \times \cdots \times \text{GF}(q_k)$.

(1) In [6] and [29], two classes of PDFs are given using the terminology of ZDB functions. Compared with [6] and [29], Construction 1 and Construction 2 provide many new and more flexible parameters, since the requirement $e(q^m_i - 1)$ or $e(e - 1)|q^m_i - 1)$ gives more flexibility in our constructions. Nevertheless, these parameters are identical to those of [27, Theorem 18] and [4, Chapter 3] respectively via the recursive constructions of PDFs. Compared with [27] and [4], our constructions are direct.

(2) Construction 3 is generic in the sense that it works for every $d$-form function with difference balanced property. When $k = 1$ and $e = q - 1$, the parameters of Theorem 3.9 are equivalent to those given by [37, Theorem 13]. When $k \neq 1$ or $e \neq q - 1$, the parameters of Theorem 3.9 are new.

| $A$ | $K$ | $\lambda$ | Constraints | Ref. |
|-----|-----|-----|---------|-----|
| $R \times \mathbb{Z}_e$ | $[(e-1)\mathbb{Z}_e + 1]$ | $e-2$ | $v = q_1q_2 \cdots q_k$, $e(q^m_i - 1)(q_k - 1)$ for $1 \leq i \leq k$ | Theorem 3.4 |
| $R$ | $[e^{2m} - 1 \mathbb{Z}_e + 1]$ | $\frac{2m - 2}{e}$ | $v = q_1q_2 \cdots q_k$, $e \geq 3$ is odd such that $e(q_k - 1)$ for $1 \leq i \leq k$ | Theorem 3.6 |
| $\mathbb{Z}_{q^m-1} \times \mathbb{Z}_k$ | $[k^{m-1} \mathbb{Z}_e + 1, k^{2m-1} \mathbb{Z}_e + 1]$ | $k^{2m-2} \mathbb{Z}_e + 1$ | $e(q-1), \gcd(e, m) = 1$, $1 \leq k \leq e$, $m > 2$ | Theorem 3.9 |

In the following, an example of PDF generated by Construction 3 is given.

**Example 3.10.** Let $q = 4$, $m = 4$ and $e = 3$. And let $h(x) = \text{Tr}_{q^4/q}(x) = x + x^q + x^{q^2} + x^{q^3}$ in Construction 3. If $k = 1$, then the set $J$ is equivalent to the function $h$ in [37, Example 15]. If $k = 2$, then the set $D$ in Construction 3 is given as

$$D = \{0, 7, 13, 14, 17, 19, 23, 26, 27, 28, 34, 38, 46, 49, 51, 52, 54, 56, 67, 68, 76, 85, 92, 98, 99, 102, 104, 108, 111, 112, 113, 119, 123, 131, 134, 136, 137, 139, 141, 152, 153, 161\}.$$

In this case, we can check that the set $J = \{D\} \cup \{\{x : x \in (\mathbb{Z}_{q^4} \times \mathbb{Z}_2) \setminus D\}$ is a $(\mathbb{Z}_{q^4} \times \mathbb{Z}_2, [42^{1128}], 10)$ PDF by using a computer.
4. An application of PDFs

Once PDFs are constructed, many interesting objects can be obtained. In this section, we will construct optimal constant composition codes by virtue of Constructions 1, 2 and 3 in Section 3.

An \((n, M, d, [\omega_0, \omega_1, \cdots, \omega_{m-1}])_m\) constant composition code (CCC) is a code over an abelian group \(\{0, 1, \cdots, b_{m-1}\}\) with length \(n\), size \(M\) and minimum Hamming distance \(d\) such that in every codeword the element \(b_i\) occurs exactly \(\omega_i\) times for any \(i \in \{0, 1, \cdots, m - 1\}\). Let \(A_m(n, M, d, [\omega_0, \omega_1, \cdots, \omega_{m-1}])\) be the maximum size of an \((n, M, d, [\omega_0, \omega_1, \cdots, \omega_{m-1}])_m\) CCC. A CCC is optimal if the bound in Lemma 4.1 is met.

**Lemma 4.1.** [30] If

\[
nd - n^2 + \sum_{i=0}^{m-1} \omega_i^2 > 0,
\]

then

\[
A_m(n, M, d, [\omega_0, \omega_1, \cdots, \omega_{m-1}]) \leq \frac{nd}{nd - n^2 + \sum_{i=0}^{m-1} \omega_i^2}.
\]

In [14], Ding et al. established the link between PDFs and optimal CCCs. Henceforth, PDFs are usually used to construct optimal CCCs.

**Theorem 4.2.** [14] If an \((A, [k_1^{u_1} k_2^{u_2} \cdots k_s^{u_s}], \lambda)\) PDF exists, then there is an optimal \((n, n - \lambda, [k_1^{u_1} k_2^{u_2} \cdots k_s^{u_s}])_m\) CCC meeting the bound of Lemma 4.1, where \(|A|=n\) and \(m = u_1 + u_2 + \cdots + u_s\).

By virtue of the method in the proof of Theorem 4.2, every PDF leads to an optimal CCC. In Table 2, we obtain new optimal CCCs using three classes of PDFs in Section 3, where \(q_1, q_2, \cdots, q_k\) are powers of primes.

**Table 2.** Some optimal CCCs with parameters \((n, M, d, [\omega_0, \omega_1, \cdots, \omega_{m-1}])_m\) from our PDFs

| Parameters | Constraints |
|------------|-------------|
| \((e^v, e^v, e^v - e + 2, [(e - 1)^{v-1}]_{\omega_0^{e^v}, \omega_1^{e^v}, \omega_2^2})\) | \(v = q_1 q_2 \cdots q_k; e(e - 1)((q_i - 1) \text{ for } 1 \leq i \leq k)\) |
| \(\left(v, v, v - \frac{e - 1}{2}, [v^{\frac{e - 1}{2}} 1^{\frac{e - 3}{2}}]\right)_{\omega_0^v, \omega_1^v, \omega_2^2}^{v-1, e+1} \) | \(v = q_1 q_2 \cdots q_k; e \geq 3 \text{ is odd such that } e(q_i - 1) \text{ for } 1 \leq i \leq k\) |
| \(k^{q^{m-1}}_e, k^{2^{q^{m-1}}}_e, k^{q^{m-2}}_e, k^{q^{m-3}}_e, \ldots, k^{q^1}_e, \ldots, k^{q^{m-1}}_e, \ldots, k^{q^{m-1}}_{e+1} \) | \(c | (q - 1), \gcd(e, m) = 1, 1 \leq k \leq e, m > 2\) |

5. Concluding remarks

In this paper, we give a unified treatment for the Zeng-Cai-Tang-Yang generalized cyclotomy over the ring \(\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}\) and the generalized cyclotomy over the ring \(\text{GF}(q_1) \times \text{GF}(q_2) \times \cdots \times \text{GF}(q_k)\). By virtue of the generalized cyclotomy on product ring of finite fields and \(d\)-form functions with difference balanced property, we presented three classes of PDFs. These PDFs can be used to construct optimal constant composition codes. In the future work, we are expected to propose more PDFs or ZDB functions, by which we can construct more optimal cryptographic objects.
ACKNOWLEDGMENTS

This work was partially supported by the National Natural Science Foundation of China (Grant No. 11771007, 11601177 and 61572027). The first author was also supported by the Funding of Nanjing Institute of Technology (Grant No. ZKJ201909 and QKJ201804).

APPENDIX A: PROOF OF LEMMA 2.2

Proof. Suppose that \(-\vec{I}_R \in D_{I_K}^{(K,e)}\), where \(I_K = (i_1, i_2, \cdots, i_k) \in \Omega_K^{(e)}\), then there exists an integer \(s\) with \(0 \leq s < e\) such that

\[
(g_1^{i_1}, g_2^{i_2}, \cdots, g_k^{i_k}) \cdot (\vec{g}_{(K,e)})^s = -\vec{I}_R.
\]

By the definition of \(\vec{g}_{(K,e)}\), we have

\[
(g_1^{i_1+s_1}, g_2^{i_2+s_2}, \cdots, g_k^{i_k+s_k}) = (-1_{R_1}, -1_{R_2}, \cdots, -1_{R_k}).
\]

Thus, we have

\[
i_d + sf_d \equiv \frac{ef_d}{2} \pmod{ef_d}
\]

for any \(1 \leq d \leq k\). By equality (14) and \(I_K \in \Omega_K^{(e)}\), if \(e\) is even, then \(i_1 = 0\), \(s = \frac{e}{2}\) and hence \(i_r = 0\) with \(2 \leq r \leq k\). If \(e\) is odd, then \(i_1 = \frac{e-1}{2}\), \(s = \frac{e-1}{2}\) and hence \(i_r = \frac{e-1}{2}\) with \(2 \leq r \leq k\). Therefore, we have \(-\vec{I}_R \in D_{I_K}^{(K,e)}\) if \(e\) is even and \(-\vec{I}_R \in D_{I_K}^{(K,e)}\) otherwise. \(\square\)

APPENDIX B: PROOF OF COROLLARY 2.4

Proof. (1) By Proposition 2.3-(1), we have

\[
\sum_{I_K \in \Omega_K^{(e)}} (I_K, I_K) = \sum_{I_K \in \Omega_K^{(e)}} (-I_K, 0) = \sum_{I_K \in \Omega_K^{(e)}} (I_K, 0) = e - 1,
\]

where the last equality is from Proposition 2.3-(4).

(2) Let \(\vec{a} \in D_{I_K}^{(K,e)}\) with \(J_K \in \Omega_K^{(e)}\). Then

\[
\sum_{I_K \in \Omega_K^{(e)}} |(D_{I_K}^{(K,e)} + \vec{a}) \cap D_{I_K}^{(K,e)}| = \sum_{I_K \in \Omega_K^{(e)}} |(\vec{a})^{-1} \cdot D_{I_K}^{(K,e)} + \vec{I}_R) \cap (\vec{a})^{-1} \cdot D_{I_K}^{(K,e)}|
\]

\[
= \sum_{I_K \in \Omega_K^{(e)}} |(D_{I_K - J_K}^{(K,e)} + \vec{I}_R) \cap D_{I_K - J_K}^{(K,e)}|
\]

\[
= \sum_{I_K \in \Omega_K^{(e)}} (I_K - J_K, I_K - J_K) = \sum_{I_K \in \Omega_K^{(e)}} (I_K, I_K) = e - 1,
\]

where the second equality and the last equality are from Lemma 2.1 and Corollary 2.4-(1), respectively. \(\square\)

APPENDIX C: PROOF OF COROLLARY 2.5

Proof. (1) Note that as the first coordinate \(i_1\) of \(I_K\) runs over the set \(\{\Lambda_K, \Lambda_K + 1, \cdots, \Lambda_K + \frac{e}{2} - 1\}\), the first coordinate \(i_1 + \frac{e}{2}\) of \(I_K + E_K\) will run over the set
\( \{\Lambda_K + \frac{f_1}{2}, \Lambda_K + \frac{f_1}{2} + 1, \cdots, \Lambda_K + f_1 - 1\} \), where \( E_K \) is defined as Lemma 2.2. Thus, according to Proposition 2.3-(2), we have

\[
\sum_{I_K = (i_1, i_2, \cdots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + \frac{f_1}{2}} (I_K, I_K) = \sum_{I_K = (i_1, i_2, \cdots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + \frac{f_1}{2}} (I_K + E_K, I_K + E_K) = \sum_{I_K = (i_1, i_2, \cdots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + \frac{f_1}{2}} (I_K, I_K).
\]

By combining this with Corollary 2.4-(1), we get

\[
\sum_{I_K = (i_1, i_2, \cdots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + \frac{f_1}{2}} (I_K, I_K) = \frac{1}{2} \sum_{I_K \in \Omega^{(e)}_K} (I_K, I_K) = \frac{e - 1}{2}.
\]

(2) Note that for each \( J_K \in \Omega^{(e)}_K \), we have

\[
\sum_{I_K \in \Omega^{(e)}_K} (I_K - J_K, I_K - J_K) = e - 1
\]

and

\[
\sum_{I_K = (i_1, i_2, \cdots, i_k) \in \Omega^{(e)}_K, \Lambda_K \leq i_1 < \Lambda_K + \frac{f_1}{2}} (I_K - J_K, I_K - J_K) = \sum_{I_K = (i_1, i_2, \cdots, i_k) \in \Omega^{(e)}_K, \Lambda_K + \frac{f_1}{2} \leq i_1 < \Lambda_K + f_1} (I_K - J_K, I_K - J_K).
\]

Therefore, we get the conclusion.

(3) It can be proved similarly to that of Corollary 2.4-(2). \( \Box \)

REFERENCES

[1] K. Arasu, J. Dillon and K. Player, Character sum factorizations yield sequences with ideal two-level autocorrelation, IEEE Trans. Inf. Theory, 61 (2015), 3276–3304.
[2] M. Buratti, Hadamard partitioned difference families and their descendants, Cryptogr. Commun., 11 (2019), 557–562.
[3] M. Buratti, On disjoint \((v, k, k - 1)\) difference families, Des. Codes Cryptogr., 87 (2019), 745–755.
[4] M. Buratti and D. Jungnickel, Partitioned difference families versus zero-difference balanced functions, Des. Codes Cryptogr., 87 (2019), 2461–2467.
[5] M. Cai, J. Yang and C. Wang, From a 1-rotational RBIBD to a partitioned difference family, Electron. J. Comb., 17 (2010), pp. R139.
[6] H. Chang, X. Zhou, Y. Tang and Y. Miao, Zero-difference balanced functions with new parameters and their applications, IEEE Trans. Inf. Theory, 63 (2017), 4379–4387.
[7] Y. Ding and C. Ding, Constructions of external difference families and disjoint difference families, Des. Codes Cryptogr., 40 (2006), 167–185.
[8] W. Chu and C. Colbourn, Optimal frequency-hopping sequences via cyclotomy, IEEE Trans. Inf. Theory, 51 (2005), 1139–1141.
[9] J. Chung and K. Yang, \(k\)-fold cyclotomy and its application to frequency-hopping sequences, IEEE Trans. Inf. Theory, 57 (2011), 2306–2317.
[10] C. Ding, Cyclic codes from cyclotomic sequences of order four, Finite Fields Appl., 23 (2013), 8–34.
[11] C. Ding, Optimal constant composition codes from zero-difference balanced functions, IEEE Trans. Inf. Theory, 54 (2008), 5766–5770.
[12] C. Ding, Optimal and perfect difference systems of sets, J. Comb. Theory, Series A, 116 (2009), 109–119.
[13] C. Ding and Y. Tan, Zero-difference balanced functions with applications, J. Stat. Theory and Practice, 116 (2012), 3–19.
Classes of partitioned difference families

[14] C. Ding and J. Yin, Combinatorial constructions of optimal constant-composition codes, IEEE Trans. Inf. Theory, 51 (2005), 3671–3674.
[15] C. Ding and T. Helleseth, New generalized cyclotomy and its applications, Finite Fields Appl., 4 (1998), 140–166.
[16] C. Ding and T. Helleseth, Generalized cyclotomic codes of length $p_1^{e_1} \cdots p_t^{e_t}$, IEEE Trans. Inf. Theory, 45 (1999), 467–474.
[17] C. Fan and G. Ge, A unified approach to Whiteman’s and Ding-Helleseth’s generalized cyclotomy over residue class rings, IEEE Trans. Inf. Theory, 60 (2014), 1326–1336.
[18] R. Fuji-Hara, Y. Miao and M. Mishima, Optimal frequency hopping sequences: A combinatorial approach, IEEE Trans. Inf. Theory, 50 (2004), 2408–2420.
[19] C. F. Gauss, Disquisitiones Arithmeticae, New York, USA: Springer-Verlag, 1986.
[20] G. Ge, Y. Miao and Z. Yao, Optimal frequency hopping sequences: Auto- and cross-correlation properties, IEEE Trans. Inf. Theory, 55 (2009), 867–879.
[21] B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, Canad. J. Math., 14 (1962), 614–625.
[22] Y. Han and K. Yang, On the Sidelnikov sequences as frequency-hopping sequences, IEEE Trans. Inf. Theory, 55 (2009), 4279–4285.
[23] T. Helleseth and G. Gong, New nonbinary sequences with ideal two-level autocorrelation, IEEE Trans. Inf. Theory, 48 (2002), 2868–2872.
[24] H. Hu, S. Shao, G. Gong and T. Helleseth, The proof of Lin’s conjecture via the decimation-Hadamard transform, IEEE Trans. Inf. Theory, 60 (2013), 5054–5064.
[25] L. Hu and Q. Yue, Gauss periods and codebooks from generalized cyclotomic sets of order four, Des. Codes Cryptogr., 69 (2013), 233–246.
[26] A. Klapper, $d$-form sequence: Families of sequences with low correlation values and large linear spans, IEEE Trans. Inf. Theory, 51 (1995), 1469–1477.
[27] S. Li, H. Wei and G. Ge, Generic constructions for partitioned difference families with applications: A unified combinatorial approach, Des. Codes Cryptogr., 82 (2017), 583–599.
[28] H. A. Lin, From cyclic Hadamard difference sets to perfectly balanced sequences, Ph.D. thesis, University of Southern California, 1998.
[29] J. Liu, Y. Jiang, Q. Zheng and D. Lin, A new construction of zero-difference balanced functions and two applications, Des. Codes Cryptogr., 87 (2019), 2251–2265.
[30] Y. Luo, F. Fu, A. Vinck, and W. Chen, On constant-composition codes over $\mathbb{Z}_q$, IEEE Trans. Inf. Theory, 49 (2003), 3010–3016.
[31] J.-S. No, New cyclic difference sets with Singer parameters constructed from $d$-homogeneous functions, Des. Codes Cryptogr., 33 (2004), 199–213.
[32] T. Storer, Cyclotomy and Difference Sets, Chicago: Markham Pub. Co., 1967.
[33] Q. Wang and Y. Zhou, Sets of zero-difference balanced functions and their applications, Adv. Math. Commun., 8 (2014), 83–101.
[34] X. Wang and J. Wang, Partitioned difference families and almost difference sets, J. Stat. Plan. Inference, 141 (2011), 1899–1909.
[35] A. L. Whiteman, A family of difference sets, Illinois J. Math., 6 (1962), 107–121.
[36] R. M. Wilson, Cyclotomic and difference families in elementary abelian groups, J. Number Theory, 4 (1972), 17–47.
[37] Y. Yang, Z. Zhou and X. Tang, Two classes of zero-difference balanced functions and their optimal constant composition codes, in Proceedings of 2016 IEEE International Symposium on Information Theory, (2016), 1327–1330.
[38] Z. Yi, Z. Lin and L. Ke, A generic method to construct zero-difference balanced functions, Cryptogr. Commun., 10 (2018), 591–609.
[39] J. Yin, X. Shan and Z. Tian, Constructions of partitioned difference families, Eur. J. Comb., 29 (2008), 1507–1519.
[40] X. Zeng, H. Cai, X. Tang, and Y. Yang, Optimal frequency hopping sequences of odd length, IEEE Trans. Inf. Theory, 59 (2013), 3237–3248.
[41] Z. Zha and L. Hu, Cyclotomic constructions of zero-difference balanced functions with applications, IEEE Trans. Inf. Theory, 61 (2015), 1491–1495.
[42] Z. Zhou, X. Tang, D. Wu and Y. Yang, Some new classes of zero-difference balanced functions, IEEE Trans. Inf. Theory, 58 (2012), 139–145.

Received February 2020; revised August 2020.
E-mail address: edzxx1163.com
E-mail address: ljqu_happy@hotmail.com
E-mail address: xwcao@nuaa.edu.cn