arXiv:1807.11181v1 [math.CO] 30 Jul 2018

GRAPHS OF VECTORIAL PLATEAUED FUNCTIONS AS DIFFERENCE SETS

AYÇA ÇEŞMELIOĞLU AND OKTAY OLMEZ

Abstract. A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, is a vectorial s-plateaued function if for each component function $F_b(\mu) = Tr_n(\alpha F(x)), b \in \mathbb{F}_{p^m}^*$ and $\mu \in \mathbb{F}_{p^n}$, the Walsh transform value $|\widehat{F_b}(\mu)|$ is either 0 or $p^{\frac{n+s}{2}}$. In this paper, we explore the relation between (vectorial) s-plateaued functions and partial geometric difference sets. Moreover, we establish the link between three-valued cross-correlation of p-ary sequences and vectorial s-plateaued functions. Using this link, we provide a partition of $\mathbb{F}_{3^n}$ into partial geometric difference sets. Conversely, using a partition of $\mathbb{F}_{3^n}$ into partial geometric difference sets, we constructed ternary plateaued functions $f : \mathbb{F}_{3^n} \to \mathbb{F}_3$. We also give a characterization of p-ary plateaued functions in terms of special matrices which enables us to give the link between such functions and second-order derivatives using a different approach.

Keywords: partial geometric designs, partial geometric difference sets, plateaued functions, three-valued cross-corelation function.

1. Introduction

A (block) design is a pair $(\mathcal{P}, \mathcal{B})$ consisting of a finite set $\mathcal{P}$ of points and a finite collection $\mathcal{B}$ of nonempty subsets of $\mathcal{P}$ called blocks. Designs serve as a fundamental tool to investigate combinatorial objects. Also designs have attracted many researchers from different fields for solutions of applications problems including binary sequences with 2-level autocorrelation, optical orthogonal codes, low density parity check codes, synchronization, radar, coded aperture imaging, and optical image alignment, distributed storage systems and cryptographic functions with high nonlinearity[15, 16, 17, 19, 27].

One of the main construction method of designs is called difference set method. This method served as a powerful tool to construct symmetric designs, error correcting codes, graphs and cryptographic functions [1, 2, 3, 4, 5, 18, 20, 29, 31]. This paper will focus on the links

Oktay Olmez's research was supported by TUBITAK Research Grant Proj. No. 115F064.

between designs and a family of a function known as plateaued functions from cryptography. Especially we will investigate the connections between partial geometric difference sets and graph of plateaued functions.

A function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called a p-ary function. If $p = 2$ then the function is simply called as Boolean. p-ary functions with various characteristics have been an active research subject in cryptography. Bent functions and plateaued functions are two well-known families which has prominent properties in this field [6, 7, 8, 9, 10, 11, 22, 23]. These two families of functions can be characterized by their Walsh spectrum. A function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called an s-plateaued function if the Walsh transform $|\widehat{f}(\mu)| \in \{0, p^{\frac{n+s}{2}}\}$ for each $\mu \in \mathbb{F}_{p^n}$. A 0-plateaued function f is called as bent and its Walsh transform satisfies $|\widehat{f}(\mu)| = p^{\frac{n}{2}}$ for each $\mu \in \mathbb{F}_{p^n}$. Plateaued functions and bent functions play a significant role in cryptography, coding theory and sequences for communications [9, 10, 11].

Boolean bent functions were introduced by Rothaus in [32]. These functions have optimal nonlinearity and can only exist when n is even. In [17], it is shown that the existence of Boolean bent functions is equivalent to the existence of a family of difference sets known as Hadamard difference sets. Boolean plateaued functions are introduced by Zheng and Zhang as a generalization of bent functions in [35]. Boolean plateaued functions have attracted the attention of researchers since these functions provide some suitable candidates that can be used in cryptosystems. A difference set characterization of these functions was recently provided by the second author. In [27], it is shown that the existence of Boolean plateaued functions is equivalent to the existence of partial geometric difference sets.

In arbitrary characteristic, the graph of $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, $G_f = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$, plays an important role for the relation to difference sets, [30, 34]. For instance, the graph of a p-ary bent function can be recognized as a relative difference set. In general, a characterization of plateaued functions in terms of difference sets is not known. A partial result in this direction is provided in [13] for partially bent functions which is a subfamily of plateaued functions.

There are recent result concerning explicit characterization of plateaued functions in odd characteristics through their second order derivatives in [12, 24, 25].

In this paper, we first investigate the link between the graph of a plateaued function and partial geometric difference set. We also provide several characterization of plateaued functions in terms of associated difference set properties. By using these characterization we provide a family of vectorial plateaued functions which has an interesting connection to three-valued cross correlation functions.

The organization of the paper is as follows. In Section 2, we provide preliminary results concerning partial geometric difference sets. In Section 3, we mainly provide the links between vectorial plateaued functions and partial geometric difference sets. We also provide a construction as a result of our characterizations. In Section 4, we focus on $p-$ary plateaued function. We provide several characteristics which are obtained from Butson-Hadamard-like matrices. This section also provides results concerning partially bent functions and partial geometric designs.

2. Preliminaries

Let G be a group of order v and let $S \subset G$ be a k-subset. For each $g \in G$, we define

$$\delta(g) := |\{(s,t) \in S \times S \colon g = st^{-1}\}|.$$

Next we define the difference sets of our interest.

Definition 1. Let v, k be positive integers with $v > k > 2$. Let G be a group of order v. A k-subset S of G is called a partial geometric difference set (PGDS) in G with parameters $(v, k; \alpha, \beta)$ if there exist constants α and β such that, for each $x \in G$,

$$\sum_{y \in S} \delta(xy^{-1}) = \begin{cases} \alpha & \text{if } x \notin S, \\ \beta & \text{if } x \in S. \end{cases}$$

There are two subclasses of PGDS namely difference sets and semiregular relative difference sets which have deep connections with coding theory, and cryptography [1, 18, 20]:

- A (v, k, λ)-difference set (DS) in a finite group G of order v is a k-subset D with the property that $\delta(g) = \lambda$ for all nonzero elements of G.
- A (m, u, k, λ)-relative difference set (RDS) in a finite group G of order m relative to a (forbidden) subgroup U is a k-subset R

with the property that

$$\delta(g) = \begin{cases} k & g = 1_G \\ \lambda & g \in G \backslash U \\ 0 & otherwise \end{cases}$$

The RDS is called *semiregular* if $m = k = u\lambda$.

Clearly a (v, k, λ)-DS is a $(v, k; k\lambda, n+k\lambda)$-PGDS and an (m, u, k, λ) semiregular RDS is a $(mu, k; \lambda(k-1), k(\lambda+1)-\lambda)$-PGDS [26].

Group characters are powerful objects to investigate various types of difference sets. A *character* χ of an abelian group G is a homomorphism from G to the multiplicative group of the complex numbers. The character χ_0 defined by $\chi_0(g) = 1$ for all $g \in G$ is called the *principal character*; all other characters are called *nonprincipal*. We define the character sum of a subset S of an abelian group G as $\chi(S) := \sum_{s \in S} \chi(s)$.

Theorem 1 (Theorem 2.12 [26])**.** *A k-subset S of an abelian group G is a partial geometric difference set in G with parameters $(v, k; \alpha, \beta)$ if and only if $|\chi(S)| = \sqrt{\beta - \alpha}$ or $\chi(S) = 0$ for every non-principal character χ of G.*

For instance, let f be a p-ary bent function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The set $G_f = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$ is called graph of f. Any non-principal character χ of the additive group of $\mathbb{F}_{p^n} \times \mathbb{F}_p$ satisfies $|\chi(G_f)|^2 = p^n$ or 0. This observation yields that G_f is a $(p^{n+1}, p^n, p^{2n-1} - p^{n-1}, p^{2n-1} - p^{n-1} + p^n)$-PGDS in $H = \mathbb{F}_{p^n} \times \mathbb{F}_p$.

Walsh transform provides interesting connections between p-ary functions and difference sets. For a prime p, we define a primitive complex p-th root of unity $\zeta_p = e^{\frac{2\pi i}{p}}$. Let f be a function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and let $F(x) = \zeta_p^{f(x)}$. The Walsh transform of f is defined as follows:

$$\widehat{f}(\mu) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) - Tr_n(\mu x)}, \ \mu \in \mathbb{F}_{p^n}$$

where

$$Tr_n(z) = \sum_{i=0}^{n-1} z^{p^i}.$$

The convolution of F and G is defined by

$$(F * G)(a) = \sum_{x \in \mathbb{F}_{p^n}} F(x) G(x - a).$$

We will also take advantage of the convolution theorem of Fourier analysis. The Fourier transform of a convolution of two functions is

$$\widehat{F * G} = \widehat{F} \cdot \widehat{G}.$$

3. Results on Vectorial Functions

Let F be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. For every $b \in \mathbb{F}_{p^m}^*$, the component function F_b of F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is defined as $F_b(x) = Tr_m(bF(x))$. A vectorial function is called *vectorial plateaued* if all its nonzero component functions are plateaued. If the nonzero component functions of a vectorial plateaued function are s-plateaued for the same $0 \leq s \leq n$ then F is called as *s-plateaued* following the terminology in [24].

The set $G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ is called the graph of F. Next we will characterize vectorial functions by their graphs.

Theorem 2. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a vectorial function. Then the graph of F is a $(p^{n+m}, p^n; \alpha, \beta)$ partial geometric difference set in $H = \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ satisfying $\beta - \alpha = \theta$ if and only if $|\widehat{F_b}(a)| \in \{0, \sqrt{\theta}\}$ for all non zero $b \in \mathbb{F}_{p^m}$ and $a \in \mathbb{F}_{p^n}$. In particular, $\alpha = p^{2n-m} - p^{n+s-m}$ and $\beta = p^{n+s} + p^{2n-m} - p^{n+s-m}$.*

Proof. A non-principal character of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ can be written as $\chi_{(a,b)}(x, y) = \zeta_p^{Tr_n(ax)+Tr_m(by)}$ for a nonzero $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$. For any nonzero $b \in \mathbb{F}_{p^n}$, the Walsh transform of F_b is

$$\begin{aligned}\widehat{F_b}(a) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{-Tr_n(ax)+Tr_m(bF(x))} = \sum_{x \in \mathbb{F}_{p^n}} \chi_{(-a,b)}(x, F_b(x)) \\ &= \chi_{(-a,b)}(G_F)\end{aligned}$$

for any $a \in F_{p^m}$. Therefore $|\widehat{F_b}(a)| \in \{0, \sqrt{\theta}\}|$ for all non zero $b \in \mathbb{F}_{p^m}$ if and only if $G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ is a $(p^{n+m}, p^n; \alpha, \beta)$ partial geometric difference set satisfying $\beta - \alpha = \theta$. Using the well-known *Parseval identiy*, one immediately sees that $\theta = p^{n+s}$ and $|\{a \in \mathbb{F}_{p^n} : \widehat{F_b}(a) \neq 0\}| = p^{n-s}$ for some $0 \leq s \leq n$. The parameters of a partial geometric difference set satisfies the relation in [26] and hence we have

$$p^{3n} = (\beta - \alpha)p^n + \alpha\nu = p^{n+s}p^n + \alpha\nu.$$

Then we see that $\alpha = p^{2n-m} - p^{n+s-m}$ and $\beta = p^{n+s} + p^{2n-m} - p^{n+s-m}$. □

Remark 1. Theorem 2 implies that a vectorial function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is s-plateaued if and only if its graph is a partial geometric difference set with the parameters $(p^{n+m}, p^n; p^{2n-m} - p^{n+s-m}, p^{n+s} + p^{2n-m} - p^{n+s-m})$.

Note that Theorem 2 is also valid for $m = 1$, i.e. the case of p-ary functions. Since for an s-plateaued p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the function $bf(x)$ is s-plateaued for each $b \in \mathbb{F}_p^*$, we can consider f as a vectorial s-plateaued function. The case $s = 0$ is the case of vectorial bent functions and if we additionally have $m = n$, these vectorial functions are known as *planar* functions [14].

Next we will investigate links between vectorial $s-$plateaued functions and partial geometric difference sets.

Proposition 3. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a vectorial function. Then F is s-plateaued if and only if*

$$\sum_{a\in\mathbb{F}_{p^n}} |\{s \in \mathbb{F}_{p^n} : y = F(s+x-a)-F(s)+F(a)\}| = \begin{cases} \alpha & \text{if } y \neq F(x), \\ \beta & \text{if } y = F(x) \end{cases}$$

Proof.

$$\begin{aligned}\delta((x,y)) &= |\{((s_1,t_1),(s_2,t_2)) \in G_F \times G_F : x = s_1 - s_2, y = t_1 - t_2 = F(s_1) - F(s_2)\}| \\ &= |\{s_2 \in \mathbb{F}_{p^n} : y = F(s_2 + x) - F(s_2)\}|\end{aligned}$$

So the criteria for PGDS is given by

$$\sum_{a\in\mathbb{F}_{p^n}} \delta((x-a, y-F(a))) = \begin{cases} \alpha & \text{if } y \neq F(x), \\ \beta & \text{if } y = F(x) \end{cases}$$

and hence

$$\sum_{a\in\mathbb{F}_{p^n}} |\{s \in \mathbb{F}_{p^n} : y = F(s+x-a)-F(s)+F(a)\}| = \begin{cases} \alpha & \text{if } y \neq F(x), \\ \beta & \text{if } y = F(x) \end{cases}$$

□

The above result can be associated with the derivative of an $s-$plateaued function. The derivative of a vectorial function is defined by

$$D_aF(x) = F(x + a) - F(x).$$

To see the connection let us first replace y in the expression

$$y = F(s + x - a) - F(s) + F(a)$$

by $F(x) - c$ for $c \in \mathbb{F}_{p^n}$. Hence we have

$$c = F(s) - F(a) - F(s + x - a) + F(x) = D_{s-a}F(a) - D_{s-a}F(x).$$

This observation yields

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_{p^n}} |\{s\in\mathbb{F}_{p^n}\colon y=F(s+x-a)-F(s)+F(a)\}|\\
=&\sum_{a\in\mathbb{F}_{p^n}} |\{s\in\mathbb{F}_{p^n}\colon D_{s-a}F(a)-D_{s-a}F(x)=c\}|\\
=&\sum_{a\in\mathbb{F}_{p^n}} |\{t\in\mathbb{F}_{p^n}\colon D_tF(a)-D_tF(x)=c\}|\\
=&|\{(t,a)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}\colon D_tF(a)-D_tF(x)=c\}|\\
=&N_F(c,x)
\end{aligned}$$

where $N_F(c,x)$ represents the number of pairs $(t,a)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$ such that

$$D_tF(a)-D_tF(x)=c$$

as in Section 2 of [24]. Thus we will have the following result concerning the derivative and PGDS parameters.

Theorem 4. *Let F be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then the set G_F is a PGDS with parameters $(p^{n+m},p^n;\alpha,\beta)$ if and only if*

$$N_F(c,x)=\begin{cases}\alpha, & c\neq 0\\ \beta, & c=0\end{cases}$$

for all $x\in\mathbb{F}_{p^n}$ and some constants α and β.

Remark 2. Using Theorem 4, Proposition 3 and Theorem 2, we are able to prove Theorem 8i. in [24] with a different approach using the properties of partial geometric difference sets. This gives an interesting relation between the parameters of a PGDS and the second order derivatives of (vectorial) plateaued functions.

3.1. **A family of vectorial $s-$plateaued functions.** In this section, we will discuss the link between vectorial s-plateaued functions $F(x)=x^d$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ and the cross-correlation function between two p-ary m-sequences that differ by a decimation d. An m-sequence and its decimation is defined by $u(t)=\sigma^t$ and $v(t)=u(dt)$ where σ is a primitive element of the finite field. The cross-correlation between the sequences u and v is defined by

$$\theta(\tau)=\sum_{t=0}^{p^n-2}\zeta_p^{u(t+\tau)-v(t)}.$$

It can be shown that

$$\theta(\tau) = -1 + \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{Tr_n(ax+x^d)}$$

where $a = -\sigma^\tau$. Therefore for $F_1(x) = Tr(x^d)$, we have

$$\theta(\tau) = -1 + \widehat{F_1}(-a). \tag{1}$$

Theorem 5. *Let $F(x) = x^d$ be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ with $gcd(d, p^n-1) = 1$. If the cross-correlation of the p-ary m-sequences that differ by decimation d takes three values, namely $-1, -1 + p^{\frac{n+s}{2}}$ and $-1 - p^{\frac{n+s}{2}}$, then F is a vectorial s-plateaued function.*

Proof. For each $b \in \mathbb{F}_{p^n}^*$, we denote by $F_b(x)$ the function $F_b(x) = Tr(bF(x)) = Tr(bx^d)$. The walsh transform

$$\widehat{F_b}(0) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{Tr_n(bx^d)} = 0$$

since x^d is a permutation. For each $a \in \mathbb{F}_{p^n}^*$, the Walsh transform of $F_b(x)$

$$\begin{aligned}
\widehat{F_b}(a) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{Tr_n(bx^d - ax)} \\
&= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{Tr_n(c^d x^d - \frac{a}{c} cx)} \\
&= \sum_{y \in \mathbb{F}_{p^n}} \zeta_p^{Tr_n(y^d - \mu y)} \\
&= \widehat{F_1}(\mu)
\end{aligned}$$

where $b = c^d$ and $\mu = a/c$. Note that any $b \in \mathbb{F}_{p^n}^*$ can be written as $b = c^d$ for some $c \in \mathbb{F}_{p^n}^*$. Then using Equation (1), we immediately obtain the result that $F(x)$ is vectorial s-plateaued.

□

Lemma 6. *Let p be an odd prime and n, k be positive integers with $gcd(n, k) = s$. If n/s is odd then* $\gcd(p^n - 1, d) = 1$ *for $d = (p^{2k}+1)/2$ and $d = p^{2k} - p^k + 1$.*

Remark 3. There are only finitely many known functions with a three-valued cross-correlation. Trachtenberg proved the following in his thesis [33]. Let n be an odd integer and k be an integer such that $gcd(n, k) = s$. Then for each of the decimations $d = \frac{p^{2k}+1}{2}$ and $d = p^{2k} - p^k + 1$ the cross-correlation function $\theta_d(\tau)$ takes the values $-1, -1 \pm p^{\frac{n+s}{2}}$.

This result is generalized later by Helleseth in Theorem 4.9 in [21]. He showed that if $gcd(n,k) = s$ and n/s is odd then for the same decimations, $\theta_d(\tau)$ has the values $-1, -1 \pm p^{\frac{n+s}{2}}$. Our result implies that the corresponding vectorial functions are $s-$plateaued.

Pott et. al. provided a classification of weakly regular bent functions via partial difference sets, [34]. In this classification authors showed that a function from $\mathbb{F}_3^n$ to $\mathbb{F}_3$ when n is even satisfying $f(-x) = f(x)$ and $f(0) = 0$ is weakly regular if and only if a $D_1 = \{x : f(x) = 1\}$ and $D_2 = \{x : f(x) = 2\}$ are partial difference sets. Later in [28], the author provided a similar classification for weakly regular bent functions from $\mathbb{F}_3^n$ to $\mathbb{F}_3$ when n is odd via partial geometric difference sets. Next we will also show that our vectorial functions have a similar classification in the case of $p = 3$ and $d = \frac{3^{2k}+1}{2}$.

Theorem 7. . *Let $n \geq 3$ be an integer and $d = \frac{3^{2k}+1}{2}$ with $\gcd(n,k) = s$ and n/s is odd. For $i = 0, 1, 2$ the sets $D_i = \{x : F(x) = Tr_n(x^d) = i\}$ are $(3^n, 3^{n-1}, 3^{2n-3} - 3^{n-2}, 3^{n-1} + 3^{2n-3} - 3^{n-2})$ partial geometric difference sets in the additive group of $\mathbb{F}_{3^n}$.*

Proof. For each $a \in \mathbb{F}_{3^n}^*$, Suppose that $\chi_a(D_1) = x_a + y_a\zeta_3$ with $x_a, y_a \in \mathbb{R}$. Actually, when we are calculating $\chi_a(D_1)$, we are summing powers of ζ_3 as many times as the number of elements in D_1 for which $Tr_n(ax) = 0, 1$ or 2. In other words, if we set

$$D_{1,i} = \{x \in D_1 : Tr(x) = i\}, i = 0, 1, 2$$

we have

$$\chi_a(D_1) = |D_{1,0}| + |D_{1,1}|\zeta_3 + |D_{1,2}|\zeta_3^2 = (|D_{1,0}| - |D_{1,2}|) + (|D_{1,1}| - |D_{1,2}|)\zeta_3$$

and hence

$$x_a = |D_{1,0}| - |D_{1,2}|, y_a = |D_{1,1}| - |D_{1,2}|$$

are both in $\mathbb{Z}$. Also note that for any $x \in \mathbb{F}_{3^n}$,

$$F_1(-x) = Tr((-x)^d) = Tr(-x^d) = -F_1(x)$$

and that gives us

$$x \in D_1 \Longleftrightarrow 2x \in D_2.$$

As a consequence, $\chi_a(D_2) = \overline{\chi_a(D_1)} = x_a + y_a\zeta_3^2$. Since D_i's form a partition of the additive group of $\mathbb{F}_{3^n}$

$$\chi_a(D_0) + \chi_a(D_1) + \chi_a(D_2) = 0,$$

and we obtain

$$\chi_a(D_0) = y_a - 2x_a$$

Consider the Walsh transform values $\widehat{F_1}(a), \widehat{F_1}(-a)$ of $F_1(x) = Tr_n(x^d)$.

$$\begin{aligned}\widehat{F_1}(-a) &= \sum_{x\in\mathbb{F}_{3^n}} \zeta_3^{Tr_n(ax+x^d)} \\ &= \chi_a(D_0) + \zeta_3\chi_a(D_1) + \zeta_3^2\chi_a(D_2) \\ &= y_a - 2x_a + \zeta_3(x_a + y_a\zeta_3) + \zeta_3^2(x_a + y_a\zeta_3^2) \\ &= y_a - 2x_a + \zeta_3(x_a + y_a) + \zeta_3^2(x_a + y_a) = -3x_a\end{aligned}$$

and

$$\begin{aligned}\widehat{F_1}(a) &= \sum_{x\in\mathbb{F}_{3^n}} \zeta_3^{Tr_n(-ax+x^d)} \\ &= \chi_{-a}(D_0) + \zeta_3\chi_{-a}(D_1) + \zeta_3^2\chi_{-a}(D_2) \\ &= \overline{\chi_a(D_0)} + \zeta_3\overline{\chi_a(D_1)} + \zeta_3^2\overline{\chi_a(D_2)} \\ &= \overline{\chi_a(D_0)} + \zeta_3\chi_a(D_2) + \zeta_3^2\chi_a(D_1) \\ &= y_a - 2x_a + \zeta_3(x_a + y_a\zeta_3^2) + \zeta_3^2(x_a + y_a\zeta_3) \\ &= 3(y_a - x_a).\end{aligned}$$

Since $\widehat{F_1}(a), \widehat{F_1}(-a) \in \{0, \pm 3^{(n+s)/2}\}$,

$(x_a, y_a) \in \{(0,0), (0,C), (0,-C), (C,C), (C,0), (C,2C), (-C,-C), (-C,-2C), (-C,0)\}$

where $C = 3^{(n+s-2)/2}$. In the following table values of $\chi_a(D_0), \chi_a(D_1), \chi_a(D_2), W_F(a), W_F(-a)$ corresponding to each possible (x_a, y_a) tuple is given.

	$(0,0)$	$(0,C)$	$(0,-C)$	(C,C)	$(C,0)$	$(C,2C)$	$(-C,-C)$	$(-C,-2C)$	$(-C,0)$
$\chi_a(D_0)$	0	C	$-C$	$-C$	$-2C$	0	C	0	$2C$
$\chi_a(D_1)$	0	$C\zeta_3$	$-C\zeta_3$	$-C\zeta_3^2$	C	$C\zeta_3 - C\zeta_3^2$	$C\zeta_3^2$	$C\zeta_3^2 - C\zeta_3$	$-C$
$\chi_a(D_2)$	0	$C\zeta_3^2$	$-C\zeta_3^2$	$-C\zeta_3$	C	$C\zeta_3^2 - C\zeta_3$	$C\zeta_3$	$C\zeta_3 - C\zeta_3^2$	$-C$
$\widehat{F_1}(a)$	0	0	0	$-3C$	$-3C$	$-3C$	$3C$	$3C$	$3C$
$\widehat{F_1}(-a)$	0	$-3C$	$3C$	-0	$-3C$	$3C$	0	$-3C$	$3C$

The tuples $(C, 2C)$ and $(-C, -2C)$ are impossible since

$$|\chi_a(D_1)| = \sqrt{x_a^2 - x_a y_a + y_a^2} = \sqrt{3C^2} = \sqrt{3^{n+s-1}}$$

which contradicts the fact that $|\chi_a(D_1)| \in \mathbb{Z}$ since $n + s - 1$ is odd. Therefore the sets D_1, D_2 are PGDS.

Next we will show that the tuples $(C, 0)$ and $(-C, 0)$ are also impossible.

First note that $\widehat{F_1}(0) = 0$ since the function $Tr(x^d)$ is balanced. For a non-zero element a the following holds

$$\begin{aligned}\widehat{F_1}(a)\widehat{F_1}(-a) =&\chi_a(D_0)\chi_a(D_0) + \zeta_p\chi_a(D_0)\chi_a(D_2) + \zeta_p^2(\chi_a(D_0)\chi_a(D_1))\\ &+ \zeta_p\chi_a(D_0)\chi_a(D_1) + \zeta_p^2\chi_a(D_1)\chi_a(D_2) + (\chi_a(D_1)\chi_a(D_1))\\ &+ \zeta_p^2(\chi_a(D_0)\chi_a(D_2)) + (\chi_a(D_2)\chi_a(D_2) + \zeta_p\chi_a(D_1)\chi_a(D_2)\\ &= (\chi_a(D_0)\chi_a(D_0) + \chi_a(D_0)\chi_a(D_1) + \chi_a(D_1)\chi_a(D_1))\,(2 - \zeta_p - \zeta_p^2)\\ &= 3\,(\chi_a(D_0)\chi_a(D_0) + \chi_a(D_0)\chi_a(D_1) + \chi_a(D_1)\chi_a(D_1))\\ &= 3\,(\chi_a(D_0)\chi_a(D_0) - \chi_a(D_1)\chi_a(D_2))\end{aligned}$$

We need the following auxiliary lemma.

Lemma 8. *Let S be a $k-$subset of an abelian group G of order v. Then*

$$\sum_{i=0}^{v-1}\chi_i(SS^{-1}) = \sum_{i=0}^{v-1}\chi_i(ke + \sum_{g\in G-e} a_g g) = vk.$$

Proof. In the group ring $\mathbb{Z}G$ the product $SS^{-1} = k\cdot e + \sum_{g\in G-e} a_g\cdot g$ where $a_g \in \mathbb{Z}$. Then

$$\begin{aligned}\sum_{i=0}^{v-1}\chi_i(SS^{-1}) &= \sum_{i=0}^{v-1}\chi_i(ke + \sum_{g\in G-e} a_g g)\\ &= \sum_{i=0}^{v-1} k\cdot\chi_i(e) + \sum_{g\in G-e} a_g\cdot\sum_{i=0}^{v-1}\chi_i(g)\\ &= vk\end{aligned}$$

This holds since for any $g \in G - e$ we have $\sum_{i=0}^{v-1}\chi_i(g) = 0$ and $\sum_{i=0}^{v-1}\chi_i(e) = v$.

□

Using the previous lemma for $S = D_0, D_1$ separately, we obtain

$$\begin{aligned}\sum_{a\in\mathbb{F}_{3^n}}\widehat{F_1}(a)\widehat{F_1}(-a) &= 3\sum_{a\in\mathbb{F}_{3^n}}(\chi_a(D_0)\chi_a(D_0) - \chi_a(D_1)\chi_a(D_2))\\ &= 3\sum_{a\in\mathbb{F}_{3^n}}\chi_a(D_0D_0^{-1}) - 3\sum_{a\in\mathbb{F}_{3^n}}\chi_a(D_1D_1^{-1})\\ &= 3\cdot 3^n\cdot 3^{n-1} - 3\cdot 3^n\cdot 3^{n-1}\\ &= 0\end{aligned}$$

On the other hand, using the values from the table, we can also write

$$\sum_{a\in\mathbb{F}_{3^n}} \widehat{F_1}(a)\widehat{F_1}(-a) = 9(\Lambda_1+\Lambda_2)C^2$$

where $\Lambda_1 = |\{a \in \mathbb{F}_{3^n}^* : (x_a, y_a) = (C, 0)\}|, \Lambda_2 = |\{a \in \mathbb{F}_{3^n}^* : (x_a, y_a) = (-C, 0)\}|$. This implies that for any $a \in \mathbb{F}_{3^n}^*$, $(x_a, y_a) \neq (C, 0), (-C, 0)$ and hence D_0 is also a PGDS. □

Remark 4. By Theorem 5 we have PGDS with parameters $(v = p^{2n}, k = p^n, \alpha = p^n - p^s, \beta = p^{s+n} + p^n - p^s)$. If $p = 3$ then by Theorem 7 we also have PGDS with parameters $(v = 3^n, k = 3^{n-1}, \alpha = 3^{2n-3} - 3^{n-2}, \beta = 3^{n-1} + 3^{2n-3} - 3^{n-2})$. Here we also note that not all decimation will lead such a partition of the finite field $\mathbb{F}_{3^n}$. For instance, let $D_i = \{x : F(x) = Tr_n(x^d) = i\}$ for $d = 3^2 - 3 + 1$. Then computational results imply that none of the D_i's is a partial geometric difference set in $\mathbb{F}_{3^5}$. In general, it is a challenging task to characterize all functions which can be used to obtain a partition of a group into partial geometric difference sets.

If there is such a partition we can define a set of complex vectors

$$z_a = (\chi_a(D_0), \chi_a(D_1), \chi_a(D_2))$$

for any $a \in \mathbb{F}_{3^n}$. Let

$$e = (1, \zeta_3, \zeta_3^2).$$

Then norm of the complex inner product of any vector z_a and e is either 0 or C for some integer C.

Theorem 9. *Let D_0, D_1 and D_2 be a partition of $\mathbb{F}_{3^n}$ and $\lambda = 3^{\frac{n+s-1}{2}}$ be an integer. Suppose for $i = 0, 1, 2$ each D_i is a partial geometric difference set such that $\chi_a(D_i) \in \{0, \pm\lambda, \pm\lambda\zeta_3, \pm\lambda\zeta_3^2\}$ for each non-principal character χ_a. If one of the cases holds*

- $|D_0| = |D_1| = |D_2|$,
- $|D_i| = |D_j| = 3^{n-1} - 3^{\frac{n+s-2}{2}}$ *and* $|D_k| = 3^{n-1} + 2.3^{\frac{n+s-2}{2}}$,
- $|D_i| = |D_j| = 3^{n-1} + 3^{\frac{n+s-2}{2}}$ *and* $|D_k| = 3^{n-1} - 2.3^{\frac{n+s-2}{2}}$.

and $| < z_a, e > |^2$ is either 0 or $3\lambda^2$ then

$$f(x) = \begin{cases} 0, & x \in D_0 \\ 1, & x \in D_1 \\ 2, & x \in D_2 \end{cases}$$

is an s-plateaued function.

Proof. The Walsh transform

$$\widehat{f}(0) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_3^{f(x)} = |D_0| + \zeta_3 |D_1| + \zeta_3^2 |D_2|.$$

With the conditions given in the theorem, we obtain

$$\widehat{f}(0) = \begin{cases} 0 & \text{if } |D_0| = |D_1| = |D_2|, \\ 3^{\frac{n+s}{2}} & \text{if } |D_i| = |D_j| = 3^{n-1} - 3^{\frac{n+s-2}{2}}, |D_k| = 3^{n-1} + 2.3^{\frac{n+s-2}{2}}, \\ -3^{\frac{n+s}{2}} & \text{if } |D_i| = |D_j| = 3^{n-1} + 3^{\frac{n+s-2}{2}}, |D_k| = 3^{n-1} - 2.3^{\frac{n+s-2}{2}}. \end{cases}$$

For each $a \in \mathbb{F}_{3^n}^*$, the Walsh transform of $f(x)$ is

$$\begin{aligned} \widehat{f}(a) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_3^{f(x) - Tr_n(ax)} \\ &= \sum_{x \in D_0} \zeta_3^{Tr_n(-ax)} + \zeta_3 \sum_{x \in D_1} \zeta_3^{Tr_n(-ax)} + \zeta_3^2 \sum_{x \in D_2} \zeta_3^{Tr_n(-ax)} \\ &= \chi_{-a}(D_0) + \zeta_3 \chi_{-a}(D_1) + \zeta_3^2 \chi_{-a}(D_2). \end{aligned}$$

Then with the assumptions of the theorem and after some easy calculations one can show that $|\widehat{f}(a)|^2 \in \{0, 3\lambda^2\}$. □

4. Results on p-ary Functions

In this section we will develop some tools to characterize $p-$ary $s-$plateaued functions. Our results are mimicking the results of [27].

Lemma 10. *Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and $M = (m_{x,y})$ be a $p^n \times p^n$ matrix where $m_{x,y} = \zeta_p^{f(x+y)}$. Then, f is an s-plateaued function if and only if*

$$MM^*M = p^{n+s}M \tag{2}$$

where M^* is the adjoint of the matrix M.

Proof. Suppose f is an plateaued function with $|\widehat{f}(x)| \in \{0, p^{(n+s)/2}\}$ for all $x \in \mathbb{F}_{p^n}$. Then,

$$\begin{aligned}
(MM^*M)_{x,y} &= \sum_{z\in\mathbb{F}_{p^n}} \left(\sum_{c\in\mathbb{F}_{p^n}} m_{x,c}\overline{m_{z,c}} \right) m_{z,y} \\
&= \sum_{z\in\mathbb{F}_{p^n}} \left(\sum_{c\in\mathbb{F}_{p^n}} F(x+c)\overline{F(z+c)} \right) F(z+y) \\
&= \sum_{c\in\mathbb{F}_{p^n}} F(x+c) \left(\sum_{w\in\mathbb{F}_{p^n}} \overline{F(w)}F(w+y-c) \right) \\
&= \sum_{c\in\mathbb{F}_{p^n}} (\overline{F} * F)(c-y)F(x+c) \\
&= \sum_{u\in\mathbb{F}_{p^n}} (F * \overline{F})(u-x-y)F(u) \\
&= ((F * \overline{F}) * F)(x+y).
\end{aligned}$$

Let $A = (F * \overline{F}) * F$. Then, the Fourier transform of A is $\widehat{A} = \widehat{F} \cdot \widehat{\overline{F}} \cdot \widehat{F}$. Now by Fourier inversion

$$\begin{aligned}
A(x+y) &= \frac{1}{p^n} \sum_{\beta\in\mathbb{F}_{p^n}} \widehat{F}(\beta)\widehat{\overline{F}}(\beta)\widehat{F}(\beta)\zeta_p^{Tr((x+y)\beta)} \\
&= p^{n+s}\frac{1}{p^n} \sum_{\beta\in\mathbb{F}_{p^n}} \widehat{F}(\beta)\zeta_p^{Tr((x+y)\beta)} \\
&= p^{n+s}F(x+y).
\end{aligned}$$

Hence the equation holds.

Suppose $MM^*M = p^{n+s}M$. This implies $((F*\overline{F})*F)(x) = p^{n+s}F(x)$ for all $x \in \mathbb{F}_{p^n}$. Apply the Fourier transform on both of the sides. Then,

$$\widehat{F}(x)(\widehat{F}(x) \cdot \overline{\widehat{F}(x)} - p^{n+s}) = 0$$

for all $x \in \mathbb{F}_{p^n}$. Hence, $|\widehat{F}(x)| \in \{0, p^{(n+s)/2}\}$ for all $x \in \mathbb{F}_{p^n}$.

□

Remark 5. An $n \times n$ complex matrix M is called a Butson-Hadamard matrix if

$$MM^* = nI_n.$$

It is easy to see that a $q^n \times q^n$ Butson-Hadamard matrix M also satisfies

$$MM^*M = q^nM.$$

Our result implies that M can be associated with $0-$plateaued function. This indicates the well-known connection between Butson-Hadamard matrices and bent functions.

As a corollary of Lemma 10, we can characterize s-plateaued functions with their first and second derivatives. First and second derivative of a $p-$ary function is defined by

$$D_a f(x) = f(x+a) - f(x)$$

and

$$D_a D_b f(x) = f(x+a+b) + f(x) - f(x+a) - f(x+b)$$

respectively.

Corollary 11 (Theorem 3, [24])**.** *f is an s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ if and only if the expression $\sum_{a,b\in\mathbb{F}_{p^n}} \zeta_p^{D_a D_b f(u)}$ does not depend on $u \in \mathbb{F}_{p^n}$. This constant expression equals to p^{n+s}.*

Proof. Since the equation

$$MM^*M = p^{n+s}M$$

holds,

$$M^*MM^* = p^{n+s}M^*$$

holds too. Fix two non-zero elements x and y of $\mathbb{F}_{p^n}$ and let $u = x+y$.

$$\begin{aligned}\sum_{z\in\mathbb{F}_{p^n}} \left(\sum_{c\in\mathbb{F}_{p^n}} \overline{m_{x,c}} m_{z,c} \right) \overline{m_{z,y}} &= \sum_{z\in\mathbb{F}_{p^n}} \left(\sum_{c\in\mathbb{F}_{p^n}} \zeta_p^{-f(x+c)} \zeta_p^{f(z+c)} \right) \zeta_p^{-f(z+y)} \\ &= \sum_{c,z\in\mathbb{F}_{p^n}} \zeta_p^{-f(x+c)+f(z+c)-f(z+y)} \\ &= p^{n+s} \zeta_p^{-f(x+y)}\end{aligned}$$

Now let $z = a+x$ and $c = b+y$. Then

$$p^{n+s} = \sum_{a,b\in\mathbb{F}_{p^n}} \zeta_p^{-f(x+y+b)+f(a+b+x+y)-f(a+x+y)+f(x+y)}$$

holds. Thus,

$$p^{n+s} = \sum_{a,b\in\mathbb{F}_{p^n}} \zeta_p^{D_a D_b f(u)}.$$

□

Corollary 12. *Let $\Delta_f(a) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{D_a f(x)}$. f is an s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ if and only if $\sum_{a\in\mathbb{F}_{p^n}} \overline{\Delta_f(a)} \Delta_f(a) = p^{2n+s}$.*

Proof. We have

$$MM^*MM^* = p^{n+s}MM^*.$$

Let

$$N = MM^*.$$

Then

$$\begin{aligned}(N)_{0,a} &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{f(x)-f(a+x)} \\ &= \overline{\Delta_f(a)}\end{aligned}$$

and

$$\begin{aligned}(N)_{a,0} &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{f(a+x)-f(x)} \\ &= \Delta_f(a)\end{aligned}$$

Therefore

$$\begin{aligned}(N^2)_{0,0} &= \sum_{a\in\mathbb{F}_{p^n}} \overline{\Delta_f(a)}\Delta_f(a) \\ &= p^{n+s}(N)_{0,0} \\ &= p^{2n+s}\end{aligned}$$

□

Now we will use our characterization to provide a simple construction of s-plateaued functions. If A is an $m \times n$ matrix and B is an $s \times t$ matrix, then the Kronecker product $A \otimes B$ is the $ms \times nt$ block matrix:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix},$$

Proposition 13. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be s_1-plateaued and s_2-plateaued functions respectively. Let M and N be the matrices whose entries determined by $m_{x,y} = \zeta_p^{f(x+y)}$ and $n_{a,b} = \zeta_p^{g(a+b)}$. Let $P = M \otimes N$ be the Kronecker product of M and N. Then*

$$PP^*P = p^{n+m+s_1+s_2}P$$

holds.

Proof. Let $P = M \otimes N$. Then

$$\begin{aligned} PP^*P &= (M \otimes N)(M^* \otimes N^*)(M \otimes N) \\ &= (MM^*M) \otimes (NN^*N) \\ &= \left(p^{n+s_1}M\right) \otimes \left(p^{m+s_2}N\right) \\ &= p^{n+m+s_1+s_2}(M \otimes N) \\ &= p^{n+m+s_1+s_2}P \end{aligned}$$

□

Corollary 14. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be two s_1-plateaued and s_2-plateaued functions respectively. Then there exists an $(s_1 + s_2)$-plateaued function from $\mathbb{F}_{p^{n+m}}$ to $\mathbb{F}_p$.*

Proof. Let M and N be matrices associated with f and g such that $m_{x,y} = \zeta_p^{f(x+y)}$ and $n_{a,b} = \zeta_p^{g(a+b)}$. Let $P = M \otimes N$. We need to show that there exist a function h such that the entries of P can be associated with h.

We will index the rows and columns of P by the elements of $\mathbb{F}_{p^{n+m}}$. First note that there is a subgroup H of the additive group of $\mathbb{F}_{p^{n+m}}$ which is isomorphic to the additive group of $\mathbb{F}_{p^m}$. Let us fix a transversal $T = \{\gamma_1, \gamma_2, \ldots, \gamma_{p^n}\}$ of this subgroup in $\mathbb{F}_{p^{n+m}}$. Now order the rows and columns of P by $\gamma_1 + H$, $\gamma_2 + H$, ..., $\gamma_{p^n} + H$ in the block form. Here we have isomorphisms namely

$$\phi_1 : H \to \mathbb{F}_{p^m}$$

and

$$\phi_2 : \{\gamma_1 + H, \gamma_2 + H, \ldots, \gamma_{p^n} + H\} \to \mathbb{F}_{p^n}$$

If $x, y \in \mathbb{F}_{p^{n+m}}$ then $x = \gamma_i + u$ and $y = \gamma_j + v$ for unique elements $u, v \in H$. Now let us examine the xy-th entry of P.

$$P_{x,y} = \zeta_p^{f(\phi_2(\gamma_i+H)+\phi_2(\gamma_j+H))} \cdot \zeta_p^{g(\phi_1(u)+\phi_1(v))} = \zeta_p^{h(x+y)}$$

where h is the desired $(s_1 + s_2)$-plateaued function from $\mathbb{F}_{p^{n+m}}$ to $\mathbb{F}_p$. Moreover if $y = 0$ then $\gamma_j = v = 0$. Thus

$$h(x) = f(\phi_2(\gamma_i + H)) + g(\phi_1(u)).$$

□

4.1. **Partially bent functions.** This section is devoted to investigate a family of $s-$plateaued functions known as partially bent functions. A $p-$ary function is called partially bent if the derivative $D_a f$ is either balanced or constant for any $a \in \mathbb{F}_{p^n}$. Here we will provide some characterization via their associated designs.

Let f be an s-plateaued function and for $a \in \mathbb{F}_{p^n}$ define the set

$$T_a = \{x + a, f(x) + f(a) : x \in \mathbb{F}_{p^n}\}.$$

Fix an element a of $\mathbb{F}_{p^n}$, then the graph of f can be also written as

$$G_f = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\} = \{(x + a, f(x + a)) : x \in \mathbb{F}_{p^n}\}.$$

Lemma 15. *Let f be an s-plateaued function with $f(0) = 0$. If f has a linear structure Λ then $T_a = G_f$ for all $a \in \Lambda$.*

Corollary 16. *Let f be an s-plateaued function with $f(0) = 0$ and linear structure Λ of dimension m. Then the incidence matrix A of the design associated with the partial geometric difference set G_f can be written as a Kronecker product of $1 \times p^m$ all-ones matrix j and an incidence matrix N of a partial geometric design.*

Proof. Let j be the $1 \times p^m$ all-ones matrix. Let D be the block design associated with G_f where the point set is $\mathbb{F}_{p^n} \times \mathbb{F}_p$ and the blocks are the translates of the graph of f. Suppose $\mathbf{B}$ is a block in D. Note that $\mathbf{B} = (u, v) + G_f$ for some $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{F}_p$. Then for each $a \in \Lambda$ we have

$$\mathbf{B} + (a, f(a)) = \mathbf{B}$$

since

$$(u, v) + G_f = \{(x + u + a, f(x + a) + v) : x \in \mathbb{F}_{p^n}\}.$$

Thus each block is repeated p^m many times. Therefore, $A = j \otimes N$ for some incidence matrix N. Now we are going to show that N is an incidence matrix of a partial geometric design. Since A is an incidence matrix of a partial geometric design,

$$\begin{aligned} AA^tA &= (\beta - \alpha)j \otimes N + \alpha J_{p^n \times p^n} \\ &= j \otimes (\beta - \alpha)N + \alpha j \otimes J_{p^n \times p^{n-m}} \\ &= j \otimes (\beta - \alpha)N + \alpha J_{p^n \times p^{n-m}}. \end{aligned}$$

We also have

$$\begin{aligned} AA^tA &= jj^tj \otimes NN^tN \\ &= p^m j \otimes NN^tN \\ &= j \otimes p^m NN^tN. \end{aligned}$$

By comparing the left hand sides we can conclude that the equation

$$NN^tN = \frac{(\beta - \alpha)}{p^m}N + \frac{\alpha}{p^m}J_{p^n \times p^{n-m}}$$

holds. □

Let f be an s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then the set D_f is a PGDS with parameters $(p^{n+1}, p^n; p^{2n-1}-p^{n+s-1}, p^{2n-1}-p^{n+s-1}+p^{n+s})$. If f is a partially bent function then there is an integer $s \geq 0$ such that f is s-plateaued and the linear space of f has dimension s. Our observation yields the following result.

Corollary 17. *If f is partially bent function then f can be associated with a partial geometric design with parameters*

$v = p^{n+1}, b = p^{n+1-s}, k = p^n, r = p^{n-s}, \alpha = p^{2n-1-s}-p^{n-1}, \beta = p^n+p^{2n-1-s}-p^{n-1}$.

References

[1] E. F. Assmus and J. D. Key. Designs and their Codes. Cambridge University Press, No. 103. (1992).

[2] A. Bernasconi, B. Codenotti, and J. M. Vanderkam. A characterization of bent functions in terms of strongly regular graphs. IEEE Transactions on Computers, Sep 1(9): pp. 984-5 (2001).

[3] T. Beth, D. Jungnickel, and H. Lenz. Design Theory, Cambridge University Press, second edition, (1999).

[4] A. E. Brouwer, O. Olmez and S. Y. Song. Directed strongly regular graphs from $1\frac{1}{2}$-designs. European Journal of Combinatorics, 33(6): pp. 1174 -1177 (2012).

[5] M. Buratti, Y. Wei, D. Wu, P. Fan, and M. Cheng: Relative difference families with variable block sizes and their related OOCs. IEEE Transactions on Information Theory, 57: pp. 7489-7497 (2011).

[6] C. Carlet and E. Prouff. On plateaued functions and their constructions. In Fast Software Encryption, Springer: pp. 54-73 (2003).

[7] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine. On cryptographic properties of the cosets of $r(1, m)$. IEEE Transactions on Information Theory 47(4), pp. 1494-1513 (2001).

[8] C. Carlet. Partially-bent functions. Designs, Codes and Cryptography 3(2), pp. 135-145 (1993).

[9] C. Carlet. Boolean functions for cryptography and error correcting codes.Boolean models and methods in mathematics, computer science, and engineering 2, pp. 257-397 (2010).

[10] C. Carlet. Boolean and vectorial plateaued functions and APN functions. IEEE Transactions on Information Theory 61(11), pp. 6272-6289 (2015).

[11] C. Carlet and S. Mesnager. Four decades of research on bent functions. Designs, Codes and Cryptography 78(1), 5-50 (2016).

[12] C. Carlet, S. Mesnager, F. Özbudak, A. Sınak. Explicit characterizations for plateauedness of $p-$ary (vectorial) functions. In: Second International Conference on Codes, Cryptology and Information Security (C2SI-2017), In Honor of Claude Carlet. pp. 328-345 (2017).

[13] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu. Partially bent functions and their properties. In: Larcher, G., Pillichshammer, F., Winterhof, A., Xing, C. (eds.) Applications of Algebra and Number Theory, pp. 22-40. Cambridge University Press, Cambridge (2014).

[14] R.S. Coulter, R.W. Matthews. Bent polynomials over finite fields. Bulletin of the Australian Mathematical Society 56(3), pp. 429-437 (1997).

[15] F. R. K. Chung, J. A. Salehi, and V. K. Wei. Optical orthogonal codes: design, analysis, and applications. IEEE Transactions on Information Theory, 35: pp. 595-604 (1989).
[16] Ph. Delsarte. Weights of linear codes and strongly regular normed spaces. Discrete Mathematics, 3(1): pp. 47-64 (1972).
[17] J. F. Dillon. Elementary Hadamard difference sets. PhD thesis, University of Maryland, (1974).
[18] T. W. Cusick, C. Ding and A. Renvall. Stream Ciphers and Number Theory. North-Holland Mathematical Library, The Netherlands: North-Holland/Elsevier, Amsterdam, vol. 55. (1998).
[19] C. Ding. Linear codes from some 2-designs. IEEE Transactions on Information Theory, 61(6): pp. 3265-3275 (2015).
[20] C. Ding. Codes from difference sets. World Scientific Publishing Company, (2015).
[21] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences, Discrete Mathematics 16, pp. 209-232 (1976).
[22] S. Mesnager. Characterizations of plateaued and bent functions in characteristic p. In: International Conference on Sequences and Their Applications. pp. 72-82 (2014).
[23] S. Mesnager. Bent functions: Fundamentals and Results. Switzerland, Springer, pp. 1-544 (2016).
[24] S. Mesnager, F. Özbudak, A. Sınak. Results on characterizations of plateaued functions in arbitrary characteristic. Cryptography and information security in the Balkans, BalkanCryptSec 2015, Koper, Slovenia, Revised Selected Papers. In: Pasalic E., Knudsen L.R. (eds.) LNCS 9540, pp. 17-30. Springer, Berlin (2016)
[25] S. Mesnager, F. Özbudak, A. Sınak. On the p-ary (cubic) bent and plateaued (vectorial) functions. Des. Codes Cryptogr., vol 86 (8), pp 1865-1892 (2018).
[26] O. Olmez. Symmetric $1\frac{1}{2}$-designs and $1\frac{1}{2}$-difference sets. J. Combin. Designs. vol. 22, No. 6, pp. 252-269, (2014).
[27] O. Olmez. Plateaued functions and one-and-half difference sets. Designs, Codes and Cryptography, Sep 1 vol. 76, No. 3, pp. 537-49, (2015).
[28] O. Olmez. A link between combinatorial designs and three-weight linear codes. Designs, Codes and Cryptography, 86(4), pp. 817-833 (2018).
[29] A. Pott. Finite Geometry and Character Theory, Springer, 1995.
[30] A. Pott. Nonlinear functions in abelian groups and realtive difference sets. Discrete Applied Mathematics, 138 (1-2), pp.177-193 (2004).
[31] A. Pott, Y. Tan, T. Feng, and S. Ling. Association schemes arising from bent functions. Designs, Codes and Cryptography, 59(1), pp. 319-331 (2011).
[32] O. S. Rothaus. On bent functions. Journal of Combinatorial Theory, Series A, 20(3), pp. 300-305 (1976).
[33] H. M. Trachtenberg. On the cross-correlation functions of maximal linear sequences. Ph. D Dissertation, University of Southern California, Los Angeles, CA (1970).
[34] Y. Tan, A. Pott, and T. Feng. Strongly regular graphs associated with ternary bent functions. Journal of Combinatorial Theory, Series A, 117(6), pp. 668-682 (2010).

[35] Y. Zheng, X. M. Zhang. Plateaued functions. In: ICICS. vol. 99, pp. 284-300 (1999).

Department of Mathematics, Faculty of Science, Ankara University, Tandogan, Ankara, 06100, Turkey.
E-mail address, O. Olmez: ooolmez@ankara.edu.tr