Commun. Korean Math. Soc. **31** (2016), No. 1, pp. 41–52
http://dx.doi.org/10.4134/CKMS.2016.31.1.041

ON GENERALIZED ZERO-DIFFERENCE BALANCED FUNCTIONS

Lin Jiang and Qunying Liao

Abstract. In the present paper, by generalizing the definition of the zero-difference balanced (ZDB) function to be the G-ZDB function, several classes of G-ZDB functions are constructed based on properties of cyclotomic numbers. Furthermore, some special constant composition codes are obtained directly from G-ZDB functions.

1. Introduction and backgrounds

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].

Definition 1.1 ([2, 3])**.** Let $(A, +)$ and $(B, +)$ be two abelian groups of order n and l respectively. A function f from A to B is called zero-difference balanced (ZDB for short) if there exists a non-negative integer λ, such that

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

for every nonzero $a \in A$. We also call the function f to be an (n, λ)-ZDB function. Sometimes we also call f to be a ZDB function with the parameters (n, λ).

For convenience, throughout the paper, we follow the notations defined in [5].

- $\mathrm{Im}(f) = \{b_0, \ldots, b_{\bar{l}-1}\} \subseteq B$ denotes the image set of f and $\bar{l} = |\mathrm{Im}(f)|$;
- $A^{'} = \{x \in A \mid f(x) = b_i\}$ and $\tau_i = |A^{'}|$ for $0 \le i \le \bar{l} - 1$;
- $\mathcal{P} = \{A^{'}, \ldots, A^{'}_{-1}\}$ denotes the set of all the preimage sets, clearly, $\mathcal{P}$ constitutes a partition of A.

Received April 7, 2015; Revised November 1, 2015.
2010 *Mathematics Subject Classification.* 06E30, 05B10, 94B25.
Key words and phrases. zero-difference balanced (ZDB) function, generalized ZDB function, cyclotomic coset, difference system of sets, constant composition code.
This research is supported by the Natural Science Foundation of China with No.11401408, Sichuan Province Foundation of China with No.14ZA0034.

Furthermore, by the ZDB property, for each i $(0 \le i \le \bar{l}-1)$, the list of differences $a-a'$ with $a, a' \in A$ and $a \neq a'$, covers all nonzero elements of A exactly λ times. In this case, the set $\mathcal{P}$ is called an $(n, \{\tau_0, \ldots, \tau_{\bar{l}-1}\}, \lambda)$-partitioned difference family (PDF). Because of the connection with PDF, each ZDB function can be identified with parameters $(n, \{\tau_0, \ldots, \tau_{\bar{l}-1}\}, \lambda)$ (all these parameters are needed in some applications), we also associate every ZDB function with the three parameters $(n, \overline{l}, \lambda)$ since in some cases the parameters $\{\tau_0, \ldots, \tau_{\bar{l}-1}\}$ may not be available.

It is well known that perfect nonlinear functions [7, 8, 12, 16, 17] and difference balanced functions [13, 18] are special types of ZDB functions. ZDB functions unify different subjects in combinatorics, algebra and finite geometry, and they have been found applications not only in these three areas but also in communications, coding theory and cryptography.

For the case $\gcd(n, \lambda) = 1$, many (n, λ)-ZDB functions are constructed [1, 2, 3, 4, 5, 18]. For $\gcd(n, \lambda) \neq 1$, Luo, et al. [11] constructed ZDB functions with parameters (p^r, p^s) $(0 \le s \le r)$, where p is a prime. Recently, by using cyclotomic cosets, Ding, et al. [5] constructed ZDB functions with parameters $(2^m-1, (2^m+m-2)/m, m-1)$ (m is a prime), $(2^m-1, (2^{m-1}+m-1)/m, 2m-1)$ (m is an odd prime), or $(n, (n+e-1)/e, e-1)$, where p_i $(1 \le i \le k)$ are distinct primes, $n = \prod_i^k p_i^{m_i}$ and $e \mid \gcd(p_1^{m_1}-1, \ldots, p_k^{m_k}-1)$.

On the other hand, let $F_l = \{0, \ldots, l-1\}$ be the l-alphabet, and F_l^n be the set of all n-tuples over F_l. An $(n, M, d, [w_0, \ldots, w_{l-1}])_l$ constant composition code (CCC) is a code over F_l^n with size M and minimum Hamming distance d such that in every codeword the element i appears exactly w_i times for every $i \in F_l$. Furthermore, let $A_l(n, M, d, [w_0, \ldots, w_{l-1}])_l$ denote the maximum size of an $(n, M, d, [w_0, \ldots, w_{l-1}])_l$-CCC, the following upper bound for the maximum size of a CCC is given [11].

Lemma 1.2 ([11]). *If* $nd - n^2 + \sum_{i=0}^{l-1} w_i^2 > 0$, *then*

$$A_l(n, M, d, [w_0, \ldots, w_{l-1}])_l \le \frac{nd}{nd - n^2 + \sum_{i=0}^{l-1} w_i^2}.$$

An $(n, M, d, [w_0, \ldots, w_{l-1}])_l$ constant composition code is optimal when the bound of Lemma 1.2 is achieved. In [2, 6], the link between ZDB functions and optimal CCCs is established.

Lemma 1.3 ([2, 6]). *Suppose that f is an $(n, \overline{l}, \lambda)$-ZDB from an abelian group $(A, +)$ of order n to an abelian group $(B, +)$ of order l, and $\mathrm{Im}(f)$ is the image set of f with $|\mathrm{Im}(f)| = \overline{l}$. Let $A = \{a_0, \ldots, a_{n-1}\}$ and $\mathrm{Im}(f) = \{b_0, \ldots, b_{\overline{l}-1}\}$. Define $\tau_i = |\{x \in A : f(x) = b_i\}$ for $0 \le i \le \overline{l}-1$. Then the code*

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

is an $(n, n, n-\lambda, [\tau_0, \ldots, \tau_{\overline{l}-1}])_{\overline{l}}$-CCC over $\mathrm{Im}(f)$ meeting the bound of Lemma 1.2, which means that such code is optimal.

Besides, it is well known that difference systems of sets (DSS) are introduced by Levenstein [9, 10] for the construction of comma-free codes for synchronization. An $(n, [\tau_0, \ldots, \tau_l - 1], \rho)$ 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 $0 \leq i < l$ and the multiset

$$\{*(b - b') \pmod n : b \in D_i,\ b' \in D_j,\ i \neq j,\ 0 \leq i, j \leq l - 1*\} \tag{1.1}$$

contains every nonzero $x \in \mathbb{Z}_n$ 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 above multiset. For applications of DSS to the code synchronization, the number $r_l(n, \rho) = \sum_{i=0}^{l-1} |D_i|$ is required to be as small as possible.

Lemma 1.4 ([14]). *For any DSS with parameters $(n, [\tau_0, \ldots, \tau_l - 1], \rho)$,*

$$r_l(n, \rho) \geq \sqrt{SQUARE\left(\rho(n-1) + \left\lceil \frac{\rho(n-1)}{l-1} \right\rceil\right)},$$

where $SQUARE(x)$ denotes the smallest square number no less than the positive integer x, and $\lceil x \rceil$ denotes the ceiling function. In particular, a DSS is called optimal when the lower bound is achieved.

The correspondence between ZDB functions and perfect DSSs is first established in [2].

Lemma 1.5 ([2]). *Suppose that f is an $(n, \overline{l}, \lambda)$-ZDB function from an abelian group $(A, +)$ of order n to an abelian group $(B, +)$ of order l, and $\mathrm{Im}(f)$ is the image set of f with $|\mathrm{Im}(f)| = \overline{l}$. Define $D_i = \{x \in \mathbb{Z}_n : f(x) = b_i\}$ and $\tau_i = |D_i|$ for $0 \leq i \leq \overline{l} - 1$. Then the set*

$$\mathcal{D} = \{D_i : 0 \leq i \leq \overline{l} - 1\}$$

is an $(n, [\tau_0, \ldots, \tau_{\overline{l}-1}], n - \lambda)$ perfect DSS. Furthermore, if $\overline{l}\lambda \leq n$, then $\mathcal{D}$ is optimal.

In the present paper, we generalize the definition of ZDB functions to the general G-ZDB functions, and then give two constructions for G-ZDB functions (Sections 2-3), which generalize the main results in [5]. Furthermore we obtain some constant composition codes and difference systems of sets directly from G-ZDB functions (Section 4), which also generalize the main results in [2, 5, 6].

2. Generalized ZDB functions and p-cyclotomic sets

This section generalizes the definition of ZDB functions to be the G-ZDB function as follows.

Definition 2.1. Let $(A, +)$ and $(B, +)$ be two abelian groups of order n and l, respectively. A function f from A to B is called generalized zero-difference balanced (G-ZDB for short) if there exists a non-empty S, such that

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

for every nonzero $a \in A$. We also call the function f to be an (n, S) (or $(n, \bar{l}, S)$)-G-ZDB function, where $\bar{l}$ is defined as above. Then ZDB functions are the special G-ZDB functions.

For any prime p, basing on p-cyclotomic cosets, we can construct several classes of G-ZDB functions and improve the constructions of ZDB functions in [5] from the even prime case $p = 2$ to the general prime cases. Furthermore, some constant composition codes (CCC) are constructed from G-ZDB functions.

Before giving our main results, we need to introduce the definition of the p-cyclotomic coset first, where p is a prime.

Let p be a prime, m be a positive integer and $n = p^m - 1$. Suppose that

$$A_i = \{i, i \times p \pmod{p^m - 1}, \ldots, i \times p^{l_i - 1} \pmod{p^m - 1}\} \subseteq \mathbb{Z}_n,$$

is the p-cyclotomic coset modulo n containing i, where l_i is the least positive integer such that $i \equiv i \times p^{l_i} \pmod{p^m - 1}$ and is called the size of this p-cyclotomic coset. The leader of a p-cyclotomic coset modulo n is the least integer in the p-cyclotomic coset. Then we have the following result.

Lemma 2.2. (1) *All the p-cyclotomic cosets modulo n form a partition of $\mathbb{Z}_n$.*

(2) *If m is a prime, then every nonzero p-cyclotomic coset has size m or 1, and the total number of nonzero p-cyclotomic cosets modulo n is $p - 2 + \frac{p^m - p}{m}$.*

(3) *If m is a prime, then every nonzero 2-cyclotomic coset has size m, and the total number of nonzero 2-cyclotomic cosets modulo n is $\frac{2^m - 2}{m}$.*

Proof. (1) It is easy to see that $A_0 = \{0\}$ and $\mathbb{Z}_n = \cup_{i \in \mathbb{Z}_n} A_i$. Now for any i and j with $1 \leq i \neq j \leq p^m - 2$, if there exists some $x \in A_i \cap A_j$, then $i \cdot p^t \equiv j \cdot p^s \pmod{p^m - 1}$ for some t and s with $0 \leq t, s \leq m - 1$. From $i \neq j$ we know that $t \neq s$. Without loss of generality, set $s = t + k$ $(1 \leq k \leq m - 1)$, then we can get $i \equiv j \cdot p^k \pmod{p^m - 1}$, thus $i \in A_j$, i.e., $A_i \subseteq A_j$. Now from the definition of the leader of the cyclotomic coset, we can obtain $i = j$, this is a contradiction. Therefore the sets A_i are disjoint to each others, which means that all the p-cyclotomic cosets modulo n form a partition of $\mathbb{Z}_n$.

(2) From $p^m \equiv 1 \pmod{n}$ we know that for any $i, |A_i| \leq m$. Now for any i $(1 \leq i \leq p^m - 2)$, we consider the size of the coset A_i. This reduces to compute the least integer l_i such that $i \cdot p^{l_i} \equiv i \pmod{p^m - 1}$, equivalently, $p^m - 1 \mid i \cdot (p^{l_i} - 1)$. Note that m is a prime and $1 \leq l_i \leq m$, thus

$$\gcd(p^m - 1, p^{l_i} - 1) = p^{\gcd(m, l_i)} - 1 = \begin{cases} p - 1, & \text{if } 1 \leq l_i \leq m - 1; \\ p^m - 1, & l_i = m, \end{cases}$$

this means that

$$l_i = \begin{cases} 1, & \text{if } \frac{p^m - 1}{p - 1} | i; \\ m, & \text{otherwise.} \end{cases}$$

Then for any $i = 1, \ldots, p^m - 2$, we have

$$|A_i| = \begin{cases} 1, & \text{if } \frac{p^m - 1}{p - 1} | i; \\ m, & \text{otherwise.} \end{cases}$$

This means that every nonzero p-cyclotomic coset A_i has size 1 or m, depending on $\frac{p^m-1}{p-1} \mid i$ or not, respectively. Note that $A_i = \{0\}$ if and only if $i = 0$, and the number of i $(1 \le i \le p^m - 2)$ satisfying $\frac{p^m-1}{p-1} \mid i$ is $p-2$. Hence the total number of nonzero p-cyclotomic cosets modulo n is

$$p - 2 + \frac{(p^m - 2) - (p - 2)}{m} = p - 2 + \frac{p^m - p}{m}.$$

(3) If $p = 2$, then for any i $(1 \le i \le 2^m - 2)$, we consider the least integer l_i such that $i \cdot 2^{l_i} \equiv i \pmod{2^m - 1}$, i.e., $2^m - 1 \mid i \cdot (2^{l_i} - 1)$. Note that m is a prime and $1 \le l_i \le m$, thus

$$\gcd(2^m - 1, 2^{l_i} - 1) = 2^{\gcd(m,l_i)} - 1 = \begin{cases} 1, & 1 \le l_i \le m-1; \\ 2^m - 1, & l_i = m. \end{cases}$$

Now from $1 \le l_i \le m-1$ and $2^m - 1 \mid i \cdot (2^{l_i} - 1)$, we have $2^m - 1 \mid i$, namely, $i \ge 2^m - 1$, which is a contradiction. Therefore, for any i $(1 \le i \le 2^m - 2)$, we can obtain $l_i = m$, and so $|A_i| = m$. This means that every nonzero 2-cyclotomic coset A_i has size m. Note that $A_i = \{0\}$ if and only if $i = 0$, hence the total number of nonzero 2-cyclotomic cosets modulo n is $\frac{2^m-2}{m}$.

Thus we complete the proof of Lemma 2.2. □

3. The constructions for two classes of G-ZDB functions

Before giving our main results and their proves, the following two lemmas are needed.

Lemma 3.1 ([15]). *Suppose that $a, n_1, n_2 \in \mathbb{Z}^+$, $n_1 \ne n_2$, then*

(1) $\gcd(a^{n_1} - 1, a^{n_2} - 1) = a^{\gcd(n_1,n_2)} - 1$;

(2) $\gcd(a^{n_1} - (-1)^{\frac{n_1}{(n_1,n_2)}}, a^{n_2} - (-1)^{\frac{n_2}{(n_1,n_2)}}) = a^{\gcd(n_1,n_2)} + 1$;

(3) *otherwise,*

$$\gcd(a^{n_1} \pm 1, a^{n_2} \pm 1) = \begin{cases} 1, & \text{if } 2 \mid a, \\ 2, & \text{if } 2 \nmid a. \end{cases}$$

Lemma 3.2 ([15]). *Suppose that m_1 and m_2 are both two positive integer numbers, b_1 and b_2 are both integer numbers, then the congruence*

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

has solutions if and only if $\gcd(m_1, m_2) \mid b_1 - b_2$. *Furthermore when the congruence has solutions, it has unique solution modulo* $\mathrm{lcm}[m_1, m_2]$.

Basing on the properties for p-cyclotomic sets, this section generalizes the main results in [5] and constructs two classes of G-ZDB functions (Theorems 3.1-3.2).

Theorem 3.1. *For any two prime p and m, there exists a G-ZDB function with the parameters*

$$(p^m-1, p-1+\frac{p^m-p}{m}, \{(m-1)(p-1), 0\}).$$

Proof. Let $n = p^m - 1$ and Γ_m be the set of all leaders of p-cyclotomic cosets modulo n. Since p and m are both primes, from (2) of Lemma 2.2, we have

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

Now we define a function f from $(\mathbb{Z}_n, +)$ to itself by $f(x) = i_x$, where i_x is the leader of the p-cyclotomic coset containing x. By (2) of Lemma 2.2, every nonzero p-cyclotomic coset has 1 or m element(s) modulo $n = p^m - 1$, and there are exactly $p - 2$ nonzero cosets with only one element, hence the sizes of the preimage sets of f form the set $\{1, \ldots, 1, m, \ldots, m\}$. Therefore $|\mathrm{Im}(f)| = |\Gamma_m| = p - 1 + \frac{p^m-p}{m}$.

On the other hand, for any given $a \neq 0 \pmod{p^m - 1}$, if there exists some x $(1 \leq x \leq p^m - 1)$ such that $f(x + a) = f(x)$, i.e., both $x + a$ and x belong to the same p-cyclotomic coset A_i, then $\frac{p^m-1}{p-1} \nmid i$. Otherwise, by the proof of (2) of Lemma 2.2, such A_i includes only one element, and so $x + a = x$, i.e., $a = 0$, this is a contradiction. Hence $x \in A_i$ with $|A_i| = m$, and so there exists some k with $1 \leq k \leq m - 1$ satisfying $x + a \equiv p^k x \pmod{p^m - 1}$, equivalently,

$$(p^k - 1)x \equiv a \pmod{p^m - 1}. \tag{3.1}$$

Note that m is a prime and $1 \leq k \leq m - 1$, thus from (1) of Lemma 3.1, we have $\gcd(p^k - 1, p^m - 1) = p - 1$. Hence (3.1) has solutions if and only if $p - 1 \mid a$. In this case, (3.1) is equivalent to

$$x \equiv \frac{a}{p^k - 1} \pmod{\frac{p^m - 1}{p - 1}}.$$

Therefore the size of the set $\{x \in \mathbb{Z}_n \mid f(x + a) = f(x)\}$ is $(m - 1)(p - 1)$ for any nonzero $a \in \mathbb{Z}_n$ with $p - 1 \mid a$.

Otherwise, i.e., congruence (3.1) has no solutions. Therefore the size of the set $\{x \in \mathbb{Z}_n \mid f(x + a) = f(x)\}$ is 0 for any nonzero $a \in \mathbb{Z}_n$ with $p - 1 \nmid a$.

Hence by Definition 2.1 of the G-ZDB function, the function f defined above is a G-ZDB function on $(\mathbb{Z}_n, +)$ with the parameters $(p^m - 1, p - 1 + \frac{p^m-p}{m}$, $\{(m - 1)(p - 1), 0\})$.

This completes the proof of Theorem 3.1. □

Theorem 3.2. *For any prime p and odd prime m, there exists a G-ZDB function with the parameters $(2^m - 1, (2^{m-1} + m - 1)/m, \{2m - 1\})$ $(p = 2)$, or $(p^m - 1, \frac{p+1}{2} + \frac{p^m-p}{2m}, \{mp - p + m + 1, 2m, 0\})$ $(p \geq 3)$.*

Proof. Let $n = p^m - 1$, $\prod_m$ be the set of all p-cyclotomic cosets modulo n, and

$$\Delta_m = \left\{ B \cup (-B) \mid B \in \prod_m \right\},$$

where $-B = \{n - i \mid i \in B\}$. Let Γ_m as defined in the proof of Theorem 3.1.

Now similarly to the proof of Theorem 3.1, for any $B \in \prod_m$, the leader of $B \cup (-B)$ is the least integer in this set. It is easy to see that B and $-B$ are disjoint to each other when $\{0\} \neq B \in \prod_m$ or $\frac{p^m-1}{2} \notin B$ with the odd prime p. Note that for any $i = 1, \ldots, p^m - 2$, we have $\frac{p^m-1}{p-1} \mid i$ if and only if $\frac{p^m-1}{p-1} \mid n-i$, and $\frac{p^m-1}{p-1} \mid \frac{p^m-1}{2} \Leftrightarrow 2 \nmid p$. Hence we have the following two cases.

(I) For the case $p = 2$, we know that B and $-B$ are disjoint for each $\{0\} \neq B \in \prod_m$. Thus by (3) of Lemma 2.2 we can get $|\Gamma_m| = 1 + \frac{2^m-2}{m}$. Hence $|\Delta_m| = 1 + \frac{2^m-2}{2m} = \frac{2^{m-1}-1+m}{m}$.

Now we define the 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, hence the sizes of the preimage sets of g is the set $\{1, 2m, \ldots, 2m\}$. Thus $|\mathrm{Im}(g)| = |\Delta_m| = \frac{2^{m-1}-1+m}{m}$.

Note that for any nonzero element $a \in \mathbb{Z}_n$, if there exists some x such that $1 \leq x \leq 2^m - 1$ and $g(x + a) = g(x)$, which means that $x + a$ belongs to the 2-cyclotomic coset B containing either x or $-x$. Note that for B with $\frac{2^m-1}{2} \in B$, we have $|B| = 1$ and $B = -B$. Hence the existence of such x means that there exists some B such that $\frac{2^m-1}{2} \notin B$ and $B \neq \{0\}$, and so there is some integer k with $1 \leq k \leq m - 1$, such that

$$x + a \equiv 2^k x \pmod{2^m - 1}, \tag{3.2}$$

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

$$x + a \equiv -2^t x \pmod{2^m - 1}. \tag{3.3}$$

As for (3.2), similarly to the proof of Theorem 3.1, the number of solutions for x is $m-1$. As for (3.3), note that m is an odd prime and $1 \leq t \leq m$, hence from (3) of Lemma 3.1, we have $\gcd(2^t + 1, 2^m - 1) = 1$ and then (3.3) is equivalent to

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

Therefore the size of the set $\{x \in \mathbb{Z}_n \mid g(x + a) = g(x)\}$ is m for any nonzero $a \in \mathbb{Z}_n$.

On the other hand, suppose that x is a solution both for (3.2) and (3.3), then from Lemma 3.2, there are some k $(1 \leq k \leq m - 1)$ and t $(1 \leq t \leq m)$ such that

$$2^m - 1 \mid \frac{a}{2^k - 1} + \frac{a}{2^t + 1},$$

equivalently, $(2^m - 1)(2^k - 1)(2^t + 1) \mid (2^k + 2^t)a$. Then we have

$$2^m - 1 \mid a(2^{|k-t|} + 1).$$

Note that m is a prime and $|k-t| < m$, thus from (3) of Lemma 3.1, we have $\gcd(2^m-1, 2^{|k-t|}+1) = 1$, and then $2^m - 1 \mid a$, this is a contradiction. Thus the total number of x satisfying either (3.2) or (3.3) is $(m-1)+m = 2m-1$.

From the above, when $p = 2$ one can get G-ZDB functions with the parameters

$$(2^m - 1, (2^{m-1} + m - 1)/m, \{2m-1\}).$$

(II) For the case $p \geq 3$, we have $\frac{p^m-1}{p-1} \mid \frac{p^m-1}{2}$. From the proof of (2) of Lemma 2.2, we know that if $\frac{p^m-1}{2} \in B$, then $|B| = 1$ and $B = -B$. Therefore there are another $p-3$ nonzero cosets B such that $|B| = 1$ and $B \neq -B$. Hence

$$|\Delta_m| = 2 + \frac{p-3}{2} + \frac{p^m - 1 - (p-1)}{2m} = \frac{p+1}{2} + \frac{p^m - p}{2m}.$$

Now we define the function h from $(\mathbb{Z}_n, +)$ to itself by $h(x) = s_x$, where s_x is the leader of the set $B \cup (-B)$ containing x. Since every nonzero set $B \cup (-B)$ with $\frac{p^m-1}{2} \notin B$ has $2m$ elements, the sizes of the preimage sets of h form the set $\{1, 1, 2, \ldots, 2, 2m, \ldots, 2m\}$. And so $|\mathrm{Im}(h)| = |\Delta_m| = \frac{p+1}{2} + \frac{p^m-p}{2m}$.

Note that for any nonzero element $a \in \mathbb{Z}_n$, if there exists some x such that $1 \leq x \leq p^m - 1$ and $h(x+a) = h(x)$, which means that $x + a$ belongs to the p-cyclotomic coset B containing either x or $-x$. Note that for B with $\frac{p^m-1}{2} \in B$, we have $|B| = 1$ and $B = -B$. Hence the existence of such x means that there exists some B such that $\frac{p^m-1}{2} \notin B$ and $B \neq \{0\}$, and so there is an integer k with $1 \leq k \leq m-1$, such that

$$x + a \equiv p^k x \pmod{p^m - 1}, \tag{3.4}$$

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

$$x + a \equiv -p^t x \pmod{p^m - 1}. \tag{3.5}$$

As for (3.4), similarly to the proof of Theorem 3.1, the number of solutions for x is $(m-1)(p-1)$ or 0 depends on that either $p-1 \mid a$ or $p-1 \nmid a$, respectively.

As for (3.5), we have

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

Since m is an odd prime and $1 \leq t \leq m$, hence from Lemma 3.1, we have $\gcd(p^t + 1, p^m - 1) = 2$. Hence (3.5) has solutions if and only if $2 \mid a$. In this case, (3.5) is equivalent to

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

Therefore the size of the set $\{x \in \mathbb{Z}_n \mid h(x+a) = h(x)\}$ is $2m$ for any nonzero $a \in \mathbb{Z}_n$ with $2 \mid a$.

Otherwise, i.e., congruence (3.5) has no solutions. Therefore the size of the set $\{x \in \mathbb{Z}_n \mid h(x+a) = h(x)\}$ is 0 for any nonzero $a \in \mathbb{Z}_n$ with $2 \nmid a$.

On the other hand, suppose that x is a solution both for (3.4) and (3.5), then from Lemma 3.2, there are some k $(1 \le k \le m-1)$ and t $(1 \le t \le m)$ such that

$$\frac{p^m-1}{p-1} \mid \frac{a}{p^k-1} + \frac{a}{p^t+1},$$

equivalently, $(p^m-1)(p^t+1)\frac{p^k-1}{p-1} \mid (p^k+p^t)$. Then we have

$$p^m - 1 \mid a(p^{|k-t|}+1).$$

Note that m is a prime and $|k-t| < m$, thus from (3) of Lemma 3.2, we have $\gcd(p^m-1, p^{|k-t|}+1) = 2$, and then $\frac{p^m-1}{2} \mid a$. Note that $p-1 \mid a$, thus $\mathrm{lcm}[p-1, \frac{p^m-1}{2}] = p^m-1 \mid a$, this is a contradiction since $0 < a \le p^m-2$. Hence the total number of x satisfying either (3.4) or (3.5) is $(m-1)(p-1)+2m = mp-p+m+1$ or $2m$ or 0.

From the above, when $p \ge 3$ one can get G-ZDB functions with the parameters

$$(p^m-1, \frac{p+1}{2} + \frac{p^m-p}{2m}, \{mp-p+m+1, 2m, 0\}).$$

This completes the proof of Theorem 3.2. □

Remark 3.3. By (3) of Lemma 2.2, we know that each nonzero 2-cyclotomic coset has exactly m elements. And so by taking $p = 2$ in the proofs of Theorems 3.1 and 3.2, the corresponding G-ZDB function is just the ZDB function constructed by Ding [2, 6], and so one can obtain Theorems 2 and 3 in [5], respectively.

4. The constant composition codes and difference systems of sets basing on G-ZDB functions

In this section, we study the applications of the G-ZDB functions for both constant composition codes and difference systems of sets. In the same way as that in [2, 6], basing on G-ZDB functions, one can construct a class of CCCs and DSSs as follows.

Theorem 4.1. *Suppose that f is an $(n, \overline{l}, S)$-G-ZDB function from an abelian group $(A,+)$ of order n to an abelian group $(B,+)$ of order l, and λ is the largest positive integer of S, and $\mathrm{Im}(f)$ is the image set of f with $|\mathrm{Im}(f)| = \overline{l}$. Let $A = \{a_0, \ldots, a_{n-1}\}$ and $\mathrm{Im}(f) = \{b_0, \ldots, b_{\overline{l}-1}\}$. Define $\tau_i = |\{x \in A : f(x) = b_i\}$ for $0 \le i \le \overline{l}-1$. Then the code*

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

is an $(n, n, n-\lambda, [\tau_0, \ldots, \tau_{\overline{l}-1}])_{\overline{l}}$-CCC over $\mathrm{Im}(f)$.

Proof. It is easy to see that the length of every codeword of $\mathcal{C}$ and the number of all codewords in $\mathcal{C}$ are both n. Now we consider the minimum Hamming

distance of $\mathcal{C}$. For any $0 \le i \ne j \le n-1$, the Hamming distance between two codes c_i and c_j is

$$\begin{aligned} d_H(c_i, c_j) &= n - \sharp\{a_k \,|\, f(a_i + a_k) = f(a_j + a_k), 0 \le k \le n-1\} \\ &= n - \sharp\{a_i + a_k \,|\, f(a_i + a_k) = f(a_i + a_k + (a_j - a_i)), 0 \le k \le n-1\} \\ &= n - \sharp\{a_k \,|\, f(a_k) = f(a_k + (a_j - a_i)), 0 \le k \le n-1\}. \end{aligned}$$

Note that f is an $(n, \overline{l}, S)$- G-ZDB function and λ is the largest positive integer of S, namely, for any nonzero $x \in A$,

$$\sharp\{a_k \,|\, f(a_k + x) = f(a_k)\} \ge \lambda.$$

Therefore the minimal distance of $\mathcal{C}$ equals $n - \lambda$. □

Theorem 4.2. *Suppose that f is an $(n, \overline{l}, \lambda)$-G-ZDB function from an abelian group $(A, +)$ of order n to an abelian group $(B, +)$ of order l, and λ is the largest positive integer of S, and $\mathrm{Im}(f)$ is the image set of f with $|\mathrm{Im}(f)| = \overline{l}$. Define $D_i = \{x \in \mathbb{Z}_n : f(x) = b_i\}$ and $\tau_i = |D_i|$ for $0 \le i \le \overline{l} - 1$. Then the set*

$$\mathcal{D} = \{D_i : 0 \le i \le \overline{l} - 1\}$$

is an $(n, [\tau_0, \ldots, \tau_{\overline{l}-1}], n - \lambda)$-DSS. In particular, such DSS is perfect if and only if the corresponding G-ZDB function f is ZDB.

Proof. Since f is an $(n, \overline{l}, S)$-G-ZDB function and λ is the largest positive integer of S, namely, for any nonzero $x \in A$,

$$\sharp\{a_k \,|\, f(a_k + x) = f(a_k)\} \ge \lambda.$$

Thus from the construction of DSSs, we know that the multiset in (1.1) contains every nonzero element $x \in \mathbb{Z}_n$ at least $n - \lambda$ times. Hence we get an $(n, [\tau_0, \ldots, \tau_{\overline{l}-1}], n - \lambda)$-DSS. In particular, such DSS is perfect if and only if for any nonzero $x \in A$,

$$\sharp\{a_k \,|\, f(a_k + x) = f(a_k)\} = \lambda,$$

namely, f is a ZDB function. This completes the proof of Theorem 4.2. □

5. Conclusions

For any prime m, basing on 2-cyclotomic sets modulo $n = 2^m - 1$, Ding et al. [5] obtains two families of ZDB functions on $(\mathbb{Z}_n, +)$ with new parameters. For any prime p, the present paper generalizes the definition of ZDB functions and the corresponding results in [5], i.e., employing p-cyclotomic sets modulo $n = p^m - 1$, constructs two families of G-ZDB functions on $(\mathbb{Z}_n, +)$. We show that these two families of ZDB functions in [5] are just the special case in our constructions.

Moreover, in the same way as that in [2, 6], we can construct constant composition codes and difference system of sets directly from G-ZDB functions. Basing on some special G-ZDB functions, we prove that the corresponding

CCCs are optimal, and the DSSs constructed by the G-ZDB function f is perfect when f is a ZDB function.

References

[1] H. Cai, X. Zeng, T. Helleseth, X. Tang, and Y. Yang, *A new construction of zero-difference balanced functions and its applications*, IEEE Trans. Inform. Theory **59** (2013), no. 8, 5008–5015.

[2] C. Ding, *Optimal constant composition codes from zero-difference balanced functions*, IEEE Trans. Inform. Theory **54** (2008), no. 12, 5766–5770.

[3] ———, *Optimal and perfect difference systems of sets*, J. Combin. Theory Ser. A **116** (2009), no. 1, 109–119.

[4] C. Ding and Y. Tan, *Zero-difference balanced functions with applications*, J. Stat. Theory Pract. **6** (2012), no. 1, 3–19.

[5] C. Ding, Q. Wang, and M. S. Xiong, *Three new families of zero-difference balanced functions with applications*, arXiv preprint arXiv:1312.4252, 2013.

[6] C. Ding and J. Yin, *Combinatorial constructions of optimal constant-composition codes*, IEEE Trans. Inform. Theory **51** (2005), no. 10, 3671–3674.

[7] T. Feng, *A new construction of perfect nonlinear functions using Galois rings*, J. Combin. Des. **17** (2009), no. 3, 229–239.

[8] X. D. Hou, *Cubic bent functions*, Discrete Math. **189** (1998), no. 1-3, 149–161.

[9] V. I. Levenšteĭn, *A certain method of constructing quasilinear codes that guarantee synchronization in the presence of errors*, Problemy Peredači Informacii **7** (1971), no. 3, 30–40.

[10] ———, *Combinatorial problems motivated by comma-free codes*, J. Combin. Des. **12** (2004), no. 3, 184–196.

[11] Y. Luo, F. W. Fu, A. J. H. Vinck, and W. Chen, *On constant-composition codes over* $\mathbb{Z}_q$, IEEE Trans. Inform. Theory **49** (2003), no. 11, 3010–3016.

[12] K. Nyberg, *Perfect nonlinear S-boxes*, in Advances in cryptology-EUROCRYPT'91 (Brighton, 1991), vol. 547 of Lecture Notes in Comput. Sci., 378–386, Berlin: Springer, 1991.

[13] A. Pott and Q. Wang, *Difference balanced functions and their generalized difference sets*, arXiv preprint arXiv:1309.7842, 2013.

[14] H. Wang, *A new bound for difference systems of sets*, J. Combin. Math. Combin. Comput. **58** (2006), 161–167.

[15] S. Yan, *Elementary Number Theory*, Springer Berlin Heidelberg, 2002.

[16] 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., 259–269, Berlin: Springer, 2006.

[17] Z. Zha, G. M. Kyureghyan, and X. Wang, *Perfect nonlinear binomials and their semifields*, Finite Fields Appl. **15** (2009), no. 2, 125–133.

[18] Z. Zhou, X. Tang, D. Wu, and Y. Yang, *Some new classes of zero-difference balanced functions*, IEEE Trans. Inform. Theory **58** (2012), no. 1, 139–145.

Lin Jiang
Institute of Mathematics and Software Science
Sichuan Normal University
Chengdu, Scihuan, P. R. China

Qunying Liao
Institute of Mathematics and Software Science
Sichuan Normal University
Chengdu, Scihuan, P. R. China
E-mail address: qunyingliao@sicnu.edu.cn