Magic action of $o-$polynomials and $EA-$equivalence of Niho bent functions

Diana Davidova

BFA - 2018
Loen, Norway
June 17 - 22, 2018

Notation and preliminaries

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

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

  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:

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

Boolean function $f\colon F_2^n \mapsto F_2$.

- Univariant representation
  Identify F_2^n with F_{2^n}. There exists the unique representation of f:

$$f(x) = \Sigma_{i=0}^{2^n-1} a_i x^i.$$

The degree of Boolean function is the maximum $w_2(i)$ of the exponents in its univariant representation.
Also Boolean function f can be written uniquely in the following univariant trace form:

$$f(x) = \Sigma_{j\in\Gamma_n} Tr_{o(j)} a_j x^j + a_{2^n-1} x^{2^n-1},$$

where Γ_n is the set of integers obtained by choosing the smallest element in each cyclotomic coset modulo $2^n - 1$ with respect to 2,
$o(j)$ is the size of cyclotomic coset containing j,
$a_j \in F_{2^{o(j)}}$, $a_{2^n-1} \in F_2$.

- Bivariant representation(for even n)
  F_2^n can be identified with $F_{2^m} \times F_{2^m} (n = 2m)$ and the argument of f is considered as an ordered pair (x, y), $x, y \in F_{2^m}$.Then there is the unique representation of f over F_{2^m}:

  $$f(x) = \Sigma_{0 \le i,j \le 2^m - 1} a_{i,j} x^i y^j.$$

  The algebraic degree of f is $\max_{i,j | a_{i,j} \neq 0}((w_2(i) + w_2(j))$.
  Bivariant representation of f in trace form:

  $$f(x, y) = Tr_m(P(x, y)),$$

  where $P(x, y)$ is some polynomialof 2 variables over F_{2^m}.

Bent functions

- **Walsh transformation**
  is a Fourier transformation of $\chi_f = (-1)^f$, whose value is defined by:
  $$\widehat{\chi_f}(w) = \Sigma_{x \in F_{2^n}} (-1)^{f(x)+Tr_n(wx)},$$
  at point $w \in F_{2^n}$.
- **The Hamming distance**
  $f, g : F_{2^n} \mapsto F_2$, $d_H(f, g) = |\{x \in F_{2^n} | f(x) \neq g(x)\}|$.
- **Nonlinearity**
  $\mathcal{NL}(f) = min_{l \in A_n} d_H(f, l)$, where
  $A_n = \{l : F_{2^n} \mapsto F_2 | l = a \cdot x + b, a \in F_{2^n}, b \in F_2\}$.
  High nonlinearity prevents the system from linear attacks and correlation attacks.

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

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

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

- **Bent function**
  A boolean function $f\colon F_{2^n} \mapsto F_2$ (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 $w \in F_{2^n}$.

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 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 $Tr_m(at^{2^m+1}), a \in F_{2^m} \setminus \{0\}$;
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 $2^r d_i = (2^m - 1)i + 2^r$, $a \in F_{2^n}$ s.t. $a + a^{2^m} \neq 0$.

Dillon's class H of bent functions[1].

The functions in this class are defined in their bivariant form:

$$f(x, y) = Tr_m(y + xF(yx^{2^m-2})),$$

where $x, y \in F_{2^m}$,

- F is a permutation of F_{2^m} s.t. $F(x) + x$ doesn't vanish
- for any $\beta \in F_{2^m} \setminus \{0\}$ the function $F(x) + \beta x$ is 2-to-1.

[1] *J.F.Dillon, "Elementary Hadamard difference sets", Ph.D. dissertation, Univ. Maryland, College Park. MD,USA,1974.*

Class $\mathcal{H}$ of bent functions[2]

This class H was modified into a class $\mathcal{H}$ of the functions:

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

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

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

$$z \mapsto F(z)+\beta z \text{ is 2-to-1 on } F_{2^m} \text{ for any } \beta \in F_{2^m}\setminus\{0\}. \qquad (2)$$

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

---

[2] *C. Carlet, M.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 $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ 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 $s \in \mathbb{F}_{2^n}$.

If we do not require $F(1) = 1$, then F is called $o-$**permutation**.

Theorem

A polynomial F defined on F_{2^m} is an $o-$polynomial, iff

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } F_{2^m} \text{ for any } \beta \in F_{2^m} \setminus \{0\}.$$

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

The list of known o-polynomials:

1. $F(z) = z^{2^i}$, $gcd(i, m) = 1$,
2. $F(z) = z^6$, m is odd,
3. $F(z) = z^{3\cdot 2^k+4}$, $m = 2k - 1$,
4. $F(z) = z^{2^k+2^{2k}}$, $m = 4k - 1$,
5. $F(z) = z^{2^{2k+1}+2^{3k+1}}$, $m = 4k + 1$,
6. $F(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$, $m = 2k - 1$,
7. $F(z) = z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$, m is odd.

Hyperovals

A hyperoval of the projective plane $PG(2, 2^m)$ is a set of $2^m + 2$ points no three of which are collinear.
There is a one-to-one correspondence between $o-$polynomials and *hyperovals*.
Any hyperoval $\mathcal{O}$ can be represented in the form:

$$\{(x, F(x), 1) | x \in F_{2^m}\} \cup \{(1, 0, 0), (0, 1, 0)\},$$

where F is an $o-$polynomial.
And conversly, for any $o-$polynomial F the set

$$\{(x, F(x), 1) | x \in F_{2^m}\} \cup \{(1, 0, 0), (0, 1, 0)\}$$

defines a hyperoval.

- hyperovals are called equivalent if they are mapped to each other by collineation(a permutation of a point set of $PG(2, 2^m)$ mapping lines to lines)).
- o-polynomials F_1 and F_2 are **projectively equivalent**, if F_1 and F_2 define equivalent hyperovals.
- Niho bent functions are **o-equivalent** if they define projectively equivalent o-polynomials.
- Boolean functions f and g are called **EA-equivalent**, if there exist an affine authomorphism A and an affine Boolean function l s.t. $f = g \circ A + l$.
  o-equivalent Niho bent fuctions defined by o-polynomials F and F^{-1} can be EA-inequivalent .[2]

Magic Action[3]

The following set

$$P\Gamma L(2,2^m) = \{x \mapsto Ax^{2^j} | A \in GL(2, F_{2^m}), 1 \leq j \leq m-1\}$$

is a group of transformations acting on the the projective line.
The Magic action is an action of the group $P\Gamma L(2,2^m)$ on the set $\mathcal{F}$ of $o-$permutations, defined in the following way:

$$\psi F(x) = |A|^{-\frac{1}{2}}\left[(bx+d)F^{2^j}\left(\frac{ax+c}{bx+d}\right) + bxF^{2^j}\left(\frac{a}{b}\right) + dF^{2^j}\left(\frac{c}{d}\right)\right],$$

where $1 \leq j \leq n-1$, $\psi : x \mapsto Ax^{2^j}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,2^m)$, $F \in \mathcal{F}$.

The magic action

- is a semi-linear transformation.
- takes $o-$permutations to $o-$permutations.

[3] *C.M.O'Keefe, T. Penttila, Automorphisms groups of generalized quadrangles via an unusual action of* $P\Gamma L(2;2^h)$, *Europ.J.Combinatorics (2002) 23, 213-232.*

The magic action can be also determined by the magic action of a collection of generators of $P\Gamma L(2, 2^m)$:

$\sigma_a : x \mapsto \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} x,\ \sigma_a F(x) = a^{-\frac{1}{2}} F(ax),\ a \in \mathbb{F}_{2^m} \setminus \{\emptyset\};$

$\tau_c : x \mapsto \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} x,\ \tau_c F(x) = F(x+c) + F(c),\ c \in \mathbb{F}_{2^m};$

$\phi : x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x,\ \phi F(x) = xF(x^{-1});$

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

Consider slightly modified generators of the magic action:

$$\tilde{\sigma}_a F(x) = \frac{a^{\frac{1}{2}}}{F(a)} \sigma_a F(x),\ a \in \mathbb{F}_{2^m} \setminus \{\emptyset\};$$
$$\tilde{\tau}_c F(x) = \frac{1}{F(1+c)+F(c)} \tau_c F(x),\ c \in \mathbb{F}_{2^m},$$
$$\phi F(x) = xF(x^{-1});$$
$$\tilde{\rho}_{2^j} F(x) = F^{2^j}(x^{2^j}),\ 1 \leq j \leq m-1.$$

The group G defined by new generators preserve condition $F(1) = 1$ of F and takes $o-$polynomials to $o-$polynomials.
The modified Magic Action geneators together with the inverse map acting on $o-$ polynomials give projectively equivalent $o-$polynomials, but they can lead to EA-inequivalent Niho bent functions.

For $o-$polynomial F the only constraction which can lead to Niho bent functions $EA-$ inequivalent to those defined by F and F^{-1} is :

$$(\phi \circ g\, F)^{-1},$$

where $g \in < G >$.
It was checked that for $o-$polynomial F Niho bent functions potentaially EA-inequivalent to those defined by F and F^{-1} may arise from $o-$polynomials :

1. $(\phi F)^{-1} = (xF(x^{-1}))^{-1} = (F\,')^{-1}(x)$;
2. $(\phi \circ \tilde{\tau}_c F)^{-1}(x) = ((\tau_c F)\,')^{-1}(x) = \Big(\alpha x((F((\alpha x)^{-1} + c) + F(c))\Big)^{-1} = F_c^{\circ}$, where $\alpha = F(1+c) + F(c)$;
3. $(\phi \circ \tilde{\tau}_c \circ \phi F)^{-1}(x) = ((\tau_c F\,')\,')^{-1}(x) = \Big((c\alpha x + 1)F\Big(\frac{\alpha x}{c\alpha x+1}\Big) + c\alpha x F(c^{-1})\Big)^{-1} = (F_c^{*})^{-1}$, where $\alpha = F(1+c) + F(c)$.

"L.Budaghyan, C.Carlet, T.Helleseth, A.Kholosha, "On o-equivalence of Niho Bent functions",WAIFI 2014, Lecture Notes in Comp. Sci. 9061, pp. 155- 168,2015"