# Shifted plateaued functions

Nurdagül Anbar[1], Canan Kaşıkcı[2], Wilfried Meidl[3], Alev Topuzoğlu[2]

[1]*Johannes Kepler University,*
*Altenbergerstrasse 69, 4040-Linz, Austria*
*Email:* nurdagulanbar2@gmail.com
[2]*Sabancı University,*
*MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey*
*Email:* canank@sabanciuniv.edu
*Email:* alev@sabanciuniv.edu
[3]*Johann Radon Institute for Computational and Applied Mathematics,*
*Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria*
*Email:* meidlwilfried@gmail.com

**Abstract**

We study generalizations of plateaued functions, partially bent functions and their relations. We extend a well-known property of bent and semibent functions, in relation to their shifts, to all plateaued functions. Focusing on the subclass of partially bent$_4$ functions, we obtain a characterization and present results on their differential properties and corresponding relative difference sets. This unifies previous work on partially bent functions.

**Keywords** Plateaued functions; bent$_4$ functions; partially bent functions; relative difference sets.

**Mathematics Subject Classification (2010)** 06E30, 05B10

# 1 Introduction

We first consider Boolean functions $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$. For an element $c \in \mathbb{F}_{2^n}$, the unitary transformation $\mathcal{V}_f^c : \mathbb{F}_{2^n} \mapsto \mathbb{C}$ is defined in [2] as

$$\mathcal{V}_f^c(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\sigma^c(x)} i^{\mathrm{Tr_n}(cx)} (-1)^{\mathrm{Tr_n}(ux)} \ , \tag{1.1}$$

where $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$ and $\sigma^c(x)$ is the Boolean function defined by

$$\sigma^c(x) = \sum_{0 \le i < j \le n-1} (cx)^{2^i} (cx)^{2^j} \ . \tag{1.2}$$

Note that for $c = 0$, $\mathcal{V}_f^c$ reduces to the conventional Walsh-Hadamard transform

$$\mathcal{V}_f^0(u) = \mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr_n}(ux)} \ . \tag{1.3}$$

A Boolean function $f$ is called a *$c$-bent$_4$* function if for some $c \in \mathbb{F}_{2^n}$, the transform $\mathcal{V}_f^c$ satisfies $|\mathcal{V}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$. A function $f$ is bent$_4$ if it is $c$-bent$_4$ for some $c \in \mathbb{F}_{2^n}$. We note that a $c$-bent$_4$ function is a classical bent function when $c = 0$. A 1-bent$_4$ function is called *negabent*. An alternative definition of a $c$-bent$_4$ function can be given in relation to the so-called *modified derivative* of $f$. The authors of [2] define $f$ to be $c$-bent$_4$ if the modified derivative

$$f(x+a) + f(x) + \mathrm{Tr_n}(c^2 ax) \tag{1.4}$$

is balanced for all nonzero $a \in \mathbb{F}_{2^n}$. As expected, this corresponds to the characterization of bent functions via the derivative when $c = 0$.

Previously, $c$-bent$_4$ functions were studied in multivariate form. Consider the unitary transform $\mathcal{U}_f^c : \mathbb{F}_2^n \mapsto \mathbb{C}$, defined as

$$\mathcal{U}_f^c(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+s_2^c(x)} i^{c \cdot x} (-1)^{u \cdot x} \ , \tag{1.5}$$

where $y \cdot z$ denotes the dot product of $y, z \in \mathbb{F}_2^n$, and

$$s_2^c(x_1, \ldots, x_n) = \sum_{1 \le i < j \le n} (c_i x_i)(c_j x_j) \text{ if } c = (c_1, \ldots, c_n). \tag{1.6}$$

A function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is called $c$-bent$_4$ in [7] if $|\mathcal{U}_f^c(u)| = 2^{n/2}$ for some $c \in \mathbb{F}_2^n$, and for all $u \in \mathbb{F}_2^n$. In fact the authors of [7] use the term bent$_4$, not $c$-bent$_4$.

The values $c = (0, \ldots, 0)$ and $c = (1, \ldots, 1) \in \mathbb{F}_2^n$ yield again the (multivariate) bent and negabent functions. An appropriate modification of the derivative to obtain an alternative definition of a multivariate $c$-bent$_4$ function is given in [2] as follows. A function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is $c$-bent$_4$ if and only if the (modified) derivative

$$f(x + a) + f(x) + c \cdot (a \odot x) \tag{1.7}$$

is balanced for every nonzero $a \in \mathbb{F}_2^n$, where $y \odot z := (y_1z_1, \ldots, y_nz_n)$ for $y = (y_1, \ldots, y_n)$, $z = (z_1, \ldots, z_n)$.

Another motivation for introducing $c$-bent$_4$ functions in [2] comes from their relation to *modified planar* functions. We recall that a function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ (or $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$) is modified planar if $F(x + a) + F(x) + ax$ (or $F(x+a)+F(x)+a\odot x$) is a permutation for every nonzero $a \in \mathbb{F}_{2^n}$ (or $a \in \mathbb{F}_2^n$), see [12, 15, 16] and also the excellent survey [10]. It is shown in [2] that bent$_4$ functions describe the components of modified planar functions.

Bent and negabent functions describe the same set of functions in both univariate and multivariate settings. We note that this property does not hold for other values of $c$. Indeed, any affine function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is $c$-bent$_4$ for every nonzero $c \in \mathbb{F}_{2^n}$, however an affine function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is $c$-bent$_4$ only when $c = (1, \ldots, 1)$, see Remark 3.1 below and [2] for details. After this brief survey of some recent generalizations of bent functions, we are ready to proceed to generalizations of plateued and partially bent functions.

We first introduce some notation that enables us to treat the univariate and multivariate interpretations together.

Let $\mathbb{V}_n$ be a vector space over $\mathbb{F}_2$ of dimension $n$. We identify $\mathbb{V}_n$ by $\mathbb{F}_{2^n}$ or $\mathbb{F}_2^n$. From now on we shall use the notation

$$\mathcal{T}_f^c(u) = \begin{cases} \mathcal{V}_f^c(u) & \text{when } \ \mathbb{V}_n = \mathbb{F}_{2^n}, \\ \mathcal{U}_f^c(u) & \text{when } \ \mathbb{V}_n = \mathbb{F}_2^n. \end{cases} \tag{1.8}$$

Recall that $V_f^0 = \mathcal{W}_f$, where $\mathcal{W}_f$ is as in (1.3), hence the Walsh-Hadamard transform is a special case of $\mathcal{T}_f^c$.

The Parseval‘s identity implies that

$$\sum_{u \in \mathbb{V}_n} |\mathcal{T}_f^c(u)|^2 = 2^{2n}. \tag{1.9}$$

We denote the modified derivative of $f : \mathbb{V}_n \mapsto \mathbb{F}_2$, by

$$\mathcal{D}_a^c(f)(x) = \begin{cases} f(x + a) + f(x) + \langle c^2, ax\rangle & \text{when } \ \mathbb{V}_n = \mathbb{F}_{2^n}, \\ f(x + a) + f(x) + \langle c, (a \odot x)\rangle & \text{when } \ \mathbb{V}_n = \mathbb{F}_2^n, \end{cases} \tag{1.10}$$

where the inner product $\langle u, v\rangle$ is $\mathrm{Tr_n}(uv)$ in case $\mathbb{V}_n = \mathbb{F}_{2^n}$, and it is the canonical dot product when $\mathbb{V}_n = \mathbb{F}_2^n$.

Recall that a Boolean function is called *plateaued* or *s-plateaued* if $|\mathcal{W}_f(u)| \in \{0, 2^{\frac{n+s}{2}}\}$ for all $u \in \mathbb{V}_n$, where $s$ is an integer depending only on $f$. When $s = 1$, $f$ is called *semibent*. A well-known proper subclass of plateaued functions are *partially bent* functions. Recall that a function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is partially bent if the derivative $\mathcal{D}_a^0(f)$ is either balanced or constant for all $a \in \mathbb{V}_n$, see [6, 17]. We note that quadratic functions are partially bent hence plateaued.

One may consider a natural generalization of $s$-plateaued functions. We define a function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ to be *c-s-plateaued* if $|\mathcal{T}_f^c(u)| \in \{0, 2^{\frac{n+s}{2}}\}$ for an integer $s$ depending only on $f$, and all $u \in \mathbb{V}_n$. The value $c = 0$ yields $s$-plateaued functions hence we use the term $s$-plateaued rather than 0-$s$-plateaued.

In [3] *partially c-bent*$_4$ functions are introduced considering the modified derivative $\mathcal{D}_a^c(f)$ as in (1.10) when $\mathbb{V}_n = \mathbb{F}_{2^n}$. Hence $f$ is partially $c$-bent$_4$ if $D_a^c(f)$ is either balanced of constant for all $a \in \mathbb{V}_n$. As shown in [3], every partially $c$-bent$_4$ function is plateaued with respect to $\mathcal{V}_f^c$, and every quadratic function is partially $c$-bent$_4$ (for every $c$).

In this article we focus on $c$-$s$-plateaued and partially $c$-bent$_4$ functions in both univariate and multivariate settings. In Section 2 we observe that functions which are $c$-$s$-plateaued are shifts of $s$-plateaued functions that have certain additional properties. This generalizes similar results for bent$_4$ functions. We construct $c$-$s$-plateaued functions with various interesting properties in Section 3. In particular we construct functions $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$, which are $c$-$s$-plateaued but not partially $c$-bent$_4$, showing that partially $c$-bent$_4$ functions form a proper subclass of $c$-$s$-plateaued functions. In Section 3 we also present the behaviour of shifts of plateaued functions, which may or may not be partially bent. In Section 4 we characterize partially $c$-bent$_4$ functions and we investigate their differential properties. We end this paper with the study of relative difference sets corresponding to partially $c$-bent$_4$ functions, see Section 5.

## 2 Shifts of Boolean Functions

Recall that for a function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$, an element $a \in \mathbb{V}_n$ is called a *linear structure* of $f$ if $\mathcal{D}_a^0(f) = f(x + a) + f(x)$ is constant. As can be seen easily, the set of linear structures of $f$ forms a subspace of $\mathbb{V}_n$ which we will denote by $\Lambda(f)$.

The concept of a linear structure has been extended to $\mathbb{V}_n = \mathbb{F}_{2^n}$ in [3], using the modified derivative $\mathcal{D}_a^c(f)$. Putting

$$\Lambda_c(f) := \{a \in \mathbb{V}_n \,:\, \mathcal{D}_a^c(f) \,\text{is constant}\}$$

for $f : \mathbb{V}_n \mapsto \mathbb{F}_2$, one may also show that $\Lambda_c(f)$ is a subspace of $\mathbb{V}_n$. For the proof in case $\mathbb{V}_n = \mathbb{F}_{2^n}$, see Lemma 1 in [3]. The proof of the case $\mathbb{V}_n = \mathbb{F}_2^n$ follows similarly.

The functions $\sigma^c(x)$ and $s_2^c(x)$ play an important role in the theory of bent$_4$ functions. The following properties of $\sigma^c(x)$ and $s_2^c(x)$ will be frequently used.

**Lemma 2.1.** *For $c \in \mathbb{V}_n$, let $\sigma^c(x) : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ and $s_2^c(x) : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ be functions defined as in* (1.2) *and* (1.6)*, respectively. Then $\sigma^c(x)$ and $s_2^c(x)$ satisfy the following.*

*(i)* $\sigma^c(x+z) = \sigma^c(x)+\sigma^c(z)+\mathrm{Tr_n}(cx)\mathrm{Tr_n}(cz)+\mathrm{Tr_n}(c^2xz)$ *for every* $x, z \in \mathbb{F}_{2^n}$.

*(ii)* $s_2^c(x+z) = s_2^c(x) + s_2^c(z) + (c\cdot x)(c\cdot z) + c\cdot(x \odot z)$ *for every* $x, z \in \mathbb{F}_2^n$.

Proof of part (i) is given in [2], part (ii) follows similarly.

From now on we set

$$s^c(x) = \begin{cases} \sigma^c(x) & \text{when } \ \mathbb{V}_n = \mathbb{F}_{2^n}, \\ s_2^c(x) & \text{when } \ \mathbb{V}_n = \mathbb{F}_2^n. \end{cases} \tag{2.1}$$

**Lemma 2.2.** *For every function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ and every $c \in \mathbb{V}_n$ we have*

$$\Lambda_c(f) = \Lambda(f + s^c) \cap \{a \in \mathbb{V}_n \,:\, \langle c, a\rangle = 0\},$$

*hence* $\dim(\Lambda_c(f)) = \dim(\Lambda(f + s^c))$ *or* $\dim(\Lambda_c(f)) = \dim(\Lambda(f + s^c)) - 1$.

*Proof.* We give a proof for the case $\mathbb{V}_n = \mathbb{F}_{2^n}$, the case $\mathbb{V}_n = \mathbb{F}_2^n$ follows similarly.
Let $a \in \Lambda_c(f)$, i.e.,

$$f(x+a) + f(x) + \mathrm{Tr_n}(c^2ax) = f(0) + f(a) \tag{2.2}$$

for all $x \in \mathbb{F}_{2^n}$. When $x = a$ one has $\mathrm{Tr_n}(c^2a^2) = \mathrm{Tr_n}(ca) = 0$. Lemma 2.1(i) implies for any $a \in \mathbb{F}_{2^n}$ that

$$\begin{aligned} \mathcal{D}_a^0(f+\sigma^c)(x) &= f(x+a) + f(x) + \sigma^c(x+a) + \sigma^c(x) \\ &= f(x+a) + f(x) + \sigma^c(a) + \mathrm{Tr_n}(cx)\mathrm{Tr_n}(ca) + \mathrm{Tr_n}(c^2ax). \end{aligned} \tag{2.3}$$

If $a \in \Lambda_c(f)$, with $\mathrm{Tr_n}(ca) = 0$ and Equation (2.2) we see that $\mathcal{D}_a^0(f+\sigma^c)(x) = \sigma^c(a)+f(0)+f(a)$, hence it is constant. Consequently, $\Lambda_c(f) \subset \Lambda(f+\sigma^c) \cap \{a \in \mathbb{F}_{2^n} : \mathrm{Tr_n}(ca) = 0\}$.

Conversely suppose that $\mathrm{Tr_n}(ca) = 0$ and $\mathcal{D}_a^0(f+\sigma^c)$ is constant. Then by Equation (2.2) we obtain $\mathcal{D}_a^0(f+\sigma^c)(x) = f(x+a)+f(x)+\sigma^c(a)+\mathrm{Tr_n}(c^2ax) = f(a)+f(0)+\sigma^c(a)$, which implies that $a \in \Lambda_c(f)$. □

Lemma 2.2, in particular, shows that the derivative $\mathcal{D}_a^0(g)$ of the shifted function $g = f + s^c$ is constant for every $a$ for which $\mathcal{D}_a^c(f)$ is constant.

Regarding the transforms $\mathcal{T}_f^c$, in Theorems 4.26, 4.28 in [16] and in [2, Corollary 14], it is shown that for even integers $n$, a function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is $c$-bent$_4$ if and only if $f + s^c$ is bent. Hence, in even dimension $n$, a $c$-bent$_4$ function is a shifted bent function. When $n$ is odd we have a similar one-to-one correspondence between the set of $c$-bent$_4$ functions and the set of semibent functions with certain additional properties, see [2, 16] and also [7, 9, 13]. The following theorem extends these results to arbitrary values of $s \geq 0$.

**Theorem 2.3.** *(i) Let $n+s$ be even. A function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is $c$-$s$-plateaued if and only if $f+s^c$ is $s$-plateaued and $|W_{f+s^c}(u)| = |W_{f+s^c}(u+c)|$ for all $u \in \mathbb{V}_n$.*

*(ii) Let $n+s$ be odd. A function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is $c$-$s$-plateaued if and only if $f+s^c$ is $(s+1)$-plateaued and $W_{f+s^c}(u+c) = 0$ for any $u \in \mathbb{V}_n$ with $|W_{f+s^c}(u)| \neq 0$.*

*Proof.* This theorem was essentially proved ($s = 0$) in [2, 16]. The proof for this generalization uses the same arguments however we sketch it for the convenience of the reader. Observe that for any $a \in \{0, 1\}$ we have $i^a = \frac{1+(-1)^a}{2} + i\frac{1-(-1)^a}{2}$, and from *Jacobi's Two–Square Theorem*, stating that for a non-negative integer $k$, the integer solutions of the Diophantine equation $R^2 + I^2 = 2^k$ are

(i) $(R, I) = (0, \pm 2^{k/2})$ or $(\pm 2^{k/2}, 0)$ if $k$ is even, and

(ii) $(R, I) = (\pm 2^{(k-1)/2}, \pm 2^{(k-1)/2})$ if $k$ is odd.

Then

$$\mathcal{T}_f^c(u) = \frac{\mathcal{W}_{f+s^c}(u) + \mathcal{W}_{f+s^c}(u+c)}{2} + i\frac{\mathcal{W}_{f+s^c}(u) - \mathcal{W}_{f+s^c}(u+c)}{2} .$$

Consequently, a function $f$ is $c$-$s$-plateaued if and only if for all $u \in \mathbb{V}_n$

$$(\mathcal{W}_{f+s^c}(u) + \mathcal{W}_{f+s^c}(u+c))^2 + (\mathcal{W}_{f+s^c}(u) - \mathcal{W}_{f+s^c}(u+c))^2 \in \{0, 2^{n+s+2}\} ,$$

or equivalently

$$\mathcal{W}_{f+s^c}(u)^2 + \mathcal{W}_{f+s^c}(u+c)^2 \in \{0, 2^{n+s+1}\}. \tag{2.4}$$

If $n+s$ is even, by Jacobi's Two–Square Theorem, we have

$$|\mathcal{W}_{f+s^c}(u)| = |\mathcal{W}_{f+s^c}(u+c)| \in \{0, 2^{(n+s)/2}\} ,$$

for all $u \in \mathbb{V}_n$. Hence $f + s^c$ is an $s$-plateaued function with the claimed additional property. The converse also follows easily from Equation (2.4).
If $n+s$ is odd, then Jacobi's Two–Square Theorem implies that for all $u \in V_n$ we have

$$(\mathcal{W}_{f+s^c}(u), \mathcal{W}_{f+s^c}(u+c)) = (0,0), (0, \pm 2^{(n+s+1)/2}) \text{ or } (\pm 2^{(n+s+1)/2}, 0) .$$

Therefore $f+s^c$ is $(s+1)$-plateaued and $|\mathcal{W}_{f+s^c}(u)| \neq 0$ implies $W_{f+s^c}(u+c) = 0$. Again the converse of the statement follows easily from Equation (2.4). □

As mentioned earlier, partially bent functions are standard examples of plateaued functions. Indeed a partially bent function $g : \mathbb{V}_n \mapsto \mathbb{F}_2$ is $s$-plateaued, where $s = \dim \Lambda(g)$. Moreover, the support of the Walsh transform $\mathcal{W}_g$ of $g$ is a coset of $\Lambda(g)^\perp$, the orthogonal complement of $\Lambda(g)$, see [5].

Similarly, a partially $c$-bent$_4$ function is $c$-$s$-plateaued where $s$ is the dimension of $\Lambda_c(f)$, see [3]. The support of the transform $\mathcal{T}_f^c$ of $f$ is also a coset of $\Lambda_c(f)^\perp$, see the proof of [3, Proposition 2]. When we wish to emphasize the value of $s$ we also use the terms *$s$-partially bent* and *$s$-partially $c$-bent$_4$*.

As pointed out in [1], given a 1-partially bent function $g : \mathbb{V}_n \mapsto \mathbb{F}_2$, the shifted function $g + s^c$ is $c$-bent$_4$ for $2^{n-1}$ different nonzero elements $c \in V_n$. More generally, by Theorem 2.3 we have the following corollary.

**Corollary 2.4.** *Let $g : \mathbb{V}_n \mapsto \mathbb{F}_2$ be a partially bent function with linear space $\Lambda(g)$ of dimension $s$. Then $f = g + s^c$ is $s$-partially $c$-bent$_4$ for all nonzero $c \in \Lambda(g)^\perp$, and $(s-1)$-partially $c$-bent$_4$ for all $c \notin \Lambda(g)^\perp$.*

*Proof.* We prove the assertion for the case $\mathbb{V}_n = \mathbb{F}_{2^n}$. Since $g$ is partially bent, $g$ is $s$-plateaued where $s = \dim(\Lambda(g))$, and there exists a coset $b + \Lambda(g)^\perp$ such that $|\mathcal{W}_g(u)| = 2^{(n+s)/2}$ if and only if $u \in b + \Lambda(g)^\perp$. Let $c \in \Lambda(g)^\perp$, then $u + c \in b + \Lambda(g)^\perp$ if and only if $u \in b + \Lambda(g)^\perp$, hence $|\mathcal{W}_g(u)| = |\mathcal{W}_g(u+c)|$ for all $u \in \mathbb{F}_{2^n}$. By Theorem 2.3, $f = g + \sigma^c$ is then $c$-$s$-plateaued. By Lemma 2.2 we have $\Lambda_c(f) = \Lambda(g)$ since $c \in \Lambda(g)^\perp$, hence $\mathrm{Tr_n}(ca) = 0$ for all $a \in \Lambda(g)$. Therefore, $\dim(\Lambda_c(f)) = s$, and $f$ is $s$-partially $c$-bent$_4$.

If on the other hand $c \notin \Lambda(g)^{\perp}$, then $u + c \notin b + \Lambda(g)^{\perp}$ if $u \in b + \Lambda(g)^{\perp}$. Therefore $|\mathcal{W}_g(u)| = 2^{(n+s)/2}$ implies $\mathcal{W}_g(u + c) = 0$, and by Theorem 2.3, $f = g+\sigma^c$ is $c$-$(s-1)$-plateaued. Moreover, by Lemma 2.2, $\dim(\Lambda_c(f)) = s-1$, hence $f$ is also $(s-1)$-partially $c$-bent$_4$. □

Although $s$-plateaued functions from $\mathbb{V}_n$ to $\mathbb{F}_2$ exist for all even $n + s$, $0 \le s \le n$, $c$-$s$-plateaued functions exist only for $0 \le s \le n-1$, $c \neq 0$ while $n + s$ may be odd or even.

**Corollary 2.5.** *Let $c$ be a nonzero element in $\mathbb{V}_n$, and $s$ with $0 \le s \le n-1$ be arbitrary. Then there exists a function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ which is $c$-$s$-plateaued.*

*Proof.* From $s$-partially bent functions $g$, with $0 \le s \le n-2$ and even $n + s$, we obtain functions which are $s$-plateaued or $c$-$(s-1)$-plateaued by Corollary 2.4. Note that for $g(x)$ and $g_v(x) = g(x) + v \cdot x$ we have $\mathcal{W}_g(u) = \mathcal{W}_{g_v}(u + v)$. Hence we can always choose the coset of $\Lambda(g)^{\perp}$ that forms the support of $\mathcal{W}_g$ by adding a suitable linear function to $g$. It remains to show that $n$-partially bent functions (i.e., affine and constant functions) only yield functions which are $c$-$(n-1)$-plateaued. For an affine or constant function $g$ we have $\Lambda(g) = \mathbb{V}_n$, hence $\Lambda(g)^{\perp} = \{0\}$. Therefore we conclude by Corollary 2.4 that, $g + s^c$ is $c$-$(n-1)$-plateaued since any nonzero $c$ is not in $\Lambda(g)^{\perp}$. □

**Remark 2.6.** The functions that are $c$-$(n-1)$-plateaued are exactly the shifted functions $s^c + \ell$ for an affine or constant function $\ell$.

# 3 Constructions of Some Special Functions

Given a semibent function $g$, which is not partially bent, the shift $g + s_2^c$ may not be plateaued with respect to $\mathcal{U}_f^c$, see [1]. This also holds for $s$-plateaued functions for arbitrary $s$. On the contrary, it is possible that the shift of an $s$-plateaued function $g$, which is not partially bent (even satisfying $\Lambda(g) = \{0\}$) may be $c$-$s$-plateaued or $c$-$(s-1)$-plateaued for some $c \in \mathbb{F}_2^n$. Theorem 3.6 below states all possible cases for the shifted function.

**Remark 3.1.** The constructions in this section are given in multivariate form, however all statements apply to the univariate case also. 1-$s$-plateaued functions in univariate and in multivariate cases form the same sets. It was pointed out in [2] that if $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ is a $c$-bent$_4$ function, $c \neq 0$, then the function $\tilde{f}(x) = f(c^{-1}x)$ is negabent. In fact, observing that $\sigma^c(c^{-1}x) = \sigma^1(x)$, with straightforward calculations we infer that $\mathcal{V}_f^c(u) = \mathcal{V}_{\tilde{f}}^1(c^{-1}u)$. Hence the spectrum of $f$ with respect to $\mathcal{V}_f^c$ and the spectrum of $\tilde{f}$ with respect to $\mathcal{V}_{\tilde{f}}^1$ are the same. Consequently many questions on the transforms $\mathcal{V}_f^c$, $c \neq 0$, can be reduced to questions on $\mathcal{V}_f^1$. In particular, if $f$ is $c$-$s$-plateaued, then $\tilde{f}$ is 1-$s$-plateaued. It is straightforward to see that $c\Lambda_c(f) = \Lambda_1(\tilde{f})$. By Theorem 2.3, the Walsh transforms of $f + \sigma^c$ and $\tilde{f} + \sigma^1$ have the same properties. This does not apply to the transforms $\mathcal{U}_f^c$ for multivariate functions.

In what follows we employ an adaptation of the Maiorana-McFarland construction for plateaued functions, presented in [17]. For integers $k, t$ with $k < t$, let $\pi : \mathbb{F}_2^k \mapsto \mathbb{F}_2^t$ be an injection, and let $g : \mathbb{F}_2^k \times \mathbb{F}_2^t \mapsto \mathbb{F}_2$ be the function defined by $g(x, y) = \pi(x) \cdot y$. Then for any $(\beta, \gamma) \in \mathbb{F}_2^k \times \mathbb{F}_2^t$ we have, see [17],

$$\mathcal{W}_g(\beta, \gamma) = \begin{cases} \pm 2^t & \text{if } \gamma \in \mathrm{Im}(\pi) \ , \\ 0 & \text{if } \gamma \notin \mathrm{Im}(\pi) \ , \end{cases} \tag{3.1}$$

where $\mathrm{Im}(\pi)$ is the image of $\pi$. Hence $g$ is $(t-k)$-plateaued, and the support of $\mathcal{W}_g$ is determined by the image of $\pi$.

We further recall and slightly extend Lemma 6 in [17].

**Lemma 3.2.** *Let $t \geq 3$.*

**i)** *There exists a set $S = \{v_0, v_1, \ldots, v_t\} \subset \mathbb{F}_2^t$ such that for any nonzero $v \in \mathbb{F}_2^t$, we have*

$$(v \cdot v_0, v \cdot v_1, \ldots, v \cdot v_t) \notin \{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\}. \tag{3.2}$$

**ii)** *For any nonzero $c \in \mathbb{F}_2^t$, the set $S$ can be chosen in such a way that $v_i \neq v_j + c$, $0 \leq i, j \leq t$.*

*Proof.* Let $\{v_1, \ldots, v_t\}$ be a linearly independent subset of $\mathbb{F}_2^t$. Then the map $\phi : \mathbb{F}_2^t \mapsto \mathbb{F}_2^t$ defined by $\phi(v) = (v \cdot v_1, \ldots, v \cdot v_t)$ is a bijection. Hence we have $\phi(v^*) = (1, \ldots, 1)$ for a unique vector $v^* \in \mathbb{F}_2^t$. Let $v_0 \in \mathbb{F}_2^t$ be a nonzero vector such that $v^* \cdot v_0 = 0$. Then $\{v_0, v_1, \ldots, v_t\}$ satisfies (3.2).

For $\{v_0, v_1, \ldots, v_t\}$ to satisfy the additional property, we have $2^t - 1$ choices for $v_1$, then $2^t - 3$ choices for $v_2$ (we also have to exclude $v_1 + c$). For $v_3$ we have at least $2^t - 2^2 - 2$ choices. Continuing with this argument, we finally have at least $2^t - 2^{t-1} - (t-1) = 2^{t-1} - t + 1$ choices for $v_t$. For $v_0$ we choose a vector other than $v_i + c$, $1 \leq i \leq t$, with $v^* \cdot v_0 = 0$, which leaves us with $2^{t-1} - t$ choices. □

**Proposition 3.3.** *Let $n \geq 7$. For any $c \in \mathbb{F}_2^n$ there exists a $c$-$s$-plateaued function, which is not partially $c$-bent$_4$.*

*Proof.* We will use the construction in [17] of an $s$-plateaued function $g$. Let $n = t + k, t > k, 2^k \geq 2(t+1)$ and $\pi : \mathbb{F}_2^k \mapsto \mathbb{F}_2^t$ be an injective function. Consider $g(x,y) = \pi(x) \cdot y$. By construction $g$ is $t-k$ plateaued. Now we consider the vectors $\{v_0, v_1, \dots, v_t\}$ as in Lemma 3.2 and impose the condition on $\pi$ that $\{v_0, v_1, \dots, v_t\} \subset \mathrm{Im}(\pi)$. This assumption guarantees that $g$ has trivial linear space $\Lambda(g) = \{0\}$ since

$$\begin{aligned}\mathcal{W}_{g(x+\alpha,y+\beta)+g(x,y)}(0) &= \sum_{(x,y)\in\mathbb{F}_2^k\times\mathbb{F}_2^t} (-1)^{g(x+\alpha,y+\beta)+g(x,y)} \\ &= \sum_{(x,y)\in\mathbb{F}_2^k\times\mathbb{F}_2^t} (-1)^{\pi(x+\alpha)\cdot(y+\beta)+\pi(x)\cdot y} \\ &= \sum_{x\in\mathbb{F}_2^k} (-1)^{\pi(x+\alpha)\cdot\beta} \sum_{y\in\mathbb{F}_2^t} (-1)^{(\pi(x+\alpha)+\pi(x))\cdot y} .\end{aligned}$$

If $\alpha \neq 0$, then $\pi(x+\alpha) + \pi(x) \neq 0$ and the inner sum vanishes for all $x \in \mathbb{F}_2^k$, and hence $|\mathcal{W}_{g(x+\alpha,y+\beta)+g(x,y)}(0)| = 0$. If $\alpha = 0$, then we have

$$\mathcal{W}_{g(x+\alpha,y+\beta)+g(x,y)}(0) = 2^t \sum_{x\in\mathbb{F}_2^k} (-1)^{\pi(x)\cdot\beta} \neq \pm 2^{k+t}$$

as $\pi(x) \cdot \beta \notin \{(0,0,\dots,0), (1,1,\dots,1)\}$. We may also assume that $\pi$ has additional properties that enable us to use Theorem 2.3 (i) and obtain a function $f = g + s_2^c$ which is $c$-$s$-plateaued. We now fix $c = (c_1, c_2) \in \mathbb{F}_2^k \times \mathbb{F}_2^t$ and assume without loss of generality $c_2 \neq 0$, otherwise we permute the variables. In order that $g$ satisfies $|\mathcal{W}_g(\beta,\gamma)| = |\mathcal{W}_g(\beta + c_1, \gamma + c_2)|$ either $\gamma, \gamma + c_2 \in \mathrm{Im}(\pi)$ or $\gamma, \gamma + c_2 \notin \mathrm{Im}(\pi)$ for all $\gamma \in \mathbb{F}_2^t$. Note that such $\pi$ exists since $\mathbb{F}_2^t$ can be expressed as the disjoint union of the sets $\mathbb{F}_2^t = \bigcup_{\nu\in\mathbb{F}_2^t} \{\nu, \nu + c_2\}$. Hence by Theorem 2.3, $f = g + s_2^c$ is $c$-$s$-plateaued. Alternatively, we can choose $\pi$ such that $\gamma \in \mathrm{Im}(\pi)$ implies $\gamma + c_2 \notin \mathrm{Im}(\pi)$, equivalently $|\mathcal{W}_g(\beta,\gamma)| \neq 0$ implies $\mathcal{W}_g(\beta + c_1, \gamma + c_2) = 0$. In this case Theorem 2.3 (ii) gives $f = g + s_2^c$ which is $c$-$(s-1)$-plateaued. In both cases Lemma 2.2 implies that $\Lambda_c(f) = \Lambda(g) = \{0\}$. We therefore have a plateaued function that is not partially $c$-bent$_4$.

□

**Remark 3.4.** The proposition above answers the question about the existence of $c$-$s$-plateaued functions that are not partially $c$-bent$_4$, which was left open in [3], see the explanation after Corollary 4 in [3].

Given a partially bent function $g$, the shifted function $f = g + s^c$ is partially $c$-bent$_4$ for every $c \in \mathbb{V}_n$ as Corollary 2.4. Standard examples are quadratic functions. Now we construct a partially $c$-bent$_4$ function $f$ such that $f + s_2^c$ is plateaued but not partially bent, showing that there exists a plateaued function $g$ which is not partially bent but its shift is partially $c$-bent$_4$.

We use the well known fact that for functions $g_1 : \mathbb{V}_n \mapsto \mathbb{F}_2$, $g_2 : \mathbb{V}_m \mapsto \mathbb{F}_2$, for $g(x, y) = g_1(x) + g_2(y)$ we have

$$\mathcal{W}_g(\alpha, \beta) = \mathcal{W}_{g_1}(\alpha)\mathcal{W}_{g_2}(\beta). \tag{3.3}$$

Note that Equation 3.3 also holds for the transforms $\mathcal{T}_f^c$.

**Proposition 3.5.** *Let $n \geq 10$. For any $c \in \mathbb{F}_2^n$, $c \neq 0$, there exists $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ such that $f$ is $s$-partially $c$-bent$_4$ and $g = f + s_2^c$ is $(s+1)$-plateaued but not partially bent.*

*Proof.* Set $n = 2k + 2t + s + 1$, where $k \geq 3$, $t \geq 1$, $s \geq 1$. Note that $\Lambda_c(f) \subset \Lambda(g)$, i.e., $\dim(\Lambda(g)) \geq s$. Hence we need to construct $g : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ satifying the following conditions:

**i)** g is $(s + 1)$-plateaued,

**ii)** $\dim(\Lambda(g)) = s$,

**iii)** $\mathcal{W}_g(u) \neq 0$ implies $\mathcal{W}_g(u + c) = 0$ for all $u \in \mathbb{F}_2^n$.

Consider $g_1 : \mathbb{F}_2^k \times \mathbb{F}_2^{k+1} \mapsto \mathbb{F}_2$ satisfying $g_1(x, y) = \pi_1(x) \cdot y$, where $\pi_1 : \mathbb{F}_2^k \mapsto \mathbb{F}_2^{k+1}$ is the same injection as the one used in the proof of Proposition 3.3. Similarly, we define $g_2 : \mathbb{F}_2^t \times \mathbb{F}_2^{t+s} \mapsto \mathbb{F}_2$ by $g_2(z, w) = \pi_2(z) \cdot w$, where $\pi_2 : \mathbb{F}_2^t \mapsto \mathbb{F}_2^{t+s}$ is injective and linear. Set $c = (c_1, c_2, c_3, c_4) \in \mathbb{F}_2^n = \mathbb{F}_2^k \times \mathbb{F}_2^{k+1} \times \mathbb{F}_2^t \times \mathbb{F}_2^{t+s}$. We can assume without loss of generality that $\mathrm{Im}(\pi_2)$ contains $c_4$.
By [6, Section 3], $g_2$ is $s$-partially bent with $\Lambda(g_2) = \{(0, b) \,:\, b \in \mathrm{Im}(\pi_2)^\perp\}$. We now define $g : \mathbb{F}_2^k \times \mathbb{F}_2^{k+1} \times \mathbb{F}_2^t \times \mathbb{F}_2^{t+1} \mapsto \mathbb{F}_2$ as $g(x, y, z, w) = g_1(x, y) + g_2(z, w)$. Since $\mathcal{W}_g(\alpha, \beta, \gamma, \delta) = \mathcal{W}_{g_1}(\alpha, \beta)\mathcal{W}_{g_2}(\gamma, \delta)$, $g$ is $(s+1)$-plateaued. Furthermore, $\mathcal{W}_g(\alpha, \beta, \gamma, \delta) \neq 0$ implies $\mathcal{W}_{g_1}(\alpha, \beta) \neq 0$. By the choice of $g_1$, $\mathcal{W}_{g_1}(\alpha, \beta) \neq 0$ implies $\mathcal{W}_{g_1}(\alpha + c_1, \beta + c_2) = 0$, i.e., $\mathcal{W}_g(\alpha + c_1, \beta + c_2, \gamma + c_3, \delta + c_4) = 0$. Therefore, $g + s_2^c$ is $c$-$s$-plateaued by Theorem 2.3 (ii). An element $(\alpha, \beta, \gamma, \delta) \in \mathbb{F}_2^n$ lies in $\Lambda(g)$ if and only if

$$\mathcal{W}_{g(x+\alpha, y+\beta, z+\gamma, w+\delta)+g(x,y,z,w)}(0, 0, 0, 0) = \pm 2^{2k+2t+s+1}.$$

Observing that

$$\begin{aligned}\mathcal{D}^0_{(\alpha,\beta,\gamma,\delta)}(g)(x, y, z, w) &= g(x + \alpha, y + \beta, z + \gamma, w + \delta) + g(x, y, z, w)\\ &= g_1(x + \alpha, y + \beta) + g_1(x, y) + g_2(z + \gamma, w + \delta) + g_2(z, w)\\ &= \mathcal{D}^0_{(\alpha,\beta)}(g_1)(x, y) + \mathcal{D}^0_{(\gamma,\delta)}(g_2)(z, w),\end{aligned}$$

we have

$$\mathcal{W}_{\mathcal{D}^0_{(\alpha,\beta,\gamma,\delta)}(g)}(0,0,0,0) = \mathcal{W}_{\mathcal{D}^0_{(\alpha,\beta)}(g_1)}(0,0)\mathcal{W}_{\mathcal{D}^0_{(\gamma,\delta)}(g_2)}(0,0).$$

This implies that $\Lambda(g) = \Lambda(g_1) \times \Lambda(g_2)$. Therefore $\Lambda(g) = \{(0,0,0,b) : b \in \mathrm{Im}(\pi_2)^\perp\}$. By Lemma 2.2, $\Lambda_c(f) = \{(0,0,0,b) \in \mathbb{F}_2^n : b \in \mathrm{Im}(\pi_2)^\perp, c_4 \cdot b = 0\}$. Recall that $c_4 \in \mathrm{Im}(\pi_2)^\perp$, i.e., $\Lambda_c(f) = \Lambda(g)$. Therefore $f$ satisfies the required properties. □

**Theorem 3.6.** *Let $g : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ be an s-plateaued function. Put $f = g + s_2^c$, $c \in \mathbb{F}_2^n$. Then the following are possible.*

*(i) $g$ is s-partially bent and $f$ is s-partially c-bent$_4$;*

*(ii) $g$ is s-partially bent and $f$ is $(s-1)$-partially c-bent$_4$;*

*(iii) $g$ is s-plateaued but not partially bent and $f$ is c-s-plateaued, but not partially c-bent$_4$;*

*(iv) $g$ is s-plateaued but not partially bent and $f$ is c-$(s-1)$-plateaued, but not partially c-bent$_4$;*

*(v) $g$ is s-plateaued but not partially bent and $f$ is $(s-1)$-partially c-bent$_4$;*

*(vi) $g$ is s-plateaued but not partially bent and $f$ is not plateaued with respect to $\mathcal{T}_f^c$.*

*Proof.* Parts (i) and (ii) follow from Corollary 2.4. Part (iii) is a consequence of Proposition 3.3. By using Equation 3.3, we observe that the sum $g$ of functions $g_1$ and $g_2$, satisfying the properties of (ii) and (iii), respectively, satisfies the condition (iv). Part (v) can be obtained from Proposition 3.5, and (vi) follows by [1, Proposition 6.3]. □

**Remark 3.7.** A characterization of plateaued functions via the Walsh transform is given in [8]. Let $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ be a function, $k$ be a positive integer,

$$S_k(f) = \sum_{u \in \mathbb{V}_n} |\mathcal{W}_f(u)|^{2k} \quad \text{and} \quad T_k(f) = S_{k+1}(f)/S_k(f).$$

Then $f$ is plateaued if and only if $T_{k+1}(f) = T_k(f)$. In particular, $f$ is plateaued if and only if $T_2(f) = T_1(f)$. Since the proof relies on Parseval's identity, an analog statement is true for every function $\mathcal{H}$ from $\mathbb{V}_n$ to $\mathbb{C}$ satisfying $\sum_{u \in \mathbb{V}_n} |\mathcal{H}|^2 = 2^{2n}$, hence for the transforms $\mathcal{T}_f^c$.

## 4 Partially $c$-bent$_4$ functions

In this section we give some characterizations of partially $c$-bent$_4$ functions.

**Definition 4.1.** Let $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ and $c \in \mathbb{V}_n$. We define the sets $D_f^{(c)}$ and $Z_f^{(c)}$ as

$$D_f^{(c)} = \{a \in \mathbb{V}_n \mid \mathcal{D}_a^c(f) \text{ is balanced}\} \ ,$$

and

$$Z_f^{(c)} = \{u \in \mathbb{V}_n \mid \mathcal{T}_f^c(u) = 0\} \ .$$

We denote the cardinalities of the sets $D_f^{(c)}$ and $Z_f^{(c)}$ by $N_{D_f^{(c)}}$ and $N_{Z_f^{(c)}}$, respectively.

In [4], the author shows that for $c = 0$, and for any $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ the inequality

$$\left(2^n - N_{D_f^{(0)}}\right)\left(2^n - N_{Z_f^{(0)}}\right) \geq 2^n \tag{4.1}$$

holds. We now generalize this inequality for any nonzero $c \in \mathbb{V}_n$, and show that the equality holds if and only if $f$ is partially $c$-bent$_4$. Note that in [4], partially bent functions have been defined as functions for which the equality in (4.1) holds for $c = 0$.

**Proposition 4.2.** *Let $f : \mathbb{V}_n \mapsto \mathbb{F}_2$, $c \in \mathbb{V}_n$, and the integers $N_{D_f^{(c)}}$ and $N_{Z_f^{(c)}}$ be defined as above. Then we have*

$$\left(2^n - N_{D_f^{(c)}}\right)\left(2^n - N_{Z_f^{(c)}}\right) \geq 2^n \ .$$

*The equality holds if and only if $f$ is partially $c$-bent$_4$.*

*Proof.* For simplicity we give the proof in univariate case. First we show that

$$2^n(2^n - N_{D_f^{(c)}}) \geq \sup_{u \in \mathbb{F}_{2^n}} |\mathcal{V}_f^c(u)|^2 \ . \tag{4.2}$$

For $|\mathcal{V}_f^c(u)|^2$ we have

$$\begin{aligned} |\mathcal{V}_f^c(u)|^2 &= \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(y)+\sigma^c(x)+\sigma^c(y)+\mathrm{Tr_n}(u(x+y))} i^{\mathrm{Tr_n}(cx)-\mathrm{Tr_n}(cy)} \\ &= \sum_{x,z \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+z)+\sigma^c(x)+\sigma^c(x+z)+\mathrm{Tr_n}(uz)} i^{\mathrm{Tr_n}(cx)-\mathrm{Tr_n}(cx+cz)}. \end{aligned}$$

Recalling that

$$\mathrm{Tr_n}(x) + \mathrm{Tr_n}(z) \equiv \mathrm{Tr_n}(x+z) + 2\mathrm{Tr_n}(x)\mathrm{Tr_n}(z) \mod 4 \ ,$$

by the property of $\sigma^c$ in Lemma 2.1 we obtain

$$|\mathcal{V}_f^c(u)|^2 = \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\sigma^c(z)+\mathrm{Tr_n}(uz)} i^{-\mathrm{Tr_n}(cz)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x+z)+f(z)+\mathrm{Tr_n}(c^2xz)} \ . \quad (4.3)$$

For $z \in D_f^{(c)}$ the inner sum vanishes, and for $z \in \mathbb{F}_{2^n} \setminus D_f^{(c)}$ the inner sum is at most $2^n$. Hence we have $2^n(2^n - N_{D_f^{(c)}}) \geq |\mathcal{V}_f^c(u)|^2$ for any $u \in \mathbb{F}_{2^n}$, which proves (4.2).

As can be observed easily , $(2^n - N_{Z_f^{(c)}})\sup_{u\in\mathbb{F}_{2^n}}|\mathcal{V}_f^c(u)|^2 \geq \sum_{u\in\mathbb{F}_{2^n}} |\mathcal{V}_f^c(u)|^2$. By Parseval's identity (1.9), we obtain

$$2^n - N_{Z_f^{(c)}} \geq \frac{2^{2n}}{\sup_{u\in\mathbb{F}_{2^n}}|\mathcal{V}_f^c(u)|^2} \ . \quad (4.4)$$

Combining equations (4.2) and (4.4) yields the claimed inequality.

It remains to show that the Equality in (4.1) holds if and only if $f$ is partially $c$-bent$_4$. First observe that for a partially $c$-bent$_4$ function $f$ with $\dim(\Lambda_c(f)) = s$ we have $2^n - N_{D_f^{(c)}} = |\Lambda_c(f)| = 2^s$, and $|\mathcal{V}_f^c(u)|^2 \in \{0, 2^{n+s}\}$, hence by Parseval's identity, $2^n - N_{Z_f^{(c)}} = 2^{n-s}$. Consequently, Equation (4.1) holds. Conversely suppose that the equality holds in (4.1), and hence the equality in (4.4) holds, i.e.,

$$\sup_{u\in\mathbb{F}_{2^n}}|\mathcal{V}_f^c(u)|^2 \left(2^n - N_{Z_f^{(c)}}\right) = 2^{2n} = \sum_{v\notin Z_f^{(c)}} |\mathcal{V}_f^c(v)|^2 \ . \quad (4.5)$$

Note that we used Parseval's identity in the second equality. Equation (4.5) holds if and only if

$$|\mathcal{V}_f^c(v)| = \sup_{u\in\mathbb{F}_{2^n}}|\mathcal{V}_f^c(u)|$$

for all $v \in \mathbb{F}_{2^n} \setminus Z_f^{(c)}$. This implies that $|\mathcal{V}_f^c(v)| \in \{0, 2^{(n+s)/2}\}$ and hence by Equation (4.5), we have $2^n - N_{Z_f^{(c)}} = 2^{n-s}$ for some non-negative integer $s$. Supposing equality in (4.1), this yields that $2^n - N_{D_f^{(c)}} = 2^s$. For an element $v$

in the support of $\mathcal{V}_f^c(v)$, Equation (4.3) can be written as

$$\begin{aligned}|\mathcal{V}_f^c(u)|^2 &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\sigma^c(z)+\mathrm{Tr_n}(uz)} i^{-\mathrm{Tr_n}(cz)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x+z)+f(z)+\mathrm{Tr_n}(c^2xz)}\\ &= \sum_{z\in\mathbb{F}_{2^n}\setminus D_f^{(c)}} (-1)^{\sigma^c(z)+\mathrm{Tr_n}(uz)} i^{-\mathrm{Tr_n}(cz)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x+z)+f(z)+\mathrm{Tr_n}(c^2xz)} = 2^{n+s}.\end{aligned}$$

Note that in the second equality we used the fact that the inner sum is 0 if and only if $z \in D_f^{(c)}$. Since $|\mathbb{F}_{2^n} \setminus D_f^{(c)}| = 2^n - N_{D_f^{(c)}} = 2^s$ we must have

$$|\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x+z)+f(z)+\mathrm{Tr_n}(c^2xz)}| = 2^n$$

for all $z \in \mathbb{F}_{2^n} \setminus D_f^{(c)}$. This applies if and only if $f(x+z)+f(z)+\mathrm{Tr_n}(c^2xz)$ is constant for all $z \in \mathbb{F}_{2^n} \setminus D_f^{(c)}$, hence $\Lambda_c(f) = \mathbb{F}_{2^n} \setminus D_f^{(c)}$, which gives the desired result. □

The following corollary generalizes characterization of partially bent functions given in [4] to arbitrary partially $c$-bent$_4$ functions.

**Corollary 4.3.** *Let $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ be a function and $c \in \mathbb{V}_n$. Then the following are equivalent.*

*(i) $f$ is partially $c$-bent$_4$.*

*(ii) $f$ is $c$-$s$-plateaued for some integer $s \geq 0$, where* $\dim(\Lambda_c(f)) = s$.

*(iii) Using the notation in Proposition 4.2 we have*

$$\left(2^n - N_{D_f^{(c)}}\right)\left(2^n - N_{Z_f^{(c)}}\right) = 2^n\ .$$

*(iv) For any complement $\Lambda^{comp}$ of $\Lambda_c(f)$ in $\mathbb{V}_n$ the function $f$ restricted to $\Lambda^{comp}$ is $c$-bent$_4$ (Corollary 3 in [3]).*

# 5 Relative Difference Sets

Recall that a $(\mu, \nu, k, \lambda)$-*relative difference set* in a group $G$ of order $\mu\nu$ relative to a subgroup $B$ of $G$ of order $\nu$, is a $k$-elementary subset $R$ of $G$ such that every element in $G \setminus B$ can be written as $r_1 - r_2$, $r_1, r_2 \in R$, in exactly $\lambda$

ways, and there is no such representation for any nonzero element in $B$. The subgroup $B$ is then called the *forbidden subgroup.* If $G = A \times B$, then $R$ is called a *splitting relative difference set.* As is well known, a Boolean function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is bent if and only if its graph is a splitting relative difference set in $\mathbb{V}_n \times \mathbb{F}_2$, see for instance [14]. We have a similar combinatorial interpretation of negabent functions and more generally of $c$-bent$_4$ functions, $c \neq 0$. Consider the operation $*_c$ on $\mathbb{V}_n \times \mathbb{F}_2$, $c \in \mathbb{V}_n \setminus \{0\}$, given by

$$(x_1, y_1) *_c (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \langle c^2, x_1 x_2 \rangle) \text{ when } \mathbb{V}_n = \mathbb{F}_{2^n}$$

and

$$(x_1, y_1) \star_c (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \langle c, x_1 \odot x_2 \rangle) \text{ when } \mathbb{V}_n = \mathbb{F}_2^n.$$

Then $\mathbb{V}_n \times \mathbb{F}_2$ under $*_c$ forms a group isomorphic to $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$. A function $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is $c$-bent$_4$ if and only if its graph $\{(x, f(x)) : x \in \mathbb{V}_n\}$ is a relative difference set in $(\mathbb{V}_n \times \mathbb{F}_2, *_c)$ relative to $\{0\} \times \mathbb{F}_2$. We refer to [2] for the details, and remark that these relative difference sets are not splitting.

In [6] it has been observed that partially bent functions $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ induce a certain generalization of a relative difference set in $\mathbb{V}_n \times \mathbb{F}_2$, which is called a *partially bent relative difference set.* More generally, partially bent functions have been characterized as functions $f$ from a group $H$ into a group $N$ for which the graph $R = \{(x, f(x)) : x \in H\}$ has the following properties, see [6, Proposition 2.8]. The group $G = H \times N$ contains a subgroup $B$ of the form $B = A \times N$ such that

(1) $g \in G \setminus B$ can be represented as $r_1 - r_2$, for $r_1, r_2 \in R$ in exactly $\lambda$ ways for some $\lambda > 0$;

(2) $g \in B \setminus A$ has no representation of the form $r_1 - r_2$, for $r_1, r_2 \in R$;

(3) $g \in A$ can be represented as $r_1 - r_2$, for $r_1, r_2 \in R$ in exactly $|R| = k$ ways.

If $A = \{0\}$ then $R$ reduces to a conventional splitting relative difference set, which corresponds to a bent function from $H$ to $N$, see [11].

In the following, we point out that partially $c$-bent$_4$ functions likewise induce generalizations of such relative difference sets in $\mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$ that come from $c$-bent$_4$ functions. We define the generalization of (not necessarily splitting) relative difference sets in a more general framework, and first discuss some of its properties.

Let $G$ be an abelian group of order $mnl$ and $A \subset B$ be subgroups of $G$ of orders $|A| = l$, $|B| = nl$. We call a $k$-subset $R$ of $G$ a *pre-relative difference set relative to* $B \setminus A$ with parameters $(m, n, l, k, \lambda)$, if the conditions (1),(2),(3) above hold.

**Theorem 5.1.** *Let $R$ be an $(m, n, l, k, \lambda)$ pre-relative difference set in $G$ relative to $B \setminus A$, and let $\bar{G} = G/A$ and $\bar{B} = B/A$. Then we have the following.*

*(i) $R$ is the union of cosets of $A$, at most one of which lies in $B$. In particular, if $|R| = k = vl$, then $(v^2 - v)l = \lambda(mn - n)$.*

*(ii) Let $\bar{R}$ be the subset of $\bar{G}$ consisting of the cosets of $A$ that lie in $R$. Then $\bar{R}$ is an $(m, n, v, \lambda/l)$-relative difference set in $\bar{G}$ relative to $\bar{B}$.*

*Proof.* (i) Let $r \in R$. We need to show that $r + a \in R$ for all $a \in A$. Since any element $a$ of $A$ can be written as a difference $r_1 - r_2$, where $r_1, r_2 \in R$ in $k$ ways, for any fixed $r \in R$, there exists a unique $\tilde{r} \in R$ such that $a = \tilde{r} - r$. Hence $r + a = \tilde{r} \in R$. Suppose that the distinct cosets $r_1 + A$, $r_2 + A$ are in $B \cap R$. Then $r_1 - r_2 = b \in B$ but $b \notin A$, which is a contradiction. If $|R| = vl$, then $|R|^2 = \lambda|G \setminus B| + |R||A|$ implies the claimed equation.

(ii) First we show that any element $\bar{b} \in \bar{B}$ can not be written as a difference of elements in $\bar{R}$. Suppose that $\bar{b} = \bar{r}_1 - \bar{r}_2 \in \bar{B} \setminus \{0\}$ for some $\bar{r}_1, \bar{r}_2 \in \bar{R}$. Then $b = r_1 - r_2 + a$ for some $a \in A$, $b \in B \setminus A$ and $r_1, r_2 \in R$. Since $a$ can be written as a difference of elements of $R$ in $k$ ways, for $r_2 \in R$, there exists $r \in R$ such that $a = r_2 - r$. Consequently, $b = r_1 - r$, which is a contradiction.

It remains to show that every element $\bar{g} \in \bar{G} \setminus \bar{B}$ can be written as a difference of elements in $\bar{R}$ in exactly $\lambda/|A| = \lambda/l$ ways. (In particular, this shows that $\lambda$ is divisible by $|A| = l$.) The element $\bar{g}$ can be represented as $g \in G \setminus B$ in exactly $|A| = l$ ways. Also we know that each $g \in G \setminus B$ can be written as a difference of elements in $R$ in exactly $\lambda$ ways. Therefore, elements in the coset $g + A$ can be expressed as a difference $r_1 - r_2$, $r_1, r_2 \in R$ in exactly $\lambda l$ ways. Since $l^2$ differences $r_1 - r_2$ give the same $\bar{g} \in \bar{G}$, we conclude that $\bar{g}$ can be represented in exactly $\lambda/l$ ways, which gives the desired result. □

**Corollary 5.2.** *Let $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ be an $s$-partially $c$-bent$_4$ function. Then the graph $R = \{(x, f(x)) \mid x \in \mathbb{F}_{2^n}\}$ is a $(2^{n-s}, 2, 2^s, 2^n, 2^{n-1})$-pre-relative difference set in $G = (\mathbb{F}_{2^n} \times \mathbb{F}_2, *_c)$.*

*Proof.* We assume without loss of generality that $f(0) = 0$ and define

$$A := \{(a, f(a)) \mid a \in \Lambda_c(f)\} \quad \text{and} \quad B := \{(a, y) \mid a \in \Lambda_c(f), y \in \mathbb{F}_2\} .$$

It is clear that $B$ is a subgroup of $G$, so we first show that $A$ is a subgroup of $G$. For $(a, f(a)), (b, f(b)) \in A$, we have

$$(a, f(a)) *_c (b, f(b)) = (a + b, f(a) + f(b) + \mathrm{Tr_n}(c^2ab)) \ .$$

Since $f(x + a) + f(x) + f(a) + \mathrm{Tr_n}(c^2ax) = 0$ for all $x \in \mathbb{F}_{2^n}$, we have $f(a) + f(b) + \mathrm{Tr_n}(c^2ab) = f(a + b)$, which gives the desired result.

To investigate the difference properties of $R$ we first observe that the inverse of $(x, f(x)) \in G$ is $(x, f(x))^{-1} = (x, f(x) + \mathrm{Tr_n}(cx))$, hence for $(x, f(x)), (x + a, f(x + a)) \in R$ we have

$$(x + a, f(x + a)) *_c (x, f(x))^{-1} = (a, f(x + a) + f(x) + \mathrm{Tr_n}(c^2xa)) \ .$$

Let $g := (a, b) \in G$. If $a \notin \Lambda_c(f)$, i.e., $(a, b) \in G \setminus B$, then $D^c_a(f) = f(x + a) + f(x) + \mathrm{Tr_n}(c^2xa)$ is balanced. Consequently every element $g \in G \setminus B$ can be represented as difference in $R$ in exactly $2^{n-1}$ ways. If $a \in \Lambda_c(f)$, i.e., $(a, b) \in B$, then $D^c_a(f) = f(x+a)+f(x)+\mathrm{Tr_n}(c^2xa) = f(a)$ is constant. Hence if $b = f(a)$, i.e., $(a, b) \in A$, then $(a, b)$ has $2^n$ representations as a difference of elements in $R$, and all elements $(a, f(a) + 1)$ of $B \setminus A$ do not have such a representation.

It can be verified easily that when $f(0) = 1$, then $A$ and $B \setminus A$ (which in this case is a subgroup) switch roles. □

**Remark 5.3.** Since we have $\mathrm{Tr_n}(ca) = 0$ for $a \in \Lambda_c(f)$, every element $g \in B$ has order 2, i.e., the subgroups $A, B$ are elementary abelian 2-groups. In particular, $A \simeq \mathbb{Z}_2^s$ and $B \simeq \mathbb{Z}_2^{s+1}$.

# Acknowledgement

N.A. is supported by the Austrian Science Fund (FWF): Project F5505-N26 and Project F5511-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". A.T. was supported by TUBITAK Project no 114F432. Parts of this paper was written while C. K. visited Johannes Kepler Univeristy and RICAM, and N.A. visited Sabancı University. Authors gratefully acknowledge the hospitality and financial support provided by all three institutions.

# References

[1] N. Anbar, W. Meidl, A. Pott, Equivalence for negabent functions and their relative difference sets, preprint 2017.

[2] N. Anbar, W. Meidl, Modified planar functions and their components, Cryptogr. Commun. 10 (2018), no. 2, 235–249.

[3] N. Anbar, W. Meidl, Bent and bent$_4$ spectra of Boolean functions over finite fields, Finite Fields Appl. 46 (2017), 163–178.

[4] C. Carlet, Partially bent functions, Des. Codes Cryptogr., vol. 3 (1993), 135–145.

[5] A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions. J. Comb. Theory, Series A, 119 (2012), 420–429.

[6] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, Partially bent functions and their properties, Applied algebra and number theory, 22–38, Cambridge Univ. Press, Cambridge, 2014.

[7] S. Gangopadhyay, E. Pasalic, P. Stănică, A note on generalized bent criteria for Boolean functions. IEEE Trans. Inform. Theory 59 (2013), no. 5, 3233–3236.

[8] S. Mesnager, Characterizations of plateaued and bent functions in characteristic $p$. Sequences and their applications–SETA 2014, 72–82, Lecture Notes in Comput. Sci., 8865, Springer, Cham, 2014.

[9] M.G. Parker, A. Pott, On Boolean functions which are bent and negabent. Sequences, subsequences, and consequences, 9–23, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 2007.

[10] A. Pott, Almost perfect and planar functions. Des. Codes Cryptogr., vol. 78 (2016), 141–195.

[11] A. Pott, Nonlinear functions in abelian groups and relative difference sets. Discrete Applied Mathematics 138 (2004), 177–193.

[12] K.U. Schmidt, Y. Zhou, Planar functions over fields of characteristic two. J. Algebraic Combin. 40 (2014), no. 2, 503–526.

[13] W. Su, A. Pott, X. Tang, Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. IEEE Trans. Inform. Theory 59 (2013), 3387–3395.

[14] Y. Tan, A. Pott, T. Feng, Strongly regular graphs associated with ternary bent functions. J. Combin. Theory Ser. A 117 (2010), no. 6, 668–682.

[15] Y. Zhou, $(2n, 2n, 2n, 1)$-relative difference sets and their representations. J. Combin. Des. 21 (2013), no. 12, 563–584.

[16] Y. Zhou, Difference Sets from Projective Planes. PhD-Thesis, OvGU Magdeburg (2013).

[17] Y. Zheng, X-M. Zhang, On plateaued functions, IEEE Trans. Inform. Theory 47 (2001), no. 3, 1215–1223.