Relation between o-equivalence and EA-equivalence for Niho bent functions

Diana Davidova
University of Bergen

join work with
Lilya Budaghyan, Claude Carlet, Tor Helleseth,
Ferdinand Ihringer, Tim Penttila

BFA–2019
Florence, Italy
June 16 - 21, 2019

Notation and preliminaries

$\mathbb{F}_{2^n}$ is a field with 2^n elements, $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$.

- **Trace function**
  A mapping $Tr_r^k : \mathbb{F}_{2^k} \mapsto \mathbb{F}_{2^r}$, defined in the following way:

$$Tr_k^r(x) = \Sigma_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$$

  for any $k, r \in \mathbb{Z}^+$, such that k is dividing by r.
  For $r = 1$, Tr_1^k is called the absolute trace:

$$Tr_1^k(x) = Tr_k(x) = \Sigma_{i=0}^{k-1} x^{2^i}.$$

Notation and preliminaries

Boolean function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$.

- **Walsh transformation**
  is a Fourier transformation of $\chi_f = (-1)^f$, whose value is defined by:
  $$\widehat{\chi_f}(w) = \Sigma_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_n(wx)},$$
  at point $w \in \mathbb{F}_{2^n}$.
- **The Hamming distance**
  $f, g : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$, $d_H(f,g) = |\{x \in \mathbb{F}_{2^n} | f(x) \neq g(x)\}|$.
- **Nonlinearity**
  $\mathcal{NL}(f) = min_{l \in A_n} d_H(f,l)$, where
  $A_n = \{l : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2 | l = Tr_n(ax) + b, a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_2\}$.
  High nonlinearity prevents cryptosystem from linear attacks and correlation attacks.

Bent functions

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in F_{2^n}} \widehat{\chi_f}(a).$$

$$\mathcal{NL}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

The $\mathcal{NL}(f)$ reach the upper bound only for even n.

- **Bent function**
  A boolean function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ (n is even), if $\mathcal{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, equivalently if $\widehat{\chi_f}(w) = \pm 2^{\frac{n}{2}}$ for any $w \in \mathbb{F}_{2^n}$.
- Boolean functions f and g are called **EA-equivalent**, if there exist an affine authomorphism A and an affine Boolean function l s.t. $f = g \circ A + l$.

Niho Bent Functions

- A positive integer d (understood modulo $2^n - 1$ with $n = 2m$) is a **Niho exponent** and $t \mapsto t^d$, is a **Niho power function**, if the restriction of t^d to $\mathbb{F}_{2^m}$ is linear, i.e. $d \equiv 2^j (mod\ 2^m - 1)$ for some $j < n$.

Example

Niho bent functions

1. Quadratic functions $Tr_m(at^{2^m+1}), a \in \mathbb{F}^*_{2^m}$;
2. Binomilas of the form $f(t) = Tr_n(\alpha_1 t_1^{d_1} + \alpha_2 t_2^{d_2})$, where $\alpha_1, \alpha_2 \in F_{2^n}$, $d_1 = (2^m - 1)\frac{1}{2} + 1$, and d_2 can be: $(2^m - 1)3 + 1$, $(2^m - 1)\frac{1}{4} + 1$ (m is odd), $(2^m - 1)\frac{1}{6} + 1$(m is even).
3. For $r > 1$ with $gcd(r, m) = 1$
$f(x) = Tr_n\left(a^2 t^{2^m+1} + (a + a^{2^m}) \sum_{i=1}^{2^{r-1}-1} t^{d_i}\right)$,
where $2^r d_i = (2^m - 1)i + 2^r$, $a \in \mathbb{F}_{2^n}$ s.t. $a + a^{2^m} \neq 0$.

Class $\mathcal{H}$ of bent functions[1]

Niho bent functions in the univariant representation are functions in the following class $\mathcal{H}$:

$$g(x,y) = \begin{cases} Tr_m\left(xG\left(\frac{y}{x}\right)\right), \text{ if } x \neq 0; \\ Tr_m(\mu y), \text{ if } x = 0, \end{cases}$$

where $\mu \in \mathbb{F}_{2^m}$, $G : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ satisfying the following conditions:

$$F : z \mapsto G(z) + \mu z \text{ is a permutation over } \mathbb{F}_{2^m} \quad (1)$$

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}_{2^m}^*. \quad (2)$$

Condition (2) implies condition (1) and it necessary and sufficient for g being bent. Functions in $\mathcal{H}$ and a class of functions introduced by Dillon in 1974 are the same up to addition a linear term.

[1] *C. Carlet, S.Mesnager "On Dillons class H of bent functions, Niho bent functions and o-polynomials", J.Combin.Theory Ser. A, vol. 118, no. 8, pp.2392-2410, 2010.*

o-polynomials

A polynomial $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is called an $o-$**polynomial**, if

1. F is a permutational polynomial satisfies $F(0) = 0, F(1) = 1$;
2. the function $F_s(x) = \begin{cases} 0, & \text{if } x = 0, \\ \frac{F(x+s)+F(s)}{x} & \text{if } x \neq 0 \end{cases}$
   is a permutation for each $s \in \mathbb{F}^*_{2^m}$.

Theorem

A polynomial F defined on F_{2^m} such that $F(0) = 0$, $F(1) = 1$ is an $o-$polynomial, iff

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}^*_{2^m}.$$

Every o-polynomial defines a Niho bent function and vice versa.

Vectorial Niho bent functions

Let F be an o-polynomial defined on $\mathbb{F}_{2^m}$. Then o-polynomial $G = A_1 \circ F \circ A_2$ defines Niho bent function EA-equivalent to F, if

1. $A_1(x) = \frac{1}{F(b)}x, A_2(x) = bx$;
2. $A_1(x)$ is an automorphism over $\mathbb{F}_{2^m}$ and $A_2 = A_1^{-1}$,
3. $A_1(x) = x + a$ and $A_2(x) = x + b$ for $a, b \in \mathbb{F}_{2^m}$, $b = F(a)$ and $F(a+1) + F(a) = 1$.

Note that from 1. easily follows that every o-polynomial on $\mathbb{F}_{2^m}$ defines a vectorial Niho bent function $xF(\frac{y}{x})$ from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.[2]

[2] S. Mesnager. Bent vectorial functions and linear codes from o-polynomials. *Journal Designs, Codes and Cryptography*. 77(1), pages 99-116, 2015

The list of known o-polynomials

1. $F(x) = x^{2^i}$, $gcd(i, m) = 1$,
2. $F(x) = x^6$, m is odd,
3. $F(x) = x^{3\cdot 2^k+4}$, $m = 2k - 1$,
4. $F(x) = x^{2^k+2^{2k}}$, $m = 4k - 1$,
5. $F(x) = x^{2^{2k+1}+2^{3k+1}}$, $m = 4k + 1$,
6. $F(x) = x^{2^k} + x^{2^k+2} + x^{3\cdot 2^k+4}$, $m = 2k - 1$,
7. $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$, m is odd.
8. $F(x) = \frac{1}{Tr_m^n}(v)\Big(Tr_m^n(v^r)(x+1)+(x+Tr_m^n(v)x^{\frac{1}{2}}+1)^{1-r}Tr_m^n(vx+v^{2^m})^r\Big)+x^{\frac{1}{2}}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}, v^{2^m+1} \neq 1, v \neq 1$,
9. $F(x) = x^4 + x^{16} + x^{28} + \omega^{11}(x^6 + x^{10} + x^{14} + x^{18} + x^{22} + x^{26}) + \omega^{20}(x^8 + x^{20}) + \omega^6(x^{12} + x^{24})$ with $\omega^5 = \omega^2 + 1$.

o-equivalence

Niho bent functions are **o-equivalent** if the corresponding o-polynomials are equivalent.

o-equivalent Niho bent functions defined by o-polynomials F and F^{-1} can be EA-inequivalent .

o-equivalent Niho bent functions

$\mathcal{F}$ is the collection of all o-polynomials defined on $\mathbb{F}_{2^m}$ and
$< H >=< \{\tilde{\sigma_a}, \tilde{\tau_c}, \varphi, \rho_{2^j} | 0 \leq j \leq m-1, c \in \mathbb{F}_{2^m}, a \in \mathbb{F}_{2^m}^*\} >$ is a group of transformations acting on $\mathcal{F}$ as follow

$$\tilde{\sigma}_a F(x) = \frac{1}{F(a)} F(ax),\ a \in \mathbb{F}_{2^m}^*;$$

$$\tilde{\tau}_c F(x) = \frac{1}{F(1+c)+F(c)}(F(x+c)+F(c)) = \alpha_F^c(F(x+c)+F(c)),\ c \in \mathbb{F}_{2^m},$$

$$\varphi F(x) = F'(x) = xF(x^{-1});$$

$$\rho_{2^j} F(x) = F^{2^j}(x^{2^{-j}}),\ 0 \leq j \leq m-1.$$

Proposition

Two o-polynomials are equivalent if and only if they lie on the same orbit of the action of the group generated by H and the inverse map.

Simplest transformation

Theorem

Let F be an o-polynomial. Then an o-polynomial $\bar{F}$ obtained from F using one transformation from H and the inverse map can produce a Niho bent function EA-inequivalent to those defined by F and F^{-1} only if $\bar{F} = (F')^{-1}$.

General transformation

Let i be a positive integer and $k_i \geq 0$. Denote by H_i a composition of length k_i of generators φ and $\tilde{\tau}_c$ as follows:

$$H_i = \underbrace{\varphi \circ \tilde{\tau}_{c_{i_1}} \circ \varphi \circ \tilde{\tau}_{c_{i_2}} \circ \dots}_{k_i} \tag{1}$$

where $c_{i_j} \in \mathbb{F}_{2^m}$.

Theorem

Let F be an o-polynomial, g_F the corresponding Niho bent function and G_F the class of all functions o-equivalent to g_F. Then o-polynomials of the form

$$(H_1(H_2(H_3(\dots(H_qF)^{-1}\dots)^{-1})^{-1})^{-1}, \tag{2}$$

where H_i is defined by (1), for all $i \in \{1 \dots q\}$, $q \geq 1$, and $k_i \geq 1$ for $i \geq 3$, $k_i \geq 0$ for $i \leq 2$, provide representatives for all EA-equivalence classes within G_F. That is, up to EA-equivalence, all Niho bent functions o-equivalent to g_F arise from (2).

Some particular cases of formula (2)

- For $q = 1$ and $k_1 = 2$:
  $F_c^{\circ}(x) = (\varphi \circ \tau_c F)^{-1}(x) = \left(\alpha_F^c x\left(F\left(\frac{1}{x} + c\right) + F(c)\right)\right)^{-1}, \quad c \in \mathbb{F}_{2^m}.$
  For $c = 0$ $F_c^{\circ} = (F^{'})^{-1}$.
  F_c° defines a sequence of Niho bent functions $g_{F_c^{\circ}}$ potentially EA-inequivalent to each other for different c, and EA-inequivalent to Niho bent functions defined by F, F^{-1}.
- For $q = 1$ and $k_1 = 3$:
  $(F_c^{*})^{-1} = (\varphi \circ \tau_c \circ \varphi F)^{-1}(x) = \left(\alpha_{F'}^c\left((1 + cx)F\left(\frac{x}{1+cx}\right) + cxF\left(\frac{1}{c}\right)\right)\right)^{-1}$,
  $c \in \mathbb{F}_{2^m}$.
  For $c = 0$, $(F_c^{*})^{-1} = F^{-1}$.
  Niho bent functions $g_{(F_c^{*})^{-1}}$ can potentially be EA-inequivalent to each other for different c and EA-inequivalent to Niho bent functions defined by F, F_c°.

The case of o-monomials

Lemma

For an o-monomial $F(x) = x^d$, the Niho bent functions defined by $F_c{}^\circ$ and $F_1{}^\circ$ are EA-equivalent, for any $c \in \mathbb{F}_{2^m}^*$.

Lemma

For an o-monomial $F(x) = x^d$, the Niho bent functions defined by $(F_c{}^*)^{-1}$, $(F^*)_1^{-1}$ and $F_1{}^\circ$ are EA-equivalent, for $c \in \mathbb{F}_{2^m}^*$.

The case of o-monomials

Lemma

Let F be an o-monomial. Then for $q \geq 3$

$$(H_1(H_2(\ldots(H_q F)^{-1}\ldots)^{-1})^{-1} = \begin{cases} \beta\tau_1 G^{-1}; \\ \gamma(\varphi \circ \tau_1 G)^{-1}; \\ \eta\varphi \circ \tau_1 G, \end{cases}$$

where $G \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$, $\beta, \gamma, \eta \in \mathbb{F}_{2^m}^*$ and H_i are defined by (1) for all i .

Proposition

For each o-monomials o-equivalence can give at most 4 EA-inequivalent functions. For an o-monomial F the 4 potentially EA-inequivalent bent functions are defined by F, F^{-1}, $(F')^{-1}$ and F_1°.

Proposition

For Frobenius map o-equivalence gives exactly 3 EA-inequivalent functions corresponding to F, F^{-1}, $(F')^{-1}$.

$F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$

Proposition

For o-polynomial $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$ o-equivalence can give EA-inequivalent Niho bent functions corresponding to o-polynomials F and F_c°, $c \in \mathbb{F}_{2^m}^*$.

Example

For $m = 5$ we checked computationally that the o-polynomial $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$ over $\mathbb{F}_{2^m}$ defines 6 EA-inequivalent Niho bent functions corresponding to o-polynomials F, $F^{-1} = F_0^\circ$ and $F_w^\circ, F_{w^3}^\circ, F_{w^5}^\circ$, where w is a primitive element of $\mathbb{F}_{2^m}$.

Example

$F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$ gives $\frac{3m+2^{m-1}-1}{m}$ EA-inequivalent Niho bent functions over the field $F_{2^{2m}}$ with prime m.
For $m = 7$ (12), $m = 11$ (96), $m = 13$ (318), $m = 17$ (3858) and so on.

The case of other o-polynomials

For Subiaco, Adelaide and $x^{2^k} + x^{2^k+2} + x^{3\cdot 2^k+4}$ o-polinomials F o-equivalence can give a sequence of EA-inequivalent functions defined by o-polynomials on the orbits F, F^{-1}, F_c°, $(\tilde{\tau}_{c_1} F)_{c_2}^{\circ}$, $(\tilde{\tau}_{c_1}(F'))_{c_2}^{\circ}$ and so on.

Example

From o-polynomial $x^{2^k} + x^{2^k+2} + x^{3\cdot 2^k+4}$ we obtain $\frac{4m+2^m-2}{m}$ EA-inequivalent Niho bent functions over the field $F_{2^{2m}}$ with prime m.
For $m = 7$ (22) $m = 11$ (190), $m = 13$ (634), $m = 17$ (7714) and so on.

Thank You! :-)