International Journal of Foundations of Computer Science
Vol. 27, No. 8 (2016) 897–908

DOI: 10.1142/S0129054116500362

Some New Constructions for Generalized Zero-Difference Balanced Functions*

Haibo Liu† and Qunying Liao‡
Institute of Mathematics and Software Science, Sichuan Normal University
Chengdu, Sichuan, P. R. China
†*1075509561@qq.com*
‡*qunyingliao@sicnu.edu.cn*

Received 25 December 2015
Accepted 19 April 2016
Communicated by Francine Blanchet-Sadri

Zero-difference balanced (ZDB) functions have many applications in coding theory, cryptography and communications engineering and so on. Recently, the authors [10, 11] generalized the definition of ZDB functions to be G-ZDB functions. In this paper, based on p-cyclotomic cosets, two classes of ZDB functions are obtained, and several new classes of G-ZDB functions are constructed. Furthermore, some frequency-hopping sequences are obtained directly from G-ZDB functions.

Keywords: Zero-difference balanced (ZDB) function; generalized ZDB function; cyclotomic coset; difference systems of sets; constant composition code; frequency-hopping sequence.

1. Introduction and Backgrounds

Zero-difference balanced functions (ZDB) were first introduced by Ding for constructing optimal constant composition codes [2] and optimal and perfect difference systems of sets [3]. Recently, Jiang and Liao [10, 11] generalized the definition of ZDB functions to be G-ZDB functions, and gave some constructions for G-ZDB functions. For convenience, throughout the paper, we need to introduce the notations defined in [5]. Let $(A, +)$ and $(B, +)$ be two Abelian groups of order n and l. Suppose that f is a function from A to B, then

- $Im(f) = \{b_0, \ldots, b_{\bar{l}-1}\} \subseteq B$ denotes the image set of f and $\bar{l} = |Im(f)|$;
- $A'_i = \{x \in A \mid f(x) = b_i\}$ and $\tau_i = |A'_i|$ for $0 \leq i \leq \bar{l} - 1$;
- $\mathcal{P} = \{A'_0, \ldots, A'_{\bar{l}-1}\}$ denotes the set of all the preimage sets, clearly, $\mathcal{P}$ constitutes a partition of A.

*This work is supported by the Natural Science Foundation of China with No. 11401408, and Project of Science and Technology Department of Sichuan Province with No. 2016JY0134.

Definition 1. [10,11] *Let $(A,+)$ and $(B,+)$ be two Abelian groups of order n and l, respectively. A function f from A to B is called a generalized zero-difference balanced function (G-ZDB for short) if there exists a non-empty $S \subseteq N$, 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.

In particular, if S is a single set $\{\lambda\}$, then a G-ZDB function is an (n,λ)-ZDB function. Thus ZDB functions defined by Ding in [5] is a special class of G-ZDB functions. For the case $\gcd(n,\lambda) = 1$, many (n,λ)-ZDB functions are constructed [1–5, 18, 20, 22]. For $\gcd(n,\lambda) \neq 1$, Luo *et al.* [14] constructed ZDB functions with parameters $(p^r, p^s)(0 \leq s \leq r)$, where p is a prime. In 2013, for $n = 2^m - 1$, where m is a prime, using cyclotomic cosets, Ding *et al.* [5] constructed two classes of ZDB functions. Recently, for $n = 2^{2m} - 1$ or $n = p^m - 1$, Jiang and Liao generalized these constructions to obtain several classes of G-ZDB functions [10, 11], where both p and m are primes.

Frequency-hopping sequences are needed in FH code-division-multiple-access (CDMA) systems [17]. Perfect nonlinear functions can be used to construct optimal frequency-hopping sequences [6], it is well known that perfect nonlinear functions [8,9,16,19,21] are special types of ZDB functions. Thus frequency-hopping sequences can be constructed by G-ZDB functions, frequency-hopping sequences constructed by a G-ZDB function f is optimal if f is a ZDB function(see Sec. 4).

Constant composition codes (CCC) have widely applications in communications engineering. Constant composition codes are a special class of constant weight codes, and include permutation codes as a subclass [7]. Thus constant composition codes are of great importance due to both practical applications and theoretic interests. Recently, it was proved that G-ZDB functions can be used to construct constant composition codes [11], especially to construct optimal CCCs. In fact, the constant composition code constructed by a G-ZDB function f is optimal if f is a ZDB function [3, 5].

Besides, it is well known that difference systems of sets (DSS) were introduced in 1973 by Levenšteĭn [12,13], DSSs have widely applications in coding theory. DSSs can be used to construct codes allowing for synchronization in the presence of errors, and DSSs are closely related to cyclic difference families [3]. Thus DSSs are required, especially optimal DSSs. The correspondence between ZDB functions and perfect DSSs was first established in [2], one can use G-ZDB functions to construct DSSs as well [11]. The DSS constructed by a G-ZDB function f is prefect if f is a ZDB function. Furthermore, the DSS is optimal, when $\bar{l}\lambda \leq n$ [2]. Thus G-ZDB functions play an important role in coding theory, cryptography and communications.

In this paper, we construct several classes of G-ZDB functions with different parameters for further applications. The rest of the paper is organized as follows. In Sec. 2, based on p-cyclotomic cosets, two classes of ZDB functions are constructed

on the group $(\mathbb{Z}_n, +)$. In Sec. 3, first we generalize the constructions in Sec. 2 and obtain two new classes of G-ZDB functions. Simultaneously, we utilize cosets and the additive decomposition of elements in the group $(\mathbb{Z}_n, +)$ to construct another two new classes of G-ZDB functions. In Sec. 4, we use G-ZDB functions to construct frequency-hopping sequences, and obtain a class of optimal frequency-hopping sequences.

2. The Constructions for Two New Classes of ZDB Functions

In this section, for a prime p, based on properties for p-cyclotomic sets, two new classes of ZDB functions are constructed. First, we need to introduce the definition of the p-cyclotomic coset, where p is a prime. Let p be a prime, n be a positive integer and $gcd(p, n) = 1$. Suppose that

$$A_i = \{i, i \times p(\text{mod } n), \ldots, i \times p^{l_i - 1}(\text{mod } n)\} \subseteq \mathbb{Z}_n$$

is the p-cyclotomic coset modulo n containing i, where l_i is the least positive integer such that $i \equiv i \times p^{l_i}(\text{mod } n)$, and l_i 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. It is easy to prove that all p-cyclotomic cosets modulo n form a partition of $\mathbb{Z}_n$. Before giving our main results and their proofs, the following lemma is needed.

Lemma 2. [23] *Suppose that both m_1 and m_2 are two positive integers, b_1 and b_2 are both integers, then the congruences*

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

have solutions if only if $gcd(m_1, m_2) \mid b_1 - b_2$. Furthermore when the congruences have solutions, it has a unique solution modulo $lcm[m_1, m_2]$.

The order of p modulo n is the least integer r such that $p^r \equiv 1 \pmod{n}$, denoted to be $ord_n(p) = r$. Based on properties for both p-cyclotomic sets and the order of p modulo n, this section generalizes the main results in [5], and then constructs two new classes of ZDB functions (Theorems 3 and 5).

Theorem 3. *Let r be a positive integer. Suppose that $(p, n = 2p - 1)$ is an odd pair primes with $ord_n(p) = r$, then there exists a ZDB function with the parameters*

$$\left(2p - 1, 1 + \frac{2p - 2}{r}, r - 1\right).$$

Proof. We define the 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. From $ord_n(p) = r$ we can get $|A_i| \leq r$ for any i. Now considering the size of the coset $A_i (1 \leq i \leq n - 1)$, this reduces to compute the least integer l_i such that $i \cdot p^{l_i} \equiv i \pmod{2p-1}$, equivalently, $2p - 1 | i \cdot (p^{l_i} - 1)$. Note that $2p - 1$ is a prime, and $ord_n(p) = r (1 \leq l_i \leq r)$, thus

$$\gcd(2p - 1, p^{l_i} - 1) = \begin{cases} 1, & 1 \leq l_i \leq r - 1; \\ 2p - 1, & l_i = r, \end{cases} \tag{1}$$

this means that

$$l_i = \begin{cases} 1, \, i = 0; \\ r, \text{ otherwise.} \end{cases}$$

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

$$|A_i| = \begin{cases} 1, \, i = 0; \\ r, \text{ otherwise.} \end{cases}$$

Hence the sizes of the preimage sets of f form the set $\{1, r, \ldots, r\}$. Therefore $|Im(f)| = 1 + \frac{2p-2}{r}$.

For any given $a \not\equiv 0 \pmod{2p-1}$, it suffices to prove that the number of $x \in \mathbb{Z}_n$ such that $f(x+a) = f(x)$ is always $r-1$. This means that both $x+a$ and x belong to the same p-cyclotomic coset A_i with $i \neq 0$. Otherwise, from $A_0 = \{0\}$ and $x + a, x \in A$, we can get $a = 0$, which is a contradiction. While for any $i \neq 0$, $|A_i| = r$, from $f(x+a) = f(x)$ we know that there exists some k with $1 \leq k \leq r-1$, such that $x + a \equiv p^k x \pmod{2p-1}$, equivalently,

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

Note that $1 \leq k \leq r-1$, thus from (1) we have $gcd(p^k - 1, 2p-1) = 1$, which means that (2) has a unique solution

$$x \equiv \frac{a}{p^k - 1} \pmod{2p-1}.$$

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

From the above and the definition of ZDB functions, the function f defined above is a ZDB function on $(\mathbb{Z}_n, +)$ with the parameters $(2p-1, 1 + \frac{2p-2}{r}, r-1)$.

This completes the proof of Theorem 3. □

Remark 4. *In* [5] *the authors take* $n = 2^m - 1$*, where* m *is a prime. It is easy to see that* $ord_n(2) \mid m$*, i.e.* $ord_n(2)$ *has only two choices* 1 *or* m*. While in Theorem* 3*, the value of* $ord_n(p)$ *has more choices for* $n = 2p-1$*, where* p *is an odd prime.*

On the other hand, for any p-cyclotomic $A_i (i \in \mathbb{Z}_n)$, we denote $-A_i = \{n - i \mid i \in A_i\}$, it is easy to see that both A_i and $-A_i$ are p-cyclotomic cosets modulo n. Now we combine A with $-A$ to be a new p-cyclotomic coset modulo n, and then construct some new ZDB functions as following.

Theorem 5. *Let* r *be a positive integer,* p *and* $n = 2p-1$ *be both odd primes. Suppose that* $ord_n(p) = r$ *is odd, then there exists a ZDB function with the parameters*

$$\left(2p-1, 1 + \frac{2p-2}{2r}, 2r-1\right).$$

Proof. Let $\prod_n$ be the set of all p-cyclotomic cosets modulo n, and

$$\Delta_n = \left\{ A \cup (-A) \mid A \in \prod_n \right\}.$$

Similar to the proof of Theorem 3, it is easy to see that A and $-A$ are disjoint to each other for $A \neq \{0\}$. Since each nonzero set $A \cup (-A)$ has $2r$ elements, hence $|\Delta_n| = 1 + \frac{2p-2}{2r}$. For any $A \in \prod_n$, the leader of $A \cup (-A)$ is the least integer in this set. Consider the function f from $(\mathbb{Z}_n, +)$ to itself by $f(x) = j_x$, where j_x is the leader of the set $A \cup (-A)$ containing x, then the size of the preimage sets of f form the set $\{1, 2r, \cdots, 2r\}$, and so $|Im(f)| = 1 + \frac{2p-2}{2r}$.

Now for any nonzero element $a \in \mathbb{Z}_n$, it suffices to prove that the number of $x \in \mathbb{Z}_n$ such that $f(x+a) = f(x)$ is always $2r-1$, which means that $x+a$ belongs to the p-cyclotomic coset $A(A \neq \{0\})$ containing either x or $-x$. Equivalently, there is an integer k with $1 \leq k \leq r-1$, such that

$$x + a \equiv p^k x \pmod{2p-1}, \tag{3}$$

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

$$x + a \equiv -p^t x \pmod{2p-1}. \tag{4}$$

As for (3), similar to the proof of Theorem 3, the number of solutions x for (3) is $r-1$. As for (4), we have

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

Note that $2p-1$ is an odd prime, $1 \leq t \leq r$, and $ord_n(p) = r$ is odd, so $gcd(1 + p^t, 2p-1) = 1$. Hence (4) has a unique solution

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

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

On the other hand, suppose that x is a common solution for both (3) and (4), then by Lemma 2, there exist $k(1 \leq k \leq r-1)$ and $t(1 \leq t \leq r)$ such that

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

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

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

Note that $2p-1$ is a prime, $ord_n(p) = r$ is odd, and $|k-t| < r$, we have $gcd(2p-1, p^{|k-t|} + 1) = 1$, which implies that $a \equiv 0 \pmod{2p-1}$, this is a contradiction to the assumption that $a \not\equiv 0 \pmod{2p-1}$. Hence the total number of x satisfying either (3) or (4) is $2r-1$.

From the above and the definition of ZDB functions, f defined above is a ZDB function with the parameters

$$\left(2p-1, 1 + \frac{2p-2}{2r}, 2r-1\right).$$

This completes the proof of Theorem 5. □

Remark 6. *Suppose that* $ord_n(p) = r$ *is even, then* $-1 \equiv p^{\frac{r}{2}} (mod\ 2p-1)$*, and so for any* $i \in \mathbb{Z}_n$*, we have* $-i \equiv ip^{\frac{r}{2}} (mod\ 2p-1)$*, hence* $-i \in A_i$*, which implies* $-A_i = A_i$*. Thus Theorem* 5 *does not work.*

3. Some New Constructions for G-ZDB Functions

In this section, for any prime p, basing on properties for p-cyclotomic cosets, we generalize the constructions of ZDB functions in Sec. 2 to obtain two new classes of G-ZDB functions. Simultaneously, using properties for cyclotomy cosets and the Abelian group $(\mathbb{Z}_n, +)$, we construct another two classes of G-ZDB functions.

Suppose that both p and $n = 2p-1$ are odd primes, the above Theorems 3 and 5 give two constructions for ZDB functions on $(\mathbb{Z}_n, +)$. Now for any positive integer $n = pq - 1$, where both p and q are primes. Basing on properties for p-cyclotomic cosets, we construct two new classes of G-ZDB functions on $\mathbb{Z}_n$.

Theorem 7. *Let* p,q *be odd primes and* $\frac{n}{2}$ *be odd prime with* $n = pq - 1$*. Set* $ord_n(p) = r$*, then there exists a G-ZDB function with the parameters*

$$\begin{cases} \left(n, 2 + \dfrac{n-2}{r}, \{2r-2, 0\}\right); & (1) \\ \left(n, 2 + \dfrac{n-2}{2r}, \{4r-2, 0\}\right), \quad \text{if } 2 \nmid r. & (2) \end{cases}$$

Proof. (I) For (1) of Theorem 7, suppose that f is defined as that in the proof of Theorem 3, from $ord_n(p) = r$ we have $|A_i| \leq r$ for any $i \in \mathbb{Z}_n$. Now consider the size of the coset $A_i (1 \leq i \leq n-1)$, this reduces to compute the least integer l_i such that $i \cdot p^{l_i} \equiv i \pmod{n}$, equivalently, $n | i \cdot (p^{l_i} - 1)$. Note that $p, q, \frac{n}{2}$ are odd primes, and $ord_n(p) = r$, thus we have

$$\gcd(n, p^{l_i} - 1) = \begin{cases} 2, & 1 \leq l_i \leq r-1; \\ n, & l_i = r, \end{cases}$$

this means that

$$l_i = \begin{cases} 1, & \frac{n}{2} | i; \\ r, & \text{otherwise.} \end{cases}$$

Hence for any $i = 1, \ldots, n-1$, we can get

$$|A_i| = \begin{cases} 1, & \frac{n}{2} | i; \\ r, & \text{otherwise.} \end{cases} \quad (5)$$

Therefore the sizes of the preimage sets of f form the set $\{1, 1, r, \ldots, r\}$, and so $|Im(f)| = 2 + \frac{n-2}{r}$.

Now for any $a \not\equiv 0 \pmod{n}$, there exists some $x (1 \leq x \leq n)$ such that $f(x+a) = f(x)$, equivalently, both $x + a$ and x belong to the same p-cyclotomic coset A_i, then $\frac{n}{2} \nmid i$. Otherwise, from $\frac{n}{2} | i$ and (5), we have $i = \frac{n}{2}$. But $|A_{\frac{n}{2}}| = 1$, thus by $x + a, x \in A_{\frac{n}{2}}$, we have $a = 0$, which is a contradiction. Hence from (5) we have

$x \in A_i$ with $|A_i| = r$, and so there exists some k with $1 \le k \le r-1$, such that $x + a \equiv p^k x \pmod{n}$, equivalently,

$$(p^k - 1)x \equiv a \pmod{n}. \tag{6}$$

Note that $\frac{n}{2}$ is a prime, and $ord_n(p) = r$, thus we have $gcd(p^k - 1, n) = 2$. Hence (6) has solutions if and only if $2 \mid a$. In this case, (6) has a unique solution

$$x \equiv \frac{a}{p^k - 1} \pmod{\frac{n}{2}}.$$

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

Otherwise, i.e. $2 \nmid a$, then congruence (6) has no solutions, and so 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 $2 \nmid a$.

From the above and the definition of G-ZDB functions, the function f defined above is a G-ZDB function on $(\mathbb{Z}_n, +)$ with the parameters $(n, 2+\frac{n-2}{r}, \{2r-2, 0\})$.

(II) As for (2) of Theorem 7, let $\prod_n$ and Δ_n be defined as that in the proof of Theorem 5. From the proof of (1), if $\frac{n}{2} \mid i$, then $|A_i| = 1$, thus $A_i = -A_i$, and so each set $A_i \cup (-A_i)$ with $\frac{n}{2} \nmid i$ has $2r$ elements. Therefore $|\Delta_n| = 2 + \frac{n-2}{2r}$. Let f be defined as that in the proof of Theorem 5, then the size of the preimage sets of f form the set $\{1, 1, 2r, \cdots, 2r\}$, and so $|Im(f)| = 2 + \frac{n-2}{2r}$.

Note that for any nonzero elements $a \in \mathbb{Z}_n$, there exists some $x \in \mathbb{Z}_n$ such that $f(x+a) = f(x)$, equivalently, $x+a$ belongs to the p-cyclotomic coset A_i containing either x or $-x$. For A_i with $\frac{n}{2} \mid i$, we have $|A_i| = 1$, this means $a = 0$, which is a contradiction. Therefore from $a \in \mathbb{Z}_n^*$ and $f(x+a) = f(x)$, we know that there is an integer k with $1 \le k \le r-1$, such that

$$x + a \equiv p^k x \pmod{n}, \tag{7}$$

or there is an integer t with $1 \le t \le r$, such that

$$x + a \equiv -p^t x \pmod{n}. \tag{8}$$

As for (7), similar to the proof of (1), the number of solutions x for (7) is $2r-2$ or 0, depending on $2 \mid a$ or not, respectively.

As for (8), we have

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

Since $\frac{n}{2}$ is an odd prime, and $ord_n(p) = r$ is odd, we have $gcd(p^t + 1, n) = 2$. Hence (8) has solutions if and only if $2 \mid a$. In this case, (8) is equivalent to

$$x \equiv \frac{-a}{p^t + 1} \left(\mathrm{mod}\ \frac{n}{2}\right).$$

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

Otherwise, i.e. $2 \nmid a$, then (8) has no solutions. Thus 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 $2 \nmid a$.

On the other hand, suppose that x is a common solution both for (7) and (8), then from Lemma 2, there exist $k(1 \le k \le r-1)$ and $t(1 \le t \le r)$ such that

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

equivalently, $n(p^t+1)\frac{p^k-1}{2} \mid a(p^k + p^t)$. Then we have

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

Note that $ord_n(p) = r$ is odd, and $|k-t| < r$, thus $gcd(n, p^{|k-t|} + 1) = 2$, and so $\frac{n}{2} \mid a$. Note that $a \in \mathbb{Z}_n^*$, hence $a = \frac{n}{2}$ is an odd prime, then $2 \nmid a$, which is a contradiction to $2 \mid a$. Hence the total number of x satisfying either (7) or (8) is $4r-2$ or 0.

From the above, the function f defined above is a G-ZDB function with the parameters

$$\left(n, 2 + \frac{n-2}{2r}, \{4r-2, 0\}\right).$$

This completes the proof of Theorem 7. □

Remark 8.

(1) *Suppose that $n = p^m - 1$ is given by the construction of G-ZDB functions in* [11]*, where both p and m are primes. Note that $ord_n(p) = m$, thus in* (1) *of Theorem* 7*, the value of $ord_n(p)$ has more choices.*

(2) *Assume that $ord_n(p) = r$ is even, then $-1 \equiv p^{\frac{r}{2}} \pmod n$. Thus for any $i \in \mathbb{Z}_n$, we have $-i \equiv ip^{\frac{r}{2}} \pmod n$, which means that $A_i = -A_i$. Therefore Theorem* 7 *does not work.*

On the other hand, the authors in [5] utilized the generalized multiplicative cyclotomy in the group $\mathbb{Z}_n$ to construct an $(n, \frac{n+e-1}{e}, e-1)$-ZDB function, where n has the canonical factorization $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}, p_1 < p_2 < \cdots < p_k$. Inspired by this idea, we utilize the additive cyclotomy in the group $\mathbb{Z}_n$ to construct some new G-ZDB functions.

Let d, n be positive integers such that $d \mid n$, and let g be a generator of the additive group $A = (\mathbb{Z}_n, +)$. Denote $e = g^{\frac{n}{d}}$, from $A = (g)$, we know that the additive order of $e \in \mathbb{Z}_n$ is d. Let $A_d \subseteq A$ be the cyclic subgroup generated by e, then $|A_d| = d$. Now we can decompose A into the disjoint unions of left cosets of A_d as

$$A = \coprod_{\alpha_d \in R_d} \alpha_d + A_d,$$

where $R_d \subseteq A$ is a fixed set of representatives for $\frac{A}{A_d}$. It easy to see that $|R_d| = \frac{|A|}{|A_d|} = \frac{n}{d}$. Now define f from $\mathbb{Z}_n$ to itself by

$$f(x) = i_x, \text{ where } i_x \text{ is the minimum element of } \alpha_d + A_d \text{ containing } x. \qquad (*)$$

Theorem 9. *The function f defined above $(*)$ is a G-ZDB function with the parameters $(n, \frac{n}{d}, \{d-1, 0\})$.*

Proof. From the definition of f, we know that $Im(f) = \frac{n}{d}$. Now for any nonzero element $a \in \mathbb{Z}_n$, there exists some $x (x \in \mathbb{Z}_n)$ such that $f(x+a) = f(x)$ if and only if both $x+a$ and x belong to the same coset $\alpha_d + A_d$. Since A_d is subgroup of A with $|A_d| = d$, this means that there exist t and s such that $0 \leq t, s \leq d-1$,

$$x + a = \alpha_d + e^t, \quad \text{and} \quad x = \alpha_d + e^s.$$

Thus $a = e^t - e^s \in A_d$. Note that a is a nonzero element in $\mathbb{Z}_n$, and so $t \neq s$, therefore the size of the set $\{x \in \mathbb{Z}_n | f(x+a) = f(x)\}$ is $d-1$ with $a \in A_d$. Otherwise, the size of the set $\{x \in \mathbb{Z}_n | f(x+a) = f(x)\}$ is 0.

This completes the proof of Theorem 9. □

Suppose that g is a generator of the additive group $A = (\mathbb{Z}_n, +)$. Consider the additive decomposition of elements in set A, i.e., for any $\beta \in \mathbb{Z}_n$, β can be uniquely written as $\beta = g + t$ with $t \in A$. Utilizing this property, we construct some new G-ZDB functions as following.

Theorem 10. *For any odd positive integer n, there exists a G-ZDB function with the parameters*

$$\left(n, \frac{n-1}{2}, \left\{0, \frac{n+1}{2}, \frac{n-1}{2}\right\}\right).$$

Proof. Let g be a generator of the additive group $A = (\mathbb{Z}_n, +)$. Then for any $x \in \mathbb{Z}_n$, x can be uniquely written as $x = g + t$ with some $t \in A$. Now we define f from $\mathbb{Z}_n$ to itself by

$$f(x) = \begin{cases} t, & \text{if } t \text{ is even;} \\ t+1, & \text{otherwise .} \end{cases}$$

From the definition of f, it easy to see that the images of f is an even number in $\mathbb{Z}_n$. Since n is odd, thus $Im(f) = \frac{n-1}{2}$.

Note that for any nonzero element $a \in \mathbb{Z}_n$, there exist some b and c $(b, c \in \mathbb{Z}_n)$ such that $b \neq c$, $x + a = g + b$, and $x = g + c$. Now from the definition of f, if there exists some $x \in \mathbb{Z}_n$ such that $f(x+a) = f(x)$, equivalently, $a = b - c = \pm 1$. Hence we have the following three cases.

Case (I). For $a = b - c = 1$, we have $x = g + c$ and $x + a = g + c + 1$. While $f(x+a) = f(x)$, this means that c is odd. Since n is odd, and there are exactly $\frac{n+1}{2}$ odd numbers in $\mathbb{Z}_n$. Therefore, the size of the set $\{x \in \mathbb{Z}_n | f(x+a) = f(x)\}$ is $\frac{n+1}{2}$.

Case (II). For $a = b - c = -1$, we can get $x = g + c$ and $x + a = g + c - 1$. While $f(x+a) = f(x)$, this means that c is even. Since n is odd, and there are exactly $\frac{n-1}{2}$ even numbers in $\mathbb{Z}_n$. Therefore, the size of the set $\{x \in \mathbb{Z}_n | f(x+a) = f(x)\}$ is $\frac{n-1}{2}$.

Case (III). Otherwise, namely $a \neq \pm 1$, which means that $f(x+a) \neq f(x)$ for any $x \in \mathbb{Z}_n$. Thus the size of the set $\{x \in \mathbb{Z}_n | f(x+a) = f(x)\}$ is 0.

From the above and the definition of G-ZDB functions, the function f defined above is a G-ZDB function on $(\mathbb{Z}_n, +)$ with the parameters $(n, \frac{n+1}{2}, \{0, \frac{n+1}{2}, \frac{n-1}{2}\})$.

This completes the proof of Theorem 10. □

Remark 11. *From the proof of Theorem* 10*, if n is even, then we can similarly obtain a G-ZDB function on $(\mathbb{Z}_n, +)$ with the parameters*

$$\left(n, \frac{n}{2}, \left\{0, \frac{n}{2}\right\}\right).$$

4. Frequency-Hopping Sequences from G-ZDB Functions

In this section, we study some applications of G-ZDB functions for frequency-hopping sequences.

Let $F = \{f_0, f_1, \cdots, f_{l-1}\}$ be a set of available frequencies called an *alphabet*. Let S be the set of all sequences of length v over F. Any element of S is called a frequency-hopping sequence of v over F. Given two frequency-hopping sequences $X = (x_0, x_1, \cdots, x_{n-1}), Y = (y_0, y_1, \cdots, y_{n-1}) \in S$, define their Hamming correlation $H_{X,Y}$ to be

$$H_{X,Y}(t) = \sum_{i=0}^{v-1} h[x_i, y_{i+t}], \quad 0 \leq t < v,$$

where $h[a, b] = 1$ if $a = b$, and 0 otherwise, and all operations among the position indices are performed modulo v.

For any distinct $X, Y \in S$, we define

$$H(X) = max_{1 \leq t < v}\{H_{X,X}(t)\}.$$

The criteria of optimality is the following [15].

Lemma 12. [15] *A sequence $X \in S$ is called optimal if $H(X) \leq H(X')$ for all $X' \in S$.*

Throughout this section, we use (v, l, λ)-FHS to denote a frequency-hopping sequence X of length v over an alphabet of size l with $\lambda = H(X)$. Basing on G-ZDB functions, we construct a class of frequency-hopping sequences as follows.

Theorem 13. *Suppose that f is an (n, 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. Set $A = \{a_0, a_1, \cdots, a_{n-1}\}$, if a frequency-hopping sequence X of length n over B is defined to be*

$$X = (f(a_0), f(a_1), \cdots, f(a_{n-1})),$$

then X is an (n, l, λ)-FHS.

Proof. It is easy to see that the length of X is n, and the size of alphabet for X is l. Now we consider the Hamming correlation of X, for any nonzero element $a \in A$, we have

$$\begin{aligned} H_{X,X}(a) &= \sum_{i=0}^{n-1} h[x_i, x_{i+a}] \\ &= |\{i : 0 \le i \le n-1 \mid f(a_i) = f(a_i + a)\}| \\ &= |\{i : 0 \le i \le n-1 \mid f(a_i + a) - f(a_i) = 0\}|. \end{aligned}$$

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

$$H_{X,X}(a) = |\{i : 0 \le i \le n-1 \mid f(i + a) - f(i) = 0\}| \le \lambda,$$

thus

$$H(X) = max_{a \in A/\{0\}}\{H_{X,X}(a)\} = \lambda.$$

Therefore X defined above is an (n, l, λ)-FHS.

This completes the proof of Theorem 13. □

Remark 14. *In Theorem* 13*, if f is an (n, λ)-ZDB function, then we have $H(X, X) = H(X)$, thus from Lemma* 12*, the frequency-hopping sequence constructed in Theorem* 13 *is optimal. Therefore, the frequency-hopping sequence constructed by a G-ZDB function f is optimal, when f is a ZDB function.*

5. Conclusions

In this paper, based on p-cyclotomic cosets, two classes of ZDB functions on $(\mathbb{Z}_n, +)$ with new parameters are constructed. In our constructions, the value of $ord_n(p)$ has more flexibility than that in [5]. Furthermore, based on p-cyclotomic cosets modulo n and the additive decomposition of elements in the group $(\mathbb{Z}_n, +)$, several classes of G-ZDB functions on $(\mathbb{Z}_n, +)$ are obtained with new parameters. In the end, we use G-ZDB functions to construct frequency-hopping sequences, and prove that frequency-hopping sequences constructed by a G-ZDB function f is optimal 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** (8) (2013) 5008-5015.

[2] C. Ding, Optimal constant composition codes from zero-difference balanced functions, *IEEE Trans. Inform. Theory.* **54** (12) (2008) 5766-5770.

[3] C. Ding, Optimal and perfect difference systems of sets, *J. Combin. Theory Ser.* A **116** (1) (2013) 109-119.

[4] C. Ding and Y. Tan, Zero-difference balanced functions with applications, *J. Statistical Theory and Practice* **6** (1) (2012) 3-19.
[5] C. Ding, Q. Wang, and M. S. Xiong, Three new families of zero-difference balanced functions with applications, *IEEE Trans. Inform. Theory.* **60** (4) (2013) 2407-2413.
[6] C. Ding, M. J. Moisio, and J. Yuan, Algebraic constructions of optimal frequency-hopping sequences, *IEEE Trans. Inform. Theory.* **53** (7) (2007) 2606-2610.
[7] C. Ding and J. Yin, Combinatorial constructions of optimal constant-composition codes, *IEEE Trans. Inform. Theory.* **51** (10) (2005) 3671-3674.
[8] T. Feng, A new construction of perfect nonlinear functions using Galois rings, *J. Comb. Des.* **17** (3) (2009) 229-239.
[9] X. D. Hou, Cubic bent functions, *Discrete Mathematics.* **189** (1-3) (1998) 149-161.
[10] L. Jiang and Q. Y. Liao, Generalized zero-difference balanced functions and their applications, *Chinese Annals of Mathmatics*(A), to appear (2016).
[11] L. Jiang and Q. Y. Liao, On generalized zero-difference balanced functions, *Commun. Korean Math. Soc.* **31** (1) (2016) 41-52.
[12] V. I. Levenšteĭn, A certain method of constructing quasilinear codes that guarantee synchronization in the presence of errors, *Problemy Peredači Informacii.* **7** (3) (1971) 30-40.
[13] V. I. Levenšteĭn, Combinatorial problems motivated by comma-free codes, *J. Combin. Des.* **12** (3) (2004) 184-196.
[14] 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** (11) (2003) 3010-3016.
[15] A. Lempel and H. Greenberger, Familes of sequences with optimal Hamming correlation properties, *IEEE Trans. Inform. Theory.* **20** (1974) 90-94.
[16] K. Nyberg, Perfect nonlinear S-boxes, *in Advances in Cryptology-EUROCRYPT'*91, Lecture Notes in Comput. Sci., Vol. 547 (Springer, Berlin, 1991), pp. 378-386.
[17] R. A. Scholtz, The spread spectrum concept, *IEEE Transactions on Communications.* **25** (1977) 748-755.
[18] Q. Wang and Y. Zhou, Sets of zero-difference balanced functions and their applications, *Adv. Math. Commun.* **8** (1) (2014) 83-101.
[19] X. Zeng, H. Guo, and J. Yuan, A note of perfect nonlinear functions, *in Cryptography and Network Security*, Lecture Notes in Comput. Sci., Vol. 4301 (Springer, Berlin, 2006), pp. 259-269.
[20] Z. Zha and L. Hu. Cyclotomic constructions of zero-difference balanced functions with applications, *IEEE Trans. Inform. Theory.* **61** (3) (2015) 1491-1495.
[21] Z. Zha, G. M. Kyureghyan, and X. Wang, Perfect nonlinear binomials and their semifields, *Finite Fields Appl.* **15** (2) (2009) 125-133.
[22] Z. Zhou, X. Tang, D. Wu, and Y. Yang, Some new classes of zero-difference balanced functions, *IEEE Trans. Inform. Theory.* **58** (1) (2012) 139-145.
[23] S. Yan, *Elementary Number Theory* (Springer, Berlin Heidelberg, 2002).