Bull. Korean Math. Soc. **59** (2022), No. 6, pp. 1327–1337
https://doi.org/10.4134/BKMS.b210183
pISSN: 1015-8634 / eISSN: 2234-3016

SOME NEW CLASSES OF ZERO-DIFFERENCE BALANCED FUNCTIONS AND RELATED CONSTANT COMPOSITION CODES

Sankhadip Roy

Abstract. Zero-difference balanced (ZDB) functions can be applied to many areas like optimal constant composition codes, optimal frequency hopping sequences etc. Moreover, it has been shown that the image set of some ZDB functions is a regular partial difference set, and hence provides strongly regular graphs. Besides, perfect nonlinear functions are zero-difference balanced functions. However, the converse is not true in general. In this paper, we use the decomposition of cyclotomic polynomials into irreducible factors over $\mathbb{F}_p$, where p is an odd prime to generalize some recent results on ZDB functions. Also we extend a result introduced by Claude et al. [3] regarding zero-difference-p-balanced functions over $\mathbb{F}_{p^n}$. Eventually, we use these results to construct some optimal constant composition codes.

1. Introduction

Zero-difference balanced (ZDB) functions were first introduced by Ding for constructing optimal constant composition codes [8] and optimal and perfect difference systems of sets [9]. Recently, Jiang and Liao [14, 15] generalized the definition of ZDB functions and introduced G-ZDB functions.

Definition ([14, 15])**.** Let $(A, +)$ and $(B, +)$ be two abelian groups of order n and l, respectively. A function $f : A \to B$ is called a generalized zero-difference balanced function (G-ZDB function) if there exists a non-empty $S \subset \mathbb{N}$ such that

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

for every non-zero $a \in A$. We call the function to be an (n, S) or $(n, |\operatorname{Im}(f)|, S)$-G-ZDB function. In particular, when $S = \{\lambda\}$, it is called an (n, λ)-ZDB. In some literature it is also called a zero-difference-λ-balanced function.

Received March 6, 2021; Revised February 4, 2022; Accepted July 15, 2022.
2010 *Mathematics Subject Classification.* 06E30, 05B10, 94B25.
Key words and phrases. Zero-difference balanced (ZDB) function, cyclotomic polynomials, cyclotomic coset, constant composition code.

So the ZDB functions introduced by Ding [8] are nothing but a special case of G-ZDB functions. For the case $\gcd(n, \lambda) = 1$, several (n, λ)-ZDB functions are constructed. For references the reader can check [2, 8–11, 22–25] and the references therein. For the case $\gcd(n, \lambda) \neq 1$, Luo, et al. [19] constructed ZDB functions with parameters (p^r, p^s), where p is prime and $0 \leq s \leq r$. For $n = 2^m - 1$, where m is prime, Ding, et al. [11] constructed two classes of ZDB functions. In their recent works, Jiang and Liao [14,15] generalized these results and introduced several new constructions for $n = 2^{2m} - 1$ or $n = p^m - 1$, where p and m are both primes. Most recently, Liu and Liao [18] introduced two classes of ZDB functions on the group $(\mathbb{Z}_n, +)$.

An $(n, M, d, [w_0, \ldots, w_{q-1}])_q$ *constant composition code* is a code over an abelian group $\{b_0, b_1, \ldots, b_{q-1}\}$ with length n, size M, and minimum Hamming distance d such that in every codeword, the element b_i appears exactly w_i times for every i. A constant composition code is called a *permutation code* if $n = q$ and $w_i = 1$ for all i.

Let $A = \{a_0, \ldots, a_{n-1}\}$ and $B = \{b_0, \ldots, b_{l-1}\}$ be two abelian groups, and let f be a function from A to B. Define $w_i = |\{x \in A : f(x) = b_i\}|$ for $0 \leq i \leq l - 1$. Now define C_f as

$$C_f = \{(f(a_0 + a_i), \ldots, f(a_{n-1} + a_i)) : 0 \leq i \leq n - 1\}. \tag{1}$$

Also let $A_q(n, d, [w_0, w_1, \ldots, w_{q-1}])$ denote the maximum size of an $(n, M, d, [w_0, \ldots, w_{q-1}])_q$ constant composition code. Luo, Fu, Han Vick and Chen [19] developed the following bound for the constant composition codes.

Lemma 1.1 ([19]). *If* $nd - n^2 + (w_0^2 + w_1^2 + \cdots + w_{q-1}^2) > 0$, *then*

$$A_q(n, d, [w_0, w_1, \ldots, w_{q-1}]) \leq \frac{nd}{nd - n^2 + (w_0^2 + w_1^2 + \ldots + w_{q-1}^2)}.$$

Ding [8] introduced the next result to construct constant composition codes from ZDB functions.

Proposition 1.2 ([8]). *If* $f : A \to B$ *is a zero-difference-*δ*-balanced function, then the* C_f *of* (1) *is an* $(n, n, n - \delta, [w_0, \ldots, w_{l-1}])_l$ *constant composition code* (*CCC*) *over* B, *and is optimal with respect to the Luo-Fu-Vinck-Chen bound of Lemma 1.1.*

Binary constant composition codes have relatively a long history. Non-binary constant composition codes were also studied since the 60's. Both algebraic and combinatorial aspects of non-binary constant composition codes have been explored so far. For more information one can check [1,4–7,12,13,19] and the references therein.

The remaining part of the correspondence is organized as follows. In Section 2, we present some basic notations and definitions on cyclotomic polynomials and their decompositions into irreducible polynomials. In Section 3, we introduce some new classes of ZDB functions which generalize the classes introduced by Luo and Liao [18]. In Section 4, we extend a result introduced

by Claude et al. [3] regarding zero-difference-p-balanced functions of the form $F_T(x) = x^{p+1} + \alpha tr_{K/F}(\beta x^{p+1})$ over $\mathbb{F}_{p^n}$ when n is even. In Section 5, we use the results from Section 3 to construct new classes of optimal constant composition codes.

2. Preliminaries

We first discuss briefly about *cyclotomic cosets* and their relations with cyclotomic polynomials.

Definition. The the set $C_j = \{jp^k \pmod n, k \in \mathbb{N}\}$ is called the cyclotomic coset of j modulo n (relative to powers of p).

Clearly, the cyclotomic cosets modulo n form a partition of $\mathbb{Z}_n$. Assuming $\gcd(n, p) = 1$, we have

$$x^n - 1 = \prod_{t=1}^{h} f_t(x) \quad \text{with} \quad f_t(x) = \prod_{i \in C_{j_t}} (x - \alpha^i),$$

where α is a primitive nth root of unity (which exists in an extension field of $\mathbb{F}_p$ since $\gcd(n, p) = 1$), and $C_{j_1}, \ldots, C_{j_h}$ are the distinct cyclotomic cosets modulo n. Recall also that for $n \geq 3$,

$$x^n - 1 = \prod_{m|n} \mathcal{Q}_m,$$

where $\mathcal{Q}_m$ denotes the m-th cyclotomic polynomial, see [17, Theorem 2.45]. The cyclotomic polynomial $\mathcal{Q}_m$ factors into irreducible polynomials $f_1, \ldots, f_{\varphi(m)/d} \in \mathbb{F}_p[x]$, each of degree d, where $d = ord_m p$ and φ is the Euler φ-function. Here $ord_m p$ denotes the smallest integer l, such that $p^l \equiv 1 \pmod m$. So precisely, we can write

$$\mathcal{Q}_m = f_1 \cdots f_{\varphi(m)/d} \quad \text{with} \quad f_t(x) = \prod_{j \in C_t} (x - \alpha^j), \tag{2}$$

where $C_1, \ldots, C_{\varphi(m)/d}$ are the cyclotomic cosets modulo n relative to powers of p (see [17, Theorem 2.47], [21, Sect. 4.4]). Also $\nu(l)$ denotes the 2-adic valuation of an integer l, i.e., $2^{\nu(l)}$ is the largest power of 2 which divides l.

Lemma 2.1 ([20, Lemma 2])**.** *Let $m = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$ be odd, relatively prime to p, $d_i = ord_{q_i} p$, $1 \leq i \leq k$, and $d = ord_m p$. Suppose the irreducible factors of $\mathcal{Q}_m$ are $f_1, \ldots, f_{\varphi(m)/d}$.*

(i) *The polynomials $f_1, \ldots, f_{\varphi(m)/d}$ are self-reciprocal if and only if $\nu(d_1) = \nu(d_2) = \cdots = \nu(d_k) > 0$.*

In particular, if m is prime, then $f_1, \ldots, f_{(m-1)/d}$ are self-reciprocal if and only if d is even.

(ii) *If $\nu(d_i) \neq \nu(d_j)$ for some $1 \leq i, j \leq k$, then none of the polynomials f_t, $1 \leq t \leq \varphi(m)/d$, is self-reciprocal, and for each t, $1 \leq t \leq \varphi(m)/d$, there exists a unique $t' \neq t$, $1 \leq t' \leq \varphi(m)/d$, such that $f_{t'} = f_t^*$ is the reciprocal of f_t.*

By Lemma 2.1 we see that the polynomial $f_t(x)$ in (2) is self-reciprocal if and only if C_{j_t}, containing the integer j_t, also contains its inverse $-j_t$ modulo n. If this is not the case, then there is another cyclotomic coset $C_{j_{t'}} = C_{n-j_t}$ consisting of the inverses of the elements of C_{j_t}. Then $f_{t'}$ is the reciprocal of f_t.

3. New classes of ZDB functions

In this section, we generalize two results of [18, Theorems 2.1 and 2.2] based on the properties of cyclotomic polynomials and cyclotomic cosets.

Theorem 3.1. *Let $(p, n = q)$ be a pair of two different odd primes with $d = ord_q p$.*

(i) *If d is even, then there exists a ZDB function with parameters*

$$(q, 1 + \frac{q-1}{d}, d - 1).$$

(ii) *If d is odd, then there exists a ZDB function with parameters*

$$(q, 1 + \frac{q-1}{2d}, 2d - 1).$$

Proof. We have $x^q - 1 = Q_1 Q_q$, where

$$\mathcal{Q}_q = f_1 \cdots f_{(q-1)/d} \quad \text{with} \quad f_t(x) = \prod_{j \in C_t} (x - \alpha^j),$$

$C_1, \ldots, C_{(q-1)/d}$ are the cyclotomic cosets modulo q relative to powers of p and α is a primitive nth root of unity (which exists in an extension field of $\mathbb{F}_p$).

(i) If $d = ord_n p$ is even, then from Lemma 2.1 we get that f_t's are all irreducible and self-reciprocal and of degree d. Following the same technique mentioned in [18], we define

$$\begin{aligned} f: \quad (\mathbb{Z}_n, +) &\to (\mathbb{Z}_n, +) \\ x &\mapsto i_x, \end{aligned}$$

where i_x is the coset leader of C_t such that $x \in C_t$.

Now we know that $\mathbb{Z}_n = C_0 \cup C_1 \cup C_2 \cup \cdots \cup C_{(q-1)/d}$ and $|C_i| = d$ except C_0 which is a singleton set. So $|Imf| = 1 + \frac{q-1}{d}$. For any given $a \not\equiv 0 \pmod{n}$, it suffices to prove that the number of x such that $f(x + a) = f(x)$ is always $d - 1$. Now $f(x + a) = f(x) \iff i_{x+a} = i_x \iff x, x + a \in C_i$ for some $i \neq 0 \iff \alpha^x, \alpha^{x+a}$ are roots of same $f_t \iff x + a \equiv p^k x \pmod{n}$ for $1 \leq k \leq d - 1 \iff$ unique solution $x \equiv \frac{a}{p^k - 1} \pmod{n}$ as $\gcd(p^k - 1, q) = 1$ for $1 \leq k \leq d - 1$. Therefore, $|\{x \in \mathbb{Z}_n : f(x + a) - f(x) = 0\}| = d - 1$ for any $a \not\equiv$

$0(\text{mod } n)$. So the function f defined above is a ZDB function with parameters $(q, 1+\frac{q-1}{d}, d-1)$.

(ii) If $d = ord_n p$ is odd, then $C_t \neq C_{-t}$ and $C_t \cap C_{-t} = \phi$ for $t \neq 0$. So following the same argument in [18] and (i), we define the coset leader of $C_t \cup C_{-t}$ to be the least integer in that set. Then we define

$$f: \quad (\mathbb{Z}_n, +) \to (\mathbb{Z}_n, +)$$
$$x \mapsto i_x,$$

where i_x is the coset leader of $C_t \cup C_{-t}$ containing x. So $|Imf| = 1 + \frac{q-1}{2d}$.

Now for $a \not\equiv 0 \pmod{n}$, $f(x+a) = f(x) \iff i_{x+a} = i_x \iff x, x+a \in C_t \cup C_{-t}$ for some t. We have the following two cases:

Case 1: $f_t(\alpha^x) = 0$, i.e., $x \in C_t$. Then $f_t(\alpha^{x+a}) = 0$ or $f_{-t}(\alpha^{x+a}) = 0$. So we must have $1 \leq k \leq d-1$ or $1 \leq r \leq d$ such that

$$x + a \equiv p^k x \pmod{n} \tag{3}$$

or

$$x + a \equiv -p^r x \pmod{n}. \tag{4}$$

We get a unique solution from (3) that is $x \equiv \frac{a}{p^k-1} \pmod{n}$ as $\gcd(p^k - 1, q) = 1$ for $1 \leq k \leq d-1$ and (4) has unique solution $x \equiv \frac{-a}{p^r+1} \pmod{n}$ as $\gcd(p^r + 1, q) = 1$ for $1 \leq r \leq d$. As $ord_n p = d$ is odd, we cannot have $p^r \equiv -1 \pmod{n}$ for $1 \leq r \leq d$. Besides, (3) and (4) cannot have common solutions as f_t and f_{-t} do not have any common roots.

Case 2: $f_{-t}(\alpha^x) = 0$, i.e., $x \in C_{-t}$. We have the same solutions like **Case 1**. Therefore, $|\{x \in \mathbb{Z}_n : f(x+a) - f(x) = 0\}| = 2d - 1$ for any $a \not\equiv 0 \pmod{n}$. So the function f defined above is a ZDB function with parameters $(q, 1 + \frac{q-1}{2d}, 2d-1)$. □

Example 3.2. For $p = 7$ and $n = 19$, we have the complete list of cosets:

$$[[0], [1, 7, 11], [2, 3, 14], [4, 6, 9], [5, 16, 17], [8, 12, 18], [10, 13, 15]].$$

Here $ord_{19} 7 = 3$. If we consider the function f in Theorem 3.1, then $|Im(f)| = 4$. For $a = 2$ the pairs $(x, x+a)$ having the same images are $\{(13, 15), (4, 6), (14, 16), (3, 5), (18, 1)\}$.

Remark 3.3. For the particular case of $(p, n = 2p-1)$ both odd primes, the first part of Theorem 3.1 reduces to Theorem 2.1 and the second part reduces to Theorem 2.2 of [18], respectively.

Theorem 3.4. *Let p, q be two different odd primes and let $ord_q p = ord_{q^2} p = d$. Then there exists a ZDB function with parameters*

$$(q^2, 1 + \frac{q^2-1}{d}, d-1) \quad \textit{if } d \textit{ is even},$$
$$(q^2, 1 + \frac{q^2-1}{2d}, 2d-1) \quad \textit{if } d \textit{ is odd}.$$

Proof. We have

$$x^n - 1 = Q_1 Q_q Q_{q^2}.$$

First, we consider $ord_q p = ord_{q^2} p = d$ and d is even, then we can write $Q_q(x) = \prod_{i=1}^{\frac{q-1}{d}} f_i$ and $Q_{q^2}(x) = \prod_{j=1}^{\frac{q(q-1)}{d}} h_j$, where f_i and h_j are irreducible self-reciprocal polynomials of degree d. We define the same function

$$\begin{aligned} f: \quad (\mathbb{Z}_n, +) &\to (\mathbb{Z}_n, +) \\ x &\mapsto i_x, \end{aligned}$$

where i_x is the coset leader of C_t such that $x \in C_t$. So $|Im(f)| = 1 + \frac{q-1}{d} + \frac{q(q-1)}{d}$. For any given $a \not\equiv 0 \pmod n$, $f(x+a) = f(x) \iff i_{x+a} = i_x \iff x, x+a \in C_t$. So $x, x+a \in C_t$ for same t. Then $x + a \equiv xp^k \pmod n$ for $1 \le k \le d-1$ which implies

$$x(p^k - 1) \equiv a \pmod n,\ 1 \le k \le q-1. \tag{5}$$

Now (5) has unique solution $x \equiv \frac{a}{p^k - 1} \pmod n$ as $\gcd(p^k - 1, n) = 1$ for $1 \le k \le d-1$. Therefore, $|\{x \in \mathbb{Z}_n : f(x+a) - f(x) = 0\}| = d - 1$ for any $a \not\equiv 0 \pmod n$. So the function f defined above is a ZDB function with parameters $(q^2, 1 + \frac{q^2-1}{d}, d-1)$.

Now when d is odd, we follow the similar arguments used in Theorem 3.1. Using the same function f, we can get the ZDB function with parameters $(q^2, 1 + \frac{q^2-1}{2d}, 2d-1)$. □

Example 3.5. For $p = 19$ and $n = 169$, we have the complete list of cosets: [[0], [1, 19, 22, 23, 70, 80, 89, 99, 146, 147, 150, 168], [2, 9, 29, 38, 44, 46, 123, 125, 131, 140, 160, 167], [3, 41, 57, 66, 69, 71, 98, 100, 103, 112, 128, 166], [4, 18, 58, 76, 77, 81, 88, 92, 93, 111, 151, 165], [5, 12, 54, 59, 62, 74, 95, 107, 110, 115, 157, 164], [6, 27, 31, 37, 55, 82, 87, 114, 132, 138, 142, 163], [7, 8, 15, 17, 36, 53, 116, 133, 152, 154, 161, 162], [10, 21, 24, 45, 51, 61, 108, 118, 124, 145, 148, 159], [11, 35, 40, 73, 75, 84, 85, 94, 96, 129, 134, 158], [13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, 156], [14, 16, 30, 34, 63, 72, 97, 106, 135, 139, 153, 155], [20, 42, 47, 48, 67, 79, 90, 102, 121, 122, 127, 149], [25, 28, 32, 43, 60, 68, 101, 109, 126, 137, 141, 144], [33, 49, 50, 56, 64, 83, 86, 105, 113, 119, 120, 136]]. Here $ord_{169} 19 = ord_{13} 19 = 12$. If we consider the function introduced in Theorem 3.4, then $|Im(f)| = 15$. For $a = 1$ the pairs $(x, x+a)$ having the same images are $\{(47, 48), (146, 147), (119, 120), (161, 162), (92, 93), (84, 85), (76, 77), (7, 8), (49, 50), (22, 23), (121, 122)\}$.

Remark 3.6. The condition mentioned in the above theorem $ord_q p = ord_{q^2} p$ can be found for some odd primes p, q. For example $ord_7 3 = ord_{7^2} 3 = 5, ord_{11} 3 = ord_{11^2} 3 = 5$ etc. But for $p = 2$, it is extremely rare to find q with that condition. Actually, when $ord_q 2 = ord_{q^2} 2$, then q is a Wieferich prime, i.e., $2^{q-1} \equiv 1 \pmod{q^2}$. It has been found by computer search [16] that the only Wieferich primes less than 1.25×10^{15} are 1039 and 3511.

4. Zero-difference-p-balanced functions over $\mathbb{F}_{p^n}$

Let p be an odd prime and set $F = GF(p)$ and $K = GF(p^n)$. Quadratic zero-difference-p-balanced functions over F_{p^n} have been discussed widely by Claude et al. [3]. They considered $F(x) = x^{p+1} + \alpha tr_{K/F}(\beta x^{p+1} + \gamma x^{p^3+1})$ over K and proved that $F(x)$ is zero-difference-p-balanced with some restrictions on $\alpha, \beta, \gamma \in K$. But they verified the result only for $n = 4$ and 6. Our next result will be an extension of Theorem 1 of [3]. We need to recall that $K^* = K - \{0\}$ and $tr_{K/F}(x) = \sum_{i=0}^{n-1} x^{p^i}$.

Theorem 4.1. *Let n be even. Let*

$$F_T(x) = x^{p+1} + \alpha tr_{K/F}(\beta x^{p+1}),$$

where $\alpha, \beta \in K^*$. Then F_T is a zero-difference-p-balanced function if and only if $tr_{K/F}(\alpha\beta) \neq -1$.

Proof. Instead of looking at $F_T(x + a) - F_T(x) = 0$ we look at

$$F_T(ax + a) - F_T(ax) = 0. \tag{6}$$

The goal is to prove that (6) has exactly p solutions in K for every $a \in K^*$.

Expanding (6) yields

$$a^{p+1}(x^p + x + 1) + \alpha tr_{K/F}(\beta a^{p+1}(x^p + x + 1)) = 0. \tag{7}$$

As n is even, $x^p + x + 1$ has p roots in K (Lemma 6 in [3]). Simply, any root of $x^p + x + 1$ is a solution of (7). Hence (7) has at least p solutions for every $a \in K^*$. The goal is then to prove that (7) has no other solutions.

Divide (7) by α

$$\alpha^{-1}a^{p+1}(x^p + x + 1) + tr_{K/F}(\beta a^{p+1}(x^p + x + 1)) = 0. \tag{8}$$

Set $k = \alpha^{-1}a^{p+1}(x^p + x + 1)$. As the image of $tr_{K/F}$ is in F, we have $k \in F$. Then (8) becomes:

$$k + tr_{K/F}(\beta\alpha k) = 0$$

or

$$k + k tr_{K/F}(\beta\alpha) = 0.$$

If $k = 0$, then $x^p + x + 1 = 0$ and we have one of the known roots. So suppose $k \neq 0$. We get $tr_{K/F}(\beta\alpha) = -1$. Thus if $tr_{K/F}(\beta\alpha) \neq -1$ there are no additional solutions to (7) and F_T is zero-difference-p-balanced. □

Remark 4.2. This theorem does extend Theorem 1(i) of [3]. The function considered in [3] is

$$F(x) = x^{p+1} + \alpha tr_{K/F}(\beta x^{p+1} + \gamma x^{p^3+1}).$$

Since $n = 4$ we have $x^{p^4} = x$. Thus

$$\begin{aligned} tr_{K/F}(\gamma x^{p^3+1}) = tr_{K/F}((\gamma x^{p^3+1})) &= tr_{K/F}(\gamma^p x^{p^4+p}) \\ &= tr_{K/F}(\gamma^p x^{p+1}). \end{aligned}$$

Hence

$$F(x) = x^{p+1} + \alpha tr_{K/F}((\beta + \gamma^p)x^{p+1}).$$

Apply the theorem. Then $F(x)$ is ZDB if and only if $tr_{K/F}(\alpha(\beta + \gamma^p)) \neq -1$. Again

$$tr_{K/F}(\alpha\gamma^p) = tr_{K/F}((\alpha\gamma^p)^{p^3}) = tr_{K/F}(\alpha^{p^3}\gamma^{p^4}) = tr_{K/F}(\alpha^{p^3}\gamma).$$

Thus the theorem says $F(x)$ is ZDB if and only if $tr_{K/F}(\alpha\beta + \alpha^{p^3}\gamma^{p^4}) \neq -1$. That is the statement of Theorem 1(i) in [3].

5. Some new classes of constant composition derived from zero-difference balanced functions

In this section, we use the above mentioned ZDB functions to construct constant composition codes.

In Theorems 3.1 and 3.4, we have introduced zero difference $d-1$ and $2d-1$-balanced functions, where $(p, n = q)$ and $(p, n = q^2)$, respectively, where p, q are distinct odd primes. Using those results we can introduce the following two CCCs.

Theorem 5.1. *Suppose that $(p, n = q)$ are distinct odd primes with $d = ord_q p$. If f is the function defined in Theorem 3.1, then C_f of (1) is an optimal CCC over $\mathbb{F}_q$ with parameters*

$$(q, q, q - (d-1), [1, \underbrace{d, d, \ldots, d}_{\frac{q-1}{d}}, \underbrace{0, \ldots, 0}_{\frac{(q-1)(d-1)}{d}}])$$

if d is even, and

$$(q, q, q - (2d-1), [1, \underbrace{2d, \ldots, 2d}_{\frac{q-1}{2d}}, \underbrace{0, \ldots, 0}_{\frac{(q-1)(2d-1)}{2d}}])$$

if d is odd.

Proof. The proof follows from Theorem 3.1 and Proposition 1.2. □

Example 5.2. For $n = q = 113$ and $p = 7$, $d = ord_q p = 14$. Then C_f of (1) with f defined in Theorem 3.1 is an optimal CCC over $\mathbb{F}_{113}$ with parameters $(113, 113, 100, [1, \underbrace{14, \ldots, 14}_{8 \text{ times}}, \underbrace{0, \ldots, 0}_{104 \text{ times}}])$.

Theorem 5.3. *Suppose that p, q are two different odd primes with $n = q^2$. Also let $ord_q p = ord_{q^2} p = d$. If f is the function defined in Theorem 3.4, then C_f of (1) is an optimal CCC over $\mathbb{F}_p$ with parameters*

$$(q^2, q^2, q^2 - (d-1), [1, \underbrace{d, d, \ldots, d}_{\frac{q^2-1}{d}}, \underbrace{0, \ldots, 0}_{\frac{(q^2-1)(d-1)}{d}}])$$

if d is even and

$$(q^2, q^2, q^2-(2d-1), [1, \underbrace{2d, 2d, \ldots, 2d}_{\frac{q^2-1}{2d}}, \underbrace{0, \ldots, 0}_{\frac{(q^2-1)(2d-1)}{2d}}])$$

if d is odd.

Proof. The proof follows from Theorem 3.4 and Proposition 1.2. □

Example 5.4. For $p = 19$ and $n = 169$, $ord_{169}19 = ord_{13}19 = 12$. If we consider the function introduced in Theorem 4.1, then $Im(f) = 15$. Then C_f of (1) with f defined in Theorem 3.1 is an optimal CCC over $\mathbb{F}_{169}$ with parameters $(169, 169, 158, [1, \underbrace{15, \ldots, 15}_{14 \text{ times}}, \underbrace{0, \ldots, 0}_{154 \text{ times}}])$.

Remark 5.5. As Theorem 4.1 extends Theorem 1 of [3], we can definitely get optimal CCC with parameter

$$(p^n, p^n, p^n-p, [1, \underbrace{p+1, p+1, \ldots, p+1}_{\frac{p^n-1}{p+1}}, \underbrace{0, \ldots, 0}_{\frac{(p^n-1)p}{p+1}}])$$

when n is even.

6. Conclusion

In this paper, we have generalized some results mentioned in [18]. The results introduced by Liao et al. [18] were for particular pair $(n = 2p-1, p)$ of odd prime numbers. We have extended those results for any pair (q, p) of distinct odd primes. We have also introduced a class of ZDB functions for $n = q^2$ with some restrictions. Later, we have extended a result on ZDB functions of the type $F_T(x) = x^{p+1} + \alpha tr_{K/F}(\beta x^{p+1})$, introduced by Claude et al. [3]. Ding used ZDB functions to construct optimal constant composition codes. Similar constructions are also possible in our cases.

Acknowledgement. I would like to thank my advisor Professor Robert Fitzgerald (retired) from department of mathematics, Southern Illinois University, Carbondale, USA for his valuable advice leading to writing this paper.

References

[1] G. T. Bogdanova and S. N. Kapralov, *Enumeration of optimal ternary constant-composition codes*, Probl. Inf. Transm. **39** (2003), no. 4, 346–351; translated from Problemy Peredachi Informatsii **39** (2003), no. 4, 35–40. https://doi.org/10.1023/B:PRIT.0000011273.98799.a8

[2] 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. https://doi.org/10.1109/TIT.2013.2255114

[3] C. Carlet, G. Gong, and Y. Tan, *Quadratic zero-difference balanced functions, APN functions and strongly regular graphs*, Des. Codes Cryptogr. **78** (2016), no. 3, 629–654. https://doi.org/10.1007/s10623-014-0022-x

[4] Y. M. Chee, A. C. H. Ling, S. Ling, and H. Shen, *The PBD-closure of constant-composition codes*, IEEE Trans. Inform. Theory **53** (2007), no. 8, 2685–2692. https://doi.org/10.1109/TIT.2007.901175

[5] W. Chu, C. J. Colbourn, and P. Dukes, *Tables for constant composition codes*, J. Combin. Math. Combin. Comput. **54** (2005), 57–65.

[6] W. Chu, C. J. Colbourn, and P. Dukes, *On constant composition codes*, Discrete Appl. Math. **154** (2006), no. 6, 912–929. https://doi.org/10.1016/j.dam.2005.09.009

[7] C. J. Colbourn, T. Klove, and A. C. H. Ling, *Permutation arrays for powerline communication and mutually orthogonal Latin squares*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1289–1291. https://doi.org/10.1109/TIT.2004.828150

[8] C. Ding, *Optimal constant composition codes from zero-difference balanced functions*, IEEE Trans. Inform. Theory **54** (2008), no. 12, 5766–5770. https://doi.org/10.1109/TIT.2008.2006420

[9] C. Ding, *Optimal and perfect difference systems of sets*, J. Combin. Theory Ser. A **116** (2009), no. 1, 109–119. https://doi.org/10.1016/j.jcta.2008.05.007

[10] C. Ding and Y. Tan, *Zero-difference balanced functions with applications*, J. Stat. Theory Pract. **6** (2012), no. 1, 3–19. https://doi.org/10.1080/15598608.2012.647479

[11] C. Ding, Q. Wang, and M. Xiong, *Three new families of zero-difference balanced functions with applications*, IEEE Trans. Inform. Theory **60** (2014), no. 4, 2407–2413. https://doi.org/10.1109/TIT.2014.2306821

[12] C. Ding and J. Yin, *Algebraic constructions of constant composition codes*, IEEE Trans. Inform. Theory **51** (2005), no. 4, 1585–1589. https://doi.org/10.1109/TIT.2005.844087

[13] C. Ding and J. Yin, *Combinatorial constructions of optimal constant-composition codes*, IEEE Trans. Inform. Theory **51** (2005), no. 10, 3671–3674. https://doi.org/10.1109/TIT.2005.855612

[14] L. Jiang and Q. Liao, *Generalized zero-difference balanced functions and their applications*, Chinese J. Contemp. Math. **37** (2016), no. 3, 201–216; translated from Chinese Ann. Math. Ser. A **37** (2016), no. 3, 243–260.

[15] L. Jiang and Q. Liao, *On generalized zero-difference balanced functions*, Commun. Korean Math. Soc. **31** (2016), no. 1, 41–52. https://doi.org/10.4134/CKMS.2016.31.1.041

[16] J. Knauer and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), no. 251, 1559–1563. https://doi.org/10.1090/S0025-5718-05-01723-0

[17] R. Lidl and H. Niederreiter, *Finite fields*, second edition, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.

[18] H. Liu and Q. Liao, *Some new constructions for generalized zero-difference balanced functions*, Internat. J. Found. Comput. Sci. **27** (2016), no. 8, 897–908. https://doi.org/10.1142/S0129054116500362

[19] Y. Luo, F. Fu, A. J. H. Vinck, and W. Chen, *On constant-composition codes over Z_q*, IEEE Trans. Inform. Theory **49** (2003), no. 11, 3010–3016. https://doi.org/10.1109/TIT.2003.819339

[20] W. Meidl and A. Topuzoğlu, *Quadratic functions with prescribed spectra*, Des. Codes Cryptogr. **66** (2013), no. 1-3, 257–273. https://doi.org/10.1007/s10623-012-9690-6

[21] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, second edition, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., New York, 1989.

[22] L.-Z. Shen, J.-J. Wen, and F.-W. Fu, *A new class of zero-difference balanced functions*, Inform. Process. Lett. **136** (2018), 9–11. https://doi.org/10.1016/j.ipl.2018.03.011

[23] Z. Yi, Z. Lin, and L. Ke, *A generic method to construct zero-difference balanced functions*, Cryptogr. Commun. **10** (2018), no. 4, 591–609. https://doi.org/10.1007/s12095-017-0247-4

[24] Z. Zha and L. Hu, *Cyclotomic constructions of zero-difference balanced functions with applications*, IEEE Trans. Inform. Theory **61** (2015), no. 3, 1491–1495. https://doi.org/10.1109/TIT.2014.2388231

[25] 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. https://doi.org/10.1109/TIT.2011.2171418

Sankhadip Roy
Department of Basic Science and Humanities
University of Engineering and Management
Kolkata-700160, India
Email address: sankhadiproy@gmail.com