Spectra and Equivalence of Boolean Functions

Nurdagül Anbar
(joint work with Wilfried Meidl and Alexander Pott)

RICAM, Linz, Austria

4-10 June 2017, Fq13

Outline

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 $c = 0$, $\mathcal{V}_f^c(u)$ is the conventional *Walsh transform* $\mathcal{W}_f(u)$.

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 $c = 0$, $\mathcal{V}_f^c(u)$ is the conventional *Walsh transform* $\mathcal{W}_f(u)$.

Remarks:

- $\mathcal{V}_f^c(u)$ is defined to describe the component functions of a 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 permutation of $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*$. (Zhou, 2013)

- (Sarkar, 2012) $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a *negabent function* if $f(x+a) + f(x) + \mathrm{Tr}(ax)$ is balanced for any $a \in \mathbb{F}_{2^n}^*$. This is equivalent c-bent$_4$ function for $c = 1$.

  Fact: (A., Meidl, 2016) A function f is c-bent$_4$ $\iff$ $f(x+a) + f(x) + \mathrm{Tr}(c^2 ax)$ is balanced $\forall a \in \mathbb{F}_{2^n}^*$

Remarks:

- $\mathcal{V}_f^c(u)$ is defined to describe the component functions of a 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 permutation of $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*$. (Zhou, 2013)

- (Sarkar, 2012) $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a *negabent function* if $f(x+a) + f(x) + \mathrm{Tr}(ax)$ is balanced for any $a \in \mathbb{F}_{2^n}^*$. This is equivalent c-bent$_4$ function for $c = 1$.

  Fact: (A., Meidl, 2016) A function f is c-bent$_4$ $\iff$ $f(x+a) + f(x) + \mathrm{Tr}(c^2 ax)$ is balanced $\forall a \in \mathbb{F}_{2^n}^*$

- Let $G_c := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ be the group, where "$*$" is defined by

$$(x_1, y_1) * (x_2, y_2) = \big(x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(c^2 x_1 x_2)\big)$$

for any $(x_1, y_1), (x_2, y_2) \in G_c$. Note that $G_c \cong \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$ for $c \neq 0$.
Define $\mathcal{G}_f := \{(x, f(x)) : x \in \mathbb{F}_{2^n}\} \subset G_c$.

Fact: f is c-bent$_4$ $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in G_c.

Recall: f is bent $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $\mathbb{Z}_2^{n+1}$.

Definition: Let $D_a(f) := f(x + a) + f(x)$. A function f is called *partially bent* if $D_a(f)$ is either balanced or constant.

Fact: $\Omega(f) = \{a \in \mathbb{F}_{2^n} | D_a(f) \text{ is constant}\}$: the linear space of f

f is partially bent $\Longrightarrow$ $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Omega(f))$

- Let $G_c := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ be the group, where "$*$" is defined by

$$(x_1, y_1) * (x_2, y_2) = \big(x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(c^2 x_1 x_2)\big)$$

for any $(x_1, y_1), (x_2, y_2) \in G_c$. Note that $G_c \cong \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$ for $c \neq 0$.
Define $\mathcal{G}_f := \{(x, f(x)) : x \in \mathbb{F}_{2^n}\} \subset G_c$.

Fact: f is c-bent$_4$ $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in G_c.

Recall: f is bent $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $\mathbb{Z}_2^{n+1}$.

Definition: Let $D_a(f) := f(x+a) + f(x)$. A function f is called *partially bent* if $D_a(f)$ is either balanced or constant.

Fact: $\Omega(f) = \{a \in \mathbb{F}_{2^n} | D_a(f) \text{ is constant}\}$: the linear space of f

f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Omega(f))$

- Let $G_c := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ be the group, where "$*$" is defined by

$$(x_1, y_1) * (x_2, y_2) = \big(x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(c^2 x_1 x_2)\big)$$

for any $(x_1, y_1), (x_2, y_2) \in G_c$. Note that $G_c \cong \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$ for $c \neq 0$.
Define $\mathcal{G}_f := \{(x, f(x)) : x \in \mathbb{F}_{2^n}\} \subset G_c$.

Fact: f is c-bent$_4$ $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in G_c.

Recall: f is bent $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $\mathbb{Z}_2^{n+1}$.

Definition: Let $D_a(f) := f(x + a) + f(x)$. A function f is called *partially bent* if $D_a(f)$ is either balanced or constant.

Fact: $\Omega(f) = \{a \in \mathbb{F}_{2^n} | D_a(f) \text{ is constant}\}$: the linear space of f

f is partially bent $\Longrightarrow$ $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Omega(f))$

- Let $G_c := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ be the group, where "$*$" is defined by

$$(x_1, y_1) * (x_2, y_2) = \left(x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(c^2 x_1 x_2)\right)$$

for any $(x_1, y_1), (x_2, y_2) \in G_c$. Note that $G_c \cong \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$ for $c \neq 0$.
Define $\mathcal{G}_f := \{(x, f(x)) : x \in \mathbb{F}_{2^n}\} \subset G_c$.

Fact: f is c-bent$_4$ $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in G_c.

Recall: f is bent $\Longleftrightarrow$ $\mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $\mathbb{Z}_2^{n+1}$.

Definition: Let $D_a(f) := f(x+a) + f(x)$. A function f is called *partially bent* if $D_a(f)$ is either balanced or constant.

Fact: $\Omega(f) = \{a \in \mathbb{F}_{2^n} | D_a(f) \text{ is constant}\}$: the linear space of f

f is partially bent $\Longrightarrow \mathcal{W}_f(u) \in \{0, \pm 2^{(n+s)/2}\}$, $s := \dim(\Omega(f))$

Lemma:

$\Omega_c(f) = \{a \in \mathbb{F}_{2^n} \mid D_a(f) + \mathrm{Tr}(c^2ax) \text{ is constant}\}$ is a subspace of $\mathbb{F}_{2^n}$.

Definition: f is called *c-partially bent* if $D_a(f) + \mathrm{Tr}(c^2ax)$ is constant or balanced for all $a \in \mathbb{F}_{2^n}$.

Proposition:

If f is a c-partially bent then $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$, where $s_c = \dim(\Omega_c(f))$.

Definition/Fact: A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is represented by $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$.

Corollary:

f is quadratic $\Longrightarrow \mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$ for some $s_c \geq 0$.

Lemma:

$\Omega_c(f) = \{a \in \mathbb{F}_{2^n} \mid D_a(f) + \mathrm{Tr}(c^2ax)$ is constant$\}$ is a subspace of $\mathbb{F}_{2^n}$.

Definition: f is called *c-partially bent* if $D_a(f) + \mathrm{Tr}(c^2ax)$ is constant or balanced for all $a \in \mathbb{F}_{2^n}$.

Proposition:

If f is a c-partially bent then $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$, where $s_c = \dim(\Omega_c(f))$.

Definition/Fact: A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is represented by $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$.

Corollary:

f is quadratic $\Longrightarrow \mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$ for some $s_c \geq 0$.

Lemma:

$\Omega_c(f) = \{a \in \mathbb{F}_{2^n} \mid D_a(f) + \mathrm{Tr}(c^2ax) \text{ is constant}\}$ is a subspace of $\mathbb{F}_{2^n}$.

Definition: f is called *c-partially bent* if $D_a(f) + \mathrm{Tr}(c^2ax)$ is constant or balanced for all $a \in \mathbb{F}_{2^n}$.

Proposition:

If f is a c-partially bent then $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$, where $s_c = \dim(\Omega_c(f))$.

Definition/Fact: A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is represented by $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$.

Corollary:

f is quadratic $\implies \mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$ for some $s_c \geq 0$.

Lemma:

$\Omega_c(f) = \{a \in \mathbb{F}_{2^n} \mid D_a(f) + \mathrm{Tr}(c^2 ax) \text{ is constant}\}$ is a subspace of $\mathbb{F}_{2^n}$.

Definition: f is called *c-partially bent* if $D_a(f) + \mathrm{Tr}(c^2 ax)$ is constant or balanced for all $a \in \mathbb{F}_{2^n}$.

Proposition:

If f is a c-partially bent then $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$, where $s_c = \dim(\Omega_c(f))$.

Definition/Fact: A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is represented by $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$.

Corollary:

f is quadratic $\implies \mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$ for some $s_c \geq 0$.

Lemma:

$\Omega_c(f) = \{a \in \mathbb{F}_{2^n} \mid D_a(f) + \mathrm{Tr}(c^2ax) \text{ is constant}\}$ is a subspace of $\mathbb{F}_{2^n}$.

Definition: f is called *c-partially bent* if $D_a(f) + \mathrm{Tr}(c^2ax)$ is constant or balanced for all $a \in \mathbb{F}_{2^n}$.

Proposition:

If f is a c-partially bent then $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$, where $s_c = \dim(\Omega_c(f))$.

Definition/Fact: A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is represented by $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$.

Corollary:

f is quadratic $\Longrightarrow \mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+s_c)/2}\}$ for some $s_c \geq 0$.

Question: What is the spectra of a quadratic function f with respect to $\mathcal{V}_f^c$ while c varies?

For $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$, set
$h(T) := \sum_{i=0}^{\lfloor n/2 \rfloor} b_i T^{2^i} + b_i^{2^{n-i}} T^{2^{n-i}}$

$$\begin{aligned} a \in \Omega_c(f) &\iff f(x+a) + f(x) + \mathrm{Tr}(c^2 a x) = 0 \\ &\iff a \in \mathrm{Ker}(h(T) + c^2 T) =: K_c \end{aligned}$$

Lemma:

$\mathbb{F}_{2^n} = \cup_{c \in \mathbb{F}_{2^n}} K_c$ with $K_{c_1} \cap K_{c_2} = \{0\}$ for $c_1 \neq c_2$.

Optimal: $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+1)/2}\}$, i.e. $\dim(K_c) = 1$, for all $c \in \mathbb{F}_{2^n}$ but one!

This holds $\iff h(T)/T$ is a permutation.

Proposition:

$h(T)/T$ is not a permutation.

Question: What is the spectra of a quadratic function f with respect to $\mathcal{V}_f^c$ while c varies?

For $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$, set
$h(T) := \sum_{i=0}^{\lfloor n/2 \rfloor} b_i T^{2^i} + b_i^{2^{n-i}} T^{2^{n-i}}$

$$a \in \Omega_c(f) \iff f(x+a) + f(x) + \mathrm{Tr}(c^2 a x) = 0$$
$$\iff a \in \mathrm{Ker}(h(T) + c^2 T) =: K_c$$

Lemma:

$\mathbb{F}_{2^n} = \cup_{c \in \mathbb{F}_{2^n}} K_c$ with $K_{c_1} \cap K_{c_2} = \{0\}$ for $c_1 \neq c_2$.

Optimal: $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+1)/2}\}$, i.e. $\dim(K_c) = 1$, for all $c \in \mathbb{F}_{2^n}$ but one!

This holds $\iff h(T)/T$ is a permutation.

Proposition:

$h(T)/T$ is not a permutation.

Question: What is the spectra of a quadratic function f with respect to $\mathcal{V}_f^c$ while c varies?

For $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$, set
$h(T) := \sum_{i=0}^{\lfloor n/2 \rfloor} b_i T^{2^i} + b_i^{2^{n-i}} T^{2^{n-i}}$

$$a \in \Omega_c(f) \iff f(x+a) + f(x) + \mathrm{Tr}(c^2 ax) = 0$$
$$\iff a \in \mathrm{Ker}(h(T) + c^2 T) =: K_c$$

Lemma:

$\mathbb{F}_{2^n} = \cup_{c \in \mathbb{F}_{2^n}} K_c$ with $K_{c_1} \cap K_{c_2} = \{0\}$ for $c_1 \neq c_2$.

Optimal: $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+1)/2}\}$, i.e. $\dim(K_c) = 1$, for all $c \in \mathbb{F}_{2^n}$ but one!

This holds $\iff$ $h(T)/T$ is a permutation.

Proposition:

$h(T)/T$ is not a permutation.

Question: What is the spectra of a quadratic function f with respect to $\mathcal{V}_f^c$ while c varies?

For $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$, set
$h(T) := \sum_{i=0}^{\lfloor n/2 \rfloor} b_i T^{2^i} + b_i^{2^{n-i}} T^{2^{n-i}}$

$$a \in \Omega_c(f) \iff f(x+a) + f(x) + \mathrm{Tr}(c^2 ax) = 0$$
$$\iff a \in \mathrm{Ker}(h(T) + c^2 T) =: K_c$$

Lemma:

$\mathbb{F}_{2^n} = \cup_{c \in \mathbb{F}_{2^n}} K_c$ with $K_{c_1} \cap K_{c_2} = \{0\}$ for $c_1 \neq c_2$.

Optimal: $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+1)/2}\}$, i.e. $\dim(K_c) = 1$, for all $c \in \mathbb{F}_{2^n}$ but one!

This holds $\iff$ $h(T)/T$ is a permutation.

Proposition:

$h(T)/T$ is not a permutation.

Question: What is the spectra of a quadratic function f with respect to $\mathcal{V}_f^c$ while c varies?

For $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$, set
$h(T) := \sum_{i=0}^{\lfloor n/2 \rfloor} b_i T^{2^i} + b_i^{2^{n-i}} T^{2^{n-i}}$

$$a \in \Omega_c(f) \iff f(x+a) + f(x) + \mathrm{Tr}(c^2 a x) = 0$$
$$\iff a \in \mathrm{Ker}(h(T) + c^2 T) =: K_c$$

Lemma:

$\mathbb{F}_{2^n} = \cup_{c \in \mathbb{F}_{2^n}} K_c$ with $K_{c_1} \cap K_{c_2} = \{0\}$ for $c_1 \neq c_2$.

Optimal: $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+1)/2}\}$, i.e. $\dim(K_c) = 1$, for all $c \in \mathbb{F}_{2^n}$ but one!

This holds $\iff h(T)/T$ is a permutation.

Proposition:

$h(T)/T$ is not a permutation.

Question: What is the spectra of a quadratic function f with respect to $\mathcal{V}_f^c$ while c varies?

For $f(x) = \mathrm{Tr}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} b_i x^{2^i+1}\right)$, set
$h(T) := \sum_{i=0}^{\lfloor n/2 \rfloor} b_i T^{2^i} + b_i^{2^{n-i}} T^{2^{n-i}}$

$$a \in \Omega_c(f) \iff f(x+a) + f(x) + \mathrm{Tr}(c^2 ax) = 0$$
$$\iff a \in \mathrm{Ker}(h(T) + c^2 T) =: K_c$$

Lemma:

$\mathbb{F}_{2^n} = \cup_{c \in \mathbb{F}_{2^n}} K_c$ with $K_{c_1} \cap K_{c_2} = \{0\}$ for $c_1 \neq c_2$.

Optimal: $\mathcal{V}_f^c(u) \in \{0, \pm 2^{(n+1)/2}\}$, i.e. $\dim(K_c) = 1$, for all $c \in \mathbb{F}_{2^n}$ but one!

This holds $\iff$ $h(T)/T$ is a permutation.

Proposition:

$h(T)/T$ is not a permutation.

Corollary:

A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is c-bent$_4$ for at least three distinct $c \in \mathbb{F}_{2^n}$.

Lemma:

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

- A function f is c-bent$_4$ if and only if $f + \sigma(c, x)$ is bent.
- A function f is c-bent$_4$ if and only if $f(dx)$ is cd-bent$_4$.

Theorem (A., Meidl, 2017):

For n even, any quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is essentially *bent–negabent*. (Sarkar 2012)

Corollary:

A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is c-bent$_4$ for at least three distinct $c \in \mathbb{F}_{2^n}$.

Lemma:

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

- A function f is c-bent$_4$ if and only if $f + \sigma(c, x)$ is bent.
- A function f is c-bent$_4$ if and only if $f(dx)$ is cd-bent$_4$.

Theorem (A., Meidl, 2017):

For n even, any quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is essentially *bent–negabent.* (Sarkar 2012)

Corollary:

A quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is c-bent$_4$ for at least three distinct $c \in \mathbb{F}_{2^n}$.

Lemma:

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

- A function f is c-bent$_4$ if and only if $f + \sigma(c, x)$ is bent.
- A function f is c-bent$_4$ if and only if $f(dx)$ is cd-bent$_4$.

Theorem (A., Meidl, 2017):

For n even, any quadratic function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is essentially *bent–negabent.* (Sarkar 2012)

Theorem (A., Meidl, 2017):

(1) Let $f(x) = \mathrm{Tr}(\alpha x^3)$ for some $\alpha \in \mathbb{F}_{2^n}$.

- If n be odd, then f is c-bent$_4$ for $(2^n + 1)/3$ different $c \in \mathbb{F}_{2^n}$, 1 partially c-bent$_4$ for 2^{n-1} different $c \in \mathbb{F}_{2^n}$ and 2 partially c-bent$_4$ for $(2^{n-1} - 1)/3$ different $c \in \mathbb{F}_{2^n}$.
- For n is even, let ζ be the primitive root of unity and N_i be the number of trace zero elements in $Q_i := \zeta^i(\mathbb{F}_{2^n}^*)^3$ for $i = 1, 2, 3$. If $\alpha \in Q_i$, then f is c-bent$_4$ for $2N_i + 1$ different $c \in \mathbb{F}_{2^n}$, 1 partially c-bent$_4$ for $2^n - -3N_i$ different $c \in \mathbb{F}_{2^n}$ and 2 partially c-bent$_4$ for N_i different $c \in \mathbb{F}_{2^n}$.

(2) Let $n = 2k$ and $f(x) = \mathrm{Tr}(\alpha x^{2^k})$ for some $\alpha \in \mathbb{F}_{2^n}$.

- If $\alpha \notin \mathbb{F}_{2^k}$, then f c-bent$_4$ for $2^n - 2^k - 1$ different $c \in \mathbb{F}_{2^n}$ and k partially c-bent$_4$ for $2^k + 1$ different $c \in \mathbb{F}_{2^n}$.
- If $\alpha \in \mathbb{F}_{2^k}$, then $f = 0$, and hence c-bent$_4$ for all $c \in \mathbb{F}_{2^n}$.

Theorem (A., Meidl, 2017):

Let $n = 2k$, $k > 1$ odd, and let $f(x) = \mathrm{Tr}(x^{2^k+3})$. Then f is negabent and not c-bent$_4$ for any $c \neq 1$.

Remark: (2016) Zhou and Qu show that $n = 2k$, $k > 1$ odd, $f(x) = \mathrm{Tr}(x^{2^k+3})$ is negabent. Moreover, by MAGMA, for $n \leq 14$ the monomial $f(x) = \mathrm{Tr}(\gamma x^{2^k+3})$ is negabent only for $\gamma = 1$.

Corollary:

For $n = 2k$ and $k > 1$ odd, $f(x) = \mathrm{Tr}(\gamma x^{2^k+3})$ is negabent only for $\gamma = 1$.

Recall: A function f is c-bent$_4$ if and only if $f(dx)$ is cd-bent$_4$.

Theorem (A., Meidl, 2017):

Let $n = 2k$, $k > 1$ odd, and let $f(x) = \mathrm{Tr}(x^{2^k+3})$. Then f is negabent and not c-bent$_4$ for any $c \neq 1$.

Remark: (2016) Zhou and Qu show that $n = 2k$, $k > 1$ odd, $f(x) = \mathrm{Tr}(x^{2^k+3})$ is negabent. Moreover, by MAGMA, for $n \leq 14$ the monomial $f(x) = \mathrm{Tr}(\gamma x^{2^k+3})$ is negabent only for $\gamma = 1$.

Corollary:

For $n = 2k$ and $k > 1$ odd, $f(x) = \mathrm{Tr}(\gamma x^{2^k+3})$ is negabent only for $\gamma = 1$.

Recall: A function f is c-bent$_4$ if and only if $f(dx)$ is cd-bent$_4$.

Theorem (A., Meidl, 2017):

Let $n = 2k$, $k > 1$ odd, and let $f(x) = \mathrm{Tr}(x^{2^k+3})$. Then f is negabent and not c-bent$_4$ for any $c \neq 1$.

Remark: (2016) Zhou and Qu show that $n = 2k$, $k > 1$ odd, $f(x) = \mathrm{Tr}(x^{2^k+3})$ is negabent. Moreover, by MAGMA, for $n \leq 14$ the monomial $f(x) = \mathrm{Tr}(\gamma x^{2^k+3})$ is negabent only for $\gamma = 1$.

Corollary:

For $n = 2k$ and $k > 1$ odd, $f(x) = \mathrm{Tr}(\gamma x^{2^k+3})$ is negabent only for $\gamma = 1$.

Recall: A function f is c-bent$_4$ if and only if $f(dx)$ is cd-bent$_4$.

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

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

Recall: For $c \neq 0$, f is c-bent$_4$ $\iff \mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $G_c \equiv \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$.

We consider $c = 1$ and set $\sigma(x) := \sigma(1, x)$.
$G := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ such that for any $(x_1, y_1), (x_2, y_2) \in G$, $(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(x_1 x_2))$.

Definition: Let f_1 and f_2 be negabent (1-bent$_4$) functions.

- f_1 and f_2 are *shifted-equivalent* if $f_1 + \sigma$ and $f_2 + \sigma$ are EA-equivalent, i.e. $(f_2 + \sigma)(x) = (f_1 + \sigma)(\mathcal{L}(x) + \alpha) + \mathrm{Tr}(\beta x) + c$ for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$.
- f_1 and f_2 are *difference set equivalent* if $\mathcal{G}_{f_1}$ and $\mathcal{G}_{f_2}$ are equivalent as an RDS, i.e. $\mathcal{G}_{f_2} = \psi(\mathcal{G}_{f_1}) * b$ for some $\psi \in \mathrm{Aut}(G)$ and $b \in G$.

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

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

Recall: For $c \neq 0$, f is c-bent$_4$ $\iff \mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $G_c \equiv \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$.

We consider $c = 1$ and set $\sigma(x) := \sigma(1, x)$.
$G := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ such that for any $(x_1, y_1), (x_2, y_2) \in G$, $(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(x_1 x_2))$.

Definition: Let f_1 and f_2 be negabent (1-bent$_4$) functions.

- f_1 and f_2 are *shifted-equivalent* if $f_1 + \sigma$ and $f_2 + \sigma$ are EA-equivalent, i.e. $(f_2 + \sigma)(x) = (f_1 + \sigma)(\mathcal{L}(x) + \alpha) + \mathrm{Tr}(\beta x) + c$ for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$.
- f_1 and f_2 are *difference set equivalent* if $\mathcal{G}_{f_1}$ and $\mathcal{G}_{f_2}$ are equivalent as an RDS, i.e. $\mathcal{G}_{f_2} = \psi(\mathcal{G}_{f_1}) * b$ for some $\psi \in \mathrm{Aut}(G)$ and $b \in G$.

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

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

Recall: For $c \neq 0$, f is c-bent$_4$ $\iff \mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $G_c \equiv \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$.

We consider $c = 1$ and set $\sigma(x) := \sigma(1, x)$.
$G := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ such that for any $(x_1, y_1), (x_2, y_2) \in G$,
$(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(x_1 x_2))$.

Definition: Let f_1 and f_2 be negabent (1-bent$_4$) functions.

- f_1 and f_2 are *shifted-equivalent* if $f_1 + \sigma$ and $f_2 + \sigma$ are EA-equivalent, i.e.
  $(f_2 + \sigma)(x) = (f_1 + \sigma)(\mathcal{L}(x) + \alpha) + \mathrm{Tr}(\beta x) + c$ for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$.
- f_1 and f_2 are *difference set equivalent* if $\mathcal{G}_{f_1}$ and $\mathcal{G}_{f_2}$ are equivalent as an RDS, i.e. $\mathcal{G}_{f_2} = \psi(\mathcal{G}_{f_1}) * b$ for some $\psi \in \mathrm{Aut}(G)$ and $b \in G$.

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

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

Recall: For $c \neq 0$, f is c-bent$_4$ $\iff \mathcal{G}_f$ is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in $G_c \equiv \mathbb{Z}_2^{n-1} \times \mathbb{Z}_4$.

We consider $c = 1$ and set $\sigma(x) := \sigma(1, x)$.
$G := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ such that for any $(x_1, y_1), (x_2, y_2) \in G$,
$(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \mathrm{Tr}(x_1 x_2))$.

Definition: Let f_1 and f_2 be negabent (1-bent$_4$) functions.

- f_1 and f_2 are *shifted-equivalent* if $f_1 + \sigma$ and $f_2 + \sigma$ are EA-equivalent, i.e.
  $(f_2 + \sigma)(x) = (f_1 + \sigma)(\mathcal{L}(x) + \alpha) + \mathrm{Tr}(\beta x) + c$ for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$.
- f_1 and f_2 are *difference set equivalent* if $\mathcal{G}_{f_1}$ and $\mathcal{G}_{f_2}$ are equivalent as an RDS, i.e. $\mathcal{G}_{f_2} = \psi(\mathcal{G}_{f_1}) * b$ for some $\psi \in \mathrm{Aut}(G)$ and $b \in G$.

Definition: Ω: the set of linearized permutations $\mathcal{L}$ of $\mathbb{F}_{2^n}$ such that $\mathrm{Tr}(x) = \mathrm{Tr}(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$.

Proposition (A., Meidl, Pott, 2017):

Let $\psi_{\mathcal{L},\beta} : \mathbb{F}_{2^n} \times \mathbb{F}_2 \to \mathbb{F}_{2^n} \times \mathbb{F}_2$ defined by

$$\psi_{\mathcal{L},\beta}(x, y) = (\,\mathcal{L}(x)\,,\ y + \sigma(x) + \sigma(\mathcal{L}(x)) + \mathrm{Tr}(\beta x)\,)\ .$$

Then

$$\mathrm{Aut}(G) = \{\psi_{\mathcal{L},\beta} \,|\, \mathcal{L} \in \Omega,\ \beta \in \mathbb{F}_{2^n}\}\ .$$

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

Theorem (A., Meidl, Pott, 2017):

Negabent functions f_1 and f_2 are difference set equivalent if and only if

$$f_2(x) = f_1(x) + \sigma(x) + \sigma(\mathcal{L}(x)) + \mathrm{Tr}(\beta x) + c$$

for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_2$ and $\mathcal{L}(x) \in \Omega$.

Definition: Ω: the set of linearized permutations $\mathcal{L}$ of $\mathbb{F}_{2^n}$ such that $\mathrm{Tr}(x) = \mathrm{Tr}(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$.

Proposition (A., Meidl, Pott, 2017):

Let $\psi_{\mathcal{L},\beta} : \mathbb{F}_{2^n} \times \mathbb{F}_2 \to \mathbb{F}_{2^n} \times \mathbb{F}_2$ defined by

$$\psi_{\mathcal{L},\beta}(x,y) = (\, \mathcal{L}(x)\,,\, y + \sigma(x) + \sigma(\mathcal{L}(x)) + \mathrm{Tr}(\beta x)\,)\ .$$

Then

$$\mathrm{Aut}(G) = \{\psi_{\mathcal{L},\beta} \,|\, \mathcal{L} \in \Omega,\ \beta \in \mathbb{F}_{2^n}\}\ .$$

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

Theorem (A., Meidl, Pott, 2017):

Negabent functions f_1 and f_2 are difference set equivalent if and only if

$$f_2(x) = f_1(x) + \sigma(x) + \sigma(\mathcal{L}(x)) + \mathrm{Tr}(\beta x) + c$$

for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_2$ and $\mathcal{L}(x) \in \Omega$.

$f_1(x)$ —shifting to bent→ $g_1(x) = f_1(x) + \sigma(x)$

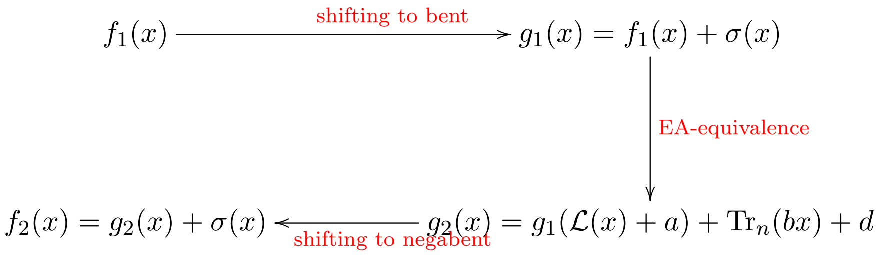
↓ EA-equivalence

$f_2(x) = g_2(x) + \sigma(x)$ ←shifting to negabent— $g_2(x) = g_1(\mathcal{L}(x) + a) + \mathrm{Tr}_n(bx) + d$

Observation:
Difference set equivalence $\Longrightarrow$ shifted equivalence

Question: Is the converse true?

Theorem (A., Meidl, Pott, 2017):
Two EA-equivalent functions can induce inequivalent different sets in G.



Observation:

Difference set equivalence $\Longrightarrow$ shifted equivalence

Question: Is the converse true?

Theorem (A., Meidl, Pott, 2017):

Two EA-equivalent functions can induce inequivalent different sets in G.

$$f_1(x) \xrightarrow{\text{shifting to bent}} g_1(x) = f_1(x) + \sigma(x)$$

$$\Big\downarrow \text{ EA-equivalence}$$

$$f_2(x) = g_2(x) + \sigma(x) \xleftarrow[\text{shifting to negabent}]{} g_2(x) = g_1(\mathcal{L}(x) + a) + \mathrm{Tr}_n(bx) + d$$

Observation:

Difference set equivalence $\Longrightarrow$ shifted equivalence

Question: Is the converse true?

Theorem (A., Meidl, Pott, 2017):

Two EA-equivalent functions can induce inequivalent different sets in G.

$$f_1(x) \xrightarrow{\text{shifting to bent}} g_1(x) = f_1(x) + \sigma(x)$$

$$\big\downarrow \ \text{EA-equivalence}$$

$$f_2(x) = g_2(x) + \sigma(x) \xleftarrow[\text{shifting to negabent}]{} g_2(x) = g_1(\mathcal{L}(x) + a) + \mathrm{Tr}_n(bx) + d$$

Observation:

Difference set equivalence $\Longrightarrow$ shifted equivalence

Question: Is the converse true?

Theorem (A., Meidl, Pott, 2017):

Two EA-equivalent functions can induce inequivalent different sets in G.

Grazie per l'attenzione!