Des. Codes Cryptogr. (2015) 76:537–549
DOI 10.1007/s10623-014-9975-z

Plateaued functions and one-and-half difference sets

Oktay Olmez

Received: 5 June 2013 / Revised: 29 April 2014 / Accepted: 29 April 2014 /
Published online: 21 May 2014

Abstract We construct an infinite family of $1\frac{1}{2}$-difference sets in non-cyclic abelian p-groups. In particular, we examine the construction in 2-groups to discover the useful relationship between $1\frac{1}{2}$-difference sets and certain Boolean functions.

Keywords $1\frac{1}{2}$-Design · $1\frac{1}{2}$-Difference set · Plateaued function · Bent function · Semibent function

Mathematics Subject Classification 05B05 · 05B10 · 06E30

1 Introduction and preliminaries

We begin this paper by recalling several combinatorial objects that will be used throughout. Let v, k and λ be integers with $2 \leq k \leq v$. A k-element subset S of a (multiplicative) abelian group G of order v is called a (v, k, λ)-difference set if every nonidentity element of G can be expressed as st^{-1} for exactly λ distinct ordered pairs (s, t) in $S \times S$. Thus, its parameters hold the identity $\lambda(v-1) = k(k-1)$. The notion of a $1\frac{1}{2}$-difference set, which was introduced in [15], may be viewed as a generalization of the notion of a difference set.

Definition 1.1 Let G be a group of order v, and let S be a k-element subset of G. For each $g \in G$, let $\zeta(g)$ denote the number of ordered pairs $(s, t) \in S \times S$ such that $st^{-1} = g$. Then, S is called a $1\frac{1}{2}$-difference set with parameters $(v, k; \alpha, \beta)$ if

(i) for each $x \in G - S$, the sum $\sum_{s\in S} \zeta(xs^{-1})$ equals α, and
(ii) for each $x \in S$, the sum $\sum_{s\in S-\{x\}}(\zeta(xs^{-1}) - 1)$ equals β.

Communicated by A. Pott.

O. Olmez (✉)
Department of Mathematics, Faculty of Science, Ankara University, Tandogan, Ankara 06100, Turkey
e-mail: oolmez@ankara.edu.tr

We can easily see that a (v, k, λ)-difference set is a $1\frac{1}{2}$-difference set with $\alpha = k\lambda$ and $\beta = (k-1)(\lambda-1)$. Difference sets have been used to construct other combinatorial structures with applications in engineering, such as binary sequences with 2-level autocorrelation functions, optical orthogonal codes, low density parity check codes, and cryptographic functions with high nonlinearity (cf. [9,10,12,16]). Difference sets have been also used in the construction of symmetric 2-designs. As a continuation of the work reported in [15], in this paper we investigate the existence and nonexistence of $1\frac{1}{2}$-difference sets by using the classical tools such as group rings and group characters. Also our aim is to show how we can make use of $1\frac{1}{2}$-difference sets in the construction of certain designs and nonlinear Boolean functions. First, we recall some basic facts related to block designs.

A block design consists of a finite set P of points and a collection $\mathcal{B}$ of (distinct) non-empty proper subsets of P. This design is denoted by the pair $(P, \mathcal{B})$ and $\mathcal{B}$ is called the block set. Given $x \in P$ and $B \in \mathcal{B}$, the point-block pair (x, B) is called a *flag* if $x \in B$ and an *antiflag* if $x \notin B$. A 1-design with parameters (v, b, k, r) is a block design $(P, \mathcal{B})$ with v points and b blocks satisfying the property that every block consists of k points and every point belongs to r blocks.[1] Its parameters satisfy the identity $vr = bk$. A 2-design is a 1-(v, b, k, r)-design satisfying the additional property that any two points occur together in λ blocks. Such a design is often denoted by 2-(v, k, λ)-design. It holds $(v-1)\lambda = r(k-1)$. A design is called symmetric if $v = b$. We note that a (v, k, λ)-difference set D in an abelian group G gives rise to a symmetric 2-(v, k, λ)-design $(G, \mathcal{B})$ with $\mathcal{B} = \{Dg : g \in G\}$ where each block $Dg := \{xg : x \in D\}$ is generated by D. We are especially interested in the following block designs that are related to $1\frac{1}{2}$-difference sets.

Definition 1.2 A 1-(v, b, k, r)-design $(P, \mathcal{B})$ is called a $1\frac{1}{2}$-design with parameters $(v, b, k, r; \alpha, \beta)$ if for any given point $x \in P$ and block $B \in \mathcal{B}$, the number of the flags (y, C) satisfying $y \in B - \{x\}$, $C \ni x$ and $C \neq B$, is α if $x \notin B$, and is β if $x \in B$.

We can see that every 2-(v, k, λ)-design is a $1\frac{1}{2}$-design with $\alpha = k\lambda$ and $\beta = (k-1)(\lambda-1)$. Other well-known examples of $1\frac{1}{2}$-designs include transversal designs and partial geometries. For more information on $1\frac{1}{2}$-designs, we refer to Neumaier [14].[2]

We now recall Boolean functions of our interest. Let $\mathbb{F} = \{0, 1\}$ be the field of order 2, and let $V_s = \{(a_1, a_2, \ldots, a_s) : a_i \in \{0, 1\}\}$, the extension field whose additive group is an elementary 2-group that is often used as an s-dimensional vector space over $\mathbb{F}$. A function f from V_s to $\mathbb{F}$ is called a Boolean function of s variables. Boolean functions with various characteristics have been an active research subject in cryptography in connection with differential and linear cryptanalysis (cf. [7,8,17]). For a Boolean function f, we can define a function $F := (-1)^f$ from V_s to the set $\{-1, 1\}$. The Fourier transform of F is defined as follows:

$$\widehat{F}(x) = \sum_{y \in V_s} (-1)^{x \cdot y} F(y)$$

where $x \cdot y$ is the inner product of two vectors $x, y \in V_s$. The nonlinearity N_f of f can be expressed as

$$N_f = 2^{s-1} - \frac{1}{2} \max \left\{ |\widehat{F}(x)| : x \in V_s \right\}.$$

[1] It is often known as a tactical configuration.

[2] Bose [2] studied $1\frac{1}{2}$-designs and called them partial geometric designs.

It holds that $N_f \leq 2^{s-1} - 2^{(s-2)/2}$. A function f is called a bent function if $|\widehat{F}(x)| = 2^{s/2}$ for all $x \in V_s$. A bent function has an optimal nonlinearity. However a bent function is not balanced and can exist only in even number of variables which are not desirable. A combinatorial characterization of bent functions is given as follows:

> Having a Hadamard difference set with parameters $(2^s, 2^{s-1} \pm 2^{(s-2)/2}, 2^{s-2} \pm 2^{(s-2)/2})$ is equivalent to having a bent function from V_s to $\mathbb{F}$ [10].

In the work of [17], plateaued functions are introduced as functions which either are bent or have a Fourier spectrum with three values 0 and $\pm 2^t$ for some integer t. It is known that these functions provide some suitable candidates that can be used in cryptosystems [7,17]. Among the subclasses of plateaued functions, semibent and partially-bent functions are studied the most [5,8]. However, the combinatorial characterization of these functions in terms of difference sets are not known.

In this paper, we not only provide some infinite families of $1\frac{1}{2}$-difference sets found in elementary abelian p-groups, but also show an interesting relation between plateaued functions and families of $1\frac{1}{2}$-difference sets in elementary abelian 2-groups. The organization of the paper is as follows. In the following section, we recall some more properties of $1\frac{1}{2}$-difference sets and main tools that will be needed later. In Sect. 3, we provide examples of $1\frac{1}{2}$-difference sets. In our constructions, we mainly focus on cosets of elementary abelian p-groups. In Sect. 4, we provide the relation between plateaued functions and $1\frac{1}{2}$-difference sets.

2 Parameters of $1\frac{1}{2}$-difference sets

We make use of the group ring and character theory to derive some characteristics of $1\frac{1}{2}$-designs. Let G be a finite abelian group and let $\mathbb{Z}G$ be the group ring of G. By the definition, $\mathbb{Z}G$ is the ring of formal polynomials

$$\mathbb{Z}G = \left\{ \sum_{g \in G} a_g \mathcal{g} : \ a_g \in \mathbb{Z} \right\}$$

where each $\mathcal{g}$ denotes the indeterminate corresponding to g. We will use calligraphic letters to denote elements of $\mathbb{Z}G$. The ring $\mathbb{Z}G$ has the operation of addition and multiplication given by

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

For any element g in G and any nonempty subset S of G, the corresponding group ring elements $\mathcal{g}$ and $\sum_{s \in S} s$ are called *simple quantities* in $\mathbb{Z}G$. We denote $\sum_{s \in S} s$ by $\mathcal{S}$, and denote the simple quantity for the set $S^{-1} = \{s^{-1} : s \in S\}$ by $\mathcal{S}^{-1}$, so that $\mathcal{S}^{-1} = \sum_{s \in S} s^{-1}$. A simple relation between the difference sets and the group ring $\mathbb{Z}G$ can be formulated in the following lemma.

Lemma 2.1 *Let G be a group of order v. If a k-element subset S of G is a (v, k, λ)-difference set, then the following equation holds in the group ring $\mathbb{Z}G$:*

$$\mathcal{S}\mathcal{S}^{-1} = (k-\lambda)e_{\mathcal{G}} + \lambda\mathcal{G}$$

where $e_{\mathcal{G}}$ denotes the simple quantity corresponding to the identity element (e_G) of G.

When G is an abelian group, character theory can be used to simplify calculations. A character χ of a finite abelian group G is a homomorphism from G to the multiplicative group of the nonzero complex numbers. The character χ of G such that $\chi(g) = 1$ for every $g \in G$, is called the principal character of G.

Lemma 2.2 *A k-element subset S of an abelian group G of order v is a (v, k, λ)-difference set if and only if $|\chi(S)| = \sqrt{k-\lambda}$ for every nonprincipal character χ of G.*

For a more detailed description of the relationship between difference sets and character theory and group rings see [1]. Similar results can also be obtained in $1\frac{1}{2}$-difference sets by using character theory and group rings. Next we provide a brief introduction to $1\frac{1}{2}$-difference sets. These results are also available in [15].

For any $g \in G$ and $S \subseteq G$, we define the *translate* of S by $Sg = \{sg : s \in S\}$, and define the *development* of S by $\text{Dev}(S) = \{Sg : g \in G\}$. Development of a $1\frac{1}{2}$-difference set is a symmetric $1\frac{1}{2}$-design [15]. Let N be the $v \times b$ point-block incidence matrix and J be the $v \times b$ all-ones matrix. Then, the following equation holds for a $1\frac{1}{2}$-design with parameters $(v, b, k, r; \alpha, \beta)$:

$$NN^tN = nN + \alpha J \tag{1}$$

where $n = k + r - 1 + \beta - \alpha$.

Lemma 2.3 [15, Lemma 2.8] *Let G be a group of order v. Let S be a subset of G of size k. Then, S is a $1\frac{1}{2}$-difference set with parameters $(v, k; \alpha, \beta)$ in G if and only if*

$$\mathcal{S}\mathcal{S}^{-1}\mathcal{S} = n\mathcal{S} + \alpha\mathcal{G} \tag{2}$$

where $n = 2k - 1 + \beta - \alpha$ in the group ring $\mathbb{Z}G$.

For the rest of the paper the parameter n will denote the number $2k-1+\beta-\alpha$ for a given $1\frac{1}{2}$-difference set with parameters $(v, k; \alpha, \beta)$. As a corollary of the above lemma, we can observe that any difference set is a $1\frac{1}{2}$-difference set with parameters $(v, k; \lambda k, \lambda k - k - \lambda + 1)$. A characterization of $1\frac{1}{2}$-difference sets is provided in the next theorem.

Theorem 2.4 [15, Theorem 2.12] *Let G be an abelian group of order v. Let S be a subset of G of size k. Then, S is a $1\frac{1}{2}$-difference set in G with parameters $(v, k; \alpha, \beta)$ if and only if $|\chi(S)| = \sqrt{n}$ or $\chi(S) = 0$ for every nonprincipal character χ of G and $k^3 = nk + \alpha v$.*

The group character values provide us with tools to investigate parameter restrictions of $1\frac{1}{2}$-difference sets. The following lemma provides an important parameter restriction.

Lemma 2.5 [15, Lemma 3.1] *If S is a $1\frac{1}{2}$-difference set in an abelian group G of order v with parameters $(v, k; \alpha, \beta)$, then $\dfrac{vk-k^2}{n}$ is an integer.*

Note that here the concurrence matrix NN^t of a symmetric $1\frac{1}{2}$-design has three eigenvalues, namely k^2, n and 0. The multiplicity of the eigenvalue n is $\dfrac{vk-k^2}{n}$. Hence $\dfrac{vk-k^2}{n}$ is an integer for a given symmetric $1\frac{1}{2}$-design.

3 A family of $1\frac{1}{2}$-difference sets

3.1 Construction I

Let q be a prime power and let s be a positive integer. Let V_{s+1} be the $(s+1)$-dimensional vector space over $GF(q)$. Then, there are $r = \dfrac{q^{s+1}-1}{q-1}$ subspaces of dimension s. We will call these subspaces, hyperplanes of V_{s+1}. Let $H_1, \ldots, H_r$ be the hyperplanes of V_{s+1}. Let E_{s+1} be the additive group of V_{s+1}. When the dimension of the vector space is clear from the context, we will simply use the notation E instead of E_{s+1}. We have the following equations in the group ring $\mathbb{Z}E$:

$$\mathcal{H}_1 + \cdots + \mathcal{H}_r = q^s e_{\mathcal{E}} + \frac{q^s-1}{q-1}\mathcal{E},$$
$$\mathcal{H}_i\mathcal{H}_i = q^s\mathcal{H}_i$$

and

$$\mathcal{H}_i\mathcal{H}_j = q^{s-1}\mathcal{E}.$$

The above equations hold since each element of H_i is exactly replicated q^s times in

$$H_i + H_i = \{x + y : x, y \in H_i\}$$

and each element of E is exactly replicated q^{s-1} times in

$$H_i + H_j = \{x + y : x \in H_i, y \in H_j\}$$

when $H_i \neq H_j$. McFarland provided a family of non-cyclic difference sets by using these cosets [13]. With a similar approach, we have the following two lemmas to construct $1\frac{1}{2}$-difference sets in non-cyclic groups.

Lemma 3.1 *Let $H_1, \ldots, H_l$ be l distinct hyperplanes of V_{s+1} and K be a group of order l such that $r \geq l \geq 2$. Then, $S = \cup_{i=1}^{l}(H_i, k_i)$ is a $1\frac{1}{2}$-difference set in $G = E \times K$ with parameters $n = q^{2s}$ and $\alpha = (l^2-1)q^{2s-1}$.*

Proof We will naturally denote the group G by $\mathcal{E}\mathcal{K}$ and the set S by $\mathcal{S} = \sum_{i=1}^{l}\mathcal{H}_i k_i$ in the group ring $\mathbb{Z}G$. Then, note that $\mathcal{S}^{-1} = \sum_{i=1}^{l}\mathcal{H}_i^{-1}k_i^{-1} = \sum_{i=1}^{l}\mathcal{H}_i k_i^{-1}$ since H_i's are subgroups of E. We check the Eq. 2. in order to show S is a $1\frac{1}{2}$-difference set in G.

$$\begin{aligned}
\mathcal{S}\mathcal{S}^{-1}\mathcal{S} &= \left(\sum_{i=1}^{l}\mathcal{H}_i k_i\right)\left(\sum_{j=1}^{l}\mathcal{H}_j k_j^{-1}\right)\left(\sum_{t=1}^{l}\mathcal{H}_t k_t\right)\\
&= \left(\sum_{i=1}^{l}\mathcal{H}_i^2 e_{\mathcal{K}} + \sum_{i\neq j}\mathcal{H}_i\mathcal{H}_j k_i k_j^{-1}\right)\left(\sum_{t=1}^{l}\mathcal{H}_t k_t\right)\\
&= \left(q^s\sum_{i=1}^{l}\mathcal{H}_i e_{\mathcal{K}} + lq^{s-1}\left(\mathcal{E}\mathcal{K} - \mathcal{E}e_{\mathcal{K}}\right)\right)\left(\sum_{t=1}^{l}\mathcal{H}_t k_t\right)\\
&= q^{2s}\sum_{i=1}^{l}\mathcal{H}_i k_i + q^s\sum_{i\neq t}\mathcal{H}_i\mathcal{H}_t k_t + l^2q^{2s-1}\mathcal{E}\mathcal{K} - lq^{2s-1}\sum_{t=1}^{l}\mathcal{E}k_t
\end{aligned}$$

$$= q^{2s}\sum_{i=1}^{l}\mathcal{H}_i k_i + \left((l-1)q^{2s-1} + l^2q^{2s-1} - lq^{2s-1}\right)\mathcal{E}\mathcal{K}$$

$$= q^{2s}\sum_{i=1}^{l}\mathcal{H}_i k_i + (l^2-1)q^{2s-1}\mathcal{E}\mathcal{K}.$$

Hence, S is a $1\frac{1}{2}$-difference set with parameters $v = lq^{s+1}, k = lq^s, n = q^{2s}$ and $\alpha = (l^2-1)q^{2s-1}$. □

Lemma 3.2 *Let $H_1, \ldots, H_{r-1}$ be $r-1$ distinct hyperplanes of V_{s+1} and K be a group of order $r = \dfrac{q^{s+1}-1}{q-1}$. Then, $S = \cup_{i=1}^{r-1}(H_i, k_i)$ is a $1\frac{1}{2}$-difference set in $G = E \times K$ with parameters $n = q^{2s}$ and $\alpha = q^{2s-1}(r-2)(r-1)$.*

Proof

$$\mathcal{S}\mathcal{S}^{-1}\mathcal{S} = \left(\sum_{i=1}^{r-1}\mathcal{H}_i k_i\right)\left(\sum_{j=1}^{r-1}\mathcal{H}_j k_j^{-1}\right)\mathcal{S}$$

$$= \left(\sum_{i=1}^{r-1}\mathcal{H}_i^2 e_{\mathcal{K}} + \sum_{i\neq j}\mathcal{H}_i\mathcal{H}_j k_i k_j^{-1}\right)\mathcal{S}$$

$$= \left(q^{2s}e_{\mathcal{E}}e_{\mathcal{K}} + \left(q^s\frac{q^s-1}{q-1} - q^{s-1}(r-2)\right)\mathcal{E}e_{\mathcal{K}} + q^{s-1}(r-2)\mathcal{E}\mathcal{K} - q^s\mathcal{H}_r e_{\mathcal{K}}\right)\mathcal{S}$$

$$= q^{2s}\sum_{i=1}^{r-1}\mathcal{H}_i k_i + q^{2s}\frac{q^s-1}{q-1}\mathcal{E}\sum_{i=1}^{r-1}k_i + q^{2s-1}(r-2)(r-1)\mathcal{E}\mathcal{K}$$

$$-q^{2s-1}(r-2)\mathcal{E}\sum_{i=1}^{r-1}k_i - q^{2s-1}\mathcal{E}\sum_{i=1}^{r-1}k_i$$

$$= q^{2s}\sum_{i=1}^{r-1}\mathcal{H}_i k_i + q^{2s-1}(r-2)(r-1)\mathcal{E}\mathcal{K}.$$

Hence, S is a $1\frac{1}{2}$-difference set with parameters $v = rq^{s+1}, k = (r-1)q^s, n = q^{2s}$ and $\alpha = q^{2s-1}(r-2)(r-1)$. □

3.2 Construction II

Consider the case $s+1 = 2m$ for an integer m. In this construction, we focus on m-dimensional disjoint subspaces to provide more constructions of $1\frac{1}{2}$-difference sets. There are at most $r = q^m + 1$ such subspaces. Let $U_1, \ldots, U_r$ be the m-dimensional disjoint subspaces of V_{2m}. Let E be the additive group of V_{2m}. Then, we have the following equations in the group ring $\mathbb{Z}E$:

$$\mathcal{U}_1 + \cdots + \mathcal{U}_r = q^m e_{\mathcal{E}} + \mathcal{E},$$
$$\mathcal{U}_i\mathcal{U}_i = q^m\mathcal{U}_i$$

and

$$\mathcal{U}_i\mathcal{U}_j = \mathcal{E}.$$

We can prove the following two lemmas similarly by checking the group ring equation for $1\frac{1}{2}$-difference sets.

Lemma 3.3 *Let $U_1, \ldots, U_l$ be l distinct m-dimensional disjoint subspaces of V_{2m} and K be a group of order l such that $r \geq l \geq 2$. Then, $S = \cup_{i=1}^{l}(H_i, k_i)$ is a $1\frac{1}{2}$-difference set in $G = E \times K$ with parameters $n = q^{2m}$ and $\alpha = (l^2 - 1)q^m$.*

Lemma 3.4 *Let $U_1, \ldots, U_{r-1}$ be $r - 1$ distinct m-dimensional disjoint subspaces of V_{2m} and K be a group of order r. Then, $S = \cup_{i=1}^{m-1}(H_i, k_i)$ is a $1\frac{1}{2}$-difference set in $G = E \times K$ with parameters $n = q^{2m}$ and $\alpha = q^m(r - 2)(r - 1)$.*

4 Plateaued functions from $1\frac{1}{2}$-difference sets

In this section, we investigate the special case $q = 2$. Let V_{s+1} be the $(s + 1)$-dimensional vector space over $\mathbb{F}$ and E_{s+1} be the additive group of V_{s+1}. Let f be a function from V_{s+1} to $\mathbb{F}$ and F be the function $(-1)^f$ from V_{s+1} to the set $\{-1, 1\}$. We are interested in the set $Spec = \{\widehat{F}(x) : x \in V_{s+1}\}$ of distinct values which we will call the Fourier spectrum of F. f is called a plateaued function if the Fourier spectrum of $F = (-1)^f$ is $\{0, \pm 2^t\}$ for some integer $t \geq \frac{s+1}{2}$. There are two well-studied subsets of plateaued functions namely bent functions ($t = \frac{s+1}{2}$ and s is odd) and semibent functions ($t = \lceil \frac{s+2}{2} \rceil$). We define $supp(F) = \{x : \widehat{F}(x) \neq 0\}$ of vectors whose Fourier spectrum is nonzero and the weight of f as $wt(f) = |\{x : f(x) \neq 0\}|$. We define the convolution of two functions as:

$$(F_1 * F_2)(a) = \sum_{x \in V_{s+1}} F_1(x + a)F_2(x) \tag{3}$$

for all $a \in V_{s+1}$. The convolution theorem of Fourier analysis states that the Fourier transform of convolution of two functions is the ordinary product of their Fourier transforms:

$$\widehat{F_1 * F_2} = \widehat{F_1} \cdot \widehat{F_2}. \tag{4}$$

Proposition 4.1 *Let f be a plateaued function from V_{s+1} to $\mathbb{F}$ with Fourier spectrum $\{0, \pm 2^t\}$ for some t. Then, $wt(f)$ is even.*

Proof Since $\widehat{F}(0) = 2^{s+1} - 2wt(f)$ and $\widehat{F}(0) \in \{0, \pm 2^t\}$ for some t, $wt(f) = 2^s \pm 2^{t-1}$ or $wt(f) = 2^s$. □

Lemma 4.2 *Let f be a function from V_{s+1} to $\mathbb{F}$ such that $s \geq 2$. Define $F = (-1)^f$ and a matrix $M_f = (m_{x,y})$ where $m_{x,y} = F(x + y)$ for all $x, y \in V_{s+1}$. Then, f is a plateaued function with Fourier spectrum $\{0, \pm 2^t\}$ if and only if*

$$M_f^3 = 2^{2t} M_f \tag{5}$$

for some integer t.

Proof Suppose f is a plateaued function with $Spec = \{0, \pm 2^t\}$ for some integer t. Then,

$$\begin{aligned}
(M_f^3)_{x,y} &= \sum_{a\in V_{s+1}} \left(\sum_{b\in V} m_{x,b} m_{b,a}\right) m_{a,y} \\
&= \sum_{a\in V_{s+1}} \left(\sum_{b\in V_{s+1}} F(x+b)F(b+a)\right) F(a+y) \\
&= \sum_{a\in V_{s+1}} \left(\sum_{w\in V_{s+1}} F(w)F(w+x+a)\right) F(a+y) \\
&= \sum_{a\in V_{s+1}} (F*F)(x+a)F(a+y) \\
&= \sum_{u\in V_{s+1}} (F*F)(u)F(u+x+y) \\
&= ((F*F)*F)(x+y).
\end{aligned}$$

Let $A = (F*F)*F$. Then, the Fourier transform of A is $\widehat{A} = \widehat{F}\cdot\widehat{F}\cdot\widehat{F}$ by Eq. 4. Now by Fourier inversion

$$\begin{aligned}
A(x+y) &= \frac{1}{2^{s+1}} \sum_{\beta\in V_{s+1}} \widehat{F}(\beta)\widehat{F}(\beta)\widehat{F}(\beta)(-1)^{(x+y)\cdot\beta} \\
&= \frac{2^{2t}}{2^{s+1}} \sum_{\beta\in supp(F)} \widehat{F}(\beta)(-1)^{(x+y)\cdot\beta} \\
&= 2^{2t}F(x+y).
\end{aligned}$$

Hence the equation $M_f^3 = 2^{2t}M_f$ holds. The above calculations hold since

$$F(x+y) = \frac{1}{2^{s+1}} \sum_{\beta\in supp(F)} \widehat{F}(\beta)(-1)^{(x+y)\cdot\beta}$$

and $\left(\widehat{F}(\beta)\right)^2$ is either 0 or 2^{2t} for any $\beta \in V_{s+1}$.

Suppose $M_f^3 = 2^{2t}M_f$. This implies $((F*F)*F)(x) = 2^{2t}F(x)$ for all $x \in V_{s+1}$. Apply the Fourier transform on both of the sides. Then,

$$(\widehat{F}(x))^3 - 2^{2t}\widehat{F}(x) = \widehat{F}(x)((\widehat{F}(x))^2 - 2^{2t}) = 0$$

for all x in V_{s+1}. Hence, the Fourier spectrum can only take values of 0 and $\pm 2^t$. □

Lemma 4.3 *Let $s \geq 2$ and f be a plateaued function from V_{s+1} to $\mathbb{F}$ with Fourier spectrum $\{0, \pm 2^t\}$ for some integer t. Then, there exists a symmetric $1\frac{1}{2}$-design associated with f.*

Proof Define a matrix $M_f = (m_{x,y})$ where $m_{x,y} = F(x+y)$ for all $x, y \in V_{s+1}$. Since f is a plateaued function, $M_f^3 = 2^{2t}M_f$ for some t. Note that M_f is a symmetric $\{\pm 1\}$-matrix. Let $wt(f) = 2^{s+1} - k$ where $k \in \{2^s \pm 2^{t-1}, 2^s\}$. Then, the row and column sum of the matrix M_f is $2k - v$ where $v = 2^{s+1}$. Now consider the matrix $N = \frac{1}{2}(J + M_f)$ where J denote all-ones matrix. N is a symmetric $\{0, 1\}$-matrix whose row sum and column sum is k. We show that the matrix N can be recognized as an incidence matrix of a symmetric $1\frac{1}{2}$-design i.e. $v = b$. For this, we need to verify Eq. 1.

$$
\begin{aligned}
NN^tN &= \left(\frac{1}{2}(J + M_f)\right)\left(\frac{1}{2}(J + M_f)\right)\left(\frac{1}{2}(J + M_f)\right) \\
&= \frac{1}{4}\left(vJ + (2k - v)J + (2k - v)J + M_f^2\right)\left(\frac{1}{2}(J + M_f)\right) \\
&= \frac{1}{8}(4k - v)vJ + (4k - v)(2k - v)J + (2k - v)^2 J + M_f^3 \\
&= \frac{2^{2t}}{8}(J + M_f) + \left(\frac{(4k - v)v + (4k - v)(2k - v) + (2k - v)^2 - 2^{2t}}{8}\right) J \\
&= \frac{2^{2t}}{8}(J + M_f) + \left(\frac{12k^2 - 6kv + v^2 - 2^{2t}}{8}\right) J \\
&= 2^{2t-2}N + \alpha J.
\end{aligned}
$$

Since k is even and $2t \geq s + 1 \geq 3, \alpha = \dfrac{12k^2 - 6kv + v^2 - 2^{2t}}{8}$ is an integer. Therefore, N defines a symmetric $1\frac{1}{2}$-design with parameters $n = 2^{2t-2}$ and α. □

Lemma 4.4 *Let N be an incidence matrix of a symmetric $1\frac{1}{2}$-design obtained from a plateaued function f from V_{s+1} to $\mathbb{F}$. Then, $1\frac{1}{2}$-design associated with N has E_{s+1} as a transitive automorphism group.*

Proof For any x in V_{s+1}, define

$$\phi_x : V_{s+1} \longrightarrow V_{s+1}$$

as follows: $\phi_x(y) = x + y$ for all $y \in V_{s+1}$. Let $E = \{\phi_x : x \in V_{s+1}\}$. We have

$$m_{\phi_x(a),\phi_x(b)} = F(x + a + x + b) = F(a + b) = m_{a,b}$$

for all $a, b \in V_{s+1}$. A block in the $1\frac{1}{2}$-design is given by

$$B_y = \{a : F(a + y) = 1,\ a \in V_{s+1}\}.$$

Then, $\{\phi_x(a) : a \in B_y\} = B_{\phi_x(y)}$. Hence,

$$\{\{\phi_x(a) : a \in B_y\} : y \in V_{s+1}\}$$

is the whole block set of the $1\frac{1}{2}$-design. Therefore, E_{s+1} is an automorphism group of the design. It is clear that E_{s+1} acts transitively on points and blocks of the $1\frac{1}{2}$-design. □

Next we provide a combinatorial classification of plateaued functions in terms of $1\frac{1}{2}$-difference sets.

Theorem 4.5 *The existence of a $1\frac{1}{2}$-difference set in E_{s+1} with parameters $(v = 2^{s+1}, k; \alpha, \beta)$ satisfying $n = 2^{2t-2}$ for some integer t and $k \in \{2^s, 2^s \pm 2^{t-1}\}$ equivalent to the existence of a plateaued function f from V_{s+1} to $\mathbb{F}$ with Fourier spectrum $\{0, \pm 2^t\}$.*

Proof Assume there exist a $1\frac{1}{2}$-difference set S in E_{s+1} with parameters $(v = 2^{s+1}, k; \alpha, \beta)$ such that $n = 2^{2t-2}$ for some integer t and $k \in \{2^s, 2^s \pm 2^{t-1}\}$. Then, the parameters satisfy the equation $12k^2 - 6kv + v^2 - 2^{2t} = 8\alpha$ since $\alpha = \dfrac{k(k^2-n)}{v}$. The matrix $M = 2N - J = m_{x,y}$ satisfies $m_{x+z,y+z} = m_{x,y}$ for all $x, y, z \in V_{s+1}$. We define a function f from V_{s+1} to $\mathbb{F}$ as follows: $f(x) = 1$ if and only if $x \in S$. Therefore, $m_{x,y} = (-1)^{f(x+y)}$. Note that under our assumptions Eq. 5 holds. This implies f is a plateaued function.

Assume f is a plateaued function. Then, by Lemmas 2.3 and 2.4, there exists a symmetric $1\frac{1}{2}$-design such that E_{s+1} acts transitively on its blocks and points. Hence, we can choose a base block S which is a k-subset of E_{s+1} where all the other blocks are translates of S. It is clear that S is a $1\frac{1}{2}$-difference set in E_{s+1}. □

Remark 4.6 Let $s = 4l + 3$ be an odd integer and C_m denote the class of elements of V_s having exactly m ones as components. Let S denote the set union of classes C_m with $m \equiv 0, 1 \pmod 4$. Then, $\mathcal{S} = \mathcal{C}_0 + \mathcal{C}_1 + \cdots \mathcal{C}_{4i} + \mathcal{C}_{4i+1} + \cdots + \mathcal{C}_{4l} + \mathcal{C}_{4l+1}$ and $\mathcal{S} = \mathcal{S}^{-1}$. One can check that $\chi(\mathcal{S}^2)$ is either 0 or 2^{s-1} for any nonprincipal character of E_s [15, Lemma 3.10]. By Lemma 2.4, this implies that S is $1\frac{1}{2}$-difference set in E_s. Now by Theorem 4.5, the function f defined by

$$f(x) = \begin{cases} 1, & \text{if } x \in S \\ 0, & \text{otherwise} \end{cases}$$

is a plateaued function with a Fourier spectrum $\{0, \pm 2^{\frac{s+1}{2}}\}$. Here also note that $|S| = 2^{s-1}$. Another example of a balanced plateaued function can be obtained by using the result of Lemma 3.1 with the group $K = E_1$ and $l = 2$. For instance, choose $H_1 = \{(0, 0), (0, 1)\}$ and $H_2 = \{(0, 0), (1, 0)\}$. Then, the set $S = \{(0, 0, 0), (0, 1, 0), (0, 0, 1), (1, 0, 1)\}$ is a $1\frac{1}{2}$-difference set in E_3. Let N denote the corresponding incidence matrix of this design. Then, we can obtain the following matrix by using the Dev(S):

$$N = \begin{pmatrix} 1&0&1&0&1&1&0&0 \\ 0&1&0&1&1&1&0&0 \\ 1&0&1&0&0&0&1&1 \\ 0&1&0&1&0&0&1&1 \\ 1&1&0&0&1&0&1&0 \\ 1&1&0&0&0&1&0&1 \\ 0&0&1&1&1&0&1&0 \\ 0&0&1&1&0&1&0&1 \end{pmatrix}.$$

Here N satisfies the equation $NN^tN = 4N + 6J$. Hence any row of this matrix will define a plateaued function with the Fourier spectrum $\{0, \pm 4\}$.

In the rest of the section, let s be an even number and f be a plateaued function from V_{s+1} to $\mathbb{F}$ with the Fourier spectrum $\{0, \pm 2^{\frac{s+2}{2}}\}$. f is also known under the names semibent and 3-valued almost optimal Boolean function. We specifically consider this case due to its close connection to Hadamard difference sets.

Lemma 4.7 *Let V_s be a $s \geq 2$ dimensional subspace of V_{s+1}. Let E_s and E_{s+1} be the additive groups of V_s and V_{s+1}, respectively. If there exists a set $D \subset E_s$, such that $S = (D, 0) \bigcup (E_s \setminus D, 1)$ is a $1\frac{1}{2}$-difference set in E_{s+1} with $n = 2^s$, then D is a Hadamard difference set in E_s.*

Proof In the group ring, the following holds

$$\mathcal{S}\mathcal{S}^{-1} = \mathcal{S}^2 = (\mathcal{D}^2, 0) + 2(\mathcal{D}\mathcal{E}_s - \mathcal{D}^2, 1) + (\mathcal{E}_s^2 - 2\mathcal{D}\mathcal{E}_s + \mathcal{D}^2, 0).$$

Then, by Lemma 2.5 we have exactly 2^s characters of E_{s+1} which takes nonzero values on $\mathcal{S}^2$. Let χ_i^j be a character of $E_{s+1} = E_s \times E_1$. Then, $\chi_i^j(x, y) = \theta_i(x)\zeta_j(y)$. Let θ_0 and ζ_0 be principal characters of E_s and E_1; respectively. Thus, $\chi_i^0(\mathcal{S}^2) = \theta_i(\mathcal{D}^2) - 2\theta_i(\mathcal{D}^2) + \theta_i(\mathcal{D}^2) = 0$ for $i \neq 0$. Hence $\chi_i^1(\mathcal{S}^2) = 2^s$ for all $i \neq 0$. If $i \neq 0$, then

$$\chi_i^1(\mathcal{S}^2) = 4\theta_i(\mathcal{D}^2) = 2^s.$$

If $i = 0$, then,

$$\chi_0^1(\mathcal{S}^2) = (2|D| - 2^s)^2 = 2^s.$$

Therefore, D is a Hadamard difference set. □

Converse of the above lemma can be verified by using group rings too.

Lemma 4.8 *Let V_s be a s-dimensional subspace of V_{s+1}. Let E_s and E_{s+1} be the additive groups of V_s and V_{s+1}, respectively. If there exists a Hadamard difference set $D \subset E_s$, then $S = (D, 0) \bigcup (E_s \setminus D, 1)$ is a $1\frac{1}{2}$-difference set in E_{s+1} with $n = 2^s$.*

Remark 4.9 We denote by W_z the set $W_z = \{y : z \cdot y = 0\}$. Note that $W_x = V_s \times \{0\}$ for $x = (0, 0, \ldots, 1) \in V_{s+1}$. Suppose there exist a $1\frac{1}{2}$-difference set S in E_{s+1} with $n = 2^s$ such that S can be written as a union of $(D, 0)$ and $(E_s \setminus D, 1)$. We can define a function f as follows:

$$f(x) = \begin{cases} 1, & \text{if } x \in S \\ 0, & \text{otherwise} \end{cases}.$$

Then, the restriction of f to the sets W_x and $V_{s+1} \setminus W_x$ are both bent functions. Note that the function f is a semibent function since $n = 2^s$ implies f has the Fourier spectrum $\{0, \pm 2^{\frac{s+2}{2}}\}$. Hence, our approach provides a family of semibent functions whose restriction to a hyperplane is a bent function. Whether a plateaued function could be bent when restricted to a hyperplane is of interest. To answer this problem, a criterion, which is based on the characteristic function of support of $\widehat{F}$, for semibent functions is provided in the work of Dillon and McGuire [11, Theorem 1]. Another characterization of plateaued functions, which is based on the derivative, is provided in [4, Theorem V.2]. A part of this result states that the restriction of a semibent function f to W_z is a bent function if and only if $\sum_{x \in V_{s+1}} (-1)^{f(x)+f(x+a)} = 0$ for all nonzero $a \in W_z$. In our approach, we provide a characterization in terms of difference sets.

Lemma 4.10 *Let X and Y be two subsets of E_{s+1}. Suppose*

$$\left(|X| = 2^s + 2^{\frac{s}{2}} \text{ or } |X| = 2^s - 2^{\frac{s}{2}}\right)$$

and $|Y| = 2^s$ holds. Then, $S = (X, 0) \bigcup (Y, 1)$ is a Hadamard difference set in $E_{s+2} = E_{s+1} \times E_1$ if and only if X and Y are $1\frac{1}{2}$-difference sets in E_{s+1} with $n = 2^s$ and any nonprincipal character χ of E_{s+1} satisfies:

$$\chi(\mathcal{X}^2) = 0 \text{ when } \chi(\mathcal{Y}^2) = n \tag{6}$$

and

$$\chi(\mathcal{X}^2) = n \text{ when } \chi(\mathcal{Y}^2) = 0. \tag{7}$$

Proof Observe that

$$\mathcal{S}^2 = (\mathcal{X}^2, 0) + 2(\mathcal{X}\mathcal{Y}, 1) + (\mathcal{Y}^2, 0).$$

Let χ_i^j be a character of $E_{s+2} = E_{s+1} \times E_1$. Then, $\chi_i^j(x, y) = \theta_i(x)\zeta_j(y)$ where θ_i and ζ_j are characters of E_{s+1} and $E_!$; respectively. Let θ_0 and ζ_0 be principal characters of E_s and E_1; respectively. First, assume that any nonprincipal character χ of E_{s+1} satisfies Eqs. 6 and 7. Then, for any nonprincipal character χ_i^j of E_{s+2} the following holds:

$$\chi_i^j(\mathcal{S}^2) = n = 2^s.$$

Therefore, $S = (X, 0) \bigcup (Y, 1)$ is a Hadamard difference set in E_{s+2}.

Now assume that $S = (X, 0) \bigcup (Y, 1)$ is a Hadamard difference set in E_{s+2}. This implies,

$$\theta_i(\mathcal{X}^2) - 2\theta_i(\mathcal{X})\theta_i(\mathcal{Y}) + \theta_i(\mathcal{Y}^2) = 2^s$$

and

$$\theta_i(\mathcal{X}^2) + 2\theta_i(\mathcal{X})\theta_i(\mathcal{Y}) + \theta_i(\mathcal{Y}^2) = 2^s$$

for any $i \neq 0$. Hence,

$$\theta_i(\mathcal{X}^2) + \theta_i(\mathcal{Y}^2) = (\theta_i(\mathcal{X}))^2 + (\theta_i(\mathcal{Y}))^2 = 2^s.$$

It is well-known that when s is even, the sum of the squares of two integers equals 2^s implies one of these squares is null and the other one equals 2^s. Thus, $\theta_i(\mathcal{X}^2)$ is either 0 or 2^s. For the sake of contradiction assume for all $i \neq 0$, $\theta_i(\mathcal{X}^2) = 0$. This implies $\mathcal{X} = m\mathcal{E}_{s+1}$ for some integer m which is a contradiction. Therefore, any nonprincipal character χ of E_{s+1} satisfies Eqs. 6. and 7. Moreover, X and Y are $1\frac{1}{2}$-difference sets in E_{s+1} with $n = 2^s$. □

Remark 4.11 The previous lemma provides a method to construct a bent function when two plateaued functions with certain properties are given. Note that we can interchange the sizes of the sets X and Y for our purposes. For example, consider the subsets

$$X = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (1, 0, 0)\}$$

and $Y = \{(0, 0, 0), (1, 1, 1)\}$ of E_3. Then, for a nonprincipal character χ of E_3 the equalities

$$\chi(\mathcal{X}^2) = 0 \text{ when } \chi(\mathcal{Y}^2) = 4$$

and

$$\chi(\mathcal{X}^2) = 4 \text{ when } \chi(\mathcal{Y}^2) = 0$$

are satisfied. Thus $S = \{(0, 0, 0, 0), (0, 0, 1, 0), (0, 1, 0, 0), (1, 0, 0, 0), (0, 0, 0, 1), (1, 1, 1, 1)\}$ is a Hadamard difference set in E_4. The existence of a bent function f of $s+2 \geq 4$ variables is equivalent to the existence of plateaued functions h_1 and h_2, which are restrictions of f to a linear hyperplane and its complement, respectively, with Fourier spectrum $\{0, \pm 2^{\frac{s+2}{2}}\}$ and the disjoint union of supports h_1 and h_2 equals to E_{s+1}. This result provides a simple way to generate plateaued functions from a bent function and can be found in [6, Theorem 11]. A more detailed study of restriction of a bent function to a subspace of codimension 1 or 2 can be found in [3].

We have the following corollary of Lemma 4.10.

Corollary 1 *Let f and g be two semibent functions from V_{s+1} to $\mathbb{F}$ with*

$$\left(wt(f) = 2^s + 2^{\frac{s}{2}} \text{ or } wt(f) = 2^s - 2^{\frac{s}{2}}\right)$$

and $wt(g) = 2^s$. Let $X = \{x : f(x) = 1\}$ and $Y = \{x : g(x) = 1\}$. Define a function h from V_{s+2} to $\mathbb{F}$ as follows:

$$h(x, y) = \begin{cases} 1, & \text{if } x \in X \text{ and } y = 0 \\ 1, & \text{if } x \in Y; \text{ and } y = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Then, h is a bent function if and only if any nonprincipal character χ of E_{s+1} satisfies:

$$\chi(\mathcal{X}^2) = 0 \text{ when } \chi(\mathcal{Y}^2) = 2^s$$

and

$$\chi(\mathcal{X}^2) = 2^s \text{ when } \chi(\mathcal{Y}^2) = 0.$$

Acknowledgments I would like to thank the anonymous referees for their insightful comments on improving the quality of the paper. This work was supported in part by NSF Grant CCF-1018148.

References

1. Beth T., Jungnickel D., Lenz H.: Design Theory I, vol. 69. Cambridge University Press, Cambridge (1999).
2. Bose R.C., Shrikhande S.S., Singhi N.M.: Edge regular multigraphs and partial geometric designs with an application to the embedding of quasi-residual designs. Colloq. Int. sulle Teorie Comb. **1**, 49–81 (1976).
3. Canteaut A., Charpin P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2003).
4. Canteaut A., Carlet C., Charpin P., Fontaine C.: On cryptographic properties of the cosets of r (1, m). IEEE Trans. Inf. Theory **47**(4), 1494–1513 (2001).
5. Carlet C.: Partially-bent functions. Des. Codes Cryptogr. **3**(2), 135–145 (1993).
6. Carlet C.: Boolean functions for cryptography and error correcting codes. Boolean Models Methods Math. Comput. Sci. Eng. **2**, 257 (2010).
7. Carlet C., Prouff E.: On plateaued functions and their constructions. In: Johansson T. (ed.) Fast Software Encryption, pp 54–73. Springer, Berlin (2003).
8. Chee S., Lee S., Kim K.: Semi-bent functions. In: Pieprzyk J., Safavi-Naini R. (eds.) Advances in Cryptology-ASIACRYPT'94, pp. 105–118. Springer, Berlin (1995).
9. Chung F.R.K., Salehi J.A., Wei V.K.: Optical orthogonal codes: design, analysis and applications. IEEE Trans. Inf. Theory **35**(3), 595–604 (1989).
10. Dillon J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland, College Park, MD (1974).
11. Dillon J.F., McGuire G.: Near bent functions on a hyperplane. Finite Fields Appl. **14**(3), 715–720 (2008).
12. Jungnickel D., Pott A.: Perfect and almost perfect sequences. Discret. Appl. Math. **95**(1–3), 331–360 (1999).
13. McFarland R.L.: A family of difference sets in non-cyclic groups. J. Comb. Theory A **15**(1), 1–10 (1973).
14. Neumaier A.: $t\frac{1}{2}$-designs. J. Comb. Theory A **28**(3), 226–248 (1980).
15. Olmez O.: Symmetric $1\frac{1}{2}$-designs and $1\frac{1}{2}$-difference sets. Comb. Des. Theory (2013). doi:10.1002/jcd.21354.
16. Vasic B., Milenkovic O.: Combinatorial constructions of low-density parity-check codes for iterative decoding. IEEE Trans. Inf. Theory **50**(6), 1156–1176 (2004).
17. Zheng Y., Zhang X.: Plateaued functions. In: Varadharajan V., Mu Y. (eds.) Information and Communication Security, pp. 284–300. Springer, Berlin (1999).