Duality of bent functions in odd characteristic

Alexander Pott

based on work with Ayça Çeşmelioğlu and Wilfried Meidl

July 2017

Outline

- p-ary bent functions.
- Duality of p-ary regular bent functions.
- Duality of p-ary bent function in the non-regular case.
- Vectorial dual.
- Bent functions and difference sets.

p-ary bent functions

Definition

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is p-ary bent if

$$\left| \sum_{x \in \mathbb{F}_p^n} \zeta_p^{\langle a,x \rangle + f(x)} \right|^2 = p^n$$

for all $a \in \mathbb{F}_p^n$.

As usual, $\zeta_p = e^{2\pi i/p}$ is a complex p-th root of unity, and $\langle a, x \rangle$ is a non-degenerate bilinear form.

If $p = 2$, these are the classical bent functions.

Quadratic examples if p is odd

$$f(x) = x^T \mathbf{A} x$$

where $\mathbf{A} \in \mathbb{F}_p^{(n,n)}$ is a non-singular symmetric matrix.
Without loss of generality

$$f(x_1, \ldots, x_n) = x_1^2 + x_2^2 + \cdots + d \cdot x_n^2$$

where $d \neq 0$.

Note: n can be odd.

Proof

One can proof this directly, or use

Observation

f is bent if and only if

$$x \mapsto f(x+a) - f(x) \quad \textit{is balanced}$$

for all $a \in \mathbb{F}_p^n$, $a \neq 0$:

$$(x+a)^T \mathbf{A}(x+a) - x^T \mathbf{A} x = 2x^T \mathbf{A} a + a^T \mathbf{A} a = b$$

has precisely p^{n-1} solutions for all b and all $a \neq 0$.

p odd: The number theory

Walsh coefficients $\widehat{f}(a) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{\langle a,x \rangle + f(x)} \in \mathbb{Z}[\zeta_p]$

If p is even, there are 2 possibilities.

If p is odd, there are $2p$ possibilities (Helleseth, Kholosha (2006)):

- $p^n \equiv 1 \bmod 4$: Walsh coefficients $\pm\zeta_p^j p^{n/2}$
- $p^n \equiv 3 \bmod 4$: Walsh coefficients $\pm i\zeta_p^j p^{n/2}$

Definition (Kumar, Scholtz, Welch (1985))

Regular: $\widehat{f}(a) = \omega\zeta_p^{f^*(a)} p^{n/2}$ for all a for some fixed element ω: Then f^* is called the **dual** of f.

Theorem (Kumar, Scholtz, Welch (1985))

f^* is bent if f is regular.

Maiorana-McFarland construction $\mathbb{F}_p^{2m} \to \mathbb{F}_p$

Theorem

$$f(x, y) = Trace(x \cdot \pi(y)) + \rho(y)$$

is bent if $\pi : \mathbb{F}_p^m \to \mathbb{F}_p^m$ *is a permutation and* $\rho : \mathbb{F}_p^m \to \mathbb{F}_p$.

Alternative:

$$f(x, y) = f_y(x) + \rho(y)$$

where $f_y : \mathbb{F}_p^m \to \mathbb{F}_p$ is linear and $f_y \neq f_{y'}$ if $y \neq y'$.

Alternative:

$$f(x, y) = g_y(x)$$

where g_y are affine and the supports of the Walsh spectra are disjoint.

Generalized Maiorana-McFarland construction

Let $g_y : \mathbb{F}_p^m \to \mathbb{F}_p$ be a collection of p^s functions such that the supports of the Walsh spectra are disjoint. If the functions are p^s-plateuead, (that is Walsh spectrum takes values 0 and $\pm p^{(m+s)/2}$) then $f : \mathbb{F}_p^m \times \mathbb{F}_p^s \to \mathbb{F}_p$ with

$$f(x, y) = g_y(x)$$

is p-ary bent.

Example

If f bent on $\mathbb{F}_p^k$, then the mappings

$$g_y(x', x'') = f(x') + \langle y, x'' \rangle$$

do the job ($x' \in \mathbb{F}_p^k$, $x'', y \in \mathbb{F}_p^s$).

Comments

Observation

The Maiorana-McFarland construction as well as all quadratic examples give regular bent functions.

Theorem (Ceşmelioğlu, McGuire, Meidl (2012))

The (non-regular) generalized Maiorana-McFarland construction gives regular and non-regular bent functions ($s \neq m$).

See also Davis, Jedwab (1997).

Non-regular bent functions and their duals

Walsh spectrum has $2p$ values $\pm\omega\zeta_p^i p^{n/2}$. We can define a dual even if the spectrum takes $2p$ values!!

Theorem

The duals of the generalized Maiorana-McFarland construction are bent if the g_y are regular.

Two more families $p = 3$

Theorem (Helleseth, Kholosha (2006), Helleseth, Hollmann, Kholosha, Wang, Xiang (2009))

The following two families of bent functions are regular:

- $n = 2k$, k *odd*, α *element of order* $4(3^k - 1)$*:*

$$Trace\left(\alpha x^{\frac{3^n-1}{4}+3^k+1}\right)$$

- Coulter, Matthews (1997)

$$Trace\left(\left(\alpha x^{\frac{3^i+1}{2}}\right)\right), \quad \gcd(i, n) = 1, \quad 3 \leq i \leq n \text{ odd}$$

Heavy proofs!

Questions

What is special about these functions that is so difficult to prove regularity.

Theorem

The two families are not in the generalised Maiorana-McFarland family.

Note: The Coulter-Matthews example is actually a component of a planar function!

Dual of diagonal quadratic function

Theorem

If

$$f(x) = d_1 x_1^2 + d_2 x_2^2 + \ldots + d_n x_n^2$$

then the dual is

$$f^*(x) = -\frac{x_1^2}{4d_1} - \frac{x_2^2}{4d_2} - \ldots - \frac{x_n^2}{4d_n}$$

Dual of Maiorana-McFarland

Theorem

Let

$$f(x, y) = Trace(x \cdot \pi(y))$$

then

$$f^*(x, y) = Trace(-y \cdot \pi^{-1}(x)) + \rho(\pi^{-1}(y))$$

where $x, y \in \mathbb{F}_{p^m}$, π *permutation*, ρ *arbitrary.*

The role of the inner product

Note that the dual function depends on the choice of the bilinear form. In the Maiorana-McFarland case, we choose

$$\mathrm{Trace}(x \cdot x' + y \cdot y')$$

on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Having a dual does not depend on the choice of the inner product, but self-duality does.

Spreads

$V = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $U_0, U_1, \ldots, U_{p^m}$ subspaces of dimension m with pairwise trivial intersection. Let $i \to \gamma_i$ be a balanced function from $\{1, 2, \ldots, p^m\}$ to $\{1, \ldots, p\}$. Then

$$f(z) = \begin{cases} \gamma_i & \text{if } z \in U_i, z \neq 0, \quad 1 \leq i \leq p^m \\ \gamma_0 & \text{if } z \in U_0. \end{cases}$$

is bent.

Theorem

$$f^*(z) = \begin{cases} \gamma_i & z \in U_i^{\perp}, z \neq 0, \quad 1 \leq i \leq p^m \\ \gamma_0 & \text{if } z \in U_0^{\perp}. \end{cases}$$

Self-duality

Theorem

There are no regular self-dual bent functions if $p^n \equiv 3 \ mod \ 4$.

Theorem

There are quadratic self-dual bent functions with respect to the classical inner product if there is a symmetrix matrix $\mathbf{A}$ *such that* $\mathbf{A}^2 = \frac{-1}{4}\mathbf{I}$. *Easy if* $p \equiv 1 \ mod \ 4$. *We can use these recursively to find self-dual bent functions of large degree.*

More examples

Theorem

Let f be a partial spread bent function for a symplectic spread with respect to an alternating bilinear form $\langle\ ,\ \rangle$. Then f is self-dual with respect to that bilinear form.

Theorem (Helleseth, Kholosha (2006))

Let $n = 2k$ and t be a positive integer satisfying $\gcd(t, 3^k + 1) = 1$. Then the function $f(x) = Trace(ax^{t(3^k-1)})$ from $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$ is bent if and only if $K_k(a^{3^k+1}) = -1$. If $K_k(a^{3^k+1}) = -1$ then $f(x)$ is regular bent and $\widehat{f}(b) = 3^k\zeta^{-Trace(a^{3^k}b^{t(3^k-1)})}$.

Observation

For $k = 3, 5, 7$ there exist self-dual bent functions of that type. with respect to the trace bilinear form.

Further non-regular examples

The following functions are not regular:

- $g_1 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_1(x) = \mathrm{Trace}(\xi^7 x^{98})$, where ξ is a primitive element of $\mathbb{F}_{3^6}$.
- $g_2 : \mathbb{F}_{3^4} \to \mathbb{F}_3$ with $g_2(x) = \mathrm{Trace}(\alpha_0 x^{22} + x^4)$, where $\alpha_0 \in \{\pm\xi^{10}, \pm\xi^{30}\}$ and ξ is a primitive element of $\mathbb{F}_{3^4}$.
- $g_3 : \mathbb{F}_{3^3} \to \mathbb{F}_3$ with $g_3(x) = \mathrm{Trace}(x^{22} + x^8)$.
- $g_4, g_5 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_4(x) = \mathrm{Trace}(\xi x^{20} + \xi^{41} x^{92}), g_5(x) = \mathrm{Trace}(\xi^7 x^{14} + \xi^{35} x^{70})$, where ξ is a primitive element of $\mathbb{F}_{3^6}$.

Helleseth, Kholosha (2006, 2010), Tan, Yang, Zhang (2010).

Observation

g_3 and g_4 have a bent dual, the others not. g_3 is generalized McFarland, g_1 not.

Infinite family of bent functions without a dual

Let $1, \alpha, \beta \in \mathbb{F}_{p^m}$ be linearly independent over $\mathbb{F}_p$. If

$$\left| \sum_{y_1, y_2 \in \mathbb{F}_p} \eta(1 + y_1\alpha + y_2\beta)\epsilon_p^{-y_1 y_2} \right| \neq p,$$

then the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_p^2 \to \mathbb{F}_p$

$$F(x, y_1, y_2) = \mathrm{Trace}(x^2) + (y_1 + \mathrm{Trace}(\alpha x^2))(y_2 + \mathrm{Trace}(\beta x^2))$$

is a bent function without a dual.

Recursive Construction

Theorem

If g is bent and h is bent without a dual, then $f(x, y) = g(x) + h(y)$ has no dual ($g : \mathbb{F}_p^m \to \mathbb{F}_p, h : \mathbb{F}_p^n \to \mathbb{F}_p$).

We have a second recursive construction.

Question

Find more functions for which the dual is not bent.

Vectorial bent functions

Most constructions of bent functions are "vectorial" constructions.

Definition

A function $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is vectorial bent if all component functions $x \mapsto \langle a, F(x) \rangle$ are bent. If $m = n$: Planar functions.

Example

$F(x, y) = x \cdot y$ as a mapping $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$.

Other example: Coulter-Matthews.

Question

Is there a duality concept for such vectorial functions?

Problem

Even if the sum of two bent functions is bent, this is not necessarily true for the duals.

Vectorial dual

Definition

A vectorial bent function has a dual if the set of dual functions form a vector space of bent functions.

Example

$F(x) = x^2$ on $\mathbb{F}_{p^m}$. The dual of $\mathrm{Trace}(ax^2)$ is $\mathrm{Trace}(-\frac{x^2}{4a})$. Hence if we look at the function $\mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, the function has a dual, but there are sub-vectorial functions $\mathbb{F}_{p^m} \to \mathbb{F}_p^2$ without a dual: The set

$$\{\frac{1}{\lambda a + \mu b} \ : \ \lambda, \mu \in \mathbb{F}_p\}$$

do not form a vector space.

In general, the duals of planar functions are not planar.

Example of a vectorial dual bent function

Theorem

The vectorial versions $F : \mathbb{F}_p^{2m} \to \mathbb{F}_p^m$ of the spread functions have a vectorial dual which is the same as the original function with respect to the alternating bilinear form (self-dual).

Question

Are there examples besides x^2 of planar functions whose dual functions also form a planar function?

$p = 2$: Difference sets

Observation

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent if and only if

$$D_f := \{x \in \mathbb{F}_2^n \ : \ f(x) = 1\}$$

is a (non-trivial) difference set in $\mathbb{F}_2^n$:

A subset $D \subset G$ of a group G is a **difference set** if any non-zero element $g \in G$ has a constant number of representations $g = d - d'$ with $d, d' \in D$.

Non-trivial: $2 \leq |D| \leq |G| - 2$.

$p = 2$: Equivalence

Two difference sets D and D' are **equivalent** if there is a group automorphism φ such that $\varphi(D) = D' + g = \{d + g \ : \ d \in D'\}$.

Strange Observation

Equivalent bent functions may give rise to inequivalent difference sets.

Reason: Adding linear functions

$p = 2$: Relative difference sets are the better objects

Definition

A subset $R \subset G$ of a group G is a **relative difference set** with respect to $N \leq G$ if all $g \in G \setminus N$ have a constant number of representations $g = d - d'$ with $d, d' \in R$, and no non-zero element in N has such a representation.

Observation

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent if and only if

$$R_f := \{(x, f(x)) \, : \, x \in \mathbb{F}_2^n\}$$

is a relative difference set in $\mathbb{F}_2^n \times \mathbb{F}_2$ relative to $\{0\} \times \mathbb{F}_2$.

Example and Observation

Example

$$\{(0,0,1),(0,1,0),(1,0,0),(1,1,0)\}$$

is a relative difference set in $\mathbb{F}_2^3$ with respect to $\{(0,0,0),(0,0,1)\}$.

Observation

f and g are equivalent bent functions if and only if R_f and R_g are equivalent.

Difference sets and incidence structures

If R is a difference set, the **development** of R is an incidence structure:

- Points: Elements in G.
- Blocks: Translates $R + g = \{r + g \ : \ r \in R\}$.

These are incidence structures with G as (regular) automorphism group and vice versa.

Observation

Equivalence of difference sets implies isomorphisms of incidence structures, but not vice versa, so it is possible that one incidence structure gives rise to several bent functions.

Difference set interpretation of dual

Vectorial bent functions also correspond to relative difference sets.

Is there an interpretation of having a dual in terms of the relative difference set?

Summary

- p-ary bent functions.
- Duality concept: The regular case.
- Duality concept: The non-regular case.
- Vectorial duality.
- Connection to difference sets?