Niho Bent Functions and Hyperovals

Claude Carlet, Tor Helleseth, Alexander Kholosha, Sihem Mesnager

Selmer Center
Department of Informatics
University of Bergen
Norway

10 November 2011

Boolean Functions - Representations

Multivariate representation

A Boolean function $f(x) : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)$ can be represented uniquely in Algebraic Normal Form(ANF)

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

Univariate representation

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

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

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

Bent Functions - Rothaus(1976)

Definition (Walsh transform)

$f(x) : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)$ Inner product $x \cdot b = \sum_{i=1}^{n} x_i b_i (= Tr_n(bx))$

$$\hat{f}(b) = \sum_{x \in \mathrm{GF}(2)^n} (-1)^{f(x)+x\cdot b} \quad (or \sum_{x \in \mathrm{GF}(2^n)} (-1)^{Tr_n(F(x)+bx)})$$

Properties:

$$\begin{aligned} \sum_{b \in \mathrm{GF}(2)^n} (\hat{f}(b))^2 &= \sum_x \sum_y (-1)^{f(x)+f(y)} \sum_b (-1)^{b\cdot(x+y)} \\ &= 2^n \sum_x (-1)^0 = 2^{2n} \end{aligned}$$

- $f(x)$ is a **bent function** iff $\hat{f}(b) = \pm 2^{n/2}$ for all $b \in \mathrm{GF}(2)^n$.
- 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 $\pi : \mathrm{GF}(2)^m \mapsto \mathrm{GF}(2)^m$ be a *permutation*.
Let $g : \mathrm{GF}(2)^m \mapsto \mathrm{GF}(2)$ any mapping.

Then
$$f(x, y) = x \cdot \pi(y) + g(y), \quad x, y \in GF(2)^m.$$
is a bent function in $n = 2m$ variable.

Representation in Bivariate Form

Let $n = 2m$ and consider $GF(2)^n \approx GF(2^m) \times GF(2^m)$.

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

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

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

for some polynomial $P(x,y)$ with coefficients in $GF(2^m)$.

The Walsh transform becomes

$$\hat{f}(a,b) = \sum_{x,y \in GF(2^m)} (-1)^{f(x,y) + Tr_m(ax+by)}, \quad a,b \in GF(2^m).$$

Dillon PS_{ap} Construction

A special case of Dillon' partial spread construction is his PS_{ap} construction

Definition

Let $n = 2m$.

$g : \mathrm{GF}(2^m) \mapsto \mathrm{GF}(2)$, a balanced Boolean function with $g(0) = 0$. Then

$$f(x,y) = g(xy^{2^m-2}) = g(\frac{x}{y}) \quad x, y \in GF(2^m)$$

is bent function.

Dillon's H Class Construction

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

Definition

$$f(x,y) = Tr_m(y + xG(yx^{2^m-2})), \quad x, y \in GF(2^m)$$

where

- $G(x)$ is a permutation of $GF(2)^m$.
- $G(x) + x$ does not vanish.
- $G(x) + \beta x$ has 0 or two solutions for any nonzero $\beta \in GF(2^m)^*$.

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

The extension to Family $\mathcal{H}$

$$g(x,y) = \begin{cases} Tr_m(xH(\frac{y}{x})) & \text{if} \quad x \neq 0 \\ Tr_m(\mu y) & \text{if} \quad x = 0 \end{cases}$$

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

Theorem

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

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

where $N_{\alpha,\beta} = |\{z \in GF(2^m) \mid H(z) + \beta z + \alpha = 0\}|$.

Theorem

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

- $G(z) = H(z) + \mu z$ *is a permutation of* $GF(2^m)$.
- $G(z) + \delta z$ *has 0 or 2 solutions for any* $\delta \in GF(2^m)^*$.

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

Family $\mathcal{H}$:

$$g(x,y) = \begin{cases} Tr_m(xH(\frac{y}{x})) & \text{if} \quad x \neq 0 \\ Tr_m(\mu y) & \text{if} \quad x = 0 \end{cases}$$

Theorem

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

$$g^*(x,y) = \begin{cases} 1 & \text{if } H(z) + \beta z = \alpha \text{ has no solution in } GF(2)^m \\ 0 & \text{otherwise} \end{cases}$$

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

Definition

A permutation polynomial $G(z)$ over $GF(2^m)$ is called an o-polynomial if $G(0) = 0$, $G(1) = 1$ and

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

is a permutation polynomial for all $\gamma \in GF(2^m)$.

Theorem

A polynomial $G(z)$ from $GF(2^m)$ to $GF(2^m)$ is an o-polynomial iff $G(x) + \beta x$ is a 2-1 mapping for any $\beta \in GF(2^m)^*$.

There is a close connection between hyperovals and o-polynomials. Maschietti used monomial hyperovals to construct new important difference sets in (1998).

Monomial o-polynomials

Monomial o-polynomials

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

Example

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

$$g(x, y) = Tr_m(y^6 x^{-5}).$$

Some further o-polynomials

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

For $q = 2^m$, m odd, let $a = 1$

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

For $q = 2^m$, $m \equiv 2 \pmod 4$, 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 $s \in GF(2^m)$.

Binomial bent functions (with Niho exponents)

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

Theorem (Dobbertin et. al. (2006))

If $a = b^{2^m+1}$ *then* $f(x) = Tr_m(ax^{2^m+1}) + Tr_n(bx^{d_2})$ *is bent on* $\mathrm{GF}(2^n)$ *if,*

- $d_2 = (2^m - 1)3 + 1$ *(with the condition that if* $m \equiv 2 \pmod 4$ *then b is a 5-th power of an element in* $\mathrm{GF}(2^n)$*).*
- $4d_2 = (2^m - 1) + 4$ *and m odd.*
- $6d_2 = (2^m - 1) + 6$*, and m even.*

Theorem (Leander and Kholosha (2006))

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

$$f(x) = Tr_m(x^{2^m+1}) + Tr_n\Big(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{1}{2^r}+1}\Big)$$

is a bent function (generalizing the second construction above).

Niho Bent Functions in 2-variables

Niho bent function in univariate form, $t \in GF(2^n)$, $n = 2m$,

$$f(t) = Tr_n(\sum_i \alpha_i t^{(2^m-1)s_i+1})$$

Niho bent function in bivariate form ($x, y \in GF(2^m)$)

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

$$g(x,y) = \begin{cases} Tr_m(xH(\frac{y}{x})) & \text{if } x \neq 0 \\ Tr_m(\mu y) & \text{if } x = 0. \end{cases}$$

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

Niho exponent $d = (2^m - 1)\frac{1}{4} + 1$ and generalizations

Theorem (Carlet, Helleseth, Kholosha, Mesnager (2011))

Let $r > 1$, $\gcd(r, m) = 1$, $a + a^{2^m} = 1$ and

$$f(t) = Tr_n(at^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{(2^m-1)\frac{1}{2^r}+1}).$$

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

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

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

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

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

Niho exponent $d = (2^m - 1)3 + 1$

Theorem (Helleseth, Kholosha, Mesnager (2011))

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

$$f(t) = Tr_m(at^{2^m+1}) + Tr_n(bt^{(2^m-1)3+1}).$$

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

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

is an o-polynomial (thus $f(t)$ bent).
m $\equiv$ 2 (mod 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*

$$G(z) = a^{\frac{1}{2}} + Tr_m^n(b) + (1 + ws + s^{\frac{1}{2}})Tr_m^n(b(u^4 + 1))f_s(z)$$

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