Shifted plateaued functions and their differential properties

Canan Kaşıkcı
(joint work with Nurdagül Anbar, Wilfried Meidl and Alev Topuzoğlu)

Sabancı University, İstanbul

16 - 21 June 2019, BFA

Recall: A Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is called bent if $|\mathcal{W}_f(u)| = 2^{n/2}$ for all $u \in \mathbb{V}_n$, where

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{V}_n} (-1)^{f(x)+\langle u,x \rangle}$$

where the inner product $\langle u, x \rangle = \mathrm{Tr}(ux)$ if $\mathbb{V}_n = \mathbb{F}_{2^n}$, and $\langle u, x \rangle = u \cdot x$ if $\mathbb{V}_n = \mathbb{F}_2^n$.

f is bent $\iff D_a(f) := f(x+a) + f(x)$ is balanced for all nonzero $a \in \mathbb{V}_n$.

Recall: A Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is called bent if $|\mathcal{W}_f(u)| = 2^{n/2}$ for all $u \in \mathbb{V}_n$, where

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{V}_n} (-1)^{f(x)+\langle u,x \rangle}$$

where the inner product $\langle u, x \rangle = \mathrm{Tr}(ux)$ if $\mathbb{V}_n = \mathbb{F}_{2^n}$, and $\langle u, x \rangle = u \cdot x$ if $\mathbb{V}_n = \mathbb{F}_2^n$.

f is bent $\iff D_a(f) := f(x+a) + f(x)$ is balanced for all nonzero $a \in \mathbb{V}_n$.

Recall: For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ the unitary transform $\mathcal{U}_f^c : \mathbb{F}_2^n \to \mathbb{C}$ is defined as

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

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

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

Definition:

f is called *c-bent$_4$* if $|\mathcal{U}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$ for some $c \in \mathbb{F}_2^n$.

f is *c-bent$_4$* $\iff \mathcal{D}_a^c(f) := f(x+a) + f(x) + c \cdot (a \odot x)$ is balanced for every nonzero $a \in \mathbb{F}_2^n$, where $a \odot x := (a_1 x_1, \ldots, a_n x_n)$.

Recall: For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ the unitary transform $\mathcal{U}_f^c : \mathbb{F}_2^n \to \mathbb{C}$ is defined as

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

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

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

Definition:

f is called *c-bent*$_4$ if $|\mathcal{U}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$ for some $c \in \mathbb{F}_2^n$.

f is *c-bent*$_4$ $\iff \mathcal{D}_a^c(f) := f(x+a) + f(x) + c \cdot (a \odot x)$ is balanced for every nonzero $a \in \mathbb{F}_2^n$, where $a \odot x := (a_1 x_1, \ldots, a_n x_n)$.

Recall: For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ the unitary transform $\mathcal{U}_f^c : \mathbb{F}_2^n \to \mathbb{C}$ is defined as

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

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

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

Definition:

f is called *c-bent*$_4$ if $|\mathcal{U}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$ for some $c \in \mathbb{F}_2^n$.

f is *c-bent*$_4$ $\iff \mathcal{D}_a^c(f) := f(x+a) + f(x) + c \cdot (a \odot x)$ is balanced for every nonzero $a \in \mathbb{F}_2^n$, where $a \odot x := (a_1 x_1, \ldots, a_n x_n)$.

Recall: For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ the unitary transform $\mathcal{V}_f^c : \mathbb{F}_{2^n} \to \mathbb{C}$ is defined by

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

where $i = \sqrt{-1}$, the function $\mathrm{Tr}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$ and $\sigma^c(x)$ is defined by

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

Definition:

f is called *c-bent*$_4$ if $|\mathcal{V}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}$.

f is *c-bent*$_4$ $\iff \mathcal{D}_a^c(f) := f(x+a) + f(x) + \mathrm{Tr}(c^2ax)$ is balanced $\forall a \in \mathbb{F}_{2^n}^*$.

Recall: For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ the unitary transform $\mathcal{V}_f^c : \mathbb{F}_{2^n} \to \mathbb{C}$ is defined by

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

where $i = \sqrt{-1}$, the function $\mathrm{Tr}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$ and $\sigma^c(x)$ is defined by

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

Definition:

f is called *c-bent$_4$* if $|\mathcal{V}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}$.

f is *c-bent$_4$* $\iff \mathcal{D}_a^c(f) := f(x+a) + f(x) + \mathrm{Tr}(c^2 ax)$ is balanced $\forall a \in \mathbb{F}_{2^n}^*$.

Recall: For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ the unitary transform $\mathcal{V}_f^c : \mathbb{F}_{2^n} \to \mathbb{C}$ is defined by

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

where $i = \sqrt{-1}$, the function $\mathrm{Tr}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$ and $\sigma^c(x)$ is defined by

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

Definition:

f is called *c-bent₄* if $|\mathcal{V}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}$.

f is *c-bent*$_4$ $\iff \mathcal{D}_a^c(f) := f(x+a) + f(x) + \mathrm{Tr}(c^2ax)$ is balanced $\forall a \in \mathbb{F}_{2^n}^*$.

Remarks:

- For $c = 0$ respectively $c = (0, \ldots, 0)$, $\mathcal{V}_f^c(u)$ respectively $\mathcal{U}_f^c$ is the conventional *Walsh transform* $\mathcal{W}_f(u)$.
- A 1-bent$_4$ function is called a *negabent function*.
- 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 a *negabent function*. Using $\sigma^c(c^{-1}x) = \sigma^1(x)$, one can get $\mathcal{V}_f^c(u) = \mathcal{V}_{\tilde{f}}^1(c^{-1}u)$.
- $\mathcal{V}_f^c(u)$ is defined to describe the component functions of modified planar functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, i.e. functions for which $F(x + a) + F(x) + ax$ is a permutation of $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*$.

Theorem (Parker, Pott, 2007; Stănică et al., 2013; Su et al, 2013; Zhou, 2013):

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

- For n even, f is c-bent$_4$ $\iff f + s_2^c$ is bent.
- For n odd, f is c-bent$_4$ $\iff f + s_2^c$ is semibent, i.e. $\mathcal{W}_{f+s_2^c}(u) \in \{0, \pm 2^{(n+1)/2}\}$, and $\mathcal{W}_{f+s_2^c}(u)\mathcal{W}_{f+s_2^c}(u+c) = 0$ for all $u \in \mathbb{F}_2^n$.

Theorem (Anbar, Meidl, 2017):

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

- For n even, f is c-bent$_4$ $\iff f + \sigma^c(x)$ is bent.
- For n odd, f is c-bent$_4$ $\iff f + \sigma^c(x)$ is semibent, i.e. $\mathcal{W}_{f+\sigma^c(x)}(u) \in \{0, \pm 2^{(n+1)/2}\}$, and $\mathcal{W}_{f+\sigma^c(x)}(u)\mathcal{W}_{f+\sigma^c(x)}(u+c) = 0$ for all $u \in \mathbb{F}_{2^n}$.

Definition: $f : \mathbb{V}_n \to \mathbb{F}_2$ is *s-plateaued* if, for all $u \in \mathbb{V}_n$, $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$.

Definition: A function f is called *partially bent* if $D_a(f)$ is either balanced or constant for all $a \in \mathbb{V}_n$.

- $\Lambda(f) = \{a \in \mathbb{V}_n | D_a(f) \text{ is constant}\}$: the linear space of f.
- f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Lambda(f))$.

Definition: $f : \mathbb{V}_n \to \mathbb{F}_2$ is *s-plateaued* if, for all $u \in \mathbb{V}_n$, $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$.

Definition: A function f is called *partially bent* if $D_a(f)$ is either balanced or constant for all $a \in \mathbb{V}_n$.

- $\Lambda(f) = \{a \in \mathbb{V}_n | D_a(f) \text{ is constant}\}$: the linear space of f.
- f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Lambda(f))$.

Definition: $f : \mathbb{V}_n \to \mathbb{F}_2$ is *s-plateaued* if, for all $u \in \mathbb{V}_n$, $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$.

Definition: A function f is called *partially bent* if $D_a(f)$ is either balanced or constant for all $a \in \mathbb{V}_n$.

- $\Lambda(f) = \{a \in \mathbb{V}_n | D_a(f) \text{ is constant}\}$: the linear space of f.
- f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Lambda(f))$.

Definition: $f : \mathbb{V}_n \to \mathbb{F}_2$ is *s-plateaued* if, for all $u \in \mathbb{V}_n$, $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$.

Definition: A function f is called *partially bent* if $D_a(f)$ is either balanced or constant for all $a \in \mathbb{V}_n$.

- $\Lambda(f) = \{a \in \mathbb{V}_n | D_a(f) \text{ is constant}\}$: the linear space of f.
- f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Lambda(f))$.

Definition: $f : \mathbb{V}_n \to \mathbb{F}_2$ is *s-plateaued* if, for all $u \in \mathbb{V}_n$, $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$.

Definition: A function f is called *partially bent* if $D_a(f)$ is either balanced or constant for all $a \in \mathbb{V}_n$.

- $\Lambda(f) = \{a \in \mathbb{V}_n | D_a(f) \text{ is constant}\}$: the linear space of f.
- f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Lambda(f))$.

Definition:

$f : \mathbb{V}_n \to \mathbb{F}_2$ is *c-s-plateaued* if $|\mathcal{V}_f^c(u)|$ $(|\mathcal{U}_f^c(u)|) \in \{0, 2^{(n+s)/2}\}$ for all $u \in \mathbb{V}_n$.

Definition:

$f : \mathbb{V}_n \to \mathbb{F}_2$ is *partially c-bent$_4$* if $\mathcal{D}_a^c(f)$ is constant or balanced for all $a \in \mathbb{V}_n$.

Theorem (Anbar, Meidl, 2017):

- $\Lambda_c(f) = \{a \in \mathbb{V}_n \,|\, \mathcal{D}_a^c(f) \text{ is constant}\}$ is a subspace of $\mathbb{V}_n$.
- Every partially c-bent$_4$ function is *c-s-plateaued* for some integer s where $s = \dim(\Lambda_c(f))$.

Definition:

$f : \mathbb{V}_n \to \mathbb{F}_2$ is *c-s-plateaued* if $|\mathcal{V}_f^c(u)|$ $(|\mathcal{U}_f^c(u)|) \in \{0, 2^{(n+s)/2}\}$ for all $u \in \mathbb{V}_n$.

Definition:

$f : \mathbb{V}_n \to \mathbb{F}_2$ is *partially c-bent$_4$* if $\mathcal{D}_a^c(f)$ is constant or balanced for all $a \in \mathbb{V}_n$.

Theorem (Anbar, Meidl, 2017):

- $\Lambda_c(f) = \{a \in \mathbb{V}_n \,|\, \mathcal{D}_a^c(f) \text{ is constant}\}$ is a subspace of $\mathbb{V}_n$.
- Every partially c-bent$_4$ function is *c-s-plateaued* for some integer s where $s = \dim(\Lambda_c(f))$.

Definition:

$f : \mathbb{V}_n \to \mathbb{F}_2$ is *c-s-plateaued* if $|\mathcal{V}_f^c(u)|$ $(|\mathcal{U}_f^c(u)|) \in \{0, 2^{(n+s)/2}\}$ for all $u \in \mathbb{V}_n$.

Definition:

$f : \mathbb{V}_n \to \mathbb{F}_2$ is *partially c-bent$_4$* if $\mathcal{D}_a^c(f)$ is constant or balanced for all $a \in \mathbb{V}_n$.

Theorem (Anbar, Meidl, 2017):

- $\Lambda_c(f) = \{a \in \mathbb{V}_n \,|\, \mathcal{D}_a^c(f) \text{ is constant}\}$ is a subspace of $\mathbb{V}_n$.
- Every partially c-bent$_4$ function is *c-s-plateaued* for some integer s where $s = \dim(\Lambda_c(f))$.

Question: What happens when we shift plateaued/partially bent functions?

LEMMA:

Let $f : \mathbb{V}_n \to \mathbb{F}_2$ and $c \in \mathbb{V}_n$ be arbitrary. We have

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

where

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

Thus $\dim(\Lambda_c(f)) = \dim(\Lambda(f + \tilde{\sigma}^c))$ or $\dim(\Lambda_c(f)) = \dim(\Lambda(f + \tilde{\sigma}^c)) - 1$.

Lemma:

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

Theorem (Anbar, K., Meidl, Topuzoğlu):

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 functions g and f satisfy exactly one of the following additional properties.

(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 at all.

Recall: A (m, n, k, λ)-*relative difference set* R in a group G of order mn, relative to a subgroup B of G of order n, is a k-elementary subset 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 λ ways, and there is no such representation for any nonzero element in B. The subgroup B is called the *forbidden subgroup*.

If $G = A \times B$, then R is called a *splitting relative difference set.*

Recall: f is bent $\Longleftrightarrow$ the graph of f, $\mathcal{G}_f := \{(x, f(x)) : x \in \mathbb{V}_n\}$ is a $(2^n, 2, 2^n, 2^{n-1})$ splitting RDS in $\mathbb{V}_n \times \mathbb{F}_2$ with the forbidden subgroup $\{0\} \times \mathbb{F}_2$.

- Let $(\mathbb{V}_n \times \mathbb{F}_2, *_c)$ be the group, where $*_c$ is defined by

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

  and

  $$(x_1, y_1) *_c (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + c \cdot (x_1 \odot x_2)) \text{ if } \mathbb{V}_n = \mathbb{F}_2^n.$$

  Note that $(\mathbb{V}_n \times \mathbb{F}_2, *_c) \cong \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$ for $c \in \mathbb{V}_n \setminus \{0\}$.

- $f : \mathbb{V}_n \mapsto \mathbb{F}_2$ is c-bent$_4$ $\iff$ $\mathcal{G}_f = \{(x, f(x)) : x \in \mathbb{V}_n\}$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $(\mathbb{V}_n \times \mathbb{F}_2, *_c)$ relative to $\{0\} \times \mathbb{F}_2$.

Theorem (Anbar, K., Meidl, Topuzoğlu):

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

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

(1) $g \in G \setminus B$ can be represented as $r_1 - r_2$, for $r_1, r_2 \in R$ in exactly λ 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.

Theorem (Anbar, K., Meidl, Topuzoğlu):

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

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

(1) $g \in G \setminus B$ can be represented as $r_1 - r_2$, for $r_1, r_2 \in R$ in exactly λ 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.

Thank you!