Niho bent functions and o-equivalence

Diana Davidova
University of Bergen

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

5-10 May 2019
COINS Winter School
Finse, Norway

Introduction

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.

Group of 24 transformations acting on o-polynomials;
Only 4 of them can lead to EA-inequivalent Niho bent functions .

Notation and preliminaries

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

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

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

- Univariant representation
  Identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$. 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.
  affine, if the degree ≤ 1.

- Bivariant representation(for even n)
  $\mathbb{F}_2^n$ can be identified with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}(n = 2m)$ and the argument of f is considered as an ordered pair (x, y), $x, y \in \mathbb{F}_{2^m}$.Then there is the unique representation of f over $\mathbb{F}_{2^m}$:

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

  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 $\mathbb{F}_{2^m}$.

Bent functions

- **Walsh transformation**
  is a Fourier transformation of $\chi_f = (-1)^f$, whose value is defined by:

$$\widehat{\chi_f}(a) = \Sigma_{x \in F_{2^n}} (-1)^{f(x)+Tr_n(ax)},$$

  at point $a \in \mathbb{F}_{2^n}$.

- **The Hamming distance**
  $f, g : \mathbb{F}_{2^n} \mapsto F_2,\ d_H(f,g) = |\{x \in \mathbb{F}_{2^n} | f(x) \neq g(x)\}|.$

- **Nonlinearity**
  $\mathcal{NL}(f) = min_{l \in A_n} d_H(f, l)$, where
  $A_n = \{l : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2 | l = a \cdot x + b, a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_2\}.$
  High nonlinearity prevents the system from linear attacks and differential 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**
  $f: \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ (n is even), if

  $$\mathcal{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}-1},$$

  equivalently

  $$\widehat{\chi}_f(a) = \pm 2^{\frac{n}{2}}$$

  for any $a \in \mathbb{F}_{2^n}$.

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 $\mathbb{F}_{2^m}$ is linear, i.e. $d \equiv 2^j (mod\, 2^m-1)$ for some $j<n$.

Example

Niho bent functions

1. Quadratic functions $Tr_m(at^{2^m+1}), a \in \mathbb{F}_{2^m} \setminus \{0\}$;
2. Binomilas of the form $f(t) = Tr_n(\alpha_1 t_1^{d_1} + \alpha_2 t_2^{d_2})$, where $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}$, $d_1 = (2^m-1)\frac{1}{2}+1$, 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 $gcd(r,m)=1$ $f(x) = Tr_n\Big(a^2 t^{2^m+1} + (a+a^{2^m}) \sum_{i=1}^{2^{r-1}-1} t^{d_i}\Big)$, where $2^r d_i = (2^m-1)i + 2^r$, $a \in \mathbb{F}_{2^n}$ s.t. $a + a^{2^m} \neq 0$.

Dillon's class H of bent functions

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

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

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

where $x, y \in \mathbb{F}_{2^m}$,

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

Class $\mathcal{H}$ of bent functions

C. Carlet, S.Messenger "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, 2011.

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

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

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

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 $Tr_m((\mu+1)y)$.

Niho bent functions are functions in $\mathcal{H}$ in the univariant representation.

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 $s \in \mathbb{F}_{2^m}$.

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

Theorem

A polynomial F defined on $\mathbb{F}_{2^m}$ is an $o-$polynomial if and only if

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

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

The list of known o-polynomials on $\mathbb{F}_{2^m}$:

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.
8. $F(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2 z^2+1} + z^{\frac{1}{2}}$, where $Tr_m(\frac{1}{\delta}) = 1$ (if $m \equiv 2 \mod 4$, then $\delta \notin F_4$),
9. $F(z) =$ $\frac{1}{Tr_m^n}(v)\Big(Tr_m^n(v^r)(z+1) + (z + Tr_m^n(v)z^{\frac{1}{2}} + 1)^{1-r} Tr_m^n(vz + v^{2^m})^r\Big) + z^{\frac{1}{2}}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $v \in F_{2^{2m}}, v^{2^m+1} \neq 1, v \neq 1$

Projective plane

Let P be a set, which elements are called points, $L \subset 2^P$ called lines and $I \subseteq P \times L$ is a relation called relation of incidence.

Projective plane Π is a triple $(P, L; I)$ satisfies the following conditions:

1. any pair of distinct points are incident with exactly one line;
2. any pair of distinct lines is incident exactly with one point;
3. there exists four points no three of which are incident with the same line.

For any projective plane Π there exists an integer $q \geq 2$ such that

- Any point (line) of projective plane Π is incident exactly with $q + 1$ lines (points).
- A projective plane Π has exactly $q^2 + q + 1$ points (lines).

q is called **the dimension of projective plane** and Π is denoted by $PG(2, q)$.

For any $q = p^n$ (p is a prime number) there exists a projective plane.
Points which are incident with the same line are called **collinear**.
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 $\mathcal{H}$ can be represented in the form:

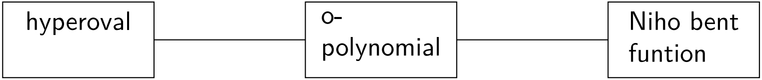
$$\{(x, f(x), 1) | x \in F_{2^m}\} \cup \{(1, 0, 0), (0, 1, 0)\},$$

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.

o-equivalence



- hyperovals are called **equivalent** if they are mapped to each other by a collineation (Colliniation is an authomorphism of projective plane which preserve incidentness.).
- o-polynomials are **projectively equivalent**, if they 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]

Modified magic action

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 23, pp.213-232, 2002.

Consider an action of a group $P\Gamma L(2, 2^m) = \{x \mapsto Ax^{2^j} | A \in GL(2, \mathbb{F}_{2^m}), 1 \leq j \leq m-1\}$ on the set of all o-polynomials, which can be described by a collection of generators $G = \{\tilde{\sigma}_a, \tilde{\tau}_c, \rho_{2^j}, \varphi | a \in F_{2^m} \setminus \{0\}, c \in F_{2^m}, 0 \leq j \leq m-1\}$:

$$\begin{aligned}
\tilde{\sigma}_a F(x) =& \frac{1}{F(a)} F(ax),\ a \in \mathbb{F}_{2^m} \setminus \{\emptyset\};\\
\tilde{\tau}_c F(x) =& \frac{1}{F(1+c)+F(c)} (F(x+c)+F(c)),\ c \in \mathbb{F}_{2^m},\\
\varphi F(x) =& xF(x^{-1});\\
\rho_{2^j} F(x) =& (F(x^{2^j}))^{2^{-j}},\ 0 \leq j \leq m-1.
\end{aligned}$$

Proposition

Two o-polynomials arise from equivalent hyperovals if and only if they lie on the same orbit under the modified magic action and the inverse map.

- Two o-poynomials are projectively equivalent if and only if the corresponding hyperovals lie on the same orbit under the modified magic action and the inverse map.
- Niho bent functions are o-equivalent iff the corresponding hyperovals lie on the same orbit under the modified magic action and the inverse map.

Theorem

For a given o-polynomial F, EA-inequivalent Niho bent functions can potentially arise from o-polynomials which lie on orbits of the modified magic action and the inverse map of the following form

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

where $H_i = \underbrace{\varphi \circ \tilde{\tau}_{c_{i_1}} \circ \varphi \circ \tilde{\tau}_{c_{i_2}} \circ \dots}_{k_i}$ *where* $i \in \{1, \dots q\}$.

- F is an o-monomial, then EA-inequivalent Niho bent functions can potentially arise from o-polynomials on the following 4 orbits

$$F, F^{-1}, (\varphi F)^{-1}, (\varphi \circ \tilde{\tau}_1 F)^{-1}.$$

$$(\varphi F)^{-1}(x) = (xF(\tfrac{1}{x}))^{-1},$$
$$F_1^{\circ} = (\varphi \circ \tilde{\tau}_1 F)^{-1} = \Big(x(F((\tfrac{1}{x} + 1) + 1)\Big)^{-1}.$$

- $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$, then *EA*-inequivalent Niho bent functions can potentially arise from o-polynomials on the following orbits

$$F, (\varphi \circ \tilde{\tau}_c F)^{-1}, c \in F_2^m.$$

$F_c^\circ(x) = (\varphi \circ \tilde{\tau}_c F)^{-1}(x) = \left(\frac{1}{F(1+c)+F(c)} x(F(\frac{1}{x} + c) + F(c))\right)^{-1}$, $c \in F_2^m$.

Example

$F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$, then o-polynomials F, $F_0^\circ = F^{-1}, F_\alpha^\circ, F_{\alpha^3}^\circ, F_{\alpha^5}^\circ$, where α is a primitive element of F_{2^5}.