Cryptography and Communications (2019) 11:1297–1306
https://doi.org/10.1007/s12095-019-00394-2

Strongly regular graphs arising from non-weakly regular bent functions

Ferruh Özbudak[1,2] · **Rumİ Melİh Pelen**[2,3]

Received: 20 September 2018 / Accepted: 7 August 2019 / Published online: 14 September 2019

Abstract
In this paper, we study two special subsets of a finite field of odd characteristics associated with non-weakly regular bent functions. We show that those subsets associated to non-weakly regular even bent functions in the *GMMF* class (see Çesmelioğlu et al. Finite Fields Appl. **24**, 105–117 2013) are never *partial difference sets (PDSs)*, and are *PDSs* if and only if they are trivial subsets. Moreover, we analyze the two known sporadic examples of non-weakly regular ternary bent functions given in Helleseth and Kholosha (IEEE Trans. Inf. Theory **52**(5), 2018–2032 2006, Cryptogr. Commun. **3**(4), 281–291 2011). We observe that corresponding subsets are non-trivial *partial difference sets*. We show that they are the union of some cyclotomic cosets and so correspond to 2-class fusion schemes of a cyclotomic scheme. We also present a further construction giving non-trivial PDSs from certain p-ary functions which are not bent functions.

Keywords Non weakly regular bent functions · Partial difference sets · Cyclotomic association schemes · Fusion schemes · Strongly regular graphs

Mathematics Subject Classification (2010) 11T22 · 11T71 · 05E30

This article is part of the Topical Collection on *Special Issue on Boolean Functions and Their Applications*

✉ Ferruh Özbudak
ozbudak@metu.edu.tr

Rumİ Melİh Pelen
rumi.pelen@metu.edu.tr; rumi.pelen@oka.org.tr

[1] Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bulvarı No. 1, 06800, Ankara, Turkey

[2] Department of Mathematics, Middle East Technical University, Dumlupınar Bulvarı No. 1, 06800, Ankara, Turkey

[3] Middle Black Sea Devolopment Agency, Tekkeköy, Samsun, Turkey

1 Introduction

In this paper we introduce a connection between partial difference sets and non-weakly regular bent functions.

Bent functions were first introduced by Rothaus in 1976 as Boolean functions having constant magnitude Walsh transform [16]. They have various applications including coding theory, cryptography and sequence designs. In [11], the authors generalized the notion of bent functions to the case of an arbitrary finite field. Unlike the binary case, not all bent functions are regular over finite field of odd characteristics. They are divided into three subclasses: regular, weakly regular and non weakly regular. Almost all known infinite families of bent functions are weakly regular. In [3], the authors gave a secondary construction method for weakly and non-weakly regular bent functions. This infinite family is called *GMMF* class. So far no primary constructions are known for non-weakly regular bent functions. There are only a few sporadic examples of non-weakly regular bent functions known not in *GMMF* class (see [6–8]).

Partial difference sets (see the Definition 2.1 in Section 2) have been studied extensively because of their connections with other combinatorial objects such as two-weight codes and strongly regular graphs. There are various constructions of partial difference sets in elementary abelian groups, for a brief survey see [12]. It is known that *Cayley* graphs such that their connection sets as are regular partial difference sets are strongly regular graphs (see the Definition 2.4 in Section 2).

One of the tools to construct partial difference sets are bent functions. In [18], the authors proved that pre-image sets of the ternary weakly regular even bent functions are partial difference sets. Shortly after, this result is generalized to arbitrary odd characteristics in [5]. As far as we know, no one introduced a relation between non-weakly regular bent functions and partial difference sets. In this paper, we study the two special subsets of a finite field of odd characteristics associated with the non-weakly regular bent functions which are introduced by the authors in [15]. As a corollary of Proposition 3.1, we prove that if the corresponding subsets of non-weakly regular even bent functions in *GMMF* class are partial difference sets then they are trivial. On the other hand, we analyze these two subsets associated with the two sporadic examples of ternary non-weakly regular bent functions which are introduced in [6, 8]. By using *Magma*, we observe that those subsets are non-trivial partial difference sets and they are the union of the cyclotomic cosets with certain parameters. As a consequence of this, they are 2-class fusion schemes of some cyclotomic association schemes (see the definitions in Section 2) with certain parameters. We also present a further construction giving non-trivial PDSs from certain p-ary functions which are not bent functions.

This paper is organized as follows: In Section 2, we give some mathematical background. In Section 3, we prove that if the two special subsets associated with the non-weakly regular even bent functions in *GMMF* class are partial difference sets then they are trivial. In Section 4, we analyze the corresponding subsets of the two sporadic examples of ternary non-weakly regular bent functions. Our further construction giving non-trivial PDSs from certain p-ary functions which are not bent functions is also given in Section 4. We conclude in Section 5.

2 Mathematical background

Let p be an odd prime and $\mathbb{F}_{p^n}$ the finite field of order p^n. Since it is a vector space of dimension n over $\mathbb{F}_p$, we also use the notation $\mathbb{F}_p^n$ which consists of n-tuples of the prime

field $\mathbb{F}_p$. Let f be a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The Walsh transform of f at $\alpha \in \mathbb{F}_p^n$ is defined as a complex valued function $\hat{f}$ on $\mathbb{F}_p^n$,

$$\hat{f}(\alpha) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x)-\alpha.x}$$

where $\epsilon_p = e^{\frac{2\pi i}{p}}$ and $\alpha.x$ denotes the usual dot product in $\mathbb{F}_p^n$.

The function f is called *bent* function if $|\hat{f}(\alpha)| = p^{n/2}$ for all $\alpha \in \mathbb{F}_p^n$. The normalized Walsh coefficient of a bent function f at α is defined by $p^{-n/2}\hat{f}(\alpha)$. The normalized Walsh coefficients of a bent function f are characterized in [11] as follows:

$$p^{-n/2}\hat{f}(\alpha) = \begin{cases} \pm\epsilon_p^{f^*(\alpha)} & \text{if } p^n \equiv 1 \bmod 4, \\ \pm i\epsilon_p^{f^*(\alpha)} & \text{if } p^n \equiv 3 \bmod 4, \end{cases}$$

where f^* is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, which is called the dual of f.

A bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *regular* if for all $\alpha \in \mathbb{F}_p^n$, we have

$$p^{-n/2}\hat{f}(\alpha) = \epsilon_p^{f^*(\alpha)}$$

and is called *weakly regular* if for all $\alpha \in \mathbb{F}_p^n$, we have

$$p^{-n/2}\hat{f}(\alpha) = \xi\epsilon_p^{f^*(\alpha)}$$

where $\xi \in \{\pm 1, \pm i\}$ is independent from α, otherwise it is called *non-weakly regular*.

Let $B_+(f)$ and $B_-(f)$ be the partitions of $\mathbb{F}_p^n$ given by

$$B_+(f) := \{w : w \in \mathbb{F}_p^n \mid \hat{f}(w) = \xi p^{\frac{n}{2}}\epsilon_p^{f^*(w)}\} \text{ and } B_-(f) := \{w : w \in \mathbb{F}_p^n \mid \hat{f}(w) = -\xi p^{\frac{n}{2}}\epsilon_p^{f^*(w)}\}.$$

where $\xi = 1$ if $p^n \equiv 1 \pmod 4$ and $\xi = i$ if $p^n \equiv 3 \pmod 4$ (see [15]). We use the notation $B_+^\star(f)$ (respectively $B_-^\star(f)$) for the non-zero elements of the corresponding sets. Any bent function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is of two types (see [15]).

$$\text{Type } (+) \text{ if } \hat{f}(0) = \epsilon p^{\frac{n}{2}}\epsilon_p^{f^*(0)}, \ \epsilon \in \{1, i\},$$

$$\text{Type } (-) \text{ if } \hat{f}(0) = \epsilon p^{\frac{n}{2}}\epsilon_p^{f^*(0)}, \ \epsilon \in \{-1, -i\}.$$

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *s-plateaued* if $|\hat{f}(\alpha)| = p^{\frac{n+s}{2}}$ or 0 for all $\alpha \in \mathbb{F}_p^n$. The Walsh spectrum of *s-plateaued* functions is given as follows (see [9]),

$$\hat{f}(\alpha) = \begin{cases} \pm p^{\frac{n+s}{2}}\epsilon_p^{f^*(\alpha)}, 0 & \text{if } n+s \text{ even or } n+s \text{ odd and } p \equiv 1 \bmod 4, \\ \pm ip^{\frac{n+s}{2}}\epsilon_p^{f^*(\alpha)}, 0 & \text{if } n+s \text{ odd and } p \equiv 3 \bmod 4. \end{cases}$$

The regularity and duality are also defined for *s-plateaued* functions in [13]. Moreover, the definitions of the sets $B_+(f)$ and $B_-(f)$ for a plateaued function f is given in [15] similarly. We denote the support of $\hat{f}$ by $\mathrm{Supp}(\hat{f})$ and it is defined as $\mathrm{Supp}(\hat{f}) := \{\alpha : \alpha \in \mathbb{F}_p^n \mid \hat{f}(\alpha) \neq 0\}$. For $v \in \mathbb{F}_p^n$ let $D_v f$ be the derivative function $D_v f(x) : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by $D_v f(x) = f(x+v) - f(x)$. A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called partially bent if the following property holds: For $v \in \mathbb{F}_{p^n}$, if the derivative function $D_v f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is not balanced then $D_v f$ is a constant function. Note that *partially bent* functions are special subclass of *plateaued* functions, and most of the known *plateaued* functions are *partially bent*. In the literature, only a few construction methods for *plateaued* but not *partially bent* functions are known, for example, see [20].

Definition 2.1 (Partial Difference Sets) Let G be a group of order v and D be a subset of G with k elements. Then D is called a (v, k, λ, μ)- *PDS* in G if the expressions $g - h$, for g and h in D with $g \neq h$, represent each non-identity element in D exactly λ times and represent each non-identity element not in D exactly μ times.

Definition 2.2 (*Cayley Graph*) Let G be a finite *abelian* group and D be a subset of G such that $0 \notin D$ and $D = -D$. Let E be the set defined as $\{(x, y)|x, y \in G,\ x - y \in D\}$. Then, (G, E) is called a *Cayley graph*, and denoted by $Cay(G, D)$.

Here, D is called the connection set of (G, E). A PDS is called *regular* if $e \notin D$ and $D^{-1} = D$. A subset D of G is called *trivial* if either $D \cup \{e\}$ or $G/D \cup \{e\}$ is a subgroup of G. It is equivalent to saying that the Cayley graph generated by $D \setminus \{e\}$ is a union of complete graphs or its complement. Otherwise, D is called *non-trivial.*

Proposition 2.1 [12, Propostion 1.5] *Let D be a regular $(v, k, \lambda, \mu)-$ PDS with $D \neq G \setminus \{e\}$. Then D is nontrivial if and only if* $1 \leq \mu \leq k - 1$.

Remark 2.1 $\mu = 0$ implies that that $D \cup \{e\}$ is a subgroup of G. The other case $\mu = k$ implies that D is equal G/H for some subgroup H of G.

Definition 2.3 (Strongly Regular Graphs) A graph Γ with v vertices is said to be a $(v, k, \lambda, \mu)-$ *strongly regular graph* if

(1) it is regular of valency k, i.e., each vertex is joined to exactly k other vertices;
(2) any two adjacent vertices are both joined to exactly λ other vertices and two non-adjacent vertices are both joined to exactly μ other vertices.

Proposition 2.2 [12, Propostion 1.5] *A Cayley graph Γ , generated by a subset D of the regular automorphism group G, is a strongly regular graph if and only if D is a regular PDS in G.*

Definition 2.4 (*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) $V \times V = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$.
(2) $R_i^t = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where $R_i^t := \{(x, y)|(y, x) \in R_i\}$. If $i' = i$, we call R_i is symmetric.
(3) For $i, j, k \in \{0, 1, \ldots, d\}$ and for any pair $(x, y) \in R_k$, the number $\#\{z \in V|(x, z) \in R_i,$ and $(z, y) \in Rj\}$ is a constant, which is denoted by p_{ij}^k.

Definition 2.5 (*Translation Scheme*) Let $\Gamma_i := (G, E_i),\ 1 \leq i \leq d$, be *Cayley graphs* on an *abelian* group G, and D_i be connection sets of (G, E_i) with $D_0 := \{0\}$. Then, $(G, \{D_i\}_{i=0}^d)$ is called a *translation scheme* if $(G, \{\Gamma_i\}_{i=0}^d)$ is an *association scheme*.

Given a d-class translation scheme $(X, \{R_i\}_{i=0}^d)$, we can take unions of classes to form graphs with larger edge sets which is called a *fusion*.

Remark 2.2 (Fusion Scheme) Note that if the fusion gives a *translation scheme* again, it is called *fusion scheme.* However, it is not the case every time.

Definition 2.6 (*Cyclotomic Scheme*) Let $\mathbb{F}_q$ be the finite field of order q, $\mathbb{F}_q^\star$ be the multiplicative group of $\mathbb{F}_q$, and S be a subgroup of $\mathbb{F}_q^\star$ s.t. $S = -S$. The partition $\mathbb{F}_q$ by $\{0\}$ and the multipicative cosets of S gives a *translation scheme* on $(\mathbb{F}_q, +)$, called a cyclotomic scheme.

Each coset (called a *cyclotomic coset*) of $\mathbb{F}_q^\star \setminus S$ is expressed as

$$C_i = w^i \langle w^N \rangle, \quad 0 \le i \le N-1,$$

where $N|q-1$ is a positive integer and w is a fixed primitive element of $\mathbb{F}_q^\star$.

3 Partial difference sets associated with non-weakly regular *GMMF* bent functions are trivial

Let p be an odd prime and $F : \mathbb{F}_p^n \times \mathbb{F}_p^s \to \mathbb{F}_p$ be the map $(x, y) \to f_y(x)$, where $f_y : \mathbb{F}_p^n \to \mathbb{F}_p$ is an *s-plateaued* function for each $y \in \mathbb{F}_p^s$ such that $\mathrm{Supp}(\hat{f}_i) \cap \mathrm{Supp}(\hat{f}_j) = \emptyset$ for $i \neq j, i, j \in \mathbb{F}_p^s$. In [3], the authors showed that F is a bent function. They use *s-partially bent* functions with disjoint supports to obtain *plateaued* functions.

Remark 3.1 In fact, it is not easy to find *s-plateaued* but not *partially bent* functions with disjoint supports. The *plateaued* functions f_a used in [3] can be obtained easily by adding a linear term to a bent function f, i.e. $f_a : \mathbb{F}_p^{n-s} \times \mathbb{F}_p^s \to \mathbb{F}_p$ such that $f_a(x, y) = f(x) + a.y$, where $f : \mathbb{F}_p^{n-s} \to \mathbb{F}_p, a \in \mathbb{F}_p^s$. Then $supp(\hat{f}_i) \cap supp(\hat{f}_j)$ becomes the empty set for all $i, j \in \mathbb{F}_p^s$.

The *bent* functions of the form $F(x, y) = f_y(x)$ are called *GMMF* (Generalized Maiorana-McFarland). The Walsh transform of F at (α, β) is given by

$$\begin{aligned} \hat{F}(\alpha, \beta) &= \sum_{x \in \mathbb{F}_p^n} \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{F(x,y) - \alpha.x - \beta.y} \\ &= \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f_y(x) - \alpha.x} \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-y.\beta} \\ &= \widehat{f_{y_0}(x)}(\alpha) \epsilon_p^{-y_0.\beta}. \end{aligned}$$

where y_0 is the unique element of $\mathbb{F}_p^s$ such that $\alpha \in supp(\widehat{f_{y_0}})$. Then we have,

$$\hat{F}(\alpha, \beta) = \xi_\alpha p^{\frac{n+s}{2}} \epsilon_p^{(f_{y_0})^*(\alpha) - y_0.\beta} \tag{1}$$

which follows from $\widehat{f_{y_0}}(\alpha) = \xi_\alpha p^{\frac{n+s}{2}} \epsilon_p^{(f_{y_0})^*(\alpha)}$, where $\xi_\alpha \in \{\pm 1, \pm i\}$.

Observation F is weakly regular if f_y is weakly regular *s-plateaued* with the same sign for all $y \in \mathbb{F}_p^s$ in their non-zero Walsh coefficients. F is non-weakly regular bent if f_y is weakly regular *s-plateaued* for all $y \in \mathbb{F}_p^s$ and there are $y_1, y_2 \in \mathbb{F}_p^s$ such that $f^{(y_1)}$ and $f^{(y_2)}$ have opposite signs in their non-zero Walsh coefficients or there exists $y \in \mathbb{F}_p^s$ such that f_y is non-weakly regular *s-plateaued*.

Let us partition weakly regular *s-plateaued* functions into two subclasses as f_y is in subclass $(+)$ if its non-zero Walsh coefficients are positive, and in subclass $(-)$ if its non-zero Walsh coefficients are negative. Let $F \in GMMF$ be a non-weakly regular bent function with $F(x) = F(-x)$. Next, we determine the structure of the sets $B_+(F)$ and $B_-(F)$ in two different cases.

Case 1 ($\mathbf{f_y}$ is weakly regular *s-plateaued* for all $\mathbf{y} \in \mathbb{F}_p^s$) By the observation above, one can partition $\mathbb{F}_p^s$ into two subsets as $W^+(F) := \{y : y \in \mathbb{F}_p^s | f_y \text{ is in subclass } (+)\}$ and $W^-(F) := \{y : y \in \mathbb{F}_p^s | f_y \text{ is in subclass } (-)\}$, where $F : \mathbb{F}_p^n \times \mathbb{F}_p^s \to \mathbb{F}_p$ is given by $F(x, y) = f_y(x)$. Then by the (1) we deduce that

$$B_+(F) = (\bigcup_{y \in W^+(F)} supp(\hat{f}_y)) \times \mathbb{F}_p^s \text{ and } B_-(F) = (\bigcup_{y \in W^-(F)} supp(\hat{f}_y)) \times \mathbb{F}_p^s. \quad (2)$$

Case 2 ($\mathbf{f_y}$ is non-weakly regular *s-plateaued* for some $\mathbf{y} \in \mathbb{F}_p^s$) Let $W^+(F)$, $W^-(F)$ be as in the Case 1, and $W_0 := \{y : y \in \mathbb{F}_p^s | f_y \text{ is non-weakly regular } s\text{-plateaued}\}$. Again by the (1) we have

$$B_+(F) = \bigcup_{y \in W_0} (B_+(f_y) \times \mathbb{F}_p^s) \cup (\bigcup_{y \in W^+(F)} supp(\hat{f}_y) \times \mathbb{F}_p^s),$$

$$B_-(F) = \bigcup_{y \in W_0} (B_-(f_y) \times \mathbb{F}_p^s) \cup (\bigcup_{y \in W^-(F)} supp(\hat{f}_y) \times \mathbb{F}_p^s).$$

Remark 3.2 In Cases 1 and 2; the sets $B_+(F)$ and $B_-(F)$ can be viewed as a union of some cosets of the subgroup $\{0\} \times \mathbb{F}_p^s$ in $\mathbb{F}_p^n \times \mathbb{F}_p^s$.

Proposition 3.1 *Let H be a subgroup of $\mathbb{F}_{p^n}$ and K be one of its complement in $\mathbb{F}_{p^n}$, i.e. $H \cap K = \{0\}$ and $H \oplus K = \mathbb{F}_{p^n}$. Let L be a proper subset of K such that $0 \notin L$ and for each $v \in L$, $-v$ is also in L. Let $D = \bigcup_{v \in L}(H + v)$. If D is a PDS in $\mathbb{F}_{p^n}$, then it is trivial.*

Proof Since $0 \notin L$, we have $0 \notin D$, and $H \subset \mathbb{F}_p^n \setminus D$. Since for $v \in L$, $-v$ is also in L, we have $D = -D$. Assume that D is a (p^n, kr, λ, μ) PDS where $\#H = k$, $\#L = r$. Since $H \subset \mathbb{F}_{p^n} \setminus D$, every non-zero elements in H can be represented as $x - y$ exactly μ times, for $x \neq y \in D$. Let $x \neq y$, $x, y \in D$. Let $x = h_1 + v_1$, $y = h_2 + v_2$, for some $h_1, h_2 \in H$ and $v_1, v_2 \in L$, then we get $x - y = (h_1 - h_2) + (v_1 - v_2)$. Clearly, if $v_1 \neq v_2$ then $x - y \notin H$. Hence $x - y \in H$ if and only if $x, y \in H + v_j$ for some $v_j \in L$. Let $x = h_1 + v_j$, $y = h_2 + v_j$. Then $x - y = h_1 - h_2 \in H$. Since H is a group, each non-zero $h \in H$ can be expressed exactly k times by the differences $h_1 - h_2$ for $h_1, h_2, \in H$. If $h \in H$; then for each $v_j \in L$, h can be represented exactly k times as $(h_1 + v_j) - (h_2 + v_j)$ for $h_1 \neq h_2 \in H$. Hence h can be expressed exactly $\#H\#L = k.r$ times as the difference $x - y$ for $x \neq y \in D$. Therefore, $\mu = k.r$, and by Proposition 2.1, we have D is a trivial PDS in $\mathbb{F}_{p^n}$. □

Corollary 3.1 *Let $F \in GMMF$ such that $F(x) = F(-x)$. If $B_+(F)$(or equivalently $B_-(F)$) is a PDS, then it is trivial.*

Proof The proof follows from the Cases 1,2 and Proposition 3.1. □

In the following example, we use a non-weakly regular ternary bent function (see [19]). In [3], the authors showed that it belongs to the *GMMF* class. By using *Magma*, we observe that the set $B_+(g_3)$ is a subgroup of $\mathbb{F}_{3^3}$. Hence, it is a trivial *PDS* in $\mathbb{F}_{3^3}$. Moreover, in [4], the authors claim that g_3 is self-dual bent. However, by *Magma* computations, we observe that the dual function g_3^* of g_3 is indeed equal to $-g_3$, and it is not self-dual.

Example 1 $g_3 : \mathbb{F}_{3^3} \to \mathbb{F}_3$, $g_3(x) = Tr_3(x^{22} + x^8)$ is non-weakly regular of Type (+).

- $B_+^{\star}(g_3)$ is a $(27, 8, 7, 0)$-*PDS* in $\mathbb{F}_{3^3}$.
- $B_-(g_3)$ is a $(27, 18, 9, 18)$-*PDS* in $\mathbb{F}_{3^3}$.

Remark 3.3 By the Corollary 3.1 it follows that if neither $\bigcup_{y\in W^+(F)} supp(\hat{f}_y)$ nor $\bigcup_{y\in W^-(F)} supp(\hat{f}_y)$ is a subgroup of $\mathbb{F}_{p^n}$, then neither $B^+(F)$ nor $B^-(F)$ is a *PDS* in $\mathbb{F}_p^n \times \mathbb{F}_p^s$. Hence, we conclude that not all non-weakly regular bent functions of the form $f(x) = f(-x)$ have the property that $B^+(f)$ or $B^-(f)$ is a partial difference set. It is interesting to determine certain conditions on those sets, so that they become non-trivial *PDSs*. To do this, in the following section we analyze the sets $B^+(f)$ and $B^-(f)$ associated with two of the known sporadic examples of ternary non-weakly regular bent functions.

4 Non-trivial PDSs from ternary non weakly regular bent functions

It is known that one of the tools to construct partial difference sets are bent functions. In [18], the authors proved that pre-image sets of the ternary weakly regular even bent functions are partial difference sets. Shortly after, this result is generalized to arbitrary odd characteristics in [5].

Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a p-ary function, and $D_i := \{x : x \in \mathbb{F}_{p^m} | f(x) = i\}$. The following is due to [18]

Theorem 4.1 *Let $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ be ternary function satisfying $f(x) = f(-x)$, and $f(0) = 0$. Then f is weakly regular bent if and only if D_1 and D_2 are both*

$$(3^{2m}, 3^{2m1} + \epsilon 3^{m1}, 3^{2m2}, 3^{2m2} + \epsilon 3^{m1}) - PDSs,$$

where $\epsilon = \pm 1$. Moreover, $D_0 \setminus \{0\}$ is a

$$(3^{2m}, 3^{2m1} - 1 - 2\epsilon 3^{m1}, 3^{2m2} - 2 - 2\epsilon 3^{m1}, 3^{2m2} - \epsilon 3^{m1}) - PDSs.$$

Later this result is generalized to arbitrary odd characteristic in [5] for the weakly regular bent functions from $\mathbb{F}_{p^{2m}}$ to $\mathbb{F}_p$ satisfying certain conditions. Namely, for a weakly regular bent function f the following subsets

$$\begin{aligned} D &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) = 0\}, \\ D_S &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) \text{ is square}\}, \\ D'_S &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) \text{ is non-zero square}\}, \\ D_N &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) \text{ is non-square}\} \end{aligned}$$

are regular partial difference sets.

As far as we know, no one introduced a relation between non-weakly regular bent functions and partial difference sets. In this section, we examine to a relation between the set $B_+(f)$ (or equivalently $B_-(f)$) and cyclotomic schemes by analyzing two known sporadic examples of non-weakly regular bent functions over $\mathbb{F}_{3^6}$ (see [6, 8]). We observe that the sets $B_+(f)$ (or equivalently $B_-(f)$) corresponding to these sporadic examples are non-trivial partial difference sets and they are fusion scheme of some cyclotomic schemes for certain parameters. Hence, this is a different relation from the previous ones in the sense of while the pre-image sets of some weakly regular bent functions give PDSs, the partition of $\mathbb{F}_{p^{2m}}$ with respect to the sign of the Walsh transformation of some non-weakly regular bent functions also gives PDSs. For the following examples we have $q = 729$, and $N = 13$. Let

w be a fixed primitive element of $\mathbb{F}_{3^6}$. Let C_0 be the multiplicative subgroup of $\mathbb{F}_{3^6}$ generated by w^{13}. For $1 \leq i \leq 12$, C_i denotes the i-th cyclotomic coset of C_0, and defined by $C_i = w^i C_0$.

Example 2 $g_1 : \mathbb{F}_{3^6} \to \mathbb{F}_3$, $g_1(x) = Tr_6(w^7 x^{98})$ is non-weakly regular of Type $(-)$. The dual of g_1 is not bent and corresponding partial difference sets and strongly regular graphs are non-trivial.

- $B_+(g_1)$ is a $(729, 504, 351, 342)$-PDS in $\mathbb{F}_{3^6}$
- $B_-^\star(g_1)$ is a $(729, 224, 62, 71)$-PDS in $\mathbb{F}_{3^6}$

By using *Magma*, we compute $B_+(g_1)$ and $B_-(g_1)$. We observe that $B_+(g_1) = \bigcup_{i\in\{0,3,5,6,7,8,9,11,12\}} C_i$ and $B_-(g_1) = \bigcup_{i\in\{1,2,4,10\}} C_i$. Hence $B_+(g_1)$ and $B_-^\star(g_1)$ are 2-class fusion schemes and correspond to non-trivial strongly regular graphs.

Example 3 $g_5 : \mathbb{F}_{3^6} \to \mathbb{F}_3$, $g_5(x) = Tr_6(w^7 x^{14} + w^{35} x^{70})$ is non-weakly regular of Type $(-)$. The dual of g_5 is not bent. Corresponding partial difference sets are non-trivial.

- $B_+(g_5)$ is a $(729, 504, 351, 342)$- regular PDS in $\mathbb{F}_{3^6}$.
- $B_-^\star(g_5)$ is a $(729, 224, 62, 71)$- regular PDS in $\mathbb{F}_{3^6}$.

Again by *Magma* computations we have, $B_+(g_5) = \bigcup_{i\in\{0,1,2,4,5,6,9,11,12\}} C_i$ and $B_-(g_5) = \bigcup_{i\in\{3,7,8,10\}} C_i$. Hence $B_+(g_5)$ and $B_-^\star(g_5)$ are 2-class fusion schemes and correspond to non-trivial strongly regular graphs.

Remark 4.1 Non-trivial strongly regular graphs correspond to g_1 and g_5 are from a unital: projective $9-ary$ $[28, 3]$ code with weights 24, 27; $VO^-(6, 3)$ affine polar graph (See, [2]).

In fact, these are not the only examples giving non-trivial strongly regular graph. We easily obtain different non-trivial partial difference sets on $\mathbb{F}_{3^6}$ by preserving the images of the functions g_1 and g_5 on C_0. For example the functions; $h_1(x) = Tr_6(w^{7k} x^{154})$ and $h_2(x) = Tr_6(w^{7k} x^{658})$ are non-weakly regular bent for any odd integer k. The corresponding subsets $B_-(h_1) \setminus \{0\}$ and $B_-(h_2) \setminus \{0\}$) are $(729, 224, 62, 71)$-PDSs in $\mathbb{F}_{3^6}$. On the other hand if we take k even the Walsh transform of the corresponding functions h_1 and h_2 have the form;

$$\widehat{h_i}(\alpha) = \begin{cases} 27\epsilon_3^{f^*(\alpha)}, \\ 0, \\ -54, \end{cases}$$

as α runs through $\mathbb{F}_{3^6}^\star$.

Let k be even, $D := \{\alpha : \alpha \in \mathbb{F}_{3^6} | \widehat{h_i}(\alpha) = 0\}$. We observe that D is a $(729, 252, 81, 90)$-PDS in $\mathbb{F}_{3^6}$. The parameters of D are different than the parameters of Examples 2 and 3. Moreover as k is even h_i is not a bent function. This gives a construction of non-trivial strongly regular graphs from certain p-ary functions which are not bent functions.

It is an interesting problem to determine fusion schemes of an N-class cyclotomic scheme on $\mathbb{F}_q$. There are a lot of research papers devoted to this problem, for example, see [1, 10, 14, 17]. Moreover, another interesting problem is to find an explicit relation between non-weakly regular bent functions and 2-class fusion schemes of cyclotomic schemes.

5 Conclusion

We study two special subsets of the finite field of odd characteristics associated with non-weakly regular bent functions. We prove that if $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is non-weakly regular in *GMMF* class, and $f(x) = f(-x)$, then $B_+(f)$ and $B_-(f)$ are *partial difference sets* if and only if they are trivial subsets. We analyze two sporadic examples of non-weakly regular ternary bent functions introduced in [6]. We observe a relation between certain cyclotomic association scheme and the subsets $B_+(f)$ (or equivalently $B_-(f)$) associated with the two sporadic examples. We show that they are non-trivial partial difference sets and 2-class fusion scheme of that cyclotomic association scheme. We give a further construction of non-trivial strongly regular graphs from certain p-ary functions which are not bent functions. It would be interesting to characterize $B_+(f)$ and $B_-(f)$ explicitly in terms of fusions of cyclotomic schemes.

Acknowledgments The authors extend thanks to the anonymous reviewers for their valuable comments and suggestions, which improved the quality and presentation of the manuscript.

References

1. Bannai, E.: Subschemes of some association schemes. J. Algebra **23**(5), 874–883 (1991)
2. Brouwer, A.: Web database of strongly regular graphs. http://www.win.tue.nl/aeb/graphs/srg/srgtab.html (online)
3. Çesmelioğlu, A., Meidl, W., Pott, A.: Generalized Maiorana Mcfarland class and normality of p-ary bent functions. Finite Fields Appl. **24**, 105–117 (2013)
4. Çesmelioğlu, A., Meidl, W., Pott, A.: On the dual of (non)-weakly regular bent functions and self-dual bent functions. Adv. Math. Commun. **7**(4), 425–440 (2013)
5. Chee, T.Y.Z.X., Y.M.: Strongly regular graphs constructed from p-ary bent functions. J. Algebr. Comb., **34**(2)
6. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
7. Helleseth, T., Kholosha, A.: New binomial bent functions over the finite fields of odd characteristic. In: 2010 IEEE International Symposium on Information Theory Proceedings (ISIT), pp. 1277–1281. IEEE (2010)
8. Helleseth, T., Kholosha, A.: Crosscorrelation of m-sequences exponential sums bent functions and jacobsthal sums. Cryptogr. Commun. **3**(4), 281–291 (2011)
9. Hyun, J.Y., Lee, J., Lee, Y.: Explicit criteria for construction of plateaued functions. IEEE Trans. Inf. Theory **62**(12), 7555–7565 (2016)
10. Ikuta, T., Munemasa, A.: Pseudocyclic association schemes and strongly regular graphs. Europ. J. Combin. **31**, 1513–1519 (2010)
11. Kumar, P., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combinatorial Theory Ser. A **40**(1), 90–107 (1985)
12. Ma, S.: A survey of partial difference sets. Des. Codes Crypt. **4**(4), 221–261 (1994)
13. Mesnager, S., Özbudak, F., Sınak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Des Codes Cryptogr. **87**(2-3), 463–480 (2019)
14. Muzychuk, M.: V-rings of permutation groups with Invariant Metric. Ph.D. Thesis, Kiev State University (1987)
15. Özbudak, F., Pelen, R.M.: Duals of non-weakly regular bent functions are not weakly regular and generalization to plateaued functions. Submitted
16. Rothaus, O.S.: On "bent" functions. J. Comb. Theory Series A **20**(3), 300–305 (1976)

17. Feng, Q.X.T., Momihara, K.: Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. Combinatorica **35**, 413–434 (2015)
18. Tan, Y., Pott, A., bent, T.Feng.: Strongly regular graphs associated with ternary functions. J. Combinatorial Theory Ser. A **117**(6), 668–682 (2010)
19. Tan, Y., Yang, J., Zhang, X.: A recursive construction of p-ary bent functions which are not weakly regular. In: 2010 IEEE International Conference on Information Theory and Information Security (ICITIS), pp. 156–159 (2010)
20. Zheng, Y., Zhang, X.-M.: Plateaued functions. In: ICICS, vol. 99, pp. 284–300. Springer (1999)