Hyperovals and bent functions

Kanat Abdukhalikov

Dept of Mathematical Sciences, UAEU
and
Institute of Mathematics, Kazakhstan

Finite Geometries
The 5th Irsee Conference
September 10-16, 2017
Germany

Outline

- Bent functions
- Spreads, ovals and line ovals
- Bent functions and ovals / line ovals
- Automorphism groups

Bent functions

A Boolean function:
$f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$

Bent function: Boolean function at maximal possible distance from affine functions

Bent function: Boolean function whose support is a Hadamard Difference Set

Bent function: Matrix $[(-1)^{f(x+y)}]_{x,y \in \mathbb{F}_{2^n}}$ is Hadamard

Bent functions exist only for even n

Bent functions

A Boolean function: $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$

Walsh transform of f : $W_f(u) = \sum_{x \in F} (-1)^{f(x)+u \cdot x}$

(Discrete Fourier Transform)

Definition

A Boolean function f on $\mathbb{F}_{2^n}$ is said to be bent if its Walsh transform satisfies $W_f(u) = \pm 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$.

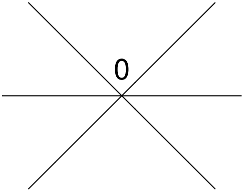
dual function $\tilde{f}$: $W_f(u) = 2^{n/2} \, (-1)^{\tilde{f}(u)}$

The dual of a bent function is bent again, and $\tilde{\tilde{f}} = f$.

Desarguesian Spreads

$F = \mathbb{F}_q$, $q = 2^m$

Desarguesian spread of $V = F \times F$ is the family of all 1-subspaces over F.



There are $q + 1$ subspaces and every nonzero point of V lies in a unique subspace.

Niho bent functions: bent functions that are linear (over $\mathbb{F}_2$) on the elements of the Desarguesian spread

Ovals

An oval in affine plane $AG(2, q)$ is a set of $q + 1$ points, no three of which are collinear.

Hyperoval: set of $q + 2$ points, no three of which are collinear.

For any oval there is a unique point (called nucleus) that completes oval to hyperoval
(in general, nucleus is in projective plane $PG(2, q)$)

Dually, a line oval in affine plane $AG(2, q)$ is a set of $q + 1$ nonparallel lines no three of which are concurrent.

Niho bent functions

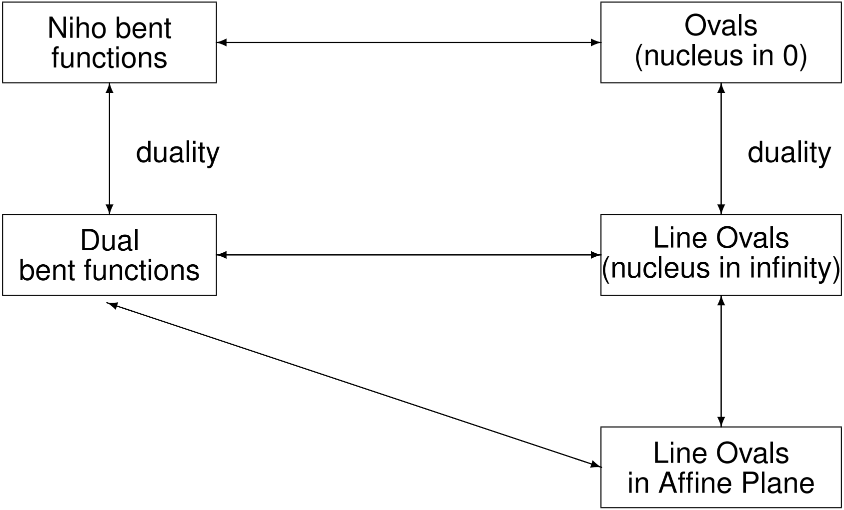
Dillon (1974)

Dobbertin-Leander-Canteaut-Carlet-Felke-Gaborit-Kholosha (2006).

Carlet-Mesnager (2011):
Niho bent function $\rightarrow$ o-polynomial $\rightarrow$ hyperoval

Penttila-Budaghyan-Carlet-Helleseth-Kholosha (unpublished - Irsee 2014):
Niho bent functions are equivalent $\Leftrightarrow$ corresponding ovals are projectively equivalent

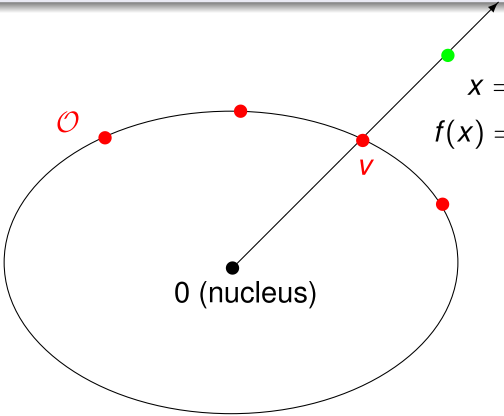
Map of Connections



Bent functions and ovals

Theorem

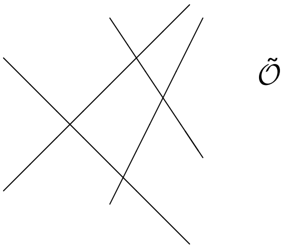
There is one-to-one correspondence between Niho bent functions and ovals $\mathcal{O}$ (with nucleus in 0) in the projective plane $PG(2, q)$.



$$x = \lambda v, \ \lambda \in F$$

$$f(x) = tr(\lambda) = tr(\tfrac{x}{v})$$

Niho bent function $f \to$ Oval $\mathcal{O} \to$ Line oval $\tilde{\mathcal{O}}$



$$\tilde{f}(x) = 0 \Leftrightarrow x \in E(\tilde{\mathcal{O}})$$

where $E(\tilde{\mathcal{O}})$ is the set of points which are on the lines of the line oval $\tilde{\mathcal{O}}$.

Polar coordinate representation

K/F field extension of degree 2, $K = \mathbb{F}_{2^n}$, $F = \mathbb{F}_{2^m}$, $n = 2m$.

Consider K as $AG(2, q)$, $q = 2^m$.
The *conjugate* of $x \in K$ over F is

$$\bar{x} = x^q.$$

Norm and *Trace* maps from K to F are

$$N(x) = x\bar{x}, \quad T = x + \bar{x}.$$

The unit circle of K is the set of elements of norm 1:

$$S = \{u \in K : N(x) = 1\}.$$

S is the multiplicative group of $(q+1)$st roots of unity in K.
Each element of K^* has a unique representation

$$x = \lambda u$$

with $\lambda \in F^*$ and $u \in S$ (polar coordinate representation).

Niho bent functions

Consider $K = \mathbb{F}_{2^n}$ as two dimensional vector space over F. Then the set

$$\{uF : u \in S\}$$

is a Desarguesian spread.

Niho bent functions:

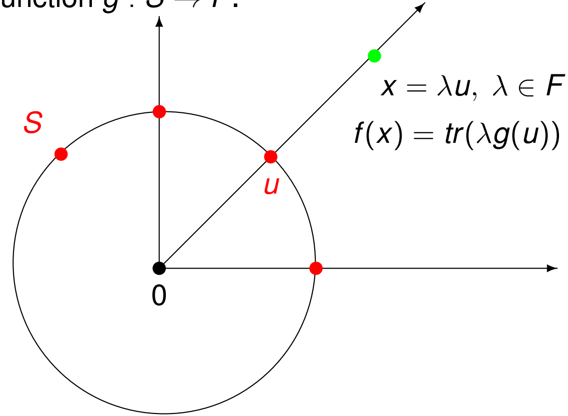
Boolean functions $f : K \to \mathbb{F}_2$, which are $\mathbb{F}_2$-linear on each element uF of the spread.

Niho bent functions

Niho bent function $f : K \to \mathbb{F}_2$ can be represented as

$$f(\lambda u) = tr(\lambda g(u))$$

for some function $g : S \to F$.



From bent functions to ovals and line ovals

Let $f : K \to \mathbb{F}_2$ be a Niho bent function such that

$$f(\lambda u) = tr(\lambda g(u))$$

for some function $g : S \to F$.

Theorem

The set $\left\{ \frac{u}{g(u)} \; : \; u \in S \right\}$ *forms an oval with nucleus in* 0.

Theorem

Lines with equations $u\overline{x} + \overline{u}x + g(u) = 0$, *where* $u \in S$, *forms a line oval in* K.

Dual functions

Let $f : K \to \mathbb{F}_2$ be a Niho bent function such that

$$f(\lambda u) = tr(\lambda g(u))$$

for some function $g : S \to F$.

Then the dual function for f is

$$\tilde{f}(x) = \prod_{u \in S} (u\overline{x} + \overline{u}x + g(u))^{q-1}.$$

Criteria for functions $g(u)$

Theorem

Let $f(\lambda u) = tr(\lambda g(u))$ for some function $g : S \to F$. Then the following statements are equivalent:

1. *The function f is bent;*
2. *Equation $g(u) + u\overline{b} + \overline{u}b = 0$ has 2 or 0 solutions for any $b \in K$;*
3. *$T(x/y) \cdot g(z) + T(z/x) \cdot g(y) + T(y/z) \cdot g(x) \neq 0$ for all distinct $x, y, z \in S$.*
4. *$(x^2 + y^2)z \cdot g(z) + (x^2 + z^2)y \cdot g(y) + (y^2 + z^2)x \cdot g(x) \neq 0$ for all distinct $x, y, z \in S$.*

O-polynomials

O-polynomial $h(t)$:

$$\{(t, h(t), 1) \mid t \in \mathbb{F}_{2^m}\} \cup (1, 0, 0) \cup (0, 1, 0)$$

is a hyperoval in $PG(2, 2^m)$

O-polynomials

W. Cherowitzo, Hyperoval webpage,
http://math.ucdenver.edu/∼wcherowi/research/hyperoval/hypero.html

Some known o-polynomials $h(t)$

1) $h(t) = t^{2^i}$, where $\gcd(i, m) = 1$.
2) $h(t) = t^6$, where m is odd (Segre 1962).
3) $h(t) = t^{2^k+2^{2k}}$, where $m = 4k - 1$ (Glynn 1983)
3') $h(t) = t^{2^{2k+1}+2^{3k+1}}$, where $m = 4k + 1$ (Glynn 1983)
4) $h(t) = t^{3 \cdot 2^k+4}$, where $m = 2k - 1$ (Glynn 1983).
5) $h(t) = t^{1/6} + t^{1/2} + t^{5/6}$, where m is odd (Payne).
6) $h(t) = t^{2^k} + t^{2^k+2} + t^{3 \cdot 2^k+4}$, where $m = 2k - 1$ (Cherowitzo).

O-polynomials

7) Adelaide o-polynomials

$$h(t) = \frac{T(b^k)}{T(b)}(t+1) + \frac{T((bt+b^q)^k)}{T(b)}(t+T(b)t^{1/2}+1)^{1-k} + t^{1/2},$$

where m even, $b \in S$, $b \neq 1$ and $k = \pm\frac{q-1}{3}$.

8) Subiaco o-polynomials

$$h(t) = \frac{d^2t^4 + d^2(1+d+d^2)t^3 + d^2(1+d+d^2)t^2 + d^2t}{(t^2+dt+1)^2} + t^{1/2}$$

where $d \in F$, $tr(1/d) = 1$, and $d \notin \mathbb{F}_4$ for $m \equiv 2 \pmod 4$. This o-polynomial gives rise to two inequivalent hyperovals when $m \equiv 2 \pmod 4$ and to a unique hyperoval when $m \not\equiv 2 \pmod 4$.

Niho bent functions

Dobbertin-Leander-Canteaut-Carlet-Felke-Gaborit-Kholosha (2006) :
Examples of Niho bent functions of the form $Tr(ax^{d_1} + x^{d_2})$

Correspond to Translation, Adelaide and Subiaco hyperovals

Adelaide hyperovals

$$g(u) = 1 + u^{(q-1)/3} + \bar{u}^{(q-1)/3}$$

Adelaide hyperoval in K:

$$\left\{ \frac{u}{1 + u^{(q-1)/3} + \bar{u}^{(q-1)/3}} \ : \ u \in S \right\} \cup \{0\}$$

Automorphism group: $Gal(K/\mathbb{F}_2)$

Subiaco hyperovals

$$
\begin{aligned}
g(u) &= 1 + u^5 + \bar{u}^5, \\
g_1(u) &= 1 + \theta u^5 + \bar{\theta}\bar{u}^5 \quad (\text{for } m \equiv 2 \pmod 4),
\end{aligned}
$$

where $\langle \theta \rangle = S$.

Subiaco hyperovals:

$$\left\{ \frac{u}{1 + u^5 + \bar{u}^5} : \ u \in S \right\} \cup \{0\},$$

$$\left\{ \frac{u}{1 + \theta u^5 + \bar{\theta}\bar{u}^5} : \ u \in S \right\} \cup \{0\}$$

Subiaco hyperovals

a) Let $m \not\equiv 2 \pmod 4$ and Subiaco hyperoval given by

$$g(u) = 1 + u^5 + \bar{u}^5.$$

Then automorphism group has order n and equal to $Gal(K/\mathbb{F}_2)$.

b) Let $m \equiv 2 \pmod 4$ and Subiaco hyperoval given by

$$g(u) = 1 + u^5 + \bar{u}^5.$$

Then automorphism group has order $5n$ and is equal to $\langle\varphi\rangle \cdot Gal(K/\mathbb{F}_2)$, where φ is a rotation of order 5.

c) Let $m \equiv 2 \pmod 4$ and Subiaco hyperoval given by

$$g(u) = 1 + \theta u^5 + \bar{\theta}\bar{u}^5.$$

Then its automorphism has order $5n/4$ and is isomorphic to $\langle\varphi\rangle\langle\sigma^4\rangle$, where φ is a rotation of order 5.

Odd characteristics

Çeşmelioğlu-Meidl-Pott (2015)

No analogs in odd characteristic

Bent Function Linear on Spreads

Theorem

Let Q be a quasifield, $\Sigma(Q)$ be its associated spread, and Q^t be the transpose quasifield of Q. Then bent functions $f(x,y)$ which are linear on elements of the spread $\Sigma(Q)$, are in one-to-one correspondence with line ovals $\mathcal{O}$ in $\mathcal{A}(Q^t)$.
The zeroes of the dual function $\tilde{f}(x,y)$ are exactly the points of the line oval $\mathcal{O}$.

Thank you for your attention!