Schemes, Codes and Quadratic Zero-Difference Balanced Functions

Yin Tan, and Guang Gong

Abstract

Zero-difference balanced (ZDB) functions were introduced by Ding for the constructions of optimal and perfect systems of sets and of optimal constant composition codes. In order to be used in these two areas of application, ZDB functions have to be defined on cyclic groups. In this paper, we investigate quadratic ZDB functions from the additive group of $\mathbb{F}_{p^n}$ to itself of the form $G(x^{p^t+1})$, where G is injective on the set of (p^t+1)-th power of $\mathbb{F}_{p^n}$. By choosing different values of p and t, such ZDB functions include certain quadratic APN and PN functions as special cases, which gives a "trans-characteristic" interpretation of these functions. We first provide a geometric characterization of such ZDB functions, and then make use of them to give a construction of a 4-class association schemes. We further determine the weight distributions of the linear codes from such ZDB functions. This includes some of the previous work on the codes generated in the same manner from APN and PN functions as special cases.

Keywords

Zero-difference balanced function; APN function; PN function; quadratic function; Schur ring; association scheme; linear code.

I. Introduction

Let F be a function from an Abelian group $(A,+)$ to an Abelian group $(B,+)$. For any $a \in A$ and $b \in B$, the numerical function $\delta_F(a,b)$ is defined by

$$\delta_F(a,b) = \#\{x \in A \mid F(x+a) - F(x) = b\}, \tag{1}$$

where $\#$ denotes the size of a set. Let Δ_F be the maximal value of $\delta_F(a,b)$ when a runs through nonzero elements of A and b through all elements of B; then we call F a *differentially Δ_F-uniform function*. The study of the functions with small Δ_F is motivated by their wide applications in cryptography when A and B are finite fields. For instance, they have been used as the Substitution boxes in many block ciphers with substitution-permutation network structure [31]. When $A = B = \mathbb{F}_{p^n}$, it is well known that the smallest value of Δ_F is 2 when p is 2; and is 1 when p is an odd prime. Such functions are called *almost perfect nonlinear* (APN) and *perfect nonlinear* (PN), respectively. In addition to the applications in cryptography, APN and PN functions are related to other topics in algebra [34], coding theory [6], [8], [29], [39], sequences [24], [25] and combinatorics [9],[11],[12],[20],[21],[36]. One may refer to [7], [10] for the well-rounded surveys of APN and PN functions.

Y. Tan and G. Gong are with the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, N2L 3G1 Canada. e-mail: {yin.tan, ggong}@uwaterloo.ca.

In [15], [16], Ding introduced the notion of zero-difference balanced functions for the construction of optimal constant composition codes and of optimal and perfect difference systems of sets. A function F is called *zero-difference δ-balanced* (ZDB) if $\delta_F(a,0)=\delta$ for all nonzero a in A. Since then, several classes of ZDB functions have been constructed and more of their applications have been investigated, see [5], [15], [16], [18], [17], [35], [40] and the references therein. It is worth mentioning that the known constructions of ZDB functions are mostly defined on a cyclic group (usually a subgroup of $\mathbb{F}_{p^n}^*$). In order to satisfy the requirement for the specific applications of ZDB functions as in [16], [18]. In this paper, we will investigate ZDB functions on the additive group of $\mathbb{F}_{p^n}$, which is a non-cyclic group when $n>1$. More precisely, we shall consider functions with the following property $\mathfrak{P}$, which are zero-difference p^t-balanced as shown in [11, Corollary 1].

Definition 1 (Property $\mathfrak{P}$). *: Let F be a quadratic function from $\mathbb{F}_{p^n}$ to itself with $F(0)=0$. The function F is of the from $F(x)=G(x^{p^t+1})$, where $n=2kt$ when $t>0$; or n is any positive integer when $t=0$. Furthermore, the function G restricted to the set of p^t+1 powers of $\mathbb{F}_{p^n}^*$, denoted by C_{p^t+1}, is injective.*

The motivation to study functions with Property $\mathfrak{P}$ comes from their applications to construct strongly regular graphs [11] and association schemes (as will be discussed in Section IV), and also from their relationship to APN and PN functions. Namely, when $p=2$ and $t=1$, there exist quadratic APN functions on $\mathbb{F}_{2^{2k}}$ that are of the form $G(x^{2^1+1})=G(x^3)$, where G is injective on the set of cubes. For example, the well-known APN function $x^3+\mathrm{Tr(x^9)}$ can be written as $(x+\mathrm{Tr(x^3)})\circ \mathrm{x}^3$; and the computer search discovered 18 such APN functions on $\mathbb{F}_{2^8}$ [37], [38]. Similarly, when p is odd and $t=0$, there exist quadratic PN functions that are of the form $G(x^{p^0+1})=G(x^2)$, where G is injective on the set of squares (see [27], [36]). All currently known PN functions, including the non-quadratic Coulter-Matthews PN functions, are of the form $G(x^2)$. Therefore, the functions with Property $\mathfrak{P}$ provide a "trans-characteristic" point of view of quadratic APN and PN functions by choosing different values of p and t. The examples of the functions with Property $\mathfrak{P}$ for other values of p and t can be found in [11, Theorem 1]. It is the aim of this paper to investigate the properties of the functions with Property $\mathfrak{P}$ and explore their applications in combinatorics and coding theory, and consequently provide more applications of quadratic APN and PN functions.

Let F be a function with Property $\mathfrak{P}$. Note that when $p=2$ and $t=0$, the function F with Property $\mathfrak{P}$ is of the form $F(x)=G(x^2)$, therefore F is quadratic permutation on $\mathbb{F}_{2^n}$ since x^2 is a permutation. This implies that F is a zero-difference 0-balanced function and its differential uniformity can be any integer 2^i for $1\le i\le n-1$ (since $F(x+a)-F(x)-F(a)$ is linear). We shall assume $t>0$ when $p=2$ in the rest of the paper. It is easy to see that the difference function $L_s(x)=F(x+s)-F(x)$ is affine for any nonzero $s\in\mathbb{F}_{p^n}$ since F is quadratic. In Section III, we study the distribution of the image sets of L_s when s runs through $\mathbb{F}_{p^n}^*$. Denoting $H_s=\mathrm{Im}(L_s)$ and $\mathcal{H}=\{H_s : s\in\mathbb{F}_{p^n}^*\}$, we show that H_s is a subspace of $\mathbb{F}_{p^n}$ (note that H_s may be an affine subspace for an arbitrary quadratic function); and that for any $H_s\in\mathcal{H}$, there are $p^{2t}-1$ elements s' which give rise to the same H_s. Moreover, the set of such elements s' together with 0 consist of a subspace of $\mathbb{F}_{p^n}$ with dimension $2t$.

In Section IV, we provide a construction of 4-class association schemes by functions with Property $\mathfrak{P}$. Association scheme was first introduced by Bose and Nair in [3] (defined in Section II-B). It is an important topic in combinatorics and have many applications, for instance in coding theory [14]. We begin by determining the magnitude of the Walsh coefficients $\widehat{F}(a,b)$ for all $a,b \in \mathbb{F}_{p^n}$. Then we characterize which a,b may have the same magnitude of the Walsh coefficient. Based on this result, we show that functions with Property $\mathfrak{P}$ can be used to construct a 4-class association scheme when $t>0$.

In Section V, we study the linear codes from functions with Property $\mathfrak{P}$. More precisely, we consider the linear code $\mathcal{C}_F$ generated by the matrix C_F, where

$$C_F = \begin{bmatrix} \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{bmatrix}_{x\in\mathbb{F}_{p^n}^*}. \tag{2}$$

Here the columns of C_F are ordered with respect to some ordering of the elements of $\mathbb{F}_{p^n}^*$; and we regard the finite field $\mathbb{F}_{p^n}$ as a vector space of dimension n over $\mathbb{F}_p$. The weight distribution of the code $\mathcal{C}_F$ has been studied in [6] when F is an APN function; and in [8], [22], [39] when F is one of the known PN functions. We determine the weight distribution of the code $\mathcal{C}_F$ in Theorem 4 for any values of p and t. This includes some results in [6], [8], [22], [39] as special cases.

The rest of the paper is organized as follows. Section II gives necessary definitions and results that will be used throughout the paper. The combinatorial properties of ZDB functions with Property $\mathfrak{P}$ are presented in Section III. We give the construction of the association schemes in Section IV. The weight distribution of the linear code $\mathcal{C}_F$ is determined in Sections V, VI, VII. Some concluding remarks are given in Section VIII.

II. Preliminaries

In this section, we introduce the definitions and results that will be used in the rest of the paper.

A. Group rings, character theory and Walsh transform

Group rings and character theory of finite fields are useful tools to study functions defined on $\mathbb{F}_{p^n}$ and their related combinatorial objects. We briefly review some definitions and results. For more details on group rings and character theory, please refer to [33] and [30] respectively. In the following, we assume G is a finite Abelian group. The group algebra $\mathbb{C}[G]$ consists of all formal sums $\sum_{g\in G} a_g g, a_g \in \mathbb{C}$. The component-wise addition and multiplication of two elements in $\mathbb{C}[G]$ are defined by

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g+b_g)g,$$

and

$$\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g = \sum_{g\in G}\left(\sum_{h\in G} a_h \cdot b_{gh^{-1}}\right) g.$$

A subset S of G is identified with the group ring element $\sum_{s\in S} s$ in $\mathbb{C}[G]$, which is also denoted by S by abuse of notation. For $A=\sum_{g\in G} a_g g$ in $\mathbb{C}[G]$ and t an integer, define $A^{(t)}=\sum_{g\in G} a_g g^t$.

A character χ of a finite Abelian group G is a homomorphism from G to $\mathbb{C}^*$. It is called *principal* if $\chi(c)=1$ for all $c\in G$, otherwise it is called *non-principal*. All characters of G form a group, which is denoted by $\widetilde{G}$. This *character group* $\widetilde{G}$ is isomorphic to G. The action of any character χ can be extended to $\mathbb{C}[G]$ by $\chi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \chi(g)$. The following well-known Inversion formula is very useful.

Result 1 (Inversion Formula)**.** *Let* $D = \sum\limits_{g\in G} a_g g \in \mathbb{C}[G]$. *Then*

$$a_g = \frac{1}{|G|}\sum_{\chi\in\widetilde{G}} \chi(D)\chi(g^{-1}).$$

The following result is an application of the Inversion formula.

Result 2. *Let $D_1, D_2 \in \mathbb{C}[G]$ be two group ring elements. Then $D_1 = D_2$ if and only if $\chi(D_1) = \chi(D_2)$ for all characters χ of G.*

For the finite field $\mathbb{F}_{p^n}$, define χ_1 by $\chi_1(x) = \zeta_p^{\mathrm{Tr(x)}}$ for all $x \in \mathbb{F}_{p^n}$, where ζ_p is a complex primitive p-th root of unity. Then χ_1 is an additive character of $\mathbb{F}_{p^n}$. Moreover, every additive character χ is of the form χ_b $(b \in \mathbb{F}_{p^n})$, where χ_b is defined by $\chi_b(x) = \chi_1(bx)$ for all $x \in \mathbb{F}_{p^n}$.

Finally, for a function F from $\mathbb{F}_{p^n}$ to itself, the *Walsh transform* of F is defined as

$$\mathcal{W}_F(a,b) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr(ax+bF(x))}}, \quad a,b \in \mathbb{F}_{p^n},$$

where $\mathrm{Tr(x)}$ is the absolute trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The multiset $\mathcal{W}_F := \{\mathcal{W}_F(a,b) : a,b \in \mathbb{F}_{p^n}\}$ is called the *Walsh spectrum* of F, and $\mathcal{W}_F(a,b)$ is called the *Walsh coefficient* at (a,b).

B. Partial difference sets, Schur rings and association schemes

In the following, we provide the definitions of some combinatorial and algebraic objects. The readers may refer to [1], [2], [23] for more details.

Definition 2 (Partial Difference Set)**.** *Let G be a multiplicative group of order v. A k-subset D of G is called a (v,k,λ,μ) partial difference set (PDS) if each non-identity element in D can be represented as gh^{-1} $(g,h \in D, g \neq h)$ in exactly λ ways, and each non-identity element in $G\backslash D$ can be represented as gh^{-1} $(g,h \in D, g \neq h)$ in exactly μ ways.*

We shall always assume that the identity element 1_G of G is not contained in D. Particularly, D is called *regular* if $D^{(-1)} = D$. Using the group ring language, a k-subset D of G with $1_G \notin D$ is a (v,k,λ,μ)-PDS if and only if the following equation holds:

$$DD^{(-1)} = (k-\mu)1_G + (\lambda-\mu)D + \mu G.$$

If χ is a non-principal character of G, then $\chi(D) \in \left\{\frac{1}{2}\left((\lambda-\mu) \pm \sqrt{(\mu-\lambda)^2 + 4(k-\mu)}\right)\right\}$. Denote these two values by a, b and define $D_a = \{\chi \in \widetilde{G} | \chi(D) = a\}, D_b = \{\chi \in \widetilde{G} | \chi(D) = b\}$, we call D_a and D_b the *dual* PDSs of D. The following result shows that both D_a and D_b are PDSs.

Result 3. *[13] Let G be an Abelian group of order v and D $(\neq \emptyset$ and $\neq G)$ be a regular (v,k,λ,μ)-PDS in G. Then both D_a and D_b are regular PDSs in $\widetilde{G}$ (the parameters are given in [32]).*

Next we introduce the definition of association schemes.

Definition 3 (Association Scheme)**.** *Let V be a finite set of vertices, and let $\{R_0, R_1, \ldots, R_d\}$ be binary relations on V with $R_0 := \{(x, x) : x \in V\}$. The configuration $(V; R_0, R_1, \ldots, R_d)$ is called an association scheme of class d on V if the following holds:*

(1) $V \times V = R_0 \bigcup R_1 \bigcup \cdots \bigcup R_d$ and $R_i \bigcap R_j = \emptyset$ for $i \neq j$;

(2) ${}^tR_i = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where ${}^tR_i := \{(x, y) : (y, x) \in R_i\}$. If $i' = i$, we call R_i is symmetric.

(3) for $i, j, k \in \{0, 1, \ldots, d\}$ and $x, y \in V$ with $(x, y) \in R_k$, the number $\sharp\{z \in V : (x, z) \in R_i, (z, y) \in R_j\}$ is a constant, which is denoted by p_{ij}^k.

Furthermore, an association scheme is said to be symmetric if every R_i is symmetric.

A well-known approach to construct association schemes is to use Schur rings. The Schur ring is defined as follows.

Definition 4 (Schur Ring)**.** *Let G be a finite group and $D_0, \ldots, D_d$ be nonempty subsets of G with the following properties:*

(1) $D_0 = \{e\}$, where e is the identity element of G;

(2) $G = D_0 \bigcup D_1 \bigcup \cdots D_d$ and $D_i \bigcap D_j = \emptyset$ for $i \neq j$;

(3) $D_i^{(-1)} = D_{i'}$ for some $i' \in \{0, \ldots, d\}$, where $D_i^{(-1)} = \{g^{-1} : g \in D_i\}$;

(4) $D_i D_j = \sum_{k=0}^{d} p_{ij}^k D_k$ for all $i, j \in \{0, \ldots, d\}$, where p_{ij}^k are integers.

The subalgebra $\langle D_0, \ldots, D_d \rangle$ of $\mathbb{C}[G]$ generated by $D_0, \ldots, D_d$ is called a Schur ring over G.

The relationship between Schur rings and association schemes is given below.

Result 4. *The configuration $(G; R_0, \ldots, R_d)$ forms an association scheme of class d on G, where $R_i := \{(g, h) : gh^{-1} \in D_i\}$ for $i \in \{0, \ldots, d\}$. Note that if $D_i^{(-1)} = D_i$ for each i, the scheme is symmetric.*

It is well known that a 2-class symmetric association scheme is equivalent to a strongly regular graph, which is the Cayley graph generated by a regular partial difference set (see [4]).

III. Combinatorial properties of ZDB functions with Property $\mathfrak{P}$

Let F be a function satisfying Property $\mathfrak{P}$. For the convenience of the discussions, we first fix some notations which will be used throughout the rest of the paper.

Notations:

- $D_F = \mathrm{Im}(F) = \{F(x) : x \in \mathbb{F}_{p^n}\}$;
- For a positive integer d, $C_d = \{x^d : x \in \mathbb{F}_{p^n}^*\}$;
- For each $s \in \mathbb{F}_{p^n}^*$, $H_s = \{F(x + s) - F(x) : x \in \mathbb{F}_{p^n}\}$;
- $\mathcal{H} = \{H_s : s \in \mathbb{F}_{p^n}^*\}$;
- $\mathcal{H}_1 = \{\chi_b \mid \chi_b$ is trivial on exactly one $H \in \mathcal{H}\}$, where χ_b is an additive character of $\mathbb{F}_{p^n}$;
- $\epsilon_\ell = (-1)^\ell$ for $\ell \in \mathbb{N}$.

We shall need the following results for the discussions in this Section, whose proof may be found in [36, Theorem 2.2] and [11, Theorem 2, Corollary 3, Proposition 3, Theorem 3] in the sequel.

Result 5. *Let F be a function satisfying Property $\mathfrak{P}$. Then the following hold:*

(1) *When p is odd and $t = 0$, the set D_F is a Payley type partial difference set (resp. skew Hadamard difference set) when $p^n \equiv 1 \mod 4$ (resp. $p^n \equiv 3 \mod 4$).*

(2) *When $t > 0$, the set D_F is a partial difference set with parameters*

$$\left(p^n, \frac{p^n-1}{p^t+1}, \frac{p^n - 3p^t - 2 - \epsilon_k p^{n/2+t}(p^t-1)}{(p^t+1)^2}, \frac{p^n - p^t - \epsilon_k p^{n/2}(1-p^t)}{(p^t+1)^2}\right).$$

Moreover, for nonzero $a \in \mathbb{F}_{p^n}$, the character values $\widehat{F}(0,b) \in \{p^{n/2}, -p^{n/2+t}\}$ when k is even; and $\widehat{F}(0,b) \in \{-p^{n/2}, p^{n/2+t}\}$ when k is odd.

(3) *Given $b \in \mathbb{F}_{p^n}^*$, the set of elements $s \in \mathbb{F}_{p^n}$ such that χ_b is trivial on H_s is either $\{0\}$ or a subspace of $\mathbb{F}_{p^n}$ with dimension $2t$.*

(4) *F is a zero-difference p^t-balanced function.*

(5) *For any $a, b \in \mathbb{F}_{p^n}, (a,b) \neq (0,0)$, the magnitude of the Walsh coefficients $|\widehat{F}(a,b)| \in \{0, p^{n/2}, p^{n/2+t}\}$, where $|x|$ denotes the magnitude of a complex number x.*

The following result provides the characterization of the subspaces in $\mathcal{H}$.

Theorem 1. *Let F be a function satisfying Property $\mathfrak{P}$. Then the following hold:*

(1) *For any $H \in \mathcal{H}$, H is a subspace of $\mathbb{F}_{p^n}$ of dimension $n - t$.*

(2) *For any $H \in \mathcal{H}$, there exists a subset Ω_H^* of $\mathbb{F}_{p^n}$ such that $H_s = H$ for all $s \in \Omega_H^*$. Define $\Omega_H = \Omega_H^* \cup \{0\}$. Then Ω_H is a subspace of $\mathbb{F}_{p^n}$ of dimension $2t$.*

(3) *The size of $\mathcal{H}$ is $(p^n-1)/(p^{2t}-1)$ when $t > 0$, and is 1 when $t = 0$.*

Proof: (1) Recall that for each $H \in \mathcal{H}$, there exists an $s \in \mathbb{F}_{p^n}^*$ such that $H = H_s = \{F(x+s) - F(x) : x \in \mathbb{F}_{p^n}\}$. Clearly H is an affine subspace of $\mathbb{F}_{p^n}$ since F is quadratic. Write $H = H' + a$, where H' is a subspace and $a \in \mathbb{F}_{p^n}$. Note that $0 \in H$ since by Result 5(4) the equation $F(x+s) - F(x) = 0$ has p^t solutions. This means $-a \in H'$ and then $a \in H'$ by the assumption that H' is a subspace, which lead to $H = H' + a = H'$. The dimension of H can be seen from $L_s(x) = F(x+s) - F(x)$ is a p^t-to-1 function and hence $\mathrm{Im}(L_s) = p^{n-t}$.

(2) We first prove Ω_H is a subspace of $\mathbb{F}_{p^n}$. Clearly Ω_H is not empty since by assumption $H \in \mathcal{H}$, i.e. $H = H_s$ for some $s \in \mathbb{F}_{p^n}^*$. For any $s_1, s_2 \in \Omega_H$ and $u, v \in \mathbb{F}_p$, we need to show that $us_1 + vs_2 \in \Omega_H$. We have

$$\begin{aligned} F(y + us_1 + vs_2) - F(y) &= \sum_{i=0}^{v-1} \Big(F(y + us_1 + (v-i)s_2) - F(y + us_1 + (v-i-1)s_2\Big) \\ &\quad + \sum_{j=0}^{u-1} \Big(F(y + (u-j)s_1) - F(y + (u-j-1)s_1\Big). \end{aligned}$$

It follows from $s_1, s_2 \in \Omega_H$ that $F(y + us_1 + (v-i)s_2) - F(y + us_1 + (v-i-1)s_2) \in H$ and $F(y + (u-j)s_1) - F(y + (u-j-1)s_1) \in H$ for $0 \leq i \leq v-1, 0 \leq j \leq u-1$. Then from H is a subspace we get $F(y + us_1 + vs_2) - F(y) \in H$, which implies $H_{us_1+vs_2} \subseteq H$. Clearly $H_{us_1+vs_2} = H$ since the dimension of $H_{us_1+vs_2}$ and H are both $n - t$.

Next we determine the dimension of Ω_H. Assume $H = H_s$, we shall show below that $\Omega_H = s\mathbb{F}_{p^{2t}}$. First, $\{s, s\lambda, \ldots, s\lambda^{p^t}\}$ is a subset of Ω_H, where $\lambda = w^{(p^n-1)/(p^t+1)}$ and w is a primitive element of

$\mathbb{F}_{p^n}$. Indeed, for any $s' = s\lambda^i$, we have $F(x+s') - F(x) = F(x+s\lambda^i) - F(x) = G((x+s\lambda^i)^{p^t+1}) - G(x^{p^t+1}) = G((\lambda^i(\lambda^{-i}x+s))^{p^t+1}) - G((\lambda^{-i}x)^{p^t+1}) = G((\lambda^{-i}x+s)^{p^t+1}) - G((\lambda^{-i}x)^{p^t+1})$. Therefore $H_{s'} = \{F(x+s') - F(x) : x \in \mathbb{F}_{p^n}\} = \{G((\lambda^{-i}x+s)^{p^t+1}) - G((\lambda^{-i}x)^{p^t+1}) : x \in \mathbb{F}_{p^n}\} = \{G((y+s)^{p^t+1}) - G(y^{p^t+1}) : y \in \mathbb{F}_{p^n}\} = \{F(y+s) - F(y) : y \in \mathbb{F}_{p^n}\} = H_s$. Now we claim that $\{s, s\lambda, \dots, s\lambda^{p^t}\}$ spans a subspace of dimension $2t$. This is equivalent to showing that the degree of the minimal polynomial of the element $\lambda = w^{(p^n-1)/(p^t+1)}$ is $2t$. It can be seen from the fact that the size of the cyclotomic set containing $(p^n-1)/(p^t+1)$ module p^n-1 is $2t$. Indeed, if $p^i\frac{p^n-1}{p^t+1} \equiv p^i\frac{p^n-1}{p^t+1} \mod (p^n-1)$ we shall have $p^t+1 \mid p^j(p^{i-j}-1)$, which leads to $2t \mid i-j$ and hence the cyclotomic set containing $(p^n-1)/(p^t+1)$ is $2t$. Now we have that Ω_H has a subset whose size is p^{2t}. Note that the subspace spanned by $\{1, \lambda, \dots, \lambda^{p^t}\}$ is $\mathbb{F}_{p^{2t}}$ and hence $\Omega_H = s\mathbb{F}_{p^{2t}}$. By Result 5(3), for each non-zero $b \in \mathbb{F}_{p^n}$, there are at most p^{2t} elements s such that χ_b is trivial on H_s. This means that, if $|\Omega_H| > p^{2t}$, there will exist χ_b such that it is trivial on more than p^{2t} subspaces H_s, which gives the contradiction. Hence Ω_H equals to the space spanned by $\{s, s\lambda, \dots, s\lambda^{p^t}\}$ and the dimension of Ω_H is $2t$.

(3) From the above proof, we see that $\Omega_{H_s} = sN$, where N is the subspace spanned by $\{1, \lambda, \dots, \lambda^{p^t}\}$. Let Ω be a set of coset representatives of the $\mathbb{F}_{p^n}^*/N^*$.

Given $H, H' \in \mathcal{H}$ and $H \neq H'$, clearly $\Omega_H \cap \Omega_{H'} = \{0\}$. Therefore there are in total $(p^n-1)/(p^{2t}-1)$ subspaces in $\mathcal{H}$. Finally, when $t = 0$, or equivalently F is a quadratic PN function. By its definition we have $H_s = \mathbb{F}_{p^n}$ for all nonzero s, which means that $|\mathcal{H}| = 1$. ■

As an application of Theorem 1, we show below that the set $\mathcal{H}_1$ is indeed the dual partial difference set of D_F.

Proposition 1. *Let $\mathcal{H}_1$ be the set of characters χ_b such that χ_b is trivial on exactly one subspace H in $\mathcal{H}$. Then $\mathcal{H}_1$ is the dual partial difference set of D_F with parameters*

$$\left(p^n, \frac{p^n-1}{p^t+1}, \frac{p^n-3p^t-2-\epsilon_k p^{n/2+t}(p^t-1)}{(p^t+1)^2}, \frac{p^n-p^t-\epsilon_k p^{n/2}(1-p^t)}{(p^t+1)^2}\right).$$

Moreover, the character values of the above PDS are

$$\chi_b(\mathcal{H}_1) = \begin{cases} \frac{(\epsilon_k+1)p^{n/2}-(\epsilon_k-1)p^{n/2+t}-2}{2(p^t+1)}, & \text{if } b \in D_F, \\ \frac{(\epsilon_k-1)p^{n/2}-(\epsilon_k+1)p^{n/2+t}-2}{2(p^t+1)}, & \text{if } b \notin D_F. \end{cases}$$

Proof: Denoting $X_F = \sum_{x\in\mathbb{F}_{p^n}} F(x) = 1+(p^t+1)D_F$. Then we get $D_F = \frac{X_F-1}{p^t+1}$. Clearly $X_F X_F^{(-1)} = \sum_{x,y\in\mathbb{F}_{p^n}}(F(x)-F(y)) = \sum_{z\in\mathbb{F}_{p^n}}\left(\sum_{y\in\mathbb{F}_{p^n}}(F(y+z)-F(y))\right) = p^n + p^t\sum_{z\neq 0} H_z$. For any $b \in \mathcal{H}_1$, χ_b is trivial on exactly one subspace in $\mathcal{H}$ and non-trivial on all the others. Assume χ_b is trivial on $H_s \in \mathcal{H}$, then we have $\chi_b(X_F X_F^{(-1)}) = p^n + p^t\sum_{z\neq 0}\chi_b(H_z) = p^n + p^t\sum_{z\in\Omega_{H_s}^*}\chi_b(H_s) = p^n + p^t\cdot p^{n-t}\cdot(p^{2t}-1) = p^{n+2t}$ (note that by Theorem 1(2) $\#\Omega_{H_s}^* = p^{2t}-1$). Substituting the value of $\chi_b(X_F X_F^{(-1)})$ into the following equation

$$\begin{aligned} \chi_b(D_F D_F^{(-1)}) &= \tfrac{1}{(p^t+1)^2}(\chi_b(X_F)-1)(\chi_b(X_F^{(-1)})-1) \\ &= \tfrac{1}{(p^t+1)^2}(\chi_b(X_F X_F^{(-1)}) - 2\chi_b(X_F) + 1), \end{aligned}$$

we get

$$(p^t+1)^2\chi_b(D_F)^2 = p^{n+2t} - 2(1+(p^t+1)\chi_b(D_F)) + 1.$$

Note that in the above we use the fact $X_F = X_F^{(-1)}$, which was proven in [11, Theorem 2]. Simplifying the above equation we obtain

$$(p^t+1)^2\chi_b(D_F)^2 + 2(p^t+1)\chi_b(D_F) - p^{n+2t} + 1 = 0.$$

Then we have $\chi_b(D_F) = (-1 \pm p^{(k+1)t})/(1+p^t)$. Note that $\chi_b(D_F) \in \mathbb{Z}$ by Result 5(2) (we shall explain in Proposition 2 that $\chi_b(D_F) = \widehat{F}(0,b)$). Hence

$$\chi_b(D_F) = \begin{cases} (-1+p^{n/2+t})/(1+p^t) & \text{if } k \text{ is odd,} \\ (-1-p^{n/2+t})/(1+p^t) & \text{if } k \text{ is even.} \end{cases}$$

By Result 3, it is routine to that $\mathcal{H}_1$ is the dual PDS of D_F with the given parameters. ■

In the following we further make use of Theorem 1 to give a characterization of the Walsh spectrum of the function F with Property $\mathfrak{P}$. Recall that by Result 5(5) the magnitude of $\widehat{F}(a,b), (a,b) \neq (0,0)$ is in the set $\{0, p^{n/2}, p^{n/2+t}\}$. Define the following subsets of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$:

$$\begin{aligned} X_0 &= \{\ (0,0)\ \}, \\ X_1 &= \{\ (a,0) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid a \neq 0\ \}, \\ X_2 &= \{\ (a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid \widehat{F}(a,b) = 0 \text{ and } b \neq 0\ \}, \\ X_3 &= \{\ (a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid |\widehat{F}(a,b)| = p^{n/2}\ \}, \\ X_4 &= \{\ (a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid |\widehat{F}(a,b)| = p^{n/2+t}\ \}, \end{aligned} \tag{3}$$

where $|x|$ denotes the module of the complex number x. One may see that when p is odd and $t = 0$, i.e. F is a quadratic PN function, $X_2 = \emptyset$ and $X_3 = X_4 = \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} - \{0\} \times \mathbb{F}_{p^n}$ since by definition $|\widehat{F}(a,b)| = p^{n/2}$ for all $b \neq 0$. Therefore in the rest of this section and in the next section we assume $t > 0$ unless explicitly stated. The following result determines the elements in X_i for $2 \le i \le 4$. To state the result, we need to define a mapping σ from $\mathcal{H}_1$ to $\mathbb{F}_{p^n}^*$. By Theorem 1, there are $(p^n-1)/(p^{2t}-1)$ subspaces in $\mathcal{H}$. Denote Ω as a set of $\#\mathcal{H} = (p^n-1)/(p^{2t}-1)$ elements s such that $\{H_s : s \in \Omega\} = \mathcal{H}$. Given $\chi_b \in \mathcal{H}_1$, i.e. χ_b is trivial on exactly one subspace in $\mathcal{H}$, say H_β for some $\beta \in \Omega$. Define $\sigma : \mathcal{H}_1 \to \mathbb{F}_{p^n}^*$ by $\sigma(\chi_b) = \beta$. In the following, for the convenience, we regard $\mathcal{H}_1$ the same as the set $\{b \in \mathbb{F}_{p^n} | \chi_b \in \mathcal{H}_1\}$.

Proposition 2. *Let X_i be subsets defined above. Then*

$$\begin{aligned} X_2 &= \{(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid \chi_a \textit{ not trivial on } \Omega_{\sigma(b)}, b \in \mathcal{H}_1\}, \\ X_3 &= \{(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid \forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}^* \setminus \mathcal{H}_1\}, \\ X_4 &= \{(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid \chi_a \textit{ is trivial on } \Omega_{\sigma(b)}, b \in \mathcal{H}_1\}. \end{aligned}$$

Proof: Define the graph of the function F by $G_F = \sum_{x \in \mathbb{F}_{p^n}} (x, F(x)) \in \mathbb{Z}[\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}]$. We have $G_F G_F^{(-1)} = \sum_{x,y \in \mathbb{F}_{p^n}} (x-y, F(x)-F(y)) = \sum_{z \in \mathbb{F}_{p^n}} \left(\sum_{y \in \mathbb{F}_{p^n}} (z, F(y+z)-F(y)) \right) = p^n + \sum_{z \neq 0} \left(\sum_{y \in \mathbb{F}_{p^n}} (z, F(y+z) - F(y)) \right) = p^n + p^t \sum_{z \neq 0} (z, H_z)$. For a character $\eta = \chi_a \chi_b$ of the group $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, it is clear that $\widehat{F}(a,b) = \eta(G_F)$. Therefore, by applying the character η on both sides of the above equation, we have that

$$\widehat{F}(a,b)^2 = p^n + p^t \sum_{z \neq 0} \chi_a(z) \chi_b(H_z). \tag{4}$$

In the following we only show that X_2 is the set in the theorem. The proof of the other sets X_3, X_4 are similar.

First, given any $(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ such that $b \in \mathcal{H}_1$ and χ_a non-trivial on $\Omega_{\sigma(b)}$. W.l.o.g. assume χ_b is trivial on $H_s \in \mathcal{H}$ and non-trivial on all $H_{s'} \in \mathcal{H} \setminus \{H_s\}$. By Eq. (4) we have $\widehat{F}(a,b)^2 = p^n + p^t \sum_{z\neq 0} \chi_a(z)\chi_b(H_z) = p^n + p^t \sum_{z\in\Omega^*_{\sigma(b)}} \chi_a(z)p^{n-t} = p^n + p^n\chi_a(\Omega_{\sigma(b)^*}) = p^n - p^n = 0$, which shows $\widehat{F}(a,b) = 0$ or equivalently $(a,b) \in X_2$.

Conversely, given any $(a,b) \in X_2$, i.e. $\widehat{F}(a,b) = 0$ and $b \neq 0$, from Eq. (4) we have $\sum_{z\neq 0} \chi_a(z)\chi_b(H_z) = -p^{n-t}$. Since H_z is a subspace of dimension $n-t$ for all $z \in \mathbb{F}^*_{p^n}$, we have $\chi_b(H_z)$ is either 0 or p^{n-t}. Therefore, we get $-p^{n-t} = \sum_{z\neq 0} \chi_a(z)\chi_b(H_z) = \sum_{z\neq 0,\ \chi_b \text{ is trivial on } H_z} p^{n-t}\chi_a(z) = p^{n-t}\chi_a(sN^*)$, which follows that $\chi_a(sN^*) = -1$ and then χ_a is non-trivial on sN. We finish the proof. ■

IV. Association schemes from ZDB functions with Property $\mathfrak{P}$

In this Section, we will present the construction of a 4-class association schemes from functions with Property $\mathfrak{P}$. We shall show that $\mathcal{X} = \{\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}; X_0, X_1, X_2, X_3, X_4\}$ constitutes a Schur ring (X_i's are defined in (3)), and therefore by Result 4 a 4-class association scheme is derived. The following several lemmas are to determine the character values of X_i for $1 \leq i \leq 4$, which will be used to prove $\mathcal{X}$ is a Schur ring.

Lemma 1. *Let $\eta = \chi_a\chi_b$ be a character of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$. Then*

$$\eta(X_1) = \begin{cases} p^n - 1, & \text{if } a = 0, \forall b \in \mathbb{F}_{p^n}, \\ -1, & \text{if } a \neq 0, \forall b \in \mathbb{F}_{p^n}. \end{cases}$$

Proof: The result is followed from $\eta(X_1) = \chi_a\chi_b(X_1) = \sum_{x\in\mathbb{F}^*_{p^n}} \chi_a(x)\chi_b(0) = \chi_a(\mathbb{F}^*_{p^n})$. ■

Lemma 2. *Let $\eta = \chi_a\chi_b$ be a character of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$. Then*

$$\eta(X_3) = \begin{cases} 0, & \text{if } a \neq 0, \\ \frac{p^{n+t}(-1+\epsilon_k p^{n/2})}{p^t+1}, & \text{if } a = 0, b \in D_F, b \neq 0, \\ -\frac{p^n(p^t+\epsilon_k p^{n/2})}{p^t+1}, & \text{if } a = 0, b \notin D_F, b \neq 0, \\ \frac{p^{n+t}(p^n-1)}{p^t+1}, & \text{if } a = 0, b = 0. \end{cases}$$

Proof: By Proposition 2 we have that $X_3 = \mathbb{F}_{p^n} \times (\mathbb{F}_{p^n} - \mathcal{H}_1 - 0)$. Therefore $\eta(X_3) = \chi_a\chi_b(X_3) = \chi_a(\mathbb{F}_{p^n})\chi_b(\mathbb{F}_{p^n} - 0 - \mathcal{H}_1)$. We split the proof into the following cases:

(i) If $a \neq 0$, one can see that $\eta(X_3) = 0$ since $\chi_a(\mathbb{F}_{p^n}) = 0$.

(ii) If $a = 0$ and $b \neq 0$, then $\eta(X_3) = p^n(-1 - \chi_b(\mathcal{H}_1))$. By Proposition 1 we know that $\mathcal{H}_1$ is the dual PDS of D_F with parameters

$$\left(p^n, \frac{p^n-1}{p^t+1}, \frac{p^n - 3p^t - 2 - \epsilon_k p^{n/2+t}(p^t-1)}{(p^t+1)^2}, \frac{p^n - p^t - \epsilon_k p^{n/2}(1-p^t)}{(p^t+1)^2}\right).$$

Therefore by Result 5 we have $\chi_b(\mathcal{H}_1) = \frac{-1-\epsilon_k p^{n/2+t}}{1+p^t}$ when $b \neq 0$ and $b \in D_F$; and $\chi_b(\mathcal{H}_1) = \frac{-1+\epsilon_k p^{n/2}}{1+p^t}$ when $b \neq 0$ and $b \notin D_F$. This follows that $\eta(X_3) = p^n(-1 - \chi_b(\mathcal{H}_1)) = p^{n+t}\frac{\epsilon_k p^{n/2}-1}{1+p^t}$ when $b \neq 0$ and $b \in D_F$; and $\eta(X_3) = p^n\frac{-p^t-\epsilon_k p^{n/2}}{1+p^t}$ when $b \neq 0$ and $b \notin D_F$.

(iii) Finally, $\eta(X_3) = \#X_3$ when $a = b = 0$. Clearly $\#X_3 = p^n(p^n - 1 - \#\mathcal{H}_1) = p^n(p^n - 1 - (p^n - 1)/(p^t+1)) = p^n(p^n-1)p^t/(p^t+1) = p^{n+t}(p^n-1)/(p^t+1)$.

■

Lemma 3. *Let $\eta = \chi_a\chi_b$ be a character of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$. Then*

$$\eta(X_4) = \begin{cases} -\frac{p^{n-2t}(\epsilon_k p^{n/2+t}+1)}{p^t+1}, & \text{if } a = 0, b \in D_F, b \neq 0, \\ \frac{p^{n-2t}(\epsilon_k p^{n/2}-1)}{p^t+1}, & \text{if } a = 0, b \notin D_F, b \neq 0, \\ p^{n-2t}\chi_b(s), & \text{if } a \neq 0, a \in \Omega_{\sigma(s)} \text{ for some } s \in \mathcal{H}_1. \\ \frac{p^{n-2t}(p^n-1)}{p^t+1}, & \text{if } a = b = 0. \end{cases}$$

Proof: By Proposition 2, we have $X_4 = \{(\alpha, \beta)|\chi_\alpha \text{ is trivial on } \Omega_{\sigma(\beta)}, \beta \in \mathcal{H}_1\}$. From Theorem 1(2) $\Omega_{\sigma(\beta)}$ is a subspace of $\mathbb{F}_{p^n}$ of dimension $2t$. Clearly the set of characters χ_α that are trivial on $\Omega_{\sigma(\beta)}$ is its dual space, and we denoted it by $\Omega^\perp_{\sigma(\beta)}$. Hence $X_4 = \sum_{\beta\in\mathcal{H}_1}(\Omega^\perp_{\sigma(\beta)}, \beta)$ and then $\eta(X_4) = \sum_{\beta\in\mathcal{H}_1} \chi_a(\Omega^\perp_{\sigma(\beta)})\chi_b(\beta)$. We split the following proof into several cases:

(i) If $a = 0$, then $\eta(X_4) = p^{n-2t}\sum_{\beta\in\mathcal{H}_1} \chi_b(\beta) = p^{n-2t}\chi_b(\mathcal{H}_1)$. This uses the fact that $\chi_0(\Omega^\perp_{\sigma(\beta)}) = \#\Omega^\perp_{\sigma(\beta)} = p^{n-2t}$. The value of $\eta(X_4)$ is then followed from $\chi_b(\mathcal{H}_1) = \frac{-1-\epsilon_k p^{n/2+t}}{1+p^t}$ when $b \neq 0$ and $b \in D_F$; and $\chi_b(\mathcal{H}_1) = \frac{-1+\epsilon_k p^{n/2}}{1+p^t}$ when $b \neq 0$ and $b \notin D_F$ (see Result 5).

(ii) If $a \neq 0$, for any non-zero element $z \in \mathbb{F}_{p^n}$, it belongs to exactly one Ω_s, where $s \in \Omega$ and Ω is the set of $\#\mathcal{H} = (p^n - 1)/(p^{2t} - 1)$ elements s such that $\{H_s : s \in \Omega\} = \mathcal{H}$. This is because that $\{\Omega^*_t : t \in \Omega\}$ is a disjoint union of $\mathbb{F}^*_{p^n}$ (see proof in Theorem 1(3)). Now, assume that $a \in \Omega_{\sigma(s)}$ for some $s \in \mathcal{H}_1$, we then have $\eta(X_4) = \sum_{\beta\in\mathcal{H}_1} \chi_a(\Omega^\perp_{\sigma(\beta)})\chi_b(\beta) = \chi_a(\Omega^\perp_{\sigma(s)})\chi_b(s) = p^{n-2t}\chi_b(s)$.

(iii) If $a = b = 0$, then $\eta(X_4) = \#X_4 = \#\Omega^\perp_{\sigma(b)}\#\mathcal{H}_1 = p^{n-2t}(p^n - 1)/(p^t + 1)$.

■

The character value of X_2 can be obtained through $\eta(X_0 + X_1 + X_2 + X_3 + X_4) = 0$ when the character η is nontrivial on $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, and $\eta(X_0 + X_1 + X_2 + X_3 + X_4) = p^{2n}$ when η is trivial. We omit the details of the proof but directly give the result below.

Lemma 4. *Let $\eta = \chi_a\chi_b$ be a character of G. Then the character value $\eta(X_2)$ is as following:*

$$\eta(X_2) = \begin{cases} -p^{n-2t}(p^t - 1)(\epsilon_k p^{n/2+t} + 1), & \text{if } a = 0, b \in D_F, b \neq 0, \\ p^{n-2t}(p^t - 1)(\epsilon_k p^{n/2} - 1), & \text{if } a = 0, b \notin D_F, b \neq 0, \\ -p^{n-2t}\chi_b(s), & \text{if } a \neq 0, a \in \Omega_{\sigma(s)} \text{ for some } s \in \mathcal{H}_1, \\ p^{n-2t}(p^t - 1)(p^n - 1), & \text{if } a = b = 0. \end{cases}$$

Now we are ready to show that $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}; X_0, X_1, X_2, X_3, X_4)$ is a Schur ring over the group $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$.

Theorem 2. *Let F be a function satisfying Property $\mathfrak{P}$. Define the subsets $X_i, 0 \leq i \leq 4$ as in* (3). *Then*

$$X_1X_2 = (p^n - p^{n-2t} - 1)X_2 + (p^n - p^{n-2t})X_4, \tag{5}$$

$$X_1X_3 = (p^n - 1)X_3, \tag{6}$$

$$X_1X_4 = p^{n-2t}X_2 + (p^{n-2t} - 1)X_4, \tag{7}$$

$$\begin{aligned} X_2X_3 = {} & \frac{p^{n-2t}(p^t-1)(p^{n/2+t}+\epsilon_k)(p^{n/2}-\epsilon_k)}{p^t+1}X_3 \\ & +\frac{p^{n-t}(p^t-1)(p^{n/2}-\epsilon_k)(p^{n/2}+\epsilon_k p^t)}{p^t+1}(X_2+X_4), \end{aligned} \tag{8}$$

$$\begin{aligned} X_2X_4 = {} & p^{2n-4t}(p^t-1)X_1 + \frac{p^{n-4t}(p^t-1)(2-p^n+3p^t-\epsilon_k p^{n/2+t}(1-p^t))}{p^t+1}(X_2+X_4) \\ & +\frac{p^{n-4t}(p^{n/2}-\epsilon_k)(p^t-1)(p^{n/2}+\epsilon_k p^t)}{1+p^t}X_3, \end{aligned} \tag{9}$$

$$X_3X_4 = \frac{p^{n-t}(p^{n/2}-\epsilon_k)(p^{n/2}+\epsilon_k p^t)}{(p^t+1)^2}(X_2+X_4) + \frac{p^{n-2t}(p^{n/2+t}+\epsilon_k)(p^{n/2}-\epsilon_k)}{(p^t+1)^2}X_3. \tag{10}$$

Therefore, X_0, X_1, X_2, X_3, X_4 span a 4-class Schur ring over the group $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$.

Proof: The proof makes use of Lemmas 1, 2, 3, 4. Since the proof for the equations (5),(6),(7),(8),(9),(10) are similar, in the following we only prove equation (5). Denoting LHS (resp. RHS) the left (resp. right) hand side of equation (5). By Result 2, we need to show that $\eta(\text{LHS}) = \eta(\text{RHS})$ for any character $\eta = \chi_a\chi_b$ of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$. In the following we split the following proof into several cases:

(i) If $a = b = 0$, we have $\eta(\text{LHS}) = |X_1| \cdot |X_2| = p^{n-2t}(p^t-1)(p^n-1)^2$. On the other hand,

$$\begin{aligned} \eta(\text{RHS}) &= (p^n - p^{n-2t} - 1)|X_2| + (p^n - p^{n-2t})|X_4| \\ &= (p^n - p^{n-2t} - 1)p^{n-2t}(p^t-1)(p^n-1) + (p^n - p^{n-2t})\tfrac{p^{n-2t}(p^n-1)}{p^t+1} \\ &= p^{n-2t}(p^n - p^{n-2t} - 1)(p^t-1)(p^n-1) + p^{2n-4t}(p^t-1)(p^n-1) \\ &= p^{n-2t}(p^t-1)(p^n-1)(p^n - p^{n-2t} - 1 + p^{n-2t}) \\ &= p^{n-2t}(p^t-1)(p^n-1)^2. \end{aligned}$$

(ii) If $a = 0$ and $b \in D_F$ and $b \neq 0$, we have $\eta(\text{LHS}) = \eta(X_1)\eta(X_2) = (p^n-1) \cdot (-p^{n-2t}(p^t-1)(\epsilon_k p^{n/2+t}+1)) = -p^{n-2t}(p^n-1)(p^t-1)(\epsilon_k p^{n/2+t}+1)$; and

$$\begin{aligned} \eta(\text{RHS}) &= (p^n - p^{n-2t} - 1)\eta(X_2) + (p^n - p^{n-2t})\eta(X_4) \\ &= (p^n - p^{n-2t} - 1)(-p^{n-2t}(p^t-1)(\epsilon_k p^{n/2+t}+1)) + (p^n - p^{n-2t})\tfrac{p^{n-2t}(-1-\epsilon_k p^{n/2+t})}{p^t+1} \\ &= -p^{n-2t}(p^t-1)(p^n - p^{n-2t} - 1)(\epsilon_k p^{n/2+t}+1) - p^{2n-4t}(p^t-1)(\epsilon_k p^{n/2+t}+1) \\ &= -p^{n-2t}(p^t-1)(\epsilon_k p^{n/2+t}+1)(p^n - p^{n-2t} - 1 + p^{n-2t}) \\ &= -p^{n-2t}(p^t-1)(\epsilon_k p^{n/2+t}+1)(p^n-1). \end{aligned}$$

(iii) If $a = 0$ and $b \notin D_F$, we have $\eta(\text{LHS}) = \eta(X_1)\eta(X_2) = (p^n-1)p^{n-2t}(p^t-1)(\epsilon_k p^{n/2}-1)$. On the other hand,

$$\begin{aligned}\eta(\text{RHS}) &= (p^n - p^{n-2t} - 1)\eta(X_2) + (p^n - p^{n-2t})\eta(X_4) \\ &= (p^n - p^{n-2t} - 1)p^{n-2t}(p^t - 1)(\epsilon_k p^{n/2} - 1) + (p^n - p^{n-2t})\tfrac{p^{n-2t}(-1+\epsilon_k p^{n/2})}{1+p^t} \\ &= p^{n-2t}(p^t - 1)(p^n - p^{n-2t} - 1)(\epsilon_k p^{n/2} - 1) + p^{2n-4t}(p^t - 1)(\epsilon_k p^{n/2} - 1) \\ &= p^{n-2t}(p^t - 1)(\epsilon_k p^{n/2} - 1)(p^n - p^{n-2t} - 1 + p^{n-2t}) \\ &= p^{n-2t}(p^t - 1)(\epsilon_k p^{n/2} - 1)(p^n - 1).\end{aligned}$$

(iv) If $a \neq 0, a \in \Omega_{\sigma(t)}$ for some $t \in \mathcal{H}_1$, we have $\eta(\text{LHS}) = \eta(X_1)\eta(X_2) = p^{n-2t}\chi_b(t)$. On the other hand

$$\begin{aligned}\eta(\text{RHS}) &= (p^n - p^{n-2t} - 1)\eta(X_2) + (p^n - p^{n-2t})\eta(X_4) \\ &= -(p^n - p^{n-2t} - 1)p^{n-2t}\chi_b(t) + (p^n - p^{n-2t})p^{n-2t}\chi_b(t) \\ &= p^{n-2t}\chi_b(t)(-p^n + p^{n-2t} + 1 + p^n - p^{n-2t}) \\ &= p^{n-2t}\chi_b(t).\end{aligned}$$

To finalize the proof that X_0, X_1, X_2, X_3, X_4 span a Schur ring over $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, we need to show that $X_iX_i = \sum_{j=0}^{4} p_{ii}^{j} X_j$ for integers p_{ii}^{j} with $0 \leq i \leq 4$ and $0 \leq j \leq 4$. This can be seen from $X_iX_i = X_i(\mathbb{F}_{p^n} - \sum_{j\neq i} X_j) = |X_i|\mathbb{F}_{p^n} - \sum_{j\neq i} X_iX_j$ along with Eqs. (5),(6),(7),(8),(9),(10). The proof is completed. ■

We give the following example to illustrate Theorem 2 by showing APN functions give rise to a 4-class Schur ring.

Example 1. *Let $F(x) = x^3 + \mathrm{Tr}(\mathrm{x}^9) = (\mathrm{x} + \mathrm{Tr}(\mathrm{x}^3)) \circ \mathrm{x}^3$ be the APN function on $\mathbb{F}_{2^8}$. We have the following*

$$\begin{aligned}X_1X_1 &= 255X_0 + 254X_1, \\ X_1X_2 &= 191X_2 + 192X_4, \\ X_1X_3 &= 255X_3, \\ X_1X_4 &= 64X_2 + 63X_4, \\ X_2X_2 &= 16320X_0 + 12224X_1 + 3456X_2 + 4320X_3 + 3456X_4, \\ X_2X_3 &= 11520X2 + 10560X_3 + 11520X_4, \\ X_2X_4 &= 4096X_1 + 1152X_2 + 1440X_3 + 1152X_4, \\ X_3X_3 &= 43520X_0 + 43520X_1 + 28160X_2 + 29184X_3 + 28160X_4, \\ X_3X_4 &= 3840X_2 + 3520X_3 + 3840X_4, \\ X_4X_4 &= 5440X_1 + 3840X_2 + 480X_3 + 3840X_4.\end{aligned}$$

By Result 4 and Theorem 2, we have the following construction of the 4-class association scheme.

Theorem 3. *Let F be the function satisfying Property $\mathfrak{P}$. Define the binary relations $R_i, 0 \leq i \leq 4$ in $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ as $R_i = \{\langle (a_1, b_1), (a_2, b_2)\rangle : (a_1 - a_2, b_1 - b_2) \in X_i\}$ for $0 \leq i \leq 4$, where X_i's are defined in* (3). *Then $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}; R_0, R_1, R_2, R_3, R_4)$ is a 4-class association scheme.*

V. Linear codes from ZDB functions with Property $\mathfrak{P}$

In this Section we consider the linear code $\mathcal{C}_F$ generated by the matrix C_F, which is defined in (2). Clearly, all codewords of $\mathcal{C}_F$ are of the form

$$c_{a,b} = \left(f_{a,b}(1), f_{a,b}(w), \ldots, f_{a,b}(w^{p^n-2})\right),$$

where $f_{a,b}(x) = \mathrm{Tr}(\mathrm{ax} + \mathrm{bf(x)})$ and w is a primitive element of $\mathbb{F}_{p^n}$. It is well known that the weight of the codeword $c_{a,b}$ can be determined as in the following result, see for instance [22]. We include a short proof for the convenience of the readers.

Lemma 5. *Let the notations the same as above. Then*

$$w(c_{a,b}) = (p^n - p^{n-1}) - \frac{1}{p}\sum_{c=1}^{p-1} \sigma_c(\widehat{F}(a,b)),$$

where σ_c is the Galois automorphism of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ defined by $\sigma_c(x) = \zeta_p^c$.

Proof: The result is followed from the following

$$\begin{aligned} w(c_{a,b}) &= (p^n - 1) - \#\{x \in \mathbb{F}_{p^n} | \mathrm{Tr}(\mathrm{ax} + \mathrm{bF(x)}) = 0\} \\ &= (p^n - 1) - \tfrac{1}{p} \textstyle\sum_{x\in\mathbb{F}_{p^n}} \sum_{c\in\mathbb{F}_p} \zeta_p^{\mathrm{Tr(c(ax+bF(x)))}} \\ &= (p^n - 1) - \tfrac{1}{p} \textstyle\sum_{c\in\mathbb{F}_p} \left(\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr(cax+cbF(x))}} \right) \\ &= (p^n - p^{n-1}) - \tfrac{1}{p} \textstyle\sum_{c=1}^{p-1} \left(\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr(cax+cbF(x))}} \right) \\ &= (p^n - p^{n-1}) - \tfrac{1}{p} \textstyle\sum_{c=1}^{p-1} \sigma_c(\widehat{F}(a,b)). \end{aligned}$$

■

The theorem below gives the Walsh spectrum of the function F with Property $\mathfrak{P}$, as well as the weight distribution of the corresponding linear code $\mathcal{C}_F$. Since the case $t = 0$ and p is odd has been considered in [22], we assume $t > 0$ in the rest of this Section.

Theorem 4. *Let F be a function with Property $\mathfrak{P}$. Then the following results hold:*

(1) *If $p = 2$ and $t > 0$, the Walsh spectrum of F as well as the weight distribution of the linear code $\mathcal{C}_F$ are in the following table*

TABLE I: Walsh spectrum of F and weight distribution of $\mathcal{C}_F$: $p = 2, t > 0$

Walsh coefficient $\widehat{F}(\alpha,\beta)$	Multiplicity
2^n	1
0	$(2^n-1)(2^{n-t}-2^{n-2t}+1)$
$2^{n/2}$	$\frac{2^{n/2+t-1}\left(2^{n/2}-1\right)\left(2^{n/2}+1\right)^2}{2^t+1}$
$-2^{n/2}$	$\frac{2^{n/2+t-1}(2^{n/2}-1)(2^n-1)}{2^t+1}$
$2^{n/2+t}$	$\frac{2^{n/2-2t-1}(2^n-1)\left(2^{n/2}+2^t\right)}{2^t+1}$
$-2^{n/2+t}$	$\frac{2^{n/2-t-1}(2^n-1)(2^{n/2-t}-1)}{2^t+1}$

Weight w	Multiplicity A_w
0	1
2^{n-1}	$(2^n-1)(2^{n-t}-2^{n-2t}+1)$
$2^{n-1}-2^{n/2-1}$	$\frac{2^{n/2+t-1}\left(2^{n/2}-1\right)\left(2^{n/2}+1\right)^2}{2^t+1}$
$2^{n-1}+2^{n/2-1}$	$\frac{2^{n/2+t-1}(2^{n/2}-1)(2^n-1)}{2^t+1}$
$2^{n-1}-2^{n/2+t-1}$	$\frac{2^{n/2-2t-1}(2^n-1)\left(2^{n/2}+2^t\right)}{2^t+1}$
$2^{n-1}+2^{n/2+t-1}$	$\frac{2^{n/2-t-1}(2^n-1)(2^{n/2-t}-1)}{2^t+1}$

(2) *If p is odd and k is even, the Walsh spectrum of F is*

TABLE II: Walsh spectrum of F: p odd, k even

Walsh coefficient $\widehat{F}(\alpha,\beta)$	Multiplicity
p^n	1
0	$(p^n-1)(p^{n-t}-p^{n-2t}+1)$
$p^{n/2}$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-p^t+p+p^{t+1}-1\right)$
$p^{n/2}\zeta_p^{\lambda}$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-p^t-1\right)$
$-p^{n/2+t}$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+p^t+p^{2t}-p^{t+1}-p^{2t+1}\right)$
$-p^{n/2+t}\zeta_p^{\lambda}$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+p^t+p^{2t}\right)$

The weight distribution of the code $\mathcal{C}_F$ is

TABLE III: Weight distribution of the code $\mathcal{C}_F$: p odd, k even

Weight w	Multiplicity A_w
0	1
p^n-p^{n-1}	$(p^n-1)(p^{n-t}-p^{n-2t}+1)$
$(p-1)(p^{n-1}-p^{n/2-1})$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-p^t+p+p^{t+1}-1\right)$
$p^{n-1}(p-1)+p^{n/2-1}$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-p^t-1\right)$
$(p-1)(p^{n-1}-p^{n/2+t-1})$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+p^t+p^{2t}-p^{t+1}-p^{2t+1}\right)$
$p^{n-1}(p-1)+p^{n/2+t-1}$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+p^t+p^{2t}\right)$

(3) *If p is odd and k is odd, the Walsh spectrum of F is*

TABLE IV: Walsh spectrum of F: p odd, k odd

Walsh coefficient $\widehat{F}(\alpha,\beta)$	Multiplicity
p^n	1
0	$(p^n-1)(p^{n-t}-p^{n-2t}+1)$
$-p^{n/2}$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-\epsilon_{(p-1)t/2}p^{t+1}-\epsilon_{(p-1)t/2}p+\epsilon_{(p-1)t/2}p^t+\epsilon_{(p-1)t/2}\right)$
$-p^{n/2}\zeta_p^{\lambda}$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+\epsilon_{(p-1)t/2}p^t+\epsilon_{(p-1)t/2}\right)$
$p^{n/2+t}$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)\left(\epsilon_{(p-1)t/2}p^t+p^{2t}\right)}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+\epsilon_{(p-1)t/2}p^{2t+1}+\epsilon_{(p-1)t/2}p^{t+1}-\epsilon_{(p-1)t/2}p^{2t}-\epsilon_{(p-1)t/2}p^t\right)$
$p^{n/2+t}\zeta_p^{\lambda}$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon_{(p-1)t/2}p^t+p^{2t})}\left(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-\epsilon_{(p-1)t/2}p^{2t}-\epsilon_{(p-1)t/2}p^t\right)$

The weight distribution of the code $\mathcal{C}_F$ is

TABLE V: Weight distribution of the code $\mathcal{C}_F$: p odd, k odd

Weight w	Multiplicity A_w
0	1
$p^n - p^{n-1}$	$(p^n-1)(p^{n-t}-p^{n-2t}+1)$
$(p-1)(p^{n-1}+p^{n/2-1})$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)(\epsilon_{(p-1)t/2}p^t+p^{2t})}\Big(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-\epsilon_{(p-1)t/2}p^{t+1}-\epsilon_{(p-1)t/2}p+\epsilon_{(p-1)t/2}p^t+\epsilon_{(p-1)t/2}\Big)$
$p^{n-1}(p-1)-p^{n/2-1}$	$\frac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)(\epsilon_{(p-1)t/2}p^t+p^{2t})}\Big(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+\epsilon_{(p-1)t/2}p^t+\epsilon_{(p-1)t/2}\Big)$
$(p-1)(p^{n-1}-p^{n/2+t-1})$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon_{(p-1)t/2}p^t+p^{2t})}\Big(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}+\epsilon_{(p-1)t/2}p^{2t+1}+\epsilon_{(p-1)t/2}p^{t+1}-\epsilon_{(p-1)t/2}p^{2t}-\epsilon_{(p-1)t/2}p^t\Big)$
$p^{n-1}(p-1)+p^{n/2+t-1}$	$\frac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon_{(p-1)t/2}p^t+p^{2t})}\Big(\epsilon_{(p-1)t/2}p^{n/2}+p^{n/2+t}-\epsilon_{(p-1)t/2}p^{2t}-\epsilon_{(p-1)t/2}p^t\Big)$

Since the proof of Theorem 4 are rather technical, we present the proofs depending on $p=2$ or p is odd in the following two sections.

VI. Proof of Theorem 4 when $p=2$

We first give the following lemma.

Lemma 6. *Let F be a function with Property $\mathfrak{P}$. Then*

$$\begin{array}{rcl}\sum_{\alpha,\beta\in\mathbb{F}_{2^n}}\widehat{F}(\alpha,\beta) & = & 2^{2n},\ \textit{and}\\ \sum_{\alpha,\beta\in\mathbb{F}_{2^n}}\widehat{F}(\alpha,\beta)^3 & = & 2^{2n}(2^t(2^n-1)+2^n).\end{array}$$

Proof: First we have

$$\begin{array}{rcl}\sum_{\alpha,\beta\in\mathbb{F}_{2^n}}\widehat{F}(\alpha,\beta) & = & \sum_{\alpha,\beta\in\mathbb{F}_{2^n}}\Big(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\alpha x+\beta F(x))}\Big)\\ & = & \sum_{x\in\mathbb{F}_{2^n}}\Big(\sum_{\alpha\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\alpha x)}\Big)\Big(\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta F(x))}\Big)\\ & = & 2^n\cdot 2^n=2^{2n}.\end{array}$$

Next, we have that

$$\begin{array}{rcl}\sum_{\alpha,\beta\in\mathbb{F}_{2^n}}\widehat{F}(\alpha,\beta)^3 & = & \sum_{\alpha,\beta\in\mathbb{F}_{2^n}}\Big(\sum_{x,y,z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\alpha(x+y+z)+\beta(F(x)+F(y)+F(z)))}\Big)\\ & = & \sum_{x,y,z\in\mathbb{F}_{2^n}}\Big(\sum_{\alpha\in\mathbb{F}_{p^n}}(-1)^{\mathrm{Tr}(\alpha(x+y+z))}\Big)\Big(\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(F(x)+F(y)+F(z)))}\Big)\\ & = & 2^{2n}\#\{(x,y,z):x,y,z\in\mathbb{F}_{2^n}\mid x+y+z=0,F(x)+F(y)+F(z)=0\}.\end{array}\tag{11}$$

Determining the number of the solutions to the system of the equations $x+y+z=0, F(x)+F(y)+F(z)=0$ is equivalent to determining the number of solutions (x,y) to the equation $F(x+y)+F(x)=F(y)$ ($z=x+y$). If $y\neq 0$, by Result 5(4) the equation $F(x+y)+F(x)=F(y)$ has either 0 or 2^t solutions. But we may see $x=0$ is a solution to this equation, therefore the number of solutions is 2^t. If $y=0$, the equation $F(x+y)+F(x)=0$ has 2^n solutions. We have in total $2^t(2^n-1)+2^n$ solutions (x,y,z). The rest of the proof follows from Eq. (11). ■

We are ready to determine the Walsh spectrum of F and the weight distribution of $\mathcal{C}_F$. Let x,y be the multiplicities of the values $2^{n/2},2^{n/2+t}$ in the Walsh spectrum of F, respectively. Then $|X_3|-x, |X_4|-y$

are the multiplicities of the values $-2^{n/2}$, $-2^{n/2+t}$, respectively. From Lemma 6 we get the following two equations:

$$2^n + 2^{n/2}x - 2^{n/2}(|X_3| - x) + 2^{n/2+t}y - 2^{n/2+t}(|X_4| - y) = 2^{2n}, \tag{12}$$

and

$$2^{3n} + 2^{3n/2}x - 2^{3n/2}(|X_3| - x) + 2^{3n/2+3t}y - 2^{3n/2+3t}(|X_4| - y) = 2^{2n}(2^t(2^n - 1) + 2^n). \tag{13}$$

Solving x, y from the above two equations, we obtain

$$\begin{aligned} x &= \tfrac{2^{n/2+t-1}\left(2^{n/2}-1\right)\left(2^{n/2}+1\right)^2}{2^t+1}, \\ y &= \tfrac{2^{n/2-2t-1}(2^n-1)\left(2^{n/2}+2^t\right)}{2^t+1}. \end{aligned}$$

This proves the Walsh spectrum of F. For the weight distribution of the code $\mathcal{C}_F$, by Lemma 5 the weight of the codeword $c_{\alpha,\beta}$ is $w_{\alpha,\beta} = 2^{n-1} - \widehat{F}(\alpha,\beta)/2$, and hence the weight distribution is followed from the Walsh spectrum of F. ■

VII. Proof of Theorem 4 when p is odd

Recall that the proof of the case p is odd and $t = 0$ is given [8], [22], [39]. In this section we assume that $t > 0$. We first give the following lemmas which will be used in the proof.

Lemma 7. *Let F be a function with Property $\mathfrak{P}$. Then we have*

$$\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta) = \sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta)^2 = p^{2n}.$$

Proof: The proof of the equation $\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta) = p^{2n}$ is similar to the one in Lemma 6 and we omit it here. For the second equation, we have

$$\begin{aligned} \textstyle\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta)^2 &= \textstyle\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \left(\sum_{x,y\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\alpha(x+y)+\beta(F(x)+F(y)))}\right) \\ &= \textstyle\sum_{x,y\in\mathbb{F}_{p^n}} \left(\sum_{\alpha\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\alpha(x+y))}\right)\left(\sum_{\beta\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\beta(F(x)+F(y)))}\right) \\ &= p^{2n}\#\{x \in \mathbb{F}_{p^n} | F(x) + F(-x) = 0\}. \end{aligned}$$

Note that $F(-x) = G((-x)^{p^t+1}) = G(x^{p^t+1}) = F(x)$ and then $F(x) + F(-x) = 0$ yields $F(x) = 0$, which implies that $x = 0$. ■

For the function $F(x)$ and $\alpha, \beta \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned} \widehat{F}(\alpha,\beta)\overline{\widehat{F}(\alpha,\beta)} &= \sum_{x,y} \zeta_p^{\mathrm{Tr}(\alpha x+\beta F(x)-\alpha y-\beta F(y))} \\ &= \sum_{u} \zeta_p^{\mathrm{Tr}(\alpha u+\beta F(u))} \sum_{x} \zeta_p^{\mathrm{Tr}(\beta(F(x+u)-F(x)-F(u)))}. \end{aligned} \tag{14}$$

Since F is quadratic, when $\beta \neq 0$, there exists a linearized polynomial L_β over $\mathbb{F}_{p^n}$ such that $\mathrm{Tr}(\beta(\mathrm{F}(x+u) - \mathrm{F}(x) - \mathrm{F}(u))) = \mathrm{Tr}(\mathrm{L}_\beta(u)x)$ holds for any $u, x \in \mathbb{F}_{p^n}$. Therefore from Eq. (14) we get

$$\widehat{F}(\alpha,\beta)\overline{\widehat{F}(\alpha,\beta)} = \sum_{u} \zeta_p^{\mathrm{Tr}(\alpha u+\beta F(u))} \sum_{x} \zeta_p^{\mathrm{Tr}(L_\beta(u)x)} = p^n \sum_{u\in\mathrm{Ker}(L_\beta)} \zeta_p^{\mathrm{Tr}(\alpha u+\beta F(u))}. \tag{15}$$

The next result gives the property of L_β.

Lemma 8. *Given $\alpha, \beta \in \mathbb{F}_{p^n}$ and $\beta \neq 0$, the following hold:*

(1) *If $|\widehat{F}(\alpha, \beta)| = p^{n/2}$, then the linear function $L_\beta(u)$ is a linearized permutation polynomial;*

(2) *If $|\widehat{F}(\alpha, \beta)| = p^{n/2+t}$, then the image set of $L_\beta(u)$ is $\Omega^{\perp}_{\sigma(\beta)}$.*

Proof: First we show that $\mathrm{Ker}(L_\beta) = \{s \in \mathbb{F}_{p^n} | \chi_\beta \text{ is trivial on } H_s\}$. This is because: for any $s \in \mathrm{Ker}(L_\beta)$, we have $0 = \mathrm{Tr(L_\beta(s)x)} = \mathrm{Tr(\beta(F(x+s) - F(x) - F(s)))}$, which implies χ_β is trivial on $H_s - F(s)$. Recall that $F(s) \in H_s$ (since $F(s) = F(0+s) - F(0)$) and H_s is a subspace by Theorem 1(1), we have $H_s - F(s) = H_s$. Hence χ_β is trivial on H_s. Conversely, for each s such that χ_β is trivial on H_s, it is clear $\mathrm{Tr(L_\beta(s)x)} = \mathrm{Tr(\beta(F(x+s) - F(x) - F(s)))} = 0$ for all x, therefore $s \in \mathrm{Ker}(L_\beta)$.

By Proposition 2, for (α, β) such that $|\widehat{F}(\alpha, \beta)| = p^{n/2}$, we have $\alpha \in \mathbb{F}_{p^n}$ and $\beta \in \mathbb{F}^*_{p^n} \backslash \mathcal{H}_1$. This means χ_β is not trivial on any $H_s \in \mathcal{H}$, i.e. $\mathrm{Ker}(L_\beta) = \{0\}$ by the above claim. Hence L_β is a linearized permutation polynomial. Similarly, by Proposition 2, if $|\widehat{F}(\alpha, \beta)| = p^{n/2+t}$, we have χ_α is trivial on $\Omega_{\sigma(\beta)}$ and $\beta \in \mathcal{H}_1$. Given any $b \in \mathrm{Im}(L_\beta)$, i.e. $b = L_\beta(u)$ for some $u \in \mathbb{F}_{p^n}$. For any $s \in \Omega_{\sigma(\beta)}$, $\mathrm{Tr(bs)} = \mathrm{Tr(L_\beta(u)s)} = \mathrm{Tr(\beta(F(s+u) - F(s) - F(u)))}$, which implies that $b \in \Omega^{\perp}_{\sigma(\beta)}$. Note that $F(s+u) - F(u) \in H_s$ and further $F(s) \in H_s$ since $F(s) = F(0+s) - F(0)$. Therefore we have that $\mathrm{Tr(bs)} = 0$ and hence $b \in \Omega^{\perp}_{\sigma(b)}$, i.e. $\mathrm{Im}(L_\beta) \subseteq \Omega^{\perp}_{\sigma(b)}$. Note that the size of $\mathrm{Im}(L_\beta)$ is p^{n-2t} and $\Omega^{\perp}_{\sigma(\beta)}$ are both p^{n-2t}, we get $\mathrm{Im}(L_\beta) = \Omega^{\perp}_{\sigma(\beta)}$. ■

We need to following result from algebraic number theory to give the next Lemma.

Result 6. *[26], [28] Let p be an odd prime.*

(1) *The ring of integers in $\mathbb{K} = \mathbb{Q}(\zeta_p)$ is $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ and $\{\zeta_p : 0 \le i \le p-2\}$ is an integral basis of $\mathcal{O}_{\mathbb{K}}$. The group of roots of unity in $\mathcal{O}_{\mathbb{K}}$ is $W = \{\pm\zeta_p^i : 0 \le i \le p-1\}$. Define $W^+ = \{\zeta_p^i : 0 \le i \le p-1\}$ and $W^- = \{-\zeta_p^i : 0 \le i \le p-1\}$.*

(2) *The field $\mathbb{K}$ has a unique quadratic subfield $\mathbb{L} = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (\frac{-1}{p})p = (-1)^{\frac{p-1}{2}}p$ and for $1 \le a \le p-1$, $(\frac{a}{p})$ is the Legendre symbol. For $1 \le a \le p-1$, $\sigma_a(\sqrt{p^*}) = (\frac{a}{p})\sqrt{p^*}$. Therefore, $Gal(\mathbb{L}/\mathbb{Q}) = \{1, \sigma_\gamma\}$, where γ is any quadratic non-residue in $\mathbb{F}_p$.*

Lemma 9. *For all $\alpha, \beta \in \mathbb{F}_{p^n}$, the followings hold:*

(1) *$\widehat{F}(\alpha, 0) = \delta_0(\alpha)p^n$, where δ_0 is the Dirac function (defined by $\delta_0(\alpha) = 0$ if $\alpha \neq 0$, and $\delta_0(\alpha) = 1$ if $\alpha = 0$).*

(2) *$\widehat{F}(0, \beta) \in \{\epsilon_k p^{n/2}, -\epsilon_k p^{n/2+t}\}$ when $\beta \neq 0$.*

(3) *If $\widehat{F}(\alpha, \beta) \neq 0$, there exists $\eta_{\alpha,\beta} \in W$ such that $\widehat{F}(\alpha, \beta) = \eta_{\alpha,\beta}(\sqrt{p^*})^n$ or $\widehat{F}(\alpha, \beta) = \eta_{\alpha,\beta}(\sqrt{p^*})^{n+2t}$, where $p^* = \left(\frac{-1}{p}\right)p = (-1)^{(p-1)/2}p$. Moreover, $\eta_{\alpha,\beta}\eta_{0,\beta} \in W^+$.*

Proof: We only prove (3), the rest two are simple and we omit the details. Now assume that $|\widehat{F}(\alpha, \beta)| = p^{n/2}$, i.e. $(\alpha, \beta) \in X_3$. We have now $\widehat{F}(\alpha, \beta)\overline{\widehat{F}(\alpha, \beta)}\mathcal{O}_K = p^n\mathcal{O}_K = P^{(p-1)n}$ and then $\widehat{F}(\alpha, \beta)\mathcal{O}_K = P^{n(p-1)/2} = (\sqrt{p^*})^n$. This shows that $\eta_{\alpha,\beta} := \widehat{F}(\alpha, \beta)/(\sqrt{p^*})^n$ is a unit in $\mathcal{O}_K$. Furthermore, we have $|\sigma_c(\eta_{\alpha,\beta})| = |\sigma_c(\widehat{F}(\alpha, \beta)/(\sqrt{p^*})^n)| = |\widehat{F}(c\alpha, c\beta)/(\pm\sqrt{p^*})^n|$. Note that from Proposition 2 we see that $(c\alpha, c\beta) \in X_3$ for all $c \in \mathbb{F}^*_p$ if $(\alpha, \beta) \in X_3$. This shows that $|\sigma_c(\eta_{\alpha,\beta})| = 1$ for all $c \in \mathbb{F}^*_p$, which implies that $\eta_{\alpha,\beta} \in W$. Next we show that $\eta_{\alpha,\beta}\eta_{0,\beta} \in W^+$. Indeed, by Lemma 8, we have that L_β is a linearized permutation on $\mathbb{F}_{p^n}$. Therefore, there exists exactly one $u \in \mathbb{F}_{p^n}$ such that $L_\beta(u) = \alpha$. Hence

$\mathrm{Tr}(\beta(\mathrm{F}(\mathrm{x}+\mathrm{u})-\mathrm{F}(\mathrm{x})-\mathrm{F}(\mathrm{u}))) = \mathrm{Tr}(\mathrm{L}_\beta(\mathrm{u})\mathrm{x}) = \mathrm{Tr}(\alpha\mathrm{x})$ for all $x \in \mathbb{F}_{p^n}$. As a result,

$$\begin{aligned}
\eta_{\alpha,\beta}(\sqrt{p^*})^n &= \widehat{F}(\alpha,\beta) = \textstyle\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\alpha\mathrm{x}+\beta\mathrm{F}(\mathrm{x}))} \\
&= \textstyle\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\beta(\mathrm{F}(\mathrm{x}+\mathrm{u})-\mathrm{F}(\mathrm{x})-\mathrm{F}(\mathrm{u})))+\mathrm{Tr}(\beta\mathrm{F}(\mathrm{x}))} \\
&= \textstyle\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\beta(\mathrm{F}(\mathrm{x}+\mathrm{u})-\mathrm{F}(\mathrm{u})))} \\
&= \zeta_p^{\mathrm{Tr}(-\beta\mathrm{F}(\mathrm{u}))} \textstyle\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(\beta(\mathrm{F}(\mathrm{x}+\mathrm{u})))} \\
&= \zeta_p^{\mathrm{Tr}(-\beta\mathrm{F}(\mathrm{u}))}\widehat{F}(0,\beta) \\
&= \eta_{0,\beta}\zeta_p^{\mathrm{Tr}(-\beta\mathrm{F}(\mathrm{u}))}(\sqrt{p^*})^n.
\end{aligned}$$

From above we can see that $\eta_{\alpha,\beta}\eta_{0,\beta} \in W^+$. The proof of the case where $|\widehat{F}(\alpha,\beta)| = (\sqrt{p^*})^{n+2t}$ is similar and we omit it here. ■

In the following we first determine the Walsh spectrum of F and then determine the weight distribution of $\mathcal{C}_F$.

A. Walsh spectrum of F

By Lemma 9, for each $(\alpha,\beta) \in X_3$, there exists $\eta_{\alpha,\beta} \in W = \{\pm\zeta_p^\lambda : 0 \le \lambda \le p-1\}$ such that $\widehat{F}(\alpha,\beta) = \eta_{\alpha,\beta}p^{n/2}$; and for each $(\alpha,\beta) \in X_4$, there exists $\eta_{\alpha,\beta} \in W$ such that $\widehat{F}(\alpha,\beta) = \eta_{\alpha,\beta}p^{n/2+t}$, where X_3 and X_4 are defined in (3). For each λ with $0 \le \lambda \le p-1$, define

$$\begin{aligned}
\ell_\lambda^+ &= \#\{(\alpha,\beta) \in X_3 \cup X_4 \mid \eta_{\alpha,\beta} = \zeta_p^\lambda\}, \\
\ell_\lambda^- &= \#\{(\alpha,\beta) \in X_3 \cup X_4 \mid \eta_{\alpha,\beta} = -\zeta_p^\lambda\}.
\end{aligned}$$

By Lemma 9, we have $\eta_{\alpha,\beta}\eta_{0,\beta} \in W^+$ and furthermore by Result 5(2) $\eta_{0,\beta} = \epsilon_k$ for $(0,\beta) \in X_3$; and $\eta_{0,\beta} = -\epsilon_k$ for $(0,\beta) \in X_4$. In the following we split the proof into two cases depending on whether k is even or odd.

1) k is even: By Lemma 9 and the above discussions, we have $\eta_{\alpha,\beta} \in W^+$ for all $(\alpha,\beta) \in X_3$ and $\eta_{\alpha,\beta} \in W^-$ for all $(\alpha,\beta) \in X_4$, where W^+ and W^- are defined in Result 6. We first claim that

$$\ell_1^\epsilon = \ell_2^\epsilon = \cdots = \ell_{p-1}^\epsilon, \tag{16}$$

for $\epsilon \in \{+,-\}$. Indeed, it follows from $n = 2kt$ that $(\sqrt{p^*})^n = \left(\frac{-1}{p}\right)^{kt} p^{kt}$ so that $\sigma_a((\sqrt{p^*})^n) = \sigma_a(\sqrt{p^*})^n = \left(\frac{a}{p}\right)^n (\sqrt{p^*})^n = (\sqrt{p^*})^n$ for $1 \le a \le p-1$. Now, for $(\alpha,\beta) \in X_3$, we have $\widehat{F}(a\alpha,a\beta) = \sigma_a(\widehat{F}(\alpha,\beta)) = \sigma_a(\zeta_p^i)(\sqrt{p^*})^n = \zeta_p^{ai}(\sqrt{p^*})^n$ for $1 \le a \le p-1$, which leads to $\ell_1^+ = \ell_2^+ = \cdots = \ell_{p-1}^+$. Similarly, for $(\alpha,\beta) \in X_4$, i.e. $\widehat{F}(\alpha,\beta) = -(\sqrt{p^*})^{n+2t}$, we have $\widehat{F}(a\alpha,a\beta) = \sigma_a(\widehat{F}(\alpha,\beta)) = -\sigma_a(\zeta_p^i)(\sqrt{p^*})^{n+2t} = -\zeta_p^{ai}(\sqrt{p^*})^{n+2t}$ for $1 \le a \le p-1$, which leads to $\ell_1^- = \ell_2^- = \cdots = \ell_{p-1}^-$. For convenience, in the following we let $\ell^+ = \ell_\lambda^+$ and $\ell^- = \ell_\lambda^-$ for $1 \le \lambda \le p-1$.

First, it is not difficult to see that

$$\ell_0^+ + (p-1)\ell^+ = \sum_{\lambda=0}^{p-1} \ell_\lambda^+ = |X_3| = \frac{p^{n+t}(p^n-1)}{p^t+1}, \tag{17}$$

and

$$\ell_0^- + (p-1)\ell^- = \sum_{\lambda=0}^{p-1} \ell_\lambda^- = |X_4| = \frac{p^{n-2t}(p^n-1)}{p^t+1}, \tag{18}$$

where the sizes of X_3, X_4 are given in Lemmas 2 and 3.

Second, by Lemma 7, we have the following two equations

$$\begin{aligned} p^{2n} &= \textstyle\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta) \\ &= p^n + (\sqrt{p^*})^n \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^+ \zeta_p^\lambda - (\sqrt{p^*})^{n+2t} \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^- \zeta_p^\lambda, \\ &= p^n + (\sqrt{p^*})^n \textstyle\sum_{\lambda=0}^{p-1} \left(\ell_\lambda^+ - (\sqrt{p^*})^{2t}\ell_\lambda^-\right) \zeta_p^\lambda, \\ &= p^n + (\sqrt{p^*})^n \Big((\ell_0^+ - (\sqrt{p^*})^{2t}\ell_0^-) + \textstyle\sum_{\lambda=1}^{p-1}(\ell^+ - (\sqrt{p^*})^{2t}\ell^-)\zeta_p^\lambda\Big) \end{aligned} \tag{19}$$

and

$$\begin{aligned} p^{2n} &= \textstyle\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta)^2 \\ &= p^{2n} + (\sqrt{p^*})^{2n} \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^+ \zeta_p^{2\lambda} + (\sqrt{p^*})^{2n+4t} \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^- \zeta_p^{2\lambda}, \\ &= p^{2n} + (\sqrt{p^*})^{2n} \textstyle\sum_{\lambda=0}^{p-1} \Big(\ell_\lambda^+ + p^{2t}\ell_\lambda^-\Big)\zeta_p^{2\lambda} \\ &= p^{2n} + (\sqrt{p^*})^{2n} \Big((\ell_0^+ + p^{2t}\ell_0^-) + \textstyle\sum_{\lambda=1}^{p-1}(\ell^+ + p^{2t}\ell^-)\zeta_p^{2\lambda}\Big). \end{aligned} \tag{20}$$

From Eq. (19) we get $(\ell_0^+ - p^t\ell_0^-) + \sum_{\lambda=1}^{p-1}(\ell^+ - (\sqrt{p^*})^{2t}\ell^-)\zeta_p^\lambda = p^{n/2}(p^n-1)$ since $n/2 = kt$ is even and $(\sqrt{p^*})^n = ((-1)^{(p-1)/2}p)^{n/2} = p^{n/2}$. Furthermore, since $\zeta_p + \cdots + \zeta_p^{p-1} = -1$, we have

$$\begin{aligned} p^{n/2}(p^n-1) &= (\ell_0^+ - (\sqrt{p^*})^{2t}\ell_0^-) + \textstyle\sum_{\lambda=1}^{p-1}(\ell^+ - (\sqrt{p^*})^{2t}\ell^-)\zeta_p^\lambda \\ &= (\ell_0^+ - (\sqrt{p^*})^{2t}\ell_0^-) + (\ell^+ - (\sqrt{p^*})^{2t}\ell^-)\textstyle\sum_{\lambda=1}^{p-1}\zeta_p^\lambda \\ &= (\ell_0^+ - (\sqrt{p^*})^{2t}\ell_0^-) - (\ell^+ - (\sqrt{p^*})^{2t}\ell^-). \end{aligned} \tag{21}$$

Similarly, from Eq. (20) we get $(\ell_0^+ + p^{2t}\ell_0^-) + \sum_{\lambda=1}^{p-1}(\ell^+ + p^{2t}\ell^-)\zeta_p^{2\lambda} = 0$ and then $(\ell_0^+ + p^{2t}\ell_0^-) - (\ell^+ + p^{2t}\ell^-) = 0$. Applying this fact together with $\sum_{\lambda=0}^{p-1}(\ell_\lambda^+ + p^{2t}\ell_\lambda^-) = |X_3| + p^{2t}|X_4|$, we obtain

$$\ell_\lambda^+ + p^{2t}\ell_\lambda^- = \frac{|X_3| + p^{2t}|X_4|}{p} = p^{n-1}(p^n-1) \tag{22}$$

for all $0 \le \lambda \le p-1$.

Finally, from Eqs. (17), (18), (21), (22) we solve $\ell_0^+, \ell_0^-, \ell_\lambda^+, \ell_\lambda^-$ as

$$\begin{aligned} \ell_0^+ &= \tfrac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})}\left(\epsilon p^{n/2} + p^{n/2+t} - p^t + p + p^{t+1} - 1\right), \\ \ell_\lambda^+ &= \tfrac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})}\left(\epsilon p^{n/2} + p^{n/2+t} - p^t - 1\right), \\ \ell_0^- &= \tfrac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})}\left(\epsilon p^{n/2} + p^{n/2+t} + p^t + p^{2t} - p^{t+1} - p^{2t+1}\right), \\ \ell_\lambda^- &= \tfrac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})}\left(\epsilon p^{n/2} + p^{n/2+t} + p^t + p^{2t}\right), \end{aligned}$$

where $\epsilon = (-1)^{(p-1)t/2}$ and $1 \le \lambda \le p-1$. We finish proving the Walsh spectrum of F when k is even.

2) k is odd: In this case, by the discussions above the proof of case (i), we have $\eta_{\alpha,\beta} \in W^-$ for all $(\alpha,\beta) \in X_3$ and $\eta_{\alpha,\beta} \in W^+$ for all $(\alpha,\beta) \in X_4$. Similarly, first we get the two equations

$$\ell_0^- + (p-1)\ell^- = \sum_{\lambda=0}^{p-1}\ell_\lambda^- = |X_3| = \frac{p^{n+t}(p^n-1)}{p^t+1}, \tag{23}$$

and

$$\ell_0^+ + (p-1)\ell^+ = \sum_{\lambda=0}^{p-1} \ell_\lambda^+ = |X_4| = \frac{p^{n-2t}(p^n-1)}{p^t+1}. \tag{24}$$

Second, by Lemma 7, we have the following two equations

$$\begin{aligned} p^{2n} &= \textstyle\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta) \\ &= p^n + (\sqrt{p^*})^{n+2t} \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^+ \zeta_p^\lambda - (\sqrt{p^*})^n \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^- \zeta_p^\lambda, \\ &= p^n + (\sqrt{p^*})^n \textstyle\sum_{\lambda=0}^{p-1} \left((\sqrt{p^*})^{2t}\ell_\lambda^+ - \ell_\lambda^-\right) \zeta_p^\lambda, \\ &= p^n + (\sqrt{p^*})^n \Big(((\sqrt{p^*})^{2t}\ell_0^+ - \ell_0^-) + \textstyle\sum_{\lambda=1}^{p-1}((\sqrt{p^*})^{2t}\ell^+ - \ell^-)\zeta_p^\lambda\Big) \end{aligned} \tag{25}$$

and

$$\begin{aligned} p^{2n} &= \textstyle\sum_{\alpha,\beta\in\mathbb{F}_{p^n}} \widehat{F}(\alpha,\beta)^2 \\ &= p^{2n} + (\sqrt{p^*})^{2n+4t} \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^+ \zeta_p^{2\lambda} + (\sqrt{p^*})^{2n} \textstyle\sum_{\lambda=0}^{p-1} \ell_\lambda^- \zeta_p^{2\lambda}, \\ &= p^{2n} + (\sqrt{p^*})^{2n} \textstyle\sum_{\lambda=0}^{p-1} \left(p^{2t}\ell_\lambda^+ + \ell_\lambda^-\right)\zeta_p^{2\lambda} \\ &= p^{2n} + (\sqrt{p^*})^{2n} \Big((p^{2t}\ell_0^+ + \ell_0^-) + \textstyle\sum_{\lambda=1}^{p-1}(p^{2t}\ell^+ + \ell^-)\zeta_p^{2\lambda}\Big). \end{aligned} \tag{26}$$

From Eq. (25) we get $((\sqrt{p^*})^{2t}\ell_0^+ - \ell_0^-) + \sum_{\lambda=1}^{p-1}((\sqrt{p^*})^{2t}\ell^+ - \ell^-)\zeta_p^\lambda = (-1)^{(p-1)n/4}p^{n/2}(p^n-1)$. Therefore, we have

$$(-1)^{(p-1)n/4}p^{n/2}(p^n-1) = ((\sqrt{p^*})^{2t}\ell_0^+ - \ell_0^-) - ((\sqrt{p^*})^{2t}\ell^+ - \ell^-). \tag{27}$$

Similarly, from Eq. (26) we get $(p^{2t}\ell_0^+ + \ell_0^-) + \sum_{\lambda=1}^{p-1}(p^{2t}\ell^+ + \ell^-)\zeta_p^{2\lambda} = 0$ and then $(p^{2t}\ell_0^+ + \ell_0^-) - (p^{2t}\ell^+ + \ell^-) = 0$. Applying this fact together with $\sum_{\lambda=0}^{p-1}(p^{2t}\ell_\lambda^+ + \ell_\lambda^-) = p^{2t}|X_4| + |X_3|$, we obtain

$$p^{2t}\ell_\lambda^+ + \ell_\lambda^- = \frac{|X_3| + p^{2t}|X_4|}{p} = p^{n-1}(p^n-1) \tag{28}$$

for all $0 \le \lambda \le p-1$. Finally, from Eqs. (23), (24), (27), (28) we solve $\ell_0^+, \ell_0^-, \ell_\lambda^+, \ell_\lambda^-$ as

$$\begin{aligned} \ell_0^+ &= \tfrac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})} \left(\epsilon p^{n/2} + p^{n/2+t} + \epsilon p^{2t+1} + \epsilon p^{t+1} - \epsilon p^{2t} - \epsilon p^t\right) \\ \ell^+ &= \tfrac{p^{n/2-t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})} \left(\epsilon p^{n/2} + p^{n/2+t} - \epsilon p^{2t} - \epsilon p^t\right), \\ \ell_0^- &= \tfrac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})} \left(\epsilon p^{n/2} + p^{n/2+t} - \epsilon p^{t+1} - \epsilon p + \epsilon p^t + \epsilon\right) \\ \ell^- &= \tfrac{p^{n/2+2t-1}(p^n-1)}{(p^t+1)(\epsilon p^t+p^{2t})} \left(\epsilon p^{n/2} + p^{n/2+t} + \epsilon p^t + \epsilon\right), \end{aligned}$$

where $\epsilon = (-1)^{(p-1)t/2}$ and $1 \le \lambda \le p-1$. Then the distribution of the Walsh transform is followed as stated in the Theorem.

B. Weight Distribution of $\mathcal{C}_F$

Based on the Walsh spectrum determined above and Lemma 5, now we start determining the weight distribution of the linear code $\mathcal{C}_F$. In the following we only prove the case that k is even, the proof of k is odd is similar and we omit it. Now,

(i) If $\alpha = \beta = 0$, then $\widehat{F}(\alpha,\beta) = p^n$ and hence $w(c_{\alpha,\beta}) = p^n - p^{n-1} - (p-1)p^{n-1} = 0$;

(ii) If $(\alpha,\beta) \in X_1 \cup X_2$, then $\widehat{F}(\alpha,\beta) = 0$ and therefore $w(c_{\alpha,\beta}) = p^n - p^{n-1}$. Furthermore, we have $|X_1| + |X_2| = (p^n-1)(p^{n-t} - p^{n-2t} + 1)$;

(iii) If $(\alpha,\beta)\in X_3$, assume $\widehat{F}(\alpha,\beta)=\zeta_p^{\lambda}p^{n/2}$ for some λ with $0\le\lambda\le p-1$. Then

$$\begin{aligned} w(c_{\alpha,\beta}) &= (p^n-p^{n-1})-\tfrac{1}{p}\textstyle\sum_{c=1}^{p-1}\sigma_c(\widehat{F}(\alpha,\beta))\\ &= (p^n-p^{n-1})-p^{n/2-1}\textstyle\sum_{c=1}^{p-1}\zeta_p^{\lambda c}\\ &= \begin{cases} p^n-p^{n-1}-p^{n/2-1}(p-1), & \text{if } \lambda=0,\\ p^n-p^{n-1}+p^{n/2-1}, & \text{if } \lambda\neq 0.\end{cases}\end{aligned}$$

The multiplicity $A_{p^n-p^{n-1}-p^{n/2-1}(p-1)}$ (resp. $A_{p^n-p^{n-1}+p^{n/2-1}}$) is clearly equal to ℓ_0^+ (resp. ℓ^+).

(iv) If $(\alpha,\beta)\in X_4$, assume $\widehat{F}(\alpha,\beta)=-\zeta_p^{\lambda}p^{n/2+t}$ for some λ with $0\le\lambda\le p-1$. Then

$$\begin{aligned} w(c_{\alpha,\beta}) &= (p^n-p^{n-1})-\tfrac{1}{p}\textstyle\sum_{c=1}^{p-1}\sigma_c(\widehat{F}(\alpha,\beta))\\ &= (p^n-p^{n-1})-p^{n/2+t-1}\textstyle\sum_{c=1}^{p-1}\zeta_p^{\lambda c}\\ &= \begin{cases} p^n-p^{n-1}+p^{n/2+t-1}(p-1), & \text{if } \lambda=0,\\ p^n-p^{n-1}-p^{n/2+t-1}, & \text{if } \lambda\neq 0.\end{cases}\end{aligned}$$

The multiplicity $A_{p^n-p^{n-1}-p^{n/2+t-1}(p-1)}$ (resp. $A_{p^n-p^{n-1}+p^{n/2+t-1}}$) is clearly equal to ℓ_0^- (resp. ℓ^-).

VIII. Concluding remarks

In this paper, we investigate the properties and applications of a type of zero-difference balanced (ZDB) functions, which are from the additive group of $\mathbb{F}_{p^n}$ to itself and of the form $G(x^{p^t+1})$ with G injective on the set of p^t+1 powers of $\mathbb{F}_{p^n}$. Such ZDB functions include certain quadratic APN and PN functions as special cases by choosing different values of p and t, then consequently the contributions in this paper provide more applications of APN and PN functions. We provide geometrical characterizations of the distribution of the subspaces $H_s=\{F(x+s)-F(s):x\in\mathbb{F}_{p^n}\}$ for $s\in\mathbb{F}_{p^n}^*$, and determine the value distribution of the Walsh coefficients $\widehat{F}(a,b)$. The former result leads to a construction of 4-class association scheme; and the latter is used to determine the weight distribution of the linear code $\mathcal{C}_F$ generated by the matrix C_F defined in (2). Some previous work on determining the weight distribution of $\mathcal{C}_F$ from APN and PN functions are included as special cases.

References

[1] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Menlo Park: Benjamin/Cumming, (1984).

[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, (1999).

[3] R. C. Bose, K. P. Nair, Partially balanced incomplete block designs, Sankhya 4, 337-372, (1939).

[4] R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, Pacific J. Math. 30, 389-419, (1963).

[5] H. Cai, X. Zeng, T. Helleseth, X. Tang and Y. Yang, A new construction of zero-difference balanced functions and its applications, IEEE Trans. Inf. Theory 59(8), 5008–5015, (2013).

[6] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography 15(2), 125-156, (1998).

[7] C. Carlet and C. Ding, Highly nonlinear mappings, Journal of Complexity 20(2-3), 205–244, (2004).

[8] C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory 51(6), 2089-2102, (2005).

[9] C. Carlet, C. Ding, H. Niederreiter, Authentication Schemes from Highly Nonlinear Functions, Designs, Codes and Cryptography 40, 71–79, (2006).

[10] C. Carlet, Vectorial Boolean Functions for Cryptography, Chapter of the monograph *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, 398-472, (2010).

[11] C. Carlet, G. Gong, Y. Tan, Quadratic Zero-Difference Balanced Functions, APN Functions and Strongly Regular Graphs, Designs, Codes and Cryptography, in press.

[12] E. R. van Dam, D. Fon-Der-Flaass, Codes, Graphs, and Schemes From Nonlinear Functions, European Journal of Combinatorics (24)1, 85–98, (2000).

[13] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Report. Suppl. No. 10, (1973).

[14] P. Delsarte, V. I. Levenshtein, Association schemes and coding theory, IEEE Trans. on Infor. Theory 44(6), 2477-2504, (1998).

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

[16] C. Ding, Optimal and perfect systems of sets, Journal of Combinatorial Theory, Series A 116, 109–119, (2009).

[17] C. Ding and Y. Tan, Zero-difference balanced functions with applications, Journal of Statistical Theory and Practice (6)1, 3–19, (2012).

[18] C. Ding, Q. Wang and M. Xiong, Three new families of zero-difference balanced functions with applications, IEEE Trans. Inf. Theory 60(4), 2407–2413, (2014).

[19] C. Ding, Linear Codes From Some 2-Designs, IEEE Trans. on Infor. Theory 61(6), 3265-3275, (2015).

[20] J.F. Dillon, H. Dobbertinb, New cyclic difference sets with Singer parameters, Finite Fields and Their Applications 10(3), 342–389, (2004).

[21] Y. Edel, On quadratic APN functions and dimensional dual hyperovals, Designs, Codes and Cryptography, 57(1), 35–44, (2010).

[22] K. Feng and J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inform. Theory 53(9), 3035–3041 (2007).

[23] C. Godsil, Association schemes, http://www.math.uwaterloo.ca/~cgodsil/pdfs/assoc2.pdf.

[24] S.W. Golomb, G. Gong, Signal design for good correlation for wireless communication, cryptography, and radar, Cambridge University Press, (2005).

[25] T. Helleseth and P. V. Kumar, Sequences with low correlation. In Handbook of Coding Theory, V. Pless and W.C. Huffman (Eds.), Amsterdam, The Netherlands: Elsevier, vol. II, 1765-1854, (1998).

[26] K. Ireland and M. Rosen, A classical introduction to modern number theory, Graduate Texts in Mathematics 84, Springer-Verlag, New York (1990).

[27] G. M. Kyureghyan and A. Pott, Some theorems on planar mappings, Arithmetic of Finite Fields, Lecture Notes in Computer Science 5130, 117–122, (2008).

[28] S. Lang, Cyclotomic fields II, Graduate Texts in Mathematics 69, Springer-Verlag, New York, (1980).

[29] C. Li, N. Li, T. Helleseth, C. Ding, The weight distributions of several classes of cyclic codes from APN monomials, IEEE Trans. on Inform. Theory 60(8), 4710-4721 (2014).

[30] R. Lidl and H. Niederreiter, Finite fields, Encyclopedia Math. Appl. 20, Cambridge University Press, (1983).

[31] K. Nyberg, Perfect nonlinear S-Boxes, Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science 547, 378–386, (1991).

[32] S.L. Ma, A survey of partial difference sets, Design, Codes and Cryptography 4, 221–261 (1994).

[33] D. S. Passman, The Algebraic Structure of Group Rings, Wiley-Interscience, New York, (1977).

[34] A. Pott, Finite geometry and character theory, Lecture Notes in Mathematics 1601, (1995).

[35] Q. Wang and Y. Zhou, Sets of zero-difference balanced functions and their applications, Advances in Mathematical Communications 8(1), 83–101, (2014).

[36] G. Weng, W. Qiu, Z. Wang and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, Designs, Codes and Cryptography 44, 49–62, (2007).

[37] G. Weng, Y. Tan and G. Gong, On almost perfect nonlinear functions and their related algebraic objects, Proceedings of International Workshop on Coding and Cryptography, 48–57, (2013).

[38] Y. Yu, M. Wang and Y. Li, A matrix approach for constructing quadratic APN functions, Proceedings of International Workshop on Coding and Cryptography, 39–47, (2013).

[39] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. on Infor. Theory 52(2), 712-717 (2006).

[40] Z. Zhou, X. Tang, D. Wu and Y. Yang, Some new classes of zero-difference balanced functions, IEEE Trans. Inf. Theory 58(1), 139–145, (2012).