

Three New Families of Zero-difference Balanced Functions with Applications

Cunsheng Ding, Qi Wang, and Maosheng Xiong

Abstract

Zero-difference balanced (ZDB) functions integrate a number of subjects in combinatorics and algebra, and have many applications in coding theory, cryptography and communications engineering. In this paper, three new families of ZDB functions are presented. The first construction, inspired by the recent work [1], gives ZDB functions defined on the abelian groups $(\text{GF}(q_1) \times \cdots \times \text{GF}(q_k), +)$ with new and flexible parameters. The other two constructions are based on 2-cyclotomic cosets and yield ZDB functions on \mathbb{Z}_n with new parameters. The parameters of optimal constant composition codes, optimal and perfect difference systems of sets obtained from these new families of ZDB functions are also summarized.

Index Terms

Constant composition codes, cyclotomic cosets, difference system of sets, generalized cyclotomy, zero-difference balanced functions.

I. INTRODUCTION

Let $(A, +)$ and $(B, +)$ be two abelian groups with orders n and ℓ respectively. A function f from A to B is called *zero-difference balanced* (ZDB for short) if

$$|\{x \in A : f(x+a) - f(x) = 0\}| = \lambda,$$

for every nonzero $a \in A$, where λ is a non-negative integer. Let $\text{Im}(f) = \{b_0, b_1, \dots, b_{\bar{\ell}-1}\} \subseteq B$ denote the image set of f and $\bar{\ell} = |\text{Im}(f)|$. Define $A_i := \{x \in A : f(x) = b_i\}$ and $\tau_i = |A_i|$ for $0 \leq i \leq \bar{\ell} - 1$. Let \mathcal{P} be the set of all the preimage sets, i.e., $\mathcal{P} = \{A_0, A_1, \dots, A_{\bar{\ell}-1}\}$. Clearly, \mathcal{P} constitutes a partition of A . Furthermore, by the ZDB property, for each $0 \leq i \leq \bar{\ell} - 1$, the list of differences $a - a'$ with $a, a' \in A_i$ and $a \neq a'$, covers all nonzero elements of A exactly λ times. In this case, the set \mathcal{P} is called an $(n, \{\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}\}, \lambda)$ -*partitioned difference family* (PDF). Because of the connection with PDF, each ZDB function can be identified with parameters $(n, \{\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}\}, \lambda)$ (all these parameters are needed in some applications, see Section IV). We also associate every ZDB function with the three parameters $(n, \bar{\ell}, \lambda)$ since in some cases the parameters $\{\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}\}$ may not be available.

Zero-difference balanced functions were first introduced by Ding in constructing optimal constant composition codes [2] and optimal and perfect difference systems of sets [3]. In the literature, perfect nonlinear functions [8], [11], [15], [19], [20] and difference balanced functions [16], [21] are special types of ZDB functions. ZDB functions unify different subjects in combinatorics, algebra and finite geometry, and they have found applications not only in these three areas but also in communications, coding theory and cryptography. Due to their applications, ZDB functions have received a lot of attention recently. Besides constant composition codes and difference systems of sets, they can also be employed to construct optimal constant weight codes [18], [21] and optimal sets of frequency hopping sequences [9], [10], [18]. In Table I below, we summarize some known ZDB functions with parameters $(n, \bar{\ell}, \lambda)$, and also the parameters $\{\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}\}$ if they are available. In tables below all the variables are positive integers, q is always a prime power, and p_i 's are primes.

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (email: cding@ust.hk).

Q. Wang is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (email: qiwang@ust.hk).

M. Xiong is with the Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (email: mamsxiong@ust.hk).

TABLE I
SOME KNOWN ZDB FUNCTIONS WITH PARAMETERS $(n, \bar{\ell}, \lambda)$

Parameters		Constraints	References
$(n, \bar{\ell}, \lambda)$	$\{\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}\}$		
(p^r, p^s, p^{r-s})		p is a prime, $0 \leq s \leq r$	[15]
(p^2, p, p)	$\{2p-1, p-1, \dots, p-1\}$	p is an odd prime	[3]
$\left(\frac{q^r-1}{N}, q, \frac{q^{r-1}-1}{N}\right)$		$N (q-1)$, and $\gcd(N, r) = 1$	[2], [3]
$(q^2+1, q, q+1)$		$q = 2^s, s \geq 1$	[2]
$(q-1, d, \frac{q-d}{d})$	$\{\frac{q}{d}-1, \frac{q}{d}, \dots, \frac{q}{d}\}$	$d q$	[4]
$(q^r-1, q^s, q^{r-s}-1)$		$1 \leq s \leq r$	[21]
$\left(t \frac{q^r-1}{N}, q^s, t \frac{q^{r-s}-1}{N}\right)$		$N (q-1)$, and $\gcd(N, r) = 1$ $1 \leq t \leq N, 1 \leq s \leq r$	[21]
$(n, \frac{n+e-1}{e}, e-1)$	$\{1, e, \dots, e\}$	$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, 2 < p_1 < p_2 < \dots < p_k$ and $e (p_i-1)$ for $1 \leq i \leq k$	[1]
$(n, \frac{n+e-1}{e}, e-1)$	$\{1, e, \dots, e\}$	$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, p_1 < p_2 < \dots < p_k$ and $e (p_i^{m_i}-1)$ for $1 \leq i \leq k$	Theorem 1
$(2^m-1, \frac{2^m+m-2}{m}, m-1)$	$\{1, m, \dots, m\}$	m is a prime	Theorem 2
$(2^m-1, \frac{2^{m-1}+m-1}{m}, 2m-1)$	$\{1, 2m, \dots, 2m\}$	m is an odd prime	Theorem 3

Very recently, in [1], Cai, Zeng, Hellesteth, Tang, and Yang constructed $(n, (n+e-1)/e, e-1)$ -ZDB functions on $(\mathbb{Z}_n, +)$, where n is odd and has the canonical factorization

$$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, \quad 2 < p_1 < p_2 < \dots < p_k,$$

and $e > 1$ such that $e|(p_i-1)$ for all $1 \leq i \leq k$. Their construction employs the tool of generalized cyclotomy in the rings \mathbb{Z}_n , and generates many ZDB functions with new parameters.

In this paper, inspired by the idea of [1] and utilizing generalized cyclotomy in the rings $\text{GF}(p_1^{m_1}) \times \dots \times \text{GF}(p_k^{m_k})$, we construct $(n, (n+e-1)/e, e-1)$ -ZDB functions on the abelian groups $(\text{GF}(p_1^{m_1}) \times \dots \times \text{GF}(p_k^{m_k}), +)$, with

$$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, \quad p_1 < p_2 < \dots < p_k,$$

and $e > 1$ such that $e|(p_i^{m_i}-1)$ for all $1 \leq i \leq k$.

One aspect of difference between [1] and our construction is that the groups \mathbb{Z}_n are cyclic, while in our case the groups $(\text{GF}(p_1^{m_1}) \times \dots \times \text{GF}(p_k^{m_k}), +)$ are not cyclic in general. This is an advantage of [1] over our construction, because ZDB functions on cyclic groups have more applications than those on noncyclic groups. On the other hand, our construction provides many new and more flexible parameters compared with [1], since in our construction n can be even and the requirement $e|(p_i^{m_i}-1)$ gives more flexibility. For example, take $n = 7^2 \cdot 13^2$, then $\gcd(7^2-1, 13^2-1) = 24$. So for $e > 1$ and $e|24$, we can take $e = 2, 3, 6, 4, 8, 12, 24$. In comparison with the construction in [1], however, since $\gcd(7-1, 13-1) = 6$, the requirement $e > 1$ and $e|6$ only allows us to take $e = 2, 3, 6$. The two constructions may overlap only when $m_1 = \dots = m_k = 1$, i.e., when n is a square-free positive integer.

In addition to this construction, we propose two other families of ZDB functions on the cyclic groups \mathbb{Z}_n with new parameters based on 2-cyclotomic cosets, where $n = 2^m - 1$ for any prime m . It may be noted that these constructions cannot be generalized to p -cyclotomic cosets on \mathbb{Z}_n where $n = p^m - 1$ for $p > 2$.

The rest of the paper is organized as follows. In Section II, we present the first construction of ZDB functions on the groups $(\text{GF}(p_1^{m_1}) \times \dots \times \text{GF}(p_k^{m_k}), +)$. In Section III, we describe the second and third construction of ZDB functions on the groups $(\mathbb{Z}_n, +)$. In Section IV, we summarize some applications of the ZDB functions. In Section V, we make some remarks.

II. THE FIRST FAMILY OF $(n, (n+e-1)/e, e-1)$ -ZDB FUNCTIONS ON THE ABELIAN GROUPS $(\text{GF}(p_1^{m_1}) \times \cdots \times \text{GF}(p_k^{m_k}), +)$

The first construction of ZDB functions is described as follows. Let q_1, \dots, q_k be distinct prime powers and let

$$n = q_1 q_2 \cdots q_k.$$

For each i , let $\text{GF}(q_i)$ be a finite field of order q_i and g_i be a generator of the multiplicative group $\text{GF}(q_i)^* := \text{GF}(q_i) \setminus \{0\}$. Consider the ring

$$A = \text{GF}(q_1) \times \text{GF}(q_2) \times \cdots \times \text{GF}(q_k).$$

For each non-empty subset $I \subseteq \{1, \dots, k\}$, let

$$A_I = \left\{ \underline{x} = (x_1, \dots, x_k) \in A : \begin{array}{ll} x_i \in \text{GF}(q_i)^*, & \text{if } i \in I, \\ x_i = 0, & \text{if } i \notin I. \end{array} \right\}$$

Without confusion we may identify A_I with $\prod_{i \in I} \text{GF}(q_i)^*$. Then A_I is a multiplicative group with identity $\underline{1} = (1, \dots, 1)$.

For each $e > 1$ with $e \mid (q_i - 1)$ for all $1 \leq i \leq k$, let

$$q_i - 1 = e \cdot f_i, \quad 1 \leq i \leq k$$

and let $\underline{g}_I \in A_I$ be given by

$$\underline{g}_I = \left(g_i^{f_i} \right)_{i \in I}.$$

Since the order of g_i is $q_i - 1$ for each i , the order of $\underline{g}_I \in A_I$ is e . Let $D_I \subseteq A_I$ be the cyclic subgroup generated by \underline{g}_I , then $|D_I| = e$. Clearly,

$$\left| (D_I - \underline{1}) \cap A_I \right| = e - 1.$$

We can decompose A_I into a disjoint union of left cosets of D_I as

$$A_I = \coprod_{\alpha_I \in R_I} \alpha_I D_I, \tag{1}$$

where $R_I \subseteq A_I$ is a fixed set of representatives for A_I/D_I . We find that

$$|R_I| = |A_I|/|D_I| = \frac{1}{e} \cdot \prod_{i \in I} (q_i - 1).$$

Let

$$\mathcal{S} := \left\{ \alpha_I D_I : \forall \alpha_I \in R_I, \forall \emptyset \neq I \subseteq \{1, \dots, k\} \right\} \cup \{ \{\underline{0}\} \}.$$

The set \mathcal{S} has order $\frac{n-1}{e} + 1$. Let $\eta(\cdot)$ be any bijection from \mathcal{S} to $\mathbb{Z}_{\frac{n-1}{e}+1}$. We define $f : A \rightarrow \mathbb{Z}_{\frac{n-1}{e}+1}$ by

$$f(\underline{x}) = \begin{cases} \eta(\alpha_I D_I) & : \text{ if } \underline{x} \in \alpha_I D_I \text{ for some } \alpha_I \in R_I, \emptyset \neq I \subseteq \{1, \dots, k\}, \\ \eta(\{\underline{0}\}) & : \text{ if } \underline{x} = \underline{0} = (0, \dots, 0). \end{cases}$$

This is well-defined, because each non-zero vector $\underline{x} \in A$ belongs to some $\alpha_I D_I$ for a unique non-empty I , and by the decomposition (1), \underline{x} belongs to some $\alpha_I D_I$ for a unique $\alpha_I \in R_I$. Since $|\alpha_I D_I| = e$ for each $\alpha_I \in R_I$, it is easily seen that the sizes of the preimage sets of f are $\{1, e, \dots, e\}$.

Theorem 1. *The function f defined above is an $(n, \frac{n+e-1}{e}, e-1)$ -ZDB function from A onto $\mathbb{Z}_{\frac{n-1}{e}+1}$.*

Proof: For each $\underline{a} = (a_i)_i \in A \setminus \{\underline{0}\}$, we may assume that $\underline{a} \in A_I$ for a unique non-empty set $I \subseteq \{1, \dots, k\}$. By definition, $f(\underline{x} + \underline{a}) = f(\underline{x})$ if and only if \underline{x} and $\underline{x} + \underline{a}$ belong to the same set in \mathcal{S} .

This implies that $\underline{x} \neq \underline{0}$. Say $\underline{x} = (x_i)_i$ and $\underline{x} + \underline{a} = (x_i + a_i)_i$ belong to the same set $\alpha D_{I'}$ for some $\alpha = (\alpha_i)_i \in R_{I'}$ and some non-empty set I' . This means that there exist $0 \leq t, s \leq e-1$ such that

$$\begin{aligned} x_i &= \alpha_i g_i^{f_i t}, & x_i + a_i &= \alpha_i g_i^{f_i s} & \forall i \in I', \\ x_i &= 0, & x_i + a_i &= 0 & \forall i \notin I'. \end{aligned}$$

In particular, we have $a_i = 0$ for all $i \notin I'$, hence $I \subseteq I'$. If $I' \neq I$, then we can find $i_1 \in I' \setminus I$, and $a_{i_1} = 0$ since $\underline{a} \in A_I$, and

$$x_{i_1} = \alpha_{i_1} g_{i_1}^{f_{i_1} t} = x_{i_1} + a_{i_1} = \alpha_{i_1} g_{i_1}^{f_{i_1} s}.$$

This implies that

$$\alpha_{i_1} g_{i_1}^{f_{i_1} t} = \alpha_{i_1} g_{i_1}^{f_{i_1} s} \implies t = s.$$

Thus we find $a_i = 0$ for all $i \in I'$. We already know that $a_i = 0$ for all $i \notin I'$. This means $\underline{a} = \underline{0}$, a contradiction. Therefore we must have $I' = I$ where $\underline{a} \in A_I$. So

$$\begin{aligned} & |\{\underline{x} \in A : f(\underline{x} + \underline{a}) = f(\underline{x})\}| \\ &= \sum_{\emptyset \neq I' \subseteq \{1, \dots, k\}} |\{\underline{x} \in A_{I'} : f(\underline{x} + \underline{a}) = f(\underline{x})\}| \\ &= |\{\underline{x} \in A_I : f(\underline{x} + \underline{a}) = f(\underline{x})\}| \\ &= \sum_{\alpha \in R_I} |\alpha D_I \cap (\alpha D_I - \underline{a})|. \end{aligned}$$

Every element in the set $\alpha D_I \cap (\alpha D_I - \underline{a})$ corresponds one-to-one to unique $\underline{x}, \underline{y} \in D_I$ such that $\alpha \underline{x} - \underline{a} = \alpha \underline{y}$, or equivalently $\underline{1} - \underline{a} \alpha^{-1} \underline{x}^{-1} = \underline{x}^{-1} \underline{y}$ with $\underline{x}^{-1}, \underline{x}^{-1} \underline{y} \in D_I$. Here for $\underline{x} \in A_I$, \underline{x}^{-1} denotes the multiplicative inverse of \underline{x} in A_I . So we have

$$|\alpha D_I \cap (\alpha D_I - \underline{a})| = |D_I \cap (\underline{1} - \underline{a} \alpha^{-1} D_I)| = |(D_I - \underline{1}) \cap (-\underline{a} \alpha^{-1}) D_I|.$$

It is easy to observe that as α runs over R_I , a set of representatives for A_I/D_I , the element $-\underline{a} \alpha^{-1}$ will also run over a set of representatives for A_I/D_I . Therefore we obtain

$$|\{\underline{x} \in A : f(\underline{x} + \underline{a}) = f(\underline{x})\}| = \sum_{\alpha \in R_I} |(D_I - \underline{1}) \cap \alpha D_I| = |(D_I - \underline{1}) \cap A_I| = e - 1.$$

This completes the proof of Theorem 1. ■

III. TWO MORE FAMILIES OF ZDB FUNCTIONS ON $(\mathbb{Z}_n, +)$ FROM 2-CYCLOTOMIC COSETS MODULO n

In this section, employing 2-cyclotomic cosets modulo $n = 2^m - 1$, we present two families of ZDB functions on $(\mathbb{Z}_n, +)$ with new parameters. The ZDB functions in one family have parameters $(2^m - 1, (2^m + m - 2)/m, m - 1)$, and those in the other family have parameters $(2^m - 1, (2^{m-1} + m - 1)/m, 2m - 1)$. Furthermore, the parameters $\{\tau_0, \tau_1, \dots, \tau_{\ell-1}\}$, i.e., the sizes of the preimage sets, of the ZDB functions are also determined.

Let $n = 2^m - 1$. The 2-cyclotomic coset modulo n containing i is defined by

$$\{i, i \times 2 \bmod n, i \times 2^2 \bmod n, \dots, i \times 2^{\ell_i} \bmod n\} \subset \mathbb{Z}_n,$$

where ℓ_i is the least positive integer such that $i \equiv i 2^{\ell_i} \pmod{n}$, and is called the size of this 2-cyclotomic coset. The leader of a 2-cyclotomic coset modulo n is the least integer in the 2-cyclotomic coset. Clearly, all the 2-cyclotomic cosets modulo n form a partition of \mathbb{Z}_n . It is noted that $n = 2^m - 1$ may not be a prime when m is a prime. For example, $n = 2^{11} - 1 = 23 \times 89$.

A. The family of $(2^m - 1, (2^m + m - 2)/m, m - 1)$ -ZDB functions on $(\mathbb{Z}_n, +)$

Let m be a prime, and let $n = 2^m - 1$. Since m is a prime, every nonzero 2-cyclotomic coset has size m , and the total number of nonzero 2-cyclotomic cosets modulo n is equal to $(2^m - 2)/m$. Let Γ_m denote the set of all 2-cyclotomic coset leaders. Then

$$|\Gamma_m| = 1 + \frac{2^m - 2}{m} = \frac{2^m + m - 2}{m}.$$

We now define a function f from $(\mathbb{Z}_n, +)$ to itself by

$$f(x) = i_x,$$

where i_x is the coset leader of the 2-cyclotomic coset containing x . Since every nonzero 2-cyclotomic coset has m elements modulo $2^m - 1$, by definition, the sizes of the preimage sets of f form the set $\{1, m, \dots, m\}$.

Theorem 2. *Let m be a prime. Then the function f defined above is a $(2^m - 1, \frac{2^m + m - 2}{m}, m - 1)$ -ZDB function on $(\mathbb{Z}_n, +)$.*

Proof: Note that $|\text{Im}(f)| = |\Gamma_m| = \frac{2^m + m - 2}{m}$. It suffices to prove that for every $a \not\equiv 0 \pmod{2^m - 1}$, the number of x with $1 \leq x \leq 2^m - 1$ such that $x + a$ and x belong to the same 2-cyclotomic set is always $m - 1$. The existence of such an x means that there is an integer k with $1 \leq k \leq m - 1$, such that

$$x + a \equiv 2^k x \pmod{2^m - 1},$$

or equivalently,

$$(2^k - 1)x \equiv a \pmod{2^m - 1}.$$

Since m is a prime and $k < m$, we have

$$\gcd(2^k - 1, 2^m - 1) = 2^{\gcd(k, m)} - 1 = 1.$$

We denote by $\overline{2^k - 1}$ the multiplicative inverse of $2^k - 1$ modulo $2^m - 1$. Thus,

$$x \equiv (\overline{2^k - 1}) \cdot a \pmod{2^m - 1},$$

and this holds for all $1 \leq k \leq m - 1$. It is also clear that $2^k - 1 \not\equiv 2^l - 1 \pmod{2^m - 1}$ for $1 \leq k \neq l \leq m - 1$, hence the number of such x is always $m - 1$. This completes the proof of Theorem 2. ■

B. The family of $(2^m - 1, (2^{m-1} + m - 1)/m, 2m - 1)$ -ZDB functions on $(\mathbb{Z}_n, +)$

Let m be an odd prime and let $n = 2^m - 1$. Same as in Section III-A, let Γ_m denote the set of all 2-cyclotomic coset leaders and further Π_m denote the set of all 2-cyclotomic cosets modulo n . Since m is prime, every nonzero 2-cyclotomic cosets modulo n has the size m and $|\Gamma_m| = 1 + (2^m - 2)/m$. Define

$$\Delta_m = \{B \cup (-B) : B \in \Pi_m\},$$

where $-B = \{n - i : i \in B\}$. Similarly, the leader of any $B \cup (-B)$ is the least integer in this set. It is easy to prove that B and $-B$ are disjoint for each $\{0\} \neq B \in \Pi_m$, and hence

$$|\Delta_m| = 1 + \frac{2^{m-1} - 1}{m} = \frac{2^{m-1} + m - 1}{m}.$$

We now define a function g from $(\mathbb{Z}_n, +)$ to itself by

$$g(x) = j_x,$$

where j_x is the leader of the set $B \cup (-B)$ containing x . Since every nonzero set $B \cup (-B)$ has $2m$ elements, the sizes of the preimage sets of g form the set $\{1, 2m, \dots, 2m\}$.

Theorem 3. *Let m be an odd prime. Then the function g defined above is a $(2^m - 1, \frac{2^{m-1} + m - 1}{m}, 2m - 1)$ -ZDB function on $(\mathbb{Z}_n, +)$.*

Proof: Note that $|\text{Im}(g)| = |\Delta_m| = \frac{2^{m-1} + m - 1}{m}$. We only need to prove that for each $a \not\equiv 0 \pmod{2^m - 1}$, the number of x with $1 \leq x \leq 2^m - 1$ such that $x + a$ belongs to the 2-cyclotomic set that contains either x or $-x$ is always $2m - 1$. The existence of such an x means that there is an integer k with $1 \leq k \leq m - 1$, such that

$$x + a \equiv 2^k x \pmod{2^m - 1}, \quad (2)$$

or there is an integer t with $1 \leq t \leq m$ such that

$$x + a \equiv -2^t x \pmod{2^m - 1}. \quad (3)$$

As for (2), similar to the proof of Theorem 2, the number of solutions for x is $m - 1$. As for (3), we get

$$(2^t + 1)x \equiv -a \pmod{2^m - 1}.$$

Notice that if $t < m$, since m is an odd prime, we have

$$\gcd(2^{2t} - 1, 2^m - 1) = 2^{\gcd(2t, m)} - 1 = 1,$$

and further $\gcd(2^t + 1, 2^m - 1) = 1$. If $t = m$, we have

$$\gcd(2^m + 1, 2^m - 1) = \gcd(2, 2^m - 1) = 1.$$

Hence, $2^t + 1$ is invertible modulo $2^m - 1$ for all $1 \leq k \leq m$. It then follows that the number of x satisfying (3) is m . On the other hand, (2) and (3) can not be satisfied simultaneously, because otherwise we obtain for some $1 \leq k \leq m - 1$, $1 \leq t \leq m$

$$(2^t + 2^k)a \equiv 0 \pmod{2^m - 1}.$$

However, we note that

$$\gcd(2^t + 2^k, 2^m - 1) = 1,$$

implying that $a \equiv 0 \pmod{2^m - 1}$, which is a contradiction to the assumption $a \not\equiv 0 \pmod{2^m - 1}$. Then the total number of x satisfying either (2) or (3) is $2m - 1$. This completes the proof. ■

IV. TWO APPLICATIONS OF THE ZDB FUNCTIONS PRESENTED IN THIS PAPER

In this section, we deal with the applications of the ZDB functions of this paper in constant composition codes and difference systems of sets.

A. Optimal constant composition codes

Let \mathcal{F}_ℓ denote the set $\{0, 1, \dots, \ell - 1\}$ (also called *alphabet*), and let \mathcal{F}_ℓ^n be the set of all n -tuples over \mathcal{F}_ℓ (also called *words*). An $(n, M, d, w)_\ell$ *constant weight code* (CWC) is a code $C \subset \mathcal{F}_\ell^n$ with size M and minimum Hamming distance d such that the Hamming weight of each codeword is w . An $(n, M, d, [w_0, w_1, \dots, w_{\ell-1}])_\ell$ *constant composition code* (CCC) is a code $C \subset \mathcal{F}_\ell^n$ with size M and minimum Hamming distance d such that in every codeword the element i appears exactly w_i times for every $i \in \mathcal{F}_\ell$. An $(n, M, d, [w_0, w_1, \dots, w_{\ell-1}])_\ell$ CCC is called a *permutation code* if $n = \ell$ and $w_i = 1$ for all $i \in \mathcal{F}_\ell$. By definition, constant composition codes are a special class of constant weight codes and permutation codes are a further special class of constant composition codes.

Let $A_\ell(n, d, [w_0, w_1, \dots, w_{\ell-1}])$ denote the maximum size of an $(n, M, d, [w_0, w_1, \dots, w_{\ell-1}])_\ell$ CCC. The following upper bound on the maximum size of a CCC was derived in [14].

Lemma 4. If $nd - n^2 + (w_0^2 + w_1^2 + \dots + w_{\ell-1}^2) > 0$,

$$A_\ell(n, d, [w_0, w_1, \dots, w_{\ell-1}]) \leq \frac{nd}{nd - n^2 + (w_0^2 + w_1^2 + \dots + w_{\ell-1}^2)}. \quad (4)$$

An $(n, M, d, [w_0, w_1, \dots, w_{\ell-1}])_\ell$ constant composition code is said to be *optimal* if the bound of (4) is met. In [2], [6], the link between ZDB functions and optimal CCCs was established, and PDFs and ZDB functions were used to construct optimal CCCs.

Lemma 5. Suppose that f is an $(n, \bar{\ell}, \lambda)$ -ZDB function from an abelian group $(A, +)$ of order n to an abelian group $(B, +)$ of order ℓ and $\text{Im}(f)$ is the image set of f with $|\text{Im}(f)| = \bar{\ell}$. Let $A = \{a_0, a_1, \dots, a_{n-1}\}$ and $\text{Im}(f) = \{b_0, b_1, \dots, b_{\bar{\ell}-1}\}$. Define $\tau_i = |\{x \in A : f(x) = b_i\}|$ for $0 \leq i \leq \bar{\ell} - 1$. Then the code

$$\mathcal{C} = \{(f(a_0 + a_i), \dots, f(a_{n-1} + a_i)) : 0 \leq i \leq n - 1\}$$

is an $(n, n, n - \lambda, [\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}])_{\bar{\ell}}$ CCC over $\text{Im}(f)$ meeting the bound of (4).

TABLE II
SOME KNOWN OPTIMAL CCCS WITH PARAMETERS $(n, M, d, [w_0, w_1, \dots, w_{\ell-1}])_\ell$

Parameters	Constraints	References
$\left(\frac{3^r-1}{2}, \frac{3^r-1}{2}, s, \left[\frac{s-1}{2}, \frac{s-s^{1/2}}{2}, \frac{s+s^{1/2}}{2}\right]\right)_3$	r is odd, $s = 3^{r-1}$	[7]
$(q, q, q - r, [2r - 1, 2, \dots, 2])_r$	$q \equiv 1 \pmod{4}$, $r = \frac{q+3}{4}$	[6]
$(q, q, q - s + 1, [s, \dots, s, 1])_r$	$q \equiv 1 \pmod{s}$, $r = \frac{q+s-1}{s}$	[6]
$(q, q, q - \frac{s-1}{2}, [s, \dots, s, 1, \dots, 1])_r$	$q \equiv 1 \pmod{2s}$ $r = \frac{q-1}{2s} + \frac{q+1}{2}$, s appears $\frac{q-1}{2s}$ times	[6]
$(q(q+1), q^2, q^2, [q+1, \dots, q+1])_q$		[6]
$(q^{2r}, q^{2r}, (q-1)q^{2r-1}, [q^{2r-1} + (q-1)q^{r-1}, q^{2r-1} - q^{r-1}, \dots, q^{2r-1} - q^{r-1}])_q$		[5]
$\left(\frac{q^r-1}{2}, \frac{q^r-1}{2}, \frac{q^r-q^{r-1}}{2}, [\tau_0, \tau_1, \dots, \tau_{q-1}]\right)_q$	q is odd	[5]
$(9s, 9^r, 6 \cdot 9^{r-1}, [5s, 2s, 2s])_3$	$s = \frac{9^r-1}{8}$	[14]
$(8s, 8^r, 6 \cdot 8^{r-1}, [3s, 3s, 2s])_3$	$s = \frac{8^r-1}{7}$	[14]
$(10s, 5^r, 7 \cdot 5^{r-1}, [6s, 2s, 2s])_3$	$s = \frac{5^r-1}{4}$	[14]
$(qt, q^r, q^r, [t, \dots, t])_q$	$t = \frac{q^r-1}{q-1}$	[14]
$\left(qt, q^r, \frac{(q+3)q^{r-1}}{2}, \left[\frac{(q-1)t}{2}, \frac{(q-1)t}{2}, t\right]\right)_3$	$t = \frac{q^r-1}{q-1}$, q is odd	[14]
$\left(\frac{q^r-1}{N}, \frac{q^r-1}{N}, \frac{q^r-q^{r-1}}{N}, [\tau_0, \tau_1, \dots, \tau_{q-1}]\right)_q$	$N (q-1)$, $\gcd(N, r) = 1$	[2]
$(q^2 + 1, q^2 + 1, q^2 - q, [\tau_0, \tau_1, \dots, \tau_{q-1}])_q$	$q = 2^s$, $s \geq 1$	[2]
$(q-1, q-1, q - \frac{q-d}{d} - 1, [\frac{q}{d} - 1, \frac{q}{d}, \dots, \frac{q}{d}])_d$	$d q$	[4]
$(q^r - 1, q^r - 1, q^r - q^{r-s}, [\tau_0, \tau_1, \dots, \tau_{q^s-1}])_{q^s}$	$1 \leq s \leq r$	[21]
$(t \frac{q^r-1}{N}, t \frac{q^r-1}{N}, t \frac{q^r-q^{r-s}}{N}, [\tau_0, \tau_1, \dots, \tau_{q^s-1}])_{q^s}$	$N (q-1)$, $\gcd(N, r) = 1$ $1 \leq t \leq N$, $1 \leq s \leq r$	[21]
$(n, n, n - e + 1, [1, e, \dots, e])_{\frac{n+e-1}{e}}$	$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, $2 < p_1 < p_2 < \dots < p_k$ and $e (p_i - 1)$ for $1 \leq i \leq k$	[1]
$(n, n, n - e + 1, [1, e, \dots, e])_{\frac{n+e-1}{e}}$	$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, $p_1 < p_2 < \dots < p_k$ and $e (p_i^{m_i} - 1)$ for $1 \leq i \leq k$	Theorem 1
$(2^m - 1, 2^m - 1, 2^m - m, [1, m, \dots, m])_{\frac{2^m+m-2}{m}}$	m is a prime	Theorem 2
$(2^m - 1, 2^m - 1, 2^m - 2m, [1, 2m, \dots, 2m])_{\frac{2^m-1+m-1}{m}}$	m is an odd prime	Theorem 3

We remark that every ZDB function corresponds to an optimal CCC using this standard method in Lemma 5. In Table II we summarize some known optimal CCCs with parameters $(n, M, d, [w_0, w_1, \dots, w_{\ell-1}])_\ell$, including the new parameters of the CCCs obtained from the three new families of ZDB functions of this paper.

B. Optimal and perfect difference systems of sets

Difference systems of sets (DSS) were introduced by Levenstein [12] (see also [13]) for the construction of comma-free codes for synchronization. Let n be a positive integer, and let \mathbb{Z}_n be the integer ring modulo n . An $(n, \{\tau_0, \tau_1, \dots, \tau_{\ell-1}\}, \rho)$ *difference system of set* (DSS) is a collection of ℓ disjoint sets $D_i \subseteq \mathbb{Z}_n$ such that $|D_i| = \tau_i$ for all $0 \leq i < \ell$ and the multiset

$$\{*(b - b') \bmod n : b \in D_i, b' \in D_j, i \neq j, 0 \leq i, j \leq \ell - 1\} \quad (5)$$

contains every nonzero element $x \in \mathbb{Z}_n$ at least ρ times. A DSS is called *perfect* if every nonzero element $x \in \mathbb{Z}_n$ is contained exactly ρ times in the multiset of (5). A DSS is said *regular* if all the subsets D_i 's are of the same size.

For the application of DSS to code synchronization, the number

$$r_\ell(n, \rho) = \sum_{i=0}^{\ell-1} |D_i|$$

is required to be as small as possible. A lower bound on $r_\ell(n, \rho)$ is the following [17].

Lemma 6. *For any DSS with parameters $(n, \{\tau_0, \tau_1, \dots, \tau_{\ell-1}\}, \rho)$,*

$$r_\ell(n, \rho) \geq \sqrt{\text{SQUARE} \left(\rho(n-1) + \left\lceil \frac{\rho(n-1)}{\ell-1} \right\rceil \right)}, \quad (6)$$

where $\text{SQUARE}(x)$ denotes the smallest square number that is no less than the positive integer x , and $\lceil x \rceil$ denotes the ceiling function.

A perfect $(n, \{\tau_0, \tau_1, \dots, \tau_{\ell-1}\}, \rho)$ DSS is called *optimal* if the bound of (6) is met. The correspondence between ZDB functions and perfect DSSs was first established in [3] (see also [21]).

Lemma 7. *Suppose that f is an $(n, \bar{\ell}, \lambda)$ -ZDB function from $(\mathbb{Z}_n, +)$ to an abelian group $(B, +)$ of order ℓ and $\text{Im}(f)$ is the image set of f with $|\text{Im}(f)| = \bar{\ell}$. Let $\text{Im}(f) = \{b_0, b_1, \dots, b_{\bar{\ell}-1}\}$. Define $D_i = \{x \in \mathbb{Z}_n : f(x) = b_i\}$, and $\tau_i = |D_i|$ for $0 \leq i \leq \bar{\ell} - 1$. Then the set*

$$\mathcal{D} = \{D_i : 0 \leq i \leq \bar{\ell} - 1\}$$

is an $(n, \{\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}\}, n - \lambda)$ perfect DSS. Furthermore, if $\bar{\ell}\lambda \leq n$, \mathcal{D} is optimal with respect to the bound of (6).

TABLE III
SOME KNOWN OPTIMAL AND PERFECT DSSS WITH PARAMETERS $(n, \{\tau_0, \tau_1, \dots, \tau_{\ell-1}\}, \rho)$

Parameters	Constraints	References
$\left(\frac{q^r-1}{N}, \{\tau_0, \tau_1, \dots, \tau_{q-1}\}, \frac{q^r-q^{r-1}}{N}\right)$	$N (q-1), \gcd(N, r) = 1$	[2]
$(q^2+1, \{\tau_0, \tau_1, \dots, \tau_{q-1}\}, q^2-q)$	$q = 2^s, s \geq 1$	[2]
$(p^2, \{2p-1, p-1, \dots, p-1\}, p^2-p)$	p is a prime	[3]
$(q-1, \{\frac{q}{d}-1, \frac{q}{d}, \dots, \frac{q}{d}\}, q - \frac{q-d}{d} - 1)$	$d q$	[4]
$(q^r-1, \{\tau_0, \tau_1, \dots, \tau_{q^s-1}\}, q^r - q^{r-s})$	$1 \leq s \leq r$	[21]
$(t\frac{q^r-1}{N}, \{\tau_0, \tau_1, \dots, \tau_{q^s-1}\}, t\frac{q^r-q^{r-s}}{N})$	$N (q-1), \gcd(N, r) = 1$ $1 \leq t \leq N, 1 \leq s \leq r$	[21]
$(n, \{1, e, \dots, e\}, n - e + 1)$	$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, 2 < p_1 < p_2 < \dots < p_k$ and $e (p_i - 1)$ for $1 \leq i \leq k, n \geq (e-1)^2$	[1]
$(2^m - 1, \{1, m, \dots, m\}, 2^m - m)$	m is a prime	Theorem 2
$(2^m - 1, \{1, 2m, \dots, 2m\}, 2^m - 2m)$	m is an odd prime, $m \geq 11$	Theorem 3

We emphasize that the DSSs constructed from ZDB functions using Lemma 7 may not be optimal unless the condition $\bar{\ell}\lambda \leq n$ is satisfied. It is easy to check that the DSSs given by the ZDB functions in Theorem 2 are optimal for all primes m , and those constructed by the ZDB functions in Theorem 3 achieve optimality for primes $m \geq 11$.

Note that the group $(\text{GF}(p_1^{m_1}) \times \cdots \times \text{GF}(p_k^{m_k}), +)$ is cyclic only when $m_1 = \cdots = m_k = 1$, that is, $n = p_1 \cdots p_k$ is square-free. The ZDB functions in Theorem 1 can be employed to construct DSSs only when $m_1 = \cdots = m_k = 1$.

In Table III, we summarize the parameters of some known optimal and perfect DSSs, including the parameters of the DSSs obtained from the two families of ZDB functions in Section III.

V. CONCLUDING REMARKS

In this paper, we present three new families of ZDB functions with parameters $\{n, \{\tau_0, \dots, \tau_{\bar{\ell}-1}\}, \bar{\ell}, \lambda\}$. The parameters of optimal constant composition codes, optimal and perfect difference systems of sets obtained from these new families of ZDB functions are also summarized.

As we have seen, with respect to applications in constant composition codes and difference systems of sets, every parameter in the set $\{n, \{\tau_0, \dots, \tau_{\bar{\ell}-1}\}, \bar{\ell}, \lambda\}$ makes a difference. Hence, when comparing the parameters of two ZDB functions, it may be more appropriate to compare not only $n, \bar{\ell}, \lambda$, but also $\tau_0, \tau_1, \dots, \tau_{\bar{\ell}-1}$ as well. Therefore, the parameters of a ZDB function shall not be considered new only when all of the parameters $\{n, \{\tau_0, \dots, \tau_{\bar{\ell}-1}\}, \bar{\ell}, \lambda\}$ of this ZDB function can be obtained by an earlier constructed ZDB function.

ACKNOWLEDGMENTS

Cunsheng Ding's and Maosheng Xiong's researches are supported by the Hong Kong Research Grants Council under Grant (Nos. 600812, Nos. 606211 and SBI12SC05), respectively.

REFERENCES

- [1] H. Cai, X. Zeng, T. Helleseht, X. Tang, and Y. Yang, "A new construction of zero-difference balanced functions and its applications," *IEEE Trans. Inform. Theory*, vol. 59, no. 8, pp. 5008–5015, 2013.
- [2] C. Ding, "Optimal constant composition codes from zero-difference balanced functions," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5766–5770, 2008.
- [3] C. Ding, "Optimal and perfect difference systems of sets," *J. Combin. Theory Ser. A*, vol. 116, no. 1, pp. 109–119, 2009.
- [4] C. Ding and Y. Tan, "Zero-difference balanced functions with applications," *Journal of Statistical Theory and Practice*, vol. 6, no. 1, pp. 3–19, 2012.
- [5] C. Ding and J. Yin, "Algebraic constructions of constant composition codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1585–1589, 2005.
- [6] C. Ding and J. Yin, "Combinatorial constructions of optimal constant-composition codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3671–3674, 2005.
- [7] C. Ding and J. Yuan, "A family of optimal constant-composition codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3668–3671, 2005.
- [8] T. Feng, "A new construction of perfect nonlinear functions using Galois rings," *J. Comb. Designs*, vol. 17, no. 3, pp. 229–239, April 2009.
- [9] G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency-hopping sequences," *J. Combin. Theory Ser. A*, vol. 113, no. 8, pp. 1699–1718, 2006.
- [10] G. Ge, Y. Miao, and Z. Yao, "Optimal frequency hopping sequences: auto- and cross-correlation properties," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 867–879, 2009.
- [11] X.-D. Hou, "Cubic bent functions," *Discrete Mathematics*, vol. 189, nos. 1–3, pp. 149–161, July 1998.
- [12] V. I. Levenšteĭn, "A certain method of constructing quasilinear codes that guarantee synchronization in the presence of errors," *Problemy Peredači Informacii*, vol. 7, no. 3, pp. 30–40, 1971.
- [13] V. I. Levenšteĭn, "Combinatorial problems motivated by comma-free codes," *J. Combin. Des.*, vol. 12, no. 3, pp. 184–196, 2004.
- [14] Y. Luo, F.-W. Fu, A. J. H. Vinck, and W. Chen, "On constant-composition codes over Z_q ," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3010–3016, 2003.
- [15] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in cryptography—EUROCRYPT '91 (Brighton, 1991)*, vol. 547 of *Lecture Notes in Comput. Sci.*, pp. 378–386, Berlin: Springer, 1991.
- [16] A. Pott and Q. Wang, "Difference balanced functions and their generalized difference sets," *arXiv preprint arXiv:1309.7842*, 2013.
- [17] H. Wang, "A new bound for difference systems of sets," *J. Combin. Math. Combin. Comput.*, vol. 58, pp. 161–167, 2006.
- [18] Q. Wang and Y. Zhou, "Sets of zero-difference balanced functions and their applications," *arXiv preprint arXiv:1208.1878*, 2012.

- [19] X. Zeng, H. Guo, and J. Yuan, "A note of perfect nonlinear functions," in *Cryptography and Network Security*, vol. 4301 of *Lecture Notes in Comput. Sci.*, pp. 259–269, Berlin: Springer, 2006.
- [20] Z. Zha, G. M. Kyureghyan, X. Wang, "Perfect nonlinear binomials and their semifields," *Finite Fields Appl.*, vol. 15, no. 2, pp. 125–133, April 2009.
- [21] Z. Zhou, X. Tang, D. Wu, and Y. Yang, "Some new classes of zero-difference balanced functions," *IEEE Trans. Inform. Theory*, vol. 58, no. 1, pp. 139–145, 2012.