On Niho Bent Functions and o-Polynomials

Alexander Kholosha
joint work with
L.Budaghyan, C.Carlet, T.Helleseth, S.Mesnager

Selmer Center, Department of Informatics, University of Bergen
Norway

5 September 2014

Boolean Functions - Representations

Multivariate representation

A Boolean function $f(x) : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ can be represented uniquely in Algebraic Normal Form(ANF)

$$f(x_1, x_2, \ldots, x_n) = \sum_{I \subset \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i, \quad a_I \in \mathbb{F}_2$$

Univariate representation

Alternatively, one can consider the Boolean function as a univariate function $f(x) : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$

$$f(x) = \sum_{i=0}^{2^n-1} b_i x^i = \mathrm{Tr}_n(F(x)), \quad b_i \in \mathbb{F}_{2^n}, b_{2i} = b_i^2$$

where $\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Bent Functions - Rothaus (1976)

Definition

Functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are *extended-affine equivalent* if there exist affine permutation L of $\mathbb{F}_2^n$ and an affine function $l : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $g(x) = (f \circ L)(x) + l(x)$. A class of functions is *complete* if it is a union of EA-equivalence classes. The *completed class* is the smallest possible complete class that contains the original one.

Definition (Walsh transform)

$f(x) : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ Inner product $x \cdot b = \sum_{i=1}^n x_i b_i (= \mathrm{Tr}_n(bx))$

$$\hat{f}(b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot b} \quad \left(or \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(F(x)+bx)}\right)$$

- $f(x)$ is a **bent function** iff $\hat{f}(b) = \pm 2^{n/2}$ for all $b \in \mathbb{F}_2^n$.
- Bent functions exist for **even** n only.
- **Dual bent function** $f^*(b)$ defined by $\hat{f}(b) = 2^{n/2}(-1)^{f^*(b)}$.

Maiorana-McFarland Construction

The best known construction of bent functions is the Maiorana-McFarland construction (not bivariate representation).

Definition

Let $n = 2m$.

Let $\pi : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$ be a *permutation*.
Let $g : \mathbb{F}_2^m \mapsto \mathbb{F}_2$ any mapping.

Then

$$f(x, y) = x \cdot \pi(y) + g(y), \quad x, y \in \mathbb{F}_2^m.$$

is a bent function in $n = 2m$ variable.

The dual of such a bent function is also a member of this class.

Representation in Bivariate Form

Let $n = 2m$ and consider $\mathbb{F}_2^n \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

$$f(x, y) = \sum_{0 \le i,j \le 2^m - 1} a_{ij} x^i y^j, \quad a_{ij} \in \mathbb{F}_{2^m}$$

Representing $f(x, y)$ in trace form

$$f(x, y) = \mathrm{Tr}_m(P(x, y))$$

for some polynomial $P(x, y)$ with coefficients in $\mathbb{F}_{2^m}$.

The Walsh transform becomes

$$\hat{f}(a, b) = \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{f(x,y) + \mathrm{Tr}_m(ax+by)}, \quad a, b \in \mathbb{F}_{2^m}.$$

Dillon's Class H

The bent functions in Dillon's class H are defined by

Definition

$$f(x, y) = \mathrm{Tr}_m(y + xF(yx^{2^m-2})), \quad x, y \in \mathbb{F}_{2^m}$$

where

- $F(x)$ is a permutation of $\mathbb{F}_{2^m}$.
- $F(x) + x$ does not vanish.
- $F(x) + \beta x$ is 2-to-1 for any $\beta \in \mathbb{F}^*_{2^m}$.

Dillon found only constructions in the Maiorana-McFarland class so this class has received less attention.

The Extension to Family $\mathcal{H}$

$$g(x,y) = \begin{cases} \mathrm{Tr}_m(xG(\frac{y}{x})) & \text{if} \quad x \neq 0 \\ \mathrm{Tr}_m(\mu y) & \text{if} \quad x = 0 \end{cases}$$

Note g is linear on $\{(x, ax) \mid x \in \mathbb{F}_{2^m}\}$ and $\{(0, y) \mid y \in \mathbb{F}_{2^m}\}$.

Theorem

The Walsh transform of $g(x,y)$ is

$$\hat{g}(\alpha,\beta) = \sum_{x,y} (-1)^{g(x,y)+\mathrm{Tr}_m(\alpha x+\beta y)} = \begin{cases} 2^m N_{\alpha,\beta} & \text{if } \beta = \mu \\ 2^m(N_{\alpha,\beta} - 1) & \text{if } \beta \neq \mu. \end{cases}$$

where $N_{\alpha,\beta} = |\{z \in \mathbb{F}_{2^m} \mid G(z) + \beta z + \alpha = 0\}|$.

Corollary

The function $g(x,y)$ is bent iff

- $F(z) = G(z) + \mu z$ *is a permutation of* $\mathbb{F}_{2^m}$.
- $F(z) + \beta z$ *is 2-to-1 on* $\mathbb{F}_{2^m}$ *for any* $\beta \in \mathbb{F}^*_{2^m}$.

Dual Bent Functions to Family $\mathcal{H}$

Theorem

The dual of $g(x, y)$ is

$$g^*(\alpha, \beta) = \begin{cases} 1 & \text{if } G(z) + \beta z = \alpha \text{ has no solution in } \mathbb{F}_{2^m} \\ 0 & \text{otherwise} \end{cases}$$

Problem

Find polynomial expressions for dual of bent functions in family $\mathcal{H}$. Expand the class $\mathcal{H}$ so it would contain also the dual functions.

Solved just for bent functions corresponding to Frobenius mappings. This dual does not belong to $\mathcal{H}$.

Family $\mathcal{H}$ and o-Polynomials

Definition

A permutation polynomial $F(z)$ over $\mathbb{F}_{2^m}$ is called an o-polynomial if $F(0) = 0$, $F(1) = 1$ and

$$\frac{F(z+\gamma)+F(\gamma)}{z}$$

is a permutation polynomial for all $\gamma \in \mathbb{F}_{2^m}$.

Theorem

A polynomial $F(z)$ over $\mathbb{F}_{2^m}$ is an o-polynomial iff $F(x)+\beta x$ is a 2-1 mapping for any $\beta \in \mathbb{F}_{2^m}^*$.

There is a close connection between hyperovals and o-polynomials. Maschietti used monomial hyperovals to construct new important difference sets.

Monomial o-Polynomials

- $F(z) = z^{2^i}$, where $(i, m) = 1$.
- $F(z) = z^6$, where m is odd. (Segre (1962))
- $F(z) = z^{2^k + 2^{2k}}$, where $m = 4k - 1$. (Glynn (1983))
- $F(z) = z^{2^{2k+1} + 2^{3k+1}}$, where $m = 4k + 1$. (Glynn (1983))
- $F(z) = z^{2^k + 2}$ with $m = 2k - 1$
- $F(z) = z^{2^{m-1} + 2^{m-2}}$ with m odd
- $F(z) = z^{3 \cdot 2^k + 4}$, where m is $2k - 1$. (Glynn (1983))

Example

To construct a bivariate bent function from $F(z) = z^6$ where m is odd:

$$g(x, y) = \mathrm{Tr}_m(y^6 x^{-5}).$$

o-Trinomials

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

Problem (Glynn conjecture)

No other o-monomials exist (up to o-equivalence).

Not all o-polynomials consist of a sum of o-monomials.

Subiaco o-Polynomials

Theorem (Cherowitzo, Penttila, Pinneri, and Royle 1996)

*If m **odd**, let $a = 1$*

$$f(z) = \frac{z^2 + z}{(z^2 + z + 1)^2} + z^{1/2} \text{ and } g(z) = \frac{z^4 + z^3}{(z^2 + z + 1)^2} + z^{1/2}.$$

If $m \equiv 2 \pmod 4$ and $\omega^2 + \omega + 1$, let $a = \omega$

$$f(z) = \frac{\omega z(z^2 + z + \omega^2)}{(z^2 + \omega z + 1)^2} + \omega^2 z^{1/2} \text{ and } g(z) = \frac{\omega z(z^2 + z + 1)}{z^2 + z + 1} + z^{1/2}.$$

Then $g(z)$ is an o-polynomial and

$$f_s(z) = \frac{f(z) + asg(z) + s^{1/2} z^{1/2}}{1 + as + s^{1/2}}$$

is an o-polynomial for any $s \in \mathbb{F}_{2^m}$.

Niho Bent Functions

Let $n = 2m$ then d is a Niho exponent if $d \equiv 2^i \pmod{2^m - 1}$.

Theorem (2006, 2012)

If $a = b^{2^m+1}$ then $f(t) = \mathrm{Tr}_m(at^{2^m+1}) + \mathrm{Tr}_n(bt^{d_2})$ is bent on $\mathbb{F}_{2^n}$ if

- $d_2 = (2^m - 1)3 + 1$
- $6d_2 = (2^m - 1) + 6$, *and m even.*

These functions have degree m and do not belong to the completed Maiorana-McFarland class.

Theorem (2006)

Take $0 < r < m$ with $\gcd(r, m) = 1$. Then

$$f(t) = \mathrm{Tr}_m(t^{2^m+1}) + \mathrm{Tr}_n\left(\sum_{i=1}^{2^{r-1}-1} t^{(2^{m-r}i+1)(2^m-1)+1}\right)$$

is a bent function of degree $r + 1$ and belongs to the completed Maiorana-McFarland class. The dual of f is not a Niho bent function.

Niho Equation

Assume that

$$d_i = (2^m - 1)s_i + 1 \quad (i = 1, \ldots, r)$$

are Niho exponents and

$$f(t) = \mathrm{Tr}_n\left(\sum_{i=1}^{r} \alpha_i t^{d_i}\right)$$

with $\alpha_i \in \mathbb{F}_{2^n}$. Then for every $c \in \mathbb{F}_{2^n}$ we have $\hat{f}(c) = (N(c) - 1)2^m$, where $N(c)$ is the number of $u \in \mathcal{S}$ such that

$$cu + \overline{cu} + \sum_{i=1}^{r}(\alpha_i u^{1-2s_i} + \overline{\alpha_i}\,\overline{u}^{1-2s_i}) = 0 \ ,$$

where $\overline{x} = x^{2^m}$ and $\mathcal{S} = \{u \in \mathbb{F}_{2^n} : u\overline{u} = 1\}$. In particular, f is bent if and only if $N(c) \in \{0, 2\}$.

Niho Bent Functions in 2-Variables

Niho bent function in univariate form ($t \in \mathbb{F}_{2^n}$, $n = 2m$)

$$f(t) = \mathrm{Tr}_n\Big(\sum_i \alpha_i t^{(2^m-1)s_i+1}\Big)$$

Niho bent function in bivariate form ($x, y \in \mathbb{F}_{2^m}$)

$$g(x,y) = f(ux+vy) \quad = \quad \mathrm{Tr}_m\Big(x\mathrm{Tr}_m^n\big(\sum_i \alpha_i (u + v\frac{y}{x})^{(2^m-1)s_i+1}\big)\Big)$$

$$g(x,y) = \begin{cases} \mathrm{Tr}_m(xG(\frac{y}{x})) & \text{if } x \neq 0 \\ \mathrm{Tr}_m(\mu y) & \text{if } x = 0. \end{cases}$$

- $G(z) = \mathrm{Tr}_m^n(\sum_i \alpha_i (u+vz)^{(2^m-1)s_i+1})$
- $\mu = \mathrm{Tr}_m^n(\sum_i \alpha_i v^{(2^m-1)s_i+1})$
- For a bent function $F(z) = G(z) + \mu z$ is an o-polynomial

Niho Polynomials with 2^{r-1} Terms (Frobenius)

Theorem (2011)

Let $r > 1$ *with* $\gcd(r, m) = 1$ *and*

$$f(t) = \mathrm{Tr}_m(t^{2^m+1}) + \mathrm{Tr}_n\Big(\sum_{i=1}^{2^{r-1}-1} t^{(2^{m-r}i+1)(2^m-1)+1}\Big).$$

Let $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ *and* $v \in \mathbb{F}_{2^m}$*. Then* $f(t)$ *belongs to* $\mathcal{H}$ *with* $\mu = v$ *and o-polynomial*

$$F(z)^{2^r} = (u + u^{2^m})^{2^r-1} vz + \frac{u^{2^m+2^r} + u^{2^{m+r}+1}}{u + u^{2^m}}.$$

Take $u + u^{2^m} = v = 1$ *then the dual of* $f(t)$ *is*

$$f^*(w) = \mathrm{Tr}_n((u(1 + w + w^{2^m}) + u^{2^{n-r}} + w^{2^m})(1 + w + w^{2^m})^{1/(2^r-1)}).$$

Both $f(t)$ *and* $f^*(w)$ *belong to the completed Maiorana-McFarland class,* $f^*(w)$ *does not belong to* $\mathcal{H}$*.*

Niho Binomial with $d = (2^m - 1)3 + 1$ (Subiaco)

Theorem (2012)

Let $n = 2m$, $a = b^{2^m+1}$ and

$$f(t) = \mathrm{Tr}_m(at^{2^m+1}) + \mathrm{Tr}_n(bt^{(2^m-1)3+1}).$$

m odd: *Let $v = 1$ and $u \in \mathbb{F}_4 \setminus \{0,1\}$. Then $F(z) = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu) + a^{\frac{1}{2}} f_s(z)$. If $b = 1$ then*

$$F(z) = \frac{z^2 + z}{(z^2 + z + 1)^2} + z^{1/2}$$

is an o-polynomial (thus $f(t)$ bent).

$m \equiv 2 \pmod 4$: *Let $v = 1$ and $u \in \mathbb{F}_{16} \setminus \mathbb{F}_4$ with $u^5 = 1$ and $u + u^{2^m} = \omega$. Then*

$$F(z) = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (1 + ws + s^{\frac{1}{2}})\mathrm{Tr}_m^n(b(u^4 + 1))f_s(z)$$

*is an o-polynomial (thus $f(t)$ bent) also for b **not** a 5-th power.*

Bent Functions from Quadratic o-Monomials (1)

Take $m > 2$ and $n = 2m$; select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. For any $0 \le J < I < m - 1$ define

$$\begin{aligned} A_1 &= a^{2^I} + 1 \\ A_2 &= a^{2^I} + a^{2^J} \\ A_3 &= a^{2^I} + a^{2^J} + 1 \quad . \end{aligned}$$

and the following Boolean function over $\mathbb{F}_{2^n}$

$$f(t) = \mathrm{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) + \mathrm{Tr}_n\Bigg(\sum_{i=1}^{2^{m-J-1}-1} C_i t^{(2^J i+1)(2^m-1)+1} \Bigg)$$

with coefficients repeated in a cycle of length 2^{c+1} (with $c = I - J$) as follows

$$\underbrace{i}_{C_i\,=} = \underbrace{1, \ldots, 2^c - 1}_{A_1}, \underbrace{2^c}_{A_2}, \underbrace{2^c + 1, \ldots, 2^{c+1} - 1}_{A_1^{2^m}}, \underbrace{2^{c+1}}_{A_3}, \ldots, 2^{m-J-1}$$

Bent Functions from Quadratic o-Monomials (2)

- For odd $m > 3$ take $I = 2$ and $J = 1$

$$F(z) = z^6 + a^6 + (a+1)(a^4 + a^2 + 1)$$

- For $m = 4k - 1 > 3$ take $I = 2k$ and $J = k$

$$F(z) = z^{2^{2k}+2^k} + a^{2^{2k}+2^k} + (a+1)(a^{2^{2k}} + a^{2^k} + 1)$$

- For $m = 4k + 1 > 5$ take $I = 3k + 1$ and $J = 2k + 1$

$$F(z) = z^{2^{3k+1}+2^{2k+1}} + a^{2^{3k+1}+2^{2k+1}} + (a+1)(a^{2^{3k+1}} + a^{2^{2k+1}} + 1)$$

- For $m = 2k - 1 > 3$ take $I = k$ and $J = 1$

$$F(z) = z^{2^k+2} + a^{2^k+2} + (a+1)(a^{2^k} + a^2 + 1)$$

To $F(z) = z^{2^{m-1}+2^{m-2}}$ apply transformation $zF(z^{-1})$ to obtain $z^{2^{m-2}}$ that is a Frobenius o-polynomial if and only if m is odd.

Bent Functions from Cubic o-Polynomials (1)

Take any $m = 2k - 1 > 5$ and $n = 2m$; select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. For any $0 < J + 1 < I < m - 1$ define $e = 2^{I-1}(2^m - 1)$,

$$\begin{aligned} A_1 &= a^{3 \cdot 2^{I-1}} \\ A_2 &= a^{2^I}(a^{2^{I-1}} + a^{2^J}) \\ A_3 &= a^{3 \cdot 2^{I-1} + 2^J} + (a+1)^{3 \cdot 2^{I-1} + 2^J} \quad . \end{aligned}$$

and the following Boolean function over $\mathbb{F}_{2^n}$

$$f(t) = \mathrm{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) + \mathrm{Tr}_n\left(\sum_{i=1}^{2^{m-J-1}-1} C_i t^{(2^J i+1)(2^m-1)+1} \right)$$

with coefficients repeated in a cycle of length 2^{c+1} (with $c = I - J$)

$$\underbrace{i}_{C_i =} = \underbrace{1, \ldots, 2^{c-1} - 1}_{A_1}, \underbrace{2^{c-1}}_{A_2}, \underbrace{2^{c-1} + 1, \ldots, 2^c - 1}_{a^e A_1}, \underbrace{2^c}_{a^e A_2},$$

$$\underbrace{2^c + 1, \ldots, 3 \cdot 2^{c-1} - 1}_{a^{2e} A_1}, \underbrace{3 \cdot 2^{c-1}}_{a^{2e} A_2}, \underbrace{3 \cdot 2^{c-1} + 1, \ldots, 2^{c+1} - 1}_{a^{3e} A_1}, \underbrace{2^{c+1}}_{A_3}, \ldots, 2^{m-J-1}$$

Bent Functions from Cubic o-Polynomials (2)

For $m = 2k - 1 > 5$ take $I = k + 1$ and $J = 2$

$$F(z) = z^{3 \cdot 2^k + 4} + a^{3 \cdot 2^k + 5} + (a + 1)^{3 \cdot 2^k + 5}$$

Take the following o-trinomial of degree three

$$F(z) = z^{2^k} + z^{2^k + 2} + z^{3 \cdot 2^k + 4} \quad \text{with} \quad m = 2k - 1 > 5 \ .$$

For $n = 2m$ select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Take a sum of three Niho bent functions that correspond to each of the following o-monomials

- Frobenius map z^{2^k} (here $r = k - 1$);
- quadratic o-monomial $z^{2^k + 2}$ (here $r = m - 1$);
- cubic o-monomial $z^{3 \cdot 2^k + 4}$ (here $r = m - 2$).

The resulting bent function has the form of LK with $r = m - 1$ and coefficients taking on one of at most ten different values.

Problem

Find explicit expressions for coefficients in any Niho bent function.

General Form of a Niho Bent Function (1)

- For any $d \in \{1, \ldots, 2^m - 1\}$ let $l \in \{0, \ldots, m-1\}$ be the position of the least significant one-digit in the binary expansion of d.
- Take any $\lambda \in \mathbb{F}_{2^m}^*$ and define bivariate function over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$

$$g(x, y) = \mathrm{Tr}_m(\lambda x^{2^m - d} y^d).$$

- Take $t \in \mathbb{F}_{2^n}$ and a a primitive element of $\mathbb{F}_{2^n}$. Use

$$x = t + t^{2^m} \quad \text{and} \quad y = at + a^{2^m} t^{2^m}$$

  to obtain the univariate form of $g(x, y)$.
- For any $d \in \{1, \ldots, 2^m - 1\}$ define

$$\tilde{d} = \begin{cases} d, & \text{if } d < 2^{m-1} \\ d + 2^{m-1}(2^m - 1), & \text{otherwise.} \end{cases}$$

General Form of a Niho Bent Function (2)

This results in

$$\mathrm{Tr}_n\left(a^{\tilde{d}}t^{2^{m-1}(2^m+1)} + \sum_{i=1}^{2^{m-l-1}-1} A_i t^{(2^m-1)(2^l i+1)+1}\right)$$

with $A_i \in \mathbb{F}_{2^n}^*$, plus a linear term. Any Niho bent function in the univariate form, up to EA-equivalence, is obtained as a sum of such functions with $l > 0$ (so $2^l i + 1$ is odd).

Problem (Dobbertin et al. (2006))

Prove that the leading term in a univariate polynomial giving a Niho bent function is always t^{2^m+1} (in particular, show that $\tilde{F}(a) \neq 0$ for any $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$). This would confirm that the only existing monomial Niho bent function is the quadratic one $\mathrm{Tr}_m(at^{2^m+1})$ with $a \in \mathbb{F}_{2^m}^*$.

Function $g(x, y) = \mathrm{Tr}_m(\lambda x^{2^m-d} y^d)$ has algebraic degree $m + wt(d) - wt(d-1) = m - l + 1 \leq m$ since $l > 0$. Therefore, algebraic degree of a Niho bent function is at most m (as for any bent function).

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.

Two hyperovals are equivalent if they are mapped to each other by a collineation (a permutation of the point set of $PG(2, 2^m)$ mapping lines to lines).

Every hyperoval is equivalent to one containing the "Fundamental Quadrangle" (i.e., the points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ and $(1, 1, 1)$).

Hyperovals

A hyperoval of the projective plane $\mathrm{PG}(2, 2^m)$ is a set of $2^m + 2$ points no three of which are collinear.

Two hyperovals are equivalent if they are mapped to each other by a collineation (a permutation of the point set of $\mathrm{PG}(2, 2^m)$ mapping lines to lines).

Every hyperoval is equivalent to one containing the "Fundamental Quadrangle" (i.e., the points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ and $(1, 1, 1)$).

o-Equivalence

If F is an o-polynomial then

$$F'(x) = \big(F(x) + F(0)\big)/\big(F(1) + F(0)\big)$$

satisfies $F'(0) = 0$ and $F'(1) = 1$. The o-polynomials F and F' define EA-equivalent Niho bent functions.

If F is an o-polynomial satisfying $F(0) = 0$ and $F(1) = 1$ then

$$\Omega = \{(x, F(x), 1) | x \in \mathbb{F}_{2^m}\} \cup \{(1, 0, 0), (0, 1, 0)\}$$

is a hyperoval containing the "Fundamental Quadrangle". Every hyperoval containing the "Fundamental Quadrangle" defines an o-polynomial F with $F(0) = 0$ and $F(1) = 1$.

o-polynomials F_1 and F_2 are projectively equivalent if F_1' and F_2' define equivalent hyperovals. Then the Niho bent functions corresponding to F_1 and F_2 are o-equivalent.

o-Equivalence and Symmetric Group S_3

The symmetric group S_3 acts on the projective plane and leaves the set of o-polynomials invariant:

(1) $(x, F(x), 1) \quad \longrightarrow \quad F(x)$;

(2) $(x, 1, F(x)) = 3 \circ 6 \circ 3 \quad \longrightarrow \quad ((F^{-1})')^{-1}(x)$;

(3) $(F(x), x, 1) \quad \longrightarrow \quad F^{-1}(x)$;

(4) $(1, x, F(x)) = 6 \circ 3 \quad \longrightarrow \quad (F^{-1})'(x)$;

(5) $(F(x), 1, x) = 3 \circ 6 \quad \longrightarrow \quad (F')^{-1}(x)$;

(6) $(1, F(x), x) \quad \longrightarrow \quad xF(x^{inv}) = F'(x)$.

Proposition Applying the symmetric group S_3 to an o-polynomial F, one can derive up to three EA-inequivalent Niho bent functions corresponding to F, F^{-1} and $(F')^{-1}$.

There exist o-polynomials where this upper bound is achieved.

S_3 can be extended to a group V of transformations of order 24 which leaves the set of o-polynomials invariant (Cherowitzo 1988). This group can be obtained by applying S_3 to the following 4 transformations:

(a) $(x, F(x), 1)$;

(b) $(x+1, F(x)+1, 1)$ —> $F(x+1)+1$;

(c) $(x, x+F(x), x+1) = 6 \circ b \circ 6$;

(d) $(x+F(x), F(x), F(x)+1) = 3 \circ 6 \circ b \circ 6 \circ 3$.

Theorem The group V gives at most four EA-inequivalent functions. For an o-polynomial F the four potentially EA-inequivalent Niho bent functions correspond to F, F^{-1}, $(F')^{-1}$ and $F^{\circ}(x) = \left(x + xF\left(\frac{x+1}{x}\right)\right)^{-1}$ obtained from F by transformation $5 \circ b$.

There exists an o-polynomial F s.t. F° is EA-inequivalent to F, F^{-1} and $(F')^{-1}$.

Open Problems on o-Equivalence

- Find representations of F^{-1}, $(F')^{-1}$ and F° for all known o-polynomials F (the cases when it is not known).
- In the group of all transformations which leave the set of o-polynomials invariant find all which lead to EA-inequivalent Niho bent functions.